kaspersky

Kaspersky Endpoint Security 14.2 for Windows

© 2026 AO Kaspersky Lab

İçindekiler

Kaspersky Endpoint Security for Windows Yardım
- Yenilikler
- Düzeltilen sorunlar
- Sıkça sorulan sorular

Kaspersky Endpoint Security for Windows
- Uygulama modları: Standart, EDR Agent, Light Agent
- Dağıtım kiti
- Donanım ve yazılım gereksinimleri
- İşletim sistemi türüne göre kullanılabilir uygulama özellikleri karşılaştırması
- Yönetim araçlarına bağlı olarak uygulama işlevlerinin karşılaştırılması
- Diğer uygulamalarla uyumluluk

Uygulamayı yükleme ve kaldırma
- Kaspersky Security Center vasıtasıyla dağıtım
  - Uygulamanın standart kurulumu
  - Kurulum paketi oluşturma
  - Kurulum paketindeki veritabanlarının güncellenmesi
  - Uzaktan kurulum görevi oluşturma
- Sihirbazı kullanarak uygulamayı yerel olarak yükleme
- Sistem Merkezi Yapılandırma Yöneticisi'ni kullanarak uygulamayı uzaktan yükleme
- setup.ini dosyası yükleme ayarlarının açıklaması
- Kaspersky Endpoint Security for Windows işlemleri
- Uygulama bileşenlerini değiştirme
- Uygulamanın önceki bir sürümünü yükseltme
  - Uygulamayı yeniden başlatma olmadan yükseltme
  - Uygulamanın SMU güncellemesi
- Uygulamayı kaldırma

Uygulama lisanslama
- Son Kullanıcı Lisans Sözleşmesi Hakkında
- Lisans hakkında
- Lisans sertifikası hakkında
- Abonelik hakkında
- Lisans anahtarı hakkında
- Etkinleştirme kodu hakkında
- Anahtar dosyası hakkında
- İş istasyonları için lisans türüne göre uygulama işlevselliği karşılaştırılması
- Sunucular için lisans türüne göre uygulama işlevselliği karşılaştırılması
- Uygulamayı etkinleştirme
- Bir lisans anahtarını kaldırma
- Lisans bilgilerini görüntüleme
- Lisans satın alma
- Aboneliği yenileme

Başlarken
Kaspersky Endpoint Security for Windows Yönetim Eklentisi Hakkında
Yönetim eklentilerinin farklı sürümleriyle çalışırken dikkat edilmesi gereken hususlar
Harici hizmetlerle etkileşim için şifrelenmiş iletişim kurallarını kullanırken özel hususlar
Uygulama arabirimi
Görev çubuğu bildirim alanındaki uygulama simgesi
Basitleştirilmiş uygulama arabirimi
Uygulama arabirim ekranını yapılandırma
Uygulamanın kullanıma hazırlanması
İlkeleri yönetme
İlke oluşturma
Bir ilkeyi dışa aktarma ve içe aktarma
Güvenlik düzeyi göstergesi
Görev yönetimi
Yerel uygulama ayarlarını yapılandırma
Kaspersky Endpoint Security'yi başlatma ve durdurma
Bilgisayar korumasını ve denetimini duraklatma ve sürdürme
Yapılandırma dosyası oluşturma ve kullanma
Varsayılan uygulama ayarlarını geri yükleme
Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu
Enerji tasarrufu modunu etkinleştirme veya devre dışı bırakma
Diğer uygulamalar için kaynak yaratmayı etkinleştirme veya devre dışı bırakma
Kaspersky Endpoint Security performansını optimize etmek için en iyi uygulamalar
Kötü Amaçlı Yazılım Taraması
Bilgisayarı tarama
Bilgisayara bağlandığında çıkarılabilir sürücüleri tarama
Arka plan taraması
Bağlam menüsünden tarama
Uygulama Bütünlüğü Kontrolü
Tarama kapsamının düzenlenmesi
Zamanlanmış bir tarama çalıştırma
Taramayı farklı bir kullanıcı olarak çalıştırma
Tarama optimizasyonu
Veritabanlarını ve uygulama yazılım modüllerini güncelleme
Veritabanı ve uygulama modülü güncelleme senaryoları
Bir sunucu veri havuzu üzerinden güncelleme
Bir paylaşım klasörü üzerinden güncelleme
Kaspersky Update Utility aracıyla güncelleme
Mobil modda güncelleme
Güncelleme görevini başlatma veya durdurma
Farklı bir kullanıcı hesabının hakları altında bir güncelleme görevi başlatma
Güncelleme görevinin çalışma modunu seçme
Güncelleme kaynağı ekleme
Uygulama modüllerini güncelleme
Güncellemeler için proxy sunucusu kullanma
Son güncellemeyi geri alma

Gelişmiş temizleme teknolojisi
İş istasyonlarındaki etkin tehditlerin temizlenmesi
Sunuculardaki etkin tehditlerin temizlenmesi
İşlenmemiş tehditleri ortadan kaldırma
Bilgisayar koruması
Gerçek Zamanlı Koruma durumu
Dosya Tehdidi Koruması
Dosya Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma
Dosya Tehdidi Koruması'nı otomatik olarak duraklatma
Dosya Tehdidi Koruması bileşeni tarafından virüslü dosyalara uygulanacak eylemi değiştirme
Dosya Tehdidi Koruması bileşeninin koruma kapsamını oluşturma
Tarama yöntemlerini kullanma
Dosya Tehdidi Koruması bileşeninin çalışması sırasında tarama teknolojilerini kullanma
Dosya taramasını optimize etme
Birleşik dosyaları tarama
Tarama modunu değiştirme
Kapsayıcı Taraması
Sunucu Yetkisiz Erişim Önleme
Sunucu Yetkisiz Erişim Önleme'yi etkinleştirme ve devre dışı bırakma
Uygulama güven gruplarını yönetme
Bir uygulamanın güvenilirlik grubunu değiştirme
Güvenilirlik grubu haklarını yapılandırma
Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güven grubu seçme
Bilinmeyen uygulamalar için bir güvenilirlik grubu seçme
Dijital olarak imzalanmış uygulamalar için bir güvenilirlik grubu seçme
Uygulama haklarını yönetme
İşletim sistemi kaynaklarını ve kişisel verileri koruma
Kullanılmayan uygulamalar hakkında bilgileri silme
Sunucu Yetkisiz Erişim Önleme izlemesi
Ses ve videoya erişimi koruma
BadUSB Saldırısı Önleme
BadUSB Saldırısı Önleme'yi Etkinleştirme ve Devre Dışı Bırakma
USB aygıtlarının kimlik doğrulaması için Ekran Klavyesinin kullanımı
Barkod tarayıcı yetkilendirmesi
AMSI Koruması
AMSI Korumasını etkinleştirme ve devre dışı bırakma
AMSI Koruması tarafından dosya taramasını optimize etme
Web Tehdidi Koruması
Web Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma
Kötü amaçlı web adresi tespit yöntemlerini yapılandırma
Kimlik Avı Koruması
Güvenilir internet adreslerinin listesini oluşturma
Güvenilir internet adresleri listesini dışa ve içe aktarma
Posta Tehdidi Koruması
Posta Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma
Virüslü e-posta mesajlarına uygulanacak eylemi değiştirme
Posta Tehdidi Koruması bileşeninin koruma kapsamını oluşturma

E-posta mesajlarına eklenen birleşik dosyaları tarama
E-posta mesajları ek filtrelemesi
Ek filtreleme için uzantıları dışa ve içe aktarma
Microsoft Office Outlook'ta e-postaları tarama
Thunderbird, MyOffice ve R7-Office'te e-postalarını tarama
Ağ Tehdidi Koruması
Ağ Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma
Saldırıda bulunan bir bilgisayarı engellemek
Engelleme istisnalarının adreslerini yapılandırma
İstisnalar listesini dışa ve içe aktarma
Ağ Tehdit Korumasını türe göre yapılandırma
Güvenlik Duvarı
Güvenlik Duvarı'nın etkinleştirilmesi veya devre dışı bırakılması
Ağ bağlantısı türünü değiştirme
Ağ paketi kurallarını yönetme
Bir ağ paketi kuralını kaldırma
Ağ paketi kuralını etkinleştirme veya devre dışı bırakma
Ağ paketi kuralı için Güvenlik Duvarı eylemini değiştirme
Ağ paketi kuralının önceliğini değiştirme
Ağ paketi kurallarını dışa ve içe aktarma
XML'de ağ paketi kurallarını tanımlama
Uygulama ağ kurallarını yönetme
Bir uygulama ağ kuralı oluşturma
Uygulama ağ kuralını etkinleştirme veya devre dışı bırakma
Ağ kuralı için Güvenlik Duvarı eylemini değiştirme
Ağ kuralının önceliğini değiştirme
Ağ İzleyicisi
Exploit Önleme
Exploit Önleme'yi etkinleştirme ve devre dışı bırakma
Sistem işlemleri bellek koruması
Davranış Tespiti
Şifreleyici Önleyici
Paylaşılan klasörlerin dış şifrelemeye karşı korunmasını etkinleştirme ve devre dışı bırakma
Güvenilir olmayan bir bilgisayarın engelleme süresini yapılandırma
Koruma kapsamının düzenlenmesi
Harici veri şifreleme için güvenilir bilgisayarlar ekleme
Paylaşılan klasörlerin dış şifrelemeye karşı korunması istisnalarının listesini içe/dışa aktarma
Düzeltme Altyapısı
Kaspersky Security Network
Kaspersky Security Network'ün kullanımını etkinleştirme ve devre dışı bırakma
Kaspersky Private Security Network'ün sınırlamaları
Koruma bileşenleri için bulut modunu etkinleştirme ve devre dışı bırakma
KSN Proxy ayarları
Kaspersky Security Network'den bir dosyanın saygınlığını kontrol etme
Şifreli bağlantıları tarama
Şifreli bağlantıları taramayı etkinleştirme
Güvenilir kök sertifikalarının yüklenmesi

Şifrelenmiş bağlantıları güvenilmeyen bir sertifikayla tarama
Kaspersky sertifikasını kendi sertifika deposuna ekleme
Şifreli bağlantıları taramanın dışında tutma
Güvenilir olmayan sertifikalara sahip etki alanlarına erişimi engelleme
Verileri sil
Bilgisayar denetimi
İnternet Denetimi
İnternet kaynağı erişim kuralı ekleme
İnternet kaynağı adreslerine göre filtrele
İnternet kaynağı içeriğine göre filtrele
İnternet kaynağı erişim kurallarını test etme
İnternet Denetimi kurallarını dışa ve içe aktarma
İnternet Denetimi kuralının web kaynak adreslerini dışa ve içe aktarma
Kullanıcı İnternet etkinliğini ileme
İnternet Denetimi mesajlarının şablonlarını düzenleme
İnternet kaynağı adreslerinin maskelerini düzenleme
Sanal makineler için İnternet Denetimi
İnternet Denetimi mesaj şablonlarındaki değişkenler
Aygıt Denetimi
Erişim kuralları hakkında
Yüklü cihazlar hakkında bilgi alma
Cihazlara erişimi türe göre yönetme
Bağlantı veri yolu ile cihazlara erişimi yönetme
Cihazlara kullanıcı erişim haklarının farklılaştırılması
Mobil cihazlara erişimi yönetme
Bluetooth cihazlarına erişimi yönetme
Yazdırma denetimi
Wi-Fi bağlantılarının kontrolü
Çıkarılabilir sürücülerin kullanımını izleme
Önbelleğe alma süresini değiştirme
Güvenilir aygıtlarla eylemler
Bir cihazı güvenilir listeye ekleme
Güvenilir aygıtlar listesini dışa ve içe aktarma
Engellenen bir aygıta erişim elde etme
Erişim vermek için çevrimiçi mod
Erişim vermek için çevrimdışı mod
Aygıt Denetimi mesajlarının şablonlarını düzenleme
Köprüleme Önleme
Köprüleme Önlemeyi Etkinleştir
Bağlantı kuralının durumunu değiştirme
Bağlantı kuralının önceliğini değiştirme
Uyarlamalı Anomali Denetimi
Uyarlamalı Anomali Denetimi eğitimi
Bir Uyarlamalı Anomali Denetimi kuralını etkinleştirme ve devre dışı bırakma
Bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde gerçekleştirilecek eylemi değiştirme
Bir Uyarlamalı Anomali Denetimi kuralına yönelik istisna oluşturma
Uyarlamalı Anomali Denetimi kuralları için istisnaları içe ve dışa aktarma

- Uyarlamalı Anomali Denetimi kurallarına yönelik güncellemeleri uygulama
- Uyarlamalı Anomali Denetimi mesaj şablonlarını düzenleme
- Uyarlamalı Anomali Denetimi işlemlerinin izlenmesi

Uygulama Denetimi

- Uygulama Denetimi işlevselliği sınırlamaları
- Yüklü uygulamalar hakkında bilgi alma
- Engellenen uygulamalar modunu etkinleştirme
- Temel bilgisayara dayalı Uygulama Denetimi
- Uygulama Denetimi kurallarını yönetme
  - Uygulama Denetimi kuralı için bir tetikleme koşulu ekleme
  - Yürütülebilir dosyalar klasöründen uygulama kategorisine yürütülebilir dosyalar ekleme
  - Olayla ilgili yürütülebilir dosyaları uygulama kategorisine ekleme
  - Uygulama Denetimi kuralı ekleme
  - Kaspersky Security Center aracılığıyla Uygulama Denetimi kuralının durumunu değiştirme
  - Uygulama Denetimi kurallarını dışa ve içe aktarma
  - Uygulama Denetimi bileşeninin işleminden kaynaklanan olayları görüntüleme
  - Engellenen uygulamalar raporunu görüntüleme
- Uygulama Denetimi kurallarını test etme
  - Uygulama Denetimi kuralı testini etkinleştirme ve devre dışı bırakma
  - Test modunda engellenen uygulamalar hakkındaki raporu görüntüleme
  - Uygulama Denetimi bileşeninin test işleminden kaynaklanan olayları görüntüleme
- Uygulama etkinlik izleyicisi
- Dosyalar veya klasörler için isim maskeleri oluşturma kuralları
- Uygulama Denetimi mesaj şablonlarını düzenleme
- Uygulama Denetimi ileti şablonlarındaki değişkenler
- Yürütülebilir dosyaların envanterini çıkarmaya yönelik en iyi uygulamalar
- İzin verilen uygulamalar listesini uygulamaya yönelik en iyi uygulamalar
  - Uygulamalar için izin verilenler listesi modunu yapılandırma
  - İzin verilenler listesi modunu test etme
  - İzin verilenler listesi modu desteği

Ağ portlarını izleme

- Tüm ağ portlarını izlemeyi etkinleştirme
- İzlenen ağ portlarının listesini oluşturma
- Tüm ağ portlarının izlendiği uygulamaların listesini oluşturma
- İzlenen portların listelerini dışa ve içe aktarma

Günlük Denetimi

- Önceden tanımlanmış kuralları yapılandırma
- Özel kurallar ekleme

Sistem Bütünlüğü İzleme

- Sistem Bütünlüğü İzleme kuralları hakkında
- Gerçek Zamanlı Sistem Bütünlüğü İzleme
- İsteğe Bağlı Sistem Bütünlük Denetimi
- Sistem Bütünlüğü İzleme kurallarını dışa ve içe aktarma
- Sistem Bütünlüğü İzleme raporlarını görüntüleme
- Sistem bütünlüğü durumu sıfırlama

Cloud Discovery

Güvenilir bölge
- Tarama istisnası oluşturma
- Tespit edilen nesnelerin türüne göre bir istisna oluşturma
- Güvenilir uygulamalar listesini düzenleme
- Yerel bir güvenilir bölge oluşturma
- Güvenilir bölge listesini dışa ve içe aktarma
- Uygulamaları güvenilir bir dijital imza ile işleme
- Ek. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Microsoft System Center Configuration Manager
  - Citrix
  - VMware
  - Microsoft Windows Server'da veri tekilleştirme

Yedeklemeyi Yönetme
- Yedekleme'deki dosyalar için maksimum depolama süresini yapılandırma
- Yedekleme için maksimum boyutu yapılandırma
- Yedekleme konumundan dosyaları geri yükleme
- Yedekleme konumundan dosyaların yedekleme kopyalarını silme

Bildirim hizmeti
- Olay günlüğü ayarlarını yapılandırma
- Bildirimlerin görüntülenmesini ve iletilmesini yapılandırma
- Bildirim alanında uygulama durumu hakkında uyarıların görüntülenmesini yapılandırma
- Kullanıcılar ile yönetici arasında mesajlaşma

Raporları yönetme
- Raporları görüntüleme
- Maksimum rapor depolama süresini yapılandırma
- Rapor dosyasının maksimum boyutunu yapılandırma
- Raporu dosya olarak kaydetme
- Raporlar temizleniyor

Kaspersky Endpoint Security Kendini Koruma
- Kendini Koruma'yı etkinleştirme ve devre dışı bırakma
- AM-PPL desteğini etkinleştirme ve devre dışı bırakma
- Uygulama hizmetlerinin harici yönetime karşı korunması
- Uzaktan yönetim uygulamalarını destekleme
- Parola koruması
  - Parola korumasını etkinleştir
  - Ayrı ayrı kullanıcılara veya gruplara izinler verme
  - İzinler vermek için geçici parola kullanma
  - Geçici parolanın iptal edilmesi
  - Parola koruması izinlerinin özel boyutları
  - KLAdmin parolasını sıfırlama
- Yönetim Sunucusu bağlantı koruması

Veri Şifreleme
- Şifreleme işlevi sınırlamaları
- Şifreleme anahtarının uzunluğunu değiştirme (AES56 / AES256)

Kaspersky Disk Encryption
- SSD sürücü şifrelemesinin özel özellikleri
- Kaspersky Disk Encryption'ı başlatma
- Şifreleme dışında tutulan sabit sürücülerin listesini oluşturma
- Şifreleme dışında tutulan sabit sürücülerin listesini içe/dışa aktarma
- Çoklu Oturum Açma (SSO) teknolojisini kullanma
- Kimlik Doğrulama Aracısı hesaplarını yönetme
- Kimlik Doğrulama Aracısı ile belirteç ve akıllı kart kullanma
- Sabit sürücü şifresini çözme
- Kaspersky Disk Encryption teknolojisi tarafından korunan bir sürücüye yeniden erişim sağlamak
- Kimlik Doğrulama Aracısı hizmet hesabıyla oturum açma
- İşletim sistemini güncelleme
- Şifreleme işlevselliğini güncelleme hatalarını ortadan kaldırma
- Kimlik Doğrulama Aracısını İzleme
- Kimlik Doğrulama Aracısı yardım metinlerini düzenleme
- Kimlik Doğrulama Aracısı'nın çalışması test edildikten sonra kalan nesnelerin ve verilerin kaldırılması

BitLocker Management
- BitLocker Drive Encryption'ı başlatma
- BitLocker tarafından korunan bir sürücünün şifresinin çözülmesi
- BitLocker tarafından korunan bir sürücüye erişimi geri yükleme
- Yazılımı güncellemek için BitLocker korumasını duraklatma

Yerel bilgisayar sürücülerinde Dosya Düzeyinde 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 dosyalara yeniden erişim sağlama
- İşletim sistemi hatasının ardından şifrelenmiş verilere yeniden erişim sağlama
- Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenleme

Çıkarılabilir sürücüleri şifreleme
- Çıkarılabilir sürücüleri şifrelemeyi başlatma
- Çıkarılabilir sürücülere şifreleme kuralı ekleme
- Çıkarılabilir sürücüler için şifreleme kuralları listesini dışa ve içe aktarma
- Çıkarılabilir sürücülerdeki şifreli dosyalara erişim için taşınabilir mod
- Çıkarılabilir sürücülerin şifresini çözme

Veri şifreleme ayrıntılarını görüntüleme
- Şifreleme durumunu görüntüleme
- Kaspersky Security Center panolarındaki şifreleme istatistiklerini görüntüleme
- Yerel bilgisayar sürücülerinde dosya şifreleme hatalarını görüntüleme
- Veri şifreleme raporunu görüntüleme

Şifrelenmiş cihazlara erişim olmadığında şifrelenmiş cihazlarla çalışma
- FDERT Geri Yükleme Yardımcı Uygulamasını kullanarak veri kurtarma
- İşletim sistemi kurtarma diskini oluşturma

Detection and Response çözümleri
MDR ve EDR Optimum lisanslama
Üçüncü taraf EDR çözümleriyle uyumluluk
Kaspersky Endpoint Agent
[KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi
Kaspersky Endpoint Agent için İlke ve Görev Geçişi
Endpoint Detection and Response Agent (EDR Agent)
EDR Agent'ı Yükleme
EDR Agent'ı MDR ile entegre etme
EDR Agent'ı EDR (KATA) ile entegre etme
EDR Agent'ı NDR (KATA) ile entegre etme
EDR Agent'ı EDR Expert (on-premises) ile entegre etme
Üçüncü taraf EPP uygulamalarla uyumluluk
Managed Detection and Response
Yerleşik aracının MDR ile entegrasyonu
MDR için KEA'dan KES'e Geçiş Kılavuzu
Endpoint Detection and Response
Yerleşik aracının EDR Optimum/EDR Expert ile entegrasyonu
Güvenlik ihlali göstergelerini (standart görev) tara
IOC Taraması için genişletilmiş telemetri
Dosyayı Karantinaya taşı
Dosyayı al
Dosyayı sil
İşlem başlangıcı
İşlemi sonlandır
Yürütme önleme
Bilgisayar ağ izolasyonu
Cloud Sandbox
EDR Optimum için KEA'dan KES'e Geçiş Kılavuzu
Kaspersky Sandbox
Yerleşik aracının Kaspersky Sandbox ile entegrasyonu
Güvenlik ihlali göstergelerini tarayın (bağımsız görev)
Kaspersky Sandbox için KEA'dan KES'e Geçiş Kılavuzu
Kaspersky Anti Targeted Attack Platform
Yerleşik aracının EDR/NDR (KATA) ile entegrasyonu
EDR (KATA) telemetrisini yapılandırma
EDR (KATA) telemetri istisnaları
Örnek 1. Hariç tutulan süreçler
Örnek 2. Hariç tutulan ağ iletişimleri
Örnek 3. Hariç tutulan dosya işlemleri
Örnek 4. Hariç tutulan kayıt defteri değişiklikleri
KATA Sandbox
Yerleşik aracının KATA Sandbox ile entegrasyonu
Tehdit Yanıtı eylemlerini yapılandırma
EDR (KATA) için KEA'dan KES'e Geçiş Kılavuzu

- Endpoint Detection and Response Expert (on-premises)
  - Yerleşik aracının EDR Expert (on-premises) ile entegrasyonu
  - EDR Expert (on-premises) telemetri ayarlarını yapılandırma
  - EDR Expert (on-premises) telemetri istisnaları
  - EDR Expert (on-premises) olay filtrelerini dışa ve içe aktarma
  - EDR Expert (on-premises) ve EDR (KATA) ile entegrasyonu yapılandırmak için ilke profillerini kullanırken dikkat edilmesi gereken özel noktalar
- Endpoint Detection and Response Expert (cloud)
  - Yerleşik aracının EDR Expert (cloud) ile entegrasyonu
  - EDR Expert (cloud) telemetri ayarlarını yapılandırma
  - EDR Expert (cloud) telemetri istisnaları
  - EDR Expert (cloud) olay filtrelerini dışa veya içe aktarma
- Karantinayı Yönetme
  - Maksimum Karantina boyutunu yapılandırma
  - Karantinaya alınan dosyalarla ilgili verileri Kaspersky Security Center'a gönderme
  - Dosyaları Karantinadan geri yükleme
- EDR eylemlerinin izlenmesi

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Kaspersky Endpoint Security'nin KUMA ile Entegrasyonu
  - KES'in KUMA ile entegrasyonuna hazırlık
  - KES'i KUMA'ya bağlama
- KUMA'ya gönderilecek olayları filtreleme
- KUMA olay filtrelerini dışa ve içe aktarma

KSWS'den KES'e Geçiş Kılavuzu
- KSWS ve KES bileşenlerinin benzerliği
- KSWS ve KES ayarlarının benzerliği
- KSWS bileşenlerini taşıma
- KSWS görevlerini ve ilkelerini taşıma
- KSWS güvenilir bölgesini taşıma
- KSWS Uygulamaları Başlatma Denetimi kurallarını taşıma
- KSWS yerine KES'i yükleme
- [KSWS+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi
- Kaspersky Security for Windows Server'ın başarıyla kaldırıldığından emin olma
- KES'i bir KSWS anahtarıyla etkinleştirme
- Yüksek yüklü sunucuların geçişi için dikkat edilmesi gereken özel hususlar
- Uygulamayı Server Core modunda bir sunucuda yönetme
- [KSWS+KEA] uygulamasının [KES+ bütünleşik aracı]'ya geçişi

Sanal makineleri korumak için Light Agent modu
- Hafif Ajan modu için özel hususlar
- Sanal makinenin ön yapılandırması
  - Citrix App Layering teknolojisi ile uyumluluk
  - Citrix Provisioning (Citrix Provisioning Services) teknolojisi ile uyumluluk
  - Omnissa App Volumes teknolojisi ile uyumluluk
- Light Agent'ı Yükleme
- Light Agent'ı SVM'ye bağlama
  - SVM keşfi
  - Light Agent için SVM seçim algoritmasını yapılandırma

- Light Agent'ların bağlantılarını SVM'lere dağıtma (etiketler)
- Light Agent ve SVM arasındaki bağlantının korunması
- Light Agent'ı etkinleştirme
- KSVLA Light Agent'tan KES Light Agent'a Geçiş Kılavuzu
- KSVLA Light Agent yerine KES Light Agent'ı yükleme
- KSVLA Light Agent ve KES Light Agent bileşenlerinin yazışmaları
- KSVLA Light Agent görevlerini ve ilkelerini geçirme
- KSVLA Light Agent+KEA] yapılandırmasını [KES Light Agent+yerleşik aracı] yapılandırmasına taşıma

Uygulamanın komut satırından yönetimi

- Setup. Uygulama yükleniyor
- Setup /x. Uygulamayı kaldırma
- msiexec /i. Uygulamanın kurtarılması
- AVP komutları
- SCAN. Kötü Amaçlı Yazılım Taraması
- UPDATE. Veritabanlarını ve uygulama yazılım modüllerini güncelleme
- ROLLBACK. Son güncellemeyi geri alma
- TRACES. İzleme
- START. Bir profilin başlatılması
- STOP. Profili durdurma
- STATUS. Profil durumu
- STATISTICS. Profil işlem istatistikleri
- RESTORE. Yedekleme konumundan dosyaları geri yükleme
- EXPORT. Uygulama ayarlarını dışa aktarma
- IMPORT. Uygulama ayarlarını içe aktarma
- ADDKEY. Anahtar dosyasını uygulama
- LICENSE. Lisanslama
- RENEW. Lisans satın alma
- PBATESTRESET. Diski şifrelemeden önce disk denetimi sonuçlarını sıfırlama
- EXIT. Uygulamadan çıkış
- EXITPOLICY. İlkeyi devre dışı bırakma
- STARTPOLICY. İlkeyi etkinleştirme
- DISABLE. Korumayı devre dışı bırakma
- SPYWARE. Casus yazılım algılama
- KSN. KSN / KPSN arasında geçiş yapma
- SERVERBINDINGDISABLE. Sunucu bağlantı korumasını devre dışı bırakma
- KESCLI komutları
- Scan. Kötü Amaçlı Yazılım Taraması
- GetScanState. Tarama tamamlanma durumu
- GetLastScanTime. Taramanın tamamlanma süresinin belirlenmesi
- GetThreats. Tespit edilen tehditler hakkında veriler alma
- UpdateDefinitions. Veritabanlarını ve uygulama yazılım modüllerini güncelleme
- GetDefinitionState. Veritabanlarının son güncellenme tarih ve saatinin belirlenmesi
- EnableRTP. Koruma etkinleştiriliyor
- GetRealTimeProtectionState. Dosya Tehdidi Koruması durumu
- GetEncryptionState. Disk şifreleme durumu
- Version. Uygulama sürümünün tanımlanması

- Detection and Response komutları
  - SANDBOX. Sandbox'ı Yönetme
  - PREVENTION. Yürütme önleme yönetimi
  - ISOLATION. Ağ izolasyonunu yönetme
  - RESTORE. Dosyaları Karantinadan geri yükleme
  - IOCSCAN. Güvenlik ihlali göstergeleri (IOC) için tara
  - MDRLICENSE. MDR etkinleştirmesi
  - EDRKATA. EDR (KATA) entegrasyonu
  - EDRExpertOnPrem. EDR Expert (on-premises) entegrasyonu
  - KUMA. KUMA Entegrasyonu
  - YARA. YARA Taramasını Çalıştırma
  - TELEMETRİ FİLTRELERİ. KUMA'ya gönderilecek olayları filtreleme
- Light Agent yönetim komutları
  - KSVLAINFO. Light Agent modunun belirlenmesi
  - VIISINFO. Entegrasyon Sunucusuna Light Agent bağlantısının durumu
  - SVMINFO. Light Agent'ın Protection Server ile bağlantısının durumu
- Hata kodları
- Ek. Uygulama profilleri

REST API aracılığıyla uygulamanın yönetilmesi
- REST API aracılığıyla uygulamanın yüklenmesi
- API ile çalışmak

Uygulama hakkında bilgi kaynakları

Teknik Destek ile irtibat kurma
- İz dosyalarının içeriği ve depolanması
- Uygulama çalışmasını izleme
- Uygulama performansı izleme
- Döküm yazımı
- Döküm dosyalarını ve iz dosyalarını koruma
- İşletim sistemi verilerini alma (Kaspersky Get System Info)

Sınırlamalar ve uyarılar

Sözlük
- Ağ Aracısı
- Antivirüs veritabanları
- Arşiv
- Bir web kaynağının adresinin normalleştirilmiş biçimi
- Cloud Discovery
- E-dolandırıcılık web adreslerinin veritabanı
- Entegrasyon Sunucusu
- Etkin anahtar
- Görev
- Güvenilir Platform Modülü
- IOC
- IOC dosyası
- Kerberos kimlik doğrulaması
- Kimlik Doğrulama Aracısı
- Koruma kapsamı
- Light Agent

- Lisans Sertifikası
- Maske
- OLE nesnesi
- OpenIOC
- Sertifika veren
- SVM
- Tarama kapsamı
- Taşınabilir Dosya Yöneticisi
- Temizlik
- Virüs bulaşabilecek dosya
- Virüslü dosya
- Yanlış alarm
- Yönetim grubu
- Zararlı web adreslerinin veritabanı

Ekler

- Ek 1. Uygulama Ayarları
  - Dosya Tehdidi Koruması
  - Web Tehdidi Koruması
  - Posta Tehdidi Koruması
  - Ağ Tehdidi Koruması
  - Güvenlik Duvarı
  - BadUSB Saldırısı Önleme
  - AMSI Koruması
  - Exploit Önleme
  - Davranış Tespiti
  - Sunucu Yetkisiz Erişim Önleme
  - Düzeltme Altyapısı
  - Kaspersky Security Network
  - Günlük Denetimi
  - Şifreleyici Önleyici
  - İnternet Denetimi
  - Aygıt Denetimi
  - Uygulama Denetimi
  - Uyarlamalı Anomali Denetimi
  - Sistem Bütünlüğü İzleme
  - Endpoint Sensor
  - Sandbox
  - Managed Detection and Response
  - Endpoint Detection and Response
  - Endpoint Detection and Response Expert (on-premises)
  - Network Detection and Response (KATA)
  - KUMA Entegrasyonu
  - Tam Disk Şifreleme
  - Dosya Düzeyinde Şifreleme
  - Çıkarılabilir sürücüleri şifreleme
  - Şablonlar (veri şifreleme)
  - İstisnalar

Uygulama Ayarları
Raporlar ve depolama
Ağ ayarları
Arabirim
Ayarları Yönet
Veritabanlarını ve uygulama yazılım modüllerini güncelleme
Ek 2. Uygulama güven grupları
Ek 3. Hızlı çıkarılabilir sürücü taraması için dosya uzantıları
Ek 4. Posta Tehdidi Koruması ek filtresi için dosya türleri
Ek 5. Dış hizmetlerle etkileşim için ağ ayarları
Ek 6. Uygulama olayları
Kritik
İşlev hatası
Uyarı
Bilgilendirici mesaj
Ek 7. Yürütme önleme için desteklenen dosya uzantıları
Ek 8. Yürütme önleme için desteklenen komut dizisi yorumlayıcıları
Ek 9. Kayıt defterindeki IOC tarama kapsamı (Registryltem)
Ek 10. IOC dosya gereksinimleri
Ek 11. EDR Tehdit Yanıtı için API
Ek 12. Uygulama bileşeni kurallarında kullanıcı hesapları
Yasal Bilgiler
Veri sağlama
Son Kullanıcı Lisans Sözleşmesi kapsamında veri sağlama
Kaspersky Security Network kullanırken veri sağlama
Detection and Response çözümlerini kullanırken veri sağlama
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform (KUMA) ile entegrasyon
Avrupa Birliği mevzuatına (GDPR) uygunluk
Ticari marka bildirimleri
Üçüncü taraf kod hakkında bilgi

Kaspersky Endpoint Security for Windows Yardım

Sürüm 14.2'deki yenilikler

Parola koruması için belirteç tabanlı kimlik doğrulama desteği eklendi

Kaspersky Endpoint Security for Windows sürümlerindeki yenilikler

Başlarken

Kaspersky Endpoint Security for Windows dağıtımı

Kaspersky Endpoint Security for Windows ilk kurulumu

Kaspersky Endpoint Security for Windows lisanslaması

Veri sağlama

Son Kullanıcı Lisans Sözleşmesi kapsamında

KSN'yi kullanırken

GDPR

Tehditleri ortadan kaldırma

İş istasyonlarında

Sunucularda

Bir Güvenlik İhlali Göstergesinin tespit edilmesine tepki verme (Ağ izolasyonu → Karantina → Yürütme önleme)

En iyi uygulamalar

Uygulama performansını optimize etme

Uygulama Denetimi'nde Varsayılan Reddetme Modunu Uygulama

KEA'yı bütünleşik ajanı kullanarak KES'e taşıma

KES'i diğer çözümlerin bir parçası olarak kullanma

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Yenilikler

Güncelleme 14.2

Kaspersky Endpoint Security 14.2 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Varsayılan olarak yüklenen bileşen seti değiştirildi. Varsayılan uygulama yapılandırması artık BadUSB Saldırısı Önleme, BitLocker yönetimi ve yerleşik EDR Optimum aracısını içeriyor.

2. Belirteç tabanlı kimlik doğrulama (Parola koruması) desteği eklendi. Artık uygulamaya erişmek için kullanıcı adınızı ve parolanızı, yönetici tarafından verilen geçici bir parolayı veya bir belirteci kullanabilirsiniz. Belirteç tabanlı kimlik doğrulama, örneğin parola gerektirmeyen hizmet kullanıcı hesapları için kullanılabilir.

3. BitLocker için yeni bir parola gücü ölçütü eklendi: parola geçmişi denetimi. Uygulama, kullanıcıların daha önce kullandıkları bir parolayı belirlemesini engeller.

4. *Uygulamayı uzaktan yükle* görevini kullanarak uygulamayı güncellerken Kaspersky Endpoint Security arabirim dilini değiştirme desteği eklendi. Artık yanlış arabirim dilini seçtiyseniz uygulamayı yeniden yüklemeniz gerekmez.

5. Kaspersky Endpoint Detection and Response çözümlerinin kullanıcıları için yeni telemetri olayları eklendi: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Bu yeni olaylar, EDR çözümlerinin tehdit algılama yeteneklerini güçlendiriyor.

6. Kaspersky Endpoint Detection and Response Expert (on-premises) kullanıcıları için yeni bir tehdit yanıtı eylemi olan *Dosyayı yerleştir* desteği eklendi. Bu görev; yapılandırma dosyalarını, tehdit yanıtı komut dosyalarını, saldırıların etkilerini azaltmaya yönelik yardımcı programları vb. bilgisayarlara göndermenizi sağlar. *Dosyayı yerleştir* görevi, Kaspersky EDR Expert (şirket içi) çözümünün 9.0 sürümünün dağıtıldığı OSMP konsolunda kullanılabilir.

7. Kaspersky Endpoint Detection and Response Optimum kullanıcıları için tehdit yanıtı eylemlerinin davranışı iyileştirildi. Artık uygulama, eylemi (*Dosyayı sil*, *Dosyayı Karantinaya taşı* veya *Yürütme önleme*) gerçekleştirmeden önce nesnenin sistem açısından kritik bir nesne (System Critical Object, SCO) olup olmadığını kontrol eder ve sistem kararlılığı üzerindeki olası etkisi konusunda uyarır. Bu eylemlerin Sistem Kritik Nesne (SCO) dosyalarına uygulanması önerilmez.

8. Kaspersky Security for Virtualization Light Agent kullanıcılarının uygulamayı yüksek kullanılabilirlikli Entegrasyon Sunucuları kümesi kapsamında çalıştırmasına yönelik destek eklendi. Entegrasyon Sunucularından oluşan yüksek kullanılabilirlik kümesi, birincil Entegrasyon Sunucusu arızalandığında SVM'lerin ve Light Agent'ların yedek Entegrasyon Sunucusuna devredilmesi sayesinde sanal ortamın kesintisiz korunmasını sağlar.

9. Kaspersky Endpoint Security'nin bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Güncelleme 14.1

Kaspersky Endpoint Security 14.1 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Windows Server 2025 işletim sistemi için destek eklendi.

2. Endpoint Detection and Response Expert (on-premises) ve Kaspersky Endpoint Detection and Response Expert (cloud) için telemetri olayı filtreleme kurallarının sayısına ilişkin sınır artırıldı. Kaspersky Endpoint Security artık toplamda en fazla 10.000 dahil etme ve hariç tutma filtreleme kuralını destekler.

3. Artık görevleri, hafta cinsinden belirtilen aralıklarla yalnızca haftanın belirli günlerinde çalışacak şekilde yapılandırabilirsiniz. Program, Kaspersky Security Center 16.1 veya daha yeni sürümlerinde mevcuttur.

4. *Kötü amaçlı yazılım taraması* görevi için, örneğin yükün arttığı dönemlerde bilgisayar performansı üzerindeki etkiyi en aza indirmek amacıyla görevin duraklatılacağı bir zaman aralığı belirtebilirsiniz.

5. Korunan bilgisayardaki sabit sürücü alt sisteminin performansı, G/Ç işlemlerinin sayısı azaltılarak optimize edilmiştir.

6. Kaspersky Endpoint Security'nin bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Güncelleme 14.0

Kaspersky Endpoint Security 14.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Artık ARM tabanlı bilgisayarlar desteklenmektedir. Uygulamayı standart modda veya EDR Agent modunda yükleyebilirsiniz. Ancak, bu uygulamanın bazı sınırlamaları vardır (örneğin, veri şifreleme teknolojileri arasında yalnızca BitLocker desteklenmektedir).

2. Genişletilmiş politika denetimi, Kaspersky Security Center Web Console sürüm 15.0 ve sonraki sürümlerde desteklenmektedir. Artık ilke değişikliklerini görüntüleyebilir ve bunları bir dosyaya kaydedebilirsiniz. Bir *revizyon*, kullanıcı tarafından kaydedilen bir dizi değiştirilmiş parametredir. Revizyonlar, ilke parametrelerindeki değişiklikleri karşılaştırmanıza ve geri almanıza olanak tanır.

3. Kaspersky Endpoint Detection and Response kullanıcıları artık yeni telemetri olaylarından yararlanabilir. Bu yeni olaylar, Kaspersky EDR çözümlerini kullanarak tehdit algılama yeteneklerini geliştirir.

4. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Güncelleme 12.12

Kaspersky Endpoint Security 12.12 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Eskiden Davranış Tespiti bileşeninin bir parçası olan paylaşılan klasörlerin harici şifrelemeye karşı korunması, artık Şifreleyici Önleyici adında ayrı bir bileşendir.

2. İnternet erişimi için bir proxy sunucusu aracılığıyla uygulamanın kimliğini doğrulamak üzere Kerberos protokolü desteği eklenmiştir.

3. Artık güvenilir bir uygulama için yalnızca tam yol değil, bir dosya karma da belirtebilirsiniz.

4. Endpoint Detection and Response (EDR) çözümleri kullanıcıları için daha fazla *IOC Taraması* görevi özelliği mevcuttur. Geriye dönük IOC Taraması işlevi artık kullanılabilir. *Geriye Dönük IOC Taraması*, Kaspersky Endpoint Security'nin belirli bir zaman dilimine ait verileri kullanarak ihlal göstergelerini taradığı *IOC Taraması* görevinin bir modudur. Bu mod, bilgisayarın ağ etkinliği verilerindeki güvenlik ihlali göstergelerini tespit etmek için tasarlanmıştır. Kaspersky Endpoint Security, bilgisayardaki işletim sistemi günlükleri ve tarayıcı günlüklerindeki verileri analiz eder.

5. Kaspersky Endpoint Detection and Response (EDR) kullanıcıları karantina boyutu sınırını kaldırabilir. Bu, YARA taraması için gerekli olabilir çünkü uygulama büyük bir bellek döküm dosyası kaydedebilir. Artık boş disk alanınızın tamamını karantina için kullanabilirsiniz.

6. Olayların Kaspersky Unified Monitoring and Analysis Platform'a (KUMA) aktarımını optimize etmek için HTTPS sıkıştırması artık destekleniyor. Bu, giden trafiği azaltmaya yardımcı olur.

7. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Güncelleme 12.11

Kaspersky Endpoint Security 12.11 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Uygulama, ayarları kaydetmeden önce kontrol bileşenlerinin yapılandırmasını kontrol eder. Uygulama Denetimi, Aygıt Denetimi ve Sistem Bütünlüğü İzleme bileşenleri için kontrol eklendi. Uygulama artık, kontrol bileşeninin geçerli ayarlarının bilgisayardaki yükü artırabileceği veya sistem arızalarına neden olabileceği durumlarda bir uyarı görüntüler. Örneğin, Uygulama Denetimi durumunda, izin verilenler dışındaki tüm uygulamaları engelleyen modu seçtiyseniz ve herhangi bir izin kuralı eklemediyseniz, uygulama bir uyarı görüntüler, çünkü bu tür bir yapılandırma sistem arızalarına neden olabilir.

2. İnceleme için KATA Sandbox'a otomatik dosya gönderimi desteği eklendi. *KATA Sandbox*, Kaspersky Anti Targeted Attack Platform'un işletim sistemlerinin sanal görüntüleri üzerinde dosya çalıştıran bir bileşenidir. Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Sandbox sunucuları) nesneleri analiz eder ve tarar. KATA Sandbox'ın otomatik modda çalışması için Kaspersky Anti Targeted Attack Platform 8.0 veya üstü sürümünün kurulması gerekir.

3. EDR telemetri gönderimi optimize edildi. Artık maksimum paket uzunluğunu belirtebilirsiniz.

4. Kaspersky Security Network'e bağlantı tanılama özelliği iyileştirildi. Kaspersky Security Network için olası sorunları çözmek üzere bağlantı hatası ayrıntıları genişletildi.

5. Kaspersky Unified Monitoring and Analysis Platform (KUMA) platformuna gönderilecek olay listelerinin yapılandırılması için destek eklendi. Artık, KUMA'daki önceden tanımlanmış olay listelerine ek olarak, telemetriye manuel olarak olaylar ekleyebilir veya Windows Olay Günlüğü'nde olayları kimliklerine göre hariç tutabilirsiniz.

6. Web Console'daki ilke arayüzü güncellendi. Temel özelliklere daha hızlı erişim için ilke bölümlerinin düzeni değiştirildi.

7. Windows 11 25H2 desteği.

8. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Güncelleme 12.10

Kaspersky Endpoint Security 12.10 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. BadUSB Saldırı Önleme bileşeni için, ekrandan bir barkod okutarak barkod tarayıcıları yetkilendirme seçeneği eklendi. Artık barkod tarayıcıları yetkilendirmek için ekran klavyesini kullanarak bir kod girmenize gerek yok.

2. Kaspersky'nin Endpoint Detection and Response (EDR) çözümlerinin kullanıcıları şu özellikleri ve iyileştirmeleri kullanabilirler:

   - Artık uyarı ayrıntılarında bilgisayarın Ağ İzolasyonunu yönetebilirsiniz. Ek olarak, uyarı ayrıntılarında bilgisayar Ağ İzolasyonu zaman periyodunu belirleyebilir ve istisnalar ekleyebilirsiniz.

   - Uyarı ayrıntılarının yeni verilerle doldurulması. Artık uyarı ayrıntıları, uygulamanın EDR tehditlerine yanıt verirken nasıl davrandığı da dahil olmak üzere tehdit hakkında daha fazla bilgi içeriyor.

   - IOC dosyalarının işlenmesi iyileştirildi. Artık Kaspersky Security Center Web Console'un arabiriminde IOC dosyalarının içeriğini görüntüleyebilir ve düzenleyebilirsiniz. Bir IOC dosyasını yükledikten sonra, uygulama IOC terimleri uygulaması hakkında bir rapor görüntüler.

   - Tespit edilen IOC'lere yanıt verme iyileştirildi. Artık *IOC Taraması* tarafından tespit edilen dosyaları doğrudan görev özelliklerindeki IOC tespit sonuçlarında karantinaya alabilirsiniz. Ayrıca görev özelliklerinde bilgisayarları ağdan izole edebilirsiniz.

   - Artık bir TXT dosyasında oluşturulan dosya karmaları, IP adresleri veya DNS adları listelerine dayalı olarak IOC dosyalarını doğrudan *IOC Taraması* görevinin özelliklerinden oluşturabilirsiniz.

   - *IOC Taraması* için genişletilmiş tarama kapsamı. Artık kayıt defterinin IOC Taraması için bir kapsam tanımlayabilirsiniz (**Windows Kayıt Defteri - Registryltem**). Uygulamanın önceki sürümlerinde, kayıt defterinde yalnızca önceden tanımlanmış bir IOC Taraması kapsamı kullanabiliyordunuz.

3. Yeni parola koruma izni eklendi, *Ayarları dışa aktar*. Varsayılan olarak, yalnızca KLAdmin kullanıcısı uygulama arabiriminde Kaspersky Endpoint Security ayarlarını içeren bir yapılandırma dosyası oluşturabilir. Diğer kullanıcılara erişim izni vermek için, onlara ilgili izni vermeniz gerekir.

4. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Güncelleme 12.9

Kaspersky Endpoint Security 12.9 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. *Geçici parolaları yönetme* için yeni işlevsellik eklendi. Geçici parola, ayrı bir bilgisayar için Parola Koruması etkinleştirilmiş Kaspersky Endpoint Security'ye erişim sağlamanıza olanak tanır. Geçici parolaların yönetimi, parola geçmişini (30 güne kadar) kaydetmeye, geçici parola durumunu (*Etkin*, *Süresi doldu*, *İptal edildi*) izlemeye ve geçici parolaları iptal etmeye olanak tanır.

2. İlke uygulandıktan hemen sonra İnternet Denetimi kuralları tarafından yasaklanan web kaynaklarına bağlantıyı sonlandırma seçeneği eklendi. Uygulamanın önceki sürümlerinde, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlıyordu.

3. Kaspersky Anti Targeted Attack Platform kullanıcıları için, YARA denetimini bilgisayarda yerel olarak çalıştırma seçeneği eklendi. Bunu yapmak için, YARA kurallarını içeren bir dosya indirmeniz ve CMD'de komutu çalıştırmanız gerekiyor.

4. Sürücülerin üçüncü taraf araçlar kullanılarak BitLocker tarafından zaten korunduğu bilgisayarlarda BitLocker etkinleştirildiğinde uygulamanın davranışı düzeltildi. Kaspersky Endpoint Security, kurtarma anahtarını Kaspersky Security Center'a göndermek için kurtarma prosedürünü başlatır. Böylece BitLocker yönetimi Kaspersky Security Center konsoluna aktarılır.

5. Yeni bir bölüm olan **Yanıt geçmişi**, Kaspersky'nin Detection and Response çözümlerinin kullanıcıları tarafından kullanılabilir. Bu bölüm, bilgisayarda gerçekleştirilen tehdit yanıt eylemleri hakkında bilgi içerir. Bu tür eylemler arasında örneğin *İşlemi sonlandır* görevinin çalıştırılması veya bilgisayarın ağdan yalıtılması yer alır. Yanıt geçmişi yalnızca şu Kaspersky çözümlerinin kullanıcıları tarafından kullanılabilir: MDR, EDR, KATA.

6. Kaspersky Unified Monitoring and Analysis Platform kullanıcıları için EDR tehdit yanıt eylemleri desteği artık kullanılabilir. Tehditlere yanıt verirken KUMA, ilgili EDR görevlerini oluşturan komut dosyalarını çalıştırır. EDR görevlerini gerçekleştirmek için, KUMA konsolunda özel komut dosyası için bir yanıt kuralı oluşturmanız ve olayları seçmeniz gerekir.

7. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Güncelleme 12.8

Kaspersky Endpoint Security 12.8 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Uygulama artık sanal ortamları korumak için Light Agent modunu destekliyor. Artık uygulamayı Kaspersky Security for Virtualization Light Agent 6.2 çözümünün bir parçası olarak Light Agent olarak dağıtabilirsiniz.

2. Sunucularda Docker konteynerlerinde dosya işlemlerinin engellenmesi artık destekleniyor. Bir *kapsayıcı*, bir uygulamanın işletim sistemiyle doğrudan etkileşime girmeden çalışabileceği yalıtılmış bir ortamdır. Kaspersky Endpoint Security, kullanıcının erişim sağladığı kapsayıcıların içindeki dosyaları tarar. Bir tehdit tespit edildiğinde, uygulamalar bu kötü niyetli etkinlikleri engeller ve konteyner içindeki dosyayı temizlemeye çalışır. Dosya temizlenemiyorsa uygulama konteyneri durdurur.

3. Artık paylaşılan klasörlerin harici şifrelemeye karşı korunması için bir koruma kapsamı tanımlayabilirsiniz (Davranış Tespiti bileşeni). Artık uygulamanın dosya etkinliği için izlemesi gereken paylaşılan klasörleri belirleyebilirsiniz. Ayrıca dosyaları koruma kapsamı dışında bırakabilirsiniz. Uygulamanın önceki sürümlerinde, Davranış Tespiti bileşeni dosya etkinliği için tüm paylaşılan klasörleri izliyordu.

4. Artık kurulum paketinde farklı işletim sistemi türleri için farklı bileşen setleri yapılandırabilirsiniz. Yani, uygulamayı aynı kurulum paketini kullanarak iş istasyonlarına ve sunuculara dağıtabilirsiniz. Belirli bir işletim sistemi türü için mevcut olmayan bileşenler, kurulum paketi özelliklerinde otomatik olarak hariç tutulur.

5. Önceden tanımlanmış tarama istisnalarını ve güvenilir uygulamaları seçme eklendi. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar, sanal bir ortamda (Citrix, VMware) uygulama için güvenilir bölgenin hızlı bir şekilde yapılandırılmasına olanak tanır. Bu tür istisnalar arasında örneğin VHD ve VHDX sanal makineler dosyaları sayılabilir. Uygulama yükleme paketi oluştururken, ilke oluştururken veya Kaspersky Endpoint Security'yi yüklerken istisnalar eklenebilir.

6. EDR telemetri artık USB bağlantılı cihazlarla yapılan işlemler için olaylar içeriyor. Bu olayları EDR telemetrisinden istisnalara da ekleyebilirsiniz.

7. Eski TLS 1.0 protokolü üzerinden ağ bağlantılarını engelle seçeneği eklendi. TLS 1.0 düşük bir güvenlik seviyesine sahiptir, bu nedenle bu protokolün devre dışı bırakılması ve daha yeni TLS 1.2 veya TLS 1.3 sürümlerinin kullanılması önerilir. Kaspersky Endpoint Security varsayılan olarak TLS 1.0 bağlantılarını engeller. Uygulama sürümünü güncelledikten sonra, TLS 1.0 protokolünü kullanan üçüncü taraf hizmetlerinin çalışması başarısız olabilir. Üçüncü taraf hizmetlerinin çalışmasında sorunlardan kaçınmak için, uygulama sürümünü güncellemeden önce grup ilkesinde TLS 1.0 protokolünün kullanımına izin verebilirsiniz.

8. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri dahil ettik: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Güncelleme 12.7

Kaspersky Endpoint Security 12.7 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Artık *Kötü Amaçlı Yazılım Taraması* görevleri için işlemci kaynak kullanımını sınırlayabilirsiniz. Bunu yapmak için, uygulama ayarlarında, bilgisayarı tararken kullanılabilecek tüm çekirdekler için maksimum işlemci yük yüzdesini belirtin.

2. Artık KATA Sandbox'ta tarama için dosyalarımanuel olarak gönderebilirsiniz. *KATA Sandbox*, Kaspersky Anti Targeted Attack Platform'un işletim sistemlerinin sanal görüntüleri üzerinde dosya çalıştıran bir bileşenidir. Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Sandbox sunucuları) nesneleri analiz eder ve tarar. KATA Sandbox'a tarama için bir dosya göndermek için dosyanın içerik menüsünden ilgili komutu seçin.

3. Artık kurumsal LAN'ı koruyan çözümle entegrasyon kurabilirsiniz, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR), Kaspersky Anti Targeted Attack Platform'un bir parçasıdır. NDR ile etkileşimi standart modun yanı sıra EDR Agent modunda da yapılandırabilirsiniz.

4. Posta Tehdidi Koruması uzantısına Microsoft Office Outlook e-posta istemcisi 2021 sürümü için destek eklendi. Uzantı, mesajların protokol düzeyi yerine posta istemcisi düzeyinde taranmasına olanak tanır. Mesajlara ek olarak, uzantı Microsoft Exchange depolarından MAPI arabirimi aracılığıyla alınan nesneleri (örneğin, Takvimdeki nesneleri) taramanızı sağlar. Bu tarama posta istemcisinde gerçekleşir.

5. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri ekledik: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Güncelleme 12.6

Kaspersky Endpoint Security 12.6 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Kaspersky SIEM çözümü – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – ile entegrasyon için işlevsellik eklendi. Artık Windows olay günlüklerinden KUMA toplayıcısına olay göndermek mümkün. Bu, KUMA'nın Kaspersky Endpoint Security'nin yüklü olduğu tüm bilgisayarlardan, bu bilgisayarlara KUMA aracıları yüklemeden Windows olaylarını (sınırlı bir EventID seti desteklenir) almasını sağlar.

2. *Sistem Bütünlüğü İzleme*, Dosya Bütünlüğü İzleyicisi bileşeninin yerini almak üzere eklenmiştir. Sistem Bütünlüğü İzleme bileşeni, Dosya Bütünlük İzleyicisinin tüm işlevlerini içerir ve ayrıca kayıt defteri değişikliklerini ve harici cihazların bağlantısını izlemeye izin verir. Sistem Bütünlüğü İzleme bileşeni, işletim sisteminde bilgisayar güvenliği ihlallerine işaret edebilecek değişiklikleri izler. Bu tür değişiklikler tespit edildiğinde, Kaspersky Endpoint Security ilgili olayları oluşturur ve yöneticiyi uyarır. Dosya Bütünlük İzleyicisi artık uygulamanın bir parçası değil. Dosya Bütünlük İzleme ayarları, uygulamayı güncellediğinizde otomatik olarak Sistem Bütünlüğü İzleme'ye taşınır. Sistem Bütünlüğü İzleme özelliğinin doğru çalışmasını sağlamak için hem Kaspersky Endpoint Security uygulaması hem de yönetim eklentisi 12.6 sürümüne güncellenmelidir.

3. Yüklü yerleşik EDR Agent (KATA) durumu, Kaspersky Security Center konsolundaki bilgisayar özelliklerine eklendi. Artık yerleşik bir EDR Agent (KATA) yüklüyse, **Endpoint Sensor durumu** sütunu bileşenin mevcut durumunu görüntüler (örneğin, *Çalışıyor*, *Durduruldu*, *Lisansla desteklenmiyor*).

4. Önceden tanımlanmış tarama istisnalarını ve güvenilir uygulamaları seçme eklendi. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar, uygulamayı SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da kullanırken güvenilir bölgenin hızla yapılandırılmasına yardımcı olur. Bu tür istisnalar arasında örneğin MDF ve LDF veritabanı dosyaları sayılabilir. İstisnalar yeni bir ilke oluşturulurken, mevcut bir ilke değiştirilirken veya Kaspersky Endpoint Security yüklenirken eklenebilir.

5. Kaspersky Endpoint Detection and Response Optimum için uyarı ayrıntılarının görüntülenmesi, Kaspersky Endpoint Security yönetim eklentisinden ayrı bir Kaspersky Endpoint Detection and Response yönetim eklentisine taşındı. EDR yönetim eklentisi, Windows, Mac ve Linux işletim sistemlerinde aracılarla çalışmak için tek bir eklentidir. Artık EDR Optimum ile çalışırken, tehdit yanıt görevleri oluşturmak için Kaspersky Endpoint Security yönetim eklentisine ve uyarı ayrıntılarını görüntülemek için EDR yönetim eklentisine ihtiyacınız olacak.

6. Windows 11 24H2 desteği.

7. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri ekledik: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Güncelleme 12.5

Kaspersky Endpoint Security 12.5 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Telemetri istisnalarını yapılandırma seçeneği eklendi. *Telemetri*, korunan bilgisayarda meydana gelen olayların bir listesidir. Telemetri verileri, Kaspersky Anti Targeted Attack Platform (EDR) tarafından kurumun BT altyapısını izlemek ve korumak için kullanılır. Telemetri istisnalarını yapılandırmak bilgisayar performansını artırmaya ve Telemetri toplama sunucusuna veri iletimini optimize etmeye yardımcı olur.

2. Uygulamanın güvenilir bölgesinin arabirimi geliştirildi. Kaspersky Endpoint Security artık, yönetici kullanıcının kendi (yerel) tarama istisnalarını ve güvenilir uygulamalarını eklemesini yasakladıysa güvenilir bölge nesnelerini kullanıcıdan gizler. Bu, bir davetsiz misafirlerin güvenilen bölgeye yetkisiz erişimini önleyerek bilgisayar güvenliği seviyesini artırır.

3. MyOffice Mail ve R7-Office Organizer posta istemcileri için trafiği tarama seçeneği eklendi. Posta Tehdit Koruması bileşeni artık yalnızca indirme sırasında mesaj eklerini değil, aynı zamanda gönderilen ve alınan mesajları da tarıyor.

4. Yeni *Üretken yapay zeka araçları* web kaynağı kategorisi eklendi. İnternet sitelerine erişimi yeni kategoriden İnternet Denetimi ile yapılandırabilirsiniz.

5. Artık Güvenlik Duvarı listesinde bir ağ paketi kuralının konumunu seçebilirsiniz. Bir ağ paketi kuralının listedeki konumu önceliğini belirler. Uygulamanın önceki sürümlerinde, yeni bir kural yalnızca listenin sonuna eklenebiliyordu, daha sonra kuralı öncelik sırasına koymak için listede manuel olarak taşımanız gerekiyordu. Artık bir kural eklerken, kuralın listenin başına mı, sonuna mı yoksa seçilen kuralın yanına mı yerleştirileceğini seçebilirsiniz.

6. Artık Kaspersky Endpoint Security bileşenlerinin kurallarında kullanıcıları yalnızca Active Directory'den değil, Kaspersky Security Center'daki kullanıcı listesinden de seçebilirsiniz. Yerel kullanıcı hesabı verilerini manuel olarak da girebilirsiniz. Bu olasılık şu bileşenlerin kuralları için eklenmiştir: Uygulama Denetimi, Cihaz Denetimi, İnternet Denetimi, Uyarlanabilir Anomali Denetimi ve Günlük Denetimi.

7. Ağ saldırısı tespit raporu artık saldıran bilgisayarın MAC adresini (Ağ Tehdit Koruması bileşeni) içeren bir sütun içermektedir. Artık raporda saldıran bilgisayarın IP adresine ek olarak MAC adresini de görebilirsiniz. Bu, olay incelemesi için yararlıdır. Saldırıya uğrayan bilgisayarın MAC adresini içeren raporlar, Kaspersky Security Center Linux konsolunun 15.1 ve sonrası sürümlerinde de mevcut olacak.

8. Bilgisayar koruma gerekliliklerinin seviyesi artırıldı. Yüksek koruma düzeyi artık uygulama hizmetlerinin harici yönetime karşı korunmasının etkinleştirilmesini gerektirmektedir. İlke penceresinin üst kısmındaki güvenlik düzeyi göstergesini kontrol edin. Orta veya düşük güvenlik düzeyine sahipseniz, güvenlik düzeyi göstergesi öneri penceresinde Uygulama hizmetlerinin harici yönetime karşı korunmasını etkinleştirebilirsiniz.

9. Uygulama Endpoint Detection and Response Agent (EDR Agent) yapılandırmasında çalışırken yeni nesne algılama olayları için destek eklendi. Bu olaylar [KES+yerleşik aracı] yapılandırmasında zaten destekleniyordu.

10. Kaspersky Endpoint Security for Windows'un bu sürümünü geliştirirken, şu özel yamalarda yer alan değişiklikleri ekledik: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Güncelleme 12.4

Kaspersky Endpoint Security 12.4 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Bilgisayarın Kaspersky Security Center'a bağlantısını korumak için yeni işlevsellik eklendi. Yeni *Yönetim Sunucusu bağlantı koruması* görevi, güvenilir bir sunucuya bağlanmak için bir parola belirlenmesini sağlar. Bu, bilgisayara yeniden bağlanmanın ve bu parola olmadan başka bir sunucudan komut çalıştırmanın mümkün olmadığı anlamına gelir.

2. Parola Koruma bileşeni için, kullanıcıları yalnızca Active Directory'den değil, manuel olarak seçebilme özelliği de eklendi. Yani, manuel olarak bir kullanıcı adı ve parola belirleyebilir ve bu hesap için Kaspersky Endpoint Security'ye erişim hakları atayabilirsiniz. Bu şekilde, uygulamaya erişimi kontrol etmek için KLAdmin parolanızı diğer kullanıcılarla paylaşmanız veya yeni Active Directory hesapları oluşturmanız gerekmez.

3. Windows 11 23H2 desteği.

Güncelleme 12.3

Kaspersky Endpoint Security 12.3 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Artık uygulamayı Endpoint Detection and Response Agent yapılandırmasına yükleyebilirsiniz. Bu yapılandırma, uygulamanın Kaspersky'nin Detection and Response çözümleri için gereken bir dizi bileşenle birlikte yüklenmesini sağlar: Kaspersky Managed Detection and Response ve Kaspersky Anti Targeted Attack Platform (EDR). Uygulamayı bu yapılandırmada üçüncü taraf çözümlerle birlikte yükleyebilirsiniz (örneğin, Dr.Web, Dallas Lock, ESET). Bu, Kaspersky'nin Detection and Response özelliğinin yanı sıra üçüncü taraf altyapı güvenlik araçlarını da kullanmanıza olanak tanır.

2. Kaspersky Endpoint Security'nin Bluetooth cihazlarla çalışması iyileştirildi. Artık istisnaları yapılandırabilir ve giriş cihazları (kablosuz klavyeler, fareler vb.) hariç tüm Bluetooth cihazlarına erişimi kısıtlayabilirsiniz.

3. Uygulama Denetimi bileşeninin yürütülebilir dosyaların veritabanı ile çalışması optimize edildi. Kaspersky Endpoint Security artık dosya bilgisayardan silindiğinde dosya bilgilerini veritabanından otomatik olarak kaldırıyor. Bu, veritabanının güncel tutulmasını ve Kaspersky Security Center kaynaklarından tasarruf edilmesini sağlar.

4. Bilgisayar koruma gerekliliklerinin seviyesi artırıldı. Yüksek koruma düzeyi artık Parola korumasının etkinleştirilmesini gerektiriyor. İlke penceresinin üst kısmındaki güvenlik düzeyi göstergesini kontrol edin. Orta veya düşük koruma düzeyine sahipseniz güvenlik düzeyi göstergesi öneri penceresinden Parola korumasını etkinleştirebilirsiniz.

5. Uygulamanın Kaspersky Security Network ile çalışmasını sağlamak için HTTPS protokol desteği eklendi. KSN proxy sunucu ayarlarındaki Yönetim Sunucusu özelliklerinde HTTPS kullanımını etkinleştirin.

Güncelleme 12.2

Kaspersky Endpoint Security 12.2 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Wi-Fi ağlarına bağlantıları kontrol etmek (Cihaz Kontrolü) için WPA3 protokol desteği eklendi. Artık güvenilir Wi-Fi ağ ayarlarında WPA3 protokolünü seçebilir ve daha az güvenli bir protokol kullanarak ağa bağlantıyı reddedebilirsiniz.

2. Artık Ağ Tehdit Koruması istisnaları için bir iletişim kuralı ve portlar seçebilirsiniz. Artık güvenilir cihazların IP adreslerini belirtmenin yanı sıra bir port ve iletişim kuralı da seçebilirsiniz. Bu, tek tek veri akışlarını hariç tutmanıza ve güvenilir IP adreslerinden gelen ağ saldırılarını önlemenize olanak tanır.

3. Bilgisayara bir ilke uygulanmışsa Yerel *Veritabanlarının ve uygulama modüllerinin güncellemesi görevi* için farklı güncelleme kaynakları sırası. Kaspersky Security Center sunucusu artık varsayılan olarak Kaspersky sunucuları yerine ilk güncelleme kaynağı olarak kullanılıyor. Bu, kullanıcı yerel *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini çalıştırdığında trafikten tasarruf edilmesine yardımcı olur.

Güncelleme 12.1

Kaspersky Endpoint Security 12.1 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Kaspersky Anti Targeted Attack Platform çözümü için yerleşik bir aracı eklendi. EDR (KATA)'yı kullanmak için artık Kaspersky Endpoint Agent'a ihtiyacınız yok. Tüm Kaspersky Endpoint Agent işlevleri Kaspersky Endpoint Security tarafından gerçekleştirilecektir. Kaspersky Endpoint Agent ilkelerinin taşınması için Geçiş Sihirbazı'nı kullanın. Uygulamayı güncelledikten sonra Kaspersky Endpoint Security, bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır. Kaspersky Endpoint Agent uyumsuz yazılımlar listesine eklendi. Kaspersky Endpoint Security, tüm Detection and Response çözümleri için yerleşik aracılara sahiptir, bu nedenle bu çözümlerle entegrasyon için Kaspersky Endpoint Agent'ın yüklenmesi artık gerekli değildir.

2. Azure WVD uyumluluk modu artık desteklenmektedir. Bu özellik, Kaspersky Anti Targeted Attack Platform konsolunda Azure sanal makine durumunun doğru görüntülenmesini sağlar. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensör Kimliği atanmasına olanak tanır.

3. iTunes veya benzeri uygulamalarda mobil cihazlara kullanıcı erişimini yapılandırabilirsiniz. Yani, örneğin, mobil cihazın yalnızca iTunes'da kullanılmasına izin verebilir ve mobil aygıtın çıkarılabilir bir sürücü olarak kullanılmasını engelleyebilirsiniz. Uygulama ayrıca Android Debug Bridge (ADB) uygulaması için bu kuralları destekler.

4. Kaspersky Security Center sürüm 11 artık desteklenmiyor. Kaspersky Security Center'ı en son sürüme yükseltin.

Düzeltilen sorunlar

Aşağıdaki tabloda, Kaspersky Endpoint Security'nin önceki sürümlerinde keşfedilen ve mevcut sürümde düzeltilen tüm sorunlar listelenmiştir.

14.2 sürümünde düzeltilen sorunların listesi

Tanımlayıcı	Açıklama
10110351	**Çıkarılabilir sürücüler** aygıt türü için **Engelle** eylemi seçildiğinde Aygıt Denetimi bileşeni, bir MTD aygıtına (SD kart) erişime izin verir.
10068496	Korumalı bir aygıtta, Ağ Tehdidi Koruması ayarları üst ilkede kilitli olsa bile MAC Sahteciliğine Karşı Koruma modu değiştirilebilir.
10095087	Şifreli bağlantıları tarama etkinleştirildiğinde, sertifikası iptal edilmiş bir yeni nesil güvenlik duvarı (NGFW) üzerinden herhangi bir web sitesine erişilmesi, güvenilmeyen sertifikaya sahip bir etki alanına yönlendirme hakkında bir bildirim tetikler.
10140912	Uygulama yüklüyken bilgisayar, Windows Mobile çalıştıran BHT1100B PDA cihazını algılamaz.
10141009	Dosya Şifreleme bileşeni yüklüyse Anthropic Claude uygulaması başlatılamayabilir.
10610853	Yeni sürüme yükseltildikten sonra, yeni sürümdeki Aygıt Denetimi ayarları önceki sürümde desteklenmeyen cihazları içerdiği için ilke açılamaz.
10720516	Uygulama yüklüyken ofis biçimindeki dosyalarda bulunan ekler açılamayabilir.
10421967	Paylaşılan posta kutusu ayrı bir hesap olarak eklendiyse bu posta kutusunda oturum açılamaz.

Web eklentisi 14.2.0.8289 için düzeltilen sorunların listesi

Tanımlayıcı	Açıklama
9946286	Bir İnternet Denetimi kuralına web sitesi adresi eklerken etki alanı ile etki alanı bölgesi arasında nokta bulunmayan bir maske kullanılamaz.
10054657 10507166	Yeni sürüme geçildikten sonra bazı bileşenler (örneğin Aygıt Denetimi ve Uygulama Denetimi) ilke aracılığıyla yönetilemez.
10084390	Aygıt Denetimi bileşeninin ayarlarında **Sabit sürücü** aygıt türü yinelenir ve bu durum kullanıcıların sabit sürücülerinin engellenmesine neden olur.
10113718	Bazı durumlarda özel Güvenlik Duvarı kuralları görüntülenmez.
10311613	Ana Bilgisayar Yetkisiz Erişim Önleme bileşeninin ayarlarında, `*` karakteri kullanılarak bir maske aracılığıyla korunan kaynak eklenemez.
10391923	Uygulama Denetiminde, bir dosyanın MD5 karma değerine dayalı bir uygulama kategorisi oluşturulurken bu kategorinin geçersiz olduğunu ve çalışmayacağını belirten bir uyarı görüntülenmez.
10571790	Uygulama Denetimi bileşeninin **Kurallar listesi hariç tümüne izin ver** modundaki engelleme kuralları listesinin başlığı düzeltildi.
10592891 10689065	Güvenilir bölgede, **Kötü Amaçlı Yazılım Taraması istisnaları** bölümündeki istisnalar için **Yorum** alanı görüntülenmez.
10613015 10689049 10592534	Aygıt Denetimi bileşeninde, güvenilir cihazlar için **Yorum** alanı görüntülenmez.
10645068 10689057	KEY biçimindeki bir anahtar dosyası seçilirse *Anahtarı kaldır* görevi çalışmaz.
10685370 10685422	Aygıt Denetimi bileşeninde, listede aynı ada sahip bir cihaz zaten varsa güvenilir cihazlar listesine yeni bir cihaz eklenemez.
10721136	Zamanlama ayarlarında tamamlanma tarihi belirtilmezse grup görevleri kaydedilemez.
10753509	Aygıt Denetimi bileşeninde güvenilir cihazlara ilişkin kullanıcı ve grup listesinin değiştirilmesi, kayıt türlerini değiştirebilir ve ayarların artık cihaz için geçerli olmamasına neden olabilir.
10773402	Bazı durumlarda, bozuk profiller nedeniyle ilke ayarlarında yapılan değişiklikler kaydedilmeyebilir.
10822620	Şifreleyiciye Karşı Koruma bileşeninin ayarları ilkede görüntülenmez ve bildirim ayarlarında yapılan değişiklikler kaydedilmez.
10817035	Bir alt ilkede, bu ayar üst ilkede devre dışı bırakılmış olsa bile (kapalı "asma kilit") güvenilir bir cihaz eklenebilir. Ancak eklenen cihaz kaydedilmez.
10678009	Kaspersky Endpoint Security web eklentisinde, daha önce IP adresi aralığı kullanılarak bir kural oluşturulmuşsa ilkeye yeni bir Güvenlik Duvarı kuralı eklenemez.

14.1 sürümünde düzeltilen sorunların listesi

Tanımlayıcı	Açıklama
10140523	Windows 11'de Yerel NVMe'nin etkinleştirilmesi, kararsız uygulama davranışına neden olabilir.
9340076	Uygulamanın yüklü olduğu ve Dosya Şifreleme bileşeninin etkinleştirildiği bir aygıtta, başka bir aygıttan değiştirildikten sonra Windows Gezgini ağ klasörünün içeriğini otomatik olarak yenilemez.
9722863	Aygıt Denetimi raporu USB belirteci bağlantı kesme olayını içermez.
10006481	Gelen trafiği reddeden bir kural uygulandıktan sonra, harici hizmetlere olan etkin TCP bağlantıları hatalı zaman aşımı hesaplaması nedeniyle zamanından önce sonlandırılabilir.
10140912	Uygulama BHT1100B PDA aygıtını algılamaz.
10157563	Folder Redirection VDI iş istasyonlarında yeniden başlatmadan sonra çalışmayabilir.
10158494	Aygıt Denetimi, çıkarılabilir bir aygıtın fiziksel olarak yeniden bağlanması olmadan birden fazla bağlantı ve bağlantı kesme olayını günlüğe kaydeder.

Sıkça sorulan sorular

GENEL

Kaspersky Endpoint Security hangi bilgisayarlarda çalışır?

Son sürümden buyana neler değişti?

Kaspersky Endpoint Security başka hangi Kaspersky uygulamalarını çalıştırabilir?

Kaspersky Endpoint Security çalışırken bilgisayar kaynaklarını nasıl koruyabilirim?

DAĞITIM

Kaspersky Endpoint Security'yi bir kuruluşun tüm bilgisayarlarına nasıl yüklerim?

Komut satırından hangi yükleme ayarları yapılandırılabilir?

Kaspersky Endpoint Security'yi uzaktan nasıl kaldırabilirim?

GÜNCELLEME

Veritabanlarını güncellemek için hangi yöntemleri kullanılabilir?

Bir güncelleme sonrasında sorunlar ortaya çıkarsa ne yapmalıyım?

Kurumsal ağın dışındaki veritabanlarını nasıl güncelleyebilirim?

Güncellemeler için bir proxy sunucusu kullanmak mümkün müdür?

GÜVENLİK

Kaspersky Endpoint Security e-postaları nasıl tarar?

Güvenilir bir dosyayı taramaların dışında nasıl tutabilirim?

Bir bilgisayarı flaş sürücülerden gelebilecek virüslere karşı nasıl koruyabilirim?

Nasıl kullanıcıdan gizli bir kötü amaçlı yazılım taraması gerçekleştirebilirim?

Kaspersky Endpoint Security'nin korumasını nasıl geçici olarak duraklatabilirim?

Kaspersky Endpoint Security'nin yanlışlıkla sildiği bir dosyayı nasıl geri yükleyebilirim?

Kaspersky Endpoint Security'yi bir kullanıcı tarafından kaldırılmaya karşı nasıl korurum?

İNTERNET

Kaspersky Endpoint Security şifrelenmiş bağlantıları (HTTPS) tarar mı?

Kullanıcıların sadece güvenilir Wi-Fi ağlarına bağlanmasına nasıl izin veririm?

Sosyal ağları nasıl engellerim?

UYGULAMALAR

Bir kullanıcının bilgisayarında hangi uygulamaların yüklü olduğunu (envanter) nasıl öğrenebilirim?

Bilgisayar oyunlarının çalıştırılmasını nasıl önleyebilirim?

Uygulama Denetiminin doğru yapılandırıldığını nasıl doğrulayabilirim?

Bir uygulamayı güvenilir listesine nasıl ekleyebilirim?

AYGITLAR

Flaş belleklerin kullanımını nasıl engelleyebilirim?

Bir aygıtı güvenilir listesine nasıl ekleyebilirim?

Engellenen bir aygıta erişim elde etmek mümkün müdür?

ŞİFRELEME

Hangi koşullar altında şifreleme mümkündür?

Bir arşive erişimi bir parola ile nasıl kısıtlayabilirim?

Şifreleme ile akıllı kartlar ve belirteçler kullanmak mümkün müdür?

Kaspersky Security Center ile bağlantı olmadığında şifrelenmiş verilere erişim kazanmak mümkün müdür?

Bilgisayarın işletim sistemi çöktüğü halde veriler şifreli kalırsa ne yapmalıyım?

DESTEK

Rapor dosyası nerede raporlanır?

Nasıl bir iz dosyası oluşturabilirim?

Döküm yazımını nasıl etkinleştirebilirim?

Kaspersky Endpoint Security for Windows

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.

Uygulama, otomatik kontrol sistemleri içeren teknolojik süreçlerde kullanılmak üzere tasarlanmamıştır. Bu tür sistemlerdeki cihazları korumak için Kaspersky Industrial CyberSecurity for Nodes uygulamasının kullanılması önerilir.

Tehdit tespit etme teknolojileri



Makine öğrenimi

Kaspersky Endpoint Security makine öğrenimi tabanlı bir model kullanır. Bu model Kaspersky uzmanları tarafından geliştirilmiştir. Ardından, model sürekli olarak KSN'den gelen tehdit verileriyle beslenir (model eğitimi).



Bulut analizi

Kaspersky Endpoint Security tehdit verilerini Kaspersky Security Network'ten alır. *Kaspersky Security Network (KSN)*; dosyaların, İnternet kaynaklarının ve yazılımın tanınırlığı hakkında bilgiler içeren çevrimiçi Kaspersky Bilgi Bankasına erişim sağlayan bir bulut hizmetleri altyapısıdır.



Uzman analizi

Kaspersky Endpoint Security, Kaspersky virüs analistleri tarafından eklenen tehdit verilerini kullanır. Virüs analistleri, bir nesnenin tanınırlığının otomatik olarak belirlenip belirlenemeyeceğini değerlendirir.



Davranış analizi

Kaspersky Endpoint Security, bir nesnenin etkinliğini gerçek zamanlı olarak analiz eder.



Otomatik analiz

Kaspersky Endpoint Security, verileri otomatik nesne analiz sisteminden alır. Sistem, Kaspersky'ye gönderilen tüm nesneleri işler. Sistem daha sonra nesnenin tanınırlığını belirler ve verileri antivirüs veritabanlarına ekler. Sistem nesnenin tanınırlığını belirleyemezse, sistem Kaspersky virüs analistlerine sorgu gönderir.



Sandbox

Kaspersky Endpoint Security, nesneyi sanal bir makinede işler. Kaspersky Sandbox nesnenin davranışını analiz eder ve tanınırlığı hakkında bir karar verir. Bu teknoloji sadece Kaspersky Sandbox çözümü ile kullanılabilir.



Cloud Sandbox

Kaspersky Endpoint Security, nesneleri Kaspersky tarafından sağlanan yalıtılmış bir ortamda tarar. Cloud Sandbox teknolojisi kalıcı olarak etkinleştirilir ve kullandıkları lisans türünden bağımsız olarak tüm Kaspersky Security Network kullanıcıları tarafından kullanılabilir. Endpoint Detection and Response çözümünü zaten dağıttıysanız Cloud Sandbox tarafından algılanan tehditler için ayrı bir sayaç etkinleştirebilirsiniz.

Seçim ağacı

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

Bölüm	Bileşen
Temel Tehdit Koruması 	**Dosya Tehdidi Koruması** Dosya Tehdidi Koruması bileşeni, bir bilgisayar dosya sistemine bulaşmasını önlemenizi sağlar. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni bilgisayarın RAM'inde kalıcı olarak bulunur ve açılan, kaydedilen veya çalıştırılan tüm dosyaları gerçek zamanlı olarak tarar. Bu bileşen, bağlı sürücüler de dahil olmak üzere tüm bilgisayar sürücülerindeki dosyaları tarar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar. **Web Tehdidi Koruması** Web Tehdidi Koruması bileşeni, internetten zararlı dosyaların indirilmesini önler ve ayrıca zararlı ve kimlik avı amaçlı web sitelerine bağlantıyı engeller. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar. **Posta Tehdidi Koruması** Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarının eklerinde virüsler ve diğer tehditler için tarama yapar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar. Posta Tehdidi Koruması hem gelen hem de giden mesajları tarayabilir. Uygulama, aşağıdaki posta istemcilerinde POP3, SMTP, IMAP ve NNTP'yi destekler: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Mozilla Thunderbird, MyOffice Mail ve R7-Office Organizer posta istemcilerindeki trafiği taramak için Kaspersky sertifikasını sertifika deposuna eklemeniz ve kendi sertifika deposunu seçmeniz gerekir. Posta Tehdidi Koruması, diğer protokolleri ve posta istemcilerini desteklemez. Posta Tehdidi Koruması her zaman mesajlara *protokol düzeyinde* erişim sağlayamayabilir (örneğin, Microsoft Exchange çözümünü kullanırken). Bu nedenle Posta Tehdidi Koruması, Microsoft Office Outlook için uzantı içerir. Uzantı, mesajların *posta istemcisi düzeyinde* taranmasına izin verir. Posta Tehdidi Koruması eklentisi, Outlook 2010, 2013, 2016, 2019, 2021, 2024 ve 365'in 32 bit ve 64 bit sürümlerini destekler. Arm tabanlı bilgisayarlarda, Posta Tehdidi Koruması uzantısı Outlook 2016, Outlook 2021, Outlook 2024 ve Arm64 için Outlook 365'in 32 bit ve 64 bit sürümlerini destekler. **Ağ Tehdidi Koruması** *Ağ Tehdidi Koruması* bileşeni (Ayrıca Intrusion Detection System, IDS olarak da adlandırılır), ağ saldırılarının karakteristik aktiviteleri için gelen ağ trafiğini izler. Uygulama kullanıcının bilgisayarına gerçekleştirilen bir ağ saldırısı tespit ederse, saldıran bilgisayarla ağ bağlantısını engeller. Şu anda bilinen ağ saldırısı türlerinin açıklamaları ve bunlara karşı koyma yolları, uygulama veritabanlarında sunulmaktadır. Ağ Tehdidi Koruması bileşeninin tespit ettiği ağ saldırıları listesi, veritabanı ve uygulama modülü güncellemeleri sırasında güncellenir. **Güvenlik Duvarı** Güvenlik Duvarı bileşeni, internet veya yerel ağ üzerinde çalışırken bir bilgisayara yetkisiz bağlantıları engeller. Güvenlik Duvarı aynı zamanda bilgisayardaki uygulamaların ağ etkinliklerini de denetler. Bu, kurumsal LAN'ınızı kimlik hırsızlığı ve diğer saldırılara karşı korumanızı sağlar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve önceden tanımlanmış *ağ kuralları* yardımıyla bilgisayar koruması sağlar. **BadUSB Saldırısı Önleme** BadUSB Saldırısı Önleme bileşeni, klavyeye öykünen virüslü USB aygıtların bilgisayara bağlanmasını engeller. **AMSI Koruması** AMSI Koruması bileşeni, Microsoft'un Antimalware Scan Interface işlevini desteklemeyi amaçlamaktadır. *Antimalware Scan Interface (AMSI)*, AMSI destekli üçüncü taraf uygulamaların, bu nesneleri ek bir tarama için Kaspersky Endpoint Security'ye göndermesine ve bu nesnelerin tarama sonuçlarını almasına (örneğin PowerShell komut dizileri) olanak tanır.

Bölüm	Bileşen
Gelişmiş Tehdit Koruması	**Kaspersky Security Network** *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. Kaspersky Security Network'e katılıyorsanız, KSN hizmetleri Kaspersky Endpoint Security'ye taranan web adreslerinin itibarı hakkında bilgi ve taranan dosyaların kategorisi ve tanınırlığı hakkında bilgi sağlar. **Davranış Tespiti** Davranış Tespiti bileşeni, bilgisayarınızdaki uygulamaların işlemleriyle ilgili veriler toplar ve bu bilgileri, performanslarını iyileştirmek için diğer koruma bileşenlerine sağlar. Davranış Tespiti bileşeni, uygulamalar için Davranış Akışı İmzalarından (BSS) yararlanır. Uygulama etkinliğinin bir davranış akımı imzasıyla eşleşmesi halinde Kaspersky Endpoint Security seçili duyarlı işlemi gerçekleştirir. Davranış akışı imzalarına dayanan Kaspersky Endpoint Security işlevi, bilgisayarınız için ileriye dönük etkili koruma sağlar. Davranış Tespiti bileşeni ayrıca bilgisayarın güvenliğini tehdit edebilecek uygulamaların işlemleri için ağ portlarını izler. Uygulama, anti-virüs veritabanları ile bu tür işlemler hakkında bilgi alır. **Şifreleyici Önleyici** Şifreleyici Önleyici bileşeni paylaşılan klasörlerdeki etkinliği analiz eder. Bu etkinlik, dış şifreleme için tipik olan bir davranış akışı imzasıyla eşleşirse Kaspersky Endpoint Security seçili eylemi gerçekleştirir. **Exploit Önleme** Exploit Önleme bileşeni, yönetici ayrıcalıklarını kullanmak ya da zararlı etkinlikler gerçekleştirmek amacıyla bilgisayardaki zayıf noktalardan faydalanan program kodunu tespit eder. Örneğin istismarcılar bir arabellek taşması saldırısı kullanabilir. İstismarcı bunu yapmak için savunmasız bir uygulamaya büyük miktarda veri gönderimi yapar. Bu verileri işleyen savunmasız uygulama da zararlı kodları çalıştırır. Bu saldırının sonucunda istismarcı zararlı bir yazılımın izinsiz yüklemesini başlatabilir. Yürütülebilir bir dosyanın hassas bir uygulama tarafından çalıştırılması girişimi kullanıcı tarafından gerçekleştirilmediyse Kaspersky Endpoint Security, bu dosyanın çalıştırılmasını engeller ve kullanıcıyı bilgilendirir. Exploit Önleme bileşeni ayrıca bilgisayarın güvenliğini tehdit edebilecek uygulamaların işlemleri için ağ portlarını izler. Uygulama, anti-virüs veritabanları ile bu tür işlemler hakkında bilgi alır. **Sunucu Yetkisiz Erişim Önleme** Sunucu Yetkisiz Erişim Önleme bileşeni, uygulamaların işletim sistemi için tehlikeli olabilecek işlemler yapmasını engeller ve işletim sistemi kaynaklarına ve kişisel verilere erişim üzerinde denetim sağlar. Bileşen, anti-virüs veritabanları ve Kaspersky Security Network bulut hizmetinin yardımıyla bilgisayar koruması sağlar. **Düzeltme Altyapısı** Düzeltme Altyapısı, Kaspersky Endpoint Security' bileşeninin işletim sisteminde zararlı yazılımların gerçekleştirdiği etkinlikleri geri almasını sağlar.
Güvenlik Denetimleri	**Uygulama Denetimi** Uygulama Denetimi, kullanıcıların bilgisayarlarındaki uygulamaların başlatılmasını yönetir. Böylece uygulamalar kullanılırken bir kurumsal güvenlik ilkesi uygulamak mümkün olur. Uygulama Denetimi ayrıca uygulamalara erişimi kısıtlayarak bilgisayara virüs bulaşma riskini azaltır. **Aygıt Denetimi** Aygıt Denetimi, bilgisayara yüklenen veya bağlanan aygıtlara (örneğin sabit sürücüler, kameralar veya Wi-Fi modülleri) kullanıcı erişimini yönetir. Bu, bu tür cihazlar bağlandığında bilgisayarı enfeksiyondan korumanıza ve veri kaybını veya veri sızıntılarını önlemenize olanak tanır. **İnternet Denetimi** İnternet Denetimi, web kaynaklarına kullanıcı erişimini yönetir. Böylece trafiğin azaltılmasına ve çalışma zamanının daha verimli kullanılmasına yardımcı olur. Bir kullanıcı İnternet Denetimi tarafından kısıtlanan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller veya bir uyarı gösterir. **Uyarlamalı Anomali Denetimi** Uyarlamalı Anomali Denetimi bileşeni, şirketin ağındaki bilgisayarlarda tipik olarak görülmeyen eylemleri izler ve engeller. Uyarlamalı Anomali Denetimi, tipik olmayan davranışı izlemek için kurallar dizisi kullanır (örneğin, *Microsoft PowerShell'in Office uygulamasından başlatılması* kuralı). Kurallar, Kaspersky uzmanları tarafından zararlı etkinliğin tipik senaryolarına dayanarak oluşturulur. Uyarlamalı Anomali Denetiminin her bir kuralı nasıl ele aldığını yapılandırabilirsiniz (örneğin, belirli iş akışı görevlerini otomatikleştiren PowerShell komut dizilerinin yürütülmesine izin vermek). Kaspersky Endpoint Security, uygulama veritabanlarıyla birlikte kurallar dizisini de günceller. **Günlük Denetimi** Günlük Denetimi, Windows olay günlüğü analizine göre korunan ortamın bütünlüğünü izler. Uygulama, sistemde tipik olmayan davranış belirtilerini tespit ettiğinde, bu davranış bir siber saldırı girişiminin göstergesi olabileceğinden yöneticiyi bilgilendirir. **Sistem Bütünlüğü İzleme** Sistem Bütünlüğü İzleme bileşeni, işletim sisteminde bilgisayar güvenliği ihlallerine işaret edebilecek değişiklikleri izler. Bu tür değişiklikler tespit edildiğinde, Kaspersky Endpoint Security ilgili olayları oluşturur ve yöneticiyi uyarır.

Bölüm	Bileşen
Görevler 	**Kötü Amaçlı Yazılım Taraması** Kaspersky Endpoint Security, bilgisayarı virüslere ve diğer tehditlere karşı tarar. Kötü Amaçlı Yazılım Taraması, örneğin düşük güvenlik düzeyi nedeniyle koruma bileşenleri tarafından tespit edilmeyen zararlı yazılımların yayılma olasılığını ortadan kaldırmaya yardımcı olur. **Veritabanlarının ve uygulama modüllerinin güncellemesi** Kaspersky Endpoint Security, güncellenen veritabanlarını ve uygulama modüllerini indirir. Güncelleme işlemi bilgisayarı en güncel virüsler ve diğer tehditlere karşı korur. Varsayılan olarak uygulama otomatik şekilde güncellenir ancak gerekirse veritabanları ve uygulama modüllerini manuel olarak güncelleyebilirsiniz. **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. **Uygulama Bütünlüğü Kontrolü** 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.
Veri Şifreleme 	**Dosya Düzeyinde Şifreleme** Bileşen, dosya şifreleme kuralları oluşturulmasına izin verir. Şifreleme için ön tanımlı klasörleri seçebilir, manuel olarak bir klasör seçebilir veya uzantıya göre dosyaları tek tek seçebilirsiniz. **Tam Disk Şifreleme** Bileşen, sabit sürücünün Kaspersky Disk Encryption veya BitLocker Drive Encryption kullanılarak şifrelenmesine izin verir. **Çıkarılabilir sürücüleri şifreleme** Bileşen, çıkarılabilir sürücülerdeki verilerin korunmasına izin verir. Tam Disk Şifreleme (FDE) veya Dosya Düzeyinde Şifreleme (FLE) kullanabilirsiniz.
Detection and Response 	**Endpoint Detection and Response Optimum** Kaspersky Endpoint Detection and Response Optimum çözümü için yerleşik aracı (bundan böyle "EDR Optimum" olarak anılacaktır). *Kaspersky Endpoint Detection and Response*, kuruluşun BT altyapısını gelişmiş siber tehditlere karşı korumaya yönelik bir çözümdür. Çözümün işlevselliği, yeni açıklar, fidye yazılımı, dosyasız saldırılar ve yasal sistem araçlarını kullanan yöntemler dahil olmak üzere gelişmiş saldırılara karşı koymak için tehditlerin otomatik olarak algılanması ile bu tehditlere yanıt verme yeteneğini birleştirir. Çözüm hakkında daha fazla bilgi almak için Kaspersky Endpoint Detection and Response Optimum Yardım içeriğine bakın. **Endpoint Detection and Response Expert** Kaspersky Endpoint Detection and Response Expert çözümü için yerleşik aracı (bundan böyle "EDR Expert" olarak anılacaktır). EDR Expert, EDR Optimum'a göre daha fazla tehdit izleme ve tehdit yanıtı işlevselliği sunar. Çözüm hakkında daha fazla bilgi almak için Kaspersky Endpoint Detection and Response Expert Yardım içeriğine bakın. **Endpoint Detection and Response Expert (on-premises)** ve **Network Detection and Response (KATA)** Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olan Endpoint Detection and Response ve Network Detection and Response bileşenlerini yönetmek için yerleşik aracılar. *Kaspersky Anti Targeted Attack Platform* hedeflenen saldırılar, gelişmiş sürekli tehditler (APT), sıfır gün saldırıları ve diğer karmaşık tehditleri zamanında tespit etmek üzere tasarlanmış bir çözümdür. Kaspersky Anti Targeted Attack Platform üç işlevsel birim içerir: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Tüm işlevsel birimleri veya tek tek işlevsel birimleri ayrı ayrı satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın. **Sandbox** Sandbox için yerleşik aracı. *Sandbox* bileşeni bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Sandbox Yardım ve Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın. **Managed Detection and Response** Kaspersky Managed Detection and Response çözümünün çalışmasını desteklemek için yerleşik aracı. *Kaspersky Managed Detection and Response (MDR)* çözümü, altyapınızdaki güvenlik olaylarını otomatik olarak algılar ve analiz eder. MDR bunu yapmak için uç noktalardan alınan telemetri verilerini ve makine öğrenimini kullanır. MDR, olay verilerini Kaspersky uzmanlarına gönderir. Uzmanlar daha sonra olayı işleyebilir ve mesela antivirüs veritabanlarına yeni bir giriş ekleyebilir. Alternatif olarak, uzmanlar olayın işlenmesiyle ilgili önerilerde bulunabilir ve mesela bilgisayarın ağdan izole edilmesini önerebilir. Çözümün nasıl çalıştığı hakkında ayrıntılı bilgi için lütfen Kaspersky Managed Detection and Response Yardım içeriğine bakın.

Uygulama modları: Standart, EDR Agent, Light Agent

Kaspersky Endpoint Security for Windows, birçok Kaspersky çözümünün bir parçasıdır. Çözüme bağlı olarak uygulama için bir mod seçmeniz gerekir.



Standart mod

Bu, uygulamanın ana ve varsayılan modudur. Kaspersky EPP çözümlerinin (Endpoint Protection Platform) bir parçası olarak uygulamayı bu modda yükleyebilirsiniz. Örneğin, Standart moddaki Kaspersky Endpoint Security, Kaspersky Endpoint Security for Business'ın bir parçasıdır. Kaspersky Endpoint Security, iş istasyonları ve sunucuların çeşitli tehditlere, ağ saldırılarına ve dolandırıcılıklara karşı kapsamlı bir şekilde korunmasını sağlar. Standart modda, EDR, MDR, KUMA ve diğerleri dahil olmak üzere Kaspersky Detection and Response çözümleriyle entegrasyon için yerleşik ajanlar da mevcuttur.



EDR Agent

Bu mod, Kaspersky Detection and Response çözümlerinin üçüncü taraf EPP çözümleriyle birlikte dağıtılmasını sağlar. Detection and Response çözümleri arasında Kaspersky Managed Detection and Response (MDR) ve Kaspersky Anti Targeted Attack Platform (KATA) vardır. EDR Agent, Kaspersky SIEM çözümü olan Kaspersky Unified Monitoring and Analysis Platform'u (KUMA) desteği de sunar.

Bu modda, Dosya Tehdidi Koruması veya Web Tehdidi Koruması gibi standart koruma bileşenleri kullanılamaz. Bilgisayarın standart koruması üçüncü taraf EPP çözümü tarafından sağlanır. EDR Agent bu bilgisayarlarda çalışan işlemleri, açık ağ bağlantılarını ve değiştirilen dosyaları sürekli olarak izler ve Detection and Response çözümleriyle etkileşime girer.



Light Agent

Bu mod sanal ortamları korumak için kullanılır. Light Agent modundaki Kaspersky Endpoint Security, Kaspersky Hybrid Cloud Security çözümünün bir parçasıdır. Light Agent, iş istasyonları ve sunucular için konuk işletim sistemlerine sahip sanal makineleri korur. Standart modda olduğu gibi aynı koruma ve kontrol bileşenleri bu modda da kullanılabilir. Aradaki fark, nesnelerin virüslere ve diğer kötü amaçlı yazılımlara karşı ayrı bir sanal makineye yüklenen özel bir çözüm bileşeni olan SVM (Secure Virtual Machine) tarafından taranmasıdır. Böylece Light Agent, sanal makinenin kaynakları yerine altyapının güvenliğini sağlamak için SVM'nin kaynaklarını kullanır.

Dağıtım kiti

Dağıtım kiti aşağıdaki dağıtım paketlerini içerir:

- **AES256**

  Bu dağıtım paketi, x86/x64 mimarisine sahip bilgisayarlara kurulmak üzere tasarlanmıştır. Bu dağıtım paketi, 256 bit etkin anahtar uzunluğuna sahip AES (Advanced Encryption Standard) şifreleme algoritmasını uygulayan şifreleme araçlarını içerir.

- **AES56**

  Bu dağıtım paketi, x86/x64 mimarisine sahip bilgisayarlara kurulmak üzere tasarlanmıştır. Bu dağıtım paketi, 56 bit etkin anahtar uzunluğuna sahip AES şifreleme algoritmasını kullanan şifreleme araçlarını içerir.

- **Arm64**

  Bu dağıtım paketi, Arm tabanlı bilgisayarlara kurulmak üzere tasarlanmıştır. Bu dağıtım paketi, sunuculara kurulmak üzere tasarlanmamıştır.

Yüklemeden önce, dağıtım paketinin işlemcinizin mimarisine uygun olduğundan emin olun. Dağıtım paketi işlemci mimarisiyle uyuşmuyorsa, yükleyici bir hata mesajı vererek yüklemeyi sonlandıracaktır.

Dağıtım paketi, EXE formatında kendiliğinden açılan bir arşivdir. Dağıtım paketinin içeriğini görüntülemek için, arşivi ayrı bir klasöre açmanız gerekir. Her bir dağıtım paketi aşağıdaki dosyaları içerir:

`kes_win.msi`	Kaspersky Endpoint Security kurulum paketi.
`setup_kes.exe`	Kullanılabilir yöntemlerden herhangi birini kullanarak uygulamaları yüklemek için gereken dosyalar.
`kes_win.kud`	Kaspersky Endpoint Security için kurulum paketleri oluşturma dosyası.
`klcfginst.msi`	Kaspersky Security Center Yönetim Konsolu'ndaki uygulama yönetimi eklentisi için kurulum paketi.
`bases.cab`	Kurulum sırasında kullanılan güncelleme paketi dosyaları.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Uyumsuz yazılımları kaldırma dosyaları.
`incompatible.txt`	Kaspersky Endpoint Security ile uyumluluk sorunlarına neden olabilecek yazılımların listesini içeren dosya. Kaspersky, Kaspersky Endpoint Security'nin listedeki yazılımlarla uyumluluğunu garanti etmez.
`ksn_<language ID>.txt`	Kaspersky Security Network'e katılma koşullarını okuyabileceğiniz dosya.
`license.txt`	Son Kullanıcı Lisans Sözleşmesi'ni ve Gizlilik İlkesi'ni okuyabileceğiniz dosya.
`installer.ini`	Dağıtım kitinin iç ayarlarını içeren dosya.
`kes.cab`	Uygulamanın grafik arabirimi için dosyalar.
`aes256.cab` / `aes56.cab`	AES şifreleme algoritması için dosyalar (Arm64 dağıtım paketine dahil değildir).
`package.kcat`	Uygulama dağıtım kitinin imzalarını içeren dosya. Dijital imza, uygulama dağıtım kitinin gerçekliğini ve bütünlüğünü garanti eder.

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

Donanım ve yazılım gereksinimleri

Bu makalede, uygulamanın üzerinde test edildiği ve doğru çalışmasının garanti edildiği yazılım sürümleri listelenmektedir. Uygulama diğer yazılım sürümleriyle de çalışabilir, ancak bu yapılandırmalar tam bir test döngüsünden geçirilmemiştir ve desteği garanti edilen sürümler listesine dahil edilmemiştir.

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

Uygulamayı yüklemek için bilgisayarda yönetici haklarına sahip olmanız gerekir.

Minimum genel gereksinimler

Minimum gereksinimler	İş istasyonu (x86/x64)	Sunucu (x86/x64)	Arm
Depolama	2 GB	2 GB	2 GB
İŞLEMCİ	1 GHz, SSE2 komut desteği	1,4 GHz, SSE2 komut desteği	1 GHz, Armv8.1 mimarisi
RAM	İş istasyonu (x86): 1 GB İş istasyonu (x64): 2 GB	2 GB Not: Kaspersky Anti Targeted Attack Platform ile entegrasyon için yerleşik ajanı içeren uygulamayı yüklemek üzere sunucuda 8 GB bellek gereklidir.	4 GB
Microsoft .NET Framework	4 veya üzeri	4 veya üzeri	4.8 veya üzeri

İş istasyonları

İş istasyonları için desteklenen işletim sistemleri:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise çoklu oturum
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise çoklu oturum
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Windows işletim sistemleri, sürüm 11 24H2'den başlayarak UDP Receive Segment Coalescing Offload (URO) teknolojisini desteklemektedir. Bilgisayarda uyumlu bir ağ kartı ve sürücüleri yüklüyse teknoloji varsayılan olarak etkindir. Bir kullanıcının bilgisayarında URO'nun devre dışı bırakılması uygulamanın performansını önemli ölçüde düşürebilir.

Kaspersky Endpoint Security'nin doğru şekilde çalıştığından emin olmak için, Windows Security Center (wscsvc) hizmeti kullanıcının bilgisayarında çalışıyor olmalıdır.

Kaspersky Endpoint Security, şu işletim sistemi güncellemeleri yüklü olmadığında Microsoft Windows 7'ye yüklenemez: KB4490628 (12 Mart 2019) ve KB4474419 (23 Eylül 2019). Ayrıntılı bilgi için Teknik Destek Bilgi Tabanına bakın.

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

Microsoft Windows 11 işletim sistemi desteği hakkında ayrıntılar için lütfen Teknik Destek Bilgi Bankası'na bakın.

Sunucular

Kaspersky Endpoint Security, sunucular için olan Windows işletim sistemini çalıştıran bilgisayarlarda uygulamanın temel bileşenlerini destekler. Kuruluşunuzun sunucularında ve kümelerinde Kaspersky Security for Windows Server yerine Kaspersky Endpoint Security for Windows'u kullanabilirsiniz (Cluster Mode). Uygulama ayrıca Server Core Mode desteği sunuyor (bkz. bilinen sorunlar).

Sunucular için desteklenen işletim sistemleri:

- Windows Small Business Server 2011 Essentials / Standard (64 bit)

  Microsoft Small Business Server 2011 Standard (64-bit), ancak Microsoft Windows Server 2008 R2 için Service Pack 1 yüklüyse desteklenir.

- Windows MultiPoint Server 2011 (64 bit)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2016 Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2019 Essentials / Standard / Datacenter (Server Core modu dahil)

- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Server Core modu dahil)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security, şu işletim sistemi güncellemeleri yüklü olmadığında Microsoft Windows Server 2008 R2 üzerine yüklenemez: KB4490628 (12 Mart 2019) ve KB4474419 (23 Eylül 2019).

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

Microsoft Windows Server 2022 işletim sistemi desteği hakkında ayrıntılar için lütfen Teknik Destek Bilgi Bankası'na bakın.

Sunucular için desteklemeyen işletim sistemleri:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Sanal platformlar

Standart modda uygulama çalışması için desteklenen sanal platformlar:

- VMware Workstation Pro 15.5.2
- VMware ESXi 7.0 Yama Sürümü ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Uygulama, Hyper-V kullanılarak oluşturulan Windows 11 Pro Arm64 işletim sistemini çalıştıran sanal makineleri desteklemektedir.

Light Agent'ı yüklemek için sanal makineler

Arm tabanlı sanal makinelerde Kaspersky Endpoint Security'nin Light Agent modunda kurulumu desteklenmemektedir.

Sanal makinelerdeki BIOS, SMBIOS spesifikasyonu sürüm 2.1 veya üstünü desteklemelidir.

Aşağıdaki paketler ve yardımcı programlar sanal makinelere yüklenmelidir:

- Microsoft Hyper-V - Integration Services paketini kullanırken.
- VMware vSphere - VMware Tools paketini kullanırken.
- XenServer - XenTools paketini kullanırken.
- HUAWEI FusionSphere - HUAWEI Tools paketini kullanırken.
- KVM tabanlı hiper yöneticiler kullanılırken – QEMU Guest Agent.

Uygulamayı Light Agent modunda çalıştırmak için sanal altyapı gereksinimleri için Kaspersky Security for Virtualization Light Agent Yardım bölümüne bakın.

Uygulamanın düzgün çalışması için en az 100 Mbit/s bant genişliğine sahip sanallaştırılmış bir arabirim kullanın.

Terminal sunucuları

Desteklenen terminal sunucusu türleri:

- Windows Server 2008 R2 SP1 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Windows Server 2012 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Windows Server 2012 R2 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Windows Server 2016 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Windows Server 2019 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Windows Server 2022 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Windows Server 2025 tabanlı Microsoft Uzak Masaüstü Hizmetleri
- Citrix Virtual Apps and Desktops 7 2507 LTSR'deki Citrix RDSH

Kaspersky Security Center desteği

Kaspersky Endpoint Security, şu Kaspersky Security Center sürümleri ile çalışmayı destekler:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

İşletim sistemi türüne göre kullanılabilir uygulama özellikleri karşılaştırması

Kullanılabilir Kaspersky Endpoint Security özellikleri, işletim sisteminin türüne bağlıdır: iş istasyonu veya sunucu (aşağıdaki tabloya bakın).

Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, kurulum paketinde farklı işletim sistemi türleri için farklı bileşen setleri yapılandırabilirsiniz. Yani, uygulamayı aynı kurulum paketini kullanarak iş istasyonlarına ve sunuculara dağıtabilirsiniz.

Arm tabanlı sanal makinelerde Kaspersky Endpoint Security'nin Light Agent modunda kurulumu desteklenmemektedir.

Kaspersky Endpoint Security özellikleri karşılaştırması

Özellik	İş istasyonu	ARM tabanlı iş istasyonu	Sunucu	Server Core modu
Gelişmiş Tehdit Koruması				
Kaspersky Security Network	✓	✓	✓	✓

Özellik	İş istasyonu	ARM tabanlı iş istasyonu	Sunucu	Server Core modu
Davranış Tespiti	✓	✓	✓	✓
Şifreleyici Önleyici	✓	✓	✓	✓
Exploit Önleme	✓	✓	✓	✓
Sunucu Yetkisiz Erişim Önleme	✓	✓	–	–
Düzeltme Altyapısı	✓	✓	✓	✓
Temel Tehdit Koruması				
Dosya Tehdidi Koruması	✓	✓	✓	✓
Web Tehdidi Koruması	✓	✓	✓	–
Posta Tehdidi Koruması	✓	✓	✓	–
Güvenlik Duvarı	✓	✓	✓	✓
Ağ Tehdidi Koruması	✓	✓	✓	✓
BadUSB Saldırısı Önleme	✓	✓	✓	–
AMSI Koruması	✓	✓	✓	✓
Güvenlik Denetimleri				
Günlük Denetimi	–	–	✓	–
Uygulama Denetimi	✓	✓	✓	✓
Aygıt Denetimi	✓	✓	✓	✓
İnternet Denetimi	✓	✓	✓	–
Uyarlamalı Anomali Denetimi	✓	✓	–	–
Sistem Bütünlüğü İzleme	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Veri Şifreleme				
Kaspersky Disk Encryption	✓	–	–	–
BitLocker Drive Encryption.	✓	✓	✓	✓
Dosya Düzeyinde Şifreleme	✓	–	–	–
Çıkarılabilir sürücüleri şifreleme	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
KUMA Entegrasyonu	✓	✓	✓	✓

Yönetim araçlarına bağlı olarak uygulama işlevlerinin karşılaştırılması

Kaspersky Endpoint Security'de kullanılabilecek işlevler, yönetim araçlarına bağlıdır (aşağıdaki tabloya bakın).

Uygulamayı, Kaspersky Security Center'ın şu konsollarını kullanarak yönetebilirsiniz:

- Yönetim Konsolu. Microsoft Yönetim Konsolu (MMC) yöneticinin iş istasyonuna ek bileşen olarak yüklenmiştir.
- Web Console. Kaspersky Security Center'ın Yönetim Sunucusuna yüklenmiş bileşenidir. Herhangi bir bilgisayardaki tarayıcıyı kullanarak Web Console'da çalışabilirsiniz.

Uygulamayı, Kaspersky Security Center Cloud Console kullanarak da yönetebilirsiniz. *Kaspersky Security Center Cloud Console*, Kaspersky Security Center'ın bulur sürümüdür. Yani Yönetim Sunucusu ve diğer Kaspersky Security Center bileşenleri, Kaspersky'nin bulut altyapısına yüklenmiştir. Uygulamayı Kaspersky Security Center Cloud Console kullanarak yönetmekle ilgili ayrıntılı bilgiler için Kaspersky Security Center Cloud Console Yardım'ına başvurun.

Kaspersky Endpoint Security, Kaspersky Next Pro View çözümünün bir parçasıdır. Bu çözümün bir parçası olarak çalıştığında mevcut uygulama özellikleri hakkında daha fazla bilgi için Kaspersky Next Yardım içeriğine bakın.

Kaspersky Endpoint Security özellikleri karşılaştırması

Özellik	Kaspersky Security Center		Kaspersky Security Center
	Yönetim Konsolu	Web Console	Cloud Console
Gelişmiş Tehdit Koruması			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Davranış Tespiti	✓	✓	✓
Şifreleyici Önleyici			
Exploit Önleme	✓	✓	✓
Sunucu Yetkisiz Erişim Önleme	✓	✓	✓
Düzeltme Altyapısı	✓	✓	✓
Temel Tehdit Koruması			
Dosya Tehdidi Koruması	✓	✓	✓
Web Tehdidi Koruması	✓	✓	✓
Posta Tehdidi Koruması	✓	✓	✓
Güvenlik Duvarı	✓	✓	✓
Ağ Tehdidi Koruması	✓	✓	✓
BadUSB Saldırısı Önleme	✓	✓	✓
AMSI Koruması	✓	✓	✓
Güvenlik Denetimleri			
Günlük Denetimi	✓	✓	✓
Uygulama Denetimi	✓	✓	✓
Aygıt Denetimi	✓	✓	✓
İnternet Denetimi	✓	✓	✓
Uyarlamalı Anomali Denetimi	✓	✓	✓
Sistem Bütünlüğü İzleme	✓	✓	✓
Cloud Discovery	–	–	✓
Veri Şifreleme			
Kaspersky Disk Encryption	✓	✓	–
BitLocker Drive Encryption.	✓	✓	✓

Özellik	Kaspersky Security Center		Kaspersky Security Center
	Yönetim Konsolu	Web Console	Cloud Console
Dosya Düzeyinde Şifreleme	✓	✓	–
Çıkarılabilir sürücüleri şifreleme	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
KUMA Entegrasyonu	✓	✓	✓
Görevler			
Anahtar ekle	✓	✓	✓
Uygulama bileşenlerini değiştirme	✓	✓	✓
Envanter	✓	✓	✓
Güncelle	✓	✓	✓
Güncellemeyi geri alma	✓	✓	✓
Kötü Amaçlı Yazılım Taraması	✓	✓	✓
Uygulama Bütünlüğü Kontrolü	✓	✓	–
Verileri sil	✓	✓	✓
Kimlik Doğrulama Aracısı hesaplarını yönet (Kaspersky Disk Encryption)	✓	✓	–
IOC Taraması (EDR)	–	✓	✓
Dosyayı Karantinaya taşı (EDR)	–	✓	✓
Dosyayı al (EDR)	–	✓	✓
Dosyayı sil (EDR)	–	✓	✓
İşlemi başlat (EDR)	–	✓	✓
İşlemi sonlandır (EDR)	–	✓	✓

Diğer uygulamalarla uyumluluk

Kaspersky Endpoint Security, bazı Kaspersky uygulamalarının yanı sıra bazı üçüncü taraf uygulamalarıyla da uyumsuzdur. Bu nedenle, uygulama sürümünü yüklemeden, güncellemeden ve uygulama bileşenlerini değiştirmeden önce Kaspersky Endpoint Security, bu tür uygulamaların mevcut olup olmadığını görmek için bilgisayarı tarar.

Üçüncü taraf uygulamalarla uyumluluk

Kaspersky Endpoint Security, üçüncü taraf uç nokta koruma sistemlerinin (Endpoint Protection Platform, EPP) bir parçası olan uygulamalarla uyumlu değildir. Kaspersky Endpoint Security diğer uygulamalarla da uyumluluk sorunları yaşayabilir. Uyumluluğu belirlemek için Kaspersky Endpoint Security, Kaspersky tarafından hazırlanan bir yazılım listesine başvurur. Bu liste incompatible.txt dosyasında yer alır. Bu dosya dağıtım kitine dahil edilmiştir.

Kaspersky, Kaspersky Endpoint Security'nin listedeki yazılımlarla uyumluluğunu garanti etmez. Listede bir uygulama bulunursa, yükleyici Kaspersky Endpoint Security dağıtımını durdurur. Yükleyici bazı uygulamaları listeden otomatik olarak silebilir. Riskleri göz ardı etmek istiyor ve Kaspersky Endpoint Security ile listedeki bir yazılımı aynı bilgisayara yüklemek istiyorsanız bilgisayar kontrolünü atlayabilirsiniz (aşağıdaki talimatlara bakın).

INCOMPATIBLE.TXT DOSYASINI İNDİRİN

Kaspersky uygulamaları ile uyumluluk

Kaspersky Endpoint Security, aşağıdaki Kaspersky uygulamaları ile uyumlu değildir:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform ve Kaspersky Endpoint Detection and Response çözümlerinin bir parçası olarak Endpoint Sensor.
- Kaspersky Endpoint Agent, Kaspersky'nin Detection and Response çözümlerinin bir parçasıdır.

  Kaspersky, tüm Detection and Response işlemlerini Kaspersky Endpoint Agent yerine Kaspersky Endpoint Security bütünleşik aracısıyla çalışmaya geçiriyor. Uygulama, 12.1 sürümünden itibaren tüm Detection and Response çözümlerini desteklemektedir.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server

  Kaspersky Endpoint Security 12.0 ile başlayarak Kaspersky Security for Windows Server'dan Kaspersky Endpoint Security for Windows'a geçebilir ve iş istasyonları ile sunucuları korumak için tek bir çözüm kullanabilirsiniz.

- Kaspersky Embedded Systems Security.

Bu listedeki Kaspersky uygulamaları bilgisayarda yüklüyse Kaspersky Endpoint Security bu uygulamaları kaldırır. Kaspersky Endpoint Security'yi yüklemeye devam etmeden önce lütfen bu işlemin tamamlanmasını bekleyin.

Uyumluluk sorunlarına neden olabilecek yazılımlar için kontrolü atlama

Kaspersky Endpoint Security incompatible.txt listesinden bir yazılım algılarsa, uygulamanın yüklenmesi sonlandırılır. Kuruluma devam etmek için bu uygulamayı kaldırmanız gerekir. Ancak, üçüncü taraf yazılım satıcısı belgelerinde yazılımlarının Endpoint Protection Platform (EPP) ile uyumlu olduğunu belirtmişse, Kaspersky Endpoint Security'yi bu satıcının uygulamasının kurulu olduğu bir bilgisayara yükleyebilirsiniz. Örneğin, Endpoint Detection and Response (EDR) çözüm sağlayıcısı, üçüncü taraf EPP sistemleriyle uyumluluklarını beyan edebilir. Bu durumda, Kaspersky Endpoint Security kurulumunu bir yüklü yazılım kontrolü çalıştırmadan başlatmanız gerekir. Bunu yapmak için yükleyiciye aşağıdaki parametreleri aktarın:

- `SKIPPRODUCTCHECK=1`. Yüklü yazılım kontrolünü devre dışı bırakın. Uyumluluk sorunlarına neden olabilecek yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında yer alır. Bu parametre için herhangi bir değer ayarlanmazsa ve listeden bir yazılım tespit edilirse Kaspersky Endpoint Security kurulumu sonlandırılır.

- `SKIPPRODUCTUNINSTALL=1`. Tespit edilen yazılımın incompatible.txt listesinden otomatik olarak kaldırılmasını devre dışı bırakın. Bu parametre için herhangi bir değer ayarlanmazsa Kaspersky Endpoint Security, uyumluluk sorunlarına neden olabilecek yazılımı kaldırmaya çalışır.

- `CLEANERSIGNCHECK=0`. Kontrolde bulunan uygulamaların dijital imza doğrulamasını devre dışı bırakın. Bu parametre ayarlanmazsa uygulama Kaspersky Security Center aracılığıyla dağıtılırken dijital imzaların doğrulanması devre dışı bırakılır. Uygulama yerel olarak yüklendiğinde, dijital imza doğrulaması varsayılan olarak etkindir.

Uygulamayı yerel olarak yüklerken parametreleri komut satırından aktarabilirsiniz.

Yükleme işlemi sırasında uyumluluk sorunlarına neden olabilecek yazılımlar için taramayı atladıysanız Kaspersky Endpoint Security, uygulama bileşenleri değiştiğinde bu kontrolü tekrar gerçekleştirebilir. Yüklü yazılım taramasını atlamak için *Uygulama bileşenlerini değiştir* görevini yapılandırmanız gerekir.

Örnek:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Kaspersky Endpoint Security'yi uzaktan yüklemek için `[Setup]` bölümünde `kes_win.kud` isimli yükleme paketi oluşturma dosyasına uygun parametreleri eklemeniz gerekir (aşağıda). `kes_win.kud` dosyası dağıtım kitine dahil edilmiştir.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Uygulamayı yükleme ve kaldırma

Kaspersky Endpoint Security bilgisayara şu yollarla yüklenebilir:

- Kurulum Sihirbazını kullanarak yerel olarak.
- komut satırını kullanarak yerel olarak.
- Kaspersky Security Center kullanarak uzaktan.
- Microsoft Windows Grup İlkesi Yönetimi Düzenleyicisini kullanarak uzaktan (ayrıntılar için Microsoft Teknik Destek web sitesini ziyaret edin).
- System Center Configuration Manager kullanarak uzaktan.

Uygulama yükleme ayarlarını birkaç şekilde yapılandırabilirsiniz. Ayarları yapılandırmak için aynı anda birden fazla yöntem kullanmanız durumunda Kaspersky Endpoint Security en yüksek önceliğe sahip olan ayarları uygular. Kaspersky Endpoint Security tarafından uygulanan öncelik sıralaması şöyledir:

1. setup.ini dosyasından alınan ayarlar.
2. installer.ini dosyasından alınan ayarlar.
3. Komut satırından alınan ayarlar.
4. Yapılandırma dosyasından (install.cfg) alınan ayarlar.

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

Kaspersky Endpoint Security'yi yüklerken, işletim sistemi kendi mesajlarını gösterebilir. Uygulama yüklenirken ağ ve İnternet bağlantıları da kesintiye uğrayabilir.

Kaspersky Endpoint Security yüklenirken, güncellenirken veya kaldırılırken hatalar oluşabilir. Bu hataları çözme hakkında daha fazla bilgi için lütfen Teknik Destek Bilgi Tabanına bakın.

Kaspersky Security Center vasıtasıyla dağıtım

Kaspersky Endpoint Security, kurumsal ağ içindeki bilgisayarlara çeşitli şekillerde dağıtılabilir. Kuruluşunuz için en uygun dağıtım senaryosunu seçebilir veya aynı anda birkaç dağıtım senaryosunu birleştirebilirsiniz. Uygulamayı yüklemeden önce, Kaspersky Security Center Network Agent'ın bilgisayarda yüklü olduğundan emin olmalısınız. *Ağ Aracısı* Yönetim Sunucusu ile istemci bilgisayar arasındaki etkileşimi kolaylaştırır.

Kaspersky Security Center, aşağıdaki ana dağıtım yöntemlerini destekler:

- Uygulamayı, Koruma Dağıtım Sihirbazını kullanarak yükleme.

  Standart kurulum yöntemi Kaspersky Endpoint Security'nin varsayılan ayarlarından memnunsanız ve kuruluşunuzda özel yapılandırma gerektirmeyen basit bir altyapıya sahipseniz uygundur.

- Uygulamayı, uzaktan kurulum görevini kullanarak yükleme.

  Evrensel kurulum yöntemi, Kaspersky Endpoint Security ayarlarını yapılandırmayı ve uzaktan kurulum görevlerini esnek bir şekilde yönetmeyi sağlar. Kaspersky Endpoint Security'nin kurulumu aşağıdaki adımlardan oluşur:

  1. Kurulum paketi oluşturma.
  2. Uzaktan kurulum görevi oluşturma.

Kaspersky Security Center, işletim sistemi görüntüsü içinden dağıtım gibi Kaspersky Endpoint Security'nin diğer kurulum yöntemlerini de destekler. Diğer dağıtım yöntemleri hakkında ayrıntılar için Kaspersky Security Center Yardım içeriğine bakın.

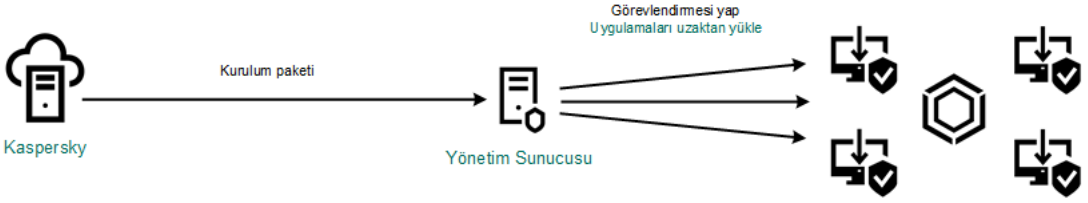
Uygulamanın standart kurulumu

Kaspersky Security Center, uygulamayı kurumsal bilgisayarlara yüklemek için bir Koruma Dağıtım Sihirbazı sağlar. Koruma Dağıtım Sihirbazı aşağıdaki ana işlemleri içerir:

1. Bir Kaspersky Endpoint Security kurulum paketi seçme.

   Yükleme paketi Kaspersky uygulamasının Kaspersky Security Center üzerinden uzaktan kurulumu için oluşturulan bir dosya grubudur. Kurulum paketi, uygulamayı yüklemek ve kurulumdan hemen sonra çalışmasını sağlamak için gereken çeşitli ayarları içerir. Kurulum paketi, uygulama dağıtım kitinde bulunan .kpd ve .kud uzantılı dosyalar kullanılarak oluşturulur. Kaspersky Endpoint Security kurulum paketi, desteklenen tüm Windows sürümleri ve işlemci mimarisi türleri için ortaktır.

2. Kaspersky Security Center Yönetim Sunucusunun *Uygulamayı uzaktan yükle* görevini oluşturma.



Kaspersky Endpoint Security dağıtımı

Yönetim Konsolu'ndaki (MMC) Koruma Dağıtım Sihirbazı nasıl kullanılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında, **Gelişmiş** → **Uzaktan kurulum** seçeneğini belirleyin.
3. **Kurulum paketini yönetilen cihazlara dağıt (iş istasyonları)** bağlantısına tıklayın.

Bu, Koruma Dağıtım Sihirbazını başlatır. Sihirbazın talimatlarını uygulayın.

İstemci bilgisayarda 139 ve 445 numaralı TCP portları ile 137 ve 138 numaralı UDP portları açılmalıdır.

1. Adım. Kurulum paketi seçme

Listeden Kaspersky Endpoint Security kurulum paketini seçin. Listede Kaspersky Endpoint Security kurulum paketi yoksa paketi Sihirbazdan oluşturabilirsiniz.

Kaspersky Security Center'da kurulum paketi ayarlarını yapılandırabilirsiniz. Örneğin bir bilgisayara yüklenecek uygulama bileşenlerini seçebilirsiniz.

Ağ Aracısı ayrıca Kaspersky Endpoint Security ile birlikte yüklenecektir. *Ağ Aracısı* Yönetim Sunucusu ile istemci bilgisayar arasındaki etkileşimi kolaylaştırır. Ağ Aracısı zaten bilgisayara yüklüyse yeniden yüklenmez.

2. Adım. Kurulum paketi kaynağını seçme

Kaspersky Security Center paketini dağıt kaynağını seçin.

3. Adım. Kurulum için aygıtlar seçme

Kaspersky Endpoint Security'nin yükleneceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Ağ Aracısı, atanmamış cihazlara yüklenmemiştir. Bu durumda, görev belirli cihazlara atanır. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Uzak kurulum görevi ayarlarını tanımlama

Şu ek uygulama ayarlarını yapılandırın:

- **Kurulum paketini indirmeye zorla**. Uygulama kurulum yöntemini seçin:
  - **Ağ Aracısı'nı kullanarak**. Ağ Aracısı, Kaspersky Endpoint Security kurulum paketini istemci bilgisayarlara dağıtmaktan sorumludur. Ağ Aracısı yüklü değilse, görev bir hata ile sonlanacaktır. Bu durumda, Ağ Aracısı kurulum paketini *Uygulamayı uzaktan yükle* görevine ekleyin ve işletim sistemi kaynakları aracılığıyla dosya aktarımını etkinleştirin. Ardından Ağ Aracısı, işletim sistemi kaynakları kullanılarak yüklenecektir. Ardından Ağ Aracısı araçları tarafından Kaspersky Endpoint Security yüklenir.
  - **Dağıtım noktaları aracılığıyla işletim sistemi kaynaklarını kullanarak**. Kurulum paketi, dağıtım noktaları aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağda en az bir dağıtım noktası varsa bu seçeneği belirleyebilirsiniz. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.
  - **Yönetim Sunucusu aracılığıyla işletim sistemi kaynaklarını kullanarak**. Dosyalar, Yönetim Sunucusu aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağ Aracısı, istemci bilgisayarda yüklü değilse ancak istemci bilgisayar, Yönetim Sunucusu ile aynı ağdaysa bu seçeneği belirleyebilirsiniz.
- **Diğer Yönetim Sunucularıyla yönetilen cihazlar için davranış**. Kaspersky Endpoint Security kurulum paketini seçin. Ağda birden fazla Yönetim Sunucusu yüklüyse bu Yönetim Sunucuları aynı istemci bilgisayarlarını görebilir. Bu, örneğin bir uygulamanın aynı istemci bilgisayara farklı Yönetim Sunucuları üzerinden birkaç kez uzaktan yüklenmesine veya başka çakışmalara neden olabilir.
- **Uygulama zaten kuruluysa yeniden yükleme**. Örneğin uygulamanın daha eski bir sürümünü yüklemek istiyorsanız bu onay kutusunun işareti kaldırın.
- **Ağ Aracısı kurulumunu Active Directory grup ilkelerinde ata**. Active Directory kaynaklarını kullanarak Ağ Aracısı'nı manuel olarak yükleme. Ağ Aracısını yüklemek için uzaktan kurulum görevinin etki alanı yöneticisi ayrıcalıklarıyla çalıştırılması gerekir.

5. Adım. Bir lisans anahtarı seçme

Uygulamayı etkinleştirmek için kurulum paketine bir anahtar ekleyin. Bu adım isteğe bağlıdır. Yönetim Sunucusu, otomatik dağıtım işlevine sahip bir lisans anahtarı içerir anahtar daha sonra otomatik olarak eklenir. Daha sonra *Anahtar ekle* görevini kullanarak da uygulamayı etkinleştirebilirsiniz.

6. Adım. İşletim sistemi yeniden başlatma ayarını seçme

Bilgisayarı yeniden başlatma gerekirse gerçekleştirilecek eylemi seçin. 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.

7. Adım. Uygulamayı kurmadan önce uyumsuz uygulamaları kaldırma

Uyumsuz uygulamalar listesini dikkatlice okuyun ve bu uygulamaların kaldırılmasına izin verin. Bilgisayarda uyumsuz uygulamalar yüklüyse Kaspersky Endpoint Security'nin kurulumu bir hata ile sonlanır.

8. Adım. Aygıtlara erişmek için bir hesap seçme

İşletim sisteminin araçlarını kullanarak Ağ Aracısını yüklemek için kullanılacak hesabı seçin. Bu durumda, bilgisayar erişimi için yönetici hakları gereklidir. Birden çok hesap ekleyebilirsiniz. Hesap yeterli haklara sahip değilse Kurulum Sihirbazı bir sonraki hesabı kullanır. Kaspersky Endpoint Security'yi Ağ Aracısı araçlarını kullanarak yüklerseniz bir hesap seçmeniz gerekmez.

9. Adım. yüklemenin başlatılması

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Koruma Dağıtım Sihirbazı Web Console'da ve Cloud Console'da nasıl başlatılır

Web Console'un ana penceresinde, **Keşif ve dağıtım** → **Dağıtım ve atama** → **Koruma dağıtım sihirbazı** seçimlerini yapın.

Bu, Koruma Dağıtım Sihirbazını başlatır. Sihirbazın talimatlarını uygulayın.

İstemci bilgisayarda 139 ve 445 numaralı TCP portları ile 137 ve 138 numaralı UDP portları açılmalıdır.

1. Adım. Kurulum paketi seçme

Listeden Kaspersky Endpoint Security kurulum paketini seçin. Listede Kaspersky Endpoint Security kurulum paketi yoksa paketi Sihirbazdan oluşturabilirsiniz. Kurulum paketini oluşturmak için dağıtım paketini aramanıza bunu bilgisayar belleğine kaydetmenize gerek yoktur. Kaspersky Security Center'da, Kaspersky sunucularında bulunan dağıtım paketlerinin listesini görüntülediğinizde kurulum paketi otomatik olarak oluşturulur. Kaspersky, yeni uygulama sürümleri yayınlandıktan sonra listeyi günceller.

Kaspersky Security Center'da kurulum paketi ayarlarını yapılandırabilirsiniz. Örneğin bir bilgisayara yüklenecek uygulama bileşenlerini seçebilirsiniz.

2. Adım. Bir lisans anahtarı seçme

Uygulamayı etkinleştirmek için kurulum paketine bir anahtar ekleyin. Bu adım isteğe bağlıdır. Yönetim Sunucusu, otomatik dağıtım işlevine sahip bir lisans anahtarı içerir anahtar daha sonra otomatik olarak eklenir. Daha sonra *Anahtar ekle* görevini kullanarak da uygulamayı etkinleştirebilirsiniz.

3. Adım. Ağ Aracısı seçme

Kaspersky Endpoint Security ile birlikte yüklenecek Ağ Aracısı sürümünü seçin. *Ağ Aracısı* Yönetim Sunucusu ile istemci bilgisayar arasındaki etkileşimi kolaylaştırır. Ağ Aracısı zaten bilgisayara yüklüyse yeniden yüklenmez.

4. Adım. Kurulum için aygıtlar seçme

Kaspersky Endpoint Security'nin yükleneceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Ağ Aracısı, atanmamış cihazlara yüklenmemiştir. Bu durumda, görev belirli cihazlara atanır. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

5. Adım. Gelişmiş ayarları yapılandırma

Şu ek uygulama ayarlarını yapılandırın:

- **Kurulum paketini indirmeye zorla**. Uygulama kurulum yöntemini seçin:
  - **Ağ Aracısı'nı kullanarak**. Ağ Aracısı, Kaspersky Endpoint Security kurulum paketini istemci bilgisayarlara dağıtmaktan sorumludur. Ağ Aracısı yüklü değilse, görev bir hata ile sonlanacaktır. Bu durumda, Ağ Aracısı kurulum paketini *Uygulamayı uzaktan yükle* görevine ekleyin ve işletim sistemi kaynakları aracılığıyla dosya aktarımını etkinleştirin. Ardından Ağ Aracısı, işletim sistemi kaynakları kullanılarak yüklenecektir. Ardından Ağ Aracısı araçları tarafından Kaspersky Endpoint Security yüklenir.
  - **Dağıtım noktaları aracılığıyla işletim sistemi kaynaklarını kullanarak**. Kurulum paketi, dağıtım noktaları aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağda en az bir dağıtım noktası varsa bu seçeneği belirleyebilirsiniz. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.
  - **Yönetim Sunucusu aracılığıyla işletim sistemi kaynaklarını kullanarak**. Dosyalar, Yönetim Sunucusu aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağ Aracısı, istemci bilgisayarda yüklü değilse ancak istemci bilgisayar, Yönetim Sunucusu ile aynı ağdaysa bu seçeneği belirleyebilirsiniz.

- **Uygulama zaten kuruluysa yeniden yükleme**. Örneğin uygulamanın daha eski bir sürümünü yüklemek istiyorsanız bu onay kutusunun işareti kaldırın.

- **Paket kurulumunu Active Directory grup ilkelerinde ata**. Kaspersky Endpoint Security, Ağ Aracısı yardımıyla veya Active Directory aracılığıyla manuel olarak yüklenir. Ağ Aracısını yüklemek için uzaktan kurulum görevinin etki alanı yöneticisi ayrıcalıklarıyla çalıştırılması gerekir.

6. Adım. İşletim sistemi yeniden başlatma ayarını seçme

Bilgisayarı yeniden başlatma gerekirse gerçekleştirilecek eylemi seçin. 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.

7. Adım. Uygulamayı kurmadan önce uyumsuz uygulamaları kaldırma

Uyumsuz uygulamalar listesini dikkatlice okuyun ve bu uygulamaların kaldırılmasına izin verin. Bilgisayarda uyumsuz uygulamalar yüklüyse Kaspersky Endpoint Security'nin kurulumu bir hata ile sonlanır.

8. Adım. Yönetim grubuna atama

Ağ Aracısı kurulduktan sonra bilgisayarların taşınacağı yönetim grubunu seçin. İlkelerin ve grup görevlerinin uygulanması için bilgisayarların bir yönetim grubuna taşınması gerekir. Bilgisayar zaten bir yönetim grubundaysa bilgisayar yeniden taşınmaz. Bir yönetim grubu seçmezseniz bilgisayarlar **Atanmamış cihazlar** grubuna eklenir.

9. Adım. Aygıtlara erişmek için bir hesap seçme

İşletim sisteminin araçlarını kullanarak Ağ Aracısını yüklemek için kullanılacak hesabı seçin. Bu durumda, bilgisayar erişimi için yönetici hakları gereklidir. Birden çok hesap ekleyebilirsiniz. Hesap yeterli haklara sahip değilse Kurulum Sihirbazı bir sonraki hesabı kullanır. Kaspersky Endpoint Security'yi Ağ Aracısı araçlarını kullanarak yüklerseniz bir hesap seçmeniz gerekmez.

10. Adım. Kurulumu başlatma

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Kurulum paketi oluşturma

Yükleme paketi Kaspersky uygulamasının Kaspersky Security Center üzerinden uzaktan kurulumu için oluşturulan bir dosya grubudur. Kurulum paketi, uygulamayı yüklemek ve kurulumdan hemen sonra çalışmasını sağlamak için gereken çeşitli ayarları içerir. Kurulum paketi, uygulama dağıtım kitinde bulunan .kpd ve .kud uzantılı dosyalar kullanılarak oluşturulur. Kaspersky Endpoint Security kurulum paketi, desteklenen tüm Windows sürümleri ve işlemci mimarisi türleri için ortaktır.

Yönetim Konsolu'nda (MMC) bir kurulum paketi nasıl oluşturulur

1. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Gelişmiş** → **Uzaktan kurulum** → **Kurulum paketleri** klasörüne gidin.

   Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.

2. **Kurulum paketi oluştur**'a tıklayın.

Yeni Paketler Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Kurulum paketi türünü seçme

Kaspersky uygulaması için kurulum paketi oluştur seçeneğini kullanın.

2. Adım. Kurulum paketi adını belirleme

Kurulum paketinin adını girin, örneğin *Kaspersky Endpoint Security for Windows 14.2*.

3. Adım. Kurulum için dağıtım paketini seçme

Gözat düğmesine tıklayın ve ardından dağıtım kitinde yer alan `kes_win.kud` dosyasını seçin.

Gerekli olduğu takdirde, **Güncellemeleri veri havuzundan kurulum paketine kopyala** onay kutusunu kullanarak kurulum paketindeki anti virüs veritabanlarını güncelleyin.

4. Adım. Son Kullanıcı Lisans Sözleşmesi ve Gizlilik İlkesi

Son Kullanıcı Lisans Sözleşmesi ile Gizlilik İlkesi'nin şartlarını okuyun ve kabul edin.

Kurulum paketi oluşturulur ve Kaspersky Security Center'a eklenir. Kurulum paketini kullanarak Kaspersky Endpoint Security'yi kurumsal ağ bilgisayarlarına yükleyebilir veya uygulama sürümünü güncelleyebilirsiniz.

Kurulum paketi ayarlarında, farklı işletim sistemi türleri için uygulama bileşenleri seçebilirsiniz. Yani, kurulum paketi iki bileşen seti içerir: iş istasyonları ve sunucular için. Kurulum paketini dağıtmadan önce, yükleyici işletim sistemi türünü algılar ve yalnızca bu işletim sistemi türü için seçtiğiniz uygulama bileşenlerini yükler. Bu şekilde, iş istasyonları ve sunucular için aynı kurulum paketini kullanabilirsiniz.

Kurulum paketinde, Yönetim Sunucusu veri havuzundan gelen anti-virüs veritabanları bulunur. Kaspersky Endpoint Security'yi yükledikten sonra veritabanlarını güncellerken trafik tüketimini azaltmak için kurulum paketindeki veritabanlarını güncelleyebilirsiniz.

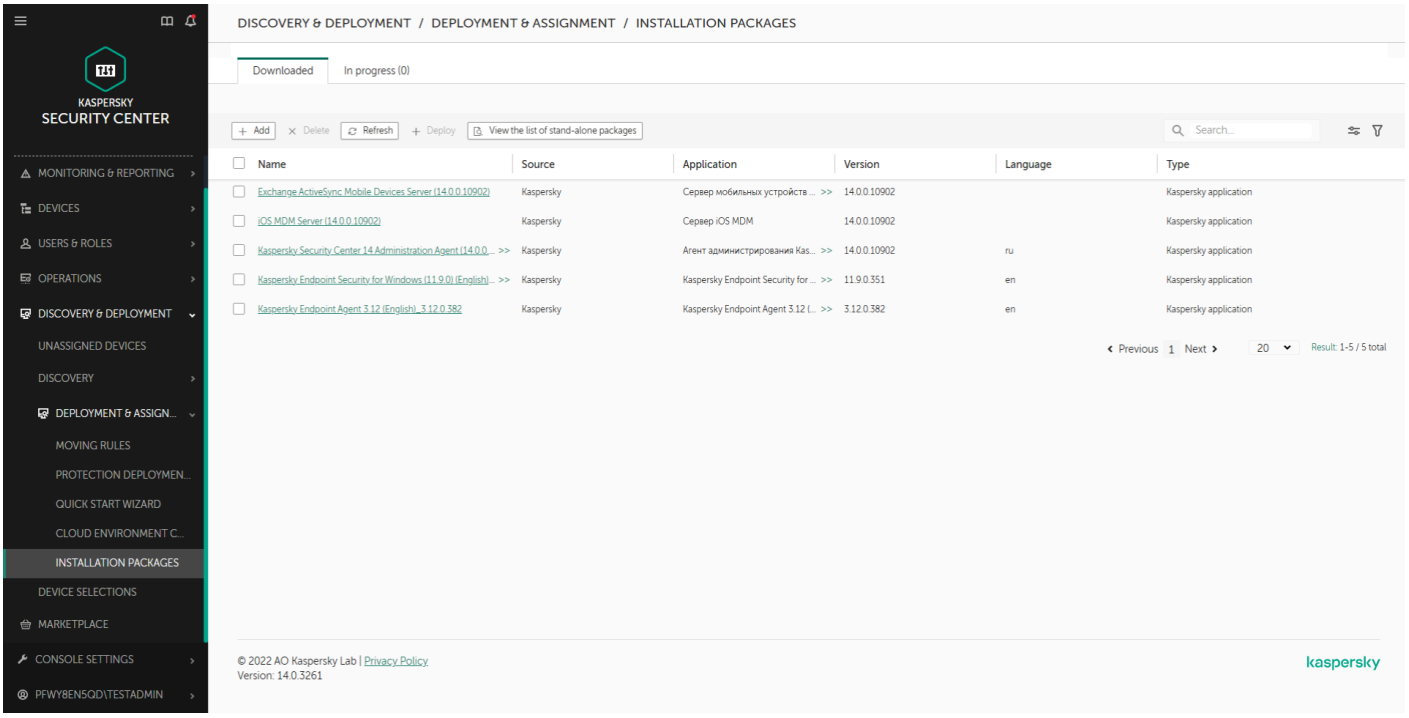
Web Console'da kurulum paketi nasıl oluşturulur

1. Web Console'un ana penceresinden **Keşif ve dağıtım → Dağıtım ve atama → Kurulum paketleri** seçimini yapın.

   Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.

2. **Ekle**'ye tıklayın.

Yeni Paketler Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.



Kurulum paketlerinin listesi

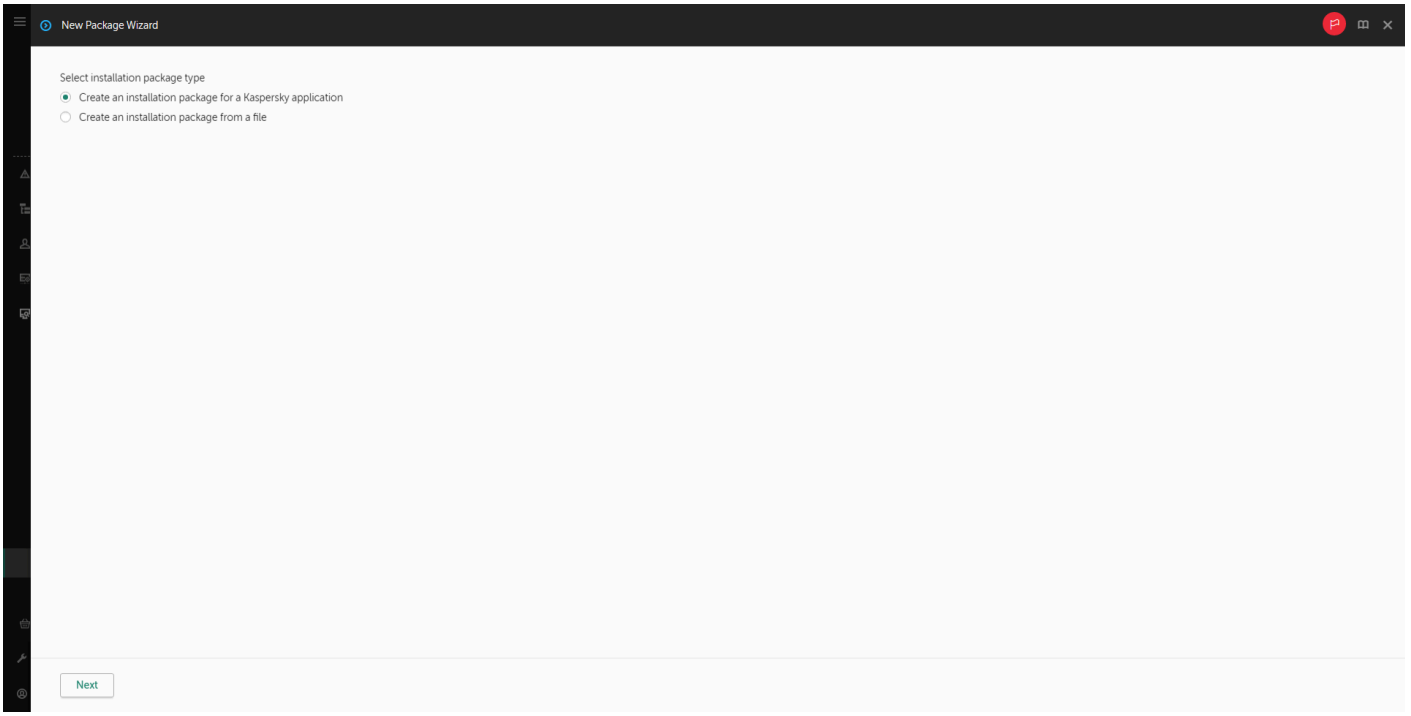
1. Adım. Kurulum paketi türünü seçme

Kaspersky uygulaması için kurulum paketi oluştur seçeneğini kullanın.

Sihirbaz, Kaspersky sunucularında bulunan dağıtım paketinden bir kurulum paketi oluşturur. Uygulamaların yeni sürümleri piyasaya sürüldükçe liste otomatik olarak güncellenir. Kaspersky Endpoint Security kurulumu için bu seçeneğin kullanılması önerilir.

Ayrıca bir dosyadan da bir kurulum paketi oluşturabilirsiniz.

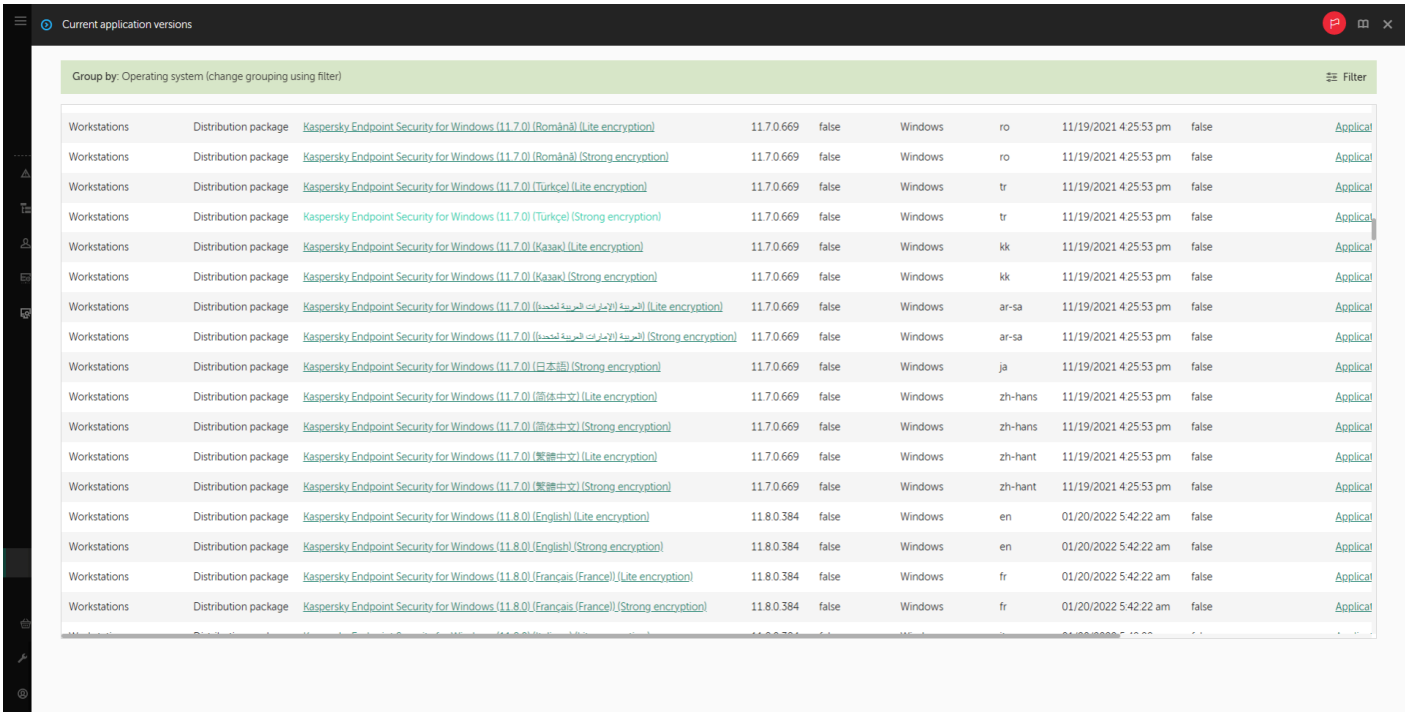
Bir dosyadan Kaspersky Endpoint Security için kurulum paketi oluşturma özelliği yalnızca Kaspersky Security Center Web Console'da kullanılabilir.



Kurulum paketi türleri

2. Adım. Kurulum paketleri

Kaspersky Endpoint Security for Windows kurulum paketini seçin. Kurulum paketi oluşturma işlemi başlar. Kurulum paketinin oluşturulması sırasında, Son Kullanıcı Lisans Sözleşmesi'nin koşullarını kabul etmeniz gerekir.

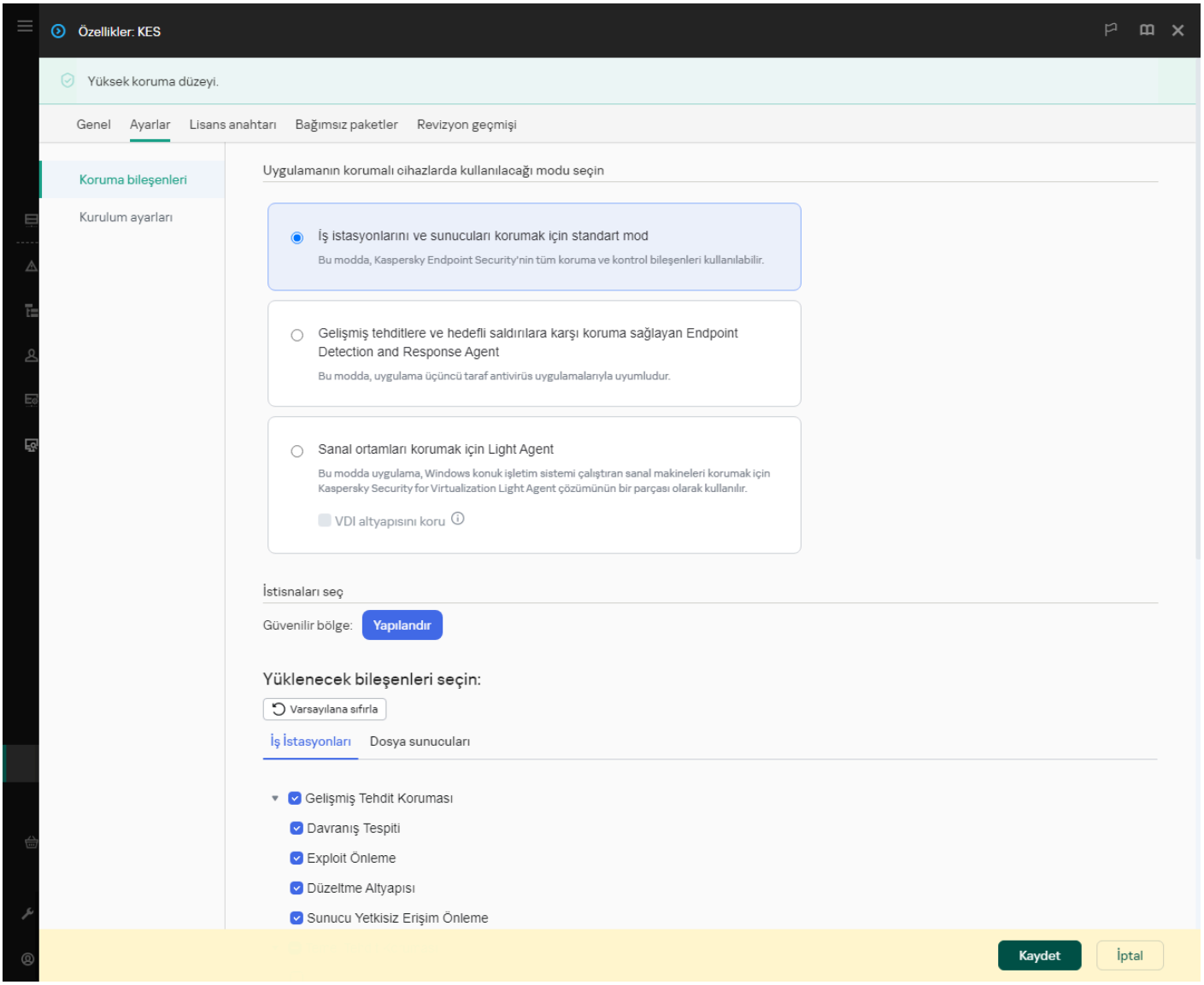


Kaspersky sunucularındaki kurulum paketlerinin listesi

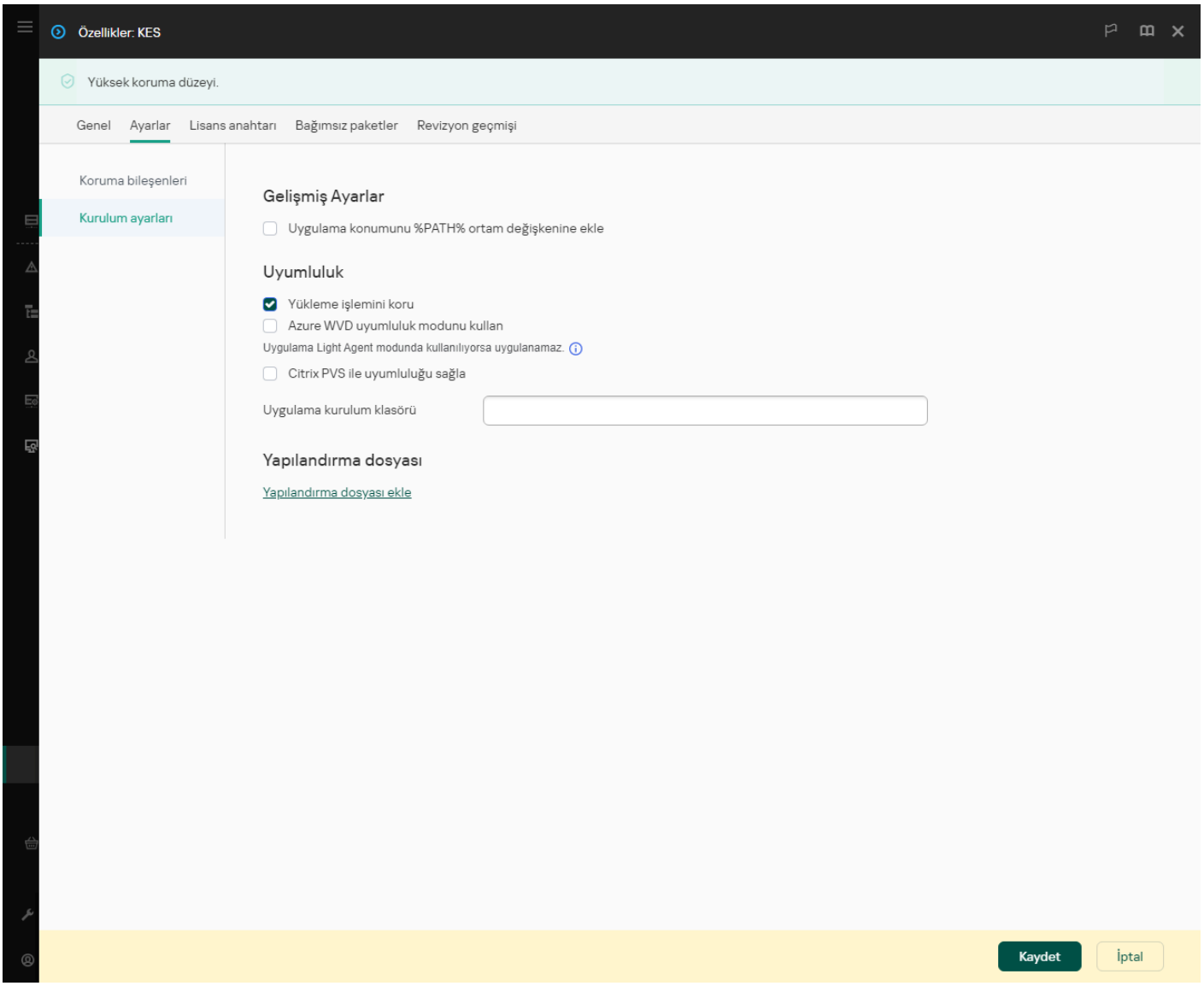
Kurulum paketi oluşturulur ve Kaspersky Security Center'a eklenir. Kurulum paketini kullanarak Kaspersky Endpoint Security'yi kurumsal ağ bilgisayarlarına yükleyebilir veya uygulama sürümünü güncelleyebilirsiniz.

Kurulum paketi ayarlarında, farklı işletim sistemi türleri için uygulama bileşenleri seçebilirsiniz. Yani, kurulum paketi iki bileşen seti içerir: iş istasyonları ve sunucular için. Kurulum paketini dağıtmadan önce, yükleyici işletim sistemi türünü algılar ve yalnızca bu işletim sistemi türü için seçtiğiniz uygulama bileşenlerini yükler. Bu şekilde, iş istasyonları ve sunucular için aynı kurulum paketini kullanabilirsiniz.

Kurulum paketinde, Yönetim Sunucusu veri havuzundan gelen anti-virüs veritabanları bulunur. Kaspersky Endpoint Security'yi yükledikten sonra veritabanlarını güncellerken trafik tüketimini azaltmak için kurulum paketindeki veritabanlarını güncelleyebilirsiniz.



Kurulum paketine dahil olan bileşenler



Kurulum paketinin kurulum ayarları

Kurulum paketi ayarları

Bölüm	Açıklama
Koruma bileşenleri	**Standart mod**. Varsayılan yapılandırma. Bu yapılandırma, Detection and Response çözümleri için destek sağlayan bileşenler de dahil olmak üzere uygulamanın tüm bileşenlerini kullanmanıza olanak tanır. Bu yapılandırma, bilgisayarın çeşitli tehditlere, ağ saldırılarına ve dolandırıcılığa karşı kapsamlı bir şekilde korunması için kullanılır. **Endpoint Detection and Response Agent** Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir. **Sanal ortamları korumak için Light Agent**. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.
İstisnalar	Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, uygulamayı sanal ortamları korumak için Light Agent modunda yükleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir. Güvenilen bölgeyi daha sonra ilke özelliklerinde de yapılandırabilirsiniz: tarama istisnaları ve güvenilir uygulamalar.

Bölüm	Açıklama
Yüklenecek bileşenleri seçin	Bu bölümde, kullanılabilir olacak uygulama bileşenlerini seçebilirsiniz. *Uygulama bileşenlerini değiştir* görevini kullanarak uygulama bileşenlerini daha sonra değiştirebilirsiniz. İş istasyonları ve sunucular için ayrı bileşen setleri oluşturabilirsiniz. Kurulum paketini dağıtmadan önce, yükleyici işletim sistemi türünü algılar ve yalnızca bu işletim sistemi türü için seçtiğiniz uygulama bileşenlerini yükler. Bu şekilde, iş istasyonları ve sunucular için aynı kurulum paketini kullanabilirsiniz. Kullanılabilir bileşenler kümesi uygulamanın yapılandırmasına bağlıdır: **Standart mod** Kaspersky Veri Şifreleme, Dosya Düzeyinde Şifreleme ve EDR Optimum dışındaki tüm yerleşik aracılar varsayılan olarak yüklenmez. Bu bileşenler kurulum paketi ayarlarında eklenebilir. **Endpoint Detection and Response Agent** Bu yapılandırmada, yalnızca Kaspersky Detection and Response çözümleri için yerleşik aracılar kullanılabilir. **Sanal ortamları korumak için Light Agent** Bu yapılandırmada, veri şifreleme bileşenleri ve Uyarlanabilir Anomali Denetimi hariç, **Standart mod** yapılandırmasında kullanılabilen uygulama bileşenlerinin neredeyse tamamını kullanabilirsiniz.
Lisans anahtarı	Bu bölümde uygulamayı etkinleştirebilirsiniz. Uygulamayı etkinleştirmek için bir lisans anahtarı seçmelisiniz. Bunu yapmadan önce anahtarı Yönetim Sunucusu'na eklemeniz gerekir. Kaspersky Security Center Yönetim Sunucusuna anahtarlar ekleme hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım 'ına bakın.
Uyumsuz uygulamalar	Uyumsuz uygulamalar listesini dikkatlice okuyun ve bu uygulamaların kaldırılmasına izin verin. Bilgisayarda uyumsuz uygulamalar yüklüyse Kaspersky Endpoint Security'nin kurulumu bir hata ile sonlanır.
Kurulum ayarları	**avp.com dosyasının yolunu %PATH% sistem değişkenine ekle**. Komut satırı arabiriminin uygun kullanımı için kurulum yolunu %PATH% değişkenine ekleyebilirsiniz. **Yükleme işlemini koru**. Kurulum koruması, dağıtım paketinin zararlı programlarla değiştirilmesine karşı koruma, Kaspersky Endpoint Security yükleme klasörüne erişimi engelleme ve uygulama anahtarlarını içeren sistem kayıt defteri bölümüne erişimi engellemeyi içerir. Ancak, uygulama yüklenemiyorsa (örneğin, Windows Remote Desktop yardımıyla uzaktan yükleme gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız önerilir. **Citrix PVS ile uyumluluğu sağla**. Kaspersky Endpoint Security'yi sanal bir makineye yüklemek için Citrix Provisioning Services desteğini etkinleştirebilirsiniz. **Azure WVD uyumluluk modunu kullan**. Bu özellik, Kaspersky Anti Targeted Attack Platform konsolunda Azure sanal makine durumunun doğru görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensor ID) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensor ID atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensor ID değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir. **Uygulama kurulum klasörü**. Bir istemci bilgisayarda Kaspersky Endpoint Security'nin kurulum yolunu değiştirebilirsiniz. Uygulama varsayılan olarak `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2` klasörüne yüklenir. **Yapılandırma dosyası**. Uygulamanın önceden tanımlanmış ayarlarla yüklenmesi. Bunu yapmak için Kaspersky Endpoint Security ayarlarını tanımlayan bir dosya yüklemeniz gerekir. Uygulamanın yerel arabiriminde bir yapılandırma dosyası oluşturabilirsiniz. Yeni paket sihirbazı, şifrelenmiş yapılandırma dosyalarını desteklemez. Yapılandırma dosyasını dışa aktarırken dosya şifreleme adımını atlayın.

Kurulum paketindeki veritabanlarının güncellenmesi

Kurulum paketinde, Yönetim Sunucusu veri havuzundan gelen ve kurulum paketinin oluşturulduğu tarihte güncel olan anti-virüs veritabanları bulunur. Kurulum paketini oluşturduktan sonra, kurulum paketindeki anti-virüs veritabanlarını güncelleyebilirsiniz. Bu, Kaspersky Endpoint Security'yi yükledikten sonra anti-virüs veritabanlarını güncellerken veri tüketimini azaltmanızı sağlar.

Yönetim Sunucusu veri havuzundaki anti-virüs veritabanlarını güncellemek için Yönetim Sunucusunun *Güncellemeleri Yönetim Sunucusu veri havuzuna indir* görevini kullanın. Yönetim Sunucusu veri havuzundaki anti-virüs veritabanlarının güncellenmesi hakkında daha fazla bilgi almak için lütfen Kaspersky Security Center Yardım Kılavuzu 'na başvurun.

Kurulum paketindeki veritabanlarını sadece Yönetim Konsolundan ve Kaspersky Security Center Web Console'dan güncelleyebilirsiniz. Kaspersky Security Center Cloud Console'dan kurulum paketindeki veritabanlarını güncellemek mümkün değildir.

Kurulum paketindeki anti-virüs veritabanları Yönetim Konsolu (MMC) aracılığıyla nasıl güncellenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacından **Gelişmiş** → **Uzaktan kurulum** → **Kurulum paketleri** klasörünü seçin.
   Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.
3. Kurulum paketinin özelliklerini açın.
4. **Genel** bölümünde **Veritabanlarını güncelle** düğmesine tıklayın.

Bunun sonucunda kurulum paketindeki anti-virüs veritabanları Yönetim Sunucusu veri havuzundan güncellenir. Dağıtım paketinde yer alan `bases.cab` dosyasının yerini `bases` klasörü alır. Güncelleme paketi dosyaları bu klasörün içinde olacaktır.

Bir kurulum paketindeki anti-virüs veritabanları Web Console aracılığıyla nasıl güncellenir

1. Web Console'un ana penceresinden **Keşif ve dağıtım** → **Dağıtım ve atama** → **Kurulum paketleri** seçimini yapın.
   Bu, Web Console'a indirilen kurulum paketlerinin listesini açar.
2. Anti-virüs veritabanlarını güncellemek istediğiniz Kaspersky Endpoint Security kurulum paketinin adına tıklayın.
   Kurulum paketi özellikleri penceresi açılır.
3. **Genel bilgiler** sekmesinden **Veritabanlarını güncelle** bağlantısına tıklayın.

Bunun sonucunda kurulum paketindeki anti-virüs veritabanları Yönetim Sunucusu veri havuzundan güncellenir. Dağıtım paketinde yer alan `bases.cab` dosyasının yerini `bases` klasörü alır. Güncelleme paketi dosyaları bu klasörün içinde olacaktır.

Uzaktan kurulum görevi oluşturma

Uygulamayı uzaktan yükle görevi, Kaspersky Endpoint Security'nin uzaktan kurulması için tasarlanmıştır. *Uygulamayı uzaktan yükle* görevi, uygulamanın kurulum paketini kuruluş içindeki tüm bilgisayarlara dağıtmanızı sağlar. Kurulum paketini dağıtmadan önce, paketin içindeki antivirüs veritabanlarını güncelleyebilirsiniz ve kurulum paketinin özelliklerinde yer alan uygulama bileşenlerini seçebilirsiniz.

Yönetim Konsolu'nda (MMC) bir uzaktan kurulum görevi nasıl oluşturulur

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
   Görevler listesi açılır.
3. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Security Center Yönetim Sunucusu → **Uygulamayı uzaktan yükle** seçimini yapın.

2. Adım. Kurulum paketi seçme

Listeden Kaspersky Endpoint Security kurulum paketini seçin. Listede Kaspersky Endpoint Security kurulum paketi yoksa paketi Sihirbazdan oluşturabilirsiniz.

Kaspersky Security Center'da kurulum paketi ayarlarını yapılandırabilirsiniz. Örneğin bir bilgisayara yüklenecek uygulama bileşenlerini seçebilirsiniz.

Ağ Aracısı ayrıca Kaspersky Endpoint Security ile birlikte yüklenecektir. *Ağ Aracısı* Yönetim Sunucusu ile istemci bilgisayar arasındaki etkileşimi kolaylaştırır. Ağ Aracısı zaten bilgisayara yüklüyse yeniden yüklenmez.

3. Adım. Ek

Ağ Aracısı kurulum paketini seçin. Kaspersky Endpoint Security ile birlikte yüklenecek olan seçili Ağ Aracısının sürümü.

4. Adım. Ayarlar

Şu ek uygulama ayarlarını yapılandırın:

- **Kurulum paketini indirmeye zorla**. Uygulama kurulum yöntemini seçin:
  - **Ağ Aracısı'nı kullanarak**. Ağ Aracısı, Kaspersky Endpoint Security kurulum paketini istemci bilgisayarlara dağıtmaktan sorumludur. Ağ Aracısı yüklü değilse, görev bir hata ile sonlanacaktır. Bu durumda, Ağ Aracısı kurulum paketini *Uygulamayı uzaktan yükle* görevine ekleyin ve işletim sistemi kaynakları aracılığıyla dosya aktarımını etkinleştirin. Ardından Ağ Aracısı, işletim sistemi kaynakları kullanılarak yüklenecektir. Ardından Ağ Aracısı araçları tarafından Kaspersky Endpoint Security yüklenir.
  - **Dağıtım noktaları aracılığıyla işletim sistemi kaynaklarını kullanarak**. Kurulum paketi, dağıtım noktaları aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağda en az bir dağıtım noktası varsa bu seçeneği belirleyebilirsiniz. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.
  - **Yönetim Sunucusu aracılığıyla işletim sistemi kaynaklarını kullanarak**. Dosyalar, Yönetim Sunucusu aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağ Aracısı, istemci bilgisayarda yüklü değilse ancak istemci bilgisayar, Yönetim Sunucusu ile aynı ağdaysa bu seçeneği belirleyebilirsiniz.
- **Diğer Yönetim Sunucularıyla yönetilen cihazlar için davranış**. Kaspersky Endpoint Security kurulum paketini seçin. Ağda birden fazla Yönetim Sunucusu yüklüyse bu Yönetim Sunucuları aynı istemci bilgisayarlarını görebilir. Bu, örneğin bir uygulamanın aynı istemci bilgisayara farklı Yönetim Sunucuları üzerinden birkaç kez uzaktan yüklenmesine veya başka çakışmalara neden olabilir.
- **Uygulama zaten kuruluysa yeniden yükleme**. Örneğin uygulamanın daha eski bir sürümünü yüklemek istiyorsanız bu onay kutusunun işareti kaldırın.

5. Adım. İşletim sistemi yeniden başlatma ayarını seçme

Bilgisayarı yeniden başlatma gerekirse gerçekleştirilecek eylemi seçin. 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.

6. Adım. Görevin atanacağı cihazları seçme

Kaspersky Endpoint Security'nin yükleneceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Ağ Aracısı, atanmamış cihazlara yüklenmemiştir. Bu durumda, görev belirli cihazlara atanır. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

7. Adım. Görevi çalıştıracak hesabı seçme

İşletim sisteminin araçlarını kullanarak Ağ Aracısını yüklemek için kullanılacak hesabı seçin. Bu durumda, bilgisayar erişimi için yönetici hakları gereklidir. Birden çok hesap ekleyebilirsiniz. Hesap yeterli haklara sahip değilse Kurulum Sihirbazı bir sonraki hesabı kullanır. Kaspersky Endpoint Security'yi Ağ Aracısı araçlarını kullanarak yüklerseniz bir hesap seçmeniz gerekmez.

8. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görevi başlatmak için bir zamanlama ayarlayın, örneğin manuel olarak ya da bilgisayar boş olduğunda.

9. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Kaspersky Endpoint Security for Windows 14.2 yükle*.

10. Adım. Görev oluşturmayı bitirme

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz. Uygulama sessiz modda yüklenecektir. Yüklemeden sonrasında kullanıcının bilgisayarındaki bildirim alanına simgesi eklenir. Simge olarak görünüyorsa uygulamayı etkinleştirdiğinizden emin olun.

Web Console'da ve Cloud Console'da nasıl bir uzaktan kurulum paketi oluşturulur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Security Center**'ı seçin.
2. **Görev türü** açılır listesinde, **Uygulamayı uzaktan yükle**'yi seçin.
3. **Görev adı** alanına kısa bir açıklama girin. Örneğin; *Yöneticiler için Kaspersky Endpoint Security kurulumu*.
4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

2. Adım. Kurulum için bilgisayar seçme

Bu adımda, Kaspersky Endpoint Security Cloud'un seçilen görev kapsamı seçeneğine göre kaldırılacağı bilgisayarları seçin.

3. Adım. Kurulum paketi yapılandırma

Bu adımda, yükleme paketini yapılandırın:

1. Kaspersky Endpoint Security for Windows (14.2) kurulum paketini seçin.
2. Ağ Aracısı kurulum paketini seçin.

   Kaspersky Endpoint Security ile birlikte yüklenecek olan seçili Ağ Aracısının sürümü. *Ağ Aracısı* Yönetim Sunucusu ile istemci bilgisayar arasındaki etkileşimi kolaylaştırır. Ağ Aracısı zaten bilgisayara yüklüyse yeniden yüklenmez.

3. **Kurulum paketini indirmeye zorla** bloğundan uygulama kurulum yöntemini seçin:

   - **Ağ Aracısı'nı kullanarak**. Ağ Aracısı, Kaspersky Endpoint Security kurulum paketini istemci bilgisayarlara dağıtmaktan sorumludur. Ağ Aracısı yüklü değilse, görev bir hata ile sonlanacaktır. Bu durumda, Ağ Aracısı kurulum paketini *Uygulamayı uzaktan yükle* görevine ekleyin ve işletim sistemi kaynakları aracılığıyla dosya aktarımını etkinleştirin. Ardından Ağ Aracısı, işletim sistemi kaynakları kullanılarak yüklenecektir. Ardından Ağ Aracısı araçları tarafından Kaspersky Endpoint Security yüklenir.

   - **Dağıtım noktaları aracılığıyla işletim sistemi kaynaklarını kullanarak**. Kurulum paketi, dağıtım noktaları aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağda en az bir dağıtım noktası varsa bu seçeneği belirleyebilirsiniz. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

   - **Yönetim Sunucusu aracılığıyla işletim sistemi kaynaklarını kullanarak**. Dosyalar, Yönetim Sunucusu aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağ Aracısı, istemci bilgisayarda yüklü değilse ancak istemci bilgisayar, Yönetim Sunucusu ile aynı ağdaysa bu seçeneği belirleyebilirsiniz.

4. **Maksimum eş zamanlı indirme sayısı** alanında, Yönetim Sunucusuna gönderilen kurulum paketi indirme isteklerinin sayısı için bir sınır belirleyin. İstek sayısındaki sınır, ağın aşırı yüklenmesini önlemeye yardımcı olur.

5. **Kurulum denemelerinin maksimum sayısı** alanında, uygulamayı yükleme girişimi için bir sınır belirleyin. Kaspersky Endpoint Security kurulumu bir hata ile sonlanırsa görev, kurulumu otomatik olarak yeniden başlatır.

6. Gerekirse **Uygulama zaten kuruluysa yeniden yükleme** onay kutusunun işaretini kaldırın. Örneğin uygulamanın önceki sürümlerinden birini yüklemenize olanak tanır.

7. Gerekirse **İndirmeden önce işletim sistemi sürümünü doğrula** onay kutusunun işaretini kaldırın. Bu seçenek, bilgisayar işletim sistemi yazılım gereksinimlerini karşılamıyorsa uygulama dağıtım paketini indirmemenize olanak tanır. Bilgisayarın işletim sisteminin yazılım gereksinimlerini karşıladığından eminseniz bu doğrulamayı atlayabilirsiniz.

8. Gerekirse **Paket kurulumunu Active Directory grup ilkelerinde ata** onay kutusunu işaretleyin. Kaspersky Endpoint Security, Ağ Aracısı yardımıyla veya Active Directory aracılığıyla manuel olarak yüklenir. Ağ Aracısını yüklemek için uzaktan kurulum görevinin etki alanı yöneticisi ayrıcalıklarıyla çalıştırılması gerekir.

9. Gerekirse **Kullanıcılardan çalışan uygulamaları kapatmalarını iste** onay kutusunu işaretleyin. Kaspersky Endpoint Security kurulumu bilgisayar kaynaklarını kullanır. Kullanıcının rahatlığı için Uygulama Kurulum Sihirbazı, kuruluma başlamadan önce çalışan uygulamaları kapatmanızı ister. Bu, diğer uygulamaların çalışmasındaki arızaları önlemeye yardımcı olur ve olası bilgisayar arızalarını önler.

10. **Diğer Yönetim Sunucularıyla yönetilen cihazlar için davranış** bloğunda, Kaspersky Endpoint Security'nin kurulum yöntemini seçin. Ağda birden fazla Yönetim Sunucusu yüklüyse bu Yönetim Sunucuları aynı istemci bilgisayarlarını görebilir. Bu, örneğin bir uygulamanın aynı istemci bilgisayara farklı Yönetim Sunucuları üzerinden birkaç kez uzaktan yüklenmesine veya başka çakışmalara neden olabilir.

4. Adım. Görevi çalıştıracak hesabı seçme

İşletim sisteminin araçlarını kullanarak Ağ Aracısını yüklemek için kullanılacak hesabı seçin. Bu durumda, bilgisayar erişimi için yönetici hakları gereklidir. Birden çok hesap ekleyebilirsiniz. Hesap yeterli haklara sahip değilse Kurulum Sihirbazı bir sonraki hesabı kullanır. Kaspersky Endpoint Security'yi Ağ Aracısı araçlarını kullanarak yüklerseniz bir hesap seçmeniz gerekmez.

5. Adım. Görev oluşturmayı tamamlama

Son düğmesine tıklayarak sihirbazı sonlandırın. Görevler listesinde yeni bir görev görüntülenir. Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçin ve **Başlat** düğmesine tıklayın. Uygulama sessiz modda yüklenecektir. Yüklemeden sonrasında kullanıcının bilgisayarındaki bildirim alanına simgesi eklenir. Simge olarak görünüyorsa uygulamayı etkinleştirdiğinizden emin olun.

Sihirbazı kullanarak uygulamayı yerel olarak yükleme

Kurulum Sihirbazı uygulamasının arabirimi uygulama kurulum adımlarına karşılık gelen sayfa sıralamalarından meydana gelir. Kurulum Sihirbaz'nı çalıştırdığınız kullanıcı hesabının yönetici grubunda olduğundan emin olun.

Kurulum Sihirbazını kullanarak uygulamayı yüklemek veya uygulamayı daha eski bir sürümden yükseltmek için:

1. Dağıtım noktası klasörünü kullanıcının bilgisayarına kopyalayın.
2. setup_kes.exe dosyasını çalıştırın.

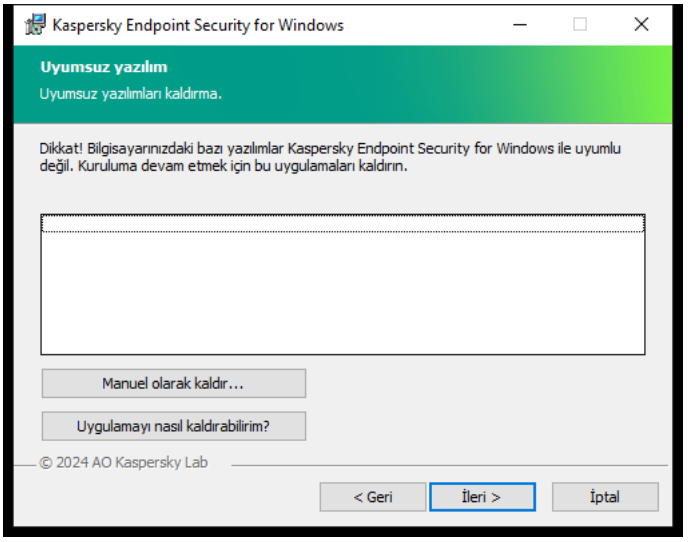
Kurulum Sihirbazı başlatılır.

Yükleme için hazırlık

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

- Kaspersky Endpoint Security ile uyumluluk sorunları yaşayabilecek herhangi bir yazılımın yüklü olup olmadığı (yazılım listesi, dağıtım paketinde bulunan incompatible.txt dosyasında mevcuttur).
- Donanım ve yazılım gereksinimlerinin karşılanıp karşılanmadığı.
- Microsoft .NET Framework'ün mevcut olup olmadığı.
- Kullanıcının yazılım ürününü yükleme haklarına sahip olup olmadığı.

Önceki gereksinimlerden herhangi biri karşılanmazsa, ekranda ilgili bildirim görüntülenir. Örneğin, uyumsuz yazılım hakkında bir bildirim (aşağıdaki şekle bakın).



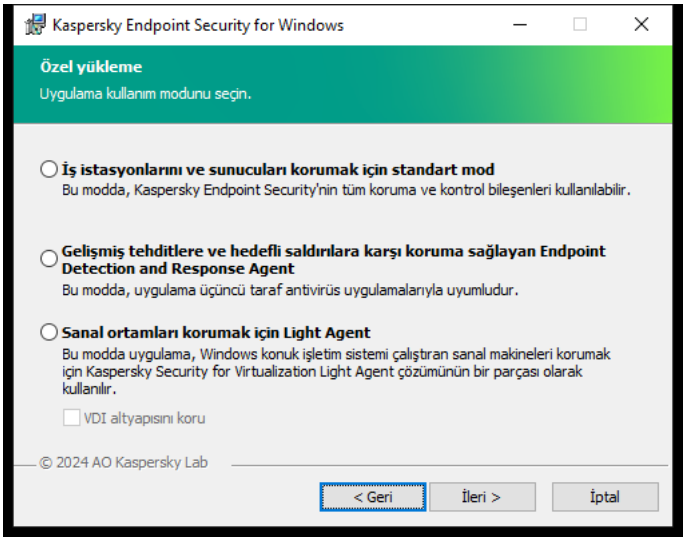
Uyumsuz yazılımları kaldırma

Bilgisayar belirtilen gereksinimleri karşılıyorsa Kurulum Sihirbazı, yüklenen uygulama ile birlikte aynı anda çalışırken çakışmaya neden olabilecek Kaspersky uygulamalarını arar. Bu uygulamalar bulunur bunları manuel olarak 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 14.2 for Windows'un yüklenmesi sırasında kullanılır ve uygulamanın önceki sürümü otomatik olarak kaldırılır. Bu, aşağıdaki uygulama sürümleri için geçerlidir:

- Kaspersky Endpoint Security 12.3 for Windows (yapı 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (yapı 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (yapı 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (yapı 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (yapı 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (yapı 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (yapı 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (yapı 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (yapı 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (yapı 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (yapı 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (yapı 14.1.0.423)

Kaspersky Endpoint Security yapılandırması



Uygulama yapılandırmasının seçilmesi

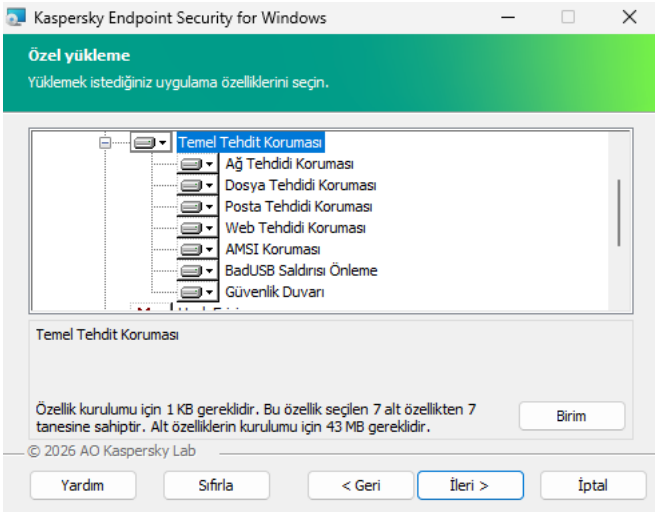
Standart mod. Varsayılan yapılandırma. Bu yapılandırma, Detection and Response çözümleri için destek sağlayan bileşenler de dahil olmak üzere uygulamanın tüm bileşenlerini kullanmanıza olanak tanır. Bu yapılandırma, bilgisayarın çeşitli tehditlere, ağ saldırılarına ve dolandırıcılığa karşı kapsamlı bir şekilde korunması için kullanılır.

Endpoint Detection and Response Agent Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.

Sanal ortamları korumak için Light Agent. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.

Kaspersky Endpoint Security bileşenleri

Yükleme sırasında, yüklemek istediğiniz Kaspersky Endpoint Security bileşenlerini seçebilirsiniz (aşağıdaki resme bakın). Dosya Tehdidi Koruması bileşeni, yüklenmesi gereken zorunlu bir bileşendir. Yüklemesini iptal edemezsiniz.



Yüklenecek uygulama bileşenlerini seçme

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

- Kaspersky Disk Encryption
- Dosya Düzeyinde Şifreleme
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- KUMA ile entegrasyon

Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz. Bunu yapmak için, Kurulum Sihirbazını tekrar çalıştırmanız ve kullanılabilir bileşenleri değiştirmeyi seçmeniz gerekir.

Detection and Response bileşenlerini yüklemeniz gerekiyorsa Kaspersky Endpoint Security aşağıdaki yapılandırmaları destekler:

- Sadece Endpoint Detection and Response Optimum
- Sadece Endpoint Detection and Response Expert (cloud)
- Yalnızca Endpoint Detection and Response Expert (on-premises)
- Sadece Network Detection and Response (KATA)

- Sadece Sandbox
- Endpoint Detection and Response Optimum ve Sandbox
- Endpoint Detection and Response Expert ve Sandbox
- Endpoint Detection and Response Expert (on-premises) ve Sandbox
- Network Detection and Response (KATA) ve Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) ve Managed Detection and Response

Kaspersky Endpoint Security, uygulamayı yüklemeden önce bileşenlerin seçimini doğrular. Detection and Response bileşenlerinin seçilen yapılandırması desteklenmiyorsa Kaspersky Endpoint Security yüklenemez.

Uygulamayı yüklemek için klasör seçme

Bir istemci bilgisayarda Kaspersky Endpoint Security'nin kurulum yolunu değiştirebilirsiniz. Uygulama varsayılan olarak `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2` klasörüne yüklenir.

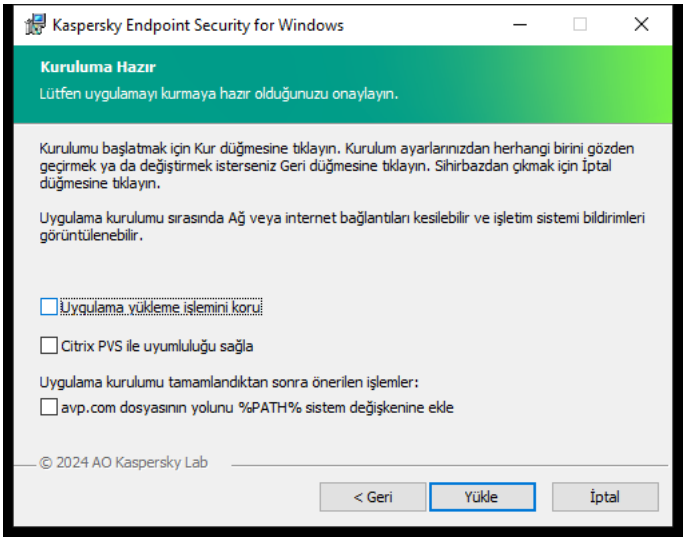
Güvenilen bölgeyi yapılandırma

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir.

Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, uygulamayı sanal ortamları korumak için Light Agent modunda yükleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir.

Güvenilen bölgeyi daha sonra ilke özelliklerinde de yapılandırabilirsiniz: tarama istisnaları ve güvenilir uygulamalar.

Gelişmiş ayarlar



Gelişmiş uygulama kurulum ayarları

Uygulama yükleme işlemini koru. Kurulum koruması, dağıtım paketinin zararlı programlarla değiştirilmesine karşı koruma, Kaspersky Endpoint Security yükleme klasörüne erişimi engelleme ve uygulama anahtarlarını içeren sistem kayıt defteri bölümüne erişimi engellemeyi içerir. Ancak, uygulama yüklenemiyorsa (örneğin, Windows Remote Desktop yardımıyla uzaktan yükleme gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız önerilir.

Citrix PVS ile uyumluluğu sağla. Kaspersky Endpoint Security'yi sanal bir makineye yüklemek için Citrix Provisioning Services desteğini etkinleştirebilirsiniz.

avp.com dosyasının yolunu %PATH% sistem değişkenine ekle. Komut satırı arabiriminin uygun kullanımı için kurulum yolunu %PATH% değişkenine ekleyebilirsiniz.

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** bloğunda **Paketler**'i seçin.
3. Kontrol panelinde konsolun üst kısmında **Paket oluştur** düğmesine tıklayın.

   Yeni Paket ve Uygulama Sihirbazı açılır.

4. Yeni Paket ve Uygulama Sihirbazı'nda:

   a. **Paket** bölümünde:

   - **Ad** alanına kurulum paketinin adını girin.
   - **Kaynak klasörü** alanında, Kaspersky Endpoint Security dağıtım paketini içeren klasörün yolunu belirtin.

   b. **Uygulama türü** bölümünde **Standart program** seçeneğini tercih edin.

   c. **Standart program** bölümünde:

   - **Ad** alanına kurulum 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.
   - **Çalışma 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 program çalıştır** 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** bloğunda **Bu program sadece belirtilen platformlarda çalıştırılabilir** seçeneğini tercih edin.

     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 kurulum paketi geçerli kurulum paketleri listesinde **Paketler** bölümünde görülür.

5. Kurulum paketinin bağlam menüsünde **Dağıt**'ı seçin.

   Dağıtım Sihirbazı başlatılır.

6. Dağıtım Sihirbazında:

   a. **Genel** bölümünde:

   - **Yazılım** alanına kurulum paketinin benzersiz adını girin veya **Gözat** düğmesine tıklayarak listeden kurulum 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 kurulumu 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 kurulması için bir görev oluşturulur.

setup.ini dosyası yükleme ayarlarının açıklaması

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

setup.ini dosyasını yalnızca uygulamayı sessiz modda yüklerken kullanın.

setup.ini dosyasında install.cfg yapılandırma dosyasına bir yol ekleyemezsiniz. Uygulama, install.cfg yapılandırma dosyası Kaspersky Endpoint Security dağıtım paketiyle aynı klasöre yerleştirilmişse bu dosyayı da atlar. install.cfg yapılandırma dosyasındaki ayarları uygulamak için, şu uygulama yükleme komutunda dosyanın yolunu belirtmeniz gerekir: `CONFIGPATH=<path to the configuration file>`.

SETUP.INI DOSYASINI İNDİRİN

setup.ini dosyası aşağıdaki bölümleri içerir:

- `[Setup]` – uygulama yüklemesinin genel ayarları.
- `[Components]` – Standart modda yüklenecek uygulama bileşenlerinin seçimi. Bileşenlerin hiçbiri belirtilmezse işletim sistemlerinin tüm bileşenleri yüklenir. Dosya Tehdidi 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, `yes`, `on`, `enable`, `enabled` ve `true` seçenekleridir. `0` değerinin alternatifleri, `no`, `off`, `disable`, `disabled` ve `false` 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 kabulü. 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.

Bölüm	Parametre	Açıklama
	`PrivacyPolicy`	Gizlilik İlkesi'nin kabul edilmesi. 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 (KSN) 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.
	`CLEANERSIGNCHECK`	incompatible.txt listesinden tespit edilen yazılım dosyalarının dijital imzalarının doğrulanması. Kaspersky Endpoint Security, yazılımı kaldırmak için yazılım yükleyici dosyasını çalıştırır. Yükleyici dosyasının dijital imzası yoksa Kaspersky Endpoint Security dosyayı güvenilmez olarak değerlendirir ve potansiyel olarak zararlı kodların çalışmasını önlemek için yazılımın kaldırılmasını durdurur. Uygulama, algılanan yazılım dosyasının dijital imzasını doğrulayamazsa Kaspersky Endpoint Security yüklemesi bir hata ile durdurulur. Varsayılan değer, yazılım yükleme yöntemine bağlı olarak farklıdır: • `0` dijital imza doğrulamasının devre dışı olduğu anlamına gelir (Kaspersky Security Center aracılığıyla dağıtıldıysa varsayılan değerdir). • `1` dijital imza doğrulamanın etkinleştirildiği anlamına gelir (uygulama yerel olarak kuruluyorsa varsayılan değerdir).
	`Login`	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için kullanıcı adını ayarlayın (Parola koruması bileşeni). Kullanıcı adı, `Password` ve `PasswordArea` parametreleriyle birlikte ayarlanır. KLAdmin kullanıcı adı varsayılan olarak kullanılır.
	`Password`	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için bir parola belirtin (parola, `Login` ve `PasswordArea` parametreleriyle birlikte belirtilir). Bir parola belirlediyseniz ancak `Login` 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 (`Login` ve `Password` parametreleri). Birden çok değer belirtmek için `;` karakterini kullanın. Kullanılabilir değerler: • `SET` – Uygulama ayarlarını değiştirme. • `EXIT` – Uygulamadan çık. • `DISPROTECT` – Koruma bileşenlerini devre dışı bırakma ve tarama görevlerini durdurma. • `DISPOLICY` – Kaspersky Security Center ilkesini devre dışı bırak. • `UNINST` – Uygulamayı bilgisayardan kaldırma. • `DISCTRL` – Denetim bileşenlerini devre dışı bırakma. • `REMOVELIC` – anahtarın kaldırılması. • `REPORTS` – raporların görüntülenmesi. • `EXPORT` – uygulama ayarlarını dışa aktarma. Örneğin, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Uygulama yükleme koruma mekanizmasını etkinleştirme veya devre dışı bırakma. Kullanılabilir değerler: • `1` – Uygulama yükleme koruma mekanizması etkin (varsayılan değer). • `0` – Uygulama yükleme koruma mekanizması devre dışı. Kurulum koruması, dağıtım paketinin zararlı programlarla değiştirilmesine karşı koruma, Kaspersky Endpoint Security yükleme klasörüne erişimi engelleme ve uygulama anahtarlarını içeren sistem kayıt defteri bölümüne erişimi engellemeyi içerir. Ancak, uygulama yüklenemiyorsa (örneğin, Windows Remote Desktop yardımıyla uzaktan yükleme gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız önerilir.
	`PROTECTOSSERVICES`	İşletim sistemi hizmetlerinin işlevselliğinin korunması. İşletim sistemi hizmetleri koruması, üçüncü taraf uygulamaların işletim sistemi hizmetlerinin çalışmasını engellemesini önler. Bu tür hizmetler arasında, örneğin, uygulama otomatik başlatma hizmeti bulunur. • `1` işletim sistemi hizmetlerinin korunmasının etkinleştirildiği anlamına gelir (varsayılan değer). • `0` işletim sistemi hizmetlerinin korunmasının devre dışı olduğu anlamına gelir.

Bölüm	Parametre	Açıklama
	`EnableAzureSupport`	Azure WVD uyumluluk modunu etkinleştirme veya devre dışı bırakma. Kullanılabilir değerler: • `1` – Azure WVD uyumluluk modu etkinleştirilir. • `0` – Azure WVD uyumluluk modu devre dışı bırakılır (varsayılan değer). Bu özellik, Kaspersky Anti Targeted Attack Platform konsolunda Azure sanal makine durumunun doğru görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensor ID) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensor ID atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensor ID değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir.
	`Reboot`	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`	Kaspersky Endpoint Security kurulum klasöründe bulunan yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyin. 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 teknolojisini (Antimalware Protected Process Light) kullanan Kaspersky Endpoint Security işlemlerinin korumasını etkinleştirir veya devre dışı bırakır. AM-PPL teknolojisi hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin. AM-PPL teknolojisi Windows Server 2019 ve Windows 10 sürüm 1703 (RS2) veya üstü işletim sistemlerinde bulunur. Kullanılabilir değerler: • `1` – AM-PPL teknolojisini kullanan Kaspersky Endpoint Security işlemlerinin koruması etkin. • `0` – AM-PPL teknolojisini kullanan Kaspersky Endpoint Security işlemlerinin koruması devre dışı.
	`UPGRADEMODE`	Uygulama yükseltme modu: • `Seamless`, uygulamayı bilgisayarı yeniden başlatarak yükseltmek anlamına gelir (varsayılan değer). • `Force`, uygulamayı yeniden başlatma yapmadan yükseltmek anlamına gelir. 11.10.0 sürümünden itibaren, uygulamayı yeniden başlatma yapmadan yükseltebilirsiniz. Uygulamanın önceki bir sürümünü yükseltmek için bilgisayarı yeniden başlatmanız gerekir. Ayrıca 11.11.0 sürümünden itibaren yamaları yeniden başlatma yapmadan da yükleyebilirsiniz. Kaspersky Endpoint Security'yi yüklerken yeniden başlatma gerekli değildir. Böylece uygulamanın yükseltme modu uygulama ayarlarında belirtilecektir. Bu parametreyi uygulama ayarlarında veya ilkede değiştirebilirsiniz. Önceden yüklenmiş bir uygulamayı yükseltirken, setup.ini dosyasında belirtilen parametrenin önceliği, uygulama ayarlarında veya komut satırında belirtilen parametrenin önceliğinden daha yüksektir. Örneğin, setup.ini dosyasında `Force` yükseltme modu belirtilmişse ve uygulama ayarlarında `Seamless` modu belirtilmişse, yükseltme yeniden başlatılmadan yüklenecektir (`Force`). `UPGRADEMODE` parametresinin belirtilmediği setup.ini dosyasını kullanıyorsanız, yükleyici varsayılan değeri (`Seamless`) kullanacak ve yükseltmeyi bilgisayar yeniden başlatıldığında yükleyecektir.
	`SetupReg`	Kayıt defteri anahtarlarının setup.reg dosyasından kayıt defterine yazılmasını etkinleştirir. `SetupReg: setup.reg` parametre değeri.
	`EnableTraces`	Uygulama izlemeyi etkinleştirme veya devre dışı bırakma. Kaspersky Endpoint Security başladıktan sonra, iz dosyalarını `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasörüne kaydeder. Kullanılabilir değerler: • `1` – izleme etkinleştirildi. • `0` – izleme devre dışı bırakıldı (varsayılan değer).

Bölüm	Parametre	Açıklama
	`TracesLevel`	İzlerin ayrıntı düzeyi. Kullanılabilir değerler: • `100` (kritik). Sadece önemli hatalarla ilgili mesajlar. • `200` (yüksek). Önemli hatalar dahil tüm hatalarla ilgili mesajlar. • `300` (tanısal). Tüm hataların yanı sıra uyarılarla ilgili mesajlar. • `400` (önemli). Tüm hata mesajları, uyarılar ve ek bilgiler. • `500` (normal). Tüm hatalar ve uyarıların yanı sıra uygulamanın normal moddaki çalışmasıyla ilgili ayrıntılı bilgiler hakkında mesajlar (varsayılan). • `600` (düşük). Tüm mesajlar.
	`RESTAPI`	REST API aracılığıyla uygulamanın yönetilmesi. Uygulamayı REST API aracılığıyla yönetmek için kullanıcı adı belirlemeniz gerekir (`RESTAPI_User` parametresi). Kullanılabilir değerler: • `1` – REST API aracılığıyla yönetime izin verilir. • `0` – REST API aracılığıyla yönetim engellenir (varsayılan değer). Uygulamayı REST API aracılığıyla yönetmek için, yönetim sistemleri kullanılarak yönetime izin verilmiş olmalıdır. Bunu yapmak için `AdminKitConnector=1` parametre ayarını yapın. Uygulamayı REST API aracılığıyla yönetiyorsanız, uygulamayı Kaspersky yönetim sistemlerini kullanarak yönetmek imkansızdır.
	`RESTAPI_User`	Uygulamanın REST API aracılığıyla yönetilmesi için kullanılan Windows etki alanının kullanıcı adı. Uygulamanın REST API aracılığıyla yönetilmesi izni sadece bu kullanıcıya verilir. Kullanıcı adını şu biçime göre girin `<DOMAIN>\<UserName>` (örneğin, `RESTAPI_User=COMPANY\Administrator`). REST API ile çalışmak üzere sadece bir kullanıcı seçebilirsiniz. Bir kullanıcı adı eklemek, uygulamanın REST API aracılığıyla yönetilmesi için bir ön şarttır.
	`RESTAPI_Port`	Uygulamanın REST API aracılığıyla yönetilmesi için kullanılan port. Varsayılan olarak 6782 portu kullanılır. Portun boş olduğundan emin olun.
	`RESTAPI_Certificate`	İstekleri tanımlama için sertifika (örneğin, `RESTAPI_Certificate=C:\cert.pem`). Kaspersky Endpoint Security'nin REST istemcisiyle güvenli etkileşimi, istek tanımlaması yapılandırılmasını gerektirir. Bunu yapmak için bir sertifika yüklemeniz ve ardından her isteğin yükünü imzalamanız gerekir.
	`StandaloneMode`	Uygulamayı Endpoint Detection and Response Agent (EDR Agent) modunda yükleme. *Endpoint Detection and Response Agent*, Kaspersky Managed Detection and Response ve Kaspersky Anti Targeted Attack Platform çözümlerini desteklemek için kurumun BT altyapısındaki bireysel iş istasyonlarına ve sunuculara yüklenen bir uygulamadır. EDR Agent üçüncü taraf EPP uygulamalarıyla uyumludur. Bu, Kaspersky'nin Detection and Response özelliğinin yanı sıra üçüncü taraf altyapı güvenlik araçlarını da kullanmanıza olanak tanır. EDR Agent'ı yüklemek için `[Components]` bölümünde `StandaloneKATA`, `StandaloneNDR` veya `StandaloneMDR` bileşenlerini seçin. EDR Agent diğer uygulama bileşenlerini desteklemez. Kullanılabilir değerler: • Uygulamayı EDR Agent modunda yüklemek için `1`. • Uygulamayı Standart modda (varsayılan) yüklemek için `0`.
	`KSVLAMode`	Uygulamayı Light Agent modunda yükleme. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Kullanılabilir değerler: • Uygulamayı Light Agent modunda yüklemek için `1`. • Uygulamayı Standart modda (varsayılan) yüklemek için `0`.
	`InstallOnVDI`	Uygulamayı Light Agent modunda (`KSVLAMode=1`) yüklerken VDI koruma modunu etkinleştirme. VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur. Kullanılabilir değerler: • VDI koruma modunu etkinleştirmek için `1`. • VDI koruma modunu devre dışı bırakmak için `0` (varsayılan).

Bölüm	Parametre	Açıklama
	`KESExclusions`	Uygulamayı sunucuya yüklerken önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar ekleme. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Örneğin, SQL sunucuları için önceden tanımlanmış tarama istisnaları MDF ve LDF veritabanı dosyalarını içerir. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Kullanılabilir değerler: • `1` önceden tanımlanmış tarama istisnalarını ve güvenilen uygulamaları etkinleştirir. • `0` önceden tanımlanmış tarama dışlamalarını ve güvenilen uygulamaları devre dışı bırakır (varsayılan).
	`LAExclusions`	Uygulamayı bir sanal makineye yüklerken önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar ekleme (Light Agent modu). Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir. Kullanılabilir değerler: • `1` önceden tanımlanmış tarama istisnalarını ve güvenilen uygulamaları etkinleştirir. • `0` önceden tanımlanmış tarama dışlamalarını ve güvenilen uygulamaları devre dışı bırakır (varsayılan).
	`EnableUniqueSensorID`	Uygulamanın yüklenmesi veya güncellenmesi sırasında benzersiz bir bilgisayar tanımlayıcısı (Sensor ID) oluşturma. Sensor ID, Kaspersky Anti Targeted Attack Platform çözümünde sunucuya telemetri gönderen bilgisayarları tanımlamak için kullanılır. Sensor ID oluşturulurken uygulama, anakart seri numarası gibi bilgisayarın yapılandırmasını dikkate alan bir algoritma kullanır. Bazı durumlarda, örneğin uygulama sanal bir ortamda kullanılırken, Sensor ID çoğaltılabilir. Sonuç olarak, Kaspersky Anti Targeted Attack Platform telemetrinin gönderildiği bilgisayarı tanımlayamaz. Benzersiz bir Sensor ID oluşturmak için `EnableUniqueSensorID=1` parametresini ayarlamanız gerekir. Sonuç olarak, uygulama Sensor ID'yi oluşturmak için bilgisayarla ilgili diğer verileri dikkate alan farklı bir algoritma kullanacaktır. Bu, benzersiz bir Sensor ID sağlar. Varsayılan olarak parametre ayarlanmamıştır. Uygulama, aşağıdaki durumlarda Sensor ID'yi devralır: • uygulama sürümünün güncellenmesi; • [KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi. Uygulama onarımının bir parçası olarak, yükleyici Sensor ID değerini devralmaya çalışır. Sensor ID geri yüklenemiyorsa, uygulama yeni bir Sensor ID oluşturur.
	`CitrixCompatibility`	Citrix Provisioning Services'ın bir sanal makineye Kaspersky Endpoint Security'yi yüklemesine yönelik desteğin etkinleştirilmesi.
`[Components]`	`ALL`	Tüm bileşenlerin yüklenmesi. Parametre değeri `1` belirtilirse her bir bileşenin yükleme ayarı ne olursa olsun tüm bileşenler yüklenir. Detection and Response çözümlerinin desteklenme biçimi nedeniyle, Endpoint Detection and Response Optimum ve Sandbox bileşenleri bilgisayara yüklenir. Endpoint Detection and Response Expert (cloud) bileşeni bu yapılandırma ile uyumlu değildir.
	`MailThreatProtection`	Posta Tehdidi Koruması.
	`WebThreatProtection`	Web Tehdidi Koruması.
	`AMSI`	AMSI Koruması.
	`HostIntrusionPrevention`	Sunucu Yetkisiz Erişim Önleme.
	`BehaviorDetection`	Davranış Tespiti.
	`ExploitPrevention`	Exploit Önleme.
	`RemediationEngine`	Düzeltme Altyapısı.
	`Firewall`	Güvenlik Duvarı.
	`NetworkThreatProtection`	Ağ Tehdidi Koruması.
	`WebControl`	İnternet Denetimi.
	`DeviceControl`	Aygıt Denetimi.

Bölüm	Parametre	Açıklama
	`ApplicationControl`	Uygulama Denetimi.
	`AdaptiveAnomaliesControl`	Uyarlamalı Anomali Denetimi.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Günlük Denetimi
	`AntiCryptor`	Şifreleyici Önleyici
	`FileThreatProtection`	Dosya Tehdidi Koruması.
	`SystemIntegrityMonitor`	Sistem Bütünlüğü İzleme.
	`FileEncryption`	Dosya Düzeyinde Şifreleme kitaplıkları.
	`DiskEncryption`	Tam Disk Şifreleme kitaplıkları.
	`MSBitLocker`	BitLocker Şifreleme yönetim kitaplıkları.
	`BadUSBAttackPrevention`	BadUSB Saldırısı Önleme.
	`EDR`	Endpoint Detection and Response Optimum Bu bileşen Endpoint Detection and Response Expert (cloud) (`EDRCloud`) ve Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) bileşenleri ile uyumlu değildir.
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Bu bileşen Endpoint Detection and Response Optimum (`EDR`) ve Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) bileşenleri ile uyumlu değildir.
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Bu bileşen Endpoint Detection and Response Expert (cloud) (`EDRCloud`) ve Endpoint Detection and Response Optimum (`EDR`) bileşenleri ile uyumlu değildir.
	`SB`	Kaspersky Sandbox veya KATA Sandbox. *Kaspersky Sandbox*, Kaspersky'nin bağımsız bir Detection and Response çözümüdür. *KATA Sandbox*, Kaspersky Anti Targeted Attack Platform çözümünün bir bileşenidir.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Bu bileşen Endpoint Detection and Response Expert (cloud) (`EDRCloud`) ve Endpoint Detection and Response Optimum (`EDR`) bileşenleri ile uyumlu değildir.
	`AdminKitConnector`	Yönetim sistemlerini kullanarak uygulama yönetimi. Yönetim sistemlerine örnek olarak Kaspersky Security Center verilebilir. Kaspersky yönetim sistemlerine ek olarak üçüncü taraf çözümler de kullanabilirsiniz. Kaspersky Endpoint Security bu amaçla bir API sunar. Kullanılabilir değerler: • `1` – yönetim sistemlerinin yardımıyla uygulama yönetimine izin verilir (varsayılan değer). • `0` – uygulama yönetimine sadece yerel arabirim üzerinden izin verilir.
	`KUMAIntegration`	KUMA ile entegrasyon.
	`StandaloneKATA`	Kaspersky Anti Targeted Attack Platform (EDR) ile entegrasyon için uygulamayı Endpoint Detection and Response Agent (EDR Agent) modunda yükleme.
	`StandaloneMDR`	Kaspersky Managed Detection and Response ile entegrasyon için uygulamayı Endpoint Detection and Response Agent (EDR Agent) modunda yükleme.

Bölüm	Parametre	Açıklama
	`StandaloneNDR`	Kaspersky Anti Targeted Attack Platform (NDR) ile entegrasyon için uygulamayı Endpoint Detection and Response Agent (EDR Agent) modunda yükleme.
	`StandaloneSiemTelemetry`	KUMA ile entegrasyon için uygulamayı Endpoint Detection and Response Agent (EDR Agent) modunda yükleme.
`[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.
	`Updater`	Güncelleme görevi. Kullanılabilir değerler: • `1` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenir. • `0` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenmez.

Kaspersky Endpoint Security for Windows işlemleri

Kaspersky Endpoint Security for Windows, aşağıdaki tabloda açıklanan işlemleri başlatır.

Kaspersky Endpoint Security for Windows işlemleri

Dosya adı	Amaç
avp.exe	Kaspersky Endpoint Security for Windows çalışma işlemi.
avpsus.exe	Bu işlem, kritik ve onaylı uygulama modülü güncellemelerinin yüklenmesini ve geri alınmasını sağlar.

Uygulama bileşenlerini değiştirme

Uygulamanın yüklenmesi sırasında, kullanılabilecek bileşenleri seçebilirsiniz. Kullanılabilecek uygulama bileşenlerini aşağıdaki şekillerde değiştirebilirsiniz:

- Kurulum Sihirbazını kullanarak yerel olarak.

  Uygulama bileşenleri, bir Windows işletim sisteminin Denetim Masasından, normal yöntem kullanılarak kaldırılır. Uygulama Kurulum Sihirbazını çalıştırın ve kullanılabilir uygulama bileşenlerini değiştirmeyi seçin. Ekrandaki talimatları uygulayın.

  > Uygulama Kaspersky Security Center aracılığıyla yüklendiyse bu yöntem kullanılamaz. Denetim Masasındaki uygulama bileşenlerinin seçimini yalnızca uygulamayı yerel olarak yükledikten sonra değiştirebilirsiniz.

- Kaspersky Security Center kullanarak uzaktan.

  Uygulama bileşenlerini değiştirme görevi, uygulama yüklendikten sonra Kaspersky Endpoint Security'nin bileşenlerini değiştirmenize olanak tanır.

Uygulama bileşenleri değiştirirken şunlara özellikle dikkat edin:

- Windows Server çalıştıran bilgisayarlara, Kaspersky Endpoint Security ürününün tüm bileşenlerini yükleyemezsiniz (örneğin, Uyarlanabilir Anomali Denetimi bileşeni kullanılamaz).
- Bilgisayarınızdaki sabit sürücüler Tam Disk Şifreleme (FDE) ile korunuyorsa Tam Disk Şifreleme bileşenini kaldıramazsınız. Tam Disk Şifreleme bileşenini kaldırmak için bilgisayarın tüm sabit sürücülerinin şifresini çözün.
- Bilgisayar şifrelenmiş dosyalara (FLE) sahipse ya da kullanıcı şifrelenmiş çıkarılabilir sürücüler (FDE veya FLE) kullanıyorsa, Veri Şifreleme bileşenleri kaldırıldıktan sonra dosyalara ve çıkartılabilir sürücülere erişmek mümkün olmaz. Dosyalara ve çıkarılabilir sürücülere, Veri Şifreleme bileşenlerini tekrar yükleyerek erişebilirsiniz.
- Uygulama bir VDI altyapısında Light Agent modunda yüklüyse, ayarlanan bileşenlerin değiştirilmesi desteklenmez.

Yönetim Konsolu'nda (MMC) uygulama bileşenleri nasıl eklenir veya kaldırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Yüklenecek bileşenleri seçin** seçimini yapın.

2. Adım. Uygulama bileşenlerini değiştirme için görev ayarları

Uygulamanın yapılandırmasını seçin:

- **Ana bilgisayarları korumak için standart mod**. Varsayılan yapılandırma. Bu yapılandırma, Detection and Response çözümleri için destek sağlayan bileşenler de dahil olmak üzere uygulamanın tüm bileşenlerini kullanmanıza olanak tanır. Bu yapılandırma, bilgisayarın çeşitli tehditlere, ağ saldırılarına ve dolandırıcılığa karşı kapsamlı bir şekilde korunması için kullanılır.

- **Gelişmiş tehditlere ve hedefli saldırılara karşı koruma sağlayan Endpoint Detection and Response Agent**. Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.

  EDR Agent'ın MDR ile çalışması için uygulama yapılandırmasını değiştirirken, telemetri almaktan sorumlu bileşenlerin etkinleştirildiğinden emin olun.

- **Sanal ortamları korumak için Light Agent**. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.

Kullanıcının bilgisayarında kullanılabilecek uygulama bileşenlerini seçin.

3. Adım. Gelişmiş ayarlar

Görev için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

4. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

5. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görevi başlatmak için bir zamanlama ayarlayın, örneğin manuel olarak ya da bilgisayar boş olduğunda.

6. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Uygulama Denetimi bileşenini ekle*.

7. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Uygulama Web Console'da ve Cloud Console'da nasıl eklenir veya kaldırılır

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2.0** seçimini yapın.
2. **Görev türü** açılır listesinde, **Uygulama bileşenlerini değiştirme**'i seçin.
3. **Görev adı** alanına, *Uygulama Denetimi bileşenini ekleyin* gibi kısa bir açıklama girin.
4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Örneğin ayrı bir yönetim grubu seçin ya da bir seçim oluşturun.

3. Adım. Görev oluşturmayı tamamlama

Oluşturma işlemi tamamlandığında görev ayrıntılarını aç onay kutusunu işaretleyin ve sihirbazı tamamlayın.

Görev ayarlarından **Uygulama ayarları** sekmesini seçin. Ardından, uygulamanın yapılandırmasını seçin:

- **İş istasyonlarını ve sunucuları korumak için standart mod**. Varsayılan yapılandırma. Bu yapılandırma, Detection and Response çözümleri için destek sağlayan bileşenler de dahil olmak üzere uygulamanın tüm bileşenlerini kullanmanıza olanak tanır. Bu yapılandırma, bilgisayarın çeşitli tehditlere, ağ saldırılarına ve dolandırıcılığa karşı kapsamlı bir şekilde korunması için kullanılır.
- **Gelişmiş tehditlere ve hedefli saldırılara karşı koruma sağlayan Endpoint Detection and Response Agent**. Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.

  EDR Agent'ın MDR ile çalışması için uygulama yapılandırmasını değiştirirken, telemetri almaktan sorumlu bileşenlerin etkinleştirildiğinden emin olun.

- **Sanal ortamları korumak için Light Agent**. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.

Kullanıcının bilgisayarında kullanılabilecek uygulama bileşenlerini seçin. Görev için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

Bunun sonucunda, kullanıcıların bilgisayarındaki Kaspersky Endpoint Security bileşenleri sessiz modda değiştirilecektir. Kullanılabilir bileşenlerin ayarları, uygulamanın yerel arabiriminde görüntülenir. Uygulamaya dahil edilmemiş bileşenler devre dışı bırakılır ve bu bileşenlerin ayarları kullanılamaz.

Kaspersky Endpoint Security yüklenirken, güncellenirken veya kaldırılırken hatalar oluşabilir. Bu hataları çözme hakkında daha fazla bilgi için lütfen Teknik Destek Bilgi Tabanına bakın.

Göervin Gelişmiş Ayarları

Parametre	Açıklama
Görev ayarları	**Uyumsuz üçüncü taraf uygulamaları olup olmadığını kontrol edin**. Kaspersky Endpoint Security, varsayılan olarak yüklü uygulamaların uyumluluğunu kontrol eder. Uyumluluk sorunlarına neden olabilecek yazılımların listesi incompatible.txt dosyasında mevcuttur. Dosya dağıtım kitine dahildir. Yüklü yazılım taraması etkinleştirilirse, listeden bir uygulama algılandığında Kaspersky Endpoint Security görevi durdurur. Üçüncü taraf yazılımın satıcı belgeleri Endpoint Protection Platform (EPP) ile uyumluluk iddia ediyorsa, yüklü yazılım taramasını devre dışı bırakabilirsiniz. **Uyumlu olmayan üçüncü taraf uygulamalarını kaldır**. Bileşen kümesini değiştirmeden önce incompatible.txt listesinde yer alan uygulamaların otomatik olarak kaldırılması. Bu işlev etkinleştirilirse Kaspersky Endpoint Security, göreve devam etmek için uyumluluk sorunlarına neden olabilecek uygulamaları kaldırmaya çalışır. **Azure WVD uyumluluk modunu kullan**. Bu özellik, Kaspersky Anti Targeted Attack Platform konsolunda Azure sanal makine durumunun doğru görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensor ID) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensor ID atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensor ID değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir.
İstisnalar	Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, uygulamayı sanal ortamları korumak için Light Agent modunda yükleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir. Güvenilen bölgeyi daha sonra ilke özelliklerinde de yapılandırabilirsiniz: tarama istisnaları ve güvenilir uygulamalar.
Ayrı mod / Birleştirilmiş mod	İş istasyonları ve sunucular için ayrı bileşen setleri oluşturabilirsiniz - **Ayrı mod**. Kurulum paketini dağıtmadan önce, yükleyici işletim sistemi türünü algılar ve yalnızca bu işletim sistemi türü için seçtiğiniz uygulama bileşenlerini yükler. Bu şekilde, iş istasyonları ve sunucular için aynı kurulum paketini kullanabilirsiniz. **Birleştirilmiş mod**, iş istasyonu ve sunucular için ortak bir bileşen listesi sunar. Bileşenlerin kullanılabilirliği işletim sistemi türüne bağlıdır. Bu modda, iş istasyonları için ayrı bir kurulum paketi ve sunucular için ayrı bir kurulum paketi oluşturmanızı öneririz. Kurulum paketindeki ortak bileşen listesini yalnızca Standart modda yapılandırabilirsiniz.
Uygulama bileşenlerini değiştirmek için parola kullan	Yöneticiler genellikle Kaspersky Endpoint Security'ye erişimi kısıtlamak için Parola korumasını etkinleştirir. Yani, uygulama bileşenlerinin seçimini değiştirmek için, **Uygulamayı kaldır/değiştir/geri yükle** iznine sahip bir kullanıcının kimlik bilgilerini girmeniz gerekir. Örneğin, KLAdmin hesabını kullanabilirsiniz.
Kaspersky Endpoint Agent ve Kaspersky Security for Windows Server'ı kaldırmak için parolayı kullan	Yöneticiler genellikle Kaspersky Endpoint Agent (KEA) ve Kaspersky Security for Windows Server'a (KSWS) erişimi kısıtlamak için bu görevlerin ayarlarında Parola korumasını etkinleştirir. Yani, [KES+KEA] yapılandırmasından [KES+yerleşik aracı] yapılandırmasına geçiş yapıyorsanız veya KSWS'den KES'e geçiş yapıyorsanız, bu uygulamaları kaldırmak için bir parola girmeniz gerekir.

Uygulamanın önceki bir sürümünü yükseltme

Uygulamanın önceki sürümünü yeni sürüme güncellerken şunlara dikkat edin:

- Güncellemeyi başlatmadan önce tüm açık uygulamaları kapatmanızı öneririz.
- Kaspersky Endpoint Security, güncellemeden önce Tam Disk Şifreleme işlevini engeller. Tam Disk Şifreleme kilitlenemiyorsa yükseltme yüklemesi başlamaz. Uygulamayı güncelledikten sonra Tam Disk Şifreleme işlevi geri yüklenir.
- Uygulamanın dilini değiştirmek için *Uygulamayı uzaktan yükle* görevinde, tercih ettiğiniz yerelleştirmeye sahip kurulum paketini seçin ve uygulamayı güncelleyin. Uygulama dilini değiştirme özelliği ilk olarak Kaspersky Endpoint Security for Windows 14.2 sürümünde kullanıma sunulmuştur.

Kaspersky Endpoint Security, uygulamanın şu sürümleri için güncellemeleri destekler:

- Kaspersky Endpoint Security 12.3 for Windows (yapı 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (yapı 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (yapı 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (yapı 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (yapı 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (yapı 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (yapı 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (yapı 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (yapı 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (yapı 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (yapı 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (yapı 14.1.0.423)

Kaspersky Endpoint Security yüklenirken, güncellenirken veya kaldırılırken hatalar oluşabilir. Bu hataları çözme hakkında daha fazla bilgi için lütfen Teknik Destek Bilgi Tabanına bakın.

Uygulama yükseltme yöntemleri

Kaspersky Endpoint Security bilgisayardan şu yollarla güncellenebilir:

- Kaspersky güncelleme hizmetini kullanma (Seamless Update – SMU).
- Kurulum Sihirbazını kullanarak yerel olarak.
- komut satırını kullanarak yerel olarak.
- Kaspersky Security Center kullanarak uzaktan.
- Microsoft Windows Grup İlkesi Yönetimi Düzenleyicisini kullanarak uzaktan (ayrıntılar için Microsoft Teknik Destek web sitesini ziyaret edin).
- System Center Configuration Manager kullanarak uzaktan.

Kurumsal ağa dağıtılan uygulama, varsayılan setten farklı bir bileşen seti içeriyorsa uygulamanın Yönetim Konsolu (MMC) üzerinden güncellenmesi, Web Console üzerinden güncellenmesinden farklıdır. Kaspersky Endpoint Security'yi güncelleyeceğiniz zaman şunları dikkate alın:

- Kaspersky Security Center Web Console.

  Uygulamanın yeni sürümü için varsayılan bileşen seti ile bir kurulum paketi oluşturursanız kullanıcının bilgisayarında bulunan bileşenler seti değiştirilmez. Kaspersky Endpoint Security'yi varsayılan bileşenler seti ile birlikte kullanmak için kurulum paketi özelliklerini açmalı, bileşen grubunu değiştirmeli ve ardından orijinal bileşen setine dönerek değişiklikleri kaydetmelisiniz.

- Kaspersky Security Center Yönetim Konsolu.

  Güncelleme sonrası uygulama bileşenleri seti, kurulum paketindeki bileşen seti ile aynı olacaktır. Yani uygulamanın yeni sürümü varsayılan bileşen setine sahipse örneğin yerleşik MDR aracısı, varsayılan sete dahil olmadığından bilgisayardan kaldırılır. Uygulamayı güncelleme öncesiyle aynı bileşen setiyle kullanmaya devam etmek için kurulum paketi ayarlarından gerekli bileşenleri seçin.

Uygulamayı yeniden başlatma olmadan yükseltme

Uygulamayı yeniden başlatma yapmadan yükseltmek, uygulama sürümü güncellendiğinde sunucunun kesintisiz çalışmasını sağlar.

Uygulamayı yeniden başlatma yapmadan yükseltmenin bazı sınırlamaları vardır:

- 11.10.0 sürümünden itibaren, uygulamayı yeniden başlatma yapmadan yükseltebilirsiniz. Uygulamanın önceki bir sürümünü yükseltmek için bilgisayarı yeniden başlatmanız gerekir.
- 11.11.0 sürümünden itibaren yamaları yeniden başlatma yapmadan yükleyebilirsiniz. Uygulamanın önceki sürümlerine yönelik yamaları yüklemek için bilgisayarın yeniden başlatılması gerekebilir.

- Uygulamayı yeniden başlatma yapmadan yükseltme, veri şifreleme (Kaspersky encryption (FDE), BitLocker, Dosya Düzeyinde Şifreleme (FLE)) etkinleştirilmiş bilgisayarlarda kullanılamaz. Uygulamayı veri şifreleme etkinleştirilmiş bilgisayarlarda yükseltmek için bilgisayarın yeniden başlatılması gerekir.

- Uygulama yeniden başlatılmadan bir sanal makinede yükseltilemez. Bir sanal makinedeki uygulamayı yükseltmek için sanal makineyi yeniden başlatmanız gerekir.

Uygulamayı yükselttikten, bir yama yükledikten, uygulama bileşenleri kümesini değiştirdikten veya geri yükledikten sonra Kaspersky Endpoint Security yeni sürümü kullanmaya başlamak için yeniden başlatılır. Kaspersky Endpoint Security'nin yeniden başlatılması bir dakika kadar sürebilir. Bu sürede bilgisayarı koruma düzeyi azalır. Uygulama yeniden başlatıldıktan sonra bilgisayarın koruma seviyesi geri yüklenecektir.

Yönetim Konsolu'nda (MMC) uygulama yükseltme modu nasıl seçilir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
5. Uygulama yükseltme modunu yapılandırmak için **Gelişmiş ayarlar** bloğunda **Uygulama güncellemelerini yeniden başlatmadan yükle** onay kutusunu işaretleyin ya da işaretini kaldırın.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

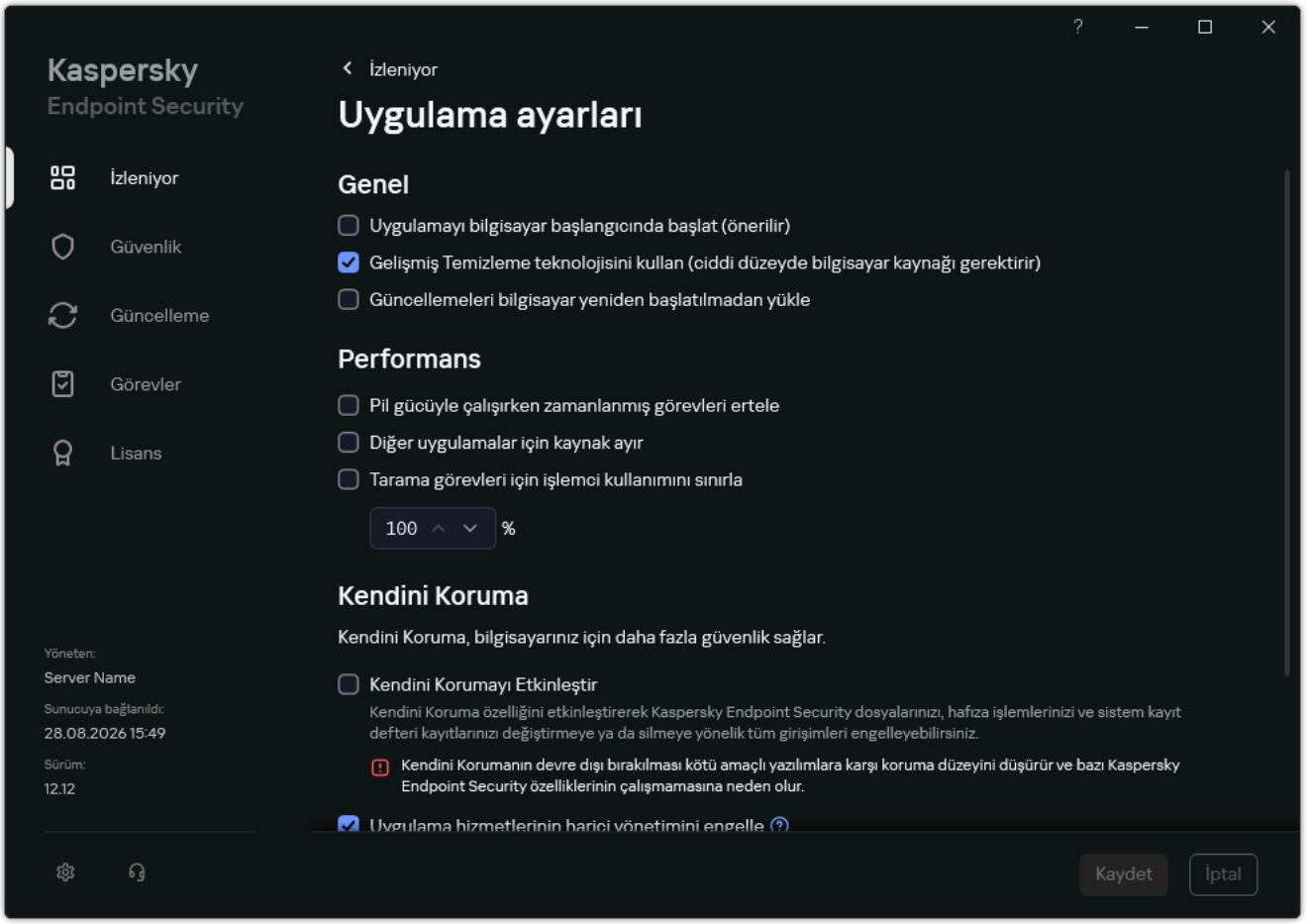
Web Console'da uygulama yükseltme modu nasıl seçilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kullanıcı Etkileşimi** bölümüne gidin.
5. **Uygulama güncelleme ayarları** bloğunda, uygulama yükseltme modunu yapılandırmak için **Uygulama güncellemelerini yeniden başlatmadan yükle** onay kutusunu seçin veya işaretini kaldırın.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde uygulama yükseltme modu nasıl seçilir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. Uygulama yükseltme modunu yapılandırmak için **Genel** bloğunda **Güncellemeleri bilgisayar yeniden başlatılmadan yükle** onay kutusunu işaretleyin ya da işaretini kaldırın.
4. Değişikliklerinizi kaydedin.

Uygulama yükseltme modunu uygulamayı komut satırından yüklerken de (`UPGRADEMODE` seçeneğini kullanarak) seçebilirsiniz.

Uygulamanın yeniden başlatma gerektirmeden güncellenmesi işlemi tamamlandıktan sonra, Kaspersky Endpoint Security'nin yeni sürümü bilgisayara yüklenmiş olacaktır. Uygulamanın önceki sürümü otomatik olarak silinir.

Önceki yükseltme işlemi tam olarak bitmeden uygulama yükseltmesini başlatamazsınız.

Kaspersky Security Center konsolundaki Kaspersky uygulama sürümü raporunu kullanarak Kaspersky Endpoint Security yükseltme durumunu kontrol edebilirsiniz.

Uygulamanın SMU güncellemesi

Kaspersky güncelleme hizmetini (Seamless Update; SMU) kullanarak uygulamayı güncellemek için diğer güncelleme yöntemlerinin aksine yükleyiciyi çalıştırmanıza gerek yoktur. Kaspersky Endpoint Security, uygulamanın yeni sürümünü antivirüs veritabanlarıyla birlikte aynı kaynaktan alıyor.

SMU güncellemesi, kuruluşunuzun tüm bilgisayarlarındaki uygulamanın en son sürüme güncellenmesini sağlar. Bir SMU güncellemesini uygulamadan önce, uygulamanın yeni sürümünü birkaç bilgisayarda test etmenizi öneririz. Bunu yapmak için, bu bilgisayarlardaki uygulamayı manuel olarak güncellemeniz gerekir (örneğin, Kurulum Sihirbazını kullanarak yerel olarak). SMU güncellemesi gerçekleştirirken bilgisayarları tek tek seçemezsiniz.

Uygulama için güncelleme takvimi Kaspersky personeli tarafından belirlenir. Uygulamanın yeni sürümünün sorunsuz çalıştığından emin olmak için Kaspersky, güncellemeleri adım adım kullanıma sunar. Bu, SMU güncellemenizi yeni bir sürümün yayınlanmasından iki ay sonrasına kadar alabileceğiniz anlamına gelir.

Veritabanlarının ve uygulama modüllerinin güncellemesi görevini kullanarak uygulamanın SMU güncellemesini yönetebilirsiniz. Uygulamanın yeni sürümünün antivirüs veritabanlarıyla aynı pakete dahil edilmesi için, *Veritabanlarının ve uygulama modüllerinin güncellemesi* görev ayarlarında *uygulama modüllerinin* güncellenmesine izin vermelisiniz. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görev ayarlarında, uygulamanın yeniden başlatılmadan güncellenmesine izin verebilirsiniz.

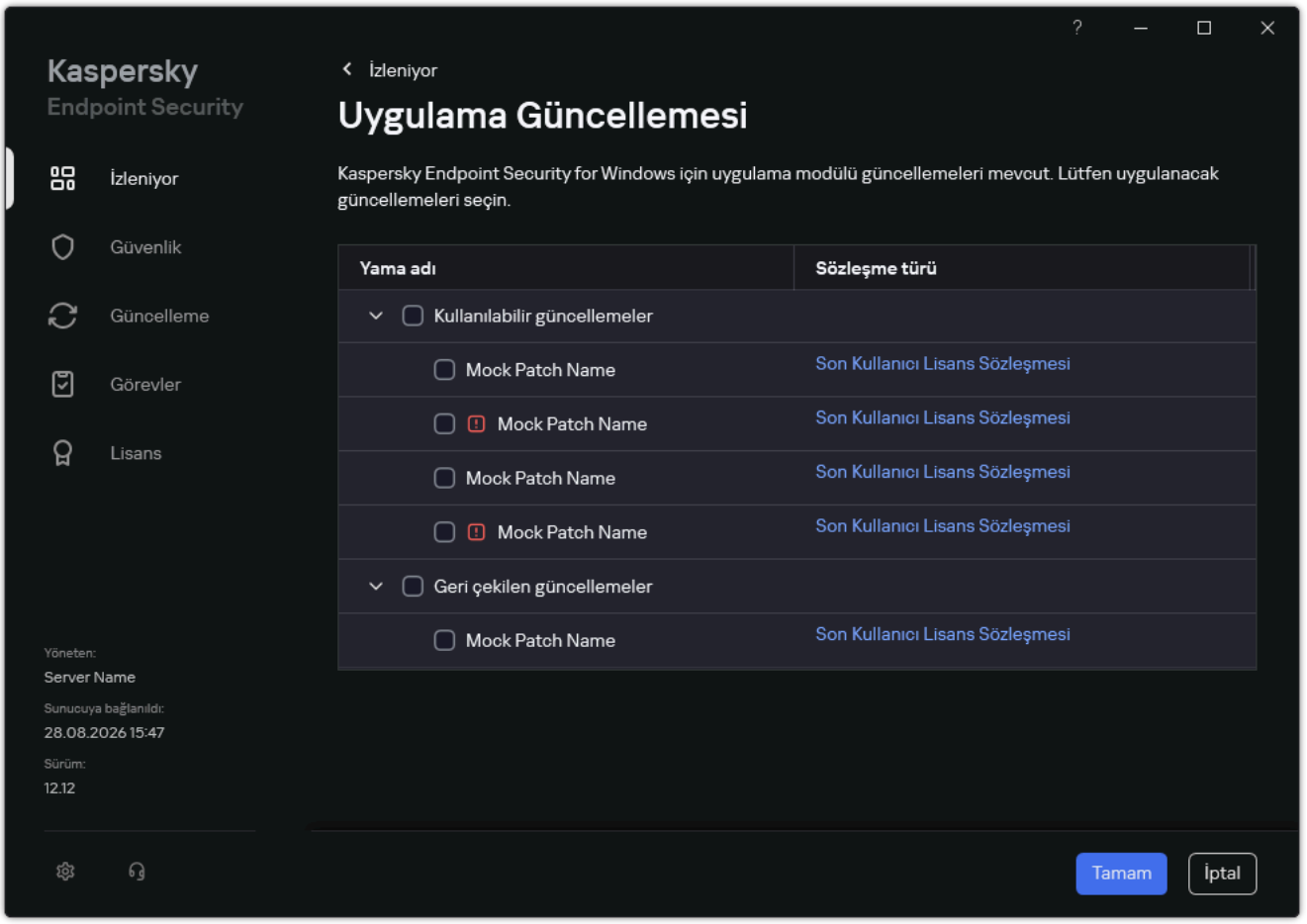
Uygulamanın SMU güncellemesinin adımları

1. **Uygulamanın yeni bir sürümü yayınlandıktan sonra Kaspersky güncellemeyi dağıtır.**
2. **Kullanıcı uygulamanın güncellenmesini onaylar.**

   Bilgisayar Kaspersky Security Center'a bağlıysa, güncelleme Kaspersky Security Center'da **Kaspersky veritabanlarının ve uygulama modüllerinin güncellemesi** bölümünde yer alır. Güncellemelerin onaylanması hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun.

   Bilgisayar Kaspersky Security Center'a bağlı değilse güncelleme, uygulama arayüzünün bildirim bölümünde bulunabilir: . Güncellemeyi onaylamak için, uygulamanın bir sürümünü seçin ve anlaşmaların hüküm ve koşullarını kabul edin (aşağıdaki resme bakın).
3. **Kaspersky Endpoint Security, yapılandırılan zamanlamaya uygun olarak *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini çalıştırır.**

Sonuç olarak, Kaspersky Endpoint Security uygulamayı “sessiz” modda günceller.



Kullanılabilir uygulama güncellemeleri

Uygulamayı kaldırma

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

Kaspersky Endpoint Security yüklenirken, güncellenirken veya kaldırılırken hatalar oluşabilir. Bu hataları çözme hakkında daha fazla bilgi için lütfen Teknik Destek Bilgi Tabanına bakın.

Uygulamayı Kaspersky Security Center üzerinden uzaktan kaldırma

Uygulamayı uzaktan kaldır görevini kullanarak uygulamayı uzaktan kaldırabilirsiniz. Bu görev uygulandığında, Kaspersky Endpoint Security uygulama kaldırma aracını kullanıcının bilgisayarına indirir. Uygulamanın kaldırma işlemi tamamlandığında araç da otomatik olarak kaldırılır.

Uygulama Yönetim Konsolu (MMC) aracılığıyla nasıl kaldırılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
   Görevler listesi açılır.
3. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Security Center Yönetim Sunucusu → Gelişmiş → Uygulamayı uzaktan kaldır seçimini yapın.

2. Adım. Kaldırılacak uygulamayı seçme

Kaspersky Security Center tarafından desteklenen uygulamayı kaldır'ı seçin.

3. Adım. Uygulama kaldırma için görev ayarları

Kaspersky Endpoint Security for Windows (14.2) seçimini yapın.

4. Adım. Kaldırma aracı ayarları

Şu ek uygulama ayarlarını yapılandırın:

- **Kaldırma yardımcı programını indirmeyi zorla**. Araç dağıtım yöntemini seçin:
  - **Ağ Aracısı'nı kullanarak**. Ağ Aracısı bilgisayara yüklü değilse öncelikle işletim sisteminin araçları kullanılarak Ağ Aracısı yüklenir. Bundan sonra, Kaspersky Endpoint Security Ağ Aracısı tarafından kaldırılır.
  - **Yönetim Sunucusu aracılığıyla işletim sistemi kaynaklarını kullanarak**. Araç, Yönetim Sunucusu aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağ Aracısı, istemci bilgisayarda yüklü değilse ancak istemci bilgisayar, Yönetim Sunucusu ile aynı ağdaysa bu seçeneği belirleyebilirsiniz.
  - **Dağıtım noktaları aracılığıyla işletim sistemi kaynaklarını kullanarak**. Araç, dağıtım noktaları aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağda en az bir dağıtım noktası varsa bu seçeneği belirleyebilirsiniz. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.
- **İndirmeden önce işletim sistemi sürümünü doğrula**. Gerekirse bu onay kutusunun işaretini kaldırın. Bu seçenek, bilgisayar işletim sistemi yazılım gereksinimlerini karşılamıyorsa kaldırma aracını indirmemenize olanak tanır. Bilgisayarın işletim sisteminin yazılım gereksinimlerini karşıladığından eminseniz bu doğrulamayı atlayabilirsiniz.

Uygulama kaldırma işlemi şifre korumalı ise şunları yapın:

1. **Kaldırma parolasını kullan** onay kutusunu işaretleyin.
2. **Düzenle** düğmesine tıklayın.
3. KLAdmin hesap parolasını girin.

5. Adım. İşletim sistemi yeniden başlatma ayarını seçme

Uygulamayı kaldırdıktan sonra bir yeniden başlatma gereklidir. Bilgisayarı yeniden başlatmak için uygulanacak eylemi seçin.

6. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

7. Adım. Görevi çalıştıracak hesabı seçme

İşletim sisteminin araçlarını kullanarak Ağ Aracısını yüklemek için kullanılacak hesabı seçin. Bu durumda, bilgisayar erişimi için yönetici hakları gereklidir. Birden çok hesap ekleyebilirsiniz. Hesap yeterli haklara sahip değilse Kurulum Sihirbazı bir sonraki hesabı kullanır. Kaspersky Endpoint Security'yi Ağ Aracısı araçlarını kullanarak kaldırırsanız bir hesap seçmeniz gerekmez.

8. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görevi başlatmak için bir zamanlama ayarlayın, örneğin manuel olarak ya da bilgisayar boş olduğunda.

9. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Kaspersky Endpoint Security 14.2 sürümünü kaldır*.

10. Adım. Görev oluşturmayı bitirme

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Uygulama sessiz modda kaldırılacaktır.

Web Console ve Cloud Console aracılığıyla uygulama nasıl kaldırılır

1. Web Console ana penceresinden **Görevler** seçimini yapın.
   Görevler listesi açılır.
2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Security Center**'ı seçin.
2. **Görev türü** açılır listesinde, **Uygulamayı uzaktan kaldır**'ı seçin.

3. **Görev adı** alanına *Teknik Destek bilgisayarlarından Kaspersky Endpoint Security'yi kaldırma* gibi kısa bir açıklama girin.

4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Örneğin ayrı bir yönetim grubu seçin ya da bir seçim oluşturun.

3. Adım. Uygulama kaldırma ayarlarını yapılandır

Bu adımda uygulama kaldırma ayarlarını yapılandırın:

1. **Yönetilen uygulamayı kaldır** türünü seçin.

2. **Kaspersky Endpoint Security for Windows**'yi seçin.

3. **Kaldırma yardımcı programını indirmeyi zorla**. Araç dağıtım yöntemini seçin:

   - **Ağ Aracısı'nı kullanarak**. Ağ Aracısı bilgisayara yüklü değilse öncelikle işletim sisteminin araçları kullanılarak Ağ Aracısı yüklenir. Bundan sonra, Kaspersky Endpoint Security Ağ Aracısı tarafından kaldırılır.

   - **Yönetim Sunucusu aracılığıyla işletim sistemi kaynaklarını kullanarak**. Araç, Yönetim Sunucusu aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağ Aracısı, istemci bilgisayarda yüklü değilse ancak istemci bilgisayar, Yönetim Sunucusu ile aynı ağdaysa bu seçeneği belirleyebilirsiniz.

   - **Dağıtım noktaları aracılığıyla işletim sistemi kaynaklarını kullanarak**. Araç, dağıtım noktaları aracılığıyla işletim sistemi kaynakları kullanılarak istemci bilgisayarlara iletilir. Ağda en az bir dağıtım noktası varsa bu seçeneği belirleyebilirsiniz. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

4. **Maksimum eş zamanlı indirme sayısı** alanında, uygulama kaldırma aracının indirilmesi için Yönetim Sunucusuna gönderilen isteklerin sayısı için bir sınır belirleyin. İstek sayısındaki sınır, ağın aşırı yüklenmesini önlemeye yardımcı olur.

5. **Kaldırma girişimlerinin maksimum sayısı** alanında, uygulamayı kaldırma girişimi için bir sınır belirleyin. Kaspersky Endpoint Security kaldırma işlemi bir hata ile sonlanırsa görev, kaldırma işlemi otomatik olarak yeniden başlatır.

6. Gerekirse **İndirmeden önce işletim sistemi sürümünü doğrula** onay kutusunun işaretini kaldırın. Bu seçenek, bilgisayar işletim sistemi yazılım gereksinimlerini karşılamıyorsa kaldırma aracını indirmemenize olanak tanır. Bilgisayarın işletim sisteminin yazılım gereksinimlerini karşıladığından eminseniz bu doğrulamayı atlayabilirsiniz.

4. Adım. Görevi çalıştıracak hesabı seçme

İşletim sisteminin araçlarını kullanarak Ağ Aracısını yüklemek için kullanılacak hesabı seçin. Bu durumda, bilgisayar erişimi için yönetici hakları gereklidir. Birden çok hesap ekleyebilirsiniz. Hesap yeterli haklara sahip değilse Kurulum Sihirbazı bir sonraki hesabı kullanır. Kaspersky Endpoint Security'yi Ağ Aracısı araçlarını kullanarak kaldırırsanız bir hesap seçmeniz gerekmez.

5. Adım. Görev oluşturmayı tamamlama

Son düğmesine tıklayarak sihirbazı sonlandırın. Görevler listesinde yeni bir görev görüntülenir.

Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçin ve **Başlat** düğmesine tıklayın. Uygulama sessiz modda kaldırılacaktır. Kaldırma tamamlandıktan sonra, Kaspersky Endpoint Security bilgisayarınızı yeniden başlatmanızı ister.

Uygulamanın kaldırılma işlemi parolayla korunuyorsa *Uygulamayı uzaktan kaldır* görevinin özelliklerine KLAdmin hesap parolasını girin. Görev, parola olmadan uygulanmayacaktır.

KLAdmin hesap parolasını Uygulamayı uzaktan kaldır görevinde kullanmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. Kaspersky Security Center'ın **Uygulamayı uzaktan kaldır** görevine tıklayın.
   Görev özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Kaldırma parolasını kullan** onay kutusunu işaretleyin.
5. KLAdmin hesap parolasını girin.
6. Değişikliklerinizi kaydedin.

Kaldırmayı tamamlamak için bilgisayarı yeniden başlatın. Bunun için Ağ Aracısı bir açılır pencere görüntüler.

Active Directory kullanarak uygulamayı uzaktan kaldırma

Bir Microsoft Windows grup ilkesi kullanarak uygulamayı uzaktan kaldırabilirsiniz. Uygulamayı kaldırmak için Grup İlkesi Yönetim Konsolu'nu (gpmc.msc) açmanız ve bir uygulama kaldırma görevi oluşturmak için Grup İlkesi Düzenleyicisini kullanmanız gerekir (daha fazla ayrıntı için lütfen Microsoft Teknik Destek web sitesi).

Uygulama kaldırma işlemi şifre korumalı ise şunları yapmanız gerekir:

1. Şu içeriğe sahip bir BAT dosyası oluşturun:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   <GUID> uygulamanın benzersiz kimliğidir. Teknik Destek Bilgi Bankasını veya aşağıdaki komutu kullanarak uygulamanın GUID'ini bulabilirsiniz:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Örnek

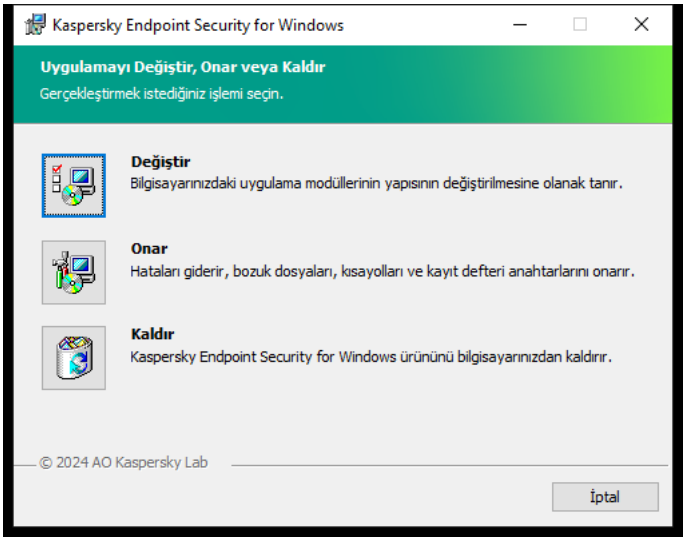
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Grup İlkesi Yönetim Konsolu'nda (gpmc.msc) bilgisayarlar için yeni bir Microsoft Windows ilkesi oluşturun.

3. Oluşturulan BAT dosyasını bilgisayarlarda çalıştırmak için yeni ilkeyi kullanın.

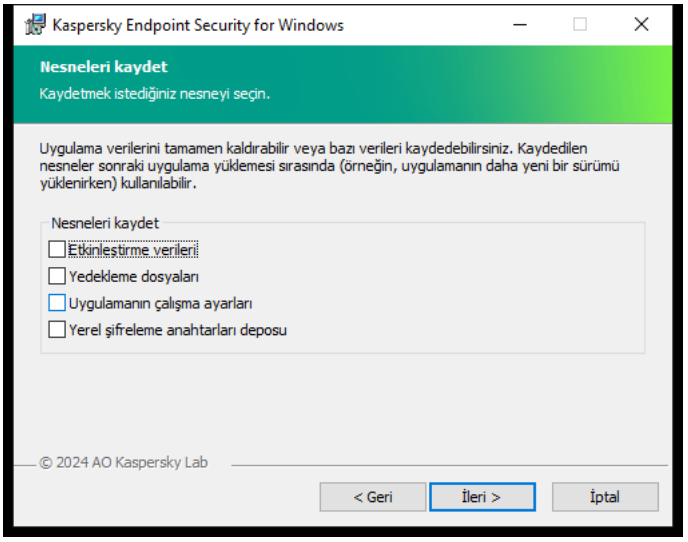
Uygulamayı yerel olarak kaldırma

Kurulum Sihirbazını kullanarak uygulamayı yerel olarak kaldırabilirsiniz. Kaspersky Endpoint Security, bir Windows işletim sisteminin Denetim Masasından ulaşılabilecek normal yöntemi kullanılarak kaldırılır. Kurulum Sihirbazı başlatılır. Ekrandaki talimatları uygulayın.



Uygulama kaldırma işlemini seçme

Uygulama tarafından kullanılan hangi verilerin daha sonra, bir uygulamanın bir sonraki yüklenmesi sırasında (uygulamanın daha yeni bir sürümüne yükseltme gibi) kullanım için saklanmasını istediğinizi belirtebilirsiniz. Herhangi bir veri belirlemek istemiyorsanız uygulama tamamen kaldırılır (aşağıdaki resme bakın).



Kaldırma sonrasında verileri kaydetme

Şu verileri kaydedebilirsiniz:

- **Etkinleştirme verileri**, uygulamayı tekrar etkinleştirmek zorunda kalmamanızı sağlar. Kaspersky Endpoint Security, lisans süresi yükleme öncesinde sona ermediği takdirde otomatik olarak bir lisans anahtarı ekler.
- **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 geri yükleyin. Bununla birlikte Kaspersky uzmanları, bilgisayarınıza zarar verebileceği için Yedekleme konumundan nesnelerin geri yüklenmesini önermez.
- **Uygulamanın çalışma ayarları** – uygulamanın yapılandırılması sırasında seçilen uygulama ayarlarının değerleridir.
- **Yerel şifreleme anahtarları deposu** – uygulamanın kaldırılmasından önce şifrelenen dosyalara ve sürücülere erişim sağlayan veridir. Şifrelenen dosyalara ve sürücülere erişim sağlamak için Kaspersky Endpoint Security'yi tekrar yüklerken veri şifreleme işlevini seçtiğinizden emin olun. Önceden şifrelenmiş dosyalara ve sürücülere erişim için başka bir işleme gerek yoktur.

Kaspersky Endpoint Security verileri `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasörüne kaydeder.

Uygulamayı, komut satırı üzerinden yerel olarak da silebilirsiniz.

Uygulama lisanslama

Bu bölümde, Kaspersky Endpoint Security lisanslamasıyla 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 paketine dahildir ve ayrıca `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES` konumundaki uygulama yükleme klasöründe bulunur.

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.

Lisans size, uygulamayı Son Kullanıcı Lisans Sözleşmesinin şartlarına uygun olarak kullanma ve teknik destek alma hakkı verir. Kullanılabilir özelliklerin listesi ve uygulama kullanım süresi, 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. Uygulama, ticari lisansla etkinleştirildikten sonra deneme lisansı altında etkinleştirilemez.

- *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:

- Lisans kimliği veya sipariş numarası.
- Lisansın verildiği kullanıcının ayrıntıları.
- Lisansı kullanarak etkinleştirilebilecek uygulamanın ayrıntıları.
- Lisanslı birim sayısı hakkındaki kısıtlamalar (örnek olarak, lisans kapsamında uygulamanın kullanılabileceği aygıt sayısı).
- Lisans süresi başlangıç tarihi.
- Lisans sona erme tarihi veya lisans süresi.
- Lisans türü.

Abonelik hakkında

Kaspersky Endpoint Security aboneliği, belirli parametrelerle (aboneliğin sona erme tarihi ve korunan aygıt sayısı gibi) 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 aboneliğin süresi dolduğunda abonelik yenilemesi için uygulamanın çalışmaya devam ettiği ödemesiz bir süre verilebilir. Böyle bir ödemesiz sürenin kullanılabilirliği ve süresi hizmet sağlayıcı tarafından belirlenir.

Kaspersky Endpoint Security'yi abonelik kapsamında kullanmak için hizmet sağlayıcıdan aldığınız etkinleştirme kodunu uygulamalısınız. Etkinleştirme kodu uygulandıktan sonra etkin anahtar eklenir. Etkin anahtar, uygulamayı abonelik kapsamında kullanma lisansını belirler. Abonelik kapsamındaki uygulamayı bir anahtarı dosyası kullanarak etkinleştiremezsiniz. Hizmet sağlayıcı sadece bir etkinleştirme kodu sağlayabilir. Bir abonelik kapsamında bir rezerve anahtar eklemek mümkün değildir.

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

Lisans anahtarı hakkında

Lisans anahtarı, uygulamayı etkinleştirmek ve ardından Son Kullanıcı Lisans Sözleşmesinin şartlarına uygun olarak kullanmak için kullanabileceğiniz bir bit dizisidir.

Lisans Sertifikası bir abonelik altında eklenen bir anahtar için sağlanmaz.

Bir lisans anahtarı eklemek için uygulamaya bir anahtar dosyası uygulayabilir ya da bir etkinleştirme kodu girebilirsiniz.

Son Kullanıcı Lisans Sözleşmesi ihlal edilirse anahtar engellenebilir. Anahtar engellendiyse alındıysa uygulamayı kullanmaya devam etmek için farklı bir anahtar eklemeniz gerekir.

İki anahtar türü mevcuttur: aktif ve yedek.

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

Bir *rezerve anahtar*, kullanıcıya uygulamayı kullanma hakkı verir ama şu anda kullanılmamaktadır. Bir rezerve anahtar, etkin anahtarın süresi dolduğunda otomatik olarak etkinleşir. Sadece etkin anahtar kullanılabilir olduğunda rezerve anahtar eklenebilir.

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

Yasaklanmış anahtarlar listesine bir anahtar eklenirse, uygulamayı etkinleştirmek için kullanılan lisansla tanımlanan uygulama işlevi sekiz gün boyunca kullanılabilir durumda kalır. Uygulama, kullanıcıya anahtarın yasaklanmış anahtarlar listesine eklendiğini bildirir. Sekiz gün geçtikten sonra, uygulamanın işlevselliği lisanın süresinin dolmasından sonra kullanılabilecek işlevsellik seviyesi ile sınırlanır. Lisansın süresi dolmadan önce yüklenmiş olan uygulama veritabanlarını kullanarak koruma ve denetim bileşenlerini kullanabilir ve bir taramayı çalıştırabilirsiniz. Uygulama, lisans sona ermeden önce değiştirilen ve şifrelenen dosyaları da şifreler ama yeni dosyaları şifrelemez. Kaspersky Security Network kullanılamaz.

Etkinleştirme kodu hakkında

Etkinleştirme kodu 20 alfasayısal karakterden meydana gelen benzersiz bir dizidir. Kaspersky Endpoint Security'yi etkinleştiren bir lisans anahtarı eklemek için bir etkinleştirme kodu girilir. Kaspersky Endpoint Security'yi satın aldıktan sonra belirtilen e-posta adresine bir etkinleştirme kodu gönderilir.

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

Uygulama bir etkinleştirme kodu kullanılarak etkinleştirildiğinde etkin anahtar eklenir. Rezerve anahtar sadece bir etkinleştirme kodu kullanılarak eklenebilir, bir anahtar dosyası kullanılarak eklenemez.

Uygulamayı etkinleştirdikten sonra etkinleştirme kodu kaybedilirse etkinleştirme kodunu geri yükleyebilirsiniz. Örneğin Kaspersky CompanyAccount'u kaydetmek için bir etkinleştirme koduna ihtiyaç duyabilirsiniz. Uygulama etkinleştirme işleminden sonra etkinleştirme kodu kaybolduğu takdirde, lisansı satın aldığınız Kaspersky iş ortağıyla iletişime geçin.

Anahtar dosyası hakkında

Anahtar dosyası, Kaspersky tarafından verilen .key uzantılı bir dosyadır. Anahtar dosyasının amacı, uygulamayı etkinleştiren bir lisans anahtarı eklemektir.

Kaspersky Endpoint Security'yi satın aldığınızda ya da Kaspersky Endpoint Security'nin deneme sürümünü sipariş ettiğinizde verdiğiniz e-posta adresine bir anahtar dosyası alırsınız.

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.
- Başka bir Yönetim Sunucusundan anahtar dosyası alma.

Uygulama bir anahtar dosyası kullanılarak etkinleştirildiğinde etkin anahtar eklenir. Rezerve anahtar, sadece bir anahtar dosyası kullanılarak eklenebilir, bir etkinleştirme kodu kullanılarak eklenemez.

İş istasyonları için lisans türüne göre uygulama işlevselliği karşılaştırılması

İş istasyonlarındaki Kaspersky Endpoint Security işlevsellikleri lisans türüne bağlıdır (aşağıdaki tabloya bakın).

Ayrıca sunucular için uygulama işlevselliği karşılaştırmasına da bakabilirsiniz

Kaspersky Next lisans türüne bağlı olarak uygulama işlevselliği karşılaştırması için Kaspersky Next Yardım bölümüne bakın.

Özellik	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Gelişmiş Tehdit Koruması								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Davranış Tespiti	✓	✓	✓	✓	✓	✓	✓	✓
Şifreleyici Önleyici	✓	✓	✓	✓	✓	✓	✓	✓
Exploit Önleme	✓	✓	✓	✓	✓	✓	✓	✓
Sunucu Yetkisiz Erişim Önleme	✓	✓	✓	✓	✓	✓	✓	✓
Düzeltme Altyapısı	✓	✓	✓	✓	✓	✓	✓	✓
Temel Tehdit Koruması								
Dosya Tehdidi Koruması	✓	✓	✓	✓	✓	✓	✓	✓
Web Tehdidi Koruması	✓	✓	✓	✓	✓	✓	✓	✓
Posta Tehdidi Koruması	✓	✓	✓	✓	✓	✓	✓	✓
Güvenlik Duvarı	✓	✓	✓	✓	✓	✓	✓	✓
Ağ Tehdidi Koruması	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB Saldırısı Önleme	✓	✓	✓	✓	✓	✓	✓	✓
AMSI Koruması	✓	✓	✓	✓	✓	✓	✓	✓
Güvenlik Denetimleri								
Günlük Denetimi	–	–	–	–	–	–	–	–
Uygulama Denetimi	✓	✓	✓	✓	✓	✓	✓	✓
Aygıt Denetimi	✓	✓	✓	✓	✓	✓	✓	✓
İnternet Denetimi	✓	✓	✓	✓	✓	✓	✓	✓
Uyarlamalı Anomali Denetimi	–	✓	✓	✓	✓	✓	–	✓
Sistem Bütünlüğü İzleme	–	–	–	–	–	–	–	–
Veri Şifreleme								
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
BitLocker Drive Encryption.	–	✓	✓	✓	✓	✓	–	✓
Dosya Düzeyinde Şifreleme	–	✓	✓	✓	✓	✓	–	✓
Çıkarılabilir sürücüleri şifreleme	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								

Özellik	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Kaspersky Sandbox lisansı ayrıca satın alınmalıdır)*	✓	✓	✓	✓	✓	✓	✓	✓
KUMA ile entegrasyon *(KUMA Entegrasyonu için lisans ayrıca satın alınmalıdır)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent modu *(uygulamayı etkinleştirmek için Light Agent'ın bağlı olduğu SVM'ye bir lisans anahtarı eklemeniz gerekir)*	–	–	–	–	–	–	✓	✓

Sunucular için lisans türüne göre uygulama işlevselliği karşılaştırılması

Sunuculardaki Kaspersky Endpoint Security işlevsellikleri lisans türüne bağlıdır (aşağıdaki tabloya bakın).

Ayrıca iş istasyonları için uygulama işlevselliği karşılaştırmasına da bakabilirsiniz

Kaspersky Next lisans türüne bağlı olarak uygulama işlevselliği karşılaştırması için Kaspersky Next Yardım bölümüne bakın.

Kaspersky Endpoint Security özellikleri karşılaştırması

Özellik	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Gelişmiş Tehdit Koruması								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Davranış Tespiti	✓	✓	✓	✓	✓	✓	✓	✓
Şifreleyici Önleyici	✓	✓	✓	✓	✓	✓	✓	✓

Özellik	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Exploit Önleme	✓	✓	✓	✓	✓	✓	✓	✓
Sunucu Yetkisiz Erişim Önleme	–	–	–	–	–	–	–	–
Düzeltme Altyapısı	✓	✓	✓	✓	✓	✓	✓	✓
Temel Tehdit Koruması								
Dosya Tehdidi Koruması	✓	✓	✓	✓	✓	✓	✓	✓
Web Tehdidi Koruması	–	✓	✓	✓	✓	✓	✓	✓
Posta Tehdidi Koruması	–	✓	✓	✓	✓	✓	✓	✓
Güvenlik Duvarı	✓	✓	✓	✓	✓	✓	✓	✓
Ağ Tehdidi Koruması	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB Saldırısı Önleme	✓	✓	✓	✓	✓	✓	✓	✓
AMSI Koruması	✓	✓	✓	✓	✓	✓	✓	✓
Güvenlik Denetimleri								
Günlük Denetimi	–	–	–	–	–	–	–	✓
Uygulama Denetimi	–	✓	✓	✓	✓	✓	–	✓
Aygıt Denetimi	–	✓	✓	✓	✓	✓	✓	✓
İnternet Denetimi	–	✓	✓	✓	✓	✓	✓	✓
Uyarlamalı Anomali Denetimi	–	–	–	–	–	–	–	–
Sistem Bütünlüğü İzleme	–	–	–	–	–	–	–	✓
Veri Şifreleme								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
BitLocker Drive Encryption.	–	✓	✓	✓	✓	✓	–	✓
Dosya Düzeyinde Şifreleme	–	–	–	–	–	–	–	–
Çıkarılabilir sürücüleri şifreleme	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–

Özellik	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Kaspersky Sandbox *(Kaspersky Sandbox lisansı ayrıca satın alınmalıdır)*	✓	✓	✓	✓	✓	✓	✓	✓
KUMA ile entegrasyon *(KUMA Entegrasyonu için lisans ayrıca satın alınmalıdır)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent modu *(uygulamayı etkinleştirmek için Light Agent'ın bağlı olduğu SVM'ye bir lisans anahtarı eklemeniz gerekir)*	–	–	–	–	–	–	✓	✓

Uygulamayı etkinleştirme

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

Uygulamayı aşağıdaki yollardan biriyle etkinleştirebilirsiniz:

- Etkinleştirme Sihirbazını kullanarak uygulama arabiriminden yerel olarak. Hem etkin anahtarı hem de rezerve anahtarı bu şekilde ekleyebilirsiniz.
- Kaspersky Security Center yazılım paketini kullanarak uzaktan.
  - *Anahtar ekle* görevini kullanarak.

    Bu yöntem belirli bir bilgisayara veya yönetim grubunun parçası olan bilgisayarlara bir anahtar eklemenize olanak tanır. Hem etkin anahtarı hem de rezerve anahtarı bu şekilde ekleyebilirsiniz.
  - Kaspersky Security Center Yönetim Sunucusunda depolanan bir anahtarı bilgisayarlara dağıtarak.

    Bu yöntemle, Kaspersky Security Center'a zaten bağlı olan bilgisayarlara ve yeni bilgisayarlara otomatik olarak bir anahtar ekleyebilirsiniz. Bu yöntemi kullanmak için önce anahtarı Kaspersky Security Center Yönetim Sunucusuna eklemeniz gerekir. Kaspersky Security Center Yönetim Sunucusuna anahtarlar ekleme hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım'ına bakın.

    Abonelikle satın alınan etkinleştirme kodu ilk seferde dağıtılır.

- Anahtarı Kaspersky Endpoint Security kurulum paketine ekleyerek.

  Bu yöntem, Kaspersky Endpoint Security dağıtımı sırasında anahtarı Kurulum paketi özelliklerine eklemenizi sağlar. Uygulama, kurulum sonrasında otomatik olarak etkinleştirilir.

- 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.

Kaspersky Endpoint Security, sanal ortamları korumak için Light Agent modunda kullanılıyorsa uygulamayı ayrıca etkinleştirmeniz gerekmez.

Uygulamayı etkinleştirme

Uygulama Yönetim Konsolu (MMC) ile nasıl uzaktan kaldırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Anahtar ekle**'yi seçin.

2. Adım. Bir anahtar eklemek

Bir etkinleştirme kodu veya bir anahtar dosyası ekleyin.

Kaspersky Security Center veri havuzuna anahtarlar ekleme hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Yardımı içeriğine bakın.

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görevi başlatmak için bir zamanlama ayarlayın, örneğin manuel olarak ya da bilgisayar boş olduğunda.

5. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Kaspersky Endpoint Security for Windows'u etkinleştir*.

6. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz. Bunun sonucunda Kaspersky Endpoint Security, kullanıcıların bilgisayarlarında sessiz modda etkinleştirilir.

Uygulama Web Console'da ve Cloud Console'da nasıl etkinleştirilir

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
2. **Görev türü** açılır listesinde, **Anahtar ekle**'yi seçin.
3. **Görev adı** alanına *Kaspersky Endpoint Security for Windows'un etkinleştirilmesi* gibi kısa bir açıklama girin.
4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin. Bir sonraki adıma geçin.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Bir lisans seçme

Uygulamayı etkinleştirmek için kullanmak istediğiniz lisansı seçin. Bir sonraki adıma geçin.

Anahtarları Web Console'a ekleyebilirsiniz (**İşlemler** → **Lisanslama**).

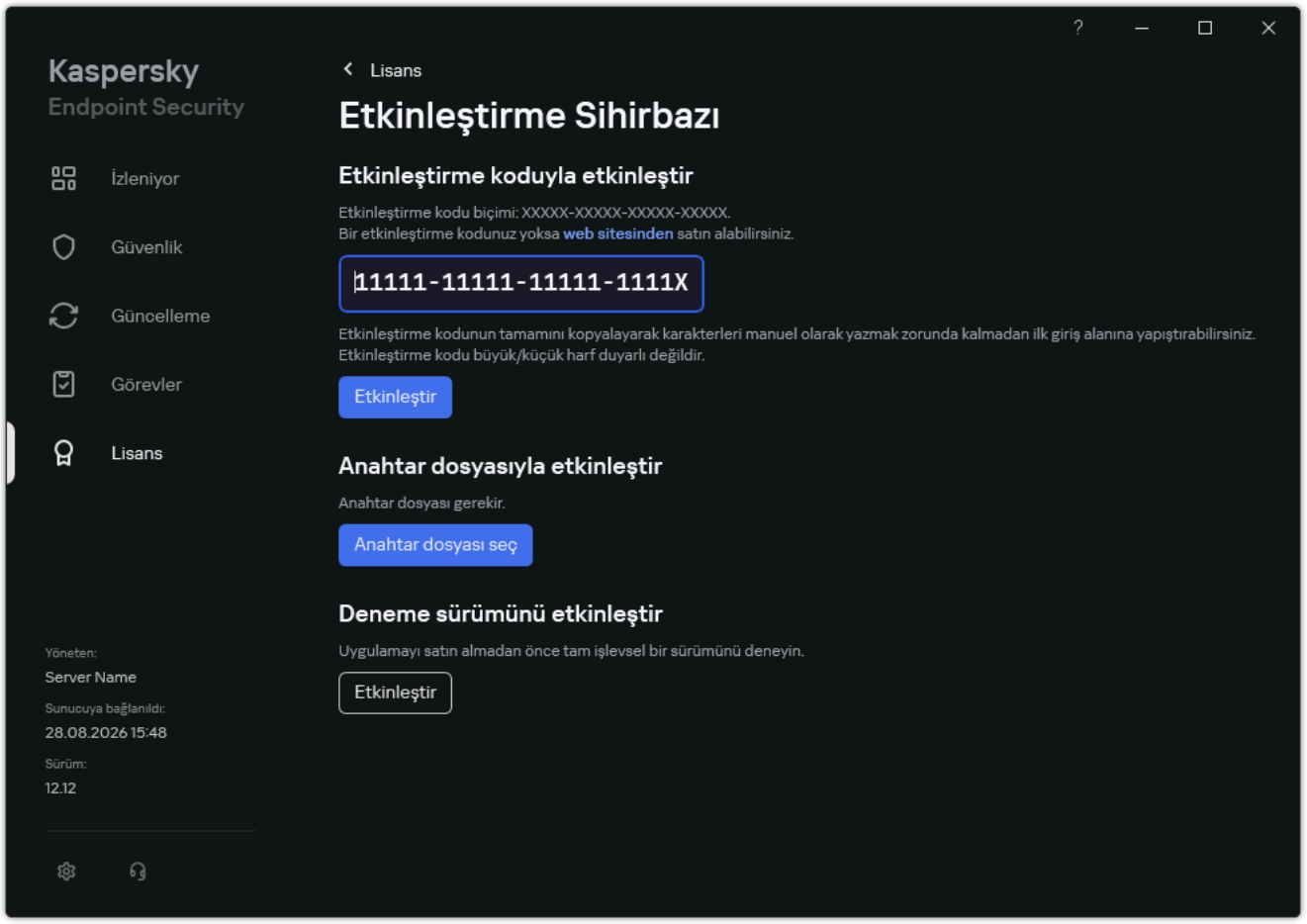
4. Adım. Görev oluşturmayı tamamlama

Son düğmesine tıklayarak sihirbazı sonlandırın. Görevler listesinde yeni bir görev görüntülenir. Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçin ve **Başlat** düğmesine tıklayın. Bunun sonucunda Kaspersky Endpoint Security, kullanıcıların bilgisayarlarında sessiz modda etkinleştirilir.

Uygulama arabiriminde uygulama etkinleştirme

1. Ana uygulama penceresinde **Lisans** bölümüne gidin.
2. **Uygulamayı yeni bir lisans kullanarak etkinleştirin**'e tıklayın.

Uygulama Etkinleştirme Sihirbazı başlatılır. Etkinleştirme Sihirbazı talimatlarını uygulayın.



Uygulamayı etkinleştirme

Anahtar ekle görevinin özelliklerinde bilgisayara bir rezerve anahtar ekleyebilirsiniz. Etkin anahtarın süresi dolduğunda *rezerve anahtar* etkinleşir. Bilgisayarda rezerve anahtar bulunması sayesinde, bir lisansın süresi dolduğunda bile uygulamayı eksiksiz bir şekilde kullanmaya devam edebilirsiniz.

Yönetim Konsolu (MMC) aracılığıyla bilgisayarlara nasıl otomatik olarak bir lisans anahtarı eklenir

1. Yönetim Konsolu'ndan **Kaspersky Lisansları** klasörüne gidin.

   Bir lisans anahtarları listesi açılır.

2. Lisans anahtarı özelliklerini açın.

3. **Genel** bölümünden **Lisans anahtarını yönetilen cihazlara otomatik olarak dağıt** onay kutusunu işaretleyin.

4. Değişikliklerinizi kaydedin.

Bu sayede anahtar uygun bilgisayarlara otomatik olarak dağıtılır. Anahtarın aktif veya rezerve anahtar olarak otomatik dağıtımı sırasında bilgisayarların sayısındaki lisanslama sınırı (anahtar özelliklerinde ayarlanır) dikkate alınır. Lisanslama sınırına ulaşılırsa anahtarların bilgisayarlara dağıtımı otomatik olarak durur. Anahtarın eklendiği bilgisayar sayısını ve anahtar özelliklerindeki diğer verileri **Cihazlar** bölümünden görüntüleyebilirsiniz.

Web Console ve Cloud Console aracılığıyla bilgisayarlara nasıl otomatik olarak bir lisans anahtarı eklenir

1. Web Console ana penceresinden **İşlemler** → **Lisanslama** → **Lisanslar** seçimini yapın.

   Bir lisans anahtarları listesi açılır.

2. Lisans anahtarı özelliklerini açın.

3. **Genel** sekmesinde **Lisans anahtarını yönetilen cihazlara otomatik olarak dağıt** geçiş anahtarını etkinleştirin.

4. Değişikliklerinizi kaydedin.

   Bu sayede anahtar uygun bilgisayarlara otomatik olarak dağıtılır. Anahtarın aktif veya rezerve anahtar olarak otomatik dağıtımı sırasında bilgisayarların sayısındaki lisanslama sınırı (anahtar özelliklerinde ayarlanır) dikkate alınır. Lisanslama sınırına ulaşılırsa anahtarların bilgisayarlara dağıtımı otomatik olarak durur. Anahtarın eklendiği bilgisayar sayısını ve anahtar özelliklerindeki diğer verileri **Cihazlar** sekmesinde görüntüleyebilirsiniz.

Uygulamayı bir *etkinleştirme kodu* ile etkinleştiriyorsanız, Kaspersky etkinleştirme sunucularına bağlanmak için internet erişimine ihtiyacınız vardır. Uygulamayı bir *anahtar dosyası* ile etkinleştiriyorsanız, internet erişimi gerekli değildir. Bilgisayarlar internet erişimi olmayan yalıtılmış bir ağ segmentindeyse, uygulamayı bir kodla etkinleştirmek için Kaspersky Security Center Yönetim Sunucusu'nun proxy sunucusu olarak kullanılmasına izin vermelisiniz. Yani uygulama, internet erişimi olan Yönetim Sunucusu üzerinden etkinleştirme sunucularına erişim sağlayabilir.

Yönetim Konsolu'nda (MMC) uygulamayı etkinleştirmek için Yönetim Sunucusunun proxy sunucusu olarak kullanılmasına izin verme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.

4. **Etkinleştirme için proxy sunucusu olarak Kaspersky Security Center'ı kullan** onay kutusunu seçin.

5. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da uygulamayı etkinleştirmek için Yönetim Sunucusunun proxy sunucusu olarak kullanılmasına izin verme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.

5. **Etkinleştirme için proxy sunucusu olarak Kaspersky Security Center'ı kullan** onay kutusunu seçin.

6. Değişikliklerinizi kaydedin.

Uygulamayı bir *etkinleştirme kodu* ile etkinleştiremiyorsanız, Kaspersky çözümünü kullanarak bir *anahtar dosyası* almayı ve uygulamayı farklı bir yöntem kullanarak tekrar etkinleştirmeyi deneyebilirsiniz.

Lisans kullanımı izleme

Lisansların kullanımını aşağıdaki adımları uygulayarak izleyebilirsiniz:

- Kuruluşun altyapısına ilişkin *Lisans anahtarı kullanım raporu*'nu görüntüleyin (**İzleme** → **Raporlar**).
- **Yönetilen cihazlar** → **Cihazlar** sekmesinde bilgisayarların durumlarını görüntüleme. Uygulama etkinleştirilmemişse bilgisayar ⚠ *Uygulama etkinleştirilmemiş* durumuna sahip olur.
- Bilgisayar özelliklerinde lisans bilgisini görüntüleyin.
- Anahtar özelliklerini görüntüleyin (**İşlemler** → **Lisanslama**).

Kaspersky Security Center Cloud Console'un bir parçası olarak uygulamayı etkinleştirme özellikleri

Kaspersky Security Center Cloud Console için bir deneme sürümü sağlanmıştır. *Deneme sürümü*, Kaspersky Security Center Cloud Console'un bir kullanıcıyı uygulamanın özelliklerini tanıtmak amacıyla tasarlanmış özel bir sürümüdür. Bu sürümde, 30 gün boyunca bir çalışma alanında işlemler gerçekleştirebilirsiniz. Kaspersky Endpoint Security dahil olmak üzere yönetilen tüm uygulamalar, Kaspersky Security Center Cloud Console için bir deneme lisansı altında otomatik olarak çalıştırılır. Ancak, Kaspersky Security Center Cloud Console deneme sürümünün süresi dolduğunda, Kaspersky Endpoint Security ürününü kendi deneme lisansını kullanarak etkinleştiremezsiniz. Kaspersky Security Center Cloud Console lisanslaması hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Cloud Console Yardımı'na başvurun.

Kaspersky Security Center Cloud Console'un deneme sürümü, daha sonra ticari bir sürüme geçmenize izin vermez. 30 günlük süre sona erdikten sonra tüm deneme çalışma alanları tüm içerikleriyle otomatik olarak silinir.

Bir lisans anahtarını kaldırma

Bir lisans anahtarını kaldırmak için bilgisayarlarınızda özel bir görev çalıştırmanız gerekir. Örneğin, lisanslama birimlerini yeniden düzenlemek için bir lisans anahtarını kaldırabilirsiniz. Ayrıca, lisansın süresi dolduğunda Kaspersky Endpoint Security sizi bilgilendirir. Uygulamayı denemek için kısa süreli bir lisans anahtarı eklediyseniz (örneğin, EDR Optimum Eklentisi), bildirimlerden kurtulmak ve bilgisayarınızın durumunu düzeltmek için bu lisans anahtarını kaldırabilirsiniz.

Anahtarı kaldır görevi bilgisayardan herhangi bir lisans anahtarının kaldırılmasını sağlar. Etkin lisans anahtarlarının yanı sıra rezerve lisans anahtarlarını da kaldırabilirsiniz. Kaspersky Endpoint Security etkinleştirme lisans anahtarına ek olarak, Kaspersky Detection and Response çözümlerinin (örneğin, EDR Optimum Eklentisi) lisans anahtarlarını tek tek kaldırabilirsiniz.

Yönetim Konsolu'nda (MMC) bir lisans anahtarını kaldırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Anahtarı kaldır**'yi seçin.

2. Adım. Bir lisans seçme

Silmek istediğiniz lisans anahtarını seçin. Kaspersky Security Center anahtar deposundan bir lisans anahtarı seçebilir veya bir anahtar dosyası seçebilirsiniz.

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görevi başlatmak için bir zamanlama ayarlayın, örneğin manuel olarak ya da bilgisayar boş olduğunda.

5. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin, *Beta için anahtarı kaldır*.

6. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console'da bir lisans anahtarını kaldırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
2. **Görev türü** açılır listesinde, **Anahtarı kaldır**'yi seçin.
3. **Görev adı** alanına kısa bir açıklama girin, örneğin, *Beta için anahtarı kaldır*.
4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin. Bir sonraki adıma geçin.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Bir lisans seçme

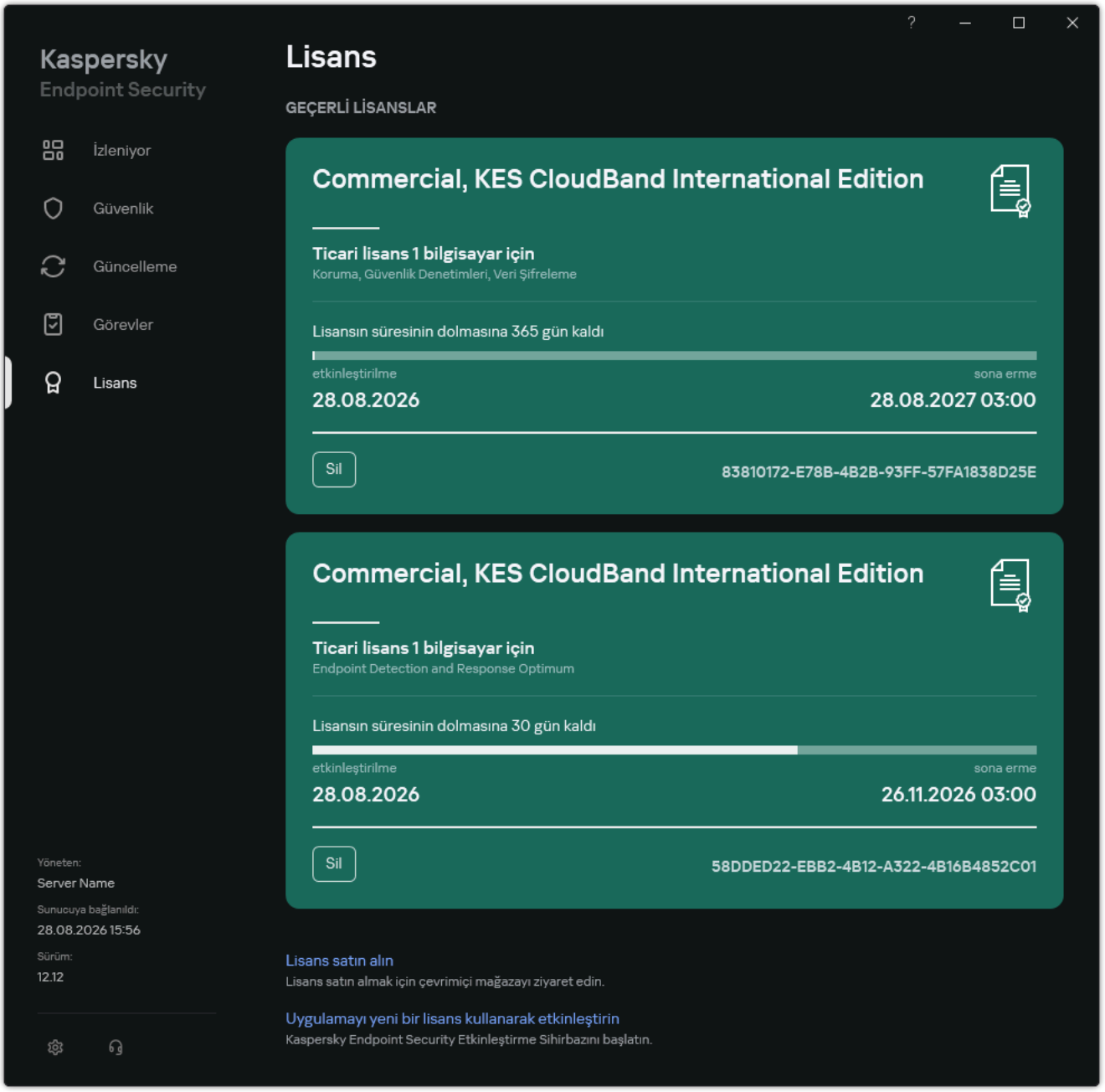
Silmek istediğiniz lisans anahtarını seçin. Kaspersky Security Center anahtar deposundan bir lisans anahtarı seçebilir veya bir anahtar dosyası seçebilirsiniz. Bir sonraki adıma geçin.

4. Adım. Görev oluşturmayı tamamlama

Son düğmesine tıklayarak sihirbazı sonlandırın. Görevler listesinde yeni bir görev görüntülenir. Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçin ve **Başlat** düğmesine tıklayın.

Uygulama arabiriminde bir lisans anahtarını kaldırma

1. Ana uygulama penceresinde **Lisans** bölümüne gidin.
2. Silmek istediğiniz anahtarı seçin ve **Sil** öğesine tıklayın.



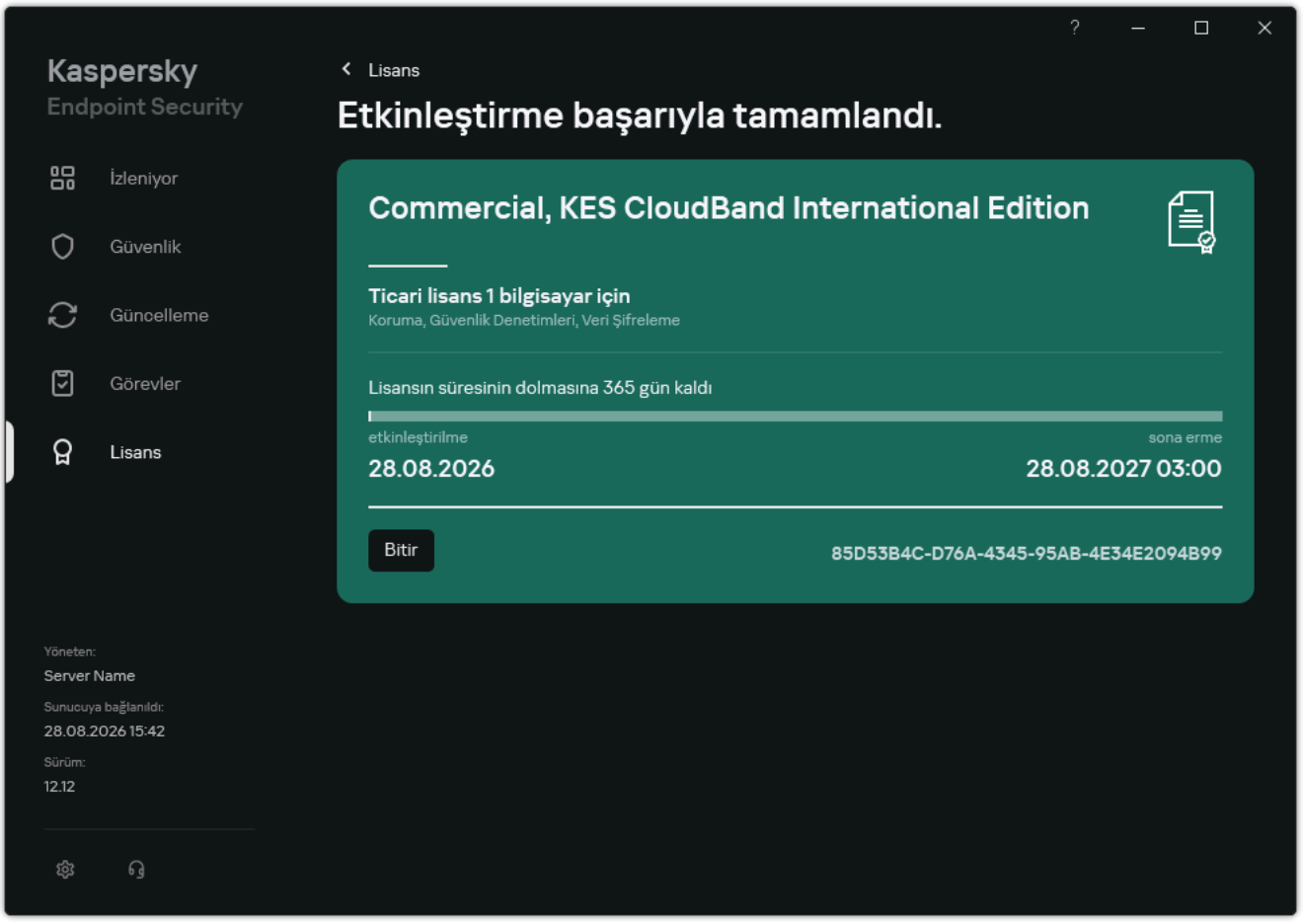
Lisanslama penceresi

Bir lisans anahtarını komut satırından da kaldırabilirsiniz.

Lisans bilgilerini görüntüleme

Bir lisans hakkındaki bilgileri görüntülemek için:

Ana uygulama penceresinden **Lisans** bölümüne gidin (aşağıdaki şekle bakın).



Lisanslama penceresi

Bu bölümde aşağıdaki ayrıntılar görüntülenir:

- *Anahtar durumu*. Bir bilgisayarda birden çok anahtar bulunabilir. İki anahtar türü mevcuttur: aktif ve yedek. Uygulamanın birden fazla etkin anahtarı olamaz. Rezerve anahtar sadece etkin anahtarın süresi dolduktan sonra veya etkin anahtar **Sil** düğmesine tıklanarak silindikten sonra etkinleştirilebilir.
- *Uygulama adı*. Satın alınan Kaspersky uygulamasının tam adı.
- *Lisans türü*. Şu lisans türleri kullanılabilir: deneme ve ticari.
- *İşlevsellik*. Lisansınız kapsamında kullanabileceğiniz uygulama özellikleri. Özellikler arasında Koruma, Güvenlik Denetimleri, Veri Şifreleme ve diğerleri vardır. Kullanılabilir özelliklerin listesi Lisans Sertifikasında da sunulmuştur.

- *Lisans hakkındaki ek bilgiler*. Lisans süresinin başlangıç ve bitiş tarihi (sadece etkin anahtar için), kalan lisans süresi.

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

- *Anahtar*. Anahtar, bir etkinleştirme kodundan veya bir anahtar dosyasından oluşturulan benzersiz bir alfa sayısal dizidir.

Lisanslama penceresinde aşağıdakilerden birini de yapabilirsiniz:

- **Lisans satın alın** / **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 kullanarak etkinleştirin**. Uygulama Etkinleştirme Sihirbazını başlatır. Bu sihirbazda bir etkinleştirme kodu veya anahtar dosyası kullanarak bir anahtar ekleyebilirsiniz. Uygulama Etkinleştirme Sihirbazı, bir etkin anahtar ve yalnızca bir adet rezerve 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 **Lisans** bölümüne gidin.

2. Aşağıdakilerden birini yapın:

   - Herhangi bir anahtar eklenmediyse veya deneme lisansı anahtarı eklendiyse **Lisans satın alın** düğmesine tıklayın.

   - Ticari lisans anahtarı eklenirse, **Lisansı yenile** düğmesine tıklayın.

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

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.

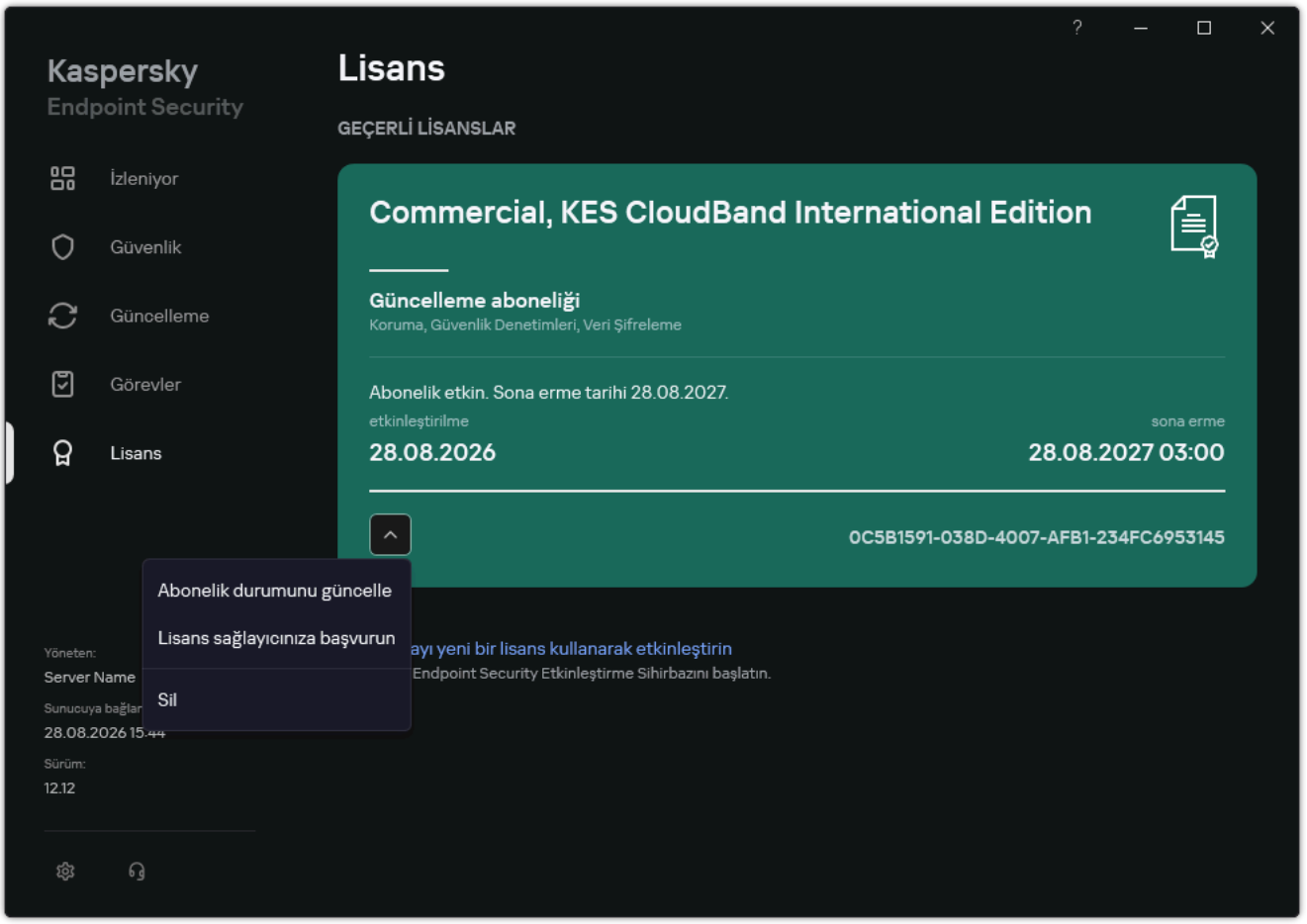
Uygulamayı sınırlı bir abonelikle kullanıyorsanız aboneliğin sona erme tarihinde (veya abonelik yenileme ödemesiz süresinin sona erme tarihinde) Kaspersky Endpoint Security sizi bu konuda bilgilendirir ve aboneliği otomatik olarak yenilemeye çalışmayı bırakır. Bu durumda Kaspersky Endpoint Security, uygulamanın ticari lisansının sona erdiği durumdaki gibi davranır: uygulama güncellemeler olmadan çalışır ve Kaspersky Security Network kullanılamaz.

Hizmet sağlayıcının İnternet sitesinde aboneliği yenileyebilirsiniz.

Uygulama arabiriminden hizmet sağlayıcının İnternet sitesini ziyaret etmek için:

1. Ana uygulama penceresinde **Lisans** bölümüne gidin.
2. **Lisans sağlayıcınıza başvurun**'a tıklayın.

Abonelik durumunu manuel olarak güncelleyebilirsiniz. Abonelik, ödemesiz süreden sonra yenilendiyse ve uygulama abonelik durumunu otomatik olarak güncellemediyse bu işlem gerekli olabilir.



Aboneliği yenileme

Başlarken

Kaspersky Endpoint Security'yi yükledikten sonra, şu arabirimleri kullanarak uygulamayı yönetebilirsiniz:

- Yerel uygulama arabirimi.
- Kaspersky Security Center Yönetim Konsolu.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Yönetim Konsolu

Kaspersky Security Center, Kaspersky Endpoint Security'yi uzaktan yüklemenizi ve kaldırmanızı, başlatmanızı ve durdurmanızı, uygulama ayarlarını yapılandırmanızı, kullanılabilir uygulama bileşenlerini değiştirmenizi, anahtar eklemenizi ve güncelleme ile tarama görevlerini başlatmanızı ve durdurmanızı sağlar.

Uygulama, Kaspersky Endpoint Security Yönetim Eklentisi kullanılarak Kaspersky Security Center aracılığıyla yönetilebilir.

Uygulamayı Kaspersky Security Center aracılığıyla yönetme hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun.

Kaspersky Security Center Web Console ve Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (bundan sonra *Web Console* olarak da anılacaktır). Bu, Kaspersky uygulamalarını temel alan bir koruma sistemini yönetmeye yönelik web arabirimidir. Kaspersky Security Center Web Console ile herhangi bir cihazdaki tarayıcıyı kullanarak çalışabilirsiniz. Kaspersky Security Center Web Console hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Yardımı'na başvurun.

Kaspersky Security Center Cloud Console (bundan sonra "*Cloud Console*" olarak anılacaktır), bir kuruluşun ağını korumak ve yönetmek için bulut tabanlı bir çözümdür. Kaspersky Security Center Cloud Console hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Cloud Console Yardımı'na başvurun.

Web Console ve Cloud Console ile şunları yapabilirsiniz:

- Kuruluşunuzun güvenlik sisteminin durumunu izleme.
- Ağınızda yer alan aygıtlara Kaspersky uygulamalarını yükleme.
- Yüklü uygulamaları yönetme.
- Güvenlik sistemi durumuna ilişkin raporları görüntüleme.

Kaspersky Endpoint Security'nin ve Kaspersky Security Center Yönetim Konsolu ile Web Console ve Cloud Console üzerinden yönetimi farklı yönetim imkanları sunar. Kullanılabilecek bileşenler ve görevler de bu Konsollar için farklıdır.

Kaspersky Endpoint Security for Windows Yönetim Eklentisi Hakkında

Kaspersky Endpoint Security for Windows Yönetim Eklentisi, Kaspersky Endpoint Security ile Kaspersky Security Center arasındaki etkileşimi sağlar. Yönetim Eklentisi, ilkeleri, görevleri ve yerel uygulama ayarlarını kullanmak suretiyle kullanarak Kaspersky Endpoint Security'yi yönetmenize olanak tanır. Kaspersky Security Center Web Console ile etkileşim, web eklentisi aracılığıyla sağlanır.

Yönetim Eklentisinin sürümü, istemci bilgisayarda yüklü olan Kaspersky Endpoint Security uygulamasının sürümünden farklı olabilir. Yönetim Eklentisinin yüklü olan sürümü, Kaspersky Endpoint Security'nin yüklü olan sürümünden daha az işleve sahipse eksik işlevlerin ayarları Yönetim Eklentisi tarafından düzenlenmez. Bu ayarlar kullanıcı tarafından Kaspersky Endpoint Security'nin yerel arabiriminden değiştirilebilir.

Web eklentisi, Kaspersky Security Center Web Console'da varsayılan olarak yüklü değildir. Web eklentisi, Kaspersky Security Center Web Console'un kurulu olduğu bir bilgisayara yüklenmelidir. Web eklentisinin işlevselliği, bir tarayıcıda Web Console'a erişimi olan tüm yöneticiler tarafından kullanılabilir. Yüklü web eklentilerini Web Console arabiriminde görüntüleyebilirsiniz: (**Konsol ayarları** → **Web eklentileri**).

Kaspersky Endpoint Security'yi Kaspersky Endpoint Detection and Response Optimum çözümünün bir parçası olarak kullanıyorsanız Kaspersky Endpoint Detection and Response yönetim eklentisini yüklemeniz gerekir. Uyarı ayrıntılarını görüntülemek için yönetim eklentisine ihtiyacınız vardır. *Uyarı Ayrıntıları*, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Bu nedenle, tehdit yanıt görevleri oluşturmak için Kaspersky Endpoint Security yönetim eklentisine ve uyarı ayrıntılarını görüntülemek için EDR yönetim eklentisine ihtiyacınız vardır.

Web eklentisini yükleme

Web eklentisini aşağıdaki gibi yükleyebilirsiniz:

- Kaspersky Security Center Web Console'un Hızlı Başlangıç Sihirbazını kullanarak web eklentisini yükleyin.

  Web Console Yönetim Sunucusuna ilk kez bağladığınızda Web Console otomatik olarak Hızlı Başlangıç Sihirbazını çalıştırmanızı ister. Web Console arabirimindeki Hızlı Başlangıç Sihirbazını da çalıştırabilirsiniz: **Keşif ve Dağıtım** → **Dağıtım ve Atama** → **Hızlı Başlangıç Sihirbazı**). Hızlı Başlangıç Sihirbazı ayrıca yüklü web eklentilerinin güncel olup olmadığını denetler ve gerekli güncellemeleri indirir. Kaspersky Security Center Web Console'daki Hızlı Başlangıç Sihirbazı hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım içeriğine bakın.

- Web Console'daki kullanılabilir dağıtım paketlerinin listesinden web eklentisini yükleyin.

  Web eklentisini yüklemek için Web Console arabiriminde Kaspersky Endpoint Security web eklentisinin dağıtım paketini seçin (**Konsol ayarları** → **Web eklentileri**). Kaspersky uygulamalarının yeni sürümleri piyasaya sürüldükçe kullanılabilir dağıtım paketlerinin listesi otomatik olarak güncellenir.

- Dağıtım paketini, Web Console'a dış bir kaynaktan indirin.

  Web eklentisini yüklemek için Web Console arabiriminde Kaspersky Endpoint Security web eklentisinin dağıtım paketinin ZIP arşiv dosyasını ekleyin (**Konsol ayarları → Web eklentileri**). Örneğin, web eklentisinin dağıtım paketi Kaspersky internet sitesinden indirilebilir.

Windows için Kaspersky Endpoint Security 12.11 ile başlayarak, web eklentisinin kurulum prosedürü değişti. Dağıtım paketi artık iki web eklentisi içeriyor: *Kaspersky Endpoint Security for Windows 14.2.0* ve *Unified Protection and Management Plug-in*. Bunun nedeni, Kaspersky uygulamalarını yönetmek için tek bir birleşik web eklentisine geçilmesidir. Birleşik web eklentisi, birden fazla Kaspersky uygulamasını (örneğin, Windows, macOS ve Linux için Kaspersky Endpoint Security) yönetmek için tek bir ilke oluşturulmasına olanak tanır. Birleşik web eklentisine geçiş birkaç sürüm alabilir. Geçiş tamamlandıktan sonra dağıtım paketi yalnızca *Birleşik Koruma ve Yönetim Eklentisini* içerecektir.

Yönetim Eklentisini güncelleme

Kaspersky Endpoint Security for Windows Yönetim Eklentisini güncellemek için eklentinin en son sürümünü (dağıtım paketinde yer alır) indirin ve eklenti kurulum sihirbazını çalıştırın.

Web eklentisinin yeni bir sürümü kullanıma sunulursa Web Console'da *Kullanılan eklentiler için güncellemeler mevcut* bildirimi görüntülenir. Bu Web Console bildiriminden web eklentisini güncelleme işlemine geçebilirsiniz. Yeni web eklentisi güncellemelerini Web Console arabiriminden manuel olarak da denetleyebilirsiniz (**Konsol ayarları → Web eklentileri**). Web eklentisinin önceki sürümü güncelleme sırasında otomatik olarak kaldırılır.

Web eklentisi güncellendiğinde, önceden var olan öğeler (örneğin ilkeler veya görevler) kaydedilir. Kaspersky Endpoint Security'nin yeni işlevlerini uygulayan öğelerin yeni ayarları mevcut öğelerde görüntülenir ve varsayılan değerlere sahip olur.

Web eklentisini aşağıdaki şekilde güncelleyebilirsiniz:

- Çevrimiçi modda web eklentilerinin listesinden web eklentisini güncelleyin.

  Web eklentisini güncellemek için Web Console arabiriminde Kaspersky Endpoint Security web eklentisinin dağıtım paketini seçin (**Konsol ayarları → Web eklentileri**). Web Console, Kaspersky sunucularında mevcut güncellemeleri denetler ve ilgili güncellemeleri indirir.

- Web eklentisini bir dosyadan güncelleyin.

  Web eklentisini güncellemek için Web Console arabiriminde Kaspersky Endpoint Security web eklentisinin dağıtım paketinin ZIP arşiv dosyasını seçmeniz gerekir (**Konsol ayarları → Web eklentileri**). Örneğin, web eklentisinin dağıtım paketi Kaspersky internet sitesinden indirilebilir. Kaspersky Endpoint Security web eklentisini yalnızca daha yeni bir sürüme güncelleyebilirsiniz. Web eklentisi daha eski bir sürüme güncellenemez.

İlke veya görev gibi herhangi bir öğe açılırsa web eklentisi uyumluluk bilgilerini denetler. Web eklentisinin sürümü uyumluluk bilgilerinde belirtilen sürüme denk veya bundan daha yüksek bir sürümse bu bileşenin ayarlarını değiştirebilirsiniz. Değilse seçilen öğenin ayarlarını web eklentisini kullanarak değiştiremezsiniz. Web eklentisini güncellemeniz önerilir.

Yönetim eklentilerinin farklı sürümleriyle çalışırken dikkat edilmesi gereken hususlar

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. Yönetim Eklentisinin gereken en düşük sürümünü dağıtım kitinde bulunan installer.ini dosyasında görüntüleyebilirsiniz.

İlke veya görev gibi herhangi bir öğe açılırsa Yönetim Eklentisi uyumluluk bilgilerini denetler. Yönetim Eklentisinin sürümü, uyumluluk bilgisinde belirtilen sürüme denk ya da daha yüksekse bu öğenin ayarlarını değiştirebilirsiniz. Değilse seçilen öğenin ayarlarını Yönetim Eklentisini kullanarak değiştiremezsiniz. Yönetim Eklentisini yükseltmeniz önerilir.

Yönetim Konsolunda Kaspersky Endpoint Security Yönetim Eklentisi yüklüyse Yönetim Eklentisinin yeni bir sürümünü yüklerken lütfen şunları dikkate alın:

- Kaspersky Endpoint Security Yönetim Eklentisinin önceki sürümü kaldırılır.
- Kaspersky Endpoint Security Yönetim Eklentisinin yeni sürümü, kullanıcı bilgisayarlarında Kaspersky Endpoint Security for Windows'un önceki sürümünün yönetilmesini destekler.
- Yönetim Eklentisinin önceki sürümü tarafından oluşturulan ilkeler, görevler ve diğer öğelerin ayarlarını değiştirmek için Yönetim Eklentisinin yeni sürümünü kullanabilirsiniz.
- Yeni ayarlar için Yönetim Eklentisinin yeni sürümü bir ilke, ilke profili veya görev ilk kez kaydedildiğinde varsayılan değerleri atar.

  Yönetim Eklentisi yükseltildikten sonra İlkelerin ve ilke profillerinin yeni ayarlarının değerlerini denetlemeniz ve kaydetmeniz önerilir. Bunu yapmazsanız kullanıcının bilgisayarındaki yeni Kaspersky Endpoint Security ayarları varsayılan değerleri alır ve düzenlenebilir (özniteliği). Ayarları, hiyerarşinin en üst düzeyindeki İlkeler ve ilke profillerinden başlayarak denetlemeniz önerilir. Ayrıca, Kaspersky Security Center'ın tüm işlevsel alanlarına erişim hakları olan kullanıcı hesabını kullanmanız da önerilir.

  Uygulamanın yeni özellikleri hakkında bilgi edinmek için lütfen Sürüm Notlarına veya uygulama yardımına başvurun.

- Yönetim Eklentisinin yeni sürümündeki bir ayarlar grubuna yeni bir parametre eklendiyse bu ayarlar grubunun / özniteliğinin önceden tanımlanan durumu değişmez.

Harici hizmetlerle etkileşim için şifrelenmiş iletişim kurallarını kullanırken özel hususlar

Kaspersky Endpoint Security ve Kaspersky Security Center, Kaspersky'nin dış hizmetleriyle çalışmak için TLS (Transport Layer Security) ile şifreli bir iletişim kanalı kullanır. Kaspersky Endpoint Security, aşağıdaki işlevler için harici hizmetler kullanır:

- Veritabanlarını ve uygulama yazılım modüllerini güncelleme;
- Uygulamanın bir aktivasyon kodu ile etkinleştirilmesi (aktivasyon 2.0);
- Kaspersky Security Network'ü kullanma.

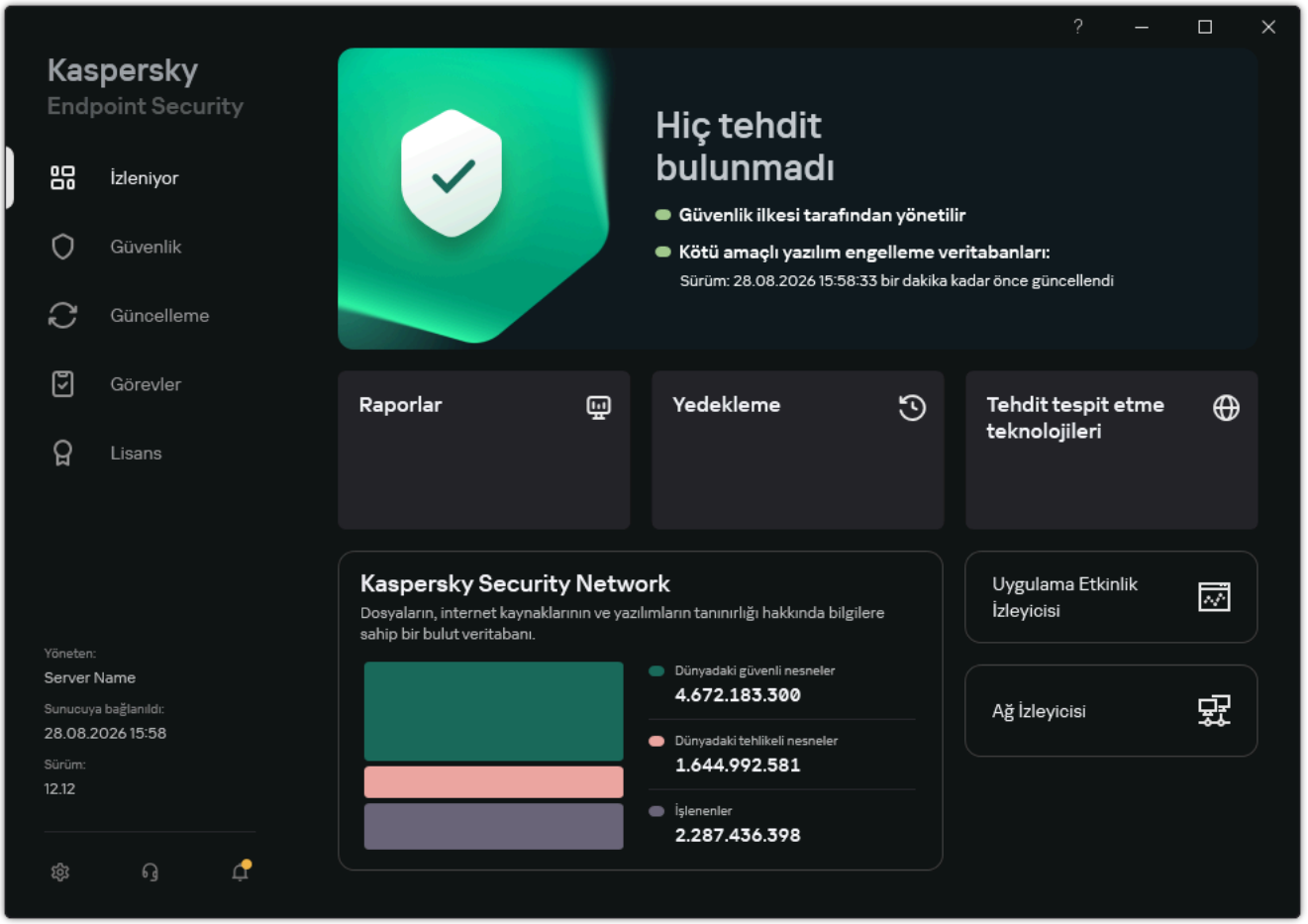
TLS kullanımı, aşağıdaki özelliklerin sunulmasıyla uygulamayı güvence altına alır:

- Şifreleme. Mesajların içeriği gizlidir ve üçüncü şahıslara açıklanmaz.
- Bütünlük. Mesaj alıcısı, mesajın gönderen tarafından iletilmesinden itibaren mesaj içeriğinin değiştirilmediğinden emindir.
- Kimlik Doğrulama. Alıcı, iletişimin yalnızca güvenilir bir Kaspersky sunucusuyla kurulduğundan emindir.

Kaspersky Endpoint Security, sunucu kimlik doğrulaması için ortak anahtar sertifikaları kullanır. Sertifikalarla çalışmak için Public Key Infrastructure (PKI) gereklidir. Sertifika Yetkilisi, PKI'nın bir parçasıdır. Kaspersky kendi Sertifika Yetkilisini kullanır çünkü Kaspersky hizmetleri son derece tekniktir ve herkese açık değildir. Bu durumda, Thawte, VeriSign, GlobalTrust ve diğerlerinin kök sertifikaları iptal edildiğinde, Kaspersky PKI kesinti olmadan çalışır durumda kalır.

MITM'ye (HTTPS iletişim kuralının ayrıştırılmasını destekleyen yazılım ve donanım araçları) sahip ortamlar, Kaspersky Endpoint Security tarafından güvensiz kabul edilir. Kaspersky hizmetleriyle çalışırken hatalarla karşılaşılabilir. Örneğin, Self-Signed Certificate kullanımı ile ilgili hatalar olabilir. Bu hatalar, ortamınızdaki bir HTTPS İnceleme aracının Kaspersky PKI'yı tanımaması nedeniyle oluşabilir. Bu sorunları gidermek için, dış hizmetlerle etkileşim için istisnaları yapılandırmanız gerekir.

Uygulama arabirimi



Ana uygulama penceresi

İzleniyor	• **Raporlar**. Uygulamanın çalışması sırasında meydana gelen olayları, bağımsız bileşenleri ve görevleri görüntüleyin. • **Yedekleme**. Uygulamanın sildiği virüslü dosyaların kaydedilmiş kopyalarının bir listesini görüntüleyin. • **Tehdit tespit etme teknolojileri**. Tehdit algılama teknolojileri ve bu teknolojiler tarafından tespit edilen tehditlerin sayısı hakkındaki bilgileri görüntüleyin. • **Kaspersky Security Network**. Kaspersky Endpoint Security ile Kaspersky Security Network arasındaki bağlantının durumu ve global KSN istatistikleri. *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. Kaspersky Security Network'e katılıyorsanız, KSN hizmetleri Kaspersky Endpoint Security'ye taranan web adreslerinin itibarı hakkında bilgi ve taranan dosyaların kategorisi ve tanınırlığı hakkında bilgi sağlar. • **Uygulama Etkinlik İzleyicisi**. Yüklü uygulamaların çalışmasıyla ilgili bilgileri görüntüleyin. Uygulama Etkinlik İzleyicisi bir uygulama ile ilişkili dosya, kayıt defteri ve işletim sistemi olaylarını izler. • **Ağ İzleyicisi**. Bilgisayarın ağ etkinliği hakkındaki bilgileri gerçek zamanlı olarak görüntüleyin. • **Şifreleme İzleyicisi**. Disk şifreleme veya şifre çözme sürecini gerçek zamanlı olarak izler. Şifreleme İzleyicisi, Kaspersky Disk Encryption bileşeni veya BitLocker Drive Encryption bileşeni yüklüyse kullanılabilir.
Güvenlik	Kurulu bileşenlerin çalışma durumu. Ayrıca bileşenleri yapılandırmaya veya raporları görüntülemeye devam edebilirsiniz.
Güncelle	Kaspersky Endpoint Security güncelleme görevlerini yönetme. Antivirüs veritabanlarını ve uygulama modüllerini güncelleyebilir ve son güncellemeyi geri alabilirsiniz. Bir yönetici şunları yapabilir: bölümü kullanıcıdan gizleme veya görev yönetimini kısıtlama.
Görevler	Kaspersky Endpoint Security tarama görevlerini yönetme. Bir kötü amaçlı yazılım taraması ve uygulama bütünlüğü kontrolü çalıştırabilirsiniz. Bir yönetici, bir kullanıcıdan gelen görevleri gizleyebilir veya görevlerin yönetimini kısıtlayabilir.
Lisans	Uygulama lisanslama. Bir lisans satın alabilir, uygulamayı etkinleştirebilir veya bir aboneliği yenileyebilirsiniz. Mevcut lisansla ilgili bilgileri de görüntüleyebilirsiniz.
⚙	Uygulama ayarlarını yapılandır. Bir yönetici, Kaspersky Security Center'daki ayarlarda değişiklik yapılmasını yasaklayabilir.

	Uygulama hakkında bilgiler: Kaspersky Endpoint Security'nin mevcut sürümü, veritabanı yayın tarihi, anahtar ve diğer bilgiler. Ayrıca yararlı bilgiler, öneriler ve uygulamanın satın alınması, yüklenmesi ve kullanımıyla ilgili sık sorulan sorulara verilen yanıtları sağlayan Kaspersky bilgi kaynaklarına ilerleyebilirsiniz.
	Mevcut güncellemeler ve şifrelenmiş dosyalara ile aygıtlara erişim talepleri hakkında bilgi içeren mesajlar.

Görev çubuğu bildirim alanındaki uygulama simgesi

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

Görev çubuğu bildirim alanındaki uygulama simgesi gizliyse, yönetici ilkede uygulama arabiriminin görüntülenmesini devre dışı bırakmıştır.

Simge aşağıdaki amaçları karşılar:

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

Uygulama çalışma bilgilerini görüntülemek için aşağıdaki uygulama simgesi durumları sunulur:

- simgesi, uygulamanın kritik öneme sahip koruma bileşenlerinin etkin olduğunu belirtir. Kullanıcının, örneğin uygulamayı güncelledikten sonra bilgisayarı yeniden başlatmak gibi bir eylem gerçekleştirmesi gerekirse, Kaspersky Endpoint Security bir uyarı görüntüler.
- simgesi, uygulamanın kritik öneme sahip koruma bileşenlerinin devre dışı bırakıldığını ya da çalışmaz hale geldiğini belirtir. Koruma bileşenleri, örneğin lisansın süresi dolduğunda ya da bir uygulama hatası nedeniyle çalışmaz hale gelebilir. Kaspersky Endpoint Security, bilgisayar korumasındaki sorunun açıklamasıyla birlikte bir uyarı görüntüler.

Uygulama simgesinin bağlam 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.
- **Korumayı duraklat** / **Korumayı sürdür**. İlkede bir kilit () ile işaretlenmemiş tüm koruma ve denetim bileşenlerini duraklatın. Bu işlem gerçekleştirmeden önce Kaspersky Security Center ilkesinin devre dışı bırakılması önerilir.

  Koruma ve denetim bileşenlerinin çalışması duraklatılmadan önce, uygulama Kaspersky Endpoint Security erişimi için parola ister (hesap parolası veya geçici parola). Süreyi duraklatmayı seçebilirsiniz: belirli bir süre için, bir yeniden başlatmaya kadar ya da kullanıcı isteği üzerine.

  Bu bağlam menüsü sadece Parolası koruması etkinleştirilmişse kullanılabilir. Koruma ve denetim bileşenlerinin çalışmasına devam etmesi için, uygulamanın bağlam menüsünden **Korumayı sürdür** seçeneğine tıklayın.

  Koruma ve denetim bileşenlerinin çalışmasının duraklatılması, güncelleme ve kötü amaçlı yazılım taraması görevlerinin gerçekleştirilmesini etkilemez. Uygulama, Kaspersky Security Network'ü kullanmaya da devam eder.

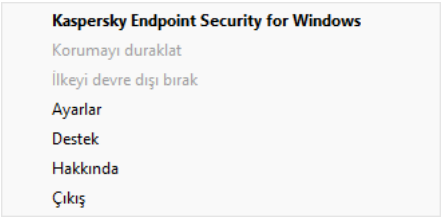
- **İlkeyi devre dışı bırak** / **İlkeyi etkinleştir**. Bilgisayardaki Kaspersky Security Center ilkesini devre dışı bırakma. İlkede kapalı bir kilit içeren ayarlar da dahil olmak üzere tüm Kaspersky Endpoint Security ayarları yapılandırılabilir ( ). İlke devre dışı bırakılmışsa, uygulama Kaspersky Endpoint Security'ye erişmek için parola talep eder (hesap parolası veya geçici parola). Bu bağlam menüsü sadece Parolası koruması etkinleştirilmişse kullanılabilir. İlkeyi etkinleştirmek için uygulamanın bağlam menüsündeki **İlkeyi etkinleştir** seçeneğini kullanın.

- **Ayarlar**. Uygulama ayarları penceresini açar.

- **Destek**. Bu, Kaspersky Teknik Destek ile iletişime geçmek için gerekli bilgileri içeren bir pencereyi açar.

- **Hakkında**. Bu öğe, uygulama ayrıntılarını içeren bilgi penceresini açar.

- **Çıkış**. Bu öğe, Kaspersky Endpoint Security'den çıkar. Bu bağlam menüsüne tıklandığında uygulama, bilgisayar RAM'inden karşıya yüklenir.



Uygulama simgesi bağlam menüsü

Basitleştirilmiş uygulama arabirimi

Basitleştirilmiş uygulama arabirimi ekranı için yapılandırılan Kaspersky Security Center ilkesi, Kaspersky Endpoint Security'nin yüklü olduğu bir istemci bilgisayara uygulanıyorsa bu istemci bilgisayarda ana uygulama penceresi kullanılamaz. Aşağıdakileri içeren Kaspersky Endpoint Security simgesinin (aşağıdaki resme bakın) bağlam menüsünü açmak için sağ tıklayın:

- **İlkeyi devre dışı bırak** / **İlkeyi etkinleştir**. Bilgisayardaki Kaspersky Security Center ilkesini devre dışı bırakma. İlkede kapalı bir kilit içeren ayarlar da dahil olmak üzere tüm Kaspersky Endpoint Security ayarları yapılandırılabilir ( ). İlke devre dışı bırakılmışsa, uygulama Kaspersky Endpoint Security'ye erişmek için parola talep eder (hesap parolası veya geçici parola). Bu bağlam menüsü sadece Parolası koruması etkinleştirilmişse kullanılabilir. İlkeyi etkinleştirmek için uygulamanın bağlam menüsündeki **İlkeyi etkinleştir** seçeneğini kullanın.

- **Görevler**. Açılır liste aşağıdaki öğeleri içerir:

  - **Uygulama Bütünlüğü Kontrolü**.

  - **Veritabanlarının önceki sürüme geri alınması**.

  - **Tam Tarama**.

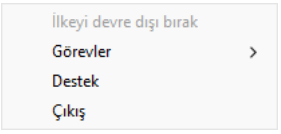
  - **Özel Tarama**.

  - **Kritik Alanları Tarama**.

  - **Güncelleme**.

- **Destek**. Bu, Kaspersky Teknik Destek ile iletişime geçmek için gerekli bilgileri içeren bir pencereyi açar.

- **Çıkış**. Bu öğe, Kaspersky Endpoint Security'den çıkar. Bu bağlam menüsüne tıklandığında uygulama, bilgisayar RAM'inden karşıya yüklenir.



Basitleştirilmiş arabirim görüntülenirken uygulama simgesinin bağlam menüsü

Uygulama arabirim ekranını yapılandırma

Bir kullanıcı için uygulama arabirimi ekranı modunu yapılandırabilirsiniz. Kullanıcı uygulama ile şu yollarla etkileşim kurabilir:

- **Basitleştirilmiş**. Bir istemci bilgisayarında, ana uygulama penceresine erişilemez, sadece Windows bildirim alanındaki simge kullanılabilir. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile kısıtlı sayıda işlem gerçekleştirebilir. Kaspersky Endpoint Security, uygulama simgesinin üzerinde yalnızca kullanıcı müdahalesi gerektiren bildirimleri gösterir.

- **Tam**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin ana penceresi ve Windows bildirim alanındaki simge vardır. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile işlemler gerçekleştirebilir. Kaspersky Endpoint Security ayrıca uygulama simgesinin üzerinde bildirimler görüntüler.

- **Kullanıcı arabirimini gösterme**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin çalıştığına dair hiçbir işaret görüntülenmez. Windows bildirim alanındaki simge ve bildirimler yoktur.

Yönetim Konsolu (MMC) üzerinden uygulama arabirim görüntüleme modu nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
4. **Kullanıcıyla etkileşim** bloğunda uygulama arabiriminin nasıl görüntüleneceğini seçin:
   - **Kullanıcı arabirimini göster**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin ana penceresi ve Windows bildirim alanındaki simge vardır. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile işlemler gerçekleştirebilir. Kaspersky Endpoint Security ayrıca uygulama simgesinin üzerinde bildirimler görüntüler. Gerekirse, **Uygulama Etkinlik İzleyicisi bölümünü gizle** bölümündeki işlevi etkinleştirerek bilgisayardaki uygulama etkinliği ile ilgili verileri gizleyebilir ve böylece kullanıcıların Uygulama Etkinlik İzleyicisi aracına erişimini kısıtlayabilirsiniz.
   - **Basitleştirilmiş arabirimi görüntüle**. Bir istemci bilgisayarında, ana uygulama penceresine erişilemez, sadece Windows bildirim alanındaki simge kullanılabilir. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile kısıtlı sayıda işlem gerçekleştirebilir. Kaspersky Endpoint Security, uygulama simgesinin üzerinde yalnızca kullanıcı müdahalesi gerektiren bildirimleri gösterir.
   - **Kullanıcı arabirimini gösterme**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin çalıştığına dair hiçbir işaret görüntülenmez. Windows bildirim alanındaki simge ve bildirimler yoktur.
5. Değişikliklerinizi kaydedin.

Web Console'da uygulama arabirimi görüntüleme modu nasıl yapılandırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kullanıcı Etkileşimi** bölümüne gidin.
5. **Kullanıcılar için görünürlük** bloğunda uygulama arabiriminin nasıl görüntüleneceğini seçin:

   - **Kullanıcı arabirimini göster**. Bu işlev devre dışı bırakılırsa, istemci bilgisayarda Kaspersky Endpoint Security'nin çalıştığına dair hiçbir işaret görünmez. Windows bildirim alanındaki simge ve bildirimler yoktur.
   - **Basitleştirilmiş**. Bir istemci bilgisayarında, ana uygulama penceresine erişilemez, sadece Windows bildirim alanındaki simge kullanılabilir. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile kısıtlı sayıda işlem gerçekleştirebilir. Kaspersky Endpoint Security, uygulama simgesinin üzerinde yalnızca kullanıcı müdahalesi gerektiren bildirimleri gösterir.
   - **Tam**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin ana penceresi ve Windows bildirim alanındaki simge vardır. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile işlemler gerçekleştirebilir. Kaspersky Endpoint Security ayrıca uygulama simgesinin üzerinde bildirimler görüntüler.
   - **Uygulama Etkinlik İzleyicisi bölümünü gizle**. Kullanıcının bilgisayarındaki uygulama etkinliği bilgilerini gizlemek istiyorsanız, kullanıcının Uygulama Etkinlik İzleyicisi aracına erişimini kısıtlayabilirsiniz.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulamanın kullanıma hazırlanması

Uygulamayı istemci bilgisayarlara dağıttıktan sonra, Kaspersky Endpoint Security'yi Kaspersky Security Center Web Console üzerinden kullanmak için aşağıdaki eylemleri gerçekleştirmeniz gerekir:

- Bir ilke oluşturun ve yapılandırın.

  Bir yönetim grubundaki bütün istemci bilgisayarlara aynı Kaspersky Endpoint Security ayarlarını uygulamak için ilkeleri kullanabilirsiniz. Kaspersky Security Center'ın Hızlı Başlangıç Sihirbazı, Kaspersky Endpoint Security için otomatik olarak bir ilke oluşturur.
- *Veritabanlarının ve uygulama modüllerinin güncellemesi* ve *Kötü Amaçlı Yazılım Taraması* görevlerini oluşturun.

  Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, bilgisayarın güvenliğini güncel tutmak için gereklidir. Görev gerçekleştirildiğinde Kaspersky Endpoint Security antivirüs veritabanları ve uygulama modüllerini günceller. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

  Kötü Amaçlı Yazılım Taraması görevi, virüs ve diğer zararlı yazılımların zamanında tespit edilmesi için gereklidir. *Kötü Amaçlı Yazılım Taraması* görevini manuel olarak oluşturmalısınız.

Yönetim Konsolu'nda (MMC) bir Kötü Amaçlı Yazılım Taraması görevi nasıl oluşturulur

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Kötü Amaçlı Yazılım Taraması** seçimini yapın.

2. Adım. Tarama kapsamı

Kaspersky Endpoint Security tarafından bir tarama görevi yürütülürken taranacak nesnelerin listesi oluşturun.

3. Adım. Kaspersky Endpoint Security eylemi

Tehdit algılandığında yapılacak eylemi seçin:

- **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.
- **Temizle; temizleme başarısız olursa bildir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme başarısız olursa Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
- **Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
- **Gelişmiş Temizleme işlemini derhal çalıştır**. Onay kutusu işaretlenirse, tarama sırasında etkin tehditlere müdahale etmek için Kaspersky Endpoint Security Gelişmiş Temizleme teknolojisini kullanır.

  Gelişmiş temizleme teknolojisi, RAM'da işlem başlatmış olan ve diğer yöntemleri kullanarak Kaspersky Endpoint Security'nin bu uygulamaları kaldırmasını önleyen zararlı uygulamaların 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 temizleme teknolojisi, oldukça fazla İşletim sistemi kaynağı kullanır ve bu da diğer uygulamaları yavaşlatabilir. Gelişmiş virüs temizleme tamamlandıktan sonra, Kaspersky Endpoint Security kullanıcının onayını istemeden bilgisayarı yeniden başlatacaktır.
- **Sadece bilgisayar boştayken çalıştır**. Bilgisayar kaynakları meşgul olduğunda görevin başlatılması ertelenir. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır. Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.

4. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

5. Adım. Görevi çalıştıracak hesabı seçme

Kötü Amaçlı Yazılım Taraması görevini çalıştırmak için bir hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır. Tarama kapsamına ağ sürücüleri veya kısıtlı erişime sahip diğer nesneler dahilse, yeterli erişim haklarına sahip bir kullanıcı hesabı seçin.

6. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görev başlatmak için bir zamanlama yapılandırın, örneğin manuel olarak ya da antivirüs veritabanları veri havuzuna indirildikten sonra.

7. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Günlük tam tarama*.

8. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz. Sonuç olarak Kötü Amaçlı Yazılım Taraması görevi kullanıcı bilgisayarlarında belirtilen zamanlamaya göre yürütülür.

Web Console'da bir Kötü Amaçlı Yazılım Taraması görevi oluşturma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Kötü Amaçlı Yazılım Taraması**'nı seçin.

   c. **Görev adı** alanına *Haftalık tarama* gibi kısa bir açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Görev zamanlamasını yapılandırmak için görev özelliklerine gidin.

   Görevin, haftada en az bir kez çalıştırılmak üzere zamanlanması tavsiye edilir.

8. Görevin yanındaki onay kutusunu seçin.

9. **Başlat**'a tıklayın.

   Görevin durumunu ve görevin başarıyla veya bir hatayla tamamlandığı aygıtların sayısını izleyebilirsiniz.

Sonuç olarak Kötü Amaçlı Yazılım Taraması görevi kullanıcı bilgisayarlarında belirtilen zamanlamaya göre yürütülür.

- Kaspersky Endpoint Security'nin performansını optimize edin.

İlkeleri yönetme

İlke, bir yönetim grubu için tanımlanan uygulama ayarları kümesidir. Bir uygulama için farklı değerlere sahip birden çok ilke yapılandırabilirsiniz. Bir uygulamada, farklı yönetim grupları için farklı ayarlar geçerli olabilir. Her yönetim grubunun, bir uygulama için kendine özgü ilkesi olabilir.

Her ilke ayarının (“asma kilit”) özniteliği vardır. Bu özelliğin durumu, ayarın yönetim grubundaki yönetilen cihazlara aktarılıp aktarılmayacağını belirler:

- “Asma kilit” simgesi açıksa (), bu ayarın değeri yönetilen cihazlara aktarılmayacaktır. Bu ayar, uygulamanın yerel arabiriminden değiştirilebilir. Bu tür ayarlara *kilitli değil* denir.

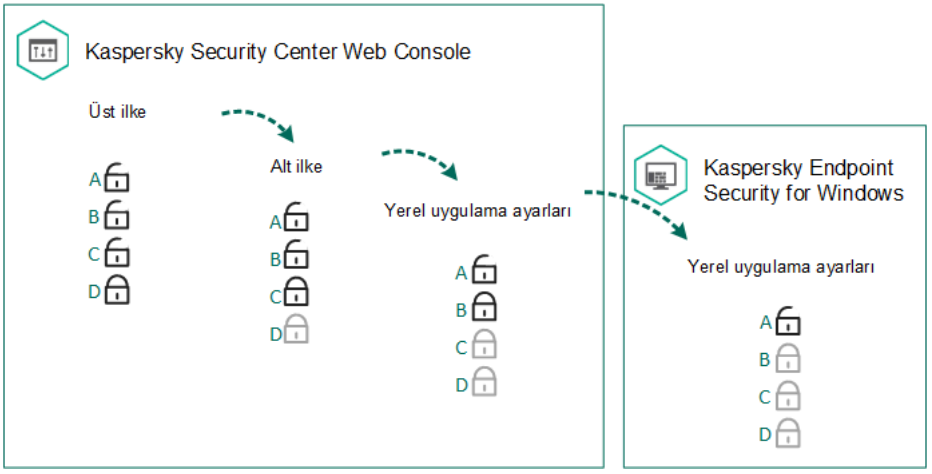
- “Asma kilit” simgesi kapalıysa (), bu ayarın değeri yönetilen cihazlara aktarılacak ve uygulanacaktır. Bu tür ayarlara *kilitli* denir. Engellenen ayarlar, uygulamanın yerel arabiriminde değiştirilemez.

İlke ayarları, *senkronizasyon* sırasında Ağ Aracısı tarafından istemci bilgisayarlara gönderilir. Yönetim Sunucusu varsayılan olarak ilke ayarları değiştirildikten hemen sonra senkronizasyon işlemi gerçekleştirir. İstemci bilgisayardaki UDP portu 15000, senkronizasyon için kullanılır. Yönetim Sunucusu varsayılan olarak her 15 dakikada bir senkronizasyon işlemi gerçekleştirir. İlke ayarları değiştirildikten sonra bir sonraki senkronizasyon denemesi başarısız olursa senkronizasyon yapılandırılmış zamanlamaya göre gerçekleştirilir.

Ayarların devralınması

Yönetim grupları gibi ilkeler bir hiyerarşi içinde düzenlenir. *Alt ilke*, iç içe geçmiş hiyerarşi düzeylerine yönelik bir ilkedir. Bir başka deyişle, iç içe geçmiş yönetim grupları ve ikincil Yönetim Sunucularına yönelik bir ilkedir.

Varsayılan olarak, bir alt ilke ana ilkenin ayarlarını devralır. Eğer üst ilkedeki ayar (kapalı "asma kilit") özniteliğine sahipse, alt ilkelerde ve yerel uygulama ayarlarında bu ayarın değeri üst ilkeye uygun olarak geçersiz kılınır ve ayar kilitlenir. Gerekirse, üst ilkeyle ilgili ayarların devralınmasını devre dışı bırakabilirsiniz. İşyeri dışında ilkeleri, yönetim gruplarının hiyerarşisi üzerinden diğer ilkeleri etkilemez.



Ayarların devralınması

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 (varsayılan olarak bu bölüm konsol arabiriminde gizlidir).

İlke revizyonları

Kaspersky Security Center, ilke değişikliklerini takip eder ve revizyonlar oluşturur. Bir *revizyon*, kullanıcı tarafından kaydedilen bir dizi değiştirilmiş parametredir. Revizyonlar, ilke parametrelerindeki değişiklikleri karşılaştırmanıza ve geri almanıza olanak tanır. Değiştirilen parametrelerin yanı sıra, bu güncelleme, değişiklikleri yapan kullanıcıya ait bilgilerin yanı sıra saat, IP adresi, kullanıcı yorumu ve diğer ilgili verileri de içermektedir.

Değişiklik günlüğünü görüntülemek için, ilke özelliklerini açın ve **Değişiklik geçmişi** bölümüne gidin. Revizyonlarla çalışmak hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

İlke oluşturma

Bir ilke oluştururken, sihirbaz seçilen modla ilgili ayarları önerir. Örneğin, Light Agent modu için bir Protection Server (SVM) eklemeniz gerekir. Uygulamayı bir SQL sunucusunu korumak için kullanırken, sunucunun çalışmasına müdahale edilmediğinden emin olmak için önceden tanımlanmış tarama istisnaları eklemeniz gerekir. Sihirbaz, bir mod seçtikten sonra ilgili ilke ayarlarını önerir. Daha sonra bu ayarları ilke özelliklerinde düzenleyebilirsiniz.

Yönetim Konsolu'nda (MMC) bir ilke oluşturma

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 seçin.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. **Yeni ilke** üzerine tıklayın.
   İlke Sihirbazı başlatılır.
5. İlke Sihirbazı talimatlarını uygulayın.

Adım 1. Grup ilkesi oluşturmak için uygulamayı seçme

Kaspersky Endpoint Security for Windows (14.2) uygulamasını seçin.

Adım 2. Grup ilkesini adlandırma

Grup ilkesi için bir ad girin; örneğin, *Ofis için İlke*.

İlke Sihirbazını kullanarak mevcut ilkeleri temel alan yeni ilkeler de oluşturabilirsiniz. Bunu yapmak için, grup ilkesi adını belirtirken **Uygulamanın daha önceki bir sürümüne ilişkin ilke ayarlarını kullan** onay kutusunu seçin. Sihirbaz ayrıca Kaspersky Security for Windows Server (KSWS) veya Kaspersky Security for Virtualization Light Agent for Windows gibi farklı bir çözümün ilkesini temel alan bir Kaspersky Endpoint Security (KES) ilkesi oluşturmaya da olanak tanır

Adım 3. Kaspersky Security Network'e katılma

Lütfen Kaspersky Security Network (KSN) Bildirimi şartlarını okuyun ve kabul edin.

4. Adım Bilgisayarlarda uygulama kullanım modunun seçilmesi

Kaspersky Endpoint Security'nin kullanım amacına bağlı olarak, aşağıdaki uygulama modları için bir ilke yapılandırabilirsiniz:

- Ana bilgisayarları korumak için standart mod

Bu modda, ilkeyi nasıl yapılandırmak istediğinizi seçebilirsiniz:

- **Varsayılan ayarlarla bir ilke oluşturun**. Varsayılan ayarlar optimum olarak kabul edilir. Kaspersky uzmanları tarafından bu ayarlar tavsiye edilmektedir. Varsayılan ayarlar, önerilen koruma düzeyini ve optimum kaynak kullanımını sağlar.

- **Sihirbazda ilke ayarlarını değiştirin**. Bu yöntem, bir sihirbaz yardımıyla ilke ayarlarını adım adım yönetmenizi sağlar. Uygulamanın yapılandırma dosyasını kullanarak da ilke ayarlarını yönetebilirsiniz (bir sonraki adıma bakın).

- Gelişmiş tehditlere ve hedefli saldırılara karşı koruma sağlayan Endpoint Detection and Response Agent.

  Endpoint Detection and Response Agent, Kaspersky'nin Detection and Response çözümlerini desteklemek için kuruluşun BT altyapısındaki bireysel iş istasyonlarına ve sunuculara yüklenen bir uygulamadır. Bir sonraki adımda, EDR Agent entegrasyonu için bir çözüm seçmeniz gerekiyor.

- Sanal ortamları korumak için Light Agent.

  Uygulamayı Light Agent modunda kullanmak için, bir SVM sanal makinesiyle bağlantı kurmanız gerekir. Bu ayarlar uygulamanın Light Agent modunda çalışması için gereklidir.

Kaspersky Endpoint Security, tüm uygulama modları ve işletim sistemi türleri için ortak bir ilke sağlar. Bu, ilkenin tüm ayarları kapsadığı anlamına gelir. Ancak, Kaspersky Endpoint Security bazı işlevlerin kullanılamadığı bir modda dağıtıldığı için uygulama bazı ilke ayarlarını yok sayabilir. Örneğin, uygulamayı Endpoint Detection and Response Agent modunda kullanırken, yalnızca Kaspersky Detection and Response çözümleriyle entegrasyon ve KUMA ile entegrasyonla ilgili ayarlar kullanılabilir.

Farklı modlar ve işletim sistemi türleri için farklı ilkeler kullanmanızı öneririz.

5. Adım. Ayarları içe aktarma

Bu adım, 4. adımda manuel ilke yapılandırmasını seçmeniz durumunda kullanılabilir.

Kaspersky Endpoint Security ayarlarından yola çıkarak bir ilke oluşturabilirsiniz. CFG yapılandırma dosyası. Yeni ilke sihirbazı, şifrelenmiş yapılandırma dosyalarını desteklemez. Yapılandırma dosyasını dışa aktarırken dosya şifreleme adımını atlayın.

Bir uygulama CFG yapılandırma dosyası içe aktarılırken sihirbaz tüm ilke ayarlarına erişemez. Örneğin, uygulama ayarlarında ilke profilleri eksik olabilir. Tüm ayarları ve profilleri ilkeye aktarmak istiyorsanız, bir KLP dosyasından başka bir ilkeyi içe aktarabilirsiniz.

Bir yapılandırma dosyası içe aktarılırken, Kaspersky Endpoint Security kripto konteyner parolalarını aktarmaz. Sunuculara bağlanırken iki aşamalı kimlik doğrulama kullanıyorsanız, kripto konteyner parolalarını baştan belirlemeniz gerekir.

6. - 10. adım. İlke ayarlarını yapılandırma

Bu adım, 4. adımda manuel ilke yapılandırmasını seçmeniz durumunda kullanılabilir.

İlke ayarlarını yönetmek için aşağıdaki adımları izleyin.

11. Adım. Güvenilen bölgeyi yapılandırma

Güvenilen bölgeyi yapılandırın. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar ekleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar da Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında Light Agent modunda hızlı bir şekilde yapılandırmanıza yardımcı olabilir.

12. Adım. İlke durumunu seçme

- **Etkin**. İlke bir sonraki senkronizasyondan sonra bilgisayarda etkin ilke olarak kullanılır.

  Bir etkin ilkenin ayarları, senkronizasyon sırasında istemci bilgisayara kaydedilir. Bir bilgisayarda aynı anda birden çok ilke uygulayamazsınız, bu nedenle her bir grupta yalnızca bir ilke etkin durumda olabilir.

- **Etkin değil**. Yedek ilke. Gerekli olduğunda etkin olmayan bir ilke etkin duruma geçebilir.

  Sınırsız sayıda etkin olmayan ilke oluşturabilirsiniz. Etkin olmayan bir ilke, ağdaki bilgisayarların uygulama ayarlarını etkilemez. Etkin olmayan ilkeler, virüs saldırısı gibi acil durumlara yöneliktir. Flash sürücüler üzerinden bir saldırı olursa flash sürücülere erişimi engelleyen bir ilkeyi etkinleştirebilirsiniz. Bu durumda, etkin ilke otomatik olarak etkin olmayan duruma geçer.

- **İşyeri dışında**. İlke, bir bilgisayar kuruluş ağından ayrıldığında etkinleştirilir.

Sihirbazı tamamlayın.

Web Console'da ve Cloud Console'da bir ilke nasıl oluşturulur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. **Ekle**'ye tıklayın.

   İlke Sihirbazı başlatılır.
3. Kaspersky Endpoint Security'yi seçin ve **İleri**'ye tıklayın.
4. Kaspersky Security Network (KSN) Bildirimi'nin hükümlerini okuyup kabul edin ve **İleri**'ye tıklayın.

5. Uygulamanın modunu seçin:

   - İş istasyonlarını ve sunucuları korumak için standart mod
   - Gelişmiş tehditlere ve hedefli saldırılara karşı koruma sağlayan Endpoint Detection and Response Agent.

     Bu modu seçerseniz, bilgisayarı Kaspersky Detection and Response çözümleriyle entegre etmek için bir ilke oluşturabilirsiniz. Sihirbaz, Kaspersky Managed Detection and Response ve ardından Kaspersky Anti Targeted Attack Platform (EDR) için entegrasyonu yapılandırmanızı ister.
   - Sanal ortamları korumak için Light Agent.

     Bu modu seçerseniz, bir sonraki adımda Protection Server (SVM) bağlantısını yapılandırmanız gerekir. Bu ayarlar uygulamanın Light Agent modunda çalışması için gereklidir.

   Kaspersky Endpoint Security, tüm uygulama modları ve işletim sistemi türleri için ortak bir ilke sağlar. Bu, ilkenin tüm ayarları kapsadığı anlamına gelir. Ancak, Kaspersky Endpoint Security bazı işlevlerin kullanılamadığı bir modda dağıtıldığı için uygulama bazı ilke ayarlarını yok sayabilir. Örneğin, uygulamayı Endpoint Detection and Response Agent modunda kullanırken, yalnızca Kaspersky Detection and Response çözümleriyle entegrasyon ve KUMA ile entegrasyonla ilgili ayarlar kullanılabilir.

   > Farklı modlar ve işletim sistemi türleri için farklı ilkeler kullanmanızı öneririz.

6. Güvenilen bölgeyi yapılandırın. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar ekleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar da Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında Light Agent modunda hızlı bir şekilde yapılandırmanıza yardımcı olabilir.

7. **Genel** sekmesinde, aşağıdaki eylemleri gerçekleştirebilirsiniz:

   - İlke adını değiştirme.
   - İlke durumunu seçme:

     - **Etkin**. İlke bir sonraki senkronizasyondan sonra bilgisayarda etkin ilke olarak kullanılır.

       Bir etkin ilkenin ayarları, senkronizasyon sırasında istemci bilgisayara kaydedilir. Bir bilgisayarda aynı anda birden çok ilke uygulayamazsınız, bu nedenle her bir grupta yalnızca bir ilke etkin durumda olabilir.
     - **Etkin değil**. Yedek ilke. Gerekli olduğunda etkin olmayan bir ilke etkin duruma geçebilir.

       Sınırsız sayıda etkin olmayan ilke oluşturabilirsiniz. Etkin olmayan bir ilke, ağdaki bilgisayarların uygulama ayarlarını etkilemez. Etkin olmayan ilkeler, virüs saldırısı gibi acil durumlara yöneliktir. Flash sürücüler üzerinden bir saldırı olursa flash sürücülere erişimi engelleyen bir ilkeyi etkinleştirebilirsiniz. Bu durumda, etkin ilke otomatik olarak etkin olmayan duruma geçer.
     - **İşyeri dışında**. İlke, bir bilgisayar kuruluş ağından ayrıldığında etkinleştirilir.

- Ayarların devralmayı yapılandırma:
  - **Ayarları üst ilkeden devral**. Bu iki durumlu düğme açılırsa ilke ayarları, üst düzeydeki ilkeden devralınır. Üst ilke için ayarlandıysa ilke ayarları düzenlenemez.
  - **Alt ilkelerdeki ayarların devralınmasını zorla**. İki durumlu düğme açılırsa ilke ayarlarının değerleri alt ilkelere aktarılır. Alt ilke özelliklerinde **Ayarları üst ilkeden devral** iki durumlu düğmesi otomatik olarak açık duruma getirilir ve kapalı duruma alınamaz. Alt ilke ayarları, ile işaretlenmiş ayarlar haricinde üst ilkeden devralınır. Üst ilke için ayarlandıysa alt ilke ayarları düzenlenemez.

8. **Uygulama ayarları** sekmesinde Kaspersky Endpoint Security ilke ayarlarını yapılandırabilirsiniz.
9. Sihirbazı tamamlayın.

Sonuç olarak Kaspersky Endpoint Security ayarları, bir sonraki senkronizasyonda istemci bilgisayarlarda yapılandırılır. Kaspersky Endpoint Security arabiriminde, bilgisayara uygulanan ilke hakkındaki bilgileri (örneğin ilke adı) ana ekrandaki düğmesine tıklayarak görüntüleyebilirsiniz. Bunu yapmak için Ağ Aracısı ilkesinin ayarlarından genişletilmiş ilke verilerinin alınmasını etkinleştirmeniz gerekir. Bir Ağ Aracısı ilkesi hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center Yardımı'na başvurun.

Bir ilkeyi dışa aktarma ve içe aktarma

Kaspersky Endpoint Security, bir ilkeyi ayarları ve profilleriyle birlikte bir KLP dosyasına aktarmanıza olanak tanır. Ardından, ilke dışa aktarma/içe aktarma işlevini kullanarak ilkeleri yedekleyebilir, ilkeleri başka bir sunucuya taşıyabilir veya örneğin Kaspersky Security Center Windows'tan Kaspersky Security Center Linux taşıyabilirsiniz. İlkeleri yönetme hakkında ayrıntılar için lütfen Kaspersky Security Center Yardım bölümüne bakın.

Yönetim Konsolu'nda (MMC) bir ilkeyi dışa ve içe aktarma

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. Bir ilkeyi dışa aktarmak için:
   a. Dışa aktarmak istediğiniz ilkeye tıklayın.
   b. Pencerenin sağ tarafındaki **İlkeyi dosyaya aktar** bağlantısını tıklayın.
   c. Açılan pencerede, ilkeyi dışa aktarmak istediğiniz KLP dosyasının adını belirtin ve dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
5. Bir ilkeyi içe aktarmak için:
   a. **Dosyadan ilke içe aktar** seçeneğine tıklayın.
   b. Açılan pencerede, içe aktarmak istediğiniz KLP ilke dosyasını seçin.
   c. Dosyayı aç.

Bu işlem, *Etkin olmayan ilke* durumuna sahip yeni bir ilke ekler.

Web Console'da ilkeyi dışa ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Bir ilkeyi dışa aktarmak için:
   a. Dışa aktarmak istediğiniz ilkenin yanındaki onay kutusunu işaretleyin.
   b. **Dışa aktar** düğmesine tıklayın.
   c. Açılan pencerede, ilkeyi dışa aktarmak istediğiniz KLP dosyasının adını belirtin ve dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
3. Bir ilkeyi içe aktarmak için:
   a. **İçe aktar**'a tıklayın.
   b. İçe aktarmak istediğiniz KLP ilkesi dosyasını seçin.
   c. İlke başarıyla işlendikten sonra, ilkeyi uygulamak istediğiniz yönetim grubunu seçin.
   d. İlkenin içe aktarılmasını tamamlamak için **Tamam** düğmesine tıklayın.

Bu işlem, *Etkin olmayan* durumuna sahip yeni bir ilke ekler.

Güvenlik düzeyi göstergesi

Güvenlik düzeyi göstergesi, ilke özellikleri penceresinin üst kısmında görüntülenir. Gösterge aşağıdaki değerlerden birini alabilir:

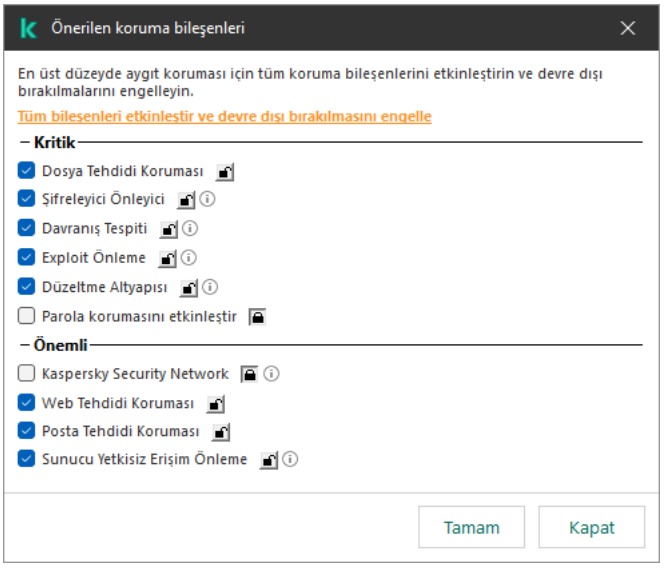
- **Yüksek koruma düzeyi**. Gösterge bu değeri alır ve aşağıdaki kategorilerdeki tüm bileşenler etkinse yeşile döner:
  - **Kritik**. Bu kategori aşağıdaki bileşenleri içerir:
    - Dosya Tehdidi Koruması.
    - Davranış Tespiti.
    - Exploit Önleme.
    - Düzeltme Altyapısı.
    - Uygulama hizmetlerinin harici yönetime karşı korunması.
  - **Önemli**. Bu kategori aşağıdaki bileşenleri içerir:
    - Kaspersky Security Network.
    - Web Tehdidi Koruması.

- Posta Tehdidi Koruması.
- Sunucu Yetkisiz Erişim Önleme.
- Parola koruması.

- **Orta koruma düzeyi**. Gösterge, bu değeri alır ve önemli bileşenlerden biri devre dışıysa sarıya döner.
- **Düşük koruma düzeyi**. Gösterge bu değeri alır ve aşağıdaki durumlardan birinde kırmızıya döner:
  - Bir veya daha fazla kritik bileşen devre dışıdır.
  - İki veya daha fazla önemli bileşen devre dışıdır.

Gösterge, **Orta koruma düzeyi** veya **Düşük koruma düzeyi** değerine sahipse, göstergenin sağında **Önerilen koruma bileşenleri** penceresini açan bir bağlantı görüntülenir. Bu pencerede, önerilen koruma bileşenlerinden herhangi birini etkinleştirebilirsiniz.

Uygulamayı yükselttikten sonra, koruma seviyesi göstergesi yükseltme öncesine göre daha düşük bir koruma düzeyi gösterebilir. Bu durum, uygulamanın yeni sürümünde bilgisayarın güvenliği için önemli olan yeni bileşenler veya özellikler eklenmesi nedeniyle meydana gelir. Uygulamayı yükselttikten sonra, koruma seviyesinin yüksek kalmasını sağlamak için yeni ayarları yönetmeniz gerekir.



İlkenin güvenlik düzeyi göstergesi

Görev yönetimi

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.
- Bilgisayar seçimine yönelik görevler.

İstediğiniz sayıda grup görevi, bilgisayar seçimine yönelik görevler veya yerel görevler oluşturabilirsiniz. Yönetim gruplarıyla çalışma, bilgisayarların ve bilgisayar aralıklarının seçimleri hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

Kaspersky Endpoint Security aşağıdaki görevleri destekler:

- **Kötü Amaçlı Yazılım Taraması**. Kaspersky Endpoint Security, görev ayarlarında belirtilen bilgisayar alanlarında virüs ve diğer tehditleri tarar. *Kötü Amaçlı Yazılım Taraması* görevi, Kaspersky Endpoint Security'nin çalışması için gereklidir ve Hızlı Başlangıç Sihirbazı ile oluşturulur. Görevin, haftada en az bir kez çalıştırılmak üzere zamanlanması tavsiye edilir.

- **Anahtar ekle**. Kaspersky Endpoint Security, ek anahtar dahil olmak üzere uygulamaların etkinleştirilmesi için bir anahtar ekler. Görevi gerçekleştirmeden önce görevin gerçekleştirileceği bilgisayar sayısının, lisans tarafından izin verilen bilgisayar sayısını geçmediğinden emin olun.

- **Uygulama bileşenlerini değiştir**. Kaspersky Endpoint Security, görev ayarlarında belirtilen bileşenlerin listesine göre istemci bilgisayarlara bileşenleri yükler veya kaldırır. Dosya Tehdidi Koruması bileşeni kaldırılamaz. Kaspersky Endpoint Security bileşenlerinin optimum seti, bilgisayar kaynaklarının daha düşük düzeyde kullanılmasını sağlar.

- **Envanter**. Kaspersky Endpoint Security, bilgisayarlarda depolanan uygulamalara ait tüm yürütülebilir dosyalarla ilgili bilgi alır. *Envanter* görevi, Uygulama Denetimi bileşeni tarafından gerçekleştirilir. Uygulama Denetimi bileşeni yüklü değilse görev bir hata vererek sonlandırılır.

- **Veritabanlarının ve uygulama modüllerinin güncellemesi**. Kaspersky Endpoint Security, veritabanlarını ve uygulama modüllerini günceller. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi, Kaspersky Endpoint Security'nin çalışması için gereklidir ve Hızlı Başlangıç Sihirbazı ile oluşturulur. Görevin günde en az bir kez gerçekleştirileceği bir zamanlama yapılandırmanız tavsiye edilir.

- **Verileri sil**. Kaspersky Endpoint Security kullanıcıların bilgisayarlarındaki dosyaları ve klasörleri anında veya Kaspersky Endpoint Security ile uzun süre boyunca hiçbir iletişim olmazsa siler.

- **Güncellemeyi geri al**. Kaspersky Endpoint Security, veritabanları ve uygulama modüllerinin son güncellemesini geri alır. Bu özellik, yeni veritabanları Kaspersky Endpoint Security'nin güvenli bir uygulamayı engellemesine neden olabilecek yanlış veriler içermesi durumunda gereklidir.

- **Uygulama Bütünlüğü Kontrolü**. Kaspersky Endpoint Security uygulama dosyalarını analiz eder, dosyalarda bozulma veya değiştirme olup olmadığını kontrol eder ve uygulama dosyalarının dijital imzalarını doğrular.

- **Kimlik Doğrulama Aracısı hesaplarını yönet**. Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı hesap ayarlarını yapılandırır. Şifrelenmiş sürücülerle çalışırken bir Kimlik Doğrulama Aracısı gereklidir. İşletim sistemi yüklenmeden önce kullanıcının Aracı ile kimlik doğrulamasını tamamlaması gerekir.

Uygulama Kaspersky'nin Detection and Response çözümünün bir parçası olarak çalışıyorsa, ek görevleri tespit yanıt eylemleri olarak çalıştırabilirsiniz (responses). Örneğin, *İşlemi sonlandır* görevini kullanarak işlemleri uzaktan sonlandırabilirsiniz.

Görevler bir bilgisayarda yalnızca Kaspersky Endpoint Security çalışıyorsa gerçekleştirilir.

Bir görev oluşturma

Yönetim Konsolu'nda (MMC) nasıl bir görev oluşturulur

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Görevler** klasörünü seçin.
3. **Yeni görev**'e tıklayın.
   Görev Sihirbazı başlatılır.
4. Görev Sihirbazı talimatlarını uygulayın.

Web Console'da görev oluşturma

1. Web Console ana penceresinden **Görevler** seçimini yapın.
   Görevler listesi açılır.
2. **Ekle**'ye tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
   b. **Görev türü** açılır listesinde, kullanıcıların bilgisayarlarında çalıştırmak istediğiniz görevi seçin.
   c. **Görev adı** alanına kısa bir açıklama girin.
   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.
5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.
6. Sihirbazı tamamlayın.

Görevler listesinde yeni bir görev görüntülenir. Görev varsayılan ayarlara sahip olacaktır. Görev ayarlarını yapılandırmak için görev özelliklerine gitmelisiniz. Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçmeli ve **Başlat** düğmesine tıklamalısınız. Görev başlatıldıktan sonra görevi duraklatabilir ve daha sonra devam ettirebilirsiniz.

Görevler listesinden, bilgisayarlardaki görev durumunu ve görev performansını içeren görev sonuçlarını takip edebilirsiniz. Görevlerin tamamlanma durumunu izlemek için bir olay seçimi kümesi de oluşturabilirsiniz (**İzleme** → **Olay seçimleri**). Olay seçimi hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun. Görev yürütme sonuçları ayrıca yerel olarak Windows olay günlüğüne ve Kaspersky Endpoint Security raporlarına kaydedilir.

Görev erişimini yönetme

Kaspersky Endpoint Security görevlerine erişim hakları (okuma, yazma, uygulama) Kaspersky Security Center Yönetim Sunucusu'na erişimi olan her bir kullanıcı için Kaspersky Endpoint Security'ye erişim ayarlarıyla belirlenmektedir. Kaspersky Endpoint Security'nin işlev alanlarına erişimi yapılandırmak için Kaspersky Security Center Yönetim Sunucusu'nun özellikler penceresinin **Güvenlik** bölümüne girin. Kaspersky Security Center'da görev yönetimi hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım içeriğine bakın.

Bir ilke kullanarak kullanıcıların görevlere erişim haklarını yapılandırabilirsiniz (*görev yönetimi modu*). Örneğin Kaspersky Endpoint Security arabirimindeki grup görevlerini gizleyebilirsiniz.

Kaspersky Endpoint Security'deki görev yönetimi modun Yönetim Konsolu (MMC) aracılığıyla nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Yerel Görevler** → **Görev yönetimi** seçimini yapın.
4. Görev yönetimi modunu yapılandırın (aşağıdaki tabloya bakın).
5. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Security'deki görev yönetimi modu Web Console aracılığıyla nasıl yapılandırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kullanıcı Etkileşimi** bölümüne gidin.
5. **İzin verilen eylemler** altında, görev yönetimi modunu yapılandırın (aşağıdaki tabloya bakın).
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Görev yönetimi ayarları

Parametre	Açıklama
Yerel görevlere erişim	Onay kutusu işaretlenirse yerel görevler Kaspersky Endpoint Security yerel arabiriminde görüntülenir. Ek ilke kısıtlamaları olmadığında kullanıcı görevleri yapılandırabilir ve çalıştırabilir. Ancak kullanıcı yine de görev çalışma zamanlamasının yapılandıramaz. Kullanıcı, görevleri yalnızca manuel olarak çalıştırabilir. Bu onay kutusunun işareti kaldırılırsa yerel görevler uygulama arabiriminde gizlenir. Bu modda, yerel görevler zamanlamaya göre çalışmaz. Görevler, Kaspersky Endpoint Security'nin yerel arabiriminde veya komut satırı ile çalışırken başlatılamaz veya yapılandırılamaz. Kullanıcı, dosya veya klasörün içerik menüsünde **Virüslere karşı tara** seçeneği işaretleyerek bir dosyanın veya klasörün virüs taramasını hala başlatabilir. Tarama görevi, özel tarama görevi için varsayılan ayar değerleri ile başlatılır.
Grup görevlerini görüntüle	Onay kutusu işaretlenirse grup görevler. Kaspersky Endpoint Security yerel arabiriminde görüntülenir. Kullanıcı, tüm görevlerin listesini uygulama arabiriminde görebilir. Onay kutusu işaretlenmezse Kaspersky Endpoint Security boş bir görev listesi görüntüler.
Grup görevlerini yönet	Onay kutusu işaretlenirse, kullanıcılar Kaspersky Security Center konsolunda belirtilen grup görevlerini başlatabilir ve durdurabilir. Kullanıcılar, uygulama arabiriminde ya da basitleştirilmiş uygulama arabiriminde görevleri başlatabilir ve durdurabilir. Onay kutusunun işaretlenmezse, Kaspersky Security Center zamanlanmış görevleri otomatik olarak başlatır ya da yönetici yönetim görevlerini Kaspersky Security Center konsolunda manuel olarak başlatır.

Yerel uygulama ayarlarını yapılandırma

Kaspersky Security Center'da, belirli bir bilgisayardaki Kaspersky Endpoint Security ayarlarını yapılandırabilirsiniz. Bunlar *yerel uygulama ayarlarıdır*. Bazı ayarlar, düzenlemek için erişilebilir olmayabilir. Bu ayarlar ilke özelliklerinde özniteliği tarafından engellenir.

Yerel uygulama ayarları Yönetim Konsolu'nda (MMC) nasıl yapılandırılır

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, **Cihazlar** sekmesini seçin.
4. İlke özellikleri penceresini açmak için çift tıklayın.
5. Bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
6. Bilgisayarda yüklü Kaspersky uygulamaları listesinde **Kaspersky Endpoint Security for Windows (14.2)** öğesini seçin ve çift tıklayarak uygulama özelliklerini açın.
7. **Genel ayarlar** bölümünde, Kaspersky Endpoint Security ile birlikte Raporlar ve Depolama Alanını da yapılandırın.

   Uygulama özellikleri penceresindeki diğer bölümler Kaspersky Security Center için standarttır. Bu bölümlerin açıklaması Kaspersky Security Center Yardım içeriğinde bulunmaktadır.

   > Uygulama, belirli ayarlarda değişiklik yapılmasını yasaklayan bir ilkeye tabi ise **Genel Ayarlar** bölümünde uygulama ayarlarını yapılandırırken bunları düzenleyemezsiniz.

8. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da yerel uygulama ayarları nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi → Varlıklar (Cihazlar)** seçimini yapın.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.

   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows 14.2** öğesine tıklayın.

   Bu, yerel uygulama ayarlarını açar.
5. **Uygulama ayarları** sekmesini seçin.
6. Yerel uygulama ayarlarını yapılandırın.
7. Değişikliklerinizi kaydedin.

Yerel uygulama ayarları, şifreleme ayarları haricinde ilke ayarları ile aynıdır.

Kaspersky Endpoint Security'yi başlatma ve durdurma

Kaspersky Endpoint Security bir kullanıcının bilgisayarına yüklendikten sonra uygulama otomatik olarak başlatılır. Kaspersky Endpoint Security varsayılan olarak işletim sistemi başlatıldıktan sonra çalıştırılır. İşletim sistemi ayarlarında uygulamanın otomatik başlatılmasını ayarlamak mümkün değildir.

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

Yönetim Konsolu'nda (MMC) Kaspersky Endpoint Security'nin başlatılması nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
4. Uygulama başlatmasını yapılandırmak için **Uygulamayı bilgisayar başlangıcında çalıştır (önerilir)** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

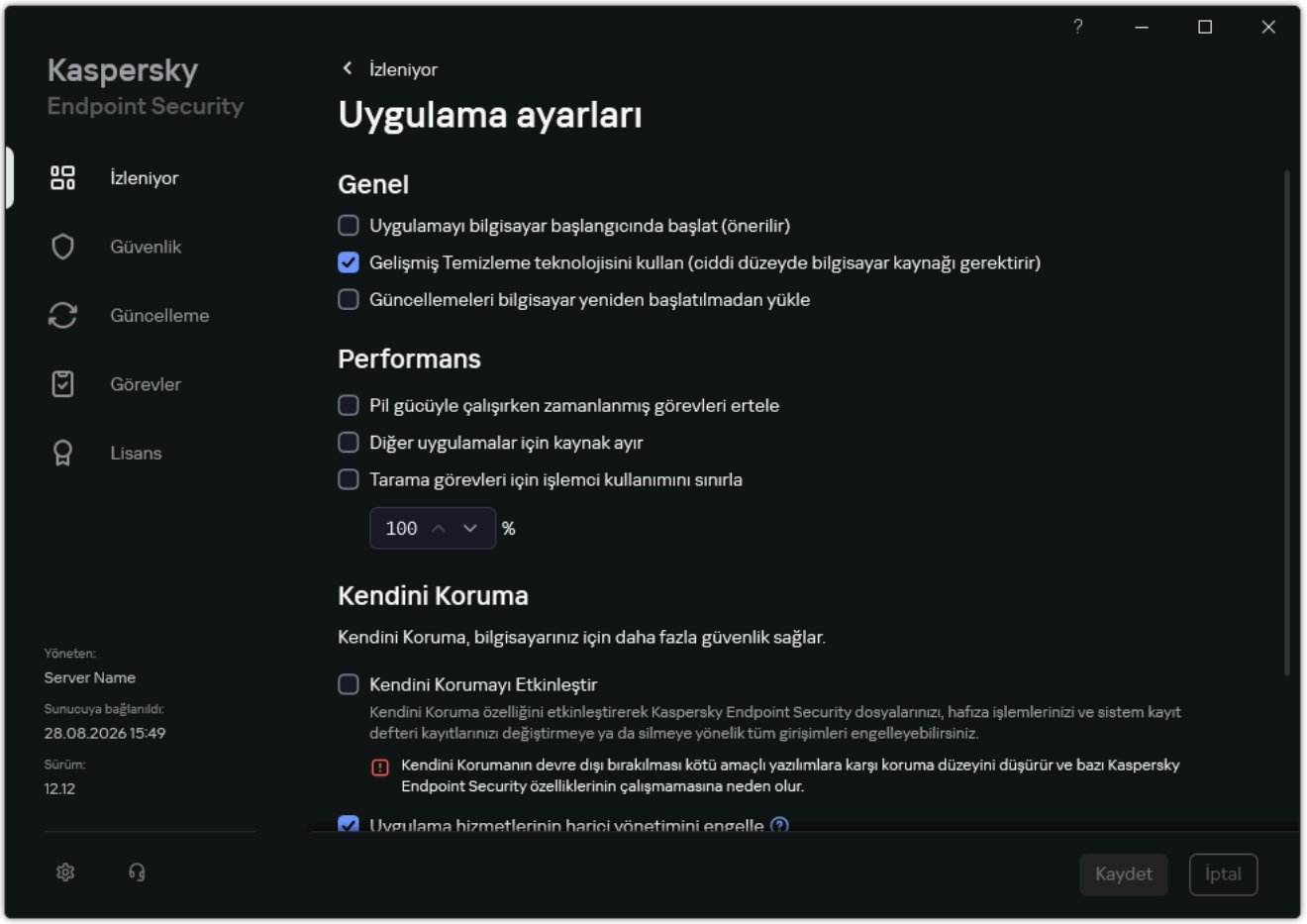
Web Console'da Kaspersky Endpoint Security'nin başlatılması nasıl yapılandırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kullanıcı Etkileşimi** bölümüne gidin.
5. Uygulama başlatmasını yapılandırmak için **Bilgisayar başlatılırken Kaspersky Endpoint Security uygulamasını çalıştır (önerilir)** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Kaspersky Endpoint Security'nin başlatılması nasıl yapılandırılır

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. Uygulama başlatmasını yapılandırmak için **Uygulamayı bilgisayar başlangıcında çalıştır (önerilir)** onay kutusunu kullanın.
4. Değişikliklerinizi kaydedin.

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

Koruma durumu pencere öğesini kullanarak uygulama durumunu izleyebilirsiniz.

Yönetim Konsolu'nda (MMC) Kaspersky Endpoint Security nasıl başlatılır veya durdurulur

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, **Cihazlar** sekmesini seçin.
4. İlke özellikleri penceresini açmak için çift tıklayın.

5. Bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
6. Bilgisayarda yüklü Kaspersky uygulamaları listesinde **Kaspersky Endpoint Security for Windows (14.2)** öğesini seçin ve çift tıklayarak uygulama özelliklerini açın.
7. Aşağıdakilerden birini yapın:
   - Uygulamayı başlatmak için Kaspersky uygulamalarının listesinin sağındaki düğmesine tıklayın.
   - Uygulamayı durdurmak için Kaspersky uygulamalarının listesinin sağındaki düğmesine tıklayın.

Web Console'da Kaspersky Endpoint Security nasıl başlatılır veya durdurulur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Kaspersky Endpoint Security'yi başlatmak veya durdurmak istediğiniz bilgisayarın adına tıklayın.
   Bilgisayar özellikleri penceresi açılır.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows**'un karşısındaki onay kutusunu seçin.
5. **Başlat** veya **Durdur** düğmesine tıklayın.

Kaspersky Endpoint Security komut satırından nasıl başlatılır veya durdurulur

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Yürütülebilir dosya klpsm.exe'nin bulunduğu klasöre gidin.
3. Uygulamayı komut satırından başlatmak için `klpsm.exe start_avp_service` komutunu girin.
4. Uygulamayı komut satırından durdurmak için `klpsm.exe stop_avp_service` komutunu girin.

> Uygulamayı komut satırından durdurmak için sistem hizmetlerinin harici yönetimini etkinleştirin.



Uygulamayı komut satırından başlatma ve durdurma

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.

- simgesi, bilgisayar koruması ve denetiminin duraklatıldığı anlamına gelir.
- simgesi, bilgisayar koruması ve denetiminin etkinleştirildiğini gösterir.

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

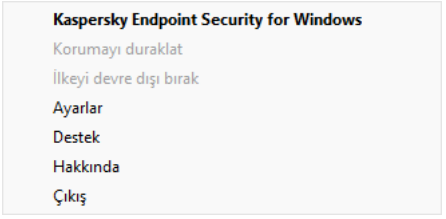
Bilgisayar koruması ve denetimini duraklattığınızda veya sürdürdüğünüzde herhangi bir ağ bağlantısı zaten kurulursa bu ağ bağlantılarının sonlandırılmasıyla ilgili bir bildirim görüntülenir.

Bilgisayar koruması ve denetimini duraklatmak için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin bağlam menüsünü açın.
2. İçerik menüsünde **Korumayı duraklat**'ı seçin (aşağıdaki resme bakın).

   Bu bağlam menüsü sadece Parolası koruması etkinleştirilmişse kullanılabilir.
3. Aşağıdaki seçeneklerden birini seçin:
   - **Duraklatma süresi: <zaman aralığı>** – aşağıdaki açılır listede belirtilen sürenin ardından bilgisayar koruması ve denetimi devam edecektir.
   - **Uygulama yeniden başlatılana dek duraklat** – uygulamayı veya işletim sistemini yeniden başlattıktan sonra bilgisayar koruması ve denetimi devam edecektir. Bu seçeneği kullanmak için uygulamanın otomatik başlatılması etkin olmalıdır.
   - **Duraklat** – yeniden etkinleştirmeye karar verdiğinizde bilgisayar koruması ve denetimi devam edecektir.
4. **Korumayı duraklat**'a tıklayın.

Kaspersky Endpoint Security, ilkede bir kilit () ile işaretlenmemiş tüm koruma ve denetim bileşenlerini duraklatacaktır. Bu işlem gerçekleştirmeden önce Kaspersky Security Center ilkesinin devre dışı bırakılması önerilir.



Uygulama simgesi bağlam menüsü

Bilgisayar koruması ve denetimini sürdürmek için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin bağlam menüsünü açın.
2. İçerik menüsünde **Korumayı sürdür**'ü seçin.

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

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.
- Önceden tanımlanmış ayarlarla Kaspersky Security Center aracılığıyla Kaspersky Endpoint Security'nin uzaktan kurulumunu yapabilirsiniz.
- Uygulama ayarlarını bir ilkeye aktarın.
- Kaspersky Endpoint Security ayarlarını bir bilgisayardan diğerine taşıyabilirsiniz (aşağıdaki talimatlara bakın).

Yapılandırma dosyasını dışa aktarma

Kaspersky Endpoint Security 14.2 sürümünden itibaren dışa aktarılan yapılandırma dosyası şifrelenebilir. Yapılandırma dosyası kimlik bilgileri içerebileceğinden dosyayı şifrelemenizi öneririz. Şifrelenmiş bir dosyayı düzenleyemezsiniz. Bir yapılandırma dosyasını değiştirmeye yönelik her türlü girişim dosyanın bozulmasına neden olacaktır.

Yapılandırma dosyası şifreleme şu özel özelliklere sahiptir:

- Kaspersky Endpoint Security, şifrelenmiş dosyaların yalnızca uygulamanın kullanıcı arabiriminde veya komut satırında içe aktarılmasına izin verir. Böyle bir dosyayı, bir ilke yapılandırmak veya uygulamayı uzaktan yüklemek için Kaspersky Security Center konsolunda kullanamazsınız. Dosyayı bir ilkeye veya kurulum paketine eklemeyi planlıyorsanız dosya şifreleme adımını atlayın.
- Şifrelenmiş bir dosyanın parolasını kurtarmak mümkün değildir.
- Kaspersky Endpoint Security'nin 14.1'den önceki sürümleri, şifrelenmiş yapılandırma dosyalarının içe aktarılmasını desteklemez. Dosyayı uygulamanın daha eski bir sürümüne aktarmayı planlıyorsanız dosya şifreleme adımını atlayın.

Bir yapılandırma dosyası oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ayarları yönet** öğesini seçin.
3. **Dışa aktar**'a tıklayın.
4. Yapılandırma dosyasını kaydetmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Ayarları dışa aktar** izninin olması gerekir.
5. Açılan pencerede 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.

6. Gerekirse **Dışa aktarılan dosyayı şifrele** geçiş anahtarını etkinleştirin ve yapılandırma dosyasının şifreleme parolasını girin.

   Parolayı güvenli bir depoda saklayın. Bu parolayı kurtarmak mümkün değildir.

7. Dosyaya kaydet.

Sonuç olarak, uygulama bir yapılandırma dosyası oluşturur.

Yapılandırma dosyasını içe aktarma

Bir yapılandırma dosyası içe aktarılırken, Kaspersky Endpoint Security kripto konteyner parolalarını aktarmaz. Sunuculara bağlanırken iki aşamalı kimlik doğrulama kullanıyorsanız, kripto konteyner parolalarını baştan belirlemeniz gerekir.

Kaspersky Endpoint Security ayarlarını bir yapılandırma dosyasından içe aktarmak için:

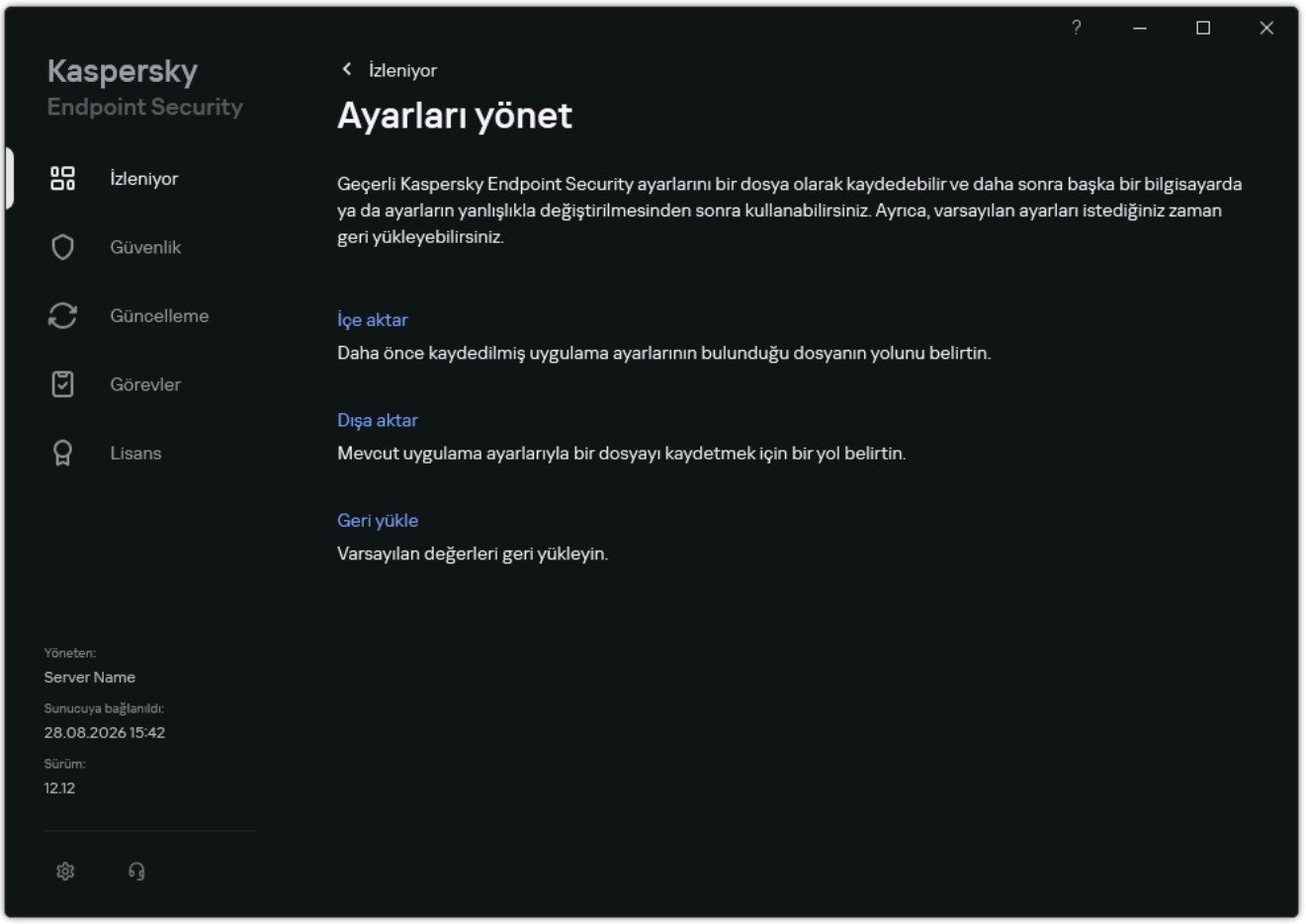
1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ayarları yönet** öğesini seçin.
3. **İçe aktar**'a tıklayın.
4. Açılan pencereye yapılandırma dosyasının yolunu girin.

5. Yapılandırma dosyası şifrelenmişse dışa aktarma sırasında belirttiğiniz parolayı girin.

> Yapılandırma dosyasının şifreleme parolasını unutursanız parolayı kurtaramazsınız. Bu durumda, yapılandırma dosyasını dışa aktarma adımlarını tekrarlamanız gerekir.

6. Dosyayı aç.

Kaspersky Endpoint Security ayarlarının bütün değerleri, seçilen yapılandırma dosyasına göre ayarlanacaktır.



Uygulama ayarlarını yönetme

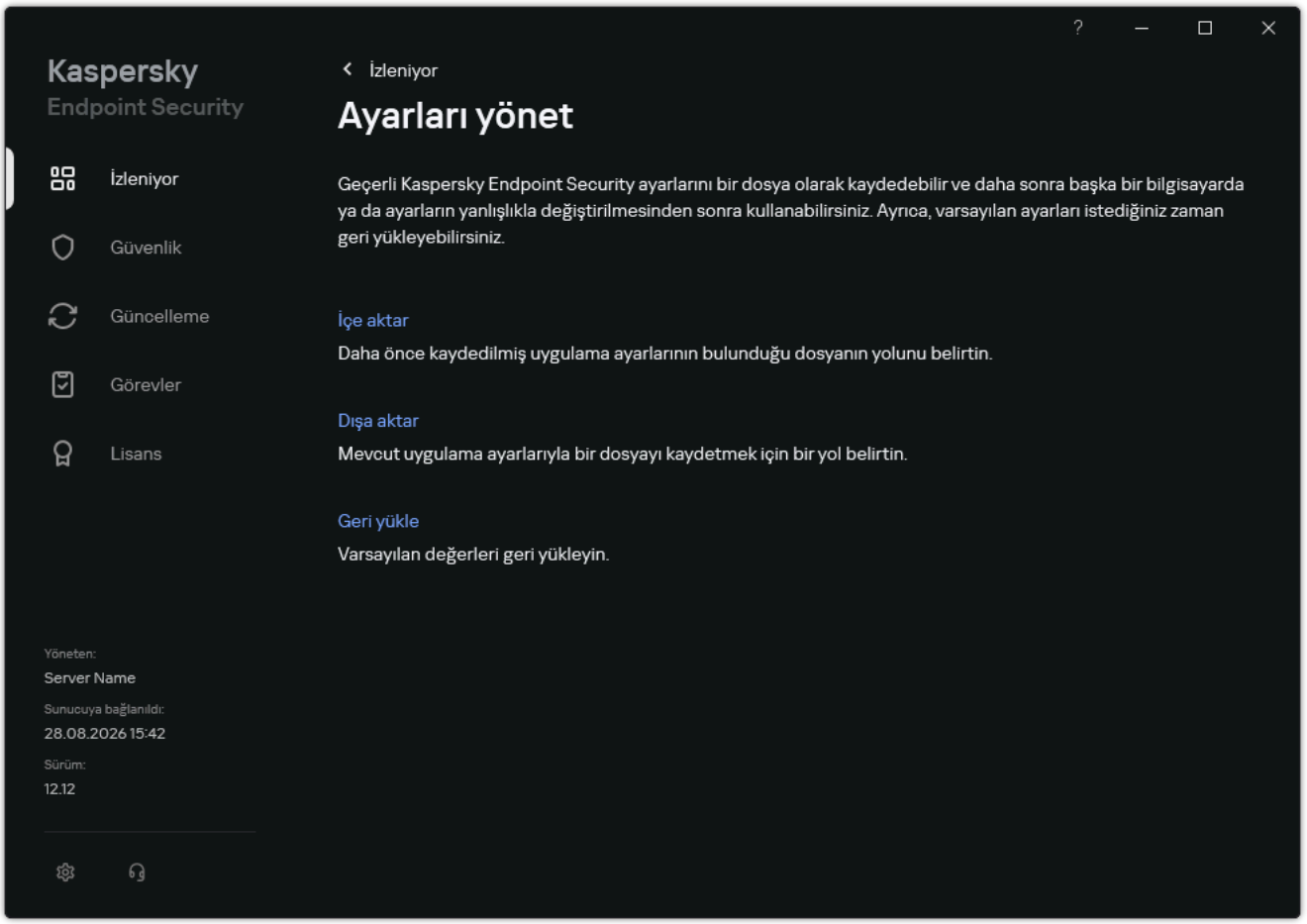
Varsayılan uygulama ayarlarını geri yükleme

Kaspersky tarafından önerilen uygulama ayarlarını dilediğiniz zaman geri yükleyebilirsiniz. Ayarlar geri yüklendiğinde tüm koruma bileşenleri için **Önerilen** güvenlik düzeyi ayarlanır.

Varsayılan uygulama ayarlarını geri yüklemek için

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ayarları yönet** öğesini seçin.
3. **Geri yükle**'ye tıklayın.

4. Değişikliklerinizi kaydedin.



Uygulama ayarlarını yönetme

Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu

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 Trojanları 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.

- Tam Tarama görevi;
- Kritik Alanları Tarama görevi;
- Özel Tarama 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

Bilgisayarı tararken bilgisayar kaynaklarının tüketilmesi, işlemci ve sabit sürücü alt sistemleri üzerindeki yükü artırabilir. CPU ve sabit sürücü alt sistemlerinde yük arttığında eşzamanlı çalışma sorununu çözmek için Kaspersky Endpoint Security diğer uygulamalar için kaynak ayırabilir.

Gelişmiş temizleme teknolojisini kullanma

Günümüzde zararlı uygulamalar bir işletim sisteminin en düşük düzeylerine nüfuz edebilmekte ve bu da, bu uygulamaların 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 uygulamaları kaldırmasını önleyen zararlı uygulamaların 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 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.

Sunucularla ilgili Kaspersky Endpoint Security özelliklerinden dolayı 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 Gelişmiş Temizleme gerektiğini belirten bilgilerle olay, Kaspersky Security Center'a aktarılır. Bir sunucudaki etkin virüsü temizlemek için sunucular için Gelişmiş Temizleme teknolojisini etkinleştirin ve sunucu kullanıcıları için uygun bir zamanda *Kötü Amaçlı Yazılım Taraması* grup görevini başlatın.

Enerji tasarrufu modunu etkinleştirme veya devre dışı bırakma

Güç tasarrufu modu, güvenlik düzeyi açısından önemli ölçüde ödün vermeden dizüstü bilgisayarın kaynakları üzerindeki yükü azaltan ve pil ömrünü uzatan bir işlevdir. Güç tasarrufu modunda, uygulama zamanlanmış görevlerin başlatılmasını sınırlar. Bu sayede, güç tasarrufu modu dizüstü bilgisayarın güvenlik düzeyi ile pil ömrü arasında bir denge sağlar.

Güç tasarrufu modu etkinleştirildiğinde ve bilgisayar pil gücüyle çalışırken, aşağıdaki görevler zamanlanmış olsa bile çalıştırılmaz:

- *Tam Tarama*.
- *Kritik Alanları Tarama*.
- *Özel Tarama*.
- *Uygulama Bütünlüğü Kontrolü*.
- *IOC Taraması*
- *Veritabanlarının ve uygulama modüllerinin güncellemesi* (sadece yamalar)

Uygulama, yalnızca dizüstü bilgisayar pil ile çalışırken ve pil seviyesi %30'un (varsayılan değer) altında olduğunda planlanmış veritabanı güncellemelerini atlar. Uygulamanın planlanmış antivirüs veritabanı güncellemelerini atlamaya başladığı minimum pil şarj düzeyini kayıt defterini düzenleyerek değiştirebilirsiniz (aşağıdaki talimatlara bakın). Diğer tüm durumlarda, Kaspersky Endpoint Security, dizüstü bilgisayarın şarja bağlı ya da pil ile çalışıyor olmasına veya uygulamanın güç tasarrufu modunda olup olmamasına bakılmaksızın, veritabanlarını zamanlamaya göre günceller.

Yönetim Konsolu'nda (MMC) güç tasarrufu modunu etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
5. **Performans** bloğunda, güç tasarrufu modunu etkinleştirmek veya devre dışı bırakmak için **Pil gücüyle çalışırken zamanlanmış görevleri ertele** onay kutusunu kullanın.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

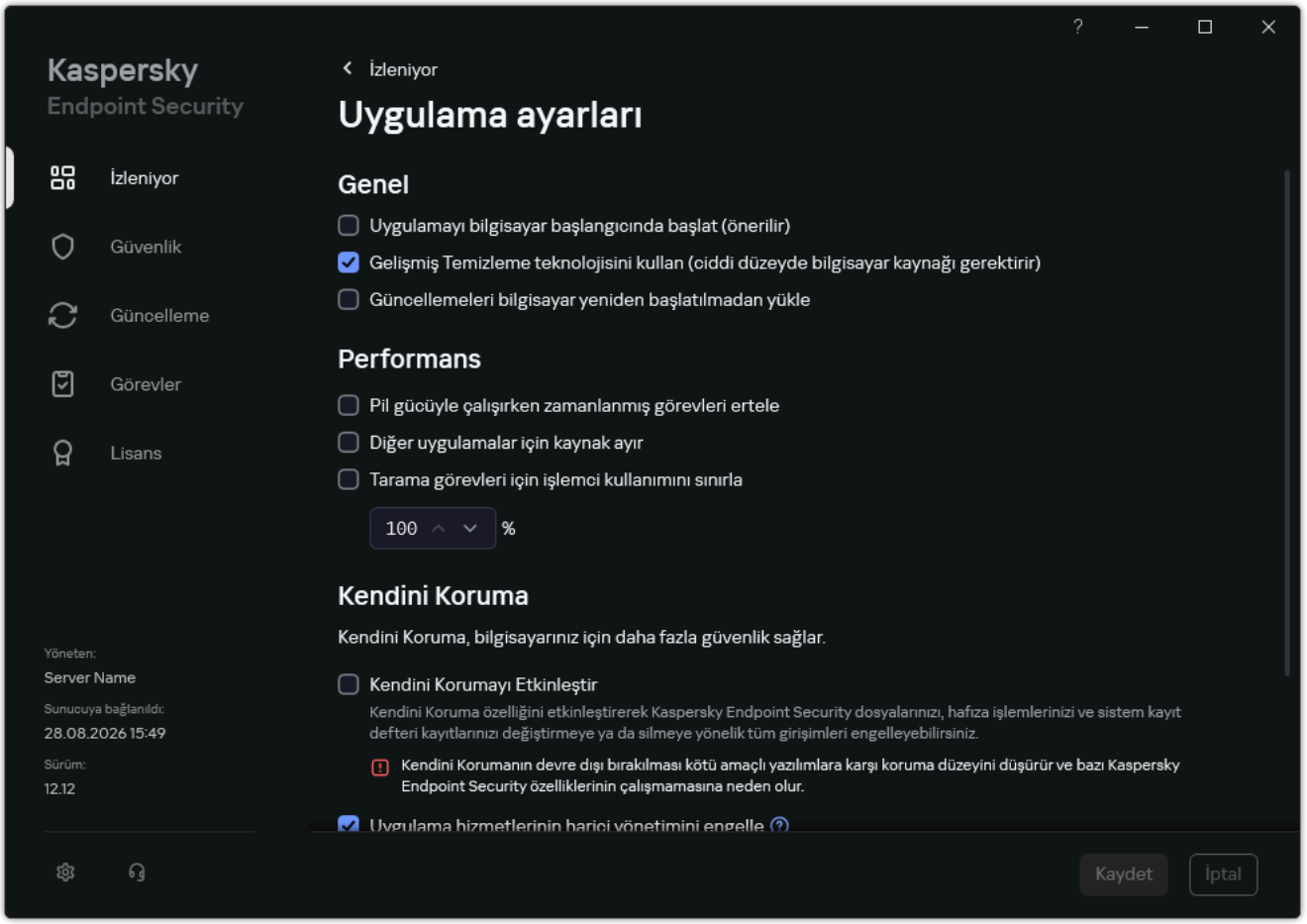
Web Console'da güç tasarrufu modunu etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Performans** bölümüne gidin.
5. **Pil gücüyle çalışırken zamanlanmış görevleri ertele veya atla** bölümünde, **Pil gücüyle çalışırken zamanlanmış görevleri ertele veya atla (işletim sistemine bağlıdır)** onay kutusunu kullanarak güç tasarrufu modunu etkinleştirebilir veya devre dışı bırakabilirsiniz.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde güç tasarrufu modunu nasıl etkinleştirilir veya devre dışı bırakılır

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. **Performans** bloğunda, güç tasarrufu modunu etkinleştirmek veya devre dışı bırakmak için **Pil gücüyle çalışırken zamanlanmış görevleri ertele** onay kutusunu kullanın.
4. Değişikliklerinizi kaydedin.

Uygulamanın planlanmış antivirüs veritabanı güncellemelerini atlamaya başladığı minimum şarj düzeyini değiştirme

1. Bilgisayardaki kayıt defteri düzenleyicisini açın.
2. Kayıt düzenleyicisinde aşağıdaki bölüme gidin:
   - 64-bit işletim sistemleri için:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - 32-bit işletim sistemleri için:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Düzenlemek için `UpdaterAccumulatorThreshold` anahtarını açın.
4. Uygulamanın planlanmış antivirüs veritabanı güncellemelerini atlamaya başlayacağı minimum şarj düzeyini belirtin.

Diğer uygulamalar için kaynak yaratmayı etkinleştirme veya devre dışı bırakma

Bir bilgisayarı tararken Kaspersky Endpoint Security tarafından bilgisayar kaynaklarının tüketilmesi, CPU ve sabit sürücü alt sistemleri üzerindeki yükü artırabilir. Bu diğer uygulamaları yavaşlatabilir. Kaspersky Endpoint Security, performansı optimize etmek için bir *kaynakları diğer uygulamalara aktarma modu* sunar. Bu modda, işletim sistemi CPU yükü yüksek olduğunda Kaspersky Endpoint Security tarama görevi iş parçacıklarının önceliğini düşürebilir. Bu, işletim sistemi kaynaklarının diğer uygulamalara yeniden dağıtılmasını sağlar. Böylece tarama görevleri daha az CPU süresi almış olur. Sonuç olarak, Kaspersky Endpoint Security'nin bilgisayarı taraması daha uzun sürer. Varsayılan olarak uygulama, kaynakları diğer uygulamalara bırakacak şekilde yapılandırılmıştır.

Yönetim Konsolu'nda (MMC) diğer uygulamalar için kaynak aktarmayı etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
4. **Performans** bloğunda, kaynakların diğer uygulamalara ayrılmasını etkinleştirmek veya devre dışı bırakmak için **Diğer uygulamalar için kaynak ayır** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da diğer uygulamalar için kaynak ayırmayı etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Performans** bölümüne gidin.

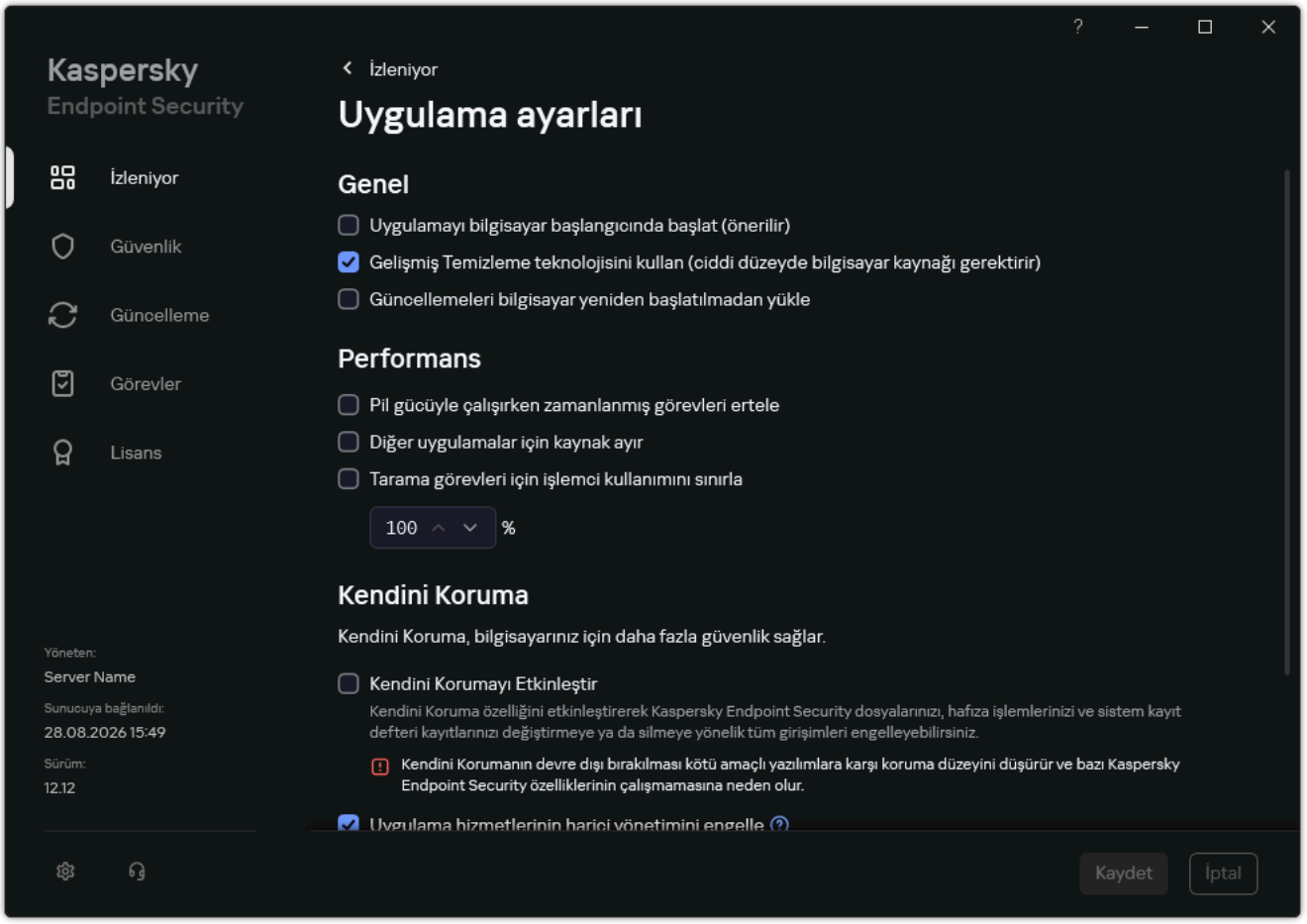
5. **Diğer uygulamalar için kaynak ayır** bloğunda, kaynakların diğer uygulamalara ayrılmasını etkinleştirmek veya devre dışı bırakmak için **Diğer uygulamalar için kaynak ayır** geçiş düğmesini kullanın.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde diğer uygulamalar için kaynak ayırmayı etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. **Performans** bloğunda, kaynakların diğer uygulamalara ayrılmasını etkinleştirmek veya devre dışı bırakmak için **Diğer uygulamalar için kaynak ayır** onay kutusunu kullanın.

4. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Security performansını optimize etmek için en iyi uygulamalar

Kaspersky Endpoint Security for Windows'u dağıtırken, bilgisayar korumasını yapılandırmak ve performansı optimize etmek için aşağıdaki önerileri kullanabilirsiniz. Bilgisayar performans sorunları hakkında daha fazla bilgi için lütfen Teknik Destek Bilgi Tabanına bakın.

Genel

Uygulamanın genel ayarlarını aşağıdaki önerilere göre yapılandırın:

1. Kaspersky Endpoint Security'yi en son sürüme yükseltin.

   Uygulamanın yeni sürümlerinde hatalar düzeltildi, kararlılık geliştirildi ve performans optimize edildi.

2. Koruma bileşenlerini varsayılan ayarlarla etkinleştirin.

   Varsayılan ayarlar optimum olarak kabul edilir. Kaspersky uzmanları tarafından bu ayarlar tavsiye edilmektedir. Varsayılan ayarlar, önerilen koruma düzeyini ve optimum kaynak kullanımını sağlar. Gerekirse varsayılan uygulama ayarlarını geri yükleyebilirsiniz.

3. Uygulama performansı optimizasyon özelliklerini etkinleştirin.

   Uygulamanın performans optimizasyonu özellikleri vardır: enerji tasarrufu modu ve kaynakların diğer uygulamalara aktarılması. Bu seçeneklerin etkinleştirildiğinden emin olun.

İş istasyonlarında Kötü Amaçlı Yazılım Taraması

İş istasyonlarının Kötü Amaçlı Yazılım Taraması için Arka plan taramasının etkinleştirilmesi önerilir. *Arka Plan Taraması*, Kaspersky Endpoint Security'nin kullanıcıya bildirim görüntülemeyen bir tarama modudur. Arka Plan Taraması diğer tarama türlerine göre (tam tarama gibi) daha az bilgisayar kaynağı gerektirir. Bu modda, Kaspersky Endpoint Security başlangıç nesnelerini, önyükleme kesimini, sistem belleğini ve sistem bölümünü tarar. Arka plan taraması ayarları optimum kabul edilir. Kaspersky uzmanları tarafından bu ayarlar tavsiye edilmektedir. Böylece bilgisayarda Kötü Amaçlı Yazılım Taraması gerçekleştirmek için diğer tarama görevlerini kullanmadan sadece arka plan taraması modunu kullanabilirsiniz.

Arka plan taraması ihtiyaçlarınızı karşılamıyorsa, *Kötü Amaçlı Yazılım Taraması* görevini aşağıdaki önerilere göre yapılandırın:

1. Bilgisayarı tararken CPU kaynak tüketimi için bir sınır belirleyin.

   Kötü Amaçlı Yazılım Taraması görevi çalıştırılırken işlemci kullanımını sınırlayabilirsiniz. Bunu yapmak için, uygulama ayarlarında, bilgisayarı tararken kullanılabilecek tüm çekirdekler için maksimum işlemci yük yüzdesini belirtin. Bu, bilgisayarınızın taranma süresini artırabilir.

2. Optimum bilgisayar taraması zamanlamasını yapılandırın.

   Görevi, bilgisayar minimum yük altında çalışırken çalışacak şekilde yapılandırabilirsiniz. Örneğin, görevi gece veya hafta sonları çalışacak şekilde yapılandırabilirsiniz.

   Kullanıcılar bilgisayarı çalışma saatleri dışında kapatırsa, LAN'da Uyandırma işlevini etkinleştirebilirsiniz. Wake-on-LAN özelliği, yerel ağ üzerinden özel bir sinyal göndererek bilgisayarın uzaktan açılmasını sağlar. Wake-on-LAN özelliğini kullanmak için BIOS ayarlarından LAN'da Uyandırmayı etkinleştirmeniz gerekir. Tarama bittikten sonra bilgisayarın otomatik olarak kapanmasını da sağlayabilirsiniz.

   En uygun tarama zamanlamasını yapılandıramazsanız, görevleri yalnızca bilgisayar boştayken çalışacak şekilde ayarlayın. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır.

3. Bir tarama kapsamı tanımlayın.

Tarama için aşağıdaki nesneleri seçin (minimum tarama kapsamı seti):

- Çekirdek Belleği
- Çalışan işlemler ve Başlangıç Nesneleri
- Önyükleme kesimleri
- %systemroot% (alt klasörler hariç)
- %systemroot%\System (alt klasörler hariç)
- %systemroot%\System32 (alt klasörler hariç)
- %systemroot%\System32\drivers (alt klasörler hariç)
- %systemroot%\SysWOW64 (alt klasörler hariç)
- %systemroot%\SysWOW64\drivers (alt klasörler hariç)

4. iSwift ve iChecker teknolojilerini açın.

   - iSwift teknolojisi.

     Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.

   - iChecker teknolojisi.

     Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).

   iSwift ve iChecker teknolojilerini yalnızca Yönetim Konsolu'nda (MMC) ve Kaspersky Endpoint Security arabiriminde açabilirsiniz. Bu teknolojileri Kaspersky Security Center Web Console'da açamazsınız.

5. Parola korumalı arşivlerin taranmasını devre dışı bırakın.

   Parola korumalı arşivlerin taranması etkinleştirilirse, arşiv taranmadan önce bir parola istemi görüntülenir. Bu görevin mesai saatleri dışında planlanması önerildiğinden, kullanıcı parola girişi yapamaz. Parola korumalı arşivleri manuel olarak tarayabilirsiniz.

6. Birkaç tarama görevinin aynı anda başlatılmasını devre dışı bırakın.

   Mevcut tarama devam ediyorsa Kaspersky Endpoint Security yeni tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur.

Sunucularda Kötü Amaçlı Yazılım Taraması

Kötü Amaçlı Yazılım Taraması görevini aşağıdaki önerilere göre yapılandırın:

1. Bilgisayarı tararken CPU kaynak tüketimi için bir sınır belirleyin.

   Kötü Amaçlı Yazılım Taraması görevi çalıştırılırken işlemci kullanımını sınırlayabilirsiniz. Bunu yapmak için, uygulama ayarlarında, bilgisayarı tararken kullanılabilecek tüm çekirdekler için maksimum işlemci yük yüzdesini belirtin. Bu, bilgisayarınızın taranma süresini artırabilir.

2. Optimum bilgisayar taraması zamanlamasını yapılandırın.

   Görevi, bilgisayar minimum yük altında çalışırken çalışacak şekilde yapılandırabilirsiniz. Örneğin, görevi gece veya hafta sonları çalışacak şekilde yapılandırabilirsiniz.

3. iSwift ve iChecker teknolojilerini açın.

   - iSwift teknolojisi.

     Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.

   - iChecker teknolojisi.

     Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).

   iSwift ve iChecker teknolojilerini yalnızca Yönetim Konsolu'nda (MMC) ve Kaspersky Endpoint Security arabiriminde açabilirsiniz. Bu teknolojileri Kaspersky Security Center Web Console'da açamazsınız.

4. Parola korumalı arşivlerin taranmasını devre dışı bırakın.

   Parola korumalı arşivlerin taranması etkinleştirilirse, arşiv taranmadan önce bir parola istemi görüntülenir. Bu görevin mesai saatleri dışında planlanması önerildiğinden, kullanıcı parola girişi yapamaz. Parola korumalı arşivleri manuel olarak tarayabilirsiniz.

5. Birkaç tarama görevinin aynı anda başlatılmasını devre dışı bırakın.

   Mevcut tarama devam ediyorsa Kaspersky Endpoint Security yeni tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur.

Kaspersky Security Network

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. Kaspersky Security Network'e katılıyorsanız, KSN hizmetleri Kaspersky Endpoint Security'ye taranan web adreslerinin itibarı hakkında bilgi ve taranan dosyaların kategorisi ve tanınırlığı hakkında bilgi sağlar.

Kaspersky Security Network ayarlarını aşağıdaki önerilere göre düzenleyin:

1. Genişletilmiş KSN modunu devre dışı bırak.

   Genişletilmiş KSN modu, Kaspersky Endpoint Security'nin Kaspersky'ye daha fazla veri gönderdiği bir moddur.

2. Kaspersky Private Security Network'ü yapılandırın.

   Kaspersky Private Security Network (KPSN), Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür.

3. Bulut modunu etkinleştir.

   Bulut modu, Kaspersky Endpoint Security'nin anti-virüs veritabanlarının daha basit bir sürümünü kullandığı uygulama çalışma moduna karşılık gelir. Kaspersky Security Network, uygulamanın basit anti-virüs veritabanlarını kullanarak çalışmasını destekler. Anti-virüs veritabanlarının basit sürümü ile kullanılan RAM miktarı, normal veritabanları ile kullanılan RAM miktarının yaklaşık olarak yarısıdır. Kaspersky Security Network'e katılmazsanız ya da bulut modu devre dışı bırakılırsa, Kaspersky Endpoint Security Kaspersky sunucularından anti-virüs veritabanlarının en son sürümünü indirir.

Kötü Amaçlı Yazılım Taraması

Kötü Amaçlı Yazılım Taraması, bilgisayar güvenliği için hayati önem taşır. Düzenli yapılan kötü amaçlı yazılım taramaları, düşük güvenlik düzeyi ayarı veya başka nedenlerle koruma bileşenleri tarafından tespit edilmeyen zararlı yazılımların yayılması olasılığı ortadan kaldırır.

Kaspersky Endpoint Security, içeriği OneDrive bulut depolama alanında bulunan dosyaları taramaz ve bu dosyaların taranmadığını belirten günlük girişleri oluşturur.

Tam Tarama

Tüm bilgisayarda gerçekleştirilen kapsamlı bir taramadır. Kaspersky Endpoint Security aşağıdaki nesneleri tarar:

- Çekirdek Belleği
- İşletim sistemi açılışında yüklenen nesneler
- Önyükleme kesimleri
- İşletim sistemi yedekleme
- Tüm sabit ve çıkarılabilir sürücüler

Kaspersky uzmanları, *Tam Tarama* görevinin tarama kapsamını değiştirmemenizi öneriyor.

Bilgisayar kaynaklarını korumak için tam tarama görevi yerine bir arka plan taraması görevi kullanılması önerilir. Bu işlem, bilgisayarın güvenlik düzeyini etkilemez.

Kritik Alanları Tarama

Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.

Kaspersky uzmanları, *Kritik Alanları Tarama* görevinin tarama kapsamını değiştirmemenizi öneriyor.

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
- Sabit, çıkarılabilir sürücüler ve ağ sürücüleri
- Seçilen herhangi bir dosya

Arka Plan Taraması

Arka Plan Taraması, Kaspersky Endpoint Security'nin kullanıcıya bildirim görüntülemeyen bir tarama modudur. Arka Plan Taraması diğer tarama türlerine göre (tam tarama gibi) daha az bilgisayar kaynağı gerektirir. Bu modda, Kaspersky Endpoint Security başlangıç nesnelerini, önyükleme kesimini, sistem belleğini ve sistem bölümünü tarar.

Uygulama Bütünlüğü Kontrolü

Kaspersky Endpoint Security, uygulama modüllerinde bozukluk veya değişiklik olup olmadığını denetler.

Bilgisayarı tarama

Tarama, bilgisayar güvenliği için hayati önem taşır. Düzenli yapılan kötü amaçlı yazılım taramaları, düşük güvenlik düzeyi ayarı veya başka nedenlerle koruma bileşenleri tarafından tespit edilmeyen zararlı yazılımların yayılması olasılığı ortadan kaldırır. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Kaspersky Endpoint Security, önceden tanımlanmış şustandart görevlere sahiptir: *Tam Tarama*, *Kritik Alanları Tarama*, *Özel Tarama*. Kuruluşunuzda Kaspersky Security Center yönetim sistemi hizmete alınmışsa, bir *Kötü Amaçlı Yazılım Taraması* görevi oluşturabilir ve taramayı yapılandırabilirsiniz.

Yönetim Konsolu'nda (MMC) bir tarama görevi nasıl çalıştırılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. Gereken tarama görevini seçin ve görev özellikleri penceresini açmak için çift tıklayın.

   Gerekirse *Kötü Amaçlı Yazılım Taraması* görevi oluşturun.

4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.
5. Tarama görevini yapılandırın (aşağıdaki tabloya bakın).

   Gerekirse, tarama görevi zamanlamasını yapılandırın.
6. Değişikliklerinizi kaydedin.
7. Tarama görevini çalıştırın.

Kaspersky Endpoint Security bilgisayarı taramaya başlayacaktır. Kullanıcı görevin yürütülmesini durdurduysa (mesela bilgisayarı kapatarak), Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır.

Web Console'da tarama görevi nasıl çalıştırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.
2. Tarama görevine tıklayın.

   Görev özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. Tarama görevini yapılandırın (aşağıdaki tabloya bakın).

   Gerekirse, tarama görevi zamanlamasını yapılandırın.
5. Değişikliklerinizi kaydedin.
6. Tarama görevini çalıştırın.

Kaspersky Endpoint Security bilgisayarı taramaya başlayacaktır. Kullanıcı görevin yürütülmesini durdurduysa (mesela bilgisayarı kapatarak), Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır.

Uygulama arabiriminde bir tarama nasıl çalıştırılır

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.

   Tarama görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

   Uygulama arabiriminde yalnızca şu yerel tarama görevlerini yapılandırabilirsiniz: *Tam Tarama*, *Kritik Alan Taraması*, *Özel Tarama*. Kaspersky Security Center Konsolu aracılığıyla eklenen grup görevleri uygulama arabiriminde yapılandırılamaz. Grup görevleri için ⚙ düğmesi görüntülenmez.
3. Tarama görevini yapılandırın (aşağıdaki tabloya bakın).

   Gerekirse, tarama görevi zamanlamasını yapılandırın.
4. Değişikliklerinizi kaydedin.
5. Tarama görevini çalıştırın.

Kaspersky Endpoint Security bilgisayarı taramaya başlayacaktır. Uygulama tarafından, tarama ilerlemesi, taranan dosya sayısı ve kalan tarama süresi görüntülenecektir. **Durdur** düğmesine tıklayarak görevi istediğiniz zaman durdurabilirsiniz.

Bilgisayarı tararken Kaspersky Endpoint Security'nin performansını en üst düzeye çıkarmak için, *Tam Tarama* görevinin gelişmiş ayarlarını yönetebilir ve işlemci kaynaklarının kullanımını sınırlayabilirsiniz.

Kaspersky Security Center'da, uygulamanın performansını optimize etmek için *Tam Tarama* görevi yerine *Arka Plan Taraması* görevini de kullanabilirsiniz. Bu işlem, bilgisayarın güvenlik düzeyini etkilemez. Arka plan taraması yapılandırılamaz.

Sonuç olarak, Kaspersky Endpoint Security bilgisayarı tarar ve bir tehdit algılanırsa uygulama ayarlarında yapılandırılan eylemi gerçekleştirir. Tipik olarak uygulama, virüslü dosyaları temizlemeye çalışır. Sonuç olarak, virüslü dosyalar aşağıdaki durumları alabilir:

- **Ertelendi**. Etkilenen dosya temizlenemedi. Uygulama, bilgisayar yeniden başlatıldıktan sonra virüslü dosyayı siler.
- **Rapora yazıldı**. Etkilenen dosya temizlenemedi. Uygulama, algılanan virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
- **Yazma desteklenmiyor** veya **Yazma hatası**. Etkilenen dosya temizlenemedi. Uygulamanın yazma erişimi yok.
- **Zaten işlendi**. Uygulama daha önce virüslü bir dosya tespit etti. Uygulama, bilgisayar yeniden başlatıldıktan sonra virüslü dosyayı temizler veya siler.

Tarama ayarları

Parametre	Açıklama
Güvenlik düzeyi	Kaspersky Endpoint Security, bir tarama çalıştırmak için farklı ayar grupları kullanabilir. Uygulamada saklanan bu ayar kümelerine *güvenlik seviyeleri* denir: • **Yüksek**. Kaspersky Endpoint Security tüm dosya türlerini tarar. Bileşik dosyaları tararken, uygulama arşivleri, dağıtım paketlerini, ofis formatlarındaki dosyaları tarar, ancak parola korumalı arşivleri taramaz. Bu güvenlik seviyesi ayarlandığında, uygulama **Ayrıntılı tarama** detay seviyesi ile sezgisel analiz kullanır. • **Önerilen**. Kaspersky Endpoint Security tüm dosya türlerini tarar. Bileşik dosyaları tararken, uygulama arşivleri, dağıtım paketlerini, ofis formatlarındaki dosyaları tarar, ancak parola korumalı arşivleri taramaz. Bu güvenlik düzeyi ayarlandığında, uygulama **Normal tarama** ayrıntı düzeyiyle sezgisel analiz kullanır. • **Düşük**. Kaspersky Endpoint Security yalnızca belirtilen dosya biçimlerini tarar. Bileşik dosyaları tararken, uygulama arşivleri, dağıtım paketlerini, ofis formatlarındaki dosyaları tarar, ancak parola korumalı arşivleri taramaz. Bu güvenlik seviyesi ayarlandığında, uygulama **Hızlı tarama** detay seviyesi ile sezgisel analiz kullanır. Ön tanımlı güvenlik düzeylerinden birini seçebilir veya güvenlik düzeyi ayarlarını manuel olarak yapılandırabilirsiniz. Güvenlik düzeyi ayarlarını değiştirirseniz önerilen güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

Parametre	Açıklama
Tehdit algılandığında yapılacak eylem	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler. **Temizle; temizleme başarısız olursa bildir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme başarısız olursa Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler. **Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler. Uygulama, virüslü bir dosyayı temizlemeye veya silmeye başlamadan önce, dosyayı geri yüklemeniz gerekip gerekmediğini veya ileride temizlenebileceğini düşünerek dosyanın bir yedekleme kopyasını oluşturur. Windows Store uygulamasının parçası olan virüslü dosyalar tespit edildiğinde Kaspersky Endpoint Security dosyayı silmeyi dener.
Gelişmiş Temizleme işlemini derhal çalıştır *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bir bilgisayardaki virüs taraması görevi sırasında Gelişmiş Temizleme işlemi yalnızca, bu bilgisayara uygulanan ilkenin özelliklerinde Gelişmiş Temizleme özelliği etkinleştirilmişse gerçekleştirilir. Bu onay kutusu işaretlendiğinde, Kaspersky Endpoint Security etkin virüs bulaşmasını, virüs tarama görevinin yürütülmesi sırasında tespit edildikten hemen sonra temizler. Etkin virüs bulaşması temizlendikten sonra, Kaspersky Endpoint Security kullanıcıya sormadan bilgisayarı yeniden başlatır. Bu onay kutusu işaretlenmezse, Kaspersky Endpoint Security etkin virüs bulaşmasını, virüs tarama görevinin yürütülmesi sırasında tespit edildikten hemen sonra temizlemez. Kaspersky Endpoint Security, yerel uygulama raporlarında ve Kaspersky Security Center tarafında etkin virüs bulaşması olayları oluşturur. Gelişmiş Temizleme özelliği açıkken virüs tarama görevi yeniden çalıştırıldığında, etkin virüs bulaşması temizlenebilir. Böylece sistem yöneticisi Gelişmiş Temizleme işlemini gerçekleştirmek için uygun zamanı seçebilir ve ardından bilgisayarları otomatik olarak yeniden başlatabilir.
Tarama kapsamı	Bir tarama görevi yürütülürken Kaspersky Endpoint Security tarafından taranan nesneler listesi. Tarama kapsamındaki nesneler sistem belleği, çalışan işlemler, önyükleme kesimleri, sistem yedekleme deposu, sabit sürücü, çıkarılabilir sürücü veya ağ sürücüsü, klasör veya dosya içerebilir. Kaspersky Endpoint Security for Windows 12.12'de e-posta, uygulama tarama kapsamından çıkarılmıştır. Gelen ve giden e-posta mesajlarının taranması, Posta Tehdit Koruması bileşeni tarafından gerçekleştirilir. Yönetim eklentisinin önceki bir sürümünü kullanıyorsanız, ilke e-postayı içerse bile uygulama e-postayı tarama kapsamı dışında bırakır.
Tarama zamanlaması	**Manuel**. Taramayı sizin için uygun olan bir zamanda manuel olarak başlatabileceğiniz çalışma modu. **Zamanlamaya göre**. Bu tarama görevi çalışma modunda, uygulama tarama görevini oluşturduğunuz zamanlamaya uygun olarak çalıştırır. Bu tarama görevi çalışma modu seçilirse tarama görevini manuel olarak da başlatabilirsiniz.
Uygulama başladıktan sonra çalışmayı şu kadar ertele N dakika	Taramanın, uygulamanın başlatılmasından sonrasında ertelenmiş olarak başlatılması. İşletim sistemi başlangıcında birçok işlem çalışır, bu nedenle tarama görevini çalıştırmayı Kaspersky Endpoint Security'nin başlatılmasından hemen sonra çalıştırmak yerine ertelemek avantajlıdır.
Atlanmış görevleri çalıştır	Onay kutusu işaretlenirse Kaspersky Endpoint Security, atlanan görevi gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış görevin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Uygulama kaçırılan görevleri yürütme fırsatı bulduğunda, bilgisayar üzerindeki yükü dağıtmak için görevleri belirli bir zaman aralığında rastgele çalıştırır. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan görevleri çalıştırmaz. Bunun yerine, bir sonraki görevi geçerli zamanlamaya uygun olarak yürütür.
Sadece bilgisayar boştayken çalıştır	Bilgisayar kaynakları meşgul olduğunda görevin başlatılması ertelenir. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır. Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.

Parametre	Açıklama
Taramayı farklı çalıştır	Tarama görevi varsayılan olarak haklarını işletim sistemine kaydettiğiniz kullanıcının adıyla çalıştırılır. Koruma kapsamı, ağ sürücülerini veya erişim için özel haklar gerektiren diğer nesneleri içerebilir. Uygulama ayarlarında gerekli haklara sahip kullanıcıyı belirtebilir ve tarama görevini bu kullanıcı hesabının altında gerçekleştirebilirsiniz.
Dosya türleri	Kaspersky Endpoint Security bir uzantısı olmayan dosyaları yürütülebilir dosyalar olarak dikkate alır. Uygulama, taranması için seçtiğiniz dosya türleri ne olursa olsun yürütülebilir dosyaları daima tarar. **Tüm dosyalar**. Bu ayar etkinleştirilirse Kaspersky Endpoint Security, tüm dosyaları istisnasız (tüm formatları ve uzantıları) olarak kontrol eder. **Biçime göre taranan dosyalar**. Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Bir dosyada kötü amaçlı kod taraması yapmadan önce dosyanın iç başlığı, dosyanın biçimini (örneğin, .txt, .doc veya .exe) belirlemek için analiz edilir. Tarama ayrıca belirli dosya uzantılarına sahip dosyaları arar. **Uzantıya göre taranan dosyalar** Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Dosya biçimi daha sonra dosyanın uzantısına göre belirlenir. Varsayılan olarak, Kaspersky Endpoint Security dosyaları kendi biçimlerine göre tarar. Dosyaları uzantıya göre taramak daha az güvenlidir, çünkü kötü amaçlı bir dosya, bulaşma olasılıkları listesinde yer almayan bir uzantıya sahip olabilir (örneğin, `.123`).
Sadece yeni ve değiştirilmiş dosyaları tara	Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.
Bu süreden daha uzun süreyle taranan dosyayı atla: N sn	Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.
Aynı anda birden fazla tarama görevi çalıştırmayın	Daha önce başlatılmış zamanlanmış bir tarama hâlâ çalışıyorsa zamanlanmış tarama görevlerini ertele. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security zamanlanmış tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, 18:00 ve 20:00'de çalışacak şekilde zamanlanmış tarama görevleriniz vardır. 18:00 için zamanlanmış tarama görevi hâlâ çalışıyorsa Kaspersky Endpoint Security, 20:00 tarama görevini erteler. Uygulama, 18:00'de başlatılan görev tamamlandıktan sonra bir tarama çalıştırır. Ancak Kaspersky Endpoint Security, aşağıdaki tarama görevlerinden biri çalışıyor olsa bile hemen bir tarama görevi başlatır: • Çıkarılabilir sürücülerin bağlanır bağlanmaz taranması. • Bağlam Menüsünden Tarama. • Kritik Alan Taraması Bir Güvenlik İhlali Göstergesinin (IoC) tespit edilmesi üzerine başlatılır. Bu onay kutusunun işareti kaldırıldığında, Kaspersky Endpoint Security aynı anda birden çok tarama görevi çalıştırmanıza izin verir. Birden çok tarama görevi çalıştırmak daha fazla bilgisayar kaynağı gerektirir.
Arşivleri tara	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Dağıtım paketlerini tara	Üçüncü taraf uygulamaların dağıtım paketlerinin taranması.
Microsoft Office biçimlerindeki dosyaları tara	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.

Parametre	Açıklama
E-posta biçimindeki dosyaları tara	E-posta formatındaki dosyaları ve e-posta veritabanını tarama. Uygulama, MS Outlook ve Windows Mail posta istemcileri tarafından kullanılan PST ve OST dosyalarının yanı sıra EML dosyalarını da tarar. Kaspersky Endpoint Security, Microsoft Outlook posta istemcisinin 64 bit sürümünü desteklemiyor. Bu, bilgisayarda Microsoft Outlook'un 64 bit sürümü yüklüyse, tarama kapsamına posta dahil edilse bile Kaspersky Endpoint Security'nin Microsoft Outlook dosyalarını (PST ve OST dosyaları) taramayacağı anlamına gelir. Onay kutusu işaretlenirse Kaspersky Endpoint Security, posta biçimli dosyayı bileşenlerine (başlık, gövde ve ekler) ayırır ve bunlarda tehdit taraması yapar. Bu onay kutusu işaretlenmezse Kaspersky Endpoint Security, posta biçimi dosyasını tek bir dosya olarak tarar. PST veya OST dosyalarında kötü amaçlı bir nesne tespit edildiğinde, Kaspersky Endpoint Security seçilen eyleme göre (örneğin, dosyanın temizleme veya silinmesi) bu nesneyi zararsız hale getirir. Diğer e-posta istemcilerinin dosyalarında (örneğin Mozilla Thunderbird) zararlı nesneler algılanırsa Kaspersky Endpoint Security, e-posta iletilerinizin istenmeden silinmesini önlemek için bu dosyaları temizlemez veya silmez. Kaspersky Endpoint Security, etkin tehditler listesine yalnızca algılanan nesneler hakkında bilgi ekler. Posta istemcinizin kullanıcı arabiriminde eklerinde zararlı dosyalar bulunan e-postaları silmek için gerekli adımları uygulamanız gerekir. Herhangi bir nedenle zararlı nesneler içeren iletiler o anda silinemiyorsa bu tehditleri Kaspersky Endpoint Security kullanıcı arabiriminde algılanan nesneleri tarama istisnaları listesine ekleyerek işleyebilirsiniz.
Parola korumalı arşivleri tara	Onay kutusu işaretlendiğinde, uygulama parola korumalı arşivleri tarar. Arşivdeki dosyalar taranmadan önce parolanızı girmeniz istenir. Onay kutusu işaretlenmediği takdirde, uygulama parola korumalı arşivlerin taramasını atlar.
Büyük bileşik dosya paketlerini açma	Bu onay kutusu işaretlendiğinde, uygulama boyutları belirtilen değeri aşan birleşik dosyaları taramaz. Bu onay kutusu işaretlenmediğinde, uygulama her boyuttaki birleşik dosyaları tarar. Uygulama, onay kutusunun seçili olup olmadığından bağımsız olarak arşivlerden çıkarılan büyük dosyaları tarar.
Makine öğrenimi ve imza analizi	Makine öğrenimi ve imza analizi yöntemi, bilinen tehditlerin açıklamalarını ve etkisiz duruma getirme yollarını içeren Kaspersky Endpoint Security veritabanlarını kullanır. Bu yöntemi kullanan koruma kabul edilebilir en düşük güvenlik düzeyini sağlar. Kaspersky uzmanları makine öğreniminin ve imza analizinin her zaman etkin olmasını önerir.
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. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
iSwift Teknolojisi *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.
iChecker Teknolojisi *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).

Bilgisayara bağlandığında çıkarılabilir sürücüleri tarama

Kaspersky Endpoint Security, çalıştırdığınız veya kopyaladığınız tüm dosyaları, dosya çıkarılabilir bir sürücüde olsa bile tarar (Dosya Tehdidi Koruması bileşeni). Virüslerin ve diğer kötü amaçlı yazılımların yayılmasını önlemek için çıkarılabilir sürücüler bilgisayara bağlandıklarında otomatik olarak taranacak şekilde yapılandırma yapabilirsiniz. Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa Kaspersky Endpoint Security, dosyaları siler. Bileşen, makine öğrenimi, sezgisel analiz (yüksek seviye) ve imza analizi uygulayan taramalar çalıştırarak bilgisayarı güvende tutar. Kaspersky Endpoint Security, iSwift ve iChecker tarama optimizasyon teknolojilerini de kullanır. Bu teknolojiler her zaman açıktır ve devre dışı bırakılamaz.

Çıkarılabilir sürücü taraması Yönetim Konsolu'nda (MMC) nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Yerel Görevler** → **Çıkarılabilir Sürücü Taraması** seçimini yapın.
4. **Çıkarılabilir sürücü bağlantısında yapılacak eylem** açılır listesinde, **Ayrıntılı Tarama** veya **Hızlı Tarama** arasından seçim yapın.
5. Çıkarılabilir sürücü taraması için gelişmiş seçenekleri yapılandırın (aşağıdaki tabloya bakın).
6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Çıkarılabilir sürücü taraması nasıl yapılandırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Çıkarılabilir Sürücüler Taraması** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Çıkarılabilir Sürücüler Taraması ETKİN** anahtarını kullanın.
6. **Tarama türü** bloğunda **Detaylı Tarama** veya **Hızlı Tarama'yı** seçin.
7. Çıkarılabilir sürücü taraması için gelişmiş seçenekleri yapılandırın (aşağıdaki tabloya bakın).
8. Değişikliklerinizi kaydedin.

Çıkarılabilir sürücü taraması uygulama arabiriminde nasıl yapılandırılır

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.
3. Bilgisayara bağlandıktan sonra çıkarılabilir sürücü taramalarını etkinleştirmek veya devre dışı bırakmak için **Çıkarılabilir Sürücü Taraması** geçiş düğmesini kullanın.

4. Çıkarılabilir sürücü taraması için gelişmiş seçenekleri yapılandırın (aşağıdaki tabloya bakın).

5. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security, belirtilen maksimum boyuttan daha büyük olmayan çıkarılabilir sürücüler için bir çıkarılabilir sürücü taraması yapar. *Çıkarılabilir Sürücü Taraması* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanılmasını yasaklamış demektir.

Çıkarılabilir sürücü taraması görev ayarları

Parametre	Açıklama
Tarama türü	**Ayrıntılı Tarama**. Bu seçenek belirlenirse Kaspersky Endpoint Security, çıkarılabilir bir sürücü bağlandığında bileşik nesneler, arşivler, dağıtım paketleri ve Office biçimlerindeki dosyalar dahil olmak üzere tüm dosyaları tarar. Kaspersky Endpoint Security, posta biçimindeki ya da parola korumalı arşivleri taramaz. **Hızlı Tarama**. Bu seçenek belirlenirse bir çıkarılabilir sürücü bağlandıktan sonra Kaspersky Endpoint Security sadece virüse karşı en hassas belirli formatlardaki dosyaları tarar ve bileşik nesnelerin paketini açmaz.
Maksimum sürücü boyutu (MB)	Bu onay kutusu işaretlendiğinde Kaspersky Endpoint Security, belirtilen maksimum sürücü boyutundan daha büyük olmayan çıkarılabilir sürücülerde seçilen eylemi gerçekleştirir. Çıkarılabilir sürücünün boyutu yapılandırılan değeri aşarsa Kaspersky Endpoint Security taramayı atlar. Onay kutusunun işareti kaldırıldığında, Kaspersky Endpoint Security seçilen eylemi herhangi bir boyuttaki çıkarılabilir sürücülerde gerçekleştirir.
Tarama ilerleme çubuğunu gizle	Onay kutusu işaretlenirse Kaspersky Endpoint Security, çıkarılabilir sürücü taramasının ilerlemesini ayrı bir pencerede ve **Görevler** bölümünde görüntüler. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, çıkarılabilir sürücü taramasını arka planda gerçekleştirir.
Kullanıcıların taramayı durdurmasını engelle	Bu onay kutusu işaretlenirse, Kaspersky Endpoint Security'nin yerel arabirimindeki çıkarılabilir sürücü taraması için **Görevler** bölümündeki **Durdur** düğmesi ve çıkarılabilir sürücü taraması penceresindeki **Durdur** düğmesi kullanılamaz.

Arka plan taraması

Arka Plan Taraması, Kaspersky Endpoint Security'nin kullanıcıya bildirim görüntülemeyen bir tarama modudur. Arka Plan Taraması diğer tarama türlerine göre (tam tarama gibi) daha az bilgisayar kaynağı gerektirir. Bu modda, Kaspersky Endpoint Security başlangıç nesnelerini, önyükleme kesimini, sistem belleğini ve sistem bölümünü tarar.

Bilgisayar kaynaklarını korumak için tam tarama görevi yerine bir arka plan taraması görevi kullanılması önerilir. Bu işlem, bilgisayarın güvenlik düzeyini etkilemez. Bu görevler aynı tarama kapsamına sahiptir. Uygulama, bilgisayardaki yükü optimize etmek için aynı anda bir Tam Tarama görevi ve bir Arka Plan Taraması görevi çalıştırmaz. Halihazırda bir Tam Tarama görevi çalıştırdıysanız Kaspersky Endpoint Security, Tam Tarama görevi tamamlandıktan sonra yedi gün boyunca bir Arka Plan Tarama görevi başlatmaz.

Arka plan taraması aşağıdaki durumlarda başlatılır:

- Antivirüs veritabanı güncellemesinden sonra.
- Kaspersky Endpoint Security başlatıldıktan 30 dakika sonra.
- Altı saatte bir.
- Bilgisayar beş dakika veya daha uzun süre boşta kaldığında (bilgisayar kilitli veya ekran koruyucu açık).

Aşağıdaki koşullardan biri gerçekleştiğinde bilgisayar uyku durumundayken arka plan taraması kesintiye uğrar:

- Bilgisayar etkin moda geçti.

  Arka plan taraması on gündür çalıştırılmamışsa tarama kesintiye uğramaz.

- Bilgisayar (dizüstü bilgisayar) pil moduna geçti.

Bir arka plan taraması yaparken Kaspersky Endpoint Security, içeriği OneDrive bulut depolama ortamında olan dosyaları taramaz.

Yönetim Konsolu'nda (MMC) arka plan taraması nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Yerel Görevler** → **Arka Plan Taraması** seçimini yapın.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Arka Plan Taramasını çalıştır** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da arka plan taraması nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Dosya Tehdidi Koruması** bölümüne gidin.
5. **Arka Plan Taraması** altında, arka plan taramasını etkinleştirmek veya devre dışı bırakmak için **Arka Plan Taraması ETKİN** geçiş anahtarını kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde arka plan taraması nasıl etkinleştirilir

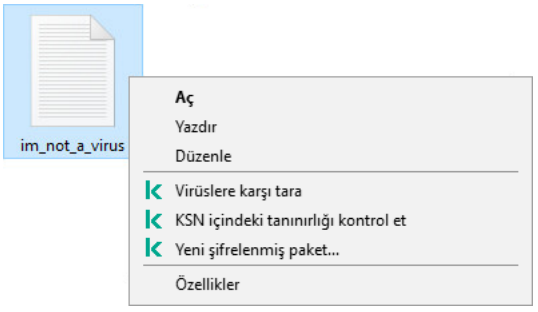
1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Arka Plan Taraması** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Arka plan taraması görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

Bağlam menüsünden tarama

Kaspersky Endpoint Security, bağlam menüsünden virüslere ve diğer zararlı yazılımlara karşı dosyaları teker teker taramanıza izin verir (aşağıdaki resme bakın).

Kaspersky Endpoint Security, Bağlam menüsünden tarama gerçekleştirirken içeriği OneDrive bulut depolama alanında bulunan dosyaları taramaz.



Bağlam menüsünden tarama

Yönetim Konsolu'nda (MMC) Bağlam Menüsünden Tarama nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Yerel Görevler** → **Bağlam Menüsünden Tarama** seçimini yapın.
4. Bağlam Menüsünden Taramayı yapılandırma (aşağıdaki tabloya bakın).
5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Bağlam Menüsünden Tarama nasıl yapılandırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Dosya Tehdidi Koruması** bölümüne gidin.
5. Bağlam Menüsünden Tara altında, **Bağlam Menüsünden Tara** için yapılandırma yapın (aşağıdaki tabloya bakın).
6. Değişikliklerinizi kaydedin.

Uygulama arabirimde Bağlam Menüsünden Tarama nasıl yapılandırılır

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.

3. Bağlam Menüsünden Taramayı yapılandırma (aşağıdaki tabloya bakın).

4. Değişikliklerinizi kaydedin.

Bağlam Menüsünden Tarama görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanılmasını yasaklamış demektir.

Bağlam Menüsünden Tarama görev ayarları

Parametre	Açıklama
Güvenlik düzeyi	Kaspersky Endpoint Security, bir tarama çalıştırmak için farklı ayar grupları kullanabilir. Uygulamada saklanan bu ayar kümelerine *güvenlik seviyeleri* denir: • **Yüksek**. Kaspersky Endpoint Security tüm dosya türlerini tarar. Bileşik dosyaları tararken, uygulama arşivleri, dağıtım paketlerini, ofis formatlarındaki dosyaları tarar, ancak parola korumalı arşivleri taramaz. Bu güvenlik seviyesi ayarlandığında, uygulama **Ayrıntılı tarama** detay seviyesi ile sezgisel analiz kullanır. • **Önerilen**. Kaspersky Endpoint Security tüm dosya türlerini tarar. Bileşik dosyaları tararken, uygulama arşivleri, dağıtım paketlerini, ofis formatlarındaki dosyaları tarar, ancak parola korumalı arşivleri taramaz. Bu güvenlik düzeyi ayarlandığında, uygulama **Normal tarama** ayrıntı düzeyiyle sezgisel analiz kullanır. • **Düşük**. Kaspersky Endpoint Security yalnızca belirtilen dosya biçimlerini tarar. Bileşik dosyaları tararken, uygulama arşivleri, dağıtım paketlerini, ofis formatlarındaki dosyaları tarar, ancak parola korumalı arşivleri taramaz. Bu güvenlik seviyesi ayarlandığında, uygulama **Hızlı tarama** detay seviyesi ile sezgisel analiz kullanır.
Tehdit algılandığında yapılacak eylem	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler. **Temizle; temizleme başarısız olursa bildir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme başarısız olursa Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler. **Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
Dosya türleri	Kaspersky Endpoint Security bir uzantısı olmayan dosyaları yürütülebilir dosyalar olarak dikkate alır. Uygulama, taranması için seçtiğiniz dosya türleri ne olursa olsun yürütülebilir dosyaları daima tarar. **Tüm dosyalar**. Bu ayar etkinleştirilirse Kaspersky Endpoint Security, tüm dosyaları istisnasız (tüm formatları ve uzantıları) olarak kontrol eder. **Biçime göre taranan dosyalar**. Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Bir dosyada kötü amaçlı kod taraması yapmadan önce dosyanın iç başlığı, dosyanın biçimini (örneğin, .txt, .doc veya .exe) belirlemek için analiz edilir. Tarama ayrıca belirli dosya uzantılarına sahip dosyaları arar. **Uzantıya göre taranan dosyalar** Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Dosya biçimi daha sonra dosyanın uzantısına göre belirlenir. Varsayılan olarak, Kaspersky Endpoint Security dosyaları kendi biçimlerine göre tarar. Dosyaları uzantıya göre taramak daha az güvenlidir, çünkü kötü amaçlı bir dosya, bulaşma olasılıkları listesinde yer almayan bir uzantıya sahip olabilir (örneğin, `.123`).
Sadece yeni ve değiştirilmiş dosyaları tara	Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.
Bu süreden daha uzun süreyle taranan dosyayı atla: N sn	Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.
Arşivleri tara	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Dağıtım paketlerini tara	Bu onay kutusu, dağıtım paketlerinin taranmasını etkinleştirir veya devre dışı bırakır.
Microsoft Office biçimlerindeki dosyaları tara	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.

Parametre	Açıklama
E-posta biçimindeki dosyaları tara	E-posta formatındaki dosyaları ve e-posta veritabanını tarama. Uygulama, MS Outlook ve Windows Mail posta istemcileri tarafından kullanılan PST ve OST dosyalarının yanı sıra EML dosyalarını da tarar. Kaspersky Endpoint Security, Microsoft Outlook posta istemcisinin 64 bit sürümünü desteklemiyor. Bu, bilgisayarda Microsoft Outlook'un 64 bit sürümü yüklüyse, tarama kapsamına posta dahil edilse bile Kaspersky Endpoint Security'nin Microsoft Outlook dosyalarını (PST ve OST dosyaları) taramayacağı anlamına gelir. Onay kutusu işaretlenirse Kaspersky Endpoint Security, posta biçimli dosyayı bileşenlerine (başlık, gövde ve ekler) ayırır ve bunlarda tehdit taraması yapar. Bu onay kutusu işaretlenmezse Kaspersky Endpoint Security, posta biçimi dosyasını tek bir dosya olarak tarar. PST veya OST dosyalarında kötü amaçlı bir nesne tespit edildiğinde, Kaspersky Endpoint Security seçilen eyleme göre (örneğin, dosyanın temizleme veya silinmesi) bu nesneyi zararsız hale getirir. Diğer e-posta istemcilerinin dosyalarında (örneğin Mozilla Thunderbird) zararlı nesneler algılanırsa Kaspersky Endpoint Security, e-posta iletilerinizin istenmeden silinmesini önlemek için bu dosyaları temizlemez veya silmez. Kaspersky Endpoint Security, etkin tehditler listesine yalnızca algılanan nesneler hakkında bilgi ekler. Posta istemcinizin kullanıcı arabiriminde eklerinde zararlı dosyalar bulunan e-postaları silmek için gerekli adımları uygulamanız gerekir. Herhangi bir nedenle zararlı nesneler içeren iletiler o anda silinemiyorsa bu tehditleri Kaspersky Endpoint Security kullanıcı arabiriminde algılanan nesneleri tarama istisnaları listesine ekleyerek işleyebilirsiniz.
Parola korumalı arşivleri tara	Onay kutusu işaretlendiğinde, uygulama parola korumalı arşivleri tarar. Arşivdeki dosyalar taranmadan önce parolanızı girmeniz istenir. Onay kutusu işaretlenmediği takdirde, uygulama parola korumalı arşivlerin taramasını atlar.
Büyük bileşik dosya paketlerini açma	Bu onay kutusu işaretlendiğinde, uygulama boyutları belirtilen değeri aşan birleşik dosyaları taramaz. Bu onay kutusu işaretlenmediğinde, uygulama her boyuttaki birleşik dosyaları tarar. Uygulama, onay kutusunun seçili olup olmadığından bağımsız olarak arşivlerden çıkarılan büyük dosyaları tarar.
Makine öğrenimi ve imza analizi	Makine öğrenimi ve imza analizi yöntemi, bilinen tehditlerin açıklamalarını ve etkisiz duruma getirme yollarını içeren Kaspersky Endpoint Security veritabanlarını kullanır. Bu yöntemi kullanan koruma kabul edilebilir en düşük güvenlik düzeyini sağlar. Kaspersky uzmanları makine öğreniminin ve imza analizinin her zaman etkin olmasını önerir.
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. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
iSwift Teknolojisi	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.
iChecker Teknolojisi	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).

Uygulama Bütünlüğü Kontrolü

Kaspersky Endpoint Security, uygulama modüllerinde bozukluk veya değişiklik olup olmadığını denetler. Örneğin bir uygulama kitaplığı yanlış bir dijital imzaya sahipse kitaplık bozuk olarak değerlendirilir. *Uygulama Bütünlüğü Kontrolü* görevinin amacı uygulama dosyalarının denetlenmesidir. Kaspersky Endpoint Security bir zararlı nesne tespit ettiği halde onu etkisiz hale getirmezse *Uygulama Bütünlüğü Kontrolü* görevini çalıştırın.

Uygulama Bütünlüğü Kontrolü görevini hem Kaspersky Security Center Web Console'da hem de Yönetim Konsolu'nda oluşturabilirsiniz. Kaspersky Security Center Cloud Console üzerinde bir görev oluşturmak mümkün değildir.

Uygulama bütünlüğü ihlalleri şu durumlarda oluşabilir:

- Bir zararlı nesne Kaspersky Endpoint Security'nin dosyalarını değiştirdiğinde. Böyle bir durumda, işletim sisteminin araçlarını kullanarak Kaspersky Endpoint Security'nin geri yüklenmesi prosedürünü uygulayın. Geri yükleme sonrasında bilgisayarda bir tam tarama gerçekleştirin ve bütünlük denetimini tekrarlayın.
- Dijital imzanın süresi dolduğunda. Bu durumda Kaspersky Endpoint Security'yi güncelleyin.

Bir uygulama bütünlüğü kontrolü Yönetim Konsolu (MMC) aracılığıyla nasıl çalıştırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Uygulama Bütünlüğü Kontrolü** öğesini seçin.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görevi başlatmak için bir zamanlama ayarlayın, örneğin manuel olarak ya da bir virüs salgını tespit edildiğinde.

4. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Bilgisayara virüs bulaştıktan sonra bütünlük denetimi*.

5. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz. Sonuç olarak Kaspersky Endpoint Security uygulamanın bütünlüğünü denetleyecektir. İsterseniz görev özelliklerinden de bir uygulama bütünlüğü kontrolü zamanlaması yapılandırabilirsiniz (aşağıdaki tabloya bakın).

Bir uygulama bütünlüğü kontrolü Web Console aracılığıyla nasıl çalıştırılır

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Uygulama Bütünlüğü Kontrolü** öğesini seçin.

   c. **Görev adı** alanına kısa bir açıklama girin, örneğin, *Bilgisayara virüs bulaştıktan sonra uygulamanın bütünlüğünü kontrol et*.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Görevin yanındaki onay kutusunu seçin.

Sonuç olarak Kaspersky Endpoint Security uygulamanın bütünlüğünü denetleyecektir. İsterseniz görev özelliklerinden de bir uygulama bütünlüğü kontrolü zamanlaması yapılandırabilirsiniz (aşağıdaki tabloya bakın).

Uygulama arabiriminde bütünlük denetimi nasıl yapılır

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.

2. Görev listesi açılır; *Uygulama Bütünlüğü Kontrolü* görevini seçin ve **Çalıştır**'a tıklayın.

Sonuç olarak Kaspersky Endpoint Security uygulamanın bütünlüğünü denetleyecektir. İsterseniz görev özelliklerinden de bir uygulama bütünlüğü kontrolü zamanlaması yapılandırabilirsiniz (aşağıdaki tabloya bakın). *Uygulama Bütünlüğü Kontrolü* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

Parametre	Açıklama
Tarama zamanlaması	**Manuel**. Taramayı sizin için uygun olan bir zamanda manuel olarak başlatabileceğiniz çalışma modu. **Zamanlamaya göre**. Bu tarama görevi çalışma modunda, uygulama tarama görevini oluşturduğunuz zamanlamaya uygun olarak çalıştırır. Bu tarama görevi çalışma modu seçilirse tarama görevini manuel olarak da başlatabilirsiniz.
Atlanmış görevleri çalıştır	Onay kutusu işaretlenirse Kaspersky Endpoint Security, atlanan görevi gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış görevin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Uygulama kaçırılan görevleri yürütme fırsatı bulduğunda, bilgisayar üzerindeki yükü dağıtmak için görevleri belirli bir zaman aralığında rastgele çalıştırır. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan görevleri çalıştırmaz. Bunun yerine, bir sonraki görevi geçerli zamanlamaya uygun olarak yürütür.
Sadece bilgisayar boştayken çalıştır	Bilgisayar kaynakları meşgul olduğunda görevin başlatılması ertelenir. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır. Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.

Tarama kapsamının düzenlenmesi

Tarama kapsamı Kaspersky Endpoint Security'nin görevi yürütürken taradığı klasörlerin ve yolların bir listesidir. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

Tarama kapsamını düzenlemek için *Özel Tarama* görevini kullanmanızı öneririz. Kaspersky uzmanları, *Tam Tarama* ve *Kritik Alanları Tarama* görevinin tarama kapsamını değiştirmemenizi öneriyor.

Kaspersky Endpoint Security, tarama kapsamının bir parçası olarak şu önceden tanımlanmış nesnelere sahiptir:

- **Sistem belleği**.
- **Çalışan işlemler ve Başlangıç Nesneleri**.

  Sistem başlangıcında çalıştırılan işlemler ve uygulama yürütülebilir dosyaları tarafından kullanılan bellek.
- **Sürücü önyükleme kesimleri**.

  Sabit sürücü ve çıkarılabilir sürücü önyükleme kesimleri.
- **Sistem Yedeği**.

  Sistem Birim Bilgisi klasörünün içeriği.
- **Tüm harici cihazlar**.
- **Tüm sabit sürücüler**.
- **Tüm ağ sürücüleri**.

Kaspersky Endpoint Security for Windows 12.12'de e-posta, uygulama tarama kapsamından çıkarılmıştır. Gelen ve giden e-posta mesajlarının taranması, Posta Tehdit Koruması bileşeni tarafından gerçekleştirilir. Yönetim eklentisinin önceki bir sürümünü kullanıyorsanız, ilke e-postayı içerse bile uygulama e-postayı tarama kapsamı dışında bırakır.

Ağ sürücülerini veya paylaşılan klasörleri taramak için ayrı bir tarama görevi oluşturmanızı öneririz. *Kötü Amaçlı Yazılım Taraması* görevinin ayarlarında, bu sürücüye yazma erişimi olan bir kullanıcı belirleyin; bu, tespit edilen tehditleri azaltmak için gereklidir. Ağ sürücüsünün bulunduğu sunucunun kendi güvenlik araçları varsa, bu sürücü için tarama görevini çalıştırmayın. Bu şekilde, nesneyi iki kez kontrol etmekten kaçınabilir ve sunucunun performansını artırabilirsiniz.

Klasörleri veya dosyaları tarama kapsamından çıkarmak için klasörü veya dosyayı güvenilir bölgeye ekleyin.

Yönetim Konsolu'nda (MMC) bir tarama kapsamı nasıl düzenlenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. Gereken tarama görevini seçin ve görev özellikleri penceresini açmak için çift tıklayın.
   Gerekirse *Kötü Amaçlı Yazılım Taraması* görevi oluşturun.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.
5. **Tarama kapsamı** bölümünde **Ayarlar**'a tıklayın.
6. Açılan pencerede, tarama kapsamına eklemek veya koruma kapsamının dışında tutmak istediğiniz nesneleri seçin.
7. Tarama kapsamına yeni bir nesne eklemek isterseniz:
   a. **Ekle**'ye tıklayın.
   b. **Nesne** alanına, dosya veya klasöre giden yolu girin.
      Maskeler kullanarak:
      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
      - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.
      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

      Maskeleri bir dosya veya klasör yolunda herhangi bir yerde kullanabilirsiniz. Örneğin, tarama kapsamının bilgisayardaki tüm kullanıcı hesapları için İndirilenler klasörünü içermesini istiyorsanız, `C:\Users\*\Downloads\` maskesini girin.

      Bilgisayarın dosya kaynakları listesindeki **Bu Bilgisayar** nesnesi şu nesneleri içerir: **Tüm sabit sürücüler**, **Tüm ağ sürücüleri** ve **Tüm çıkarılabilir sürücüler**.

Tarama kapsamındaki nesneler listesinden, bir nesneyi silmeden taramaların dışında bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir tarama kapsamı nasıl düzenlenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. Tarama görevine tıklayın.

   Görev özellikleri penceresi açılır. Gerekirse *Kötü Amaçlı Yazılım Taraması* görevi oluşturun.

3. **Uygulama ayarları** sekmesini seçin.

4. **Tarama kapsamı** bölümünde, tarama kapsamına eklemek veya kapsamın dışında tutmak istediğiniz nesneleri seçin.

5. Tarama kapsamına yeni bir nesne eklemek isterseniz:

   a. **Ekle**'ye tıklayın.

   b. Klasör veya dosyanın yolunu girin.

      Maskeler kullanarak:

      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

      - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

      Maskeleri bir dosya veya klasör yolunda herhangi bir yerde kullanabilirsiniz. Örneğin, tarama kapsamının bilgisayardaki tüm kullanıcı hesapları için İndirilenler klasörünü içermesini istiyorsanız, `C:\Users\*\Downloads\` maskesini girin.

   Tarama kapsamındaki nesneler listesinden, bir nesneyi silmeden taramaların dışında bırakabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir tarama kapsamı nasıl düzenlenir

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesi açılır; buradan *Özel Tarama* görevini seçin ve **Seç**'e tıklayın.

   Diğer görevler için de tarama kapsamını düzenleyebilirsiniz. Kaspersky uzmanları, *Tam Tarama* ve *Kritik Alanları Tarama* görevinin tarama kapsamını değiştirmemenizi öneriyor.
3. Açılan pencerede, tarama kapsamına eklemek istediğiniz nesneleri seçin.
4. Değişikliklerinizi kaydedin.

Tarama görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

Zamanlanmış bir tarama çalıştırma

Kötü Amaçlı Yazılım Taraması görevini kullanarak kötü amaçlı yazılım taraması yapmak zaman alıcı olabilir ve Kaspersky Endpoint Security'nin bilgisayar kaynaklarını daha fazla kullanmasına neden olabilir. Bu nedenle, diğer uygulamaların performansına olan etkiyi en aza indirmek için görevi çalıştırmak üzere en uygun zamanı seçmeniz önerilir.

Örneğin, kuruluşunuzdaki çalışanlar sabit bir çalışma programına göre çalışıyorsa, bilgisayar taramasının gece veya hafta sonları çalışacak şekilde ayarlanmasını sağlayabilirsiniz. Görevi herhangi bir nedenle çalıştırmak mümkün değilse (örneğin bilgisayar o sırada kapalıysa) atlanan görevi mümkün olur olmaz otomatik olarak çalışacak şekilde yapılandırabilirsiniz. Bu işlev, sabahları bilgisayar açıldığında kullanıcı bilgisayarındaki uygulamaların yavaşlamasına neden olabileceğinden dikkatli kullanılmalıdır.

İhtiyaçlarınıza uygun en uygun tarama zamanlamasını belirleyemiyorsanız, taramanın aşağıdaki özel koşullardan biri karşılandığında çalışacak şekilde yapılandırabilirsiniz:

- Bir veritabanı güncellemesinden sonra.

  Kaspersky Endpoint Security, bilgisayar taramasını güncellenmiş imza veritabanlarıyla çalıştırır.
- Uygulama başlatıldıktan sonra.

  Kaspersky Endpoint Security, uygulamanın başlatılmasından belirli bir süre sonra bilgisayarda bir tarama gerçekleştirir. İşletim sistemi başlangıcında birçok işlem çalışır, bu nedenle tarama görevini çalıştırmayı Kaspersky Endpoint Security'nin başlatılmasından hemen sonra çalıştırmak yerine ertelemek avantajlıdır.
- Wake-on-LAN özelliği.

  Kaspersky Endpoint Security, bilgisayar kapalı olsa bile zamanlamaya göre bir bilgisayar taraması gerçekleştirir. Bunu yapmak için uygulama, işletim sisteminin Wake-on-LAN özelliğini kullanır. Wake-on-LAN özelliği, yerel ağ üzerinden özel bir sinyal göndererek bilgisayarın uzaktan açılmasını sağlar. Wake-on-LAN özelliğini kullanmak için BIOS ayarlarından LAN'da Uyandırmayı etkinleştirmeniz gerekir.

  Taramayı çalıştırmayı Wake-on-LAN özelliğini kullanarak sadece Kaspersky Security Center'daki *Kötü Amaçlı Yazılım Taraması* görevi için yapılandırabilirsiniz. Uygulama arabiriminde bilgisayarı taramak için Wake-on-LAN özelliğini etkinleştiremezsiniz.
- Bilgisayar boştayken.

  Kaspersky Endpoint Security, ekran koruyucu etkinken veya ekran kilitliyken zamanlamaya göre bir bilgisayar taraması gerçekleştirir. Kullanıcı bilgisayarın kilidini açarsa Kaspersky Endpoint Security taramayı duraklatır. Bu durumda, Tam Tarama işleminin tamamlanması birkaç gün sürebilir.

- Görev atlandığında.

  Kaspersky Endpoint Security, atlanan görevi mümkün olur olmaz çalıştırır. Örneğin, zamanlanmış görevin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Uygulama kaçırılan görevleri yürütme fırsatı bulduğunda, bilgisayar üzerindeki yükü dağıtmak için görevleri belirli bir zaman aralığında rastgele çalıştırır.

Web Console'da ve Cloud Console'da bir tarama zamanlaması nasıl yapılandırılır

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Tarama görevine tıklayın.

   Görev özellikleri penceresi açılır.

3. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

4. Tarama görevi zamanlamasını yapılandırın.

5. Seçilen sıklığa bağlı olarak görev çalışma zamanlamasını belirten gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde tarama zamanlaması nasıl yapılandırılır

Tarama zamanlamasını, yalnızca bilgisayara bir ilke uygulanmadığında yapılandırabilirsiniz. İlke uygulanan bilgisayarlar için Kaspersky Security Center'da *Kötü Amaçlı Yazılım Taraması* görev zamanlaması yapılandırabilirsiniz.

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.

2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.

   Bir Tam Tarama, Kritik Alanları Tarama veya Bütünlük Denetimi çalıştırmak için bir zamanlama yapılandırabilirsiniz. Özel Taramayı yalnızca manuel olarak çalıştırabilirsiniz.

3. **Tarama zamanlaması**'na tıklayın.

4. Açılan pencerede, tarama görevi çalıştırma zamanlamasını yapılandırın.

5. Seçilen sıklığa bağlı olarak görev çalışma zamanlamasını belirten gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

6. Değişikliklerinizi kaydedin.

Tarama zamanlama ayarları

Parametre	Açıklama
Tarama zamanlaması	**Manuel**. Taramayı sizin için uygun olan bir zamanda manuel olarak başlatabileceğiniz çalışma modu. **Zamanlamaya göre**. Bu tarama görevi çalışma modunda, uygulama tarama görevini oluşturduğunuz zamanlamaya uygun olarak çalıştırır. Bu tarama görevi çalışma modu seçilirse tarama görevini manuel olarak da başlatabilirsiniz.
Uygulama başladıktan sonra çalışmayı şu kadar ertele N dakika	Taramanın, uygulamanın başlatılmasından sonrasında ertelenmiş olarak başlatılması. İşletim sistemi başlangıcında birçok işlem çalışır, bu nedenle tarama görevini çalıştırmayı Kaspersky Endpoint Security'nin başlatılmasından hemen sonra çalıştırmak yerine ertelemek avantajlıdır.

Parametre	Açıklama
Atlanmış görevleri çalıştır	Onay kutusu işaretlenirse Kaspersky Endpoint Security, atlanan görevi gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış görevin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Uygulama kaçırılan görevleri yürütme fırsatı bulduğunda, bilgisayar üzerindeki yükü dağıtmak için görevleri belirli bir zaman aralığında rastgele çalıştırır. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan görevleri çalıştırmaz. Bunun yerine, bir sonraki görevi geçerli zamanlamaya uygun olarak yürütür.
Sadece bilgisayar boştayken çalıştır	Bilgisayar kaynakları meşgul olduğunda görevin başlatılması ertelenir. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır. Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.
Görev başlatmalar için otomatik olarak rastgele hale getirilmiş gecikme kullan *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu onay kutusu seçildiğinde, görev tam olarak zamanlamaya göre değil, belirli bir aralıkta rastgele yürütülür, yani görevin başlangıç zamanları yayılır. Rastgele başlangıç zamanları, görev zamanında çalıştırıldığında çok sayıda bilgisayarın aynı anda Yönetim Sunucusu'na erişmesinin önlenmesine yardımcı olur. Rastgele başlangıç zamanları aralığı, görevin atandığı bilgisayarların sayısına bağlı olarak görev oluşturulduğunda otomatik olarak hesaplanır. Ardından, görev her zaman hesaplanan başlangıç zamanında çalıştırılır. Ancak görev ayarları değiştirildiğinde veya görev manuel olarak çalıştırıldığında, hesaplanan başlangıç zamanı değişir. Onay kutusunun işareti kaldırıldığında, görev tam olarak zamanlanan saatte çalıştırılır.
İki görevi başlatırken verilecek rastgele aralık üst sınırı (dk.)	Bu onay kutusu işaretlendiğinde, görev bilgisayarlarda belirli bir zaman dilimi içinde rastgele bir zamanda çalıştırılır. Rastgele başlangıç zamanları, görev zamanında çalıştırıldığında çok sayıda bilgisayarın aynı anda Yönetim Sunucusu'na erişmesinin önlenmesine yardımcı olur. Onay kutusunun işareti kaldırıldığında, görev tam olarak zamanlanan saatte çalıştırılır.
Görev şundan uzun süredir çalışıyorsa durdur (dk) *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır. Görev yürütme süresini azaltmak için, örneğin tarama kapsamını yapılandırabilir ya da taramayı optimize edebilirsiniz.
Görev başlatılmadan önce Wake-on-LAN işlevini kullanarak cihazları aç (dakika) *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu onay kutusu işaretlendiğinde, görev çalıştırılmadan önce bilgisayarın işletim sistemine başlatmayı tamamlaması için belirli bir bekleme süresi verilir. Varsayılan bekleme süresi 5 dakikadır. Görevi, kapalı bilgisayarlar da dahil olmak üzere tüm bilgisayarlarda çalıştırmak istiyorsanız bu onay kutusunu seçin.
Görev gerçekleştirildikten sonra cihazları kapat *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu onay kutusu işaretlenirse görev tamamlandıktan sonra bilgisayar kapatılır. Örneğin, Cuma günleri mesai saatlerinden sonra bilgisayarı taramak için bu işlevi etkinleştirebilirsiniz. Görev tamamlandığında, uygulama bilgisayarı hafta sonu için kapatır.
Görevi duraklat	Önceden zamanlanmış bir görevin yürütülmesinin duraklatılacağı zaman aralığını belirtebilirsiniz. Belirtilen süre dolduğunda, görev devam edecektir. Örneğin, yoğun kullanım dönemlerinde Kaspersky Endpoint Security'nin bilgisayarınızın performansına olan etkisini en aza indirmek için bu gerekli olabilir.
Zamanlamayı şu tarihten itibaren devre dışı bırak	Onay kutusu işaretlenirse Kaspersky Endpoint Security, belirtilen tarihten itibaren zamanlanmış görevi çalıştırmayı durdurur. Görev **Manuel** moduna ayarlanacaktır.

Taramayı farklı bir kullanıcı olarak çalıştırma

Tarama görevi varsayılan olarak haklarını işletim sistemine kaydettiğiniz kullanıcının adıyla çalıştırılır. Koruma kapsamı, ağ sürücülerini veya erişim için özel haklar gerektiren diğer nesneleri içerebilir. Uygulama ayarlarında gerekli haklara sahip kullanıcıyı belirtebilir ve tarama görevini bu kullanıcı hesabının altında gerçekleştirebilirsiniz.

Aşağıdaki taramaları farklı bir kullanıcı olarak çalıştırabilirsiniz:

- Kritik Alanları Tarama.
- Tam Tarama.

- Özel Tarama.
- Bağlam Menüsünden Tarama.

Bir Çıkarılabilir sürücü taraması, bir Arka plan taraması ya da bir Bütünlük denetimi çalıştırmak için kullanıcı haklarını yapılandıramazsınız.

Yönetim Konsolu'nda (MMC) nasıl farklı bir kullanıcı olarak bir tarama çalıştırılır

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, **Görevler** sekmesini seçin.
4. Gereken tarama görevini seçin ve görev özellikleri penceresini açmak için çift tıklayın.
5. Görev özellikleri penceresinde **Hesap** bölümünü seçin.
6. Bir tarama görevini çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin.
7. Değişikliklerinizi kaydedin.

Web Console'da veya Cloud Console'da farklı bir kullanıcı olarak tarama nasıl çalıştırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.
2. Tarama görevine tıklayın.

   Görev özellikleri penceresi açılır.
3. **Ayarlar** sekmesini seçin.
4. **Hesap** bloğunda, **Ayarlar** düğmesine tıklayın.
5. Bir tarama görevini çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde nasıl farklı bir kullanıcı olarak bir tarama çalıştırılır

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.
3. Görev özelliklerinden **Gelişmiş ayarlar** → **Taramayı farklı çalıştır** seçimini yapın.
4. Açılan pencerede, bir tarama görevini çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin.
5. Değişikliklerinizi kaydedin.

Tarama görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

Tarama optimizasyonu

Bilgisayar taranırken işlemci kullanımının sınırlandırılması

Kötü Amaçlı Yazılım Taraması görevi çalıştırılırken işlemci kullanımını sınırlayabilirsiniz. Bu, bilgisayarınızın taranma süresini artırabilir.

Yönetim Konsolu'nda (MMC) bilgisayar taranırken işlemci kullanımını sınırlandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
4. **Performans** bölümünde, **Tarama görevleri için işlemci kullanımını sınırla** onay kutusunu seçin ve işlemci kaynak tüketiminin ortalama değerini yüzde olarak girin.
5. Değişikliklerinizi kaydedin.

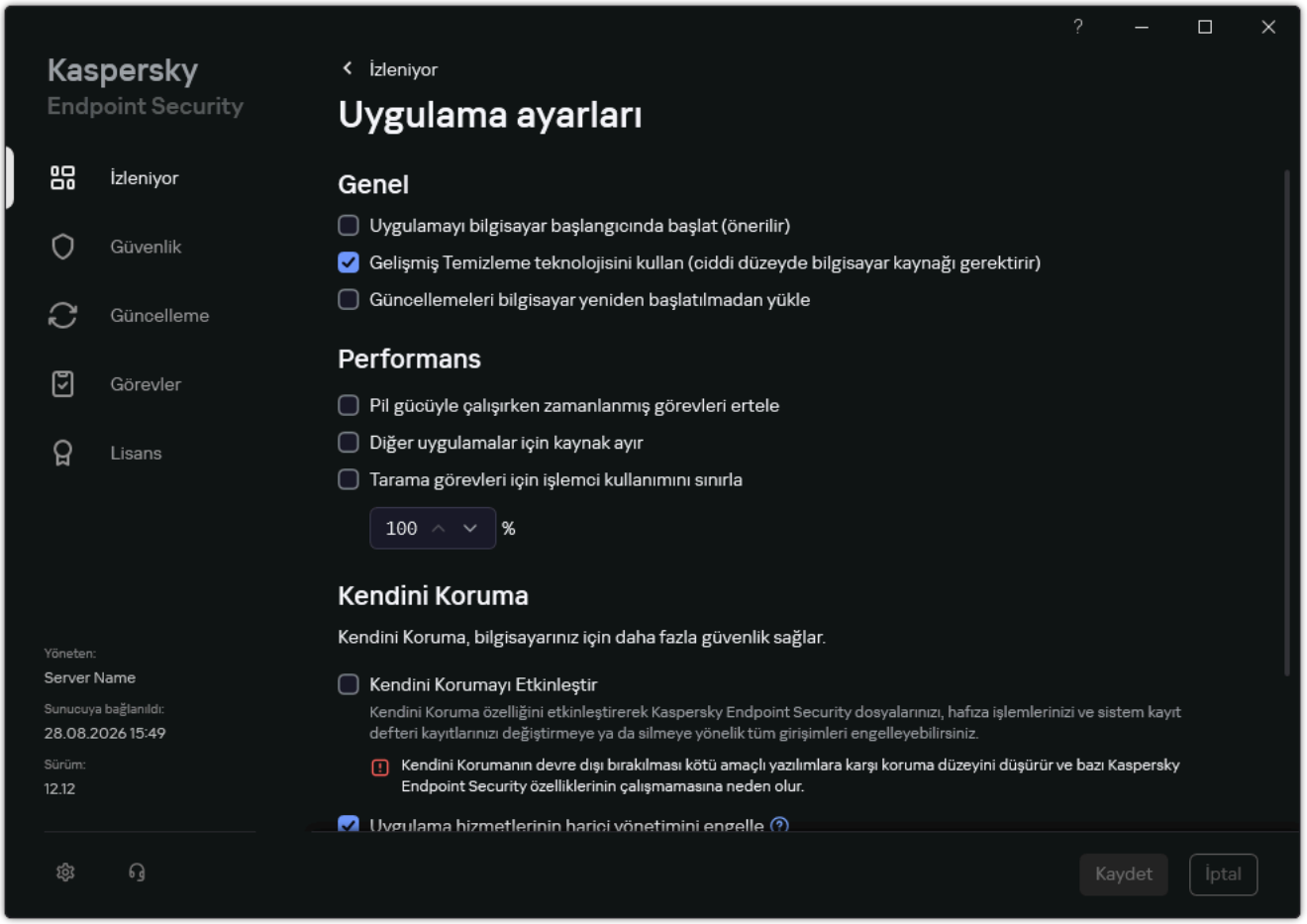
Web Konsolu'nda bilgisayar taranırken CPU kullanımını sınırlandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Performans** bölümüne gidin.
5. **Tarama görevleri için işlemci kullanımını sınırla** bölümünde, anahtarını **Tarama görevleri için işlemci kullanımını sınırla** olarak ayarlayın ve İşlemci kaynak tüketiminin ortalama değerini yüzde olarak girin.
6. Değişikliklerinizi kaydedin.

Uygulama arayüzünde bilgisayar taranırken CPU kullanımını sınırlandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. **Performans** bölümünde, **Tarama görevleri için işlemci kullanımını sınırla** onay kutusunu seçin ve işlemci kaynak tüketiminin ortalama değerini yüzde olarak girin.

4. Değişikliklerinizi kaydedin.

Kötü Amaçlı Yazılım Taraması için gelişmiş görev ayarlarının yapılandırılması.

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.

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.

iChecker ve iSwift teknolojilerini de etkinleştirebilirsiniz. iChecker ve iSwift teknolojileri, en son taramadan beri değiştirilmemiş dosyaları hariç tutarak dosyaları taramanın hızını optimize edebilir.

Yönetim Konsolu'nda (MMC) tarama nasıl optimize edilir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. Gereken tarama görevini seçin ve görev özellikleri penceresini açmak için çift tıklayın.

   Gerekirse *Kötü Amaçlı Yazılım Taraması* görevi oluşturun.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.
5. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, tarama görevi ayarları penceresini açar.
6. **Optimizasyon** bloğunda, tarama ayarlarını yapılandırın:

   - **Sadece yeni ve değiştirilmiş dosyaları tara**. Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.

     Yeni dosyaların türe göre taranmasını da yapılandırabilirsiniz. Örneğin, tüm dağıtım paketlerini tarayabilir ve yalnızca yeni arşivleri ve ofis dosyalarını tarayabilirsiniz.

   - **Bu süreden daha uzun süreyle taranan dosyaları atla N sn**. Görev yürütme süresini sınırlama. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.

   - **Aynı anda birden fazla tarama görevi çalıştırmayın**. Daha önce başlatılmış zamanlanmış bir tarama hâlâ çalışıyorsa zamanlanmış tarama görevlerini ertele. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security zamanlanmış tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, 18:00 ve 20:00'de çalışacak şekilde zamanlanmış tarama görevleriniz vardır. 18:00 için zamanlanmış tarama görevi hâlâ çalışıyorsa Kaspersky Endpoint Security, 20:00 tarama görevini erteler. Uygulama, 18:00'de başlatılan görev tamamlandıktan sonra bir tarama çalıştırır.
7. **Diğer**'e tıklayın.

   Bu, birleşik dosyaları tarama ayarları penceresini açar.
8. **Boyut sınırı** bloğunda, **Büyük bileşik dosya paketlerini açma** onay kutusunu işaretleyin. Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.

   Kaspersky Endpoint Security, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük dosyaları tarar.
9. **Tamam**'a tıklayın.
10. **Ek** sekmesine gidin.

11. **Tarama teknolojileri** bloğunda, tarama sırasında kullanmak istediğiniz teknolojilerin adının yanındaki onay kutularını seçin:

    - **iSwift Teknolojisi**. Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.

    - **iChecker Teknolojisi**. Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).

12. Değişikliklerinizi kaydedin.

Web Konsolu'nda tarama nasıl optimize edilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. Tarama görevine tıklayın.

   Görev özellikleri penceresi açılır. Gerekirse *Kötü Amaçlı Yazılım Taraması* görevi oluşturun.

3. **Uygulama ayarları** sekmesini seçin.

4. **Tehdit algılandığında yapılacak eylem** bloğunda, **Sadece yeni ve değiştirilmiş dosyaları tara** onay kutusunu işaretleyin. Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.

   Yeni dosyaların türe göre taranmasını da yapılandırabilirsiniz. Örneğin, tüm dağıtım paketlerini tarayabilir ve yalnızca yeni arşivleri ve ofis dosyalarını tarayabilirsiniz.

5. **Tarama optimizasyonu** bloğunda, **Büyük bileşik dosya paketlerini açma** onay kutusunu işaretleyin. Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.

   > Kaspersky Endpoint Security, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük dosyaları tarar.

6. **Aynı anda birden fazla tarama görevi çalıştırmayın** onay kutusunu seçin. Daha önce başlatılmış zamanlanmış bir tarama hâlâ çalışıyorsa zamanlanmış tarama görevlerini ertele. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security zamanlanmış tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, 18:00 ve 20:00'de çalışacak şekilde zamanlanmış tarama görevleriniz vardır. 18:00 için zamanlanmış tarama görevi hâlâ çalışıyorsa Kaspersky Endpoint Security, 20:00 tarama görevini erteler. Uygulama, 18:00'de başlatılan görev tamamlandıktan sonra bir tarama çalıştırır.

7. **Gelişmiş ayarlar** bloğundan **Şundan daha uzun süre taranan dosyayı atla (sn):** N saniyeden onay kutusunu işaretleyin. Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.

8. Değişikliklerinizi kaydedin.

Uygulama arabiriminde tarama nasıl optimize edilir

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.
2. Görev listesinden tarama görevini seçin ve ⚙ düğmesine tıklayın.
3. **Gelişmiş ayarlar**'a tıklayın.
4. **Optimizasyon** bloğunda, tarama ayarlarını yapılandırın:
   - **Sadece yeni ve değiştirilmiş dosyaları tara**. Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.

     Yeni dosyaların türe göre taranmasını da yapılandırabilirsiniz. Örneğin, tüm dağıtım paketlerini tarayabilir ve yalnızca yeni arşivleri ve ofis dosyalarını tarayabilirsiniz.
   - **Bu süreden daha uzun süreyle taranan dosyayı atla: N saniye**. Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.
   - **Aynı anda birden fazla tarama görevi çalıştırmayın**. Daha önce başlatılmış zamanlanmış bir tarama hâlâ çalışıyorsa zamanlanmış tarama görevlerini ertele. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security zamanlanmış tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, 18:00 ve 20:00'de çalışacak şekilde zamanlanmış tarama görevleriniz vardır. 18:00 için zamanlanmış tarama görevi hâlâ çalışıyorsa Kaspersky Endpoint Security, 20:00 tarama görevini erteler. Uygulama, 18:00'de başlatılan görev tamamlandıktan sonra bir tarama çalıştırır.
5. **Boyut sınırı** bloğunda, **Büyük bileşik dosya paketlerini açma** onay kutusunu işaretleyin. Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.

   Kaspersky Endpoint Security, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük dosyaları tarar.
6. **Tarama teknolojileri** bloğunda, tarama sırasında kullanmak istediğiniz teknolojilerin adının yanındaki onay kutularını seçin:
   - **iSwift Teknolojisi**. Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.
   - **iChecker Teknolojisi**. Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).
7. Değişikliklerinizi kaydedin.

Tarama görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

Veritabanlarını ve uygulama yazılım modüllerini güncelleme

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.

Güncellemeler işlevselliği (anti-virüs imza güncellemeleri ve kod temeli güncellemeleri sağlama dahil olmak üzere) ABD'de yazılımda kullanılabilir olmayabilir.

Düzenli güncellemeler için geçerli bir lisans gerekir. Geçerli bir lisans yoksa, güncellemeyi günde sadece bir kez gerçekleştirebilirsiniz.

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, proxy sunucusu ayarlarını yapılandırmanız gerekir.

Güncellemeler, HTTPS protokolü üzerinden indirilir. HTTPS protokolü üzerinden güncellemeleri indirmek mümkün olmadığında HTTP protokolü de kullanılabilir.

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.

Veritabanları eskiyse, güncelleme paketi çok büyük olabilir ve ek internet trafiğine (onlarca MB) neden olabilir.

Kaspersky Endpoint Security veritabanlarının geçerli durumuyla ilgili bilgiler, ana uygulama penceresinde veya imleci bildirim alanındaki uygulamanın simgesinin üzerine getirdiğinizde gördüğünüz araç ipucunda görüntülenir.

Güncelleme sonuçları ve güncelleme görevinin gerçekleştirilmesi sırasında gerçekleşen tüm olaylarla ilgili bilgiler Kaspersky Endpoint Security raporuna kaydedilir.

Uygulama Light Agent modunda çalışıyorsa, uygulama veritabanlarının ve modüllerinin güncellenmesinde özel hususlar söz konusudur.

Veritabanı ve uygulama modülü güncelleme senaryoları

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.

Aşağıdaki nesneler kullanıcıların bilgisayarlarında güncellenir:

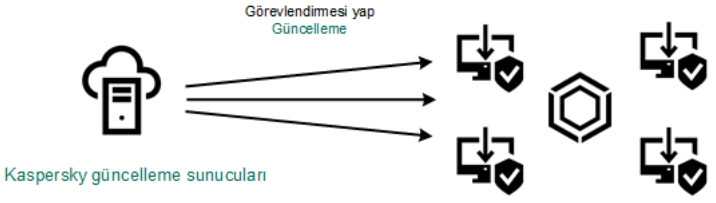
- Anti-virüs veritabanları. Anti-virüs veritabanları; zararlı yazılım imzalarının veritabanlarını, ağ saldırılarının açıklamasını, şüpheli ve kimlik avı yapan İnternet adreslerinin veritabanlarını, reklam pencerelerinin veritabanlarını, spam veritabanlarını ve diğer verileri içerir.

- Uygulama modülleri. Modül güncellemeleri, uygulamadaki zayıf noktaları ortadan kaldırmayı ve bilgisayar koruma yöntemlerini geliştirmeyi amaçlar. Modül güncellemeleri, uygulama bileşenlerinin davranışını değiştirebilir ve yeni özellikler ekleyebilir.

Kaspersky Endpoint Security, veritabanlarını ve uygulama modüllerini güncelleme işlemi için aşağıdaki durumları destekler:

- Kaspersky sunucuları üzerinden güncelleme.

  Kaspersky güncelleme sunucuları birçok farklı ülkede bulunmaktadır. Bu sayede güncelleme işlemlerinde yüksek güvenilirlik sağlanır. Güncelleme bir sunucu üzerinden gerçekleştirilemiyorsa Kaspersky Endpoint Security bir sonraki sunucuya geçiş yapar.



Kaspersky sunucuları üzerinden güncelleme

- Merkezi güncelleme.

  Merkezi güncelleme işlemleri, dış İnternet trafiğini azaltır ve güncellemelerin rahat bir şekilde izlenebilmesini sağlar.

  Merkezi güncelleme, aşağıdaki adımları içerir:

  1. Kuruluşun ağındaki bir veri havuzuna güncelleme paketi indirme.

     Güncelleme paketi veri havuzuna, *Güncellemeleri Yönetim Sunucusu veri havuzuna indir* adlı Yönetim Sunucusu görevi tarafından indirilir.

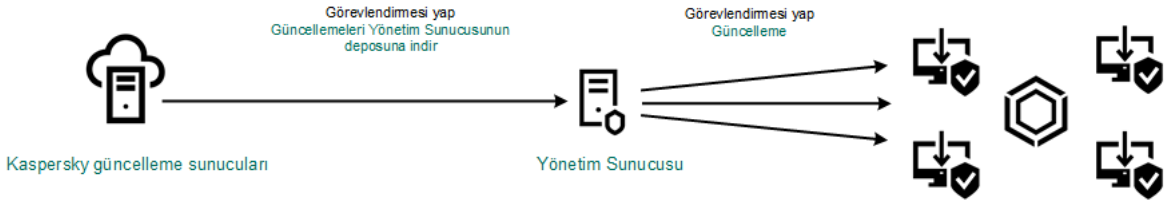
  2. Güncelleme paketini bir paylaşılan klasöre indirin (isteğe bağlı).

Güncelleme paketini paylaşılan bir klasöre aşağıdaki yöntemleri kullanarak indirebilirsiniz:

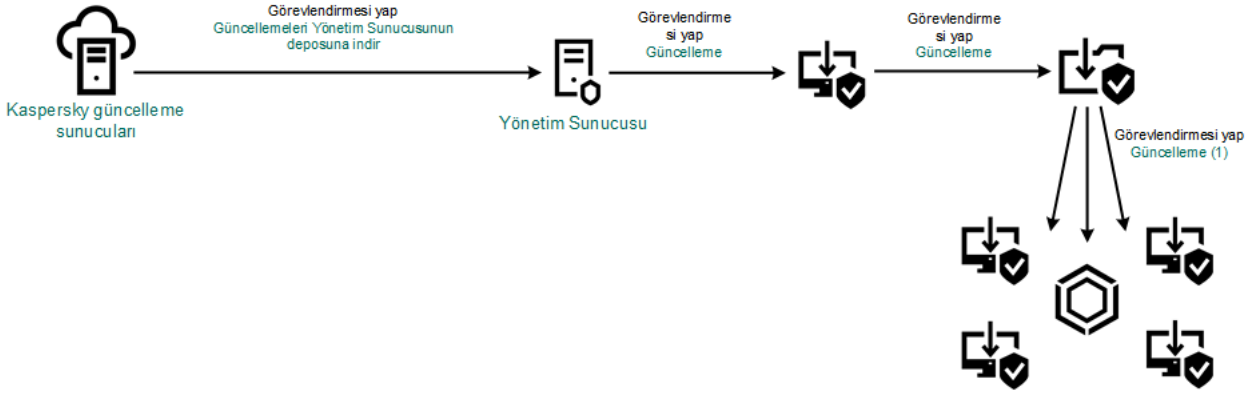
- Kaspersky Endpoint Security *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini kullanma. Görev, yerel şirket ağındaki bilgisayarlardan biri için tasarlanmıştır.
- Kaspersky Update Utility'yi Kullanma. Kaspersky Update Utility'yi kullanma hakkında ayrıntılı bilgi için Kaspersky Bilgi Bankası 'na bakın.

3. Güncelleme paketini istemci bilgisayarlara dağıtın.

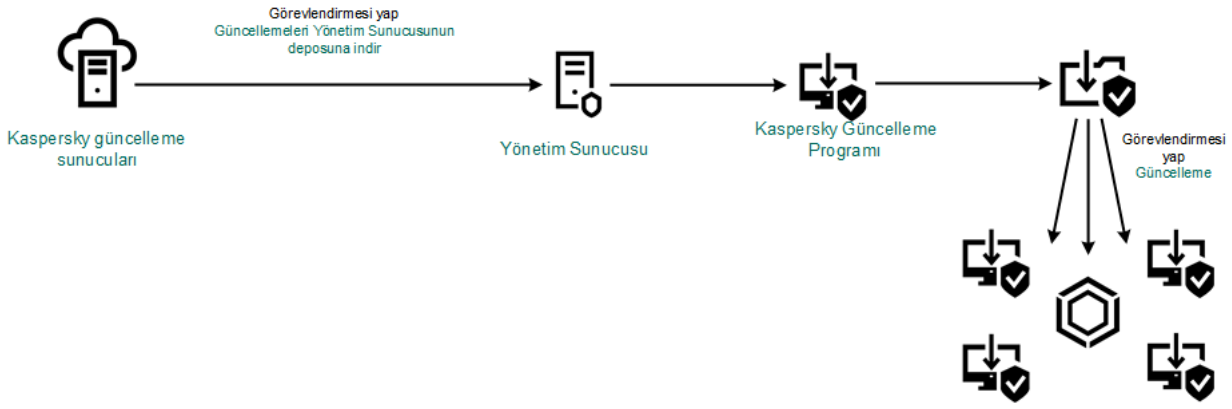
   Güncelleme paketi, Kaspersky Endpoint Security *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi ile istemci bilgisayarlara dağıtılır. Her bir yönetim grubu için sınırsız sayıda güncelleme görevi oluşturabilirsiniz.



Bir sunucu veri havuzu üzerinden güncelleme



Bir paylaşım klasörü üzerinden güncelleme



Kaspersky Update Utility aracıyla güncelleme

Kaspersky Security Center için varsayılan güncelleme kaynakları listesi, Kaspersky Security Center Yönetim Sunucusunu ve Kaspersky güncelleme sunucularını içerir. Kaspersky Security Center Cloud Console için varsayılan güncelleme kaynakları listesi dağıtım noktalarını ve Kaspersky güncelleme sunucularını içerir. Dağıtım noktaları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Cloud Console Yardım içeriğine bakın. Listeye başka güncelleme kaynakları da ekleyebilirsiniz. HTTP/FTP sunucuları ve paylaşım klasörlerini güncelleme kaynakları olarak belirtebilirsiniz. Bir güncelleme kaynağı üzerinden güncelleme yapılmıyorsa Kaspersky Endpoint Security bir sonraki kaynağa geçiş yapar.

Güncellemeler, Kaspersky güncelleme sunucularından veya standart ağ iletişim kurallarının geçerli olduğu diğer FTP veya HTTP sunucularından indirilir. Güncelleme kaynağına erişmek için proxy sunucusu bağlantısı gerekiyorsa proxy sunucusu ayarlarını Kaspersky Endpoint Security ilkesi ayarlarında belirtin.

Bir sunucu veri havuzu üzerinden güncelleme

İnternet trafiğini düşük tutmak için kuruluşun LAN ağındaki bilgisayarların veritabanları ve uygulama modülleri güncellemelerini bir sunucu veri havuzu üzerinden gerçekleştirilmek üzere yapılandırabilirsiniz. Bu amaçla Kaspersky Security Center, Kaspersky güncelleme sunucularından bir güncelleme paketini veri havuzuna (FTP veya HTTP sunucusu, ağ veya yerel klasör) indirmelidir. Böylelikle kuruluşun LAN ağındaki diğer bilgisayarlar, ilgili güncelleme paketini sunucu veri havuzundan alabilir.

Aşağıdaki adımları uygulayarak veritabanı ve uygulama modüllerini bir sunucu veri havuzu üzerinden güncellenecek şekilde yapılandırma:

1. Bir güncelleme paketini Yönetim Sunucusu veri havuzuna indirilecek şekilde yapılandırın (*Güncellemeleri Yönetim Sunucusu veri havuzuna indir* görevi).

   Güncellemeleri Yönetim Sunucusu veri havuzuna indir görevi, Yönetim Sunucusu hızlı başlangıç sihirbazı tarafından otomatik olarak oluşturulur ve bu görevden yalnızca bir adet bulunur. Varsayılan olarak, Kaspersky Security Center güncelleme paketini `\\<server name>\KLSHARE\Updates` klasörüne kopyalar. Güncellemeleri Yönetim Sunucusu deposuna indirme hakkında daha fazla bilgi için lütfen Kaspersky Security Center Yardım bölümüne bakın.

2. Kuruluşun LAN ağındaki diğer bilgisayarları veritabanı ve uygulama modülü güncellemelerini belirtilen sunucu veri havuzu üzerinden yapacak şekilde yapılandırma (*Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi).

   Yönetim Konsolu'nda (MMC) belirtilen sunucu depolama alanından Kaspersky Endpoint Security güncellemesi nasıl yapılandırılır

   1. Kaspersky Security Center Yönetim Konsolu'nu açın.

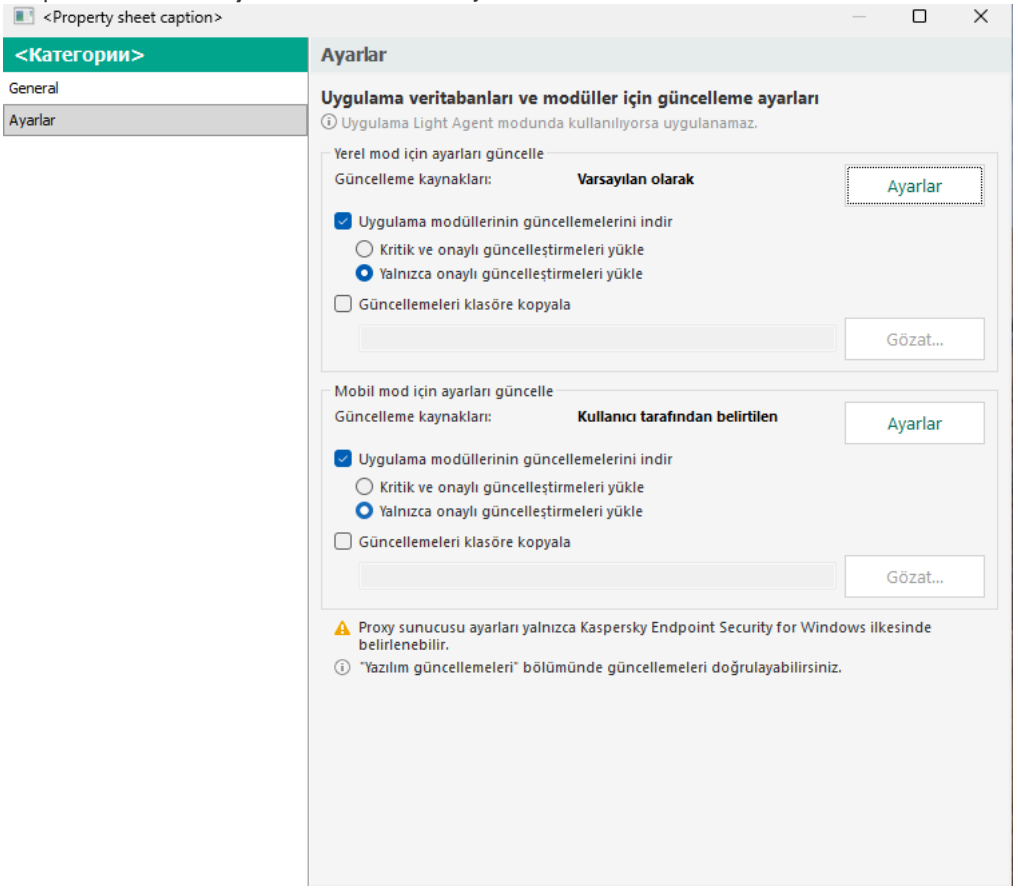
      Konsol ağacında **Görevler**'i seçin.

   2. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

      Görev özellikleri penceresi açılır.

      Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Veritabanlarının ve uygulama modüllerinin güncellemesi görev ayarları

4. **Yerel mod için ayarları güncelle** bloğunda, **Ayarlar** düğmesine tıklayın.

5. Güncelleme kaynakları listesinde, **Kaspersky Security Center** kaynağından güncellemenin etkinleştirildiğinden emin olun. Ayrıca, **Kaspersky Security Center** kaynağı en yüksek önceliğe sahip olmalıdır.

6. Gerekirse güncelleme kaynaklarını ekleyin:

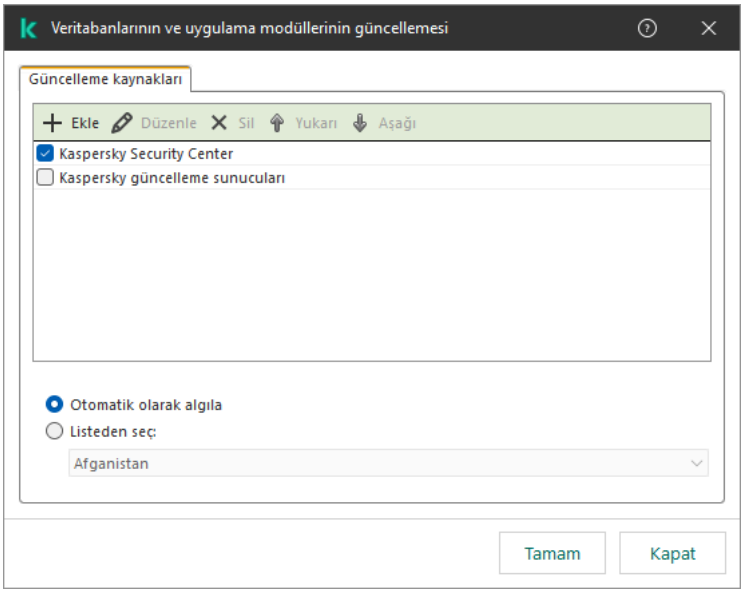
   a. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

   b. **Güncelleme kaynakları** alanında, Kaspersky Security Center'ın Kaspersky sunucularından aldığı güncelleme paketini kopyalayacağı FTP veya HTTP sunucusu, ağ klasörü ya da yerel klasör adresini belirtin.

   > Güncelleme kaynağının adresi, güncellemelerin sunucu depolama alanına indirilmesini yapılandırırken **Güncellemelerin depolanacağı klasör** alanında belirttiğiniz adresle eşleşmelidir (*Güncellemeleri Yönetim Sunucusu veri havuzuna indir* görevi).

   c. **Tamam**'a tıklayın.

Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.



Güncelleme kaynakları

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

8. Görev özellikleri penceresinde, **Zamanlama** bölümünü seçin ve görev çalışma modunu yapılandırın.

9. Varsayılan olarak, Kaspersky Endpoint Security görevi manuel modda çalıştırır.

10. Değişikliklerinizi kaydedin.

Web Console'da belirtilen sunucu depolama alanından Kaspersky Endpoint Security güncellemesi nasıl yapılandırılır

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Güncelleme** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Güncelleme görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Güncelleme* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. **Uygulama ayarları** → **Yerel mod** sekmesini seçin.

4. Güncelleme kaynakları listesinde, **Kaspersky Security Center** kaynağından güncellemenin etkinleştirildiğinden emin olun. Ayrıca, **Kaspersky Security Center** kaynağı en yüksek önceliğe sahip olmalıdır.

5. Gerekirse güncelleme kaynaklarını ekleyin:

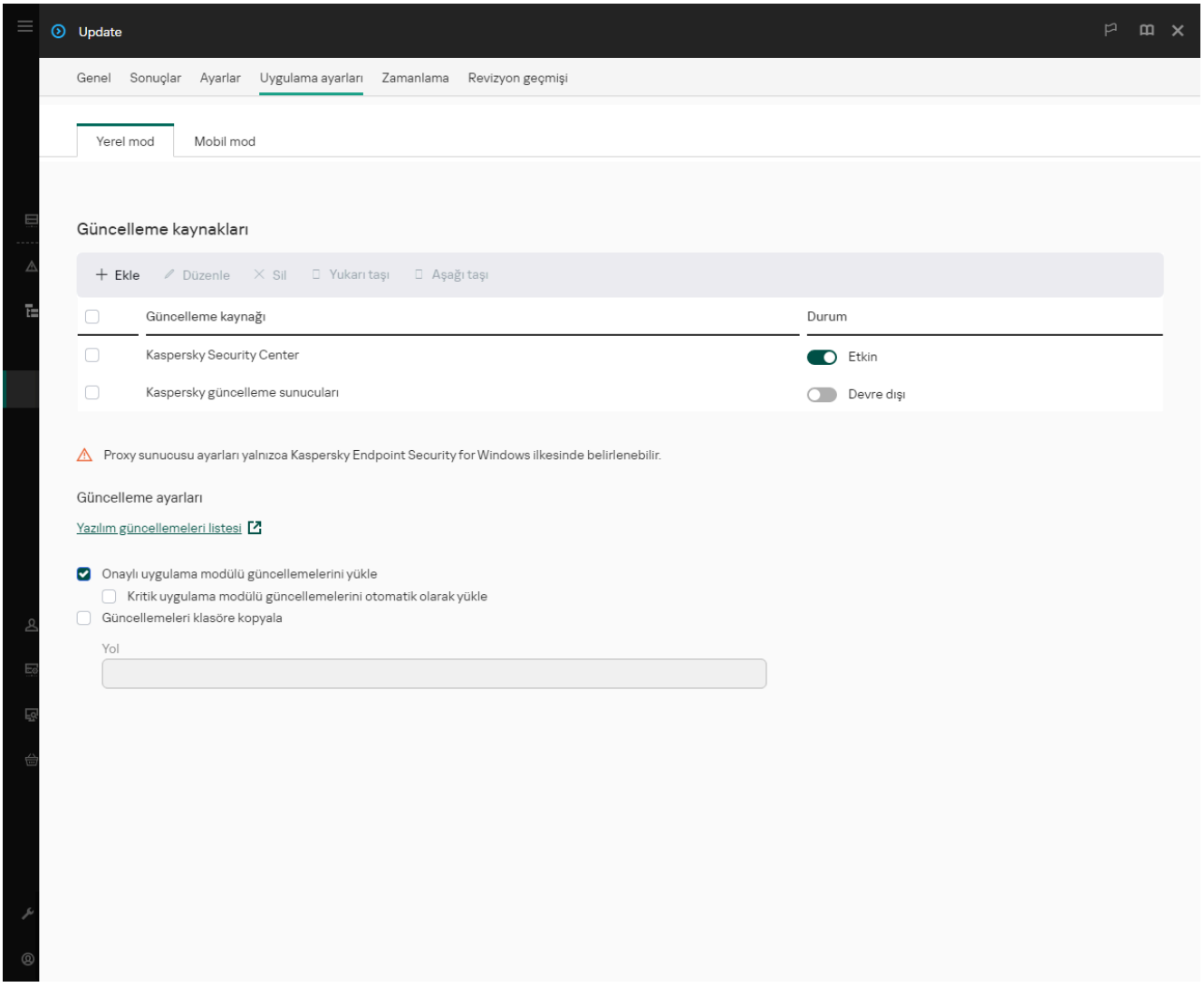
   a. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

   b. **Güncelleme kaynakları** alanında, Kaspersky Security Center'ın Kaspersky sunucularından aldığı güncelleme paketini kopyalayacağı FTP veya HTTP sunucusu, ağ klasörü ya da yerel klasör adresini belirtin.

   > Güncelleme kaynağının adresi, güncellemelerin sunucu depolama alanına indirilmesini yapılandırırken **Güncellemelerin depolanacağı klasör** alanında belirttiğiniz adresle eşleşmelidir (*Güncellemeleri Yönetim Sunucusu veri havuzuna indir* görevi).

   c. **Kaydet**'e tıklayın.

Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.



Güncelleme kaynakları

6. **Yukarı taşı** ve **Aşağı taşı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

7. Görev özellikleri penceresinde, **Zamanlama** bölümünü seçin ve görev çalışma modunu yapılandırın.

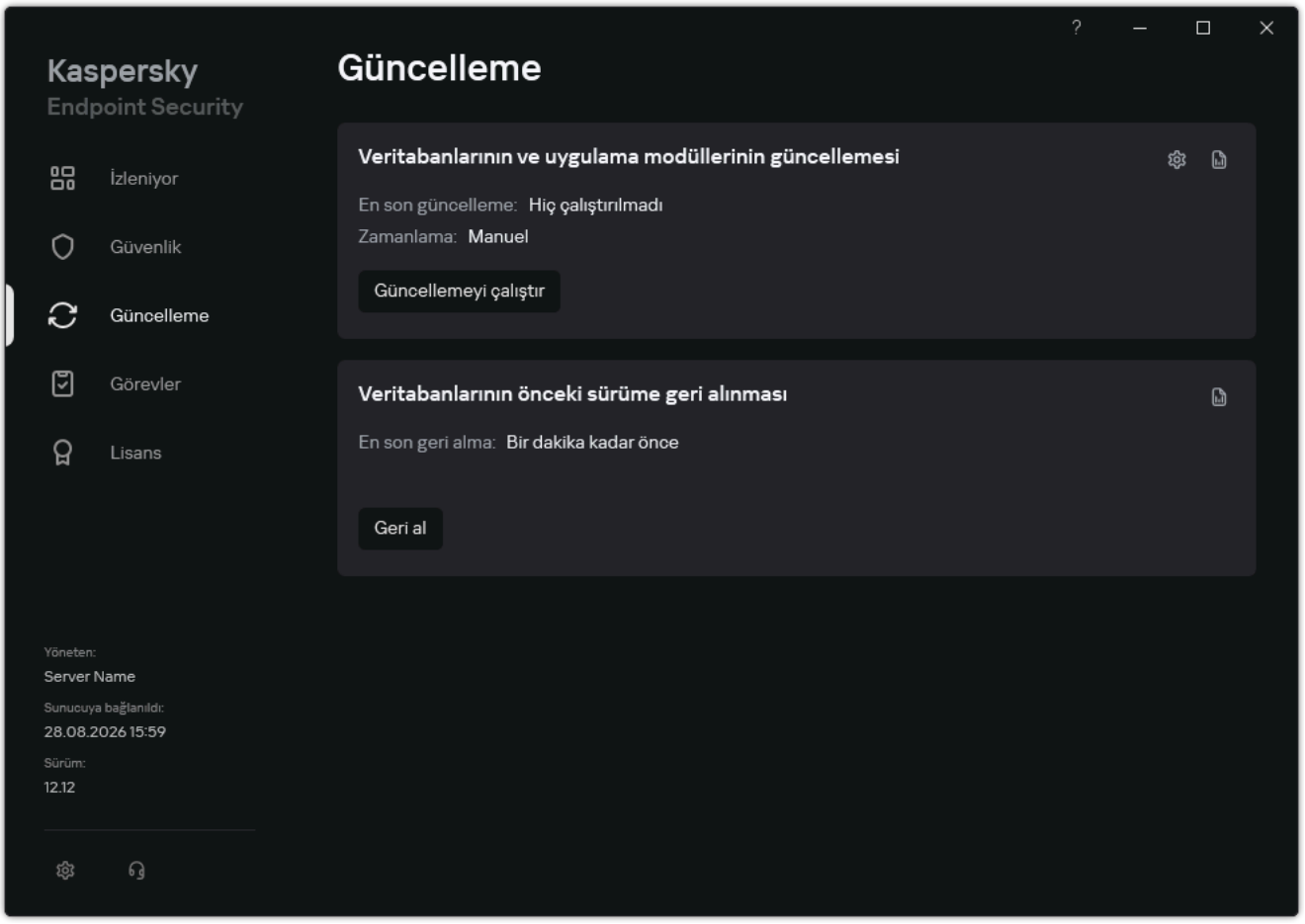
8. Varsayılan olarak, Kaspersky Endpoint Security görevi manuel modda çalıştırır.

9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde belirtilen sunucu depolama alanından Kaspersky Endpoint Security güncellemesi nasıl yapılandırılır

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

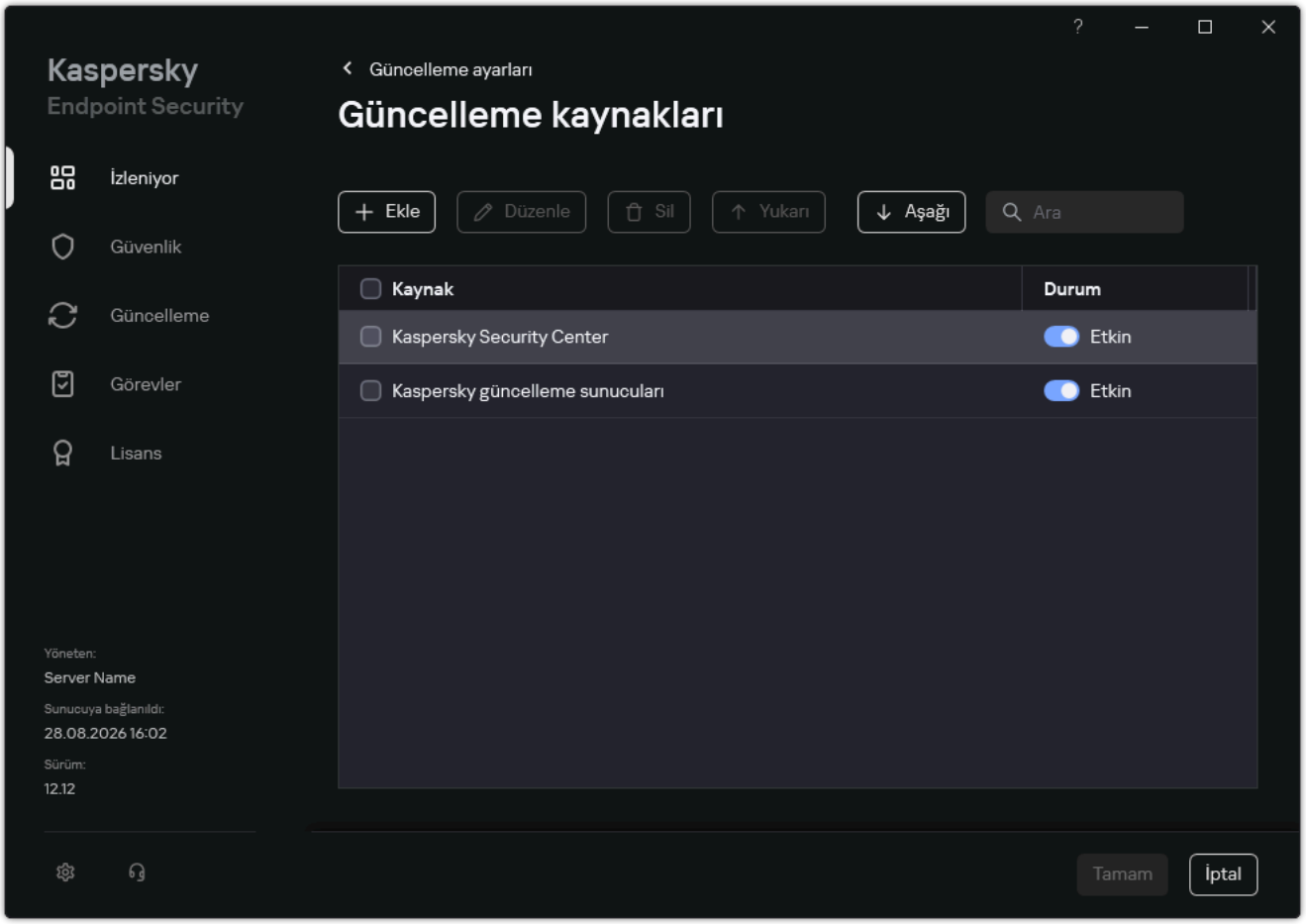
   Görev özellikleri penceresi açılır.

3. Görev özellikleri penceresinde **Güncelleme kaynaklarını seç**'e tıklayın.

4. Güncelleme kaynakları listesinde, **Kaspersky Security Center** kaynağından güncellemenin etkinleştirildiğinden emin olun. Ayrıca, **Kaspersky Security Center** kaynağı en yüksek önceliğe sahip olmalıdır.

5. Gerekirse güncelleme kaynaklarını ekleyin:

   a. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.



Güncelleme kaynakları

   a. Kaspersky Security Center'ın Kaspersky sunucularından aldığı güncelleme paketini kopyalayacağı FTP veya HTTP sunucusu, ağ klasörü ya da yerel klasör adresini belirtin.

> Güncelleme kaynağının adresi, güncellemelerin sunucu depolama alanına indirilmesini yapılandırırken **Güncellemelerin depolanacağı klasör** alanında belirttiğiniz adresle eşleşmelidir (*Güncellemeleri Yönetim Sunucusu veri havuzuna indir* görevi).

   b. **Seç**'e tıklayın.

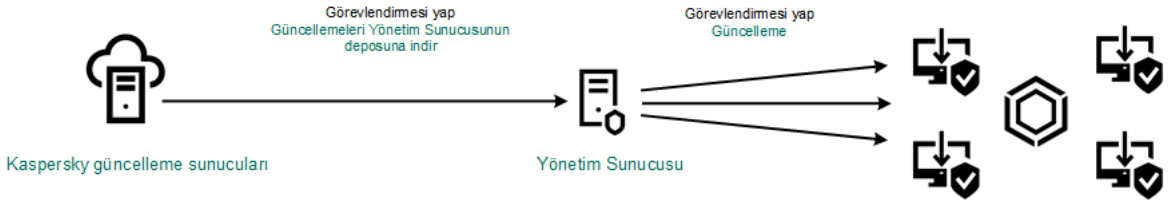
   Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.

6. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

> Bir bilgisayar Kaspersky Security Center tarafından yönetiliyorsa, *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi için çalışma modunu yapılandırmak mümkün değildir. Görevi yalnızca manuel olarak çalıştırabilirsiniz.

7. Değişikliklerinizi kaydedin.



Bir sunucu veri havuzu üzerinden güncelleme

Bir paylaşım klasörü üzerinden güncelleme

İnternet trafiğini düşük tutmak için kuruluşun LAN ağındaki bilgisayarların veritabanları ve uygulama modülleri güncellemelerini bir paylaşım klasörü üzerinden gerçekleştirilmek üzere yapılandırabilirsiniz. Bu amaçla, kuruluşun LAN ağındaki bilgisayarlardan biri Kaspersky Security Center Yönetim Sunucusu veya Kaspersky güncelleme sunucularından güncelleme paketlerini almalı ve alınan güncelleme paketleri paylaşım klasörüne kopyalamalıdır. Böylelikle, kuruluşun LAN ağındaki diğer bilgisayarlar bu paylaşım klasöründen ilgili güncelleme paketlerini alabilir.

Güncelleme paketini paylaşılan bir klasöre kopyalayan Kaspersky Endpoint Security uygulamasının sürümü ve yerelleştirmesi, veritabanlarını paylaşılan klasörden güncelleyen uygulamanın sürümü ve yerelleştirmesi ile eşleşmelidir. Uygulamaların sürümleri veya yerelleştirmeleri eşleşmezse, veritabanı güncellemesi bir hatayla sonlanabilir.

Aşağıdaki adımları uygulayarak veritabanı ve uygulama modüllerini bir paylaşım klasörü üzerinden güncellenecek şekilde yapılandırma:

1. Veritabanı ve uygulama modülü güncellemelerini bir sunucu veri havuzundan yapılandırma.
2. Yerel ağ üzerindeki bilgisayarlardan birindeki bir paylaşım klasörüne bir güncelleme paketinin kopyalanmasını etkinleştirme.

   Yönetim Konsolu'nda (MMC) güncelleme paketinin paylaşılan klasöre kopyalanmasını etkinleştirme

   1. Kaspersky Security Center Yönetim Konsolu'nu açın.
   2. Konsol ağacında **Görevler**'i seçin.

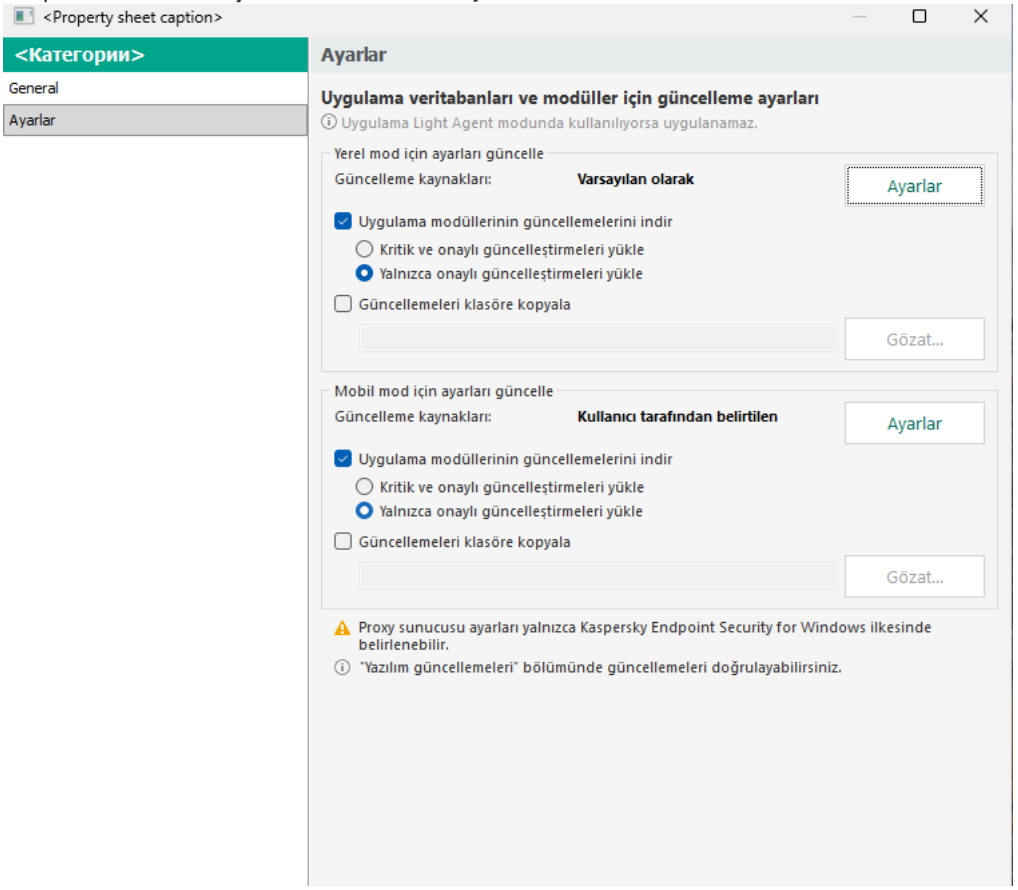
      Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, güncelleme kaynağı olarak kullanılacak bir bilgisayara atanmalıdır.

   3. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

      Görev özellikleri penceresi açılır.

      Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Veritabanlarının ve uygulama modüllerinin güncellemesi görev ayarları

5. **Yerel mod için ayarları güncelle** bloğunda, **Ayarlar** düğmesine tıklayın.

6. Güncelleme kaynaklarını yapılandırın.

   Güncelleme kaynakları; Kaspersky güncelleme sunucuları, Kaspersky Security Center Yönetim Sunucusu, diğer FTP veya HTTP sunucuları, yerel klasörler veya ağ klasörleri olabilir.

7. **Güncellemeleri klasöre kopyala** onay kutusunu işaretleyin.

8. **Klasör yolu** alanına paylaşılan klasöre giden UNC yolunu girin (örneğin `\\<server name>\KLSHARE\Updates`).

   Alan boş bırakılırsa Kaspersky Endpoint Security, güncelleme paketini `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` klasörüne kopyalar.

9. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da güncelleme paketinin paylaşılan klasöre kopyalanmasını etkinleştirme

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

   > *Güncelleme* görevi, güncelleme kaynağı olarak kullanılacak bir bilgisayara atanmalıdır.

2. Kaspersky Endpoint Security'nin **Güncelleme** görevine tıklayın.

   Görev özellikleri penceresi açılır.

Güncelleme görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Güncelleme* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. **Uygulama ayarları** → **Yerel mod** sekmesini seçin.

4. Güncelleme kaynaklarını yapılandırın.

   Güncelleme kaynakları; Kaspersky güncelleme sunucuları, Kaspersky Security Center Yönetim Sunucusu, diğer FTP veya HTTP sunucuları, yerel klasörler veya ağ klasörleri olabilir.

5. **Güncellemeleri klasöre kopyala** onay kutusunu işaretleyin.

6. **Yol** alanına paylaşılan klasöre giden UNC yolunu girin (örneğin `\\<server name>\KLSHARE\Updates`).

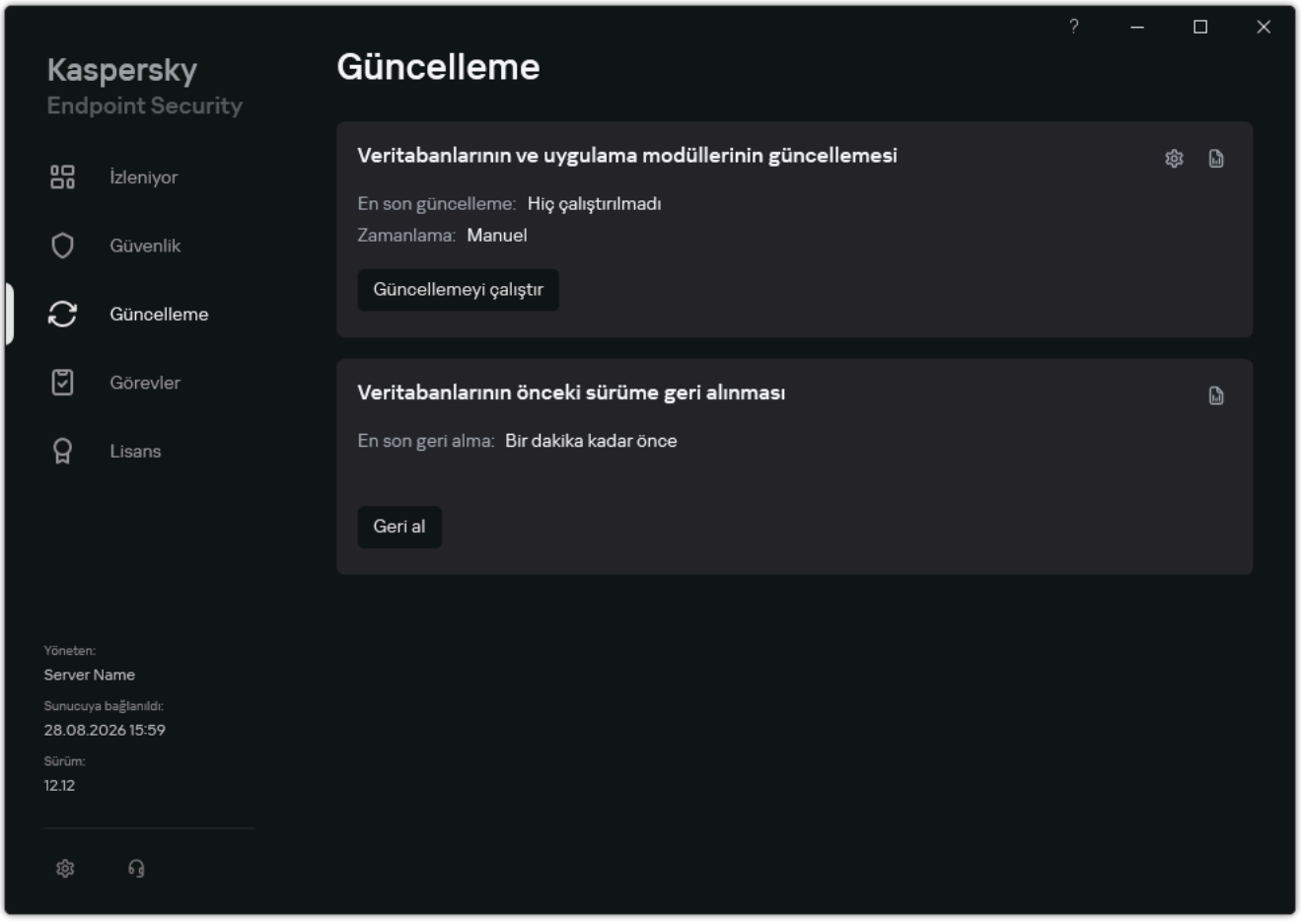
   Alan boş bırakılırsa Kaspersky Endpoint Security, güncelleme paketini `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` klasörüne kopyalar.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde güncelleme paketinin paylaşılan klasöre kopyalanmasını etkinleştirme

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Güncellemeler dağıtılıyor** bloğunda, **Güncellemeleri klasöre kopyala** onay kutusunu seçin.

4. Paylaşılan klasöre giden UNC yolunu girin (örneğin `\\<server name>\KLSHARE\Updates`).

5. Değişikliklerinizi kaydedin.

3. Kuruluşun LAN ağındaki diğer bilgisayarları veritabanı ve uygulama modülü güncellemelerini belirli bir paylaşım klasörü üzerinden yapacak şekilde yapılandırma.

Yönetim Konsolu'nda (MMC) paylaşılan klasörden güncellemeleri yapılandırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Veritabanlarının ve uygulama modüllerinin güncellemesi** seçimini yapın.

4. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

5. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → Veritabanlarının ve uygulama modüllerinin güncellemesi öğesini seçin.

Adım 2. Güncelleme kaynaklarını seçme

Yeni bir güncelleme kaynağı ekleyin: paylaşılan bir klasör. Kaynak adresi, daha önce paylaşılan güncelleme paketinin kopyalanmasını yapılandırırken **Klasör yolu** alanında belirtmiş olduğunuz adresle aynı olmalıdır. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, güncelleme kaynağı olarak kullanılan bilgisayar hariç kuruluşun LAN ağındaki tüm bilgisayarlara atanmalıdır.

4. Adım. Görevi çalıştıracak hesabı seçme

Veritabanlarının ve uygulama modüllerinin güncellemesi görevini çalıştırmak için bir hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

5. Adım. Bir görev başlatma zamanlaması yapılandırma

Bir görev başlatmak için bir zamanlama yapılandırın, örneğin manuel olarak ya da antivirüs veritabanları veri havuzuna indirildikten sonra.

6. Adım. Görev adını tanımlama

Görevin adını girin, örneğin *Paylaşım klasörü üzerinden güncelleme*.

7. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz. Sonuç olarak, güncelleme işlemi kullanıcıların bilgisayarlarında belirtilen programa göre gerçekleştirilecektir.

Web Console'da ve Cloud Console'da paylaşılan klasörden güncellemeleri yapılandırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinden **Güncelleme**'yi seçin.

   c. **Görev adı** alanına, *Paylaşım klasörü üzerinden güncelleme* gibi bir kısa açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

   > *Güncelleme* görevi, güncelleme kaynağı olarak kullanılan bilgisayar hariç kuruluşun LAN ağındaki tüm bilgisayarlara atanmalıdır.

4. Seçili görev kapsamı seçeneğine göre aygıtları belirleyin ve sonraki adıma geçin.

5. Sihirbazı tamamlayın.

   Görevler tablosunda yeni bir görev görüntülenir.

6. Yeni oluşturulan *Güncelleme* görevine tıklayın.

   Görev özellikleri penceresi açılır.

7. **Uygulama ayarları** → Yerel mod sekmesini seçin.

8. **Güncelleme kaynakları** bloğunda, **Ekle** düğmesine tıklayın.

9. Açılan pencereye paylaşım klasörünün yolunu girin.

   > Kaynak adresi, daha önce paylaşılan güncelleme paketinin kopyalanmasını yapılandırırken **Yol** alanında belirtmiş olduğunuz adresle aynı olmalıdır (yukarıdaki talimata bakın).

10. **Tamam**'a tıklayın.

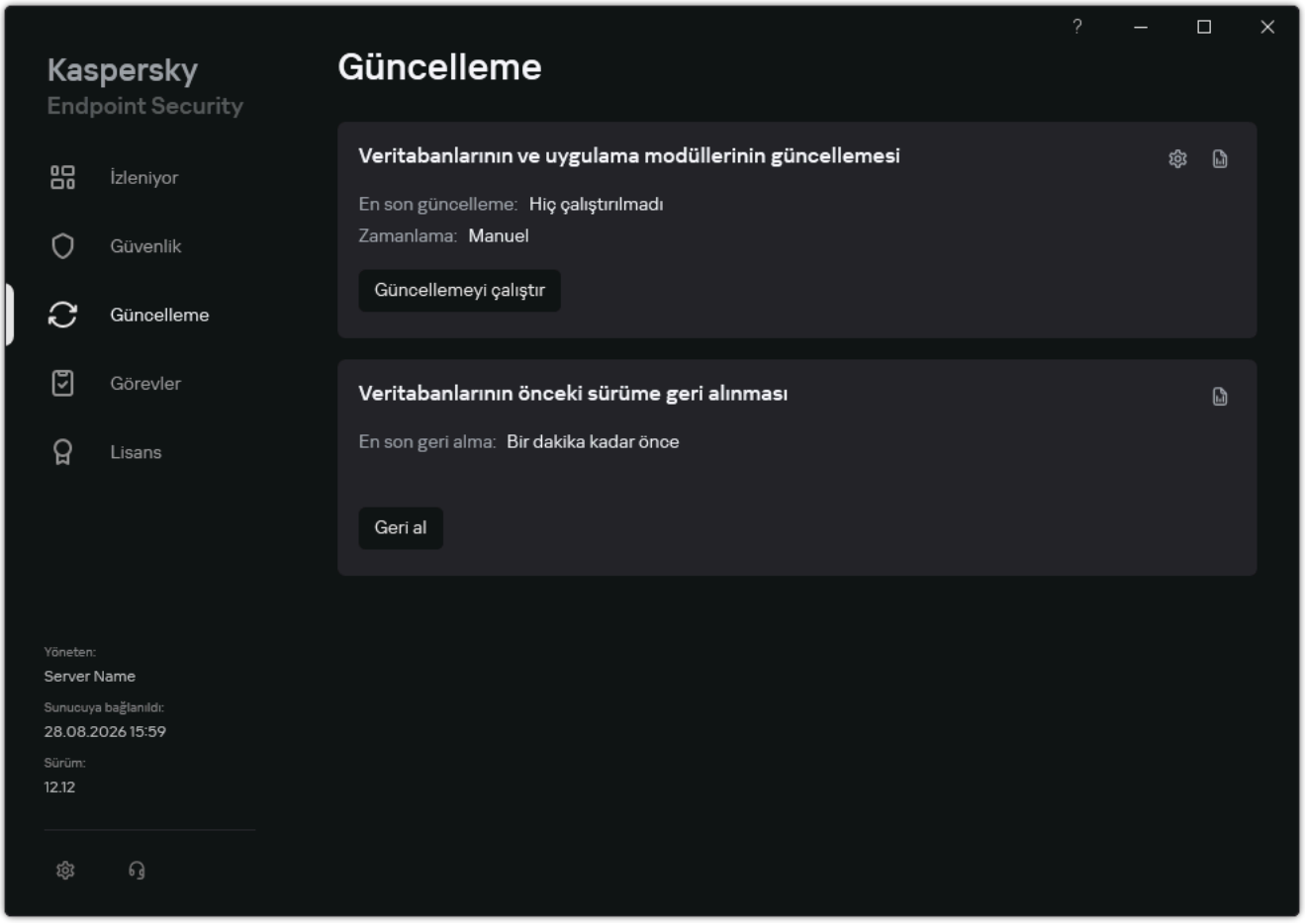
11. **Yukarı taşı** ve **Aşağı taşı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

12. Değişikliklerinizi kaydedin.

Uygulama arabiriminde paylaşılan klasörden güncellemeleri yapılandırma

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Güncelleme kaynaklarını seç**'e tıklayın.

4. Açılan pencerede **Ekle** düğmesine tıklayın.

5. Açılan pencereye paylaşım klasörünün yolunu girin.

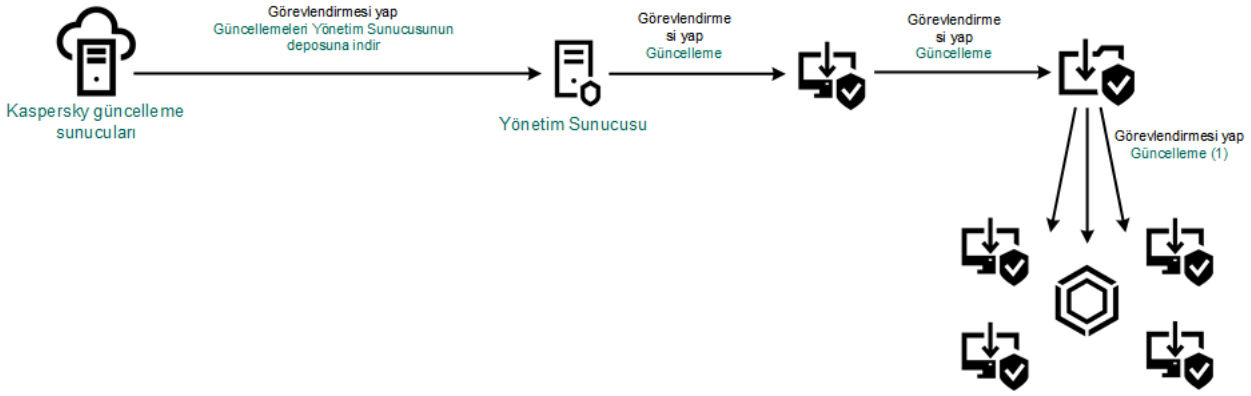
   Kaynak adresi, daha önce paylaşılan güncelleme paketinin kopyalanmasını yapılandırırken belirtmiş olduğunuz adresle aynı olmalıdır (yukarıdaki talimata bakın).

6. **Seç**'e tıklayın.

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

8. Değişikliklerinizi kaydedin.



Bir paylaşım klasörü üzerinden güncelleme

Kaspersky Update Utility aracıyla güncelleme

İnternet trafiğini düşük tutmak için Kaspersky Update Utility kullanılarak kuruluşun LAN ağındaki bilgisayarların veritabanları ve uygulama modülleri güncellemelerini bir paylaşım klasörü üzerinden gerçekleştirilmek üzere yapılandırabilirsiniz. Bu amaçla, kuruluşun LAN ağındaki bilgisayarlardan biri Kaspersky Security Center Yönetim Sunucusu veya Kaspersky güncelleme sunucularından aracı kullanarak güncelleme paketlerini almalı ve alınan güncelleme paketleri paylaşım klasörüne kopyalamalıdır. Böylelikle, kuruluşun LAN ağındaki diğer bilgisayarlar bu paylaşım klasöründen ilgili güncelleme paketlerini alabilir.

Güncelleme paketini paylaşılan bir klasöre kopyalayan Kaspersky Endpoint Security uygulamasının sürümü ve yerelleştirmesi, veritabanlarını paylaşılan klasörden güncelleyen uygulamanın sürümü ve yerelleştirmesi ile eşleşmelidir. Uygulamaların sürümleri veya yerelleştirmeleri eşleşmezse, veritabanı güncellemesi bir hatayla sonlanabilir.

Aşağıdaki adımları uygulayarak veritabanı ve uygulama modüllerini bir paylaşım klasörü üzerinden güncellenecek şekilde yapılandırma:

1. Veritabanı ve uygulama modülü güncellemelerini bir sunucu veri havuzundan yapılandırma.

2. Kaspersky Update Utility'yi kuruluşun yerel alan ağında bulunan bilgisayarlardan birine yükleyin.

3. Kaspersky Update Utility ayarlarından güncelleme paketinin paylaşılan klasöre kopyalanmasını yapılandırın.

   Kaspersky Update Utility dağıtım paketini Kaspersky Teknik Destek İnternet sitesinden indirebilirsiniz. Aracı indirdikten sonra güncelleme kaynağını (örneğin Yönetim Sunucusu veri havuzu) ve Kaspersky Update Utility'nin güncelleme paketlerini kopyalayacağı paylaşılan klasörü seçin. Kaspersky Update Utility'yi kullanma hakkında ayrıntılı bilgi için Kaspersky Bilgi Bankası'na bakın.

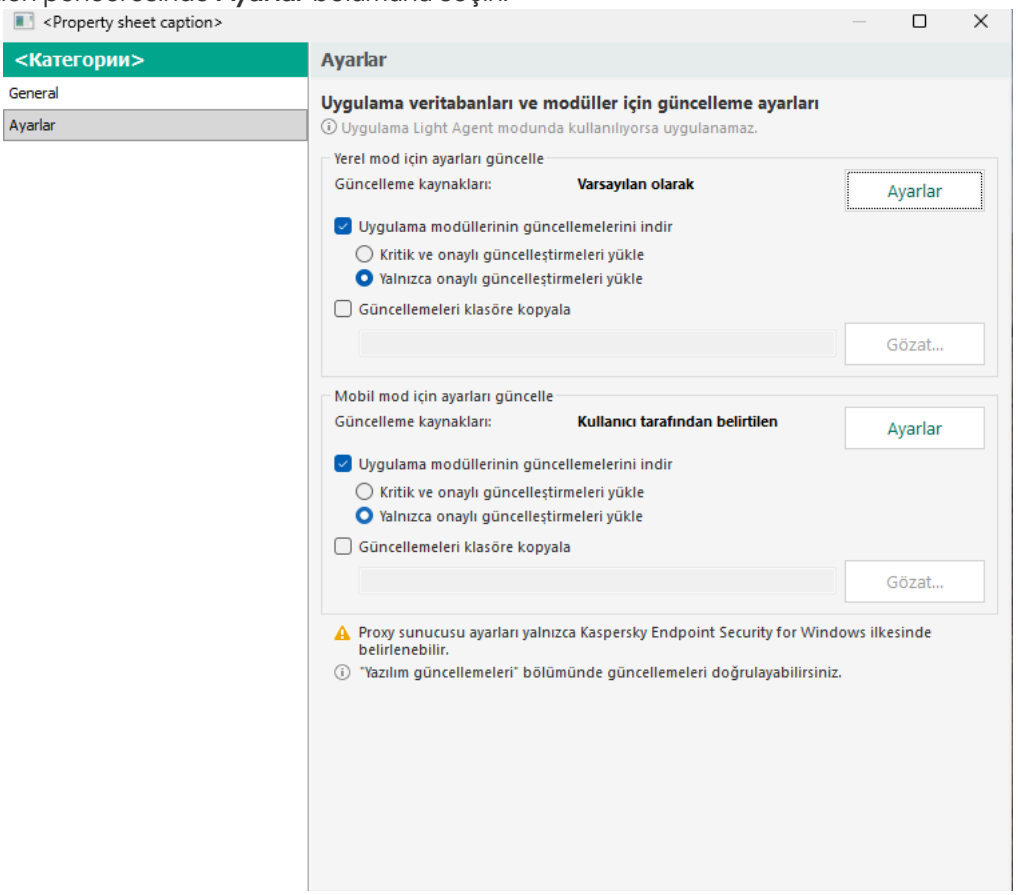
4. Kuruluşun LAN ağındaki diğer bilgisayarları veritabanı ve uygulama modülü güncellemelerini belirli bir paylaşım klasörü üzerinden yapacak şekilde yapılandırma.

Yönetim Konsolu'nda (MMC) paylaşılan klasörden güncellemeleri yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Veritabanlarının ve uygulama modüllerinin güncellemesi görev ayarları

5. **Yerel mod için ayarları güncelle** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.
7. Açılan pencerede paylaşılan klasöre giden UNC yolunu girin (örneğin `\\<server name>\KLSHARE\Updates`).

   Kaynak adresi, Kaspersky Update Utility ayarlarında belirtilen adresle aynı olmalıdır.
8. **Tamam**'a tıklayın.

9. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

10. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da paylaşılan klasörden güncellemeleri yapılandırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Güncelleme** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Güncelleme görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Güncelleme* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. **Uygulama ayarları** → **Yerel mod** sekmesini seçin.

4. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

5. Açılan pencerede paylaşılan klasöre giden UNC yolunu girin (örneğin `\\<server name>\KLSHARE\Updates`).

   Kaynak adresi, Kaspersky Update Utility ayarlarında belirtilen adresle aynı olmalıdır.

6. **Tamam**'a tıklayın.

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

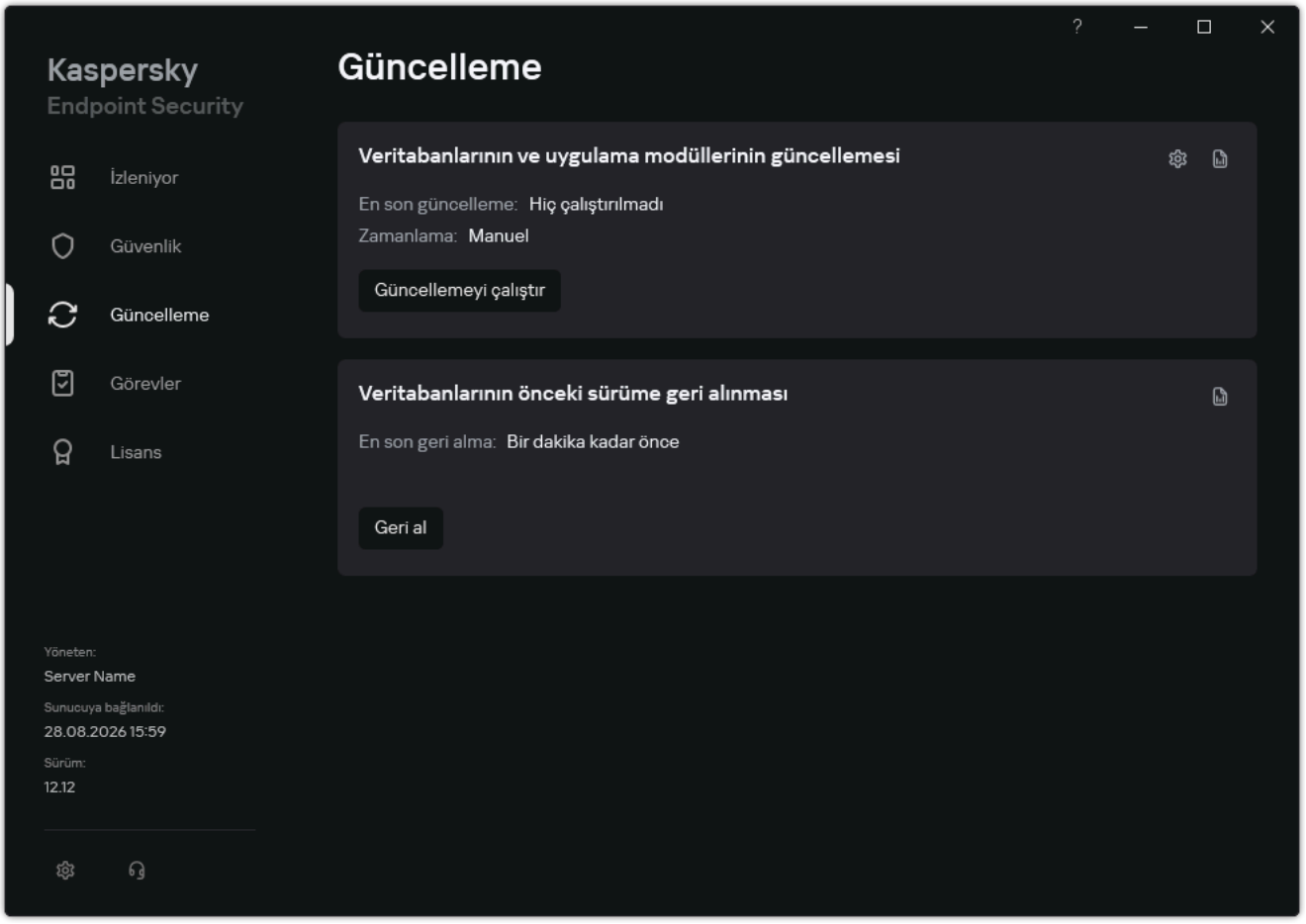
   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

8. Değişikliklerinizi kaydedin.

Uygulama arabiriminde paylaşılan klasörden güncellemeleri yapılandırma

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



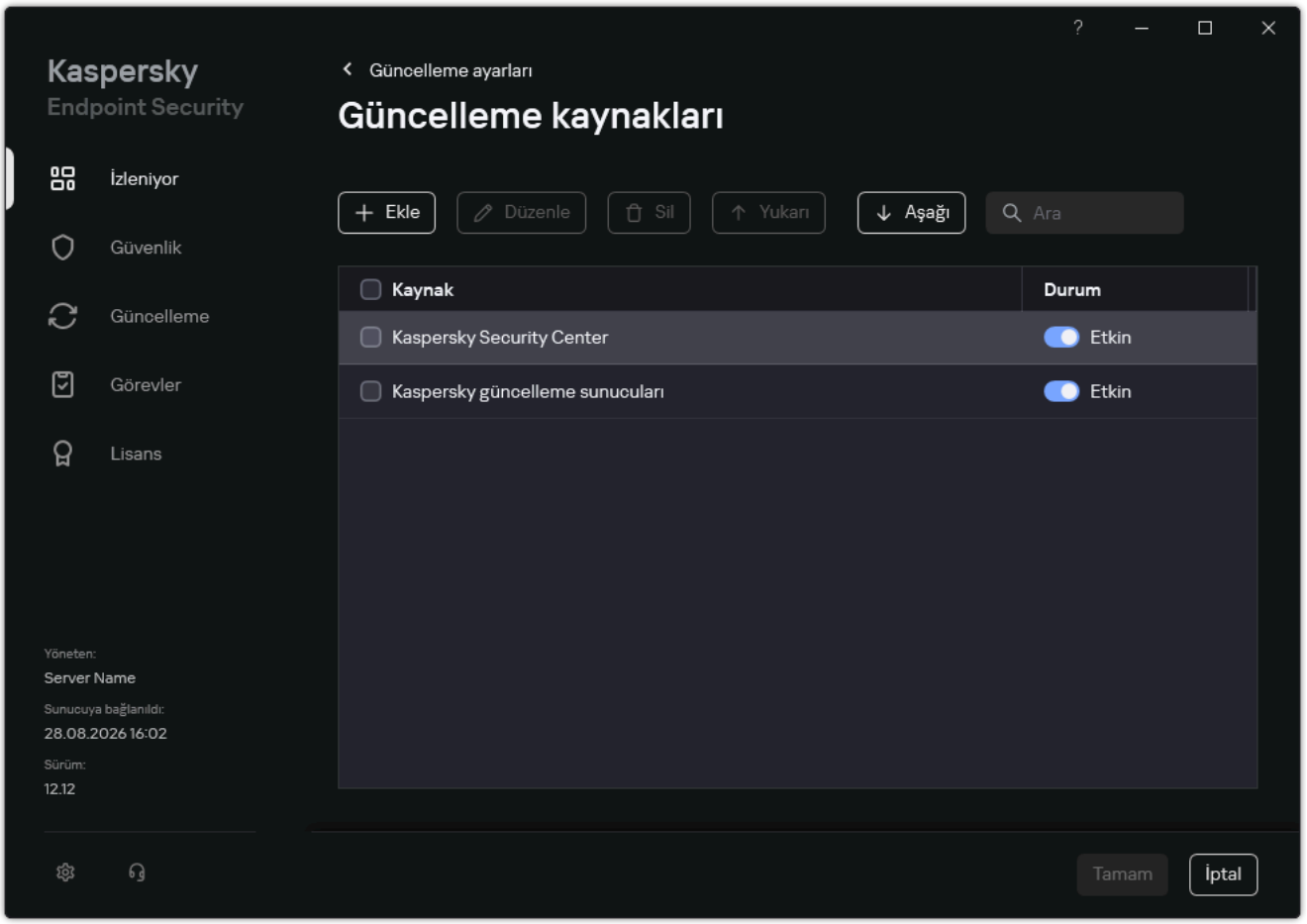
Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. Görev özellikleri penceresinde **Güncelleme kaynaklarını seç**'e tıklayın.

4. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.



Güncelleme kaynakları

5. Paylaşılan klasöre giden UNC yolunu girin (örneğin `\\<server name>\KLSHARE\Updates`).

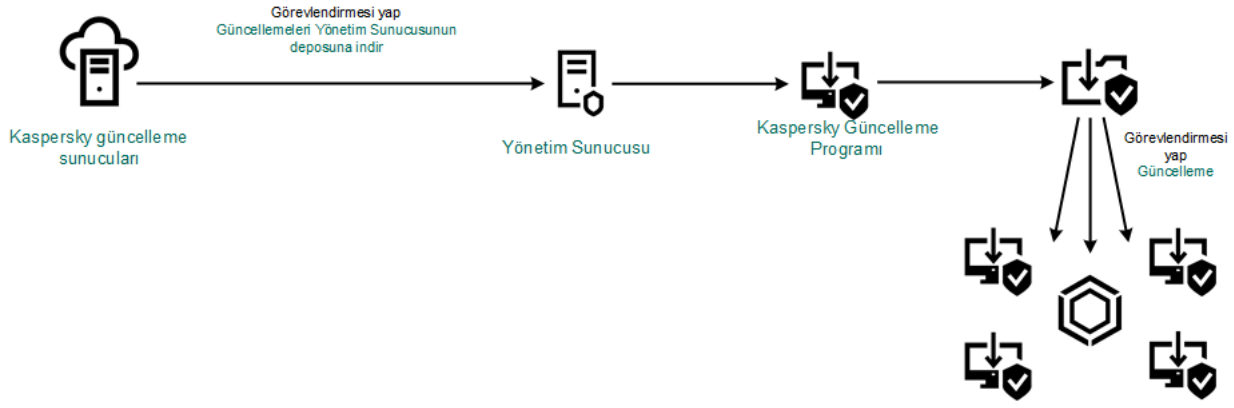
> Kaynak adresi, Kaspersky Update Utility ayarlarında belirtilen adresle aynı olmalıdır.

6. **Seç**'e tıklayın.

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

8. Değişikliklerinizi kaydedin.



Kaspersky Update Utility aracıyla güncelleme

Mobil modda güncelleme

Mobil mod, Kaspersky Endpoint Security'nin bir bilgisayar kuruluş ağından ayrıldığı zamanki (*çevrimdışı bilgisayar*) işlem modudur. Çevrimdışı bilgisayarlarla ve işyeri dışındaki kullanıcılarla çalışma hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardımı içeriğine bakın.

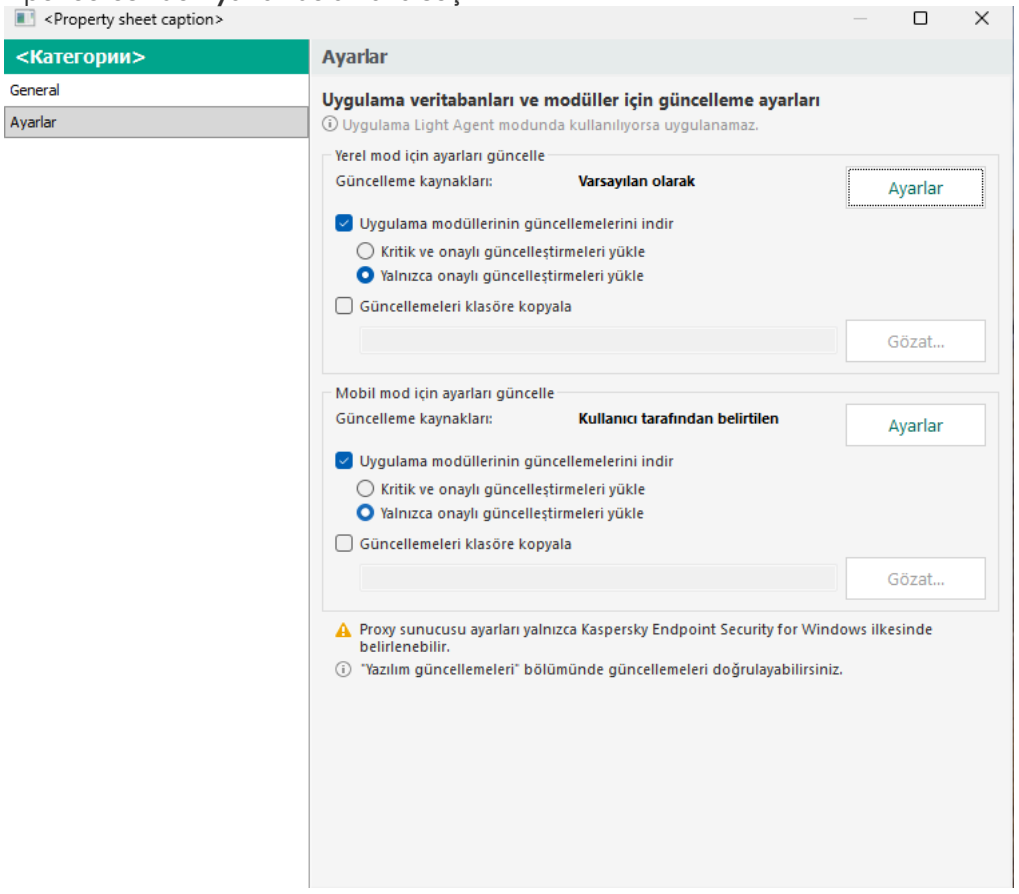
Kuruluş ağının dışındaki bir çevrimdışı bilgisayar, veritabanlarını ve uygulama modüllerini güncellemek için Yönetim Sunucusuna bağlanamaz. Kaspersky güncelleme sunucuları varsayılan olarak, mobil modda veritabanlarını ve uygulama modüllerini güncellemek için güncelleme kaynakları olarak kullanılır. İnternete bağlanmak için kullanılan proxy sunucusu, özel bir ofis dışı ilkesi ile belirlenir. İşyeri dışında ilkesi ayrıca oluşturulmalıdır. Kaspersky Endpoint Security, mobil moda geçtiğinde güncelleme görevi her iki saatte bir başlatılır.

Yönetim Konsolu'nda (MMC) mobil mod için güncelleme ayarlarını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Veritabanlarının ve uygulama modüllerinin güncellemesi görev ayarları

5. **Mobil mod için ayarları güncelle** bloğunda, **Ayarlar** düğmesine tıklayın.

6. Güncelleme kaynaklarını yapılandırın. Güncelleme kaynakları; Kaspersky güncelleme sunucuları, diğer FTP ve HTTP sunucuları, yerel klasörler veya ağ klasörleri olabilir.

7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da mobil mod için güncelleme ayarlarını yapılandırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Güncelleme** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Güncelleme görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Güncelleme* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. **Uygulama ayarları** → **Mobil mod** sekmesini seçin.

4. Güncelleme kaynaklarını yapılandırın. Güncelleme kaynakları; Kaspersky güncelleme sunucuları, diğer FTP ve HTTP sunucuları, yerel klasörler veya ağ klasörleri olabilir.

5. Değişikliklerinizi kaydedin.

Sonuç olarak kullanıcılar mobil moda geçtiğinde kullanıcı bilgisayarlarındaki veritabanları ve uygulama modülleri güncellenir.

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.

Bir güncelleme görevini başlatmak veya durdurmak için:

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.

2. **Veritabanlarının ve uygulama modüllerinin güncellemesi** kutucuğunda, güncelleme görevini başlatmak istiyorsanız **Güncelle** düğmesine tıklayın.

   Kaspersky Endpoint Security, uygulama modüllerini ve veritabanlarını güncellemeye başlar. Uygulama görev ilerlemesini, indirilen dosyaların boyutunu ve güncelleme kaynağını gösterir. **Güncellemeyi durdur** düğmesine tıklayarak görevi istediğiniz zaman durdurabilirsiniz.

Basitleştirilmiş uygulama arabirimi görüntülendiğinde güncelleme görevini başlatmak veya durdurmak için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin bağlam 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

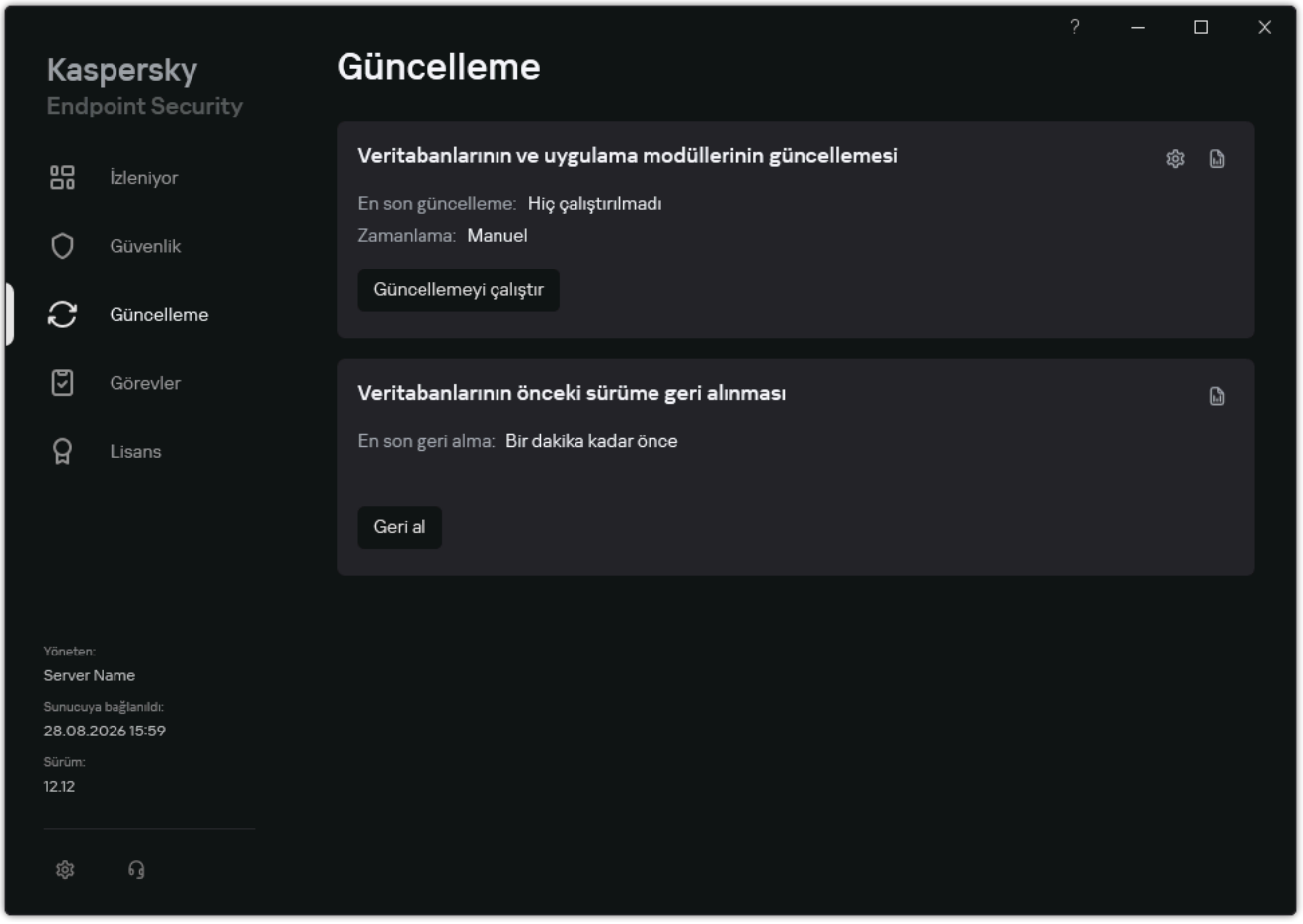
Farklı bir kullanıcı hesabının hakları altında bir güncelleme görevi başlatma

Varsayılan olarak Kaspersky Endpoint Security güncelleme görevi, işletim sisteminde oturum açmak için hesabını kullandığınız kullanıcı adına başlatılır. Ancak Kaspersky Endpoint Security, gerekli hakların olmaması nedeniyle kullanıcının erişemediği bir güncelleme kaynağından (örneğin bir güncelleme paketi içeren bir paylaşım klasöründen) veya proxy sunucusu kimlik doğrulamasının yapılandırılmadığı bir güncelleme kaynağından güncellenebilir. Uygulama 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:

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Veritabanı güncellemelerini kullanıcı haklarıyla çalıştır**'a tıklayın.

4. Açılan pencerede, **Diğer kullanıcı** seçimini yapın.

5. Güncelleme kaynağına erişmek için gerekli izinlere sahip bir kullanıcının hesap kimlik bilgilerini girin.

6. Değişikliklerinizi kaydedin.

Güncelleme görevinin çalışma modunu seçme

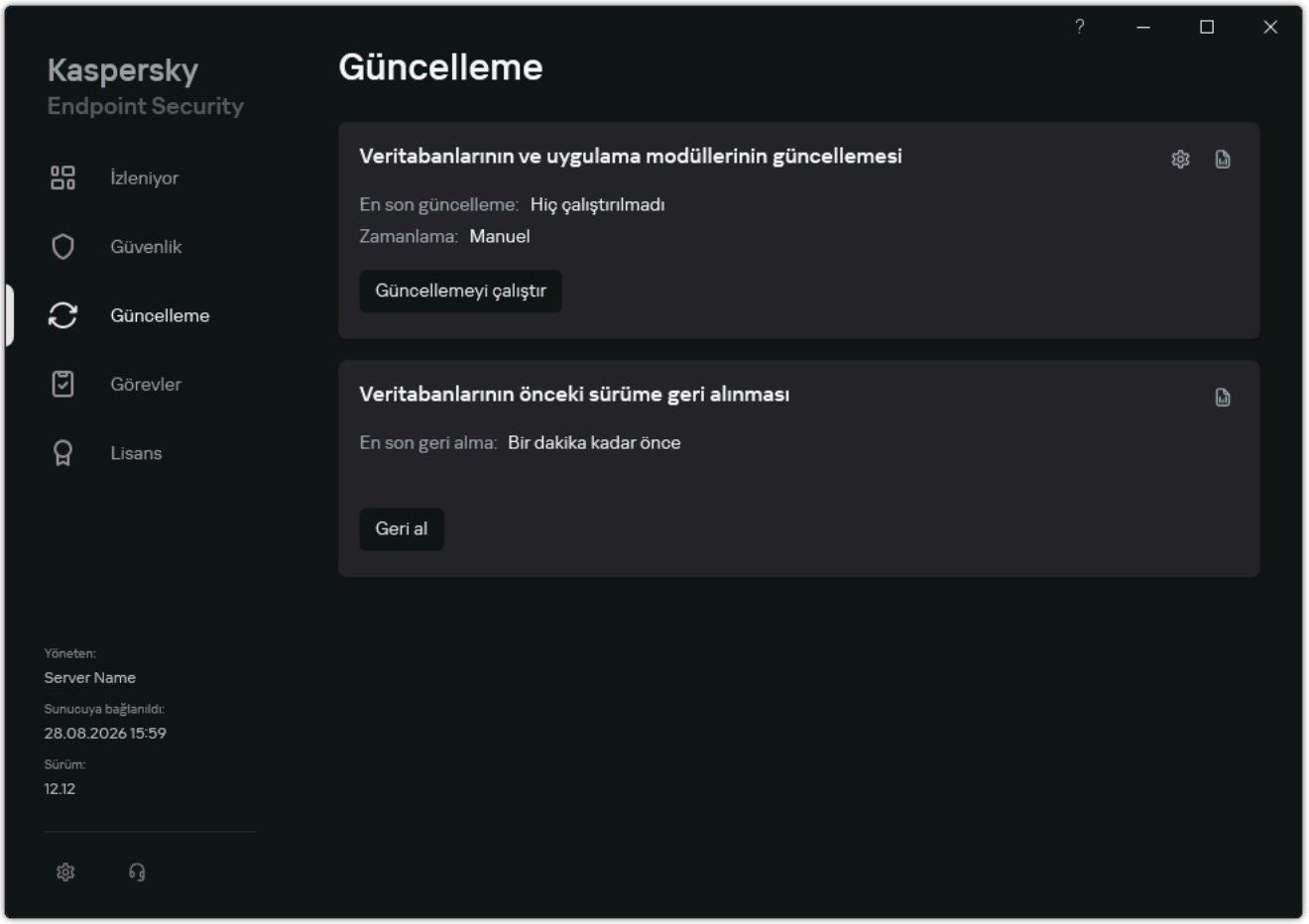
Güncelleme görevini herhangi bir nedenle çalıştırmak mümkün değilse (örneğin bilgisayar o sırada açık değilse) atlanan görevi mümkün olur olmaz otomatik olarak başlayabilecek şekilde yapılandırabilirsiniz.

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 görevinin çalışma modunu seçmek için:

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Çalışma modu**'na tıklayın.

4. Açılan pencerede güncelleme görevi çalışma modunu 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 **Manuel** seçeneğini seçin.

   - Güncelleme görevini çalıştırmak için bir zamanlama yapılandırmak isterseniz diğer seçenekleri seçin. Güncelleme görevini başlatmak için gelişmiş ayarları yapılandırın:

     - **Uygulama başladıktan sonra çalışmayı şu kadar ertele**: **N dakika** alanında, Kaspersky Endpoint Security başlatıldıktan sonra güncelleme görevinin ne kadar süre ertelenmesini istiyorsanız belirtin.

     - Kaspersky Endpoint Security'nin kaçırılan güncelleme görevlerini ilk fırsatta çalıştırmasını istiyorsanız **Bilgisayar kapalıysa zamanlanmış taramayı sonraki gün çalıştır**'ı seçin. Uygulama kaçırılan görevleri yürütme fırsatı bulduğunda, bilgisayar üzerindeki yükü dağıtmak için görevleri belirli bir zaman aralığında rastgele çalıştırır.

5. Değişikliklerinizi kaydedin.

Güncelleme kaynağı ekleme

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.

Kaspersky güncelleme sunucuları erişilemez durumdaysa, Kaspersky Endpoint Security veritabanlarını ve uygulama yazılımı modüllerini güncellemek için alternatif etki alanlarını kullanabilir. Ayrıntılı bilgi için Teknik Destek Bilgi Tabanına bakın.

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.

Kaspersky Endpoint Security, Kaspersky'nin güncelleme sunucuları olmadığı sürece, HTTPS sunucularından gelen güncellemeleri desteklemez.

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.

Kaspersky Endpoint Security ilk güncelleme kaynağı olarak varsayılan olarak Kaspersky Security Center sunucusunu kullanır. Bu, güncelleme sırasında trafiğin korunmasına yardımcı olur. Bilgisayara bir ilke uygulanmazsa, uygulamanın Kaspersky Security Center sunucusuna erişimi olmayabileceğinden, Yerel *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevinin ayarlarında ilk güncelleme kaynağı olarak Kaspersky sunucuları seçilir.

Uygulama Light Agent modunda çalışıyorsa, SVM üzerindeki bir klasör güncelleme kaynağı olarak seçilir.

Yönetim Konsolu'nda (MMC) bir güncelleme kaynağı ekleme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

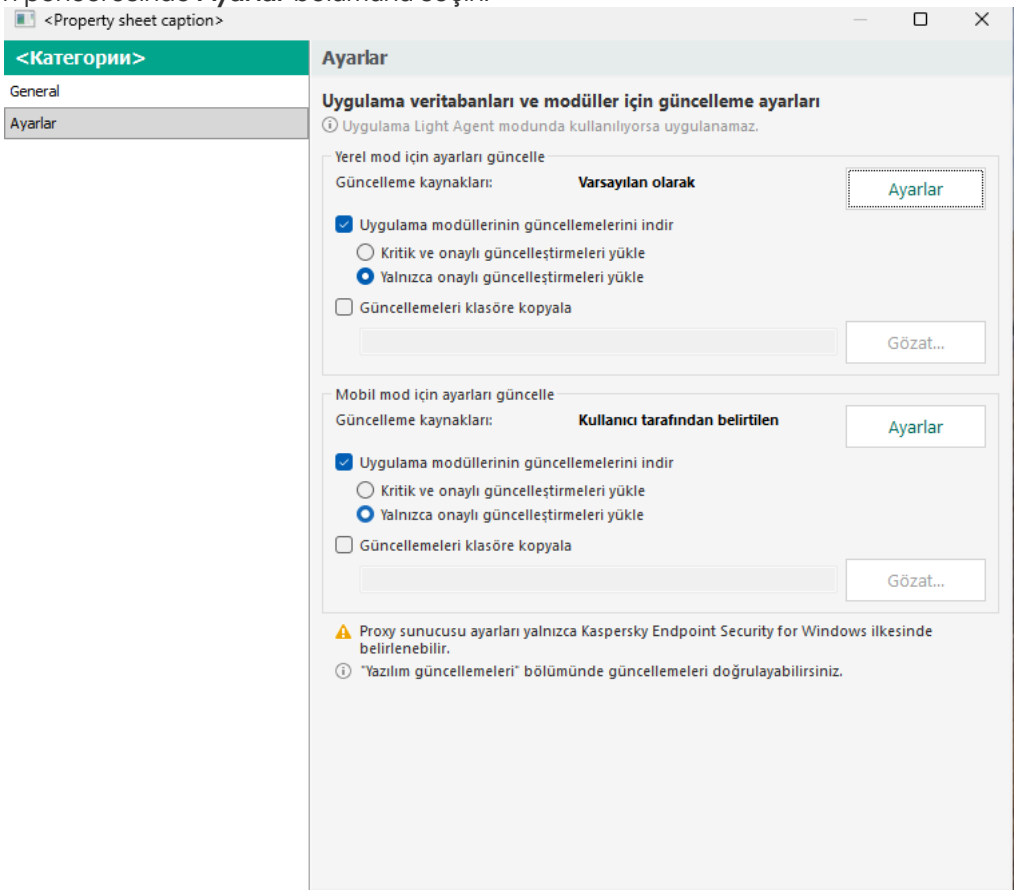
   Konsol ağacında **Görevler**'i seçin.

2. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

   Görev özellikleri penceresi açılır.

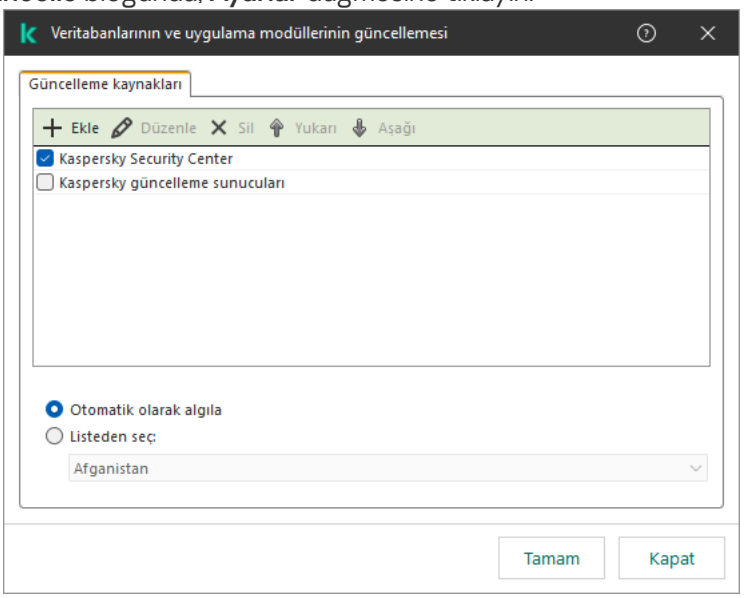
   Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Veritabanlarının ve uygulama modüllerinin güncellemesi görev ayarları

4. **Yerel mod için ayarları güncelle** bloğunda, **Ayarlar** düğmesine tıklayın.



Güncelleme kaynakları

5. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

6. **Güncelleme kaynakları** alanında, FTP veya HTTP sunucusunun adresini, güncelleme paketini içeren ağ klasörünü ya da yerel klasörü belirtin.

   Güncelleme kaynağı için aşağıdaki yol biçimi kullanılır:

   - FTP veya HTTP sunucusu için İnternet adresini veya IP adresini girin.

     Örneğin `http://dnl-01.geo.kaspersky.com/` veya `93.191.13.103`.

     Bir FTP sunucusu için kimlik doğrulama ayarlarını adres içinde aşağıdaki biçimde belirtebilirsiniz: `ftp://<user name>:<password>@<node>:<port>`.

   - Bir ağ klasörü için UNC yolunu girin.

     Örneğin, `\\Server\Share\Update distribution`.

   - Bir yerel klasör için o klasörün tam yolunu girin.

     Örneğin, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

7. **Tamam**'a tıklayın.

8. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

9. Gerekirse, mobil mod için bir güncelleme kaynağı ekleyin. *Mobil mod*, Kaspersky Endpoint Security'nin bir bilgisayar kuruluş ağından ayrıldığı zamanki (*çevrimdışı bilgisayar*) işlem modudur.

10. Değişikliklerinizi kaydedin.

Web Konsolu'nda bir güncelleme kaynağı ekleme

1. Web Console ana penceresinden **Görevler** seçimini yapın.

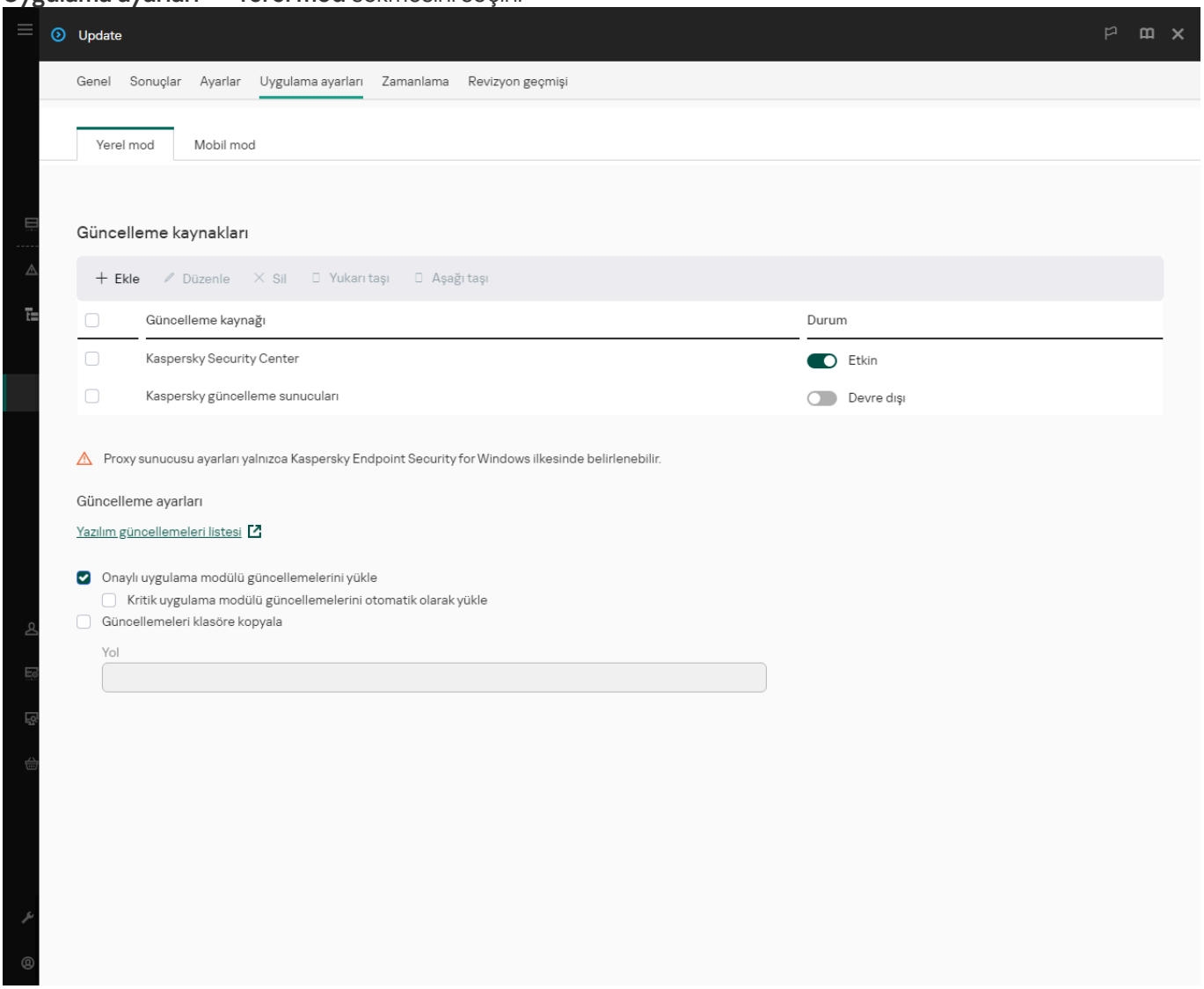
   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Güncelleme** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Güncelleme görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Güncelleme* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. **Uygulama ayarları** → **Yerel mod** sekmesini seçin.



Güncelleme kaynakları

4. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

5. Açılan pencerede, FTP veya HTTP sunucusunun adresini, güncelleme paketini içeren ağ klasörünü ya da yerel klasörü belirtin.

   Güncelleme kaynağı için aşağıdaki yol biçimi kullanılır:

   - FTP veya HTTP sunucusu için İnternet adresini veya IP adresini girin.

     Örneğin `http://dnl-01.geo.kaspersky.com/` veya `93.191.13.103`.

Bir FTP sunucusu için kimlik doğrulama ayarlarını adres içinde aşağıdaki biçimde belirtebilirsiniz: `ftp://<user name>:<password>@<node>:<port>`.

- Bir ağ klasörü için UNC yolunu girin.

  Örneğin, `\\Server\Share\Update distribution`.

- Bir yerel klasör için o klasörün tam yolunu girin.

  Örneğin, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.

6. **Tamam**'a tıklayın.

7. **Yukarı taşı** ve **Aşağı taşı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

   Güncelleme, ilk güncelleme kaynağı üzerinden gerçekleştirilemezse Kaspersky Endpoint Security otomatik olarak bir sonraki sunucuya geçiş yapar.

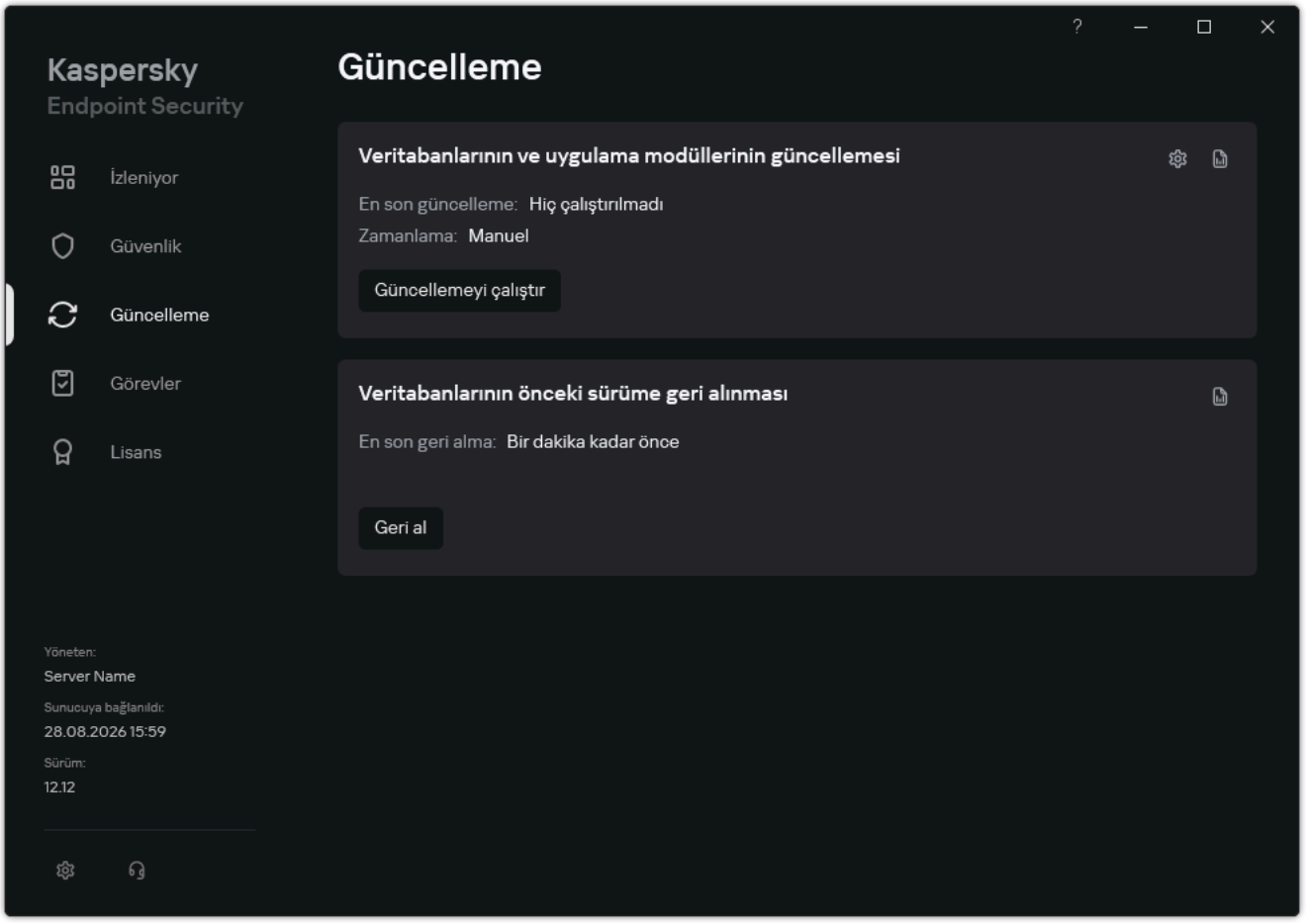
8. Gerekirse, mobil mod için bir güncelleme kaynağı ekleyin. *Mobil mod*, Kaspersky Endpoint Security'nin bir bilgisayar kuruluş ağından ayrıldığı zamanki (*çevrimdışı bilgisayar*) işlem modudur.

9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir güncelleme kaynağı ekleme

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



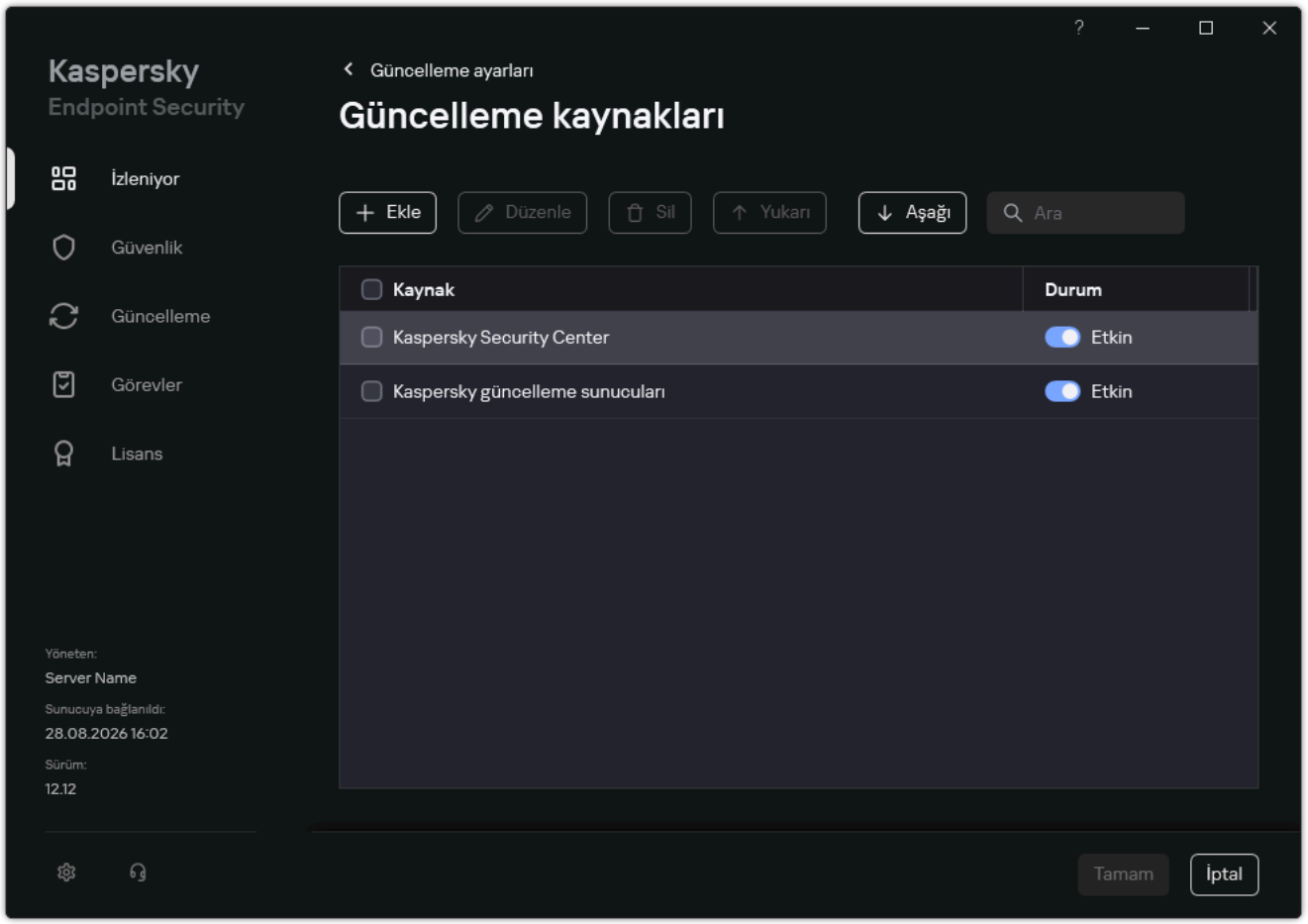
Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Güncelleme kaynaklarını seç**'e tıklayın.

4. Açılan pencerede **Ekle** düğmesine tıklayın.



Güncelleme kaynakları

5. Açılan pencerede, FTP veya HTTP sunucusunun adresini, güncelleme paketini içeren ağ klasörünü ya da yerel klasörü belirtin.

   Güncelleme kaynağı için aşağıdaki yol biçimi kullanılır:

   - FTP veya HTTP sunucusu için İnternet adresini veya IP adresini girin.

     Örneğin `http://dnl-01.geo.kaspersky.com/` veya `93.191.13.103`.

     Bir FTP sunucusu için kimlik doğrulama ayarlarını adres içinde aşağıdaki biçimde belirtebilirsiniz: `ftp://<user name>:<password>@<node>:<port>`.

   - Bir ağ klasörü için UNC yolunu girin.

     Örneğin, `\\Server\Share\Update distribution`.

   - Bir yerel klasör için o klasörün tam yolunu girin.

     Örneğin, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. **Seç**'e tıklayın.

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

8. Değişikliklerinizi kaydedin.

Uygulama modüllerini güncelleme

Uygulama modülü güncellemeleri hataları düzeltir, performansı iyileştirir ve yeni özellikler ekler. Yeni bir uygulama modülü güncellemesi mevcut olduğunda, güncellemenin kurulumunu onaylamanız gerekir. Bir uygulama modülü güncellemesinin kurulumunu uygulama arabiriminde veya Kaspersky Security Center'da onaylayabilirsiniz. Bir güncelleme kullanılabilir olduğunda, uygulama Kaspersky Endpoint Security'nin ana penceresinde bir bildirim görüntüler: . Uygulama modülü güncellemeleri, Son Kullanıcı Lisans Sözleşmesi koşullarının gözden geçirilmesini ve kabul edilmesini gerektirirse uygulama, Son Kullanıcı Lisans Sözleşmesi koşullarının kabul edilmesinden sonra güncellemeleri yükler.

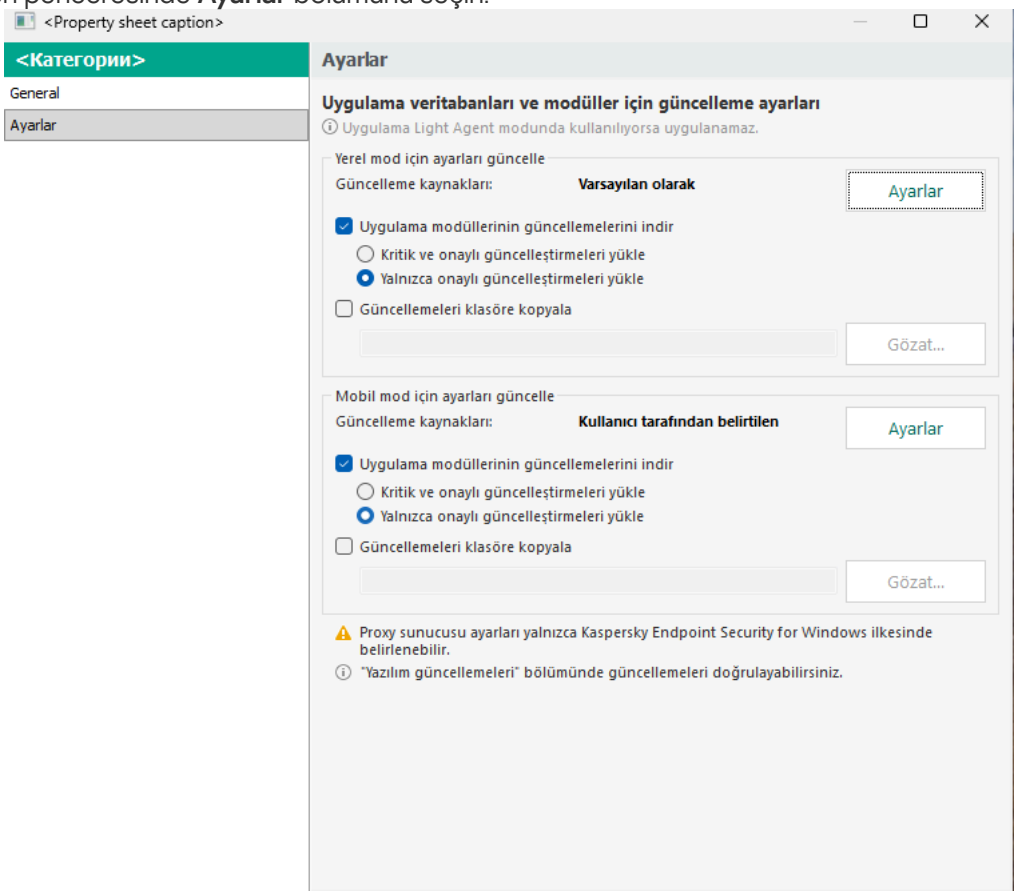
Bir uygulama güncellemesini yükledikten sonra bilgisayarınızı yeniden başlatmanız gerekebilir.

Yönetim Konsolu'nda (MMC) uygulama modülü güncellemelerini yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Veritabanlarının ve uygulama modüllerinin güncellemesi görev ayarları

5. **Yerel mod için ayarları güncelle** bloğunda, **Uygulama modüllerinin güncellemelerini indir** onay kutusunu seçin.

   Uygulama modülü güncellemelerinin indirilmesini önlemek istiyorsanız, **Uygulama modüllerinin güncellemelerini indir** onay kutusunun işaretini kaldırın ve yerel görevlerin kullanıcı tarafından kullanılmasını yasaklayın.

6. Yüklemek istediğiniz uygulama modülü güncellemelerini seçin.

   - **Kritik ve onaylı güncelleştirmeleri yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, kritik güncellemeleri otomatik olarak ve tüm diğer uygulama modülü güncellemelerini ise uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler.

   - **Yalnızca onaylı güncelleştirmeleri yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, güncellemeleri uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler. Bu seçenek varsayılan olarak seçilidir.

7. Gerekirse, mobil mod için uygulama modülü güncellemelerini yapılandırın. *Mobil mod*, Kaspersky Endpoint Security'nin bir bilgisayar kuruluş ağından ayrıldığı zamanki (*çevrimdışı bilgisayar*) işlem modudur.

8. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da uygulama modülü güncellemelerini yapılandırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

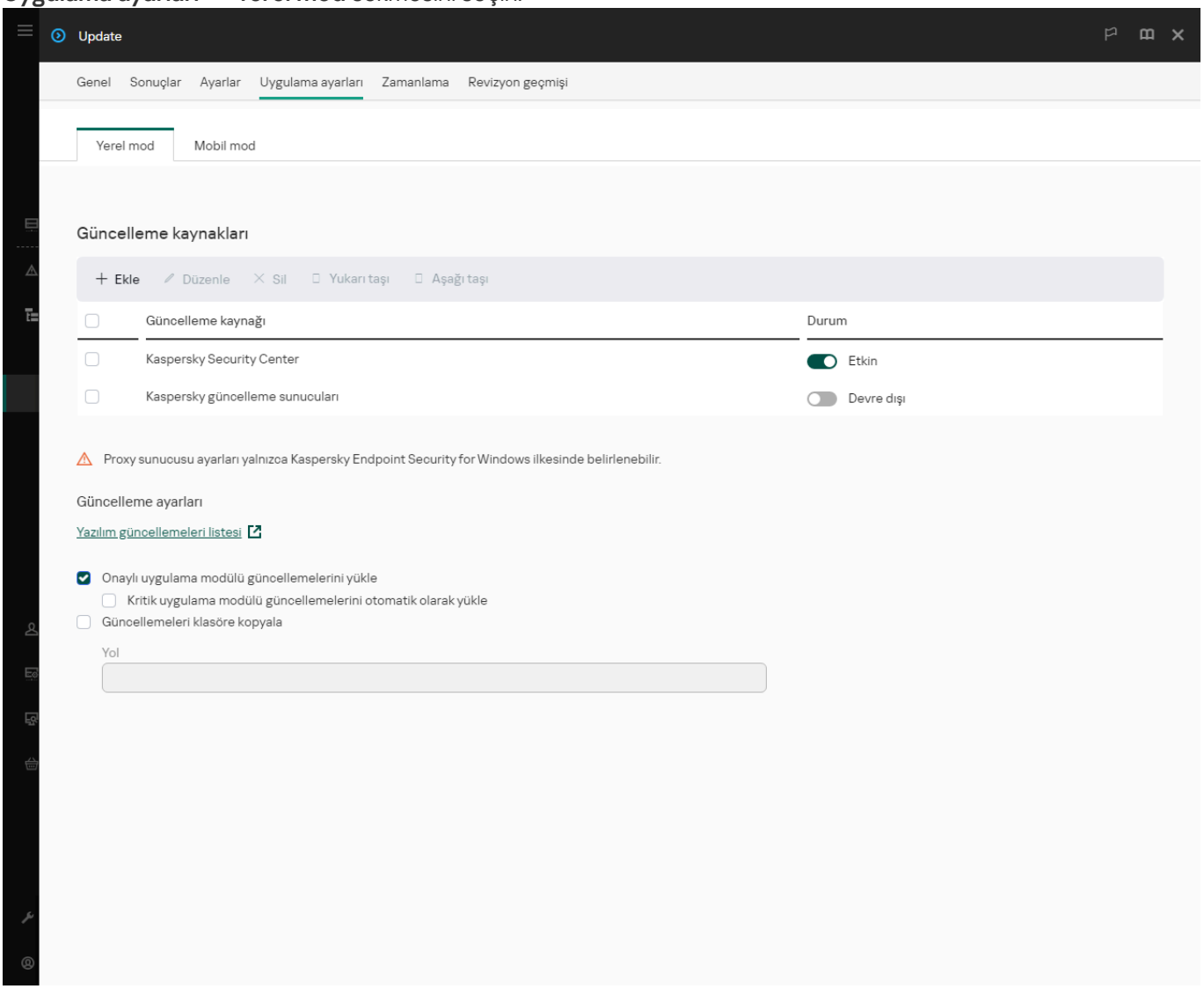
   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Veritabanlarının ve uygulama modüllerinin güncellemesi** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Veritabanlarının ve uygulama modüllerinin güncellemesi görevi, Yönetim Sunucusu hızlı başlatma sihirbazı tarafından otomatik olarak oluşturulur. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini oluşturmak için Sihirbaz çalışırken Kaspersky Endpoint Security for Windows Yönetim Eklentisini yükleyin.

3. **Uygulama ayarları** → **Yerel mod** sekmesini seçin.



Güncelleme görevi ayarları

4. **Güncelleme ayarlarından**, yüklemek istediğiniz uygulama modülü güncellemelerini seçin:

   - **Onaylı uygulama modülü güncellemelerini yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, güncellemeleri uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler. Bu seçenek varsayılan olarak seçilidir.

   - **Kritik uygulama modülü güncellemelerini otomatik olarak yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, kritik güncellemeleri otomatik olarak ve tüm diğer uygulama modülü güncellemelerini ise uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler.

   Uygulama modülü güncellemelerinin indirilmesini önlemek istiyorsanız, **Onaylı uygulama modülü güncellemelerini yükle** ve **Kritik uygulama modülü güncellemelerini otomatik olarak yükle** onay kutularının işaretini kaldırın ve kullanıcı tarafından yerel görevlerin kullanılmasını yasaklayın.

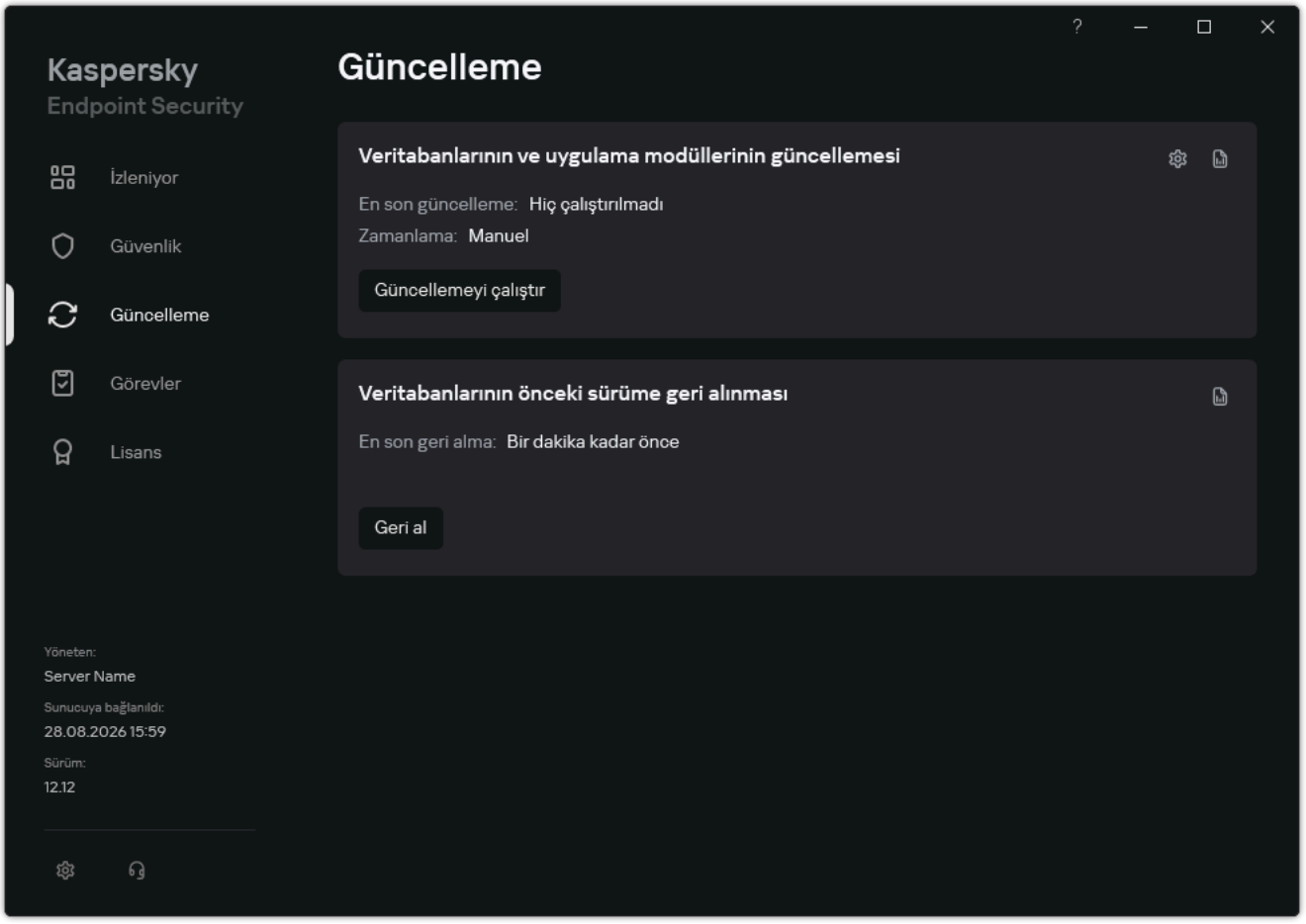
5. Gerekirse, mobil mod için uygulama modülü güncellemelerini yapılandırın. *Mobil mod*, Kaspersky Endpoint Security'nin bir bilgisayar kuruluş ağından ayrıldığı zamanki (*çevrimdışı bilgisayar*) işlem modudur.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde uygulama modülü güncellemelerini yapılandırma

Veritabanlarının ve uygulama modüllerinin güncellemesi grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellemesi* kullanıcı tarafından kullanılabilir. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Uygulama modüllerinin güncellemelerini indirme ve yükleme** bloğunda, **Uygulama modüllerinin güncellemelerini indir** onay kutusunu işaretleyin.

4. Yüklemek istediğiniz uygulama modülü güncellemelerini seçin.

   - **Kritik ve onaylı güncelleştirmeleri yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, kritik güncellemeleri otomatik olarak ve tüm diğer uygulama modülü güncellemelerini ise uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler.

   - **Yalnızca onaylı güncelleştirmeleri yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, güncellemeleri uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler. Bu seçenek varsayılan olarak seçilidir.

5. Değişikliklerinizi kaydedin.

Güncellemeler için proxy sunucusu kullanma

Güncelleme kaynağından veritabanı ve uygulama modülü güncellemelerini indirmek için belirli proxy sunucusu ayarlarına ihtiyacınız olabilir. Birden çok güncelleme kaynağı bulunursa proxy sunucusu ayarları tüm kaynaklar için uygulanır. Bazı güncelleme kaynakları için proxy sunucusu gerekli değilse ilke özelliklerinde bir proxy sunucusu kullanımını devre dışı bırakabilirsiniz. Kaspersky Endpoint Security, Kaspersky Security Network ve etkinleştirme sunucularına erişmek için bir proxy sunucu da kullanacaktır.

Bir proxy sunucusu üzerinden güncelleme kaynaklarına yönelik bağlantı yapılandırmak için:

1. Web Console ana penceresinde ⚙ öğesine tıklayın.

   Yönetim Sunucusu özellikleri penceresi açılır.

2. **İnternet erişimini yapılandırma** bölümüne gidin.

3. **Proxy sunucusunu kullan** onay kutusunu işaretleyin.

4. Proxy sunucusu bağlantı ayarlarını yapılandırın: proxy sunucusu adresi, bağlantı noktası ve kimlik doğrulama ayarları (kullanıcı adı ve parola).

5. Değişikliklerinizi kaydedin.

Belirli bir yönetim grubuna yönelik proxy sunucusunun kullanımını devre dışı bırakmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.

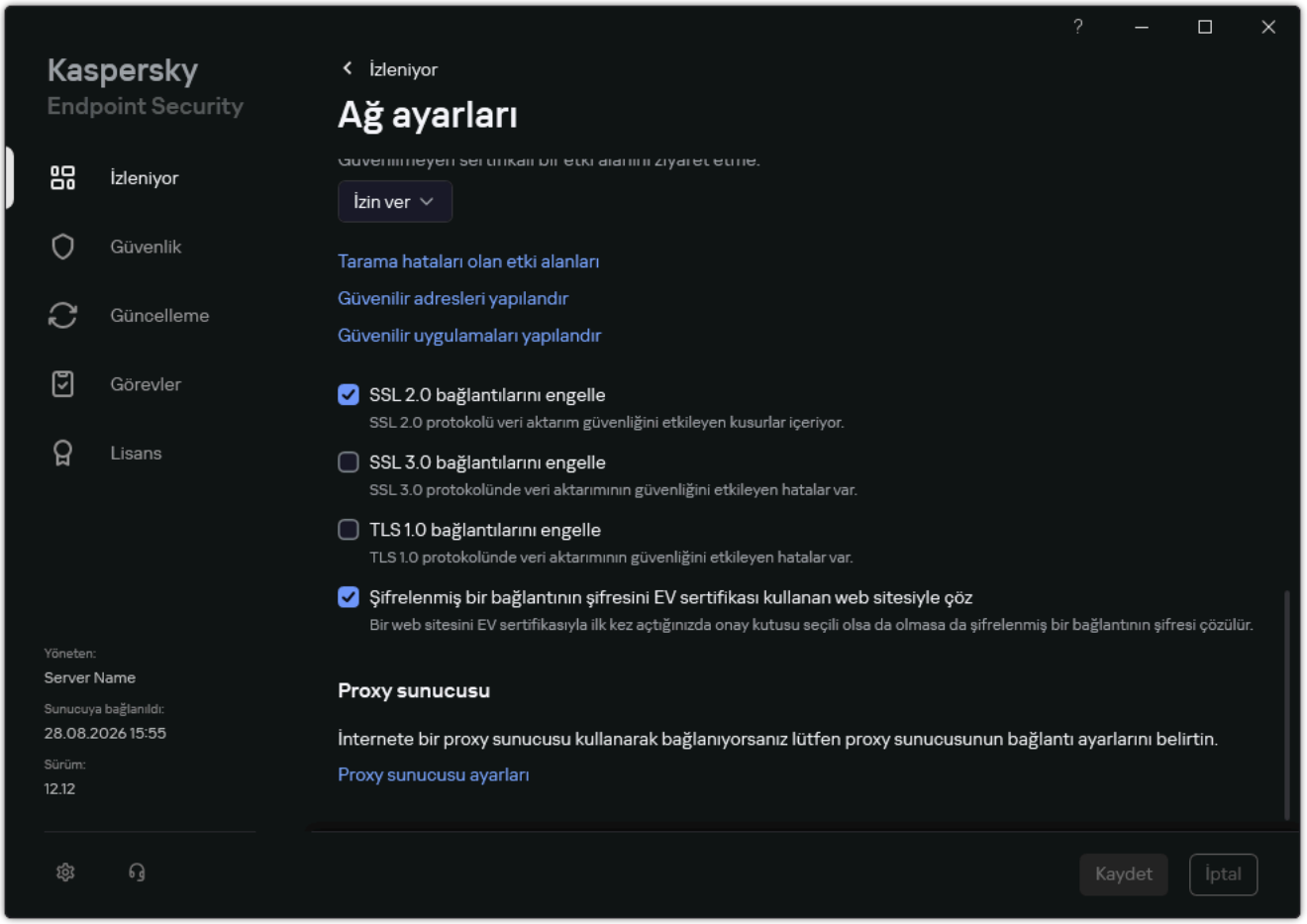
5. **Proxy sunucusu** bloğunda **Ayarlar** düğmesine tıklayın.

6. Açılan pencerede **Yerel adresler için proxy sunucusu atla** onay kutusunu seçin.

7. Değişikliklerinizi kaydedin.

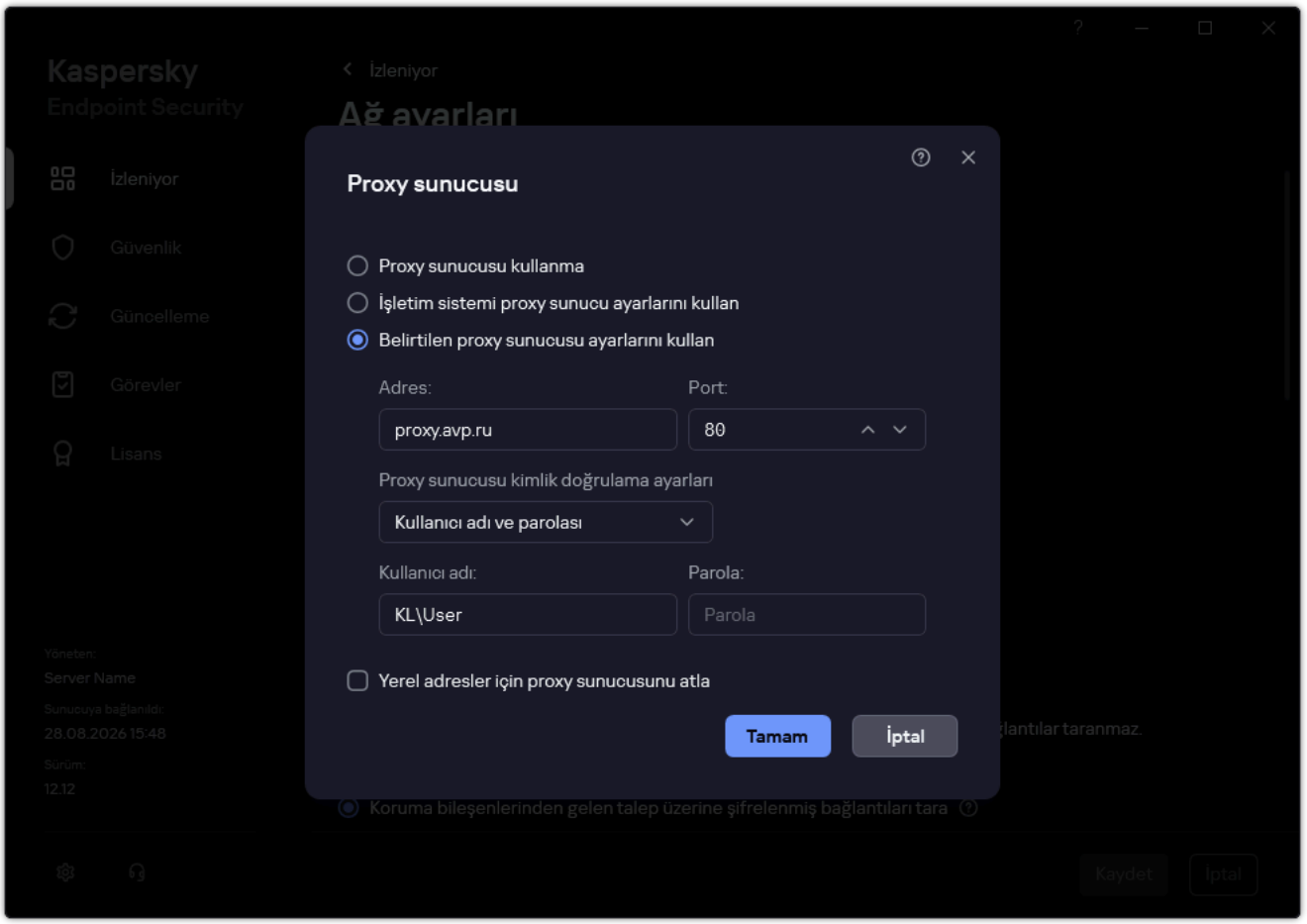
Proxy sunucusu ayarlarını uygulama arabiriminde yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



Uygulama ağ ayarları

3. **Proxy sunucusu** bloğunda, **Proxy sunucusu ayarları** bağlantısını tıklayın.



Proxy sunucusu bağlantı ayarları

4. Açılan pencerede, proxy sunucusu adresini belirlemek üzere aşağıdaki seçeneklerden birini seçin:

   - **İşletim sistemi proxy sunucusu ayarlarını kullan**.

     Bu seçenek varsayılan olarak seçilidir. Kaspersky Endpoint Security, işletim sistemi ayarlarında belirlenmiş olan proxy sunucusu ayarlarını kullanır.

   - **Belirtilen proxy sunucusu ayarlarını kullan**.

     Bu seçeneği seçtiyseniz, proxy sunucusuna bağlanmak için ayarları yapılandırın: proxy sunucu adresi ve bağlantı noktası.

5. Uygulamanın proxy sunucuda nasıl kimlik doğrulaması yapmasını istediğinizi seçin. Varsayılan olarak, uygulama geçerli kullanıcının etki alanı NTLM kimlik doğrulamasını kullanır.

6. Veritabanlarını ve uygulama modüllerini bir paylaşım klasöründen güncellerken proxy sunucusu kullanımını devre dışı bırakmak isterseniz **Yerel adresler için proxy sunucusunu atla** onay kutusunu işaretleyin.

7. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security, uygulama modülünü ve veritabanı güncellemelerini indirmek için proxy sunucusunu kullanacaktır. Kaspersky Endpoint Security, KSN sunucuları ve Kaspersky etkinleştirme sunucularına erişmek için bir proxy sunucusu da kullanacaktır. Proxy sunucusunda kimlik doğrulaması gerekiyorsa, ancak kullanıcı hesabı kimlik bilgileri girilmediyse veya yanlışsa, Kaspersky Endpoint Security sizden kullanıcı adı ve parola isteyecektir.

Son güncellemeyi geri alma

Veritabanları ve uygulama modülleri ikinci kez güncellendikten sonra, veritabanlarını ve uygulama modüllerini önceki sürümlerine geri alma işlevi kullanılabilir hale gelir.

Kullanıcı güncelleme işlemine her başladığında Kaspersky Endpoint Security, mevcut veritabanları ve uygulama modüllerinin bir yedekleme kopyasını oluşturur. Bu, gerektiğinde veritabanlarını ve uygulama modüllerini önceki sürümlerine geri almanıza olanak tanır. Son güncellemeyi geri almak, örneğin yeni bir veritabanı sürümünün hatalı pozitif bir sonuca yol açması ve bunun sonucunda Kaspersky Endpoint Security'nin güvenli bir uygulamayı engellemesi durumunda yararlı olabilir.

Light Agent modundaki Kaspersky Endpoint Security, *Güncellemeyi geri al* görevini desteklemez.

Yönetim Konsolu (MMC) üzerinde son güncellemeyi geri alma

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

1. **Kaspersky Endpoint Security for Windows (14.2)** → **Güncellemeyi geri al** seçimini yapın.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Bir görev başlatma zamanlaması yapılandırma

Görev zamanlamasını örneğin manuel olarak yapılandırın.

4. Adım. Görev adını tanımlama

Görev için bir ad girin.

7. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console'da son güncellemeyi geri alma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde **Geri Alma** seçeneğini belirleyin.

   c. **Görev adı** alanına kısa bir açıklama girin, örneğin, *Güncellemeyi geri al*.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

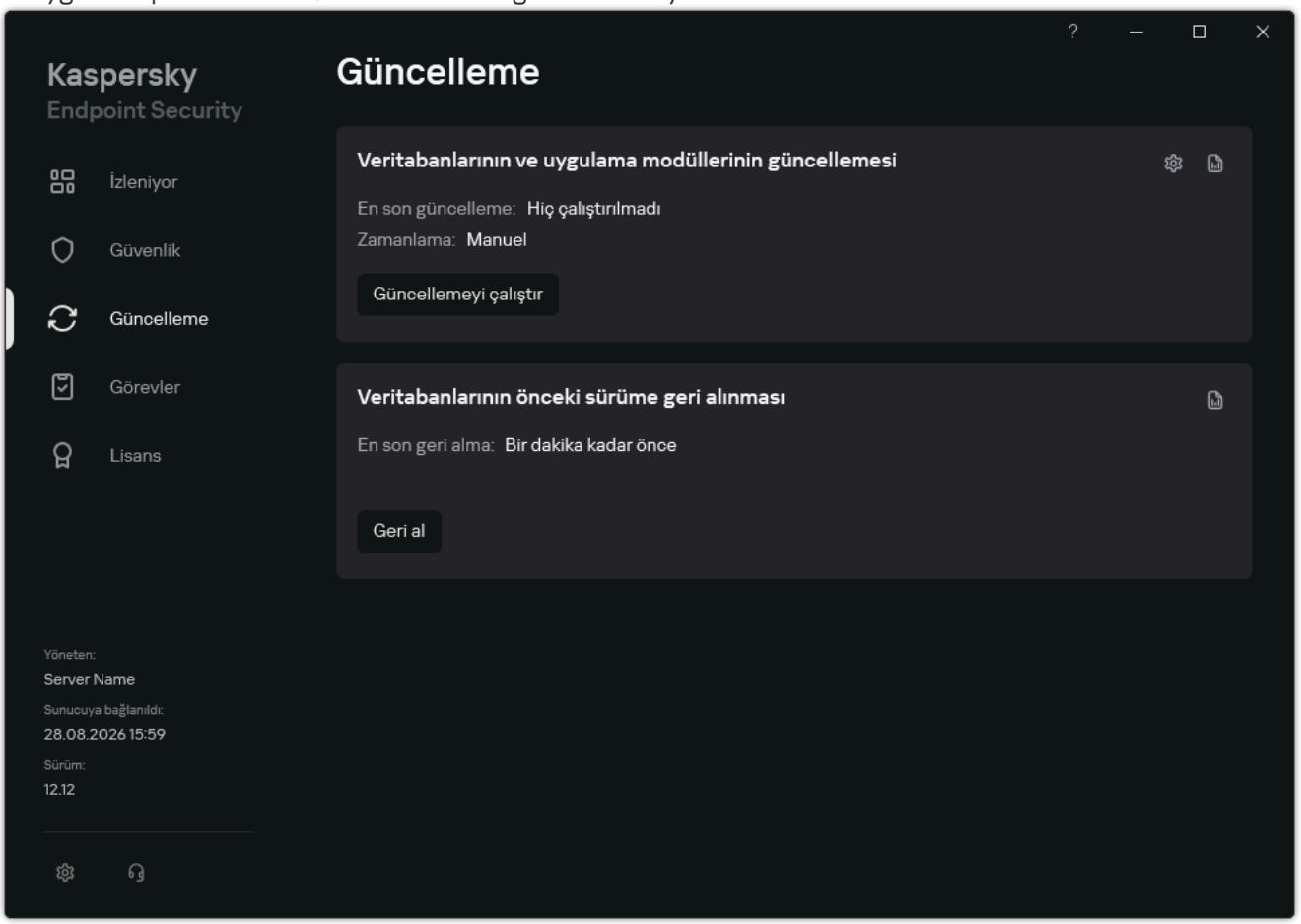
7. Görevler listesinde yeni bir görev görüntülenir.

8. Görevin yanındaki onay kutusunu seçin.

9. **Başlat**'a tıklayın.

Uygulama arabiriminde son güncellemeyi geri alma

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. **Veritabanlarının önceki sürüme geri alınması** kutucuğunda, **Geri al** düğmesine tıklayın.

Kaspersky Endpoint Security, son veritabanı güncellemesini geri almaya başlayacak. Uygulama geri alma ilerlemesini, indirilen dosyaların boyutunu ve güncelleme kaynağını gösterecektir. **Güncellemeyi durdur** düğmesine tıklayarak görevi istediğiniz zaman durdurabilirsiniz.

Gelişmiş temizleme teknolojisi

Kaspersky Endpoint Security, etkin tehditlerle çalışma için Gelişmiş Temizleme teknolojisini kullanır. Gelişmiş Temizleme, iş istasyonları ve sunucular için farklı çalışır. *Kötü Amaçlı Yazılım Taraması* görev ayarlarında ve uygulama ayarlarında gelişmiş temizlemeyi yapılandırabilirsiniz.

Kaspersky Endpoint Security bir kötü amaçlı yazılımın çalışmasını durduramadığında, Gelişmiş Temizleme teknolojisini kullanabilirsiniz. İlke kapsamındaki bilgisayarlar için, Gelişmiş Temizleme çok fazla bilgisayar kaynağı kullandığından varsayılan olarak devre dışı durumdadır. İlke kapsamına girmeyen bilgisayarlar için, Gelişmiş Temizleme varsayılan olarak etkindir.

Gelişmiş Temizleme, iş istasyonları ve sunucular için farklı çalışır. Bu teknolojiyi sunucularda kullanmak için, *Kötü Amaçlı Yazılım Tarama* görevinin özelliklerinde anında Gelişmiş Temizlemeyi etkinleştirmeniz gerekir. Bu ön şart, teknolojinin iş istasyonlarında kullanımı için gerekli değildir.

Yönetim Konsolu'nda (MMC) Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma

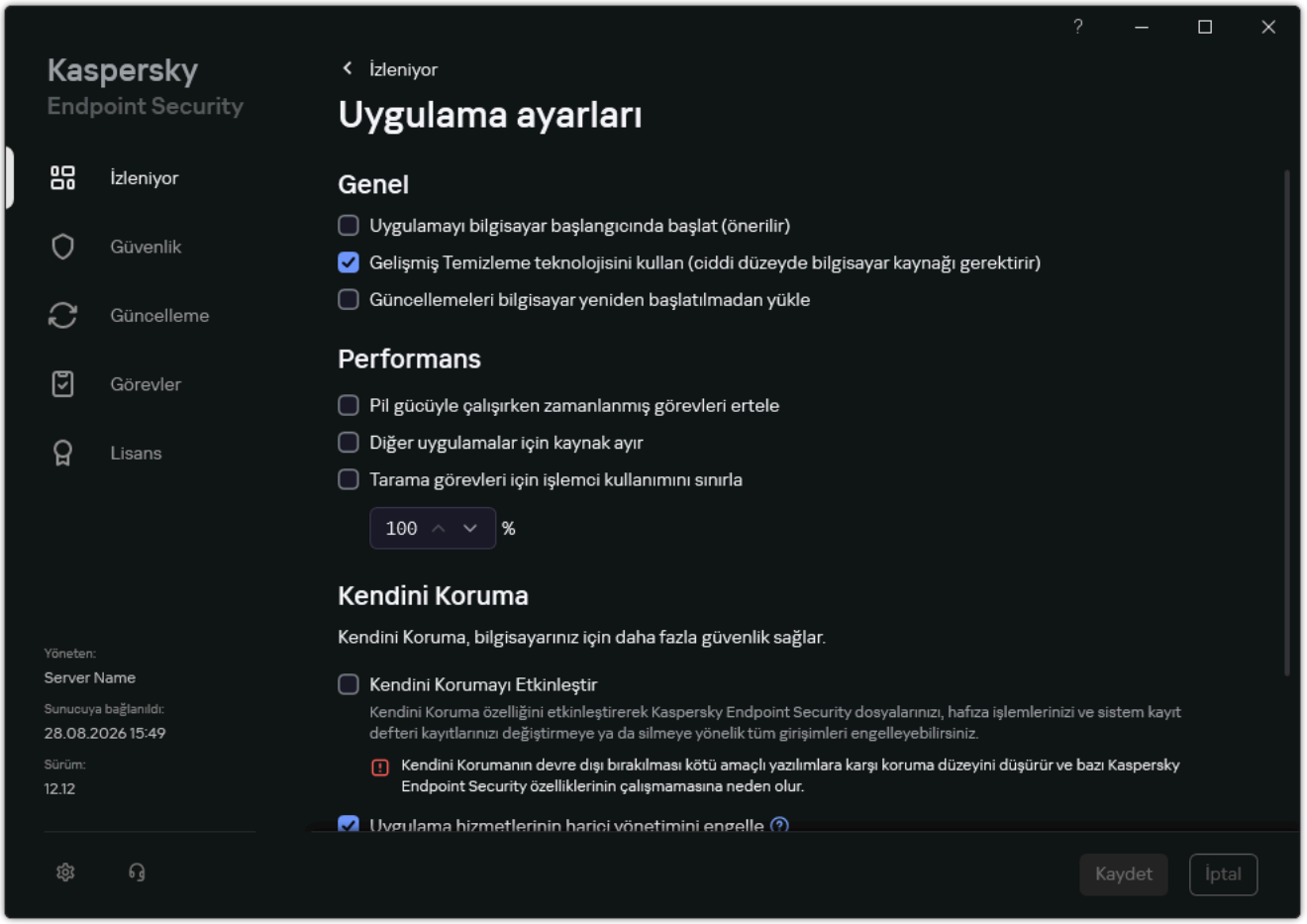
1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
4. **Genel** bloğunda, Gelişmiş Temizleme teknolojisini etkinleştirmek veya devre dışı bırakmak için **Gelişmiş Temizleme teknolojisini etkinleştir** onay kutusunu işaretleyin ya da işaretini kaldırın.
5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Gelişmiş Temizleme teknolojisi etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Tespit Ayarları** seçimini yapın.
5. **Gelişmiş Temizleme Teknolojisi** bloğunda, Gelişmiş Temizleme teknolojisini etkinleştirmek veya devre dışı bırakmak için **Gelişmiş Temizleme Teknolojisi ETKİN** anahtarını açın veya kapatın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

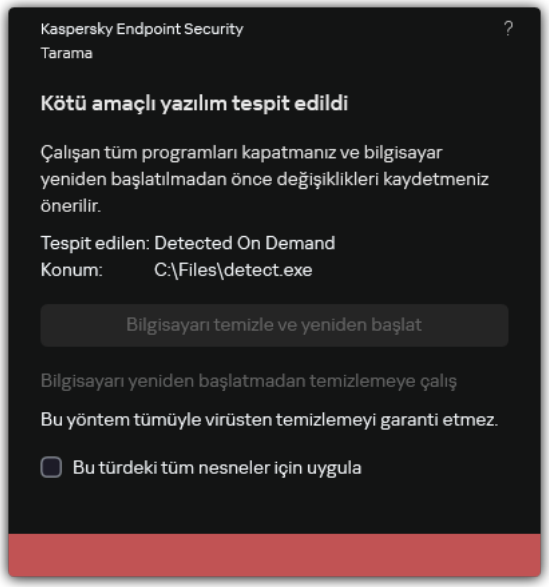
3. **Genel** bloğunda, Gelişmiş Temizleme teknolojisini etkinleştirmek veya devre dışı bırakmak için **Gelişmiş Temizleme teknolojisini kullan (ciddi düzeyde bilgisayar kaynağı gerektirir)** onay kutusunu işaretleyin ya da işaretini kaldırın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak kullanıcı, Gelişmiş Temizleme devam ederken çoğu işletim sistemi özelliğini kullanamaz. Temizlik tamamlandığında bilgisayar yeniden başlatılır.

İş istasyonlarındaki etkin tehditlerin temizlenmesi

İş istasyonlarındaki etkin tehditlerle çalışma için uygulama ayarlarından Gelişmiş Temizleme teknolojisini etkinleştirin. Ardından, *Kötü Amaçlı Yazılım Taraması* görev özelliklerinden kullanıcı deneyimini yapılandırın. Görev özelliklerinde **Gelişmiş Temizleme işlemini derhal çalıştır** şeklinde bir kutucuk vardır. Bu bayrak ayarlandığında, Kaspersky Endpoint Security temizleme işlemini kullanıcıya bildirim yapmadan gerçekleştirir. Temizlik tamamlandığında bilgisayar yeniden başlatılır. Bayrak ayarlanmadığında, Kaspersky Endpoint Security etkin tehditler hakkında bir bildirim görüntüler (aşağıdaki şekle bakın). Dosyayı işlemeden bu bildirimi kapatamazsınız.

Bir bilgisayardaki virüs taraması görevi sırasında Gelişmiş Temizleme işlemi yalnızca, bu bilgisayara uygulanan ilkenin özelliklerinde Gelişmiş Temizleme özelliği etkinleştirilmişse gerçekleştirilir.



Etkin tehdit hakkında bildirim

Sunuculardaki etkin tehditlerin temizlenmesi

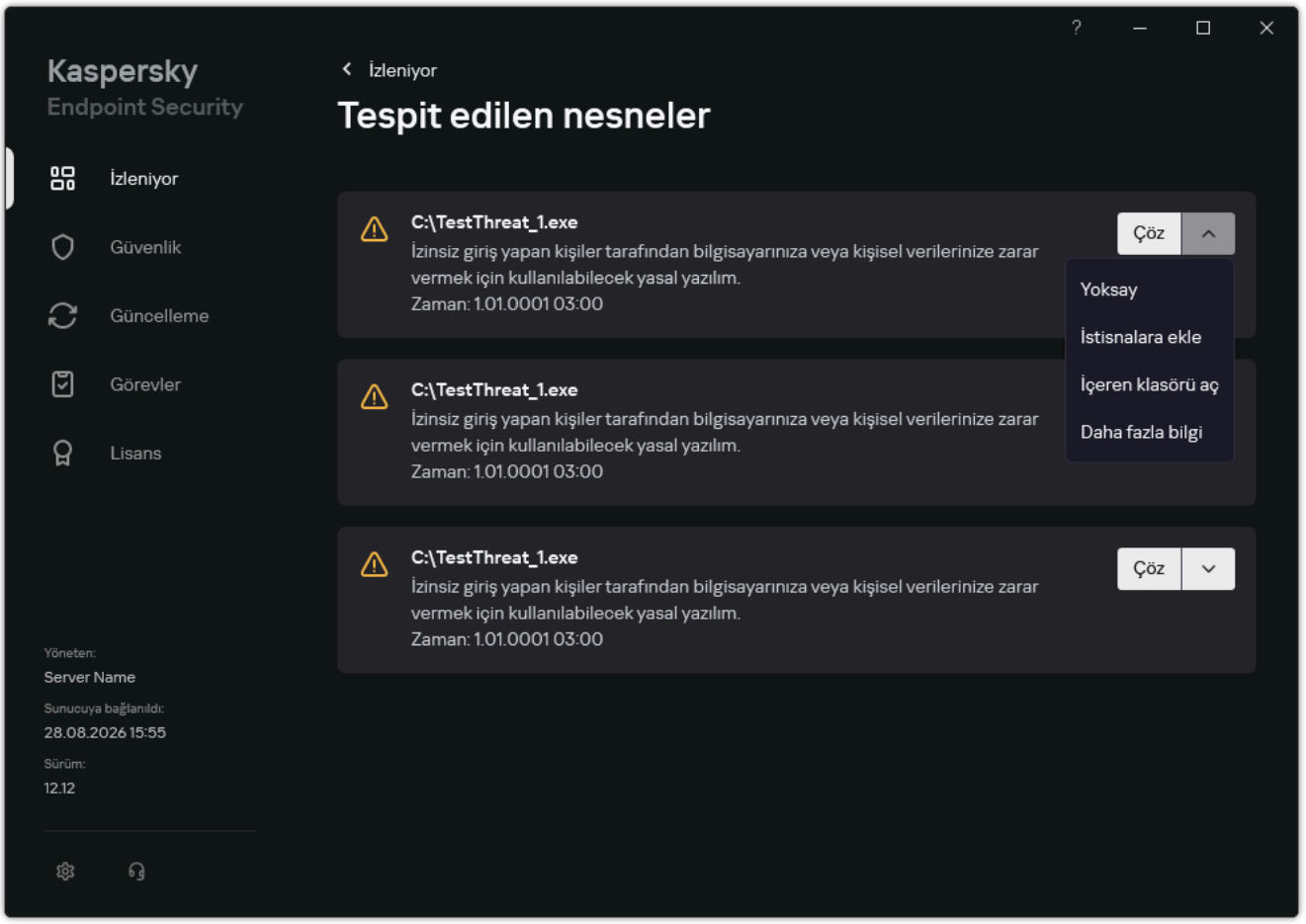
Sunuculardaki etkin tehditlerle çalışma için şunları yapmanız gerekir:

- uygulama ayarlarından Gelişmiş Temizleme teknolojisini etkinleştirin;
- *Kötü Amaçlı Yazılım Taraması* görev ayarlarından Gelişmiş temizlemeyi derhal çalıştırın.

Kaspersky Endpoint Security, Windows for Servers çalıştıran bir bilgisayarda yüklüyse Kaspersky Endpoint Security bildirimi görüntülemez. Bu nedenle, etkin bir tehdidi temizlemek için bir eylem seçemezsiniz. Bir tehdidi temizlemek için uygulama ayarlarından Gelişmiş Temizleme teknolojisini etkinleştir ve *Kötü Amaçlı Yazılım Taraması* görev ayarlarından Gelişmiş Temizlemeyi derhal çalıştır seçimini yapın. Ardından *Kötü Amaçlı Yazılım Taraması* görevini başlatmalısınız.

İşlenmemiş tehditleri ortadan kaldırma

Kaspersky Endpoint Security bazı nedenlerle işlemediği dosyalar hakkında bilgi kaydeder. Bu bilgiler, etkin tehditler listesine olaylar biçiminde kaydedilir (aşağıdaki resme bakın).



Etkin tehditlerin listesi

Virüslü bir dosya, Kaspersky Endpoint Security bilgisayarı virüslere ve diğer kötü amaçlı yazılımlara karşı taramanın bir parçası olarak dosyayı temizlediyse veya tehdidi kaldırdıysa *işlenmiş* kabul edilir.

Kaspersky Endpoint Security, bilgisayarda virüs ve diğer tehditlerin taramasını yaparken herhangi bir nedenle belirtilen uygulama ayarlarına göre bu virüslü dosyada bir işlem gerçekleştiremezse dosyayı etkin tehditler listesine taşır.

Bu durumla aşağıdaki örneklerde karşılaşılabilir:

- Taranan dosya erişilemez durumdadır (örneğin bir ağ sürücüsünde veya yazma ayrıcalığı bulunmayan bir çıkarılabilir sürücüde bulunmaktadır).
- *Kötü Amaçlı Yazılım Taraması* görev ayarlarında, tehdit algılandığında yapılacak eylem olarak **Bilgilendir** ayarlıdır. Ardından, ekranda virüslü dosya bildirimi görüntülendiğinde, kullanıcı **Yoksay** seçimini yapar.

İşlenmemiş tehditler varsa Kaspersky Endpoint Security simgeyi olarak değiştirir. Ana uygulama penceresinde tehdit bildirimi görüntülenir (aşağıdaki şekle bakın). Kaspersky Security Center konsolunda, bilgisayarın durumu *Kritik* - olarak değiştirilir.

Yönetim Konsolu'nda (MMC) bir tehdit nasıl işlenir

1. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Gelişmiş** → **Veri havuzları** → **Etkin tehditler** klasörüne gidin.

   Etkin tehditler listesi açılır.

2. İşlemek istediğiniz nesneyi seçin.

3. Tehdit karşısında ne yapılmasını istediğinizi seçin:

   - **Temizle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.

   - **Sil**. Bu seçenek seçildiğinde, uygulama aktif tehditler deposundan tespit edilen virüslü dosyaları siler. Bu durumda, uygulama algılanan dosyayı bilgisayarın belleğinde tutar. Bilgisayardaki tehdidi ortadan kaldırmak için **Temizle**'yi seçin.

Web Console'da ve Cloud Console'da bir tehdit nasıl işlenir

1. Web Console ana penceresinden **İşlemler** → **Veri havuzları** → **Etkin tehditler** seçimini yapın.

   Etkin tehditler listesi açılır.

2. İşlemek istediğiniz nesneyi seçin.

3. Tehdit karşısında ne yapılmasını istediğinizi seçin:

   - **Temizle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.

   - **Sil**. Bu seçenek seçildiğinde, uygulama aktif tehditler deposundan tespit edilen virüslü dosyaları siler. Bu durumda, uygulama algılanan dosyayı bilgisayarın belleğinde tutar. Bilgisayardaki tehdidi ortadan kaldırmak için **Temizle**'yi seçin.

Uygulama arabiriminde bir tehdit nasıl işlenir

1. Ana uygulama penceresinde, **İzleniyor** bölümündeki **Koruma risk altında** kutucuğuna tıklayın.

   Etkin tehditler listesi açılır.

2. İşlemek istediğiniz nesneyi seçin.

3. Tehdit karşısında ne yapılmasını istediğinizi seçin:

   - **Çöz**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.

   - **İstisnalara ekle**. Bu eylem seçilirse, Kaspersky Endpoint Security dosyayı tarama istisnaları listesine ekleme önerisinde bulunur. İstisna ayarları otomatik olarak yapılandırılır. Bir istisna eklenemiyorsa bu, yöneticinin ilke ayarlarında istisna eklemeyi devre dışı bıraktığı anlamına gelir.

   - **Yoksay**. Bu seçenek işaretlenirse, Kaspersky Endpoint Security girişi etkin tehditler listesinden siler. Listede etkin tehdit kalmadığında, bilgisayar durumu *Tamam* olarak değiştirilir. Nesne tekrar tespit edilirse, Kaspersky Endpoint Security etkin tehditler listesine yeni bir giriş ekler.

- **İçeren klasörü aç**. Bu seçenek işaretlenirse, Kaspersky Endpoint Security nesneyi içeren klasörü dosya yöneticisinde açar. Daha sonra nesneyi manuel olarak silebilir veya nesneyi koruma kapsamında olmayan bir klasöre taşıyabilirsiniz.

- **Daha fazla bilgi**. Bu seçenek seçildiğinde, Kaspersky Endpoint Security, Kaspersky zayıf noktalar ve tehditler veritabanı web sitesini açar.

Kaspersky Security Center konsolunda etkin tehditleri işlemek için, işlenmemiş dosyalar hakkındaki bilgilerin Yönetim Sunucusu'na aktarılmasını etkinleştirmeniz gerekir. Veri aktarımı varsayılan olarak etkindir.

Yönetim Konsolu'nda (MMC) işlenmemiş dosya verilerinin aktarımı nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.
4. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Ayarlar** düğmesine tıklayın.
5. **İşlenmemiş dosyalar** onay kutusunu seçin.
6. Değişikliklerinizi kaydedin.

Web Console'da işlenmemiş dosya verilerinin aktarımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.

5. **Yönetim Sunucusu'na veri aktarımı** bloğundan **İşlenmemiş dosyalar hakkında** onay kutusunu işaretleyin.

6. Değişikliklerinizi kaydedin.



Bir tehdit algılandığında ana uygulama penceresi

Bilgisayar koruması

Gerçek Zamanlı Koruma durumu

Kaspersky Endpoint Security, **Gerçek zamanlı koruma durumu** ayarını Kaspersky Security Center Yönetim Sunucusuna gönderir; bu ayarın değeri, korunan bilgisayardaki uygulama koruma bileşenlerinin geçerli durumuna bağlıdır (aşağıdaki tabloya bakın).

Kaspersky Endpoint Security, gerçek zamanlı koruma durumunu aşağıdaki uygulama bileşenlerinin durumuna göre belirler:

- Dosya Tehdidi Koruması.
- Web Tehdidi Koruması.
- Posta Tehdidi Koruması.
- AMSI Koruması.
- BadUSB Saldırısı Önleme.
- Ağ Tehdidi Koruması.
- Güvenlik Duvarı.
- Exploit Önleme.
- Davranış Tespiti.
- Düzeltme Altyapısı.
- Sunucu Yetkisiz Erişim Önleme.

Uygulamanın gerçek zamanlı koruma durumunu Kaspersky Security Center konsolundan kontrol edebilirsiniz.

Yönetim Konsolu'nda (MMC) Gerçek Zamanlı Koruma durumu nasıl öğrenilir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Yönetilen cihazlar**.

Geçerli Gerçek Zamanlı Koruma durumu, cihazlar listesindeki **Gerçek zamanlı koruma durumu** sütununda görüntülenir. **Gerçek zamanlı koruma durumu** sütunu yoksa **Sütun Ekle/Kaldır** bağlantısına tıklayarak sütun ayarlarını yönetin.

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Yönetilen cihazlar**.

Geçerli Gerçek Zamanlı Koruma durumu, cihazlar listesindeki **Gerçek zamanlı koruma durumu** sütununda görüntülenir. **Gerçek zamanlı koruma durumu** sütunu yoksa **Sütun Ekle/Kaldır** bağlantısına tıklayarak sütun ayarlarını yönetin.

Web Console'da Gerçek zamanlı bilgisayar koruması nasıl öğrenilir

Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.

Geçerli Gerçek Zamanlı Koruma durumu, cihazlar listesindeki **Gerçek zamanlı koruma durumu** sütununda görüntülenir. **Gerçek zamanlı koruma durumu** sütunu yoksa sütun ayarlarını yönetin (⚙).

Gerçek zamanlı koruma durumu ayarının olası değerleri

Değer	Açıklama
Bilinmiyor	Yönetim Sunucusu, bu bilgisayarın gerçek zamanlı koruma durumu hakkında bilgi sahibi değildir.
Yüklü değil	Hiçbir bileşen yüklü değil.
Lisans tarafından desteklenmiyor	Uygulama etkinleştirilmemiştir veya lisans, yüklü bileşenlerin çalışmasına izin vermiyordur.
Başarısız	Bir veya daha fazla bileşen arızalanmıştır.
Durduruldu	Bir veya daha fazla bileşen devre dışıdır.
Duraklatıldı	Bir veya daha fazla bileşen duraklatılmıştır.
Başlatılıyor	Bir veya daha fazla bileşen etkinleştiriliyor.
Çalışıyor	Uygulama bileşenleri çalışır durumdadır.

Kaspersky Security Center'daki **Gerçek zamanlı koruma durumu** ayarının değeri *Çalışıyor* değerinden farklıysa listedeki yüklü Kaspersky Endpoint Security bileşenlerinin etkinleştirildiğini ve uygulamanın etkinleştirilmiş olduğunu kontrol edin.

Dosya Tehdidi Koruması

Dosya Tehdidi Koruması bileşeni, bir bilgisayar dosya sistemine bulaşmasını önlemenizi sağlar. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni bilgisayarın RAM'inde kalıcı olarak bulunur ve açılan, kaydedilen veya çalıştırılan tüm dosyaları gerçek zamanlı olarak tarar. Bu bileşen, bağlı sürücüler de dahil olmak üzere tüm bilgisayar sürücülerindeki dosyaları tarar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Bileşen, kullanıcı veya uygulama tarafından erişilen dosyaları tarar. Zararlı bir nesnenint epsit edilmesi durumunda Kaspersky Endpoint Security dosyanın çalışmasını engeller. Uygulama bundan sonra zararlı dosyayı Dosya Tehdidi Koruması bileşeninin ayarlarına göre temizler veya siler.

OneDrive bulut depolama alanında bulunan bir dosyaya erişmeye çalışırken, Kaspersky Endpoint Security dosya içeriğini indirir ve tarar.

Dosya Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Dosya Tehdidi Koruması bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Dosya Tehdidi Koruması için Kaspersky Endpoint Security, farklı ayar grupları uygulayabilir. Uygulama içinde saklanan bu ayar gruplarına *güvenlik düzeyleri* denir: **Yüksek**, **Önerilen**, **Düşük**. **Önerilen** güvenlik düzeyi ayarları Kaspersky uzmanları tarafından tavsiye edilen en iyi ayarlar olarak değerlendirilir (aşağıdaki tabloya bakın). Ön tanımlı güvenlik düzeylerinden birini seçebilir veya güvenlik düzeyi ayarlarını manuel olarak yapılandırabilirsiniz. Güvenlik düzeyi ayarlarını değiştirirseniz önerilen güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

Dosya tehdidi koruması bileşeni, diğer uygulama bileşenlerinden alınan verileri kullanır. Bu bileşenlerin etkinleştirilmesi isteğe bağlıdır. Ek veriler sunan bileşenler şunlardır:

- Kaspersky Security Network.
- Sunucu Yetkisiz Erişim Önleme.
- Davranış Tespiti.

Yönetim Konsolu'nda (MMC) Dosya Tehdidi Koruması bileşeni nasıl etkinleştirilir veya devre dışı bırakılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Dosya Tehdidi Koruması** kutucuğunu işaretleyin.
5. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:
   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.
     - **Yüksek**. Bu dosya güvenlik düzeyi seçildiğinde Dosya Tehdidi Koruması bileşeni açılan, kaydedilen ve başlatılan tüm dosyaların en sıkı denetimini gerçekleştirir. Dosya Tehdidi Koruması bileşeni, bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde bulunan tüm dosya türlerini tarar. Ayrıca arşivleri, kurulum paketlerini ve gömülü OLE nesnelerini de tarar.
     - **Önerilen**. Kaspersky Lab uzmanları bu dosya güvenlik düzeyini önerir. Dosya Tehdidi Koruması bileşeni, bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde bulunan yalnızca belirtilen dosya biçimlerini ve gömülü OLE nesnelerini tarar. Dosya Tehdidi Koruması bileşeni, arşivleri veya kurulum paketlerini taramaz.
     - **Düşük**. Bu dosya güvenliği düzeyi ayarları maksimum tarama hızı sağlar. Dosya Tehdidi Koruması bileşeni bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde yalnızca belirtilen uzantılara sahip dosya türlerini tarar. Dosya Tehdidi Koruması bileşeni birleşik dosyaları taramaz.
   - Özel bir güvenlik düzeyi yapılandırmak istiyorsanız **Ayarlar** düğmesine tıklayın ve kendi bileşen ayarlarınızı tanımlayın (aşağıdaki tabloya bakın).

     Varsayılan olarak düğmesine tıklayarak önceden ayarlanmış güvenlik düzeylerinin değerlerini geri yükleyebilirsiniz.
6. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı nesneler üzerinde gerçekleştireceği eylemi seçin:
   - **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.
   - **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama bu dosyayı engeller.
   - **Engelle**. Bu seçenek seçildiğinde, uygulama virüs bulaşmış dosyayı temizlemeye veya silmeye çalışmadan otomatik olarak engeller.
   - **Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.

Uygulama, virüslü bir dosyayı temizlemeye veya silmeye başlamadan önce, dosyayı geri yüklemeniz gerekip gerekmediğini veya ileride temizlenebileceğini düşünerek dosyanın bir yedekleme kopyasını oluşturur.

7. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Dosya Tehdidi Koruması bileşenini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Dosya Tehdidi Koruması** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Dosya Tehdidi Koruması ETKİN** geçiş düğmesini kullanın.
6. Koruma kapsamına yeni bir nesne eklemek isterseniz:
   a. **Gelişmiş ayarlar** bölümünde, **Koruma kapsamı** sekmesini seçin.
   b. **Ekle**'ye tıklayın.
   c. Bir pencere açılır; bu pencerede koruma kapsamına eklemek istediğiniz nesneleri seçin.
      Maskeler kullanarak:
      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
      - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.
      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

      Maskeleri bir dosya veya klasör yolunda herhangi bir yerde kullanabilirsiniz. Örneğin, tarama kapsamının bilgisayardaki tüm kullanıcı hesapları için İndirilenler klasörünü içermesini istiyorsanız, `C:\Users\*\Downloads\` maskesini girin.

      Bir nesneyi, koruma kapsamındaki nesneler listesinden kaldırmadan korumanın dışında bırakabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.
   d. Değişikliklerinizi kaydedin.

7. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı nesneler üzerinde gerçekleştireceği eylemi seçin:

   - **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.
   - **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama bu dosyayı engeller.
   - **Engelle**. Bu seçenek seçildiğinde, uygulama virüs bulaşmış dosyayı temizlemeye veya silmeye çalışmadan otomatik olarak engeller.

   Uygulama, virüslü bir dosyayı temizlemeye veya silmeye başlamadan önce, dosyayı geri yüklemeniz gerekip gerekmediğini veya ileride temizlenebileceğini düşünerek dosyanın bir yedekleme kopyasını oluşturur.

8. Gerekirse, Dosya Tehdidi Koruması için gelişmiş ayarları düzenleyin.
9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Dosya Tehdidi Koruması bileşenini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Dosya Tehdidi Koruması**'nı seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Dosya Tehdidi Koruması** geçiş düğmesini kullanın.
4. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:

   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.
     - **Yüksek**. Bu dosya güvenlik düzeyi seçildiğinde Dosya Tehdidi Koruması bileşeni açılan, kaydedilen ve başlatılan tüm dosyaların en sıkı denetimini gerçekleştirir. Dosya Tehdidi Koruması bileşeni, bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde bulunan tüm dosya türlerini tarar. Ayrıca arşivleri, kurulum paketlerini ve gömülü OLE nesnelerini de tarar.
     - **Önerilen**. Kaspersky Lab uzmanları bu dosya güvenlik düzeyini önerir. Dosya Tehdidi Koruması bileşeni, bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde bulunan yalnızca belirtilen dosya biçimlerini ve gömülü OLE nesnelerini tarar. Dosya Tehdidi Koruması bileşeni, arşivleri veya kurulum paketlerini taramaz.
     - **Düşük**. Bu dosya güvenliği düzeyi ayarları maksimum tarama hızı sağlar. Dosya Tehdidi Koruması bileşeni bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde yalnızca belirtilen uzantılara sahip dosya türlerini tarar. Dosya Tehdidi Koruması bileşeni birleşik dosyaları taramaz.
   - Özel bir güvenlik düzeyi yapılandırmak istiyorsanız **Gelişmiş ayarlar** düğmesine tıklayın ve kendi bileşen ayarlarınızı tanımlayın (aşağıdaki tabloya bakın).

     Önerilen güvenlik düzeyini geri yükle düğmesine tıklayarak önceden ayarlanmış güvenlik seviyelerinin değerlerini geri yükleyebilirsiniz.

5. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı nesneler üzerinde gerçekleştireceği eylemi seçin:

   - **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.
   - **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama bu dosyayı engeller.
   - **Engelle**. Bu seçenek seçildiğinde, uygulama virüs bulaşmış dosyayı temizlemeye veya silmeye çalışmadan otomatik olarak engeller.
   - **Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.

   Uygulama, virüslü bir dosyayı temizlemeye veya silmeye başlamadan önce, dosyayı geri yüklemeniz gerekip gerekmediğini veya ileride temizlenebileceğini düşünerek dosyanın bir yedekleme kopyasını oluşturur.

6. Değişikliklerinizi kaydedin.

Kaspersky uzmanları tarafından önerilen Dosya Tehdidi Koruması ayarları (önerilen güvenlik düzeyi)

Parametre	Değer	Açıklama
Dosya türleri	**Biçime göre taranan dosyalar**	Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Bir dosyada kötü amaçlı kod taraması yapmadan önce dosyanın iç başlığı, dosyanın biçimini (örneğin, .txt, .doc veya .exe) belirlemek için analiz edilir. Tarama ayrıca belirli dosya uzantılarına sahip dosyaları arar.
Sezgisel analiz	**Hızlı tarama**	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. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
Sadece yeni ve değiştirilmiş dosyaları tara	**Açık**	Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.
iSwift teknolojisini kullan	**Açık**	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.
iChecker teknolojisini kullan	**Açık**	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).
Microsoft Office biçimlerindeki dosyaları tara	**Açık**	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.
E-posta biçimindeki dosyaları tara	**Açık**	E-posta biçimindeki dosyaları tarar. Uygulama MSG ve EML dosyalarını tarar. E-posta biçimindeki dosyalar da OLE nesnelerini ve MHT dosyalarını içerir. Kaspersky Endpoint Security, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük e-posta biçimlerindeki dosyaları tarar.
Tarama modu	**Akıllı mod**	Bu modda, Dosya Tehdidi Koruması bir nesneyi o nesnede yapılan eylemlerin çözümlemesine dayalı olarak tarar. Örneğin, bir Microsoft Office belgesi ile çalışırken Kaspersky Endpoint Security dosyayı ilk açıldığında ve son kapandığında tarar. Dosyanın üzerine yazan ara işlemler taranmasına neden olmaz.
Tehdit algılandığında yapılacak eylem	**Temizle; temizleme başarısız olursa sil**	Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.

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 bileşen çalışırken herhangi bir çakışma meydana gelirse, Kaspersky Teknik Destek ile iletişime geçmeniz önerilir. 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 ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.
4. **Dosya Tehdidi Korumasını Duraklat** bloğunda, **Dosya Tehdidi Korumasını Duraklat** bağlantısına tıklayın.
5. Açılan pencerede, Dosya Tehdidi Korumasını duraklatmak için ayarları yapılandırın:
   a. Dosya Tehdidi Korumasını otomatik olarak duraklatmak için bir zamanlama yapılandırın.
   b. Çalışması, Dosya Tehdidi Korumasının etkinliklerini duraklatmasına neden olması gereken uygulamaların bir listesini oluşturun.
6. Değişikliklerinizi kaydedin.

Dosya Tehdidi Koruması bileşeni tarafından virüslü dosyalara uygulanacak eylemi değiştirme

Varsayılan olarak, Dosya Tehdidi Koruması bileşeni tespit edilen tüm virüslü dosyaları otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa Dosya Tehdidi Koruması bileşeni bu dosyaları siler.

Dosya Tehdidi Koruması bileşeni tarafından virüslü dosyalara uygulanacak eylemi değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.

3. **Tehdit algılandığında yapılacak eylem** bloğunda gereken seçeneği seçin:

   - **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler.
   - **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama bu dosyayı engeller.
   - **Engelle**. Bu seçenek seçildiğinde, uygulama virüs bulaşmış dosyayı temizlemeye veya silmeye çalışmadan otomatik olarak engeller.

   Uygulama, virüslü bir dosyayı temizlemeye veya silmeye başlamadan önce, dosyayı geri yüklemeniz gerekip gerekmediğini veya ileride temizlenebileceğini düşünerek dosyanın bir yedekleme kopyasını oluşturur.

4. Değişikliklerinizi kaydedin.

Dosya Tehdidi Koruması bileşeninin koruma kapsamını oluşturma

Koruma kapsamı, etkinleştirildiği zaman bileşenin taradığı nesneleri ifade eder. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir. Taranacak dosyaların konumu ve türü, Dosya Tehdidi Koruması bileşeninin koruma kapsamının özellikleridir. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni yalnızca sabit sürücülerde, çıkarılabilir sürücülerde ve ağ sürücülerinde çalıştırılan potansiyel olarak virüs bulaşabilecek dosyaları tarar.

Taranacak dosya türünü seçerken aşağıdakileri unutmayın:

1. Belirli biçimlerdeki dosyalara kötü amaçlı kod girmesi ve daha sonra etkinleşmesi olasılığı düşüktür (örneğin TXT biçimi). Aynı zamanda yürütülebilir kod içeren dosya biçimleri de (.exe, .dll gibi) bulunmaktadır. Yürütülebilir kod aynı zamanda bu amaç için olmayan dosya biçimlerinde de yer alabilir (örneğin DOC biçimi). Bu tür dosyaların kötü amaçlı kod içerme ve etkinleştirme riski yüksektir.

2. Bir saldırgan .txt uzantılı olarak yeniden adlandırılmış yürütülebilir bir dosya şeklinde bir virüs veya zararlı uygulamayı bilgisayarınıza gönderebilir. Uzantıya göre dosyaların taranmasını seçerseniz tarama sırasında uygulama bu dosyayı atlar. Biçime göre dosya taraması seçilirse Kaspersky Endpoint Security, uzantıdan bağımsız olarak dosya başlığını analiz eder. Bu analizde dosyanın yürütülebilir dosya formatında olduğu tespit edilirse (örneğin, EXE) uygulama bu dosyayı tarar.

Koruma kapsamını oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Dosya Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.

4. **Dosya türleri** bloğunda, Dosya Tehdidi Koruması bileşeninin taramasını istediğiniz dosya türlerini belirtin:

   - **Tüm dosyalar**. Bu ayar etkinleştirilirse Kaspersky Endpoint Security, tüm dosyaları istisnasız (tüm formatları ve uzantıları) olarak kontrol eder.

   - **Biçime göre taranan dosyalar**. Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Bir dosyada kötü amaçlı kod taraması yapmadan önce dosyanın iç başlığı, dosyanın biçimini (örneğin, .txt, .doc veya .exe) belirlemek için analiz edilir. Tarama ayrıca belirli dosya uzantılarına sahip dosyaları arar.

   - **Uzantıya göre taranan dosyalar** Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Dosya biçimi daha sonra dosyanın uzantısına göre belirlenir.

5. **Koruma kapsamını düzenle** bağlantısına tıklayın.

6. Açılan pencerede, tarama kapsamına eklemek veya tarama kapsamının dışında tutmak istediğiniz nesneleri seçin.

   Varsayılan koruma kapsamına dahil edilen nesneleri kaldırabilir veya düzenleyebilirsiniz.

7. Koruma kapsamına yeni bir nesne eklemek isterseniz:

   a. **Ekle**'ye tıklayın.

      Klasör ağacı açılır.

   b. **Yol** alanına, dosya veya klasöre giden yolu girin.

      Maskeler kullanarak:

      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

      - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

      - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

      Maskeleri bir dosya veya klasör yolunda herhangi bir yerde kullanabilirsiniz. Örneğin, tarama kapsamının bilgisayardaki tüm kullanıcı hesapları için İndirilenler klasörünü içermesini istiyorsanız, `C:\Users\*\Downloads\` maskesini girin.

      Bilgisayarın dosya kaynakları listesindeki **Bu Bilgisayar** nesnesi şu nesneleri içerir: **Tüm sabit sürücüler**, **Tüm ağ sürücüleri** ve **Tüm çıkarılabilir sürücüler**.

   Tarama kapsamındaki nesneler listesinden, bir nesneyi silmeden taramaların dışında bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

8. Değişikliklerinizi kaydedin.

Tarama yöntemlerini kullanma

Kaspersky Endpoint Security, Makine öğrenimi ve imza analizi olarak adlandırılan bir tarama tekniği kullanır. İmza analizi sırasında Kaspersky Endpoint Security, algılanan nesneyi veritabanındaki kayıtlarla eşleştirir. Kaspersky uzmanları makine öğreniminin ve imza analizinin her zaman etkin olmasını önerir.

Koruma etkinliğini artırmak için sezgisel analizi kullanabilirsiniz. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.

Dosya Tehdidi Koruması bileşeninin çalışması sırasında sezgisel analiz kullanmayı yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.
4. Uygulamanın dosya tehditlerine karşı koruma için sezgisel analiz kullanmasını istiyorsanız, **Tarama yöntemleri** bloğundaki **Sezgisel analiz** onay kutusunu işaretleyin. Sonra sezgisel analiz düzeyini ayarlamak için kaydırma çubuğunu kullanın: **Hızlı tarama**, **Normal tarama** ya da **Ayrıntılı tarama**.
5. Değişikliklerinizi kaydedin.

Dosya Tehdidi Koruması bileşeninin çalışması sırasında tarama teknolojilerini kullanma

Dosya Tehdidi Koruması bileşeninin çalışması sırasında tarama teknolojilerinin kullanımını yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.

4. **Tarama teknolojileri** bloğunda, dosya tehdidi koruması için kullanmak istediğiniz teknolojilerin adının yanındaki onay kutularını seçin:

   - **iSwift teknolojisini kullan**. Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.

   - **iChecker teknolojisini kullan**. Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).

5. Değişikliklerinizi kaydedin.

Dosya taramasını optimize etme

Dosya Tehdidi Koruması bileşeni tarafından gerçekleştirilen dosya taramasını optimize ederek, tarama süresini kısaltabilir ve Kaspersky Endpoint Security'nin çalışma hızını artırabilirsiniz. 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.

Dosya taramasını optimize etmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.

3. **Gelişmiş ayarlar**'a tıklayın.

4. **Optimizasyon** bloğunda, **Sadece yeni ve değiştirilmiş dosyaları tara** onay kutusunu işaretleyin.

5. Değişikliklerinizi kaydedin.

Birleşik 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.

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

Dosya Tehdidi Koruması bileşeni, ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR ve ICE biçimlerindeki bileşik dosyaları temizler ve tüm diğer biçimlerdeki dosyaları (posta veri tabanları haricinde) siler.

Bileşik dosyaların taranmasını yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.
4. **Birleşik dosyaları tara** bloğunda, taramak istediğiniz bileşik dosya türlerini belirtin: arşivler, dağıtım paketleri, posta veya ofis biçimi dosyaları.
5. Yalnızca yeni ve değiştirilmiş dosyaları tarama devre dışıysa, her bir bileşik dosya türünü taramak için ayarları yapılandırın: bu türdeki tüm dosyaları veya yalnızca yeni dosyaları tarayın.

   Yalnızca yeni ve değiştirilmiş dosyaları tarama etkinleştirilirse, Kaspersky Endpoint Security her türden bileşik dosya için yalnızca yeni ve değiştirilmiş dosyaları tarar.
6. Birleşik dosyaları taramak için gelişmiş ayarları yapılandırın.

   - **Büyük bileşik dosya paketlerini açma**.

     Bu onay kutusu işaretlenirse Kaspersky Endpoint Security, boyutları belirtilen değeri aşan birleşik dosyaları taramaz.

     Bu onay kutusu işaretlenmezse Kaspersky Endpoint Security, her boyuttaki birleşik dosyaları tarar.

     Kaspersky Endpoint Security, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük dosyaları tarar.

   - **Bileşik dosyaları arka planda çıkart**.

     Onay kutusu işaretlenirse, Kaspersky Endpoint Security, bu dosyalar taranmadan önce belirtilen değerden daha büyük bileşik dosyalara erişim sağlar. Bu durumda, Kaspersky Endpoint Security arka planda bileşik dosyaları açar ve tarar.

     Kaspersky Endpoint Security sadece bu dosyaları paketinden çıkardıktan ve taradıktan sonra bu değerden küçük bileşik dosyalara erişim sağlar.

Onay kutusu işaretlenmezse, Kaspersky Endpoint Security bileşik dosyalara yalnızca herhangi bir boyuttaki dosyaları açıp taradıktan sonra erişim sağlar.

7. Değişikliklerinizi kaydedin.

Tarama modunu değiştirme

Tarama modu, Dosya Tehdidi Koruması bileşeni ile dosya taramasını tetikleyen koşulu ifade eder. Varsayılan olarak, Kaspersky Endpoint Security dosyaları akıllı modda tarar. Bu dosya tarama modunda Dosya Tehdidi Koruması bileşeni, 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. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Dosya Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.
4. **Tarama modu** bloğunda, gerekli modu seçin:
   - **Akıllı mod**. Bu modda, Dosya Tehdidi Koruması bir nesneyi o nesnede yapılan eylemlerin çözümlemesine dayalı olarak tarar. Örneğin, bir Microsoft Office belgesi ile çalışırken Kaspersky Endpoint Security dosyayı ilk açıldığında ve son kapandığında tarar. Dosyanın üzerine yazan ara işlemler taranmasına neden olmaz.
   - **Erişim ve değiştirme durumunda** Bu modda, Dosya Tehdidi Koruması nesneleri açma veya değişiklik yapma girişimi olduğunda tarar.
   - **Erişim durumunda**. Bu modda, Dosya Tehdidi Koruması nesneleri yalnızca onları açma girişimi olduğunda tarar.
   - **Yürütme durumunda**. Bu modda Dosya Tehdidi Koruması nesneleri yalnızca onları çalıştırma girişimi olduğunda tarar.
5. Değişikliklerinizi kaydedin.

Kapsayıcı Taraması

Bir *kapsayıcı*, bir uygulamanın işletim sistemiyle doğrudan etkileşime girmeden çalışabileceği yalıtılmış bir ortamdır. Konteyner kullanımı aşağıdaki riskleri içerir:

- Bilgisayar korsanları konteyner içindeki uygulamaların güvenliğini aşmak için konteynerizasyon açıklarından faydalanabilir.
- Bilgisayar korsanları, bilgisayardaki verilere yetkisiz erişim sağlamak veya sistemin bütünlüğünü tehlikeye atmak için kapsayıcı ortamının güvensiz bir yapılandırmasından yararlanabilir.

- Bir kapsayıcıya yapılan başarılı bir saldırı, bir bilgisayar korsanının bilgisayardaki verilere erişmesini sağlayabilir.
- Bilgisayar korsanları ağ trafiğini kesmek için ağdaki zayıf noktalardan faydalanabilir.

Kaspersky Endpoint Security, dosyaları yalnızca disklerde değil, kapsayıcıların içinde de tarar. Yani Kaspersky Endpoint Security, konteynerlerin içindeki kötü amaçlı etkinlikleri tespit eden harici bir araçtır. Bu, konteynerlerin performansının korunmasını sağlar ve konteyner içindeki diğer uygulamalarla çakışmaları önler. Kaspersky Endpoint Security'nin konteyner içine yüklenmesi desteklenmez.

Kaspersky Endpoint Security, konteyner güvenliğini sağlamanın yanı sıra Uygulama Denetimi'ni kullanarak kapsayıcıların içindeki uygulamaları yönetmeye olanak tanır. Uygulama Denetimi, konteynerler için bilgisayarda yüklü uygulamalarla aynı şekilde yapılandırılır. Sistem Bütünlüğü İzleme ayrıca kapsayıcıları da destekler.

Konteyner gereksinimleri

- Konteyner, bir Docker konteyneri olmalıdır. Diğer konteynerleştirme araçları desteklenmez.
- Konteyner, işlem izolasyon modunda çalışmalıdır. Hyper-V izolasyon modu desteklenmez.
- Konteyner bir Windows Server 2016, 2019 veya 2022 sunucusuna (Docker Host) yerleştirilmelidir.
- Konteyner bir Windows görüntüsü (Docker Image) içermelidir. Windows 10 ve 11 desteklenmez. Linux görüntüleri desteklenmez.

Tehdit algılandığında yapılacak eylem

Bir kapsayıcı içinde bir tehdit algılanırsa, uygulama Dosya Tehdit Koruması bileşeni için seçilen eylemi uygular. Kapsayıcı Taraması ek ayarlara sahiptir (aşağıdaki talimatlara bakın). Bir tehdit tespit edilirse, uygulama kötü amaçlı etkinliği engeller ve seçilen eylemi gerçekleştirir (örneğin, nesneyi temizlemeye çalışır). Kaspersky Endpoint Security, algılanan nesne dezenfekte edilemezse kapsayıcıyı durdurabilir. Varsayılan olarak, kapsayıcı durdurma işlevi devre dışıdır.

Yönetim Konsolu'nda (MMC) kapsayıcı taraması yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.
4. **Ayarlar**'a tıklayın.
5. Bu işlem bir pencere açar; bu pencerede **Ek** sekmesini seçin.

6. **Windows kapsayıcılarında yürütülen dosya işlemlerinin taranması** bloğunda, kapsayıcı tarama ayarlarını yapılandırın:

   - **Temizleme başarısız olursa kapsayıcıyı durdur**. Uygulama, algılanan nesne için yeterli okuma ve yazma haklarına sahip olmayabilir. Bu durumda, tespit edilen nesnenin temizlenmesi veya silinmesi mümkün değildir. Bu onay kutusu işaretlendiğinde, uygulama algılanan nesneyi engeller ve kapsayıcıyı durdurur. Bu onay kutusunun işareti kaldırıldığında, uygulama yalnızca algılanan nesneyi engeller.

   - **Windows kapsayıcılarında yürütülen dosya işlemlerini tarama**. Onay kutusu işaretlendiğinde, uygulama kapsayıcı yalnızca kapsayıcı başlangıcında tarar. Onay kutusunun işareti kaldırıldığında, uygulama kapsayıcıyı gerçek zamanlı olarak sürekli tarar.

7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da kapsayıcı taraması nasıl yapılandırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması** → **Dosya Tehdidi Koruması** bölümüne gidin.

5. **Gelişmiş ayarlar** bölümünde, **Performans** sekmesini seçin.

6. **Tarama optimizasyonu** bloğunda, kapsayıcı tarama ayarlarını yapılandırın:

   - **Temizleme başarısız olursa kapsayıcıyı durdur**. Uygulama, algılanan nesne için yeterli okuma ve yazma haklarına sahip olmayabilir. Bu durumda, tespit edilen nesnenin temizlenmesi veya silinmesi mümkün değildir. Bu onay kutusu işaretlendiğinde, uygulama algılanan nesneyi engeller ve kapsayıcıyı durdurur. Bu onay kutusunun işareti kaldırıldığında, uygulama yalnızca algılanan nesneyi engeller.

   - **Windows kapsayıcılarında yürütülen dosya işlemlerini tarama**. Onay kutusu işaretlendiğinde, uygulama kapsayıcı yalnızca kapsayıcı başlangıcında tarar. Onay kutusunun işareti kaldırıldığında, uygulama kapsayıcıyı gerçek zamanlı olarak sürekli tarar.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde kapsayıcı taramasını yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Dosya Tehdidi Koruması**'nı seçin.

3. **Windows kapsayıcılarında yürütülen dosya işlemlerinin taranması** bloğunda, kapsayıcı tarama ayarlarını yapılandırın:

   - **Temizleme başarısız olursa kapsayıcıyı durdur**. Uygulama, algılanan nesne için yeterli okuma ve yazma haklarına sahip olmayabilir. Bu durumda, tespit edilen nesnenin temizlenmesi veya silinmesi mümkün değildir. Bu onay kutusu işaretlendiğinde, uygulama algılanan nesneyi engeller ve kapsayıcıyı durdurur. Bu onay kutusunun işareti kaldırıldığında, uygulama yalnızca algılanan nesneyi engeller.

   - **Windows kapsayıcılarında yürütülen dosya işlemlerini tarama**. Onay kutusu işaretlendiğinde, uygulama kapsayıcı yalnızca kapsayıcı başlangıcında tarar. Onay kutusunun işareti kaldırıldığında, uygulama kapsayıcıyı gerçek zamanlı olarak sürekli tarar.

4. Değişikliklerinizi kaydedin.

Sunucu Yetkisiz Erişim Önleme

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

Sunucu Yetkisiz Erişim Önleme bileşeni, uygulamaların işletim sistemi için tehlikeli olabilecek işlemler yapmasını engeller ve işletim sistemi kaynaklarına ve kişisel verilere erişim üzerinde denetim sağlar. Bileşen, anti-virüs veritabanları ve Kaspersky Security Network bulut hizmetinin yardımıyla bilgisayar koruması sağlar.

Bileşen, *uygulama haklarını* kullanarak uygulamaların çalışmasını denetler. Uygulama hakları şu erişim parametrelerini kapsar:

- İşletim sistemi kaynaklarına erişim (örneğin seçeneklerin, kayıt defteri anahtarlarının otomatik başlatılması)
- Kişisel verilere erişim (örneğin, dosyalar ve uygulamalar)

Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.

Uygulamanın ilk başlatılması sırasında, Sunucu Yetkisiz Erişim Önleme bileşeni şu eylemleri gerçekleştirir:

1. İndirilen anti virüs veritabanlarını kullanarak uygulamanın güvenliğini kontrol eder.
2. Kaspersky Security Network'teki uygulamanın güvenliğini denetler.

   Sunucu Yetkisiz Erişim Önleme bileşeninin daha etkin çalışmasını sağlamak için Kaspersky Security Network'e katılmanız önerilir.

3. Uygulamayı güven gruplarından birine sokar: *Güvenilir*, *Düşük Kısıtlamalı*, *Yüksek Kısıtlamalı*, *Güvenilmez*.

   Güvenilirlik grubu, Kaspersky Endpoint Security'nin uygulama etkinliğini denetlerken uyguladığı hakları tanımlar. Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, bu uygulamanın bilgisayar için oluşturduğu tehdidin seviyesine göre yerleştirir.

Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, Güvenlik Duvarı ve Sunucu Yetkisiz Erişim Önleme bileşenleri için yerleştirir. Güven grubunu sadece Güvenlik Duvarı ya da Sunucu Yetkisiz Erişim Önleme için değiştiremezsiniz.

KSN'ye katılmayı reddederseniz ya da ağ bağlantısı olmazsa, Kaspersky Endpoint Security uygulamayı Sunucu Yetkisiz Erişim Önleme bileşeninin ayarlarına göre bir güven grubuna yerleştirir. KSN'den uygulamanın saygınlığı alındıktan sonra, güven grubu otomatik olarak değiştirilebilir.

4. Uygulama eylemlerini güven grubuna göre engeller. Örneğin, *Yüksek Kısıtlamalı* güven grubundan olan uygulamaların işletim sistemi modüllerine erişimi reddedilir.

Uygulamanın bir sonraki başlatılmasında, Kaspersky Endpoint Security uygulamanın bütünlüğünü kontrol eder. Uygulama değişmediyse bileşen, geçerli uygulama haklarını kullanır. Uygulama değiştirildiyse Kaspersky Endpoint Security ilk kez başlatılıyormuş gibi uygulamayı analiz eder.

Sunucu Yetkisiz Erişim Önleme'yi etkinleştirme ve devre dışı bırakma

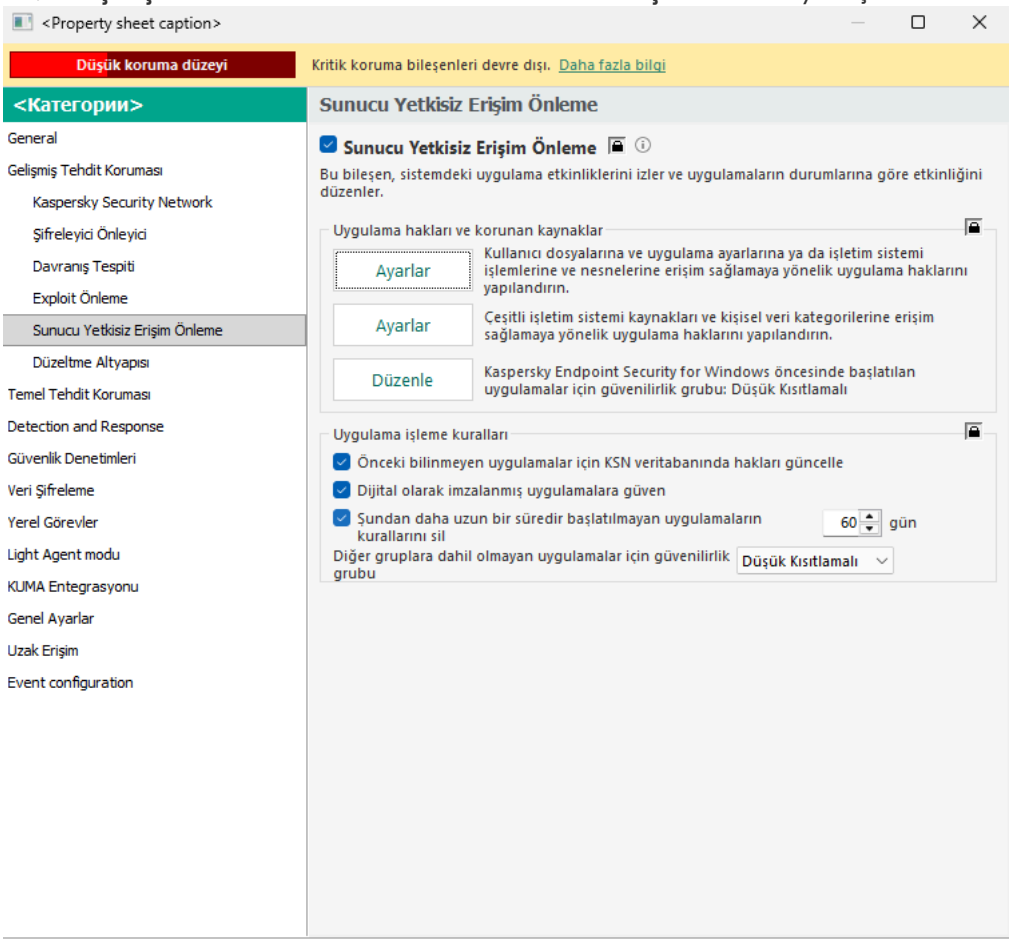
Varsayılan olarak, Sunucu Yetkisiz Erişim Önleme bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır.

Yönetim Konsolu'nda (MMC) Sunucu Yetkisiz Erişim Önleme bileşenini etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sunucu Yetkisiz Erişim Önleme** onay kutusunu kullanın.

5. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Sunucu Yetkisiz Erişim Önleme bileşenini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'ye gidin.

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sunucu Yetkisiz Erişim Önleme ETKİN** geçiş düğmesini kullanın.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Sunucu Yetkisiz Erişim Önleme bileşenini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sunucu Yetkisiz Erişim Önleme** geçiş düğmesini kullanın.

4. Değişikliklerinizi kaydedin.

Sunucu Yetkisiz Erişim Önleme bileşeni etkinleştirildiğinde, Kaspersky Endpoint Security bir uygulamayı, bu uygulamanın bilgisayar için oluşturduğu tehdidin seviyesine göre bir güvenilirlik grubuna yerleştirir. Kaspersky Endpoint Security, daha sonra güvenilirlik grubuna bağlı olarak uygulamanın eylemlerini engeller.

Uygulama güven gruplarını yönetme

Her uygulama ilk kez başlatıldığında Sunucu Yetkisiz Erişim Önleme bileşeni, uygulamanın güvenliğini denetler ve uygulamayı güven gruplarından birine yerleştirir.

Kaspersky Endpoint Security, uygulama taramanın ilk aşamasında eşleşen bir giriş için bilinen uygulamaların dahili veritabanını arar ve aynı zamanda Kaspersky Security Network veritabanına (İnternet bağlantısı varsa) bir istek gönderir. Dahili veritabanında ve Kaspersky Security Network veritabanında yapılan aramanın sonuçlarına dayanarak uygulama bir güvenilirlik grubuna yerleştirilir. Uygulamanın sonradan başlatıldığı her seferinde Kaspersky Endpoint Security, KSN veritabanına yeni bir sorgu gönderir ve uygulamanın KSN veritabanındaki tanınırlığı değiştiyse uygulamayı farklı bir güvenilirlik grubuna yerleştirir.

Kaspersky Endpoint Security'nin bilinmeyen tüm uygulamaları otomatik olarak yerleştirmesini istediğiniz bir güvenilirlik grubu seçebilirsiniz. Kaspersky Endpoint Security başlatılmadan önce çalışan uygulamalar otomatik olarak Sunucu Yetkisiz Erişim Önleme ayarlarında belirlenen güvenilirlik grubuna yerleştirilir.

Kaspersky Endpoint Security'den önce başlatılan uygulamalar için yalnızca ağ etkinliği denetlenir. Denetim, Güvenlik Duvarı ayarlarında tanımlanan ağ kurallarına göre gerçekleştirilir.

Bir uygulamanın güvenilirlik grubunu değiştirme

Her uygulama ilk kez başlatıldığında Sunucu Yetkisiz Erişim Önleme bileşeni, uygulamanın güvenliğini denetler ve uygulamayı güven gruplarından birine yerleştirir.

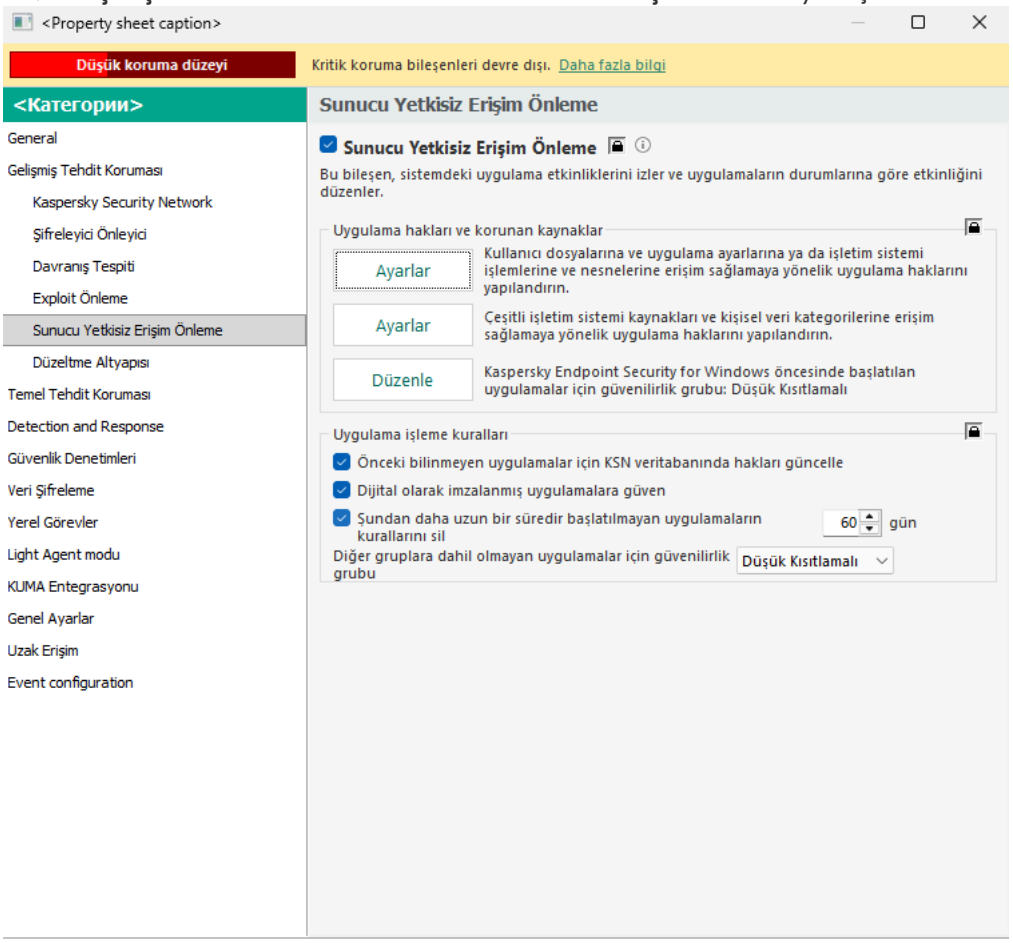
Kaspersky uzmanları, uygulamaların otomatik olarak atandıkları güvenilirlik grubundan farklı bir güvenilirlik grubuna taşınmasını önermez. Bunun yerine gerekirse tek bir uygulamanın haklarını değiştirebilirsiniz.

Bir uygulamanın güvenilirlik grubu Yönetim Konsolu (MMC) ile nasıl değiştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

5. **Uygulama hakları** sekmesini seçin.

6. **Ekle**'ye tıklayın.

7. Açılan pencerede, güvenilirlik grubunu değiştirmek istediğiniz uygulamayı aramak için kriterleri girin.

   Uygulamanın adını veya satıcının adını girebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

8. **Yenile**'ye tıklayın.

   Kaspersky Endpoint Security uygulamayı, yönetilen bilgisayarlardaki yüklü uygulamalar birleştirilmiş listesinde arar. Kaspersky Endpoint Security, arama kriterlerinizi karşılayan uygulamaların bir listesini görüntüler.

9. Gereken uygulamayı seçin.

10. **Seçilen uygulamayı güvenilirlik grubuna ekle** açılır listesinden uygulama için gerekli güvenilirlik grubunu seçin.

11. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da bir uygulamanın güvenilirlik grubu nasıl değiştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.
5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Uygulama hakları ve korunan kaynaklar** bağlantısına tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.
6. **Uygulama hakları** sekmesini seçin.

   Pencerenin sol tarafında güvenilirlik gruplarının bir listesini, sağ tarafında ise bunların özelliklerini göreceksiniz.
7. **Ekle**'ye tıklayın.

   Bir güvenilirlik grubuna uygulama eklemek için Sihirbaz başlatılır.
8. Uygulama için ilgili güvenilirlik grubunu seçin.
9. **Uygulama** türünü seçin. Bir sonraki adıma geçin.

   Birden çok uygulama için güvenilirlik grubunu değiştirmek istiyorsanız **Grup** türünü seçin ve uygulama grubu için bir ad tanımlayın.
10. Açık uygulamalar listesinden, güvenilirlik grubunu değiştirmek istediğiniz uygulamaları seçin.

    Bir filtre kullanın. Uygulamanın adını veya satıcının adını girebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
11. Sihirbazı tamamlayın.

    Uygulama güvenilirlik grubuna eklenir.
12. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir uygulamanın güvenilirlik grubu nasıl değiştirilir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'yi seçin.
3. **Uygulamaları yönet**'e tıklayın.

   Bu, yüklü uygulamaların listesini açar.
4. Gereken uygulamayı seçin.
5. Uygulamanın bağlam menüsünde **Kısıtlamalar** → **<güvenilirlik grubu>** seçeneğine tıklayın.
6. Değişikliklerinizi kaydedin.

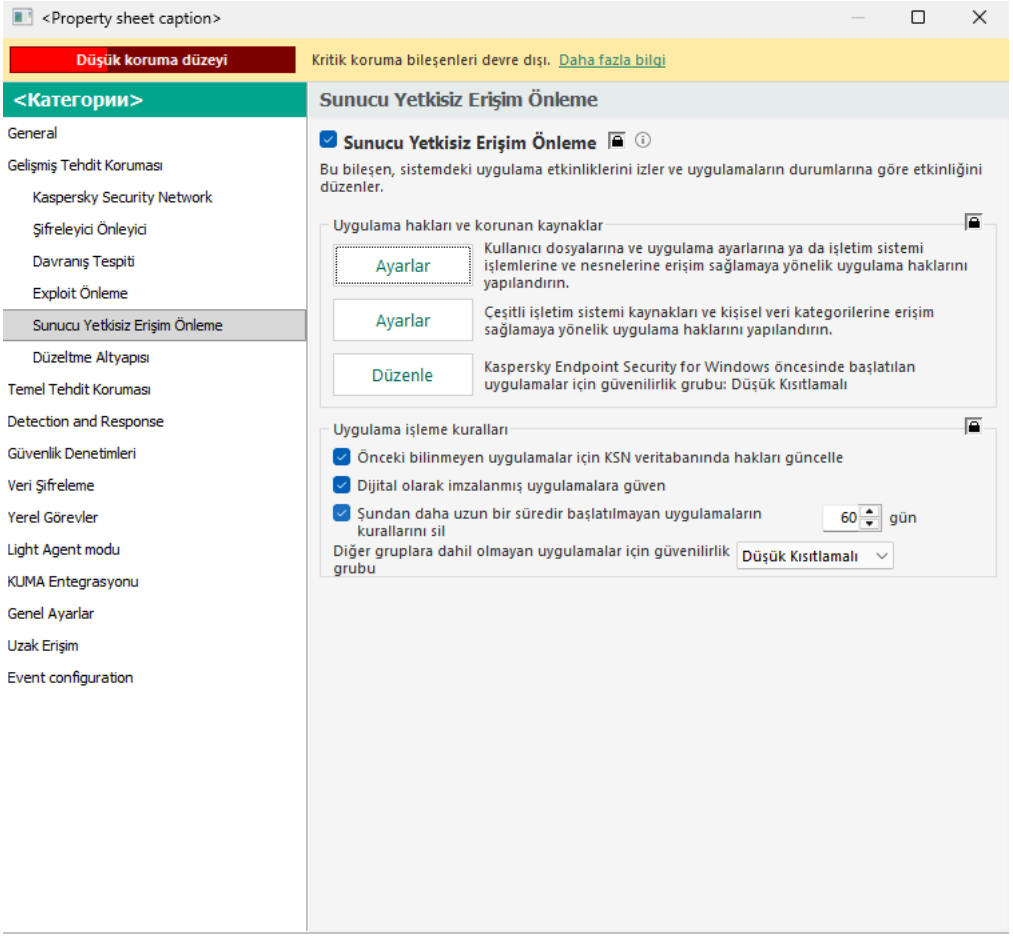
Sonuç olarak, uygulama diğer güvenilirlik grubuna konulacaktır. Kaspersky Endpoint Security, daha sonra güvenilirlik grubuna bağlı olarak uygulamanın eylemlerini engeller. Uygulamaya *(kullanıcı tanımlı)* durumu atanır. Kaspersky Security Network'te uygulamanın tanınırlığı değişirse, Sunucu Yetkisiz Erişim Önleme bileşeni bu uygulamanın güvenilirlik grubunu değiştirmeden bırakır.

Güvenilirlik grubu haklarını yapılandırma

Varsayılan olarak farklı güvenilirlik grupları için en uygun uygulama hakları oluşturulur. Bir güvenilirlik grubunda bulunan uygulama gruplarının hak ayarları, değerleri güvenilirlik grubu haklarının ayarlarından devralır.

Yönetim Konsolu (MMC) ile güvenilirlik grubu nasıl değiştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.
5. **Uygulama hakları** sekmesine gidin.
6. Gerekli güvenilirlik grubunu seçin.
7. Güvenilirlik grubunun bağlam menüsünde **Grup hakları**'nı seçin.

   Güvenilirlik grubu özellikleri açılır.

8. Aşağıdakilerden birini yapın:

   - İşletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarlarıyla ilgili işlemleri düzenleyen güvenilirlik grubu haklarını düzenlemek için **Dosya ve sistem kayıt defteri** seçeneğini kullanın.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** seçeneğini kullanın.

   Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.

9. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** (✓) veya **Engelle** (⊘).
10. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin (✓ / ⊘).

    Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.
11. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da güvenilirlik grubu hakları nasıl değiştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.
5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Uygulama hakları ve korunan kaynaklar** bağlantısına tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.
6. **Uygulama hakları** sekmesine gidin.

   Pencerenin sol tarafında güvenilirlik gruplarının bir listesini, sağ tarafında ise bunların özelliklerini göreceksiniz.
7. Pencerenin sol tarafından ilgili güvenilirlik grubunu seçin.
8. Pencerenin sağ tarafındaki açılır listede şunlardan birini yapın:

   - İşletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarlarıyla ilgili işlemleri düzenleyen güvenilirlik grubu haklarını düzenlemek için **Dosya ve sistem kayıt defteri** seçeneğini kullanın.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** seçeneğini kullanın.

   Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.

9. İlgili kaynak için, ilgili eylemin sütunundan gerekli seçeneği seçin: **Devral**, **İzin ver** (✓), **Engelle** (✗).

10. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin (/).

    Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.

11. Değişikliklerinizi kaydedin.

Uygulama arabiriminde güvenilirlik grubu hakları nasıl değiştirilir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.
3. **Uygulamaları yönet**'e tıklayın.

   Bu, yüklü uygulamaların listesini açar.
4. Gerekli güvenilirlik grubunu seçin.
5. Güvenilirlik grubunun bağlam menüsünde **Ayrıntılar ve kurallar**'ı seçin.

   Güvenilirlik grubu özellikleri açılır.
6. Aşağıdakilerden birini yapın:

   - İşletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarlarıyla ilgili işlemleri düzenleyen güvenilirlik grubu haklarını düzenlemek için **Dosya ve sistem kayıt defteri** seçeneğini kullanın.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** seçeneğini kullanın.

   Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.
7. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** ( ) veya **Reddet** ( ).
8. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin ( ).

   Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.
9. Değişikliklerinizi kaydedin.

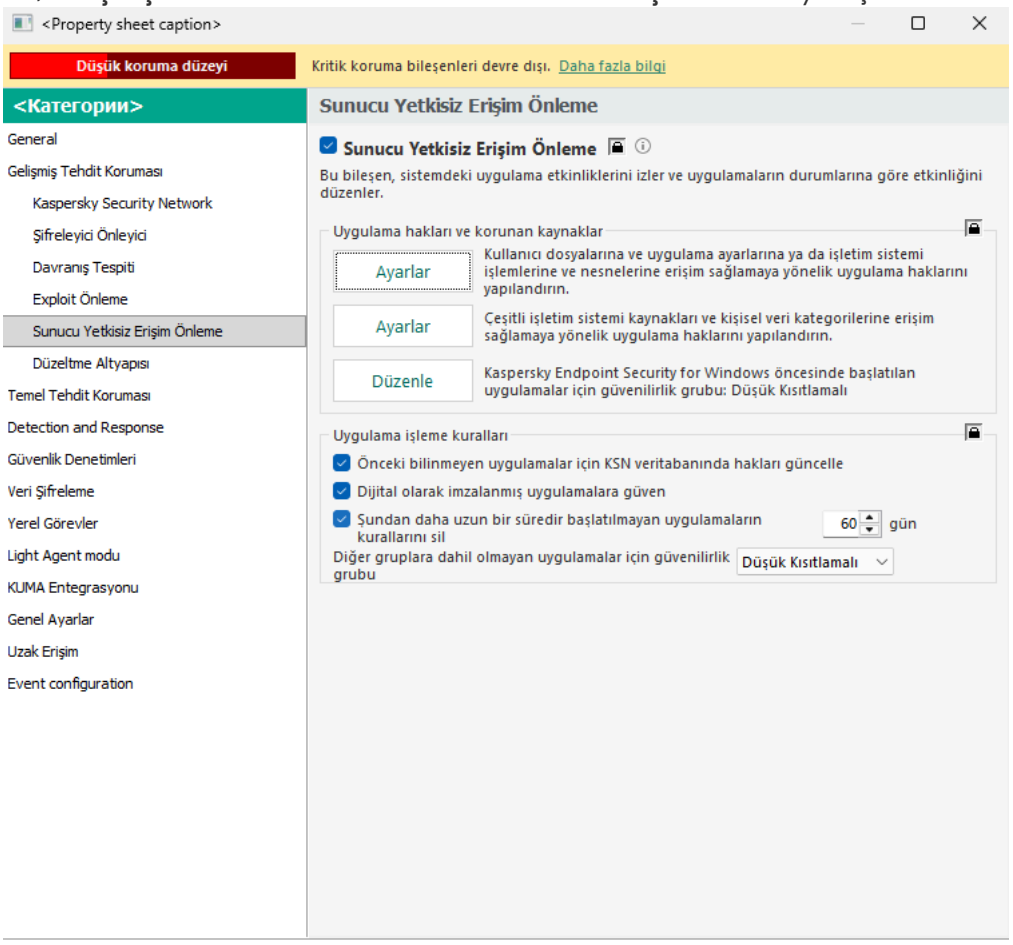
Güvenilirlik grubu hakları değiştirilecek. Kaspersky Endpoint Security, daha sonra güvenilirlik grubuna bağlı olarak uygulamanın eylemlerini engeller. Durum (*Özel ayarlar*) güvenilirlik grubuna atanacaktır.

Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güven grubu seçme

Kaspersky Endpoint Security'den önce başlatılan uygulamalar için yalnızca ağ etkinliği denetlenir. Denetim, Güvenlik Duvarı ayarlarında tanımlanan ağ kurallarına göre gerçekleştirilir. Bu tür uygulamaları izlemek için ağ etkinliğine uygulanması gereken ağ kurallarının belirlemek için bir güvenilirlik grubu seçmeniz gerekir.

Yönetim Konsolu'nda (MMC) Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güvenilirlik grubu seçme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Düzenle** düğmesine tıklayın.
5. **Kaspersky Endpoint Security öncesinde başlatılan uygulamalar için güvenilirlik grubu** ayarı için uygun güvenilirlik grubu seçimini yapın.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güvenilirlik grubu seçme

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'ye gidin.

5. **Kaspersky Endpoint Security öncesinde başlatılan uygulamalar için güvenilirlik grubu** ayarı için uygun güvenilirlik grubu seçimini yapın.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güvenilirlik grubu seçme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.

3. **Kaspersky Endpoint Security öncesinde başlatılan uygulamalar için güvenilirlik grubu** bloğundan uygun güvenilirlik grubu seçimini yapın.

4. Değişikliklerinizi kaydedin.

Böylece Kaspersky Endpoint Security'den önce başlatılan bir uygulama diğer güvenilirlik grubuna konulacaktır. Kaspersky Endpoint Security, daha sonra güvenilirlik grubuna bağlı olarak uygulamanın eylemlerini engeller.

Bilinmeyen uygulamalar için bir güvenilirlik grubu seçme

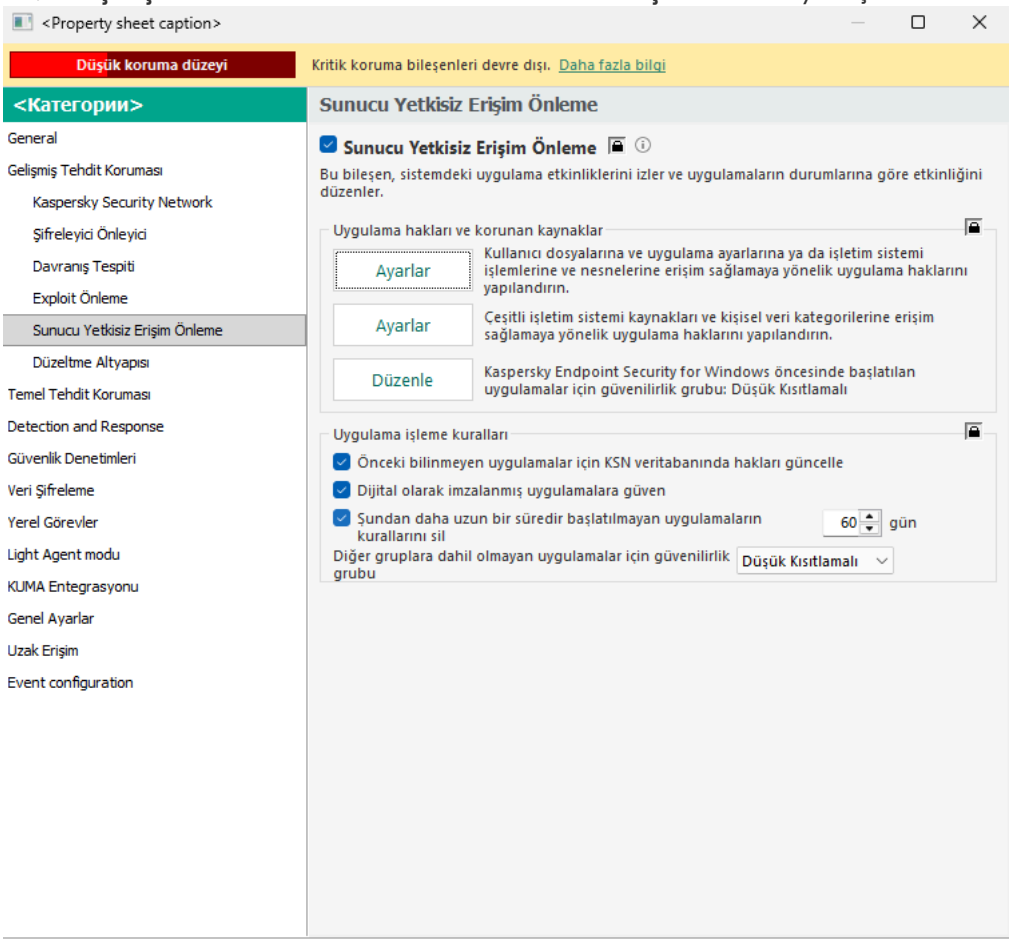
Bir uygulamanın ilk başlatılması sırasında, Sunucu Yetkisiz Erişim Önleme bileşeni uygulamanın güvenilirlik grubunu belirler. İnternet erişiminiz yoksa veya Kaspersky Security Network bu uygulama hakkında hiçbir bilgiye sahip değilse Kaspersky Endpoint Security uygulamayı varsayılan olarak *Düşük Kısıtlamalı* grubuna yerleştirir. KSN'de önceden bilinmeyen bir uygulama hakkında bilgi algılandığında, Kaspersky Endpoint Security bu uygulamanın haklarını günceller. Ardından uygulama haklarını elle düzenleyebilirsiniz.

Yönetim Konsolu'nda (MMC) bilinmeyen uygulamalar için bir güvenilirlik grubu nasıl seçilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama işleme kuralları** bloğunda, gerekli güvenilirlik grubunu seçmek için **Diğer gruplara dahil olmayan uygulamalar için güvenilirlik grubu** açılır listesini kullanın.

   Kaspersky Security Network'e katılım etkinleştirilirse uygulama her başlatıldığında Kaspersky Endpoint Security, KSN'ye uygulamanın tanınırlığı için bir talep gönderir. Alınan yanıta bağlı olarak uygulama, Sunucu Yetkisiz Erişim Önleme bileşeni ayarlarında belirtilenden farklı bir güven grubuna taşınabilir.

5. Bilinmeyen uygulamaların haklarının otomatik güncellemesini yapılandırmak için **Önceki bilinmeyen uygulamalar için KSN veritabanında hakları güncelle** onay kutusunu kullanın.

6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bilinmeyen uygulamalar için bir güvenilirlik grubu nasıl seçilir

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'ye gidin.

5. **Uygulama işleme kuralları** bloğunda, gerekli güvenilirlik grubunu seçmek için **Diğer gruplara dahil olmayan uygulamalar için güvenilirlik grubu** açılır listesini kullanın.

   Kaspersky Security Network'e katılım etkinleştirilirse uygulama her başlatıldığında Kaspersky Endpoint Security, KSN'ye uygulamanın tanınırlığı için bir talep gönderir. Alınan yanıta bağlı olarak uygulama, Sunucu Yetkisiz Erişim Önleme bileşeni ayarlarında belirtilenden farklı bir güven grubuna taşınabilir.

6. Bilinmeyen uygulamaların haklarının otomatik güncellemesini yapılandırmak için **Önceki bilinmeyen uygulamalar için KSN veritabanında hakları güncelle** onay kutusunu kullanın.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bilinmeyen uygulamalar için güvenilirlik grubu seçme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.

3. **Uygulama işleme kuralları** bloğunda uygun güvenilirlik grubunu seçin.

   Kaspersky Security Network'e katılım etkinleştirilirse uygulama her başlatıldığında Kaspersky Endpoint Security, KSN'ye uygulamanın tanınırlığı için bir talep gönderir. Alınan yanıta bağlı olarak uygulama, Sunucu Yetkisiz Erişim Önleme bileşeni ayarlarında belirtilenden farklı bir güven grubuna taşınabilir.

4. Bilinmeyen uygulamaların haklarının otomatik güncellemesini yapılandırmak için **KSN'den eskiden bilinmeyen uygulamalar için kuralları güncelle** onay kutusunu kullanın.

5. Değişikliklerinizi kaydedin.

Dijital olarak imzalanmış uygulamalar için bir güvenilirlik grubu seçme

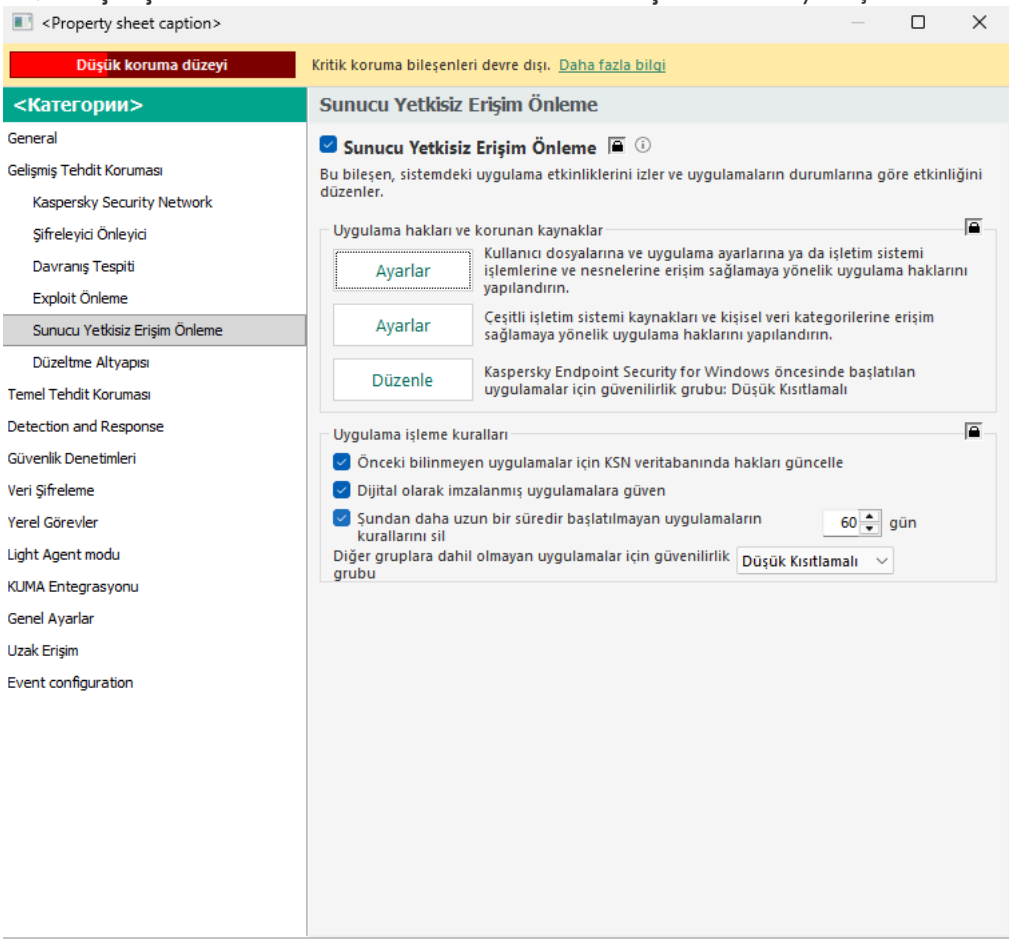
Kaspersky Endpoint Security her zaman Microsoft sertifikaları veya Kaspersky sertifikaları tarafından imzalanan uygulamaları *Güvenilir* gruba yerleştirir.

Dijital imzalı uygulamalar için bir güvenilirlik grubu Yönetim Konsolu (MMC) ile nasıl seçilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama işleme kuralları** bloğunda, güvenilen satıcıların dijital imzasını içeren uygulamalar için Güvenilir grubuna otomatik atamayı etkinleştirmek veya devre dışı bırakmak için **Dijital olarak imzalanmış uygulamalara güven** onay kutusunu kullanın.

   Güvenilir satıcılar, Kaspersky tarafından güvenilir gruba dahil edilen yazılım satıcılarıdır. Güvenilir sistem sertifika deposuna manuel olarak da satıcı sertifikası ekleyebilirsiniz.

   Onay kutusunun işareti kaldırılırsa Sunucu Yetkisiz Erişim Önleme bileşeni, dijital olarak imzalanan uygulamaları güvenilir kabul etmez ve onların güvenilirlik gruplarını belirlemek için başka parametreler kullanır.

5. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Dijital imzalı uygulamalar için bir güvenilirlik grubu Web Console ve Cloud Console ile nasıl seçilir

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'ye gidin.

5. **Uygulama işleme kuralları** bloğunda, güvenilen satıcıların dijital imzasını içeren uygulamalar için Güvenilir grubuna otomatik atamayı etkinleştirmek veya devre dışı bırakmak için **Dijital olarak imzalanmış uygulamalara güven** onay kutusunu kullanın.

   Güvenilir satıcılar, Kaspersky tarafından güvenilir gruba dahil edilen yazılım satıcılarıdır. Güvenilir sistem sertifika deposuna manuel olarak da satıcı sertifikası ekleyebilirsiniz.

Onay kutusunun işareti kaldırılırsa Sunucu Yetkisiz Erişim Önleme bileşeni, dijital olarak imzalanan uygulamaları güvenilir kabul etmez ve onların güvenilirlik gruplarını belirlemek için başka parametreler kullanır.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde dijital olarak imzalanmış uygulamalar için güvenilirlik grubu seçme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.
3. **Uygulama işleme kuralları** bloğunda, güvenilen satıcıların dijital imzasını içeren uygulamalar için Güvenilir grubuna otomatik atamayı etkinleştirmek veya devre dışı bırakmak için **Dijital olarak imzalanmış uygulamalara güven** onay kutusunu kullanın.

   Güvenilir satıcılar, Kaspersky tarafından güvenilir gruba dahil edilen yazılım satıcılarıdır. Güvenilir sistem sertifika deposuna manuel olarak da satıcı sertifikası ekleyebilirsiniz.

   Onay kutusunun işareti kaldırılırsa Sunucu Yetkisiz Erişim Önleme bileşeni, dijital olarak imzalanan uygulamaları güvenilir kabul etmez ve onların güvenilirlik gruplarını belirlemek için başka parametreler kullanır.

4. Değişikliklerinizi kaydedin.

Uygulama haklarını yönetme

Varsayılan olarak uygulama etkinliği, Kaspersky Endpoint Security'nin uygulamaya ilk kez başladığında atadığı belirli güvenilirlik grubu için tanımlanmış uygulama haklarına göre denetlenir. Gerekirse bütün bir güvenilirlik grubu, tek bir uygulama veya bir güvenilirlik grubu içindeki bir grup uygulamanın, uygulama haklarını düzenleyebilirsiniz.

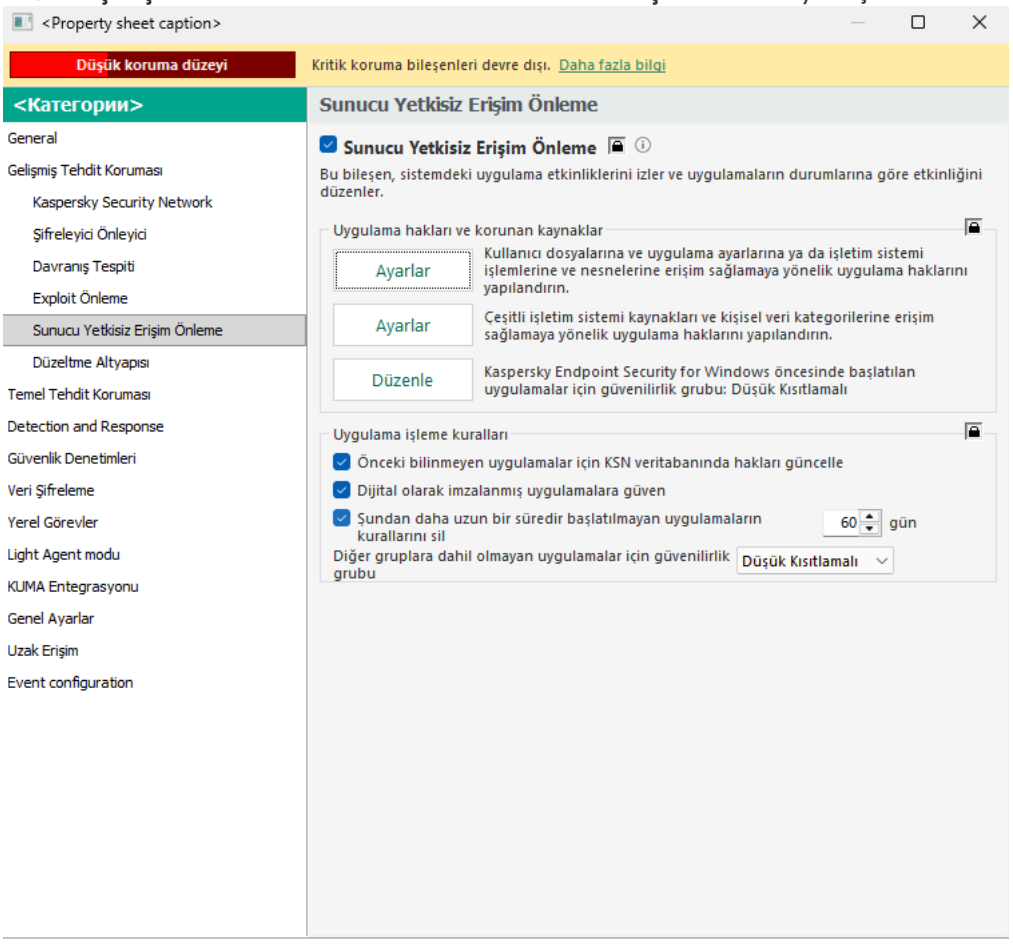
Manuel olarak tanımlanan uygulama hakları, bir güvenilirlik grubu için tanımlanan uygulama haklarından daha yüksek önceliğe sahiptir. Diğer bir deyişle, manuel olarak tanımlanan uygulama hakları, bir güvenilirlik grubu için tanımlanan uygulama haklarından farklıysa, Sunucu Yetkisiz Erişim Önleme bileşeni uygulama etkinliğini manuel olarak tanımlanan uygulama haklarına göre denetler.

Uygulamalar için oluşturduğunuz kurallar, alt uygulamalar tarafından devralınır. Örneğin, cmd.exe için tüm ağ etkinliğini reddederseniz, cmd.exe kullanılarak başlatılmışsa notepad.exe için tüm ağ etkinlikleri reddedilir. Bir uygulama çalıştığı uygulamanın alt uygulaması değilse kurallar devralınmaz.

Yönetim Konsolu'nda (MMC) uygulama hakları nasıl eklenir veya kaldırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

5. **Uygulama hakları** sekmesine gidin.

6. **Ekle**'ye tıklayın.

7. Açılan pencerede, uygulama haklarını değiştirmek istediğiniz uygulamayı aramak için kriterleri girin.

   Uygulamanın adını veya satıcının adını girebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

8. **Yenile**'ye tıklayın.

   Kaspersky Endpoint Security uygulamayı, yönetilen bilgisayarlardaki yüklü uygulamalar birleştirilmiş listesinde arar. Kaspersky Endpoint Security, arama kriterlerinizi karşılayan uygulamaların bir listesini görüntüler.

9. Gereken uygulamayı seçin.

10. **Seçilen uygulamayı güvenilirlik grubuna ekle** açılır listesinden **Varsayılan gruplar** seçimini yapın ve **Tamam**'a tıklayın.

    Uygulama varsayılan gruba eklenecektir.

11. İlgili uygulamayı seçin ve ardından uygulamanın bağlam menüsünden **Uygulama hakları**'nı seçin.

    Bu, uygulama özelliklerini açar.

12. Aşağıdakilerden birini yapın:

    - İşletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarlarıyla ilgili işlemleri düzenleyen güvenilirlik grubu haklarını düzenlemek için **Dosya ve sistem kayıt defteri** seçeneğini kullanın.
    - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** seçeneğini kullanın.

    Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.

13. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** (✓) veya **Engelle** (⊘).

14. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin (✓ / ⊘).

    Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.

15. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da uygulama hakları nasıl değiştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.
5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Uygulama hakları ve korunan kaynaklar** bağlantısına tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.
6. **Uygulama hakları** sekmesine gidin.

   Pencerenin sol tarafında güvenilirlik gruplarının bir listesini, sağ tarafında ise bunların özelliklerini göreceksiniz.
7. **Ekle**'ye tıklayın.

   Bir güvenilirlik grubuna uygulama eklemek için Sihirbaz başlatılır.
8. Uygulama için ilgili güvenilirlik grubunu seçin.
9. **Uygulama** türünü seçin. Bir sonraki adıma geçin.

   Birden çok uygulama için güvenilirlik grubunu değiştirmek istiyorsanız **Grup** türünü seçin ve uygulama grubu için bir ad tanımlayın.
10. Açık uygulamalar listesinden, uygulamalar haklarını değiştirmek istediğiniz uygulamaları seçin.

    Bir filtre kullanın. Uygulamanın adını veya satıcının adını girebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
11. Sihirbazı tamamlayın.

    Uygulama güvenilirlik grubuna eklenir.

12. Pencerenin sol kısmından ilgili uygulamayı seçin.

13. Pencerenin sağ tarafındaki açılır listede şunlardan birini yapın:

    - İşletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarlarıyla ilgili işlemleri düzenleyen güvenilirlik grubu haklarını düzenlemek için **Dosya ve sistem kayıt defteri** seçeneğini kullanın.
    - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** seçeneğini kullanın.

    Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.

14. İlgili kaynak için, ilgili eylemin sütunundan gerekli seçeneği seçin: **Devral**, **İzin ver** (), **Engelle** ().

15. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin (/).

    Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.

16. Değişikliklerinizi kaydedin.

Uygulama arabiriminde uygulama hakları nasıl değiştirilir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'yi seçin.
3. **Uygulamaları yönet**'e tıklayın.

   Bu, yüklü uygulamaların listesini açar.
4. Gereken uygulamayı seçin.
5. Uygulamanın bağlam menüsünde **Ayrıntılar ve kurallar**'ı seçin.

   Bu, uygulama özelliklerini açar.
6. Aşağıdakilerden birini yapın:

   - İşletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarlarıyla ilgili işlemleri düzenleyen güvenilirlik grubu haklarını düzenlemek için **Dosya ve sistem kayıt defteri** seçeneğini kullanın.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** seçeneğini kullanın.
7. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** () veya **Reddet** ().
8. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin ().

   Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.
9. **İstisnalar** sekmesini seçin ve uygulamanın gelişmiş ayarlarını yapılandırın (aşağıdaki tabloya bakın).

10. Değişikliklerinizi kaydedin.

Uygulamanın Gelişmiş Ayarları

Parametre	Açıklama
Uygulama tarafından açılan dosyaları tarama	Uygulama tarafından açılan tüm dosyalar Kaspersky Endpoint Security tarafından taramaların dışında tutulur. Örneğin, dosyaları yedeklemek için uygulamalar kullanıyorsanız, bu özellik Kaspersky Endpoint Security tarafından tüketilen kaynağın azaltılmasına yardımcı olur.
Uygulama etkinliğini izleme	Kaspersky Endpoint Security, uygulamanın işletim sistemindeki dosya ve ağ etkinliğini izlemez. Kaspersky Endpoint Security'nin farklı bileşenleri için uygulama etkinliği izlemeyi yapılandırabilirsiniz: • **Koruma ve kontrol bileşenleri için izleme yapma**. Uygulama etkinliği aşağıdaki bileşenler tarafından izlenir: Davranış Tespiti, Exploit Önleme, Sunucu Yetkisiz Erişim Önleme, Düzeltme Altyapısı ve Güvenlik Duvarı. • **Managed Detection and Response ve Endpoint Detection and Response için izleme**. Uygulama etkinliği yerleşik MDR aracısı ve yerleşik EDR (KATA) aracısı tarafından izlenir. • **Endpoint Detection and Response için konsol etkileşimli girişine müdahale etme**. Kaspersky Endpoint Security, konsolda uygulamanın yönetilmesiyle ilgili telemetri verileri göndermez. Telemetri verileri Kaspersky Anti Targeted Attack Platform (EDR) tarafından kullanılır.
Üst işlemin (uygulama) sınırlamalarını devralma	Üst işlem için yapılandırılan kısıtlamalar Kaspersky Endpoint Security tarafından bir alt işleme uygulanmayacaktır. Üst işlem, kendisi için uygulama haklarının (Sunucu Yetkisiz Erişim Önleme) ve uygulama ağ kurallarının (Güvenlik Duvarı) yapılandırıldığı bir uygulama tarafından başlatılır.
Alt uygulama etkinliğini izleme	Kaspersky Endpoint Security, bu uygulama tarafından başlatılan uygulamaların dosya veya ağ etkinliklerini izlemez. İstisnayı yinelemeli olarak uygulayabilirsiniz. Böylece uygulama, tüm alt uygulama zincirinin etkinliklerini izlemez.
Kaspersky Endpoint Security arabirimiyle etkileşime izin ver	Kaspersky Endpoint Security Self-Defense, uzak bir bilgisayardan uygulama hizmetlerini yönetmeye yönelik tüm girişimleri engeller. Onay kutusu işaretlenirse uzaktan erişim uygulamasının Kaspersky Endpoint Security arabirimi aracılığıyla Kaspersky Endpoint Security ayarlarını yönetmesine izin verilir.
Şifrelenmiş trafiği tarama/Tüm trafiği tarama	Uygulama tarafından başlatılan ağ trafiği, Kaspersky Endpoint Security tarafından taramaların dışında bırakılacaktır. Taramalardan ya tüm trafiği ya da yalnızca şifrelenmiş trafiği hariç tutabilirsiniz. Ayrı ayrı IP adreslerini ve port numaralarını da taramalardan hariç tutabilirsiniz. Kaspersky Endpoint Security 14.0 veya önceki sürümleri, güvenilir bir uygulama için yol yerine karma belirtildiğinde ağ trafiğinin hariç tutulmasını desteklemez.

İşletim sistemi kaynaklarını ve kişisel verileri koruma

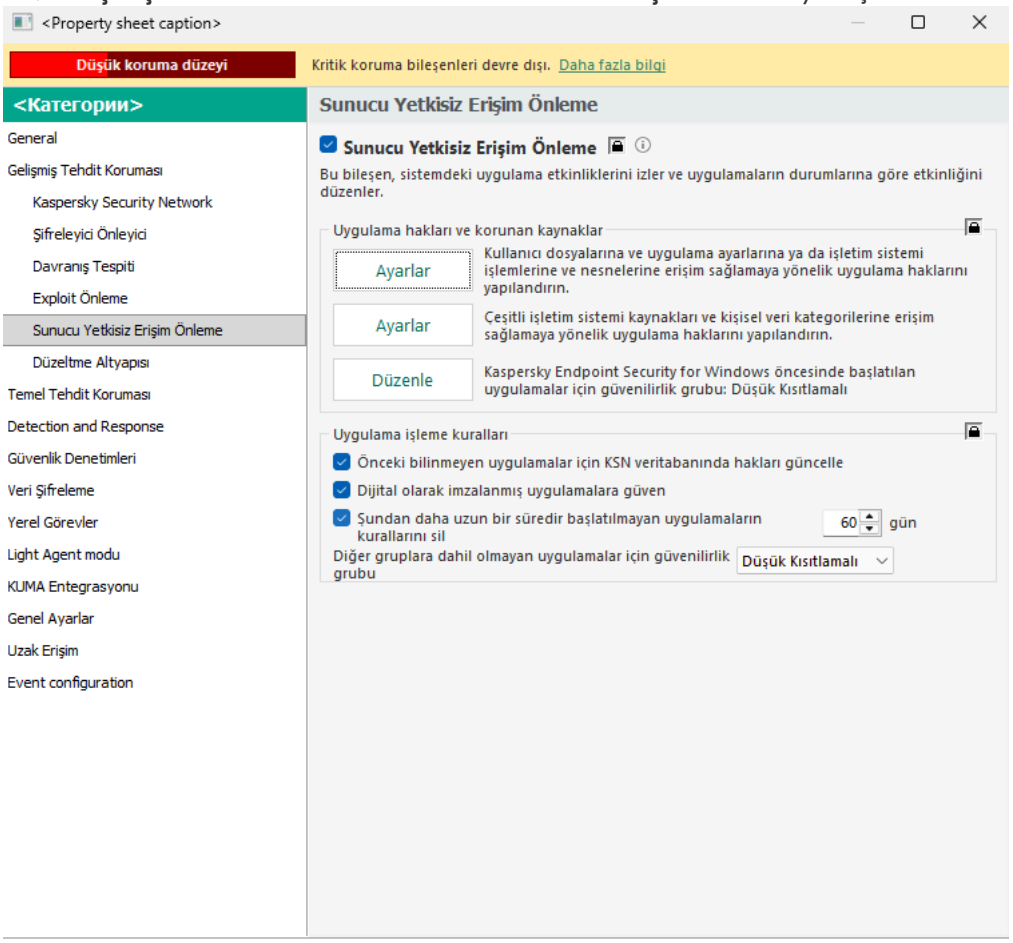
Sunucu Yetkisiz Erişim Önleme bileşeni, çeşitli işletim sistemi kaynakları ve kişisel veri kategorileri üzerinde işlem yapmak için uygulamaların haklarını yönetir. Kaspersky uzmanları, önceden ayarlanmış korunan kaynaklar kategorileri oluşturmuştur. Örneğin *İşletim sistemi* kategorisinde, uygulamaların otomatik olarak çalıştırılmasıyla ilişkili tüm kayıt defteri anahtarlarını listeleyen bir *Başlangıç ayarları* alt kategorisi vardır. Önceden ayarlanmış korunan kaynaklar kategorilerini ya da bu kategorilerdeki korunan kaynakları düzenleyemez ya da silemezsiniz.

Yönetim Konsolu'nda (MMC) korumalı bir kaynak nasıl eklenir veya kaldırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

5. **Korunan kaynaklar** sekmesine gidin.

   Pencerenin sol tarafında korunan kaynakların bir listesini ve belirli bir güvenilirlik grubuna bağlı olarak bu kaynaklara erişim için karşılık gelen hakları göreceksiniz.

6. Yeni bir korumalı kaynak eklemek istediğiniz korumalı kaynaklar kategorisini seçin.

   Bir alt kategori eklemek istiyorsanız, **Ekle → Kategori**'ye tıklayın.

7. **Ekle** düğmesine tıklayın. Açılır listeden eklemek istediğiniz kaynak türünü seçin: **Dosya veya klasör** veya **Kayıt defteri anahtarı**.

8. Açılan pencerede bir dosya, klasör veya kayıt defteri anahtarı seçin.

   Eklenen kaynaklara erişmek için uygulamaların haklarını görüntüleyebilirsiniz. Bunu yapmak için, pencerenin sol kısmında ek bir kaynak seçin; Kaspersky Endpoint Security her güvenilirlik grubu için erişim haklarını gösterecektir. Ayrıca, yeni bir kaynağın yanındaki onay kutusunu kullanarak kaynaklarla uygulama etkinliğinin denetimini devre dışı bırakabilirsiniz.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir korumalı kaynak nasıl oluşturulur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.
5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Uygulama hakları ve korunan kaynaklar** bağlantısına tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.
6. **Korunan kaynaklar** sekmesine gidin.

   Pencerenin sol tarafında korunan kaynakların bir listesini ve belirli bir güvenilirlik grubuna bağlı olarak bu kaynaklara erişim için karşılık gelen hakları göreceksiniz.
7. **Ekle**'ye tıklayın.

   Yeni Kaynak Sihirbazı başlatılır.
8. **Grup adı** bloğunda, yeni bir korunan kaynak eklemek istediğiniz korunan kaynak kategorisini seçin.

   Bir alt kategori eklemek istiyorsanız **Korunan kaynaklar kategorisi** seçeneğini tercih edin.
9. Eklemek istediğiniz kaynak türünü seçin: **Dosya veya klasör** veya **Kayıt defteri anahtarı**.
10. Bir dosya, klasör veya kayıt defteri anahtarı seçin.
11. Sihirbazı tamamlayın.

    Eklenen kaynaklara erişmek için uygulamaların haklarını görüntüleyebilirsiniz. Bunu yapmak için, pencerenin sol kısmında ek bir kaynak seçin; Kaspersky Endpoint Security her güvenilirlik grubu için erişim haklarını gösterecektir. Kaynaklarla uygulama etkinliğinin denetimini devre dışı bırakmak için **Durum** sütunundaki onay kutusunu da kullanabilirsiniz.
12. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir korunan kaynak nasıl eklenir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'yi seçin.
3. **Kaynakları yönet**'e tıklayın.

   Korunan kaynaklar listesi açılır.
4. Yeni bir korumalı kaynak eklemek istediğiniz korumalı kaynaklar kategorisini seçin.

   Bir alt kategori eklemek istiyorsanız, **Ekle** → **Kategori**'ye tıklayın.
5. **Ekle** düğmesine tıklayın. Açılır listeden eklemek istediğiniz kaynak türünü seçin: **Dosya veya klasör** veya **Kayıt defteri anahtarı**.

6. Açılan pencerede bir dosya, klasör veya kayıt defteri anahtarı seçin.

   Eklenen kaynaklara erişmek için uygulamaların haklarını görüntüleyebilirsiniz. Bunu yapmak için, pencerenin sol kısmında ek bir kaynak seçin; Kaspersky Endpoint Security her uygulama için bir uygulamalar listesi ve erişim hakları gösterecektir. **Durum** sütunundaki **Denetimi etkinleştir** düğmesini kullanarak da kaynaklarla uygulama etkinliği denetimini devre dışı bırakabilirsiniz.

7. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Security, eklenen işletim sistemi kaynaklarına ve kişisel verilere erişimi denetler. Kaspersky Endpoint Security, bir uygulamanın kaynaklara erişimini uygulamaya atanan güvenilirlik grubuna göre denetler. bir uygulamanın güvenilirlik grubunu değiştirmeniz de mümkündür.

Kullanılmayan uygulamalar hakkında bilgileri silme

Kaspersky Endpoint Security uygulamaların etkinliklerini kontrol etmek için uygulama haklarını kullanır. Başvuru hakları güvenilirlik grupları tarafından belirlenir. Kaspersky Endpoint Security, uygulama ilk kez başlatıldığında bir uygulamayı bir güvenilirlik grubuna yerleştirir. Bir uygulamanın güvenilirlik grubunu manuel olarak değiştirebilirsiniz. Ayrıca tek bir uygulamanın haklarını da manuel olarak yapılandırabilirsiniz. Kaspersky Endpoint Security bir uygulama hakkında şu bilgileri depolar: uygulamanın güvenilirlik grubu ve uygulamanın hakları.

Kaspersky Endpoint Security, bilgisayar kaynaklarını kaydetmek için kullanılmayan uygulamalar hakkındaki bilgileri otomatik olarak siler. Kaspersky Endpoint Security uygulama bilgilerini aşağıdaki kurallara göre siler:

- Bir uygulamanın güven grubu ve hakları otomatik olarak belirlenirse, Kaspersky Endpoint Security 30 gün sonra bu uygulama hakkındaki bilgileri siler. Uygulama bilgileri için saklama süresini değiştirmek veya otomatik silmeyi kapatmak mümkün değildir.

- Bir uygulamayı manuel olarak bir güvenilirlik grubuna koyarsanız veya erişim haklarını yapılandırırsanız, Kaspersky Endpoint Security bu uygulama hakkındaki bilgileri 60 gün sonra siler (varsayılan depolama süresi). Uygulama bilgileri için saklama süresini değiştirebilir veya otomatik silmeyi kapatabilirsiniz (aşağıdaki talimatlara bakın).

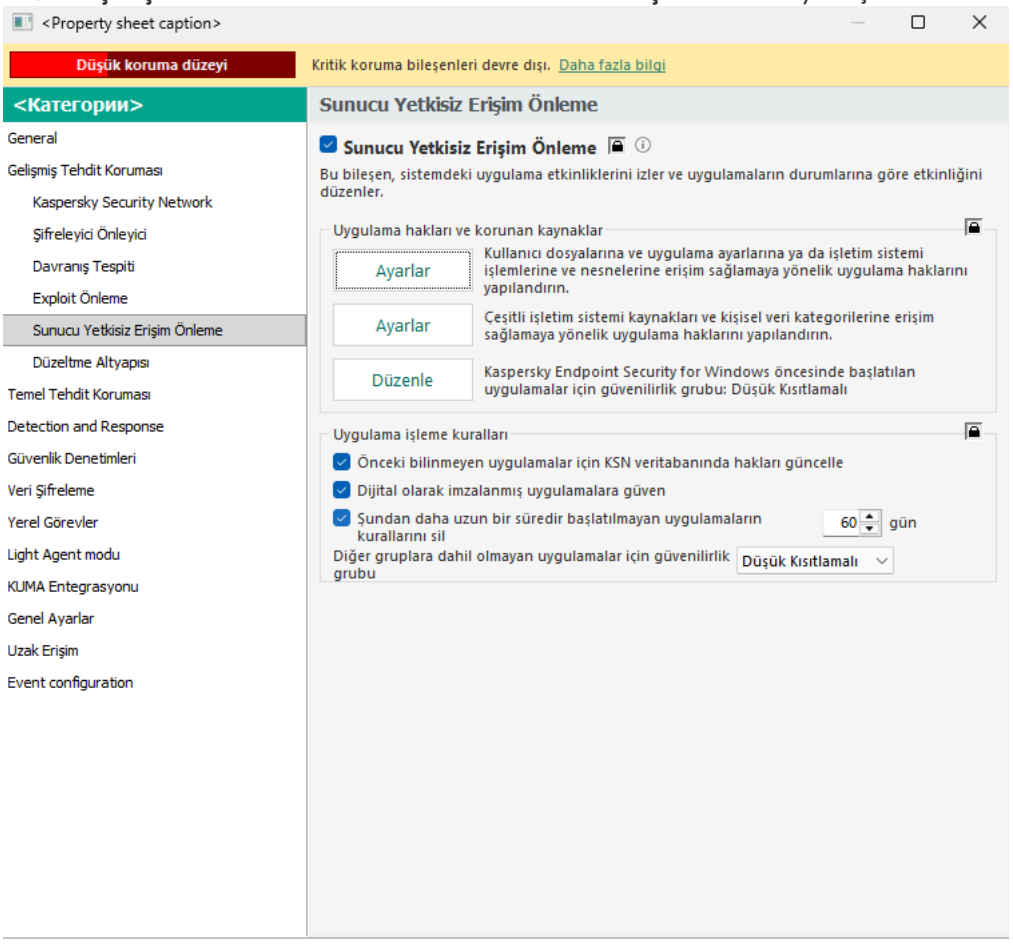
Bilgileri silinmiş bir uygulamayı başlattığınızda, Kaspersky Endpoint Security uygulamayı ilk kez başlatılıyormuş gibi analiz eder.

Yönetim Konsolu'nda (MMC) kullanılmayan uygulamalar hakkındaki bilgilerin otomatik olarak silinmesini yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

4. **Uygulama işleme kuralları** bloğunda aşağıdakilerden birini yapın:

   - Otomatik silmeyi yapılandırmak isterseniz **Şundan daha uzun bir süredir başlatılmayan uygulamaların kurallarını sil: N gün** onay kutusunu işaretleyin ve gerekli gün sayısını belirtin.

     Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından belirlenen sayıda gün geçtikten sonra silinir. Güven grubu ve uygulama hakları otomatik olarak belirlenen uygulamalar hakkındaki bilgiler de Kaspersky Endpoint Security tarafından 30 gün sonra silinir.

   - Otomatik silme özelliğini kapatmak isterseniz **Şundan daha uzun bir süredir başlatılmayan uygulamaların kurallarını sil: N gün** onay kutusunun işaretini kaldırın.

     Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından herhangi bir depolama süresi sınırı olmadan süresiz olarak saklanır. Kaspersky Endpoint Security, yalnızca güven grubu ve uygulama hakları otomatik olarak belirlenmiş uygulamalar hakkındaki bilgileri 30 gün geçtikten sonra siler.

5. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console kullanılmayan uygulamalar hakkındaki bilgilerin otomatik olarak silinmesini yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.

5. **Uygulama işleme kuralları** bloğunda aşağıdakilerden birini yapın:

   - Otomatik silme işlemini yapılandırmak istiyorsanız, **(gün, 1 ila 90)'dan uzun süredir başlatılmamış uygulamalar için kuralları sil** onay kutusunu seçin ve gün sayısını girin.

     Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından belirlenen sayıda gün geçtikten sonra silinir. Güven grubu ve uygulama hakları otomatik olarak belirlenen uygulamalar hakkındaki bilgiler de Kaspersky Endpoint Security tarafından 30 gün sonra silinir.

   - Otomatik silme özelliğini kapatmak isterseniz **Şundan uzun süredir başlatılmamış uygulamalar için kuralları sil: (gün, 1 - 90 arası)** onay kutusunun işaretini kaldırın.

     Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından herhangi bir depolama süresi sınırı olmadan süresiz olarak saklanır. Kaspersky Endpoint Security, yalnızca güven grubu ve uygulama hakları otomatik olarak belirlenmiş uygulamalar hakkındaki bilgileri 30 gün geçtikten sonra siler.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde kullanılmayan uygulamalar hakkındaki bilgilerin otomatik olarak silinmesini yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'yi seçin.

3. **Uygulama işleme kuralları** bloğunda aşağıdakilerden birini yapın:

   - Otomatik silmeyi yapılandırmak isterseniz **Şundan daha uzun bir süredir başlatılmayan uygulamaların kurallarını sil: N gün (1 - 90 arası)** onay kutusunu işaretleyin ve gerekli gün sayısını belirtin.

     Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından belirlenen sayıda gün geçtikten sonra silinir. Güven grubu ve uygulama hakları otomatik olarak belirlenen uygulamalar hakkındaki bilgiler de Kaspersky Endpoint Security tarafından 30 gün sonra silinir.

   - Otomatik silme özelliğini kapatmak isterseniz **Şundan daha uzun bir süredir başlatılmayan uygulamaların kurallarını sil: N gün (1 - 90 arası)** onay kutusunun işaretini kaldırın.

     Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından herhangi bir depolama süresi sınırı olmadan süresiz olarak saklanır. Kaspersky Endpoint Security, yalnızca güven grubu ve uygulama hakları otomatik olarak belirlenmiş uygulamalar hakkındaki bilgileri 30 gün geçtikten sonra siler.

4. Değişikliklerinizi kaydedin.

Sunucu Yetkisiz Erişim Önleme izlemesi

Sunucu Yetkisiz Erişim Önleme bileşeninin işleyişi hakkında raporlar alabilirsiniz. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.

Sunucu Yetkisiz Erişim Önleme işlemlerini izlemek için rapor yazmayı etkinleştirmelisiniz. Örneğin Sunucu Yetkisiz Erişim Önleme bileşeninin ayarlarında, bireysel uygulamalar için raporların iletilmesini etkinleştirebilirsiniz.

Sunucu Yetkisiz Erişim Önleme izlemesini yapılandırırken, olayların Kaspersky Security Center'a iletilmesi sırasında ortaya çıkabilecek ağ yükünü hesaba katın. Raporların sadece Kaspersky Endpoint Security'nin yerel günlüğüne kaydedilmesini de etkinleştirebilirsiniz.

Ses ve videoya erişimi koruma

Ses sinyali koruma özelliği ve web kamerası erişim koruma özelliği, Arm tabanlı bilgisayarlarda desteklenmemektedir.

Siber suçlular, ses ve video kaydeden cihazlara (mikrofonlar veya web kameraları gibi) erişim sağlamaya çalışmak için özel programlar kullanabilir. Kaspersky Endpoint Security, uygulamaların ne zaman ses akışı veya video akışı aldığını kontrol eder ve yetkisiz müdahalelere karşı verileri korur.

Varsayılan olarak, Kaspersky Endpoint Security yalnızca *Güvenilir* grubundaki uygulamalar için ses ve video akışlarının alınmasına izin verir. *Düşük Kısıtlamalı*, *Yüksek Kısıtlamalı* ve *Güvenilmez* gruplarındaki uygulamaların cihazlardan ses akışı ve video akışı almasına izin verilmez. Uygulamaların ses akışını ve video akışını almasına manuel olarak izin verebilirsiniz.

Ses akışı korumasının özel özellikleri

Ses akışı koruması şu özel karakteristiklere sahiptir:

- 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 Kısıtlamalı* 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 (mesela 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 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.

Uygulama web kamerası erişim korumasının özel özellikleri

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.
- 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.

BadUSB Saldırısı Önleme

Bazı virüsler, işletim sistemini USB aygıtını bir klavye gibi algılayacak şekilde kandırmak için USB aygıtların üretici yazılımını değiştirir. Sonuç olarak virüs, örneğin zararlı yazılım indirmek için kullanıcı hesabınız altında komutlar yürütebilir.

BadUSB Saldırısı Önleme bileşeni, klavyeye öykünen virüslü USB aygıtların bilgisayara bağlanmasını engeller.

Bilgisayara bir USB cihazı bağlandığında ve işletim sistemi tarafından klavye olarak algılandığında, uygulama kullanıcıdan uygulama tarafından üretilen sayısal bir kodu bu klavyeyi ya da varsa Ekran Klavyesini kullanarak girmesini ister (aşağıdaki şekle bakın). Bu işlem, klavye yetkilendirme olarak bilinir.

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 klavye yetkilendirmenin tekrarlanması gerekmez.

Yetkilendirilen klavye bilgisayarın farklı bir USB portuna bağlandığında, uygulama bu klavyenin yetkilendirilmesi için bir istem görüntüler.

Sayısal kod yanlış girildiyse uygulama yeni bir kod üretir. Sayısal kodun girişmesi için deneme sayısını yapılandırabilirsiniz. Sayısal kod birkaç kez yanlış girilirse veya klavye yetkilendirme penceresi kapatılırsa (aşağıdaki şekle bakın), uygulama bu klavyeden giriş yapılmasını engeller. USB aygıtı engelleme süresi dolduğunda ya da işletim sistemi yeniden başlatıldığında, uygulama kullanıcıdan yeniden klavye yetkilendirme yapmasını ister.

Uygulama yetkilendirilmiş bir klavyenin kullanımına izin verir ve yetkilendirilmemiş bir klavyeyi engeller.



Klavye yetkilendirme

BadUSB Saldırısı Önleme'yi Etkinleştirme ve Devre Dışı Bırakma

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

Yönetim Konsolu'nda (MMC) BadUSB Saldırısı Önleme bileşenini etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **BadUSB Saldırısı Önleme** seçimini yapın
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **BadUSB Saldırısı Önleme** onay kutusunu kullanın.

5. **Bağlandığında USB cihazı yetkilendirme** bloğunda, yetkilendirme kodunu girmek için güvenlik ayarlarını yapın:

   - **Maksimum sayıda USB cihazı doğrulama girişimi**. Yetkilendirme kodunun belirtilen sayıda yanlış girilmesi durumunda USB cihazı otomatik olarak bloke edilir. Geçerli değerler 1 ila 10 arasındadır. Örneğin, yetkilendirme kodunu girmek için beş denemeye izin verirseniz, uygulama beşinci başarısız denemeden sonra USB cihazını engeller. Kaspersky Endpoint Security, USB cihazı için engelleme süresini görüntüler. Bu süre dolduktan sonra, yetkilendirme kodunu girmek için yine beş deneme hakkınız vardır.

   - **Maksimum girişim sayısına ulaşılırken zaman aşımı (dakika)**. Yetkilendirme kodunu girmek için belirtilen sayıda başarısız denemeden sonra USB cihazı engelleme süresi. Geçerli değerler 1 ila 180 (dakika) arasındadır.

6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da BadUSB Saldırısı Önleme bileşenini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması** → **BadUSB Saldırısı Önleme** bölümüne gidin.

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **BadUSB Saldırısı Önleme ETKİN** geçiş düğmesini kullanın.

6. **USB cihazlarının yetkilendirilmesi** bloğunda, yetkilendirme kodunu girmek için güvenlik ayarlarını yapın:

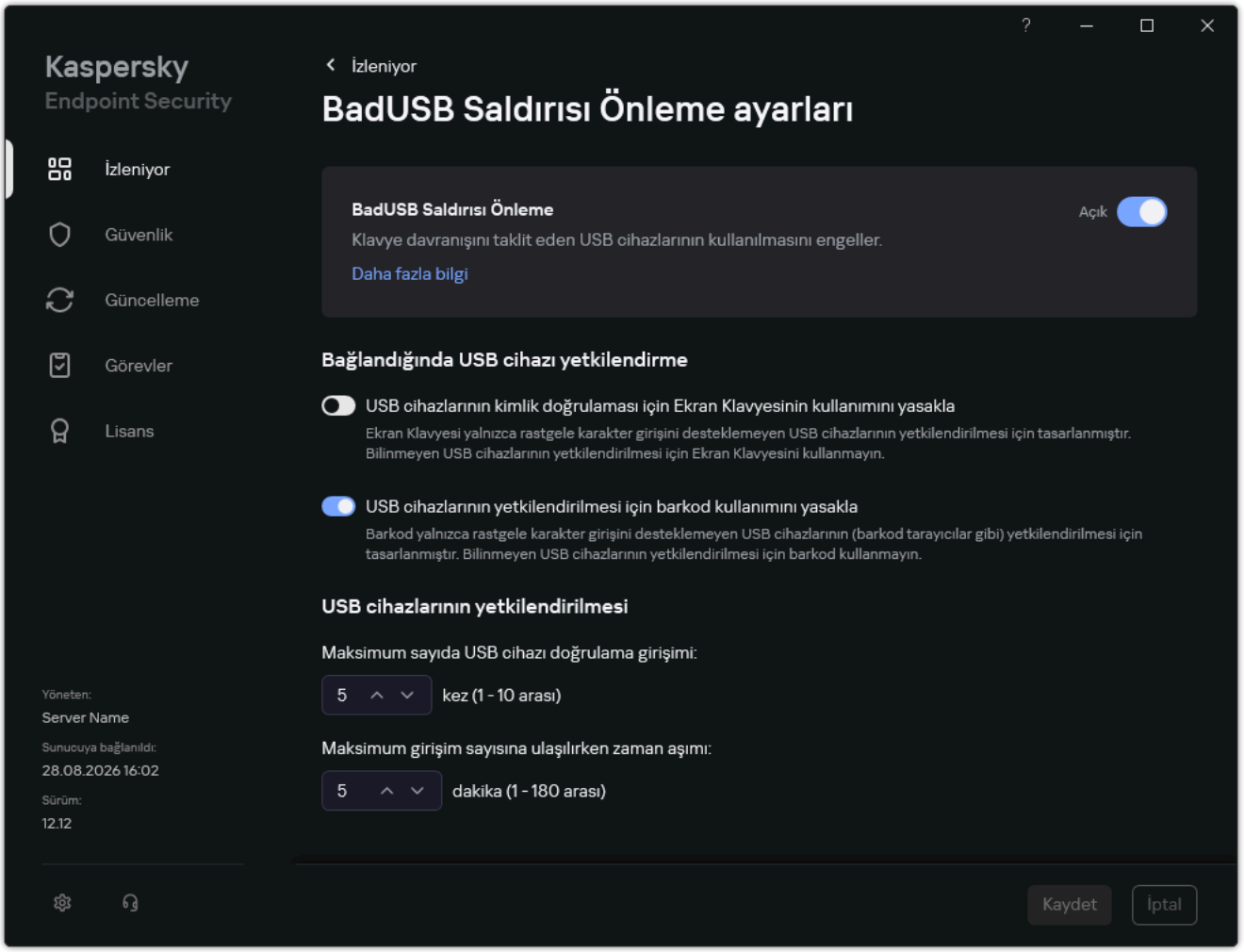
   - **Maksimum sayıda USB cihazı doğrulama girişimi**. Yetkilendirme kodunun belirtilen sayıda yanlış girilmesi durumunda USB cihazı otomatik olarak bloke edilir. Geçerli değerler 1 ila 10 arasındadır. Örneğin, yetkilendirme kodunu girmek için beş denemeye izin verirseniz, uygulama beşinci başarısız denemeden sonra USB cihazını engeller. Kaspersky Endpoint Security, USB cihazı için engelleme süresini görüntüler. Bu süre dolduktan sonra, yetkilendirme kodunu girmek için yine beş deneme hakkınız vardır.

   - **Maksimum girişim sayısına ulaşılırken zaman aşımı (dk)**. Yetkilendirme kodunu girmek için belirtilen sayıda başarısız denemeden sonra USB cihazı engelleme süresi. Geçerli değerler 1 ila 180 (dakika) arasındadır.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde BadUSB Saldırısı Önleme bileşenini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → BadUSB Saldırısı Önleme**'yi seçin.



BadUSB Saldırısı Önleme bileşeni ayarları

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **BadUSB Saldırısı Önleme** geçiş düğmesini kullanın.
4. **Bağlandığında USB cihazı yetkilendirme** bloğunda, yetkilendirme kodunu girmek için güvenlik ayarlarını yapın:
   - **Maksimum sayıda USB cihazı doğrulama girişimi**. Yetkilendirme kodunun belirtilen sayıda yanlış girilmesi durumunda USB cihazı otomatik olarak bloke edilir. Geçerli değerler 1 ila 10 arasındadır. Örneğin, yetkilendirme kodunu girmek için beş denemeye izin verirseniz, uygulama beşinci başarısız denemeden sonra USB cihazını engeller. Kaspersky Endpoint Security, USB cihazı için engelleme süresini görüntüler. Bu süre dolduktan sonra, yetkilendirme kodunu girmek için yine beş deneme hakkınız vardır.
   - **Maksimum girişim sayısına ulaşılırken zaman aşımı**. Yetkilendirme kodunu girmek için belirtilen sayıda başarısız denemeden sonra USB cihazı engelleme süresi. Geçerli değerler 1 ila 180 (dakika) arasındadır.
5. Değişikliklerinizi kaydedin.

Sonuç olarak, BadUSB Saldırısı Önleme etkinleştirilirse, Kaspersky Endpoint Security, işletim sistemi tarafından klavye olarak tanımlanan bağlı bir USB cihazının yetkilendirilmesini gerektirir. Kullanıcı, yetkilendirilmemiş bir klavyeyi yetkilendirilene kadar kullanamaz.

USB aygıtlarının kimlik doğrulaması için Ekran Klavyesinin kullanımı

Ekran Klavyesi yalnızca rastgele karakter girişini desteklemeyen USB cihazlarının (barkod tarayıcılar gibi) yetkilendirilmesi için kullanılmalıdır. Bilinmeyen USB aygıtların yetkilendirilmesi için Ekran Klavyesi'nin kullanılması önerilmez.

Yönetim Konsolu'nda (MMC) yetkilendirme için Ekran Klavyesinin kullanımına izin verme veya yasaklama

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **BadUSB Saldırısı Önleme** seçimini yapın
4. Yetkilendirme için Ekran Klavyesinin kullanımına izin vermek için **USB cihazlarının kimlik doğrulaması için Ekran Klavyesinin kullanımını yasakla** onay kutusunun işaretini kaldırın.
5. Değişikliklerinizi kaydedin.

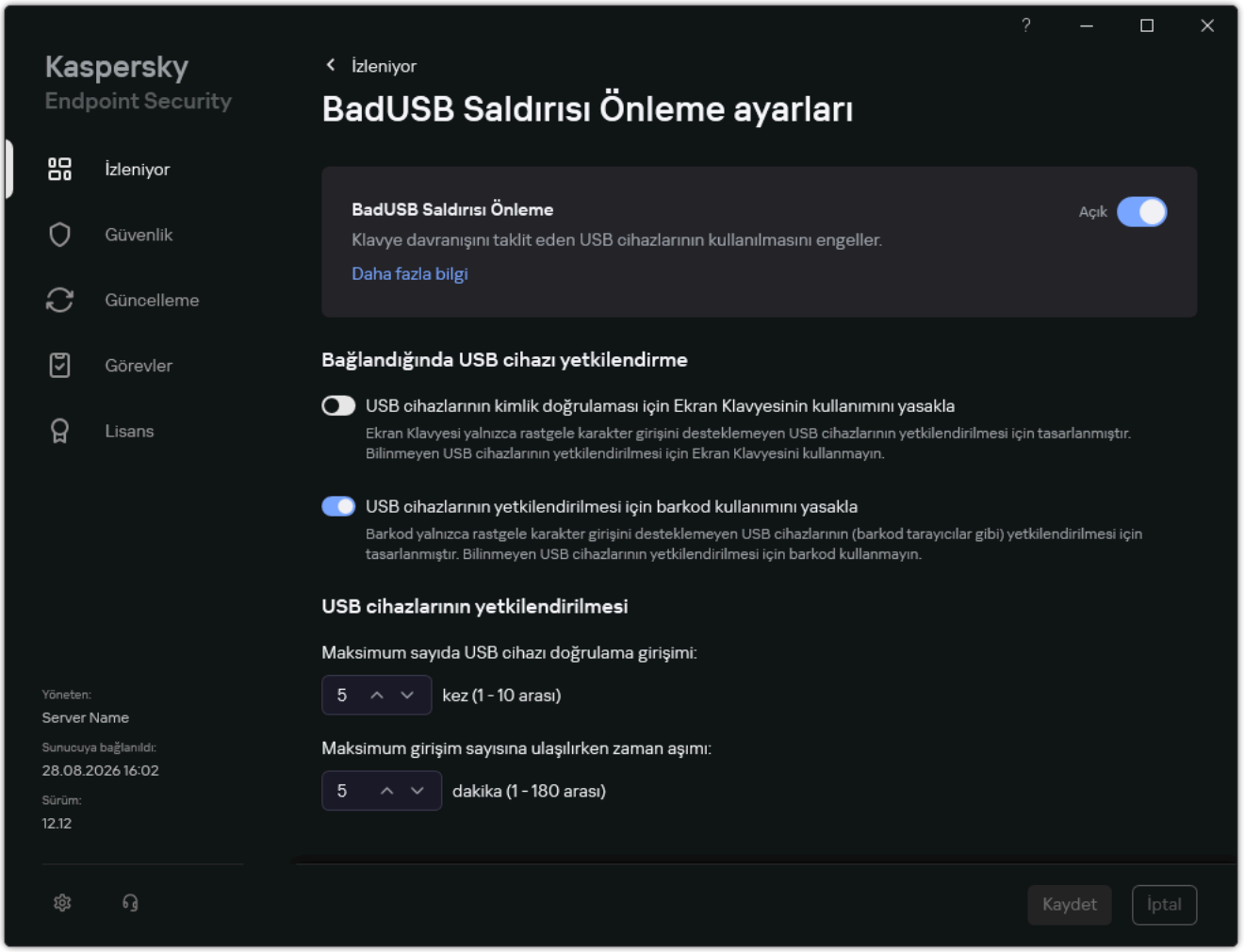
Web Console ve Cloud Console'da yetkilendirme için Ekran Klavyesi kullanımına izin verme veya yasaklama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **BadUSB Saldırısı Önleme** bölümüne gidin.
5. Yetkilendirme için Ekran Klavyesinin kullanımını engellemek veya izin vermek için **USB cihazlarının kimlik doğrulaması için Ekran Klavyesinin kullanımını yasakla** iki durumlu düğmesini kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde yetkilendirme için Ekran Klavyesi kullanımına izin verme veya yasaklama

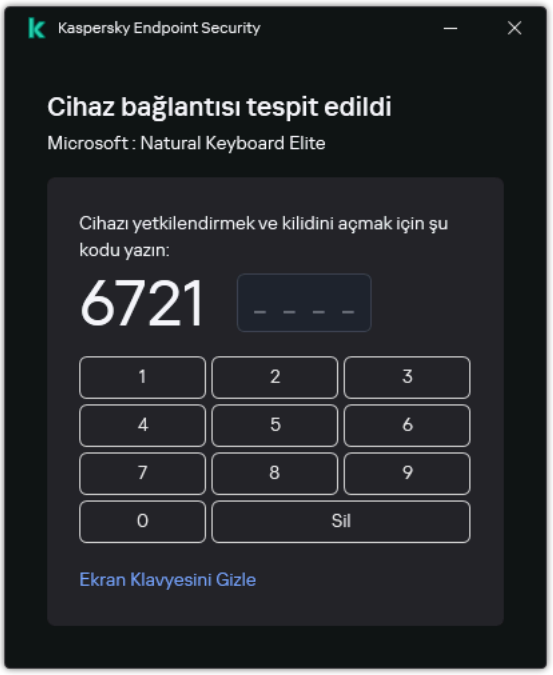
1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → BadUSB Saldırısı Önleme**'yi seçin.



BadUSB Saldırısı Önleme bileşeni ayarları

3. Yetkilendirme için Ekran Klavyesinin kullanımını engellemek veya izin vermek için **USB cihazlarının kimlik doğrulaması için Ekran Klavyesinin kullanımını yasakla** iki durumlu düğmesini kullanın.

4. Değişikliklerinizi kaydedin.



USB cihazlarının yetkilendirilmesi

Barkod tarayıcı yetkilendirmesi

Bilgisayara bir barkod tarayıcı bağlarken, BadUSB Saldırısı Önleme bileşeni bu cihazı bir giriş cihazı olarak tanımlar ve sizden yetkilendirme yapmanızı ister. Barkod tarayıcıyı yetkilendirmek için ekranda görüntülenen bir barkodu taramanız gerekir. Uygulama, çoğu barkod ve QR kodu tarayıcısı tarafından desteklenen Code39 biçiminde bir barkod oluşturur.

Kaspersky Endpoint Security başka bir barkod tarayıcı yetkilendirmesi yöntemini daha destekler. Dokunmatik ekranlı cihazlar kullanıyorsanız, bir kod yazmak için ekran klavyesini kullanabilirsiniz. Bunu yapmak için ekran klavyesine izin vermeniz gerekir. Bu yöntem, örneğin yazar kasalara yerleştirilmiş sabit barkod tarayıcılar söz konusu olduğunda kullanışlıdır. Diğer barkod tarayıcı doğrulama yöntemleri yasaktır.

Uygulama varsayılan olarak USB cihazlarının yetkilendirilmesi için bir barkod kullanmaz.

Yönetim Konsolu'nda (MMC) barkod ile USB cihazı yetkilendirmesi nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Konsol ağacında **İlkeler**'i seçin.

3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

4. İlke penceresinde, **Temel Tehdit Koruması** → **BadUSB Saldırısı Önleme** seçimini yapın

5. Yetkilendirme için barkodların kullanımını engellemek veya izin vermek için **USB cihazlarının yetkilendirilmesi için barkod kullanımını yasakla** onay kutusunu kullanın.

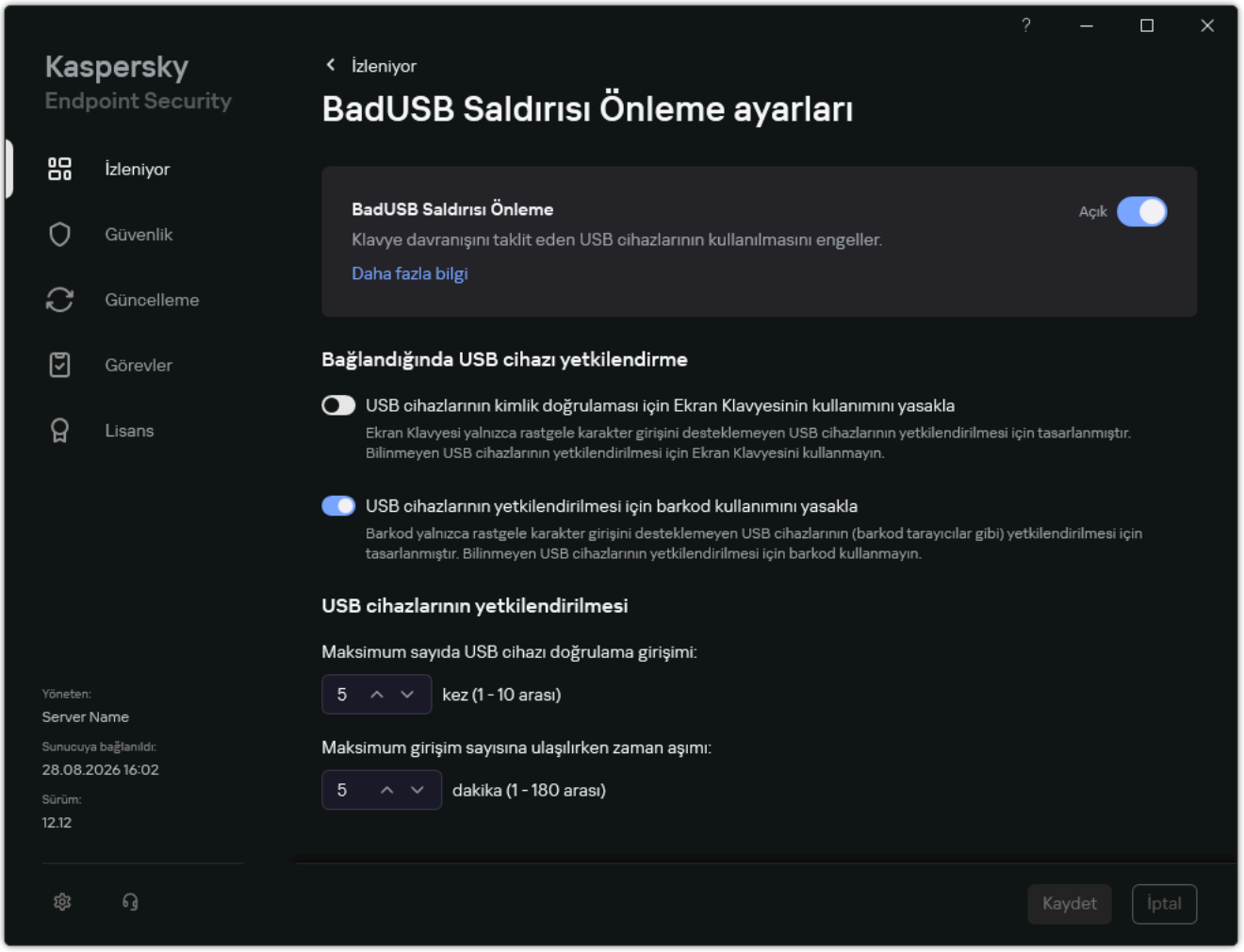
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da barkod ile USB cihazı yetkilendirmesi nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **BadUSB Saldırısı Önleme** bölümüne gidin.
5. Yetkilendirme için barkodların kullanımını engellemek veya izin vermek için **USB cihazlarının yetkilendirilmesi için barkod kullanımını yasakla** onay kutusunu kullanın.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde barkod ile USB cihazı yetkilendirmesi nasıl etkinleştirilir

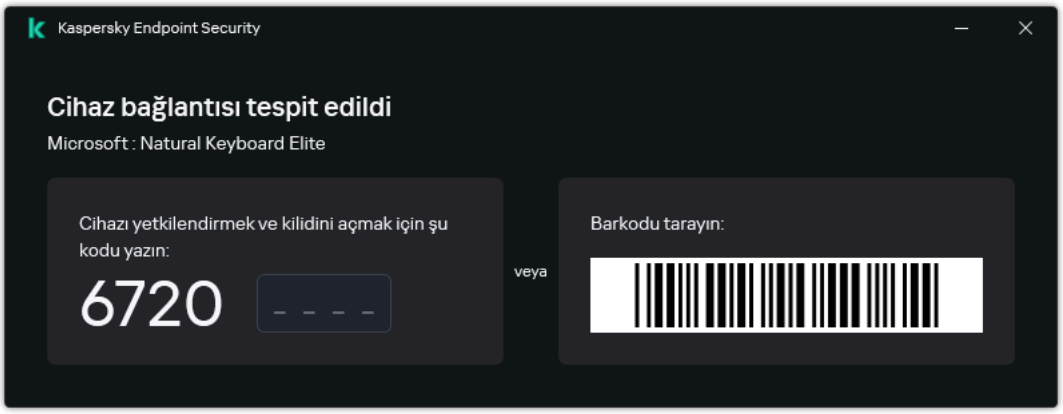
1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **BadUSB Saldırısı Önleme**'yi seçin.



BadUSB Saldırısı Önleme bileşeni ayarları

3. Yetkilendirme için barkodların kullanımını engellemek veya izin vermek için **USB cihazlarının yetkilendirilmesi için barkod kullanımını yasakla** onay kutusunu kullanın.

4. Değişikliklerinizi kaydedin.

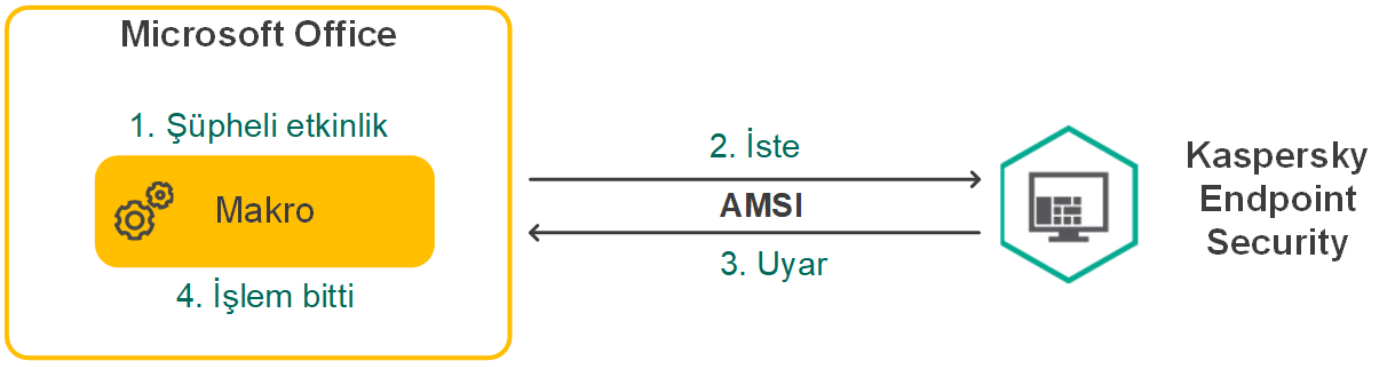


Barkod tarayıcı yetkilendirmesi

AMSI Koruması

AMSI Koruması bileşeni, Microsoft'un Antimalware Scan Interface işlevini desteklemeyi amaçlamaktadır. *Antimalware Scan Interface (AMSI)*, AMSI destekli üçüncü taraf uygulamaların, bu nesneleri ek bir tarama için Kaspersky Endpoint Security'ye göndermesine ve bu nesnelerin tarama sonuçlarını almasına (örneğin PowerShell komut dizileri) olanak tanır. Üçüncü taraf uygulamalarına örnek olarak Microsoft Office uygulamaları verilebilir (aşağıdaki resme bakın). AMSI hakkında ayrıntılar için lütfen Microsoft belgelerine bakın.

AMSI Koruması yalnızca bir tehdidi tespit edebilir ve tespit edilen tehditle ilgili bilgilendirme yapar. Bir üçüncü taraf uygulaması, bir tehdit bildirimi aldıktan sonra, kötü niyetli eylemlere izin vermez (örneğin, eylemi sonlandırır).



AMSI çalışma örneği

AMSI Koruması bileşeni, üçüncü taraf uygulamadan gelen bir isteği reddedebilir (örneğin bu uygulama, belirtilen bir aralıktaki maksimum istek sayısını aşıyorsa). Kaspersky Endpoint Security, üçüncü taraf bir uygulamadan gelen talebin reddedilmesine ilişkin bilgileri Yönetim Sunucusuna iletir. AMSI Koruma bileşeni, AMSI Koruma bileşeniyle sürekli entegrasyon etkin durumda olan üçüncü taraf uygulamalarından gelen istekleri reddetmez.

AMSI Koruması, iş istasyonları ve sunucular için aşağıdaki işletim sistemlerinde kullanılabilir:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise çoklu oturum
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise çoklu oturum
- Windows Server 2016 Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2019 Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Server Core modu dahil)
- Windows Server 2025 Standard / Datacenter

AMSI Korumasını etkinleştirme ve devre dışı bırakma

Varsayılan olarak, AMSI Koruması etkindir ve Kaspersky tarafından önerilen modda çalışır (aşağıdaki tabloya bakın).

Yönetim Konsolu'nda (MMC) AMSI Korumasını etkinleştirme veya devre dışı bırakma

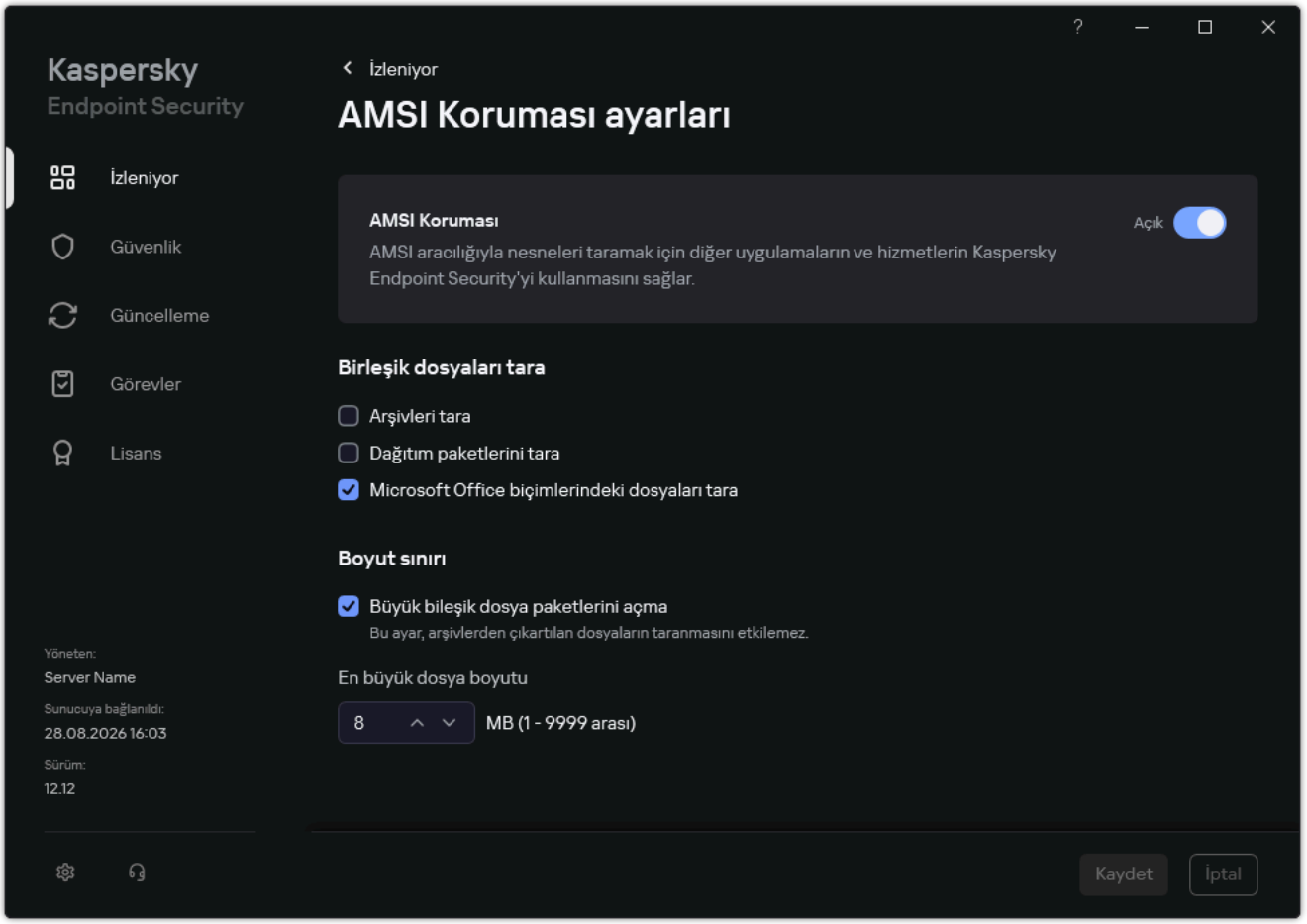
1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **AMSI Tarayıcı** seçimini yapın.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **AMSI Tarayıcı** onay kutusunu kullanın.
5. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da AMSI Korumasını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **AMSI Koruması** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **AMSI Koruması ETKİN** geçiş düğmesini kullanın.
6. Değişikliklerinizi kaydedin. İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın .

Uygulama arabiriminde AMSI Korumasını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **AMSI Koruması** seçimini yapın.



AMSI Koruması ayarları

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **AMSI Koruması** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Kaspersky uzmanları tarafından önerilen AMSI Koruması ayarları

Parametre	Değer	Açıklama
Arşivleri tara	**Kapalı**	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Dağıtım paketlerini tara	**Kapalı**	Üçüncü taraf uygulamaların dağıtım paketlerinin taranması.
Microsoft Office biçimlerindeki dosyaları tara	**Açık**	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.
Büyük bileşik dosya paketlerini açma	**En büyük dosya boyutu 8 MB**	Bu onay kutusu işaretlendiğinde, uygulama boyutları belirtilen değeri aşan birleşik dosyaları taramaz. Bu onay kutusu işaretlenmediğinde, uygulama her boyuttaki birleşik dosyaları tarar. Uygulama, onay kutusunun seçili olup olmadığından bağımsız olarak arşivlerden çıkarılan büyük dosyaları tarar.

AMSI Koruması tarafından dosya taramasını optimize etme

Dosya taramayı optimize edebilirsiniz: tarama zamanını azaltın ve Kaspersky Endpoint Security'nin çalışma hızını arttırın. Taranması gereken bileşik dosyaları seçebilirsiniz: arşivler, dağıtım paketleri veya ofis biçimlerindeki dosyalar. Taranacak bileşik dosyaların boyutunu da sınırlayabilirsiniz. AMSI Koruması bileşeni, belirtilen boyuttan daha büyük olan bileşik dosyaları açmayacaktır.

Virüsleri ve diğer zararlı yazılımları gizlemek için yaygın bir teknik, arşivler 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 türlerini sınırlayarak, taramayı hızlandırabilirsiniz.

Yönetim Konsolu'nda (MMC) AMSI Koruması tarafından dosya taramasını optimize etme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **AMSI Tarayıcı** seçimini yapın.
4. **Birleşik dosyaları tara** bloğunda, taramak istediğiniz bileşik dosyaların türünü belirtin: arşivler, dağıtım paketi veya Office biçimlerindeki dosyalar.
5. **Boyut sınırı** bloğunda aşağıdakilerden birini yapın:
   - AMSI Koruması bileşeninin büyük bileşik dosyaları açmasını engellemek için **Büyük bileşik dosyaları açma** onay kutusunu seçin ve gerekli değeri belirtin. AMSI Koruması bileşeni, belirtilen boyuttan daha büyük olan bileşik dosyaları açmayacaktır.
   - AMSI Koruması bileşeninin Büyük bileşik dosya paketlerini açmasına izin vermek için **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretini kaldırın.

   AMSI Koruması bileşeni, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük boyutlu dosyaları tarar.
6. Değişikliklerinizi kaydedin. İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın.

Web Console ve Cloud Console'da AMSI Protection tarafından dosya taramasını optimize etme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **AMSI Koruması** bölümüne gidin.
5. **Birleşik dosyaları tara** bloğunda, taramak istediğiniz bileşik dosyaların türünü belirtin: arşivler, dağıtım paketi veya Office biçimlerindeki dosyalar.

6. **Tarama optimizasyonu** bloğunda aşağıdakilerden birini yapın:

   - AMSI Koruması bileşeninin büyük bileşik dosyaları açmasını engellemek için **Boyut sınırları etkin** onay kutusunu seçin ve gerekli değeri belirtin. AMSI Koruması bileşeni, belirtilen boyuttan daha büyük olan bileşik dosyaları açmayacaktır.

   - AMSI Koruma bileşeninin büyük bileşik dosyaları açmasına izin vermek için **Boyut sınırları etkin** onay kutusunun işaretini kaldırın.

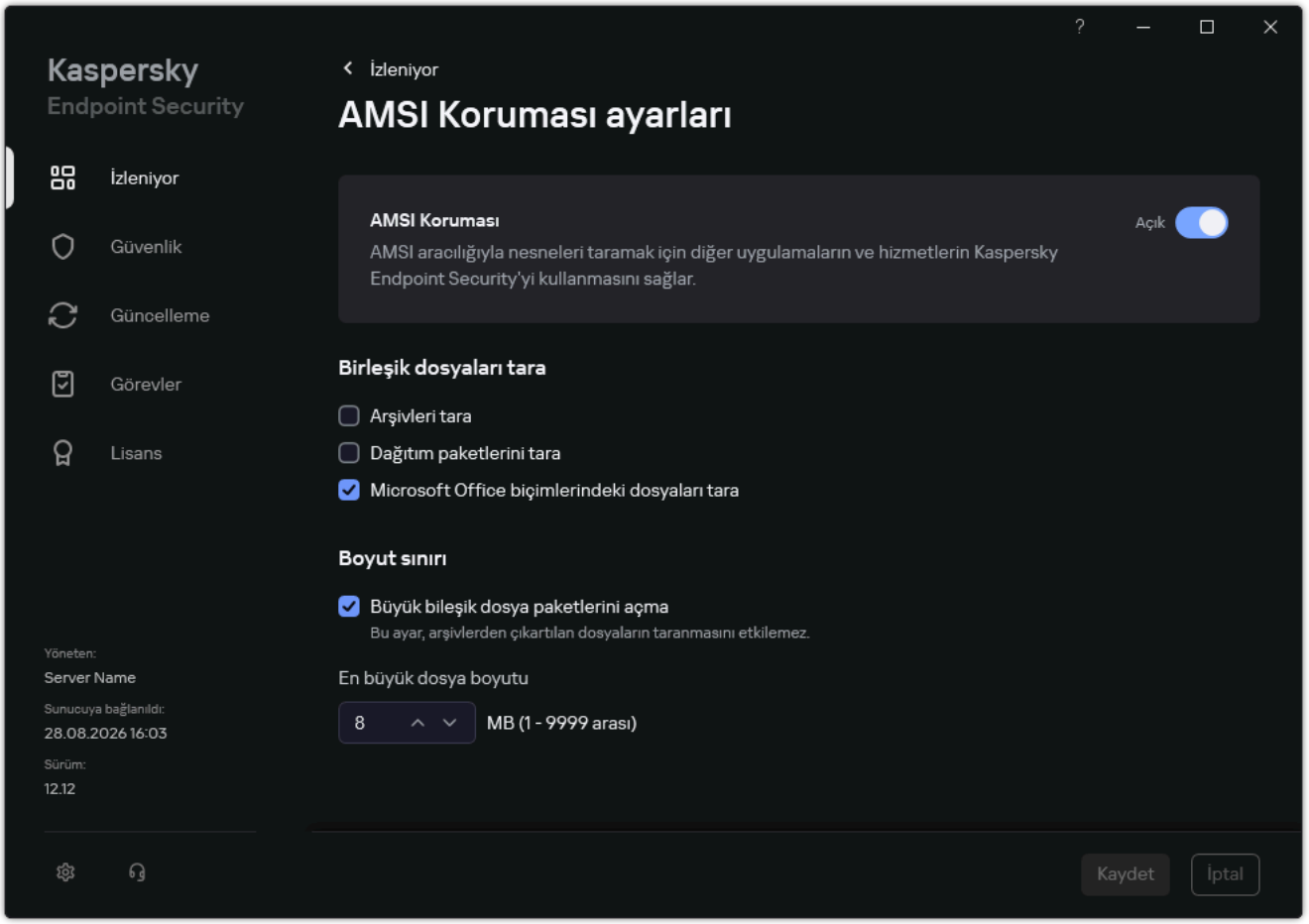
   AMSI Koruması bileşeni, **Boyut sınırları etkin** onay kutusunun seçili olup olmadığına bakılmaksızın arşivlerden çıkarılan büyük dosyaları tarar.

7. Değişikliklerinizi kaydedin. İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın.

Uygulama arabiriminde AMSI Koruması ile dosya taramasını optimize etme

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **AMSI Koruması** seçimini yapın.



AMSI Koruması ayarları

3. **Birleşik dosyaları tara** bloğunda, taramak istediğiniz bileşik dosyaların türünü belirtin: arşivler, dağıtım paketi veya Office biçimlerindeki dosyalar.

4. **Boyut sınırı** bloğunda aşağıdakilerden birini yapın:

   - AMSI Koruması bileşeninin büyük bileşik dosyaları açmasını engellemek için **Büyük bileşik dosyaları açma** onay kutusunu seçin ve gerekli değeri belirtin. AMSI Koruması bileşeni, belirtilen boyuttan daha büyük olan bileşik dosyaları açmayacaktır.

   - AMSI Koruması bileşeninin Büyük bileşik dosya paketlerini açmasına izin vermek için **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretini kaldırın.

   AMSI Koruması bileşeni, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük boyutlu dosyaları tarar.

5. Değişikliklerinizi kaydedin.

Web Tehdidi Koruması

Web Tehdidi Koruması bileşeni, internetten zararlı dosyaların indirilmesini önler ve ayrıca zararlı ve kimlik avı amaçlı web sitelerine bağlantıyı engeller. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Kaspersky Endpoint Security sadece HTTP, HTTPS ve FTP trafiğini tarar. Kaspersky Endpoint Security URL'leri ve IP adreslerini tarar.

Tehdit Korumasını kullanmak için uygulamanın ilk yapılandırmasını tamamlamanız gerekir:

- HTTPS trafiğini izlemek için şifreli bağlantı taramasını etkinleştirin (varsayılan olarak etkindir).
- Kaspersky Endpoint Security'nin izlemesi gereken portları seçin (varsayılan olarak uygulama tüm portları izler).
- Kaspersky Endpoint Security'nin trafiğini izlemesini istediğiniz uygulamaları seçin. Çoğu tarayıcı Kaspersky tarafından önerilen uygulamalar listesinde zaten vardır. Eğer tarayıcınız listede yoksa manuel olarak ekleyin.
- Web trafiğine bir web sayfası etkileşim komut dosyası enjekte etmenizi öneririz (varsayılan olarak komut dosyası enjeksiyonu devre dışıdır). Bu komut dosyası, uygulama olay günlüğü, işletim sistemi olay günlüğü ve raporlar için Web Tehdidi Koruması olaylarının kaydını sağlar.

Bir kullanıcı kötü amaçlı veya kimlik avı yapan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller ve bir uyarı gösterir.

Web Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Web Tehdidi Koruması bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Uygulama, Web Tehdidi Koruması için farklı ayar grupları uygulayabilir. Uygulama içinde saklanan bu ayar gruplarına *güvenlik düzeyleri* denir: **Yüksek**, **Önerilen**, **Düşük**. **Önerilen** İnternet trafiği güvenlik düzeyi ayarları Kaspersky uzmanları tarafından tavsiye edilen en iyi ayarlar olarak değerlendirilir (aşağıdaki tabloya bakın). HTTP ve FTP protokolleri aracılığıyla alınan veya iletilen internet trafiği için önceden yüklenmiş güvenlik düzeylerinden birini seçebilir veya özel bir internet trafiği güvenlik düzeyi yapılandırabilirsiniz. E-posta güvenlik düzeyi ayarlarını değiştirirseniz önerilen e-posta güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

Güvenlik düzeyini yalnızca Yönetim Konsolu'nda (MMC) veya uygulamanın yerel arabiriminde seçebilir veya yapılandırabilirsiniz. Web Console veya Cloud Console'da güvenlik düzeyini seçemez veya yapılandıramazsınız.

Yönetim Konsolu'nda (MMC) Web Tehdidi Koruması bileşeni nasıl etkinleştirilir veya devre dışı bırakılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Web Tehdidi Koruması** kutucuğunu işaretleyin.
5. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:
   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.
     - **Yüksek**. Web Tehdidi Koruması bileşeninin, bir bilgisayarın HTTP ve FTP yoluyla aldığı web trafiğinin maksimum taramasını gerçekleştirdiği güvenlik düzeyi. Web Tehdidi Koruması, uygulama veritabanlarının tam setini kullanarak tüm İnternet trafiği nesnelerini ayrıntılı olarak tarar ve mümkün olan en ayrıntılı sezgisel analizi gerçekleştirir.
     - **Önerilen**. Uygulamanın performansı ve İnternet trafiği güvenliği arasında en iyi dengeyi sağlayan güvenlik düzeyidir. Web Tehdidi Koruması bileşeni, normal tarama düzeyinde sezgisel analiz yapar. Bu İnternet trafiği güvenlik düzeyi Kaspersky uzmanları tarafından önerilir. Önerilen güvenlik düzeyi için ayarların değerleri aşağıdaki tabloda verilmiştir.
     - **Düşük**. Bu İnternet trafiği güvenlik düzeyinin ayarları, en yüksek İnternet trafiğin tarama hızını sağlar. Web Tehdidi Koruması bileşeni, hızlı tarama düzeyinde sezgisel analiz yapar.
   - Özel bir güvenlik düzeyi yapılandırmak istiyorsanız **Ayarlar** düğmesine tıklayın ve kendi bileşen ayarlarınızı tanımlayın (aşağıdaki tabloya bakın).

     Varsayılan olarak düğmesine tıklayarak önceden ayarlanmış güvenlik düzeylerinin değerlerini geri yükleyebilirsiniz.

6. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı İnternet trafiği üzerinde gerçekleştireceği eylemi seçin:

   - **Engelle**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Web Tehdidi Koruması bileşeni nesneye erişimi engeller ve tarayıcıda bir mesaj görüntüler.

   - **Bilgilendir**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Kaspersky Endpoint Security bu nesnenin bilgisayara indirilmesine izin verir ancak nesneyi virüslü nesne hakkında etkin tehditler listesine ekler.

7. Değişikliklerinizi kaydedin.

Web Console'da Web Tehdidi Koruması bileşeni nasıl etkinleştirilir veya devre dışı bırakılır

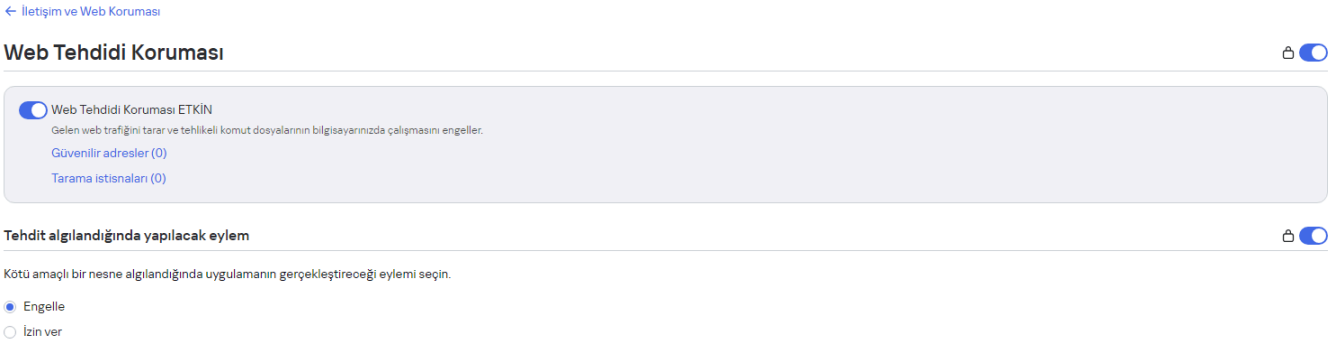
1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Web Tehdidi Koruması** bölümüne gidin.



Web Tehdidi Koruması ayarları

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Web Tehdidi Koruması ETKİN** geçiş düğmesini kullanın.

6. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı İnternet trafiği üzerinde gerçekleştireceği eylemi seçin:

   - **Engelle**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Web Tehdidi Koruması bileşeni nesneye erişimi engeller ve tarayıcıda bir mesaj görüntüler.

   - **İzin ver, bilgilendir veya eylem için uyarı ver (işletim sistemine bağlıdır)**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Kaspersky Endpoint Security bu nesnenin bilgisayara indirilmesine izin verir ancak nesneyi virüslü nesne hakkında etkin tehditler listesine ekler.

7. Gerektiğinde, güvenilir web adreslerinin bir listesini yapın.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Tehdidi Koruması bileşenini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Web Tehdidi Koruması** geçiş düğmesini kullanın.

4. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:

   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.

     - **Yüksek**. Web Tehdidi Koruması bileşeninin, bir bilgisayarın HTTP ve FTP yoluyla aldığı web trafiğinin maksimum taramasını gerçekleştirdiği güvenlik düzeyi. Web Tehdidi Koruması, uygulama veritabanlarının tam setini kullanarak tüm İnternet trafiği nesnelerini ayrıntılı olarak tarar ve mümkün olan en ayrıntılı sezgisel analizi gerçekleştirir.

     - **Önerilen**. Uygulamanın performansı ve İnternet trafiği güvenliği arasında en iyi dengeyi sağlayan güvenlik düzeyidir. Web Tehdidi Koruması bileşeni, normal tarama düzeyinde sezgisel analiz yapar. Bu İnternet trafiği güvenlik düzeyi Kaspersky uzmanları tarafından önerilir. Önerilen güvenlik düzeyi için ayarların değerleri aşağıdaki tabloda verilmiştir.

     - **Düşük**. Bu İnternet trafiği güvenlik düzeyinin ayarları, en yüksek İnternet trafiğin tarama hızını sağlar. Web Tehdidi Koruması bileşeni, hızlı tarama düzeyinde sezgisel analiz yapar.

   - Özel bir güvenlik düzeyi yapılandırmak istiyorsanız **Gelişmiş ayarlar** düğmesine tıklayın ve kendi bileşen ayarlarınızı tanımlayın (aşağıdaki tabloya bakın).

     Önerilen güvenlik düzeyini geri yükle düğmesine tıklayarak önceden ayarlanmış güvenlik seviyelerinin değerlerini geri yükleyebilirsiniz.

5. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı İnternet trafiği üzerinde gerçekleştireceği eylemi seçin:

   - **Engelle**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Web Tehdidi Koruması bileşeni nesneye erişimi engeller ve tarayıcıda bir mesaj görüntüler.

   - **Bilgilendir**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Kaspersky Endpoint Security bu nesnenin bilgisayara indirilmesine izin verir ancak nesneyi virüslü nesne hakkında etkin tehditler listesine ekler.

6. Değişikliklerinizi kaydedin.

Kaspersky uzmanları tarafından önerilen Web Tehdidi Koruması ayarları (önerilen güvenlik düzeyi)

Parametre	Değer	Açıklama
Web adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et	**Açık**	Kötü amaçlı web adresleri veritabanına dahil edilip edilmediğini belirlemek için bağlantıların taranması, red listesine alınmış web sitelerini izlemenize olanak tanır. Kaspersky tarafından güncellenen kötü amaçlı web adreslerinin veritabanı, uygulama kurulum paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri sırasında güncellenir.
Web adresini kimlik avı internet adresleri veritabanıyla karşılaştırarak kontrol et	**Açık**	E-dolandırıcılık web adreslerinin veritabanı, e-dolandırıcılık saldırıları başlatmak için kullanılan halihazırda bilinen web sitelerinin web adreslerini içerir. Kaspersky, kimlik avı bağlantılarından oluşan veritabanını, Anti-Phishing Çalışma Grubu olarak da bilinen uluslararası kuruluştan alınan adreslerle destekler. E-dolandırıcılık adresleri veritabanı, uygulama yükleme paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri ile tamamlanmaktadır.
Sezgisel analiz kullan (Web Tehdidi Koruması)	**Normal tarama**	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. Virüs ve tehdit oluşturan diğer uygulamalar için web trafiği tarandığında, sezgisel çözümleyici yürütülebilir dosyalarda talimatları uygular. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
Sezgisel analiz kullan (Kimlik Avı Engelleyici)	**Açık**	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.
Tehdit algılandığında yapılacak eylem	**Engelle**	Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Web Tehdidi Koruması bileşeni nesneye erişimi engeller ve tarayıcıda bir mesaj görüntüler.

Kötü amaçlı web adresi tespit yöntemlerini yapılandırma

Web Tehdidi Koruması, antivirüs veritabanlarını, Kaspersky Security Network bulut hizmetini ve sezgisel analizi kullanarak kötü amaçlı internet adreslerini tespit eder.

Kötü amaçlı internet adresi tespit yöntemlerini yalnızca Yönetim Konsolu'nda (MMC) veya uygulamanın yerel arabiriminde seçebilirsiniz. Web Console veya Cloud Console'da kötü amaçlı internet adresi tespit yöntemlerini seçemezsiniz. Varsayılan seçenek, sezgisel analiz (normal tarama) ile internet adreslerini kötü amaçlı adresler veritabanına göre kontrol etmektir.

Kötü amaçlı adresler veritabanını kullanarak tarama

Kötü amaçlı web adresleri veritabanına dahil edilip edilmediğini belirlemek için bağlantıların taranması, red listesine alınmış web sitelerini izlemenize olanak tanır. Kaspersky tarafından güncellenen kötü amaçlı web adreslerinin veritabanı, uygulama kurulum paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri sırasında güncellenir.

Kaspersky Endpoint Security, kötü amaçlı web adreslerinin veritabanlarında listelenip listelenmediğini belirlemek için tüm bağlantıları tarar. Uygulamanın güvenli bağlantı tarama ayarları, bağlantı tarama işlevini etkilemez. Diğer bir deyişle, şifrelenmiş bağlantıların taranması devre dışı bırakıldığında, Kaspersky Endpoint Security, ağ trafiği şifrelenmiş bir bağlantı üzerinden iletilse bile bağlantıları kötü amaçlı internet adreslerinin veritabanlarına göre denetler.

Yönetim Konsolu'nu (MMC) kullanarak kötü amaçlı internet adresleri veritabanına göre internet adreslerinin kontrol edilmesini etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması → Web Tehdidi Koruması**'nı seçin.
4. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.
5. Açılan pencerede, adreslerin kötü amaçlı internet adresleri veritabanına göre kontrol edilmesini etkinleştirmek veya devre dışı bırakmak için bu penceredeki **Tarama yöntemleri** bloğundan **Web adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et** onay kutusunu işaretleyin ya da işaretini kaldırın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde adreslerin kötü amaçlı adres veritabanına göre kontrol edilmesini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Web Tehdidi Koruması**'nı seçin.

3. **Gelişmiş ayarlar**'a tıklayın.

4. Adreslerin kötü amaçlı internet adresleri veritabanına göre kontrol edilmesini etkinleştirmek veya devre dışı bırakmak için **Tarama yöntemleri** bloğunda **Web adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et** onay kutusunu işaretleyin ya da işaretini kaldırın.

5. Değişikliklerinizi kaydedin.

Sezgisel analiz

Sezgisel analiz sırasında Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz eder. Sezgisel analiz, Kaspersky Endpoint Security'nin veritabanlarında kayıt bulunmayan tehditleri tespit edebilir.

Virüs ve tehdit oluşturan diğer uygulamalar için web trafiği tarandığında, sezgisel çözümleyici yürütülebilir dosyalarda talimatları uygular. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.

Yönetim Konsolu'nda (MMC) sezgisel analiz kullanımını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.

4. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.

5. Açılan penceredeki **Tarama yöntemleri** bloğunda, uygulamanın web trafiğini virüslere ve diğer zararlı yazılımlara karşı tararken sezgisel analiz kullanmasını istiyorsanız **Sezgisel analiz kullan** onay kutusunu seçin.

6. Sezgisel analiz düzeyini ayarlamak için kaydırma çubuğunu kullanın: **hızlı tarama**, **normal tarama** ya da **ayrıntılı tarama**.

   Virüs ve tehdit oluşturan diğer uygulamalar için web trafiği tarandığında, sezgisel çözümleyici yürütülebilir dosyalarda talimatları uygular. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde sezgisel analiz kullanımını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.

3. **Gelişmiş ayarlar**'a tıklayın.

4. **Tarama yöntemleri** bloğunda, uygulamanın web trafiğini virüslere ve diğer zararlı yazılımlara karşı tararken sezgisel analiz kullanmasını istiyorsanız **Sezgisel analiz kullan** onay kutusunu seçin.

   Virüs ve tehdit oluşturan diğer uygulamalar için web trafiği tarandığında, sezgisel çözümleyici yürütülebilir dosyalarda talimatları uygular. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.

5. Değişikliklerinizi kaydedin.

Kimlik Avı Koruması

Web Tehdidi Koruması, kimlik avı web adreslerine ait olup olmadıklarını görmek için bağlantıları kontrol eder. Bu, *kimlik avı saldırılarının* önlenmesine yardımcı olur. Kimlik avı saldırısı, bankanın resmi İnternet sitesinin bağlantısını içeren ve sözde 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 mesajlaşma uygulamaları gibi diğer kaynaklardan da gelebileceği için Web Tehdidi Koruması bileşeni, İnternet trafiği tarama düzeyinde bir e-dolandırıcılık web sitesine erişim denemelerini izler ve bu web sitelerine erişimi engeller. E-dolandırıcılık URL'lerinin listeleri Kaspersky Endpoint Security dağıtım kitinde bulunmaktadır.

Kimlik Avı Korumasını yalnızca Yönetim Konsolu'nda (MMC) veya uygulamanın yerel arabiriminde seçebilir veya yapılandırabilirsiniz. Web Console veya Cloud Console'da Kimlik Avı Korumasını yapılandıramazsınız. Varsayılan olarak, sezgisel analiz ile Kimlik Avı Koruması etkindir.

Yönetim Konsolu'nda (MMC) Kimlik Avı Korumasını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Temel Tehdit Koruması → Web Tehdidi Koruması**'nı seçin.

4. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.

5. Açılan pencerede, Kimlik Avı Korumasını etkinleştirmek veya devre dışı bırakmak için bu penceredeki **Kimlik Avı Koruması ayarları** bloğundan **Web adresini kimlik avı internet adresleri veritabanıyla karşılaştırarak kontrol et** onay kutusunu işaretleyin ya da işaretini kaldırın.

   E-dolandırıcılık web adreslerinin veritabanı, e-dolandırıcılık saldırıları başlatmak için kullanılan halihazırda bilinen web sitelerinin web adreslerini içerir. Kaspersky, kimlik avı bağlantılarından oluşan veritabanını, Anti-Phishing Çalışma Grubu olarak da bilinen uluslararası kuruluştan alınan adreslerle destekler. E-dolandırıcılık adresleri veritabanı, uygulama yükleme paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri ile tamamlanmaktadır.

6. Uygulamanın web sayfalarını kimlik avı bağlantılarına göre tararken sezgisel analiz kullanmasını istiyorsanız **Sezgisel analiz kullan** onay kutusunu işaretleyin.

   Sezgisel analiz sırasında Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz eder. Sezgisel analiz, Kaspersky Endpoint Security'nin veritabanlarında kayıt bulunmayan tehditleri tespit edebilir.

Bağlantıları taramak için anti virüs veritabanı ve sezgisel analize ek olarak Kaspersky Security Network tanınırlık veritabanlarını da kullanabilirsiniz.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Kimlik Avı Korumasını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.
4. Web Tehdidi Koruması bileşeninin, bağlantıları kimlik avı web adreslerinin veritabanlarına göre kontrol etmesini istiyorsanız, **Kimlik Avı Koruması** bloğundaki **Web adresini kimlik avı internet adresleri veritabanıyla karşılaştırarak kontrol et** onay kutusunu seçin. E-dolandırıcılık web adreslerinin veritabanı, e-dolandırıcılık saldırıları başlatmak için kullanılan halihazırda bilinen web sitelerinin web adreslerini içerir. Kaspersky, kimlik avı bağlantılarından oluşan veritabanını, Anti-Phishing Çalışma Grubu olarak da bilinen uluslararası kuruluştan alınan adreslerle destekler. E-dolandırıcılık adresleri veritabanı, uygulama yükleme paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri ile tamamlanmaktadır.
5. Uygulamanın web sayfalarını kimlik avı bağlantılarına göre tararken sezgisel analiz kullanmasını istiyorsanız **Sezgisel analiz kullan** onay kutusunu işaretleyin.

   Sezgisel analiz sırasında Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz eder. Sezgisel analiz, Kaspersky Endpoint Security'nin veritabanlarında kayıt bulunmayan tehditleri tespit edebilir.

   Bağlantıları taramak için anti virüs veritabanı ve sezgisel analize ek olarak Kaspersky Security Network tanınırlık veritabanlarını da kullanabilirsiniz.
6. Değişikliklerinizi kaydedin.

Güvenilir internet adreslerinin listesini oluşturma

Web Tehdidi Koruması, kötü amaçlı ve kimlik avı web sitelerine ek olarak diğer web sitelerini de engelleyebilir. Örneğin, Web Tehdidi Koruması, RFC standartlarını karşılamayan HTTP trafiğini engeller. İçeriğine güvenmeniz gereken URL'lerin listesini oluşturabilirsiniz. Web Tehdidi Koruması bileşeni, Güvenilir internet adreslerindeki bilgilerde virüs veya diğer tehditleri analiz etmez. Bu seçenek, örneğin Web Tehdidi Koruması bileşeni bilinen bir İnternet sitesinden bir dosya indirmeye karıştığında faydalı olabilir.

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

Yönetim Konsolu (MMC) kullanılarak bir güvenilir internet adresi nasıl eklenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.
5. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.

6. Açılan pencerede, **Güvenilir internet adresleri** sekmesini seçin.

7. **Güvenilir adreslerin web trafiğini tarama** onay kutusunu seçin.

   Bu seçenekt ercih edildiğinde, Web Tehdidi Koruması bileşeni, adresleri güvenilir internet adresleri listesinde bulunan web sayfalarının veya web sitelerinin içeriğini taramaz. İnternet sayfasının/İnternet sitesinin hem tam adresini hem de adres maskesini güvenilir internet adresleri listesine ekleyebilirsiniz.

8. İçeriğine güvendiğiniz URL'lerin / İnternet sayfalarının bir listesini oluşturabilirsiniz.

   Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

   Ayrıca, bir XML dosyasından bir güvenilir adresler listesini içe aktarabilirsiniz.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da güvenilir bir web adresi nasıl eklenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenilir Bölge** bölümüne gidin.

5. Açılan pencerede **Web adresleri** bağlantısına tıklayın.

   Güvenilir web adreslerinin listesini içeren bir pencere açılır.

6. İçeriğine güvendiğiniz URL'lerin / İnternet sayfalarının bir listesini oluşturabilirsiniz.

   Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

   Ayrıca, bir JSON dosyasından bir güvenilir adresler listesini içe aktarabilirsiniz.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde bir güvenilir internet adresi nasıl eklenir

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.

3. **Gelişmiş ayarlar**'a tıklayın.

4. **Güvenilir URL'lerden gelen internet trafiğini tarama** onay kutusunu seçin.

   Bu seçenekt ercih edildiğinde, Web Tehdidi Koruması bileşeni, adresleri güvenilir internet adresleri listesinde bulunan web sayfalarının veya web sitelerinin içeriğini taramaz. İnternet sayfasının/İnternet sitesinin hem tam adresini hem de adres maskesini güvenilir internet adresleri listesine ekleyebilirsiniz.

5. İçeriğine güvendiğiniz URL'lerin / İnternet sayfalarının bir listesini oluşturabilirsiniz.

   Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

   Ayrıca, bir XML dosyasından bir güvenilir adresler listesini içe aktarabilirsiniz.

6. Değişikliklerinizi kaydedin.

Sonuç olarak, Web Tehdidi Koruması, güvenilir internet adreslerinin trafiğini taramaz. Kullanıcı her zaman güvenilir bir internet sitesi açabilir ve bu internet sitesinden dosya indirebilir. İnternet sitesine erişemezseniz, Şifreli bağlantıları tarama, İnternet Denetimi ve Ağ portları izleme bileşenlerinin ayarlarını kontrol edin. Kaspersky Endpoint Security, güvenilir bir internet sitesinden indirilen bir dosyayı kötü amaçlı olarak algıladığı takdirde bu dosyayı istisnalara ekleyebilirsiniz.

Ayrıca şifrelenmiş bağlantılar için genel bir istisna listesi oluşturabilirsiniz. Bu durumda, Kaspersky Endpoint Security, Web Tehdidi Koruması, Posta Tehdidi Koruması, İnternet Denetimi bileşenleri işlerini yaparken güvenilir internet adreslerinin HTTPS trafiğini taramaz.

Güvenilir internet adresleri listesini dışa ve içe aktarma

Güvenilir internet adreslerinin listesini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda web adresi eklemek için dosyayı değiştirebilirsiniz. Güvenilir web adresleri listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) güvenilir web adreslerinin listesi nasıl içe/dışa aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Web Tehdidi Koruması**'nı seçin.
4. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.
5. Açılan pencerede, **Güvenilir internet adresleri** sekmesini seçin.
6. Güvenilir internet adreslerinin listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz güvenilir web adreslerini seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
      Herhangi bir güvenilir web adresi seçmediyseniz, Kaspersky Endpoint Security tüm web adreslerini dışa aktarır.
   b. **Dışa aktar** bağlantısına tıklayın.
   c. Açılan pencerede, güvenilir internet adresleri listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
      Kaspersky Endpoint Security, güvenilir internet adresleri listesinin tamamını XML dosyasına aktarır.
7. Güvenilir internet adresleri listesini içe aktarmak için:
   a. **İçe aktar** bağlantısına tıklayın.
      Açılan pencerede, Güvenilir internet adresleri listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir Güvenilir internet adresleri listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

8. Değişikliklerinizi kaydedin.

Güvenilir web adreslerinin bir listesini Web Console ve Cloud Console'da dışa akarma ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **İletişim ve Web Koruması** → **Web Tehdidi Koruması** bölümüne gidin.
5. **Kurallar listesi** bloğundaki istisnaların listesini dışa aktarmak için:

a. Dışa aktarmak istediğiniz güvenilir web adreslerini seçin.

b. → **Dışa aktar** düğmesine tıklayın.

Kaspersky Endpoint Security, güvenilen adreslerin listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

6. **Kurallar listesi** bloğundaki istisnaların listesini içe aktarmak için:

a. → **İçe aktar** düğmesine tıklayın.

Açılan pencerede, Güvenilir internet adresleri listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir Güvenilir internet adresleri listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

7. Değişikliklerinizi kaydedin.

Posta Tehdidi Koruması

Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarının eklerinde virüsler ve diğer tehditler için tarama yapar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Posta Tehdidi Koruması hem gelen hem de giden mesajları tarayabilir. Uygulama, aşağıdaki posta istemcilerinde POP3, SMTP, IMAP ve NNTP'yi destekler:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail

- MyOffice Mail
- R7-Office Organizer

Mozilla Thunderbird, MyOffice Mail ve R7-Office Organizer posta istemcilerindeki trafiği taramak için Kaspersky sertifikasını sertifika deposuna eklemeniz ve kendi sertifika deposunu seçmeniz gerekir.

Posta Tehdidi Koruması, diğer protokolleri ve posta istemcilerini desteklemez.

Posta Tehdidi Koruması her zaman mesajlara *protokol düzeyinde* erişim sağlayamayabilir (örneğin, Microsoft Exchange çözümünü kullanırken). Bu nedenle Posta Tehdidi Koruması, Microsoft Office Outlook için uzantı içerir. Uzantı, mesajların *posta istemcisi düzeyinde* taranmasına izin verir. Posta Tehdidi Koruması eklentisi, Outlook 2010, 2013, 2016, 2019, 2021, 2024 ve 365'in 32 bit ve 64 bit sürümlerini destekler. Arm tabanlı bilgisayarlarda, Posta Tehdidi Koruması uzantısı Outlook 2016, Outlook 2021, Outlook 2024 ve Arm64 için Outlook 365'in 32 bit ve 64 bit sürümlerini destekler.

Posta Tehdidi Koruması bileşeni, posta istemcisi bir tarayıcıda açıldığında mesajları taramaz.

Bir ekte kötü amaçlı bir dosya algılandığında, Kaspersky Endpoint Security mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

Posta Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Posta Tehdidi Koruması bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Uygulama, Posta Tehdidi Koruması için farklı ayar grupları uygulayabilir. Uygulama içinde saklanan bu ayar gruplarına *güvenlik düzeyleri* denir: **Yüksek**, **Önerilen**, **Düşük**. **Önerilen** posta güvenlik düzeyi ayarları Kaspersky uzmanları tarafından tavsiye edilen en iyi ayarlar olarak değerlendirilir (aşağıdaki tabloya bakın). Önceden yüklenmiş e-posta güvenlik düzeylerinden birini seçebilir veya özel bir e-posta güvenlik düzeyi yapılandırabilirsiniz. E-posta güvenlik düzeyi ayarlarını değiştirmeniz durumunda önerilen e-posta güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

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

Yönetim Konsolu'nda (MMC) Posta Tehdidi Koruması bileşeni nasıl etkinleştirilir veya devre dışı bırakılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Posta Tehdidi Koruması**'nı seçin.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Posta Tehdidi Koruması** kutucuğunu işaretleyin.

5. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:

   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.

     - **Yüksek**. Bu e-posta güvenlik düzeyi seçildiğinde Posta Tehdidi Koruması bileşeni e-posta mesajlarını en kapsamlı şekilde tarar. Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarını tarar ve derin sezgisel analiz gerçekleştirir. Yüksek riskli ortamlar için Yüksek posta güvenlik düzeyi önerilir. Merkezi e-posta koruması tarafından korunmayan bir ev ağından bağlanılan ücretsiz bir e-posta hizmeti bağlantısı böyle bir ortama örnektir.

     - **Önerilen**. Uygulamanın performansı ve e-posta güvenliği arasında en iyi dengeyi sağlayan e-posta güvenlik düzeyidir. Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarını tarar ve orta düzeyde sezgisel analiz yapar. Bu e-posta trafiği güvenlik düzeyi Kaspersky uzmanları tarafından önerilmektedir. Önerilen güvenlik düzeyi için ayarların değerleri aşağıdaki tabloda verilmiştir.

     - **Düşük**. Bu e-posta güvenlik düzeyi seçildiğinde Posta Tehdidi Koruması bileşeni, yalnızca gelen e-posta mesajlarını tarar, hafif sezgisel analiz gerçekleştirir ve e-posta mesajlarına eklenen arşivleri taramaz. Bu e-posta güvenlik düzeyinde, Posta Tehdidi Koruması bileşeni e-posta mesajlarını maksimum hızla tarar ve işletim sistemi kaynaklarını minimum seviyede kullanır. Düşük e-posta güvenlik düzeyinin, iyi korunmuş bir ortamda kullanılması önerilir. Bu tip bir çevreye örnek olarak merkezi e-posta güvenliği içeren bir kurumsal LAN gösterilebilir.

   - Özel bir güvenlik düzeyi yapılandırmak istiyorsanız **Ayarlar** düğmesine tıklayın ve kendi bileşen ayarlarınızı tanımlayın (aşağıdaki tabloya bakın).

     Varsayılan olarak düğmesine tıklayarak önceden ayarlanmış güvenlik düzeylerinin değerlerini geri yükleyebilirsiniz.

6. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı nesneler üzerinde gerçekleştireceği eylemi seçin:

   - **Temizle; temizleme başarısız olursa sil**. Gelen veya giden bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse uygulama virüslü nesneyi siler. Uygulama, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

   - **Temizle; temizleme başarısız olursa engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

   - **Engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da Posta Tehdidi Koruması bileşenini etkinleştirme veya devre dışı bırakma

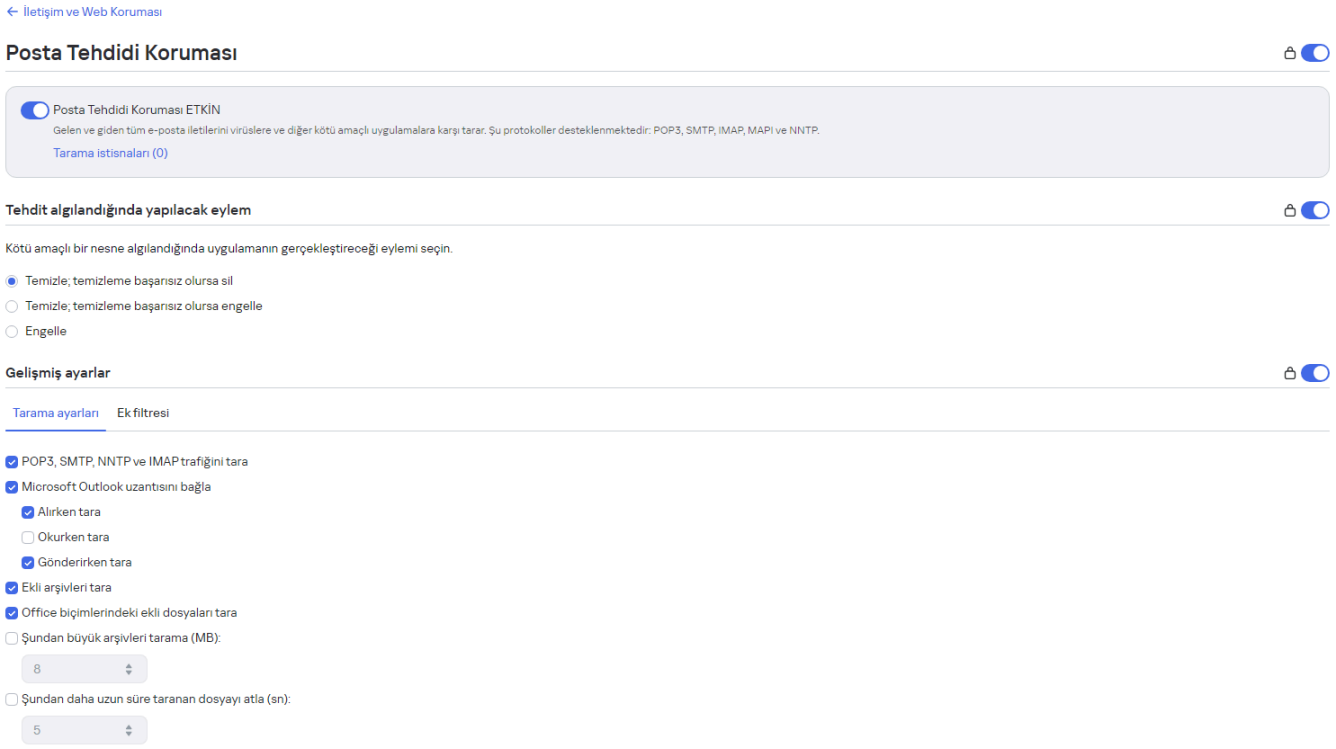
1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Posta Tehdidi Koruması** bölümüne gidin.



Posta Tehdidi Koruması ayarları

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Posta Tehdidi Koruması ETKİN** geçiş düğmesini kullanın.

6. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı nesneler üzerinde gerçekleştireceği eylemi seçin:

   - **Temizle; temizleme başarısız olursa sil**. Gelen veya giden bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse uygulama virüslü nesneyi siler. Uygulama, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

   - **Temizle; temizleme başarısız olursa engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

   - **Engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

7. Gerekirse, Posta Tehdidi Koruması için gelişmiş ayarları düzenleyin.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Posta Tehdidi Koruması bileşenini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Posta Tehdidi Koruması**'nı seçin.

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Posta Tehdidi Koruması** geçiş düğmesini kullanın.

4. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:

   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.

     - **Yüksek**. Bu e-posta güvenlik düzeyi seçildiğinde Posta Tehdidi Koruması bileşeni e-posta mesajlarını en kapsamlı şekilde tarar. Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarını tarar ve derin sezgisel analiz gerçekleştirir. Yüksek riskli ortamlar için Yüksek posta güvenlik düzeyi önerilir. Merkezi e-posta koruması tarafından korunmayan bir ev ağından bağlanılan ücretsiz bir e-posta hizmeti bağlantısı böyle bir ortama örnektir.

     - **Önerilen**. Uygulamanın performansı ve e-posta güvenliği arasında en iyi dengeyi sağlayan e-posta güvenlik düzeyidir. Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarını tarar ve orta düzeyde sezgisel analiz yapar. Bu e-posta trafiği güvenlik düzeyi Kaspersky uzmanları tarafından önerilmektedir. Önerilen güvenlik düzeyi için ayarların değerleri aşağıdaki tabloda verilmiştir.

     - **Düşük**. Bu e-posta güvenlik düzeyi seçildiğinde Posta Tehdidi Koruması bileşeni, yalnızca gelen e-posta mesajlarını tarar, hafif sezgisel analiz gerçekleştirir ve e-posta mesajlarına eklenen arşivleri taramaz. Bu e-posta güvenlik düzeyinde, Posta Tehdidi Koruması bileşeni e-posta mesajlarını maksimum hızla tarar ve işletim sistemi kaynaklarını minimum seviyede kullanır. Düşük e-posta güvenlik düzeyinin, iyi korunmuş bir ortamda kullanılması önerilir. Bu tip bir çevreye örnek olarak merkezi e-posta güvenliği içeren bir kurumsal LAN gösterilebilir.

   - Özel bir güvenlik düzeyi yapılandırmak istiyorsanız **Gelişmiş ayarlar** düğmesine tıklayın ve kendi bileşen ayarlarınızı tanımlayın (aşağıdaki tabloya bakın).

     Önerilen güvenlik düzeyini geri yükle düğmesine tıklayarak önceden ayarlanmış güvenlik seviyelerinin değerlerini geri yükleyebilirsiniz.

5. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin kötü amaçlı nesneler üzerinde gerçekleştireceği eylemi seçin:

   - **Temizle; temizleme başarısız olursa sil**. Gelen veya giden bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse uygulama virüslü nesneyi siler. Uygulama, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

   - **Temizle; temizleme başarısız olursa engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

   - **Engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

6. Değişikliklerinizi kaydedin.

Kaspersky uzmanları tarafından önerilen Posta Tehdidi Koruması ayarları (önerilen güvenlik düzeyi)

Parametre	Değer	Açıklama
Koruma kapsamı	**Gelen ve giden mesajlar**	*Koruma kapsamı*, bileşenin çalıştırıldığında denetlediği nesneleri içerir: gelen ve giden mesajlar veya sadece gelen mesajlar. Bilgisayarlarınızı korumak için yalnızca gelen mesajları taramanız gerekir. Etkilenen dosyaların arşivlere gönderilmesini önlemek için giden mesajların taranmasını açabilirsiniz. Ses ve video dosyaları gibi belirli biçimlerde dosyaların gönderilmesini önlemek istiyorsanız, giden mesajların taranmasını da açabilirsiniz.
Microsoft Outlook uzantısını bağla	**Açık**	Bu onay kutusu işaretlenirse POP3, SMTP, NNTP, IMAP iletişim kuralları yoluyla iletilen e-posta mesajlarının taranması, Microsoft Outlook'a entegre uzantıda etkinleştirilir. Posta Microsoft Outlook uzantısı kullanılarak taranıyorsa, Cached Exchange Mode kullanılması önerilir. Önbelleklenmiş Exchange modu ve nasıl kullanıldığıyla ilgili öneriler hakkında daha ayrıntılı bilgi için Microsoft Bilgi Bankası 'na bakın.
Ekli arşivleri tara	**Açık**	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Microsoft Office biçimlerindeki ekli dosyaları tara	**Açık**	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.
Ek filtresi	**Seçili türlerdeki ekleri yeniden adlandır**	Bu seçenek seçilmişse, Posta Tehdidi Koruması bileşeni, belirtilen türdeki ekli dosyalarda bulunan son uzantı karakterini alt çizgi karakteriyle değiştirir (örneğin attachment.doc_). Bu nedenle, dosyayı açmak için kullanıcının dosyayı yeniden adlandırması gerekir.
Sezgisel analiz	**Normal tarama**	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. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
Tehdit algılandığında yapılacak eylem	**Temizle; temizleme başarısız olursa sil**	Gelen veya giden bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse uygulama virüslü nesneyi siler. Uygulama, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

Virüslü e-posta mesajlarına uygulanacak eylemi değiştirme

Varsayılan olarak, Posta Tehdidi Koruması bileşeni, tespit edilen tüm virüslü e-posta mesajlarını otomatik olarak temizleme girişiminde bulunur. Temizleme başarısız olursa Posta Tehdidi Koruması bileşeni virüslü e-posta mesajlarını siler.

Virüslü e-posta mesajlarına uygulanacak eylemin değiştirilmesi için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Posta Tehdidi Koruması**'nı seçin.

3. **Tehdit algılandığında yapılacak eylem** bloğunda Kaspersky Endpoint Security'nin virüslü bir mesajı tespit ettiğinde gerçekleştireceği eylemi seçin:

   - **Temizle; temizleme başarısız olursa sil**. Gelen veya giden bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse uygulama virüslü nesneyi siler. Uygulama, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

   - **Temizle; temizleme başarısız olursa engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

   - **Engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.

4. Değişikliklerinizi kaydedin.

Posta Tehdidi Koruması bileşeninin koruma kapsamını oluşturma

Koruma kapsamı, etkinken bileşen tarafından taranan nesneleri ifade eder. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir. Posta Tehdidi Koruması bileşeninin koruma kapsamının özellikleri, e-posta istemcilerine Posta Tehdidi Koruması bileşeninin entegrasyonu için ayarları ve trafiği Posta Tehdidi Koruması bileşeni tarafından taranan e-posta mesajlarının ve e-posta iletişim kurallarının 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 Tehdidi Koruması bileşeninin koruma kapsamını oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Posta Tehdidi Koruması**'nı seçin.

3. **Gelişmiş ayarlar**'a tıklayın.

4. **Koruma kapsamı** bloğunda, taranacak mesajları seçin:

   - **Gelen ve giden mesajlar**.

   - **Sadece gelen mesajlar**.

   Bilgisayarlarınızı korumak için yalnızca gelen mesajları taramanız gerekir. Etkilenen dosyaların arşivlere gönderilmesini önlemek için giden mesajların taranmasını açabilirsiniz. Ses ve video dosyaları gibi belirli biçimlerde dosyaların gönderilmesini önlemek istiyorsanız, giden mesajların taranmasını da açabilirsiniz.

   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.

5. **Bağlanabilirlik** bloğunda aşağıdakilerden birini yapın:

   - Posta Tehdidi Koruması bileşeninin POP3, SMTP, NNTP ve IMAP iletişim kuralları üzerinden aktarılan mesajları kullanıcının bilgisayarı tarafından alınmadan taramasını istiyorsanız **POP3, SMTP, NNTP ve IMAP trafiğini tara** onay kutusunu işaretleyin.

     Posta Tehdidi Koruması bileşeninin POP3, SMTP, NNTP ve IMAP iletişim kuralları üzerinden aktarılan mesajları kullanıcının bilgisayarına ulaşmadan taramasını istemiyorsanız **POP3, SMTP, NNTP ve IMAP trafiğini tara** onay kutusunun işaretini kaldırın. Bu durumda **Microsoft Outlook uzantısını bağla** onay kutusu işaretlenirse mesajlar kullanıcı bilgisayarına ulaştıktan sonra Microsoft Office Outlook e-posta istemcisine yerleşik olan Posta Tehdidi Koruması uzantısı tarafından taranır.

     > Microsoft Office Outlook dışında bir posta istemcisi kullanıyorsanız, **POP3, SMTP, NNTP ve IMAP trafiğini tara** onay kutusunun işareti kaldırıldığında Posta Tehdidi Koruması bileşeni, POP3, SMTP, NNTP ve IMAP protokolleri aracılığıyla iletilen iletileri taramaz.

   - Microsoft Office Outlook'tan Posta Tehdidi Koruması bileşeni ayarlarına erişime izin vermek ve Microsoft Office Outlook'ta yerleşik eklentiyi kullanarak POP3, SMTP, NNTP, IMAP ve MAPI iletişim kuralları üzerinden aktarılan mesajların bilgisayara ulaştıktan sonra taranmasını etkinleştirmek istiyorsanız **Microsoft Outlook uzantısını bağla** onay kutusunu işaretleyin.

     Microsoft Office Outlook'tan Posta Tehdidi Koruması bileşeni ayarlarına erişimi engellemek ve Microsoft Office Outlook'a yerleşik eklentiyi kullanarak POP3, SMTP, NNTP, IMAP ve MAPI iletişim kuralları üzerinden aktarılan mesajların bilgisayara ulaştıktan sonra taranmasını devre dışı bırakmak istiyorsanız **Microsoft Outlook uzantısını bağla** onay kutusunun işaretini kaldırın.

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

6. Değişikliklerinizi kaydedin.

E-posta mesajlarına eklenen birleşik dosyaları tarama

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

E-posta mesajlarına eklenen bileşik dosyaların taranmasını yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Posta Tehdidi Koruması**'nı seçin.
3. **Gelişmiş ayarlar**'a tıklayın.

4. **Birleşik dosyaları tara** bloğunda tarama ayarlarını yapılandırın:

   - **Microsoft Office biçimlerindeki ekli dosyaları tara**. Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.

   - **Ekli arşivleri tara**. ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.

     Tarama sırasında uygulama mesaj metninde bir arşiv parolası tespit ederse, bu parola arşivin içeriğini kötü amaçlı uygulamalara karşı taramak için kullanılır. Bu durumda şifre kaydedilmez. Bir arşiv tarama sırasında açılır. Çıkarma işlemi sırasında bir uygulama hatası oluşursa, şu yola kaydedilen paketten çıkarılmış dosyaları manuel olarak silebilirsiniz: %systemroot%\temp. Dosyalarda PR öneki bulunur.

   - **Şundan büyük arşivleri tarama: N MB (1 - 9999 arası)**. Bu onay kutusu işaretlenirse Posta Tehdidi Koruması bileşeni, boyutları belirtilen değeri aşarsa e-posta mesajlarına eklenen arşivleri tarama kapsamının dışında tutar. Onay kutusunun işareti kaldırılırsa Posta Tehdidi Koruması bileşeni, herhangi bir boyuttaki e-posta eki arşivlerini tarar.

   - **Arşivleri kontrol süresini şununla sınırla: N sn (1 - 9999 arası)**. Onay kutusu işaretlenirse e-posta mesajlarına ekli arşivleri taramak için ayrılan süre belirtilen süreyle sınırlandırılır.

5. Değişikliklerinizi kaydedin.

E-posta mesajları ek filtrelemesi

Ek filtresi, giden e-posta mesajlarına uygulanmaz.

Zararlı uygulamalar, 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 bir zararlı uygulamanın otomatik olarak çalıştırılmasına karşı koruyabilir.

Eklerin filtrelenmesini yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Posta Tehdidi Koruması**'nı seçin.

3. **Gelişmiş ayarlar**'a tıklayın.

4. **Ek filtresi** bloğunda aşağıdakilerden birini yapın:

   - **Filtrelemeyi devre dışı bırak**. Bu seçenek tercih edilirse Posta Tehdidi Koruması bileşeni e-posta mesajlarına eklenen dosyaları filtrelemez.

   - **Seçili türlerdeki ekleri yeniden adlandır**. Bu seçenek seçilmişse, Posta Tehdidi Koruması bileşeni, belirtilen türdeki ekli dosyalarda bulunan son uzantı karakterini alt çizgi karakteriyle değiştirir (örneğin attachment.doc_). Bu nedenle, dosyayı açmak için kullanıcının dosyayı yeniden adlandırması gerekir.

   - **Seçili türlerdeki ekleri sil**. Bu seçenek tercih edilirse Posta Tehdidi Koruması bileşeni, belirtilen türlerin ekli dosyalarını e-posta mesajlarından siler.

5. Önceki adımda **Seçili türlerdeki ekleri yeniden adlandır** seçeneğini veya **Seçili türlerdeki ekleri sil** seçeneğini belirlerseniz ilgili dosya türlerinin karşısındaki onay kutusunu işaretleyin.

6. Değişikliklerinizi kaydedin.

Ek filtreleme için uzantıları dışa ve içe aktarma

Ek filtre uzantılarının listesini bir XML dosyasına aktarabilirsiniz. Uzantı listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) bir ek filtre uzantıları listesini dışa veya içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Posta Tehdidi Koruması** bölümüne gidin.

5. **Ek filtresi** bloğundaki uzantıların listesini dışa aktarmak için:

   a. Dışa aktarmak istediğiniz uzantıları seçin.

   b. **Dışa aktar** bağlantısına tıklayın.

   c. Açılan pencerede, uygulama uzantıları listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, genişletmeler listesinin tamamını XML dosyasına aktarır.

6. **Ek filtresi** bloğundaki uzantıların listesini içe aktarmak için:

   a. **İçe aktar** bağlantısına tıklayın.

   b. Açılan pencerede, uzantılar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

c. Dosyayı aç.

Bilgisayar zaten bir uzantılar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

7. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması → Posta Tehdidi Koruması**'nı seçin.
4. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.
5. Bu işlem bir pencere açar; bu pencerede **Ek filtresi** sekmesini seçin.
6. Uzantılar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz uzantıları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
   b. **Dışa aktar** bağlantısına tıklayın.
   c. Açılan pencerede, uygulama uzantıları listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.

   Kaspersky Endpoint Security, genişletmeler listesinin tamamını XML dosyasına aktarır.
7. Uzantılar listesini içe aktarmak için:
   a. **İçe aktar** bağlantısına tıklayın.
   b. Açılan pencerede, uzantılar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.
   c. Dosyayı aç.

   Bilgisayar zaten bir uzantılar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.
8. Değişikliklerinizi kaydedin.

Microsoft Office Outlook'ta e-postaları tarama

Kaspersky Endpoint Security'nin yüklenmesi sırasında Posta Tehdidi Koruması eklentisi, Microsoft Office Outlook'a eklenir (bundan sonra Outlook olarak ifade edilecektir). Uzantı, mesajların protokol düzeyi yerine posta istemcisi düzeyinde taranmasına olanak tanır. Mesajlara ek olarak, uzantı Microsoft Exchange depolarından MAPI arabirimi aracılığıyla alınan nesneleri (örneğin, Takvimdeki nesneleri) taramanızı sağlar. Bu tarama posta istemcisinde gerçekleşir.

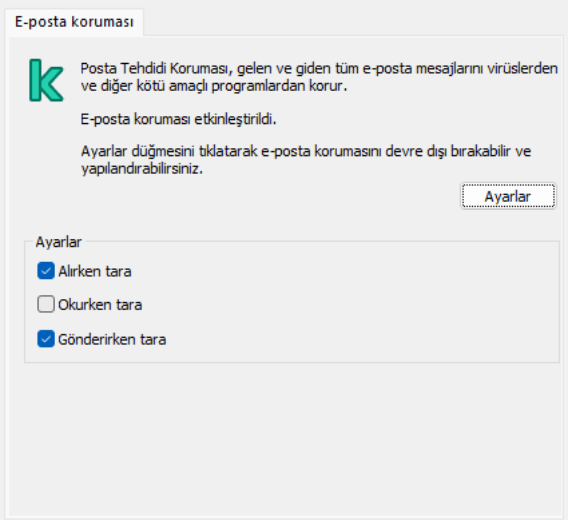
Outlook'tan Posta Tehdit Koruması bileşeni ayarlarını açabilir ve e-posta iletilerinin virüslere ve diğer tehditlere karşı ne zaman taranacağını belirleyebilirsiniz.

Posta Tehdidi Koruması eklentisi, Outlook 2010, 2013, 2016, 2019, 2021, 2024 ve 365'in 32 bit ve 64 bit sürümlerini destekler.

Arm tabanlı bilgisayarlarda, Posta Tehdidi Koruması uzantısı Outlook 2016, Outlook 2021, Outlook 2024 ve Arm64 için Outlook 365'in 32 bit ve 64 bit sürümlerini destekler.

Outlook'ta gelen mesajlar öncelikle Posta Tehdidi Koruması bileşeni tarafından (Kaspersky Endpoint Security'nin arabiriminde POP3, SMTP, NNTP ve IMAP trafiğini tara onay kutusu işaretlendiyse) ve ardından Outlook'un Posta Tehdidi Koruması eklentisi tarafından taranır. Posta Tehdidi Koruması bileşeni bir mesajda zararlı nesne tespit ederse size bu olayı bildirir.

Posta Tehdidi Koruması bileşeninin ayaları, Kaspersky Endpoint Security'nin arabiriminde Microsoft Office Outlook uzantısı bağlı ise doğrudan yapılandırılabilir (aşağıdaki resme bakın)..



Outlook'ta Posta Tehdit Koruması bileşeni ayarları

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

Outlook için Posta Tehdidi Koruması uzantısıyla e-posta tararken Exchange Server Önbellekli Modu'nu (Use Cached Exchange Mode) kullanmanızı öneririz. Önbelleklenmiş Exchange modu ve nasıl kullanıldığıyla ilgili öneriler hakkında daha ayrıntılı bilgi için Microsoft Bilgi Bankası'na bakın.

Outlook için Posta Tehdidi Koruması uzantısının işletim modu Yönetim Konsolu'nda (MMC) nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Temel Tehdit Koruması** → **Posta Tehdidi Koruması**'nı seçin.
5. **Güvenlik düzeyi** bloğunda, **Ayarlar** düğmesine tıklayın.

6. Açılan penceredeki **Bağlantı** bloğunda **Microsoft Outlook uzantısını bağla** onay kutusunu seçin.

7. **Ayarlar**'a tıklayın.

8. **E-posta koruması** penceresinde aşağıdakilerden birini yapın:

   - Outlook için Posta Tehdit Koruması uzantısının gelen iletileri posta kutusuna ulaştıklarında taramasını istiyorsanız **Alırken tara** onay kutusunu seçin.
   - Outlook için Posta Tehdit Koruması uzantısının gelen iletileri kullanıcı bunları açtığında taramasını istiyorsanız, **Okurken tara** onay kutusunu seçin.
   - Outlook için Posta Tehdit Koruması uzantısının giden iletileri gönderilirken taramasını istiyorsanız, **Gönderirken tara** onay kutusunu seçin.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Outlook için Posta Tehdidi Koruması uzantısının işletim modu Web Console'da nasıl yapılandırılır

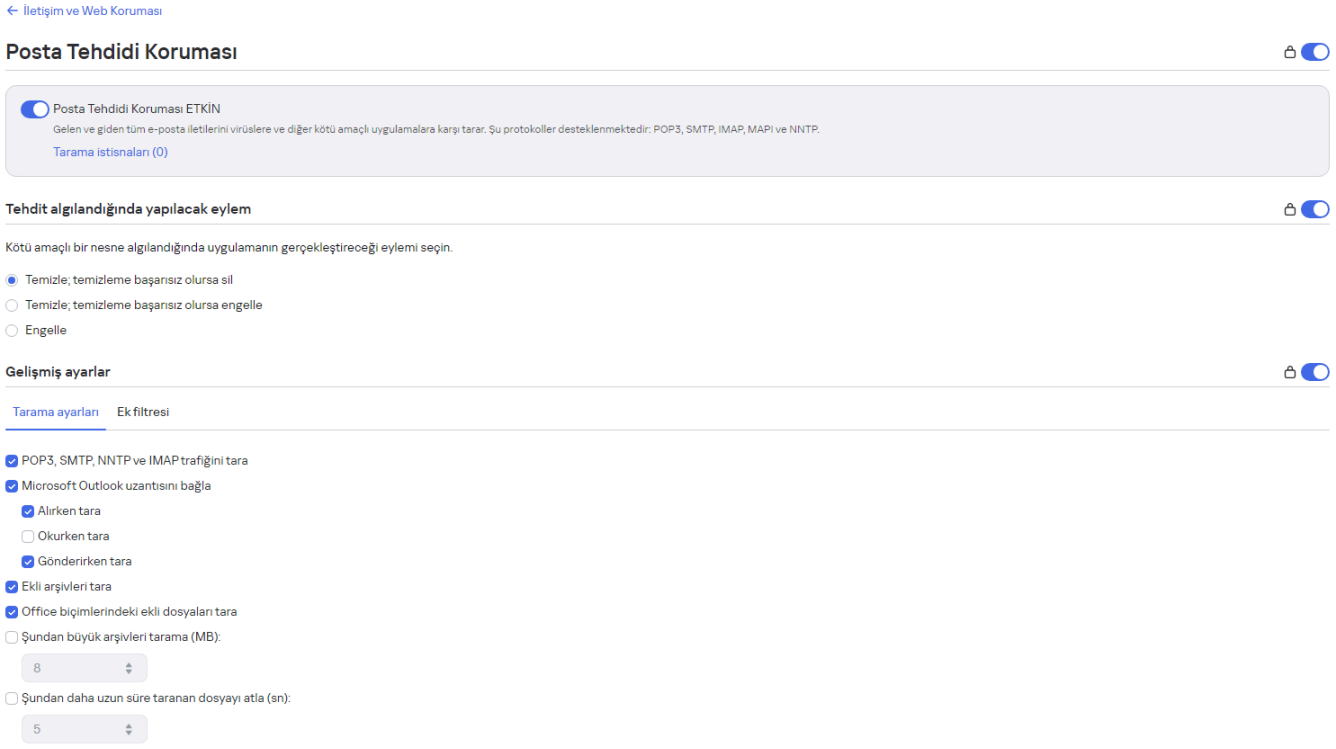
1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Posta Tehdidi Koruması** bölümüne gidin.



Posta Tehdidi Koruması ayarları

5. **Gelişmiş ayarlar** bölümünde **Tarama ayarları** sekmesini seçin.

6. **Microsoft Outlook uzantısını bağla** onay kutusunu seçin.

7. Uzantının modunu yapılandırın:

   - Outlook için Posta Tehdit Koruması uzantısının gelen iletileri posta kutusuna ulaştıklarında taramasını istiyorsanız **Alırken tara** onay kutusunu seçin.
   - Outlook için Posta Tehdit Koruması uzantısının gelen iletileri kullanıcı bunları açtığında taramasını istiyorsanız, **Okurken tara** onay kutusunu seçin.
   - Outlook için Posta Tehdit Koruması uzantısının giden iletileri gönderilirken taramasını istiyorsanız, **Gönderirken tara** onay kutusunu seçin.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Thunderbird, MyOffice ve R7-Office'te e-postalarını tarama

Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarının eklerinde virüsler ve diğer tehditler için tarama yapar. Mozilla Thunderbird, MyOffice Mail ve R7-Office Organizer posta istemcileri için, uygulama iletilere yalnızca *iletişim kuralı düzeyinde* (POP3, SMTP, IMAP, NNTP) erişim kazanır.

Mozilla Thunderbird, MyOffice Mail ve R7-Office Organizer posta istemcilerindeki trafiği taramak için Kaspersky sertifikasını sertifika deposuna eklemeniz ve kendi sertifika deposunu seçmeniz gerekir.

Posta Tehdidi Koruması bileşeni, posta istemcisi bir tarayıcıda açıldığında mesajları taramaz.

Gerçek Zamanlı E-posta Tehdit Koruması

Posta Tehdidi Koruması hem gelen hem de giden mesajları tarayabilir. Varsayılan olarak, Posta Tehdidi Koruması bileşeni, tespit edilen tüm virüslü e-posta mesajlarını otomatik olarak temizleme girişiminde bulunur. Temizleme başarısız olursa Posta Tehdidi Koruması bileşeni virüslü e-posta mesajlarını siler. Bir ekte kötü amaçlı bir dosya algılandığında, Kaspersky Endpoint Security mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

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

E-posta veritabanlarında kötü amaçlı yazılım taraması

Posta Tehdidi Koruması, bilgisayara iletişim kuralları düzeyinde virüs bulaşmasını önler ancak bilgisayara Kaspersky Endpoint Security yüklenmeden önce virüs bulaşmışsa uygulama, *Kötü Amaçlı Yazılım Taraması* görevini kullanarak posta veritabanlarındaki tehdidi algılayabilir. Uygulama, görev ayarlarından bağımsız olarak posta veritabanlarındaki virüslü dosyaları temizleme etmez veya silmez. Bunun nedeni, Kaspersky Endpoint Security'nin Thunderbird, MyOffice ve P7-Office iletilerini Microsoft Office Outlook iletilerinde olduğu gibi bileşenlerine (üst bilgi, gövde ve ekler) ayırmamasıdır. Uygulama, etkin tehditler listesine yalnızca algılanan nesneler hakkında bilgi ekler.

Aktif tehditleri ortadan kaldırmak için:

1. Posta istemcisinin arabiriminde algılanan nesne ile mesajı manuel olarak bulun ve silin.

   Uygulama, aktif tehditler listesinde tespit edilen nesne hakkında bilgi görüntüler.

   Algılanan nesne kartı örneği:

!	**HEUR:Trojan.PDF.Phish.gen** Nesne: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Veritabanı sıkıştırma işlemini gerçekleştirin.

   Kullanıcı arabiriminde bir mesaj silindiğinde, posta istemcisi yalnızca bir silme işareti ekler. Posta istemcisi iletiyi ancak bir veritabanı sıkıştırmasından sonra gerçekten siler. Veritabanı sıkıştırma hakkında ayrıntılar için posta istemcinizin yardımına bakın (örneğin, Mozilla Thunderbird).

3. *Kötü Amaçlı Yazılım Taraması* görevini tekrar çalıştırın ve tehdidin artık mevcut olmadığından emin olun.

Virüslü dosyalar içeren iletilerin silinmesi herhangi bir nedenle o anda mümkün değilse bu tür tehditleri Kaspersky Endpoint Security kullanıcı arabiriminde işleyebilirsiniz. E-posta istemcisi dosyaları için bir tehdidi işlemeye yönelik iki seçeneğiniz vardır: **Yoksay** ve **İstisnalara ekle**. Uygulamanın yeniden tarama sırasında bu nesneleri etkin tehditler listesine eklemesini önlemek için bunları tarama istisnaları listesine ekleyin.

Ağ Tehdidi Koruması

Ağ Tehdidi Koruması bileşeni (Ayrıca Intrusion Detection System, IDS olarak da adlandırılır), ağ saldırılarının karakteristik aktiviteleri için gelen ağ trafiğini izler. Uygulama kullanıcının bilgisayarına gerçekleştirilen bir ağ saldırısı tespit ederse, saldıran bilgisayarla ağ bağlantısını engeller. Şu anda bilinen ağ saldırısı türlerinin açıklamaları ve bunlara karşı koyma yolları, uygulama veritabanlarında sunulmaktadır. Ağ Tehdidi Koruması bileşeninin tespit ettiği ağ saldırıları listesi, veritabanı ve uygulama modülü güncellemeleri sırasında güncellenir.

Ağ Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

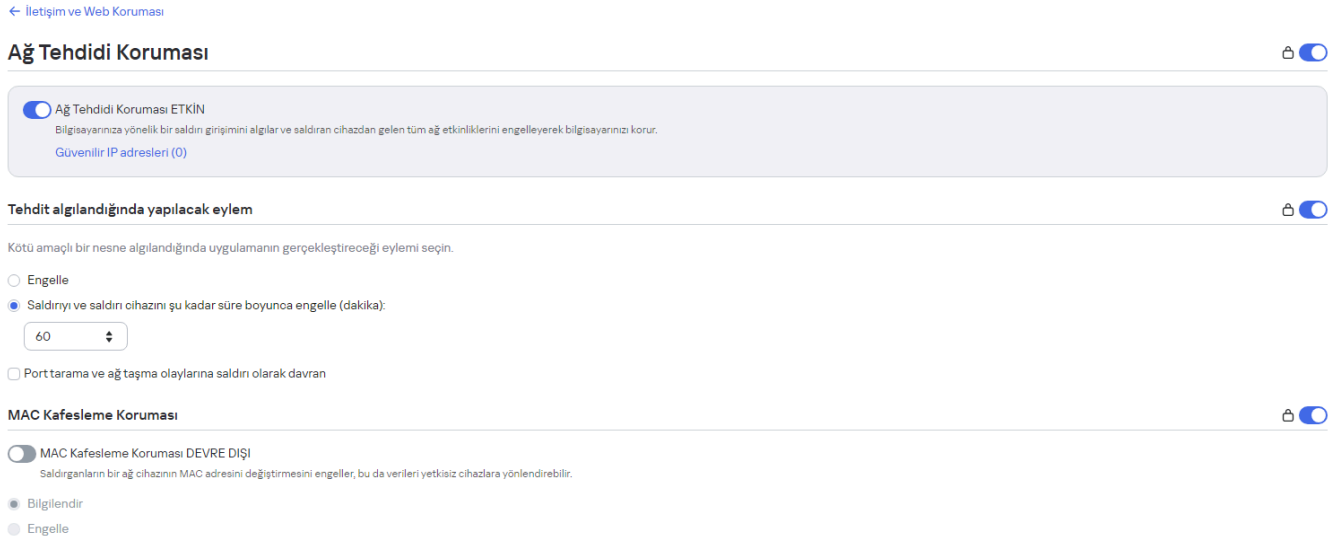
Varsayılan olarak Ağ Tehdidi Koruması etkinleştirilmiştir ve optimum modda çalışır. Kaspersky Endpoint Security, gelen ağ trafiğini ağ saldırılarına özgü etkinliklere karşı izler ve saldırıları engeller.

Yönetim Konsolu'nda (MMC) Ağ Tehdidi Korumasını etkinleştirmek veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Ağ Tehdidi Koruması** kutucuğunu işaretleyin.
5. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da Ağ Tehdidi Korumasını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **İletişim ve Web Koruması** → **Ağ Tehdidi Koruması** bölümüne gidin.

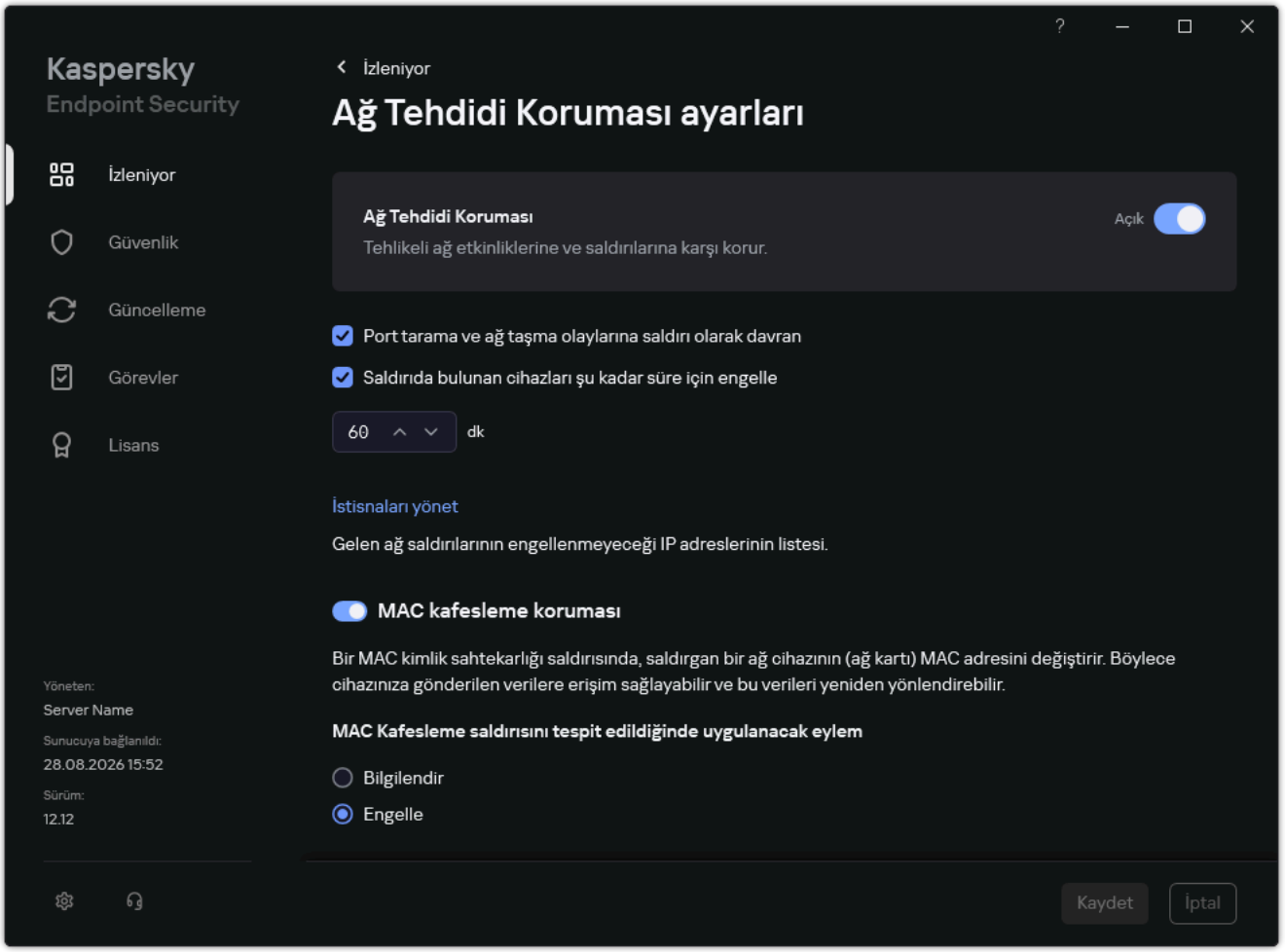


Ağ Tehdidi Koruması ayarları

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Ağ Tehdidi Koruması ETKİN** geçiş düğmesini kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Ağ Tehdidi Korumasını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.



Ağ Tehdidi Koruması ayarları

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Ağ Tehdidi Koruması** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Saldırıda bulunan bir bilgisayarı engellemek

Ağ Tehdit Koruması bileşeni etkinleştirilirse Kaspersky Endpoint Security ağ tehditlerini otomatik olarak engeller. Ayrıca, uygulama saldıran bilgisayarı engelleyebilir ve ağ paketlerinin gönderilmesini belirli bir süre için kısıtlayabilir. Varsayılan olarak, Kaspersky Endpoint Security bilgisayarı bir saat boyunca engeller.

Yönetim Konsolu'nda (MMC) saldıran bir bilgisayarı engelleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.

4. **Ağ Tehdidi Koruması ayarları** bölümünde, **Saldırıda bulunan cihazları şu kadar süre için engelle N dk** onay kutusunu seçin.

   Bu seçenek etkinleştirilirse, Ağ Tehdidi Koruması bileşeni saldıran bilgisayarı engellenenler listesine ekler. Bu, Ağ Tehdidi Koruması bileşeninin saldırgan bir bilgisayarın ağ bağlantısını, ilk ağ saldırısı denemesinden sonra belirli bir süre boyunca engellediği anlamına gelir. Bu engelleme aynı adresten gelecekteki olası ağ saldırılarına karşı kullanıcının bilgisayarını otomatik olarak korur. Saldıran bir bilgisayarın engelleme listesinde geçirmesi gereken minimum süre bir dakikadır. Maksimum süre 999 dakikadır.

5. **Saldırıda bulunan cihazları şu kadar süre için engelle N dk** onay kutusunun sağındaki alanda, saldırıda bulunan bir bilgisayar için farklı bir engelleme süresi belirleyin.

6. Değişikliklerinizi kaydedin.

Web Console'da saldıran bir bilgisayarı engelleme

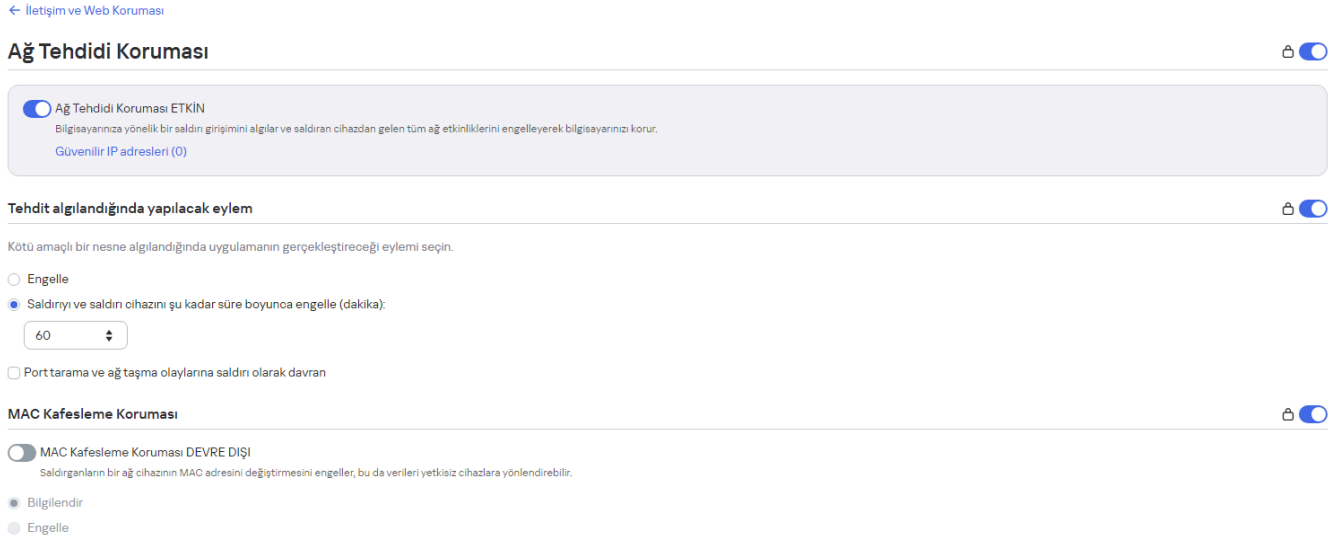
1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Ağ Tehdidi Koruması** bölümüne gidin.



Ağ Tehdidi Koruması ayarları

5. **Tehdit algılandığında yapılacak eylem** bloğunda, **Saldırıyı ve saldıran cihazı (dakika) boyunca engelle** onay kutusunu seçin.

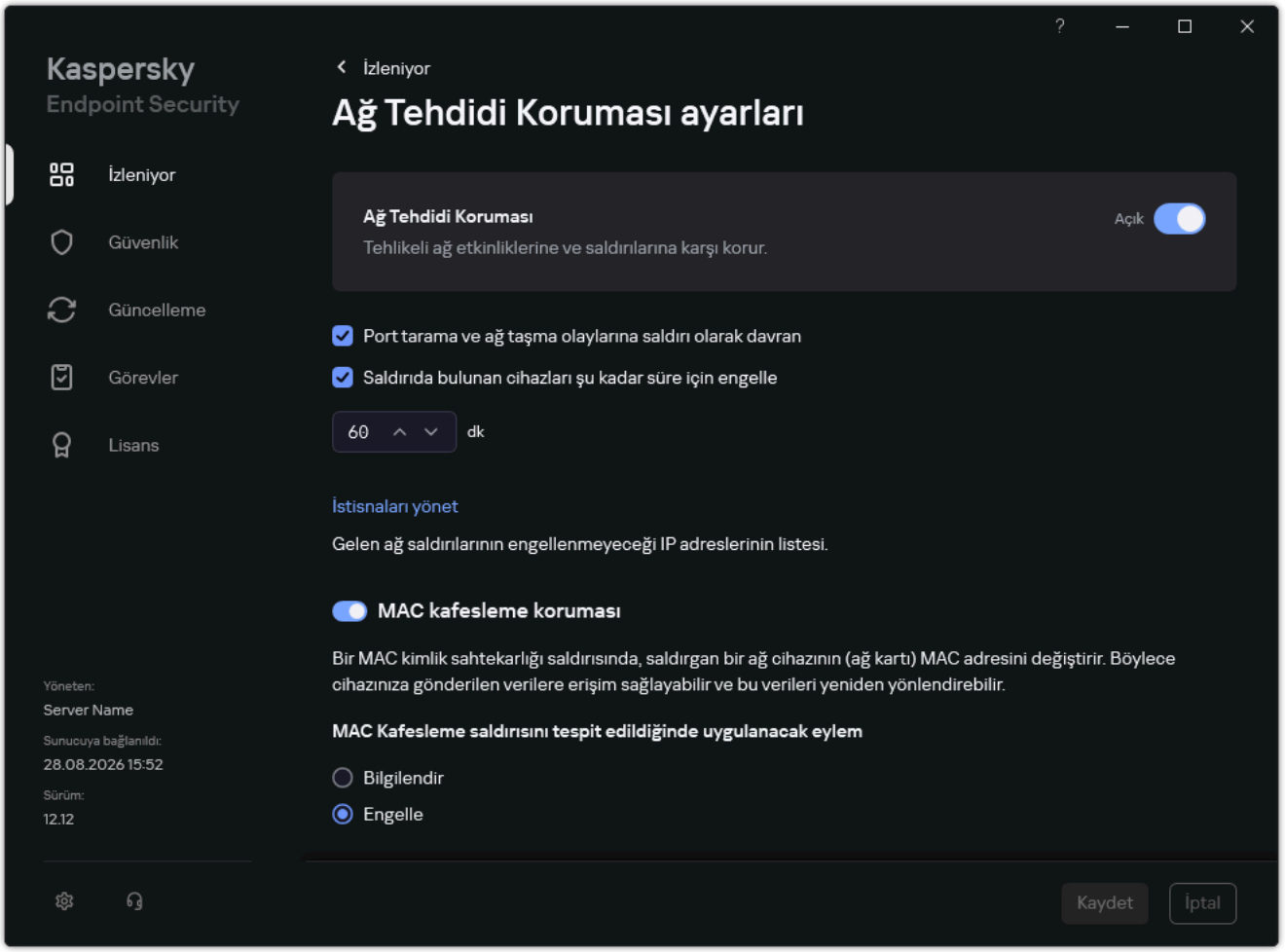
   Bu seçenek etkinleştirilirse, Ağ Tehdidi Koruması bileşeni saldıran bilgisayarı engellenenler listesine ekler. Bu, Ağ Tehdidi Koruması bileşeninin saldırgan bir bilgisayarın ağ bağlantısını, ilk ağ saldırısı denemesinden sonra belirli bir süre boyunca engellediği anlamına gelir. Bu engelleme aynı adresten gelecekteki olası ağ saldırılarına karşı kullanıcının bilgisayarını otomatik olarak korur. Saldıran bir bilgisayarın engelleme listesinde geçirmesi gereken minimum süre bir dakikadır. Maksimum süre 999 dakikadır.

6. Saldıran bilgisayarın engelleme süresini değiştirin.

7. Değişikliklerinizi kaydedin.

Uygulamanın kullanıcı arabiriminde saldırıda bulunan bir bilgisayarı engelleme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.



Ağ Tehdidi Koruması ayarları

3. **Saldırıda bulunan cihazları şu kadar süre için engelle N dk** düğmesini açık duruma getirin.

   Bu seçenek etkinleştirilirse, Ağ Tehdidi Koruması bileşeni saldıran bilgisayarı engellenenler listesine ekler. Bu, Ağ Tehdidi Koruması bileşeninin saldırgan bir bilgisayarın ağ bağlantısını, ilk ağ saldırısı denemesinden sonra belirli bir süre boyunca engellediği anlamına gelir. Bu engelleme aynı adresten gelecekteki olası ağ saldırılarına karşı kullanıcının bilgisayarını otomatik olarak korur. Saldıran bir bilgisayarın engelleme listesinde geçirmesi gereken minimum süre bir dakikadır. Maksimum süre 999 dakikadır.

4. **Saldırıda bulunan cihazları şu kadar süre için engelle N dk** düğmesinin altındaki alanda saldırıda bulunan bir bilgisayar için farklı bir engelleme süresi belirleyin.

5. Değişikliklerinizi kaydedin.

Sonuç olarak, Kaspersky Endpoint Security kullanıcının bilgisayarına gerçekleştirilen bir ağ saldırısı tespit ederse, saldıran bilgisayarla ağ bağlantısını engeller. Kaspersky Endpoint Security, *Ağ saldırısı tespit edildi* olayı oluşturur. Olay, saldıran bilgisayar hakkında bilgiler içerir: IP ve MAC adresleri.

Saldırıya uğrayan bilgisayarın MAC adresini uygulamanın kullanıcı arabiriminde veya Kaspersky Security Center konsolunun 15.1 veya sonraki sürümlerinde görüntüleyebilirsiniz.



Ağ saldırısı tespiti hakkında bildirim

Kaspersky Endpoint Security, belirtilen süre dolduğunda bilgisayarın engelini kaldırır. Kaspersky Security Center konsolu, rapordaki *Ağ saldırısı tespit edildi* olayları haricinde engellenen bilgisayarları izlemek için araçlar sağlamaz. Uygulamanın arabiriminde yalnızca engellenen bilgisayarların bir listesini görüntüleyebilirsiniz. Bu işlevsellik *Ağ İzleyicisi* aracı tarafından sağlanır. Bir bilgisayarın engellemesini kaldırmak için Ağ İzleyicisi aracını da kullanabilirsiniz.

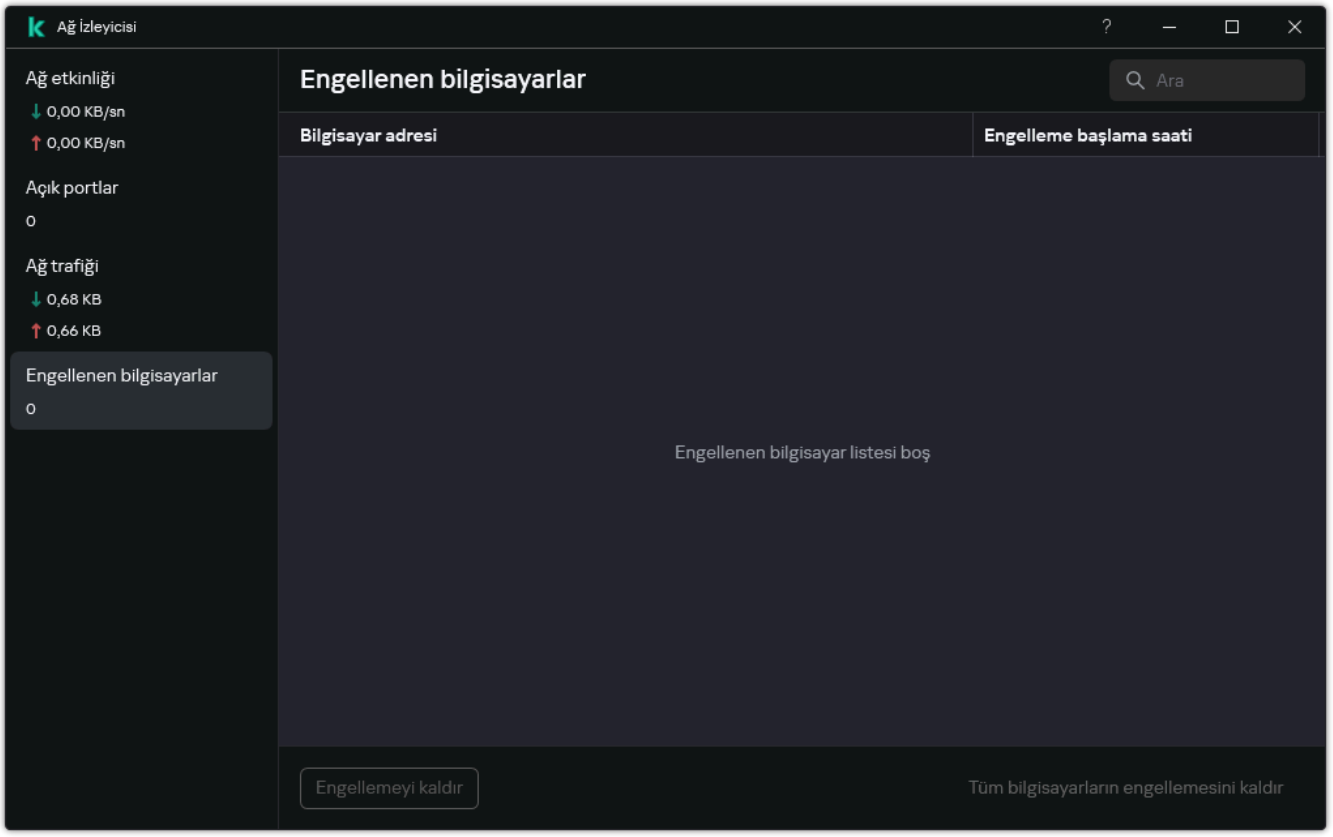
Bir bilgisayarın engellemesini kaldırmak için:

1. Ana uygulama penceresinin **İzleniyor** bölümünde, **Ağ İzleyicisi** kutucuğuna tıklayın.
2. **Engellenen bilgisayarlar** sekmesine gidin.

   Engellenen bilgisayarların bir listesi açılır (aşağıdaki resme bakın).

   Kaspersky Endpoint Security, uygulama yeniden başlatıldığında ve Ağ Tehdidi Koruması ayarları değiştirildiğinde engelleme listesini temizler.

3. Engellemesini kaldırmak istediğiniz bilgisayarı seçin ve **Engellemeyi kaldır**'a tıklayın.



Engellenen bilgisayarların listesi

Engelleme istisnalarının adreslerini yapılandırma

Kaspersky Endpoint Security, bir ağ saldırısını algılayabilir ve çok sayıda paket (örneğin, gözetim kameralarından) ileten güvenli olmayan bir ağ bağlantısını engelleyebilir. Güvenilir cihazlarla çalışmak için bu cihazların IP adreslerini istisnalar listesine ekleyebilirsiniz. Ayrıca iletişim için kullanılan protokolü ve bağlantı noktasını seçebilir ve belirli ağ etkinliklerine izin verebilirsiniz.

Yönetim Konsolu'nda (MMC) engellemenin dışında tutulan adresler nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.
5. **Ağ Tehdidi Koruması ayarları** bloğunda, **İstisnalar** düğmesini tıklayın.
6. Açılan pencerede **Ekle** düğmesine tıklayın.
7. Ağ saldırılarının engellenmemesi gereken bilgisayarın IP adresini girin.

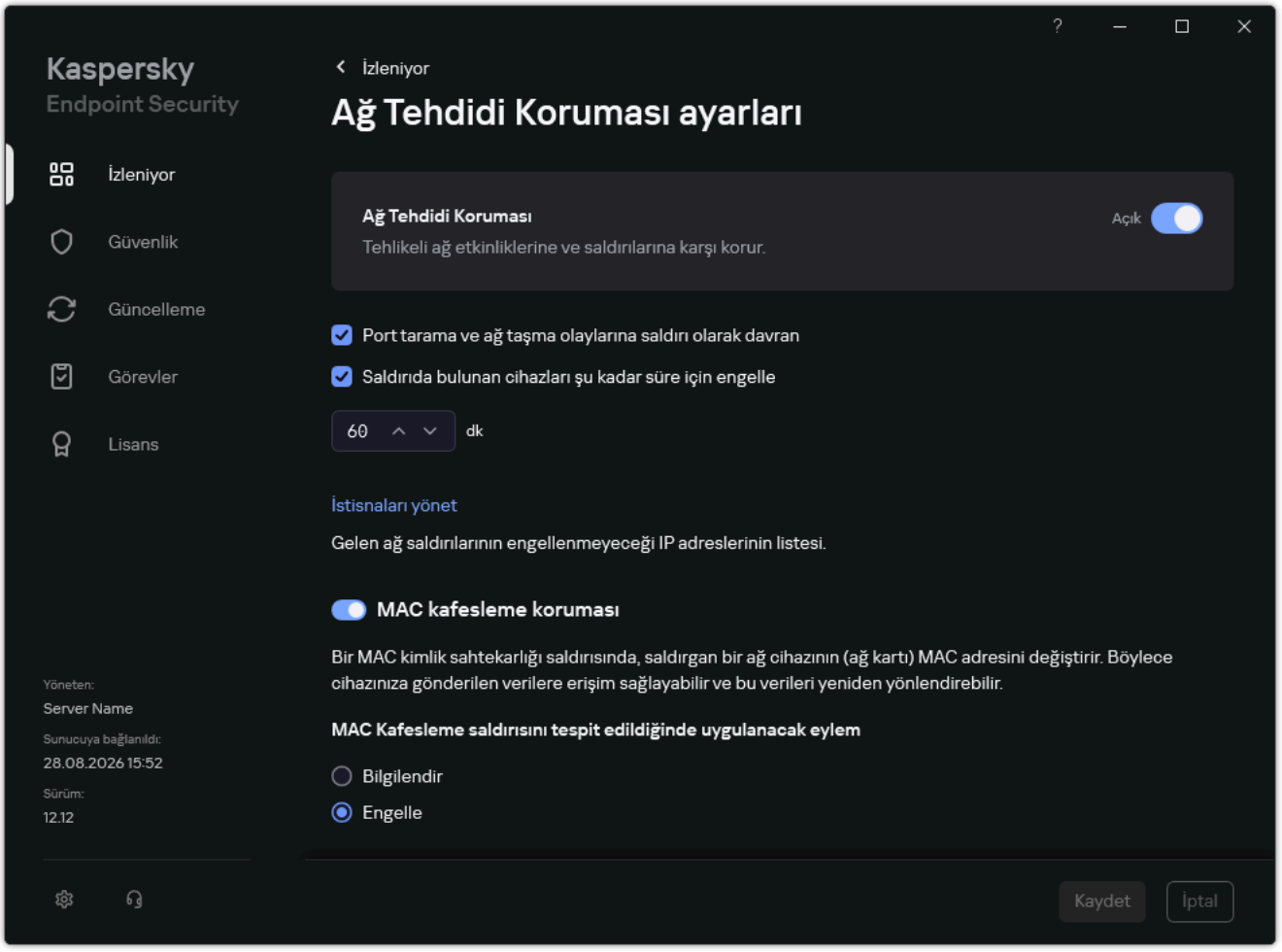
   Gerekirse, verilerin iletileceği protokolü ve portları seçin.
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da engelleme dışında bırakılan adresleri yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenilir Bölge** bölümüne gidin.
5. Açılan pencerede **IP adresleri** bağlantısına tıklayın.
   Güvenilen IP adreslerinin listesini içeren bir pencere açılır.
6. Açılan pencerede **Ekle** düğmesine tıklayın.
7. Ağ saldırılarının engellenmemesi gereken bilgisayarın IP adresini girin.
   Gerekirse alt ağı belirtin.
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulamanın kullanıcı arabiriminde engellemenin dışında tutulan adresleri yapılandırma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.



Ağ Tehdidi Koruması ayarları

3. **İstisnaları yönet** bağlantısını tıklayın.
4. Açılan pencerede **Ekle** düğmesine tıklayın.
5. Ağ saldırılarının engellenmemesi gereken bilgisayarın IP adresini girin.

   Gerekirse, verilerin iletileceği protokolü ve portları seçin.
6. Değişikliklerinizi kaydedin.

İstisnalar listesini dışa ve içe aktarma

Dışlama listesini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda adres eklemek için dosyayı değiştirebilirsiniz. İstisnalar listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

Yönetim Konsolunda (MMC) bir dışlama listesi nasıl içe ve dışa aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.
4. **Ağ Tehdidi Koruması ayarları** bloğunda, **İstisnalar** düğmesini tıklayın.
5. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

      Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.
   b. → **Dışa aktar** düğmesine tıklayın.
   c. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.
6. İstisnalar listesini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
   b. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.
   c. Dosyayı aç.

      Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.
7. Değişikliklerinizi kaydedin.

Kaspersky Security Center Web Console'da istisnalar listesini dışa ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **İletişim ve Web Koruması** → **Ağ Tehdidi Koruması** bölümüne gidin.
5. Pencerenin üst kısmında, **Güvenilir IP adresleri** bağlantısına tıklayın.
   İstisnalar listesi açılır.
6. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin.
   b. → **Dışa aktar** düğmesine tıklayın.
      Kaspersky Endpoint Security, istisnalar listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.
7. İstisnalar listesini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
      Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.
   b. Dosyayı aç.
      Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.
8. Değişikliklerinizi kaydedin.

Ağ Tehdit Korumasını türe göre yapılandırma

Kaspersky Endpoint Security, aşağıdaki ağ saldırısı türlerine karşı korumayı yönetmenizi sağlar:

- *Ağ Taşma*, bir kuruluşun ağ kaynaklarına (web sunucuları gibi) yapılan bir saldırıdır. Bu saldırıda, ağ kaynaklarının bant genişliğini aşırı yüklemek için çok sayıda istek gönderimi yapılır. Bu olduğunda, kullanıcılar kuruluşun ağ kaynaklarına erişim sağlayamaz.
- *Port Tarama* saldırısı, bilgisayardaki UDP portlarının, TCP portlarının ve ağ hizmetlerini taramaktan oluşur. Bu saldırı, saldırganın daha tehlikeli ağ saldırıları gerçekleştirmeden önce bilgisayarın güvenlik açığı düzeyini belirlemesine olanak tanır. Port Tarama sayesinde saldırgan aynı zamanda bilgisayardaki işletim sistemini tanımlayabilir ve bu işletim sistemi için uygun ağ saldırılarını seçebilir.
- *MAC kafesleme saldırısı*, bir ağ aygıtının (ağ kartı) MAC adresini değiştirmeye çalışır. Böylece saldırgan bir aygıta gönderilen verileri başka bir aygıta yönlendirerek bu verilere erişim sağlayabilir. Kaspersky Endpoint Security, MAC Aldatma saldırılarını engellemenizi ve bu saldırılar hakkında bildirimler almanızı sağlar.

İzin verilen uygulamalardan bazılarının bu tür saldırılar için tipik olan işlemleri gerçekleştirmesi durumunda, bu tür saldırıların algılanmasını devre dışı bırakabilirsiniz. Bu, yanlış alarmların önlenmesine yardımcı olacaktır.

Kaspersky Endpoint Security varsayılan olarak Ağ Taşma, Port Tarama ve MAC aldatma saldırılarını izlemez.

Bu saldırı türleri için ayrı istisnalar yapılandıramazsınız. Bu, ayrı IP adresleri güvenilir bölgeye eklense bile böyle bir saldırı algılandığında Kaspersky Endpoint Security'nin saldıran bilgisayarı engellediği anlamına gelir. Bu tür saldırıların algılanmasını etkinleştirebilir veya devre dışı bırakabilirsiniz.

Microsoft Hyper-V altyapısındaki sanal makinelerde MAC kafesleme korumasının etkinleştirilmesini önermiyoruz. Microsoft Hyper-V platformunun özellikleri nedeniyle Kaspersky Industrial CyberSecurity for Nodes, hatalı pozitif sonuçlar nedeniyle hipervizörü engelleyebilir.

Yönetim Konsolu'nda (MMC) türe göre Ağ Tehdidi Korumasını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.
4. Bu saldırıların algılanmasını etkinleştirmek veya devre dışı bırakmak için **Port tarama ve ağ taşma olaylarına saldırı olarak davran** onay kutusunu kullanın.

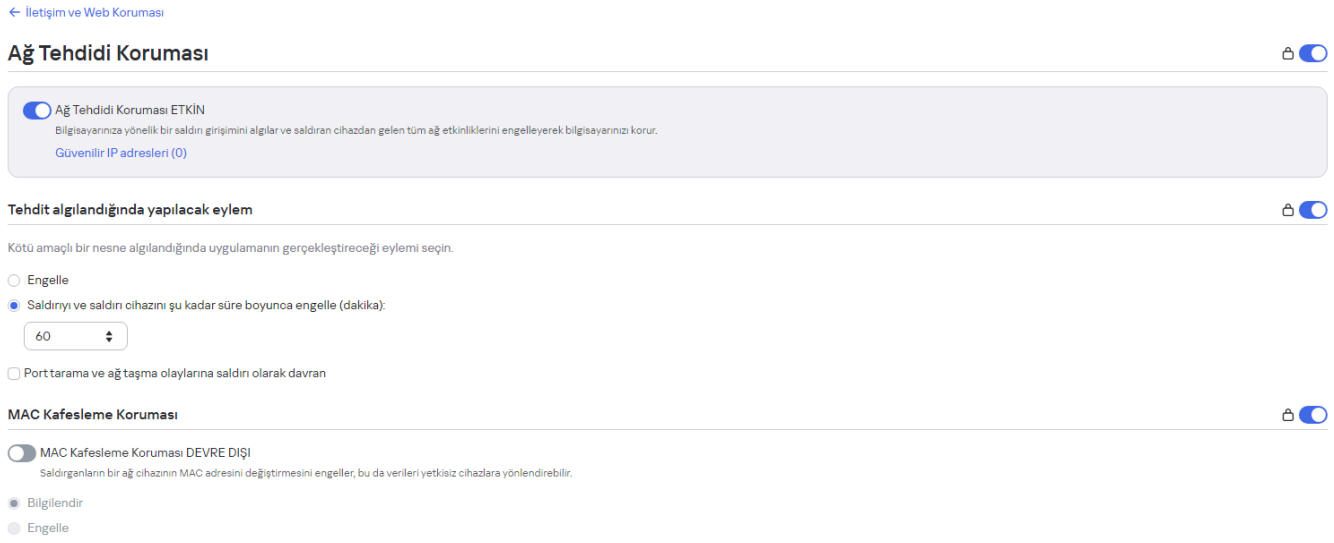
   Bu işlev etkinleştirilirse Kaspersky Endpoint Security, port taraması ve ağ taşma olayları için ağ trafiğini izler. Böyle bir davranış tespit edilirse, uygulama kullanıcıyı bilgilendirir ve ilgili olayı Kaspersky Security Center'a gönderir. Uygulama, istekleri yapan bilgisayar hakkında bilgi sağlar. Bu bilgi zamanında müdahale için gereklidir. Ancak, Kaspersky Endpoint Security istekleri yapan bilgisayarı engellemez çünkü bu tür trafik şirket ağında normal bir durum olabilir.
5. **MAC kafesleme koruması modu** bloğunda, aşağıdaki seçeneklerden birini seçin:
   - **MAC yanıltmalarını takip etme**
   - **Bilgilendir**.
   - **Engelle**.
6. Değişikliklerinizi kaydedin.

Web Console'da Ağ Tehdidi Korumasını türe göre yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Ağ Tehdidi Koruması** bölümüne gidin.



Ağ Tehdidi Koruması ayarları

5. Bu saldırıların algılanmasını etkinleştirmek veya devre dışı bırakmak için **Port tarama ve ağ taşma olaylarına saldırı olarak davran** onay kutusunu kullanın.

   Bu işlev etkinleştirilirse Kaspersky Endpoint Security, port taraması ve ağ taşma olayları için ağ trafiğini izler. Böyle bir davranış tespit edilirse, uygulama kullanıcıyı bilgilendirir ve ilgili olayı Kaspersky Security Center'a gönderir. Uygulama, istekleri yapan bilgisayar hakkında bilgi sağlar. Bu bilgi zamanında müdahale için gereklidir. Ancak, Kaspersky Endpoint Security istekleri yapan bilgisayarı engellemez çünkü bu tür trafik şirket ağında normal bir durum olabilir.

6. **MAC Kafesleme Koruması** altında, MAC Kafesleme saldırılarının algılanmasını yapılandırın:

   a. Bu saldırıların algılanmasını etkinleştirmek veya devre dışı bırakmak için **MAC Kafesleme Koruması ETKİN** geçiş anahtarını kullanın.

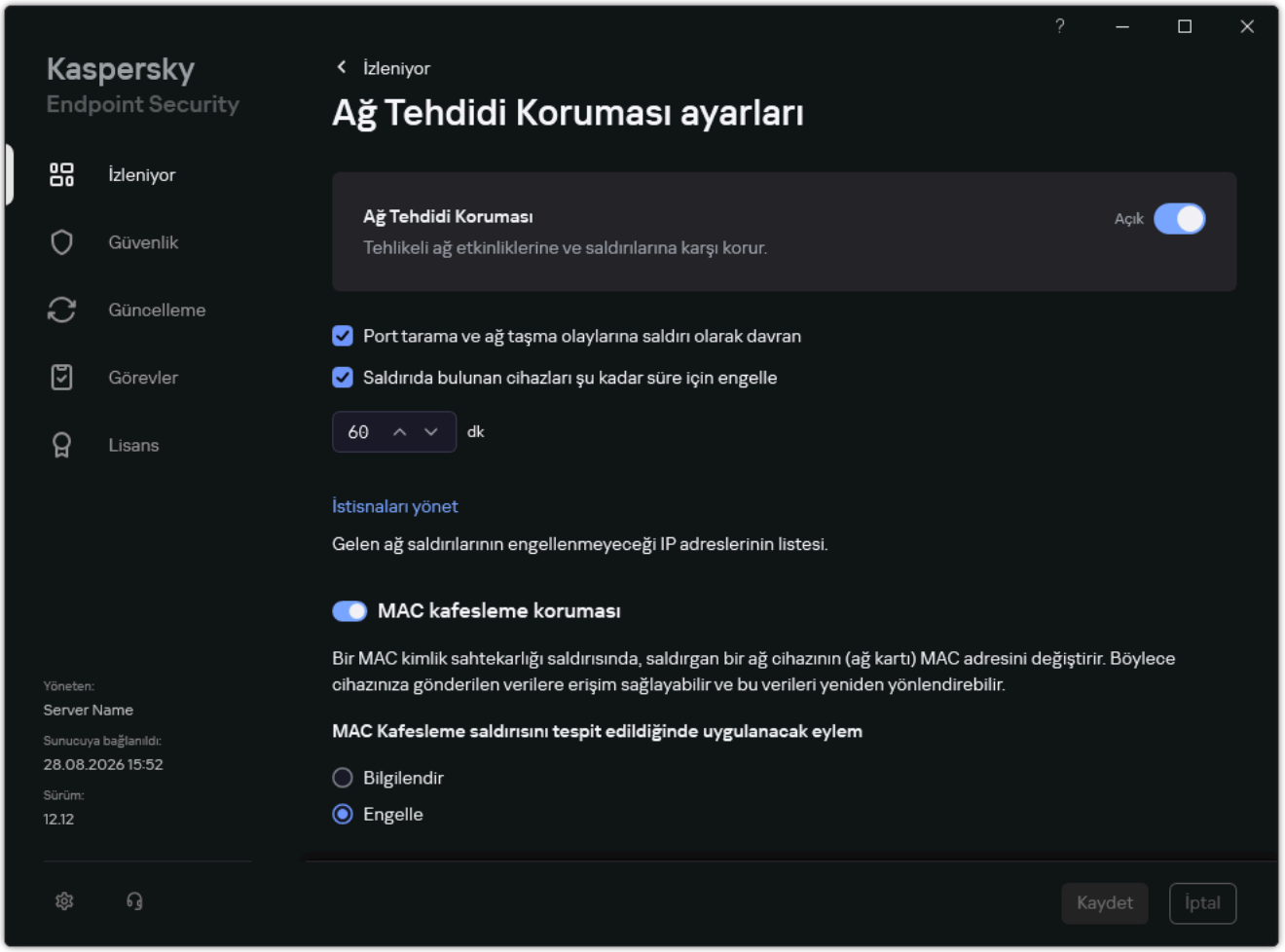
   b. Bir MAC Kafesleme saldırısı algılandığında gerçekleştirilecek eylemi seçin:

   - **Bilgilendir**.
   - **Engelle**.

7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde türe göre Ağ Tehdidi Korumasını yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.



Ağ Tehdidi Koruması ayarları

3. Bu saldırıların algılanmasını etkinleştirmek veya devre dışı bırakmak için **Port tarama ve ağ taşma olaylarına saldırı olarak davran** geçiş düğmesini kullanın.

   Bu işlev etkinleştirilirse Kaspersky Endpoint Security, port taraması ve ağ taşma olayları için ağ trafiğini izler. Böyle bir davranış tespit edilirse, uygulama kullanıcıyı bilgilendirir ve ilgili olayı Kaspersky Security Center'a gönderir. Uygulama, istekleri yapan bilgisayar hakkında bilgi sağlar. Bu bilgi zamanında müdahale için gereklidir. Ancak, Kaspersky Endpoint Security istekleri yapan bilgisayarı engellemez çünkü bu tür trafik şirket ağında normal bir durum olabilir.

4. Bu saldırıların algılanmasını etkinleştirmek veya devre dışı bırakmak için **MAC kafesleme koruması** düğmesini kullanın.

5. **MAC Kafesleme saldırısını tespit edildiğinde uygulanacak eylem** bloğunda, aşağıdaki seçeneklerden birini seçin:

   - **Bilgilendir**.
   - **Engelle**.

6. Değişikliklerinizi kaydedin.

Güvenlik Duvarı

Güvenlik Duvarı bileşeni, internet veya yerel ağ üzerinde çalışırken bir bilgisayara yetkisiz bağlantıları engeller. Güvenlik Duvarı aynı zamanda bilgisayardaki uygulamaların ağ etkinliklerini de denetler. Bu, kurumsal LAN'ınızı kimlik hırsızlığı ve diğer saldırılara karşı korumanızı sağlar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve önceden tanımlanmış *ağ kuralları* yardımıyla bilgisayar koruması sağlar.

Kaspersky Security Center ile etkileşim için Ağ Aracısı kullanılır. Güvenlik duvarı, uygulamanın ve Ağ Aracısının çalışması için gereken ağ kurallarını otomatik olarak oluşturur. Sonuç olarak, Güvenlik Duvarı bilgisayarda birkaç port açar. Hangi portların açılacağı bilgisayarın rolüne bağlıdır (örneğin, dağıtım noktası). Bilgisayarda açılacak portlar hakkında daha fazla bilgi edinmek için Kaspersky Security Center Yardım içeriğine bakın.

Ağ kuralları

Ağ kurallarını şu düzeylerde yapılandırabilirsiniz:

- *Ağ paketi kuralları*. Ağ paketi kuralları, uygulamaya bakılmaksızın ağ paketlerine sınırlamalar getirir. Bu kurallar, seçilen veri iletişim kuralının belirli portları yoluyla gelen ve giden ağ trafiğini sınırlar. Kaspersky Endpoint Security'nin, Kaspersky uzmanları tarafından önerilen izinlere sahip önceden tanımlanmış ağ paketi kuralları vardır.

- *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.

Uygulamaların işletim sistemi kaynaklarına, işlemlerine ve kişisel verilere kontrollü erişimi, Sunucu Yetkisiz Erişim Önleme bileşeni tarafından *uygulama hakları* kullanılarak sağlanır.

Uygulamanın ilk başlatılması sırasında, Güvenlik Duvarı şu eylemleri gerçekleştirir:

1. İndirilen anti virüs veritabanlarını kullanarak uygulamanın güvenliğini kontrol eder.

2. Kaspersky Security Network'teki uygulamanın güvenliğini denetler.

   Güvenlik Duvarının daha etkin çalışmasını sağlamak için Kaspersky Security Network'e katılmanız önerilir.

3. Uygulamayı güven gruplarından birine sokar: *Güvenilir*, *Düşük Kısıtlamalı*, *Yüksek Kısıtlamalı*, *Güvenilmez*.

   Güvenilirlik grubu, Kaspersky Endpoint Security'nin uygulama etkinliğini denetlerken uyguladığı hakları tanımlar. Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, bu uygulamanın bilgisayar için oluşturduğu tehdidin seviyesine göre yerleştirir.

   Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, Güvenlik Duvarı ve Sunucu Yetkisiz Erişim Önleme bileşenleri için yerleştirir. Güven grubunu sadece Güvenlik Duvarı ya da Sunucu Yetkisiz Erişim Önleme için değiştiremezsiniz.

KSN'ye katılmayı reddederseniz ya da ağ bağlantısı olmazsa, Kaspersky Endpoint Security uygulamayı Sunucu Yetkisiz Erişim Önleme bileşeninin ayarlarına göre bir güven grubuna yerleştirir. KSN'den uygulamanın saygınlığı alındıktan sonra, güven grubu otomatik olarak değiştirilebilir.

4. Güven grubuna bağlı olarak uygulamanın ağ etkinliklerini engeller. Örneğin *Yüksek Kısıtlamalı* güven grubundaki uygulamaların herhangi bir ağ bağlantısını kullanmasına izin verilmez.

Uygulamanın bir sonraki başlatılmasında, Kaspersky Endpoint Security uygulamanın bütünlüğünü kontrol eder. Uygulama değişmediyse bileşen, geçerli ağ kurallarını kullanır. Uygulama değiştirildiyse Kaspersky Endpoint Security ilk kez başlatılıyormuş gibi uygulamayı analiz eder.

Ağ Kuralı Öncelikleri

Her kuralın bir önceliği vardır. Bir kural listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Ağ etkinliğinin birkaç kurala eklenmesi halinde, Güvenlik Duvarı ağ etkinliğini en yüksek önceliğe sahip kurala göre düzenler.

Ağ paketi kuralları, uygulamalar için ağ kurallarından daha yüksek bir 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 belirli bir şekilde çalışır. Uygulamalar için ağ kuralı, ağ durumuna dayalı erişim kurallarını içerir: *Ortak ağ*, *Yerel ağ*, *Güvenilir ağ*. 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 türleri

Güvenlik Duvarı, ağ bağlantısının türüne bağlı olarak ağ etkinliklerini kontrol etmenize olanak tanır. Kaspersky Endpoint Security ağ bağlantısı türünü bilgisayarın işletim sisteminden alır. İşletim sistemindeki ağ bağlantısının türü, bağlantının ayarlanması sırasında kullanıcı tarafından ayarlanır. Kaspersky Endpoint Security ayarlarından ağ bağlantısı türünü değiştirebilirsiniz. Güvenlik Duvarı ağ etkinliklerini işletim sistemindeki ağ türüne göre değil Kaspersky Endpoint Security ayarlarındaki ağ durumuna göre izleyecektir.

Aşağıdaki ağ bağlantısı türleri mevcuttur:

- **Ortak ağ**. Ağ antivirüs uygulamaları, güvenlik duvarları veya filtreler tarafından korunmaz (bir kafedeki Wi-Fi gibi). 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 internete *Ortak ağ* türünü atar. İnternetin türünü değiştiremezsiniz.

- **Yerel ağ**. Bu bilgisayardaki dosyalara ve yazıcılara kısıtlı erişime sahip kullanıcılar için olan ağdır (bir kurumsal LAN veya ev ağı gibi).
- **Güvenilir ağ**. Bilgisayarın saldırılara veya yetkisiz veri erişim girişimlerine açık olmadığı güvenli bir ağdır. Güvenlik Duvarı, bu durumdaki ağlarda her tür ağ etkinliğine izin verir.

Windows Defender Güvenlik Duvarı uyumluluğu

İşletim sisteminde kendi yerleşik güvenlik duvarı olan *Windows Defender Güvenlik Duvarı* bulunur. Uygulama, işletim sisteminin türüne bağlı olarak farklı davranır:

- **İş istasyonu**. Kaspersky Güvenlik Duvarının Windows Defender Güvenlik Duvarı ile paralel olarak kullanılması, işletim sisteminin hatalı çalışmasına neden olabilir. Bu nedenle Kaspersky Endpoint Security, her iki Güvenlik Duvarının aynı anda kullanılmasını önleyen bir mekanizmaya sahiptir. Kaspersky Güvenlik Duvarını etkinleştirdiğinizde işletim sistemi, Windows Defender Güvenlik Duvarını otomatik olarak devre dışı bırakır. Kaspersky Güvenlik Duvarını devre dışı bıraktığınızda işletim sistemi, bilgisayarın korunmasını sağlamak için Windows Defender Güvenlik Duvarını otomatik olarak yeniden etkinleştirir.
- **Sunucu**. Kaspersky Güvenlik Duvarı ile Windows Defender Güvenlik Duvarı birbiriyle uyumlu değildir. Kaspersky Endpoint Security yükleyicisi, uygulamayı yüklerken Windows Defender Güvenlik Duvarını otomatik olarak kaldırır.

Güvenlik Duvarı'nın etkinleştirilmesi veya devre dışı bırakılması

Varsayılan olarak Güvenlik Duvarı etkinleştirilmiştir ve optimum modda çalışır.

Yönetim Konsolu'nda (MMC) Güvenlik Duvarını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Güvenlik Duvarı** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

Web Console'da Güvenlik Duvarını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **İletişim ve Web Koruması** → **Güvenlik Duvarı**'nı seçin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Güvenlik duvarı ETKİN** geçiş düğmesini kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Güvenlik Duvarını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Güvenlik Duvarı** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak, Güvenlik Duvarı etkinleştirildiğinde Kaspersky Endpoint Security ağ etkinliğini kontrol eder ve bilgisayarınıza gerçekleştirilen yetkisiz ağ bağlantılarını engeller, ayrıca bilgisayarınızdaki uygulamaların yetkisiz ağ etkinliğini de engeller. Ağ etkinliği ayrıca Ağ Tehdit Koruması bileşeni tarafından da kontrol edilir. Ağ Tehdidi Koruması bileşeni (ayrıca Intrusion Detection System, IDS olarak da adlandırılır), ağ saldırılarına özgü etkinlikleri tespit etmek için gelen ağ trafiğini izler.

Kaspersky Endpoint Security, Güvenlik Duvarı ayarlarından bağımsız olarak ağ saldırısı olaylarını raporlarında günlüğe kaydeder. Ağ Tehdit Koruması bileşeni, Güvenlik Duvarı kuralları kullanarak ağ bağlantısını engellese ve böylece bir ağ saldırısını önlese bile ağ saldırısı olaylarını kaydeder. Kuruluşunuzdaki bilgisayarlara yapılan ağ saldırıları hakkında istatistiksel bilgi üretilmesi gerekmektedir.

Ağ bağlantısı türünü değiştirme

Güvenlik Duvarı varsayılan olarak internete *Ortak ağ* türünü atar. İnternetin türünü değiştiremezsiniz.

Ağ bağlantısı türünü değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. **Kullanılabilir ağlar**'a tıklayın.
4. Türü değiştirmek istediğiniz ağ bağlantısını seçin.
5. **Ağ türü** sütununda ağ bağlantısının türünü seçin:
   - **Ortak ağ**. Ağ antivirüs uygulamaları, güvenlik duvarları veya filtreler tarafından korunmaz (bir kafedeki Wi-Fi gibi). 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.
   - **Yerel ağ**. Bu bilgisayardaki dosyalara ve yazıcılara kısıtlı erişime sahip kullanıcılar için olan ağdır (bir kurumsal LAN veya ev ağı gibi).
   - **Güvenilir ağ**. Bilgisayarın saldırılara veya yetkisiz veri erişim girişimlerine açık olmadığı güvenli bir ağdır. Güvenlik Duvarı, bu durumdaki ağlarda her tür ağ etkinliğine izin verir.
6. Değişikliklerinizi kaydedin.

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* durumundaki ağ paketi kuralları listesinde görülmesini önlemek için bir ağ paketi kuralını kaldırabilirsiniz.

Bir ağ paketi kuralını kaldırma

Güvenlik Duvarı, ağ paketi kurallarına uygun olarak bilgisayardaki tüm ağ etkinliğini filtreler. Ağ paketi kuralları, Güvenlik Duvarının bilgisayarın ağ bağlantılarını kontrol etmek için uyguladığı koşulları (örneğin, yön, iletişim kuralı) içerir. Ağ paketi kuralları, Güvenlik Duvarının kuralla eşleşen bağlantıyla gerçekleştireceği eylemi de belirtir (bağlantıya izin verme veya bağlantıyı engelleme).

Ağ paketi kuralları oluşturmaya yönelik öneriler

Ağ etkinliğini filtrelemek için bir IP adresi veya IP adresi aralığı belirtebilirsiniz. Ayrıca bir DNS adı da belirtebilirsiniz.

Bir kuralda DNS adı kullanılırsa Kaspersky Endpoint Security bu DNS adını bir IP adresine çözümler ve ardından kuralı, bu IP adresi belirtilmiş gibi işler.

Kaspersky Endpoint Security aşağıdaki durumlarda DNS adlarını çözümleyebilir:

- Uygulamanın başlatılması
- Güvenlik Duvarı ayarlarının değiştirilmesi

Uygulama, yüklü olduğu bilgisayardan DNS adlarını çözümlerken DNS sunucusuna çok sayıda sorgu gönderilebilir. Bunu önlemek için kural oluştururken DNS adları yerine IP adresleri kullanmanızı öneririz.

Bazı durumlarda, DNS sunucusunun sahibi DNS kaydının parametrelerini değiştirebildiğinden ağ paketi adlarında DNS adlarının kullanılması güvenli olmayabilir. Kötü niyetli bir taraf ayrıca DNS mesajlarını taklit edebilir ve Güvenlik Duvarı kurallarını atlatabilir.

İnternet Denetimi kurallarını kullanarak ağ bağlantılarını DNS adlarına göre kontrol edebilirsiniz. Güvenlik Duvarı kurallarında bir DNS adı belirtmeniz gerekiyorsa:

- Kurumsal LAN'ın güvenliğini sağlayın.
- Önbelleğe alma ve yetkili DNS sunucuları için güvenlik sağlayın.
- DNS kaydının değiştirilmeye karşı korunmasını etkinleştirin.

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

Ağ paket kuralları oluşturma yöntemleri

Bir ağ paketi kuralını aşağıdaki yöntemlerle oluşturabilirsiniz:

- Ağ İzleyicisi aracı'nı kullanın.

  Ağ İzleyicisi, bir bilgisayarın ağ etkinliği hakkında gerçek zamanlı bilgi görüntülemek için tasarlanmış bir araçtır. Bu, tüm kural ayarlarını yapılandırmanıza gerek olmadığından uygundur. Bazı Güvenlik Duvarı ayarları, Ağ İzleyicisi verilerinden otomatik olarak eklenecektir. Ağ İzleyicisi yalnızca uygulama arabiriminde mevcuttur.

- Güvenlik Duvarı ayarlarını yapılandırın.

  Bu, Güvenlik Duvarı için ince ayarlamalar yapmanıza olanak tanır. Şu anda herhangi bir ağ etkinliği olmasa bile, herhangi bir ağ etkinliği için kurallar oluşturabilirsiniz.

Uygulama arabiriminden bir ağ paketi kuralı oluşturmak için Ağ İzleyicisi aracını kullanma

1. Ana uygulama penceresinin **İzleniyor** bölümünde, **Ağ İzleyicisi** kutucuğuna tıklayın.
2. **Ağ etkinliği** sekmesine gidin.

   Ağ etkinliği sekmesinde, bilgisayardaki etkin tüm ağ bağlantıları görüntülenir. Hem giden hem de gelen ağ bağlantıları görüntülenir.
3. Bir ağ bağlantısının bağlam menüsünde **Ağ paket kuralı oluştur**'u seçin.

   Paket kuralı özellikleri açılır.
4. Paket kuralı için **Etkin** durumu ayarlayın.

5. Ağ hizmetinin adını **Ad** alanına manuel olarak girin.

6. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

   Ağ kuralı şablonu bağlantısına tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

   Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

7. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

8. **Kaydet**'e tıklayın.

   Yeni ağ kuralı listeye eklenir.

9. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

10. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir ağ paketi kuralı oluşturmak için Güvenlik Duvarı ayarlarını kullanma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

3. **Paket kuralları**'na tıklayın.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

4. **Ekle** açılır listesini kullanarak kuralın listedeki konumunu seçin: listenin en üstünde, listenin en altında veya seçili kuralın yanında.

   Kuralın listedeki konumu, kuralın önceliğini belirler. Listenin en üstündeki kural en yüksek önceliğe sahip olur.

5. Paket kuralı için **Etkin** durumu ayarlayın.

6. Ağ hizmetinin adını **Ad** alanına manuel olarak girin.

7. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

   Ağ kuralı şablonu bağlantısına tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

   Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

8. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

9. **Kaydet**'e tıklayın.

   Yeni ağ kuralı listeye eklenir.

10. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

11. Değişikliklerinizi kaydedin.

Yönetim Konsolu'nda (MMC) bir ağ paketi kuralı nasıl oluşturulur

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

4. **Güvenlik Duvarı ayarları** bloğunda **Ayarlar** düğmesine tıklayın.

   Ağ paketi kuralları listesi ve uygulama ağ kuralları listesi açılır.

5. **Ağ paket kuralları** sekmesine gidin.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

6. **Ekle** açılır listesini kullanarak kuralın listedeki konumunu seçin: listenin en üstünde, listenin en altında veya seçili kuralın yanında.

   Kuralın listedeki konumu, kuralın önceliğini belirler. Listenin en üstündeki kural en yüksek önceliğe sahip olur.

7. Ağ hizmetinin adını **Ad** alanına manuel olarak girin.

8. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

   düğmesine tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

   Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

9. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

10. Yeni ağ kuralını kaydet.

11. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

12. Değişikliklerinizi kaydedin.

Güvenlik Duvarı, kurala göre ağ paketlerini kontrol eder. Bir paket kuralını listeden silmeden Güvenlik Duvarı çalışmasında devre dışı bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

Web Console'da ağ paketi kuralı nasıl oluşturulur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Güvenlik Duvarı**'nı seçin.

5. **Ağ paketi kuralları** sekmesini seçin.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

6. **Ekle**'ye tıklayın.

   Bu, yeni bir ağ kuralı formunu açar.

7. Ağ hizmetinin adını **Kural adı** alanına manuel olarak girin.

8. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

   Kural şablonu seçin bağlantısına tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

   Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

9. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

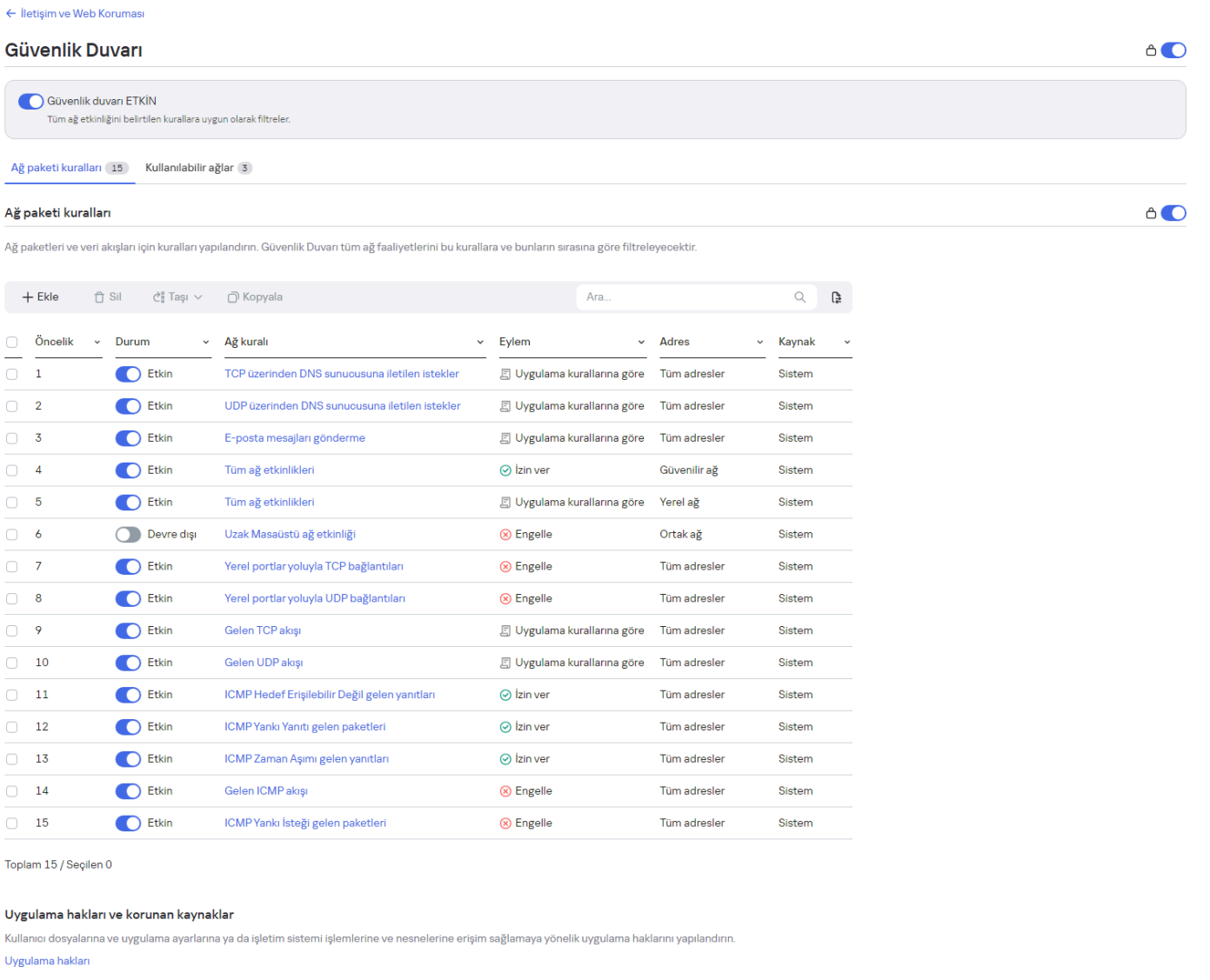
10. Ağ kuralını kaydet.

    Yeni ağ kuralı listeye eklenir.

11. Ağ kuralının önceliğini ayarlamak için **Taşı** düğmesini kullanın.

12. Değişikliklerinizi kaydedin.

Güvenlik Duvarı, kurala göre ağ paketlerini kontrol eder. Bir paket kuralını listeden silmeden Güvenlik Duvarı çalışmasında devre dışı bırakabilirsiniz. Paket kuralını etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş düğmesini kullanın.



Güvenlik Duvarı paket kuralları

Ağ paketi kuralı ayarları

Parametre	Açıklama
Eylem	**İzin ver**. **Engelle**. **Uygulama kurallarına göre**. Bu seçenek tercih edildiğinde, Güvenlik Duvarı uygulama ağ kurallarını ağ bağlantısına uygular.

Parametre	Açıklama
İletişim kuralı	Seçilen protokol üzerinden ağ etkinliğini kontrol edin: TCP, UDP, ICMP, ICMPv6, IGMP ve GRE. İletişim kuralı olarak ICMP veya ICMPv6 seçilirse, ICMP paket türünü ve kodunu belirleyebilirsiniz: İletişim kuralı türü olarak TCP veya UDP seçilirse, arasındaki bağlantının izleneceği yerel ve uzak bilgisayarların port numaralarını belirtebilirsiniz. Port numaraları için olası değer aralığı: 0–65535. Her alana, `,` ile ayrılmış birden fazla değer girebilir veya `-` kullanarak bir değer aralığı belirleyebilirsiniz.. Örneğin: • `100,101` • `100-130` • `100,110-130`
Yön	**Gelen (paket)**. Güvenlik duvarı, ağ kuralını tüm gelen ağ paketlerine uygular. **Gelen**. Güvenlik Duvarı, ağ kuralını, bir uzak bilgisayar tarafından başlatılan bir bağlantı üzerinden gönderilen tüm ağ paketlerine uygular. **Gelen/Giden**. Güvenlik Duvarı, ağ kuralını tüm gelen ve giden ağ paketlerine uygular. **Giden (paket)**. Güvenlik Duvarı, ağ kuralını tüm giden ağ paketlerine uygular. **Giden**. Güvenlik Duvarı, ağ kuralını, kullanıcı bilgisayarı tarafından başlatılan bir bağlantı üzerinden gönderilen tüm ağ paketlerine uygular.
Ağ bağdaştırıcıları	Ağ paketleri gönderebilen ve/veya alabilen ağ bağdaştırıcıları. Ağ bağdaştırıcılarının ayarlarını belirtilmesi, aynı IP adreslerine sahip olan ağ bağdaştırıcıları tarafından gönderilen veya alınan ağ paketleri arasında ayrım yapılmasını mümkün kılar.
Yaşam süresi (TTL)	Ağ paketlerinin kontrolünün yaşam sürelerine göre sınırlandırılması (Time to Live, TTL).
Uzak adresler	Ağ paketlerini alabilecek ve gönderebilecek uzak bilgisayarların ağ adresleri. Güvenlik duvarı, uzak ağ adreslerinin belirtilen aralığına ağ kuralını uygular. Tüm IP adreslerini bir ağ kuralına dahil edebilir, ayrı bir IP adresi listesi oluşturabilir, bir IP adresleri aralığı belirleyebilir veya bir alt ağ seçebilirsiniz (Güvenilir ağlar, Yerel ağlar, Ortak ağlar). Bir bilgisayarın IP adresi yerine bir DNS adı da belirtebilirsiniz. DNS adlarını sadece LAN bilgisayarları veya dahili hizmetler için kullanmalısınız. Bulut hizmetleriyle (Microsoft Azure gibi) ve diğer İnternet kaynaklarıyla etkileşim, İnternet Denetimi bileşeni tarafından gerçekleştirilmelidir. Ağ paketi kuralında, IP adresi belirlenemeyen bir DNS adı eklediyseniz Kaspersky Endpoint Security bir uyarı görüntüler. Web Console'daki ağ paketi kuralları listesine, hatanın açıklamasını içeren bir sütun eklenir. Yönetim Konsolu'nda (MMC) hata açıklaması yoktur. Bu tür paket kuralları renkli olarak vurgulanır.
Yerel adresler	Ağ paketlerini alabilecek ve/veya gönderebilecek uzak bilgisayarların ağ adresleri. Güvenlik duvarı, yerel ağ adreslerinin belirtilen aralığına bir ağ kuralı uygular. Tüm IP adreslerini bir ağ kuralına dahil edebilir, ayrı bir IP adresleri listesi oluşturabilir ya da bir IP adresleri aralığı belirleyebilirsiniz. Uygulama yerel adresleri yalnızca uzak adreslerin bir listesi belirtilmişse saklar. Yani **Uzak adresler** için **Listeden adresler** değeri seçilmiş ve en az bir adres eklenmiştir. Bazen uygulamalar için yerel adres elde edilemez. Bu durumda, bu parametre yok sayılır.

Ağ paketi kuralını etkinleştirme veya devre dışı bırakma

Bir ağ paketi kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. **Paket kuralları**'na tıklayın.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ paketi kurallarının listesini açar.
4. Listede gerekli ağ paketi kuralını seçin.

5. Kuralı etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş düğmesini kullanın.

6. Değişikliklerinizi kaydedin.

Ağ paketi kuralı için Güvenlik Duvarı eylemini değiştirme

Ağ paketi kuralına uygulanan Güvenlik Duvarı eylemini değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

3. **Paket kuralları**'na tıklayın.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ paketi kurallarının listesini açar.

4. Ağ paketi kurallarının listesinde seçin ve **Düzenle** düğmesine tıklayın.

5. **Eylem** açılır listesinde, bu ağ etkinliği tespit edildiğinde Güvenlik Duvarı tarafından gerçekleştirilecek eylemi seçin:

   - **İzin ver**.
   - **Engelle**.
   - **Uygulama kurallarına göre**. Bu seçenek tercih edildiğinde, Güvenlik Duvarı uygulama ağ kurallarını ağ bağlantısına uygular.

6. Değişikliklerinizi kaydedin.

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. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

3. **Paket kuralları**'na tıklayın.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ paketi kurallarının listesini açar.

4. Listede önceliğini değiştirmek istediğiniz ağ paketi kuralını seçin.

5. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

6. Değişikliklerinizi kaydedin.

Ağ paketi kurallarını dışa ve içe aktarma

Ağ paketi kuralları listesini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda kural eklemek için dosyayı değiştirebilirsiniz. Ağ paketi kuralları listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) ağ paketi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

4. **Güvenlik Duvarı ayarları** bloğunda **Ayarlar** düğmesine tıklayın.

   Ağ paketi kuralları listesi ve uygulama ağ kuralları listesi açılır.

5. **Ağ paket kuralları** sekmesine gidin.

6. Ağ paketi kuralları listesini dışa aktarmak için:

   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

      Herhangi bir kural seçmezseniz, Kaspersky Endpoint Security tüm istisnaları dışa aktaracaktır.

   b. **Dışa aktar** bağlantısına tıklayın.

   c. Açılan pencerede, kurallar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, kurallar listesini XML dosyasına aktarır.

7. Ağ paketi kurallarının listesini içe aktarmak için.

   a. **İçe aktar** bağlantısına tıklayın.

      Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   b. Dosyayı aç.

      Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

8. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da ağ paketi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **İletişim ve Web Koruması** → **Güvenlik Duvarı**'nı seçin.
5. Kural listesini dışa aktarmak için **Ağ paketi kuralları** bloğunda:
   a. Düzenlemek istediğiniz kuralları seçin.
   b. → **Dışa aktar** düğmesine tıklayın.
      Kaspersky Endpoint Security, kural listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.
6. Kural listesini içe aktarmak için **Ağ paketi kuralları** bloğunda:
   a. → **İçe aktar** düğmesine tıklayın.
      Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.
   b. Dosyayı aç.
      Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.
7. Değişikliklerinizi kaydedin.

XML'de ağ paketi kurallarını tanımlama

Güvenlik Duvarı, ağ paketi kurallarının XML biçiminde dışa aktarılmasına izin verir. Daha sonra, örneğin, aynı türden çok sayıda kural eklemek için dosyayı değiştirebilirsiniz.

XML dosyası iki ana düğüm içerir: `Rules` ve `Resources`. `Rules` düğümünde ağ paketi kuralları listelenir. Bu düğüm, varsayılan olarak yapılandırılmış kuralları (*önceden tanımlanmış kurallar*) ve kullanıcı tarafından eklenen kuralları (*özel kurallar*) içerir.

Ağ paketi kuralı işaretlemesi

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

XML formatında ağ paketi kuralı ayarları

Parametre	Açıklama	Değer
`<key name="0000">`	Kuralın önceliği. Değer ne kadar düşük olursa öncelik o kadar yüksektir.	Tamsayı Öncelik değeri 4 basamaktan oluşmalıdır. XML dosyasındaki düğümler `0000` değeri ile başlayarak öncelik değerine göre düzenlenmelidir.
`RuleId`	Kuralın kimliği.	**Önceden tanımlanmış kurallar** `100` – **TCP üzerinden DNS sunucusuna iletilen istekler**. `101` – **UDP üzerinden DNS sunucusuna iletilen istekler**. `102` – **E-posta mesajları gönderme**. `110` – **Tüm ağ etkinlikleri** (Güvenilir ağlar). `125` – **Tüm ağ etkinlikleri** (Yerel ağlar). `130` – **Uzak Masaüstü ağ etkinliği**. `131` – **Yerel portlar yoluyla TCP bağlantıları**. `132` – **Yerel portlar yoluyla UDP bağlantıları**. `133` – **Gelen TCP akışı**. `134` – **Gelen UDP akışı**. `137` – **ICMP Hedef Erişilebilir Değil gelen yanıtları**. `138` – **ICMP Yankı Yanıtı gelen paketleri**. `140` – **ICMP Zaman Aşımı gelen yanıtları**. `142` – **Gelen ICMP akışı**. `266` – **ICMPv6 Yankı İsteği gelen paketleri**.
`RuleState`	Kuralın durumu.	`0` – önceden tanımlanmış kural devre dışı `1` – önceden tanımlanmış kural etkin `2` – özel kural devre dışı `3` – özel kural etkin
`RuleTypeId`	Kural türünün kimliği.	`4` – ağ paketi kuralı.
`AppIdEx`	Ağ paketi kuralının ait olduğu uygulamanın kimliği.	Kural herhangi bir uygulamaya ait değilse, değer `0` olur.
`ResIdEx`	Kural ayarlarını içeren kaynağın ana kimliği. Bu tanımlayıcıyı `Resources` düğümünde kural ayarlarını içeren bir bloğun konumunu belirlemek için kullanabilirsiniz.	Tamsayı
`ResIdEx2`	Ağ türünün kimliği.	`0` – **Tüm adresler**. `50` – **Güvenilir ağlar**. `51` – **Yerel ağlar**. `52` – **Ortak ağlar**. `<Network Identifier>` – **Listeden adresler** (adresler manuel olarak tanımlanır).
`AccessFlag`	**Eylem** parametresinin değeri.	`0` – **İzin ver**. `2` **Uygulama kurallarına göre**. `3` – **Engelle**. `4` – **İzin ver** ve **Olayları günlüğe kaydet**. `6` – **Uygulama kurallarına göre** ve **Olayları günlüğe kaydet**. `7` – **Engelle** ve **Olayları günlüğe kaydet**.
`</key>`		

`Resources` düğümü ağ paketi kural ayarlarını içerir. Özel ağ paketi kural ayarları `<key name="0004">` bloğunda listelenir.

Özel ağ paketi kuralı işaretlemesi

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Özel ağ paketi kuralı ayarları

Parametre	Açıklama	Değer
`<key name="Data">`	Parametre bloğunun kimliği.	Tamsayı
`RemotePorts`	**Uzak portlar** parametresinin değeri.	Uzak port aralıklarının listesi.
`LocalPorts`	**Yerel portlar** parametresinin değeri.	Yerel port aralıklarının listesi.

Parametre	Açıklama	Değer
`AdapterBindings`	**Ağ bağdaştırıcıları** parametresinin değeri.	`IpAddresses` – **IP adresleri** parametresinin değeri. `MacAddresses` – **MAC adresleri** parametresinin değeri. `AdapterName` – ağ bağdaştırıcısının adı. `InterfaceType` – **Arabirim türü** parametresinin değeri: • `0` – **Diğer**. • `1` – **Geri Döngü**. • `2` – **Kablolu ağ (Ethernet)**. • `3` – **Kablosuz ağ (Wi-Fi)**. • `4` – **Tünel**. • `5` – **PPP bağlantısı**. • `6` – **PPPoE bağlantısı**. • `7` – **VPN bağlantısı**. • `8` – **Modem bağlantısı**.
`unique`	Yapının dahili kimliği.	Tamsayı Bu parametrenin değiştirilmeden bırakılması önerilir.
`Proto`	**İletişim kuralı** parametresinin değeri.	`0` – devre dışı. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	**Yön** parametresinin değeri.	`1` – **Gelen (paket)**. `2` – **Giden (paket)**. `3` – **Gelen/Giden**. `4` – **Gelen**. `5` – **Giden**.

Parametre	Açıklama	Değer
`IcmpType`	**ICMP türü** parametresinin değeri.	**ICMP protokolü** `0` – **Yankı Yanıtı** (ICMP) veya devre dışı bırakılmış. `3` – **Hedefe Erişilemiyor** (ICMP). `4` – **Kaynak Yavaşlatma**. `5` – **Yeniden Yönlendir**. `6` – **Diğer Ana Bilgisayar Adresi**. `8` – **Yankı İsteği**. `9` – **Yönlendirici Tanıtımı**. `10` – **Yönlendirici İsteme**. `11` – **Süre Aşıldı**. `12` – **Parametre Sorunu**. `13` – **Zaman Damgası**. `14` – **Zaman Damgası Yanıtı**. `15` – **Bilgi İsteği**. `16` – **Bilgi Yanıtı**. `17` – **Adres Maskesi İsteği**. `18` – **Adres Maskesi Yanıtı**. `30` – **İzleme yolu**. `31` – **Datagram Dönüştürme Hatası**. `32` – **Mobil Ana Bilgisayar Yeniden Yönlendirme**. `33` – **IPv6 Neredesin**. `34` – **IPv6 Buradayım**. `35` – **Mobil Kayıt İsteği**. `36` – **Mobil Kayıt Yanıtı**. `37` – **Etki Alanı Adı İsteği**. `38` – **Etki Alanı Adı Yanıtı**. `40` – **Photuris**. **ICMPv6 protokolü** `1` – **Hedefe Erişilemiyor**. `2` – **Paket Çok Büyük**. `3` – **Süre Aşıldı**. `4` – **Parametre Sorunu**. `128` – **Yankı İsteği**. `129` – **Yankı Yanıtı**. `130` – **Çok Noktaya Yayın Dinleyici Sorgusu**. `131` – **Çok Noktaya Yayın Dinleyici Raporu**. `132` – **Çok Noktaya Yayın Dinleyici Tamamlandı**. `133` – **Yönlendirici İsteme**. `134` – **Yönlendirici Tanıtımı**. `135` – **Komşu İsteme**. `136` – **Komşu Tanıtımı**. `137` – **Yeniden Yönlendirme Mesajı**. `138` – **Yönlendirici Yeniden Numaralandırma**. `139` – **ICMP Düğüm Bilgisi Sorgusu**. `141` – **Ters Komşu Bulma İsteği Mesajı**. `142` – **Ters Komşu Bulma Tanıtımı Mesajı**. `143` – **Sürüm 2 Çok Noktaya Yayın Dinleyici Raporu**.

Parametre	Açıklama	Değer
		`144` – **Ev Aracısı Adres Bulma İsteği Mesajı**. `145` – **Ev Aracısı Adres Bulma Yanıtı Mesajı**. `146` – **Mobil Önek İsteme**. `147` – **Mobil Önek Tanıtımı**. `148` – **Sertifika Yolu İsteme Mesajı**. `149` – **Sertifika Yolu Tanıtım Mesajı**. `151` – **Çok Noktaya Yayın Yönlendirici Tanıtımı**. `152` – **Çok Noktaya Yayın Yönlendirici İsteme**. `153` – **Çok Noktaya Yayın Yönlendirici Sonlandırması**.
`IcmpCode`	**ICMP kodu** parametresinin değeri.	`0` – **Kod 0** veya devre dışı. `1` – **Kod 1**. `2` – **Kod 2**.
`Flags`	Yapı özniteliği işaretçisi.	Tamsayı Bu parametrenin değiştirilmeden bırakılması önerilir.
`TTL`	**Yaşam süresi (TTL)** parametresinin değeri.	Saniye cinsinden değer. Devre dışı bırakılırsa değer `0` olur.
`</key>`		
`Id`	Kaynağın ana kimliği (`Rules` düğümüne bakın).	Tamsayı
`ParentID`	Ana grubun kimliği.	Tamsayı Bu parametrenin değiştirilmeden bırakılması önerilir.
`Flags`	Kuralın durumu.	`6` – kural devre dışı. `38` – kural etkin.
`Name`	Ağ paketi kuralının adı.	Dize

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 güvenilirlik grupları kategorilerine ayırılır. Tüm uygulamalar ve uygulama grupları üst grubunun özelliklerini devralır: uygulama denetimi kuralları, uygulama ağ kuralları ve yürütülme öncelikleri.

Sunucu Yetkisiz Erişim Önleme bileşeni gibi, varsayılan olarak Güvenlik Duvarı bileşeni 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.

Bir uygulama ağ kuralı oluşturma

Varsayılan olarak uygulama etkinliği, Kaspersky Endpoint Security'nin uygulamayı ilk başlatmada atadığı güvenilirlik grubu için tanımlanan ağ kuralları tarafından denetlenir. Gerekirse bütün bir güvenilirlik grubu, tek bir uygulama veya bir güvenilirlik grubu içindeki bir grup uygulama için ağ kuralları oluşturabilirsiniz.

Manuel olarak tanımlanan ağ kuralları, bir güvenilirlik grubu için belirlenen ağ kurallarından daha yüksek önceliğe sahiptir. Diğer bir deyişle, manuel olarak tanımlanan uygulama kuralları bir güvenilirlik grubu için belirlenen uygulama kurallarından farklıysa, Güvenlik Duvarı uygulama etkinliğini uygulamalar için manuel olarak tanımlanan kurallara göre kontrol eder.

Güvenlik Duvarı her uygulama için varsayılan olarak aşağıdaki ağ kurallarını oluşturur:

- Güvenilir ağlardaki herhangi bir ağ etkinliği.
- Yerel ağlardaki herhangi bir ağ etkinliği.
- Ortak ağlardaki herhangi bir ağ etkinliği.

Kaspersky Endpoint Security, uygulamaların ağ etkinliğini önceden tanımlanmış ağ kurallarına göre aşağıdaki şekilde kontrol eder:

- Güvenilir ve Düşük Kısıtlamalı: tüm ağ etkinliklerine izin verilir.
- Yüksek Kısıtlamalı ve Güvenilmez: tüm ağ etkinliği engellenir.

Önceden tanımlanmış uygulama kuralları düzenlenemez veya silinemez.

Bir uygulama ağı kuralı oluşturmak için şu yöntemleri kullanabilirsiniz:

- Ağ İzleyicisi aracı'nı kullanın.

  Ağ İzleyicisi, bir bilgisayarın ağ etkinliği hakkında gerçek zamanlı bilgi görüntülemek için tasarlanmış bir araçtır. Bu, tüm kural ayarlarını yapılandırmanıza gerek olmadığından uygundur. Bazı Güvenlik Duvarı ayarları, Ağ İzleyicisi verilerinden otomatik olarak eklenecektir. Ağ İzleyicisi yalnızca uygulama arabiriminde mevcuttur.

- Güvenlik Duvarı ayarlarını yapılandırın.

  Bu, Güvenlik Duvarı için ince ayarlamalar yapmanıza olanak tanır. Şu anda herhangi bir ağ etkinliği olmasa bile, herhangi bir ağ etkinliği için kurallar oluşturabilirsiniz.

Uygulamalar için ağ kuralları oluştururken, ağ paketi kurallarının, uygulama ağ kurallarına göre önceliğe sahip olduğunu unutmayın.

Uygulama arabiriminde bir uygulama ağ kuralı oluşturmak için Ağ İzleyicisi aracını kullanma

1. Ana uygulama penceresinin **İzleniyor** bölümünde, **Ağ İzleyicisi** kutucuğuna tıklayın.
2. **Ağ etkinliği** veya **Açık portlar** sekmesine gidin.

Ağ etkinliği sekmesinde, bilgisayardaki etkin tüm ağ bağlantıları görüntülenir. Hem giden hem de gelen ağ bağlantıları görüntülenir.

Açık portlar sekmesinde, bilgisayarın açık ağ portlarını tamamı listelenir.

3. Bir ağ bağlantısının bağlam menüsünde **Bir uygulama ağ kuralı oluştur**'u seçin.

   Uygulama kuralları ve özellikler penceresi açılır.

4. **Ağ kuralları** sekmesini seçin.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

5. **Ekle**'ye tıklayın.

   Paket kuralı özellikleri açılır.

6. Ağ hizmetinin adını **Ad** alanına manuel olarak girin.

7. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

   Ağ kuralı şablonu bağlantısına tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

   Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

8. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

9. **Kaydet**'e tıklayın.

   Yeni ağ kuralı listeye eklenir.

10. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

11. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir uygulama ağı kuralı oluşturmak için Güvenlik Duvarı ayarlarını kullanma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

3. **Uygulamalar için kurallar**'a tıklayın.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

4. Uygulamalar listesinde, ağ kuralını oluşturmak istediğiniz uygulamayı veya uygulama grubunu seçin.

5. İçerik menüsünü görüntülemek için sağ tıklayın ve **Ayrıntılar ve kurallar** seçeneğini seçin.

   Uygulama kuralları ve özellikler penceresi açılır.

6. **Ağ kuralları** sekmesini seçin.

7. **Ekle**'ye tıklayın.

   Paket kuralı özellikleri açılır.

8. Ağ hizmetinin adını **Ad** alanına manuel olarak girin.

9. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

Ağ kuralı şablonu bağlantısına tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

10. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

11. **Kaydet**'e tıklayın.

    Yeni ağ kuralı listeye eklenir.

12. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

13. Değişikliklerinizi kaydedin.

Yönetim Konsolu'nda (MMC) bir uygulama ağ kuralı nasıl oluşturulur

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.

4. **Güvenlik Duvarı ayarları** bloğunda **Ayarlar** düğmesine tıklayın.

   Ağ paketi kuralları listesi ve uygulama ağ kuralları listesi açılır.

5. **Uygulama ağ kuralları** sekmesine gidin.

6. **Ekle**'ye tıklayın.

7. Açılan pencerede, bir ağ kuralı oluşturmak istediğiniz uygulamayı aramak için kriterleri girin.

   Uygulamanın adını veya satıcının adını girebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

8. **Yenile**'ye tıklayın.

   Kaspersky Endpoint Security uygulamayı, yönetilen bilgisayarlardaki yüklü uygulamalar birleştirilmiş listesinde arar. Kaspersky Endpoint Security, arama kriterlerinizi karşılayan uygulamaların bir listesini görüntüler.

9. Gereken uygulamayı seçin.

10. **Seçilen uygulamayı güvenilirlik grubuna ekle** açılır listesinden **Varsayılan gruplar** seçimini yapın ve **Tamam**'a tıklayın.

    Uygulama varsayılan gruba eklenecektir.

11. İlgili uygulamayı seçin ve ardından uygulamanın bağlam menüsünden **Uygulama hakları**'nı seçin.

    Uygulama kuralları ve özellikler penceresi açılır.

12. **Ağ kuralları** sekmesini seçin.

    Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

13. **Ekle**'ye tıklayın.

    Paket kuralı özellikleri açılır.

14. Ağ hizmetinin adını **Ad** alanına manuel olarak girin.

15. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

    düğmesine tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

    Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

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

17. Yeni ağ kuralını kaydet.

18. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

19. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir uygulama ağ kuralı oluşturma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Güvenlik Duvarı**'nı seçin.

5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Uygulama hakları** bağlantısına tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

6. **Uygulama hakları** sekmesine gidin.

   Pencerenin sol tarafında güvenilirlik gruplarının bir listesini, sağ tarafında ise bunların özelliklerini göreceksiniz.

7. **Uygulamalar** bloğunda, **Ekle** düğmesine tıklayın.

   Bir güvenilirlik grubuna uygulama eklemek için Sihirbaz başlatılır.

8. Uygulama için ilgili güvenilirlik grubunu seçin.

9. **Uygulama** türünü seçin. Bir sonraki adıma geçin.

   Birden çok uygulama için bir ağ kuralı oluşturmak değiştirmek istiyorsanız **Grup** türünü seçin ve uygulama grubu için bir ad tanımlayın.

10. Açılan uygulamalar listesinden bir ağ kuralı oluşturmak istediğiniz uygulamaları seçin.

    Bir filtre kullanın. Uygulamanın adını veya satıcının adını girebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

11. Sihirbazı tamamlayın.

    Uygulama güvenilirlik grubuna eklenir.

12. Pencerenin sol kısmından ilgili uygulamayı seçin.

13. Pencerenin sağ tarafında, açılır listeden **Ağ kuralları**'nı seçin.

    Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

14. **Ekle**'ye tıklayın.

    Uygulama kuralı özellikleri açılır.

15. Ağ hizmetinin adını **Kural adı** alanına manuel olarak girin.

16. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

    Kural şablonu seçin bağlantısına tıklayarak önceden tanımlanmış bir kural şablonu seçebilirsiniz. Kural şablonları, en sık kullanılan ağ bağlantılarını açıklar.

    Tüm ağ kuralı ayarları otomatik olarak doldurulacaktır.

17. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.

18. Ağ kuralını kaydet.

    Yeni ağ kuralı listeye eklenir.

19. Ağ kuralının önceliğini ayarlamak için **Taşı** düğmesini kullanın.

20. Değişikliklerinizi kaydedin.

Uygulama ağ kuralları ayarları

Parametre	Açıklama
Eylem	**İzin ver**. **Engelle**.
İletişim kuralı	Seçilen protokol üzerinden ağ etkinliğini kontrol edin: TCP, UDP, ICMP, ICMPv6, IGMP ve GRE. İletişim kuralı olarak ICMP veya ICMPv6 seçilirse, ICMP paket türünü ve kodunu belirleyebilirsiniz: İletişim kuralı türü olarak TCP veya UDP seçilirse, arasındaki bağlantının izleneceği yerel ve uzak bilgisayarların port numaralarını belirtebilirsiniz. Port numaraları için olası değer aralığı: 0–65535. Her alana, `,` ile ayrılmış birden fazla değer girebilir veya `-` kullanarak bir değer aralığı belirleyebilirsiniz.. Örneğin: • `100,101` • `100-130` • `100,110-130`
Yön	**Gelen**. **Gelen/Giden**. **Giden**.
Uzak adresler	Ağ paketlerini alabilecek ve gönderebilecek uzak bilgisayarların ağ adresleri. Güvenlik duvarı, uzak ağ adreslerinin belirtilen aralığına ağ kuralını uygular. Tüm IP adreslerini bir ağ kuralına dahil edebilir, ayrı bir IP adresi listesi oluşturabilir, bir IP adresleri aralığı belirleyebilir veya bir alt ağ seçebilirsiniz (Güvenilir ağlar, Yerel ağlar, Ortak ağlar). Bir bilgisayarın IP adresi yerine bir DNS adı da belirtebilirsiniz. DNS adlarını sadece LAN bilgisayarları veya dahili hizmetler için kullanmalısınız. Bulut hizmetleriyle (Microsoft Azure gibi) ve diğer İnternet kaynaklarıyla etkileşim, İnternet Denetimi bileşeni tarafından gerçekleştirilmelidir. Ağ paketi kuralında, IP adresi belirlenemeyen bir DNS adı eklediyseniz Kaspersky Endpoint Security bir uyarı görüntüler. Web Console'daki ağ paketi kuralları listesine, hatanın açıklamasını içeren bir sütun eklenir. Yönetim Konsolu'nda (MMC) hata açıklaması yoktur. Bu tür paket kuralları renkli olarak vurgulanır.
Yerel adresler	Ağ paketlerini alabilecek ve/veya gönderebilecek uzak bilgisayarların ağ adresleri. Güvenlik duvarı, yerel ağ adreslerinin belirtilen aralığına bir ağ kuralı uygular. Tüm IP adreslerini bir ağ kuralına dahil edebilir, ayrı bir IP adresleri listesi oluşturabilir ya da bir IP adresleri aralığı belirleyebilirsiniz. Uygulama yerel adresleri yalnızca uzak adreslerin bir listesi belirtilmişse saklar. Yani **Uzak adresler** için **Listeden adresler** değeri seçilmiş ve en az bir adres eklenmiştir. Bazen uygulamalar için yerel adres elde edilemez. Bu durumda, bu parametre yok sayılır.

Uygulama ağ kuralını etkinleştirme veya devre dışı bırakma

Bir uygulama ağ kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. **Uygulamalar için kurallar**'a tıklayın.

   Bu, uygulama kuralları listesini açar.
4. Uygulamalar listesinde, ağ kuralını oluşturmak veya düzenlemek istediğiniz uygulamayı veya uygulamalar grubunu seçin.
5. İçerik menüsünü görüntülemek için sağ tıklayın ve **Ayrıntılar ve kurallar** seçeneğini seçin.

   Uygulama kuralları ve özellikler penceresi açılır.
6. **Ağ kuralları** sekmesini seçin.
7. Uygulama grubu için ağ kuralları listesinde ilgili ağ kuralını seçin.

   Ağ kuralı özellikleri penceresi açılır.
8. Ağ kuralında **Etkin** veya **Etkin değil** durumunu ayarlayın.

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

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. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. **Uygulamalar için kurallar**'a tıklayın.

   Bu, uygulama kuralları listesini 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. İçerik menüsünü açmak için sağ tıklayın, **Ağ kuralları**'nı seçin, ardından atamak istediğiniz eylemi seçin:
   - **Devral**.
   - **İzin ver**.
   - **Engelle**.
6. Değişikliklerinizi kaydedin.

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

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. **Uygulamalar için kurallar**'a tıklayın.
   Bu, uygulama kuralları listesini açar.
4. Listede, tek ağ kuralı için değiştirmek istediğiniz uygulamayı veya uygulamalar grubunu seçin.
5. İçerik menüsünü görüntülemek için sağ tıklayın ve **Ayrıntılar ve kurallar** seçeneğini seçin.
   Uygulama kuralları ve özellikler penceresi açılır.
6. **Ağ kuralları** sekmesini seçin.
7. Güvenlik Duvarı eylemini değiştirmek istediğiniz ağ kuralını seçin.
8. **İzin** sütununda sağ tıklayarak bağlam menüsünü açın ve atamak istediğiniz eylemi seçin.
   - **Devral**.
   - **İzin ver**.
   - **Reddet**.
   - **Olayları günlüğe kaydet**.
9. Değişikliklerinizi kaydedin.

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. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
3. **Uygulamalar için kurallar**'a tıklayın.
   Bu, uygulama kuralları listesini açar.
4. Uygulamalar listesinde, ağ kuralı önceliğini değiştirmek istediğiniz uygulamayı veya uygulamalar grubunu seçin.
5. İçerik menüsünü görüntülemek için sağ tıklayın ve **Ayrıntılar ve kurallar** seçeneğini seçin.
   Uygulama kuralları ve özellikler penceresi açılır.
6. **Ağ kuralları** sekmesini seçin.
7. Önceliğini değiştirmek istediğiniz ağ kuralını seçin.
8. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.
9. Değişikliklerinizi kaydedin.

Ağ İzleyicisi

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

Ağ İzleyicisini başlatmak için:

Ana uygulama penceresinin **İzleniyor** bölümünde, **Ağ İzleyicisi** kutucuğuna tıklayın.

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. Bu sekmede, Güvenlik Duvarının çalışması için ağ paketi kuralları da oluşturabilirsiniz.
- **Açık portlar** sekmesinde, bilgisayarın açık ağ portlarını tamamı listelenir. Bu sekmede, Güvenlik Duvarının çalışması için ağ paketi kuralları ve uygulama kuralları da oluşturabilirsiniz.
- **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 etkinliği Ağ Tehdidi Koruması bileşeni tarafından engellenen uzak bilgisayarların IP adresleri listelenir.

Exploit Önleme

Exploit Önleme bileşeni, yönetici ayrıcalıklarını kullanmak ya da zararlı etkinlikler gerçekleştirmek amacıyla bilgisayardaki zayıf noktalardan faydalanan program kodunu tespit eder. Örneğin istismarcılar bir arabellek taşması saldırısı kullanabilir. İstismarcı bunu yapmak için savunmasız bir uygulamaya büyük miktarda veri gönderimi yapar. Bu verileri işleyen savunmasız uygulama da zararlı kodları çalıştırır. Bu saldırının sonucunda istismarcı zararlı bir yazılımın izinsiz yüklemesini başlatabilir. Yürütülebilir bir dosyanın hassas bir uygulama tarafından çalıştırılması girişimi kullanıcı tarafından gerçekleştirilmediyse Kaspersky Endpoint Security, bu dosyanın çalıştırılmasını engeller ve kullanıcıyı bilgilendirir.

Exploit Önleme bileşeni ayrıca bilgisayarın güvenliğini tehdit edebilecek uygulamaların işlemleri için ağ portlarını izler. Uygulama, anti-virüs veritabanları ile bu tür işlemler hakkında bilgi alır.

Exploit Önleme'yi etkinleştirme ve devre dışı bırakma

Varsayılan olarak Exploit Önleme etkinleştirilmiştir ve optimum modda çalışır. Kaspersky Endpoint Security, güvenlik açığı olan uygulamalar tarafından çalıştırılan yürütülebilir dosyaları izler. Kaspersky Endpoint Security, hassas bir uygulamadan başlatılan yürütülebilir bir dosyanın kullanıcı dışında çalıştırıldığını tespit ederse Kaspersky Endpoint Security, seçilen eylemi gerçekleştirecektir (örneğin, işlemi engelleyecektir).

Yönetim Konsolu'nda (MMC) Exploit Önlemeyi etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Exploit Önleme** seçimini yapın.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Exploit Önleme** onay kutusunu kullanın.
5. **Exploit algılandığında** bloğunda gereken eylemi seçin:
   - **Engelle**. Bu öğe işaretliyse Kaspersky Endpoint Security, bir açıktan yararlanma tespit ettiğinde bu açıktan yararlanma işlemlerini engeller ve bu açıktan yararlanma hakkında bilgileri içeren bir günlük girişi yapar.
   - **Bilgilendir**. Bu öğe seçiliyse ve Kaspersky Endpoint Security exploit tespit ederse exploit hakkında bilgileri içeren bir olayı günlüğe kaydeder ve bu exploit hakkında bilgileri etkin tehditler listesine ekler.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Exploit Önleme teknolojisi etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Davranış Analizi** → **Exploit Önleme** bölümüne gidin.

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Exploit Önleme** geçiş düğmesini kullanın.

6. **Tehdit algılandığında yapılacak eylem** bloğunda gereken eylemi seçin:

   - **Engelle**. Bu öğe işaretliyse Kaspersky Endpoint Security, bir açıktan yararlanma tespit ettiğinde bu açıktan yararlanma işlemlerini engeller ve bu açıktan yararlanma hakkında bilgileri içeren bir günlük girişi yapar.

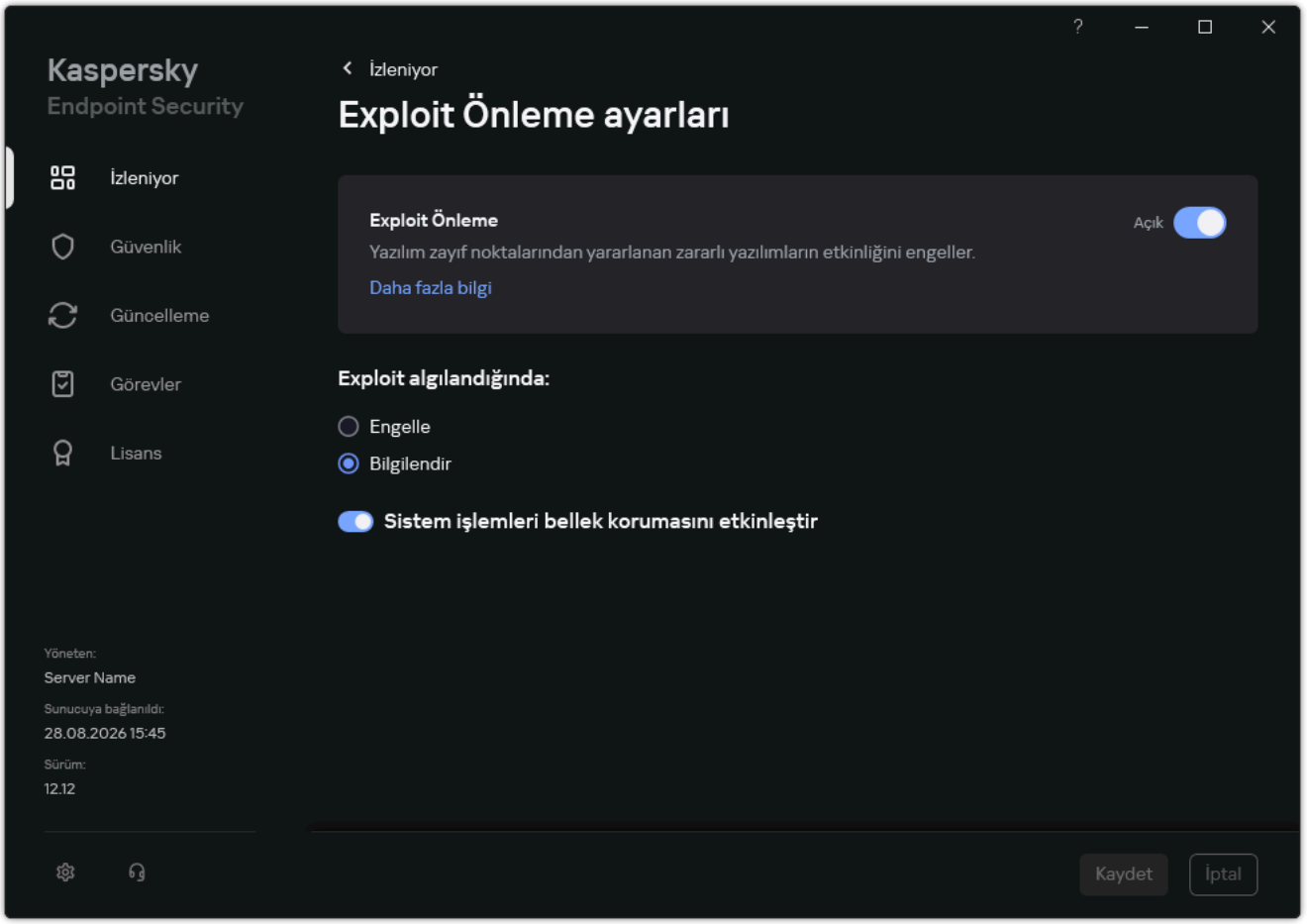
   - **Bilgilendir**. Bu öğe seçiliyse ve Kaspersky Endpoint Security exploit tespit ederse exploit hakkında bilgileri içeren bir olayı günlüğe kaydeder ve bu exploit hakkında bilgileri etkin tehditler listesine ekler.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Exploit Önlemeyi etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Exploit Önleme**'yi seçin.



Exploit Önleme ayarları

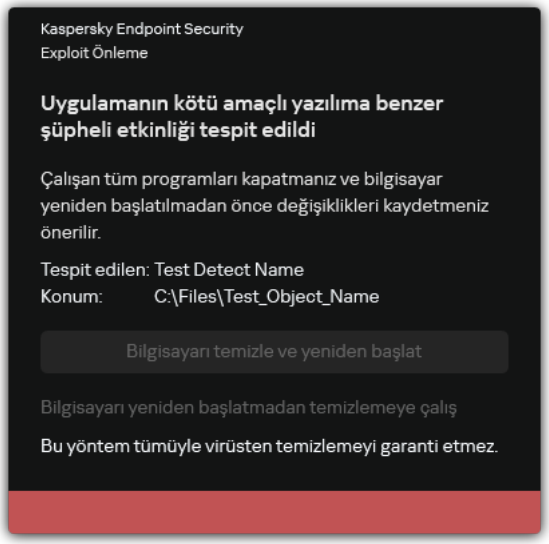
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Exploit Önleme** geçiş düğmesini kullanın.

4. **Exploit algılandığında** bloğunda gereken eylemi seçin:

   - **Engelle**. Bu öğe işaretliyse Kaspersky Endpoint Security, bir açıktan yararlanma tespit ettiğinde bu açıktan yararlanma işlemlerini engeller ve bu açıktan yararlanma hakkında bilgileri içeren bir günlük girişi yapar.

   - **Bilgilendir**. Bu öğe seçiliyse ve Kaspersky Endpoint Security exploit tespit ederse exploit hakkında bilgileri içeren bir olayı günlüğe kaydeder ve bu exploit hakkında bilgileri etkin tehditler listesine ekler.

5. Değişikliklerinizi kaydedin.



Etkin tehdit hakkında bildirim

Sistem işlemleri bellek koruması

Varsayılan olarak sistem işlemi bellek koruması etkindir. Kaspersky Endpoint Security, sistem işlemlerine erişmeye çalışan harici işlemleri engeller.

Yönetim Konsolu'nda (MMC) sistem işlemleri bellek korumasını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Exploit Önleme** seçimini yapın.

4. Bu seçeneği etkinleştirmek veya devre dışı bırakmak için **Sistem işlemleri bellek korumasını etkinleştir** onay kutusunu kullanın.

5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da sistem işlemleri bellek korumasını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

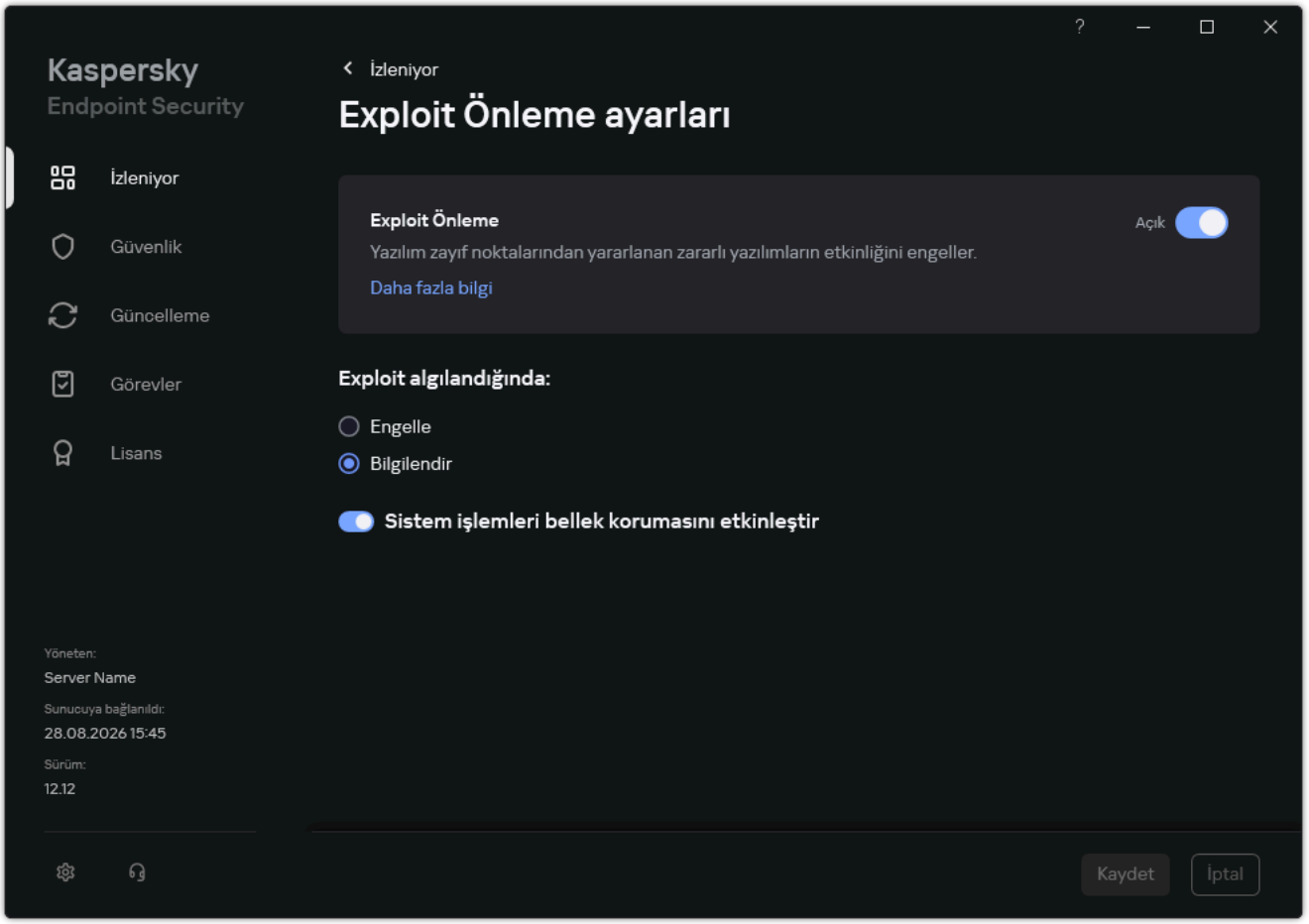
   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması → Davranış Analizi → Exploit Önleme** bölümüne gidin.
5. Bu özelliği etkinleştirmek veya devre dışı bırakmak için **Sistem işlemleri bellek korumas ETKİN** anahtarını kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde sistem işlem belleği korumasını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Exploit Önleme**'yi seçin.



Exploit Önleme ayarları

3. Bu özelliği etkinleştirmek veya devre dışı bırakmak için **Sistem işlemleri bellek korumasını etkinleştir** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Davranış Tespiti

Davranış Tespiti bileşeni, bilgisayarınızdaki uygulamaların işlemleriyle ilgili veriler toplar ve bu bilgileri, performanslarını iyileştirmek için diğer koruma bileşenlerine sağlar. Davranış Tespiti bileşeni, uygulamalar için Davranış Akışı İmzalarından (BSS) yararlanır. Uygulama etkinliğinin bir davranış akımı imzasıyla eşleşmesi halinde Kaspersky Endpoint Security seçili duyarlı işlemi gerçekleştirir. Davranış akışı imzalarına dayanan Kaspersky Endpoint Security işlevi, bilgisayarınız için ileriye dönük etkili koruma sağlar.

Davranış Tespiti bileşeni ayrıca bilgisayarın güvenliğini tehdit edebilecek uygulamaların işlemleri için ağ portlarını izler. Uygulama, anti-virüs veritabanları ile bu tür işlemler hakkında bilgi alır.

Varsayılan olarak Davranış Tespiti etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Kötü amaçlı etkinlik tespit edildiğinde, Kaspersky Endpoint Security kötü amaçlı uygulamanın yürütülebilir dosyasını siler.

Mutlaka gerekmedikçe Davranış Tespiti'nin devre dışı bırakılması önerilmez çünkü bu, koruma bileşenlerinin etkinliğini azaltabilir. Koruma bileşenleri, tehditlerin tespit edilmesi için Davranış Tespiti bileşeni tarafından toplanan verileri isteyebilir.

Yönetim Konsolu'nda (MMC) Davranış Tespitini etkinleştirmr veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Gelişmiş Tehdit Koruması** → **Davranış Tespiti**'ni seçin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Davranış Tespiti** kutucuğunu işaretleyin.
6. **Kötü amaçlı yazılım etkinliği tespit edildiğinde gerçekleştirilecek eylem** bloğunda gereken eylemi seçin:
   - **Sil**. Bu öğe seçilirse Kaspersky Endpoint Security zararlı yazılım etkinliği tespit edildiğinde zararlı uygulamanın yürütülebilir dosyasını siler ve dosyanın bir yedekleme kopyasını Yedekleme'de oluşturur.
   - **Engelle**. Bu öğe seçilirse zararlı yazılımların etkinlikleri tespit edildiğinde Kaspersky Endpoint Security, bu uygulamayı sonlandırır.
   - **Bilgilendir**. Bu öğe seçilirse ve uygulamanın zararlı yazılım etkinliği tespit edilirse Kaspersky Endpoint Security, uygulamanın zararlı yazılım etkinliği hakkındaki bilgileri etkin tehditler listesine ekler.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Davranış Tespitini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Davranış Analizi** → **Davranış Tespiti** bölümüne gidin
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Davranış Tespiti ETKİN** anahtarını kullanın.

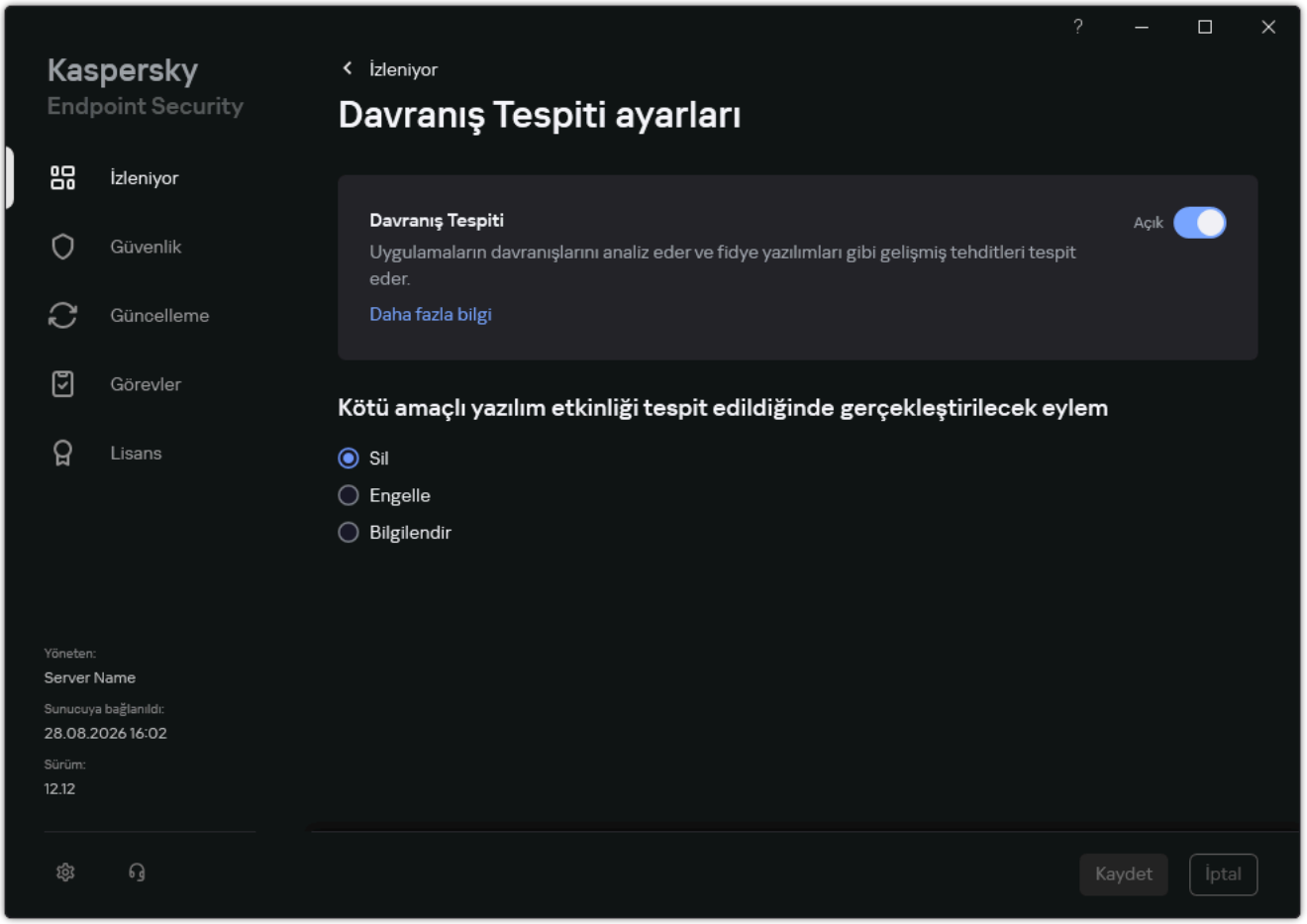
6. **Tehdit algılandığında yapılacak eylem** bloğunda gereken eylemi seçin:

   - **Sil**. Bu öğe seçilirse Kaspersky Endpoint Security zararlı yazılım etkinliği tespit edildiğinde zararlı uygulamanın yürütülebilir dosyasını siler ve dosyanın bir yedekleme kopyasını Yedekleme'de oluşturur.
   - **Engelle**. Bu öğe seçilirse zararlı yazılımların etkinlikleri tespit edildiğinde Kaspersky Endpoint Security, bu uygulamayı sonlandırır.
   - **Bilgilendir**. Bu öğe seçilirse ve uygulamanın zararlı yazılım etkinliği tespit edilirse Kaspersky Endpoint Security, uygulamanın zararlı yazılım etkinliği hakkındaki bilgileri etkin tehditler listesine ekler.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Davranış Tespitini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Davranış Tespiti**'ni seçin.



Davranış Tespiti ayarları

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Davranış Tespiti** geçiş düğmesini kullanın.

4. **Kötü amaçlı yazılım etkinliği tespit edildiğinde gerçekleştirilecek eylem** bloğunda gereken eylemi seçin:

   - **Sil**. Bu öğe seçilirse Kaspersky Endpoint Security zararlı yazılım etkinliği tespit edildiğinde zararlı uygulamanın yürütülebilir dosyasını siler ve dosyanın bir yedekleme kopyasını Yedekleme'de oluşturur.
   - **Engelle**. Bu öğe seçilirse zararlı yazılımların etkinlikleri tespit edildiğinde Kaspersky Endpoint Security, bu uygulamayı sonlandırır.
   - **Bilgilendir**. Bu öğe seçilirse ve uygulamanın zararlı yazılım etkinliği tespit edilirse Kaspersky Endpoint Security, uygulamanın zararlı yazılım etkinliği hakkındaki bilgileri etkin tehditler listesine ekler.

5. Değişikliklerinizi kaydedin.

Sonuç olarak, Davranış Tespiti etkinleştirilirse, Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz etmek için davranış akışı imzalarını kullanır.

Şifreleyici Önleyici

Kaspersky Endpoint Security for Windows 12.12'den itibaren, eskiden Davranış Tespiti bileşeninin bir parçası olan paylaşılan klasörlerin harici şifrelemeye karşı korunması ayrı bir bileşen olan Şifreleyici Önleyici'ye dönüştürüldü.

Bileşen yalnızca NTFS dosya sistemli ve EFS ile şifrelenmemiş yığın depolama aygıtlarında saklanan dosyalarda gerçekleştirilen işlemleri görüntüler.

Şifreleyici Önleyici bileşeni paylaşılan klasörlerdeki etkinliği analiz eder. Bu etkinlik, dış şifreleme için tipik olan bir davranış akışı imzasıyla eşleşirse Kaspersky Endpoint Security seçili eylemi gerçekleştirir.

Şifreleyici Önleyici bileşeninin çalışması için Davranış Tespiti bileşenini etkinleştirmeniz gerekir.

Kaspersky Endpoint Security paylaşılan klasörlerde bir dosya değiştirme girişimi algılarsa şu eylemleri yapar:

- Kötü amaçlı etkinliği başlatan oturum için dosya değişikliğine erişimi engeller (dosya salt okunur olacaktır).
- Değiştirilen dosyaların yedek kopyalarını oluşturur.
- Yerel uygulama arabirimi raporlarına bir giriş ekler ve tespit edilen kötü amaçlı etkinlikle ilgili bilgileri Kaspersky Security Center'a gönderir.
- Ayrıca Düzeltme Altyapısı bileşeni etkinse değiştirilen dosyalar yedek kopyalarından geri yüklenir.

Paylaşılan klasörlerin dış şifrelemeye karşı korunmasını etkinleştirme ve devre dışı bırakma

Varsayılan olarak, paylaşılan klasörlerin harici şifrelemeye karşı korunması etkindir ve Kaspersky uzmanları tarafından önerildiği gibi çalışır. Bu işlevi yapılandırmak için bir koruma kapsamı oluşturabilir ve gerekirse istisnaları yapılandırabilirsiniz. Varsayılan olarak, uygulama paylaşılan klasörleri otomatik olarak tanımlar ve tüm klasörlerdeki dosya etkinliğini izler. Paylaşılan klasörlerdeki dosyaları harici olarak şifreleme girişimi tespit edildiğinde, Kaspersky Endpoint Security uzak kullanıcının oturumunu bir saat süreyle engeller (varsayılan olarak).

Kaspersky Endpoint Security yüklendikten sonra paylaşılan klasörlerin dış şifrelemeye karşı korunması bilgisayar yeniden başlatılıncaya kadar sınırlıdır.

Yönetim Konsolu'nda (MMC) paylaşılan klasörlerin harici şifrelemeye karşı korunmasını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.
4. Harici şifrelemeye özgü etkinliklerin algılanmasını etkinleştirmek veya devre dışı bırakmak için **Şifreleyici Önleyici** onay kutusunu kullanın.
5. Paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında uygulamanın gerçekleştireceği ilgili eylemi seçin:
   - **Bağlantıyı şu kadar süre engelle**: **N dk**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security paylaşılan klasörlerdeki dosyaları değiştirme girişimi algıladığında, kötü amaçlı etkinliği başlatan oturum için dosya değiştirme erişimini engeller ve değiştirilen dosyaların yedek kopyalarını oluşturur.

     Düzeltme Altyapısı bileşeni etkinse ve **Bağlantıyı şu kadar süre engelle**: **N dk** seçeneği belirlenmişse değiştirilen dosyalar yedek kopyalarından geri yüklenir.

   - **Bilgilendir**. Bu seçenek belirlenirse, paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında Kaspersky Endpoint Security, bu girişim hakkındaki bilgileri etkin tehditler listesine ekler, yerel uygulama arabirimi raporlarına bir giriş ekler ve tespit edilen algılanan kötü amaçlı etkinlikle ilgili bilgileri Kaspersky Security Center'a gönderir.
6. Gerekirse, bir koruma kapsamını düzenleyin ve istisnaları tanımlayın.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da paylaşılan klasörlerin harici şifrelemeye karşı korunmasını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması → Davranış Analizi → Şifreleyici Önleyici** bölümüne gidin.

5. Harici şifrelemeye özgü etkinliklerin algılanmasını etkinleştirmek veya devre dışı bırakmak için **Şifreleyici Önleyici ETKİN** anahtarını kullanın.

6. Paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında uygulamanın gerçekleştireceği ilgili eylemi seçin:

   - **Bağlantıyı şu kadar süre engelle (dk)**: **N dk**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security paylaşılan klasörlerdeki dosyaları değiştirme girişimi algıladığında, kötü amaçlı etkinliği başlatan oturum için dosya değiştirme erişimini engeller ve değiştirilen dosyaların yedek kopyalarını oluşturur.

     > Düzeltme Altyapısı bileşeni etkinse ve **Bağlantıyı şu kadar süre engelle (dk)**: **N dk** seçeneği belirlenmişse değiştirilen dosyalar yedek kopyalarından geri yüklenir.

   - **Bilgilendir**. Bu seçenek belirlenirse, paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında Kaspersky Endpoint Security, bu girişim hakkındaki bilgileri etkin tehditler listesine ekler, yerel uygulama arabirimi raporlarına bir giriş ekler ve tespit edilen algılanan kötü amaçlı etkinlikle ilgili bilgileri Kaspersky Security Center'a gönderir.

7. Gerekirse, bir koruma kapsamını düzenleyin ve istisnaları tanımlayın.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde paylaşılan klasörlerin harici şifrelemeye karşı korunmasını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Şifreleyici Önleyici** seçimini yapın.

3. Dış şifrelemeye özgü etkinliklerin algılanmasını etkinleştirmek veya devre dışı bırakmak için **Paylaşılan klasörlerin harici şifrelemeye karşı korunması** onay kutusunu kullanın.

4. Dış şifrelemeye özgü etkinliklerin algılanmasını etkinleştirmek veya devre dışı bırakmak için **Paylaşılan klasörlerin harici şifrelemeye karşı korunması** onay kutusunu kullanın.

5. Paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında uygulamanın gerçekleştireceği ilgili eylemi seçin:

   - **Bağlantıyı şu kadar süre engelle (dk)**: **N dk**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security paylaşılan klasörlerdeki dosyaları değiştirme girişimi algıladığında, kötü amaçlı etkinliği başlatan oturum için dosya değiştirme erişimini engeller ve değiştirilen dosyaların yedek kopyalarını oluşturur.

     > Düzeltme Altyapısı bileşeni etkinse ve **Bağlantıyı şu kadar süre engelle (dk)**: **N dk** seçeneği belirlenmişse değiştirilen dosyalar yedek kopyalarından geri yüklenir.

   - **Bilgilendir**. Bu seçenek belirlenirse, paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında Kaspersky Endpoint Security, bu girişim hakkındaki bilgileri etkin tehditler listesine ekler, yerel uygulama arabirimi raporlarına bir giriş ekler ve tespit edilen algılanan kötü amaçlı etkinlikle ilgili bilgileri Kaspersky Security Center'a gönderir.

6. Gerekirse, bir koruma kapsamını düzenleyin ve istisnaları tanımlayın.

7. Değişikliklerinizi kaydedin.

Güvenilir olmayan bir bilgisayarın engelleme süresini yapılandırma

Güvenilmez bir bilgisayar, kötü niyetli faaliyetlerde bulunan veya veri şifreleyen uzak bir bilgisayardır. Varsayılan olarak, Kaspersky Endpoint Security uzak kullanıcının oturumunu bir saat süreyle engeller. Engelleme süresi sona erdiğinde, Kaspersky Endpoint Security bilgisayarı engelleme listesinden kaldırır ve paylaşılan klasöre erişimi geri yükler.

Yönetim Konsolu'nda (MMC) güvenilir olmayan bir bilgisayarın engelleme süresini yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.

4. **Tehdit algılandığında uygulanacak eylem** bölümünden **Bağlantıyı N dakika engelle** seçimini yapın.

5. Kötü amaçlı etkinlik veya veri şifreleme yapan güvenilir olmayan bir bilgisayarın engelleme süresini yapılandırın.

6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da güvenilmeyen bir bilgisayarın engelleme süresini yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması** → **Davranış Analizi** → **Şifreleyici Önleyici** bölümüne gidin.

5. **Tehdit algılandığında uygulanacak eylem** bölümünde, kötü amaçlı etkinlik veya veri şifreleme yapan güvenilmeyen bir bilgisayarın engelleme süresini yapılandırın.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde güvenilir olmayan bir bilgisayarın engelleme süresini yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.

3. **Tehdit algılandığında yapılacak eylem** bölümünde, **Bağlantıyı (dakika) engelle** seçimini yapın.

4. Kötü amaçlı etkinlik veya veri şifreleme yapan güvenilir olmayan bir bilgisayarın engelleme süresini yapılandırın.

5. Değişikliklerinizi kaydedin.

Sonuç olarak, uzak bilgisayar kilitlenir. Uzak bilgisayarın kilidini açmak için Kaspersky Endpoint Security'yi yeniden başlatabilirsiniz.

Koruma kapsamının düzenlenmesi

Koruma kapsamı, Kaspersky Endpoint Security'nin dosya etkinliğini izlediği paylaşılan klasörlere giden yolların bir listesidir. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. Varsayılan olarak, uygulama paylaşılan klasörleri otomatik olarak tanımlar ve tüm klasörlerdeki dosya etkinliğini izler.

Bir klasörü koruma kapsamından çıkarmak, kuruluşunuz paylaşılan klasörleri kullanarak dosya alışverişi yaparken veri şifreleme kullanıyorsa hatalı pozitiflerin miktarını azaltabilir. Örneğin, Davranış Tespiti, kullanıcı paylaşılan bir klasörde ENC uzantılı dosyalarla çalıştığında hatalı pozitif sonuçlara neden olabilir. Bu etkinlik türü, dış şifreleme için tipik olan bir davranış kalıbıyla eşleşir. Verileri korumak için paylaşılan bir klasörde şifrelenmiş dosyalarınız varsa o klasörü istisnalara ekleyin.

Harici şifreleme girişimlerinin işlenmemesi gereken bilgisayarları da hariç tutabilirsiniz.

Yönetim Konsolu'nda (MMC) bir koruma kapsamı nasıl düzenlenir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.
4. **Koruma kapsamı** bloğunda, **Yalnızca belirtilen paylaşılan klasörler** öğesini seçin.
5. Klasörler listesinden **Ekle**'ye tıklayın.
6. Bir pencere açılır; bu pencerede koruma kapsamına dahil etmek istediğiniz paylaşımlı klasörün yolunu girin (örneğin `C:\Share`).

   Koruma kapsamına paylaşılan bir klasör eklemek için yerel bir yol kullanın.

7. **Tamam**'a tıklayın.
8. Gerekirse, koruma kapsamı istisnalarını tanımlayın:
   a. **Tarama istisnaları** bloğunda, **Maskeye göre** düğmesine tıklayın.
   b. Açılan pencerede **Ekle** düğmesine tıklayın.
   c. Görüntülenen pencerede, `*.<file extension>` biçiminde bir dosya uzantısı veya bir klasör yolu belirtin. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

      Uygulama bazı istisna dosya uzantılarını desteklemez. Bu yüzden, `*.docx` or `**\Folder\**` şeklinde bir istisna belirleyebilirsiniz.

Bir nesneyi, koruma kapsamındaki nesneler listesinden kaldırmadan taramanın dışında bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

9. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir koruma kapsamı nasıl düzenlenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması** → **Davranış Analizi** → **Şifreleyici Önleyici** bölümüne gidin.
5. **Koruma kapsamı** bloğunda, **Yalnızca belirtilen paylaşılan klasörler** öğesini seçin.
6. Klasörler listesinden **Ekle**'ye tıklayın.
7. Bir pencere açılır; bu pencerede koruma kapsamına dahil etmek istediğiniz paylaşımlı klasörün yolunu girin (örneğin `C:\Share`).

   > Koruma kapsamına paylaşılan bir klasör eklemek için yerel bir yol kullanın.

8. **Tamam**'a tıklayın.
9. Gerekirse, koruma kapsamı istisnalarını tanımlayın:

   a. Pencerenin üst kısmında **Tarama istisnaları** bağlantısına tıklayın.

   b. Açılan pencerede **Ekle** düğmesine tıklayın.

   c. Görüntülenen pencerede, `*.<file extension>` biçiminde bir dosya uzantısı veya bir klasör yolu belirtin. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

   Uygulama bazı istisna dosya uzantılarını desteklemez. Bu yüzden, `*.docx` or `**\Folder\**` şeklinde bir istisna belirleyebilirsiniz.

   Bir nesneyi, koruma kapsamındaki nesneler listesinden kaldırmadan taramanın dışında bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

10. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir koruma kapsamı nasıl düzenlenir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.
3. **Koruma kapsamı** bloğunda, **Yalnızca belirtilen paylaşılan klasörler** öğesini seçin.
4. Klasörler listesinden **Ekle**'ye tıklayın.

5. Bir pencere açılır; bu pencerede koruma kapsamına dahil etmek istediğiniz paylaşımlı klasörün yolunu girin (örneğin `C:\Share`).

   > Koruma kapsamına paylaşılan bir klasör eklemek için yerel bir yol kullanın.

6. **Tamam**'a tıklayın.

7. Gerekirse, koruma kapsamı istisnalarını tanımlayın:

   a. Pencerenin üst kısmında, **Maskeye göre istisnalar** bağlantısına tıklayın.

   b. Açılan pencerede **Ekle** düğmesine tıklayın.

   c. Görüntülenen pencerede, `*.<file extension>` biçiminde bir dosya uzantısı veya bir klasör yolu belirtin. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

   Uygulama bazı istisna dosya uzantılarını desteklemez. Bu yüzden, `*.docx` or `**\Folder\**` şeklinde bir istisna belirleyebilirsiniz.

   Bir nesneyi, koruma kapsamındaki nesneler listesinden kaldırmadan taramanın dışında bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

8. Değişikliklerinizi kaydedin.

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.

3. **İstisnalar** bloğunda, **İstisnaları yönet** bağlantısını tıklayın.

4. **Ekle**'ye tıklayın.

5. **Gözat**'a tıklayın ve paylaşım klasörünü seçin.

   Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler:

   - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

   - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

   - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

   Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `?:\Users\*\Folder\` maskesini girin.

6. **Koruma bileşenleri** bloğundan **Davranış Tespiti** bileşenini seçin.

7. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

8. İstisna için **Etkin** durumu seçin.

   İstediğiniz zaman bir istisnayı durdurmak için geçiş düğmesini kullanabilirsiniz.

9. Değişikliklerinizi kaydedin.

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenilir Bölge** bölümüne gidin.

5. Açılan pencerede **Kötü Amaçlı Yazılım Tarama istisnaları** bağlantısına tıklayın.

6. Şirketteki tüm bilgisayarlar için birleştirilmiş bir istisnalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki istisnaların listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki istisnalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin istisnalarının değiştirilmesi veya silinmesi mümkün değildir.

7. Kullanıcının yerel bir istisnalar listesi oluşturmasını sağlamak istiyorsanız, **Yerel istisnaların kullanılmasına izin ver** onay kutusunu seçin. Bu şekilde, bir kullanıcı, ilkede oluşturulan genel istisnalar listesine ek olarak kendi yerel istisnalar listesini de oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan istisnaların genel listesine erişebilir. Ayrıca, bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, uygulamanın kullanıcı arabirimindeki birleştirilmiş tarama istisnaları listesini gizler.

8. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Tarama istisnalarını ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir tarama istisnası ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir tarama istisnası ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış tarama istisnalarını* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış tarama istisnaları eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış tarama istisnalarını seçmelisiniz.

9. İstisnayı nasıl eklemek istediğinizi seçin: **Dosya veya klasörün yolu**.

10. Paylaşılan klasörün yolunu girin.

Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler:

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

- İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `C:\Users\*\Folder\` maskesini girin.

11. **İstisnayı şunlara uygula** bloğundan **Davranış Tespiti** bileşenini seçin.

12. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

13. İstisna için **İstisnaya ekle** durumu seçin.

    İstediğiniz zaman bir istisnayı durdurmak için geçiş düğmesini kullanabilirsiniz.

14. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.

4. **Tarama istisnaları ve güvenilir uygulamalar** → **Tarama istisnaları** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, istisnaların listesini içeren bir pencere açar.

5. Şirketteki tüm bilgisayarlar için birleştirilmiş bir istisnalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki istisnaların listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki istisnalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin istisnalarının değiştirilmesi veya silinmesi mümkün değildir.

6. Kullanıcının yerel bir istisnalar listesi oluşturmasını sağlamak istiyorsanız, **Yerel istisnaların kullanılmasına izin ver** onay kutusunu seçin. Bu şekilde, bir kullanıcı, ilkede oluşturulan genel istisnalar listesine ek olarak kendi yerel istisnalar listesini de oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan istisnaların genel listesine erişebilir. Ayrıca, bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, uygulamanın kullanıcı arabirimindeki birleştirilmiş tarama istisnaları listesini gizler.

7. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Tarama istisnalarını ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir tarama istisnası ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir tarama istisnası ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış tarama istisnalarını* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış tarama istisnaları eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış tarama istisnalarını seçmelisiniz.

8. **Ekle**'ye tıklayın.

9. **Özellikler** bloğunda **Dosya veya klasör** onay kutusunu işaretleyin.

10. **Dosya veya klasör adı** penceresinde **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğunda **Dosya veya klasör seç** bağlantısına tıklayın.

11. **Gözat**'a tıklayın ve paylaşım klasörünü seçin.

    Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler:

    - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

    - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

    - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

    Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `?:\Users\*\Folder\` maskesini girin.

12. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

13. **Koruma bileşenleri** penceresini açmak için **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğundaki bağlantıya tıklayın.

14. **Davranış Tespiti** bileşeninin yanındaki onay kutusunu seçin.

15. Değişikliklerinizi kaydedin.

Harici veri şifreleme için güvenilir bilgisayarlar ekleme

Kuruluşunuz dosya alışverişi iş akışında harici veri şifrelemesi kullanıyorsa, bir güvenilen bilgisayarlar listesi oluşturmanız gerekir. Kaspersky Endpoint Security, güvenilir bilgisayarlar tarafından veri şifrelemeyi izlemez.

Oturum Açı Denetle hizmetinin, paylaşılan klasörlerin dış şifrelemeye karşı korunmasına karşı istisnaları etkinleştirmek amacıyla etkinleştirilmesi gerekir. Varsayılan olarak Oturum Açı Denetle hizmeti devre dışıdır (Oturum Açı Denetle hizmetini etkinleştirme hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin).

Uzak bilgisayar, Kaspersky Endpoint Security başlatılmadan önce açıldıysa paylaşılan klasör korumasından adresleri hariç tutma işlevselliği bu uzak bilgisayarda çalışmaz. Paylaşılan klasör korumasından adresleri hariç tutma işlevselliğinin bu uzak bilgisayarda çalıştığından emin olmak için bu uzak bilgisayarı, Kaspersky Endpoint Security başlatıldıktan sonra yeniden başlatabilirsiniz.

Yönetim Konsolu'nda (MMC) harici veri şifreleme için güvenilen bir bilgisayar nasıl eklenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.
5. **Tarama istisnaları** bloğunda, **Ada veya IP adresine göre** düğmesine tıklayın.
6. Açılan pencerede, **Ada veya IP adresine göre** düğmesine tıklayın.
7. Harici şifreleme girişimlerinin işlenmemesi gereken bilgisayarların IP adreslerini, IP adres aralığını veya adlarını girin.
   Örnekler:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Kaspersky Security Center Web Console'da verilerin harici olarak şifrelenmesi için güvenilir bilgisayar ekleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenilir Bölge** bölümüne gidin.
5. Pencerenin sağ kısmında **Şifreleyici Önleyici istisnaları** bağlantısına tıklayın.
6. Açılan pencerede **Ekle** düğmesine tıklayın.
7. Harici şifreleme girişimlerinin işlenmemesi gereken bilgisayarların IP adreslerini, IP adres aralığını veya adlarını girin.
   Örnekler:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde harici veri şifreleme için güvenilen bir bilgisayar nasıl eklenir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.
3. Pencerenin üst kısmında, **Ad veya IP adresine göre istisnalar** bağlantısına tıklayın.
4. Açılan pencerede **Ekle** düğmesine tıklayın.
5. Harici şifreleme girişimlerinin işlenmemesi gereken bilgisayarların IP adreslerini, IP adres aralığını veya adlarını girin.
   Örnekler:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
6. Değişikliklerinizi kaydedin.

Paylaşılan klasörlerin dış şifrelemeye karşı korunması istisnalarının listesini içe/dışa aktarma

Dışlama listesini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda adres eklemek için dosyayı değiştirebilirsiniz. İstisnalar listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

Yönetim Konsolunda (MMC) bir dışlama listesi nasıl içe ve dışa aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Gelişmiş Tehdit Koruması** → **Şifreleyici Önleyici** seçimini yapın.
4. **Tarama istisnaları** bloğunda, **Ada veya IP adresine göre** düğmesine tıklayın.
5. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
      Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.
   b. → **Dışa aktar** düğmesine tıklayın.
   c. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
      Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.
6. İstisnalar listesini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
   b. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.
   c. Dosyayı aç.
      Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.
7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bir istisnalar listesinş dışa aktarma ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.

4. **Ana Bilgisayar Tehdit Koruması** → **Davranış Analizi** → **Şifreleyici Önleyici** bölümüne gidin.
5. **Ad veya IP adresine göre istisnalar** bağlantısına tıklayın.
6. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin.
   b. → **Dışa aktar** düğmesine tıklayın.
   Kaspersky Endpoint Security, istisnalar listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.
7. İstisnalar listesini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
   Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.
   b. Dosyayı aç.
   Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.
8. Değişikliklerinizi kaydedin.

Düzeltme Altyapısı

Düzeltme Altyapısı, Kaspersky Endpoint Security' bileşeninin işletim sisteminde zararlı yazılımların gerçekleştirdiği etkinlikleri geri almasını sağlar.

Kaspersky Endpoint Security, işletim sistemindeki zararlı yazılım etkinliğini geri alırken aşağıdaki zararlı yazılım türlerine işlem yapar:

- **Dosya etkinliği**
  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:
  - Zararlı yazılımlar tarafından oluşturulan yürütülebilir dosyaları (ağ sürücüleri hariç tüm ortamlardakileri) siler.
  - Zararlı yazılımların sızdığı programlar tarafından oluşturulmuş yürütülebilir dosyaları siler.
  - Zararlı yazılımlar tarafından değiştirilmiş veya silinmiş dosyaları geri yükler.

  Dosya kurtarma özelliğinin bazı sınırlamaları vardır.
- **Kayıt defteri etkinliği**
  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:
  - Zararlı yazılımlar tarafından oluşturulmuş kayıt defteri anahtarlarını siler.
  - Zararlı yazılımlar tarafından değiştirilmiş veya silinmiş kayıt defteri anahtarlarını geri yüklemez.
- **Sistem etkinliği**

Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

- Zararlı yazılımlar tarafından başlatılmış işlemleri sonlandırır.
- Zararlı uygulamaların girdiği işlemleri sonlandırır.
- Zararlı yazılımlar tarafından durdurulan işlemleri sürdürmez.

- **Ağ etkinliği**

  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

  - Zararlı yazılımların ağ etkinliğini engeller.
  - Zararlı yazılımların sızdığı işlemlerin ağ etkinliğini engeller.

Zararlı yazılım eylemlerini geri alma işlemi Dosya Tehdidi Koruması veya Davranış Tespiti bileşeni tarafından ya da kötü amaçlı yazılım 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.

Yönetim Konsolu'nda (MMC) Düzeltme Altyapısı bileşeni nasıl etkinleştirilir veya devre dışı bırakılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Gelişmiş Tehdit Koruması → Düzeltme Altyapısı** seçimini yapın.
4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Düzeltme Altyapısı** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Düzeltme Altyapısı bileşenini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Ana Bilgisayar Tehdit Koruması → Davranış Analizi → Düzeltme Altyapısı** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Düzeltme Altyapısı ETKİN** anahtarını kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Düzeltme Altyapısı bileşenini etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Düzeltme Altyapısı**'nı seçin.

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Düzeltme Altyapısı** geçiş düğmesini kullanın.

4. Değişikliklerinizi kaydedin.

Sonuç olarak, Düzeltme Altyapısı etkinleştirilirse, Kaspersky Endpoint Security, işletim sistemindeki zararlı uygulamalar tarafından gerçekleştirilen eylemleri geri alır.

Kaspersky Security Network

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.

KSN işlevselliği ABD'de yazılımda kullanılabilir olmayabilir.

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. Kaspersky Security Network'e katılıyorsanız, KSN hizmetleri Kaspersky Endpoint Security'ye taranan web adreslerinin itibarı hakkında bilgi ve taranan dosyaların kategorisi ve tanınırlığı hakkında bilgi sağlar. KSN'ye erişim ayarları hakkında daha fazla ayrıntı için Kaspersky Security Center Yardım bölümüne bakın.

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.

KSN'ye katılım sırasında oluşturulan istatistiksel bilgilerin Kaspersky'ye gönderilmesi ve bu bilgilerin depolanması ve imhası hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Network Bildirimi'ne ve Kaspersky web sitesi'ne başvurun. Kaspersky Security Network Bildirimi metnine sahip ksn_<dil kodu>.txt dosyası dağıtım kitinde mevcuttur.

Kaspersky tanınırlık veritabanlarının altyapısı

Kaspersky Endpoint Security, Kaspersky tanınırlık veritabanlarıyla çalışmak için şu altyapı çözümlerini destekler:

- *Kaspersky Security Network (KSN)*, çoğu Kaspersky uygulaması tarafından kullanılan çözümdür. KSN katılımcıları Kaspersky'denbilgiler alır ve kullanıcının bilgisayarında tespit edilen nesneler hakkındaki Kaspersky bilgilerini, Kaspersky analistleri tarafından ek analize tabi tutulması ve tanınırlık ve istatistiksel veritabanlarına dahil edilmesi için gönderir.

- *Kaspersky Private Security Network (KPSN),* Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür. KPSN, aşağıdaki sebeplerden herhangi birinden ötürü Kaspersky Security Network'e katılamayan kurumsal müşteriler için tasarlanmıştır:

  - Yerel iş istasyonları İnternet'e bağlı değildir.

  - Verilerin ülke ya da kurumsal LAN dışına aktarılması yasalarca yasaklanmış ya da kurumsal güvenlik politikaları nedeniyle kısıtlanmıştır.

Kaspersky Security Network'ün kullanımını etkinleştirme ve devre dışı bırakma

Kaspersky Endpoint Security varsayılan olarak Genişletilmiş KSN modunu kullanır. *Genişletilmiş KSN modu*, Kaspersky Endpoint Security'nin Kaspersky'ye daha fazla veri gönderdiği bir moddur.

Yönetim Konsolu'nda (MMC) KSN Kullanımını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Gelişmiş Tehdit Koruması** → **Kaspersky Security Network**'yi seçin.

4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Kaspersky Security Network** geçiş düğmesini kullanın.

   KSN kullanımını etkinleştirdiyseniz Kaspersky Endpoint Security, Kaspersky Security Network Bildirimi'ni görüntüler. Kabul ediyorsanız lütfen Kaspersky Security Network (KSN) Bildirimi kullanım şartlarını okuyun ve kabul edin.

5. **Genişletilmiş KSN modunu etkinleştir** onay kutusunun işaretini kaldırın. Varsayılan olarak, genişletilmiş KSN modu etkindir.

6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da KSN Kullanımını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Kaspersky Security Network**'e gidin.

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Kaspersky Security Network (KSN) Kullanımı ETKİN** anahtarını kullanın.

   KSN kullanımını etkinleştirdiyseniz Kaspersky Endpoint Security, Kaspersky Security Network Bildirimi'ni görüntüler. Kabul ediyorsanız lütfen Kaspersky Security Network (KSN) Bildirimi kullanım şartlarını okuyun ve kabul edin.

6. Gerekirse **Genişletilmiş KSN modunu kullan** anahtarını kapalı konuma getirin. Varsayılan olarak, genişletilmiş KSN modu etkindir.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde KSN Kullanımını etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Kaspersky Security Network** seçimini yapın.

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Kaspersky Security Network** geçiş düğmesini kullanın.

   KSN kullanımını etkinleştirdiyseniz Kaspersky Endpoint Security, Kaspersky Security Network Bildirimi'ni görüntüler. Kabul ediyorsanız lütfen Kaspersky Security Network (KSN) Bildirimi kullanım şartlarını okuyun ve kabul edin.

4. Gerekirse **Genişletilmiş KSN modunu etkinleştir** geçiş düğmesini kapalı konuma getirin. Varsayılan olarak, genişletilmiş KSN modu etkindir.

5. Değişikliklerinizi kaydedin.

Sonuç olarak, KSN kullanımı etkinleştirilirse Kaspersky Endpoint Security, Kaspersky Security Network'ten alınan dosyaların, internet kaynaklarının ve uygulamaların tanınırlıkları hakkındaki bilgileri kullanır.

Kaspersky Private Security Network'ün sınırlamaları

Kaspersky Private Security Network (KPSN), Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür. Kaspersky Private Security Network, nesnelerin (dosyalar veya web adresleri) tanınırlığını kontrol etmek için kendi yerel tanınırlık veritabanınızı kullanmanıza olanak tanır. Yerel tanınırlık veritabanına eklenen bir nesnenin tanınırlığı, KSN/KPSN'ye eklenenden daha yüksek önceliğe sahiptir. Örneğin, Kaspersky Endpoint Security'nin bir bilgisayarı taradığını ve KSN/KPSN'deki bir dosyanın tanınırlığını talep ettiğini düşünün. Dosyanın yerel tanınırlık veritabanında *Güvenilmez* bir tanınırlığı varsa ancak KSN/KPSN'de *Güvenilir* bir tanınırlığa sahipse, Kaspersky Endpoint Security dosyayı *Güvenilmez* olarak algılar ve algılanan tehditler için tanımlanan eylemi gerçekleştirir.

Ancak, bazı durumlarda Kaspersky Endpoint Security, KSN/KPSN'deki bir nesnenin tanınırlığını talep etmeyebilir. Böyle bir durumda Kaspersky Endpoint Security, KPSN'nin yerel tanınırlık veritabanından veri almayacaktır. Aşağıdaki sebeplerden dolayı Kaspersky Endpoint Security, KSN/KPSN'deki bir nesnenin tanınırlığını talep etmeyebilir:

- Kaspersky uygulamaları çevrimdışı tanınırlık veritabanlarını kullanıyor. Çevrimdışı tanınırlık veritabanları, Kaspersky uygulamalarının çalışması sırasında kaynakları optimize etmek ve bilgisayardaki kritik öneme sahip nesneleri korumak için tasarlanmıştır. Çevrimdışı tanınırlık veritabanları, Kaspersky Security Network'ten gelen verilere dayalı olarak Kaspersky uzmanları tarafından oluşturulur. Kaspersky uygulamaları, çevrimdışı tanınırlık veritabanlarını belirli bir uygulamanın antivirüs veritabanları ile günceller. Çevrimdışı tanınırlık veritabanları taranan bir nesne hakkında bilgi içeriyorsa, uygulama KSN/KPSN'den bu nesnenin tanınırlığını talep etmez.

- Tarama istisnaları (güvenilen bölge) uygulama ayarlarında yapılandırılır. Böyle bir durumda uygulama, nesnenin yerel tanınırlık veritabanındaki tanınırlığını hesaba katmaz.

- Uygulama, iSwift veya iChecker gibi tarama optimizasyon teknolojilerini kullanır veya KSN /KPSN'ye yapılan tanınırlık isteklerini önbellekler. Durum böyleyse, uygulama daha önce taranmış nesnelerin tanınırlığını talep etmeyebilir.

- Uygulama, iş yükünü optimize etmek için belirli bir biçim ve boyuttaki dosyaları tarar. İlgili biçimlerin listesi ve boyut sınırları Kaspersky uzmanları tarafından belirlenir. Bu liste, uygulamanın anti-virüs veritabanları ile güncellenir. Uygulama arabiriminde, örneğin Dosya Tehdidi Koruması bileşeni için tarama optimizasyon ayarlarını da yapılandırabilirsiniz.

- Light Agent modundaki Kaspersky Endpoint Security, KSN sunucularıyla bir KSN proxy sunucusu aracılığıyla iletişim kurar. KSN ile doğrudan iletişim desteklenmez.

Koruma bileşenleri için bulut modunu etkinleştirme ve devre dışı bırakma

Bulut modu, Kaspersky Endpoint Security'nin anti-virüs veritabanlarının daha basit bir sürümünü kullandığı uygulama çalışma moduna karşılık gelir. Kaspersky Security Network, uygulamanın basit anti-virüs veritabanlarını kullanarak çalışmasını destekler. Anti-virüs veritabanlarının basit sürümü ile kullanılan RAM miktarı, normal veritabanları ile kullanılan RAM miktarının yaklaşık olarak yarısıdır. Kaspersky Security Network'e katılmazsanız ya da bulut modu devre dışı bırakılırsa, Kaspersky Endpoint Security Kaspersky sunucularından anti-virüs veritabanlarının en son sürümünü indirir.

Kaspersky Private Security Network'ü kullanırken bulut modu işlevselliği Kaspersky Private Security Network sürüm 3.0'dan başlayarak kullanılabilir.

Uygulama Light Agent modunda çalışıyorsa Bulut modu kullanılamaz.

Yönetim Konsolu'nda (MMC) koruma bileşenleri için bulut modunu etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Gelişmiş Tehdit Koruması** → **Kaspersky Security Network**'yi seçin.

4. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Bulut modunu etkinleştir** kutucuğunu işaretleyin.
5. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da koruma bileşenleri için bulut modunu etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kaspersky Security Network**'e gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Bulut modunu kullan** anahtarını kullanın.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde koruma bileşenleri için bulut modunu etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Kaspersky Security Network** seçimini yapın.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Bulut modunu etkinleştir** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security, bir sonraki güncelleme sırasında antivirüs veritabanlarının basit bir sürümünü veya tam sürümünü indirir.

> Antivirüs veritabanlarının basit sürümü kullanıma açık değilse Kaspersky Endpoint Security otomatik olarak antivirüs veritabanlarının üst düzey sürümüne geçer.

KSN Proxy ayarları

Kaspersky Security Center Yönetim Sunucusu tarafından yönetilen kullanıcı bilgisayarları, KSN ile doğrudan ya da KSN Proxy hizmeti aracılığıyla etkileşime girebilir.

> Uygulama Light Agent modunda çalışıyorsa KSN ile doğrudan iletişim desteklenmez. Kaspersky Endpoint Security, KSN sunucularıyla bir KSN proxy sunucusu aracılığıyla iletişim kurar.

KSN Proxy hizmeti aşağıdaki özellikleri sunar:

- Kullanıcının bilgisayarı, doğrudan İnternet erişimi olmadan bile KSN'ye soru sorabilir ve KSN'ye bilgi gönderebilir.
- KSN Proxy hizmeti işlenmiş verileri önbelleğe alır, böylece dış ağ iletişim kanalının üzerindeki yükü azaltır ve kullanıcının bilgisayarı tarafından istenen bilginin alınmasını hızlandırır.

Varsayılan olarak, KSN etkinleştirildikten ve KSN Bildirimi kabul edildikten sonra uygulama, Kaspersky Security Network'e bağlanmak için bir proxy sunucusu kullanır. Uygulama tarafından kullanılan proxy sunucusu, 13111 numaralı TCP portuna sahip Kaspersky Security Center Yönetim Sunucusu'dur. Bu nedenle, KSN Proxy kullanılabilir olmadığında aşağıdakileri doğrulamanız gerekir:

- Yönetim Sunucusunda `ksnproxy` hizmetinin çalıştığı.
- Bilgisayardaki Güvenlik Duvarının 13111 numaralı portunu engellemediği.

KSN Proxy akullanımını şu şekilde yapılandırabilirsiniz: KSN Proxy'yi etkinleştirin veya devre dışı bırakın ve bağlantı için portunu yapılandırın. Bunu yapmak için Yönetim Sunucusu özelliklerini açmanız gerekir. KSN Proxy yapılandırması hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun. Kaspersky Endpoint Security ilkesinde, ayrı bilgisayarlar için de KSN Proxy'yi etkinleştirebilir veya devre dışı bırakabilirsiniz.

Yönetim Konsolu'nda (MMC) KSN Proxy'yi etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Gelişmiş Tehdit Koruması → Kaspersky Security Network**'yi seçin.
4. KSN Proxy'yi etkinleştirmek veya devre dışı bırakmak için **KSN Proxy Ayarları** bloğundaki **Yönetim Sunucusunu KSN proxy sunucusu olarak kullan** onay kutusunu kullanın.
5. Gerekirse, **KSN proxy sunucusu kullanılamıyorsa Kaspersky Security Network sunucularını kullan** onay kutusunu seçin.

   Onay kutusu işaretlenirse Kaspersky Endpoint Security, KSN Proxy hizmeti kullanılabilir olmadığında KSN sunucularını kullanır. KSN sunucuları hem Kaspersky'nin tarafında hem de üçüncü taraflar tarafında bulunabilir (Kaspersky Private Security Network kullanıldığında).
6. Değişikliklerinizi kaydedin.

Web Console'da KSN Proxy'yi etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar → Kaspersky Security Network**'e gidin.
5. KSN Proxy'yi etkinleştirmek veya devre dışı bırakmak için **Yönetim Sunucusunu KSN proxy sunucusu olarak kullan** onay kutusu.
6. Gerekirse, **KSN proxy sunucusu kullanılamıyorsa Kaspersky Security Network sunucularını kullan** onay kutusunu seçin.

   Onay kutusu işaretlenirse Kaspersky Endpoint Security, KSN Proxy hizmeti kullanılabilir olmadığında KSN sunucularını kullanır. KSN sunucuları hem Kaspersky'nin tarafında hem de üçüncü taraflar tarafında bulunabilir (Kaspersky Private Security Network kullanıldığında). Varsayılan olarak, onay kutusu temizlenmiştir.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

KSN Proxy adresi, Yönetim Sunucusu adresiyle eşleşir. Yönetim Sunucusu etki alanı adı değiştirildiğinde, KSN Proxy adresini manuel olarak güncellemeniz gerekir.

KSN Proxy adresini yapılandırmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacından **Gelişmiş** → **Uzaktan kurulum** → **Kurulum paketleri** klasörünü seçin.
3. **Kurulum paketleri** klasörünün bağlam menüsünden **Özellikler**'i seçin.
4. Açılan penceredeki **Genel** sekmesinde, KSN proxy sunucusunun yeni adresini belirtin.
5. Değişikliklerinizi kaydedin.

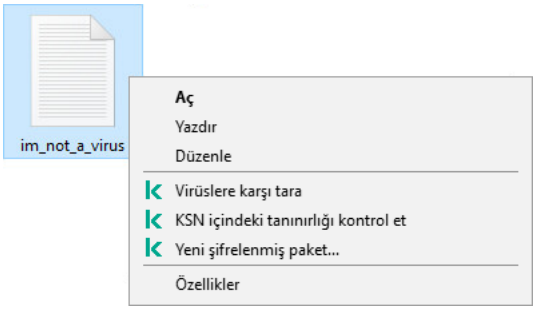
Kaspersky Security Network'den bir dosyanın saygınlığını kontrol etme

Bir dosyanın güvenliği konusunda şüpheleriniz olması durumunda, Kaspersky Security Network'te bu dosyanın tanınırlığını kontrol edebilirsiniz.

Kaspersky Security Network Bildirimi şartlarını kabul ettiyseniz bir dosyanın tanınırlığını kontrol edebilirsiniz.

Kaspersky Security Network'den bir dosyanın tanınırlığını kontrol etmek için:

İçerik menüsünü açın ve **KSN'de tanınırlığı denetle** seçeneğini seçin (aşağıdaki resme bakın).



Dosya bağlam menüsü

Kaspersky Endpoint Security tanınırlığı görüntüler:

Güvenilir (Kaspersky Security Network). Aşağıdaki koşullardan biri veya daha fazlası karşılanırsa uygulama bir dosyayı güvenilir olarak kabul eder:

- dosya güvenilir bir satıcı tarafından dijital olarak imzalanmışsa;
- dosya Kaspersky Security Network'te güvenilir bir itibara sahipse;
- kullanıcı dosyayı Güvenilir grubuna yerleştirmişse.

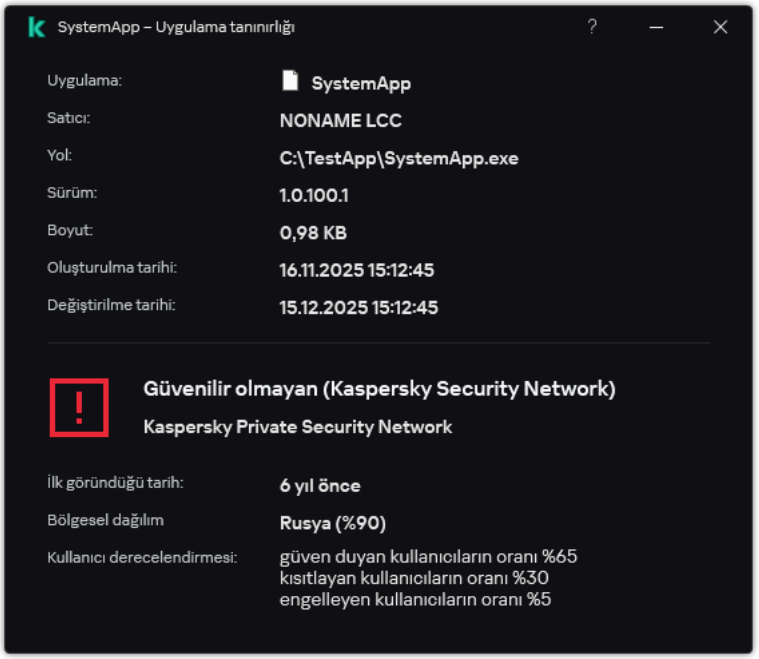
İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım. Kötü amaçlı işlevler içermese bile bu uygulamalar saldırganlar tarafından kullanılabilir. Suçlular tarafından bir kullanıcının bilgisayarına veya kişisel verilerine zarar vermek amacıyla kullanılabilecek yasal yazılımlarla ilgili ayrıntılar için lütfen Kaspersky IT Ansiklopedisi web sitesine bakın. Bu uygulamaları güvenilir listeye ekleyebilirsiniz.

Güvenilir olmayan (Kaspersky Security Network). Bir virüs ya da bir tehdit teşkil eden başka bir uygulama.

Bilinmeyen (Kaspersky Security Network). Kaspersky Security Network dosya hakkında herhangi bir bilgiye sahip değildir. Bir dosyayı antivirüs veritabanlarını kullanarak tarayabilirsiniz (bağlam menüsündeki **Virüslere karşı tara** seçeneği).

Kaspersky Endpoint Security, dosyanın tanınırlığı belirlemek için kullanılan KSN çözümünü görüntüler: *Kaspersky Security Network* veya *Kaspersky Private Security Network*.

Kaspersky Endpoint Security aynı zamanda dosya hakkında ek bilgiler de görüntüler (aşağıdaki resme bakın).



Bir dosyanın Kaspersky Security Network'deki tanınırlığını

Şifreli bağlantıları tarama

Yükleme sonrasında, Kaspersky Endpoint Security, Kaspersky sertifikasını güvenilir sertifikaların sistem depolamasına ekler (Windows sertifika deposu). Kaspersky Endpoint Security, şifrelenmiş bağlantıları taramak için bu sertifikayı kullanır. Kaspersky Endpoint Security ayrıca, bu uygulamaların trafiğini taramak için Firefox ve Thunderbird'te güvenilir sertifikaların sistem depolaması kullanımını kapsar.

İnternet Denetimi, Posta Tehdidi Koruması, Web Tehdidi Koruması, Davranış Tespiti ve Exploit Önleme bileşenleri, aşağıdaki iletişim kurallarını kullanarak şifrelenmiş bağlantılar üzerinden aktarılan ağ trafiğinin şifresini çözebilir ve bu ağ trafiğini tarayabilir:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Şifreli bağlantıları taramayı etkinleştirme

Kaspersky Endpoint Security varsayılan olarak şifrelenmiş bağlantıları her zaman değil, yalnızca koruma bileşenleri tarafından talep edildiğinde tarar.

Yönetim Konsolu'nda (MMC) şifreli bağlantıları taramayı etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
5. **Şifreli bağlantıları tarama** bloğunda, şifrelenmiş bağlantı tarama modunu seçin:
   - **Şifrelenmiş bağlantıları tara**. Kaspersky Endpoint Security, adresleri `https://` ile başlayan web sitelerinin içeriklerine erişmeyecektir.
   - **Koruma bileşenlerinden gelen talep üzerine şifrelenmiş bağlantıları tara**. Kaspersky Endpoint Security, şifrelenmiş trafiği sadece Web Tehdidi Koruması, Posta Tehdidi Koruması ve İnternet Denetimi bileşenleri tarafından istendiğinde tarayacaktır.
   - **Şifrelenmiş bağlantıları her zaman tara**. Kaspersky Endpoint Security şifrelenmiş ağ trafiğini, koruma bileşenleri devre dışı bırakılsa bile tarayacaktır.

   Kaspersky Endpoint Security, trafik taramanın devre dışı bırakıldığı güvenilir uygulamalar tarafından kurulan şifreli bağlantıları taramaz. Kaspersky Endpoint Security, önceden tanımlanmış güvenilir web siteleri listesinden şifrelenmiş bağlantıları taramaz. Önceden tanımlanmış güvenilir web siteleri listesi Kaspersky uzmanları tarafından oluşturulur. Bu liste, uygulamanın anti-virüs veritabanları ile güncellenir. Önceden tanımlanmış güvenilir web siteleri listesini yalnızca Kaspersky Endpoint Security arabiriminde görüntüleyebilirsiniz. Listeyi Kaspersky Security Center Konsolunda görüntüleyemezsiniz.
6. Gerekirse tarama istisnaları ekleyin: güvenilir internet adresleri ve uygulamalar.
7. Şifreli bağlantıları tarama için ayarları yapılandırın (aşağıdaki tabloya bakın).
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da şifreli bağlantıları taramayı etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.

5. **Şifreli Bağlantı Taraması** altında, **Şifreli Bağlantı Taraması ETKİN** anahtarını açık duruma getirin.

   Anahtar kapalı durumda olduğunda, Kaspersky Endpoint Security, adresleri `https://` ile başlayan web sitelerinin içeriklerine erişmez.

6. **Ayarlar** seçeneğine tıklayın ve şifreli bağlantı tarama modunu seçin:

   - **Koruma bileşenlerinden gelen talep üzerine şifrelenmiş bağlantıları tara**. Kaspersky Endpoint Security, şifrelenmiş trafiği sadece Web Tehdidi Koruması, Posta Tehdidi Koruması ve İnternet Denetimi bileşenleri tarafından istendiğinde tarayacaktır.

   - **Şifrelenmiş bağlantıları her zaman tara**. Kaspersky Endpoint Security şifrelenmiş ağ trafiğini, koruma bileşenleri devre dışı bırakılsa bile tarayacaktır.

   Kaspersky Endpoint Security, trafik taramanın devre dışı bırakıldığı güvenilir uygulamalar tarafından kurulan şifreli bağlantıları taramaz. Kaspersky Endpoint Security, önceden tanımlanmış güvenilir web siteleri listesinden şifrelenmiş bağlantıları taramaz. Önceden tanımlanmış güvenilir web siteleri listesi Kaspersky uzmanları tarafından oluşturulur. Bu liste, uygulamanın anti-virüs veritabanları ile güncellenir. Önceden tanımlanmış güvenilir web siteleri listesini yalnızca Kaspersky Endpoint Security arabiriminde görüntüleyebilirsiniz. Listeyi Kaspersky Security Center Konsolunda görüntüleyemezsiniz.

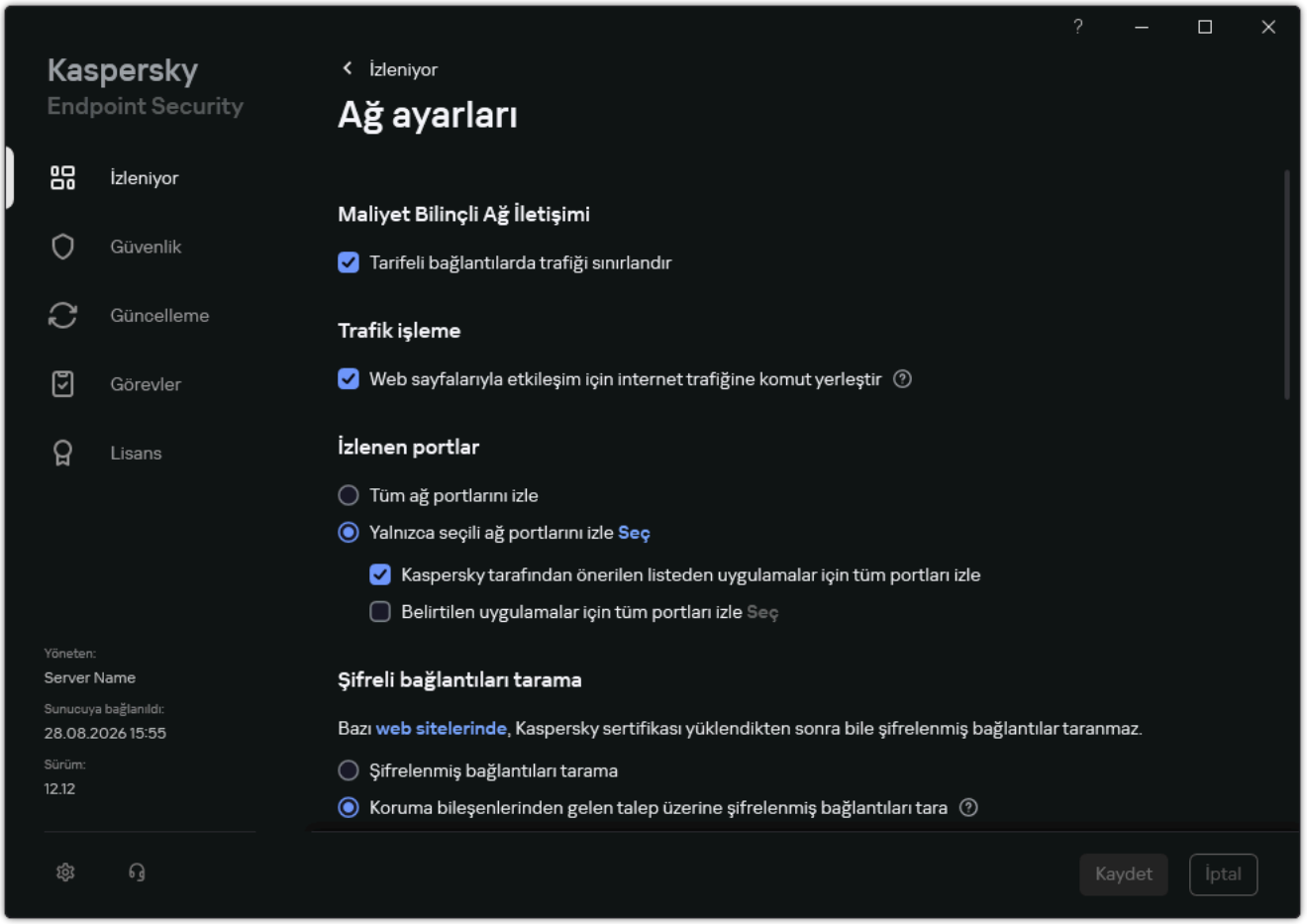
7. Gerekirse tarama istisnaları ekleyin: güvenilir internet adresleri ve uygulamalar.

8. Şifreli bağlantıları tarama için ayarları yapılandırın (aşağıdaki tabloya bakın).

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde şifreli bağlantıları taramayı etkinleştirme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



Şifreli bağlantıları tarama ayarları

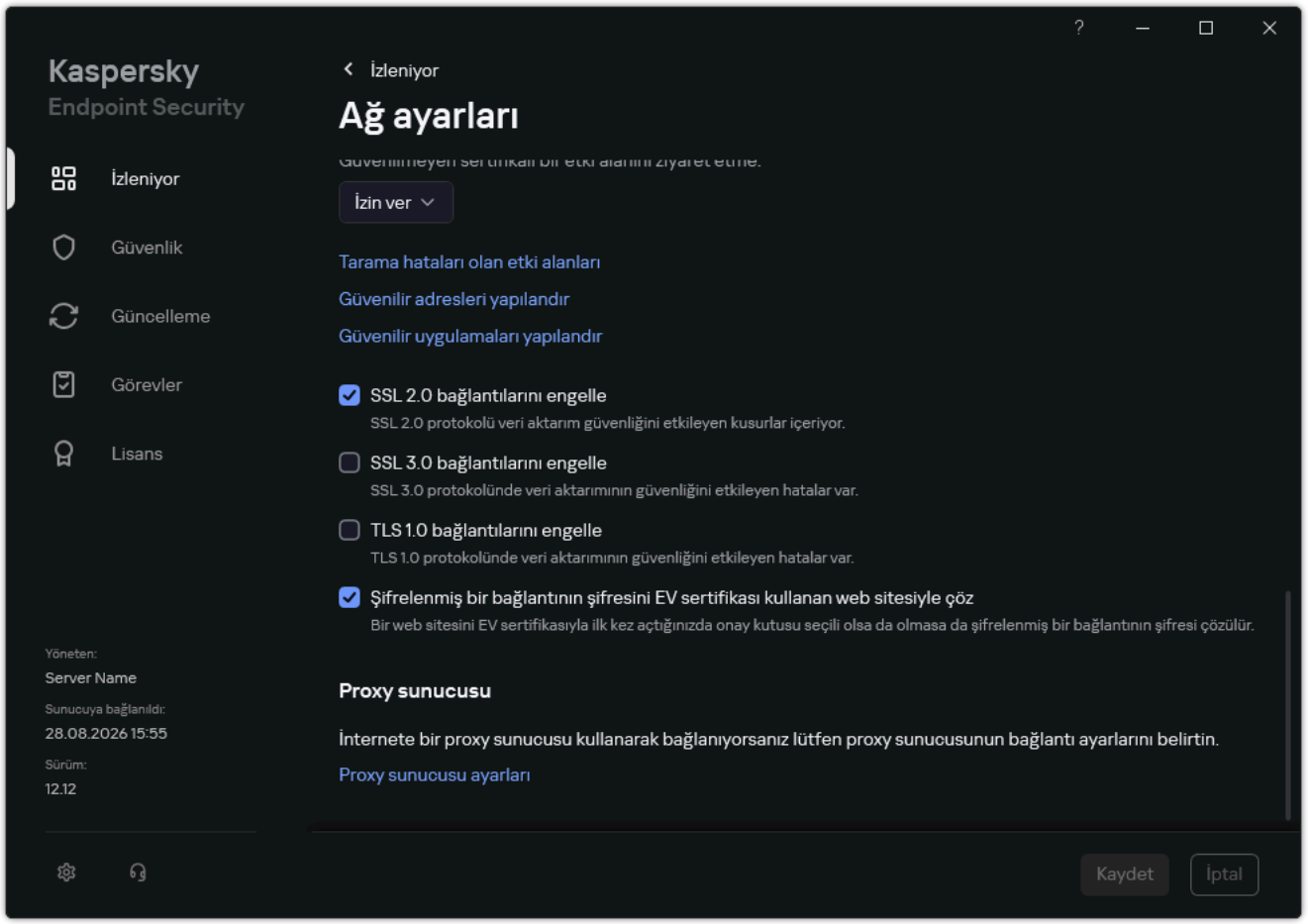
3. **Şifreli bağlantıları tarama** bloğunda, şifrelenmiş bağlantı tarama modunu seçin:

   - **Şifrelenmiş bağlantıları tarama**. Kaspersky Endpoint Security, adresleri `https://` ile başlayan web sitelerinin içeriklerine erişmeyecektir.
   - **Koruma bileşenlerinden gelen talep üzerine şifrelenmiş bağlantıları tara**. Kaspersky Endpoint Security, şifrelenmiş trafiği sadece Web Tehdidi Koruması, Posta Tehdidi Koruması ve İnternet Denetimi bileşenleri tarafından istendiğinde tarayacaktır.
   - **Şifrelenmiş bağlantıları her zaman tara**. Kaspersky Endpoint Security şifrelenmiş ağ trafiğini, koruma bileşenleri devre dışı bırakılsa bile tarayacaktır.

   Kaspersky Endpoint Security, trafik taramanın devre dışı bırakıldığı güvenilir uygulamalar tarafından kurulan şifreli bağlantıları taramaz. Kaspersky Endpoint Security, önceden tanımlanmış güvenilir web siteleri listesinden şifrelenmiş bağlantıları taramaz. Önceden tanımlanmış güvenilir web siteleri listesi Kaspersky uzmanları tarafından oluşturulur. Bu liste, uygulamanın anti-virüs veritabanları ile güncellenir. Önceden tanımlanmış güvenilir web siteleri listesini yalnızca Kaspersky Endpoint Security arabiriminde görüntüleyebilirsiniz. Listeyi Kaspersky Security Center Konsolunda görüntüleyemezsiniz.

4. Gerekirse tarama istisnaları ekleyin: güvenilir internet adresleri ve uygulamalar.

5. Şifreli bağlantıları tarama için ayarları yapılandırın (aşağıdaki tabloya bakın).



Şifreli bağlantıları taramak için ek ayarlar

6. Değişikliklerinizi kaydedin.

Şifreli bağlantıları tarama ayarları

Parametre	Açıklama
Güvenilir kök sertifikaları	Güvenilir kök sertifikalarının listesi. Kaspersky Endpoint Security, örneğin yeni bir sertifikalandırma merkezi kullanılma almanız gerektiğinde, güvenilir kök sertifikalarını yüklemenize izin verir. Uygulama Kaspersky Endpoint Security sertifika deposuna bir sertifika eklemenize izin verir. Bu durumda, sertifika sadece Kaspersky Endpoint Security uygulaması için güvenilir kabul edilir. Başka bir deyişle, kullanıcı tarayıcıdaki yeni bir sertifika ile bir web sitesine erişim kazanabilir. Başka bir uygulamanın web sitesine erişim kazanmaya çalışması durumunda, bir sertifika sorunu nedeniyle bir bağlantı hatası alabilirsiniz. Sistem sertifika deposuna eklemek için Active Directory grubu ilkelerini kullanabilirsiniz.
Güvenilmeyen sertifikalı bir etki alanını ziyaret etme	• **İzin ver**. Kaspersky Endpoint Security güvenilir olmayan bir sertifikaya sahip bir etki alanını ziyaret ederken ağ bağlantısı kurulmasına izin verir. Kaspersky Endpoint Security, güvenilmeyen bir sertifikaya sahip bir etki alanını tarayıcıda açarken bir uyarı ve bu etki alanının ziyaret edilmesinin neden önerilmediğini gösteren bir HTML sayfası gösterir. Kullanıcı, talep edilen internet kaynağına erişim elde etmek için HTML uyarı sayfasındaki bağlantıya tıklayabilir. Eğer bir üçüncü taraf uygulaması veya hizmeti güvenilmez bir sertifikaya sahip bir etki alanıyla bağlantı kurarsa, Kaspersky Endpoint Security trafiği taramak için kendi sertifikasını oluşturur. Yeni ilke *Güvenilmez* durumuna sahiptir. Bu, üçüncü taraf uygulamasını güvenilmez bağlantı hakkında uyarmak için gereklidir, çünkü bu durumda HTML sayfası görüntülenemez ve bağlantı arka plan modunda kurulabilir. • **Engelle**. Kaspersky Endpoint Security güvenilir olmayan bir sertifikaya sahip bir etki alanını ziyaret ederken ağ bağlantısı kurulmasını engeller. Kaspersky Endpoint Security, güvenilmeyen bir sertifikaya sahip bir etki alanını tarayıcıda açarken bu etki alanının neden engellendiğini gösteren bir HTML sayfası gösterir.
Şifrelenmiş bağlantı tarama hatası olan bir etki alanını ziyaret etme	• **Engelle**. Bir şifreli bağlantıları tarama hatası meydana geldiğinde, Kaspersky Endpoint Security, ağ bağlantısını engeller. • **İzin ver ve etki alanını istisnalara ekle**. Şifreli bağlantıları tarama hatası oluştuğunda Kaspersky Endpoint Security, hatayla sonuçlanan etki alanını tarama hatası olan etki alanları listesine ekler ve bu etki alanı ziyaret edildiğinde şifrelenmiş ağ trafiğini izlemez. Şifreli bağlantılar tarama hatalarına sahip etki alanlarının bir listesini sadece uygulamanın yerel arabiriminde görüntüleyebilirsiniz. Listenin içeriğini temizlemek için **Engelle**'i seçin. Kaspersky Endpoint Security ayrıca şifrelenmiş bağlantıları tarama hatası için bir olay oluşturur.
SSL 2.0 bağlantılarını engelle	Onay kutusu işaretlendiğinde, uygulama SSL 2.0 iletişim kuralı üzerinden kurulmuş ağ bağlantılarını izler ve engeller. Onay kutusunun işareti kaldırıldığında, uygulama SSL 2.0 iletişim kuralı üzerinden kurulan ağ bağlantılarını engellemez. Ancak, uygulama bu iletişim kuralı üzerinden ağ trafiğini izlemez.

Parametre	Açıklama
SSL 3.0 bağlantılarını engelle	Onay kutusu işaretlendiğinde, uygulama SSL 3.0 protokolü üzerinden kurulmuş ağ bağlantılarını engeller. Onay kutusunun işareti kaldırıldığında, uygulama SSL 3.0 iletişim kuralı üzerinden kurulan ağ bağlantılarını engellemez. Uygulama bu iletişim kuralı üzerinden ağ trafiğini izler. Uygulamanın tüm bileşenleri kısıtlama olmaksızın çalışır.
TLS 1.0 bağlantılarını engelle	Onay kutusu işaretlendiğinde, uygulama TLS 1.0 protokolü üzerinden kurulmuş ağ bağlantılarını engeller. Onay kutusunun işareti kaldırıldığında, uygulama TLS 1.0 iletişim kuralı üzerinden kurulan ağ bağlantılarını engellemez. Uygulama bu iletişim kuralı üzerinden ağ trafiğini izler. Uygulamanın tüm bileşenleri kısıtlama olmaksızın çalışır.
Şifrelenmiş bir bağlantının şifresini EV sertifikası kullanan web sitesiyle çöz	EV sertifikaları (Extended Validation Certificate), web sitelerinin gerçekliğini onaylar ve bağlantının güvenliğini artırır. Tarayıcılar, bir web sitesinin bir EV sertifikasına sahip olduğunu belirtmek için adres çubuğunda bir kilit simgesi görüntüler. Tarayıcılar ayrıca adres çubuğunu yeşil renkte de görüntüleyebilir. Bu kutucuk seçildiğinde, uygulama bir EV sertifikası kullanan web siteleriyle şifreli bağlantıların şifresini çözer ve izler. Bu kutucuğun işareti kaldırıldığında, uygulama HTTPS trafiğinin içeriğine erişemez. Bu nedenle, uygulama HTTPS trafiğini sadece web sitesi adresine göre izler, örneğin `https://bing.com`. EV sertifikasına sahip bir web sitesini ilk kez açıyorsanız, şifreli bağlantı bu kutucuğun işareti olup olmadığından bağımsız olarak çözülür.

Güvenilir kök sertifikalarının yüklenmesi

Kaspersky Endpoint Security, örneğin yeni bir sertifikalandırma merkezi kullanılma almanız gerektiğinde, güvenilir kök sertifikalarını yüklemenize izin verir. Uygulama Kaspersky Endpoint Security sertifika deposuna bir sertifika eklemenize izin verir. Bu durumda, sertifika sadece Kaspersky Endpoint Security uygulaması için güvenilir kabul edilir. Başka bir deyişle, kullanıcı tarayıcıdaki yeni bir sertifika ile bir web sitesine erişim kazanabilir. Başka bir uygulamanın web sitesine erişim kazanmaya çalışması durumunda, bir sertifika sorunu nedeniyle bir bağlantı hatası alabilirsiniz. Sistem sertifika deposuna eklemek için Active Directory grubu ilkelerini kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) güvenilir kök sertifikalarını yükleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
4. **Güvenilir kök sertifikaları** bloğundan **Ekle** düğmesine tıklayın.
5. Bu bir pencere açar; bu pencerede bir güvenilir kök sertifika seçin.
   Kaspersky Endpoint Security, PEM, DER ve CRT uzantılı sertifikaları destekler.
6. Değişikliklerinizi kaydedin.

Web Console'da güvenilir kök sertifikalarını yükleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.

5. **Güvenilir kök sertifikaları** bağlantısına tıklayın.
6. Bu bir pencere açar; bu pencerede **Ekle**'ye tıklayın ve bir güvenilir kök sertifika seçin.

   Kaspersky Endpoint Security, PEM, DER ve CRT uzantılı sertifikaları destekler.
7. Değişikliklerinizi kaydedin.

Uygulama arabiriminde güvenilir kök sertifikalarını yükleme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **Şifreli bağlantıları tarama** bloğunda **Sertifikaları görüntüle** düğmesine tıklayın.
4. Bu bir pencere açar; bu pencerede **Ekle**'ye tıklayın ve bir güvenilir kök sertifika seçin.

   Kaspersky Endpoint Security, PEM, DER ve CRT uzantılı sertifikaları destekler.
5. Değişikliklerinizi kaydedin.

Sonuç olarak, trafik taranırken, Kaspersky Endpoint Security sistem sertifika deposuna ek olarak kendi sertifika deposunu da kullanır.

Şifrelenmiş bağlantıları güvenilmeyen bir sertifikayla tarama

Yükleme sonrasında, Kaspersky Endpoint Security, Kaspersky sertifikasını güvenilir sertifikaların sistem depolamasına ekler (Windows sertifika deposu). Kaspersky Endpoint Security, şifrelenmiş bağlantıları taramak için bu sertifikayı kullanır. Geçersiz sertifikalı bir etki alanını ziyaret ederken, o etki alanına kullanıcı erişimine izin verebilir veya bunu reddedebilirsiniz (aşağıdaki talimatlara bakın).

Kullanıcının geçersiz sertifikalara sahip alanları ziyaret etmesine izin verdiyseniz Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

- *Tarayıcı* ile geçersiz sertifikalı bir etki alanını ziyaret ederken, Kaspersky Endpoint Security trafiği taramak için Kaspersky sertifikasını kullanır. Kaspersky Endpoint Security, ilgili etki alanını ziyaret etmenin neden önerilmediğine ilişkin bir uyarı ve bilgiler içeren bir HTML sayfası görüntüler (aşağıdaki resme bakın). Kullanıcı, talep edilen internet kaynağına erişim elde etmek için HTML uyarı sayfasındaki bağlantıya tıklayabilir. Bu bağlantıyı takip ettikten sonraki bir saat boyunca Kaspersky Endpoint Security, aynı etki alanındaki diğer kaynakların ziyaret edilmesi sırasında güvenilir olmayan sertifika ile ilgili herhangi bir uyarı göstermez. Kaspersky Endpoint Security ayrıca, güvenilmez bir sertifika ile şifrelenmiş bir bağlantı kurma hakkında da bir olay oluşturur.

  Bazı durumlarda Kaspersky Endpoint Security, tarayıcıda bir uyarı içeren bir HTML sayfasını teknik olarak görüntüleyemez (aşağıdaki şekle bakın). Mesela, bir web kaynağı bir ağ protokolünün eski bir sürümünü ve standart olmayan bir bağlantı noktasını kullanıyorsa. Bu durumlarda, Kaspersky Endpoint Security bu etki alanına erişimi engeller ve tarayıcı standart `ERR_CONNECTION_RESET` penceresi görüntülenir. Bir web kaynağına erişmek için etki alanını istisnalara ekleyebilir veya bir güvenilir sertifika kullanabilirsiniz.

- Eğer *bir üçüncü taraf uygulaması veya hizmeti* güvenilmez bir sertifikaya sahip bir etki alanıyla bağlantı kurarsa, Kaspersky Endpoint Security trafiği taramak için kendi sertifikasını oluşturur. Yeni ilke *Güvenilmez* durumuna sahiptir. Bu, üçüncü taraf uygulamasını güvenilmez bağlantı hakkında uyarmak için gereklidir, çünkü bu durumda HTML sayfası görüntülenemez ve bağlantı arka plan modunda kurulabilir. Bu nedenle, bir üçüncü taraf uygulamasının yerleşik sertifika doğrulama araçları varsa bağlantı sonlandırılabilir. Bu durumda, etki alanının sahibiyle iletişime geçerek güvenilir bir bağlantı kurmanız gerekir. Güvenilir bir bağlantı kurmak mümkün olmazsa bu üçüncü taraf uygulamasını güvenilir uygulamalar listesine ekleyebilirsiniz. Kaspersky Endpoint Security ayrıca, güvenilmez bir sertifika ile şifrelenmiş bir bağlantı kurma hakkında da bir olay oluşturur.

Yönetim Konsolu'nda (MMC) güvenilmez bir sertifika ile şifrelenmiş bağlantıların taranmasını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
4. **Şifreli bağlantıları tarama** bloğunda **Gelişmiş ayarlar** düğmesine tıklayın.
5. Açılan pencerede, güvenilmez bir sertifikaya sahip bir etki alanını ziyaret ederken kullanılacak uygulama işletim modunu seçin: **İzin ver** veya **Engelle**.
6. Değişikliklerinizi kaydedin.

Web Console'da güvenilmez bir sertifikaya sahip şifreli bağlantıların taranmasını yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.
5. **Şifreli Bağlantıları Tarama** bloğunda, **Ayarlar** bağlantısına tıklayın.

6. Açılan pencerede, güvenilmez bir sertifikaya sahip bir etki alanını ziyaret ederken kullanılacak uygulama işletim modunu seçin: **Bağlantıya izin ver** veya **Bağlantıyı engelle**.

7. Değişikliklerinizi kaydedin.

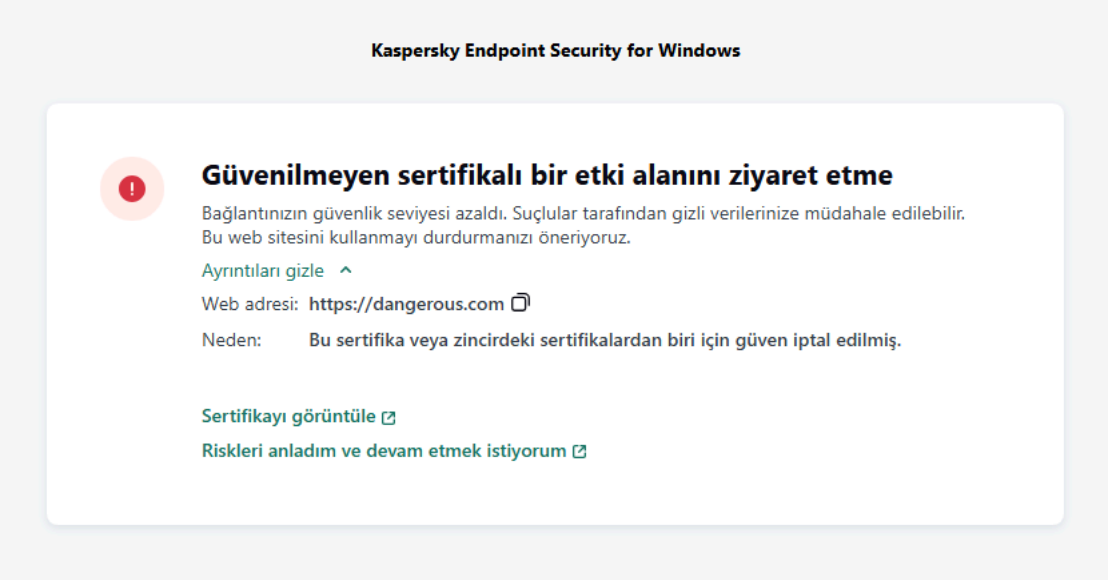
Uygulama arabiriminde güvenilmez bir sertifika ile şifrelenmiş bağlantıların taranmasını yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.

3. **Şifreli bağlantıları tarama** bölümünde, güvenilmez bir sertifikaya sahip bir etki alanını ziyaret ederken kullanılacak uygulama işletim modunu seçin: **İzin ver** veya **Engelle**.

4. Değişikliklerinizi kaydedin.



Sertifikasına güvenilmeyen bir etki alanını ziyaret etme hakkında uyarı

Kaspersky sertifikasını kendi sertifika deposuna ekleme

Tarayıcılar ve posta istemcileri, web kaynaklarının güvenliğini ve gerçekliğini doğrulamak için sertifikayı kullanır. Sertifika ayrıca web kaynakları ile kullanıcı arasında veri şifrelemesi sağlar. Çoğu tarayıcı ve posta istemcisi güvenilir sertifika deposunu (Windows sertifika deposu) kullanır. Örneğin, Google Chrome. Bazı tarayıcılar ve posta istemcileri varsayılan olarak Windows sertifika deposu yerine kendi sertifika depolarını kullanır. Örneğin, Firefox ve Thunderbird.

Yükleme sonrasında, Kaspersky Endpoint Security, Kaspersky sertifikasını güvenilir sertifikaların sistem depolamasına ekler (Windows sertifika deposu). Kaspersky Security Center kuruluşunuzda dağıtılmışsa ve bir bilgisayara bir ilke uygulanıyorsa Kaspersky Endpoint Security, bu uygulamaların trafiğini taramak için tarayıcılarda ve posta istemcilerinde Windows sertifika deposunun kullanılmasını otomatik olarak etkinleştirir. Bilgisayara bir ilke uygulanmıyorsa, tarayıcılar ve posta istemcileri tarafından kullanılacak sertifika deposunu seçebilirsiniz. Kendi sertifika deposunu seçtiyseniz Kaspersky sertifikasını depoya manuel olarak ekleyin. Bu, HTTPS trafiğiyle çalışırken hataların önlenmesine yardımcı olacaktır.

Mozilla Firefox tarayıcısında ve Thunderbird posta istemcisinde trafiği taramak için Şifreli Bağlantıları Taramayı etkinleştirmelisiniz. Şifreli Bağlantıları Tarama devre dışı bırakıldığı takdirde, uygulama Mozilla Firefox tarayıcısında ve Thunderbird posta istemcisindeki şifrelenmiş trafiği taramaz. MyOffice Mail ve R7-Office Organizer posta istemcilerindeki trafiği taramak için şifreli bağlantı taramasının da etkinleştirilmesi gerekir.

Tarayıcının veya posta aracısının kendi sertifika deposuna bir sertifika eklemeden önce, Kaspersky sertifikasını Windows Denetim Masasından (İnternet özellikleri) dışa aktarın. Örneğin, Mozilla teknik destek web sitesinde mağazaya sertifika ekleme hakkında daha fazla bilgi edinebilirsiniz.

Sertifika deposunu yalnızca uygulamanın yerel arabiriminde seçebilirsiniz.

Tarayıcılarda ve posta istemcilerinde şifrelenmiş bağlantıları taramak üzere bir sertifika deposu seçmek için:

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **Şifreli bağlantıları tarama** bloğunda, **Kendi sertifika deposuna sahip uygulamalarda şifrelenmiş bağlantıları taramak için şunu kullanın** onay kutusunu seçin.
4. Bir sertifika deposu seçin:
   - **Windows sertifika deposu (önerilir)**. Kaspersky kök sertifikası, Kaspersky Endpoint Security kurulumu sırasında bu depoya eklenir.
   - **Kendi sertifika deposu**. Mozilla Firefox ve Thunderbird kendi sertifika depolarını kullanır. Mozilla sertifika deposu seçilirse, Kaspersky kök sertifikasını tarayıcı özelliklerinden bu depoya manuel olarak eklemeniz gerekir.

     MyOffice Mail ve R7-Office Organizer posta istemcileri de kendi sertifika depolarını kullanırlar.
5. Değişikliklerinizi kaydedin.

Şifreli bağlantıları taramanın dışında tutma

Çoğu web kaynağında şifrelenmiş bağlantılar kullanılır. Kaspersky, Şifreli bağlantıları tarama özelliğini etkinleştirmenizi önerir. Şifrelenmiş bağlantıları tarama işle ilgili faaliyetlerle karışırsa bir web sitesini istisnalara *güvenilir internet adresleri* olarak ekleyebilirsiniz. Bu durumda, Kaspersky Endpoint Security, Web Tehdidi Koruması, Posta Tehdidi Koruması, İnternet Denetimi bileşenleri işlerini yaparken güvenilir internet adreslerinin HTTPS trafiğini taramaz.

Güvenilir uygulama şifrelenmiş bir bağlantı kullanıyorsa bu uygulama için şifrelenmiş bağlantıları taramayı devre dışı bırakabilirsiniz. Örneğin kendi sertifikası ile iki faktörlü kimlik doğrulaması kullanan bulut depolama uygulamaları için şifrelenmiş bağlantıları taramayı devre dışı bırakabilirsiniz.

Yönetim Konsolu'nda (MMC) bir web adresini şifreli bağlantı taramalarından hariç tutma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
5. **Şifreli bağlantıları tarama** bloğunda **Güvenilir adresleri yapılandır** düğmesine tıklayın.
6. **Ekle**'ye tıklayın.

7. Kaspersky Endpoint Security'nin bir etki alanı ziyaret edilirken kurulan şifrelenmiş bağlantıları taramasını istemiyorsanız bir etki alanı adı veya IP adresi ekleyin.

   Kaspersky Endpoint Security alan adına maske girilmesi için `*` karakterini destekler.

   > Kaspersky Endpoint Security, IP adresleri için `*` sembolünü desteklemez. Bir alt ağ maskesi kullanarak bir IP adresi aralığı seçebilirsiniz (örneğin, 198.51.100.0/24).

   Örnekler:

   - `domain.com` - kayıt şu adresleri içerir: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Kayıt, alt etki adlarını içermez (örneğin, `subdomain.domain.com`).
   - `subdomain.domain.com` – kayıt şu adresleri içerir: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.
   - `*.domain.com` – kayıt şu adresleri içerir: `https://movies.domain.com`, `https://images.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da bir web adresini şifreli bağlantı taramalarının dışında tutma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.
5. **Şifreli Bağlantıları Tarama** bloğunda, **Güvenilen etki alanları** düğmesine tıklayın.
6. **Ekle**'ye tıklayın.
7. Kaspersky Endpoint Security'nin bir etki alanı ziyaret edilirken kurulan şifrelenmiş bağlantıları taramasını istemiyorsanız bir etki alanı adı veya IP adresi ekleyin.

   Kaspersky Endpoint Security alan adına maske girilmesi için `*` karakterini destekler.

   > Kaspersky Endpoint Security, IP adresleri için `*` sembolünü desteklemez. Bir alt ağ maskesi kullanarak bir IP adresi aralığı seçebilirsiniz (örneğin, 198.51.100.0/24).

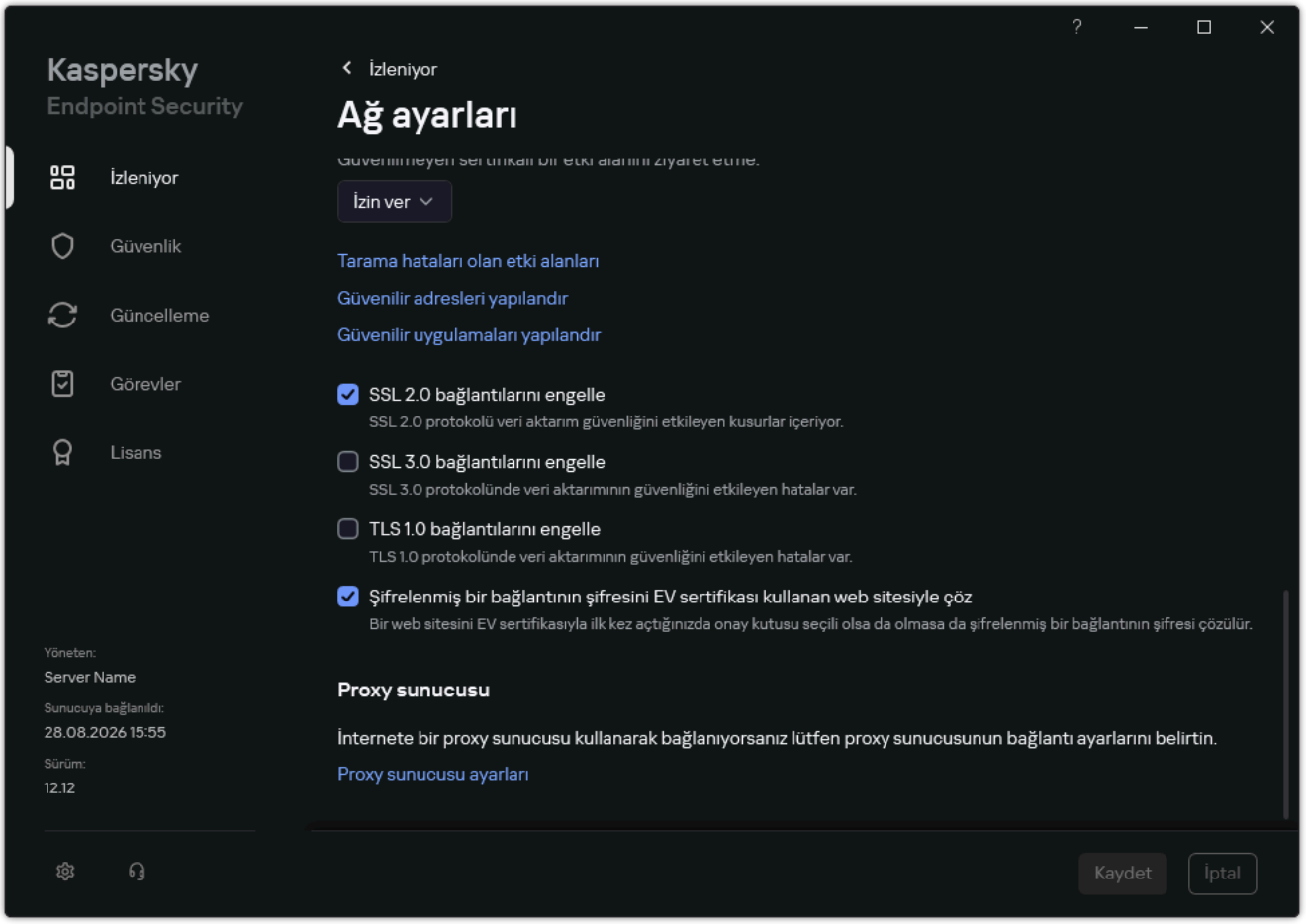
Örnekler:

- `domain.com` - kayıt şu adresleri içerir: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Kayıt, alt etki adlarını içermez (örneğin, `subdomain.domain.com`).
- `subdomain.domain.com` – kayıt şu adresleri içerir: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.
- `*.domain.com` – kayıt şu adresleri içerir: `https://movies.domain.com`, `https://images.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Bir web adresini uygulama arayüzündeki şifreli bağlantı taramalarından hariç tutma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



Uygulama ağ ayarları

3. **Şifreli bağlantıları tarama** bloğunda **Güvenilir adresleri yapılandır** düğmesine tıklayın.
4. **Ekle**'ye tıklayın.
5. Kaspersky Endpoint Security'nin bir etki alanı ziyaret edilirken kurulan şifrelenmiş bağlantıları taramasını istemiyorsanız bir etki alanı adı veya IP adresi ekleyin.

   Kaspersky Endpoint Security alan adına maske girilmesi için `*` karakterini destekler.

Kaspersky Endpoint Security, IP adresleri için `*` sembolünü desteklemez. Bir alt ağ maskesi kullanarak bir IP adresi aralığı seçebilirsiniz (örneğin, 198.51.100.0/24).

Örnekler:

- `domain.com` - kayıt şu adresleri içerir: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Kayıt, alt etki adlarını içermez (örneğin, `subdomain.domain.com`).
- `subdomain.domain.com` – kayıt şu adresleri içerir: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.
- `*.domain.com` – kayıt şu adresleri içerir: `https://movies.domain.com`, `https://images.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.

6. Değişikliklerinizi kaydedin.

Varsayılan olarak, Kaspersky Endpoint Security hatalar meydana geldiğinde şifrelenmiş bağlantıları taramaz ve web sitesini özel bir *Tarama hataları olan etki alanları* listesine ekler. Kaspersky Endpoint Security her kullanıcı için ayrı bir liste derler ve verileri Kaspersky Security Center'a göndermez. Bir tarama hatası meydana geldiğinde bağlantının engellenmesini etkinleştirebilirsiniz. Şifreli bağlantılar tarama hatalarına sahip etki alanlarının bir listesini sadece uygulamanın yerel arabiriminde görüntüleyebilirsiniz.

Tarama hatası olan etki alanlarının listesini görüntülemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **Şifreli bağlantıları tarama** bloğunda **Tarama hataları olan etki alanları** düğmesine tıklayın.

Tarama hatası olan etki alanlarının bir listesi açılır. Listeyi sıfırlamak için ilkede tarama hataları meydana geldiğinde bağlantıyı engellemeyi etkinleştirin, ilkeyi uygulayın ve arından parametreleri ilk değerine sıfırlayarak ilkeyi tekrar uygulayın.

Kaspersky uzmanları bir *küresel istisnalar* listesi yapar. Bu liste Kaspersky Endpoint Security'nin uygulama ayarları ne olursa olsun kontrol etmeyeceği güvenilir web sitelerini içeren bir listedir.

Şifrelenmiş trafik taramasından gelen küresel istisnaları görüntülemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **Şifreli bağlantıları tarama** bloğunda güvenilir web siteleri bağlantısına tıklayın.

Bu, Kaspersky uzmanları tarafından derlenen web sitelerinin bir listesini açar. Kaspersky Endpoint Security, listedeki web siteleri için korumalı bağlantıları taramaz. Kaspersky Endpoint Security veritabanları ve modülleri güncellendiğinde liste güncellenebilir.

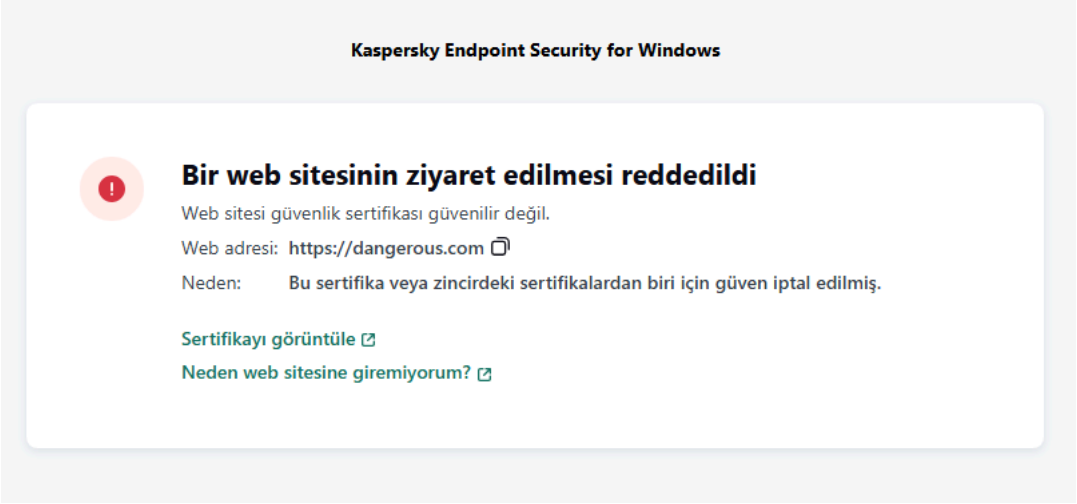
Güvenilir olmayan sertifikalara sahip etki alanlarına erişimi engelleme

Bazı durumlarda Kaspersky Endpoint Security, güvenilir olmayan bir sertifikaya sahip etki alanına erişimi engellerken tarayıcıda istenen web kaynağına yönlendiren bağlantının bulunmadığı bir HTML uyarı sayfası görüntüler.

Bunun nedeni aşağıdakilerden biri olabilir:

- Yönetici, güvenilir olmayan bir sertifikaya sahip etki alanına erişimi engelledi.
- Etki alanının güvenilir olmayan veya geçersiz bir sertifikası vardır ve web sunucusu HTTP Strict Transport Security (HSTS) mekanizmasını kullanır. *HSTS*, bir istemci ile web sunucusu arasındaki iletişimde güvenli HTTPS protokolünün kullanılmasını zorunlu kılan bir güvenlik mekanizmasıdır. Bu durumda, etki alanını güvenilir adresler listesine eklemiş olsanız bile etki alanına erişemezsiniz. HSTS mekanizması RFC 6797 'de açıklanmıştır.

  Bazı durumlarda web sitesi, Kaspersky Endpoint Security kullanılmadan doğrudan bir tarayıcıda açılabilir. Tarayıcılar iptal edilmiş sertifikaları her zaman tespit etmez. Kaspersky Endpoint Security ise bağlantı kurarken sertifikanın iptal edilip edilmediğini çevrimiçi olarak kontrol eder. Bu sayede uygulama, sertifikayla ilgili sorunu tarayıcıdan önce tespit edip ilgili hata mesajını görüntüleyebilir.



Sertifikasına güvenilmeyen bir etki alanını ziyaret etme hakkında uyarı

Verileri sil

Kaspersky Endpoint Security, kullanıcıların bilgisayarlarından uzaktan veri silmek için bir görev kullanmanıza izin verir.

Kaspersky Endpoint Security verileri aşağıdaki gibi siler:

- Sessiz modda;
- Sabit sürücüler ve çıkarılabilir sürücülerde;
- Bilgisayardaki tüm kullanıcı hesapları için.

Kaspersky Endpoint Security *Verileri sil* görevini hangi lisans türü kullanıldığından bağımsız olarak ve lisansın süresi dolmuş olsa bile gerçekleştirilir.

Veri Silme modları

Bu görev, verileri şu modlarda silmenizi sağlar:

- Anında veri silme.

  Bu modda, örneğin disk alanını boşaltmak için tarihi geçmiş verileri silebilirsiniz.

- Ertelenen veri silme.

  Bu modun amacı, örneğin çalınan veya kaybolmuş bir dizüstü bilgisayardaki verileri korumaktır. Dizüstü bilgisayar kurumsal ağın sınırları dışına çıkarsa ve Kaspersky Security Center ile uzun süre boyunca senkronizasyon yapılmazsa otomatik veri silme yapılması için yapılandırma yapabilirsiniz.

Görev özelliklerinde veri silme için bir zamanlama ayarlamak mümkün değildir. Verileri sadece görevi manuel olarak başlattıktan hemen sonra silebilirsiniz ya da Kaspersky Security Center ile hiçbir bağlantı yoksa gecikmeli veri silme yapılandırabilirsiniz.

Sınırlamalar

Veri Silme şu sınırlamalara sahiptir:

- Sadece bir Kaspersky Security Center yöneticisi *Verileri sil* görevini yönetebilir. Kaspersky Endpoint Security'nin yerel arabiriminde bir görevi yapılandıramaz ya da başlatamazsınız.
- NTFS dosya sistemi için, Kaspersky Endpoint Security sadece ana veri akışlarının adlarını siler. Alternatif veri akış adları silinemez.
- Bir sembolik bağlantı dosyasını sildiğinizde, Kaspersky Endpoint Security aynı zamanda sembolik yolda yolları belirtilmiş olan dosyaları da siler.

Bir Veri silme görevi oluşturmak

Kullanıcıların bilgisayarlarındaki verileri silmek için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Verileri sil**'i seçin.

   c. **Görev adı** alanına, *Verileri sil (Hırsızlığa karşı koruma)* gibi bir kısa açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

   Görev kapsamında bir yönetim grubuna yeni bilgisayarlar eklenirse, anında veri silme görevi yeni bilgisayarlarda ancak görev yeni bilgisayarların eklenmesinden sonraki 5 dakika içinde tamamlanırsa çalıştırılır.

5. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

6. Kaspersky Endpoint Security'nin **Verileri sil** görevine tıklayın.

   Görev özellikleri penceresi açılır.

7. **Uygulama ayarları** sekmesini seçin.

8. Veri silme yöntemini seçin:

   - **İşletim sistemi aracılığıyla sil**. Kaspersky Endpoint Security dosyaları geri dönüşüm kutusuna göndermeden silmek için işletim sistemi kaynaklarını kullanır.
   - **Tamamen sil, kurtarma mümkün değildir**. Kaspersky Endpoint Security dosyaların üzerine rastgele veriler yazar. Silme işleminden sonra verileri kurtarmak neredeyse imkansızdır.

9. Veri silme işlemini ertelemek istiyorsanız **Kaspersky Security Center ile şundan daha uzun süre bağlantı kesildiğinde verileri otomatik olarak sil N gün** onay kutusunu seçin. Gün sayısını seçin.

   Ertelenen veri silme görevi, Kaspersky Security Center ile belirlenen süre boyunca bağlantı her kurulmadığında gerçekleştirilir.

Ertelenmiş veri silme işlemini yapılandırırken, çalışanların farklı çalışma programlarına sahip olabileceğini unutmayın. Ayrıca çevrimdışı kullanıcıların çalışma programını da dikkate alın. Çevrimdışı bilgisayarlarla ve işyeri dışındaki kullanıcılarla çalışma hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardımı içeriğine bakın.

Bilgisayar kapalıysa ve bağlantı yapılandırılan süreden daha uzun süredir yoksa, bilgisayar açıldıktan sonra Kaspersky Endpoint Security verileri hemen silmez. Uygulama bir saat boyunca Kaspersky Security Center ile senkronize edilmeyi bekler. Bu, örneğin tatile çıkmadan önce bilgisayarlarını kapatan kullanıcıların bilgisayarlarındaki yetkisiz veri silinmesini önlemek için gereklidir.

Bu onay kutusunun işareti kaldırılırsa görev Kaspersky Security Center ile senkronizasyon sağlandıktan hemen sonra gerçekleştirilir.

10. Silinecek nesnelerin bir listesini oluşturun:

- **Klasörler**. Kaspersky Endpoint Security klasördeki ve onun alt klasörlerindeki tüm dosyaları siler. Kaspersky Endpoint Security, klasör yolu girişi için maskeleri ve ortam değişkenlerini desteklemez.
- **Uzantıya göre dosyalar**. Kaspersky Endpoint Security, çıkarılabilir sürücüler de dahil olmak üzere bilgisayarın tüm sürücülerinde belirtilen uzantılara sahip dosyaları arar. Birden fazla değer belirtmek için "`;`" veya "`,`" karakterlerini kullanın.
- **Ön tanımlı kapsam**. Kaspersky Endpoint Security şu alanlardan dosyaları silecek:
  - **Belgeler**. İşletim sisteminin standart *Belgeler* klasörü ve onun alt klasörleri.
  - **Çerezler**. Tarayıcının kullanıcı tarafından ziyaret edilen web sitelerinden veri kaydettiği dosyalar (kullanıcı kimlik doğrulama verileri gibi).
  - **Masaüstü**. İşletim sisteminin standart *Masaüstü* klasörü ve onun alt klasörleri.
  - **Geçici Internet Explorer dosyaları**. Internet Explorer'ın çalışmasıyla ilgili, web sayfalarının, görüntü ve medya dosyalarının kopyaları gibi geçici dosyalar.
  - **Geçici dosyalar**. Bilgisayara yüklenmiş uygulamaların çalışmasıyla ilgili geçici dosyalar. Örneğin Microsoft Office uygulamaları, belgelerin yedek kopyalarını içeren geçici dosyalar oluşturur.
  - **Outlook dosyaları**. Outlook posta istemcisinin çalışmasıyla ilgili dosyalar: veri dosyaları (PST), çevrimdışı veri dosyaları (OST), çevrimdışı adres defteri dosyaları (OAB) ve kişisel adres defteri dosyaları (PAB).
  - **Kullanıcı profili**. Yerel kullanıcı hesabı için işletim sistemi ayarlarını saklayan dosyalar ve klasörler.

Sekmelerin her birinde silinecek nesnelerin bir listesini oluşturabilirsiniz. Kaspersky Endpoint Security birleştirilmiş bir liste oluşturacak ve görev tamamlandığında dosyaları bu listeden silecektir.

Kaspersky Endpoint Security'nin çalışması için gerekli olan dosyaları silemezsiniz.

11. Değişikliklerinizi kaydedin.
12. Görevin yanındaki onay kutusunu seçin.
13. **Başlat**'a tıklayın.

Sonuç olarak kullanıcıların bilgisayarlarındaki veriler seçilen moda göre silinecektir: anında ya da bir bağlantı

olmadığında. Kaspersky Endpoint Security örneğin bir kullanıcının bir dosyayı kullanıyor olmasından dolayı bir dosyayı silemezse, uygulama bu dosyayı tekrar silmeyi denemez. Görevi tamamlamak için görevi tekrar çalıştırın.

Bilgisayar denetimi

İnternet Denetimi

İnternet Denetimi, web kaynaklarına kullanıcı erişimini yönetir. Böylece trafiğin azaltılmasına ve çalışma zamanının daha verimli kullanılmasına yardımcı olur. Bir kullanıcı İnternet Denetimi tarafından kısıtlanan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller veya bir uyarı gösterir (aşağıdaki şekle bakın).

İnternet Denetimini kullanmak için uygulamanın ilk yapılandırmasını tamamlamanız gerekir:

- HTTPS trafiğini izlemek için şifreli bağlantı taramasını etkinleştirin (varsayılan olarak etkindir).
- Kaspersky Endpoint Security'nin izlemesi gereken portları seçin (varsayılan olarak uygulama tüm portları izler).
- Kaspersky Endpoint Security'nin trafiğini izlemesini istediğiniz uygulamaları seçin. Çoğu tarayıcı Kaspersky tarafından önerilen uygulamalar listesinde zaten vardır. Eğer tarayıcınız listede yoksa manuel olarak ekleyin.
- Web trafiğine bir web sayfası etkileşim komut dosyası enjekte etmenizi öneririz (varsayılan olarak komut dosyası enjeksiyonu devre dışıdır). Bu komut dosyası, uygulama olay günlüğü, işletim sistemi olay günlüğü ve raporlar için İnternet Denetimi olaylarının kaydını sağlar.

İnternet sitelerine erişimi yönetme yöntemleri

İnternet Denetimi, şu yöntemleri kullanarak web sitelerine erişimi yapılandırır:

- **Web sitesi kategorisi**. Web siteleri, Kaspersky Security Network bulut hizmeti, sezgisel analiz ve bilinen web siteleri veritabanını (uygulama veritabanlarının içindedir) kullanarak kategorize eder. Örneğin, kullanıcı erişimini *Sosyal ağlar* kategorisiyle veya diğer kategorilerle kısıtlayabilirsiniz.
- **Veri tipi**. Örneğin, bir web sitesindeki verilere kullanıcı erişimini kısıtlayabilir ve görüntüleri gizleyebilirsiniz. Kaspersky Endpoint Security veri türünü uzantısına göre değil dosya biçimine göre belirler.

  > Kaspersky Endpoint Security arşivlerin içindeki dosyaları taramaz. Örneğin resim dosyaları bir arşivin içindeyse, Kaspersky Endpoint Security bu dosyanın türünü *Grafikler* olarak değil *Arşivler* veri tipi olarak belirler.

- **Tek tek adresler**. Bir web adresi girebilir ya da maskeler kullanabilirsiniz.

Web sitelerine erişimi düzenlemek için birkaç yöntemi aynı anda kullanmak mümkündür. Örneğin *Ofis uygulama dosyaları* veri türüne erişimi sadece *Web tabanlı e-posta* web sitesi kategorisi için kısıtlayabilirsiniz.

Web sitesi erişim kuralları

İnternet Denetimi, *erişim kuralları* kullanarak web sitelerine kullanıcı erişimini düzenler. Bir web sitesi erişim kuralı için şu gelişmiş ayaları yapılandırabilirsiniz:

- Kuralın uygulanacağı kullanıcılar.

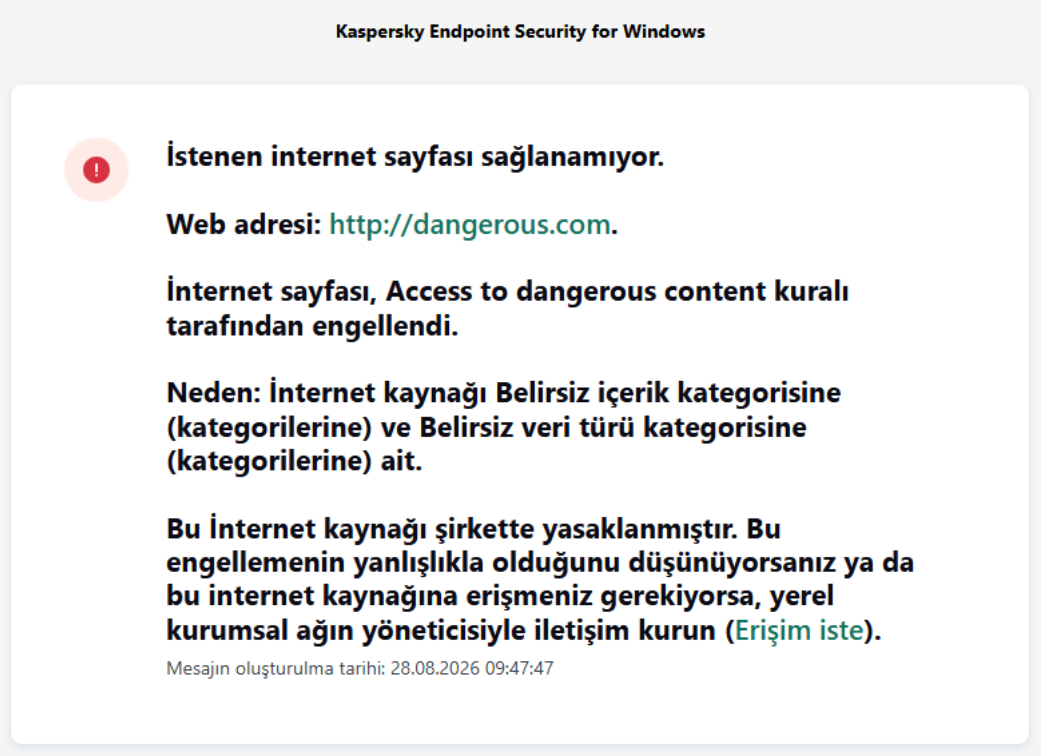
  Örneğin BT departmanı hariç olmak üzere şirketin tüm çalışanlarının bir tarayıcı üzerinden İnternete erişmesini kısıtlayabilirsiniz.

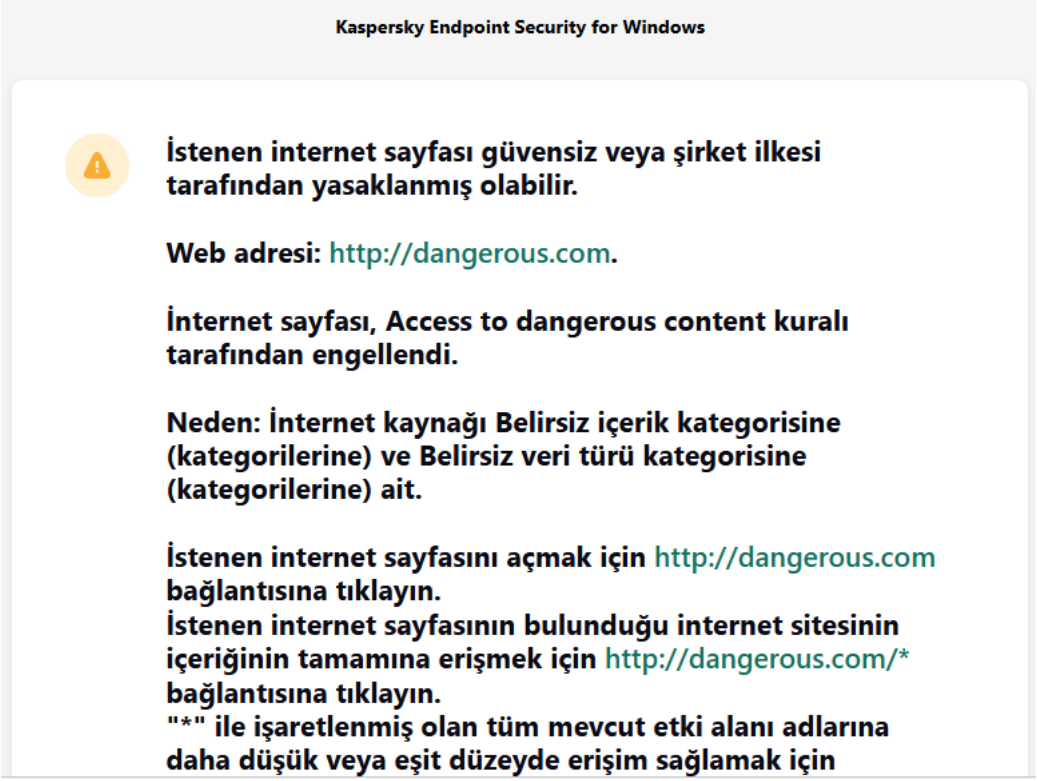
- Kural zamanlaması.

  Örneğin sadece çalışma saatleri içinde bir tarayıcıdan İnternete erişimi kısıtlayabilirsiniz.

Erişim kuralı öncelikleri

Her kuralın bir önceliği vardır. Bir kural listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Bir web sitesinin birden fazla kurala eklenmesi durumunda, İnternet Denetimi web sitesine erişimi en yüksek önceliğe sahip kurala göre düzenler. Örneğin Kaspersky Endpoint Security bir kurumsal portalı bir sosyal ağ olarak tanımlayabilir. Sosyal ağlara erişimi kısıtlarken kurumsal web portalına erişim sağlamak için iki kural oluşturun: *Sosyal ağlar* web sitesi kategorisi için bir kural ve kurumsal web postalı için bir kural. Kurumsal web portalına erişim kuralı, sosyal ağlara erişim kuralından daha yüksek önceliğe sahip olmalıdır.





İnternet Denetimi mesajları

İnternet kaynağı erişim kuralı ekleme

Bir *web kaynağı erişim kuralı*, kullanıcılar web kaynaklarını ziyaret ettiğinde Kaspersky Endpoint Security'nin uyguladığı bir dizi filtre ve eylemdir. Erişim kuralları bir kural çizelgesi içerebilir.

Sistemin kararsız hale gelmesine neden olabileceğinden 1000'den fazla İnternet kaynakları erişim kuralı oluşturulması önerilmez.

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, İnternet kaynaklarını ve veri türünü içeriğe göre kategorilere ayırır. Bu kategoriler tarafından tanımlanan türlere giren içerik ve verilerle İnternet kaynaklarına kullanıcı erişimini 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. *Varsayılan kural* önceden ayarlanmıştır. Bu kural, diğer kuralların kapsamadığı tüm İnternet kaynakları için geçerlidir ve tüm kullanıcılar için bu İnternet kaynaklarına erişime izin verir veya erişimi engeller.

Her kuralın bir önceliği vardır. Bir kural listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Bir web sitesinin birden fazla kurala eklenmesi durumunda, İnternet Denetimi web sitesine erişimi en yüksek önceliğe sahip kurala göre düzenler. Örneğin Kaspersky Endpoint Security bir kurumsal portalı bir sosyal ağ olarak tanımlayabilir. Sosyal ağlara erişimi kısıtlarken kurumsal web portalına erişim sağlamak için iki kural oluşturun: *Sosyal ağlar* web sitesi kategorisi için bir kural ve kurumsal web postalı için bir kural. Kurumsal web portalına erişim kuralı, sosyal ağlara erişim kuralından daha yüksek önceliğe sahip olmalıdır.

Yönetim Konsolu'nda (MMC) internet kaynağı erişim kuralı nasıl eklenir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri → İnternet Denetimi** seçimini yapın.
4. **İnternet Denetimi** onay kutusunu seçin.
5. **İnternet Denetimi ayarları** bloğundan **Ekle** düğmesine tıklayın.
   İnternet kaynaklarına erişim kuralı penceresi açılır.
6. Web kaynağı erişim kuralını yapılandırın (aşağıdaki tabloya bakın).
7. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

   İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

   Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.
8. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir internet kaynağı erişim kuralı nasıl eklenir

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri → İnternet Denetimi**'ne gidin.

5. **İnternet Denetimi ETKİN** anahtarını açık konuma getirin.

6. **Kurallar listesi** bloğunda **Ekle** düğmesine tıklayın.

7. Web kaynağı erişim kuralını yapılandırın (aşağıdaki tabloya bakın).

8. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

   İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

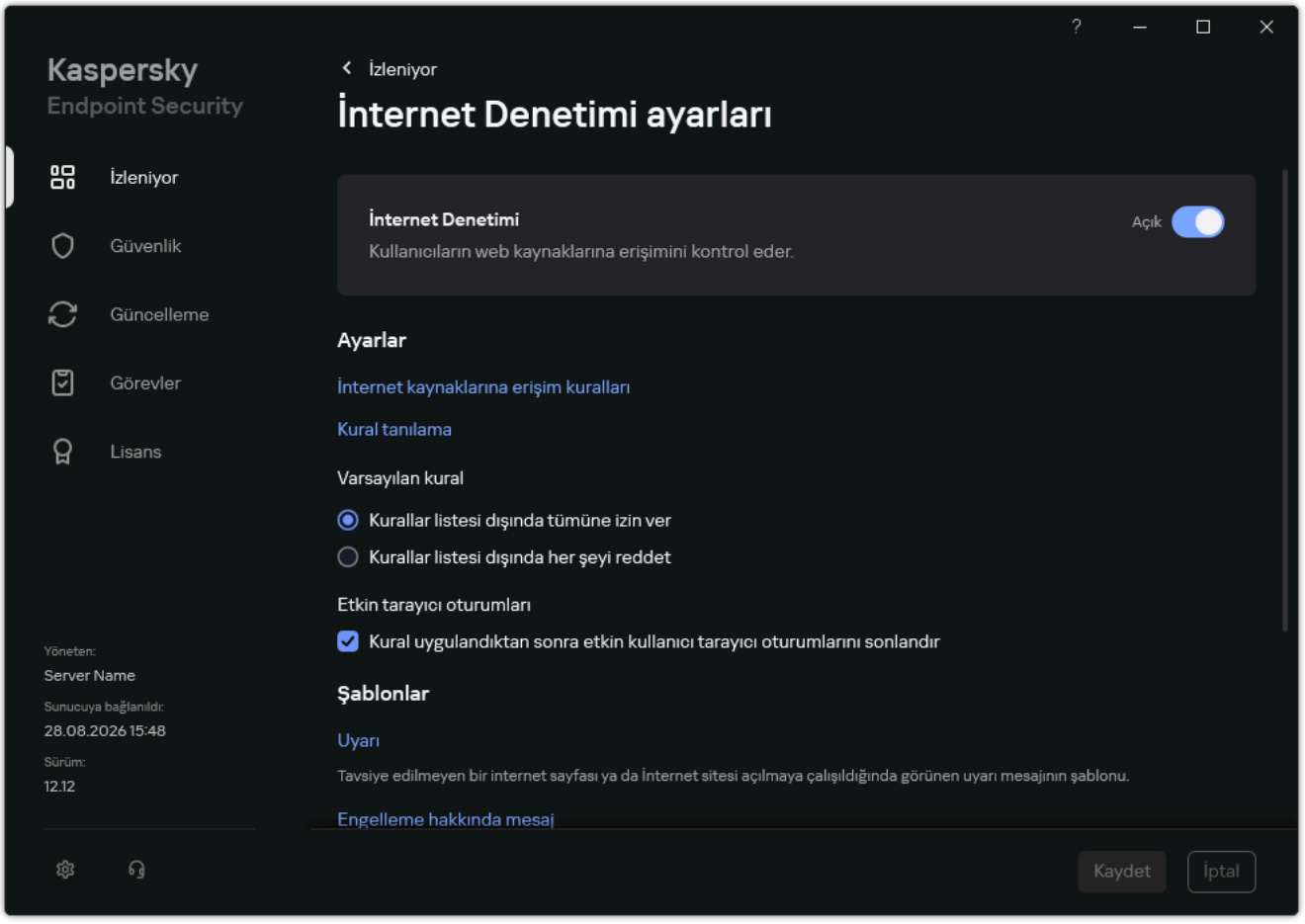
   Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.

9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde internet kaynağı erişim kuralı nasıl eklenir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **İnternet Denetimi** düğmesini açık konumuna getirin.

4. **Ayarlar** bloğunda, **İnternet kaynaklarına erişim kuralları** düğmesine tıklayın.

5. Açılan pencerede **Ekle** düğmesine tıklayın.

   İnternet kaynaklarına erişim kuralı penceresi açılır.

6. Web kaynağı erişim kuralını yapılandırın (aşağıdaki tabloya bakın).

7. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

   İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

   Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.

8. Değişikliklerinizi kaydedin.

Sonuç olarak, yeni İnternet Denetimi kuralı listeye eklenir. Gerekirse, İnternet Denetimi kuralının önceliğini değiştirin. Web kaynağı erişim kuralını listeden kaldırmadan istediğiniz zaman devre dışı bırakmak için geçiş düğmesini de kullanabilirsiniz.

İnternet Denetimi kural parametreleri

Parametre	Açıklama
Kural adı	İnternet Denetimi kuralının adı.
Durum	• **Açık**. • **Kapalı**. İstediğiniz zaman web kaynağı erişim kuralını devre dışı bırakmak için geçiş düğmesini kullanabilirsiniz.
Eylem	• **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir. • **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler. • **Uyar**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.
Filtrenin içeriği	• **İçerik kategorilerine göre**. Kullanıcıların internet kaynaklarına erişimini kategoriye göre kontrol edebilirsiniz (örneğin, *Sosyal ağlar* kategorisi). • **Veri türlerine göre**. İnternet kaynaklarına kullanıcı erişimini, yayınlanan verilerinin belirli veri türüne (örneğin *Grafikler*) göre kontrol edebilirsiniz.
Adresler	• **Tüm adreslere**. İnternet Denetimi, internet kaynaklarını adrese göre filtrelemeyecektir. • **Tek tek adreslere**. İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir. Şifreli Bağlantıları Tarama devre dışı bırakılırsa HTTPS iletişim kuralı için yalnızca sunucu adıyla filtreleme yapabilirsiniz.
Kullanıcılar	• **Tüm kullanıcılara**. İnternet Denetimi, belirli kullanıcılar için internet kaynaklarını filtrelemez. • **Tek tek kullanıcılara ve/veya gruplara uygula**. İnternet Denetimi, internet kaynaklarını yalnızca belirli kullanıcılar için filtreleyecektir. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.
Kural zamanlaması	Kural zamanlaması, Kaspersky Endpoint Security'nin İnternet kaynaklarına erişimi kurala göre izlediği süreyi belirler. Örneğin sadece çalışma saatleri içinde bir tarayıcıdan İnternete erişimi kısıtlayabilirsiniz.

İnternet kaynağı adreslerine göre filtrele

Wweb kaynakları için erişimi ayrı ayrı denetlemek için bir İnternet Denetimi kuralı oluşturmanız, bir web adresleri listesi oluşturmanız ve bir İnternet Denetimi eylemi seçmeniz gerekir. Bir web adresi listesi oluştururken, URL adreslerini girebilir veya maskeler kullanabilirsiniz.

Kurallar, bir kural çizelgesi ve kuralın uygulanacağı kullanıcıların bir listesini içerebilir. Örneğin, web sitelerine erişimi yalnızca çalışma saatleri içinde kısıtlayabilir veya web sitelerini belirli gruplardaki kullanıcıların ziyaret etmesine izin verebilirsiniz.

Yönetim Konsolu'nda (MMC) bir web kaynağı adresi nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi** seçimini yapın.
4. **İnternet Denetimi** onay kutusunu seçin.
5. **İnternet Denetimi ayarları** bloğundan **Ekle** düğmesine tıklayın.
   İnternet kaynaklarına erişim kuralı penceresi açılır.
6. Web kaynağı erişim kurallarını yapılandırın:
   a. **Ad** alanında, kuralın adını girin veya düzenleyin.
   b. **Adreslere uygula** açılır listesindeki **Tek tek adreslere** seçeneğini kullanın.
   c. Web kaynağı adreslerinin bir listesini oluşturun. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz.

      Şifreli Bağlantıları Tarama devre dışı bırakılırsa HTTPS iletişim kuralı için yalnızca sunucu adıyla filtreleme yapabilirsiniz.

   d. **Şu kullanıcılara uygula** açılır listesinde, kullanıcılar için ilgili filtreyi seçin:
      - **Tüm kullanıcılara**. İnternet Denetimi, internet kaynaklarını adrese göre filtrelemeyecektir.
      - **Ayrı ayrı kullanıcılara veya gruplara**. İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

e. **Eylem** açılır listesinden bir seçenek belirleyin:

- **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir.
- **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler.
- **Uyar**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

f. **Kural zamanlaması** açılır listesinde bir zamanlama seçin veya yeni bir zamanlama oluşturun.

7. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

> İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.

8. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da web kaynak adresi filtresi nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **İnternet Denetimi**'ne gidin.
5. **İnternet Denetimi ETKİN** anahtarını açık konuma getirin.
6. **Kurallar listesi** bloğunda **Ekle** düğmesine tıklayın.
7. Web kaynağı erişim kurallarını yapılandırın:

   a. **Kural adı** alanında, kuralın adını girin veya düzenleyin.

   b. Web kaynağı erişim kuralı için **Etkin** durumunu seçin.

   Web kaynağı erişim kuralını listeden kaldırmadan istediğiniz zaman devre dışı bırakmak için geçiş düğmesini kullanabilirsiniz.

c. **Eylem** bloğundan ilgili seçeneği seçin:

- **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir.
- **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler.
- **Bilgilendir**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

d. **Kapsam** bölümünde, **Tek tek web siteleri** seçimini yapın.

e. İçerik filtresini yapılandırın:

- **Tek tek adresler**. Web kaynağı adreslerinin bir listesini oluşturun. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz.

  > Şifreli Bağlantıları Tarama devre dışı bırakılırsa HTTPS iletişim kuralı için yalnızca sunucu adıyla filtreleme yapabilirsiniz.

- **Veri tipi**. İnternet kaynaklarına kullanıcı erişimini, yayınlanan verilerinin belirli veri türüne (örneğin *Grafikler*) göre kontrol edebilirsiniz.

f. **Kullanıcı veya grup** bölümünde, İnternet Denetimi'nin kuralı uygulamasını istediğiniz kullanıcıları seçin.

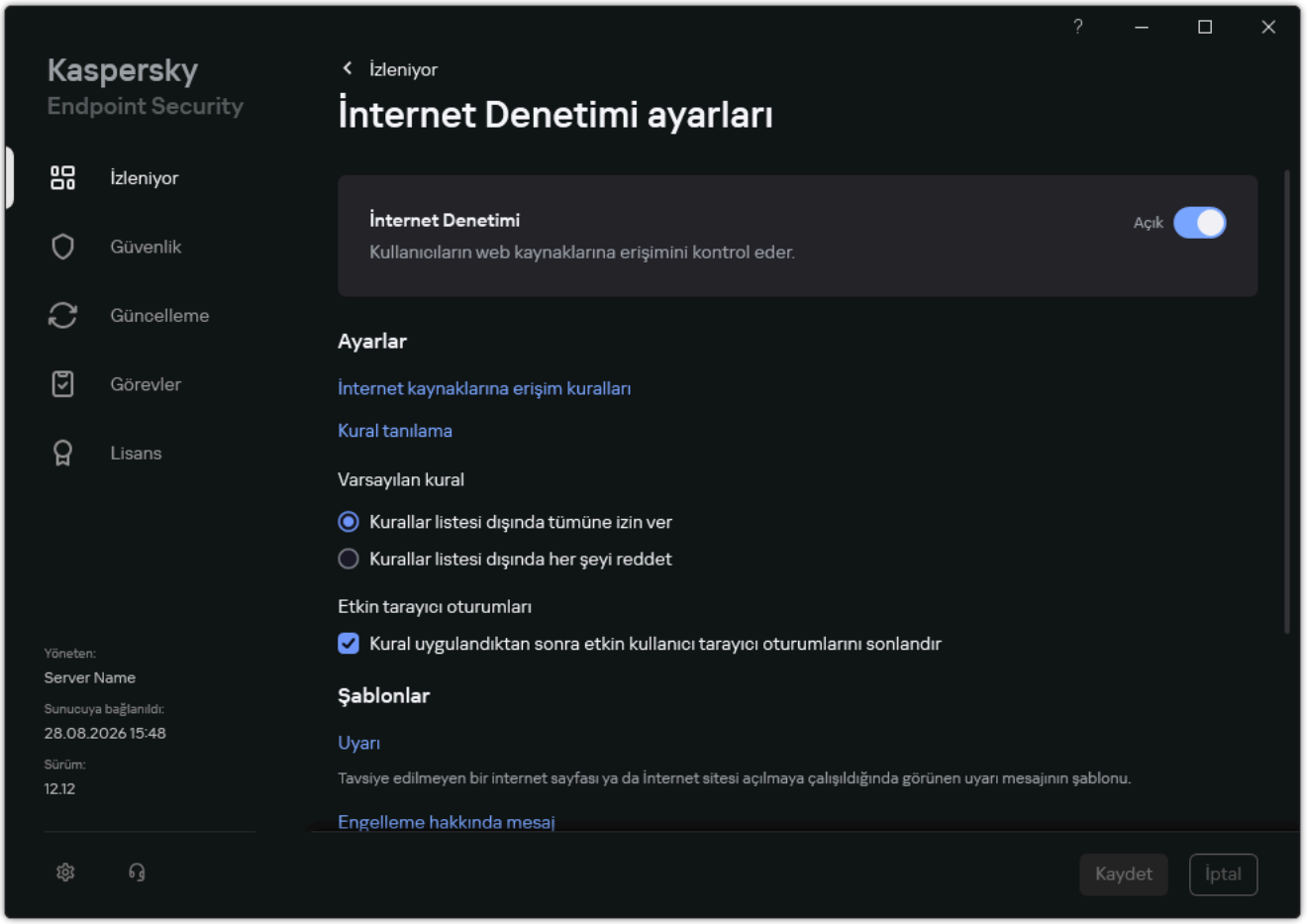
İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

g. **Erişim zamanlaması** bloğunda bir zamanlama seçin veya yeni bir zamanlama oluşturun.

8. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir web kaynağı adresi nasıl etkinleştirilir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **Ayarlar** bloğunda, **İnternet kaynaklarına erişim kuralları** düğmesine tıklayın.
4. Açılan pencerede **Ekle** düğmesine tıklayın.
   İnternet kaynaklarına erişim kuralı penceresi açılır.
5. **Kural adı** alanında, kuralın adını girin veya düzenleyin.
6. Web kaynağı erişim kuralı için **Açık** durumunu seçin.
   İstediğiniz zaman web kaynağı erişim kuralını devre dışı bırakmak için geçiş düğmesini kullanabilirsiniz.
7. **Eylem** bloğundan ilgili seçeneği seçin:
   - **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir.
   - **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler.
   - **Uyar**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.
8. **Adresler** bölümünde, **Tek tek adreslere** seçimini yapın.

Web kaynağı adreslerinin bir listesini oluşturun. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz.

> Şifreli Bağlantıları Tarama devre dışı bırakılırsa HTTPS iletişim kuralı için yalnızca sunucu adıyla filtreleme yapabilirsiniz.

9. **Kullanıcılar** bloğundan kullanıcılar için ilgili filtreyi seçin:

   - **Tüm kullanıcılara**. İnternet Denetimi, belirli kullanıcılar için internet kaynaklarını filtrelemez.
   - **Tek tek kullanıcılara ve/veya gruplara uygula**. İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

10. **Kural zamanlaması** açılır listesinde bir zamanlama seçin veya yeni bir zamanlama oluşturun.

11. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

    > İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

    Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.

12. Değişikliklerinizi kaydedin.

Sonuç olarak, yeni İnternet Denetimi kuralı listeye eklenir. Gerekirse, İnternet Denetimi kuralının önceliğini değiştirin. Web kaynağı erişim kuralını listeden kaldırmadan istediğiniz zaman devre dışı bırakmak için geçiş düğmesini de kullanabilirsiniz.

İnternet kaynağı içeriğine göre filtrele

Web kaynağı içeriğine göre erişimi kontrol etmek için İnternet Denetimi bir kategori filtresi ve bir veri türü filtresi sağlar.

Web siteleri, Kaspersky Security Network bulut hizmeti, sezgisel analiz ve bilinen web siteleri veritabanını (uygulama veritabanlarının içindedir) kullanarak kategorize eder. Örneğin, kullanıcı erişimini *Sosyal ağlar* kategorisiyle veya diğer kategorilerle kısıtlayabilirsiniz.

Örneğin görüntüleri gizlemek için, bir web sitesine veri türüne göre kullanıcı erişimini kısıtlayabilirsiniz. Kaspersky Endpoint Security veri türünü uzantısına göre değil dosya biçimine göre belirler. İnternet Denetimi aşağıdaki veri türlerini ayırt eder:

- Video
- Ses

- Ofis uygulama dosyaları
- Yürütülebilir dosyalar
- Arşivler
- Grafikler
- Komut dizileri

Kaspersky Endpoint Security arşivlerin içindeki dosyaları taramaz. Örneğin resim dosyaları bir arşivin içindeyse, Kaspersky Endpoint Security bu dosyanın türünü *Grafikler* olarak değil *Arşivler* veri tipi olarak belirler.

Kurallar, bir kural çizelgesi ve kuralın uygulanacağı kullanıcıların bir listesini içerebilir. Örneğin, web sitelerine erişimi yalnızca çalışma saatleri içinde kısıtlayabilir veya web sitelerini belirli gruplardaki kullanıcıların ziyaret etmesine izin verebilirsiniz.

Yönetim Konsolunda (MMC) bir web kaynağı içerik filtresi nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi** seçimini yapın.
4. **İnternet Denetimi** onay kutusunu seçin.
5. **İnternet Denetimi ayarları** bloğundan **Ekle** düğmesine tıklayın.
   İnternet kaynaklarına erişim kuralı penceresi açılır.
6. Web kaynağı erişim kurallarını yapılandırın:
   a. **Ad** alanında, kuralın adını girin veya düzenleyin.
   b. **İçeriği filtrele** açılır listesinde ilgili içerik filtresini seçin:
      - **İçerik kategorilerine göre**. Kullanıcıların internet kaynaklarına erişimini kategoriye göre kontrol edebilirsiniz (örneğin, *Sosyal ağlar* kategorisi).
      - **Veri türlerine göre**. İnternet kaynaklarına kullanıcı erişimini, yayınlanan verilerinin belirli veri türüne (örneğin *Grafikler*) göre kontrol edebilirsiniz.
      - **İçerik kategorilerine ve veri türlerine göre**. İçerik kategorilerine ve veri türlerine göre filtreler etkinleştirilmiştir.

   Filtreleri seçtikten sonra filtre parametrelerini yapılandırın.

c. **Şu kullanıcılara uygula** açılır listesinde, kullanıcılar için ilgili filtreyi seçin:

- **Tüm kullanıcılara**. İnternet Denetimi, internet kaynaklarını adrese göre filtrelemeyecektir.
- **Ayrı ayrı kullanıcılara veya gruplara**. İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

d. **Eylem** açılır listesinden bir seçenek belirleyin:

- **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir.
- **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler.
- **Uyar**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

e. **Kural zamanlaması** açılır listesinde bir zamanlama seçin veya yeni bir zamanlama oluşturun.

7. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

   İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

   Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.

8. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da web kaynak içerik filtresi nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **İnternet Denetimi**'ne gidin.
5. **İnternet Denetimi ETKİN** anahtarını açık konuma getirin.
6. **Kurallar listesi** bloğunda **Ekle** düğmesine tıklayın.

7. Web kaynağı erişim kurallarını yapılandırın:

   a. **Kural adı** alanında, kuralın adını girin veya düzenleyin.

   b. Web kaynağı erişim kuralı için **Etkin** durumunu seçin.

      İstediğiniz zaman web kaynağı erişim kuralını devre dışı bırakmak için geçiş düğmesini kullanabilirsiniz.

   c. **Eylem** bloğundan ilgili seçeneği seçin:

      - **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir.
      - **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler.
      - **Bilgilendir**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

   d. **Kapsam** bölümünden **İçerik kategorisini** seçin.

   e. İçerik filtresini yapılandırın:

      - **İçerik kategorisi**. Kullanıcıların internet kaynaklarına erişimini kategoriye göre kontrol edebilirsiniz (örneğin, *Sosyal ağlar* kategorisi).
      - **Veri tipi**. İnternet kaynaklarına kullanıcı erişimini, yayınlanan verilerinin belirli veri türüne (örneğin *Grafikler*) göre kontrol edebilirsiniz.

   f. **Kullanıcı veya grup** bölümünde, İnternet Denetimi'nin kuralı uygulamasını istediğiniz kullanıcıları seçin.

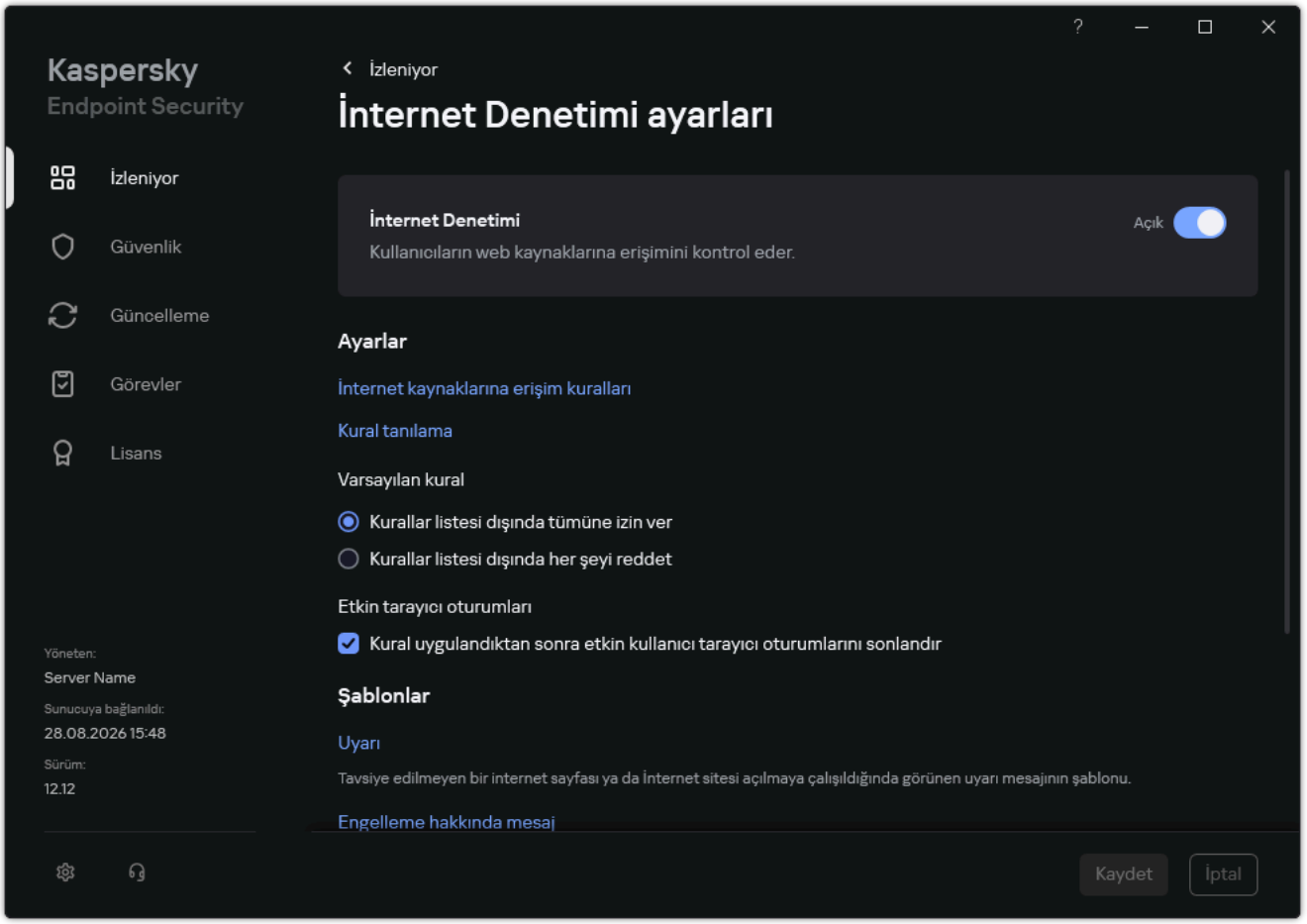
      İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   g. **Erişim zamanlaması** bloğunda bir zamanlama seçin veya yeni bir zamanlama oluşturun.

8. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir web kaynağı içerik filtresi nasıl etkinleştirilir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **Ayarlar** bloğunda, **İnternet kaynaklarına erişim kuralları** düğmesine tıklayın.
4. Açılan pencerede **Ekle** düğmesine tıklayın.
   İnternet kaynaklarına erişim kuralı penceresi açılır.
5. **Kural adı** alanında, kuralın adını girin veya düzenleyin.
6. Web kaynağı erişim kuralı için **Açık** durumunu seçin.
   İstediğiniz zaman web kaynağı erişim kuralını devre dışı bırakmak için geçiş düğmesini kullanabilirsiniz.
7. **Eylem** bloğundan ilgili seçeneği seçin:
   - **İzin ver**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişime izin verir.
   - **Engelle**. İnternet Denetimi, kuralın parametreleriyle eşleşen web kaynaklarına erişimi engeller ve bir web sitesi erişim engellendi mesajı görüntüler.
   - **Uyar**. Kullanıcı kuralla eşleşen bir web kaynağına erişmeye çalıştığında, İnternet Denetimi web kaynağını ziyaret etmenin tavsiye edilmediğini belirten bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

8. **Filtrenin içeriği** bloğundan ilgili içerik filtresini seçin:

   - **İçerik kategorilerine göre**. Kullanıcıların internet kaynaklarına erişimini kategoriye göre kontrol edebilirsiniz (örneğin, *Sosyal ağlar* kategorisi).

   - **Veri türlerine göre**. İnternet kaynaklarına kullanıcı erişimini, yayınlanan verilerinin belirli veri türüne (örneğin *Grafikler*) göre kontrol edebilirsiniz.

   İçerik filtresini yapılandırmak için:

   a. **Ayarlar** bağlantısına tıklayın.

   b. 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.

   c. Web kaynağı erişim kuralını yapılandırmak için pencereye geri dönün.

9. **Kullanıcılar** bloğundan kullanıcılar için ilgili filtreyi seçin:

   - **Tüm kullanıcılara**. İnternet Denetimi, internet kaynaklarını adrese göre filtrelemeyecektir.

   - **Tek tek kullanıcılara ve/veya gruplara uygula**. İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Bir web adresi girebilir ya da maskeler kullanabilirsiniz. Ayrıca, bir TXT dosyasından web kaynağı adreslerinin bir listesini dışa aktarabilirsiniz. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir. Kuralı uygulamak istediğiniz kullanıcıların bir listesini oluşturmak için:

     a. **Ekle**'ye tıklayın.

     b. Açılan pencerede, web kaynağı erişim kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.

     c. Web kaynağı erişim kuralını yapılandırmak için pencereye geri dönün.

10. **Kural zamanlaması** açılır listesinde, gereken zamanlamanın adını seçin veya seçilen kural zamanlamasına dayalı olarak yeni bir zamanlama oluşturun. Bunun için:

    a. **Düzenle veya yeni ekle**'ye tıklayın.

    b. Açılan pencerede **Ekle** düğmesine tıklayın.

    c. Açılan pencerede, kural zamanlaması adını girin.

    d. Kullanıcılar için web kaynağı erişim zamanlamasını yapılandırın.

    e. Web kaynağı erişim kuralını yapılandırmak için pencereye geri dönün.

11. İnternet Denetiminin ilke uygulandıktan hemen sonra yasaklanan web kaynağıyla bağlantıyı sonlandırmasını istiyorsanız, **Kural uygulandıktan sonra etkin kullanıcı tarayıcı oturumlarını sonlandır** onay kutusunu seçin.

İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar.

Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.

12. Değişikliklerinizi kaydedin.

Sonuç olarak, yeni İnternet Denetimi kuralı listeye eklenir. Gerekirse, İnternet Denetimi kuralının önceliğini değiştirin. Web kaynağı erişim kuralını listeden kaldırmadan istediğiniz zaman devre dışı bırakmak için geçiş düğmesini de kullanabilirsiniz.

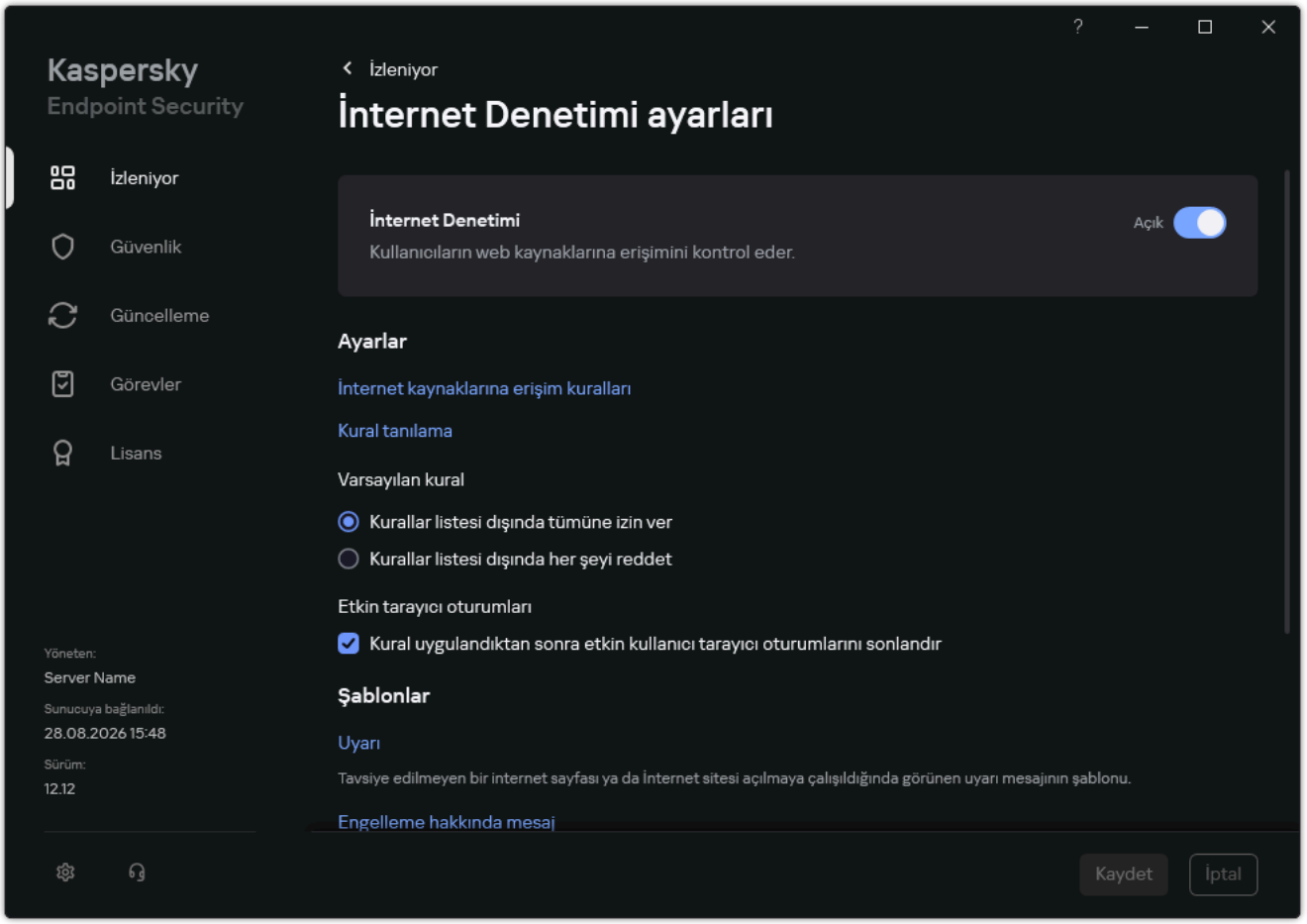
İnternet kaynağı erişim kurallarını test etme

İnternet Denetimini yapılandırırken, kullanıcıların işleri için ihtiyaç duydukları web kaynaklarına erişimi yanlışlıkla engelleyebilirsiniz. Hangi İnternet Denetimi kuralının web kaynaklarına erişimi engellediğini bulmak için *İnternet Denetimi Kuralları tanılama* aracını kullanabilirsiniz. İnternet Denetimi Kuralları tanılaması yalnızca Kaspersky Endpoint Security arabiriminde kullanılabilir. Kaspersky Security Center konsolunda, belirli bir kaynağı hangi İnternet Denetimi kuralının içerdiğini bulamazsınız.

Kullanıcı İnternet kaynağının yanlışlıkla engellendiğini düşünüyorsa yerel kurumsal ağ yöneticisine önceden oluşturulmuş bir mesaj göndermek için İnternet kaynağı engelleme bildirimi mesajındaki bağlantıya tıklayabilir.

İnternet kaynağı erişim kurallarını test etmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **Ayarlar** bloğunda, **Kural tanılama** bağlantısına tıklayın.

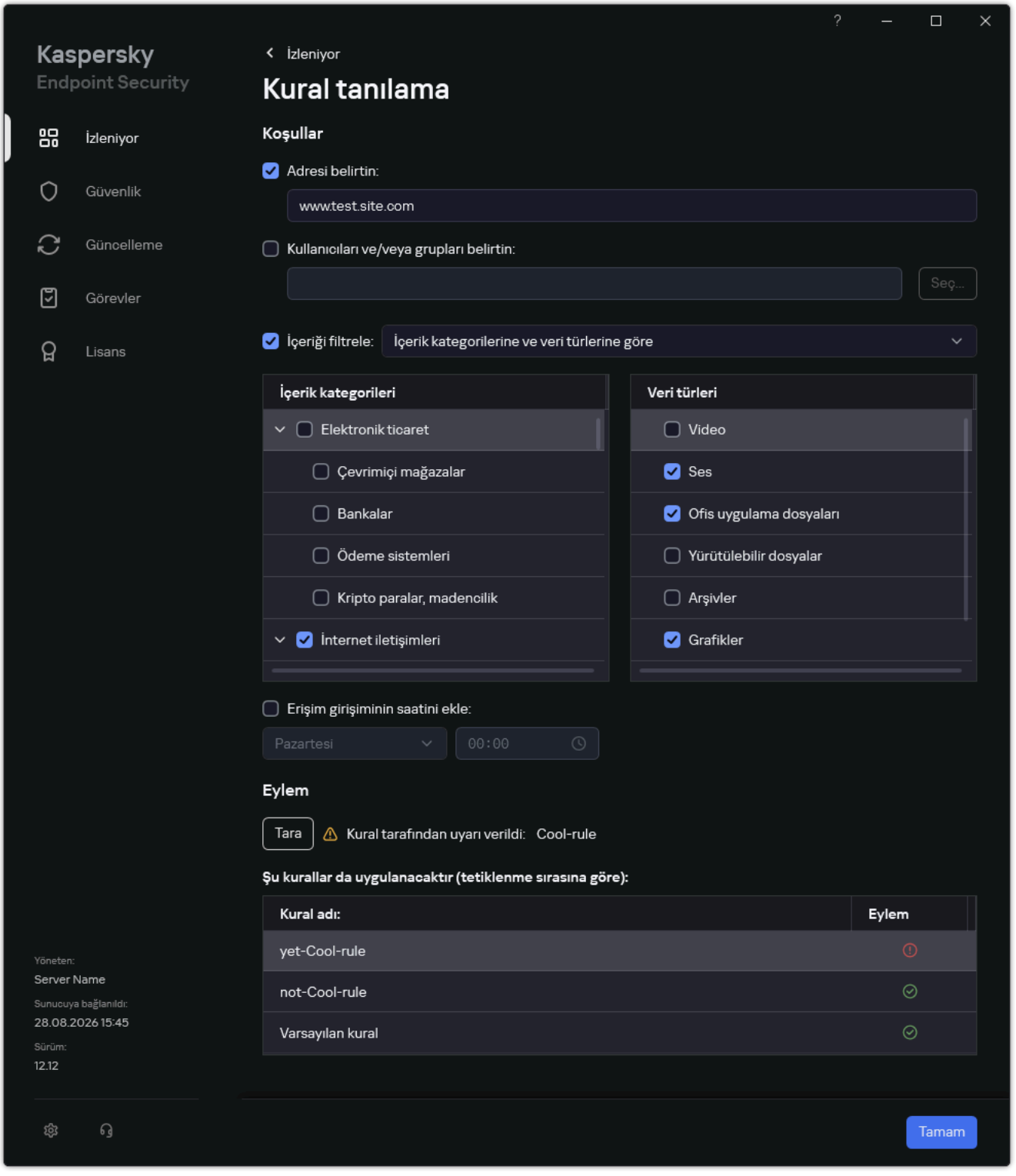
   Kural tanılama penceresi açılır.

4. Kaspersky Endpoint Security'nin belirli bir Web kaynağına erişimi denetlemek için kullandığı kuralları test etmek istiyorsanız, **Adresi belirtin** onay kutusunu seçin. Aşağıdaki alana Web kaynağının adresini girin.
5. 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.
6. Kaspersky Endpoint Security'nin belirli içerik kategorilerinin ve/veya veri türü kategorilerinin İnternet kaynaklarına erişimi denetlemek için kullandığı kuralları test etmek isterseniz, **İçeriği filtrele** onay kutusunu seçin ve açılır listesinden ilgili seçeneği seçin (**İçerik kategorilerine göre**, **Veri türlerine göre** veya **İçerik kategorilerine ve veri türlerine göre**).

7. 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.

8. **Tara**'ya tıklayın.

Testin tamamlanmasının ardından, belirtilen İnternet kaynağına erişim girişiminde tetiklenen ilk kurala göre Kaspersky Endpoint Security tarafından uygulanan işlem (izin ver, engelle veya uyarı) hakkında bilgi yer alan bir mesaj görüntülenir. Tetiklenecek ilk kural, İnternet Denetimi kurallarında tanılama koşullarını karşılayan diğer kurallardan daha yüksek bir sıradaki kuraldır. Mesaj, **Tara** düğmesinin sağında görüntülenir. Aşağıdaki tabloda, Kaspersky Endpoint Security tarafından uygulanan işlemi belirten diğer tetiklenen kurallar yer almaktadır. Kurallar yukarıdan aşağı öncelik sıralamasına göre belirtilmiştir.



Web kaynağı erişim testi sonucu

İnternet Denetimi kurallarını dışa ve içe aktarma

İnternet Denetimi kuralları listesini bir XML veya JSON dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda adres eklemek için dosyayı değiştirebilirsiniz. İnternet Denetimi kuralları listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) İnternet Denetimi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri → İnternet Denetimi** seçimini yapın.
4. İnternet Denetimi kuralları listesini dışa aktarmak için:
   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
      Herhangi bir kural seçmezseniz, Kaspersky Endpoint Security tüm istisnaları dışa aktaracaktır.
   b. **Dışa aktar** bağlantısına tıklayın.
   c. Açılan pencerede, kurallar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
      Kaspersky Endpoint Security, kurallar listesini XML dosyasına aktarır.
5. İnternet Denetimi kuralları listesini içe aktarmak için:
   a. **İçe aktar** bağlantısına tıklayın.
      Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.
   b. Dosyayı aç.
      Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.
6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da İnternet Denetimi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri → İnternet Denetimi**'ne gidin.

5. Kural listesini dışa aktarmak için **Kurallar listesi** bloğunda:

   a. Düzenlemek istediğiniz kuralları seçin.

   b. → **Dışa aktar** düğmesine tıklayın.

   Kaspersky Endpoint Security, kural listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

6. Kural listesini içeri aktarmak için **Kurallar listesi** bloğunda:

   a. → **İçe aktar** düğmesine tıklayın.

   Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.

   b. Dosyayı aç.

   Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

7. Değişikliklerinizi kaydedin.

İnternet Denetimi kuralının web kaynak adreslerini dışa ve içe aktarma

Bir İnternet kaynağı erişim kuralında İnternet kaynağı adreslerinin listesini oluşturduysanız bir dosyasına dışa aktarabilirsiniz:

- Yönetim Konsolunda (MMC) TXT biçiminde
- Web Console'da JSON biçiminde
- Uygulama arabiriminde CSV biçiminde

Ardından bir erişim kuralını yapılandırırken İnternet kaynağı adreslerinin yeni listesini manuel olarak 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.

Ayrıca, sadece tek bir kuralın web kaynağı adreslerini değil, tüm İnternet Denetimi kurallarını dışa/içe aktarabilirsiniz.

Yönetim Konsolu'nda (MMC) İnternet Denetimi kuralının web kaynak adresleri nasıl dışa/içe aktarılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi** seçimini yapın.
5. **İnternet Denetimi ayarları** bloğunda, web kaynağı adresleri listesini vermek veya almak istediğiniz kuralı seçin.

   İnternet Denetimi kural özellikleri görüntülenir.

6. Web kaynakları listesini dışa aktarmak için adres listesinde şunları yapın:

   a. Dışa aktarmak istediğiniz adresleri seçin.

      Herhangi bir adres seçmezseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.

   b. düğmesine tıklayın.

   c. Açılan pencerede, web kaynağı adreslerinin listesini dışa aktarmak istediğiniz TXT dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, web kaynağı adreslerinin listesini bir TXT dosyasına dışa aktarır.

7. Web kaynakları listesini içe aktarmak için adres listesinde şunları yapın:

   a. düğmesine tıklayın.

      Açılan pencerede, internet kaynakları listesini içe aktarmak için kullanmak istediğiniz TXT dosyasını seçin.

   b. Dosyayı aç.

      Bilgisayar zaten bir adresler listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye TXT dosyasından yeni girişler ekler.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da İnternet Denetimi kuralının web kaynağı adreslerini dışa/içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **İnternet Denetimi**'ne gidin.

5. **Kurallar listesi** bloğunda, web kaynağı adresleri listesini dışa veya içe aktarmak istediğiniz kuralı seçin.

   İnternet Denetimi kural özellikleri görüntülenir.

6. **Kapsam** → **Tek tek web siteleri** bloğunda **Düzenle** düğmesine tıklayın.

7. Web kaynakları listesini dışa aktarmak için adres listesinde şunları yapın:

   a. Dışa aktarmak istediğiniz adresleri seçin.

   b. → **Dışa aktar** düğmesine tıklayın.

      Kaspersky Endpoint Security, web kaynağı adreslerinin listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

8. Web kaynakları listesini içe aktarmak için adres listesinde şunları yapın:

   a. → **İçe aktar** düğmesine tıklayın.

      Açılan pencerede, web kaynağı adresleri listesini içe aktarmak istediğiniz JSON dosyasını seçin.

b. Dosyayı aç.

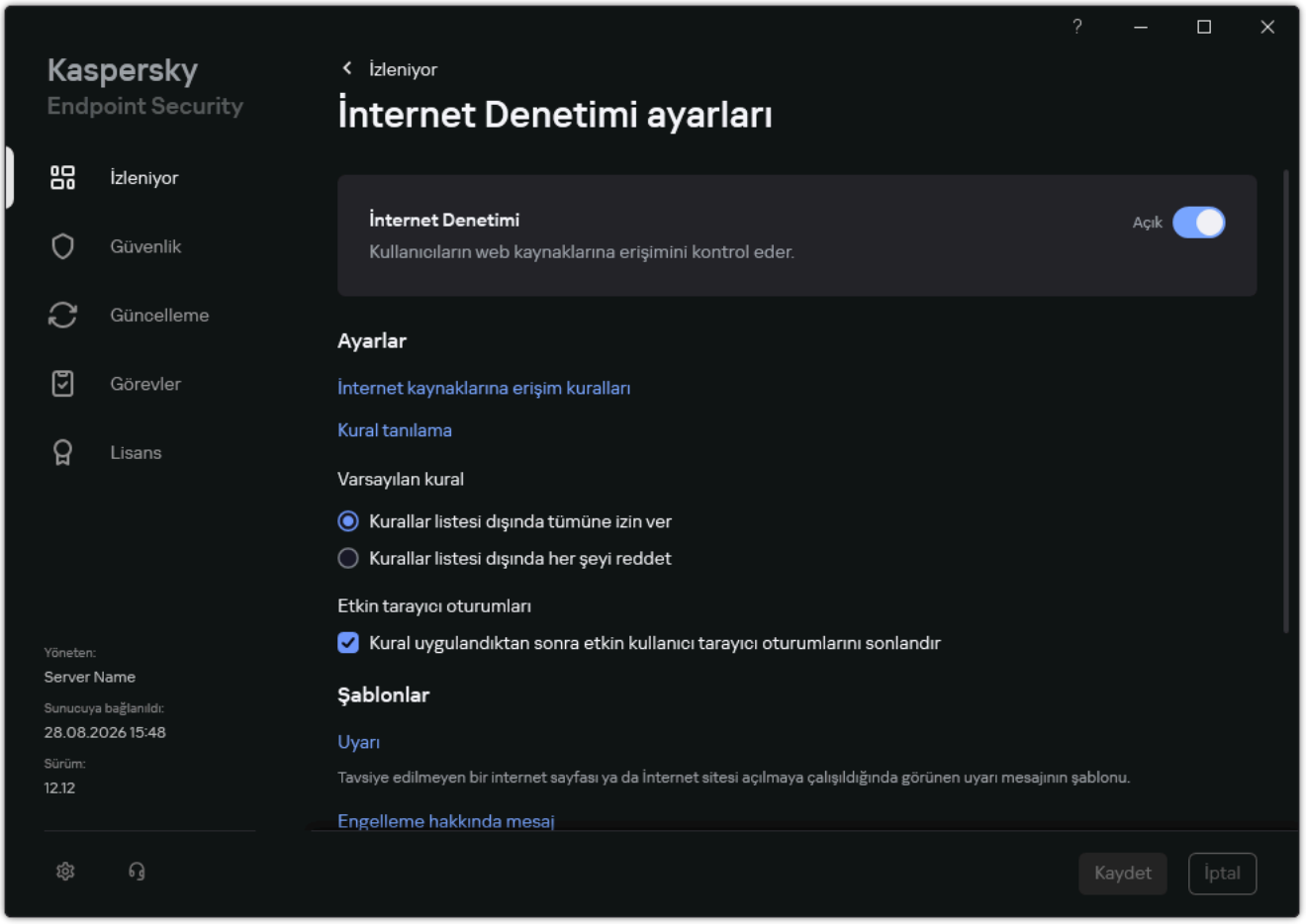
Bilgisayar zaten bir adresler listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

Web sitesi gruplarını da aynı şekilde dışa ve içe aktarabilirsiniz.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde İnternet Denetimi kuralının web kaynak adreslerini dışa/içe aktarma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **Ayarlar** bloğunda, **İnternet kaynaklarına erişim kuralları** düğmesine tıklayın.
4. İnternet kaynağı adreslerinin listesini içe/dışa aktarmak istediğiniz kuralı seçin.
5. Güvenilir web adreslerinin listesini dışa aktarmak için **Adresler** bloğunda şunları yapın:

a. Dışa aktarmak istediğiniz adresleri seçin.

Herhangi bir adres seçmezseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.

b. **Dışa aktar**'a tıklayın.

c. Açılan pencerede, web kaynağı adreslerinin listesini dışa aktarmak istediğiniz CSV dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

d. Dosyaya kaydet.

Kaspersky Endpoint Security, web kaynağı adreslerinin listesini bir CSV dosyasına dışa aktarır.

6. İnternet kaynakları listesini içe aktarmak için **Adresler** bloğunda şunları yapın:

a. **İçe aktar**'a tıklayın.

Açılan pencerede, internet kaynakları listesini içe aktarmak için kullanmak istediğiniz CSV dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir adresler listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye CSV dosyasından yeni girişler ekler.

7. Değişikliklerinizi kaydedin.

Kullanıcı İnternet etkinliğini ileme

Kaspersky Endpoint Security, izin verilenler de dahil olmak üzere tüm web sitelerine yapılan kullanıcı ziyaretlerinin verilerini günlük dosyası olarak saklamanıza izin verir. Böylece tarayıcı görüntülemelerinizin tam bir geçmişine sahip olursunuz. Kaspersky Endpoint Security, kullanıcı etkinliği olaylarını Kaspersky Security Center'a, Kaspersky Endpoint Security'nin yerel günlük kaydına ve Windows Olay günlüğüne gönderir. Olayları Kaspersky Security Center'da almak için Yönetim Konsolu'nda veya Web Console'da bir ilke olarak olaylar için ayarlar yapılandırmanız gerekir. İnternet Denetimi olaylarının aktarımını e-posta ile de yapılandırabilir ve ekran bildirimlerini kullanıcının bilgisayarında görüntüleyebilirsiniz.

İzleme işlevini destekleyen tarayıcılar: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Kullanıcı etkinliği izleme diğer tarayıcılarda çalışmaz.

Kaspersky Endpoint Security şu İnternet etkinliği olaylarını oluşturur:

- Web sitesini engelleme (*Kritik* durumu ⓘ).
- Önerilmeyen bir web sitesini ziyaret etme (*Uyarı* durumu ⚠).
- İzin verilen bir web sitesine ziyaret (*Bilgi* durumu ⓘ).

Kullanıcı İnternet etkinliği izlemeyi etkinleştirmeden önce aşağıdakileri yapmanız gerekir:

- İnternet trafiğine bir web sayfası etkileşim komut dosyası ekleyin (aşağıdaki talimatlara bakın). Komut dosyası, İnternet Denetimi olaylarının kaydını sağlar.
- HTTPS trafiğini izleme için şifrelenmiş bağlantı taramasını etkinleştirin.

Bir web sayfası etkileşim komut dosyası enjekte etme

Yönetim Konsolu'nda (MMC) web trafiğine bir web sayfası etkileşim komut dosyası enjekte etme

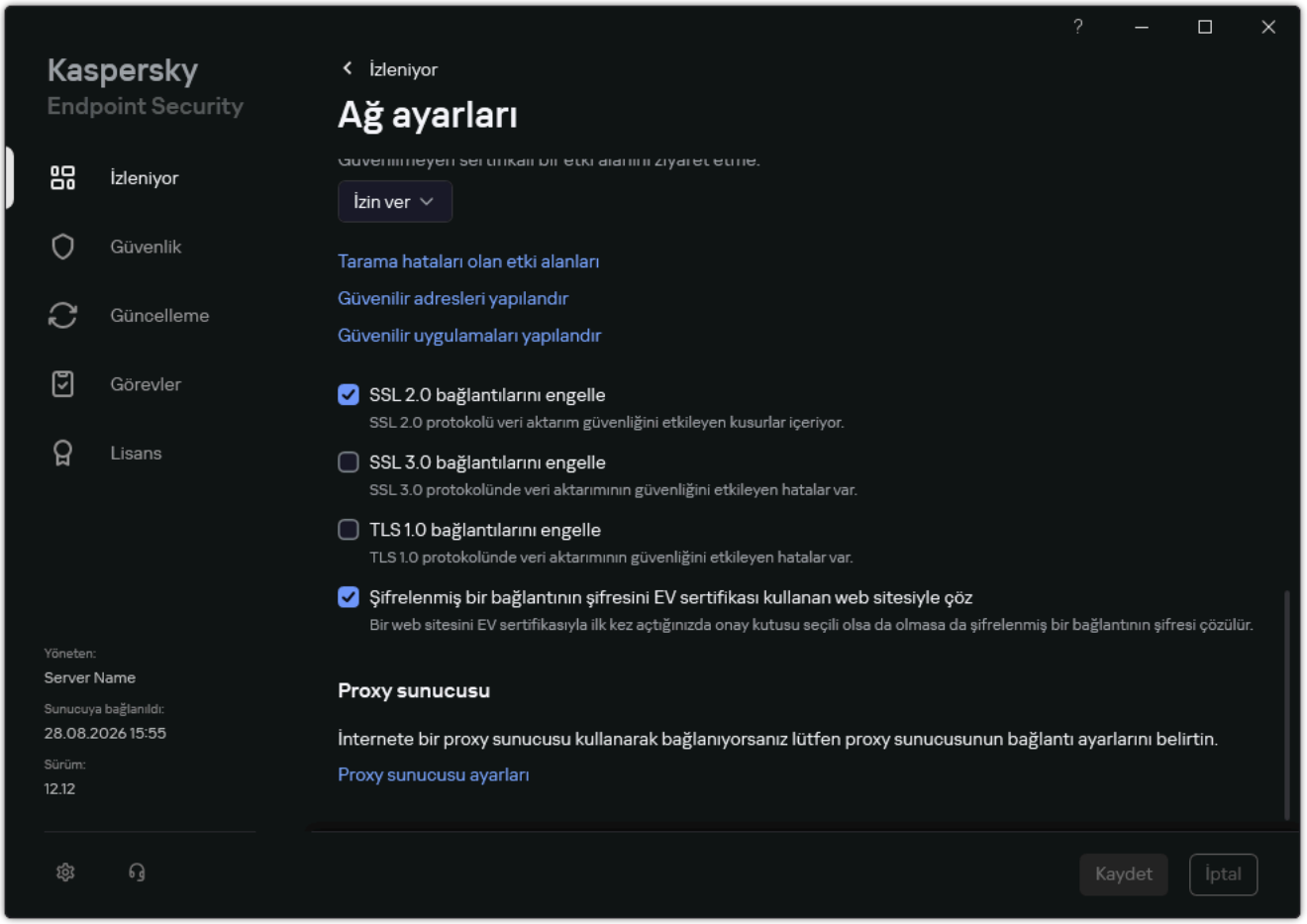
1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
4. **Şifreli bağlantıları tarama** bloğundan, **Web sayfalarıyla etkileşim için internet trafiğine komut yerleştir** onay kutusunu işaretleyin.
5. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da web trafiğine bir web sayfası etkileşim komut dosyası enjekte etme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
5. **İnternet bağlantılarının izlenmesi** altında, **İnternet bağlantılarının izlenmesi ETKİN** anahtarını açık duruma getirin.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde web trafiğine bir web sayfası etkileşim komut dosyası enjekte etme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



Uygulama ağ ayarları

3. **Trafik işleme** bloğundan, **Web sayfalarıyla etkileşim için internet trafiğine komut yerleştir** onay kutusunu işaretleyin.
4. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security, internet trafiğine bir web sayfası etkileşim komut dosyası ekleyecektir. Bu komut dosyası, uygulama olay günlüğü, işletim sistemi olay günlüğü ve raporlar için İnternet Denetimi olaylarının kaydını sağlar.

İnternet Denetimi olaylarının günlüğe kaydedilmesini yapılandırma

İnternet Denetimi olaylarının kullanıcının bilgisayarına günlük kaydını yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
3. **Bildirimler** bloğunda **Bildirimleri yapılandır** düğmesine tıklayın.

4. Açılan pencerede, **İnternet Denetimi** bölümünü seçin.

   Böylece İnternet Denetimi olayları tablosu ve bildirim yöntemleri açılır.

5. Her etkinlik için bildirim yöntemini yapılandırın: **Yerel rapora kaydet** ya da **Windows Olay Günlüğüne kaydet**.

   İzin verilen web sitesi ziyaret etkinliklerini günlüğe kaydetmek için İnternet Denetimi yapılandırması da yapmanız gerekir (aşağıdaki talimatlara bakın).

   Etkinlikler tablosunda ekran bildirimini ve e-posta bildirimini etkinleştirebilirsiniz. Bildirimleri e-posta ile göndermek için SMTP sunucu ayarlarını yapılandırmalısınız. E-posta ile bildirimler göndermekle ilgili daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

6. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security kullanıcının İnternet etkinlik olaylarının günlük kaydını yapmaya başlar.

İnternet Denetimi, kullanıcı etkinliklerini Kaspersky Security Center'a şu şekilde gönderir:

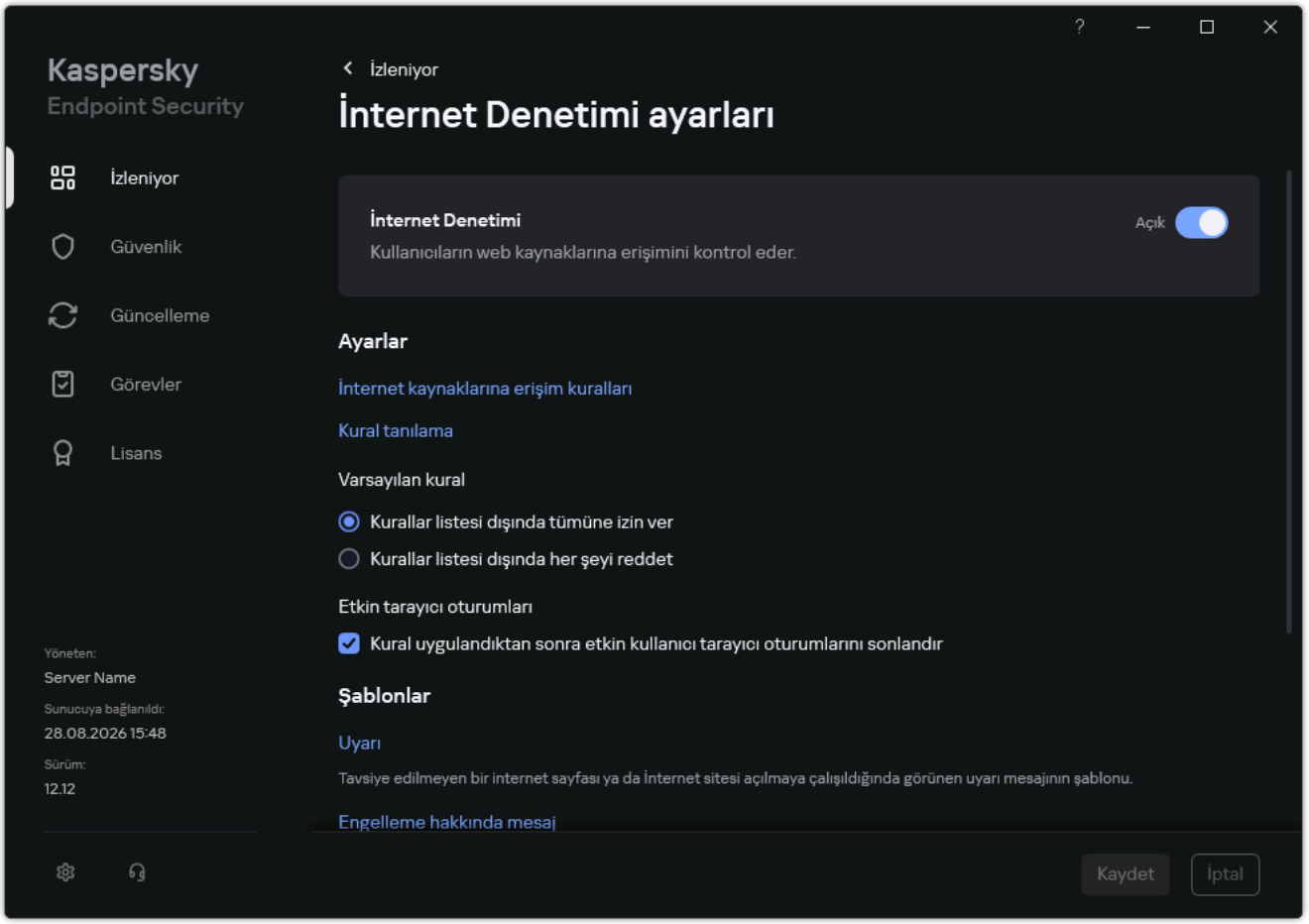
- Kaspersky Security Center'ı kullanıyorsanız İnternet Denetimi, İnternet sayfasını meydana getiren tüm nesneler için etkinlikleri gönderir. Bu nedenle, bir web sayfası engellendiğinde birden fazla olay oluşturulabilir. Örneğin, http://www.example.com şeklinde bir web sayfası engellenirken, Kaspersky Endpoint Security şu nesneler için etkinlikleri iletebilir: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js gibi.

- Kaspersky Security Center Cloud Console kullanıyorsanız, İnternet Denetimi etkinlikleri gruplar ve sadece İnternet sitesinin protokolünü ve etki alanını gönderir. Örneğin bir kullanıcı http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery şeklindeki önerilmeyen İnternet sitelerini ziyaret ederse, Kaspersky Endpoint Security sadece http://www.example.com nesnesi ile bir etkinlik gönderecektir.

İzin verilen web siteleri ziyaret edildiğinde olay günlük kaydı

İzin verilen web siteleri ziyaret edildiğinde olay günlük kaydını etkinleştirmek için:

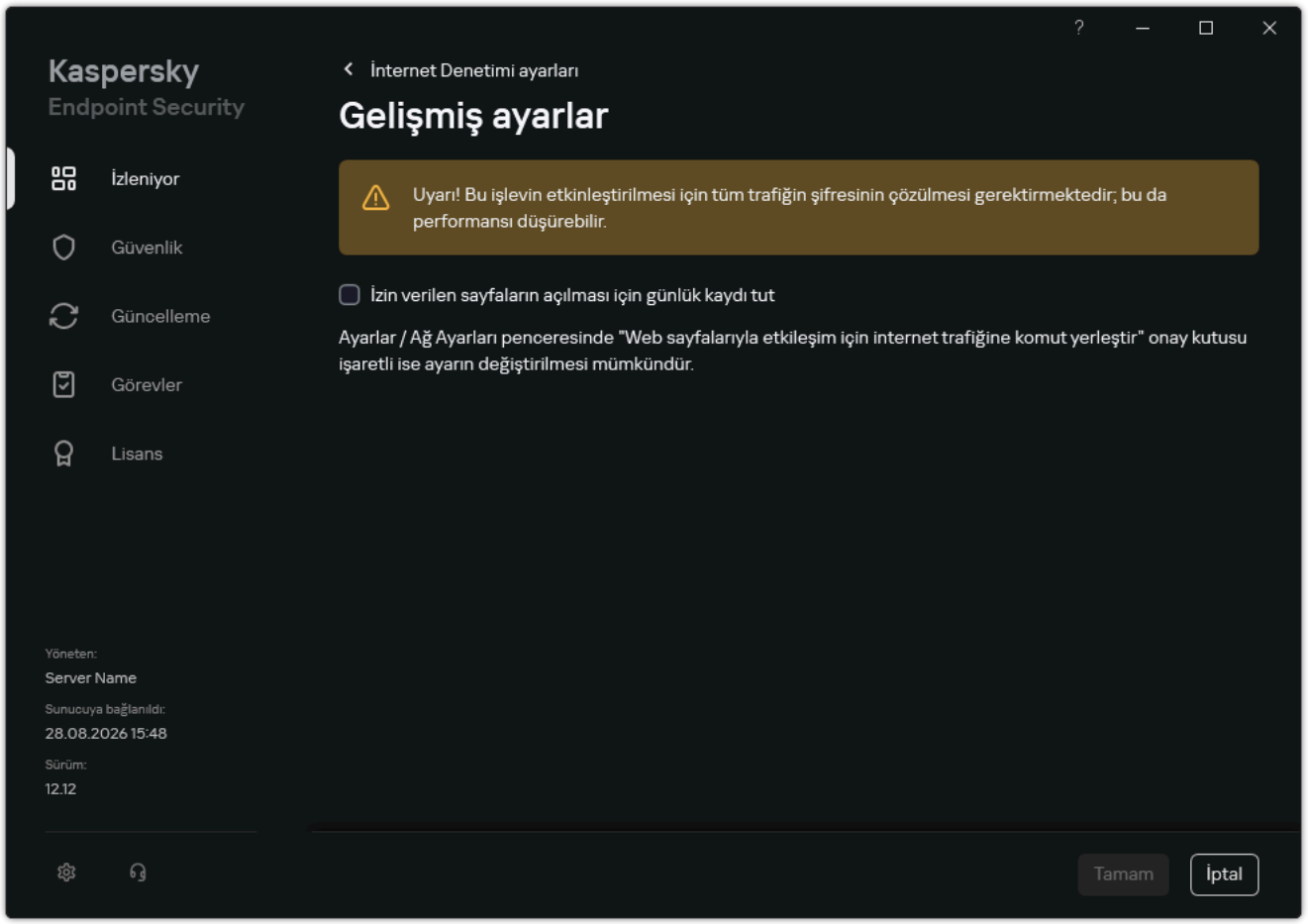
1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **Diğer** bloğunda **Gelişmiş ayarlar** düğmesine tıklayın.

4. Açılan pencerede, **İzin verilen sayfaların açılması için günlük kaydı tut** kutucuğunu işaretleyin.



İnternet Denetimi gelişmiş ayarları

5. Değişikliklerinizi kaydedin.

Sonuç olarak tüm tarayıcı geçmişini görüntülemeniz mümkün olacaktır.

İnternet Denetimi mesajlarının şablonlarını düzenleme

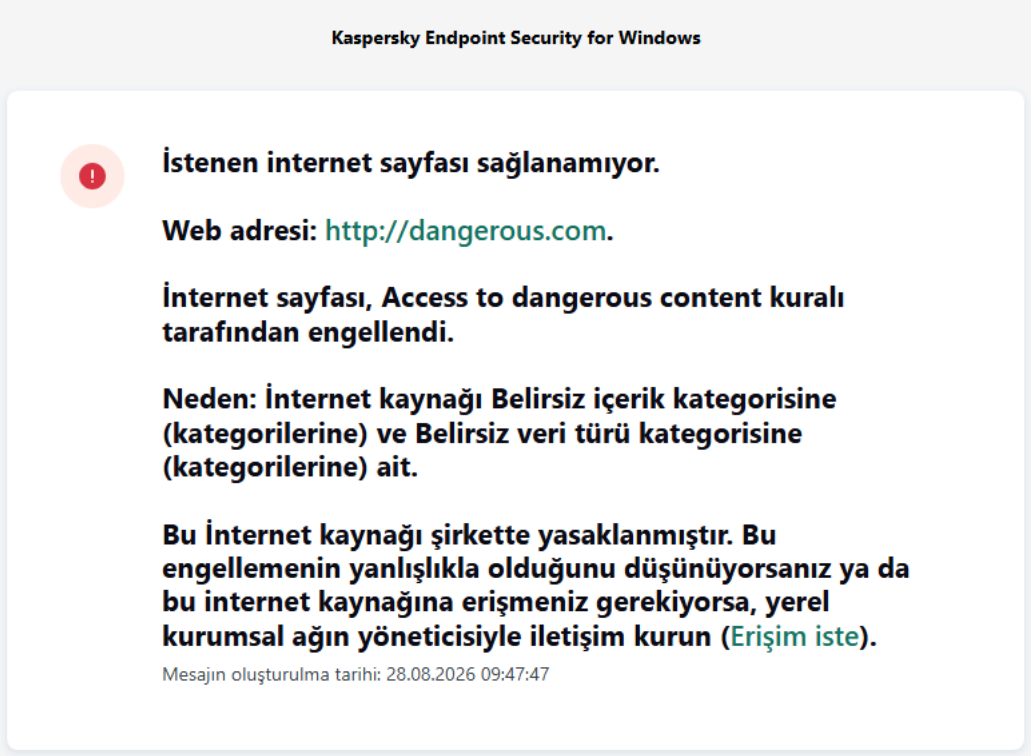
İnternet Denetimi kurallarının özelliklerinde belirtilen eylem türüne bağlı olarak Kaspersky Endpoint Security, kullanıcının İnternet kaynaklarına erişmeye çalıştığı zamanda aşağıdaki türden bir mesaj görüntüler (uygulama, HTML sayfasını HTTP sunucu yanıtı mesajı ile değiştirir):

- 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 **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 **Engelle** seçeneği seçilirse Kaspersky Endpoint Security, İnternet kaynağının engellendiğini bildiren bir mesaj görüntüler (aşağıdaki şekle bakın).

Kullanıcı İnternet kaynağının yanlışlıkla engellendiğini düşünüyorsa yerel kurumsal ağ yöneticisine önceden oluşturulmuş bir mesaj göndermek için İnternet kaynağı engelleme bildirimi mesajındaki bağlantıya tıklayabilir.



Web kaynaklarını engelleme hakkında mesaj

Uyarı mesajı, bir İnternet kaynağının engellendiğini bildiren mesaj ve LAN yöneticisine gönderilen mesaj için özel şablonlar sağlanmaktadır. Mesaj şablonlarını yönetmek için özel değişkenler sağlanır (örneğin, `%USER_NAME%`). Değişkenler, tek bir mesaj şablonunun farklı bilgisayarlar için kullanılmasına olanak tanır. Bir mesaj oluştururken, Kaspersky Endpoint Security değişkenin değerini işletim sistemi ayarlarından alır ve belirli bilgisayar, kullanıcı ve olayla eşleşen mesaja ekler.

Yönetim Konsolu'ndaki (MMC) İnternet Denetimi mesaj şablonu nasıl değiştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi** seçimini yapın.
4. **Mesaj şablonu ayarları** bloğunda, **Şablonlar** düğmesine tıklayın.
5. İnternet Denetimi mesaj şablonlarını yapılandırın:

   - **Uyarı**. Giriş alanı, istenmeyen bir İnternet kaynağına erişme girişimleri hakkında uyarı amaçlı bir kural tetiklendiğinde görüntülenen mesaj şablonundan oluşur.
   - **Engelleme hakkında mesaj**. Giriş alanı, bir İnternet kaynağına erişimi engelleyen bir kural tetiklenirse görüntülenen mesajın şablonunu içerir.
   - **Yöneticiye mesaj**. Kullanıcının engellemenin bir hata olduğunu değerlendirmesi halinde LAN yöneticisine gönderilecek mesaj şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için web sayfası erişimini engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken**'e tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

Varsayılan olarak düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.

6. Değişikliklerinizi kaydedin.

İnternet Denetimi mesaj şablonu Web Console'da ve Cloud Console'da nasıl değiştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **İnternet Denetimi**'ne gidin.
5. **Mesaj şablonları** bloğunda, **Web sitesi engelleme hakkında mesaj** bağlantısına tıklayın ve İnternet Denetimi mesajları için şablonları yapılandırın:

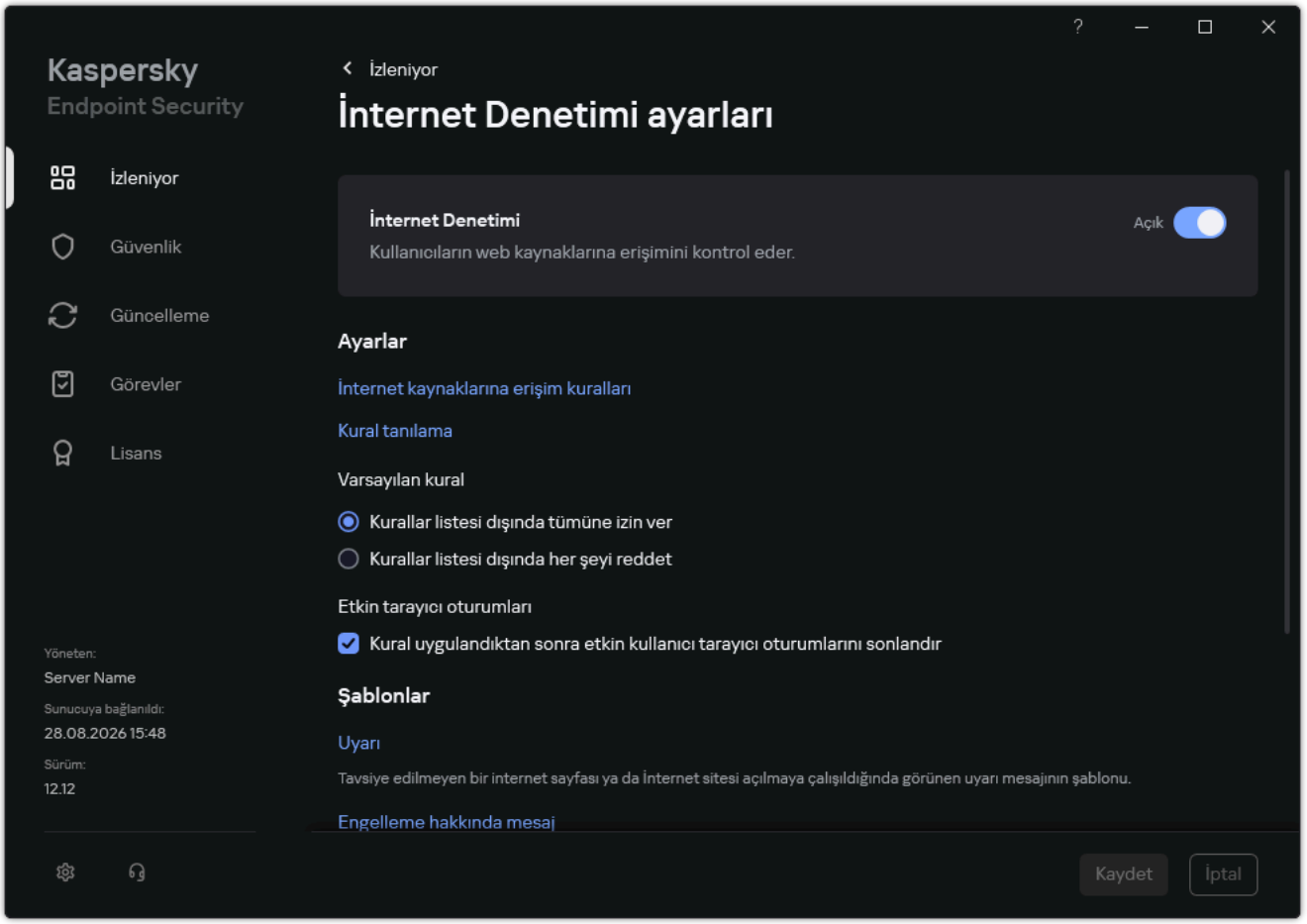
   - **Uyarı**. Giriş alanı, istenmeyen bir İnternet kaynağına erişme girişimleri hakkında uyarı amaçlı bir kural tetiklendiğinde görüntülenen mesaj şablonundan oluşur.
   - **Engelleme hakkında mesaj**. Giriş alanı, bir İnternet kaynağına erişimi engelleyen bir kural tetiklenirse görüntülenen mesajın şablonunu içerir.
   - **Yöneticiye mesaj**. Kullanıcının engellemenin bir hata olduğunu değerlendirmesi halinde LAN yöneticisine gönderilecek mesaj şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için web sayfası erişimini engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılana sıfırla düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde İnternet Denetimi mesaj şablonu nasıl değiştirilir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.



İnternet Denetimi ayarları

3. **Şablonlar** bloğunda, İnternet Denetimi mesajları için şablonları yapılandırın:

   - **Uyarı**. Giriş alanı, istenmeyen bir İnternet kaynağına erişme girişimleri hakkında uyarı amaçlı bir kural tetiklendiğinde görüntülenen mesaj şablonundan oluşur.
   - **Engelleme hakkında mesaj**. Giriş alanı, bir İnternet kaynağına erişimi engelleyen bir kural tetiklenirse görüntülenen mesajın şablonunu içerir.
   - **Yöneticiye mesaj**. Kullanıcının engellemenin bir hata olduğunu değerlendirmesi halinde LAN yöneticisine gönderilecek mesaj şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için web sayfası erişimini engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Sıfırla düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.

4. Değişikliklerinizi kaydedin.

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. Örnek: `http://www.example.com/page_0-9abcdef.html`.

2. `*.` dizisi karakterler (bir *etki alanı maskesi* olarak bilinir) bir adresin tüm etki alanlarını seçmenize izin verir. `*.` etki alanı maskesi, herhangi bir etki alanını, alt etki alanını veya boş bir satırı temsil eder.

   Örnek: `*.example.com` maskesi aşağıdaki adresleri temsil eder:

   - `http://pictures.example.com`. Etki alanı maskesi `*.` `pictures.` temsil eder.
   - `http://user.pictures.example.com`. `*.` etki alanı maskesi `pictures.` ve `user.` temsil eder.
   - `http://example.com`. `*.` etki alanı maskesi boş bir satır olarak yorumlanır.

3. Adres maskesinin başındaki `www.` karakter dizisi, `*.` dizisi olarak yorumlanır.

   Örneğin: `www.example.com` adres maskesi `*.example.com` olarak yorumlanır. Bu maske `www2.example.com` ve `www.pictures.example.com` adreslerini kapsar.

4. Adres maskesi `*` karakteri ile başlamıyorsa adres maskesinin içeriği `*.` ön ekli aynı içeriğe eşdeğerdir.

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 eki ile 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.

     Örnek: adres maskesi `example.com`, `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, port ve karakterin büyük/küçük harf durumu göz önünde bulundurulur.

Adres maskeleri oluştururken kuralların nasıl kullanılacağının örnekleri

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	2. 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	3., 2. ve 1. kurala bakınız.
7	www.example.com	https://www.example.com	Evet	3., 2. ve 1. kurala bakınız.
8	http://www.*.example.com	http://123.example.com	Evet	3., 4. ve 1. kurala bakınız.
9	www.example.com	http://www.example.com/abc	Evet	3., 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.

Sanal makineler için İnternet Denetimi

İnternet Denetimi, bilgisayardaki trafiğin yanı sıra bilgisayarda yerel olarak dağıtılmış bir sanal makine üzerindeki trafiği de denetler. Bu, Kaspersky Endpoint Security uygulamasını yerel sanal makineye yüklemek zorunda kalmadan çalışır. Bu, kullanıcı *sanal makinedeki* bir tarayıcıda İnternet Denetimi kuralı tarafından engellenen bir web sitesini açmaya çalıştığında, *bilgisayarın* ana işletim sisteminde yüklü olan uygulamanın bu web sitesine erişimi reddedeceği anlamına gelir.

İnternet Denetimi farklı sanal makinelerde farklı şekilde çalışır.

Oracle VM VirtualBox

Kaspersky Endpoint Security, Oracle VM VirtualBox sanal makinelerindeki İnternet Denetimi kurallarını sınırlama olmaksızın destekler. Uygulama, sanal makinenin tüm trafiğini kontrol edebilir. İnternet Denetimi kurallarında kullanıcıya göre bir filtre yapılandırılırsa, sanal makinelerin tüm işlemleri yerel kullanıcı tarafından başlatıldığı için uygulama doğru şekilde çalışır.

VMware Workstation

Kaspersky Endpoint Security, VMware Workstation sanal makinelerinde İnternet Denetimi kurallarını sınırlamalarla destekler. Uygulama, kullanıcı tarafından yapılandırılmış bir filtreye sahip kuralları desteklemez. Sanal makine işlemleri sistem kullanıcısı (SYSTEM) altında çalışır. Bu, sanal makinede web sitesini açmaya çalışan kullanıcıyı tanımlamayı imkansız hale getirir.

Microsoft Hyper-V

Kaspersky Endpoint Security, Microsoft Hyper-V sanal makinelerinde İnternet Denetimi kurallarını desteklemez.

İnternet Denetimi mesaj şablonlarındaki değişkenler

Kullanıcı mesajı şablonlarında veya yönetici mesajı şablonlarında aşağıdaki değişkenleri kullanabilirsiniz:

- **Kullanıcı adı** – `%USER_NAME%`.

  İletinin oluşturulduğu bilgisayardaki geçerli kullanıcı hesabının adı; `<device name>\<user alias>` format (for example, `DESKTOP-123\John.Smith`).

- **Web kaynağı adresi** – `%CANONIC_REQUEST_URL%`.

  Engellenen web kaynağının adresi.

- **Kural adı** – `%RULE%`.

  Web kaynağını engelleyen kuralın adı.

- **Mesaj gönderme e-postası** – `%COMPLAIN_EMAIL%`.

  Web kaynak blokları hakkında geri bildirim için e-posta adresi. E-posta adresine tıklandığında, kullanıcının yöneticiye mesaj yazabileceği bir pencere açılır.

- **İçerik kategorisi adı** – `%CONTENT_CATEGORY_LIST%`.

  Engellenen kaynağın ait olduğu web sitesi kategorisi (örneğin, *Ödeme sistemleri*).

- **Veri türü kategorisi adı** – `%TYPE_CATEGORY_LIST%`.

  Engellenen web kaynağındaki veri türü kategorisi (örneğin, *Grafikler*).

- **İstenen internet kaynağına bağlantı** – %CONTINUE_PAGE%.

  İstenen web sayfasına bağlantı (örneğin, `http://www.example.com/pagename.html`).

- **Web sitesine bağlantı** – %CONTINUE_SITE%.

  İstenen web sayfasını içeren web sitesine bağlantı (örneğin, `http://www.example.com/`).

- **Etki alanlarına erişim bağlantısı** – %CONTINUE_DOMAIN%.

  Bu bağlantıya tıklayarak alan adına ait tüm mevcut web sayfalarına erişim sağlanabilir. Örneğin, engellenen web sayfasının adresi `http://www.example.com` ise, %CONTINUE_DOMAIN% değişkeni `http://*.example.com` bağlantısı ile değiştirilir. Bu bağlantıya tıklandığında, alt alan adları da dahil olmak üzere `http://www.example.com/` http://www.example.com/ temel alan adının tüm web adreslerine erişim sağlanır; örneğin, `http://start.example.com/*` veya `http://domain.domain.example.com/*`, burada * karakteri herhangi bir karakter dizisini (boş bir dize dahil) temsil eder.

Aygıt Denetimi

Aygıt Denetimi, bilgisayara yüklenen veya bağlanan aygıtlara (örneğin sabit sürücüler, kameralar veya Wi-Fi modülleri) kullanıcı erişimini yönetir. Bu, bu tür cihazlar bağlandığında bilgisayarı enfeksiyondan korumanıza ve veri kaybını veya veri sızıntılarını önlemenize olanak tanır.

Aygıt Denetimi etkinleştirilirse, uygulama bağlı cihazlar hakkındaki bilgileri Kaspersky Security Center'a aktarır. Bağlı cihazların listesini Kaspersky Security Center'daki **Gelişmiş** → **Veri havuzları** → **Donanım** klasöründe görüntüleyebilirsiniz.

Cihaz erişim düzeyleri

Aygıt Denetimi aşağıdaki düzeylerde erişimi denetler:

- **Aygıt türü**. Örneğin yazıcılar, çıkarılabilir sürücüler ve CD/DVD sürücüleri.

  Aygıt erişimini aşağıdaki şekilde yapılandırabilirsiniz:

  - İzin ver – .
  - Engelle – .
  - Kurallara göre (yalnızca yazıcılar ve taşınabilir cihazlar) – .
  - Bağlantı veriyoluna bağlıdır (Wi-Fi hariç) – .
  - İstisnalarla engelle (yalnızca Wi-Fi) - .

- **Bağlantı veri yolları**. *Bağlantı veri yolu*, bilgisayara aygıtları (örneğin USB veya FireWire) bağlamak için kullanılan bir arabirimdir. Cihaz tipi için **Bağlantı veriyoluna bağlıdır** modu seçilirse, uygulama bağlantı arabirimine (örneğin USB) bağlı olarak cihaza erişime izin verir veya erişimi reddeder.

  Aygıt erişimini aşağıdaki şekilde yapılandırabilirsiniz:

  - İzin ver – .
  - Engelle – .

- **Güvenilir aygıtlar**. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

  Güvenilir aygıtları aşağıdaki verilere göre ekleyebilirsiniz:

  - **Kimliğe göre aygıtlar**. Her cihazın benzersiz bir tanımlayıcısı (Hardware ID veya HWID) vardır. Bu kimliği, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. Cihaz kimliği örneği: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Birkaç belirli cihazı eklemek istiyorsanız cihazları kimliğe göre eklemek uygundur.

  - **Modele göre aygıtlar**. Her cihazın bir Vendor ID (VID) ve bir Product ID (PID) vardır. Bu kimlikleri, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. VID ve PID girme şablonu: `VID_1234&PID_5678`. Kuruluşunuzda belirli bir model cihazlar kullanıyorsanız cihazları modele göre eklemek uygundur. Böylece bu model tüm cihazları ekleyebilirsiniz.

  - **Kimlik maskesine göre aygıtlar**. Benzer kimliklere sahip birden fazla cihaz kullanıyorsanız, cihazları güvenilir listeye maskeler kullanarak ekleyebilirsiniz. `*` karakteri herhangi bir karakter kümesinin yerini alır. Kaspersky Endpoint Security, bir maske girişi yapılırken `?` karakterinin kullanımını desteklemez. Örneğin, `WDC_C*`.

  - **Model maskesine göre aygıtlar**. Benzer VID veya PID sahibi birden fazla aygıt kullanıyorsanız (örneğin aynı üreticinin aygıtları) maskeler kullanarak güvenilir listeye aygıt ekleyebilirsiniz. `*` karakteri herhangi bir karakter kümesinin yerini alır. Kaspersky Endpoint Security, bir maske girişi yapılırken `?` karakterinin kullanımını desteklemez. Örneğin, `VID_05AC&PID_*`.

Aygıt Denetimi, *erişim kuralları* kullanarak aygıtlara kullanıcı erişimini düzenler. Aygıt Denetimi, aygıt bağlantısı/aygıt bağlantının kesilmesi olaylarını kaydetmenize de izin verir. Olayları kaydetmek için olayların kaydını bir ilke içinde yapılandırmanız gerekir.

Bir aygıta erişim bağlantı veri yoluna bağlıysa (durumu) Kaspersky Endpoint Security, aygıt bağlantısı/aygıt bağlantısının kesilmesi olaylarını kaydetmez. Kaspersky Endpoint Security'nin aygıt bağlantısı/aygıt bağlantısının kesilmesi olaylarını kaydetmesini etkinleştirmek için ilgili aygıt türüne erişime izin verin (durumu) veya aygıtı güvenilir listeye ekleyin.

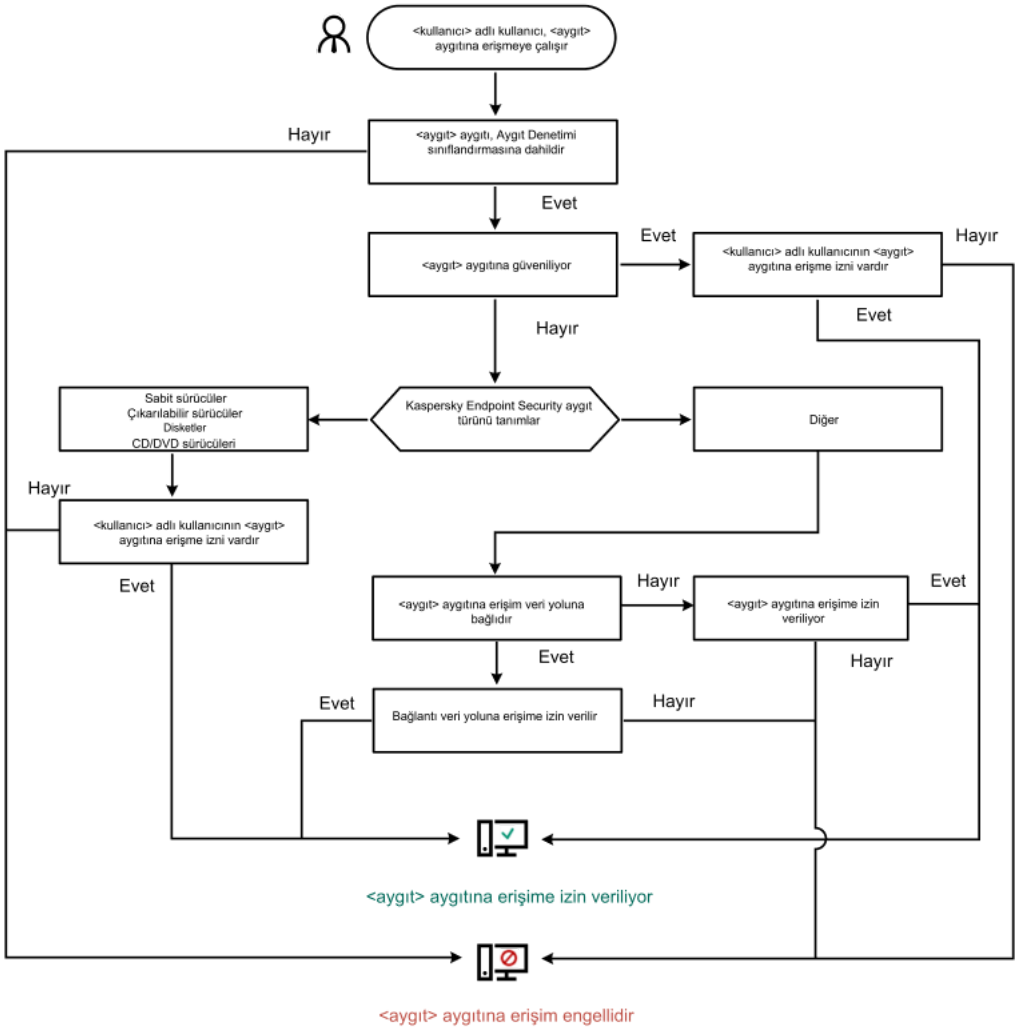
Aygıt Denetimi tarafından engellenen bir aygıt bilgisayara bağlandığında, Kaspersky Endpoint Security erişimi engeller ve bir bildirim gösterir (aşağıdaki şekle bakın).



Aygıt Denetimi bildirimi

Aygıt Denetimi işlem algoritması

Kaspersky Endpoint Security, kullanıcı aygıtı bilgisayara bağladıktan sonra aygıta erişime izin verip vermeyeceği hakkında bir karar verir (aşağıdaki resme bakın).



Aygıt Denetimi işlem algoritması

Bir cihaz bağlı ve erişim iznine sahipse erişim kuralını düzenleyebilir ve erişimini engelleyebilirsiniz. Bu durumda, bir kişinin bu aygıta bir sonraki bağlanma denemesinde (örneğin klasör ağacını görüntülemek ya da yazma veya okuma işlemleri gerçekleştirmek), 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.

Erişim kuralları hakkında

Aygıt erişim kuralı, kullanıcıların bilgisayarda yüklü veya bağlı olan aygıtlara nasıl bağlanabileceklerini belirleyen ayarlar grubudur. Bu ayarlar, belirli bir cihaza erişim, bir erişim zamanlaması ve okuma veya yazma izinlerini içerir. Aygıt Denetimi sınıflandırmasının dışında bir aygıt ekleyemezsiniz. Bu tür aygıtlara tüm kullanıcılar erişim sağlayabilir.

Aygıt Erişim Kuralları

Bir erişim kuralının ayarlar grubu, aygıtın türüne bağlı olarak farklılık gösterir (aşağıdaki tabloya bakın).

Erişim kuralı ayarları

Aygıtlar	Erişim denetimi	Aygıta erişim için zamanlama	Kullanıcılar ve/veya kullanıcı grupları ataması	Öncelik	Okuma/yazma izni
Sabit sürücüler	✓	✓	✓	✓	✓
Çıkarılabilir sürücüler (USB flash sürücüler dahil)	✓	✓	✓	✓	✓
Disketler	✓	✓	✓	✓	✓
CD/DVD sürücüleri	✓	✓	✓	✓	✓
Taşınabilir aygıtlar (MTP)	✓	✓	✓	✓	✓
Yerel yazıcılar	✓	–	✓	✓	–
Ağ yazıcıları	✓	–	✓	✓	–
Modemler	✓	–	–	–	–
Teyp aygıtları	✓	–	–	–	–
Çok işlevli aygıtlar	✓	–	–	–	–
Akıllı kart okuyucular	✓	–	–	–	–
Windows CE USB ActiveSync aygıtları	✓	–	–	–	–
Harici ağ bağdaştırıcıları	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Kameralar ve tarayıcılar	✓	–	–	–	–

Wi-Fi ağları için erişim kuralları

Wi-Fi ağ erişim kuralı, Wi-Fi ağlarının kullanılmasına izin verildiğini (✓ durumu) veya bu ağların kullanılmasının yasaklandığını (⊘ durumu) belirtir. Bir kurala *güvenilir Wi-Fi ağı* (durumu) ekleyebilirsiniz. Güvenilir bir Wi-Fi ağının kullanılmasına sınırlama olmadan izin verilmektedir. Varsayılan olarak, Wi-Fi ağ erişim kuralı tüm Wi-Fi ağlarına erişime izin verir.

Bağlantı veri yolu erişim kuralları

Cihaz türüne göre erişim kuralı için **Bağlantı veriyoluna bağlıdır** değeri seçilirse, uygulama bağlantı arabirimine bağlı olarak cihaza erişime izin verir veya erişimi reddeder. Veri yollarına erişime izin veren kurallar, varsayılan olarak Aygıt Denetimi bileşeni sınıflandırmasında bulunan bütün bağlantı veri yolları için oluşturulur.

Bağlantı veri yolu erişim kuralları, aygıtlara bağlantıya izin verildiğini (durumu) veya bu erişimin yasaklandığını (durumu) belirtir. Cihaz tipi erişim kurallarının önceliği, bağlantı veriyolu erişim kurallarının önceliğinden daha yüksektir.

Klavye ve fare Aygıt Denetimi kullanılarak kilitlenemez. USB bağlantı veri yoluna erişimi yasaklarsanız, kullanıcı USB üzerinden bağlı bir klavye ve fare ile çalışmaya devam edecektir. BadUSB Saldırısı Önleme bileşeni, klavyeleri taklit eden virüslü USB cihazlarının bilgisayara bağlanmasını önlemek için tasarlanmıştır.

Yüklü cihazlar hakkında bilgi alma

Kaspersky Security Center, yüklü cihazlar hakkında şu sağlayıcılardan bilgi alır: Ağ Aracısı ve Kaspersky Endpoint Security. Yüklü cihazlar hakkındaki bilgiler, erişim yönetimi ve güvenilir cihazlar listesinin oluşturulması için gereklidir.

Bilgisayar donanımı hakkında bilgiler

Ağ Aracısı bir Windows cihazına yüklenmişse cihazın donanımıyla ilgili aşağıdaki bilgileri Yönetim Sunucusuna gönderir:

- RAM
- depolama cihazları (sabit sürücüler dahil)
- ana kart
- İŞLEMCİ
- ağ bağdaştırıcısı
- monitörler
- GPU
- ses kartı

Ağ Aracısı, Kaspersky Security Center ile her senkronizasyonda bu bilgileri sağlar. Bir bilgisayarın donanımını bilgisayar özelliklerinde (**Donanım kaydı**) görüntüleyebilirsiniz.

Donanım bilgileri

Kaspersky Endpoint Security; yazıcılar, çıkarılabilir sürücüler, taşınabilir cihazlar (MTP) ve benzeri yüklü donanımlar hakkında bilgi sağlar. Donanım bilgilerini almak için yüklü cihazlara ilişkin bilgilerin iletimini etkinleştiren etkin bir ilke uygulamanız gerekir (bu iletim varsayılan olarak etkindir).

Yönetim Konsolu'nda (MMC) yüklü cihazlarla ilgili veri iletimini etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.

3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.
5. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Ayarlar** düğmesine tıklayın.
6. **Yüklü cihazlar** onay kutusunu seçin.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da yüklü cihazlarla ilgili veri iletimini etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.
5. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Gelişmiş ayarlar** düğmesine tıklayın.
6. **Yüklü cihazlar hakkında** onay kutusunu seçin.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Bunun sonucunda, Kaspersky Security Center konsolunda yüklü cihazların listesini görüntüleyebilirsiniz (**Veri havuzları** → **Donanım**).

Cihazlara erişimi türe göre yönetme

Aygıt Denetimi, cihazlara erişimi türe göre yönetmeyi sağlar. Cihazın türü, cihaz bağlandığında işletim sistemi tarafından belirlenir. İşletim sisteminde yerleşik olarak bulunan Aygıt Yöneticisi aracını kullanarak cihazın türüne bakabilirsiniz. Cihazlara erişimi yönetmek için kuralları yapılandırmanız gerekir. *Aygıt erişim kuralı*, kullanıcıların bilgisayarda yüklü veya bağlı olan aygıtlara nasıl bağlanabileceklerini belirleyen ayarlar grubudur. Bu ayarlar, belirli bir cihaza erişim, bir erişim zamanlaması ve okuma veya yazma izinlerini içerir. Aygıt Denetimi sınıflandırmasının dışında bir aygıt ekleyemezsiniz. Bu tür aygıtlara tüm kullanıcılar erişim sağlayabilir.

Aygıt Denetimi varsayılan olarak tüm kullanıcılar için tüm aygıtlara erişime izin verir.

Cihazlara erişimi aşağıdaki gibi yapılandırabilirsiniz:

- **İzin ver**.
  Kaspersky Endpoint Security, tüm kullanıcılara cihazlara tam erişim izni verir.
- **Engelle**.
  Kaspersky Endpoint Security cihaz bağlantılarını engeller. Uygulama yalnızca güvenilir aygıtların bağlanmasına izin verir.
- **Bağlantı veriyoluna bağlıdır**.
  Kaspersky Endpoint Security, cihazların bağlantı arabirimini belirler ve veriyolu bağlantı durumlarına göre cihazlara erişimi kısıtlar. Uygulama ayrıca güvenilir aygıtların bağlanmasına da izin verir.

- **Kurallara göre**.

  Bazı cihaz türleri için, cihazları kullanmasına izin verilen bireysel kullanıcıları veya bir grup kullanıcıyı belirleyebilir, cihazlara erişim için bir zamanlama ayarlayabilir ve okuma ve yazma izinlerini yapılandırabilirsiniz. Uygulama ayrıca güvenilir aygıtların bağlanmasına da izin verir.

Sabit sürücüler türündeki cihazlara erişimi yapılandırırken dikkatli olun. Sistem diskine erişimi engellerseniz, uygulama işletim sisteminin önyüklenmesi sırasında çökmeye (BSOD) neden olabilir.

Bir cihaz Aygıt Denetimi sınıflandırma şemasına uymuyorsa, böyle bir cihaza erişim kısıtlanamaz.

Yönetim Konsolu'nda (MMC) cihazlara erişimi türe göre yönetme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
5. **Aygıt Denetimi ayarları** bölümünden **Aygıt türleri** sekmesini seçin.

   Aygıt türleri sekmesi, Aygıt Denetimi sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.
6. Cihazlar için erişim kurallarını yapılandırın:

   a. Erişim modunu seçin: **İzin ver**, **Engelle**, **Bağlantı veriyoluna bağlıdır**, **Kurallara göre**.

   Kurallara göre erişim modunu seçmek için, erişim kuralı özelliklerini açmak üzere çift tıklayın.

   b. **Bağlantı veri yoluna bağlı** erişim modunu seçtiğinizde, **Bağlantı veri yolları** sekmesinden bağlantı arabirimleri için erişim kurallarını yapılandırmanız gerekir.

   c. Depolama cihazları (örneğin, çıkarılabilir medya) söz konusu olduğunda, tek tek kullanıcılar için erişim izinlerini yapılandırabilirsiniz. Ayrıca cihazlara erişim için bir zamanlama ayarlayabilir ve okuma ve yazma izinlerini yapılandırabilirsiniz.

   Güvenilenler listesine cihaz ekleyebilirsiniz. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

   d. Gerekirse, yazdırma kurallarını yapılandırın.

   e. Gerekirse, Bluetooth aygıt erişim kurallarını yapılandırın.

   f. Gerekirse, bilgisayar Wi-Fi bağlantı kurallarını yapılandırın.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da cihazlara erişimi türe göre yönetme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.

5. **Cihaz erişim kuralları** bölümünde, **Cihazlar ve Wi-Fi ağları** sekmesini seçin.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.

6. Cihazlar için erişim kurallarını yapılandırın:

   a. Erişim modunu seçin: **İzin ver**, **Engelle**, **Veri yoluna bağlı**, **Özel**.

      Açılır menüde erişim modu yoksa, cihaz türüne çift tıklayarak erişim kuralı özelliklerini açın.

   b. **Veri yoluna bağlı** erişim modunu seçtiğinizde, **Bağlantı veri yolları** sekmesinden bağlantı arabirimleri için erişim kurallarını yapılandırmanız gerekir.

   c. Depolama cihazları (örneğin, çıkarılabilir medya) söz konusu olduğunda, tek tek kullanıcılar için erişim izinlerini yapılandırabilirsiniz. Ayrıca cihazlara erişim için bir zamanlama ayarlayabilir ve okuma ve yazma izinlerini yapılandırabilirsiniz.

      Güvenilenler listesine cihaz ekleyebilirsiniz. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

   d. Gerekirse, yazdırma kurallarını yapılandırın.

   e. Gerekirse, Bluetooth aygıt erişim kurallarını yapılandırın.

   f. Gerekirse, bilgisayar Wi-Fi bağlantı kurallarını yapılandırın.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde cihazlara erişimi yönetme

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.

3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** bağlantısına tıklayın.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.

4. Cihazlar için erişim kurallarını yapılandırın:

   a. Erişim modunu seçin: **İzin ver**, **Engelle**, **Bağlantı veriyoluna bağlıdır**, **Kurallara göre**.

      Açılır menüde erişim modu yoksa, cihaz türüne çift tıklayarak erişim kuralı özelliklerini açın.

   b. **Bağlantı veri yoluna bağlı** erişim modunu seçtiğinizde, **Bağlantı veri yolları** sekmesinden bağlantı arabirimleri için erişim kurallarını yapılandırmanız gerekir.

   c. Depolama cihazları (örneğin, çıkarılabilir medya) söz konusu olduğunda, tek tek kullanıcılar için erişim izinlerini yapılandırabilirsiniz. Ayrıca cihazlara erişim için bir zamanlama ayarlayabilir ve okuma ve yazma izinlerini yapılandırabilirsiniz.

      Güvenilenler listesine cihaz ekleyebilirsiniz. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

   d. Gerekirse, yazdırma kurallarını yapılandırın.

e. Gerekirse, Bluetooth aygıt erişim kurallarını yapılandırın.

f. Gerekirse, bilgisayar Wi-Fi bağlantı kurallarını yapılandırın.

5. Değişikliklerinizi kaydedin.

Sonuç olarak, bir kullanıcı bir cihaza erişim sağlamaya çalıştığında, uygulama kurallara uygun olarak erişimi engeller. Kaspersky Endpoint Security ayrıca ilgili bir olayı da günlüğe kaydeder. Tek tek cihazlara erişim izni vermek istiyorsanız, bu cihazları güvenilen cihazlar listesine ekleyebilirsiniz.

Bağlantı veri yolu ile cihazlara erişimi yönetme

Bir bağlantı veri yolu erişim kuralını düzenlemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Bağlantı veri yolları** düğmesine tıklayın.

   Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm bağlantı veri yolları için erişim kurallarını gösterir.
4. Düzenlemek istediğiniz erişim kuralını seçin.
5. **Erişim** sütununda, bağlantı veri yoluna erişime izin verilip verilmeyeceğini seçin: **İzin ver** veya **Engelle**.

   Bağlantı veriyoluna erişimi değiştirdiyseniz **Seri Port** (COM) veya **Paralel Port** (LPT), erişim kuralını etkinleştirmek için bilgisayarı yeniden başlatmanız gerekir.
6. Değişikliklerinizi kaydedin.

Cihazlara kullanıcı erişim haklarının farklılaştırılması

Kullanıcı erişim haklarını cihaz türüne veya güvenilen cihazlara göre yapılandırabilirsiniz.

Kullanıcı erişim haklarının cihaz türüne göre farklılaştırılması

Aygıt Denetimi, *depolama cihazlarındaki* verilere kullanıcı erişim haklarının yapılandırılmasını sağlar. Bu tür cihazlar için yazma ve okuma izinlerini yapılandırabilirsiniz. Aygıt Denetimi aşağıdaki *depolama cihazı* türlerini destekler:

- Sabit sürücüler
- Çıkarılabilir sürücüler (USB flash sürücüler dahil)
- Disketler

- CD/DVD sürücüleri
- Taşınabilir aygıtlar (MTP). Taşınabilir aygıtlar (MTP) örneğin mobil cihazları, fotoğraf makinelerini, medya oynatıcıları vb. içerir.

Bu şekilde, örneğin, çıkarılabilir medyanın yalnızca yöneticiler grubu tarafından kullanılmasına izin verebilirsiniz. Diğer cihaz türleri için, tüm kullanıcıların erişimini reddedebilir veya izin verebilirsiniz. Yazıcıları kullanmak için kullanıcı erişim haklarını da yapılandırabilirsiniz.

Yönetim Konsolu'nda (MMC) depolama aygıtlarındaki verilere kullanıcı erişim hakları nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
5. **Aygıt Denetimi ayarları** bölümünden **Aygıt türleri** sekmesini seçin.

   Aygıt türleri sekmesi, Aygıt Denetimi sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.
6. Depolama aygıtı erişim kurallarını yapılandırmak için, çift tıklayarak kural listesini açın.
7. Depolama aygıtı erişim kuralını yapılandırın:
   a. **Erişim kuralları** bloğunda, **Ekle** düğmesine tıklayın.

      Bu, yeni bir depolama aygıtı erişim kuralı eklemek için bir pencere açar.

   b. **Kural önceliği** alanında, *kural yazma* önceliğini ayarlayın. Bir kural şu öznitelikleri içerir: kullanıcı hesabı, zamanlama, izinler (okuma/yazma) ve öncelik.

      Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

      Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

      Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

   c. **Kullanıcılar ve gruplar için kural** altında, kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   d. **Tamam**'a tıklayın.
8. **Seçilen erişim kuralı için zamanlamalar** bölümünde, kullanıcılar için bir depolama aygıtı erişim zamanlaması yapılandırın.

   Örneğin, kullanıcıların depolama aygıtlarını yalnızca çalışma saatleri içinde kullanmalarına izin verebilirsiniz.

9. Dosya yöneticisinde kullanıcıların depolama aygıtlarına erişim izinlerini yapılandırın (**Okuma** / **Yazma**).

10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da depolama aygıtlarındaki verilere kullanıcı erişim haklarını yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.

5. **Cihaz erişim kuralları** bloğunda, erişim kuralları tablosunda, depolama cihazları için erişim kurallarının özelliklerini açın.

6. **Cihaz erişim kuralları** bloğunda **Özel** öğesini seçin.

7. Depolama aygıtı erişim kuralını yapılandırın:

   a. **Kullanıcılar ve hakları** bloğunda **Ekle** düğmesine tıklayın.

      Bu, yeni bir depolama aygıtı erişim kuralı eklemek için bir pencere açar.

   b. **Öncelik** alanında, *kural yazma* önceliğini ayarlayın. Bir kural şu öznitelikleri içerir: kullanıcı hesabı, zamanlama, izinler (okuma/yazma) ve öncelik.

      Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

      Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

      Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

   c. **Kullanıcı veya grup** bölümünde, kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   d. **Erişim zamanlaması** bölümünde, kullanıcılar için bir depolama cihazı erişim zamanlaması yapılandırın.

      Örneğin, kullanıcıların depolama aygıtlarını yalnızca çalışma saatleri içinde kullanmalarına izin verebilirsiniz.

   e. Dosya yöneticisinde kullanıcıların depolama aygıtlarına erişim izinlerini yapılandırın (**Okuma** / **Yazma**).

   f. **Kaydet**'e tıklayın.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde depolama aygıtlarındaki verilere kullanıcı erişim haklarını yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** bağlantısına tıklayın.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
4. Depolama aygıtı erişim kurallarını yapılandırmak için, sağ tıklayarak kural listesini açın.
5. Depolama aygıtı erişim kuralını yapılandırın:

   a. **Kullanıcıların hakları** bloğunda, **Ekle** düğmesine tıklayın.

   Bu, yeni bir depolama aygıtı erişim kuralı eklemek için bir pencere açar.

   b. **Öncelik** alanında, *kural yazma* önceliğini ayarlayın. Bir kural şu öznitelikleri içerir: kullanıcı hesabı, zamanlama, izinler (okuma/yazma) ve öncelik.

   Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

   Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

   Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

   c. **Kullanıcılar** bölümünde kullanıcıları veya kullanıcı gruplarını seçin. Active Directory'deki kullanıcıları seçebilir veya manuel olarak yerel bir kullanıcı adı girebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   d. **Tamam**'a tıklayın.
6. **Aygıtlara erişim için zamanlama** bölümünde, kullanıcılar için bir depolama aygıtı erişim zamanlaması yapılandırın.

   Örneğin, kullanıcıların depolama aygıtlarını yalnızca çalışma saatleri içinde kullanmalarına izin verebilirsiniz.
7. Dosya yöneticisinde kullanıcıların depolama aygıtlarına erişim izinlerini yapılandırın (**Okuma** / **Yazma**).
8. Değişikliklerinizi kaydedin.

Güvenilir cihazlara kullanıcı erişim haklarının farklılaştırılması

Güvenilir aygıtlar, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır. Güvenilir aygıtlarla çalışmak için bir kullanıcıya, bir kullanıcı grubuna ya da kuruluşun tüm kullanıcılarına erişim verebilirsiniz. Kullanıcı erişim haklarını güvenilen cihazın özelliklerinden yapılandırabilirsiniz.

Mobil cihazlara erişimi yönetme

Kaspersky Endpoint Security, Android ve iOS çalıştıran mobil cihazlardaki verilere erişimi kontrol etmenizi sağlar. Mobil cihazlar, taşınabilir aygıtlar (MTP) kategorisine aittir. Bu nedenle, mobil cihazlara erişimi yapılandırmak için taşınabilir aygıtlara (MTP) yönelik veri erişim ayarlarını düzenlemeniz gerekir.

Bilgisayara bir mobil cihaz bağlandığında işletim sistemi cihaz türünü belirler. Bilgisayarda Android Debug Bridge (ADB), iTunes veya bunların dengi uygulamalar yüklü ise işletim sistemi mobil cihazları ADB veya iTunes cihazları olarak tanımlar. Diğer tüm durumlarda işletim sistemi mobil cihaz türünü dosya aktarımı için taşınabilir aygıt (MTP), resim aktarımı için bir PTP cihazı (kamera) ya da başka bir cihaz olarak tanımlayabilir. Cihaz türü, mobil cihazın modeline ve seçilen USB bağlantı moduna bağlıdır. Kaspersky Endpoint Security, ADB uygulamaları, iTunes veya dosya yöneticisinde mobil cihazlardaki veriler için ayrı erişim izinleri yapılandırmanıza olanak tanır. Diğer tüm durumlarda, Aygıt Denetimi, taşınabilir aygıtlar (MTP) erişim kurallarına uygun olarak mobil cihazlara erişime izin verir.

Mobil cihazlara erişimi yönetme

Mobil cihazlar, taşınabilir aygıtlar (MTP) kategorisine aittir, bu nedenle onlar için ayarlar aynıdır. Mobil cihazlara aşağıdaki erişim modlarından birini seçebilirsiniz:

- **İzin ver** ✓. Kaspersky Endpoint Security, mobil cihazlara tam erişim sağlar. Dosya yöneticisini veya ADB ve iTunes uygulamalarını kullanarak mobil cihazlarda dosya açabilir, oluşturabilir, değiştirebilir, kopyalayabilir veya silebilirsiniz. Mobil cihazı bilgisayarın bir USB portuna bağlayarak da cihazın pilini şarj edebilirsiniz.

- **Engelle** ⊘. Kaspersky Endpoint Security, dosya yöneticisinde ve ADB ve iTunes uygulamalarında mobil cihazlara erişimi kısıtlar. Uygulama yalnızca güvenilir mobil cihazlara erişime izin verir. Mobil cihazı bilgisayarın bir USB portuna bağlayarak da cihazın pilini şarj edebilirsiniz.

- **Bağlantı veriyoluna bağlıdır**. Kaspersky Endpoint Security, mobil cihazlara şunlara uygun olarak bağlanmaya izin verir: USB bağlantı durumu (**İzin ver** ✓ veya **Engelle** ⊘).

- **Kurallara göre**. Kaspersky Endpoint Security, mobil cihazlara erişimi kurallara uygun olarak kısıtlar. Kurallarda, erişim haklarını (okuma/yazma) yapılandırabilir, mobil cihazlara erişebilecek kullanıcıları veya bir grup kullanıcıyı seçebilir ve mobil cihazlar için bir erişim zamanlaması yapılandırabilirsiniz. ADB ve iTunes uygulamaları aracılığıyla mobil aygıtlardaki verilere erişimi de kısıtlayabilirsiniz.

Mobil cihaz erişim kurallarını yapılandırma

Taşınabilir aygıtlar (MTP), ADB aygıtları ve iTunes aygıtları için erişim kuralları farklı şekilde yapılandırılır. Taşınabilir aygıtlar (MTP) ve ADB cihazları için, tek tek kullanıcılar veya kullanıcı grupları için kurallar yapılandırabilir ve kuralların ne zaman uygulanacağına ilişkin bir zamanlama oluşturabilirsiniz. iTunes aygıtları için bunu yapamazsınız. Tüm kullanıcılar için yalnızca iTunes uygulaması üzerinden verilere erişime izin verebilir veya erişimi reddedebilirsiniz.

Yönetim Konsolu'nda (MMC) mobil cihaz erişim kurallarını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.

4. **Aygıt Denetimi ayarları** bölümünden **Aygıt türleri** sekmesini seçin.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.

5. **Taşınabilir aygıtlar (MTP)** cihaz türü için bağlam menüsünde, mobil cihaz erişim modunu yapılandırın: **İzin ver**, **Engelle**, veya **Bağlantı veriyoluna bağlıdır**.

6. Mobil cihaz erişim kurallarını yapılandırmak için çift tıklayarak kural listesini açın.

7. Mobil cihaz erişim kuralını yapılandırın:

   a. **Erişim kuralları** bloğunda, **Ekle** düğmesine tıklayın.

      Bu, yeni bir mobil cihaz erişim kuralı eklemek için bir pencere açar.

   b. **Öncelik** alanında, kural yazma önceliğini ayarlayın. Bir kural şu öznitelikleri içerir: kullanıcı hesabı, zamanlama, izinler (okuma/yazma/ADB erişimi) ve öncelik.

      Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

      Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

      Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

   c. **Kullanıcılar ve gruplar için kural** altında, kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   d. **Tamam**'a tıklayın.

8. **Seçilen erişim kuralı için zamanlamalar** böllümünde, kullanıcılar için bir mobil cihaz erişim programı yapılandırın.

   ADB cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir. ADB cihazları ve taşınabilir aygıtlar (MTP) için ortak bir erişim planı yapılandırabilirsiniz.

9. Dosya yöneticisinde kullanıcıların mobil cihazlara erişim izinlerini yapılandırın (**Okuma**/**Yazma**).

10. **ADB üzerinden erişim** onay kutusunu kullanarak ADB uygulaması aracılığıyla bir mobil cihazdaki verilere erişimi yapılandırın.

    Onay kutusunun işareti kaldırılırsa, mobil cihaz bağlandığında ADB uygulamasının cihazı algılaması engellenir.

11. **iTunes üzerinden erişim** altında, iTunes uygulaması aracılığıyla mobil aygıttaki verilere erişimi yapılandırın.

    Kaspersky Endpoint Security, tüm kullanıcılar için iTunes uygulaması aracılığıyla mobil cihaz erişimi ayarlarını uygular. iTunes cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir.

12. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da mobil cihaz erişim kurallarını yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.
5. **Aygıt erişim kuralları** bloğunda, **Aygıtlar ve Wi-Fi ağları** bağlantısına tıklayın.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **Taşınabilir aygıtlar (MTP)** cihaz ürünü seçin.

   Taşınabilir aygıtlar (MTP) erişim hakları açılır.
7. Mobil cihazların erişim modunu yapılandırın: **İzin ver**, **Engelle**, **Veri yoluna bağlı** veya **Özel**.
8. **Tüm kullanıcılar için iTunes üzerinden erişim ETKİN** anahtarını kullanarak, iTunes uygulaması aracılığıyla mobil cihazdaki verilere erişimi yapılandırın.

   > Kaspersky Endpoint Security, tüm kullanıcılar için iTunes uygulaması aracılığıyla mobil cihaz erişimi ayarlarını uygular. iTunes cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir.
9. **Özel** modunu seçtiğinizde, yazıcılar için yazdırma kuralları eklemelisiniz. Bunu yapmak için, **Kullanıcılar ve hakları** bölümünden **Ekle** düğmesine tıklayın ve mobil cihaz erişim kuralını yapılandırın:

   a. **Öncelik** alanında, kural yazma önceliğini ayarlayın. Bir kural şu öznitelikleri içerir: kullanıcı hesabı, zamanlama, izinler (okuma/yazma/ADB erişimi) ve öncelik.

   Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

   Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

   Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

   b. **Kullanıcı veya grup** bölümünde, mobil cihazlara erişim için kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   c. **Erişim zamanlaması** bölümünde, kullanıcılar için bir mobil cihaz erişim zamanlaması yapılandırın.

   > ADB cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir. ADB cihazları ve taşınabilir aygıtlar (MTP) için ortak bir erişim planı yapılandırabilirsiniz.

   d. Dosya yöneticisinde kullanıcıların mobil cihazlara erişim izinlerini yapılandırın (**Okuma**/**Yazma**).

e. **ADB üzerinden erişim** onay kutusunu kullanarak ADB uygulaması aracılığıyla bir mobil cihazdaki verilere erişimi yapılandırın.

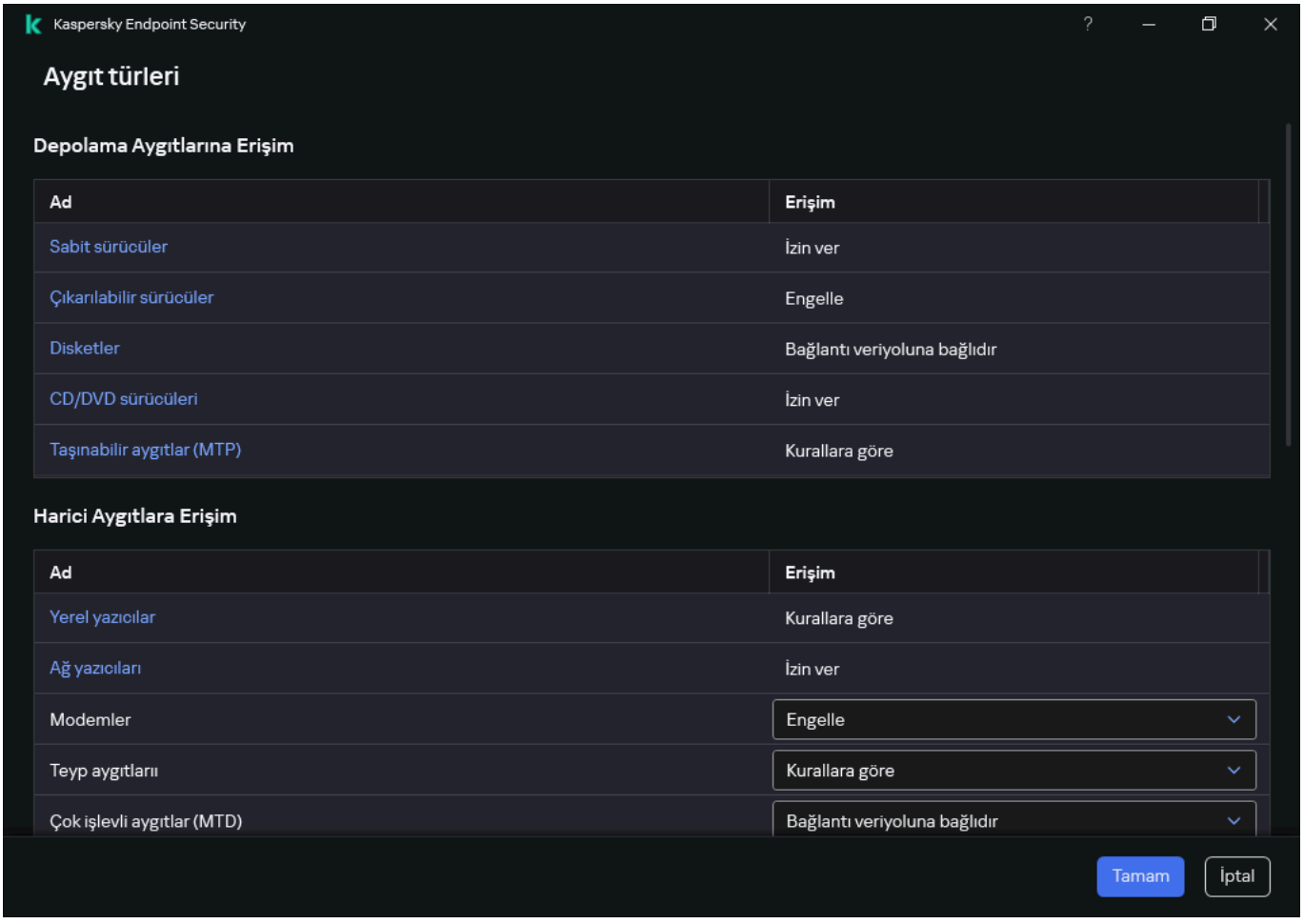
Onay kutusunun işareti kaldırılırsa, mobil cihaz bağlandığında ADB uygulamasının cihazı algılaması engellenir.

10. Değişikliklerinizi kaydedin.

Uygulama arabiriminde mobil cihaz erişim kurallarını yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** düğmesine tıklayın.

Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.



Aygıt Denetimi bileşenindeki aygıt türleri

4. **Depolama Aygıtlarına Erişim** bloğunda, **Taşınabilir aygıtlar (MTP)** bağlantısına tıklayın.

Taşınabilir aygıtlar (MTP) erişim kurallarını içeren bir pencere açılır.

5. **Erişim** bölümünde mobil cihazların erişim modunu yapılandırın: **İzin ver**, **Engelle**, **Bağlantı veriyoluna bağlıdır** veya **Kurallara göre**.
6. **Kurallara göre** modunu seçtiğinizde, yazıcılar için yazdırma kuralları eklemelisiniz:

a. **Kullanıcıların hakları** bloğunda, **Ekle** düğmesine tıklayın.

Bu, yeni bir mobil cihaz erişim kuralı eklemek için bir pencere açar.

b. **Öncelik** alanında, kural yazma önceliğini ayarlayın. Bir kural şu öznitelikleri içerir: kullanıcı hesabı, zamanlama, izinler (okuma/yazma/ADB erişimi) ve öncelik.

Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

c. **Durum** bölümünden mobil cihaz erişim kuralını açın.

d. **Erişim kuralları** bölümünde, kullanıcılar için mobil cihaz erişim izinlerini yapılandırın.

- Dosya yöneticisinde kullanıcıların mobil cihazlara erişim izinlerini yapılandırın (**Okuma**/**Yazma**).
- **ADB üzerinden erişim** onay kutusunu kullanarak ADB uygulaması aracılığıyla bir mobil cihazdaki verilere erişimi yapılandırın.

  Onay kutusunun işareti kaldırılırsa, mobil cihaz bağlandığında ADB uygulamasının cihazı algılaması engellenir.

e. **Kullanıcılar** bölümünde, mobil cihazlara erişim için kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

f. **Aygıtlara erişim için zamanlama** altında, kullanıcılar için bir cihaz erişim zamanlaması yapılandırın.

> ADB cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir. ADB cihazları ve taşınabilir aygıtlar (MTP) için ortak bir erişim planı yapılandırabilirsiniz.

g. **iTunes üzerinden erişim** altında, iTunes uygulaması aracılığıyla mobil aygıttaki verilere erişimi yapılandırın.

> Kaspersky Endpoint Security, tüm kullanıcılar için iTunes uygulaması aracılığıyla mobil cihaz erişimi ayarlarını uygular. iTunes cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir.

7. Değişikliklerinizi kaydedin.

Sonuç olarak, mobil cihazlara kullanıcı erişimi kurallara uygun olarak kısıtlanır. ADB ve iTunes uygulamalarında mobil cihazlara erişimi yasakladıysanız, bir mobil cihaz bağladığınızda ADB ve iTunes uygulamalarının mobil cihazı algılaması engellenir.

Güvenilir mobil cihazlar

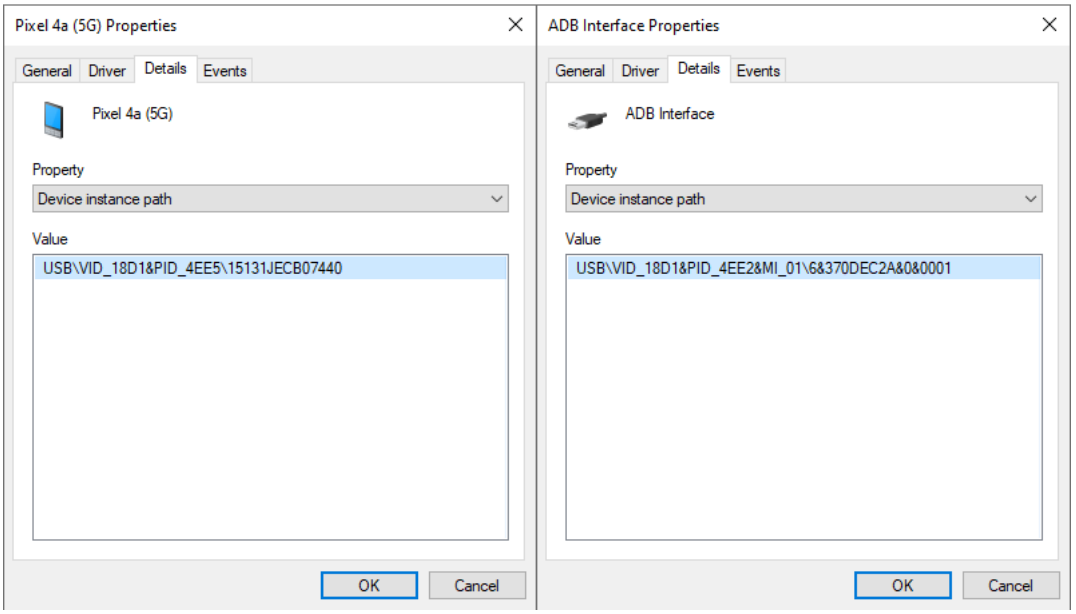
Güvenilir aygıtlar, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

Güvenilir bir mobil cihaz ekleme prosedürü diğer güvenilir cihaz türleri ile tamamen aynıdır. Bir mobil cihazı kimliğine veya cihaz modeline göre ekleyebilirsiniz.

Kimliğe göre güvenilir bir mobil cihaz eklemek için benzersiz bir kimliğe (Hardware ID – HWID) ihtiyacınız olacaktır. Kimliği, işletim sistemi araçlarını kullanarak cihaz özelliklerinde bulabilirsiniz (aşağıdaki şekle bakın). Aygıt Yöneticisi aracı bunu yapmanızı sağlar. Taşınabilir aygıtlar (MTP) ve ADB, iTunes cihazlarının kimlikleri, aynı mobil cihaz için bile farklıdır. Bir taşınabilir aygıtın (MTP) kimliği şöyle görünebilir: `15131JECB07440`. Bir ADB cihazının kimliği şöyle görünebilir: `6&370DEC2A&0&0001`. Birkaç belirli cihazı eklemek istiyorsanız cihazları kimliğe göre eklemek uygundur. Maskeler de kullanabilirsiniz.

Bilgisayara bir cihaz bağladıktan sonra ADB veya iTunes uygulamalarını yüklediyseniz, cihazın benzersiz kimliği sıfırlanabilir. Bu, Kaspersky Endpoint Security'nin bu cihazı yeni bir cihaz olarak tanımlayacağı anlamına gelir. Bir cihaz güvenilirse, cihazı tekrar güvenilir listeye ekleyin.

Cihaz modeline göre güvenilir bir mobil cihaz eklemek için Vendor ID (VID) ve Product ID (PID)ye ihtiyacınız olacaktır. Kimlikleri, işletim sistemi araçlarını kullanarak cihaz özelliklerinde bulabilirsiniz (aşağıdaki şekle bakın). VID ve PID girme şablonu: `VID_18D1&PID_4EE5`. Kuruluşunuzda belirli bir model cihazlar kullanıyorsanız cihazları modele göre eklemek uygundur. Böylece bu model tüm cihazları ekleyebilirsiniz.



Aygıt Yöneticisinde Aygıt Kimliği

Bluetooth cihazlarına erişimi yönetme

Kaspersky Endpoint Security, Bluetooth cihazlarına tam erişime olanak sağlar. Bluetooth cihazları arasında kablosuz klavyeler, fareler, kulaklıklar, yazıcılar vb. bulunur. Bluetooth'u örneğin bir mobil cihazla iletişim kurmak için de kullanabilirsiniz.

Bluetooth cihazları bağlandığında veya bağlantısı kesildiğinde, uygulama cihaz hakkında birden fazla olay oluşturabilir. Bunun nedeni, işletim sisteminin bir Bluetooth cihazını farklı türlerde birden fazla cihaz olarak algılayabilmesidir. Kaspersky Endpoint Security, cihazın bağlı olduğu Bluetooth adaptörünü de ayrı bir cihaz olarak yönetir. Bu nedenle uygulama, tespit edilen cihazların her biri için bir olay oluşturur.

Bluetooth cihazlarına erişim için şu modlardan birini seçebilirsiniz:

- **İzin ver ve günlüğe kaydetme** Kaspersky Endpoint Security, herhangi bir Bluetooth cihazının bağlanmasına izin verir ve bağlantı hakkındaki bilgileri olay günlüğüne kaydetmez. Bluetooth giriş cihazlarını (klavyeler, fareler, vb.) bağlayabilir, Bluetooth üzerinden veri gönderebilir, diğer Bluetooth cihazlarını (kulaklık, vb.) yönetebilirsiniz.
- **İzin ver**. Kaspersky Endpoint Security, herhangi bir Bluetooth cihazının bağlanmasına izin verir. Bluetooth giriş cihazlarını (klavyeler, fareler, vb.) bağlayabilir, Bluetooth üzerinden veri gönderebilir, diğer Bluetooth cihazlarını (kulaklık, vb.) yönetebilirsiniz.
- **Engelle**. Kaspersky Endpoint Security, Bluetooth cihazlarına erişimi kısıtlar. Sadece Bluetooth giriş cihazlarının bağlanmasına izin verebilirsiniz (Human Interface Devices sınıfı). Bu cihazlar arasında klavyeler, fareler, oyun kolları vb. bulunur.

Güvenilir Bluetooth cihazlarının bir listesini oluşturmak mümkün değildir. Bluetooth cihazlarına erişiminiz kısıtlıysa, yalnızca Bluetooth giriş cihazlarını bağlayabilirsiniz.

Yönetim Konsolu'nda (MMC) Bluetooth cihazı erişim kurallarını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
5. **Aygıt Denetimi ayarları** bölümünden **Aygıt türleri** sekmesini seçin.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **Bluetooth** cihaz türünün bağlam menüsünde, Bluetooth cihaz erişim modunu yapılandırın: **İzin ver** ( ), **Engelle** ( ), **İzin ver ve günlüğe kaydetme** ( ).
7. **Engelle** modunu seçerseniz, sadece Bluetooth giriş cihazlarının (klavyeler, fareler, vb.) bağlanmasına izin verebilirsiniz. Bunu yapmak için, **İstisnalar** altında **Giriş cihazları (fare ve klavyeler)** onay kutusunu seçin.
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Bluetoot cihazı erişim kurallarını yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.
5. **Aygıt erişim kuralları** bloğunda, **Aygıtlar ve Wi-Fi ağları** bağlantısına tıklayın.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.

6. **Bluetooth cihazları** cihazı türünü seçin.

   Bu, Bluetooth cihazı erişim ayarlarını açar.

7. Bluetooth cihazı erişim modunu yapılandırın: **İzin ver**, **Engelle**, **İzin ver ve günlüğe kaydetme**.

8. **Engelle** modunu seçerseniz, sadece Bluetooth giriş cihazlarının (klavyeler, fareler, vb.) bağlanmasına izin verebilirsiniz. Bunu yapmak için, **İstisnalar** altında **Giriş cihazları (fare ve klavyeler)** onay kutusunu seçin.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

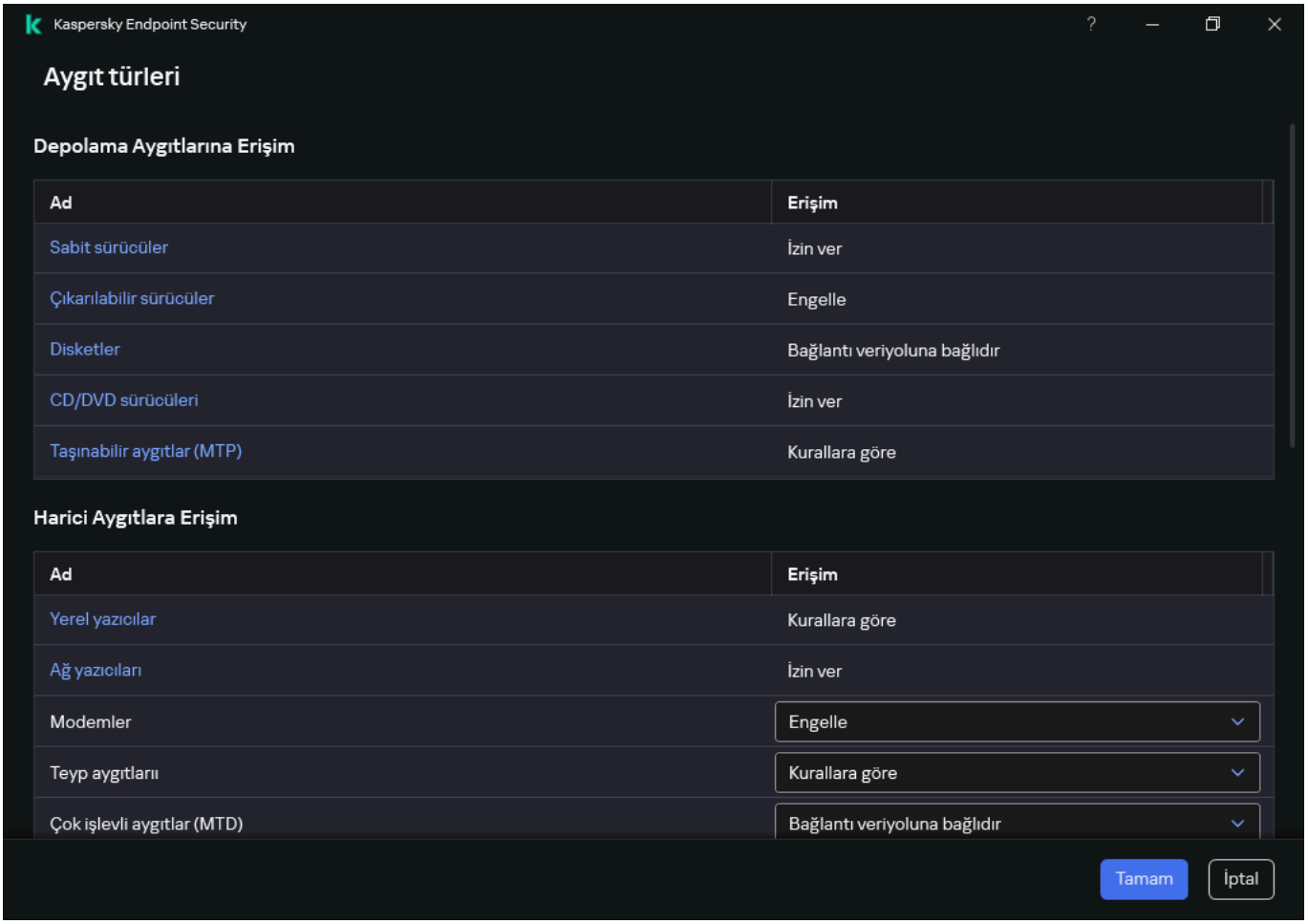
Uygulama arabiriminde Bluetooth cihaz erişim kurallarını yapılandırma

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.

3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** düğmesine tıklayın.

   Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.



Aygıt Denetimi bileşenindeki aygıt türleri

4. **Harici Aygıtlara Erişim** bloğunda, **Bluetooth** bağlantısına tıklayın.

   Bu, Bluetooth cihazı erişim ayarlarını açar.

5. **Erişim** altında, Bluetooth cihazı erişim modunu yapılandırın: **İzin ver**, **Engelle**, **İzin ver ve günlüğe kaydetme**.

6. **Engelle** modunu seçerseniz, sadece Bluetooth giriş cihazlarının (klavyeler, fareler, vb.) bağlanmasına izin verebilirsiniz. Bunu yapmak için, **İstisnalar** altında **Giriş cihazları (fare ve klavyeler)** onay kutusunu seçin.

7. Değişikliklerinizi kaydedin.

Yazdırma denetimi

Arm tabanlı bilgisayarlarda yazdırma denetimi desteklenmemektedir.

Yerel ve ağ yazıcılarına kullanıcı erişimini yapılandırmak için Yazdırma denetimini kullanabilirsiniz.

Yerel yazıcı denetimi

Kaspersky Endpoint Security, yerel yazıcılara erişimin iki düzeyde yapılandırılmasına olanak tanır: *Bağlanıyor* ve *yazdırılıyor*.

Kaspersky Endpoint Security, şu veri yolları üzerinden yerel yazıcı bağlantısını kontrol eder: USB, Seri Bağlantı Noktası (COM), Paralel Bağlantı Noktası (LPT).

Kaspersky Endpoint Security, yerel yazıcıların COM ve LPT portlarına bağlantısını yalnızca veri yolu düzeyinde kontrol eder. Bu nedenle, COM ve LPT portları üzerinden yazıcı bağlantılarını önlemek için yerel yazıcılar için Bağlantı veriyoluna bağlıdır erişim modunu seçmeniz ve COM ve LPT veriyollarına bağlantıları yasaklamanız gerekir.

USB'ye bağlı yazıcılar için uygulama iki seviyede kontrol uygular: cihaz türü (yerel yazıcılar) ve bağlantı veriyolu (USB).

USB üzerinden yerel yazıcılara şu erişim modlarından birini seçebilirsiniz:

- **İzin ver** . Kaspersky Endpoint Security, tüm kullanıcılara yerel yazıcılara tam erişim verir. Kullanıcılar, işletim sisteminin sağladığı araçları kullanarak yazıcıları bağlayabilir ve belgeleri yazdırabilir.
- **Engelle** . Kaspersky Endpoint Security, yerel yazıcıların bağlantısını engeller. Uygulama yalnızca güvenilir yazıcıların bağlanmasına izin verir.
- **Bağlantı veriyoluna bağlıdır** . Kaspersky Endpoint Security, yerel yazıcılara aşağıdakilere uygun olarak bağlanmaya izin verir: USB veri yolu bağlantı durumu (**İzin ver** veya **Engelle**).
- **Kurallara göre** . Yazdırmayı kontrol etmek için *yazdırma kuralları* eklemeniz gerekir. Kurallarda, yerel yazıcılarda belge yazdırma erişimine izin vermek veya erişimi engellemek istediğiniz kullanıcıları veya bir kullanıcı grubunu seçebilirsiniz.

Ağ yazıcısı denetimi

Kaspersky Endpoint Security, ağ yazıcılarında yazdırma erişiminin yapılandırılmasına izin verir. Ağ yazıcılarına şu erişim modlarından birini seçebilirsiniz:

- **İzin ver ve günlüğe kaydetme**. Kaspersky Endpoint Security ağ yazıcılarında yazdırmayı kontrol etmez. Uygulama tüm kullanıcılara yazdırma erişimi verir ve yazdırma ile ilgili bilgileri olay günlüğüne kaydetmez.
- **İzin ver**. Kaspersky Endpoint Security, tüm kullanıcılara ağ yazıcılarında yazdırma erişimi verir.
- **Engelle**. Kaspersky Endpoint Security, tüm kullanıcılar için ağ yazıcılarına erişimi kısıtlar. Uygulama yalnızca güvenilir yazıcılara erişime izin verir.
- **Kurallara göre**. Kaspersky Endpoint Security, yazdırma kurallarına uygun olarak yazdırmaya erişim sağlar. Kurallarda, ağ yazıcısında belge yazdırmasına izin verilecek veya belge yazdırması engellenecek kullanıcıları veya bir kullanıcı grubunu seçebilirsiniz.

Yazıcılar için yazdırma kuralları ekleme

Yönetim Konsolu'nda (MMC) yazdırma kuralları ekleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
4. **Aygıt Denetimi ayarları** bölümünden **Aygıt türleri** sekmesini seçin.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
5. **Yerel yazıcılar** bağlam menüsünde ve **Ağ yazıcıları** aygıt türlerinde, ilgili yazıcılar için erişim modunu yapılandırın: **İzin ver**, **Engelle**, **İzin ver ve günlüğe kaydetme** (sadece ağ yazıcıları için) veya **Bağlantı veriyoluna bağlıdır** (yalnızca yerel yazıcılar için).
6. Yerel ve ağ yazıcılarında yazdırma kurallarını yapılandırmak için, kural listelerini çift tıklayarak açın.
7. Yazıcı erişim modu olarak **Kurallara göre** seçimini yapın.
8. Yazdırma kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.

   a. **Ekle**'ye tıklayın.

      Yeni bir yazdırma kuralı eklemek için bir pencere açılır.

   b. Kural girişine bir öncelik atayın. Bir kural girişi şu öznitelikleri içerir: kullanıcı hesabı, eylem (izin ver/engelle) ve öncelik.

      Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

c. **Eylem** bölümünde kullanıcının yazıcıdaki yazdırma erişimini yapılandırın.

d. **Kullanıcılar ve gruplar**'a tıklayın ve yazdırmaya erişim için kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

e. **Tamam**'a tıklayın.

9. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da yazdırma kuralları ekleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.
5. **Aygıt erişim kuralları** bloğunda, **Aygıtlar ve Wi-Fi ağları** bağlantısına tıklayın.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **Yerel yazıcılar** veya **Ağ yazıcıları** cihaz türünü seçin.

   Yazıcı erişim kuralları açılır.
7. İlgili yazıcılar için erişim modunu yapılandırın: **İzin ver**, **Engelle**, **İzin ver ve günlüğe kaydetme** (yalnızca ağ yazıcıları için), **Veri yoluna bağlıdır** (yalnızca yerel yazıcılar için) veya **Özel**.
8. **Özel** modunu seçtiğinizde, yerel yazıcılar veya ağ yazıcıları için yazdırma kuralları eklemelisiniz. Bunu yapmak için yazdırma kuralları tablosundaki **Ekle** düğmesine tıklayın.

   Yeni yazdırma kuralının ayarları açılır.
9. Kural girişine bir öncelik atayın. Bir kural girişi şu öznitelikleri içerir: kullanıcı hesabı, eylem (izin ver/engelle) ve öncelik.

   Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

   Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

   Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.
10. **Eylem** bölümünde kullanıcının yazıcıdaki yazdırma erişimini yapılandırın.

11. **Kullanıcı ve grup** bölümünde, yazdırmaya erişim için kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

12. Değişikliklerinizi kaydedin.

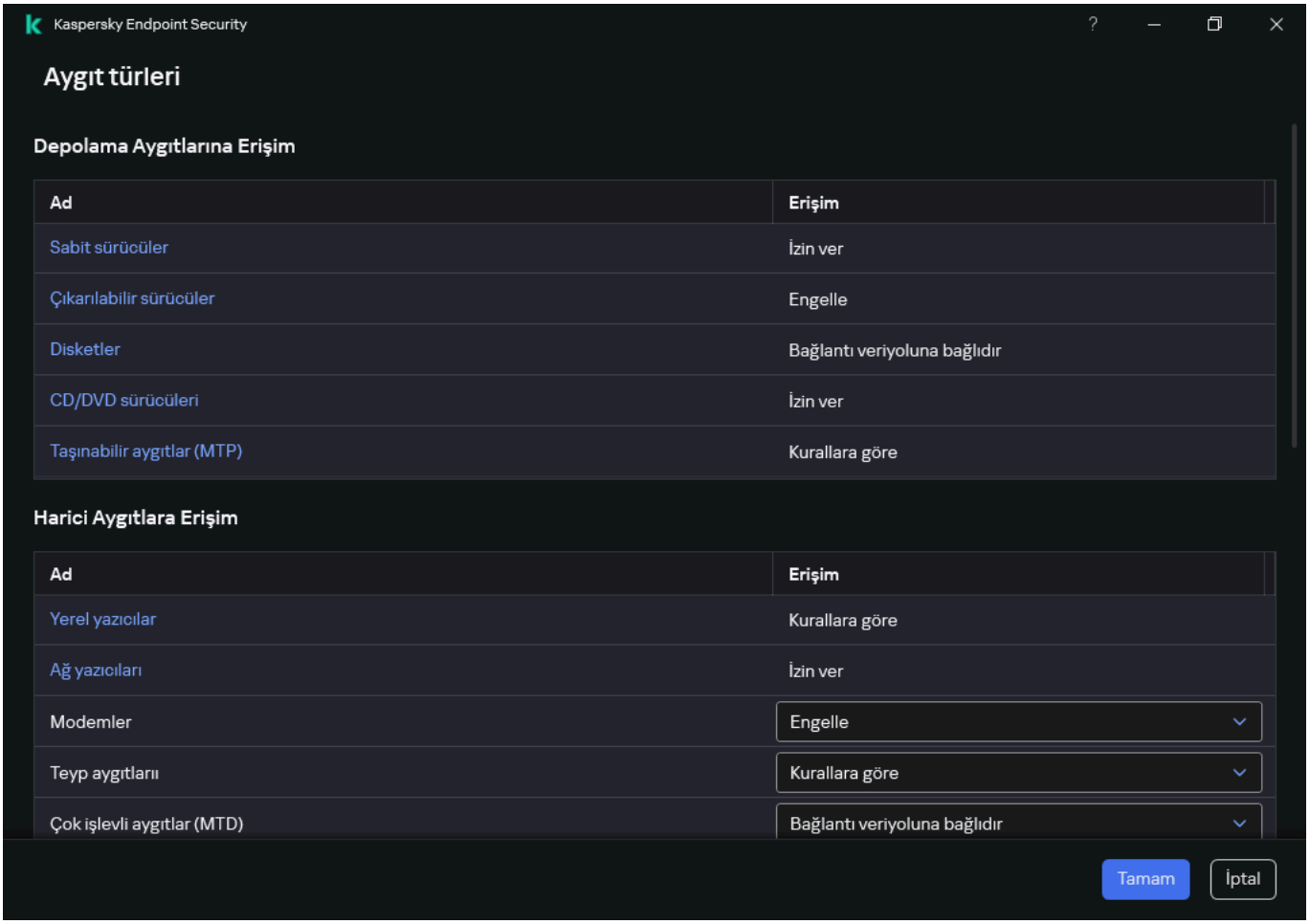
Uygulama arabiriminde yazdırma kuralları nasıl eklenir

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.

3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** düğmesine tıklayın.

   Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.



Aygıt Denetimi bileşenindeki aygıt türleri

4. **Harici Aygıtlara Erişim** bölümünde, **Yerel yazıcılar** veya **Ağ yazıcıları** seçimini yapın.

   Yazıcı erişim kurallarını içeren bir pencere açılır.

5. **Yerel yazıcılara erişim** veya **Ağ yazıcılarına erişim** altında yazıcılar için erişim modunu yapılandırın: **İzin ver**, **Engelle**, **İzin ver ve günlüğe kaydetme** (yalnızca ağ yazıcıları için), **Bağlantı veriyoluna bağlıdır** (yalnızca yerel yazıcılar için) veya **Kurallara göre**.

6. **Kurallara göre** modunu seçtiğinizde, yazıcılar için yazdırma kuralları eklemelisiniz. Yazdırma kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.

   a. **Ekle**'ye tıklayın.

      Yeni bir yazdırma kuralı eklemek için bir pencere açılır.

b. Kural girişine bir öncelik atayın. Bir kural girişi şu öznitelikleri içerir: kullanıcı hesabı, izinler (izin ver/engelle) ve öncelik.

   Bir kuralın belirli bir önceliği vardır. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Kaspersky Endpoint Security, 0 ila 10.000 arasında öncelik atamanıza olanak tanır. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

   Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

   Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Diğer bir deyişle, bir kullanıcı birden fazla gruba eklenmişse ve tüm kuralların önceliği aynıysa, Kaspersky Endpoint Security, aygıt erişimini mevcut engelleme kurallarına göre düzenler.

c. **Eylem** bölümünde, yazdırmaya erişim için kullanıcı izinlerini yapılandırın.

d. **Kullanıcılar ve gruplar** bölümünde, yazdırmaya erişim için kullanıcıları veya kullanıcı gruplarını seçin. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

7. Değişikliklerinizi kaydedin.

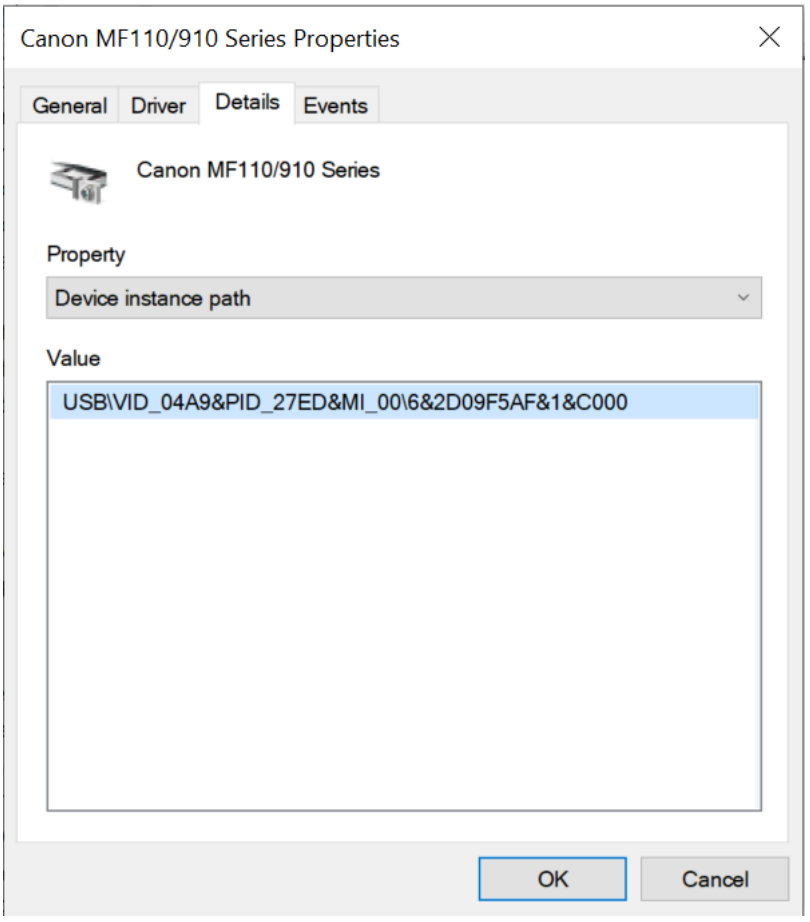
Güvenilir yazıcılar

Güvenilir aygıtlar, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

Güvenilir yazıcılar ekleme prosedürü diğer güvenilir cihaz türleri ile tamamen aynıdır. Kimliğe veya cihaz modeline göre yerel yazıcılar ekleyebilirsiniz. Ağ yazıcılarını yalnızca cihaz kimliğine göre ekleyebilirsiniz.

Kimliğe göre güvenilir bir yerel yazıcı eklemek için benzersiz bir kimliğe (Hardware ID – HWID) ihtiyacınız olacaktır. Kimliği, işletim sistemi araçlarını kullanarak cihaz özelliklerinde bulabilirsiniz (aşağıdaki şekle bakın). Device Manager aracı bunu yapmanızı sağlar. Yerel bir yazıcının kimliği şöyle görünebilir: `6&2D09F5AF&1&C000`. Birkaç belirli cihazı eklemek istiyorsanız cihazları kimliğe göre eklemek uygundur. Maskeler de kullanabilirsiniz.

Cihaz modeline göre güvenilir bir yerel yazıcı eklemek için Vendor ID (VID) ve Product ID (PID)ye ihtiyacınız olacaktır. Kimlikleri, işletim sistemi araçlarını kullanarak cihaz özelliklerinde bulabilirsiniz (aşağıdaki şekle bakın). VID ve PID girme şablonu: `VID_04A9&PID_27FD`. Kuruluşunuzda belirli bir model cihazlar kullanıyorsanız cihazları modele göre eklemek uygundur. Böylece bu model tüm cihazları ekleyebilirsiniz.



Aygıt Yöneticisinde Aygıt Kimliği

Güvenilir bir ağ yazıcısı eklemek için, ağ yazıcısının aygıt kimliğine ihtiyacınız olacak. Ağ yazıcıları için aygıt kimliği, yazıcının ağ adı (paylaşılan yazıcının adı), yazıcının IP adresi veya yazıcının URL'si olabilir.

Wi-Fi bağlantılarının kontrolü

Aygıt Denetimi, bilgisayarın (dizüstü bilgisayar) Wi-Fi bağlantısını yönetmeye olanak tanır. Genel Wi-Fi ağları güvenli olmayabilir ve bu tür ağların kullanılması veri kaybına neden olabilir. Aygıt Denetimi, bir kullanıcının Wi-Fi ağına bağlanmasını engellemenizi veya yalnızca güvenilir ağlara bağlanmasına izin vermenizi sağlar. Örneğin, yalnızca yeterince güvenli olan kurumsal Wi-Fi ağına bağlanmaya izin verebilirsiniz. Aygıt Denetimi, güvenilir listede belirtilenlerin haricinde tüm Wi-Fi ağlarına erişimi engeller.

Windows 11 çalıştıran bilgisayarlarda Wi-Fi bağlantılarını kontrol etmek için Konum hizmetlerini etkinleştirmeniz gerekir. Bunu yapmak için, işletim sistemi ayarlarında **Konum hizmetleri** anahtarını etkinleştirmeniz gerekir (**Ayarlar** → **Gizlilik ve güvenlik** → **Konum**). Konum hizmetleri devre dışı bırakılırsa Kaspersky Endpoint Security, Wi-Fi ağlarına olan bağlantıları kontrol etmez.

Yönetim Konsolu'nda (MMC) Wi-Fi bağlantılarını kısıtlama

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
4. **Aygıt Denetimi ayarları** bölümünden **Aygıt türleri** sekmesini seçin.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
5. **Wi-Fi** cihaz türünün bağlam menüsünde, Wi-Fi'ye bağlanırken gerçekleştirilen Aygıt Denetimi işlemini seçin: **İzin ver** (), **Engelle** () veya **İstisnalarla engelle** ().
6. **İstisnalarla engelle** seçeneğini seçtiyseniz güvenilir Wi-Fi ağlarının bir listesini oluştur:

   a. Güvenilir Wi-Fi ağlarının listesini açmak için çift tıklayın.

   b. **Güvenilir Wi-Fi ağları** bloğunda **Ekle** düğmesine tıklayın.

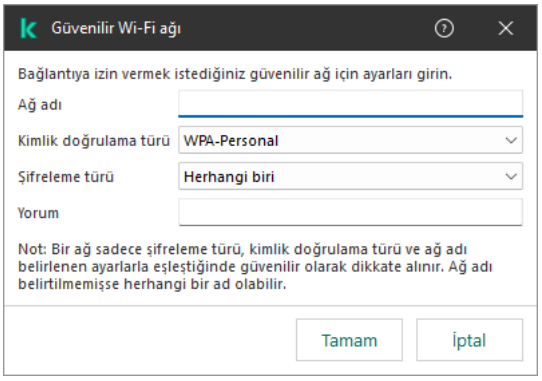
   c. Böylece açılan pencerede, güvenilir Wi-Fi ağını yapılandırın (aşağıdaki şekle bakın):

   - **Ağ adı**. Wi-Fi ağının adı veya SSID'si (Service Set Identifier).
   - **Kimlik doğrulama türü**. Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türü.

     Kaspersky Endpoint Security for Windows sürüm 12.0'dan itibaren uygulamaya WPA3 protokol desteği eklendi. Bir bilgisayara Kaspersky Endpoint Security sürüm 12.2 ilkesi uygulanırsa, Kaspersky Endpoint Security sürüm 11.11.0 ve önceki sürümlere sahip bilgisayarlarda WPA2 protokolü seçilir; 12.0 ila 12.1 sürümleri için WPA2/WPA3 seçilir; 12.2 ve sonraki sürümler için WPA3 seçilir.
   - **Şifreleme türü**. Wi-Fi trafiğini korumak için kullanılan şifreleme türü.
   - **Yorum**. Eklenen Wi-Fi ağı hakkında daha fazla bilgi.

   Güvenilir Wi-Fi ağının ayarlarını yönlendirici ayarlarında görüntüleyebilirsiniz.

   Bir Wi-Fi ağı, ayarları kuralda belirtilen tüm ayarlarla eşleşiyorsa güvenilir kabul edilir.
7. Değişikliklerinizi kaydedin.



Güvenilir Wi-Fi ağ ayarları

Web Console ve Cloud Console'da Wi-Fi bağlantılarını kısıtlama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.
5. **Cihaz erişim kuralları** bölümünde, **Cihazlar ve Wi-Fi ağları** sekmesini seçin.
   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **Wi-Fi ağları** bloğunda, **Wi-Fi** bağlantısına tıklayın.
7. Açılan pencerede, Wi-Fi'ye bağlanırken gerçekleştirilen Aygıt Denetimi eylemini seçin: **İzin Ver**, **Engelle** veya **İstisnalarla Engelle**.
8. **İstisnalarla engelle** seçeneğini tercih ettiğinizde, güvenilir Wi-Fi ağlarının bir listesini oluşturun:
   a. Güvenilir Wi-Fi ağlarının listesini açmak için çift tıklayın.
   b. **Güvenilir Wi-Fi ağları** bloğunda **Ekle** düğmesine tıklayın.
   c. Böylece açılan pencerede, güvenilir Wi-Fi ağını yapılandırın (aşağıdaki şekle bakın):
      - **Ad**. Wi-Fi ağının adı veya SSID'si (Service Set Identifier).
      - **Kimlik doğrulama türü**. Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türü.

        Kaspersky Endpoint Security for Windows sürüm 12.0'dan itibaren uygulamaya WPA3 protokol desteği eklendi. Bir bilgisayara Kaspersky Endpoint Security sürüm 12.2 ilkesi uygulanırsa, Kaspersky Endpoint Security sürüm 11.11.0 ve önceki sürümlere sahip bilgisayarlarda WPA2 protokolü seçilir; 12.0 ila 12.1 sürümleri için WPA2/WPA3 seçilir; 12.2 ve sonraki sürümler için WPA3 seçilir.

      - **Şifreleme türü**. Wi-Fi trafiğini korumak için kullanılan şifreleme türü.
      - **Yorum**. Eklenen Wi-Fi ağı hakkında daha fazla bilgi.

   Güvenilir Wi-Fi ağının ayarlarını yönlendirici ayarlarında görüntüleyebilirsiniz.

   Bir Wi-Fi ağı, ayarları kuralda belirtilen tüm ayarlarla eşleşiyorsa güvenilir kabul edilir.
9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Wi-Fi bağlantılarını kısıtlama

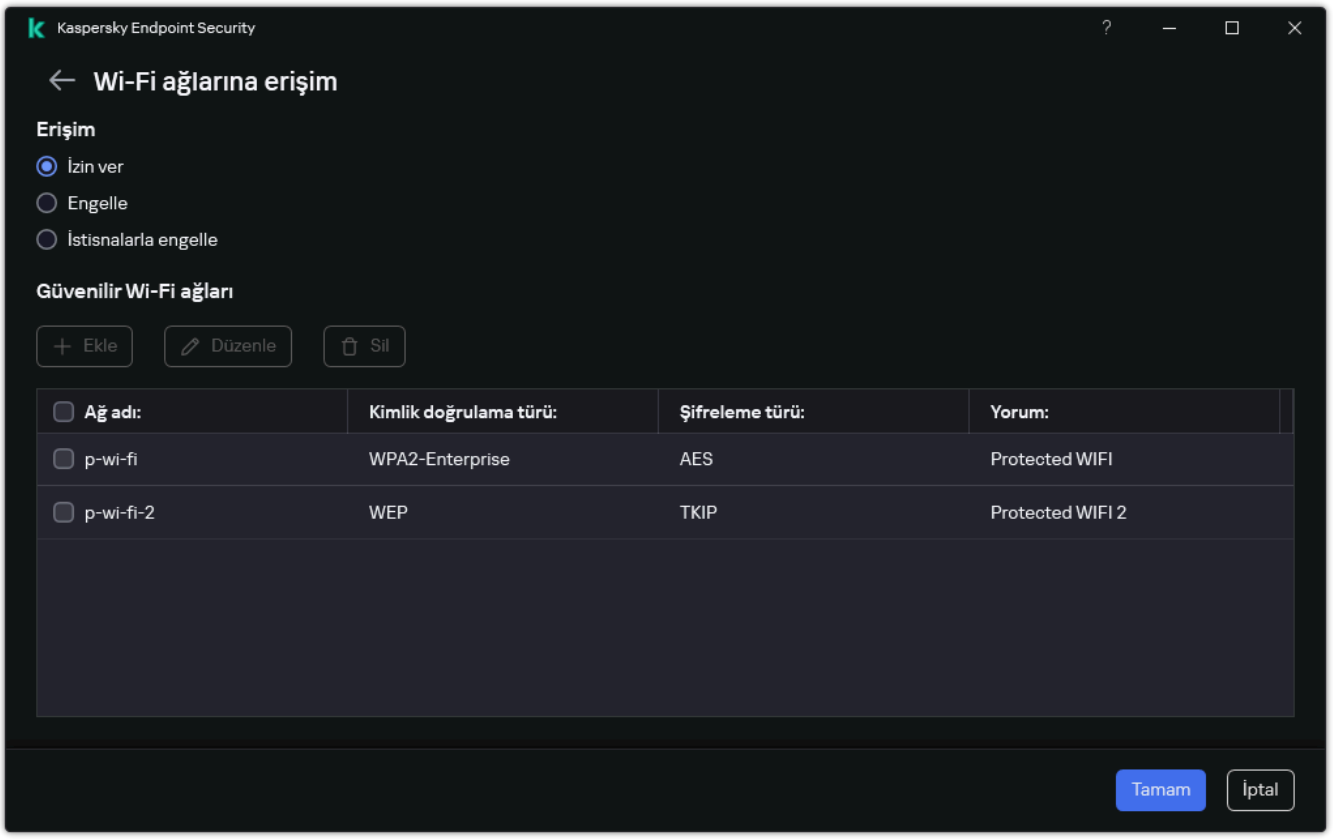
1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.

3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** düğmesine tıklayın.

   Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.

4. **Wi-Fi ağlarına erişim** bloğunda, **Wi-Fi** bağlantısına tıklayın.

   Açılan pencerede Wi-Fi ağ erişim kuralları görüntülenir.



Wi-Fi erişim ayarları

5. **Erişim** bölümünde Wi-Fi'ye bağlanırken gerçekleştirilen Aygıt Denetimi eylemini seçin: **İzin ver**, **Engelle** veya **İstisnalarla engelle**.

6. **İstisnalarla engelle** seçeneğini seçtiyseniz güvenilir Wi-Fi ağlarının bir listesini oluştur:

   a. **Güvenilir Wi-Fi ağları** bloğunda **Ekle** düğmesine tıklayın.

   b. Böylece açılan pencerede, güvenilir Wi-Fi ağını yapılandırın (aşağıdaki şekle bakın):

   - **Ağ adı**. Wi-Fi ağının adı veya SSID'si (Service Set Identifier).
   - **Kimlik doğrulama türü**. Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türü.

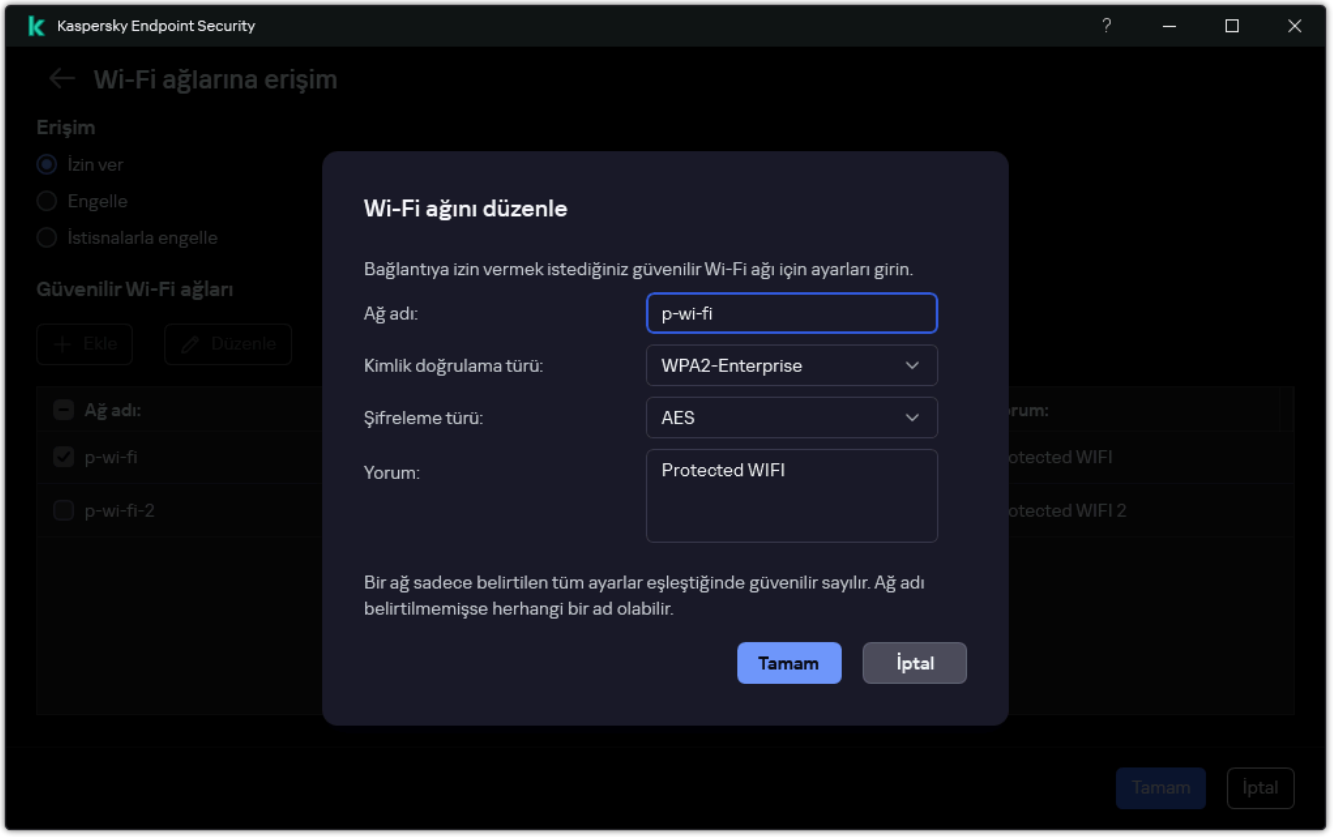
     Kaspersky Endpoint Security for Windows sürüm 12.0'dan itibaren uygulamaya WPA3 protokol desteği eklendi. Bir bilgisayara Kaspersky Endpoint Security sürüm 12.2 ilkesi uygulanırsa, Kaspersky Endpoint Security sürüm 11.11.0 ve önceki sürümlere sahip bilgisayarlarda WPA2 protokolü seçilir; 12.0 ila 12.1 sürümleri için WPA2/WPA3 seçilir; 12.2 ve sonraki sürümler için WPA3 seçilir.

   - **Şifreleme türü**. Wi-Fi trafiğini korumak için kullanılan şifreleme türü.
   - **Yorum**. Eklenen Wi-Fi ağı hakkında daha fazla bilgi.

Güvenilir Wi-Fi ağının ayarlarını yönlendirici ayarlarında görüntüleyebilirsiniz.

Bir Wi-Fi ağı, ayarları kuralda belirtilen tüm ayarlarla eşleşiyorsa güvenilir kabul edilir.

7. Değişikliklerinizi kaydedin.



Güvenilir Wi-Fi ağ ayarları

Sonuç olarak, bir kullanıcı güvenilir olarak listelenmeyen bir Wi-Fi ağına bağlanmaya çalıştığında, uygulama bağlantıyı engeller ve bir bildirim görüntüler (aşağıdaki şekle bakın).



Aygıt Denetimi bildirimi

Çıkarılabilir sürücülerin kullanımını izleme

Çıkarılabilir sürücülerin kullanımını izleme şunları kapsar:

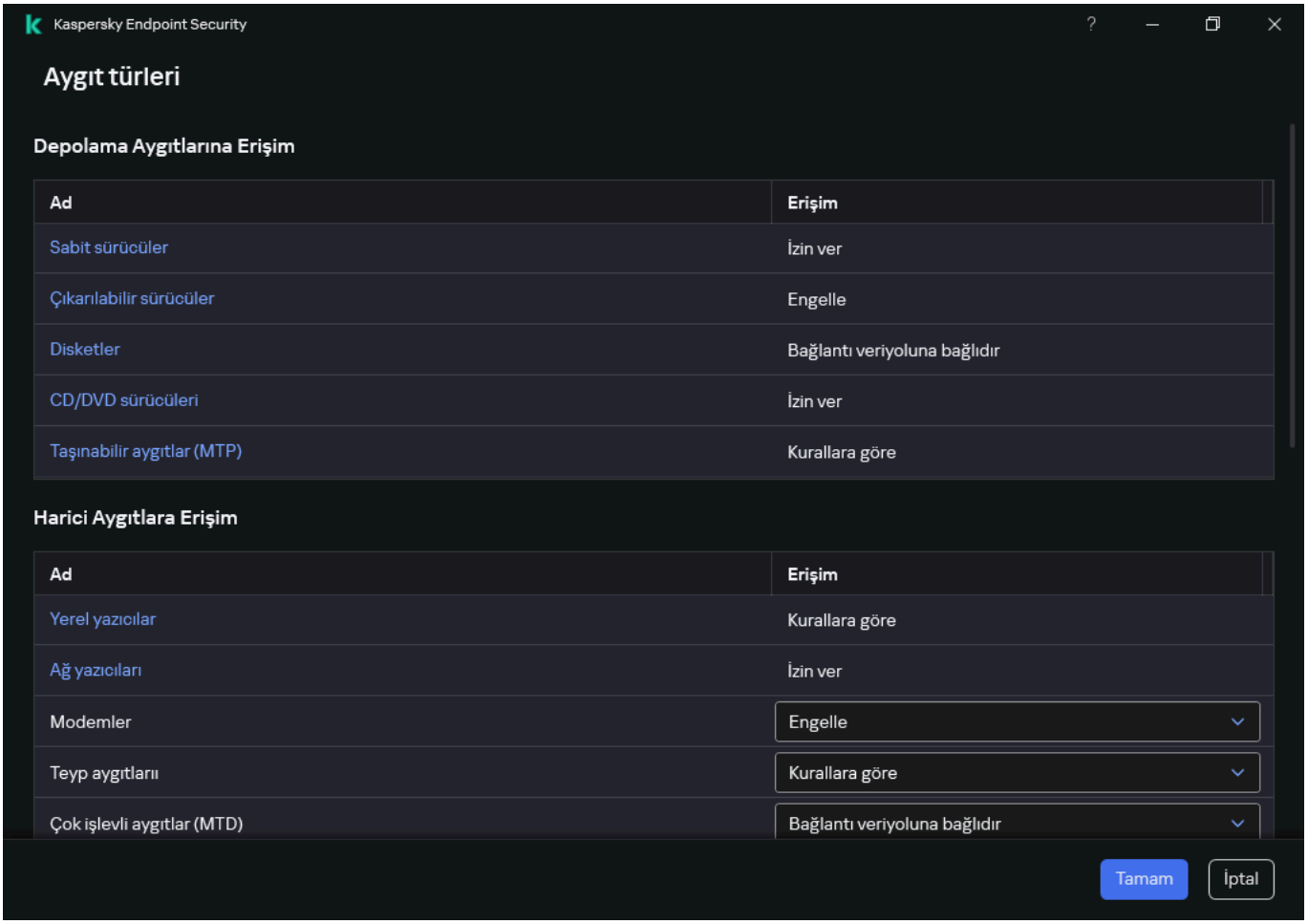
- Çıkarılabilir sürücülerdeki dosyalar üzerinde gerçekleştirilen işlemleri izleme.
- Güvenilir çıkarılabilir sürücüler için bağlantı ve bağlantı kesme işlemlerini izleme.

  Kaspersky Endpoint Security, yalnızca çıkarılabilir sürücülerin değil, tüm güvenilir cihazlar için bağlantı ve bağlantı kesme işlemlerinin izlenmesine olanak tanır. Aygıt Denetimi bileşeni için bildirim ayarları bölümünden olay günlük kaydını açabilirsiniz. Olaylar *Bilgilendirici mesaj* önem seviyesine sahiptir.

Çıkarılabilir sürücü kullanımını izlemeyi etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları** düğmesine tıklayın.

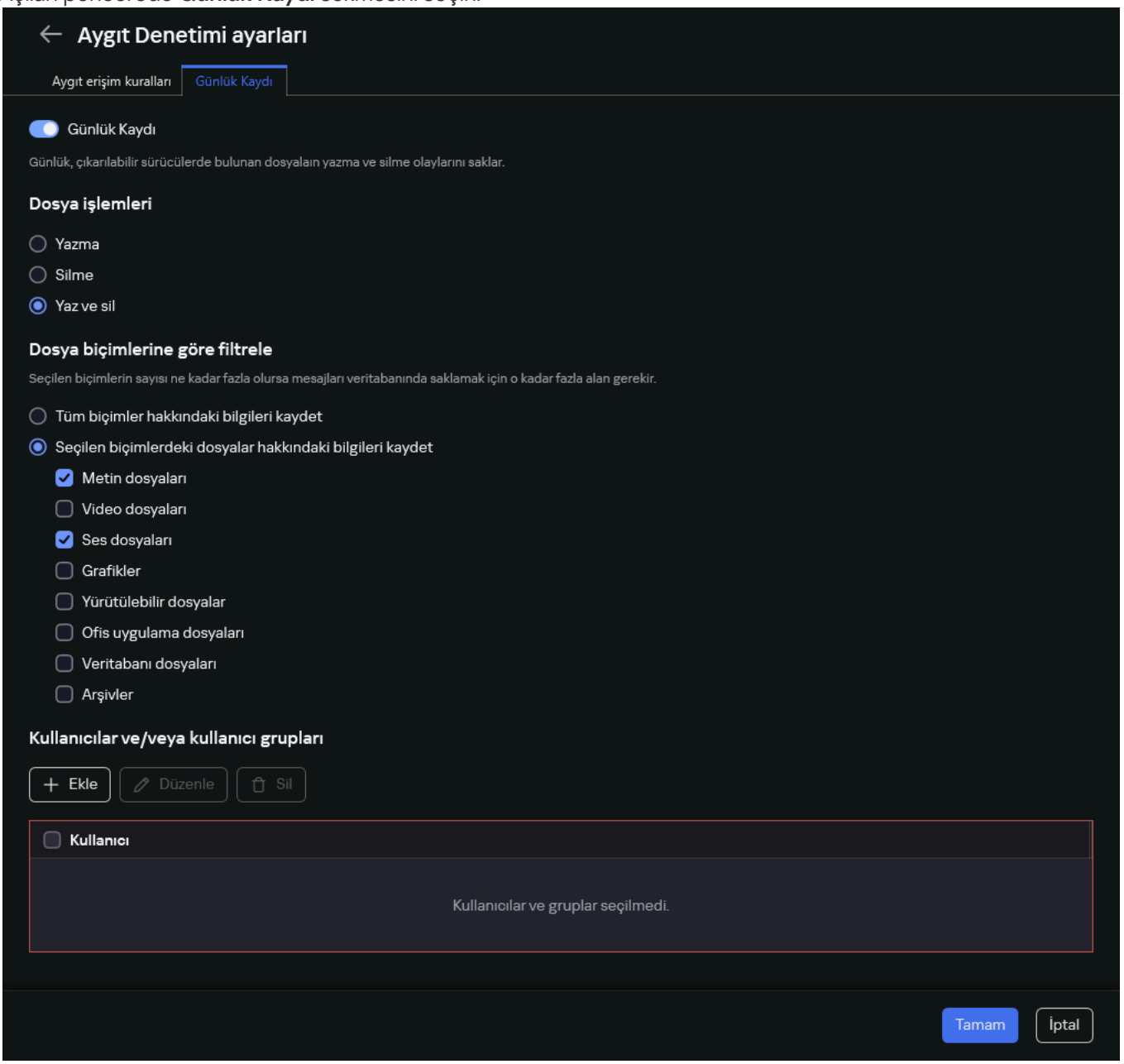
   Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.



Aygıt Denetimi bileşenindeki aygıt türleri

4. **Depolama Aygıtlarına Erişim** bloğundan **Çıkarılabilir sürücüler** öğesini seçin.

5. Açılan pencerede **Günlük Kaydı** sekmesini seçin.



Çıkarılabilir sürücü kullanımı izleme ayarları

6. **Günlük Kaydı** geçiş düğmesini açın.

7. **Dosya işlemleri** bloğunda, izlemek istediğiniz işlemleri seçin: **Yazma**, **Silme**.

8. **Dosya biçimlerine göre filtrele** bloğunda, ilişkili işlemlerinin Aygıt Denetimi tarafından günlüğe kaydedilmesi gereken dosyaların türlerini seçin.

9. Çıkarılabilir sürücü kullanımını izlemek istediğiniz kullanıcıları veya kullanıcı grubunu seçin.

10. Değişikliklerinizi kaydedin.

Sonuç olarak, kullanıcılar çıkarılabilir sürücülerdeki dosyalara yazdığında ya da çıkarılabilir sürücülerden dosya sildiklerinde Kaspersky Endpoint Security bu işlemler hakkında olay günlüğüne bilgi kaydeder ve olayları Kaspersky Security Center'a gönderir. Çıkarılabilir sürücülerdeki dosyalarla ilişkili olayları Kaspersky Security Center Yönetim Konsolu'nda **Olaylar** sekmesindeki **Yönetim Sunucusu** düğümünün çalışma alanından görüntüleyebilirsiniz. Olayların yerel Kaspersky Endpoint Security olay günlüğünde görüntülenmesi için Aygıt Denetimi bileşeni için bildirim ayarlarındaki **Dosya işlemi gerçekleştirildi** onay kutusunu seçmelisiniz.

Önbelleğe alma süresini değiştirme

Aygıt Denetimi bileşeni, bir aygıtın bağlanması ve bağlantısının kesilmesi, bir aygıttan bir dosyanın okunması, bir aygıta bir dosyanın yazılması ve diğer olaylar gibi izlenen aygıtlarla ilgili olayları kaydeder. Aygıt Denetimi daha sonra Kaspersky Endpoint Security ayarlarına göre eyleme izin verir veya eylemi engeller.

Aygıt Denetimi, olaylar hakkındaki bilgileri *önbelleğe alma dönemi* adı verilen belirli bir süre boyunca kaydeder. Bir olay hakkındaki bilgiler önbelleğe alınırsa ve bu olay tekrarlanırsa, Kaspersky Endpoint Security'yi bu konuda bilgilendirmeye veya bir aygıtı bağlamak gibi ilgili eyleme erişim izni vermek için başka bir bilgi istemi göstermeye gerek yoktur. Bu, bir aygıtla çalışmayı daha kolay hale getirir.

Aşağıdaki olay ayarlarının tümü önbellekteki kayıtla eşleşirse, olay yinelenen olay olarak kabul edilir:

- aygıt kimliği
- Erişmeye çalışan kullanıcı hesabının SID'si
- Aygıt kategorisi
- Aygıtla yapılan işlem
- Bu eylem için uygulama izni: izin verildi veya reddedildi
- Eylemi gerçekleştirmek için kullanılan sürecin yolu
- Erişilmekte olan dosya

Önbelleğe alma süresini değiştirmeden önce Kaspersky Endpoint Security Kendini Korumayı devre dışı bırakın. Önbelleğe alma süresini değiştirdikten sonra, Kendini Korumayı etkinleştirin.

Önbelleğe alma süresini değiştirmek için:

1. Bilgisayardaki kayıt defteri düzenleyicisini açın.
2. Kayıt düzenleyicisinde aşağıdaki bölüme gidin:
   - 64-bit işletim sistemleri için:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - 32-bit işletim sistemleri için:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Düzenlemek için `DeviceControlEventsCachePeriod` anahtarını açın.
4. Bu bilgiler silinmeden önce Aygıt Denetiminin bir olay hakkındaki bilgileri kaydetmesi gereken dakika sayısını tanımlayın.

Güvenilir aygıtlarla eylemler

Güvenilir aygıtlar, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

Güvenilir aygıtlarla çalışmak için bir kullanıcıya, bir kullanıcı grubuna ya da kuruluşun tüm kullanıcılarına erişim verebilirsiniz.

Örneğin, kuruluşunuz çıkarılabilir sürücülerin kullanılmasına izin vermediği halde yöneticiler işlerinde çıkarılabilir sürücüleri kullanıyorlarsa, çıkarılabilir sürücülere sadece bir grup yönetici için izin verebilirsiniz. Bunu yapmak için çıkarılabilir sürücüleri güvenilir listeye ekleyin ve kullanıcı erişim izinlerini yapılandırın.

Sistem kararsızlığına neden olabileceği için 5000'den fazla güvenilir cihaz eklenmesi önerilmez.

Kaspersky Endpoint Security, bir aygıtı güvenilir listeye şu şekillerde eklemenize izin verir:

- Kaspersky Security Center kuruluşunuzda dağıtılmamışsa cihazı bilgisayara bağlayabilir ve uygulama ayarlarından güvenilir listeye ekleyebilirsiniz. Güvenilir aygıtlar listesini kuruluşunuzdaki tüm bilgisayarlara dağıtmak için bir ilkedeki güvenilir aygıtların listesini birleştirmeyi etkinleştirebilir ya da dışa aktar/içe aktar prosedürünü kullanabilirsiniz.

- Kaspersky Security Center kuruluşunuza dağıtılmamışsa tüm bağlı cihazları uzaktan tespit edebilir ve ilkede bir güvenilir aygıtlar listesi oluşturabilirsiniz. Güvenilir aygıtlar listesi, ilkenin uygulandığı bütün bilgisayarlarda kullanılabilir olacaktır.

Kaspersky Endpoint Security, güvenilir aygıtların kullanımının (bağlantı ve bağlantı kesme) kontrol edilmesini sağlar. Aygıt Denetimi bileşeni için bildirim ayarları bölümünden olay günlük kaydını açabilirsiniz. Olaylar *Bilgilendirici mesajlar* önem seviyesine sahiptir.

Bir cihazı güvenilir listeye ekleme

Kaspersky Security Center, Kaspersky Endpoint Security bilgisayarlarda yüklüyse, Aygıt Denetimi etkinleştirilmişse ve cihaz verilerinin iletimi etkinleştirilmişse cihazlar hakkında bilgi alır. Kaspersky Security Center'da bu aygıt hakkındaki bilgiler kullanılabilir olmadığında, bu aygıtı güvenilir listeye eklemek mümkün olmaz.

Varsayılan olarak güvenilir aygıtlar listesine bir aygıt eklendiğinde tüm kullanıcılara aygıtlara erişim izni verilir (Herkes kullanıcı grubu).

Bir aygıtı güvenilir listeye şu verilere göre ekleyebilirsiniz:

- **Kimliğe göre aygıtlar**. Her cihazın benzersiz bir tanımlayıcısı (Hardware ID veya HWID) vardır. Bu kimliği, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. Cihaz kimliği örneği: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Birkaç belirli cihazı eklemek istiyorsanız cihazları kimliğe göre eklemek uygundur.

- **Modele göre aygıtlar**. Her cihazın bir Vendor ID (VID) ve bir Product ID (PID) vardır. Bu kimlikleri, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. VID ve PID girme şablonu: `VID_1234&PID_5678`. Kuruluşunuzda belirli bir model cihazlar kullanıyorsanız cihazları modele göre eklemek uygundur. Böylece bu model tüm cihazları ekleyebilirsiniz.

- **Kimlik maskesine göre aygıtlar**. Benzer kimliklere sahip birden fazla cihaz kullanıyorsanız, cihazları güvenilir listeye maskeler kullanarak ekleyebilirsiniz. `*` karakteri herhangi bir karakter kümesinin yerini alır. Kaspersky Endpoint Security, bir maske girişi yapılırken `?` karakterinin kullanımını desteklemez. Örneğin, `WDC_C*`.

- **Model maskesine göre aygıtlar**. Benzer VID veya PID sahibi birden fazla aygıt kullanıyorsanız (örneğin aynı üreticinin aygıtları) maskeler kullanarak güvenilir listeye aygıt ekleyebilirsiniz. `*` karakteri herhangi bir karakter kümesinin yerini alır. Kaspersky Endpoint Security, bir maske girişi yapılırken `?` karakterinin kullanımını desteklemez. Örneğin, `VID_05AC&PID_*`.

Yönetim Konsolu'nda (MMC) güvenilir listeye cihaz nasıl eklenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
5. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.
6. Şirketteki tüm bilgisayarlar için birleştirilmiş bir güvenilir aygıtlar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin.

   Ana ve alt ilkelerdeki güvenilir aygıtlar listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki güvenilir aygıtlar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin güvenilir aygıtlarının değiştirilmesi veya silinmesi mümkün değildir.
7. **Ekle** düğmesine tıklayın ve bir aygıtı güvenilir listeye eklemek için bir yöntem seçin.
8. Aygıtları filtrelemek için **Aygıt türü** açılır listesinden bir aygıt türü seçin (örneğin, **Çıkarılabilir sürücüler**).

   Kaspersky Endpoint Security, **Disketler** türündeki cihazların güvenilirler listesine eklenmesini desteklemez.
9. **Ad / Model** alanına, seçilen ekleme yöntemine bağlı olarak aygıt kimliği, modeli (VID ve PID) veya maske girin.

   Aygıtlar model maskesine (VID ve PID) göre eklenince şöyle bir işleyiş gerçekleşir: herhangi bir modelle eşleşmeyen bir model maskesi girmeniz girerseniz Kaspersky Endpoint Security aygıt kimliğinin (HWID) maske ile eşleşip eşleşmediğini denetler. Kaspersky Endpoint Security, aygıt kimliğinin sadece üretici ve aygıt türü kısmını denetler (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Model maskesinin aygıt kimliğinin bu kısmı ile eşleşmesi halinde, maske ile eşleşen aygıtlar bilgisayardaki güvenilir aygıtlar listesine eklenecektir. Aynı zamanda, **Yükselt** düğmesine tıkladığınızda Kaspersky Security Center'daki aygıtlar listesi boş kalır. Aygıtların listesini doğru bir şekilde görüntülemek için aygıtları aygıt kimliği maskesine göre ekleyebilirsiniz.
10. Aygıtları filtrelemek için **Bilgisayar** alanına bilgisayar adını veya aygıtın bağlandığı bilgisayarın adı için bir maske girin.

    `*` karakteri herhangi bir karakter kümesinin yerini alır. `?` karakteri herhangi bir karakterin yerini alır.
11. **Yükselt** seçeneğine tıklayın.

    Tabloda, tanımlanan filtreleme kriterlerini sağlayan bir aygıtlar listesi görüntülenir.

12. Güvenilir listeye eklemek istediğiniz aygıt adlarının karşısındaki onay kutularını seçin.

13. **Yorum** alanına, aygıtların güvenilir listeye eklenme sebebi için bir açıklama girin.

14. **Kullanıcılara ve/veya kullanıcı gruplarına izin verin** alanının sağındaki **Seç** düğmesine tıklayın.

    Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

    Varsayılan olarak, Herkes grubu için güvenilir aygıtlara erişime izin verilir.

15. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da güvenilir listeye cihaz nasıl eklenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenilir Bölge** bölümüne gidin.

5. Açılan pencerede **Cihazlar** bağlantısına tıklayın.

   Bu, güvenilir cihazların listesini içeren bir pencere açar.

6. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.

7. Şirketteki tüm bilgisayarlar için birleştirilmiş bir güvenilir aygıtlar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin.

   Ana ve alt ilkelerdeki güvenilir aygıtlar listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki güvenilir aygıtlar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin güvenilir aygıtlarının değiştirilmesi veya silinmesi mümkün değildir.

8. **Ekle**'ye tıklayın.

   Güvenilir cihaz ekleme formu açılır.

9. **Kullanıcı veya grup** bölümünde, güvenilir cihazlara erişmesine izin vermek istediğiniz kullanıcıları seçin.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   Varsayılan olarak, Herkes grubu için güvenilir aygıtlara erişime izin verilir.

10. Aygıtları filtrelemek için **Aygıt türü** açılır listesinden bir aygıt türü seçin (örneğin, **Çıkarılabilir sürücüler**).

    Kaspersky Endpoint Security, **Disketler** türündeki cihazların güvenilirler listesine eklenmesini desteklemez.

11. Tam cihaz kimliğini veya cihaz modelini bilmiyorsanız **Maske kullan** onay kutusunu işaretleyin.

12. Cihazı nasıl eklemek istediğinizi seçin: cihaz kimliğine veya modeline göre (VID ve PID).

    Aygıtlar model maskesine (VID ve PID) göre eklenince şöyle bir işleyiş gerçekleşir: herhangi bir modelle eşleşmeyen bir model maskesi girmeniz girerseniz Kaspersky Endpoint Security aygıt kimliğinin (HWID) maske ile eşleşip eşleşmediğini denetler. Kaspersky Endpoint Security, aygıt kimliğinin sadece üretici ve aygıt türü kısmını denetler (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Model maskesinin aygıt kimliğinin bu kısmı ile eşleşmesi halinde, maske ile eşleşen aygıtlar bilgisayardaki güvenilir aygıtlar listesine eklenecektir. Aynı zamanda Kaspersky Security Center'da boş cihaz listesi görüntülenir. Aygıtların listesini doğru bir şekilde görüntülemek için aygıtları aygıt kimliği maskesine göre ekleyebilirsiniz.

13. Cihazları filtrelemek için **Güvenilir cihazları ara** alanına bilgisayar adını veya cihazın bağlı olduğu bilgisayarın adı için bir maske girin.

    `*` karakteri herhangi bir karakter kümesinin yerini alır. `?` karakteri herhangi bir karakterin yerini alır.

    Tabloda, tanımlanan filtreleme kriterlerini sağlayan bir aygıtlar listesi görüntülenir.

14. Güvenilir listeye eklemek istediğiniz aygıt adlarının karşısındaki onay kutularını seçin.

15. **Yorum** alanına, aygıtların güvenilir listeye eklenme sebebi için bir açıklama girin.

16. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde güvenilir listeye cihaz nasıl eklenir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Güvenilir aygıtlar** düğmesine tıklayın.

   Bu, güvenilir aygıtlar listesini açar.

4. **Seç**'e tıklayın.

   Bu, bağlı aygıtların listesini açar. Aygıtlar listesi, **Bağlı aygıtları görüntüle** açılır listesinde seçilen değere bağlıdır.

5. Aygıtlar listesinde, güvenilir listesine eklemek istediğiniz aygıtı seçin.

   Kaspersky Endpoint Security, **Disketler** türündeki cihazların güvenilirler listesine eklenmesini desteklemez.

6. **Yorum** alanında, güvenilir aygıtla ilgili her türlü bilgiyi sağlayabilirsiniz.
7. Güvenilir aygıtlara erişmesine izin vermek istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

8. Değişikliklerinizi kaydedin.

Bir aygıt bağlandığında, Kaspersky Endpoint Security kimliği doğrulanmış bir kullanıcı için güvenilir aygıtlar listesini kontrol eder. Aygıt güvenilir ise, Kaspersky Endpoint Security, aygıt türüne erişim ya da bağlantı veri yolu engellenmiş olsa bile aygıta tüm izinlerle erişime izin verir. Aygıt güvenilir değil ve erişim reddedilmişse kilitli cihaza erişim isteyebilirsiniz.

Güvenilir aygıtlar listesini dışa ve içe aktarma

Güvenilir aygıtlar listesini kuruluşunuzdaki tüm bilgisayarlara dağıtmak için dışa aktar/içe aktar prosedürünü kullanabilirsiniz.

Örneğin, bir güvenilir çıkarılabilir sürücüler listesini dağıtmak isterseniz şunları yapın:

1. Çıkarılabilir sürücüleri bilgisayarınıza sırayla bağlayın.
2. Kaspersky Endpoint Security ayarlarında çıkarılabilir sürücüleri güvenilir listeye ekleyin. Gerekirse kullanıcı erişim izinlerini yapılandırın. Örneğin sadece yöneticilerin çıkarılabilir sürücülere erişmesine izin verin.
3. Kaspersky Endpoint Security ayarlarındaki güvenilir aygıtlar listesini dışa aktarın (aşağıdaki talimatlara bakın).
4. Güvenilir aygıtlar listesi dosyasını kuruluşunuzdaki diğer bilgisayarlara dağıtın. Örneğin dosyayı bir paylaşım klasöre yerleştirin.
5. Kuruluşta bulunan diğer bilgisayarlardaki Kaspersky Endpoint Security ayarlarındaki güvenilir aygıtlar listesini içe aktarın (aşağıdaki talimatlara bakın).

Güvenilir aygıtlar listesini içe veya dışa aktarmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Güvenilir aygıtlar** düğmesine tıklayın.

   Bu, güvenilir aygıtlar listesini açar.
4. Güvenilir aygıtlar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz güvenilir aygıtları seçin.
   b. **Dışa aktar**'a tıklayın.
   c. Açılan pencerede, güvenilir aygıtlar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, güvenilir aygıtlar listesinin tamamını XML dosyasına aktarır.

5. Güvenilir aygıtlar listesini içe aktarmak için:

   a. **İçe aktar** açılır listesinde ilgili eylemi seçin: **İçe aktar ve mevcut olana ekle** veya **İçe aktar ve mevcut olanı değiştir**.

   b. Açılan pencerede, güvenilir aygıtlar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   c. Dosyayı aç.

6. Değişikliklerinizi kaydedin.

Bir aygıt bağlandığında, Kaspersky Endpoint Security kimliği doğrulanmış bir kullanıcı için güvenilir aygıtlar listesini kontrol eder. Aygıt güvenilir ise, Kaspersky Endpoint Security, aygıt türüne erişim ya da bağlantı veri yolu engellenmiş olsa bile aygıta tüm izinlerle erişime izin verir.

Engellenen bir aygıta erişim elde etme

Aygıt Denetimini yapılandırılırken, çalışma için gerekli olan bir aygıta erişimi yanlışlıkla engelleyebilirsiniz.

Kaspersky Security Center kuruluşunuzda dağıtılmamışsa, Kaspersky Endpoint Security ayarlarında bir aygıta erişim sağlayabilirsiniz. Örneğin aygıtı güvenilir listesine ekleyebilir ya da geçici olarak Aygıt Denetimini devre dışı bırakabilirsiniz.

Kaspersky Security Center kuruluşunuzda dağıtılmışsa ve ilke bilgisayarlara uygulanmışsa, Yönetim Konsolundan bir aygıta erişim sağlayabilirsiniz.

Erişim vermek için çevrimiçi mod

Çevrimiçi modda engellenen bir hizmete erişim verme, ancak Kaspersky Security Center kuruluşta dağıtıldıysa ve bilgisayara bir ilke uygulandıysa yapılabilir. Bilgisayar, Yönetim Sunucusu ile bir bağlantı kurabilmelidir.

Çevrimiçi modda erişim vermek şu adımlardan oluşur:

1. Kullanıcı yöneticiye bir erişim isteği mesajı gönderir.

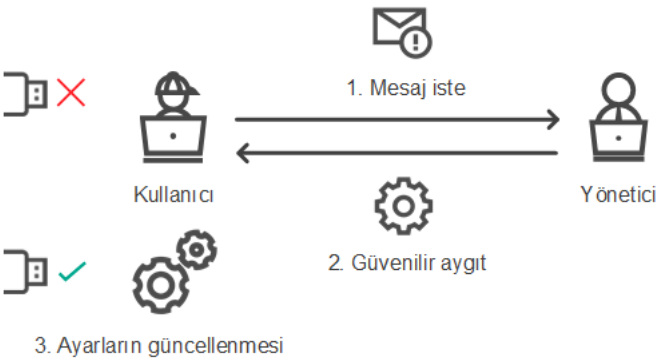
2. Yönetici, Kaspersky Security Center konsolunda isteği içeren bir mesaj alır.

   Kaspersky Security Center konsolunda, kullanıcılardan gelen mesajların kolay takibi için önceden ayarlanmış bir olay seçimi *Kullanıcı istekleri* yer alır.

3. Yönetici aygıtı güvenilir listesine ekler.

   Güvenilir bir aygıtı yönetim grubu için bir ilkeye ya da tek bir bilgisayar için yerel uygulama ayarlarına ekleyebilirsiniz.

4. Yönetici, Kaspersky Endpoint Security ayarlarını kullanıcının bilgisayarında günceller.



Çevrimiçi modda bir cihaza erişim verme şeması

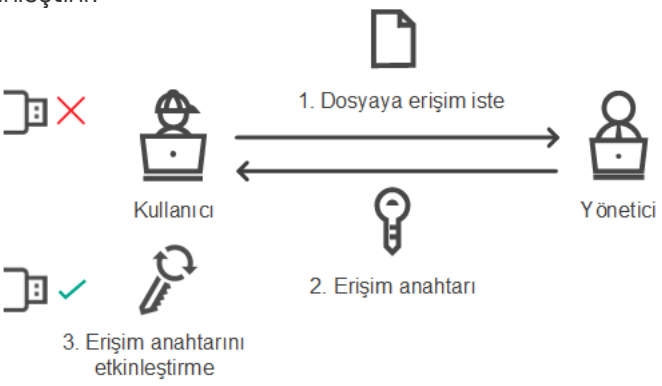
Erişim vermek için çevrimdışı mod

Çevrimdışı modda engellenen bir hizmete erişim verme, ancak Kaspersky Security Center kuruluşta dağıtıldıysa ve bilgisayara bir ilke uygulandıysa yapılabilir. İlke ayarlarında **Aygıt Denetimi** bölümünde yer alan **Geçici erişim isteğine izin ver** onay kutusu seçilmelidir.

Engellenmiş bir aygıta geçici olarak erişim vermeniz gerekiyor ancak aygıtı güvenilir listesine ekleyemiyorsanız, bu aygıta çevrimdışı modda erişim verebilirsiniz. Böylelikle, bilgisayarın ağ erişimi olmasa da ya da bilgisayar kurumsal ağın dışında olsa bile engellenen bir aygıta erişim verebilirsiniz.

Çevrimdışı modda erişim vermek şu adımlardan oluşur:

1. Kullanıcı bir istek erişim dosyası oluşturur ve bu dosyayı yöneticiye gönderir.
2. Yönetici istek erişim dosyasından bir erişim anahtarı oluşturur ve bunu kullanıcıya gönderir.
3. Kullanıcı erişim anahtarını etkinleştirir.



Çevrimdışı modda bir cihaza erişim verme şeması

Erişim vermek için çevrimiçi mod

Çevrimiçi modda engellenen bir hizmete erişim verme, ancak Kaspersky Security Center kuruluşta dağıtıldıysa ve bilgisayara bir ilke uygulandıysa yapılabilir. Bilgisayar, Yönetim Sunucusu ile bir bağlantı kurabilmelidir.

Bir kullanıcı, engellenmiş bir aygıta erişmeyi şu şekilde ister:

1. Aygıtı bilgisayara bağlayın.

   Kaspersky Endpoint Security, aygıta erişimin engellendiğini belirten bir bildirim görüntüler (aşağıdaki resme bakın).

2. **Erişim iste** bağlantısına tıklayın.

   Böylece, yönetici için bir mesaj içeren bir pencere açılır. Bu mesajda engellenen cihaz hakkındaki bilgiler yer alır.

3. **Gönder**'e tıklayın.



Aygıt Denetimi bildirimi

Ardından, Kaspersky Security Center konsolundaki yönetici, *Yöneticiye aygıta erişimin engellenmesine yönelik mesaj* etkinliği alır. Olay, kullanıcı adını, bilgisayar adını, kullanıcının erişim sağlamaya çalıştığı cihazın ayrıntılarını ve diğer bilgileri içerir. Yöneticinin bu tür olaylar hakkında nasıl bilgilendirileceğini yapılandırabilir ve örneğin e-posta bildirimlerini seçebilirsiniz. Kaspersky Security Center konsolunda, kullanıcılardan gelen mesajların kolay takibi için önceden ayarlanmış bir olay seçimi *Kullanıcı istekleri* yer alır.

Erişime izin vermek için cihazı güvenilir listesine eklemeniz gerekir. Bilgisayarda Kaspersky Endpoint Security ayarlarını güncelledikten sonra kullanıcı cihaza erişim sağlayabilir.

Erişim vermek için çevrimdışı mod

Çevrimdışı modda engellenen bir hizmete erişim verme, ancak Kaspersky Security Center kuruluşta dağıtıldıysa ve bilgisayara bir ilke uygulandıysa yapılabilir. İlke ayarlarında **Aygıt Denetimi** bölümünde yer alan **Geçici erişim isteğine izin ver** onay kutusu seçilmelidir.

Bir kullanıcı, engellenmiş bir aygıta erişmeyi şu şekilde ister:

1. Aygıtı bilgisayara bağlayın.

   Kaspersky Endpoint Security, aygıta erişimin engellendiğini belirten bir bildirim görüntüler (aşağıdaki resme bakın).

2. **Geçici erişim iste** bağlantısına tıklayın.

   Bu, bağlı cihazların listesini içeren bir pencere açar.

3. Bağlanan aygıtlar listesinden erişim elde etmek istediğiniz aygıtı seçin.

4. **İstek erişim dosyası oluştur**'a tıklayın.

5. **Erişim süresi** alanında aygıta erişmek istediğiniz süreyi belirtin.

6. Dosyayı bilgisayar belleğine kaydedin.

Böylece bilgisayar belleğine *.akey uzantısına sahip bir istek erişim dosyası indirilir. Aygıt istek erişim dosyasını kurumsal LAN yöneticisine göndermek için kullanılabilir yöntemlerden birini seçin.



Aygıt Denetimi bildirimi

Yönetici tarafından Yönetim Konsolu'nda (MMC) engellenen cihaz için bir erişim anahtarı oluşturma

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, **Cihazlar** sekmesini seçin.

4. İstemci bilgisayarların listesinde, kullanıcısına engellenen cihaza geçici erişim verilmesi gereken bilgisayarı seçin.

5. Bilgisayarın bağlam menüsünde **Çevrimdışı modda erişim ver** öğesini seçin.

6. Bu işlem bir pencere açar; bu pencerede **Cihaz Denetimi** sekmesini seçin.

7. **Gözat** düğmesine tıklayın ve kullanıcıdan alınan istek erişim dosyasını indirin.

   Kullanıcının erişim istediği engellenmiş aygıt hakkında bilgileri göreceksiniz.

8. Gerekirse, **Erişim süresi** ayarının değerini değiştirin.

   Erişim süresi ayarı varsayılan olarak istek erişim dosyası oluşturulurken kullanıcı tarafından belirtilen değeri alır.

9. **Şu tarihe kadar etkinleştir** ayarını belirtin.

   Bu ayar, sağlanan erişim anahtarını kullanarak kullanıcının engellenen aygıta erişimi etkinleştirebileceği süreyi tanımlar.

10. Erişim anahtarı dosyasını bilgisayar belleğine kaydedin.

Yönetici tarafından Web Console ve Cloud Console'da engellenen cihaz için erişim anahtarı oluşturma

1. Web Console'un ana penceresinde **Varlık yönetimi → Varlıklar (Cihazlar)** seçimini yapın.

2. İstemci bilgisayarların listesinde, kullanıcısına engellenen cihaza geçici erişim verilmesi gereken bilgisayarı seçin.

3. Bilgisayar listesinin üzerindeki üç nokta düğmesine (...) tıklayın ve ardından **Cihaza çevrimdışı modda erişim izni ver** düğmesine tıklayın.

4. Açılan pencerede, **Aygıt Denetimi** bölümünü seçin.

5. **Genel Bakış** düğmesine tıklayın ve kullanıcıdan alınan erişim isteği dosyasını indirin.

   Kullanıcının erişim istediği engellenmiş aygıt hakkında bilgileri göreceksiniz.

6. Gerekirse, **Erişim süresi (saat)** ayarının değerini değiştirin.

   Erişim süresi (saat) ayarı varsayılan olarak istek erişim dosyası oluşturulurken kullanıcı tarafından belirtilen değeri alır.

7. Erişim anahtarının cihazda etkinleştirilebileceği süreyi belirtin.

   Bu ayar, sağlanan erişim anahtarını kullanarak kullanıcının engellenen aygıta erişimi etkinleştirebileceği süreyi tanımlar.

8. Erişim anahtarı dosyasını bilgisayar belleğine kaydedin.

Sonuç olarak, engellenen cihaz erişim anahtarı bilgisayar belleğine indirilir. Bir erişim anahtarı dosyası *.acode uzantısını taşır. Engellenen aygıt erişim anahtarını kullanıcıya göndermek için kullanılabilir yöntemlerden birini seçin.

Kullanıcı, erişim anahtarını şu şekilde etkinleştirir:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.

3. **Erişim isteği** bloğunda, **Aygıta erişim iste** düğmesini tıklayın.

4. Açılan pencerede **Erişim anahtarını etkinleştir** düğmesine tıklayın.

5. Açılan pencerede, kurumsal LAN yöneticisinden alınan aygıt erişim anahtarı dosyasını seçin.

   Erişim sağlama hakkında bilgiler içeren bir pencere açılır.

6. **Tamam**'a tıklayın.

Sonuç olarak kullanıcı, yönetici tarafından ayarlanan bir süre boyunca aygıta erişim kazanır. Kullanıcı, aygıta erişim için tüm hakları elde eder (okuma ve yazma). Anahtarın süresi dolduğunda aygıta erişim tekrar engellenir. Kullanıcının aygıta kalıcı bir erişime ihtiyacı varsa aygıtı güvenilir listesine ekleyin.

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. Kaspersky uzmanları, kullanıcıya cihaza erişimin neden engellendiğini açıklayan bir mesaj şablonu sunar (aşağıdaki şekle bakın).

Mesaj şablonlarını yönetmek için özel değişkenler sağlanır (örneğin, %USER_NAME%). Değişkenler, tek bir mesaj şablonunun farklı bilgisayarlar için kullanılmasına olanak tanır. Bir mesaj oluştururken, Kaspersky Endpoint Security değişkenin değerini işletim sistemi ayarlarından alır ve belirli bilgisayar, kullanıcı ve olayla eşleşen mesaja ekler.



Aygıt Denetimi bildirimi

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. Bunu yapmak için, kullanıcı **Erişim iste** veya **Geçici erişim iste** düğmelerine tıklamalı ve yöneticiye durumu açıklayan bir mesaj göndermelidir. Ayrıca yöneticiye gönderilecek mesajın bir şablonunu hazırlayabilir ve cihaza erişime izin verme veya erişimi engelleme kararınızı etkileyebilecek verileri ekleyebilirsiniz. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yöneticiye aygıta erişimin engellenmesine yönelik mesaj**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

Yönetim Konsolu'nda (MMC) Aygıt Denetimi mesaj şablonlarını değiştirme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi** seçimini yapın.
4. **Mesaj şablonu ayarları** bloğunda, **Şablonlar** düğmesine tıklayın.
5. Bir pencere açılır; bu pencerede Uygulama Denetimi şablonlarını yapılandırın:

   - **Engelleme hakkında mesaj**. Bir kullanıcı engellenen bir cihaza erişmeyi denediğinde görüntülenen mesajın şablonu. Bu mesaj aynı zamanda bir kullanıcı bu kullanıcı için engellenmiş olan cihaz içeriğinde bir işlem gerçekleştirmeyi denediğinde de görüntülenir.
   - **Yöneticiye mesaj**. Kullanıcı cihaza erişimin yanlışlıkla engellendiğine veya cihaz içeriği ile ilgili bir işlemin yanlışlıkla yasaklandığına inandığında LAN yöneticisine gönderilecek mesaj için bir şablon.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken**'e tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılan şablon metnini de geri yükleyebilirsiniz.
6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Aygıt Denetimi mesaj şablonlarını değiştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Aygıt Denetimi**'ne gidin.
5. **Mesaj şablonları** bloğunda, Uygulama Denetimi mesajları için şablonları yapılandırın:

   - **Kullanıcıya mesaj**. Bir kullanıcı engellenen bir cihaza erişmeyi denediğinde görüntülenen mesajın şablonu. Bu mesaj aynı zamanda bir kullanıcı bu kullanıcı için engellenmiş olan cihaz içeriğinde bir işlem gerçekleştirmeyi denediğinde de görüntülenir.
   - **Yöneticiye mesaj**. Kullanıcı cihaza erişimin yanlışlıkla engellendiğine veya cihaz içeriği ile ilgili bir işlemin yanlışlıkla yasaklandığına inandığında LAN yöneticisine gönderilecek mesaj için bir şablon.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılan şablon metnini de geri yükleyebilirsiniz.
6. Değişikliklerinizi kaydedin.

Uygulama arayüzünde Aygıt Denetimi mesaj şablonlarını değiştirme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. **Mesaj şablonları** bloğunda, Uygulama Denetimi mesajları için şablonları yapılandırın:

   - **Engelleme hakkında mesaj**. Bir kullanıcı engellenen bir cihaza erişmeyi denediğinde görüntülenen mesajın şablonu. Bu mesaj aynı zamanda bir kullanıcı bu kullanıcı için engellenmiş olan cihaz içeriğinde bir işlem gerçekleştirmeyi denediğinde de görüntülenir.
   - **Yöneticiye mesaj**. Kullanıcı cihaza erişimin yanlışlıkla engellendiğine veya cihaz içeriği ile ilgili bir işlemin yanlışlıkla yasaklandığına inandığında LAN yöneticisine gönderilecek mesaj için bir şablon.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılan şablon metnini de geri yükleyebilirsiniz.
4. Değişikliklerinizi kaydedin.

Köprüleme Önleme

Köprüleme Önleme, bir bilgisayar için aynı anda birden fazla ağ bağlantısının kurulmasını engelleyerek ağ köprülerinin oluşturulmasını önler. Bu, bir kurumsal ağı korunmasız, yetkisiz ağlar üzerinden gelen saldırılara karşı korumanızı sağlar.

Köprüleme Önleme, *bağlantı kuralları* kullanılarak kurulan ağ bağlantılarını düzenler.

Bağlantı kuralları aşağıdaki ön tanımlı aygıt türleri için oluşturulur:

- Ağ bağdaştırıcıları;
- Wi-Fi bağdaştırıcıları;
- Modemler.

Bağlantı kuralı etkinse Kaspersky Endpoint Security:

- Kuralda belirtilen aygıt türü her iki bağlantı için de kullanılıyorsa yeni bir bağlantı kurarken etkin bağlantıyı engeller;
- Düşük öncelikli kuralların kullanıldığı aygıt türlerini kullanarak kurulan bağlantıları engeller.

Köprüleme Önlemeyi Etkinleştir

Köprüleme Önleme, varsayılan olarak devre dışıdır.

Köprüleme Önlemeyi etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Köprüleme Önleme** düğmesine tıklayın.
4. Bu özelliği etkinleştirmek veya devre dışı bırakmak için **Köprüleme Önlemeyi Etkinleştir** geçiş düğmesini kullanın.
5. Değişikliklerinizi kaydedin.

Köprüleme Önleme etkinleştirildikten sonra Kaspersky Endpoint Security bağlantı kurallarına göre önceden kurulmuş bağlantıları engeller.

Bağlantı kuralının durumunu değiştirme

Bağlantı kuralının durumunu değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Köprüleme Önleme** düğmesine tıklayın.
4. **Aygıt kuralları** bloğunda, durumunu değiştirmek istediğiniz kuralı seçin.
5. Kuralı etkinleştirmek veya devre dışı bırakmak için **Denetim** sütunundaki geçiş düğmesini kullanın.
6. Değişikliklerinizi kaydedin.

Bağlantı kuralının önceliğini değiştirme

Bağlantı kuralının önceliğini değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Erişim ayarları** bloğunda, **Köprüleme Önleme** düğmesine tıklayın.
4. **Aygıt kuralları** bloğunda, önceliğini değiştirmek istediğiniz kuralı seçin.
5. Bağlantı kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.

   Kurallar tablosunun üst sıralarındaki bir kural, daha yüksek önceliğe sahiptir. Köprüleme Önleme en yüksek öncelikli kuralın kullanıldığı aygıt türüyle kurulan bir bağlantı dışında tüm bağlantıları engeller.
6. Değişikliklerinizi kaydedin.

Uyarlamalı Anomali Denetimi

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

Uyarlamalı Anomali Denetimi bileşeni, şirketin ağındaki bilgisayarlarda tipik olarak görülmeyen eylemleri izler ve engeller. Uyarlamalı Anomali Denetimi, tipik olmayan davranışı izlemek için kurallar dizisi kullanır (örneğin, *Microsoft PowerShell'in Office uygulamasından başlatılması* kuralı). Kurallar, Kaspersky uzmanları tarafından zararlı etkinliğin tipik senaryolarına dayanarak oluşturulur. Uyarlamalı Anomali Denetiminin her bir kuralı nasıl ele aldığını yapılandırabilirsiniz (örneğin, belirli iş akışı görevlerini otomatikleştiren PowerShell komut dizilerinin yürütülmesine izin vermek). Kaspersky Endpoint Security, uygulama veritabanlarıyla birlikte kurallar dizisini de günceller. Kurallar dizisinde yapılan güncellemeler elle onaylanmalıdır.

Uyarlamalı Anomali Denetimi ayarları

Uyarlamalı Anomali Denetimini yapılandırma işlemi şu adımlardan oluşur:

1. Uyarlamalı Anomali Denetimi eğitimi.

   Uyarlamalı Anomali Denetimini etkinleştirmenizin ardından kurallar *eğitim modunda* çalışır. Eğitim sırasında Uyarlamalı Anomali Denetimi, kural tetiklemeyi izler ve tetikleme etkinliklerini Kaspersky Security Center'a gönderir. Her kuralın kendi eğitim modu süresi vardır. Eğitim modunun süresi Kaspersky uzmanları tarafından belirlenir. Normalde eğitim modu iki hafta boyunca etkindir.

   Bir kural eğitim boyunca hiç tetiklenmezse Uyarlamalı Anomali Denetimi bu kuralla ilgili eylemleri tipik değil olarak ele alır. Kaspersky Endpoint Security bu kuralla ilgili tüm eylemleri engeller.

   Eğitim sırasında bir kural tetiklendiyse Kaspersky Endpoint Security, etkinlikleri kural tetikleme raporunda ve **Akıllı Eğitim durumundaki kural tetikleyicileri** veri havuzunda günlüğe kaydeder.

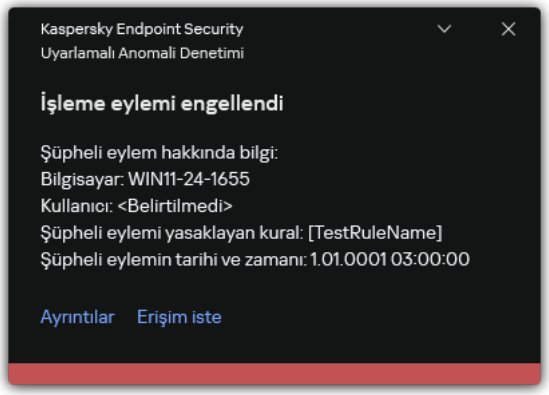
2. Kural tetikleme raporunu analiz etme.

   Yönetici, kural tetikleme raporunu veya **Akıllı Eğitim durumundaki kural tetikleyicileri** veri havuzunun içeriğini analiz eder. Ardından yönetici, kural tetiklendiğinde Uyarlamalı Anomali Denetiminin davranışını seçebilir: engelleme veya izin verme. Yönetici ayrıca kuralın nasıl çalıştığını izlemeye devam edebilir ve eğitim modunun süresini uzatabilir. Yönetici hiçbir eylemde bulunmazsa uygulama da eğitim modunda çalışmaya devam eder. Eğitim modu süresi yeniden başlatılır.

Uyarlamalı Anomali Denetimi aşağıdaki kanallar aracılığıyla gerçek zamanlı olarak yapılandırılır:

- Uyarlamalı Anomali Denetimi, eğitim modunda hiç tetiklenmeyen kurallarla ilgili eylemleri otomatik olarak engellemeye başlar.
- Kaspersky Endpoint Security yeni kurallar ekler veya kullanılmayan kuralları kaldırır.
- Yönetici, kural tetikleme raporunu ve **Akıllı Eğitim durumundaki kural tetikleyicileri** veri havuzunun içeriğini gözden geçirdikten sonra Uyarlamalı Anomali Denetiminin çalışmasını yapılandırır. Kuralların tetiklenmesiyle ilgili raporu ve **Akıllı Eğitim durumundaki kural tetikleyicileri** deposunun içeriğini kontrol etmenizi öneririz.

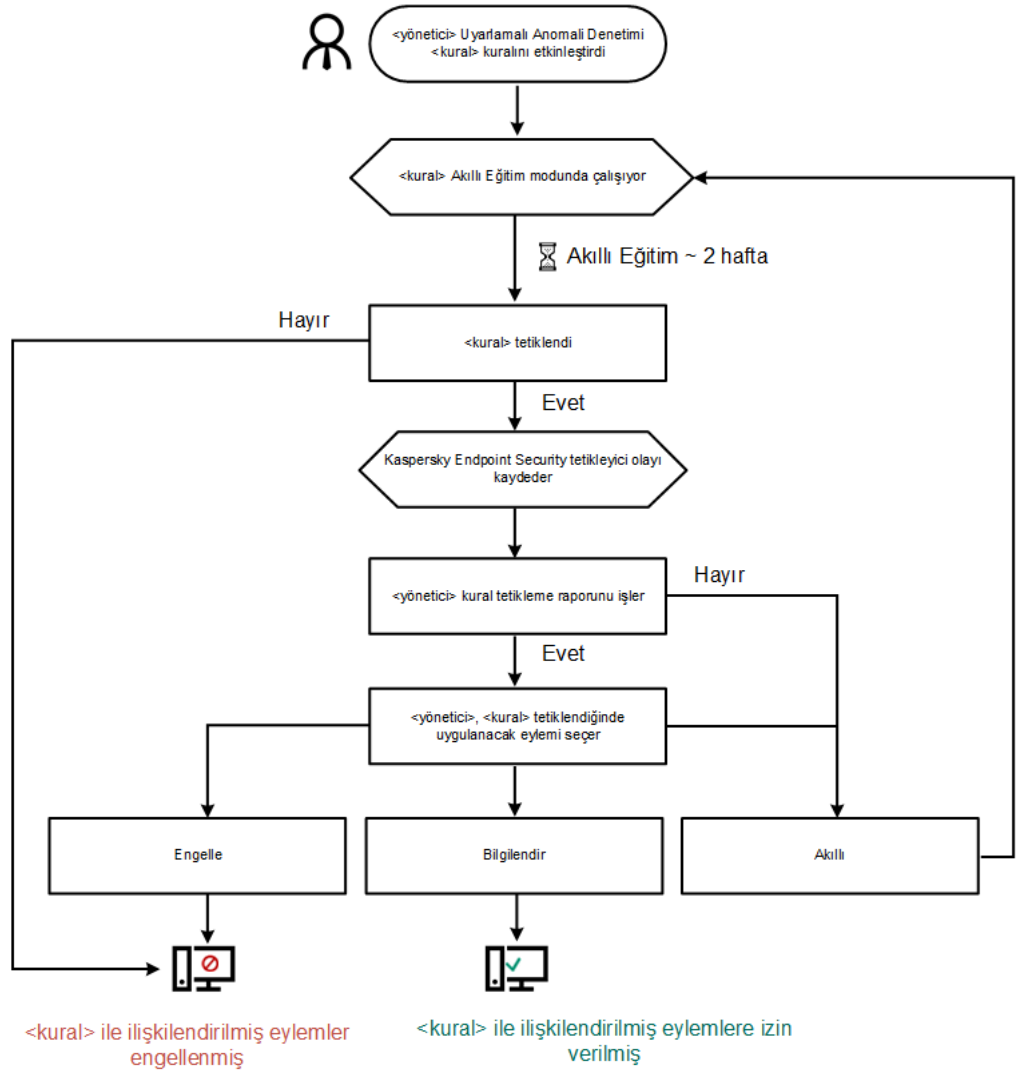
Zararlı bir uygulama eylemde bulunmaya çalıştığında Kaspersky Endpoint Security, eylemi engeller ve bir bildirim gösterir (aşağıdaki resme bakın).



Uyarlamalı Anomali Denetimi bildirimi

Uyarlamalı Anomali Denetimi çalışma algoritması

Kaspersky Endpoint Security, bir kuralla ilgili eyleme izin verilip verilmeyeceğini aşağıdaki algoritmaya (aşağıdaki resme bakın) göre belirler.



Uyarlamalı Anomali Denetimi çalışma algoritması

Uyarlamalı Anomali Denetimi eğitimi

Uyarlamalı Anomali Denetimi bir dizi kural (davranış kalıpları) içerir. Uyarlamalı Anomali Denetimini etkinleştirmenizin ardından kurallar *eğitim modunda* çalışır. Eğitim sırasında Uyarlamalı Anomali Denetimi, kural tetiklemeyi izler ve tetikleme etkinliklerini Kaspersky Security Center'a gönderir. Uyarlamalı Anomali Denetimi bilgisayardaki uygulama etkinliğini engellemez, sadece yöneticiyi bilgilendirir. Bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde gerçekleştirilecek eylemi manuel olarak da seçebilirsiniz.

Yönetim Konsolu'nda (MMC) Uyarlamalı Anomali Denetimi kurallarının listesini görüntüleme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

4. İlke penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.

5. **Uyarlamalı Anomali Denetimi** onay kutusunu seçin.

6. **Uyarlamalı Anomali Denetimi kural ayarları** bölümündeki kural listesine bakın.

   Varsayılan olarak, tüm kurallar **Akıllı** modda çalışır.

7. Gerekirse, Uyarlamalı Anomali Denetimi kuralının güncellemesini onaylayın.

8. Gerekirse, bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde bir eylem seçin:

   - **Engelle**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliği engeller ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.

   - **Bilgilendir**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliğe izin verir ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.

9. Gerekirse, kullanmak istemediğiniz kuralları devre dışı bırakın.

10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Uyarlamalı Anomali Denetimi kurallarını görüntüleme

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ne gidin.

5. **Uyarlamalı Anomali Denetimi ETKİN** düğmesini açık konumuna getirin.

6. **Kurallar** bölümünde, kurallar listesine bakın.

   Varsayılan olarak, tüm kurallar **Akıllı** modda çalışır.

7. Gerekirse, Uyarlamalı Anomali Denetimi kuralının güncellemesini onaylayın.

8. Gerekirse, bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde bir eylem seçin:

   - **Engelle**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliği engeller ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.

   - **Bilgilendir**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliğe izin verir ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.

9. Gerekirse, kullanmak istemediğiniz kuralları devre dışı bırakın.

10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Uyarlanabilir Anomali Denetimi kurallarının listesini görüntüleme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.
3. **Uyarlamalı Anomali Denetimi** düğmesini açık konumuna getirin.
4. **Kurallar** bloğunda, **Kuralları düzenle** bağlantısına tıklayın.
   Uyarlamalı Anomali Denetimi kuralı listesi açılır. Varsayılan olarak, tüm kurallar **Akıllı** modda çalışır.
5. Gerekirse, Uyarlamalı Anomali Denetimi kuralının güncellemesini onaylayın.
6. Gerekirse, bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde bir eylem seçin:
   - **Engelle**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliği engeller ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.
   - **Bilgilendir**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliğe izin verir ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.
7. Gerekirse, kullanmak istemediğiniz kuralları devre dışı bırakın.
8. Değişikliklerinizi kaydedin.

Her kuralın kendi eğitim modu süresi vardır. Eğitim modunun süresi Kaspersky uzmanları tarafından belirlenir. Normalde eğitim modu iki hafta boyunca etkindir.

Eğitim sırasında bir kural hiç tetiklenmezse, Uyarlamalı Anomali Denetimi bu davranışı atipik olarak değerlendirir ve kuralın durumunu **Akıllı engelleme** olarak değiştirir. Daha sonra, uygulama bu kuralla eşleşen tüm etkinlikleri engeller.

Eğitim sırasında bir kural tetiklenirse, uygulamanın bu kuralla eşleşen algılanan etkinliğe uygulayacağı eylemi manuel olarak yapılandırmanız gerekir. Kural tetiklendiğinde gerçekleştirilecek eylemi seçmezseniz, Uyarlamalı Anomali Denetimi eğitim modunda devam eder.

Bir Uyarlamalı Anomali Denetimi kuralını etkinleştirme ve devre dışı bırakma

Bir Uyarlamalı Anomali Denetimi kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.
3. **Kurallar** bloğunda, **Kuralları düzenle** düğmesini tıklayın.
   Uyarlamalı Anomali Denetimi kuralı listesi açılır.
4. Tabloda bir dizi kural seçin (örneğin, *Ofis uygulamalarının faaliyeti*) ve seti genişletin.
5. Bir kural seçin (örneğin, *Windows PowerShell'i ofis uygulamalarından başlat*).

6. Uyarlamalı Anomali Denetimi kuralını etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş anahtarını kullanın.

7. Değişikliklerinizi kaydedin.

Bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde gerçekleştirilecek eylemi değiştirme

Bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde gerçekleştirilecek eylemi düzenlemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.

3. **Kurallar** bloğunda, **Kuralları düzenle** düğmesini tıklayın.

   Uyarlamalı Anomali Denetimi kuralı listesi açılır.

4. Tablodan bir kural seçin.

5. **Düzenle**'ye tıklayın.

   Uyarlamalı Anomali Denetimi kuralı özellikleri penceresi açılır.

6. **Eylem** listesinde, aşağıdaki seçeneklerden birini seçin:

   - **Akıllı**. Bu seçenek seçildiğinde, Uyarlamalı Anomali Denetimi kuralı, Kaspersky uzmanlarının belirlediği bir süre boyunca Akıllı eğitim durumunda çalışır. Bu modda, bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde Kaspersky Endpoint Security, kuralın kapsadığı etkinliğe izin verir ve Kaspersky Security Center Yönetim Sunucusunun **Akıllı Eğitim durumundaki kural tetikleyicileri** depolama alanına bir girdi kaydeder. Akıllı Eğitim durumunda çalışmak için belirlenen süre sona erdiğinde Kaspersky Endpoint Security, bir Uyarlamalı Anomali Denetimi kuralının kapsadığı etkinliği engeller ve etkinlikle ilgili bilgileri içeren bir girişi günlüğe kaydeder.

   - **Engelle**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliği engeller ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.

   - **Bilgilendir**. Bu eylem seçildiğinde, bir Uyarlamalı Anomali Denetimi kuralının tetiklenmesi durumunda Kaspersky Endpoint Security, kuralın kapsadığı etkinliğe izin verir ve etkinlikle ilgili bilgileri içeren bir girdiyi günlüğe ekler.

7. Değişikliklerinizi kaydedin.

Bir Uyarlamalı Anomali Denetimi kuralına yönelik istisna oluşturma

Uyarlamalı Anomali Denetimi kuralları için en fazla 1000 istisna oluşturabilirsiniz. 200 istisnadan fazlasının oluşturulması önerilmez. Kullanılan istisna sayısını azaltmak için istisnalar ayarlarında maske kullanılması önerilir.

Uyarlamalı Anomali Denetimi kuralının bir istisnası, kaynak ve hedef nesnelerin açıklamasını içerir. *Kaynak nesne*, eylemleri gerçekleştiren nesnedir. *Hedef nesne*, üzerinde eylem gerçekleştirilen nesnedir. Örneğin, `file.xlsx` adlı bir dosya açtığınızı varsayalım. Bunun sonucunda bilgisayar belleğine DLL uzantılı bir kitaplık dosyası yüklenir. Bu kitaplık bir tarayıcı tarafından kullanılır (`browser.exe` adlı yürütülebilir dosya). Bu örnekte `file.xlsx` kaynak nesne, Excel kaynak işlem, `browser.exe` hedef dosya ve Tarayıcı da hedef işlemdir.

Bir Uyarlamalı Anomali Denetimi kuralına yönelik istisna oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.
3. **Kurallar** bloğunda, **Kuralları düzenle** düğmesini tıklayın.

   Uyarlamalı Anomali Denetimi kuralı listesi açılır.
4. Tablodan bir kural seçin.
5. **Düzenle**'ye tıklayın.

   Uyarlamalı Anomali Denetimi kuralı özellikleri penceresi açılır.
6. **İstisnalar** bloğunda **Ekle** düğmesine tıklayın.

   İstisna özellikleri penceresi açılır.
7. Bir istisna yapılandırmak istediğiniz kullanıcıyı seçin.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

   > Uyarlamalı Anomali Denetimi, kullanıcı grupları için istisnaları desteklemez. Bir kullanıcı grubu seçerseniz, Kaspersky Endpoint Security istisnayı uygulamaz.
8. **Açıklama** alanında istisnaya yönelik bir açıklama girin.
9. Kaynak nesne veya nesne tarafından başlatılan kaynak işlemin ayarlarını tanımlayın:

   - **Kaynak işlem**. Dosya veya dosyaları içeren klasör yolu ya da dosya veya dosyaları içeren klasör yolunun maskesi (örneğin `C:\Dir\File.exe` veya `Dir\*.exe`).
   - **Kaynak işlem karması**. Dosyanın SHA256 karması.
   - **Kaynak nesne**. Dosya veya dosyaları içeren klasör yolu ya da dosya veya dosyaları içeren klasör yolunun maskesi (örneğin `C:\Dir\File.exe` veya `Dir\*.exe`). Örneğin, hedef işlemleri başlatmak için bir kod veya makro kullanan `document.docm` dosya yolu.

     İnternet adresi, makro, komut satırındaki komut, kayıt defteri yolu ve benzeri gibi hariç tutulacak diğer nesneleri de belirtebilirsiniz. Nesneyi aşağıdaki şablona göre belirtin: `object://<object>`; burada `<object>`, nesnenin adıdır, örneğin `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Ayrıca `object://*C:\Windows\temp\*` gibi maskeler de kullanabilirsiniz.
   - **Kaynak nesne karması**. Dosyanın SHA256 karması.

   Uyarlamalı Anomali Denetimi kuralı, nesne tarafından gerçekleştirilen eylemlere veya nesne tarafından başlatılmış işlemlere uygulanmaz.

10. Hedef nesnenin veya nesne üzerinde başlatılmış hedef işlemlerin ayarlarını belirtin.

    - **Hedef işlem**. Dosya veya dosyaları içeren klasör yolu ya da dosya veya dosyaları içeren klasör yolunun maskesi (örneğin `C:\Dir\File.exe` veya `Dir\*.exe`).
    - **Hedef işlem karması**. Dosyanın SHA256 karması.
    - **Hedef nesne**. Hedef işlemi başlatma komutu. `object://<command>` aşağıdaki düzeni kullanarak komutu belirtin, ör. `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Ayrıca `object://*C:\Windows\temp\*` gibi maskeler de kullanabilirsiniz.
    - **Hedef nesne karması**. Dosyanın SHA256 karması.

    Uyarlamalı Anomali Denetimi kuralı, nesne üzerinde yapılan eylemlere veya nesne üzerinde başlatılmış işlemlere uygulanmaz.

11. Değişikliklerinizi kaydedin.

Uyarlamalı Anomali Denetimi kuralları için istisnaları içe ve dışa aktarma

Seçili kurallar için istisnalar listesini dışa veya içe aktarmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uyarlamalı Anomali Denetimi**'ni seçin.
3. **Kurallar** bloğunda, **Kuralları düzenle** düğmesini tıklayın.

   Uyarlamalı Anomali Denetimi kuralı listesi açılır.
4. Kurallar listesini dışa aktarmak için:
   a. Önceliklerini dışa aktarmak istediğiniz kuralı seçin.
   b. **Dışa aktar**'a tıklayın.
   c. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Yalnızca seçili istisnaları veya tüm istisnalar listesini dışa aktarmak istediğinizi onaylayın.
   e. Dosyaya kaydet.
5. İstisnalar listesini içe aktarmak için:
   a. **İçe aktar**'a tıklayın.
   b. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

c. Dosyayı aç.

Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

6. Değişikliklerinizi kaydedin.

Uyarlamalı Anomali Denetimi kurallarına yönelik güncellemeleri uygulama

Antivirüs veritabanları güncellendiğinde yeni Uyarlamalı Anomali Denetimi kuralları kurallar tablosuna eklenebilir ve mevcut Uyarlamalı Anomali Denetimi kuralları kurallar tablosundan silinebilir. Kaspersky Endpoint Security, söz konusu kurallara ilişkin bir güncelleme uygulanmadıysa tablodan silinecek veya tabloya eklenecek Uyarlamalı Anomali Denetimi kurallarını belirler.

Kaspersky Endpoint Security, güncelleme uygulanana kadar güncelleme tarafından silinecek şekilde ayarlanmış Uyarlamalı Anomali Denetimi kurallarını kurallar tablosunda görüntüler ve bu kurallara *Devre dışı* durumunu atar. Bu kuralların ayarlarını değiştirmek mümkün değildir.

Uyarlamalı Anomali Denetimi kurallarına yönelik güncellemeleri uygulamak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.
3. **Kurallar** bloğunda, **Kuralları düzenle** düğmesini tıklayın.

   Uyarlamalı Anomali Denetimi kuralı listesi açılır.
4. Açılan pencerede **Güncellemeleri onayla** düğmesine tıklayın.

   Güncellemeleri onayla düğmesi, Uyarlamalı Anomali Denetimi kurallarına yönelik bir güncelleme mevcutsa kullanılabilir.
5. Değişikliklerinizi kaydedin.

Uyarlamalı Anomali Denetimi mesaj şablonlarını düzenleme

Kullanıcı, Uyarlamalı Anomali Denetimi kuralları tarafından engellenen bir eylemi gerçekleştirmeyi denediğinde Kaspersky Endpoint Security, potansiyel olarak zararlı eylemlerin engellendiğini belirten bir mesaj görüntüler. Kullanıcı, eylemin başlatılmasının yanlışlıkla engellendiğini düşünüyorsa mesaj metnindeki bağlantıyı kullanarak yerel kurumsal ağ yöneticisi için bir mesaj gönderebilir.

Yöneticiye potansiyel olarak zararlı eylemlerin engellenmesi hakkında mesajlar için özel şablonlar mevcuttur. Mesaj şablonlarını yönetmek için özel değişkenler sağlanır (örneğin, `%USER_NAME%`). Değişkenler, tek bir mesaj şablonunun farklı bilgisayarlar için kullanılmasına olanak tanır. Bir mesaj oluştururken, Kaspersky Endpoint Security değişkenin değerini işletim sistemi ayarlarından alır ve belirli bilgisayar, kullanıcı ve olayla eşleşen mesaja ekler.

Bir mesaj şablonunu düzenlemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.
3. **Şablonlar** bloğunda, Uyarlamalı Anomali Denetimi mesajları için şablonları yapılandırın:
   - **Engelleme hakkında mesaj**. Tipik olmayan bir eylemi engelleyen bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde kullanıcıya gösterilecek mesajın şablonu.
   - **Yöneticiye mesaj**. Kullanıcı, engelleme işleminin bir hata olduğunu düşünüyorsa yerel kurumsal ağ yöneticisine gönderebileceği mesaj şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için uygulama etkinliği engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Sıfırla düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.
4. Değişikliklerinizi kaydedin.

Uyarlamalı Anomali Denetimi işlemlerinin izlenmesi

Uyarlamalı Anomali Denetimi çeşitli izleme araçları içerir. Uyarlamalı Anomali Denetimi izlemenin temel amacı, eğitim sırasında bileşeni yapılandırmaktır.

Uyarlamalı Anomali Denetimi raporları

Uyarlamalı Anomali Denetimi aşağıdaki raporları kullanır:

- **Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor**. Rapor, Uyarlamalı Anomali Denetimi kurallarının durumu hakkında bilgi içerir (*Kapalı*, *Akıllı Eğitim*, *Akıllı Engelleme*, *Bildir*, *Engelle*). Bu rapor, Uyarlamalı Anomali Denetiminin eğitim seviyesinin analiz edilmesine ve *Akıllı Eğitim* modundan normal çalışma moduna (örneğin, *Akıllı Engelleme*) geçen kuralların sayısının değerlendirilmesine olanak tanır.
- **Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor**. Rapor, kural tetikleyicileri hakkında bilgi içerir. Rapor ayrıca kural tetikleme modunu da gösterir: *Engelle* (*Akıllı Engelleme* dahil) veya *Bildir*. Bu raporlar, kullanıcı bilgisayarlarındaki Uyarlamalı Anomali Denetimi etkinliğinin değerlendirilmesini sağlar.

Yönetim Konsolu'nda (MMC) Uyarlamalı Anomali Denetimi raporlarını görüntüleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri → Uyarlamalı Anomali Denetimi**'ni seçin.

4. Aşağıdakilerden birini yapın:

   - Uyarlamalı Anomali Denetimi kuralları durumu hakkındaki raporu görüntülemek istiyorsanız **Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor** bağlantısına tıklayın.

   - Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkındaki raporu görüntülemek istiyorsanız **Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor** bağlantısına tıklayın.

5. Rapor üretme işlemi başlar.

   Rapor yeni bir pencerede görüntülenir.

Web Console'da Uyarlamalı Anomali Denetimi raporlarını görüntüleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Uyarlamalı Anomali Denetimi**'ne gidin.

5. **Kurallar** bloğunda aşağıdakilerden birini yapın:

   - Uyarlamalı Anomali Denetimi kurallarının durumu hakkında raporu görüntülemek istiyorsanız, **Raporu görüntüle** → **Kuralların durumu** seçeneğini seçin.

   - Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında raporu görüntülemek istiyorsanız, **Raporu görüntüle** → **Algılamalar** seçeneğine tıklayın.

6. Rapor üretme işlemi başlar.

   Rapor yeni bir pencerede görüntülenir.

Kaspersky Security Center konsolunda raporlar oluşturmak için Yönetim Sunucusu'na veri aktarımını etkinleştirmeniz gerekir. Veri aktarımı varsayılan olarak etkindir.

Yönetim Konsolu'nda (MMC) Uyarlamalı Anomali Denetimi için veri aktarımı nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.

4. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Ayarlar** düğmesine tıklayın.

5. Aşağıdaki kutuları işaretleyin:

   - **Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor**.

   - **Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor**.

6. Değişikliklerinizi kaydedin.

Web Console'da Uyarlamalı Anomali Denetimi için veri aktarımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.
5. **Yönetim Sunucusu'na veri aktarımı** altında aşağıdaki onay kutularını seçin:
   - **Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor**.
   - **Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor**.
6. Değişikliklerinizi kaydedin.

Akıllı Eğitim durumundaki kural tetikleyicileri depolama

Eğitim modunda, Uyarlamalı Anomali Denetimi tetiklenen kurallar hakkındaki bilgileri ayrı bir depolama alanına gönderir, **Akıllı Eğitim durumundaki kural tetikleyicileri**. Tetiklenen kurallar hakkındaki bilgiler depoda bir olay listesi olarak temsil edilir. Uyarlamalı Anomali Denetimi'ni ayarlamak için, bilgisayardaki atipik davranışı onaylayabilir veya kurala bir istisna ekleyebilirsiniz.

Uyarlamalı Anomali Denetimi olayları

Uyarlamalı Anomali Denetimi, *Engelle* (*Akıllı Engelleme* dahil) ve *Bildirim* modlarında kural tetikleme olaylarını günlüğe kaydeder. Aşağıdaki etkinlikler bu amaç için sağlanmıştır:

İşleme eylemi engellendi

İşleme eylemi atlandı

Olaylar, dosya sağlama toplamları, ilgili kullanıcılar, kural tetikleme zamanı ve bilgisayar adı dahil olmak üzere şüpheli etkinlik hakkında bilgiler içerir. Olayı analiz ettikten sonra, etkinliğin meşru olduğunu tespit ederseniz hemen kurala istisnalar ekleyebilirsiniz.

Uygulama Denetimi

Uygulama Denetimi, kullanıcıların bilgisayarlarındaki uygulamaların başlatılmasını yönetir. Böylece uygulamalar kullanılırken bir kurumsal güvenlik ilkesi uygulamak mümkün olur. Uygulama Denetimi ayrıca uygulamalara erişimi kısıtlayarak bilgisayara virüs bulaşma riskini azaltır.

Uygulama Denetimi yapılandırması şu adımlardan oluşur:

1. Uygulama kategorileri oluşturma.

   Yönetici tarafından yönetilmek istenen uygulama kategorileri oluşturur. Uygulama kategorileri, yönetim gruplarından bağımsız olarak kurumsal ağdaki tüm bilgisayarlar içindir. Bir kategori oluşturmak için şu kriterleri kullanabilirsiniz: KL kategorisi (örneğin, *Tarayıcılar* veya başka bir kategori), dosya karması, uygulama satıcısı ve diğer kriterler.

2. Uygulama Denetimi kuralları oluşturma.

   Yönetici, yönetim grubu için ilkede Uygulama Denetimi kuralları oluşturur. Kural uygulama kategorilerini ve şu kategorilerdeki uygulamaların başlatma durumlarını içerir: engellenen veya izin verilen. Yönetici birçok kural oluşturabilir. Bir uygulama birden fazla kuralın kriterleriyle eşleşebilir. Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Kaspersky Endpoint Security, bir uygulamanın her başlatıldığında bir kuralla eşleşip eşleşmediğini kontrol eder. Kaspersky Endpoint Security, uygulamayı tüm Uygulama Denetimi kurallarıyla sıralı olarak eşleştirir.

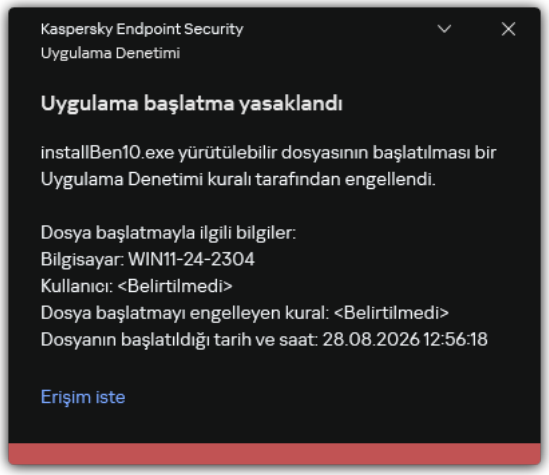
3. Uygulama Denetimi modunu seçme.

   Yönetici, şu kuralların herhangi birine dahil olmayan uygulamalarla çalışmak için mod seçimi yapar (uygulama reddedilenler ve izin verilenler listesi).

Bir kullanıcı yasaklanmış bir uygulamayı başlatmayı denediğinde, Kaspersky Endpoint Security uygulamanın başlatılmasını engeller ve bir bildirim görüntüler (aşağıdaki resme bakın).

Uygulama Denetimi yapılandırmasının kontrolü için bir *test modu* sunulur. Bu modda, Kaspersky Endpoint Security şunları yapar:

- Yasaklanmış olanlar da dahil olmak üzere uygulamaların başlatılmasına izin verir.
- Yasaklanmış bir uygulamanın başlatılması hakkında bir bildirim gösterir ve bilgileri kullanıcının bilgisayarındaki rapora ekler.
- Yasaklanan uygulamaların başlatılması hakkındaki bilgileri Kaspersky Security Center'a gönderir.



Uygulama Denetimi bildirimi

Uygulama Denetimi işletim modları

Uygulama Denetimi bileşeni iki modda çalışır:

- **Reddedilenler listesi**. Bu modda Uygulama Denetimi, Uygulama Denetimi kurallarında yasaklanan uygulamalar hariç olmak üzere tüm uygulamaların kullanıcılar tarafından başlatılmasına izin verir.

  Uygulama Denetimi'nin bu modu varsayılan olarak etkindir.

- **İzin verilenler listesi**. Bu modda Uygulama Denetimi, kullanıcıların Uygulama Denetimi izin ver kurallarında izin verilen ve yasaklanmamış uygulamalar haricinde herhangi bir uygulamayı başlatmasını engeller.

  Uygulama Denetimi izin ver kuralları tamamen yapılandırılırsa bileşen, işletim sisteminin ve kullanıcıların çalışmalarında güvendiği güvenilir uygulamaların çalışmasına izin verirken, LAN yöneticisi tarafından doğrulanmamış tüm yeni uygulamaların başlatılmasını engeller.

  Uygulama denetimi kurallarını izin verilenler listesi modunda yapılandırma hakkında öneriler'i okuyabilirsiniz.

Uygulama Denetimi, Kaspersky Endpoint Security yerel arabirimi ve Kaspersky Security Center kullanılarak 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.

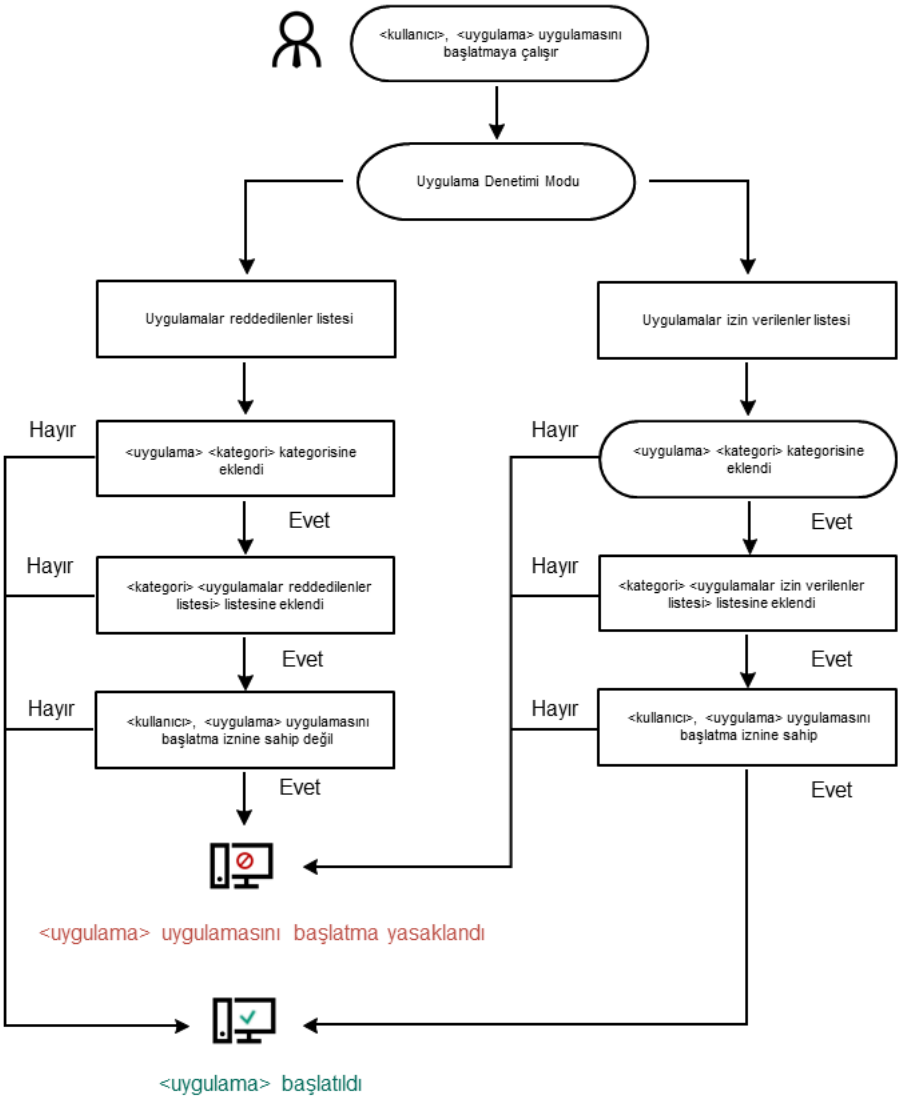
  Kaspersky Security Center Yönetim Konsolunda oluşturulan Uygulama Denetimi kuralları, Kaspersky Endpoint Security yerel arabiriminde olduğu gibi dahil etme ve hariç tutma koşullarına değil, özel uygulama kategorilerine dayanır.

- Kurumsal LAN bilgisayarlarına yüklenen uygulamalar hakkında bilgi toplama.

Uygulama Denetimi bileşeninin çalışmasını yapılandırmak için Kaspersky Security Center'ı kullanmanın önerilmesinin nedeni budur.

Uygulama Denetimi işlem algoritması

Kaspersky Endpoint Security, bir uygulamanın başlatılması hakkında karar vermek için bir algoritma kullanır (aşağıdaki resme bakın).



Uygulama Denetimi işlem algoritması

Uygulama Denetimi işlevselliği sınırlamaları

Uygulama Denetimi bileşeninin çalışması aşağıdaki durumlarda sınırlandırılır:

- Uygulama sürümü yükseltildiğinde, Uygulama Denetimi bileşen ayarlarını içe aktarma desteklenmez.
- KSN sunucuları ile bağlantı yoksa Kaspersky Endpoint Security uygulamaların ve modüllerinin tanınırlığı hakkında bilgileri sadece yerel veritabanlarından alır.

  Kaspersky Endpoint Security'nin **KSN'deki tanınırlığa göre güvenilen Diğer Yazılım\Uygulamalar** KL kategorisi olarak belirlediği uygulamaların listesi, KSN sunucularına bağlantı olup olmamasına bağlı olarak değişebilir.

- 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.

  Yorumlayıcının başlatılmasına Uygulama Denetimi kuralları tarafından izin verilirse bileşen bu yorumlayıcıdan başlayan bir komut dizisini engellemez.

  Yorumlayıcı komut satırında belirtilen komut dizilerinden en az birinin başlatılması, Uygulama denetimi kuralları tarafından engellenirse bileşen, yorumlayıcı komut satırında belirtilen tüm komut dizilerini engeller.

- Bileşen, Kaspersky Endpoint Security tarafından desteklenmeyen yorumlayıcılar tarafından komut dizilerinin başlatılmasını denetlemez.

  Kaspersky Endpoint Security aşağıdaki yorumlayıcıları destekler:

  - Java
  - PowerShell

  Aşağıdaki yorumlayıcı türleri desteklenmektedir:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe
  - %SystemRoot%\system32\wscript.exe

- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Yüklü uygulamalar hakkında bilgi alma

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.

Uygulama bilgilerini görüntüleme

Yüklü uygulamalar hakkındaki bilgiler Kaspersky Security Center Network Agent tarafından sağlanır. Yüklü uygulamalarla ilgili bilgiler **Uygulama kayıt defteri** klasöründeki Kaspersky Security Center konsolunda mevcuttur. Ağ Aracısı, Kaspersky Security Center ile her senkronizasyonda bilgi güncellemesi yapar. Ağ Aracısı tarafından gönderilen bilgilerle ilgili ayrıntılar için lütfen Kaspersky Security Center Yardım bölümüne bakın.

Uygulama kayıt defteri klasöründe bulunan uygulama özellikleri penceresini açmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Uygulama kayıt defteri** seçimini yapın.

3. Bir uygulama seçin.

4. Uygulamanın bağlam menüsünde **Özellikler**'i seçin.

Yürütülebilir dosyalar hakkındaki bilgileri görüntüleme

Yürütülebilir dosyalar hakkındaki bilgileri sorgularken veritabanı üzerindeki yükü azaltabilirsiniz. Bunu yapabilmek için, *Envanter* görevini standart yazılım setinizin yüklü olduğu birkaç referans bilgisayarda çalıştırmanızı öneririz.

Yürütülebilir dosyalar hakkındaki bilgiler Kaspersky Endpoint Security tarafından sağlanır. Donanım bilgilerini almak için yüklü uygulamalara ilişkin bilgilerin iletimini etkinleştiren etkin bir ilke uygulamanız gerekir (bu iletim varsayılan olarak etkindir).

Yönetim Konsolu'nda (MMC) uygulama bilgilerinin gönderilmesini etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.

4. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Ayarlar** düğmesine tıklayın.

5. **Başlatılmış uygulamalar** onay kutusunu seçin.

6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da uygulama bilgilerinin gönderilmesini etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.

5. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Gelişmiş ayarlar** düğmesine tıklayın.

6. Açılan pencerede, **Başlatılmış uygulamalar hakkında** kutucuğunu işaretleyin.

7. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Security'nin *Envanter* görevini kullanarak yürütülebilir dosyaların bir listesini alabilirsiniz. Yürütülebilir dosyaların listesini Kaspersky Security Center konsolunda, **Yürütülebilir dosyalar** klasöründe görüntüleyebilirsiniz.

Envanter görevini çalıştırmadan önce, veritabanının Kaspersky Security Center'ın önerilerini karşıladığından emin olun. Veritabanı sınırlamaları hakkında ayrıntılar için lütfen Kaspersky Security Center Yardım bölümüne bakın.

Yönetim Konsolu'nda (MMC) Envanter görevi nasıl çalıştırılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Envanter** seçimini yapın.

2. Adım. Envanter kapsamı

Kaspersky Endpoint Security'nin yürütülebilir dosyaları aramasını istediğiniz klasörlerin bir listesini oluşturun. Envanter ayarlarını yapılandırın (aşağıdaki tabloya bakın).

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Görevi çalıştıracak hesabı seçme

Envanter görevini çalıştırmak için bir hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır. Envanter kapsamına ağ sürücüleri veya kısıtlı erişime sahip diğer nesneler dahilse, yeterli erişim haklarına sahip bir kullanıcı hesabı seçin.

5. Adım. Bir görev başlatma zamanlaması yapılandırma

Görev zamanlamasını örneğin manuel olarak yapılandırın.

6. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Ana envanter*.

7. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz. Sonuç olarak, yapılandırılan programa uygun olarak kullanıcıların bilgisayarlarında yürütülebilir dosyaların aranması gerçekleştirilir.

Web Console ve Cloud Console'da Envanter görevini çalıştırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.
   Görevler listesi açılır.
2. **Ekle**'ye tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
   b. **Görev türü** açılır listesinden **Envanter** seçimini yapın.
   c. **Görev adı** alanına kısa bir açıklama girin, örneğin, *Ana Envanter*.
   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.
5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Görevi yapılandırmak için görev özelliklerine gidin (aşağıdaki tabloya bakın).

8. Görevin yanındaki onay kutusunu seçin.

9. **Başlat**'a tıklayın.

   Görevin durumunu ve görevin başarıyla veya bir hatayla tamamlandığı aygıtların sayısını izleyebilirsiniz. Sonuç olarak, yürütülebilir dosyalar belirtilen programa uygun olarak kullanıcı bilgisayarlarında aranacaktır.

Yürütülebilir dosyalar klasöründeki bir yürütülebilir dosyanın özellikler penceresini açmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Yürütülebilir dosyalar** seçimini yapın.

3. Yürütülebilir bir dosya seçin.

4. Yürütülebilir dosyanın bağlam menüsünden **Özellikler**'i seçin.

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.

Yüklü uygulamalar ve yürütülebilir dosyalar hakkındaki bilgilerin güncellenmesi

Kaspersky Endpoint Security'de Uygulama Denetimi bileşeninin yürütülebilir dosya veritabanıyla çalışması optimize edilmiştir. Kaspersky Endpoint Security, dosya bilgisayardan silindikten sonra veritabanını otomatik olarak günceller. Bu, veritabanının güncel tutulmasını ve Kaspersky Security Center kaynaklarından tasarruf edilmesini sağlar. Yüklü uygulamaların veritabanını güncel tutmak için, uygulama bilgilerinin Yönetim Sunucusu'na gönderilmesi etkinleştirilmelidir (varsayılan olarak etkindir).

Envanter ayarları

Parametre	Açıklama
Envanter kapsamları	Envanter kapsamını oluşturacak nesnelerin listesi.
DLL modülleri envanteri	Kaspersky Endpoint Security, envanter kapsamındaki DLL modüllerini arar ve bilgileri Kaspersky Security Center'a gönderir. DLL modülleri envanterini etkinleştirmek, Envanter görevini tamamlamak için gereken süreyi ve veritabanının boyutunu önemli ölçüde artırır.
Komut dosyaları envanteri	Kaspersky Endpoint Security, envanter kapsamındaki komut dizilerini arar ve bilgileri Kaspersky Security Center'a gönderir. Komut dosyaları envanterini etkinleştirmek, Envanter görevini tamamlamak için gereken süreyi ve veritabanının boyutunu önemli ölçüde artırır.

Parametre	Açıklama
Sadece bilgisayar boştayken çalıştır	Bilgisayar kaynakları meşgul olduğunda görevin başlatılması ertelenir. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır. Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.
Sadece yeni ve değiştirilmiş dosyaları tara	Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.
Bu süreden daha uzun süreyle taranan dosyayı atla: N sn	Görev yürütme süresini sınırlandırma. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. Görev tamamlandı olarak işaretlenmemiş. Kaspersky Endpoint Security, görevi bir sonraki çalıştırışında, baştan ve zamanlamaya göre çalıştırılacaktır.
Arşivleri tara	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Dağıtım paketlerini tara	Üçüncü taraf uygulamaların dağıtım paketlerinin taranması.
Büyük bileşik dosya paketlerini açma	Bu onay kutusu işaretlendiğinde, uygulama boyutları belirtilen değeri aşan birleşik dosyaları taramaz. Bu onay kutusu işaretlenmediğinde, uygulama her boyuttaki birleşik dosyaları tarar. Uygulama, onay kutusunun seçili olup olmadığından bağımsız olarak arşivlerden çıkarılan büyük dosyaları tarar.

Engellenen uygulamalar modunu etkinleştirme

Engellenen uygulamalar modu, Uygulama Denetiminin, Uygulama Denetimi kurallarında yasaklanan uygulamalar hariç olmak üzere kullanıcıların tüm uygulamaları başlatmasına izin verdiği moddur. Yani, herhangi bir reddetme kuralı yoksa, Uygulama Denetimi uygulamanın başlatılmasına izin verir. Uygulama Denetimi'nin bu modu varsayılan olarak etkindir.

Engellenen uygulamalar modunu etkinleştirmeden önce Uygulama Denetimi kurallarınızı test etmenizi öneririz. Bu amaçla test modunu etkinleştirebilirsiniz.

Yönetim Konsolu'nda (MMC) Engellenen uygulamalar modunu etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi** seçimini yapın.
5. **Uygulama Denetimi** onay kutusunu seçin.
6. **Uygulama Denetimi ayarları** bloğunda, **Reddedilenler listesi** seçimini yapmak için **Denetim modu** açılır listesini kullanın.
7. **Eylem** açılır listesinde Uygulama Denetimi için eylemi seçin:
   - **Kuralı test et**. Uygulama Denetimi, kurallar tarafından çalışması engellenen uygulamaları engellemez, ancak aksi takdirde engellenecek olan uygulamaların çalışmasıyla ilgili olaylar oluşturur.
   - **Kuralları uygula** Uygulama Denetimi engellenen uygulamaları bloke eder ve ilgili olayları oluşturur.

8. Uygulama Denetimi kuralları için durumu seçin:

   - **Açık**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın kullanıldığı anlamına gelir.
   - **Kapalı**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın yok sayıldığı anlamına gelir.
   - **Test**. Bu durum, Kaspersky Endpoint Security'nin kuralın uygulandığı uygulamaların başlatılmasına izin verdiği ancak bu uygulamaların başlatılması hakkında bilgileri günlüğe kaydettiği anlamına gelir.

   Gerekirse, yeni Uygulama Denetimi kuralları ekleyin.

9. Uygulama Denetiminin gelişmiş ayarlarını yapılandırın:

   - **DLL modüllerinin yüklenmesini izle (sistem yükünü önemli ölçüde artırır)**. Onay kutusu işaretlenirse, kullanıcılar uygulamaları başlatmaya çalıştığında Kaspersky Endpoint Security, DLL modüllerinin yüklenmesini denetler. DLL modülü ve DLL modülünü yükleyen uygulama hakkında bilgi, rapora kaydedilir.

     DLL modüllerinin ve sürücülerin yüklenmesine ilişkin denetimi etkinleştirirken, Uygulama Denetimi ayarlarındaki kurallardan varsayılan **Altın İmaj** kuralının ya da "**Altın İmaj\Güvenilir Sertifikalar**" KL kategorisini içeren başka bir kuralın etkinleştirildiğinden ve bu kuralın güvenilir DLL modüllerinin ve sürücülerin Kaspersky Endpoint Security başlatılmadan önce yüklenmesini sağladığından emin olun. **Altın İmaj** kuralı devre dışı bırakıldığında DLL modüllerinin ve sürücülerinin yükleme denetiminin etkinleştirilmesi, işletim sisteminde kararsızlığa neden olabilir.

     Kaspersky Endpoint Security, yalnızca onay kutusu seçildikten sonra yüklenen DLL modüllerini ve sürücüleri izler. Kaspersky Endpoint Security başlatılmadan önce, uygulamanın yüklenenler de dahil olmak üzere tüm DLL modüllerini ve sürücüleri izlemesi için bilgisayarın yeniden başlatılması önerilir.

   - **Sıkı dijital imza doğrulaması kullanın**. Bir Uygulama Denetimi kuralı için tetikleyici koşul olarak bir sertifika seçebilirsiniz. Bu onay kutusu seçilirse Kaspersky Endpoint Security, kuralları yalnızca güvenilir sistem sertifika deposundaki sertifikalarla imzalanmış uygulamalara uygular. Böyle bir sertifika ile imzalanmış uygulamalar, örneğin *Kötü Amaçlı Yazılım Taraması* görevi gibi koruma bileşenleri tarafından da güvenilir olarak kabul edilir. Ancak, bir Uygulama Denetimi kuralında farklı bir depodan sertifika belirtirseniz Kaspersky Endpoint Security böyle bir kuralı uygulamaz.

     Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, kuralları Windows Trusted Root Certificate Store'dan bir sertifika tarafından imzalanmış uygulamalara uygular. Bu tür uygulamalar güvenilir bölgenin bir parçası değildir. Koruma bileşenleri bu tür uygulamaların etkinliğini izler.

   - **Engelleme hakkında mesaj**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir.
   - **Yöneticiye mesaj**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu.

10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Engellenen uygulamalar modunu etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri → Uygulama Denetimi** bölümüne gidin.

5. **Uygulama Denetimi ETKİN** anahtarını açık konuma getirin.

6. **Çalışma modu** bloğunda, **Kurallar listesi hariç tümünü engelle** öğesini seçin.

7. **Eylem** bloğunda, Uygulama Denetimi için eylemi seçin:

   - **Bilgilendir**. Uygulama Denetimi, kurallar tarafından çalışması engellenen uygulamaları engellemez, ancak aksi takdirde engellenecek olan uygulamaların çalışmasıyla ilgili olaylar oluşturur.
   - **Kuralları uygula** Uygulama Denetimi engellenen uygulamaları bloke eder ve ilgili olayları oluşturur.

8. Uygulama Denetimi kuralları için durumu seçin:

   - **Etkin**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın kullanıldığı anlamına gelir.
   - **Devre dışı**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın yok sayıldığı anlamına gelir.
   - **Test modu**. Bu durum, Kaspersky Endpoint Security'nin kuralın uygulandığı uygulamaların başlatılmasına izin verdiği ancak bu uygulamaların başlatılması hakkında bilgileri günlüğe kaydettiği anlamına gelir.

   Gerekirse, yeni Uygulama Denetimi kuralları ekleyin.

9. Uygulama Denetiminin gelişmiş ayarlarını yapılandırın:

   - **DLL modüllerinin yüklenmesini izle**. Onay kutusu işaretlenirse, kullanıcılar uygulamaları başlatmaya çalıştığında Kaspersky Endpoint Security, DLL modüllerinin yüklenmesini denetler. DLL modülü ve DLL modülünü yükleyen uygulama hakkında bilgi, rapora kaydedilir.

     DLL modüllerinin ve sürücülerin yüklenmesine ilişkin denetimi etkinleştirirken, Uygulama Denetimi ayarlarındaki kurallardan varsayılan **Altın İmaj** kuralının ya da "**Altın İmaj\Güvenilir Sertifikalar**" KL kategorisini içeren başka bir kuralın etkinleştirildiğinden ve bu kuralın güvenilir DLL modüllerinin ve sürücülerin Kaspersky Endpoint Security başlatılmadan önce yüklenmesini sağladığından emin olun. **Altın İmaj** kuralı devre dışı bırakıldığında DLL modüllerinin ve sürücülerinin yükleme denetiminin etkinleştirilmesi, işletim sisteminde kararsızlığa neden olabilir.

     Kaspersky Endpoint Security, yalnızca onay kutusu seçildikten sonra yüklenen DLL modüllerini ve sürücüleri izler. Kaspersky Endpoint Security başlatılmadan önce, uygulamanın yüklenenler de dahil olmak üzere tüm DLL modüllerini ve sürücüleri izlemesi için bilgisayarın yeniden başlatılması önerilir.

   - **Sıkı dijital imza doğrulaması kullanın**. Bir Uygulama Denetimi kuralı için tetikleyici koşul olarak bir sertifika seçebilirsiniz. Bu onay kutusu seçilirse Kaspersky Endpoint Security, kuralları yalnızca güvenilir sistem sertifika deposundaki sertifikalarla imzalanmış uygulamalara uygular. Böyle bir sertifika ile imzalanmış uygulamalar, örneğin *Kötü Amaçlı Yazılım Taraması* görevi gibi koruma bileşenleri tarafından da güvenilir olarak kabul edilir. Ancak, bir Uygulama Denetimi kuralında farklı bir depodan sertifika belirtirseniz Kaspersky Endpoint Security böyle bir kuralı uygulamaz.

     Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, kuralları Windows Trusted Root Certificate Store'dan bir sertifika tarafından imzalanmış uygulamalara uygular. Bu tür uygulamalar güvenilir bölgenin bir parçası değildir. Koruma bileşenleri bu tür uygulamaların etkinliğini izler.

- **Kullanıcıya mesaj**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir.

- **Yöneticiye mesaj**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu.

10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Engellenen uygulamalar modunu etkinleştirme

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.

3. **Uygulama Denetimi** düğmesini açık konumuna getirin.

4. **Uygulama Denetimi modu** bloğunda **Reddedilenler listesi seçimini yapın. Kural listesindekiler hariç tüm uygulamalara izin verilir**.

5. **Kurallar tarafından engellenen uygulamaları başlatma eylemi** bloğunda, Uygulama Denetimi içi bir eylem seçin:

   - **Şuradaki olaylar hakkında bilgi ver (Test modu) günlüğe kaydet: raporu**. Uygulama Denetimi, kurallar tarafından çalışması engellenen uygulamaları engellemez, ancak aksi takdirde engellenecek olan uygulamaların çalışmasıyla ilgili olaylar oluşturur.

   - **Engelle**. Uygulama Denetimi engellenen uygulamaları bloke eder ve ilgili olayları oluşturur.

6. Uygulama Denetimi kuralları için durumu seçin:

   - **Etkin**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın kullanıldığı anlamına gelir.

   - **Devre dışı**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın yok sayıldığı anlamına gelir.

   - **Test modu**. Bu durum, Kaspersky Endpoint Security'nin kuralın uygulandığı uygulamaların başlatılmasına izin verdiği ancak bu uygulamaların başlatılması hakkında bilgileri günlüğe kaydettiği anlamına gelir.

   Gerekirse, yeni Uygulama Denetimi kuralları ekleyin.

7. Uygulama Denetiminin gelişmiş ayarlarını yapılandırın:

   - **DLL modüllerinin yüklenmesini izle**. Onay kutusu işaretlenirse, kullanıcılar uygulamaları başlatmaya çalıştığında Kaspersky Endpoint Security, DLL modüllerinin yüklenmesini denetler. DLL modülü ve DLL modülünü yükleyen uygulama hakkında bilgi, rapora kaydedilir.

     DLL modüllerinin ve sürücülerin yüklenmesine ilişkin denetimi etkinleştirirken, Uygulama Denetimi ayarlarındaki kurallardan varsayılan **Altın İmaj** kuralının ya da "**Altın İmaj\Güvenilir Sertifikalar**" KL kategorisini içeren başka bir kuralın etkinleştirildiğinden ve bu kuralın güvenilir DLL modüllerinin ve sürücülerin Kaspersky Endpoint Security başlatılmadan önce yüklenmesini sağladığından emin olun. **Altın İmaj** kuralı devre dışı bırakıldığında DLL modüllerinin ve sürücülerinin yükleme denetiminin etkinleştirilmesi, işletim sisteminde kararsızlığa neden olabilir.

Kaspersky Endpoint Security, yalnızca onay kutusu seçildikten sonra yüklenen DLL modüllerini ve sürücüleri izler. Kaspersky Endpoint Security başlatılmadan önce, uygulamanın yüklenenler de dahil olmak üzere tüm DLL modüllerini ve sürücüleri izlemesi için bilgisayarın yeniden başlatılması önerilir.

- **Sıkı dijital imza doğrulaması kullanın**. Bir Uygulama Denetimi kuralı için tetikleyici koşul olarak bir sertifika seçebilirsiniz. Bu onay kutusu seçilirse Kaspersky Endpoint Security, kuralları yalnızca güvenilir sistem sertifika deposundaki sertifikalarla imzalanmış uygulamalara uygular. Böyle bir sertifika ile imzalanmış uygulamalar, örneğin *Kötü Amaçlı Yazılım Taraması* görevi gibi koruma bileşenleri tarafından da güvenilir olarak kabul edilir. Ancak, bir Uygulama Denetimi kuralında farklı bir depodan sertifika belirtirseniz Kaspersky Endpoint Security böyle bir kuralı uygulamaz.

  Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, kuralları Windows Trusted Root Certificate Store'dan bir sertifika tarafından imzalanmış uygulamalara uygular. Bu tür uygulamalar güvenilir bölgenin bir parçası değildir. Koruma bileşenleri bu tür uygulamaların etkinliğini izler.

- **Uygulama engelleme hakkında mesaj şablonları**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir.

- **Uygulamanın başlatılması engellendiğinde görüntülenen mesaj metni şablonu**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu.

8. Değişikliklerinizi kaydedin.

Sonuç olarak, Uygulama Denetimi engellenen uygulamaları engeller. Kaspersky Endpoint Security ayrıca *Uygulama başlatma yasaklandı* olayları da oluşturur. Bu olayları, Kaspersky Security Center konsolunda *Yasaklı uygulamalar hakkında rapor* oluşturmak için kullanabilirsiniz. Raporun özetinde, Uygulama Denetimi kuralının tetiklendiği uygulamaların ve bilgisayarların listesini görüntüleyebilirsiniz.

Temel bilgisayara dayalı Uygulama Denetimi

İhtiyacınız olan bir dizi uygulama ile bir görüntü oluşturmak için temel bir bilgisayar kullanabilirsiniz. Daha sonra bu görüntüyü işletim sistemini ve uygulamaları diğer bilgisayarlara dağıtmak için kullanabilirsiniz. Görüntüyü her zaman güncel tutmak mümkün olmayabilir. Uygulama Denetimi, temel bir bilgisayara dayalı olarak izin verilen uygulamaların bir listesini tutmanıza olanak tanır. Uygulama Denetimi, temel bilgisayara hangi uygulamaların yüklendiğini otomatik olarak belirler ve kategoriyi günceller. Bu şekilde, bilgisayarlar izin verilen uygulamaların güncel bir listesini alır.

Uygulama Denetimini bir temel bilgisayarı temel alarak yapılandırmak aşağıdaki adımları içerir:

1. Otomatik olarak güncellenen bir kategori oluşturma. Yeni kategori oluştururken, **Belirli bir klasördeki yürütülebilir dosyaları içeren kategori** kategorisini seçin ve temel bilgisayarınızı seçin.

   Yönetim Konsolu'nda (MMC) otomatik olarak güncellenen bir kategorisi oluşturma

   1. Kaspersky Security Center Yönetim Konsolu'nu açın.

   2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Uygulama kategorileri** seçimini yapın.

   3. Çalışma alanında **Yeni kategori** düğmesine tıklayın.

      Böylece uygulama kategorisi oluşturma sihirbazı başlatılır.

   4. Uygulama kategorisi oluşturma sihirbazının talimatlarını uygulayın.

1. Adım. Kategori türünü seçme

Kategori türü olarak **Seçilen cihazlardaki yürütülebilir dosyaları içeren kategori** seçimini yapın.

2. Adım. Kullanıcı kategorisi adı girme

Bu adımda, uygulama kategorisi için bir ad belirtin.

3. Adım. Ayarlar

> **Seçili aygıtlardan yürütülebilir dosyaları içeren kategori** adlı kategori türünü seçtiyseniz bu adım uygulanabilir.

Bu adımda, **Ekle** düğmesine tıklayın ve yürütülebilir dosyaları Kaspersky Security Center tarafından uygulama kategorisine eklenecek bilgisayarları belirtin. Kaspersky Security Center tarafından **Yürütülebilir dosyalar** klasöründe sunulan belirli bilgisayarlardaki tüm yürütülebilir dosyalar, uygulama kategorisine eklenir.

Bu adımda aşağıdaki ayarları da yapılandırabilirsiniz:

- Karma fonksiyonu hesaplaması için algoritma. Algoritma seçmek için aşağıdaki onay kutularından en az birini işaretlemeniz gerekir:
  - **Bu kategorideki dosyalar için SHA256'yı hesapla (Kaspersky Endpoint Security 10 Service Pack 2 for Windows ve sonraki sürümler tarafından desteklenir)**.
  - **Bu kategorideki dosyalar için MD5 hesapla (Kaspersky Endpoint Security 10 Service Pack 2 for Windows'tan önceki sürümler tarafından desteklenir)**.
- **Verileri Yönetim Sunucusu veri havuzuyla senkronize et** onay kutusu. Kaspersky Security Center'ın uygulama kategorisini düzenli olarak temizlemesini ve **Yürütülebilir dosyalar** klasöründe belirtilen bilgisayarlardan tüm yürütülebilir dosyaları buna eklemesini istiyorsanız bu onay kutusunu işaretleyin.

  Verileri Yönetim Sunucusu veri havuzuyla senkronize et onay kutusunun işareti kaldırılmışsa Kaspersky Security Center bir uygulama kategorisi oluşturulduktan sonra uygulama kategorisinde herhangi bir değişiklik yapmaz.

4. Adım. Filtre

Bu adımda dosyalar için bir filtre yapılandırın.

Uygulama kategorisini oluşturmak için kullanmak istediğiniz dosya türünü belirtebilirsiniz.

- **Tüm dosyalar**. Kategori tüm dosyalarla eşleşecektir. Bu seçenek varsayılan olarak seçilidir.
- **Yalnızca uygulama kategorilerinin dışındaki dosyalar**. Kategori yalnızca uygulama kategorileri dışındaki dosyalarla eşleşecektir.

Uygulama kategorisini oluşturmak için kullanmak istediğiniz dosyaları içeren seçili bilgisayarların klasörlerini belirtebilirsiniz.

- **Tüm klasörler**. Kategori tüm klasörlerle eşleşecektir. Bu seçenek varsayılan olarak seçilidir.
- **Belirtilen klasör**. Kategori yalnızca belirtilen klasörle eşleşecektir. Bu seçeneği tercih etmeniz durumunda bir klasör yolu belirtmeniz gerekir.

5. Adım. Özel kategori oluşturma

Sihirbazı tamamlayın.

Web Console ve Cloud Console'da otomatik olarak eklenen içeriğe sahip bir kategori oluşturma

1. Web Console ana penceresinden **İşlemler → Üçüncü taraf uygulamaları → Uygulama kategorileri** seçimini yapın.

   Bu, uygulama kategorileri listesini açar.

2. **Ekle**'ye tıklayın.

   Böylece uygulama kategorisi oluşturma sihirbazı başlatılır.

3. Uygulama kategorisinin genel ayarlarını yapılandırın:

   - Kategori adı.
   - Kategori oluşturma yöntemi. Kategori türü olarak **Seçilen cihazlardaki yürütülebilir dosyaları içeren kategori** seçimini yapın.

   Bir sonraki adıma geçin.

4. Uygulama kategorisinin gelişmiş ayarlarını yapılandırın:

   - Kaspersky Security Center'ın yürütülebilir dosyaları uygulama kategorisine ekleyeceği bilgisayarları belirtin. Kaspersky Security Center tarafından **Yürütülebilir dosyalar** klasöründe sunulan belirli bilgisayarlardaki tüm yürütülebilir dosyalar, uygulama kategorisine eklenir.
   - Karma fonksiyonu hesaplaması için bir algoritma seçin.
   - Verileri Yönetim Sunucusu depolama alanıyla senkronize etmek için bir aralık yapılandırın.
   - Dosyalar için bir filtre yapılandırın.

5. Sihirbazı tamamlayın.

Otomatik olarak güncellenen bir kategori oluştururken, dosyaları birden fazla kategoriye ayırmak uygun olabilir. Örneğin, işletim sistemi dosyaları ve Program Files klasöründeki dosyalar. Bunu yapmak için, kategori ayarlarında bir filtre kullanabilir ve klasörleri tek tek seçebilirsiniz.

2. Uygulama Denetimi modunu seçme. Açıkça izin verilmeyen tüm uygulamaların yürütülmesini engellemeniz gerekir. Bunu yapmak için *Engellenen uygulamalar* modunu seçin.

3. Uygulama Denetimi kuralı oluşturma. Kural ayarlarında, temel bilgisayardaki yürütülebilir dosyaların ait olduğu kategoriyi seçin.

Yönetim Konsolu'nda (MMC) bir temel bilgisayara dayalı olarak Uygulama Denetimini yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi** seçimini yapın.
5. **Uygulama Denetimi** onay kutusunu seçin.
6. **Uygulama Denetimi ayarları** bloğunda, **Reddedilenler listesi** seçimini yapmak için **Denetim modu** açılır listesini kullanın.
7. **Eylem** açılır listesinde Uygulama Denetimi için eylemi seçin:
   - **Kuralı test et**. Uygulama Denetimi, kurallar tarafından çalışması engellenen uygulamaları engellemez, ancak aksi takdirde engellenecek olan uygulamaların çalışmasıyla ilgili olaylar oluşturur.
   - **Kuralları uygula** Uygulama Denetimi engellenen uygulamaları bloke eder ve ilgili olayları oluşturur.
8. Uygulama Denetimi kuralları listesinde **Ekle** düğmesine tıklayın.

   Bu, bir Uygulama Denetimi kuralı ekleme sihirbazını başlatır.
9. **Kategori** açılır listesinde, temel bilgisayarı temel alarak otomatik olarak güncellenen bir kategori seçin.
10. Uygulama Denetimi kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.
11. Uygulama Denetimi kuralının gelişmiş ayarlarını yapılandırın:
    - **Diğer kullanıcılar için reddet**. Uygulama, listede yer almayan tüm kullanıcılar için seçilen kategoriye ait uygulamaların başlatılmasını engeller.
    - **Güvenilir Güncelleyiciler**. Kaspersky Endpoint Security, seçilen kategoriye dahil olan uygulamaları, daha sonra çalıştırılmasına izin verilecek diğer yürütülebilir dosyaları oluşturmasına izin verilen güvenilir güncelleyiciler olarak kabul eder.
12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bir temel bilgisayara dayalı olarak Uygulama Denetimini yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Uygulama Denetimi** bölümüne gidin.
5. **Uygulama Denetimi ETKİN** anahtarını açık konuma getirin.
6. **Çalışma modu** bloğunda, **Kurallar listesi hariç tümünü engelle** öğesini seçin.
7. **Eylem** bloğunda, Uygulama Denetimi için eylemi seçin:
   - **Bilgilendir**. Uygulama Denetimi, kurallar tarafından çalışması engellenen uygulamaları engellemez, ancak aksi takdirde engellenecek olan uygulamaların çalışmasıyla ilgili olaylar oluşturur.
   - **Kuralları uygula** Uygulama Denetimi engellenen uygulamaları bloke eder ve ilgili olayları oluşturur.
8. Uygulama Denetimi kuralları listesinde **Ekle** düğmesine tıklayın.

   Bu, bir Uygulama Denetimi kuralı ekleme sihirbazını başlatır.
9. **Kategoriler/Uygulamalar** bölümünden, temel bilgisayarı temel alarak otomatik olarak güncellenen bir kategori seçin.
10. Uygulama Denetimi kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.
11. Uygulama Denetimi kuralının gelişmiş ayarlarını yapılandırın:
    - **Kullanıcılar**. Uygulama, listede yer almayan tüm kullanıcılar için seçilen kategoriye ait uygulamaların başlatılmasını engeller.
    - **Güvenilir Güncelleyiciler**. Kaspersky Endpoint Security, seçilen kategoriye dahil olan uygulamaları, daha sonra çalıştırılmasına izin verilecek diğer yürütülebilir dosyaları oluşturmasına izin verilen güvenilir güncelleyiciler olarak kabul eder.
12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde bir temel bilgisayara dayalı olarak Uygulama Denetimini yapılandırma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. **Uygulama Denetimi** düğmesini açık konumuna getirin.
4. **Uygulama Denetimi modu** bloğunda **Reddedilenler listesi seçimini yapın. Kural listesindekiler hariç tüm uygulamalara izin verilir**.
5. **Kurallar tarafından engellenen uygulamaları başlatma eylemi** bloğunda, Uygulama Denetimi içi bir eylem seçin:
   - **Şuradaki olaylar hakkında bilgi ver (Test modu) günlüğe kaydet: raporu**. Uygulama Denetimi, kurallar tarafından çalışması engellenen uygulamaları engellemez, ancak aksi takdirde engellenecek olan uygulamaların çalışmasıyla ilgili olaylar oluşturur.
   - **Engelle**. Uygulama Denetimi engellenen uygulamaları bloke eder ve ilgili olayları oluşturur.

6. Uygulama Denetimi kuralları listesinde **Ekle** düğmesine tıklayın.

   Bu, bir Uygulama Denetimi kuralı ekleme sihirbazını başlatır.

7. **Kategori** bölümünden, temel bilgisayarı temel alarak otomatik olarak güncellenen bir kategori seçin.

8. Uygulama Denetimi kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı gruplarını seçin.

9. Uygulama Denetimi kuralının gelişmiş ayarlarını yapılandırın:

   - **Diğer kullanıcılar için reddet**. Uygulama, listede yer almayan tüm kullanıcılar için seçilen kategoriye ait uygulamaların başlatılmasını engeller.

   - **Güvenilir Güncelleyiciler**. Kaspersky Endpoint Security, seçilen kategoriye dahil olan uygulamaları, daha sonra çalıştırılmasına izin verilecek diğer yürütülebilir dosyaları oluşturmasına izin verilen güvenilir güncelleyiciler olarak kabul eder.

10. Değişikliklerinizi kaydedin.

Uygulama Denetimi kurallarını yönetme

Kaspersky Endpoint Security, kurallar kullanarak uygulamaların kullanıcılar tarafından başlatılmasını kontrol eder. Uygulama Denetimi kuralı, tetikleme koşullarını ve kural tetiklendiğinde (kullanıcılar tarafından uygulamanın başlatılmasına izin verir veya engeller) Uygulama Denetimi tarafından gerçekleştirilen eylemleri belirtir.

Kural tetikleme koşulları

Bir kural tetikleme koşulu şu korelasyona sahiptir: "koşul türü - koşul kriteri - koşul değeri". Kural tetikleme koşullarına dayalı olarak Kaspersky Endpoint Security, uygulamaya bir kural uygular (veya uygulamaz).

Kurallarda aşağıdaki koşul türleri kullanılır:

- *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 tetikleme koşulu olarak bir sertifika seçtiyseniz, bu sertifikanın bilgisayardaki güvenilir sistem depolamasına eklendiğinden emin olmanız ve uygulamada güvenilir sistem depolaması kullanım ayarlarını kontrol etmeniz gerekir.

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:

- **Etkin**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın kullanıldığı anlamına gelir.
- **Devre dışı**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın yok sayıldığı anlamına gelir.
- **Test modu**. Bu durum, Kaspersky Endpoint Security'nin kuralların uygulandığı uygulamaların başlatılmasına izin verdiği fakat bu uygulamaların başlatılması hakkında bilgileri rapora kaydettiği anlamına gelir.

Uygulama Denetimi kuralı için bir tetikleme koşulu ekleme

Uygulama Denetimi kuralları oluştururken daha fazla kolaylık için uygulama kategorileri oluşturabilirsiniz.

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.

Yönetim Konsolu'nda bir uygulama kategorisi oluşturmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Uygulama kategorileri** seçimini yapın.
3. Çalışma alanında **Yeni kategori** düğmesine tıklayın.
   Kullanıcı kategorisi oluşturma sihirbazı başlar.
4. Yeni kategori oluşturma sihirbazının talimatlarını uygulayın.

1. Adım. Kategori türünü seçme

Bu adımda, aşağıdaki uygulama kategorileri türlerinden birini seçin:

- İçeriğin yer aldığı kategori manuel olarak eklenir. Yürütülebilir dosyaların verileri manuel olarak kategoriye eklenir. Bu kategori türünü seçtiyseniz, *Koşulları uygulamaların kategorilere dahil edilmesi için yapılandırma* adımında ve *Uygulamaların kategorilerden hariç tutulmasıyla ilgili koşulları yapılandırma* adımında, yürütülebilir dosyaların kategoriye dahil edileceği kriterleri tanımlayabileceksiniz.
- Seçili cihazlardaki yürütülebilir dosyaları içeren kategori. Bu yürütülebilir dosyalar otomatik olarak işlenir ve metrikleri kategoriye eklenir. Bu kategori türünü seçtiyseniz, *Ayarlar* adımında yürütülebilir dosyalarının otomatik olarak kategoriye dahil edileceği bir bilgisayar belirtebilirsiniz.
- Belirli bir klasördeki yürütülebilir dosyaları içeren kategori. Belirtilen klasöre kopyalanan uygulamaların yürütülebilir dosyaları otomatik olarak işlenir ve metrikleri kategoriye eklenir. Bu kategori türünü seçtiyseniz, *Veri havuzu klasörü* adımında yürütülebilir dosyaların otomatik olarak kategoriye dahil edileceği bir klasör belirtebileceksiniz.

İçeriği otomatik olarak eklenen bir kategori oluştururken Kaspersky Security Center, şu biçimlerdeki dosyalarda envanter gerçekleştirir: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX ve SCR.

2. Adım. Kullanıcı kategorisi adı girme

Bu adımda, uygulama kategorisi için bir ad belirtin.

3. Adım. Uygulamaları bir kategoriye dahil etme koşullarını yapılandırma

Uygulama Denetimi kurallarına çok sayıda koşul eklendiğinde (örneğin, dosya karmaları), bilgisayar kaynaklarının tüketimi artar. Toplam koşul sayısı 50.000'e ulaştığında performans sorunları ortaya çıkabilir. Performansı optimize etmek için koşul sayısının gözden geçirilmesi ve azaltılması önerilir.

İçeriğin yer aldığı kategori manuel olarak eklendi kategori türünü seçtiyseniz bu adım uygulanabilir.

Bu adımda, uygulamaları kategoriye dahil etmek için **Ekle** açılır listesinde bulunan aşağıdaki koşullardan birini seçin:

- **Yürütülebilir dosyaların listesinden**. İstemci aygıttaki yürütülebilir dosyalar listesinden özel kategoriye uygulamalar ekleyin.
- **Dosya özelliklerinden**. Özel kategoriye uygulamalar ekleme koşulu olarak yürütülebilir dosyaların ayrıntılı verilerini belirtin.
- **Klasördeki dosyalardan meta veriler**. İstemci cihazda yürütülebilir dosyaları içeren bir klasör seçin. Kaspersky Security Center, bu yürütülebilir dosyaların meta verilerini, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **Klasördeki dosyaların sağlama toplamı**. İstemci cihazda yürütülebilir dosyaları içeren bir klasör seçin. Kaspersky Security Center, bu yürütülebilir dosyaların karma kodlarını, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **Klasörden alınan dosyalar için sertifikalar**. İstemci aygıtta sertifikalarla imzalanan yürütülebilir dosyaları içeren bir klasör seçin. Kaspersky Security Center, bu yürütülebilir dosyaların sertifikalarını, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.

  Özellikleri belirtilen **Sertifika parmak izi** parametresine sahip olmayan koşulların kullanılması önerilmez.

- **MSI yükleyici dosyaları meta verisi**. MSI paketini seçin. Kaspersky Security Center, bu MSI paketinde sıkıştırılan yürütülebilir dosyaların meta verisini, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **Uygulamanın MSI yükleyicisindeki dosyalarının sağlama toplamları**. MSI paketini seçin. Kaspersky Security Center, bu MSI paketinde sıkıştırılan yürütülebilir dosyaların karma kodlarını, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **KL kategorisinden**. Özel kategoriye uygulamalar ekleme koşulu olarak bir KL kategorisi belirtin. *KL kategorisi*, ortak tema özelliklerine sahip bir uygulamalar listesidir. Liste, Kaspersky uzmanları tarafından düzenlenir. Örneğin, *Office Uygulamaları* olarak bilinen KL kategorisi, Microsoft Office paketinden uygulamalar, Adobe Acrobat ve diğerlerini kapsar.

  Genişletilmiş güvenilir uygulamalar listesi oluşturmak için tüm KL kategorilerini seçebilirsiniz.
- **Uygulama yolunu belirtin (maske desteklenir)**. İstemci cihazda bir klasör seçin. Kaspersky Security Center, bu klasörden özel kategoriye yürütülebilir dosyalar ekler.
- **Veri havuzundan sertifika seçin**. Yürütülebilir dosyaları, özel kategorisine uygulamalar eklemek üzere bir koşul olarak imzalamak için kullanılan sertifikaları seçin.

  Özellikleri belirtilen **Sertifika parmak izi** parametresine sahip olmayan koşulların kullanılması önerilmez.

  Sertifika deposunu seçebilirsiniz. Varsayılan olarak, Uygulama Denetimi yalnızca güvenilir sistem sertifika deposundan bir sertifika ile imzalanmış uygulamalar için kuralları uygular. Bu, **Sıkı dijital imza doğrulaması kullanın** onay kutusu ile etkinleştirilir.

- **Sürücü türü**. Özel kategoriye uygulamalar eklemenin koşulu olarak depolama aygıtı türünü (tüm sabit sürücüler ve çıkarılabilir sürücüler veya yalnızca çıkarılabilir sürücüler) belirtin.

4. Adım. Uygulamaları bir kategoriden hariç tutma koşullarını yapılandırma

İçeriğin yer aldığı kategori manuel olarak eklendi kategori türünü seçtiyseniz bu adım uygulanabilir.

Bu adımda belirtilen uygulamalar, "Uygulamaları bir kategoriye dahil etme koşullarını yapılandırma" adımında belirtilmiş olsa bile, kategoriden hariç tutulur.

Bu adımda, uygulamaları kategoriye dahil etmek için **Ekle** açılır listesinde bulunan aşağıdaki koşullardan birini seçin:

- **Yürütülebilir dosyaların listesinden**. İstemci aygıttaki yürütülebilir dosyalar listesinden özel kategoriye uygulamalar ekleyin.
- **Dosya özelliklerinden**. Özel kategoriye uygulamalar ekleme koşulu olarak yürütülebilir dosyaların ayrıntılı verilerini belirtin.
- **Klasördeki dosyalardan meta veriler**. İstemci cihazda yürütülebilir dosyaları içeren bir klasör seçin. Kaspersky Security Center, bu yürütülebilir dosyaların meta verilerini, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **Klasördeki dosyaların sağlama toplamı**. İstemci cihazda yürütülebilir dosyaları içeren bir klasör seçin. Kaspersky Security Center, bu yürütülebilir dosyaların karma kodlarını, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **Klasörden alınan dosyalar için sertifikalar**. İstemci aygıtta sertifikalarla imzalanan yürütülebilir dosyaları içeren bir klasör seçin. Kaspersky Security Center, bu yürütülebilir dosyaların sertifikalarını, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **MSI yükleyici dosyaları meta verisi**. MSI paketini seçin. Kaspersky Security Center, bu MSI paketinde sıkıştırılan yürütülebilir dosyaların meta verisini, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **Uygulamanın MSI yükleyicisindeki dosyalarının sağlama toplamları**. MSI paketini seçin. Kaspersky Security Center, bu MSI paketinde sıkıştırılan yürütülebilir dosyaların karma kodlarını, uygulamaları özel kategoriye ekleme koşulu olarak gösterir.
- **KL kategorisinden**. Özel kategoriye uygulamalar ekleme koşulu olarak bir KL kategorisi belirtin. *KL kategorisi*, ortak tema özelliklerine sahip bir uygulamalar listesidir. Liste, Kaspersky uzmanları tarafından düzenlenir. Örneğin, *Office Uygulamaları* olarak bilinen KL kategorisi, Microsoft Office paketinden uygulamalar, Adobe Acrobat ve diğerlerini kapsar.

  Genişletilmiş güvenilir uygulamalar listesi oluşturmak için tüm KL kategorilerini seçebilirsiniz.
- **Uygulama yolunu belirtin (maske desteklenir)**. İstemci cihazda bir klasör seçin. Kaspersky Security Center, bu klasörden özel kategoriye yürütülebilir dosyalar ekler.
- **Veri havuzundan sertifika seçin**. Yürütülebilir dosyaları, özel kategorisine uygulamalar eklemek üzere bir koşul olarak imzalamak için kullanılan sertifikaları seçin.
- **Sürücü türü**. Özel kategoriye uygulamalar eklemenin koşulu olarak depolama aygıtı türünü (tüm sabit sürücüler ve çıkarılabilir sürücüler veya yalnızca çıkarılabilir sürücüler) belirtin.

5. Adım. Ayarlar

Seçili aygıtlardan yürütülebilir dosyaları içeren kategori adlı kategori türünü seçtiyseniz bu adım uygulanabilir.

Bu adımda, **Ekle** düğmesine tıklayın ve yürütülebilir dosyaları Kaspersky Security Center tarafından uygulama kategorisine eklenecek bilgisayarları belirtin. Kaspersky Security Center tarafından **Yürütülebilir dosyalar** klasöründe sunulan belirli bilgisayarlardaki tüm yürütülebilir dosyalar, uygulama kategorisine eklenir.

Bu adımda aşağıdaki ayarları da yapılandırabilirsiniz:

- Karma fonksiyonu hesaplaması için algoritma. Algoritma seçmek için aşağıdaki onay kutularından en az birini işaretlemeniz gerekir:
  - **Bu kategorideki dosyalar için SHA256'yı hesapla (Kaspersky Endpoint Security 10 Service Pack 2 for Windows ve sonraki sürümler tarafından desteklenir)**.
  - **Bu kategorideki dosyalar için MD5 hesapla (Kaspersky Endpoint Security 10 Service Pack 2 for Windows'tan önceki sürümler tarafından desteklenir)**.
- **Verileri Yönetim Sunucusu veri havuzuyla senkronize et** onay kutusu. Kaspersky Security Center'ın uygulama kategorisini düzenli olarak temizlemesini ve **Yürütülebilir dosyalar** klasöründe belirtilen bilgisayarlardan tüm yürütülebilir dosyaları buna eklemesini istiyorsanız bu onay kutusunu işaretleyin.

  Verileri Yönetim Sunucusu veri havuzuyla senkronize et onay kutusunun işareti kaldırılmışsa Kaspersky Security Center bir uygulama kategorisi oluşturulduktan sonra uygulama kategorisinde herhangi bir değişiklik yapmaz.

6. Adım. Veri havuzu klasörü

Seçili klasörden yürütülebilir dosyaları içeren kategori adlı kategori türünü seçtiyseniz bu adım kullanılabilir.

Bu adımda, Kaspersky Security Center'ın uygulamaları uygulama kategorisine otomatik olarak eklemek için yürütülebilir dosyaları arayacağı klasörü belirtin.

Bu adımda aşağıdaki ayarları da yapılandırabilirsiniz:

- **Bu kategoriye dinamik bağlantı kitaplıkları (.DLL) ekle** onay kutusu. Dinamik bağlantı kitaplıklarının (DLL dosyaları) uygulama kategorisine dahil edilmesini istiyorsanız bu onay kutusunu işaretleyin.

  Uygulama kategorisine DLL dosyalarını dahil etmek Kaspersky Security Center'ın performansını azaltabilir.

- **Kod verilerini bu kategoriye dahil et** onay kutusu. Komut dosyalarının uygulama kategorisine dahil edilmesini istiyorsanız bu onay kutusunu işaretleyin.

  Uygulama kategorisine komut dosyalarını dahil etmek Kaspersky Security Center'ın performansını azaltabilir.

- Karma fonksiyonu hesaplaması için algoritma. Algoritma seçmek için aşağıdaki onay kutularından en az birini işaretlemeniz gerekir:

  - **Bu kategorideki dosyalar için SHA256'yı hesapla (Kaspersky Endpoint Security 10 Service Pack 2 for Windows ve sonraki sürümler tarafından desteklenir)**.

  - **Bu kategorideki dosyalar için MD5 hesapla (Kaspersky Endpoint Security 10 Service Pack 2 for Windows'tan önceki sürümler tarafından desteklenir)**.

- **Klasördeki değişikliklerin taranmasını zorla** onay kutusu. Kaspersky Security Center'ın, uygulama kategorisine otomatik olarak eklemek için kullandığı klasördeki yürütülebilir dosyaları düzenli olarak aramasını isterseniz bu onay kutusunu işaretleyin.

  Klasördeki değişikliklerin taranmasını zorla onay kutusunun işareti kaldırılırsa Kaspersky Security Center, yalnızca klasörde değişiklikler yapılmışsa veya dosyalar klasöre eklenmiş ya da silinmişse uygulama kategorisine otomatik olarak ekleme yapmak için kullandığı klasördeki yürütülebilir dosyaları arar.

- **Tarama aralığı (1-168 saat)** alanlar. Bu alanda, Kaspersky Security Center'ın yürütülebilir dosyaları, uygulama kategorisine otomatik olarak ekleme yapmak için kullanılan klasörde arayacağı zaman aralığını (saat cinsinden) belirtebilirsiniz.

  Bu alan, **Klasördeki değişikliklerin taranmasını zorla** onay kutusu işaretlenirse kullanılabilir.

7. Adım. Özel kategori oluşturma

Sihirbazı tamamlayın.

Uygulama arabiriminde bir Uygulama Denetimi kuralına yeni tetikleme koşulu eklemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. **Engellenen uygulamalar** veya **İzin verilen uygulamalar** düğmesine tıklayın.

   Bu, Uygulama Denetimi kurallarının listesini açar.
4. Bir tetikleme koşulu yapılandırmak istediğiniz kuralı seçin.

   Uygulama Denetimi kuralı özellikleri açılır.
5. **Koşullar: N** sekmesini veya **İstisnalar** sekmesini seçin ve **Ekle** düğmesini tıklayın.
6. Uygulama Denetimi kuralı için tetikleme koşullarını seçin:

   - **Başlatılan uygulamaların özelliklerinden koşullar**. Çalışan uygulamalar listesinde, Uygulama Denetimi kuralının uygulanacağı uygulamaları seçebilirsiniz. Kaspersky Endpoint Security ayrıca daha önce bilgisayarda çalışan uygulamaları da listeler. Bir veya daha fazla kural tetikleme koşulu oluşturmak için kullanmak istediğiniz kriteri seçmeniz gerekir: **Dosya karması**, **Sertifika**, **KL kategorisi**, **Meta veriler** veya **Dosya veya klasör yolu**.

   - **Koşullar "KL kategorisi"**. *KL kategorisi*, ortak tema özelliklerine sahip bir uygulamalar listesidir. Liste, Kaspersky uzmanları tarafından düzenlenir. Örneğin, "Office uygulamaları" olarak bilinen KL kategorisi, Microsoft Office paketinden uygulamalar, Adobe® Acrobat® ve diğerlerini kapsar.

   - **Özel koşul**. Uygulama dosyasını seçebilir ve kural tetikleme koşullarından birini seçebilirsiniz: **Dosya karması**, **Sertifika**, **Meta veriler** veya **Dosya veya klasör yolu**.

- **Dosya sürücüsüne göre koşul (çıkarılabilir sürücü)**. Uygulama Denetimi kuralı yalnızca çıkarılabilir bir sürücüde çalıştırılan dosyalara uygulanır.

- **Belirtilen klasördeki dosyaların özelliklerinden koşullar**. Uygulama Denetimi kuralı yalnızca belirtilen klasördeki dosyalara uygulanır. Ayrıca, alt klasörlerdeki dosyaları da dahil edebilir veya hariç tutabilirsiniz. Bir veya daha fazla kural tetikleme koşulu oluşturmak için kullanmak istediğiniz kriteri seçmeniz gerekir: **Dosya karması**, **Sertifika**, **KL kategorisi**, **Meta veriler** veya **Dosya veya klasör yolu**.

7. Değişikliklerinizi kaydedin.

Koşulları eklerken, lütfen Uygulama Denetimi için aşağıdaki özel hususları dikkate alın:

- Kaspersky Endpoint Security, meta verilerde maske girmek için `*` ve `?` karakterlerini destekler: **Dosya adı**, **Uygulama adı**, **Satıcı**.

- 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.

- Kural tetikleme koşulları olarak sadece **Veren** ve **Sertifika konusu** kriterlerinin kullanılması önerilir. Bu kriterlerin kullanımı güvenilir değildir.

- **Dosya veya klasör yolu** alanında sembolik bağlantı kullanıyorsanız Uygulama Denetimi kuralının doğru çalışması için sembolik bağlantıyı çözmeniz önerilir. Bunun için **Sembolik bağlantıyı çöz** düğmesine tıklayın.

Yürütülebilir dosyalar klasöründen uygulama kategorisine yürütülebilir dosyalar ekleme

Yürütülebilir dosyalar klasöründe, bilgisayarlarda tespit edilen yürütülebilir dosyaların listesi görüntülenir. Kaspersky Endpoint Security, Envanter görevini yürüttükten sonra yürütülebilir dosyaların listesini oluşturur.

Yürütülebilir dosyalar klasöründen uygulama kategorisine yürütülebilir dosyalar eklemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Yürütülebilir dosyalar** seçimini yapın.

3. Çalışma alanında, uygulama kategorisine eklemek istediğiniz yürütülebilir dosyaları seçin.

4. Seçili yürütülebilir dosyalara yönelik bağlam menüsünü açmak için sağ tıklayın ve **Kategoriye ekle**'yi seçin.

5. Açılan pencerede şunları yapın:

   - Pencerenin üst kısmında aşağıdaki seçeneklerden birini belirleyin:

     - **Yeni bir uygulama kategorisine ekle**. Yeni bir uygulama kategorisi oluşturmak ve yürütülebilir dosyaları bu kategoriye eklemek istiyorsanız bu seçeneği belirleyin.

     - **Mevcut bir uygulama kategorisine ekle**. Mevcut bir uygulama kategorisi seçmek ve yürütülebilir dosyaları bu kategoriye eklemek istiyorsanız bu seçeneği belirleyin.

- **Kural türü** bloğunda aşağıdakilerden birini seçin:
  - **Dahil edilenlere ekleme kuralları**. Yürütülebilir dosyaları uygulama kategorisine ekleyen bir koşul oluşturmak istiyorsanız bu seçeneği belirleyin.
  - **İstisnalara ekleme kuralları**. Yürütülebilir dosyaları uygulama kategorisinden çıkaran bir koşul oluşturmak istiyorsanız bu seçeneği belirleyin.
- **Bir koşul olarak kullanılan parametre** bloğundan aşağıdaki seçimlerden birini yapın:
  - **Sertifika ayrıntıları (veya bir sertifikası olmayan dosyalar için SHA256 karmaları)**.
  - **Sertifika ayrıntıları (bir sertifikası olmayan dosyalar atlanacak)**.
  - **Yalnızca SHA256 (bir karmaya sahip olmayan dosyalar atlanacak)**.
  - **Yalnızca MD5 (üretilmiyor modu, yalnızca Kaspersky Endpoint Security 10 Service Pack 1 sürümü için)**.

6. Değişikliklerinizi kaydedin.

Olayla ilgili yürütülebilir dosyaları uygulama kategorisine ekleme

Uygulama kategorisine Uygulama Denetimi olaylarıyla ilişkili yürütülebilir dosyalar eklemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Olaylar** sekmesini seçin.
3. Uygulama Denetimi bileşeninin işlemiyle ilgili olayların seçimini (Uygulama Denetimi bileşeni işleminden kaynaklanan olayları görüntüleme, Uygulama Denetimi bileşeninin test işleminden kaynaklanan olayları görüntüleme) **Olay seçimleri** açılır listesinden yapın.
4. **Seçimi çalıştır** düğmesine tıklayın.
5. İlişkili yürütülebilir dosyalarını uygulama kategorisine eklemek istediğiniz olayları seçin.
6. Seçili olaylara yönelik bağlam menüsünü açmak için sağ tıklayın ve **Kategoriye ekle** öğesini seçin.
7. Açılan pencerede uygulama kategorisinin ayarlarını yapılandırın:
   - Pencerenin üst kısmında aşağıdaki seçeneklerden birini belirleyin:
     - **Yeni bir uygulama kategorisine ekle**. Yeni bir uygulama kategorisi oluşturmak ve yürütülebilir dosyaları bu kategoriye eklemek istiyorsanız bu seçeneği belirleyin.
     - **Mevcut bir uygulama kategorisine ekle**. Mevcut bir uygulama kategorisi seçmek ve yürütülebilir dosyaları bu kategoriye eklemek istiyorsanız bu seçeneği belirleyin.

- **Kural türü** bloğunda aşağıdakilerden birini seçin:
  - **Dahil edilenlere ekleme kuralları**. Yürütülebilir dosyaları uygulama kategorisine ekleyen bir koşul oluşturmak istiyorsanız bu seçeneği belirleyin.
  - **İstisnalara ekleme kuralları**. Yürütülebilir dosyaları uygulama kategorisinden çıkaran bir koşul oluşturmak istiyorsanız bu seçeneği belirleyin.
- **Bir koşul olarak kullanılan parametre** bloğundan aşağıdaki seçimlerden birini yapın:
  - **Sertifika ayrıntıları (veya bir sertifikası olmayan dosyalar için SHA-256 karmaları)**.
  - **Sertifika ayrıntıları (bir sertifikası olmayan dosyalar atlanacak)**.
  - **Yalnızca SHA-256 (bir karmaya sahip olmayan dosyalar atlanacak)**.
  - **Yalnızca MD5 (üretilmiyor modu, yalnızca Kaspersky Endpoint Security 10 Service Pack 1 sürümü için)**.

8. Değişikliklerinizi kaydedin.

Uygulama Denetimi kuralı ekleme

Kaspersky Security Center'ı kullanarak Uygulama Denetimi kuralı eklemek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri → Uygulama Denetimi** seçimini yapın.
   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.
4. **Ekle**'ye tıklayın.
   Uygulama Denetimi kuralı penceresi açılır.
5. Aşağıdakilerden birini yapın:
   - Yeni bir kategori oluşturmak istiyorsanız:
     a. **Kategori oluştur**'a tıklayın.
     Kullanıcı kategorisi oluşturma sihirbazı başlar.
     b. Yeni kategori oluşturma sihirbazının talimatlarını uygulayın.
     c. **Kategori** açılır listesinde oluşturulan uygulama kategorisini seçin.
   - Mevcut bir kategoriyi düzenlemek istiyorsanız:
     a. **Kategori** açılır listesinden düzenlemek istediğiniz uygulama kategorisini seçin.
     b. **Özellikler**'e tıklayın.
     c. Seçili uygulama kategorisinin ayarlarını değiştirin.

d. Değişikliklerinizi kaydedin.

e. **Kategori** açılır listesinden kural oluştururken kullanmak istediğiniz oluşturulmuş uygulama kategorisini seçin.

6. **Kullanıcılar ve hakları** tablosunda **Ekle** düğmesine tıklayın.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

7. **Kullanıcılar ve hakları** tablosunda şunları yapın:

   - Kullanıcıların ve/veya kullanıcı gruplarının seçilen kategoriye ait uygulamaları başlatmalarına izin vermek isterseniz ilgili satırların karşısındaki **İzin ver** onay kutusunu işaretleyin.
   - Kullanıcıların ve/veya kullanıcı gruplarının seçilen kategoriye ait uygulamaları başlatmalarını engellemek isterseniz ilgili satırlardaki **Engelle** onay kutusunu işaretleyin.

8. **Kullanıcı veya grup** sütununda görülmeyen ve **Kullanıcı veya grup** sütununda belirtilen kullanıcı grubunun parçası olmayan tüm kullanıcıların seçilen kategorilere ait uygulamaları başlatmasını engellemek isterseniz **Diğer kullanıcılar için reddet** onay kutusunu işaretleyin.

9. Kaspersky Endpoint Security'nin, seçili uygulama kategorisinde bulunan uygulamaları, sonradan çalıştırılma yetkisi olan başka yürütülebilir dosyalar oluşturmasına izin verilen güvenilir güncelleyiciler olarak değerlendirmesini istiyorsanız **Güvenilir Güncelleyiciler** onay kutusunu işaretleyin.

   > Kaspersky Endpoint Security ayarları taşınırken güvenilir güncelleyiciler tarafından oluşturulan yürütülebilir dosyaların listesi de taşınır.

10. Değişikliklerinizi kaydedin.

Uygulama Denetimi kuralı eklemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. **Engellenen uygulamalar** veya **İzin verilen uygulamalar** düğmesine tıklayın.

   Bu, Uygulama Denetimi kurallarının listesini açar.

4. **Ekle**'ye tıklayın.

   Uygulama Denetimi kural ayarları penceresi açılır.

5. **Genel Ayarlar** sekmesinde, kuralın ana ayarlarını tanımlayın:

   a. **Kural adı** alanında, kuralın adını girin veya düzenleyin.

   b. **Açıklama** alanında kurala yönelik bir açıklama girin.

   c. **Kullanıcılar ve hakları** tablosunda **Ekle** düğmesine tıklayın.

      Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.

Kural varsayılan olarak tüm kullanıcılar için geçerlidir.

Tabloda belirtilen kullanıcı yoksa kural kaydedilemez.

d. **Kullanıcılar ve hakları** tablosunda, geçiş düğmesini kullanıcıların uygulamaları başlatma hakkını tanımlamak için kullanın.

e. Uygulamanın, **Kullanıcılar ve hakları** tablosunda listelenmeyen ve **Kullanıcılar ve hakları** tablosunda listelenen kullanıcı gruplarının üyesi olmayan tüm kullanıcılar için kural tetikleme koşullarını karşılayan uygulamaların çalışmasını engellemesini istiyorsanız **Diğer kullanıcılar için reddet** onay kutusunu işaretleyin.

Diğer kullanıcılar için reddet onay kutusu işaretlenmezse Kaspersky Endpoint Security, **Kullanıcılar ve hakları** tablosunda belirtilmeyen ve **Kullanıcılar ve hakları** tablosunda belirtilen kullanıcılar grubuna ait olmayan kullanıcılar tarafından uygulamaların başlatılmasını denetlemez.

f. Kaspersky Endpoint Security'nin kural tetikleme koşullarıyla eşleşen uygulamaları güvenilir güncelleyiciler olarak değerlendirmesini istiyorsanız **Güvenilir Güncelleyiciler** onay kutusunu işaretleyin. *Güvenilir Güncelleyiciler* daha sonra çalışmasına izin verilecek başka yürütülebilir dosyalar oluşturmasına izin verilen uygulamalardır.

Bir uygulama birden çok kuralı tetiklerse Kaspersky Endpoint Security, aşağıdaki koşullar yerine getirildiğinde *Güvenilir Güncelleyiciler* bayrağını ayarlar:

- Tüm kurallar uygulamanın çalışmasına izin verir.
- En az bir kuralda **Güvenilir Güncelleyiciler** onay kutusu seçilidir.

6. **Koşullar: N** sekmesinde, kuralı tetiklemek için dahil etme koşulları listesini oluşturun veya düzenleyin.
7. **İstisnalar: N** sekmesinde, kuralı tetiklemek için istisna koşulları listesini oluşturun veya düzenleyin.

   Kaspersky Endpoint Security ayarları taşınırken güvenilir güncelleyiciler tarafından oluşturulan yürütülebilir dosyaların listesi de taşınır.
8. Değişikliklerinizi kaydedin.

Kaspersky Security Center aracılığıyla Uygulama Denetimi kuralının durumunu değiştirme

Uygulama Denetimi kuralının durumunu Yönetim Konsolu üzerinden değiştirmek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri → Uygulama Denetimi** seçimini yapın.

   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.

4. İçerik menüsünü görüntülemek için **Durum** sütununa sol tıklayın ve aşağıdakilerden birini seçin:

   - **Açık**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın kullanıldığı anlamına gelir.
   - **Kapalı**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın yok sayıldığı anlamına gelir.
   - **Test**. Bu durum, Kaspersky Endpoint Security'nin kuralın uygulandığı uygulamaların başlatılmasına izin verdiği ancak bu uygulamaların başlatılması hakkında bilgileri günlüğe kaydettiği anlamına gelir.

5. Değişikliklerinizi kaydedin.

Uygulama Denetimi kuralının durumunu uygulama arabiriminden değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri → Uygulama Denetimi**'ni seçin.
3. **Engellenen uygulamalar** veya **İzin verilen uygulamalar** düğmesine tıklayın.

   Bu, Uygulama Denetimi kurallarının listesini açar.
4. İçerik menüsünü görüntülemek için **Durum** sütununa sağ tıklayın ve aşağıdakilerden birini seçin:

   - **Etkin**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın kullanıldığı anlamına gelir.
   - **Devre dışı**. Bu durum, Uygulama Denetimi bileşeni çalıştırıldığında kuralın yok sayıldığı anlamına gelir.
   - **Test modu**. Bu durum, Kaspersky Endpoint Security'nin bu kuralın uygulandığı uygulamaların başlatılmasına izin verdiği ancak bu uygulamaların başlatılması hakkında bilgileri günlüğe kaydettiği anlamına gelir.

5. Değişikliklerinizi kaydedin.

Uygulama Denetimi kurallarını dışa ve içe aktarma

Uygulama Denetimi kuralları listesini bir XML dosyasına aktarabilirsiniz. Uygulama Kontrol kuralları listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini kullanabilirsiniz.

Uygulama Denetimi kurallarını dışa ve içe aktarırken, lütfen aşağıdaki özel hususları aklınızda bulundurun:

- Kaspersky Endpoint Security, sadece etkin Uygulama Denetimi modu için kurallar listesini dışa aktarır. Başka bir deyişle, Uygulama Denetimi reddedilenler listesi modunda çalışıyorsa, Kaspersky Endpoint Security sadece bu mod için kuralları dışa aktarır. İzin verilenler listesi modu için kural listesini dışa aktarmak için, modu değiştirmeniz ve dışa aktarma işlemini yeniden çalıştırmanız gerekir.
- Kaspersky Endpoint Security, Uygulama Denetim kurallarının çalışması için uygulama kategorileri kullanır. Uygulama Denetim kuralları listesini farklı bir sunucuya taşırken, uygulama kategorileri listesini de taşımanız gerekir. Uygulama kategorilerini dışa veya içe aktarmayla ilgili daha fazla ayrıntı için lütfen Kaspersky Security Center Yardım içeriğine bakın.

Yönetim Konsolu'nda (MMC) Uygulama Denetimi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi** seçimini yapın.

4. Uygulama Denetimi kuralları listesini dışa aktarmak için:

   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

   Herhangi bir kural seçmezseniz, Kaspersky Endpoint Security tüm istisnaları dışa aktaracaktır.

   b. **Dışa aktar** bağlantısına tıklayın.

   c. Açılan pencerede, kurallar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   d. Dosyaya kaydet.

   Kaspersky Endpoint Security, kurallar listesini XML dosyasına aktarır.

5. Uygulama Denetimi kurallarının listesini içe aktarmak için:

   a. **İçe aktar** bağlantısına tıklayın.

   Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   b. Dosyayı aç.

   Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Uygulama Denetimi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Uygulama Denetimi** bölümüne gidin.

5. **Çalışma modu** altında, bir kural listesi seçin: uygulama reddedenler listesi veya allowlist.

6. Kurallar listesini dışa aktarmak için:

   a. Düzenlemek istediğiniz kuralları seçin.

   b. → **Dışa aktar** düğmesine tıklayın.

   Kaspersky Endpoint Security, kural listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

7. Kurallar listesini içe aktarmak için:

   a. → **İçe aktar** düğmesine tıklayın.

   Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

8. Değişikliklerinizi kaydedin.

Uygulama Denetimi bileşeninin işleminden kaynaklanan olayları görüntüleme

Kaspersky Security Center tarafından alınan Uygulama Denetimi bileşeninin işleminden kaynaklanan olayları görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Olaylar** sekmesini seçin.
3. **Seçim oluştur** düğmesine tıklayın.
4. Açılan pencerede **Olaylar** bölümüne gidin.
5. **Tümünü temizle** düğmesine tıklayın.
6. **Olaylar** tablosunda **Uygulama başlatma yasaklandı** onay kutusunu işaretleyin.
7. Değişikliklerinizi kaydedin.
8. **Olay seçimleri** açılır listesinde oluşturulan seçimi seçin.
9. **Seçimi çalıştır** düğmesine tıklayın.

Engellenen uygulamalar raporunu görüntüleme

Engellenen uygulamalar hakkındaki raporu görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Raporlar** sekmesini seçin.
3. **Yeni rapor şablonu** düğmesine tıklayın.

   Yeni Rapor Şablonu Sihirbazı başlatılır.
4. Rapor Şablonu Sihirbazı talimatlarını uygulayın. **Rapor şablon türünü seçme** adımında **Diğer → Yasaklanmış uygulamalar hakkında rapor** öğesini seçin.

   Yeni Rapor Şablonu Sihirbazı ile işlemi tamamladıktan sonra yeni rapor şablonu **Raporlar** sekmesindeki tabloda görünür.
5. Raporu, üzerine çift tıklayarak açın.

Rapor üretme işlemi başlar. Rapor yeni bir pencerede görüntülenir.

Uygulama Denetimi kurallarını test etme

Uygulama Denetimi kurallarının, çalışması gereken uygulamaları engellemediğinden emin olmak için yeni kurallar oluşturulduktan sonra Uygulama Denetimi kurallarını test etme işleminin etkinleştirilmesi ve işlemlerinin analiz edilmesi önerilir. Uygulama Denetimi kurallarının testi etkin olduğunda Kaspersky Endpoint Security, Uygulama Denetimi tarafından başlatılması yasaklanan uygulamaları engellemez ancak bunun yerine Yönetim Sunucusu'na başlatıldıkları hakkında bildirimler gönderir.

Uygulama Denetimi kurallarının çalışmasının analizi, Kaspersky Security Center'a rapor edilen Uygulama Denetimi olaylarının sonuçlarının gözden geçirilmesini gerektirir. Test modu, bilgisayar kullanıcısının çalışması için gereken tüm uygulamalar için engellenmiş herhangi bir başlatma olayı ile sonuçlanmıyorsa bu, doğru kuralların oluşturulduğu anlamına gelir. Aksi takdirde oluşturduğunuz kuralların ayarlarını güncellemeniz, ek kurallar oluşturmanız veya mevcut kuralları silmeniz önerilir.

Varsayılan olarak, Kaspersky Endpoint Security, kurallar tarafından yasaklananlar hariç olmak üzere tüm uygulamaların başlatılmasına izin verir.

Uygulama Denetimi kuralı testini etkinleştirme ve devre dışı bırakma

Kaspersky Security Center'da Uygulama Denetimi kurallarının testini etkinleştirmek veya devre dışı bırakmak için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi** seçimini yapın.

   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.
4. **Denetim modu** açılır listesinde, aşağıdaki öğelerden birini seçin:

   - **Reddedilenler listesi**. Bu seçenek belirlenirse Uygulama Denetimi engelleme kurallarının koşullarının yerine getirildiği durumlar haricinde, Uygulama Denetimi tüm kullanıcıların herhangi bir uygulamayı başlatmasına izin verir.
   - **İzin verilenler listesi**. Bu seçenek belirlenirse Uygulama Denetimi izin verme kuralları koşullarının yerine getirildiği durumlar haricinde, Uygulama Denetimi tüm kullanıcıların herhangi bir uygulamayı başlatmasını engeller.
5. Aşağıdakilerden birini yapın:

   - Uygulama Denetimi kurallarına yönelik olarak testi etkinleştirmek istiyorsanız **Eylem** açılır listesinde **Kuralı test et** seçeneğini belirleyin.
   - Kullanıcı bilgisayarlarında uygulamalarının başlatılmasını yönetmek için Uygulama Denetimini etkinleştirmek isterseniz açılır listeden **Kuralları uygula**'yı seçin.
6. Değişikliklerinizi kaydedin.

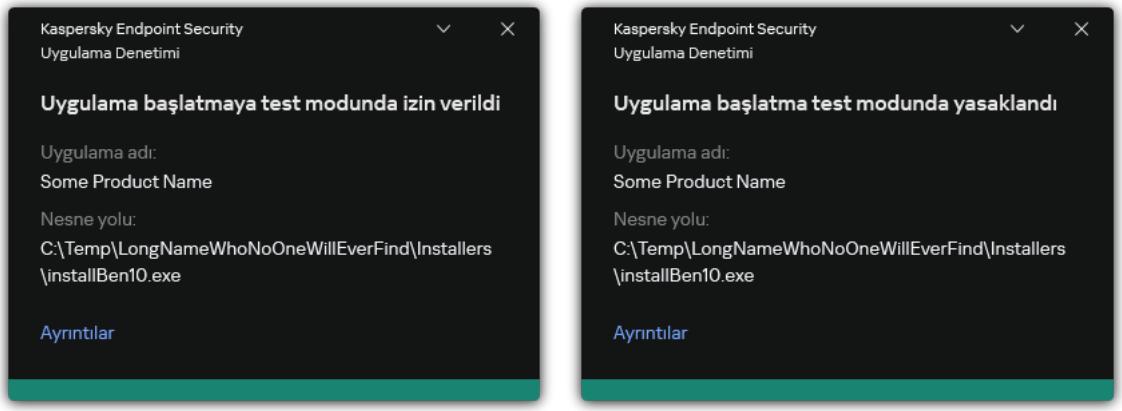
Uygulama Denetimi kurallarının test edilmesini etkinleştirmek veya Uygulama Denetimi için bir engelleme eylemi seçmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. **Engellenen uygulamalar** veya **İzin verilen uygulamalar** düğmesine tıklayın.

   Bu, Uygulama Denetimi kurallarının listesini açar.
4. **Durum** bölümünde **Test modu** seçimini yapın.

   Bu durum, Kaspersky Endpoint Security'nin bu kuralın uygulandığı uygulamaların başlatılmasına izin verdiği ancak bu uygulamaların başlatılması hakkında bilgileri günlüğe kaydettiği anlamına gelir.
5. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Security, Uygulama Denetimi bileşeni tarafından başlatılması yasaklanan uygulamaları engellemez ancak başlatılmalarıyla ilgili Yönetim Sunucusu'na bildirimler gönderir. Ayrıca kullanıcının bilgisayarındaki kural testi hakkındaki bildirimlerin görüntülenmesini yapılandırabilirsiniz (aşağıdaki resme bakın).



Test modunda Uygulama Denetimi bildirimleri

Test modunda engellenen uygulamalar hakkındaki raporu görüntüleme

Test modunda engellenen uygulamalar hakkındaki raporu görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Raporlar** sekmesini seçin.
3. **Yeni rapor şablonu** düğmesine tıklayın.

   Yeni Rapor Şablonu Sihirbazı başlatılır.

4. Rapor Şablonu Sihirbazı talimatlarını uygulayın. **Rapor şablon türünü seçme** adımında **Diğer → Test modunda yasaklanmış uygulamalar hakkında rapor** öğesini seçin.

   Yeni Rapor Şablonu Sihirbazı ile işlemi tamamladıktan sonra yeni rapor şablonu **Raporlar** sekmesindeki tabloda görünür.

5. Raporu, üzerine çift tıklayarak açın.

Rapor üretme işlemi başlar. Rapor yeni bir pencerede görüntülenir.

Uygulama Denetimi bileşeninin test işleminden kaynaklanan olayları görüntüleme

Kaspersky Security Center tarafından alınan Uygulama Denetimi test olaylarını görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Olaylar** sekmesini seçin.
3. **Seçim oluştur** düğmesine tıklayın.
4. Açılan pencerede **Olaylar** bölümüne gidin.
5. **Tümünü temizle** düğmesine tıklayın.
6. **Olaylar** tablosunda **Uygulama başlatma test modunda yasaklandı** ve **Uygulama başlatmaya test modunda izin verildi** onay kutularını işaretleyin.
7. Değişikliklerinizi kaydedin.
8. **Olay seçimleri** açılır listesinde oluşturulan seçimi seçin.
9. **Seçimi çalıştır** düğmesine tıklayın.

Uygulama etkinlik izleyicisi

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

Uygulama Etkinlik İzleyicisi, bir kullanıcının bilgisayarındaki uygulamaların etkinlikleri hakkında gerçek zamanlı bilgi görüntülemek için tasarlanmış bir araçtır.

Uygulama Etkinliği İzleyicisi'nin kullanılması, Uygulama Denetimi ve Sunucu İzinsiz Giriş Önleme bileşenlerinin yüklenmesini gerektirir. Bu bileşenler kurulu değilse, Uygulama Etkinliği İzleyicisi bölümündeki ana uygulama penceresi gizlenir.

Uygulama Etkinlik İzleyicisi'ni başlatmak için:

Ana uygulama penceresinin **İzleniyor** bölümünde, **Uygulama Etkinlik İzleyicisi** kutucuğuna tıklayın.

Bu pencerede, kullanıcının bilgisayarındaki uygulamaların etkinlikleri hakkındaki bilgiler üç sekmede sunulur:

- **Tüm uygulamalar** sekmesinde, bilgisayarda yüklü olan tüm uygulamalar hakkında bilgiler görüntülenir.
- **Çalışıyor** sekmesinde, her bir uygulama tarafından tüketilen bilgisayar kaynakları hakkındaki bilgiler gerçek zamanlı olarak görüntülenir. Bu sekmeden, tek bir uygulama için izinleri yapılandırmaya da devam edebilirsiniz.
- **Açılışta çalıştır** sekmesinde, işletim sistemi başlatıldığında çalıştırılan uygulamalar listelenir.

Kullanıcının bilgisayarındaki uygulama etkinliği bilgilerini gizlemek istiyorsanız, kullanıcının Uygulama Etkinlik İzleyicisi aracına erişimini kısıtlayabilirsiniz.

Yönetim Konsolu (MMC) kullanılarak uygulama arabiriminde Uygulama Etkinlik İzleyicisi nasıl gizlenir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
4. Araca erişim vermek ya da erişimi iptal etmek için **Uygulama Etkinlik İzleyicisi bölümünü gizle** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console kullanılarak uygulama arabiriminde Uygulama Etkinlik İzleyicisi nasıl gizlenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kullanıcı Etkileşimi** bölümüne gidin.
5. Araca erişim vermek ya da erişimi iptal etmek için **Uygulama Etkinlik İzleyicisi bölümünü gizle** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Dosyalar veya klasörler için isim maskeleri oluşturma kuralları

Dosya veya klasör adı maskesi, ortak karakterler kullanılarak bir *klasör adının veya bir dosya adının* ve uzantısının temsilidir.

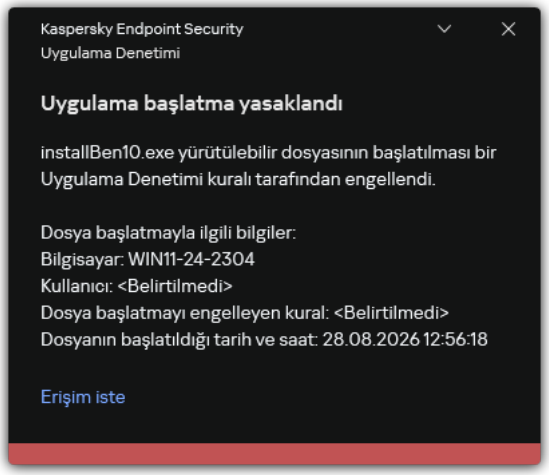
Dosya veya klasör adı maskesi oluşturmak için aşağıdaki ortak karakterleri kullanabilirsiniz:

- `*` (yıldız) karakteri, herhangi bir karakter kümesinin (boş küme dahil) yerine geçer. Örneğin, `C:\*.txt` maskesi, C: sürücüsündeki klasörlerde yer alan `txt` uzantılı tüm klasörleri ve alt klasörleri içerir.

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

Uygulama Denetimi mesaj şablonlarını düzenleme

Kullanıcı, Uygulama Denetimi kuralı tarafından engellenen bir uygulamayı başlatmaya çalıştığında Kaspersky Endpoint Security, uygulamanın başlatılmasının engellendiğini belirten bir mesaj görüntüler. Kaspersky uzmanları, kullanıcıya uygulamanın neden engellendiğini açıklayan bir mesaj şablonu sunar (aşağıdaki şekle bakın). Mesaj şablonlarını yönetmek için özel değişkenler sağlanır (örneğin, `%USER_NAME%`). Değişkenler, tek bir mesaj şablonunun farklı bilgisayarlar için kullanılmasına olanak tanır. Bir mesaj oluştururken, Kaspersky Endpoint Security değişkenin değerini işletim sistemi ayarlarından alır ve belirli bilgisayar, kullanıcı ve olayla eşleşen mesaja ekler.



Uygulama Denetimi bildirimi

Kullanıcı, uygulamanın başlatılmasının yanlışlıkla engellendiğini düşünüyorsa mesaj metnindeki bağlantıyı kullanarak yerel kurumsal ağ yöneticisine bir mesaj gönderebilir. Bunu yapmak için, kullanıcı **Erişim iste** düğmesine tıklamalı ve yöneticiye durumu açıklayan bir mesaj göndermelidir. Ayrıca yöneticiye gönderilecek mesajın bir şablonunu hazırlayabilir ve uygulamaya erişime izin verme veya erişimi engelleme kararınızı etkileyebilecek verileri ekleyebilirsiniz. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için uygulama başlatmasını engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

Yönetim Konsolu'ndaki (MMC) Uygulama Denetimi mesaj şablonunu düzenleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi** seçimini yapın.

4. **Mesaj şablonu ayarları** bloğunda, **Şablonlar** düğmesine tıklayın.

5. Bir pencere açılır; bu pencerede Uygulama Denetimi şablonlarını yapılandırın:

   - **Engelleme hakkında mesaj**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir.

     Test modunda Uygulama Denetimi için mesaj şablonlarını yapılandıramazsınız. Test modunda Uygulama Denetimi, önceden ayarlanmış bildirimleri görüntüler.

   - **Yöneticiye mesaj**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken**'e tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılan olarak düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.

6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Uygulama Denetimi mesaj şablonunu düzenleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Uygulama Denetimi** bölümüne gidin.

5. **Mesaj şablonları** bloğunda, **Uygulama başlatma hakkında mesajlar bloğu** bağlantısına tıklayın ve Uygulama Denetimi mesajları için şablonları yapılandırın:

   - **Kullanıcıya mesaj**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir.

     Test modunda Uygulama Denetimi için mesaj şablonlarını yapılandıramazsınız. Test modunda Uygulama Denetimi, önceden ayarlanmış bildirimleri görüntüler.

   - **Yöneticiye mesaj**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılana sıfırla düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Uygulama Denetimi mesaj şablonunu düzenleme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.

3. **Uygulama engelleme hakkında mesaj şablonları** bloğunda, Uygulama Denetimi mesajları için şablonları yapılandırın:

   - **Engelleme hakkında mesaj**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir.

     Test modunda Uygulama Denetimi için mesaj şablonlarını yapılandıramazsınız. Test modunda Uygulama Denetimi, önceden ayarlanmış bildirimleri görüntüler.

   - **Yöneticiye mesaj**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken ekle**'ye tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Sıfırla düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.

4. Değişikliklerinizi kaydedin.

Uygulama Denetimi ileti şablonlarındaki değişkenler

Kullanıcı mesajı şablonlarında veya yönetici mesajı şablonlarında aşağıdaki değişkenleri kullanabilirsiniz:

- **Tetiklenen kuralın adı** – `%RULE%`.

  Bir dosyanın yürütülmesini engelleyen kuralın adı.

- **Geçerli tarih** – `%DATE%`.

  Dosyanın yürütülmesinin GG.AA.YYYY biçiminde engellendiği tarih.

- **Geçerli saat** – `%TIME%`.

  SS:DD biçiminde dosya yürütmesinin engellendiği zaman.

- **Kullanıcı adı** – `%USER_NAME%`.

  Dosya yürütmesinin engellendiği bilgisayardaki geçerli kullanıcı hesabının adı, `<device name>\<user alias>` formatında (örneğin, `DESKTOP-123\John.Smith`).

- **Bilgisayar adı** – `%COMPUTER_NAME%`.

  Dosya yürütmesinin engellendiği bilgisayarın adı.

- **Yürütülebilir dosya adı** – `%FILE_NAME%`.

  Engellenen uygulamanın yürütülebilir dosyasının adı.

- **Yürütülebilir dosyanın KL kategorisi** – `%KL_CAT%`.

  Engellenen uygulamanın ait olduğu KL kategorisi (örneğin, *Tarayıcılar* veya başka kategori).

- **Yürütülebilir dosya yolu** – `%FILE_PATH%`.

  Engellenen uygulamanın yürütülebilir dosyasının tam yolu.

- **Yürütülebilir dosya sürümü** – `%FILE_VERSION%`.

  Engellenen uygulamanın yürütülebilir dosyasının sürümü.

- **Yürütülebilir dosyanın orijinal adı** – `%ORIGINAL_FILE_NAME%`.

  Engellenen uygulamanın yürütülebilir dosyasının orijinal adı. Dosya adı, uygulamanın yürütülebilir dosyasının özelliklerinde belirtilir.

- **Satıcı** – `%FILE_PUBLISHER%`.

  Engellenen uygulamanın sağlayıcısı.

- **Uygulama adı** – `%FILE_PRODUCT_NAME%`.

  Engellenen uygulamanın adı.

- **Uygulama sürümü** – `%PRODUCT_VERSION%`.

  Engellenen uygulamanın sürümü.

- **Yürütülebilir dosya karması** – `%FILE_HASH%`.

  Engellenen uygulamanın yürütülebilir dosyasının karması.

- **Sertifika veren** – `%CERT_ISSUER%`.

  Yürütülebilir dosyanın imzalandığı sertifikayı veren.

- **Sertifika konusu** – `%CERT_SUBJECT%`.

  Yürütülebilir dosyanın imzalandığı sertifikanın konusu.

- **Sertifika parmak izi** – `%CERT_THUMBPRINT%`.

  Yürütülebilir dosyanın imzalandığı sertifikanın parmak izi.

Yürütülebilir dosyaların envanterini çıkarmaya yönelik en iyi uygulamalar

Envanter görevi; yürütülebilir dosyalar (örneğin EXE, BAT, CMD), DLL modülleri ve komut dosyaları (PowerShell, JS ve diğerleri) hakkında bilgi toplar. Bu bilgiler, Uygulama Denetimi kategorilerini ve Sunucu Yetkisiz Erişim Önleme bileşenine ilişkin uygulama izinlerini yapılandırmak için gereklidir. Bilgileri güncel tutmak için *Envanter* görevi düzenli aralıklarla çalıştırılmalıdır. *Envanter* görevi de *Kötü Amaçlı Yazılım Taraması* görevi gibi yoğun kaynak kullanır. Bu nedenle, görevi geceleri veya hafta sonlarında çalışacak şekilde yapılandırmanızı öneririz.

Yürütülebilir dosya envanteri adımları

1. Standart yazılım grubunuzun yüklü olduğu referans bilgisayar grubunu seçin. Yürütülebilir dosya envanteri işlemi için bilgisayar sayısını asgari düzeyde tutmanızı öneririz. *Envanter* görevi sayısı ne kadar az olursa Kaspersky Security Center Yönetim Sunucusu üzerindeki yük de o kadar düşük olur.

2. Referans bilgisayarları Kaspersky Security Center konsolunda ayrı bir yönetim grubuna taşıyın. Gruba örneğin *Referans bilgisayarlar* adını verebilirsiniz.

3. *Referans bilgisayarlar* yönetim grubu için bir *Envanter* görevi oluşturun. Varsayılan görev ayarlarını korumanızı öneririz.

Bir kuruluştaki yürütülebilir dosya envanteri örneği

Örneğin, kuruluşunuzda Windows 11 25H2 çalıştıran 100 bilgisayar vardır. Tüm bilgisayarlarda işletim sisteminin aynı sürümü ve dil yerelleştirmesi bulunur. Bilgisayarlarda yüklü olan güncelleme kümesi de aynıdır.

Böyle bir kuruluşta *Envanter* görevini tüm bilgisayarlarda çalıştırmanız gerekmez. Bu bilgisayarlardaki yürütülebilir dosyaların çoğu aynıdır. Tek bir referans bilgisayar için görev oluşturmak yeterlidir. Referans yapılandırmadan farklı bir yapılandırmaya sahip bilgisayarlar için ek *Envanter* görevleri oluşturabilirsiniz.

İzin verilen uygulamalar listesini uygulamaya yönelik en iyi uygulamalar

İzin verilen uygulamalar listesinin uygulanmasını planlarken, aşağıdaki işlemlerin gerçekleştirilmesi önerilir:

1. Aşağıdaki grup türlerini oluşturun:
   - Kullanıcı grupları. Çeşitli uygulama kümelerini kullanmalarına izin vermeniz gereken kullanıcı grupları.
   - Yönetim grupları. Kaspersky Security Center'ın izin verilen uygulamaların listesini uygulayacağı bir veya daha fazla bilgisayar grubu. Bu gruplar için farklı izin listesi ayarları kullanılıyorsa, birden çok bilgisayar grubu oluşturmak gerekir.
2. Başlatılmasına izin verilmesi gereken uygulamaların bir listesini oluşturun.

   Liste oluşturmadan önce aşağıdakileri yapmanız önerilir:

   a. Envanter görevini çalıştırın.

      Envanter görevinin oluşturulması, yeniden yapılandırılması ve başlatılması hakkındaki bilgiler Görev yönetimi bölümünde mevcuttur.

   b. Yürütülebilir dosyalar listesini görüntüleyin.

Uygulamalar için izin verilenler listesi modunu yapılandırma

Beyaz liste modunu test ederken aşağıdaki işlemlerin gerçekleştirilmesi önerilir:

1. Başlatılmasına izin verilmesi gereken uygulamaları içeren uygulama kategorileri oluşturun.

Uygulama kategorileri oluşturmak için aşağıdaki yöntemlerden birini seçebilirsiniz:

- **İçeriğin yer aldığı kategori manuel olarak eklendi**. Aşağıdaki koşulları kullanarak bu kategoriye elle ekleme yapabilirsiniz:
  - Dosya meta verisi. Kaspersky Security Center, belirtilen meta verinin yer aldığı tüm yürütülebilir dosyaları uygulama kategorisine ekler.
  - Dosya karma kodu. Kaspersky Security Center, belirtilen karma koduna sahip tüm yürütülebilir dosyaları uygulama kategorisine ekler.

    Farklı dosya sürümleri farklı karma koda sahip olacağından bu koşulun kullanılması, güncellemelerin otomatik olarak yüklenme özelliğini hariç tutar.

  - Dosya sertifikası. Kaspersky Security Center, belirtilen sertifika ile imzalanmış tüm yürütülebilir dosyaları uygulama kategorisine ekler.
  - KL kategorisi. Kaspersky Security Center, belirtilen KL kategorisindeki tüm yürütülebilir dosyaları uygulama kategorisine ekler.
  - Uygulama klasörü. Kaspersky Security Center, tüm yürütülebilir dosyaları bu klasörden uygulama kategorisine ekler.

    Belirtilen klasörden herhangi bir uygulamanın başlatılmasına izin verilebileceğinden **Uygulama klasörü** koşulunun kullanımı güvenli olmayabilir. **Uygulama klasörü** koşulu bulunan uygulama kategorilerini kullanan kuralların yalnızca otomatik güncellemelerin yüklenmesine izin verilmesi gereken kullanıcılara uygulanması önerilir.

- **Belirli bir klasördeki yürütülebilir dosyaları içeren kategori**. Yürütülebilir dosyaların, oluşturulan uygulama kategorisine otomatik olarak atanacağı bir klasör belirtebilirsiniz.
- **Seçili cihazlardaki yürütülebilir dosyaları içeren kategori**. Tüm yürütülebilir dosyaların, oluşturulan uygulama kategorisine otomatik olarak atanacağı bir bilgisayar belirtebilirsiniz.

  Bu uygulama kategorileri oluşturma yöntemini kullanırken Kaspersky Security Center, **Yürütülebilir dosyalar** klasöründen bilgisayardaki uygulamalar hakkında bilgiler alır.

2. Uygulama Denetimi bileşeni için İzin listesi modunu seçin.
3. Oluşturulan uygulama kategorilerini kullanarak Uygulama Denetimi kuralları oluşturun.

   Altın İmaj kuralı ve **Güvenilir Güncelleyiciler** kuralı ilk olarak İzin Listesi modu için tanımlanmıştır. Bu Uygulama Denetimi kuralları KL kategorilerine karşılık gelir. *Altın İmaj* KL kategorisi, işletim sisteminin normal çalışmasını sağlayan programlar içerir. *Güvenilir Güncelleyiciler* KL kategorisi en çok tanınan yazılım satıcıları için güncelleyiciler içerir. Bu kuralları silemezsiniz. Bu kuralların ayarları düzenlenemez. Varsayılan olarak **Altın İmaj** kuralı etkindir ve **Güvenilir Güncelleyiciler** kuralı devre dışıdır. Tüm kullanıcıların, bu kuralların tetikleme koşullarıyla eşleşen uygulamaları başlatmasına izin verilir.
4. Güncellemelerin otomatik yüklenmesine izin verilmesi gereken uygulamaları belirleyin.

Güncellemelerin otomatik olarak yüklenmesine aşağıdaki yollardan biriyle izin verebilirsiniz:

- Herhangi bir KL kategorisine ait tüm uygulamaların başlatılmasına izin vererek izin verilen uygulamaların genişletilmiş bir listesini belirtin.
- Sertifikalarla imzalanmış tüm uygulamaların başlatılmasına izin vererek izin verilen uygulamaların genişletilmiş bir listesini belirtin.

  Sertifikalarla imzalanmış tüm uygulamaların başlatılmasına izin vermek için yalnızca `*` değerine sahip **Konu** parametresini kullanan sertifika tabanlı bir koşulla bir kategori oluşturabilirsiniz.
- Uygulama Denetimi kuralı için **Güvenilir Güncelleyiciler** parametresini seçin. Bu onay kutusu işaretlenirse Kaspersky Endpoint Security, bu kurala dahil olan uygulamaları Güvenilir Güncelleyiciler olarak kabul eder. Kaspersky Endpoint Security, ilgili uygulamalara herhangi bir engelleme kuralı uygulanmadığı takdirde ilgili kurala dahil olan uygulamalar tarafından yüklenen veya güncellenen uygulamaların başlatılmasına izin verir.

  Kaspersky Endpoint Security ayarları taşınırken güvenilir güncelleyiciler tarafından oluşturulan yürütülebilir dosyaların listesi de taşınır.
- Bir klasör oluşturun ve güncellemelerinin otomatik olarak yüklenmesine izin vermek istediğiniz uygulamaların yürütülebilir dosyalarını buraya yerleştirin. Ardından **Uygulama klasörü** koşuluyla bir uygulama kategorisi oluşturun ve yolu bu klasöre yönlendirecek şekilde ayarlayın. Bir izin verme kuralı oluşturun ve bu kategoriyi seçin.

  Belirtilen klasörden herhangi bir uygulamanın başlatılmasına izin verilebileceğinden **Uygulama klasörü** koşulunun kullanımı güvenli olmayabilir. **Uygulama klasörü** koşulu bulunan uygulama kategorilerini kullanan kuralların yalnızca otomatik güncellemelerin yüklenmesine izin verilmesi gereken kullanıcılara uygulanması önerilir.

İzin verilenler listesi modunu test etme

Uygulama Denetimi kurallarının, çalışması gereken uygulamaları engellemediğinden emin olmak için yeni kurallar oluşturulduktan sonra Uygulama Denetimi kurallarını test etme işleminin etkinleştirilmesi ve işlemlerinin analiz edilmesi önerilir. Test etkin olduğunda Kaspersky Endpoint Security, Uygulama Denetimi kuralları tarafından başlatılması yasaklanan uygulamaları engellemez ancak bunun yerine Yönetim Sunucusu'na başlatıldıkları hakkında bildirimler gönderir.

İzin listesi modunu teste ederken aşağıdaki işlemlerin gerçekleştirilmesi önerilir:

1. Test süresini belirleyin (birkaç günden iki aya kadar değişen aralıklarda).
2. Uygulama Denetimi kurallarının test etme işlemini etkinleştirin.
3. Test sonuçlarını analiz etmek için Uygulama Denetiminin çalışmasının test edilmesi sonucu meydana gelen olayları ve test modunda engellenen uygulamalar hakkındaki raporu inceleyin.
4. Analiz sonuçlarına göre izin listesi modu ayarlarında değişiklikler yapın.

   Özellikle, test sonuçlarına göre, etkinliklerle ilgili yürütülebilir dosyaları bir uygulama kategorisine ekleyebilirsiniz.

İzin verilenler listesi modu desteği

Uygulama Denetimi için bir engelleme eylemi seçildikten sonra aşağıdaki işlemleri gerçekleştirerek izin listesi modunu desteklemeye devam etmeniz önerilir:

- Uygulama Denetimi'nin etkinliğini analiz etmek için Uygulama Denetimi işleminden kaynaklanan olayları inceleyin ve engellenen çalıştırmaları raporlayın.
- Kullanıcıların uygulamalara erişim taleplerini analiz edin.
- Bilinmeyen yürütülebilir dosyaları, Kaspersky Security Network'te tanınırlıklarını kontrol ederek analiz edin.
- İşletim sistemi veya yazılım için güncellemeleri yüklemeden önce bu güncellemelerin Uygulama Denetimi kuralları tarafından nasıl işleneceğini kontrol etmek için güncellemeleri bir bilgisayar test grubuna yükleyin.
- Gerekli uygulamaları, Uygulama Denetimi kurallarında kullanılan kategorilere ekleyin.

Ağ portlarını izleme

Kaspersky Endpoint Security'nin çalışması sırasında İnternet Denetimi, Posta Tehdidi Koruması, Web Tehdidi Koruması, Davranış Tespiti ve Exploit Önleme bileşenleri, belirli iletişim kurallarından aktarılan ve kullanıcı bilgisayarında TCP ve UDP gibi belirli açık portlarından geçen veri akışlarını izler. Örneğin Posta Tehdidi Koruması bileşeni, SMTP aracılığıyla iletilen bilgileri analiz ederken, Web Tehdidi Koruması bileşeni HTTP ve FTP aracılığıyla aktarılan bilgileri analiz eder.

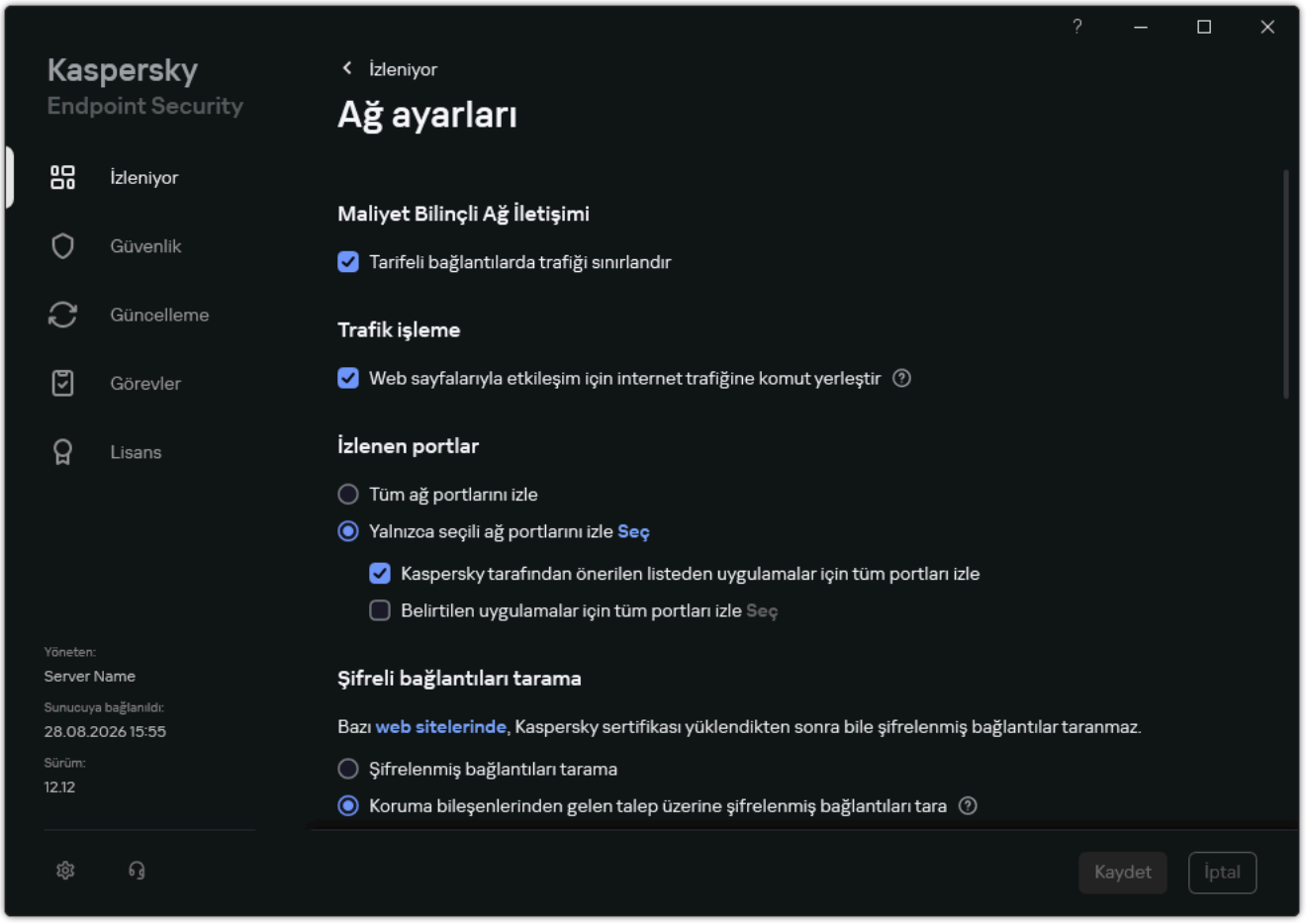
Kaspersky Endpoint Security, kullanıcının bilgisayarının TCP ve UDP portlarını riskten etkilenme olasılığına bağlı olarak birkaç gruba ayırır. Bazı ağ portları hassas hizmetler için ayrılmıştır. Bu portların daha iyi izlemeniz önerilir çünkü bunların bir ağ saldırısı tarafından hedef alınma ihtimali daha fazladır. Standart olmayan ağ portlarından yararlanan standart olmayan hizmetler kullanıyorsanız, bu ağ portları da saldıran bilgisayar tarafından hedeflenebilir. Ağa erişim isteyen ağ portlarının listesini ve uygulamaların listesini de belirtebilirsiniz. Ağ trafiğini izleme sırasında Posta Tehdidi Koruması ve Web Tehdidi Koruması bileşenleri bu portlara ve uygulamalara özellikle dikkat eder.

Bilgisayarın güvenliğini sağlamaya yardımcı olmak için Davranış Tespiti ve Exploit Önleme bileşenleri ağ portlarından geçen veri akışlarını da izler. Bileşenler, tehdit oluşturabilecek münferit süreçler için ağ trafiğini sürekli olarak izler.

Tüm ağ portlarını izlemeyi etkinleştirme

Tüm ağ portlarını izlemeyi etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



Ağ portları izleme ayarları

3. **İzlenen portlar** bloğunda, **Tüm ağ portlarını izle**'yi seçin.
4. Değişikliklerinizi kaydedin.

İzlenen ağ portlarının listesini oluşturma

İzlenen ağ portlarının listesini oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **İzlenen portlar** bloğunda, **Yalnızca seçili ağ portlarını izle**'yi seçin.

4. **Seç**'e tıklayın.

   Bu, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ portlarının listesini açar. Ağ portlarının listesi, Kaspersky Endpoint Security paketinde yer alır.

5. Ağ portu izlemeyi etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş düğmesini kullanın.

6. Ağ portlarının listesinde bir ağ portu görülmüyorsa aşağıdaki işlemleri yaparak ekleyin:

   a. **Ekle**'ye tıklayın.

   b. Açılan pencerede, ağ portu numarası ve kısa açıklama girin.

   c. Ağ portu izleme için **Etkin** veya **Etkin değil** durumunu ayarlayın.

7. Değişikliklerinizi kaydedin.

FTP iletişim kuralı pasif modda çalıştığında, izlenen ağ portlarının listesine eklenmeyen rastgele bir ağ portu üzerinden bağlantı kurulur. Bu tür bağlantıları korumak için, tüm ağ portlarının izlenmesini etkinleştirin veya FTP bağlantıları kuran uygulamalar için ağ portlarının denetimini yapılandırın.

Tüm ağ portlarının izlendiği uygulamaların listesini oluşturma

Kaspersky Endpoint Security'nin tüm ağ portlarını izlediği uygulamaların bir listesini oluşturabilirsiniz.

FTP iletişim kuralı üzerinden veri alan veya ileten uygulamaların, Kaspersky Endpoint Security'nin tüm ağ portlarını izlediği uygulamalar listesine eklenmesini öneririz.

Tüm ağ portlarının izlendiği uygulamaların listesini oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.

3. **İzlenen portlar** bloğunda, **Yalnızca seçili ağ portlarını izle**'yi seçin.

4. **Kaspersky tarafından önerilen listeden uygulamalar için tüm portları izle** onay kutusunu işaretleyin.

   Bu onay kutusu işaretlenirse Kaspersky Endpoint Security aşağıdaki uygulamalar için tüm portları izler:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.
   - Microsoft Edge.
   - Mozilla Firefox.
   - Internet Explorer.

- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.
- Yandex Browser.

5. **Belirtilen uygulamalar için tüm portları izle** onay kutusunu işaretleyin.
6. **Seç**'e tıklayın.
   Bu, Kaspersky Endpoint Security'nin ağ portlarını izlediği uygulamaların bir listesini açar.
7. Ağ portu izlemeyi etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş düğmesini kullanın.
8. Bir uygulama, uygulamalar listesinde yer almıyorsa aşağıdaki şekilde ekleyin:
   a. **Ekle**'ye tıklayın.
   b. Açılan pencereye, uygulamanın yürütülebilir dosyasının yolunu ve kısa bir açıklama girin.
   c. Ağ portlarını izleme için **Etkin** veya **Etkin değil** durumunu ayarlayın.
9. Değişikliklerinizi kaydedin.

İzlenen portların listelerini dışa ve içe aktarma

Kaspersky Endpoint Security, ağ portlarını izlemek için aşağıdaki listeleri kullanır: ağ portlarının listesi ve portları Kaspersky Endpoint Security tarafından izlenen uygulamaların listesi. İzlenen portların listelerini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin aynı açıklamaya sahip çok sayıda bağlantı noktası eklemek için dosyayı değiştirebilirsiniz. İzlenen portların listelerini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) izlenen portların listelerini dışa ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.

5. Ağ portları listesini dışa aktarmak için:

   a. **İzlenen portlar** bloğunda, **Yalnızca seçili ağ portlarını izle**'yi seçin.

   b. **N port seçildi** bağlantısına tıklayın.

      Ağ portları penceresi açılır. **Ağ portları** penceresinde, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ portlarının listesi görüntülenir. Ağ portlarının listesi, Kaspersky Endpoint Security paketinde yer alır.

   c. Ağ portları listesinden dışa aktarmak istediğiniz portları seçin.

   d. **Dışa aktar**'a tıklayın.

   e. Açılan pencerede, ağ portları listesini dışa aktarmak istediğiniz XML dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   f. Dosyaya kaydet.

      Kaspersky Endpoint Security, ağ portları listesinin tamamını XML dosyasına aktarır.

6. Kaspersky Endpoint Security tarafından portları izlenen uygulamaların listesini dışa aktarmak için:

   a. **İzlenen portlar** bloğunda, **Belirtilen uygulamalar için tüm portları izle** onay kutusunu seçin.

   b. **N uygulama seçildi** bağlantısına tıklayın.

   c. Uygulamalar listesinden, dışa aktarmak istediğiniz uygulamaları seçin.

   d. **Dışa aktar**'a tıklayın.

   e. Açılan pencerede, uygulamalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   f. Dosyaya kaydet.

      Kaspersky Endpoint Security, uygulamalar listesinin tamamını XML dosyasına aktarır.

7. Ağ portları listesini içe aktarmak için:

   a. Ağ portları listesinde **İçe aktar** düğmesine tıklayın.

      Açılan pencerede, ağ portları listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   b. Dosyayı aç.

      Bilgisayar zaten bir ağ portları listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

8. Kaspersky Endpoint Security tarafından portları izlenen uygulamaların listesini içe aktarmak için:

   a. Ugulamalar listesinde **İçe aktar** düğmesine tıklayın.

      Açılan pencerede, uygulamalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir uygulamar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

9. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde **Genel Ayarlar → Ağ ayarları** öğesini seçin.

4. **İzlenen portlar** bloğunda, **Yalnızca seçili ağ portlarını izle**'yi seçin.

5. **Ayarlar**'a tıklayın.

Ağ portları penceresi açılır. **Ağ portları** penceresinde, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ portlarının listesi görüntülenir. Ağ portlarının listesi, Kaspersky Endpoint Security paketinde yer alır.

6. Ağ portları listesini dışa aktarmak için:

a. Ağ portları listesinden dışa aktarmak istediğiniz portları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

Herhangi bir port seçmediyseniz, Kaspersky Endpoint Security tüm portları dışa aktarır.

b. **Dışa aktar**'a tıklayın.

c. Açılan pencerede, ağ portları listesini dışa aktarmak istediğiniz XML dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

d. Dosyaya kaydet.

Kaspersky Endpoint Security, ağ portları listesinin tamamını XML dosyasına aktarır.

7. Kaspersky Endpoint Security tarafından portları izlenen uygulamaların listesini dışa aktarmak için:

a. **Belirtilen uygulamalar için tüm portları izle** onay kutusunu işaretleyin.

b. Uygulamalar listesinden, dışa aktarmak istediğiniz uygulamaları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

Herhangi bir uygulama seçmediyseniz, Kaspersky Endpoint Security tüm uygulamaları dışa aktarır.

c. **Dışa aktar**'a tıklayın.

d. Açılan pencerede, uygulamalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

e. Dosyaya kaydet.

Kaspersky Endpoint Security, uygulamalar listesinin tamamını XML dosyasına aktarır.

8. Ağ portları listesini içe aktarmak için:

a. Ağ portları listesinde **İçe aktar** düğmesine tıklayın.

Açılan pencerede, ağ portları listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir ağ portları listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

9. Kaspersky Endpoint Security tarafından portları izlenen uygulamaların listesini içe aktarmak için:

a. Ugulamalar listesinde **İçe aktar** düğmesine tıklayın.

Açılan pencerede, uygulamalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir uygulamar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

10. Değişikliklerinizi kaydedin.

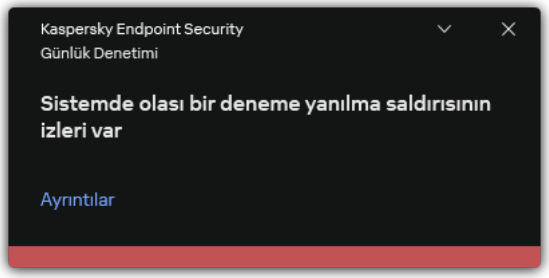
Günlük Denetimi

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

Günlük Denetimi, Windows olay günlüğü analizine göre korunan ortamın bütünlüğünü izler. Uygulama, sistemde tipik olmayan davranış belirtilerini tespit ettiğinde, bu davranış bir siber saldırı girişiminin göstergesi olabileceğinden yöneticiyi bilgilendirir.

Kaspersky Endpoint Security, Windows olay günlüklerini analiz eder ve kurallara uygun olarak ihlali tespit eder. Bileşen, önceden tanımlanmış kuralları içerir. Önceden tanımlanmış kurallar, sezgisel analiz tarafından desteklenir. Ayrıca kendi kurallarınızı ekleyebilirsiniz (özel kurallar). Bir kural tetiklendiğinde, uygulama, *Kritik* durumuna sahip bir olay oluşturur (aşağıdaki şekle bakın).

Günlük Denetimini kullanmak istiyorsanız, denetim ilkesinin güvenlik ayarlarının yapılandırıldığından ve sistemin ilgili olayları günlüğe kaydettiğinden emin olun (ayrıntılar için bkz. Microsoft teknik destek web sitesi.).



Günlük Denetimi bildirimi

Önceden tanımlanmış kuralları yapılandırma

Önceden tanımlanmış kurallar, korunan bilgisayardaki anormal etkinlik şablonlarını içerir. Anormal etkinlik, saldırı girişimi anlamına gelebilir. Önceden tanımlanmış kurallar, sezgisel analiz tarafından desteklenir. Günlük Denetimi için önceden tanımlanmış yedi kural mevcuttur. Bu kuralların herhangi birini etkinleştirebilir veya devre dışı bırakabilirsiniz. Önceden tanımlanmış kurallar silinemez.

Aşağıdaki işlemler için olayları izleyen kurallar için tetikleme kriterlerini yapılandırabilirsiniz:

- Parola deneme yanılma sldırısı algılama
- Ağ oturum açma algılama

Yönetim Konsolu'nda (MMC) önceden tanımlanmış kuralları yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Günlük Denetimi** seçimini yapın.
4. **Günlük Denetimi** onay kutusunun seçili olduğundan emin olun.
5. **Önceden tanımlanmış kurallar** bloğunda **Ayarlar** düğmesine tıklayın.
6. Önceden tanımlanmış kuralları yapılandırmak için onay kutularını seçin veya temizleyin:
   - **Sistemde olası bir deneme yanılma saldırısının izleri var**.
   - **Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var**.
   - **Olası bir Windows Olay Günlüğü kötüye kullanımının izleri var**.
   - **Yüklenen yeni bir hizmet adına alışılmadık eylemler tespit edildi**.
   - **Açık kimlik bilgileri kullanan alışılmadık oturum açma algılandı**.
   - **Sistemde olası bir Kerberos sahte PAC (MS14-068) saldırısının izleri var**.
   - **Ayrıcalıklı yerleşik Yöneticiler grubunda şüpheli değişiklikler tespit edildi**.
7. Gerekirse **Sistemde olası bir deneme yanılma saldırısının izleri var** kuralını yapılandırın:
   a. Kuralın altında bulunan **Ayarlar** düğmesine tıklayın.
   b. Açılan pencerede, kuralın tetiklenmesi için parola girme denemelerinin gerçekleştirilmesi gereken deneme sayısını ve süreyi belirtin.
   c. **Tamam**'a tıklayın.

8. **Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var** kuralını seçmeniz durumunda ayarlarını yapılandırmanız gerekir:

   a. Kuralın altında bulunan **Ayarlar** düğmesine tıklayın.

   b. **Ağ oturum açma tespiti** bloğunda, zaman aralığının başlangıcını ve bitişini belirtin.

   Kaspersky Endpoint Security, tanımlanan aralıkta gerçekleştirilen oturum açma girişimlerini olağandışı etkinlik olarak değerlendirir.

   Aralık varsayılan olarak ayarlanmamıştır ve uygulama oturum açma girişimlerini izlemez. Uygulamanın oturum açma girişimlerini sürekli olarak izlemesi için aralığı 00:00 - 23:59 olarak ayarlayın. Aralığın başlangıcı ve bitişi çakışmamalıdır. Bunlar aynı ise uygulama oturum açma girişimlerini izlemez.

   c. Güvenilir kullanıcılar ve güvenilir IP adreslerinin (IPv4 ve IPv6) listesini oluşturun.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir. Kaspersky Endpoint Security, bu kullanıcılar ve bilgisayarlar için oturum açma girişimlerini izlemez.

   d. **Tamam**'a tıklayın.

9. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da önceden tanımlanmış kuralları yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Günlük Denetimi**'ne gidin.
5. **Günlük Denetimi ETKİN** anahtarının açık durumda olduğundan emin olun.
6. **Önceden tanımlanmış kurallar** bloğunda, geçişleri kullanarak önceden tanımlanmış kuralları etkinleştirin veya devre dışı bırakın:

   - **Sistemde olası bir deneme yanılma saldırısının izleri var**.
   - **Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var**.
   - **Olası bir Windows Olay Günlüğü kötüye kullanımının izleri var**.
   - **Yüklenen yeni bir hizmet adına alışılmadık eylemler tespit edildi**.
   - **Açık kimlik bilgileri kullanan alışılmadık oturum açma algılandı**.
   - **Sistemde olası bir Kerberos sahte PAC (MS14-068) saldırısının izleri var**.

   a. **Ayrıcalıklı yerleşik Yöneticiler grubunda şüpheli değişiklikler tespit edildi**.

7. Gerekirse **Sistemde olası bir deneme yanılma saldırısının izleri var** kuralını yapılandırın:

   a. Kuralın altında **Ayarlar**'a tıklayın.

   b. Açılan pencerede, kuralın tetiklenmesi için parola girme denemelerinin gerçekleştirilmesi gereken deneme sayısını ve süreyi belirtin.

   c. **Tamam**'a tıklayın.

8. **Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var** kuralını seçmeniz durumunda ayarlarını yapılandırmanız gerekir:

   a. Kuralın altında **Ayarlar**'a tıklayın.

   b. **Ağ oturum açma tespiti** bloğunda, zaman aralığının başlangıcını ve bitişini belirtin.

   Kaspersky Endpoint Security, tanımlanan aralıkta gerçekleştirilen oturum açma girişimlerini olağandışı etkinlik olarak değerlendirir.

   Aralık varsayılan olarak ayarlanmamıştır ve uygulama oturum açma girişimlerini izlemez. Uygulamanın oturum açma girişimlerini sürekli olarak izlemesi için aralığı 00:00 - 23:59 olarak ayarlayın. Aralığın başlangıcı ve bitişi çakışmamalıdır. Bunlar aynı ise uygulama oturum açma girişimlerini izlemez.

   c. **İstisnalar** bloğundan güvenilir kullanıcılar ve güvenilir IP adresleri (IPv4 ve IPv6) ekleyin.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir. Kaspersky Endpoint Security, bu kullanıcılar ve bilgisayarlar için oturum açma girişimlerini izlemez.

   d. **Tamam**'a tıklayın.

9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde önceden tanımlanmış kuralları yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Günlük Denetimi**'ni seçin.
3. **Günlük Denetimi** onay kutusunun açık durumda olduğundan emin olun.
4. **Önceden tanımlanmış kurallar** bloğunda **Yapılandır** düğmesine tıklayın.
5. Önceden tanımlanmış kuralları yapılandırmak için onay kutularını seçin veya temizleyin:

   - **Sistemde olası bir deneme yanılma saldırısının izleri var**.
   - **Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var**.
   - **Olası bir Windows Olay Günlüğü kötüye kullanımının izleri var**.
   - **Yüklenen yeni bir hizmet adına alışılmadık eylemler tespit edildi**.

- **Açık kimlik bilgileri kullanan alışılmadık oturum açma algılandı**.
- **Sistemde olası bir Kerberos sahte PAC (MS14-068) saldırısının izleri var**.

a. **Ayrıcalıklı yerleşik Yöneticiler grubunda şüpheli değişiklikler tespit edildi**.

6. Gerekirse **Sistemde olası bir deneme yanılma saldırısının izleri var** kuralını yapılandırın:

   a. Kuralın altında **Ayarlar**'a tıklayın.

   b. Açılan pencerede, kuralın tetiklenmesi için parola girme denemelerinin gerçekleştirilmesi gereken deneme sayısını ve süreyi belirtin.

7. **Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var** kuralını seçmeniz durumunda ayarlarını yapılandırmanız gerekir:

   a. Kuralın altında **Ayarlar**'a tıklayın.

   b. **Ağ oturum açma tespiti** bloğunda, zaman aralığının başlangıcını ve bitişini belirtin.

   Kaspersky Endpoint Security, tanımlanan aralıkta gerçekleştirilen oturum açma girişimlerini olağandışı etkinlik olarak değerlendirir.

   Aralık varsayılan olarak ayarlanmamıştır ve uygulama oturum açma girişimlerini izlemez. Uygulamanın oturum açma girişimlerini sürekli olarak izlemesi için aralığı 00:00 - 23:59 olarak ayarlayın. Aralığın başlangıcı ve bitişi çakışmamalıdır. Bunlar aynı ise uygulama oturum açma girişimlerini izlemez.

   c. **İstisnalar** bloğundan güvenilir kullanıcılar ve güvenilir IP adresleri (IPv4 ve IPv6) ekleyin.

   Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir. Kaspersky Endpoint Security, bu kullanıcılar ve bilgisayarlar için oturum açma girişimlerini izlemez.

8. Değişikliklerinizi kaydedin.

Sonuç olarak, kural tetiklendiğinde Kaspersky Endpoint Security, *Kritik olay* oluşturur.

Özel kurallar ekleme

Kendi Günlük Denetimi kuralı tetikleme kriterlerinizi belirleyebilirsiniz. Bunu yapmak için bir olay kimliği girmeli ve bir olay kaynağı seçmelisiniz. Olay kimliğini Microsoft teknik destek web sitesinden arayabilirsiniz. Standart günlükler arasından bir olay kaynağı seçebilirsiniz: *Uygulama*, *Güvenlik* veya *Sistem*. Ayrıca bir üçüncü taraf uygulamasının günlüğünü de belirtebilirsiniz. Olay Görüntüleyicisi aracını kullanarak üçüncü taraf uygulama günlüğünün adını öğrenebilirsiniz. Üçüncü taraf uygulama günlükleri, Uygulama ve Hizmet Günlükleri klasöründe tutulur (örneğin *Windows PowerShell* günlüğü).

Uygulama, belirtilen günlüğün gerçekten Windows olay günlüğünde olup olmadığını kontrol etmez. Günlüğün adında bir hata olduğu takdirde uygulama o günlükteki olayları izlemez.

Özel kurallar listesi, Kaspersky uzmanları tarafından oluşturulmuş üç kuralı varsayılan olarak içerir.

Yönetim Konsolu'nda (MMC) özel bir kural ekleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri → Günlük Denetimi** seçimini yapın.
4. **Günlük Denetimi** onay kutusunun seçili olduğundan emin olun.
5. **Özel kurallar** bloğunda **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, etkinleştirmek istediğiniz özel kuralların yanındaki onay kutularını seçin.
7. Gerekirse, kendi özel kurallarınızı oluşturmak için **Ekle**'ye tıklayın.
8. Bir pencere açılır; bu pencerede özel kuralı yapılandırın:
   - **Kural adı**.
   - **Günlük adı**. Windows Olay Günlükleri. Şu günlükler mevcuttur: *Uygulama*, *Güvenlik*, *Sistem*.
   - **Kaynak**. Üçüncü taraf uygulama günlükleri. Olay Görüntüleyicisi aracını kullanarak üçüncü taraf uygulama günlüğünün adını öğrenebilirsiniz. Üçüncü taraf uygulama günlükleri, Uygulama ve Hizmet Günlükleri klasöründe tutulur (örneğin *Windows PowerShell* günlüğü).
   - **Olay tanımlayıcıları**. Windows Olay Günlüğündeki olay kimlikleri. Olay kimliğine Microsoft teknik belgelerinde bakabilirsiniz.
9. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir özel kaynak nasıl oluşturulur

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri → Günlük Denetimi**'ne gidin.
5. **Günlük Denetimi ETKİN** anahtarının açık durumda olduğundan emin olun.
6. **Özel kurallar** bloğundan etkinleştirmek istediğiniz özel kuralları seçin.
7. Gerekirse, kendi özel kurallarınızı oluşturmak için **Ekle**'ye tıklayın.
8. Bir pencere açılır; bu pencerede özel kuralı yapılandırın:
   - **Kural adı**.
   - **Özel günlük adı**. Windows Olay Günlükleri. Şu günlükler mevcuttur: *Uygulama*, *Güvenlik*, *Sistem*.

- **Köken**. Üçüncü taraf uygulama günlükleri. Olay Görüntüleyicisi aracını kullanarak üçüncü taraf uygulama günlüğünün adını öğrenebilirsiniz. Üçüncü taraf uygulama günlükleri, Uygulama ve Hizmet Günlükleri klasöründe tutulur (örneğin *Windows PowerShell* günlüğü).

- **Olay tanımlayıcıları**. Windows Olay Günlüğündeki olay kimlikleri. Olay kimliğine Microsoft teknik belgelerinde bakabilirsiniz.

9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde bir özel kural nasıl eklenir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Günlük Denetimi**'ni seçin.
3. **Günlük Denetimi** onay kutusunun açık durumda olduğundan emin olun.
4. **Özel kurallar** bloğunda **Yapılandır** düğmesine tıklayın.
5. Açılan pencerede, etkinleştirmek istediğiniz özel kuralların yanındaki onay kutularını seçin.
6. Gerekirse, kendi özel kurallarınızı oluşturmak için **Ekle**'ye tıklayın.
7. Bir pencere açılır; bu pencerede özel kuralı yapılandırın:

   - **Kural adı**.
   - **Günlük adı**. Windows Olay Günlükleri. Şu günlükler mevcuttur: *Uygulama*, *Güvenlik*, *Sistem*.
   - **Kaynak**. Üçüncü taraf uygulama günlükleri. Olay Görüntüleyicisi aracını kullanarak üçüncü taraf uygulama günlüğünün adını öğrenebilirsiniz. Üçüncü taraf uygulama günlükleri, Uygulama ve Hizmet Günlükleri klasöründe tutulur (örneğin *Windows PowerShell* günlüğü).
   - **Olay tanımlayıcısı**. Windows Olay Günlüğündeki olay kimlikleri. Olay kimliğine Microsoft teknik belgelerinde bakabilirsiniz.

8. Değişikliklerinizi kaydedin.

Sonuç olarak, kural tetiklendiğinde Kaspersky Endpoint Security, *Kritik* olay oluşturur.

Sistem Bütünlüğü İzleme

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

Kaspersky Endpoint Security for Windows, 12.6 sürümünden itibaren Dosya Bütünlük İzleyicisi bileşeni yerine Sistem Bütünlüğü İzleme bileşenini içerir. Sistem Bütünlüğü İzleme bileşeni, Dosya Bütünlük İzleyicisinin tüm işlevlerini içerir ve ayrıca kayıt defteri değişikliklerini ve harici cihazların bağlantısını izlemeye izin verir.

Sistem Bütünlüğü İzleme bileşeni, işletim sisteminde bilgisayar güvenliği ihlallerine işaret edebilecek değişiklikleri izler. Bu tür değişiklikler tespit edildiğinde, Kaspersky Endpoint Security ilgili olayları oluşturur ve yöneticiyi uyarır. Sistem Bütünlüğü İzleme gerçek zamanlı modda çalışabilir ve ayrıca talep üzerine sistem bütünlüğü kontrolleri gerçekleştirebilir.

Gerçek Zamanlı Sistem Bütünlüğü İzleme

Gerçek zamanlı modda, Sistem Bütünlüğü İzleme, bileşenin kapsamına (*izleme kapsamı*) dahil ettiğiniz nesnelerdeki değişiklikleri izler. Sistem Bütünlüğü İzleme, bu tür nesnelere yetkisiz erişimin gerçek zamanlı olarak engellenmesine de olanak tanır.

İsteğe Bağlı Sistem Bütünlük Denetimi

İsteğe Bağlı Sistem Bütünlük Denetimi, manuel olarak veya bir zamanlamaya göre çalıştırabileceğiniz bir görevdir. *Sistem Bütünlük Denetimi* görevini çalıştırmak için bileşenin kapsamını (*izleme kapsamı*) yapılandırmanız ve bir temel oluşturmanız gerekir. *Temel*, uygulamanın mevcut durumla karşılaştırırken referans olarak kullandığı, sistemdeki nesnelerin kaydedilmiş bir durumudur.

Dosya Bütünlük İzleyicisi ayarlarını taşıma

Kaspersky Endpoint Security'yi 12.6 sürümüne güncellediğinizde, Dosya Bütünlüğü İzleyicisi ayarları otomatik olarak taşınır. Bu geçişin bir parçası olarak uygulama, izleme kurallarını Sistem Bütünlüğü İzlemeye taşır. KSWS'den KES'e geçiş yapılırken Dosya Bütünlüğü İzleme kuralları da Sistem Bütünlüğü İzleme'ye taşınır.

> Sistem Bütünlüğü İzleme özelliğinin doğru çalışmasını sağlamak için Kaspersky Endpoint Security uygulaması hem de yönetim eklentisi 12.6 sürümüne güncellenmelidir. Yönetim eklentisinin önceki bir sürümü yüklüyse, yönetim eklentisinde **Sistem Bütünlüğü İzleme** bölümü bulunmadığından Sistem Bütünlüğü İzlemeyi yapılandıramazsınız.

Sistem Bütünlüğü İzleme kuralları hakkında

Sistem Bütünlüğü İzlemenin çalışması için en az bir kural eklemeniz gerekir. *Sistem Bütünlüğü İzleme kuralı*, kullanıcıların dosyalara ve kayıt defterine erişimini tanımlayan bir dizi kriterdir. Sistem Bütünlüğü İzleme, belirtilen *izleme kapsamına* giren dosyalardaki ve kayıt defterindeki değişiklikleri saptar. İzleme kapsamı, bir Sistem Bütünlüğü İzleme kuralının kriterlerinden biridir.

Sistem Bütünlüğü İzleme aşağıdaki nesnelerin izlenmesini sağlar:

- Dosyalar
- Kayıt defteri
- Harici cihazlar

Dosya izlemeyle ilgili özel hususlar

Sistem Bütünlüğü İzleme, dosya ve klasörlerdeki değişikliklerin yanı sıra izleme kapsamına eklenen veya kapsamdan çıkarılan dosyaları da izler. Bu değişiklikler bir bilgisayar güvenlik ihlalini gösterebilir. Nadiren değiştirilen nesneleri veya yalnızca yöneticinin erişebildiği nesneleri eklemenizi öneririz. Bu, Sistem Bütünlüğü İzleme olaylarının sayısını azaltmaya yardımcı olur.

Sistem Bütünlüğü İzleme, sunucu paylaşımlı klasörlerindeki dosyalardaki değişiklikleri izlemez. Sistem Bütünlüğü İzleme yalnızca yerel olarak kullanılabilir.

Kaspersky Endpoint Security, yalnızca Gerçek Zamanlı Sistem Bütünlüğü İzleme çalışmaya başladığında bağlı olan disklerdeki dosya ve klasör değişikliklerini izler. Gerçek Zamanlı Sistem Bütünlüğü İzleme çalışmaya başladığında bir disk bağlı değilse, dosyalar ve klasörler izleme kapsamına eklense bile uygulama bu diskteki dosya ve klasörlerin değişikliklerini izlemez.

Kayıt defteri izleme ile ilgili özel hususlar

Sistem Bütünlüğü İzleme kayıt defterini izler. Bu değişiklikler bir bilgisayar güvenlik ihlalini gösterebilir.

Sistem Bütünlüğü İzleme, kayıt defterinin aşağıdaki kök anahtarlarını izler:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (Yalnızca Gerçek Zamanlı Sistem Bütünlüğü İzlemede kullanılabilir)
- `HKEY_CURRENT_USER` (Yalnızca Gerçek Zamanlı Sistem Bütünlüğü İzlemede kullanılabilir)

Sistem Bütünlük Denetimi görevi `HKEY_CURRENT_USER` anahtarını desteklemez. `HKEY_USERS` altında `HKEY_USERS\<user profile ID>\<key>` şeklinde bir anahtar belirleyebilirsiniz.

Harici cihaz izleme ile ilgili özel hususlar

Sistem Bütünlüğü İzleme, harici cihazların bağlantısını ve bağlantısının kesilmesini izler. Bu, bilgisayarı bu tür cihazlarla dosya alışverişinden kaynaklanabilecek güvenlik tehditlerinden korumak için gereklidir. Sistem Bütünlüğü İzleme harici aygıtlara erişimi izlemez ve dosya alışverişini engellemez. Aygıtlara erişimi farklı bir uygulama bileşeni olan Aygıt Denetimini kullanarak yapılandırabilirsiniz.

> *Temel Sistem Bütünlüğü İzleyicisi* görevini çalıştırırken, uygulama, cihazların işletim sisteminde aynı sürücü harfine sahip olması durumunda harici cihazların yeniden bağlanmasını yok sayar. Giriş yapmak için, yeniden bağlanan cihazların farklı sürücü harflerine sahip olması gerekir.

Sistem Bütünlüğü İzleme, aşağıdaki harici aygıt türlerinin bağlantısını izler:

- Çıkarılabilir sürücü (USB flash sürücüler dahil).
- Sabit sürücü
- Harici ağ bağdaştırıcısı
- CD/DVD/Blu-ray sürücüsü
- Tarayıcı / kamera

Gerçek Zamanlı Sistem Bütünlüğü İzleme

Sistem Bütünlüğü İzleme, işletim sistemindeki değişikliklerin gerçek zamanlı olarak izlenmesini sağlar. Bilgisayarda güvenlik ihlallerine işaret edebilecek değişiklikleri izleyebilirsiniz. Bileşen, bu değişiklikleri engellemeye veya yalnızca değişiklik olaylarını günlüğe kaydetmeye izin verir.

Sistem Bütünlüğü İzlemenin çalışması için en az bir kural eklemeniz gerekir. *Sistem Bütünlüğü İzleme kuralı*, kullanıcıların dosyalara ve kayıt defterine erişimini tanımlayan bir dizi kriterdir. Sistem Bütünlüğü İzleme, belirtilen *izleme kapsamına* giren dosyalardaki ve kayıt defterindeki değişiklikleri saptar. İzleme kapsamı, bir Sistem Bütünlüğü İzleme kuralının kriterlerinden biridir.

Gerçek Zamanlı Sistem Bütünlüğü İzleme modları

Sistem Bütünlüğü İzleme kurallarının işletim sisteminin veya diğer hizmetlerin çalışması için kritik olan kaynaklarla ilgili herhangi bir eylemi engellemediğinden emin olmak için Test modunu etkinleştirmenizi ve bileşenin sistemi nasıl etkilediğini analiz etmenizi öneririz. Test modu açıkken Kaspersky Endpoint Security, kurallar tarafından yasaklanan kullanıcı etkinliklerini engellemez, bunun yerine *Uyarı* ⚠ olayları oluşturur.

Gerçek Zamanlı Sistem Bütünlüğü İzleme bileşeninin iki modu vardır:

- Engelle

  Bu modda, Sistem Bütünlüğü İzleme sistemdeki değişiklikleri izler ve kurallara uygun olarak bir eylem gerçekleştirir: **İzin ver** veya **Engelle**. Sistem Bütünlüğü İzleme ayrıca ilgili bir olay oluşturur ve Kaspersky Security Center konsolunda cihazın durumunu değiştirir.

- Bilgilendir

  Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir. Dosyalar veya kayıt defteri ile eylem yasaklanmışsa, uygulama bir olay oluşturur: *Yasaklanan işlemin test modunda çalışmasına izin verildi*. Kuralların sistemi nasıl etkilediğini analiz etmek için raporlara bakabilirsiniz.

Gerçek Zamanlı Sistem Bütünlüğü İzlemeyi etkinleştirme

Yönetim Konsolu'nda (MMC) Gerçek Zamanlı Sistem Bütünlüğü İzlemeyi etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme** seçimini yapın.
4. **Sistem Bütünlüğü İzleme** onay kutusunu seçin.
5. **Engelleme kuralları için çalışma modu** altında, Gerçek Zamanlı Sistem Bütünlüğü İzleme için bir mod seçin:
   - **Engelle**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarlarıyla yapılan eylemleri engeller ve ilgili bir olay oluşturur.
   - **Bilgilendir**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir ve ilgili bir olay oluşturur.
6. **Gerçek Zamanlı Sistem Bütünlüğü İzleme** bloğunda, **Gerçek Zamanlı Sistem Bütünlüğü İzleme** onay kutusunu seçin.
7. Harici cihaz izlemeyi yapılandırın:
   a. **Cihazları izle** onay kutusunu seçin.
   b. **Olay önem düzeyi** açılır listesinde, harici cihaz izleme olaylarının önem düzeyini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   Sistem Bütünlüğü İzleme, harici cihazların geçerli bağlantısını kaydeder. Bileşen uygulama ayarlarında etkinleştirildikten sonra uygulama, harici cihazların bağlantısını ve bağlantısının kesilmesini izlemeye başlar. Daha sonra, harici bir cihaz bağlandığında veya bağlantısı kesildiğinde, uygulama ilgili bir olay oluşturur.
8. Dosya ve kayıt defteri izlemeyi yapılandırın:
   a. **Dosyaları ve kayıt defterini izle** onay kutusunu seçin.
   b. **Ayarlar**'a tıklayın.

      Sistem Bütünlük İzleme kurallarının listesi açılır.
   c. **Ekle**'ye tıklayın.

      Kuralları başka bir kaynaktan da içe aktarabilirsiniz.
   d. Sistem Bütünlüğü İzleme kuralını yapılandırın (aşağıdaki tabloya bakın).
9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da Gerçek Zamanlı Sistem Bütünlüğü İzleme nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme**'ye gidin.
5. **Sistem Bütünlüğü İzleme ETKİN** anahtarını açık duruma getirin.
6. **Windows** sekmesini seçin.
7. **Gerçek Zamanlı Sistem Bütünlüğü İzleme** bölümünden, Gerçek Zamanlı Sistem Bütünlüğü İzleme için bir mod seçin:

   - **Kuralları uygula** Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarlarıyla yapılan eylemleri engeller ve ilgili bir olay oluşturur.
   - **Test kuralları (Bilgilendir)**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir ve ilgili bir olay oluşturur.
8. Dosya ve kayıt defteri izlemeyi yapılandırın:

   a. **Dosyaları ve kayıt defterini izle** onay kutusunu seçin.

   b. **Kurallar**'a tıklayın.

   Sistem Bütünlük İzleme kurallarının listesi açılır.

   c. **Ekle**'ye tıklayın.

   Kuralları başka bir kaynaktan da içe aktarabilirsiniz.

   d. Sistem Bütünlüğü İzleme kuralını yapılandırın (aşağıdaki tabloya bakın).
9. Harici cihaz izlemeyi yapılandırın:

   a. **Cihazları izle** onay kutusunu seçin.

   b. **Olay önem düzeyi** açılır listesinde, harici cihaz izleme olaylarının önem düzeyini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   Sistem Bütünlüğü İzleme, harici cihazların geçerli bağlantısını kaydeder. Bileşen uygulama ayarlarında etkinleştirildikten sonra uygulama, harici cihazların bağlantısını ve bağlantısının kesilmesini izlemeye başlar. Daha sonra, harici bir cihaz bağlandığında veya bağlantısı kesildiğinde, uygulama ilgili bir olay oluşturur.
10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Gerçek Zamanlı Sistem Bütünlüğü İzleme nasıl etkinleştirilir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme** seçimini yapın.

3. **Sistem Bütünlüğü İzleme** geçişini açık duruma getirin.

4. **Engelleme kuralları için çalışma modu** altında, Gerçek Zamanlı Sistem Bütünlüğü İzleme için bir mod seçin:

   - **Engelle**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarlarıyla yapılan eylemleri engeller ve ilgili bir olay oluşturur.
   - **Bilgilendir**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir ve ilgili bir olay oluşturur.

5. **Gerçek Zamanlı Sistem Bütünlüğü İzleme** bloğunda, **Gerçek Zamanlı Sistem Bütünlüğü İzleme** onay kutusunu seçin.

6. Harici cihaz izlemeyi yapılandırın:

   a. **Cihazları izle** onay kutusunu seçin.

   b. **Olay önem düzeyi** açılır listesinde, harici cihaz izleme olaylarının önem düzeyini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   Sistem Bütünlüğü İzleme, harici cihazların geçerli bağlantısını kaydeder. Bileşen uygulama ayarlarında etkinleştirildikten sonra uygulama, harici cihazların bağlantısını ve bağlantısının kesilmesini izlemeye başlar. Daha sonra, harici bir cihaz bağlandığında veya bağlantısı kesildiğinde, uygulama ilgili bir olay oluşturur.

7. Dosya ve kayıt defteri izlemeyi yapılandırın:

   a. **Dosyaları ve kayıt defterini izle** onay kutusunu seçin.

   b. **Ayarla**'ya tıklayın.

   Sistem Bütünlük İzleme kurallarının listesi açılır.

   c. **Ekle**'ye tıklayın.

   Kuralları başka bir kaynaktan da içe aktarabilirsiniz.

8. Sistem Bütünlüğü İzleme kuralını yapılandırın (aşağıdaki tabloya bakın).

9. Değişikliklerinizi kaydedin.

Gerçek Zamanlı Sistem Bütünlüğü İzleme kural ayarları

Parametre	Açıklama
Kural adı	Gerçek Zamanlı Sistem Bütünlüğü İzleme kuralının adı
Dosyalarda ve kayıt defterinde yapılan işlemler	• **İzin ver**. Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir. • **Engelle**. Sistem Bütünlüğü İzleme davranışı seçilen moda bağlıdır. *Sistem koruma modunu* seçtiyseniz Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarlarıyla yapılan eylemleri engeller, ilgili bir olay oluşturur ve Kaspersky Security Center konsolunda cihazın durumunu değiştirir. *Test modunu* seçtiyseniz, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir.

Parametre	Açıklama
Olay önem düzeyi	Kaspersky Endpoint Security, izleme kapsamındaki bir dosya veya kayıt defteri anahtarı değiştirildiğinde dosya değiştirme olaylarını günlüğe kaydeder. Olay önem seviyeleri şunlardır: *Bilgilendirici*, *Uyarı*, *Kritik*.

İzleme kapsamı	• **Dosya**. Bileşen tarafından izlenen dosya ve klasörlerin listesi. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
	Maskeler kullanarak:
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
	  • İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karakter sahip olan tüm dosya yollarını içerir.
	• **Kayıt defteri**. Bileşen tarafından izlenen kayıt defteri anahtarlarının ve değerlerinin listesi. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

İstisnalar	• **Dosya**. İzleme kapsamı istisnalar listesi. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. Örneğin, `C:\Folder\Application\*.log`. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.
	Maskeler kullanarak:
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
	  • İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karakter sahip olan tüm dosya yollarını içerir.
	• **Kayıt defteri**. İzleme kapsamı istisnalar listesi. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.

Güvenilir kullanıcılar ve/veya kullanıcı grupları	*Güvenilir kullanıcılar*, izleme kapsamındaki dosyalar ve kayıt defteri anahtarlarıyla eylem gerçekleştirmesine izin verilen kullanıcılardır. Kaspersky Endpoint Security, güvenilir bir kullanıcı tarafından gerçekleştirilen bir eylem tespit ederse Sistem Bütünlüğü İzleme, *Bilgilendirici* bir olay oluşturur. Kullanıcıları Active Directory'de, Kaspersky Security Center'daki hesap listesinden veya yerel bir kullanıcı adını manuel olarak girerek seçebilirsiniz. Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir.
Dosya işlemi işaretleyiciler / İzlenen işlemler	Uygulamanın izleyeceği dosyalar veya kayıt defteri anahtarları ile eylemi karakterize eden işaretleyiciler.
Karma	Değişiklik üzerine bir dosya karmasını hesaplama. Kaspersky Endpoint Security, bir olay oluşturulduğunda dosyanın karması hakkında bilgi ekler.

İsteğe Bağlı Sistem Bütünlük Denetimi

İsteğe Bağlı Sistem Bütünlük Denetimi, manuel olarak veya bir zamanlamaya göre çalıştırabileceğiniz bir görevdir. *Sistem Bütünlük Denetimi* görevini çalıştırırken, uygulama izleme kapsamına dahil edilen nesnelerin mevcut durumunu *temel* durumlarıyla karşılaştırır. Gerçek Zamanlı Sistem Bütünlüğü İzlemeden farklı olarak, *Sistem Bütünlük Denetimi* görevi olay sayısını sınırlamaya yardımcı olur ve işletim sistemindeki değişikliklerin genel bir raporunu oluşturmanızı sağlar.

Sistem Bütünlüğü İzlemenin çalışması için en az bir kural eklemeniz gerekir. *Sistem Bütünlüğü İzleme kuralı*, kullanıcıların dosyalara ve kayıt defterine erişimini tanımlayan bir dizi kriterdir. Sistem Bütünlüğü İzleme, belirtilen *izleme kapsamına* giren dosyalardaki ve kayıt defterindeki değişiklikleri saptar. İzleme kapsamı, bir Sistem Bütünlüğü İzleme kuralının kriterlerinden biridir. Gerçek Zamanlı Sistem Bütünlüğü İzleme ve *Sistem Bütünlük Denetimi* görevi tarafından paylaşılacak kuralları yapılandırabilir veya görev için ayrı kurallar oluşturabilirsiniz. Kaspersky Endpoint Security, bir temel oluşturmak için *Sistem Bütünlük Denetimi* görevindeki izleme kapsamını *Temel güncelleme* görevine uygular.

Temel oluşturma ve güncelleme

Sistem Bütünlük Denetimi görevinin çalışması için bir temele ihtiyacı vardır. *Temel*, uygulamanın mevcut durumla karşılaştırırken referans olarak kullandığı, sistemdeki nesnelerin kaydedilmiş bir durumudur. Sistemin geçerli durumu, sistemin temel çizgide kaydedilen durumundan farklıysa Kaspersky Endpoint Security ilgili olayı oluşturur. *Temel güncelleme* görevini kullanarak bir temel oluşturabilir veya güncelleyebilirsiniz.

Temeli aşağıdaki modlarda güncelleyebilirsiniz:

- Tam güncelleme.

  Uygulama, izleme kapsamındaki tüm nesneleri günceller.

- Artımlı güncelleme.

  Uygulama yalnızca değiştirilen veya yeni nesneleri algılar ve günceller.

Yönetim Konsolu'nda (MMC) bir temel nasıl oluşturulur veya güncellenir

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Temel güncelleme** seçimini yapın.

Adım 2. Temel güncelleme modunun seçilmesi

Bir temel güncelleme modu seçin:

- **Tam güncelleme**. Uygulama, izleme kapsamındaki tüm nesneleri günceller.
- **Artımlı güncelleme**. Uygulama yalnızca değiştirilen veya yeni nesneleri algılar ve günceller.

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Görev adını tanımlama

Görevin adını girin, örneğin *Temel 2024*.

5. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console'da bir temel nasıl oluşturulur veya güncellenir

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinden **Temel güncelleme**'yi seçin.

   c. **Görev adı** alanına kısa bir açıklama girin, örneğin, *Temel 2024*.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. Bir temel güncelleme modu seçin:

   - **Tam güncelleme**. Uygulama, izleme kapsamındaki tüm nesneleri günceller.
   - **Artımlı güncelleme**. Uygulama yalnızca değiştirilen veya yeni nesneleri algılar ve günceller.

10. Değişikliklerinizi kaydedin.

11. Görevin yanındaki onay kutusunu seçin.

12. **Başlat**'a tıklayın.

Sistem Bütünlük Denetimi görevi için izleme kapsamını yapılandırma

Varsayılan olarak, *Sistem Bütünlük Denetimi* görevinin izleme kapsamı Gerçek Zamanlı Sistem Bütünlük Denetiminin izleme kapsamı ile aynıdır. Görev için farklı bir izleme kapsamı yapılandırabilirsiniz.

Sistem Bütünlüğü İzleme, *Sistem Bütünlük Denetimi* görevi için `HKEY_CURRENT_USER` ve `HKEY_CURRENT_CONFIG` anahtarlarının içe aktarılmasını desteklemez. Görevin izleme kapsamı bu anahtarları içeriyorsa, uygulama *İzleme kapsamı hatalı nesneleri içeriyor* olayını oluşturur.

Yönetim Konsolu'nda (MMC) Sistem Bütünlük Denetimi görevi için farklı bir izleme kapsamı yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme** seçimini yapın.
4. **Sistem Bütünlüğü İzleme** onay kutusunu seçin.
5. **Sistem Bütünlük Denetimi** altında, görev yapılandırma modunu seçin: **Özel ayarlar**.
6. Harici cihaz izlemeyi yapılandırın:
   a. **Cihazları izle** onay kutusunu seçin.
   b. **Olay önem düzeyi** açılır listesinde, harici cihaz izleme olaylarının önem düzeyini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   Sistem Bütünlüğü İzleme, temel oluşturulduğu sırada bağlı harici cihazlar hakkındaki bilgileri kaydeder. Daha sonra, harici bir cihaz bağlandığında uygulama ilgili bir olay oluşturur. *Sistem Bütünlük Denetimi* görevini çalıştırırken, uygulama harici cihazların bağlantısının kesilmesini izlemez.

7. Dosya ve kayıt defteri izlemeyi yapılandırın:

   a. **Dosyaları ve kayıt defterini izle** onay kutusunu seçin.

   b. **Ayarlar**'a tıklayın.

      Sistem Bütünlük İzleme kurallarının listesi açılır.

   c. **Ekle**'ye tıklayın.

      Kuralları başka bir kaynaktan da içe aktarabilirsiniz.

   d. Sistem Bütünlüğü İzleme kuralını yapılandırın (aşağıdaki tabloya bakın).

8. Değişikliklerinizi kaydedin.

Web Console'da Sistem Bütünlük Denetimi görevi için farklı bir izleme kapsamı yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme**'ye gidin.

5. **Windows** sekmesini seçin.

6. **Sistem Bütünlüğü İzleme ETKİN** anahtarını açık duruma getirin.

7. **Sistem Bütünlük Denetimi** altında, görev yapılandırma modunu seçin: **Özel ayarlar**.

8. Harici cihaz izlemeyi yapılandırın:

   a. **Cihazları izle** onay kutusunu seçin.

   b. **Olay önem düzeyi** açılır listesinde, harici cihaz izleme olaylarının önem düzeyini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   Sistem Bütünlüğü İzleme, temel oluşturulduğu sırada bağlı harici cihazlar hakkındaki bilgileri kaydeder. Daha sonra, harici bir cihaz bağlandığında uygulama ilgili bir olay oluşturur. *Sistem Bütünlük Denetimi* görevini çalıştırırken, uygulama harici cihazların bağlantısının kesilmesini izlemez.

9. Dosya ve kayıt defteri izlemeyi yapılandırın:

   a. **Dosyaları ve kayıt defterini izle** onay kutusunu seçin.

   b. **Kurallar**'a tıklayın.

      Sistem Bütünlük İzleme kurallarının listesi açılır.

c. **Ekle**'ye tıklayın.

Kuralları başka bir kaynaktan da içe aktarabilirsiniz.

d. Sistem Bütünlüğü İzleme kuralını yapılandırın (aşağıdaki tabloya bakın).

10. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Sistem Bütünlük Denetimi görevi için farklı bir izleme kapsamı yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme** seçimini yapın.
3. **Sistem Bütünlüğü İzleme** geçişini açık duruma getirin.
4. **Sistem Bütünlük Denetimi** altında, görev yapılandırma modunu seçin: **Özel ayarlar**.
5. Harici cihaz izlemeyi yapılandırın:

   a. **Cihazları izle** onay kutusunu seçin.

   b. **Olay önem düzeyi** açılır listesinde, harici cihaz izleme olaylarının önem düzeyini seçin: *Bilgilendirici* ⓘ, *Uyarı* ⚠, *Kritik* ⓘ.

   Sistem Bütünlüğü İzleme, temel oluşturulduğu sırada bağlı harici cihazlar hakkındaki bilgileri kaydeder. Daha sonra, harici bir cihaz bağlandığında uygulama ilgili bir olay oluşturur. *Sistem Bütünlük Denetimi* görevini çalıştırırken, uygulama harici cihazların bağlantısının kesilmesini izlemez.

6. Dosya ve kayıt defteri izlemeyi yapılandırın:

   a. **Dosyaları ve kayıt defterini izle** onay kutusunu seçin.

   b. **Ayarla**'ya tıklayın.

   Sistem Bütünlük İzleme kurallarının listesi açılır.

   c. **Ekle**'ye tıklayın.

   Kuralları başka bir kaynaktan da içe aktarabilirsiniz.

   d. Sistem Bütünlüğü İzleme kuralını yapılandırın (aşağıdaki tabloya bakın).

7. Değişikliklerinizi kaydedin.

Bir Sistem Bütünlük Denetimi görev kuralının ayarları

Parametre	Açıklama
Kural adı	*Sistem Bütünlük Denetimi* görev kuralının adı.
Olay önem düzeyi	Kaspersky Endpoint Security, izleme kapsamındaki bir dosya veya kayıt defteri anahtarı değiştirildiğinde dosya değiştirme olaylarını günlüğe kaydeder. Olay önem seviyeleri şunlardır: *Bilgilendirici*, *Uyarı*, *Kritik*.

İzleme kapsamı	• **Dosya**. Bileşen tarafından izlenen dosya ve klasörlerin listesi. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
	Maskeler kullanarak:
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
	  • İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.
	• **Kayıt defteri**. Bileşen tarafından izlenen kayıt defteri anahtarlarının ve değerlerinin listesi. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler.

İstisnalar	• **Dosya**. İzleme kapsamı istisnalar listesi. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. Örneğin, `C:\Folder\Application\*.log`. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.
	Maskeler kullanarak:
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
	  • İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.
	  • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.
	• **Kayıt defteri**. İzleme kapsamı istisnalar listesi. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.

Sistem Bütünlük Denetimi görevini çalıştırmak

Sistem Bütünlük Denetimi görevi, dosyaların veya kayıt defteri anahtarlarının değişikliklere göre kontrol edilmesini ve ayrıca harici cihazların bağlantısının kontrol edilmesini sağlar. Dosyalarda değişiklik olup olmadığını kontrol etmek için *Sistem Bütünlük Denetimi* görevini aşağıdaki modlarda çalıştırabilirsiniz:

- Hızlı Tarama.

  Değişiklikler için dosyaları kontrol ederken, uygulamalar yalnızca dosya özniteliklerini kontrol eder. Uygulama, dosyaların içeriğini kontrol etmez.

- Tam Tarama.

  Değişiklikler için dosyaları kontrol ederken, uygulamalar tüm dosya özniteliklerini ve dosyaların içeriğini kontrol eder.

Görevin çalıştığı mod, kayıt defterinin veya harici cihazların kontrolünü etkilemez.

Yönetim Konsolu'nda (MMC) Sistem Bütünlük Denetimi görevini çalıştırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.

   Görevler listesi açılır.
3. **Yeni görev**'e tıklayın.

   Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.
4. **Kaspersky Endpoint Security → Temel Sistem Bütünlüğü İzleyicisi** öğesini seçin. Bir Sistem Bütünlüğü İzleme modu seçin:
   - **Tam Tarama**. Bu modda, uygulama dosyaların tüm özniteliklerini ve karmalarını kontrol eder.
   - **Hızlı Tarama**. Bu modda, uygulama yalnızca dosyaların özniteliklerini kontrol eder.
5. Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:
   - Yönetim Sunucusu tarafından ağda atanmamış cihazlar olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
   - Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.
   - Görevi çalıştırmak istediğiniz cihazların seçimini belirtin.
   - Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
6. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.
7. Örneğin manuel olarak veya haftanın belirli bir gününde bir görevi başlatmak için bir zamanlama yapılandırın.
8. Görev için bir ad girin.
9. Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console'da Sistem Bütünlük Denetimi görevini çalıştırma

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.
2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
   b. **Görev türü** açılır listesinde, **Sistem Bütünlük Denetimi**'ni seçin.

c. **Görev adı** alanına, örneğin *Haftalık Sistem Bütünlük Denetimi* gibi kısa bir açıklama girin.

d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. Bir Sistem Bütünlük Denetimi modu seçin:

   - **Hızlı Tarama**. Uygulama yalnızca dosya özniteliklerini kontrol eder. Uygulama, dosyaların içeriğini kontrol etmez.
   - **Tam Tarama**. Uygulama, dosyaların içeriğinin yanı sıra tüm niteliklerini de kontrol eder.

10. Değişikliklerinizi kaydedin.

11. Görevin yanındaki onay kutusunu seçin.

12. **Başlat**'a tıklayın.

Sistem Bütünlük Denetimi görevinin başarıyla tamamlanması için, *Sistem Bütünlük Denetimi* görevinin izleme kapsamının temel ile tamamen eşleşmesi gerekir. İzleme kapsamı farklıysa, görev bir hatayla sonlandırılır. İzleme kapsamlarını senkronize etmek için, yeni bir izleme kapsamı ile *Temel güncelleme* görevini çalıştırın.

Sistem Bütünlüğü İzleme kurallarını dışa ve içe aktarma

Sistem Bütünlüğü İzleme kurallarının listesini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda kayıt eklemek için dosyayı değiştirebilirsiniz. Sistem Bütünlüğü İzleme kuralları listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışarı/içeri aktarma işlevini kullanabilirsiniz.

Sistem Bütünlüğü İzleme, *Sistem Bütünlük Denetimi* görevi için `HKEY_CURRENT_USER` ve `HKEY_CURRENT_CONFIG` anahtarlarının içe aktarılmasını desteklemez. Görevin izleme kapsamı bu anahtarları içeriyorsa, uygulama *İzleme kapsamı hatalı nesneleri içeriyor* olayını oluşturur.

Yönetim Konsolu'nda (MMC) Sistem Bütünlüğü İzleme kurallarının listesini dışarı/içeri aktarma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme** seçimini yapın.

4. *Gerçek Zamanlı Sistem Bütünlüğü İzleme* kurallarını dışa veya içe aktarmak için:

   a. **Gerçek Zamanlı Sistem Bütünlüğü İzleme** bloğunda, **Ayarlar** düğmesine tıklayın.

   b. Gerçek Zamanlı Sistem Bütünlüğü İzleme kurallarının bir listesini dışa aktarmak için:

      1. Düzenlemek istediğiniz kuralları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

         Herhangi bir kural seçmezseniz, Kaspersky Endpoint Security tüm istisnaları dışa aktaracaktır.

      2. **Dışa aktar** bağlantısına tıklayın.

      3. Açılan pencerede, kurallar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

      4. Dosyaya kaydet.

         Kaspersky Endpoint Security, kurallar listesini XML dosyasına aktarır.

   c. Gerçek Zamanlı Sistem Bütünlüğü İzleme kurallarının bir listesini içe aktarmak için:

      1. **İçe aktar** bağlantısına tıklayın.

         Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

      2. Dosyayı aç.

         Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

5. *Sistem Bütünlük Denetimi* kurallarını dışa veya içe aktarmak için:

   a. **Sistem Bütünlük Denetimi** bloğunda **Özel ayarlar** öğesini seçin.

   b. **Ayarlar**'a tıklayın.

   c. Sistem Bütünlük Denetimi kurallarının listesini dışa aktarmak için:

      1. Düzenlemek istediğiniz kuralları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

         Herhangi bir kural seçmezseniz, Kaspersky Endpoint Security tüm istisnaları dışa aktaracaktır.

      2. **Dışa aktar** bağlantısına tıklayın.

      3. Açılan pencerede, kurallar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

      4. Dosyaya kaydet.

      Kaspersky Endpoint Security, kurallar listesini XML dosyasına aktarır.

   d. Sistem Bütünlük Denetimi kurallarının bir listesini içe aktarmak için:

      1. **İçe aktar** bağlantısına tıklayın.

         Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

      2. Dosyayı aç.

Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

6. Değişikliklerinizi kaydedin.

Web Console'da Sistem Bütünlüğü İzleme kurallarının bir listesini verme ve alma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Sistem Bütünlüğü İzleme**'ye gidin.
5. **Windows** sekmesini seçin.
6. *Gerçek Zamanlı Sistem Bütünlüğü İzleme* kurallarını dışa veya içe aktarmak için:
   a. **Gerçek Zamanlı Sistem Bütünlüğü İzleme** bloğunda **Kurallar** bağlantısına tıklayın.
   b. Gerçek Zamanlı Sistem Bütünlüğü İzleme kurallarının bir listesini dışa aktarmak için:
      1. Düzenlemek istediğiniz kuralları seçin.
      2. → **Dışa aktar** düğmesine tıklayın.
         Kaspersky Endpoint Security, kural listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.
   c. Gerçek Zamanlı Sistem Bütünlüğü İzleme kurallarının bir listesini içe aktarmak için:
      1. → **İçe aktar** düğmesine tıklayın.
         Açılan pencerede, Güvenilir internet adresleri listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.
      2. Dosyayı aç.
         Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.
7. *Sistem Bütünlük Denetimi* kurallarını dışa veya içe aktarmak için:
   a. **İsteğe Bağlı Sistem Bütünlük Denetimi** bloğunda **Özel ayarlar** öğesini seçin.
   b. **Kurallar** bağlantısına tıklayın.
   c. Sistem Bütünlük Denetimi kurallarının listesini dışa aktarmak için:
      1. Düzenlemek istediğiniz kuralları seçin.
      2. → **Dışa aktar** düğmesine tıklayın.
         Kaspersky Endpoint Security, kural listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

d. Sistem Bütünlük Denetimi kurallarının bir listesini içe aktarmak için:

1. → **İçe aktar** düğmesine tıklayın.

   Açılan pencerede, Güvenilir internet adresleri listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.

2. Dosyayı aç.

   Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

8. Değişikliklerinizi kaydedin.

Sistem Bütünlüğü İzleme raporlarını görüntüleme

Sistem Bütünlüğü İzleme kurallarının performansını analiz etmek için uygulama tarafından oluşturulan raporlara ve olaylara bakabilirsiniz. Kaspersky Endpoint Security, bileşenle ilgili aşağıdaki raporları oluşturur:

- Uygulama arabiriminde:
  - Sistem Bütünlüğü İzleme raporu
  - Sistem Bütünlük Denetimi raporu
  - Temel güncelleme raporu

  Sistem Bütünlüğü İzleme olaylarını raporlar.
- Kaspersky Security Center Konsolunda:
  - İzleme kurallarının en fazla tetiklendiği bilgisayarlara ilişkin rapor
  - En sık tetiklenen izleme kurallarına ilişkin rapor

  Varsayılan olarak, raporun oluşturulduğu tarihi de içeren önceki 30 gün için bir rapor oluşturulur.

  Yönetim Konsolu'nda (MMC) Sistem Bütünlüğü İzleme raporlarını görüntüleme

  1. Kaspersky Security Center Yönetim Konsolu'nu açın.
  2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Raporlar** sekmesini seçin.
  3. **Yeni rapor şablonu** düğmesine tıklayın.

     Yeni Rapor Şablonu Sihirbazı başlatılır.
  4. Rapor Şablonu Sihirbazı talimatlarını uygulayın. **Rapor şablon türünü seçme** adımında, Sistem Bütünlüğü İzleme raporunu seçin (**Diğer** bölümü):
     - **Dosya Bütünlüğü İzleyici/Sistem Bütünlüğü izleme kurallarının en sık tetiklendiği ilk 10 cihaz**.
     - **Cihazlarda en sık tetiklenen en iyi 10 Dosya Bütünlüğü İzleyici/Sistem Bütünlüğü İzleme kuralı**.

Yeni Rapor Şablonu Sihirbazı ile işlemi tamamladıktan sonra yeni rapor şablonu **Raporlar** sekmesindeki tabloda görünür.

5. Raporu, üzerine çift tıklayarak açın.

Rapor üretme işlemi başlar. Rapor yeni bir pencerede görüntülenir.

Web Console'da Sistem Bütünlüğü İzleme raporlarını görüntüleme

1. Web Console ana penceresinden **İzleme** → **Raporlar** seçimini yapın.
2. **Ekle**'ye tıklayın.

   Yeni Rapor Şablonu Sihirbazı başlatılır.
3. **Şablon türü** altında, **Diğer** bölümünde bir Sistem Bütünlüğü İzleme raporu seçin:
   - **Dosya Bütünlüğü İzleyici/Sistem Bütünlüğü izleme kurallarının en sık tetiklendiği ilk 10 cihaz**.
   - **Cihazlarda en sık tetiklenen en iyi 10 Dosya Bütünlüğü İzleyici/Sistem Bütünlüğü İzleme kuralı**.

   Yeni Rapor Şablonu Sihirbazı ile işlemi tamamladıktan sonra yeni rapor şablonu tabloda görünür.
4. Raporu seçin ve çalıştırın.

Rapor üretme işlemi başlar. Rapor yeni bir pencerede görüntülenir.

Uygulama tarafından oluşturulan olayları görüntülemek için Kaspersky Security Center konsolundaki olay seçimlerini de kullanabilirsiniz.

Sistem bütünlüğü durumu sıfırlama

Kaspersky Security Center konsolundaki bilgisayarlar aşağıdaki durumlardan birine sahiptir: *Tamam*, *Uyarı* veya *Kritik*. Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalarda veya kayıt defteri anahtarlarında değişiklik tespit ederse, bilgisayarın durumu *Uyarı* veya *Kritik* olarak değişir. Sistem Bütünlüğü İzleme tarafından atanan duruma *sistem bütünlüğü durumu* denir. Örneğin, analiz sizi nesnelerde tespit edilen değişikliğin bilgisayarın güvenliğini etkilemediğine ikna ederse, sistem bütünlüğü durumunu sıfırlayabilirsiniz.

Yönetim Konsolu'nda (MMC) sistem bütünlüğü durumunu sıfırlama

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.
2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Sistem bütünlüğü durumu sıfırlama** seçimini yapın.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Bir görev başlatma zamanlaması yapılandırma

Görev zamanlamasını örneğin manuel olarak yapılandırın.

4. Adım. Görev adını tanımlama

Görevin adını girin, örneğin, *İzleme kapsamını değiştirdikten sonra durumu sıfırlama*.

5. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console'da sistem bütünlüğü durumunu sıfırlama

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Sistem bütünlüğü durumu sıfırlama** seçimini yapın.

   c. **Görev adı** alanına kısa bir açıklama girin, örneğin, *İzleme kapsamını değiştirdikten sonra durumu sıfırlama*.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Görevi çalıştırmak için hesap seçin. Kaspersky Endpoint Security, görevi varsayılan olarak yerel bir kullanıcı hesabının hakları ile başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Görevin yanındaki onay kutusunu seçin.

8. **Başlat**'a tıklayın.

Sonuç olarak, Sistem Bütünlüğü İzleme olayları nedeniyle bilgisayarın durumu *Uyarı* veya *Kritik* olarak değiştirildiyse, bilgisayarın durumu *Tamam* olarak sıfırlanır. Bilgisayarın durumu başka olaylar nedeniyle de değişmişse, bilgisayarın durumu değişmeden kalır.

Cloud Discovery

Cloud Discovery, bulut hizmetlerine kullanıcı erişimini yönetir. Bulut hizmetleri arasında örneğin Microsoft Teams, Salesforce ve Microsoft Office 365 yer alır. Bulut hizmetleri kategoriler halinde gruplandırılmıştır, örneğin *Dosya paylaşımı*, *Mesajlaşma Uygulamaları*, *E-posta*. Kaspersky uzmanları, Cloud Discovery kategorilerini ve kategorilerde sınıflandırılan bulut hizmetlerini düzenli olarak günceller. Kaspersky Endpoint Security, uygulama veritabanlarıyla kategori ve bulut hizmetleri kümesini günceller. Bu, Cloud Discovery'nin bulut hizmetlerini kategorize etmek için Kaspersky Security Network'ü kullanmadığı anlamına gelir.

Cloud Discovery aşağıdaki işlevleri sağlar:

- Bulut hizmeti kullanımını izleme
- Bulut hizmetlerine kullanıcı erişimini engelleme

Sistem gereklilikleri

Cloud Discovery, şu koşullar yerine getirilirse kullanılabilir:

- Uygulama, iş istasyonları için Windows çalıştıran bir bilgisayara yüklenir.

  Bileşen sunucular için mevcut değildir.

- Kaspersky Security Center sürüm 15.1 veya üstü.

  Bileşen, Yönetim Konsolu'nda (MMC) bulunmaz. Cloud Discovery'yi Kaspersky Security Center Web Console ve Kaspersky Security Center Cloud Console'da yapılandırabilirsiniz.

- Kaspersky Next lisansı.

Cloud Discovery bileşeninin gerektirdiği uygulama işlevselliğini etkinleştirin:

1. **Şifrelenmiş bağlantıları tara**. Bu, HTTPS trafiğinin izlenmesi için gereklidir. Bu işlevi **Ağ ayarları** bölümünden yönetebilirsiniz.

2. **Web sayfalarıyla etkileşim için internet trafiğine komut yerleştir**. Komut dosyası, Cloud Discovery olaylarının kaydını sağlar. Komut dizisi ayrıca bulut hizmetlerine erişimin tam özellikli olarak engellenmesini sağlar. Komut dizisi olmadan, uygulama yalnızca bulut hizmeti etki alanları tarafından erişimi engeller. Bu işlevi **Ağ ayarları** bölümünden yönetebilirsiniz.

İzin verilen sayfaların açılması için günlük kaydı tut işlevini de etkinleştirebilirsiniz. İşlevsellik, bir kullanıcı aynı etki alanına ait web sayfalarını ziyaret ettiğinde olayların gruplandırılmasını içerir. Bu şekilde, bir kullanıcı bir bulut hizmetini kullandığında, Cloud Discovery her web sayfası için birden fazla olay yerine yalnızca bir olayı günlüğe kaydeder. Bu işlevi **İnternet Denetimi** bölümünden yönetebilirsiniz.

Bulut hizmetlerinin izlenmesi

Bir kullanıcı bir bulut hizmetini kullanmaya başladığında, Kaspersky Endpoint Security bu olayı kaydeder ve raporda bir giriş oluşturur. Cloud Discovery, tarayıcıda ve ilgili uygulamalarda bulut hizmeti kullanımını kontrol eder. Cloud Discovery, HTTP ve HTTPS üzerinden bulut hizmeti kullanımını kontrol eder.

Cloud Console'da bulut hizmeti izlemeyi etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **İletişim ve Web Koruması** → **Cloud Discovery** bölümüne gidin.

5. **Cloud Discovery ETKİN** düğmesini açık konumuna getirin.

6. Değişikliklerinizi kaydedin.

Sonuç olarak uygulama, kullanılan bulut hizmetleri hakkındaki bilgileri Kaspersky Security Center'a iletir. Bulut hizmeti kullanım bilgilerini raporlarda görüntüleyebilirsiniz. Gerekirse, bulut hizmetlerine erişimi engelleyebilirsiniz.

Bulut hizmetlerine erişimi engelleme

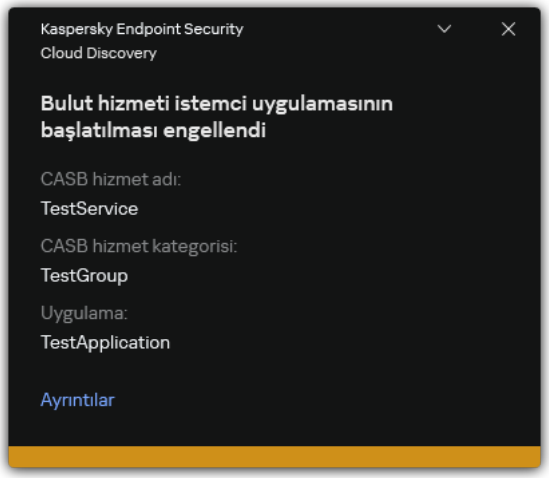
Bulut hizmetlerine erişimi engelleme yalnızca Kaspersky Next EDR Optimum ve XDR Expert lisansı için kullanılabilir. Bu özellik Kaspersky Next EDR Foundations lisansı için kullanılamaz. Kaspersky Next lisans türüne bağlı olarak uygulama işlevselliği karşılaştırması için Kaspersky Next Yardım bölümüne bakın.

Yönetici, kullanıcı erişimini Cloud Discovery kategorilerine veya tek tek bulut hizmetlerine kısıtlayabilir. Bu şekilde, yönetici yalnızca güvenli bulut hizmetlerine izin verebilir ve veri sızıntılarını önleyebilir. *Risk düzeyi bilgileri* Cloud Discovery'deki her bulut hizmeti için görüntülenir. Risk düzeyi, kuruluşun güvenlik gereksinimlerini karşılamayan hizmetlerin tespit edilmesine yardımcı olur.

Risk düzeyi bir tahmindir ve bulut hizmetinin veya satıcısının kalitesi hakkında herhangi bir beyan içermez. Risk düzeyi sadece Kaspersky uzmanlarının bir tavsiyesidir.

Bulut hizmetlerinin risk düzeyleri, ilkenin **Cloud Discovery** bölümünde, kontrol edilen tüm bulut hizmetleri listesinde görüntülenir.

Diğer Kaspersky Endpoint Security bileşenleri, bulut hizmetlerini kullanırken tehditlere karşı koruma ve şüpheli kullanıcı etkinliklerinin izlenmesini sağlar.



Cloud Discovery bildirimi

Cloud Discovery, Kaspersky Endpoint Security'den önce başlatılan bulut uygulamalarını engellemez.

Cloud Console'da bulut hizmetlerine erişimi engelleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **İletişim ve Web Koruması** → **Cloud Discovery** bölümüne gidin.
5. **Cloud Discovery ETKİN** düğmesini açık konumuna getirin.

   Tüm bulut hizmetlerinin bir listesi görüntülenir. Bulut hizmetleri kategoriler halinde gruplandırılmıştır, örneğin *Dosya paylaşımı*, *Mesajlaşma Uygulamaları*, *E-posta*. Kaspersky uzmanları, Cloud Discovery kategorilerini ve kategorilerde sınıflandırılan bulut hizmetlerini düzenli olarak günceller. Kaspersky Endpoint Security, uygulama veritabanlarıyla kategori ve bulut hizmetleri kümesini günceller.
6. Bulut hizmetlerine erişimi yapılandırmak için **Erişim** sütunundaki geçiş anahtarını kullanın.
7. Değişikliklerinizi kaydedin.

Sonuç olarak uygulama, tarayıcıda ve ilgili uygulamalarda bulut hizmeti kullanımını kontrol eder.

Güvenilir bölge

Güvenilir bölge, Kaspersky Endpoint Security'nin etkin olduğunda izlemediği nesnelerin ve uygulamaların sistem yöneticisi tarafından yapılandırılan listesidir.

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. Bir yönetici, bir kullanıcının belirli bir bilgisayar için kendi yerel güvenilir bölgesini oluşturmasına da izin verebilir. Bu şekilde, kullanıcılar bir ilkedeki genel güvenilen bölgeye ek olarak kendi yerel istisnalar ve güvenilir uygulamalar listelerini oluşturabilir.

Kaspersky Endpoint Security 12.5 for Windows ile başlayarak, EDR telemetrisini güvenilir bölgeye ekleyebilirsiniz. Bu, uygulamanın Kaspersky Anti Targeted Attack Platform (EDR) çözümü için telemetri toplama sunucusuna gönderdiği verilerin optimize edilmesini sağlar.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir.

Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, uygulamayı sanal ortamları korumak için Light Agent modunda yükleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir.

Tarama istisnası oluşturma

Tarama istisnası, Kaspersky Endpoint Security'nin belirli bir nesnede virüsleri ve diğer tehditleri taramaması için karşılanması gereken koşullar kümesidir. Tarama istisnaları, suçlular tarafından bir bilgisayara veya kullanıcı verilerine zarar vermek için kullanılabilecek yasal yazılımların güvenli bir şekilde kullanılmasını mümkün kılar. Bu tür uygulamaların mutlaka zararlı bir amacı yoktur ancak bilgisayar korsanları tarafından istismar edilebilirler. Saldırganların bilgisayarın veya kullanıcı verilerinin güvenliğini tehlikeye atmak için kullanabileceği meşru uygulamalar hakkında ayrıntılı bilgi edinmek için lütfen Kaspersky Ansiklopedisi web sitesini ziyaret edin.

Bu uygulamalar, Kaspersky Endpoint Security tarafından engellenebilir. Uygulamaların engellenmesini önlemek için kullanılan uygulamaların tarama istisnalarını yapılandırabilirsiniz. Bunun için Kaspersky IT 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 IT 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.
- *Kötü Amaçlı Yazılım Taraması* görevi

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.

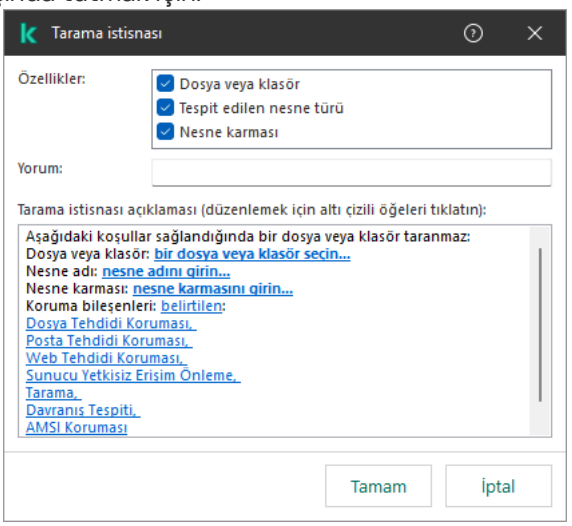
Yönetim Konsolu'nda (MMC) nasıl bir tarama istisnası oluşturulur

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Tarama istisnaları ve güvenilir uygulamalar** → **Tarama istisnaları** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, istisnaların listesini içeren bir pencere açar.
6. Şirketteki tüm bilgisayarlar için birleştirilmiş bir istisnalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki istisnaların listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki istisnalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin istisnalarının değiştirilmesi veya silinmesi mümkün değildir.
7. Kullanıcının yerel bir istisnalar listesi oluşturmasını sağlamak istiyorsanız, **Yerel istisnaların kullanılmasına izin ver** onay kutusunu seçin. Bu şekilde, bir kullanıcı, ilkede oluşturulan genel istisnalar listesine ek olarak kendi yerel istisnalar listesini de oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan istisnaların genel listesine erişebilir. Ayrıca, bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, uygulamanın kullanıcı arabirimindeki birleştirilmiş tarama istisnaları listesini gizler.
8. **Ekle**'ye tıklayın ve bir eylem seçin:
   - **Kategori**. Tarama istisnalarını ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir tarama istisnası ekleyin.
   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir tarama istisnası ekler.
   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış tarama istisnalarını* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış tarama istisnaları eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış tarama istisnalarını seçmelisiniz.
   - **Seçilen kategoriye yeni istisna**. Belirli bir kategoriye yeni bir tarama istisnası eklemek için bir kategori seçin.

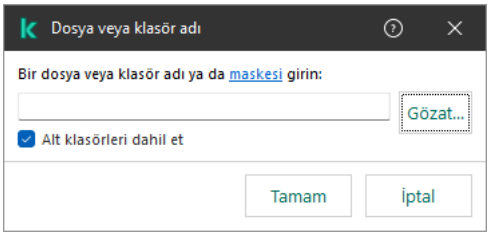
9. Bir dosya veya klasörü tarama dışında tutmak için:



İstisna ayarları

a. **Özellikler** bloğunda **Dosya veya klasör** onay kutusunu işaretleyin.

b. **Dosya veya klasör adı** penceresini açmak için aşağıdaki blokta yer alan bağlantıya tıklayın.



Dosya veya klasör seçin

a. Dosya veya klasör adını veya dosya veya klasör adı maskesini girin veya **Gözat** düğmesine tıklayarak klasör ağacındaki dosya veya klasörü seçin.

   Maskeler kullanarak:

   - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

   - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

   - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

   Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `?:\Users\*\Folder\` maskesini girin.

   Kaspersky Endpoint Security ortam değişkenlerini destekler

   Ağ klasörlerini hariç tutabilirsiniz. Bunu yapmak için ağ klasörünün yolunu manuel olarak girin (örneğin, `\\Network Share\*`).

Kaspersky Endpoint Security, Kaspersky Security Center konsolunda bir istisnalar listesi listesi oluştururken `%userprofile%` ortam değişkenini desteklemez. Girişi tüm kullanıcı hesaplarına uygulamak için `*` karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

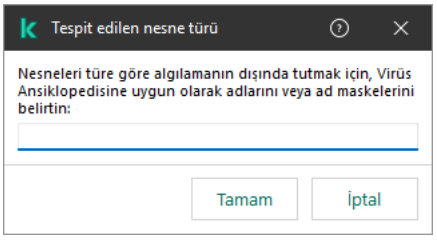
b. Gerekirse **Alt klasörleri dahil et** işlevini devre dışı bırakın. Bu işlev etkinleştirilirse uygulama tüm alt klasörlerdeki dosyaları taramaz. Bu işlev devre dışı bırakılırsa uygulama yalnızca seçilen klasörü tarama kapsamı dışında bırakır. Bu seçenek varsayılan olarak etkindir.

c. Değişikliklerinizi kaydedin.

10. Belirli bir ada sahip nesneleri tarama dışında tutmak için:

a. **Özellikler** bloğunda **Tespit edilen nesne türü** onay kutusunu işaretleyin.

b. **Tespit edilen nesne türü** penceresini açmak için aşağıdaki blokta yer alan bağlantıya tıklayın.



Nesne seç

a. Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Email-Worm`, `Rootkit` veya `RemoteAdmin`).

Maskeleri `?` karakteri (herhangi bir tek karakteri değiştirir) ve `*` karakteri ile (herhangi bir sayıda karakteri değiştirir) kullanabilirsiniz. Örneğin, `Client*` maskesi belirtilirse, Kaspersky Endpoint Security, `Client-IRC`, `Client-P2P` ve `Client-SMTP` nesnelerini taramaların dışında tutar.

b. Değişikliklerinizi kaydedin.

11. Tek bir dosyayı taramaların dışında tutmak istiyorsanız:

a. **Özellikler** bloğunda **Nesne karması** onay kutusunu işaretleyin.

b. **Nesne karması** penceresini açmak için aşağıdaki blokta yer alan bağlantıya tıklayın.



Dosya seç

a. Dosya karmasını girin veya **Gözat** düğmesine tıklayarak dosyayı seçin.

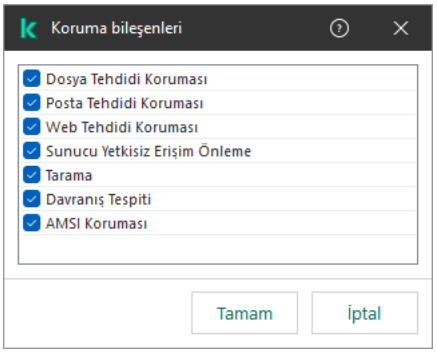
Dosya değiştirilirse, dosya karması da değiştirilecektir. Böyle bir durumda, değiştirilen dosya istisnalara eklenmeyecektir.

b. Değişikliklerinizi kaydedin.

12. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

13. Tarama istisnasını kullanması gereken Kaspersky Endpoint Security bileşenlerini belirtin:

    a. **Koruma bileşenleri** penceresini açmak için aşağıdaki blokta yer alan bağlantıya tıklayın.



Koruma bileşenlerini devre seçme

    a. Tarama istisnasının uygulanması gereken bileşenlerin karşısındaki onay kutularını işaretleyin.

       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.

14. **Tamam**'a tıklayın.

    Yeni istisna listeye eklenecektir. Nesnenin yanındaki onay kutusunu kullanarak istediğiniz zaman istisnayı devre dışı bırakabilirsiniz.

15. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Kaspersky Security Center Web Console'da tarama istisnası nasıl oluşturulur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenilir Bölge** bölümüne gidin.

5. Açılan pencerede **Kötü Amaçlı Yazılım Tarama istisnaları** bağlantısına tıklayın.

6. Şirketteki tüm bilgisayarlar için birleştirilmiş bir istisnalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki istisnaların listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki istisnalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin istisnalarının değiştirilmesi veya silinmesi mümkün değildir.

7. Kullanıcının yerel bir istisnalar listesi oluşturmasını sağlamak istiyorsanız, **Yerel istisnaların kullanılmasına izin ver** onay kutusunu seçin. Bu şekilde, bir kullanıcı, ilkede oluşturulan genel istisnalar listesine ek olarak kendi yerel istisnalar listesini de oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan istisnaların genel listesine erişebilir. Ayrıca, bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, uygulamanın kullanıcı arabirimindeki birleştirilmiş tarama istisnaları listesini gizler.

8. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Tarama istisnalarını ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir tarama istisnası ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir tarama istisnası ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış tarama istisnalarını* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış tarama istisnaları eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış tarama istisnalarını seçmelisiniz.

   Belirli bir kategoriye yeni bir tarama istisnası eklemek için, o kategorinin yanındaki onay kutusunu seçin ve **Yeni istisna** seçeneğini seçin.

9. İstisnayı nasıl eklemek istediğinizi seçin: **Dosya veya klasörün yolu**, **Nesne adı** veya **Nesne karması**.

10. Bir dosya veya klasörü tarama dışında bırakmak için yolu manuel olarak girin. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler:

    - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

    - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

    - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

      Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `?:\Users\*\Folder\` maskesini girin.

      Ağ klasörlerini hariç tutabilirsiniz. Bunu yapmak için ağ klasörünün yolunu manuel olarak girin (örneğin, `\\Network Share\*`).

11. Belirli bir nesne türünü taramaların dışında bırakmak istiyorsanız, **Nesne türü** alanına Kaspersky Ansiklopedisi'nin sınıflandırmasına göre nesne türünün adını girin (örneğin, `Email-Worm`, `Rootkit` veya `RemoteAdmin`).

    Maskeleri `?` karakteri (herhangi bir tek karakteri değiştirir) ve `*` karakteri ile (herhangi bir sayıda karakteri değiştirir) kullanabilirsiniz. Örneğin, `Client*` maskesi belirtilirse, Kaspersky Endpoint Security, `Client-IRC`, `Client-P2P` ve `Client-SMTP` nesnelerini taramaların dışında tutar.

12. Tek bir dosyayı taramaların dışında tutmak istiyorsanız, **Nesne karması** alanına dosya karma değerini girin.

    Dosya değiştirilirse, dosya karması da değiştirilecektir. Böyle bir durumda, değiştirilen dosya istisnalara eklenmeyecektir.

13. **İstisnaları şunlara uygula** bloğunda, tarama istisnasının uygulanmasını istediğiniz bileşenleri seçin.

14. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

15. **Tamam**'a tıklayın.

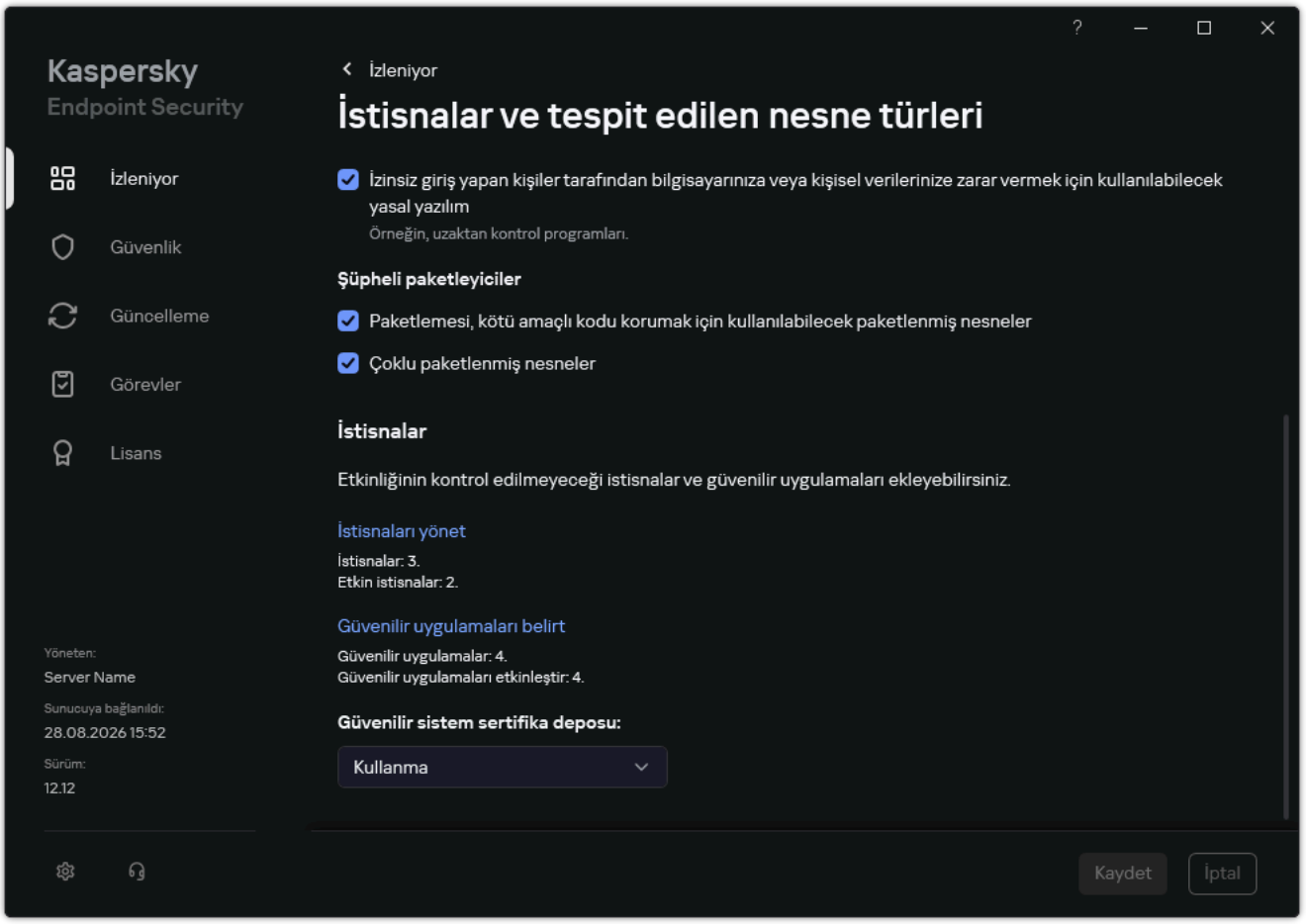
    Yeni istisna listeye eklenecektir. İstediğiniz zaman bir istisnayı durdurmak için geçiş düğmesini kullanabilirsiniz.

16. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde tarama istisnası nasıl oluşturulur

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
3. **İstisnalar** bloğunda, **İstisnaları yönet** bağlantısını tıklayın.

Kaspersky Endpoint Security, tarama istisnalarının yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel tarama istisnaları yasaklanmışsa (**Yerel istisnaların kullanılmasına izin ver** onay kutusunun işareti kaldırılmışsa) uygulamanın kullanıcı arabirimindeki tarama istisnaları listesini gizler.



İstisna ayarları

4. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Tarama istisnalarını ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir tarama istisnası ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir tarama istisnası ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış tarama istisnalarını* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış tarama istisnaları eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış tarama istisnalarını seçmelisiniz.

   Belirli bir kategoriye yeni bir tarama istisnası eklemek için, o kategorinin yanındaki onay kutusunu seçin ve **Yeni istisna** seçeneğini seçin.

5. Bir dosyayı veya klasörü taramaların dışında tutmak istiyorsanız, **Gözat** düğmesini tıklayarak dosyayı veya klasörü seçin.

   Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler:

   - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

   - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

   - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

     Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `?:\Users\*\Folder\` maskesini girin.

     Ağ klasörlerini hariç tutabilirsiniz. Bunu yapmak için ağ klasörünün yolunu manuel olarak girin (örneğin, `\\Network Share\*`).

6. Eğer taramalardan nesnenin belirli türünü dışlamak istiyorsanız, **Tespit edilen nesne türü** alanında Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Email-Worm`, `Rootkit` veya `RemoteAdmin`).

   Maskeleri `?` karakteri (herhangi bir tek karakteri değiştirir) ve `*` karakteri ile (herhangi bir sayıda karakteri değiştirir) kullanabilirsiniz. Örneğin, `Client*` maskesi belirtilirse, Kaspersky Endpoint Security, `Client-IRC`, `Client-P2P` ve `Client-SMTP` nesnelerini taramaların dışında tutar.

7. Tek bir dosyayı taramaların dışında tutmak istiyorsanız, **Nesne karması** alanına dosya karma değerini girin.

   Dosya değiştirilirse, dosya karması da değiştirilecektir. Böyle bir durumda, değiştirilen dosya istisnalara eklenmeyecektir.

8. **Koruma bileşenleri** bloğunda, tarama istisnasının uygulanmasını istediğiniz bileşenleri seçin.

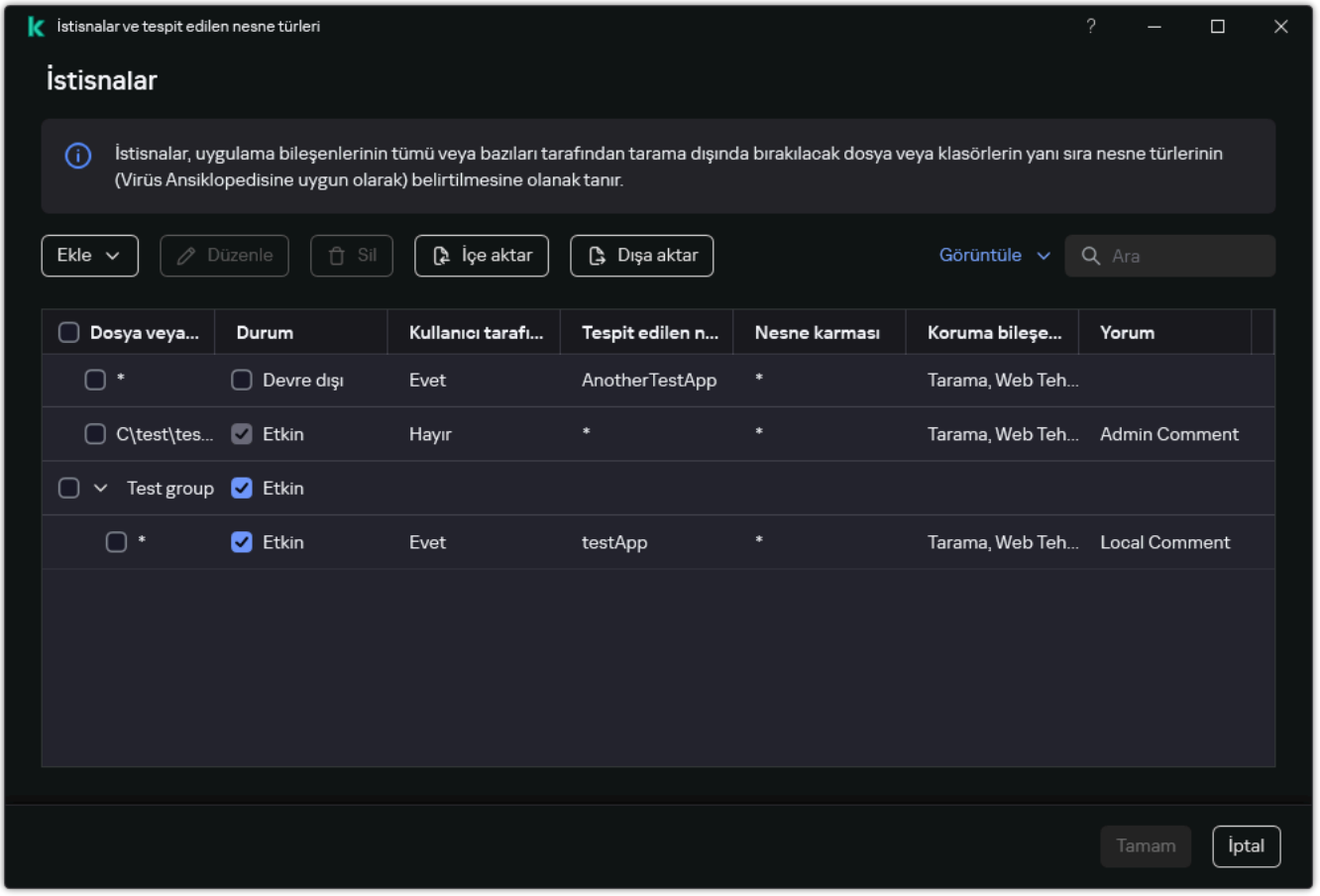
9. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

10. İstisna için **Etkin** durumu seçin.

11. **Ekle**'ye tıklayın.

    Yeni istisna listeye eklenecektir. **Durum** sütunundaki onay kutusunu kullanarak istediğiniz zaman istisnayı devre dışı bırakabilirsiniz.

12. Değişikliklerinizi kaydedin.



İstisnalar listesi

Yol maskesi örnekleri:

Mutlak yollar yerine göreceli yollar belirtmenizi öneririz. Bu, yalnızca dosya sistemi nesnelerini değil, dosyasız nesneleri de dışarıda tutmayı sağlar. Örneğin, `*\Program Files (x86)\Folder\Subfolder`.

Herhangi bir klasörde bulunan dosya yolları:

- "`*.exe`" maskesi, exe uzantısı olan tüm dosya yollarını içerir.
- `example*` maskesi, EXAMPLE 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, alt klasörleriyle birlikte içerir.
- `C:\dir\` maskesi, `C:\dir\` klasöründe bulunan tüm dosya yollarını, alt klasörleriyle birlikte içerir.
- `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.
- `C:\dir1\*\dir3\` maskesi, dir3 alt klasörlerindeki dosyaların tüm yollarını `C:\dir1\` klasörüne bir düzey dahil edecektir.
- `C:\dir1\**\dirN\` maskesi, `C:\dir1\` klasöründeki dirN alt klasörlerindeki dosyaların tüm yollarını herhangi bir düzeyde içerecektir.

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.

Tespit edilen nesnelerin türüne göre bir istisna oluşturma

Kaspersky Endpoint Security algılanan nesneleri şöyle sınıflandırır:

- **Virüs ve solucanlar**

  Alt kategori: Virüs ve solucanlar (Viruses_and_Worms)

  Tehlike düzeyi: Yüksek

  Klasik virüs ve solucanlar, kullanıcılar tarafından yetkilendirilmeyen eylemleri gerçekleştirir. Kendi kendilerini çoğaltabilme kabiliyetine sahip kopyalarını oluşturabilirler.

  Klasik virüs

  Klasik bir virüs bilgisayara sızdığında, bir dosyaya bulaşır, etkinleşir, kötü amaçlı eylemleri gerçekleştirir ve kendi kopyalarını diğer dosyalara ekler.

Klasik bir virüs, yalnızca bilgisayarın yerel kaynakları üzerinde çoğalır; kendi başına diğer bilgisayarlara giremez. Virüs, başka bir bilgisayara yalnızca paylaşımlı bir klasörde veya takılı bir CD'de bulunan bir dosyaya kendi kopyasını eklerse veya kullanıcı virüslü dosya ekli bir e-posta mesajını iletirse geçebilir.

Klasik virüs kodu, bilgisayarların, işletim sistemlerinin ve uygulamaların çeşitli alanlarına girebilir. Ortama bağlı olarak virüsler, *dosya virüslerine*, *önyükleme virüslerine*, *komut dizisi virüslerine* ve *makro virüslerine* ayrılır.

Virüsler, çeşitli teknikler kullanarak dosyalara bulaşabilir. *Overwriting* virüsler kodlarını bulaştıkları dosyanın kodunun üzerine yazarak dosyanın içeriğini silerler. Virüslü dosya çalışmaz ve geri yüklenemez. *Parasitic* virüsler dosyaları değiştirerek tamamen veya kısmen işlevsel hale getirir. *Companion* dosyaları değiştirmez, bunun yerine kopyalar oluşturur. Virüslü bir dosya açıldığında, dosyanın (aslında bir virüs olan) kopyası başlatılır. Şu virüs türleriyle de karşılaşılmaktadır: *Link virüsleri*, *OBJ virüsleri*, *LIB virüsleri*, *kaynak kodu* virüsleri ve daha pek çok tür

Worm

Klasik virüslerde olduğu gibi, solucan kodu da bilgisayara sızdıktan sonra etkinleşir ve kötü amaçlı eylemler gerçekleştirir. Solucanların bu şekilde adlandırılmalarının nedeni, bir bilgisayardan diğerine "gezinme" kabiliyetleri ve kullanıcının izni olmaksızın çok sayıda veri kanalı üzerinden kopyalarını yaymalarıdır.

Çeşitli solucan türleri arasında ayrım yapmaya izin veren ana özellik, yayılma biçimleridir. Aşağıdaki tabloda, yayılma biçimlerine göre sınıflandırılan çeşitli solucan türlerine genel bir bakış sağlanmaktadır.

Solucanların yayılma biçimleri

Tür	Ad	Açıklama
Email-Worm	Email-Worm	E-posta yoluyla yayılır. Virüslü bir e-posta mesajı, bir solucan kopyasına sahip bir dosya veya hacklenmiş ya da özellikle bu amaç için oluşturulmuş bir İnternet sitesine yüklenen bir dosyanın bağlantısını içerir. Eklenen dosyayı açtığınızda solucan etkinleştirilir. Bağlantıya tıklayıp, dosyayı indirip açtığınızda, solucan da kötü amaçlı eylemlerini gerçekleştirmeye başlar. Bundan sonra kendi kopyalarını yaymaya, diğer e-posta adreslerini aramaya ve virüslü mesajlar göndermeye devam eder.
IM-Worm	Anlık Mesajlaşma istemcisi solucanları	Anlık ileti uygulamaları aracılığıyla yayılır. Genellikle bu tür solucanlar, kullanıcının iletişim listelerini kullanarak bir İnternet sitesindeki solucanın bir kopyasıyla bir dosyaya bağlantı içeren mesajlar gönderir. Kullanıcı dosyayı indirip açtığında solucan etkinleşir.
IRC-Worm	İnternet sohbeti solucanları	Gerçek zamanlı olarak İnternet üzerinden diğer insanlarla iletişim kurmaya izin veren hizmet sistemlerinden Internet Relay Chats aracılığıyla yayılır. Bu solucanlar, bir İnternet sohbetinde kendilerinin bir kopyası veya bir dosya bağlantısı içeren bir dosya yayınlar. Kullanıcı dosyayı indirip açtığında solucan etkinleşir.
Net-Worm	Ağ solucanları	Bu solucanlar, bilgisayar ağları üzerinden yayılır. Diğer solucan türlerinden farklı olarak, tipik bir ağ solucanı kullanıcının katılımı olmadan yayılır. Yerel ağlarda zayıf noktalara sahip programlar bulunan bilgisayarları tarar. Bunun için solucan kodunu veya bir bölümünü içeren özel olarak oluşturulmuş bir ağ paketi (açık bırakıcı) gönderir. Ağda "hassas" bir bilgisayar varsa, bu ağ paketini alır. Solucan bilgisayara tamamen girdiğinde etkinleşir.
P2P-Worm	Dosya paylaşımı ağ solucanları	Eşdüzey dosya paylaşım ağları üzerinden yayılır. Bir P2P ağına sızmak için solucan genellikle kullanıcının bilgisayarında bulunan bir dosya paylaşım klasörüne kendisini kopyalar. P2P ağı, bu dosyayla ilgili bilgileri görüntüler, böylece kullanıcı ağdaki virüslü dosyayı başka herhangi bir dosya gibi "bulabilir" ve ardından dosyayı indirip açabilir. Daha karmaşık solucanlar belirli bir P2P ağının ağ iletişim kuralını taklit eder: arama sorgularına olumlu tepki verirler ve indirmek için kopyalarını sunarlar.
Worm	Solucanların diğer türleri	Solucanların diğer türleri aşağıdakileri içerir: • Kendi kopyalarını ağ kaynaklarına yayan solucanlar. İşletim sisteminin işlevlerini kullanarak, etkin ağ klasörlerini tarar, İnternet'teki bilgisayarlara bağlanır ve disk sürücülerine tam erişim elde etmeye çalışırlar. Daha önce açıklanan solucan türlerinden farklı olarak diğer solucan türleri kendi başlarına değil, kullanıcı tarafından solucanın kopyasını içeren bir dosya açıldığında etkinleşir. • Yayılmak için önceki tabloda açıklanan yöntemlerin hiçbirini kullanmayan solucanlar (örneğin, cep telefonlarından yayılanlar).

- **Truva atları (fidye yazılımı dahil)**;

  Alt kategori: Truva atları

  Tehlike düzeyi: Yüksek

  Solucanlar ve virüslerden farklı olarak Truva atları kendi kendine çoğalmamaktadır. Örneğin, kullanıcı virüslü bir İnternet sayfasını ziyaret ettiğinde, bir bilgisayara e-posta veya tarayıcı aracılığıyla girerler. Truva atları kullanıcının katılımıyla başlatılır. Kötü amaçlı eylemlerini başlatıldıktan hemen sonra yapmaya başlarlar.

  Farklı Truva atları virüslü bilgisayarlarda farklı davranır. Truva atlarının başlıca işlevleri, bilgileri engellemek, değiştirmek veya yok etmek ve bilgisayarları veya ağları devre dışı bırakmaktır. Truva atları ayrıca dosyaları alabilir veya gönderebilir, çalıştırabilir, mesajları ekranda gösterebilir, İnternet sayfalarını isteyebilir, programları indirip yükleyebilir ve bilgisayarı yeniden başlatabilir.

  Bilgisayar korsanları sıklıkla çeşitli Truva atlarının "setlerini" kullanırlar.

  Truva atı davranışının türleri aşağıdaki tabloda açıklanmaktadır.

  Virüslü bir bilgisayardaki Truva atı davranışı türleri

Tür	Ad	Açıklama
Trojan-ArcBomb	Truva atları - "arşiv bombaları"	Paket açıldığında, bu arşivler bilgisayarın çalışmasını etkileyecek büyüklükteki boyuta ulaşırlar. Kullanıcı bu tür bir arşivin paketini açmaya çalıştığında, bilgisayar yavaşlayabilir ya da donabilir: sabit sürücü "boş" veri ile doldurulabilir. "Arşiv bombaları" özellikle dosya ve e-posta sunucuları için tehlikelidir. Sunucu, gelen bilgiyi işlemek için otomatik bir sistem kullanıyorsa bir "arşiv bombası" sunucuyu durdurabilir.
Backdoor	Uzaktan yönetim için truva atları	Bunlar en tehlikeli Truva atı türü olarak kabul edilir. Bunlar işlevlerinde, bilgisayarlara yüklenen uzaktan yönetim uygulamalarına benzerdir. Bu programlar kullanıcının dikkatini çekmeden kendisini bilgisayara yükler ve saldırganın bilgisayarı uzaktan yönetmesini sağlar.
Trojan	Truva atları	Bunlar aşağıdaki zararlı uygulamaları içerir: • **Klasik Truva Atları**. Bu programlar, yalnızca Truva atlarının ana işlevlerini gerçekleştirir: bilgiyi engelleme, değiştirme ve yok etme ile bilgisayarları veya ağları devre dışı bırakma. Tabloda açıklanan Truva atı türlerinden farklı olarak hiçbir ileri düzey özelliğe sahip değillerdir. • **Çok yönlü Truva atları**. Bu programlar, çeşitli Truva atları türlerine özgü gelişmiş özelliklere sahiptir.
Trojan-Ransom	Fidye Truva atları	Kullanıcının bilgilerini "rehin" alır, değiştirir veya engeller ya da bilgisayarın çalışmasına etki eder; böylece kullanıcı bilgiyi kullanma kabiliyetini kaybeder. Saldırgan, bilgisayarın performansını ve üzerine depolanan verileri geri yüklemek için bir uygulama göndermeyi vaat ederek kullanıcıdan bir fidye ister.
Trojan-Clicker	Truva atı tıklayıcılar	Komutları kendi başına bir tarayıcıya göndererek veya işletim sistemi dosyalarında belirtilen İnternet adreslerini değiştirerek İnternet sayfalarına kullanıcının bilgisayarından erişirler. Bu programları kullanarak saldırganlar ağ saldırılarını gerçekleştirir ve İnternet sitesi ziyaretlerini arttırır, böylece reklam pencerelerinin gösterim sayısını artırır.
Trojan-Downloader	Truva atı indiriciler	Saldırganın İnternet sayfasına erişir, diğer zararlı uygulamaları buradan indirir ve kullanıcının bilgisayarına yükler. İndirilecek zararlı uygulamanın dosya adını içerebilir veya bunu erişilen İnternet sayfasından alabilir.
Trojan-Dropper	Truva atı bırakıcılar	Sabit sürücüye yükledikleri ve daha sonra kurdukları diğer Truva atlarını içerirler. Saldırganlar, aşağıdaki amaçlar için Truva atı-Bırakıcı türü programları kullanabilir: • Kullanıcı tarafından fark edilmeden bir zararlı uygulama yükleme: Truva atı-Bırakıcı türü programlar hiçbir mesaj görüntülemez veya örneğin bir arşivdeki veya işletim sisteminin uyumsuz bir sürümündeki bir hatayı bildiren sahte mesajlar görüntüler. • Bilinen diğer zararlı uygulamayı tespit edilmekten korur: tüm anti-virüs yazılımları Truva atı-Bırakıcı türü bir uygulama içindeki zararlı bir uygulamayı tespit edemez.
Trojan-Notifier	Truva atı uyarıcılar	Bir saldırgana virüslü bilgisayara erişilebilir olduğu bildirilir, saldırgana bilgisayar hakkında bilgiler gönderir: IP adresi, açık port numarası veya e-posta adresi. Saldırgan ile e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla bağlantı kurar. Truva atı-Uyarıcı türü programlar genellikle birkaç Truva atından oluşan setler halinde kullanılır. Saldırgana diğer Truva atlarının kullanıcının bilgisayarına başarılı bir şekilde yüklendiğini bildirir.

Tür	Ad	Açıklama
Trojan-Proxy	Truva atı proxy'leri	Saldırganın, kullanıcının bilgisayarını kullanarak isimsiz bir şekilde İnternet sayfalarına erişmesine izin verir; genellikle spam göndermek için kullanılır.
Trojan-PSW	Parola-çalma-yazılımı	Parola-çalma-yazılımı, yazılım kayıt verileri gibi kullanıcı hesaplarını çalan bir Truva atı türüdür. Bu Truva atları, sistem dosyalarında ve kayıt defterinde gizli verileri bulur ve e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla "saldırgana" gönderir. Bu Truva atlarından bazıları, bu tabloda açıklanan ayrı türlerde kategorilere ayrılmıştır. Bunlar; banka hesaplarını çalan (Truva atı-Banker), anlık ileti uygulamaları kullanıcılarından gelen verileri çalan (Truva atı-IM) ve çevrimiçi oyun kullanıcılarından gelen bilgileri çalan (Truva atı-OyunHırsızı) Truva atlarıdır.
Trojan-Spy	Truva atı casusları	Kullanıcı ile ilgili casusluk yapar, kullanıcının bilgisayarında çalışırken yaptığı işlemler hakkında bilgi toplar. Kullanıcının klavyede girdiklerini okuyabilir, ekran görüntülerini alabilir veya etkin uygulamaların listelerini toplayabilir. Bilgileri aldıktan sonra bunları saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla iletir.
Trojan-DDoS	Truva atı ağ saldırganları	Kullanıcı bilgisayarından uzaktaki bir sunucuya çok sayıda istek gönderirler. Sunucunun tüm istekleri işlemek için yeterli kaynağı bulunmamaktadır; bu nedenle çalışmayı durdurur (Hizmet Reddi veya yalnızca DoS). Bilgisayar korsanları, genellikle bu programlarla çok sayıda bilgisayara virüs bulaştırır; böylece bilgisayarları aynı anda tek bir sunucuya saldırmak için kullanabilirler. DoS programları, kullanıcının bilgisi dahilinde tek bir bilgisayardan bir saldırı gerçekleştirir. DDoS (Dağıtılan DoS) programları, virüslü bilgisayar kullanıcısı tarafından fark edilmeden çeşitli bilgisayarlardan dağıtılan saldırılar gerçekleştirir.
Trojan-IM	Truva atları anlık ileti uygulamaları kullanıcılarından bilgi çalar	Anlık ileti uygulamaları kullanıcılarının hesap numaralarını ve parolalarını çalar. Verileri saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla iletir.
Rootkit	Rootkit'ler	Diğer zararlı uygulamaları ve onların etkinliklerini maskeler, dahası programların işletim sistemindeki kalıcılığını uzatırlar. Ayrıca dosyaları, virüs bir bilgisayarın belleğindeki işlemleri veya zararlı uygulamaları çalıştıran kayıt defteri anahtarlarını gizleyebilirler. Rootkit'ler, kullanıcı bilgisayarındaki ve ağdaki diğer bilgisayarlardaki uygulamalar arasındaki veri alışverişini maskeleyebilir.
Trojan-SMS	SMS mesajları biçimindeki Truva atları	Cep telefonlarına virüs bulaştırır, özel tarifeli telefon numaralarına SMS mesajları gönderir.
Trojan-GameThief	Çevrimiçi oyun kullanıcılarından bilgi çalan Truva atları	Çevrimiçi oyunların kullanıcılarından hesap kimlik bilgilerini çalar ve daha sonra verileri saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla iletir.
Trojan-Banker	Banka hesaplarını çalan Truva atları	Banka hesap bilgilerini veya e-para sistem verilerini çalar, daha sonra verileri bilgisayar korsanına e-posta ile, FTP üzerinden, bilgisayar korsanının İnternet sayfasına erişerek ya da başka bir yöntem kullanarak iletir.
Trojan-Mailfinder	E-posta adreslerini toplayan Truva atları	Bir bilgisayarda saklanan e-posta adreslerini toplar ve bunları saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla gönderir. Saldırganlar, toplanan adreslere spam gönderebilir.

- **Zararlı araçlar**;

  Alt kategori: Zararlı araçlar

  Tehlike düzeyi: Orta

  Zararlı yazılımların diğer türlerinden farklı olarak zararlı araçlar başlatıldıktan hemen sonra eylemlerini gerçekleştirmez. Güvenle saklanabilir ve kullanıcının bilgisayarında başlatılır. Saldırganlar genellikle virüs, solucan ve Truva atı oluşturmak, ağ saldırılarını uzak sunucularda gerçekleştirmek, bilgisayarları hacklemek veya diğer zararlı eylemleri gerçekleştirmek için bu programların özelliklerini kullanır.

  Zararlı araçların çeşitli özellikleri, aşağıdaki tabloda açıklanan türlere göre gruplandırılmıştır.

  Zararlı araçların özellikleri

Tür	Ad	Açıklama
Constructor	Oluşturucular	Yeni virüsler, solucanlar ve Truva atları oluşturmaya izin verir. Bazı oluşturucular, oluşturulacak zararlı uygulamanın türünün, hata ayıklayıcıları önleme biçiminin ve diğer özelliklerin kullanıcılar tarafından seçilebildiği standart bir pencere tabanlı arabirime sahiptir.
DoS	Ağ saldırıları	Kullanıcı bilgisayarından uzaktaki bir sunucuya çok sayıda istek gönderirler. Sunucunun tüm istekleri işlemek için yeterli kaynağı bulunmamaktadır; bu nedenle çalışmayı durdurur (Hizmet Reddi veya yalnızca DoS).
Exploit	Açık bırakıcılar	Bir *açık bırakıcı*, işlendiği uygulamanın zayıf noktalarını kullanan veri seti veya program kodudur ve bilgisayarda kötü amaçlı eylemler gerçekleştirir. Örneğin, bir açık bırakıcı dosyaları yazabilir veya okuyabilir ya da "virüslü" İnternet sayfalarını isteyebilir. Farklı açık bırakıcılar, farklı uygulamalar veya ağ hizmetlerinde zayıf noktaları kullanır. Ağ paketi olarak gizlenmiş bir açık bırakıcı ağ üzerinden çok sayıda bilgisayara iletilir, hassas ağ hizmetlerine sahip bilgisayarları arar. Bir DOC dosyasında bulunan açık bırakıcı bir metin düzenleyicinin zayıf noktalarını kullanır. Kullanıcı virüslü dosyayı açtığında hacker tarafından önceden programlanmış eylemleri gerçekleştirmeye başlayabilir. Bir e-posta mesajında gömülü olan bir açık bırakıcı herhangi bir e-posta istemcisindeki zayıf noktaları arar. Kullanıcı bu e-posta istemcisindeki virüslü mesajı açar açmaz kötü amaçlı bir eylemi gerçekleştirmeye başlayabilir. Net-Solucanları, açık bırakıcıları kullanarak ağlara yayılırlar. Nuke atıcı açık bırakıcıları, bilgisayarları devre dışı bırakan ağ paketleridir.
FileCryptor	Şifreleyiciler	Anti virüs uygulamasından gizlemek için diğer zararlı uygulamaları şifrelerler.
Flooder	"Kirleten" ağlar için programlar	Ağ kanalları üzerinden çok sayıda mesaj gönderir. Bu tür araçlar, İnternet Bağlantılı Sohbetleri kirleten programları içerir. Bombacı tipteki araçlar, e-postalar, Anlık ileti uygulamaları ve mobil iletişim sistemleri tarafından kullanılan kanalları "kirleten" programları içermez. Bu programlar, tabloda açıklanan farklı türler olarak ayrılırlar (Email-Flooder, IM-Flooder, ve SMS-Flooder).
HackTool	Saldırı araçları	Yüklendikleri bilgisayarlara veya başka bilgisayarlara saldırmayı mümkün kılar (örneğin, kullanıcının izni olmadan yeni sistem hesapları ekleyerek veya işletim sistemindeki varlıklarının izini gizlemek için sistem kayıtlarını silerek). Bu tür araçlar, parola ele geçirme gibi zararlı işlevlerin özelliğindeki bazı dinleyicileri içerir. Dinleyiciler, ağ trafiğinin görüntülenmesine olanak tanıyan programlardır.
Hoax	Asılsız uyarılar	Bunlar kullanıcıyı virüs benzeri mesajlarla uyarırlar: virüslü olmayan bir dosyada "bir virüs tespit edebilirler" veya kullanıcıya, gerçekte olmadığı halde, sürücünün biçimlendirildiği bildiriminde bulunurlar.
Spoofer	Aldatma araçları	Göndericinin sahte bir adresini içeren mesajlar ve ağ istekleri gönderir. Saldırganlar, Aldatıcı türü araçları örneğin kendilerini mesajların gerçek göndericisiymiş süsü vermek için kullanır.
VirTool	Zararlı uygulamaları değiştiren araçlar	Diğer kötü amaçlı programların değiştirilmesine olanak tanır ve kötü amaçlı programları anti-virüs uygulamalarından gizler.
Email-Flooder	E-posta adreslerini "kirleten" programlardır	Çeşitli e-posta adreslerine çok sayıda mesaj gönderirler, böylece söz konusu adresleri "kirletirler". Büyük miktardaki gelen mesaj, kullanıcının gelen kutusunda faydalı mesajları görmesine engel olur.
IM-Flooder	Anlık ileti uygulamalarının trafiğini "kirleten" programlar	Anlık ileti uygulamalarının kullanıcılarını mesajlarla bombalar. Büyük miktardaki mesajlar, kullanıcının faydalı gelen mesajları görmesine engel olur.
SMS-Flooder	SMS mesajlarıyla trafiği "kirleten" programlar	Cep telefonlarına çok sayıda SMS mesajları gönderir.

- **Reklam yazılımı**

  Alt kategori: Reklam yazılımı (Reklam Yazılımı);

  Tehlike düzeyi: Orta

  Reklam yazılımı, kullanıcıya reklam bilgilerini gösterir. Reklam yazılımı programları, diğer programların arabiriminde reklam penceresi görüntüler ve arama sorgularını reklam İnternet sayfalarına yönlendirir. Bunlardan bazıları, kullanıcı hakkında pazarlama bilgileri toplar ve geliştiriciye gönderir: bu bilgiler kullanıcının ziyaret ettiği İnternet sitelerinin adlarını ve kullanıcının arama sorgularının içeriğini kapsar. Truva atı-Casus türü programlardan farklı olarak, reklam yazılımları bu bilgileri geliştiriciye kullanıcının izni ile gönderir.

- **Otomatik çeviriciler**

  Alt kategori: Otomatik çeviriciler (Dialer).

  Tehlike düzeyi: Orta

  Otomatik çeviriciler bir modem kullanarak gizlice telefon bağlantıları kurabilir.

- **İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım**

  Alt kategori: İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım içeriyor.

  Tehlike düzeyi: Orta

  Bu uygulamaların çoğu faydalıdır, bu yüzden çoğu kullanıcı bunları çalıştırır. Bu uygulamalar IRC istemcilerini, otomatik çeviricileri, dosya indirme programlarını, bilgisayar sistem etkinliği ekranlarını, parola özelliklerini ve FTP, HTTP ve Telnet için İnternet sunucularını içerir.

  Bununla birlikte, saldırganlar bu programlara erişim kazanırsa veya kullanıcının bilgisayarına yerleştirirse uygulamanın özelliklerinin bazıları güvenlik ihlali için kullanılabilir.

  Bu uygulamalar işleve göre farklılık gösterebilir; türleri aşağıdaki tabloda açıklanmıştır.

Tür	Ad	Açıklama
Client-IRC	İnternet sohbeti istemcileri	Kullanıcılar bu programları İnternet Bağlantılı Sohbetlerde insanlarla konuşmak için yükler. Saldırganlar bunları zararlı yazılımları yaymak için kullanır.
Downloader	İndirilecek programlar	İnternet sayfalarından programları gizli modda indirir.
Monitor	İzleme programları	Bunlar, yüklendikleri bilgisayarla ilgili etkinlik izlemeye olanak tanır (hangi uygulamaların etkin olduğunu ve diğer bilgisayarlara yüklü uygulamalarla nasıl veri alışverişi yapıldığını görürler).
PSWTool	Parola geri yükleyiciler	Unutulan parolaların görüntülenmesine ve yeniden yüklenmesine olanak tanır. Saldırganlar, aynı amaçla bunları kullanıcının bilgisayarına gizlice yerleştirir.
RemoteAdmin	Uzaktan yönetim programları	Çoğunlukla sistem yöneticileri tarafından kullanılır. Bu programlar, izlemek ve yönetmek için uzak bilgisayarın arabirimine erişim elde etmeye olanak tanır. Saldırganlar, uzak bilgisayarları izlemek ve yönetmek amacıyla bunları kullanıcının bilgisayarına yerleştirir. Yasal uzaktan yönetim programları, uzaktan yönetim için arkak apı türü Truva atlarından farklıdır. Truva atları işletim sistemlerine bağımsız olarak girme ve kendilerini yükleme kabiliyetine sahiptirler: yasal programlar bunu gerçekleştiremez.
Server-FTP	FTP sunucuları	FTP sunucuları olarak işlev gösterir. Saldırganlar, FTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Server-Proxy	Proxy sunucular	Proxy sunucuları olarak işlev gösterir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
Server-Telnet	Telnet sunucuları	Telnet sunucuları olarak işlev gösterir. Saldırganlar, Telnet aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Server-Web	İnternet sunucuları	İnternet sunucuları olarak işlev gösterir. Saldırganlar, HTTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
RiskTool	Yerel bir bilgisayarda çalışmak için araçlar	Kullanıcının kendi bilgisayarında çalışırken kullanıcıya ek seçenekler sağlar. Araçlar kullanıcıya etkin uygulamaların dosyalarını veya pencerelerini gizleme olanağı tanır ve etkin işlemleri sonlandırır.
NetTool	Ağ araçları	Kullanıcıya ağdaki başka bilgisayarla çalışırken ek seçenekler sunar. Bu araçlar, yeniden başlatmaya, açık portları tespit etmeye ve bilgisayarda yüklü uygulamaları başlatmaya olanak tanır.
Client-P2P	P2P ağ istemcileri	Eşdüzey ağlarda çalışmaya olanak tanır. Saldırganlar tarafından zararlı yazılımların yayılması için kullanılır.
Client-SMTP	SMTP istemcileri	Kullanıcının bilgisi olmadan e-posta mesajları gönderir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.

Tür	Ad	Açıklama
WebToolbar	İnternet Araç çubukları	Arama motorlarını kullanmak için araç çubuklarını diğer uygulamaların arabirimlerine ekler.
FraudTool	Sahte programlar	Kendilerine başka program süsü verir. Örneğin, zararlı yazılımların tespit edilmeleri hakkında mesajlar görüntüleyen sahte anti-virüs programları vardır. Bununla birlikte, gerçekte herhangi bir şey bulamazlar veya temizleyemezler.

- **Paketlemesi, kötü amaçlı kodu korumak için kullanılabilecek paketlenmiş nesneler**;

  Alt kategori: Zarar verebilecek paketlenmiş dosyalar.

  Tehlike düzeyi: orta.

  Dosya, kötü amaçlı yazılımları paketlemek için kullanılan özel bir paketleyici kullanılarak paketlenir: virüsler, solucanlar, Truva atları. Kaspersky Endpoint Security, SFX (kendi başına açılan) arşivlerindeki paket açıcı modülünü tarar.

  Bilgisayar korsanları, kötü amaçlı yazılımları antivirüs tarafından tespit edilmekten gizlemek için özel paketleyiciler kullanarak paketlemektedir. Kaspersky uzmanları bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

- **Çoklu paketlenmiş nesneler**.

  Alt kategori: Çoklu paketlenmiş dosyalar.

  Tehlike düzeyi: orta.

  Dosya bir veya daha fazla paketleyici ile üç veya daha fazla kez paketlenir.

  Kötü amaçlı yazılımları bir antivirüs tarafından tespit edilmekten gizlemek için, bilgisayar korsanları bir dosyayı birden çok kez paketleyebilir. Kaspersky Endpoint Security paketlenmiş dosyaları tarar.

Kaspersky Endpoint Security varsayılan olarak tüm nesne türlerini algılar. Bilgisayarın güvenliğini artırmak için tüm nesne türlerinin algılanmasını etkin bırakmanızı öneririz. Uygulamanın kötü amaçlı olarak algıladığı şirket içi yardımcı programlar kullanıyorsanız, bu yardımcı programları bir istisna listesine ekleyin, ancak tüm nesne türlerinin algılanmasını devre dışı bırakmayın.

Yönetim Konsolu (MMC) ile algılanabilir nesne türleri nasıl seçilir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Tespit edilen nesne türleri** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, Kaspersky Endpoint Security'nin algılamasını istediğiniz nesne türlerinin karşısındaki onay kutularını seçin.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

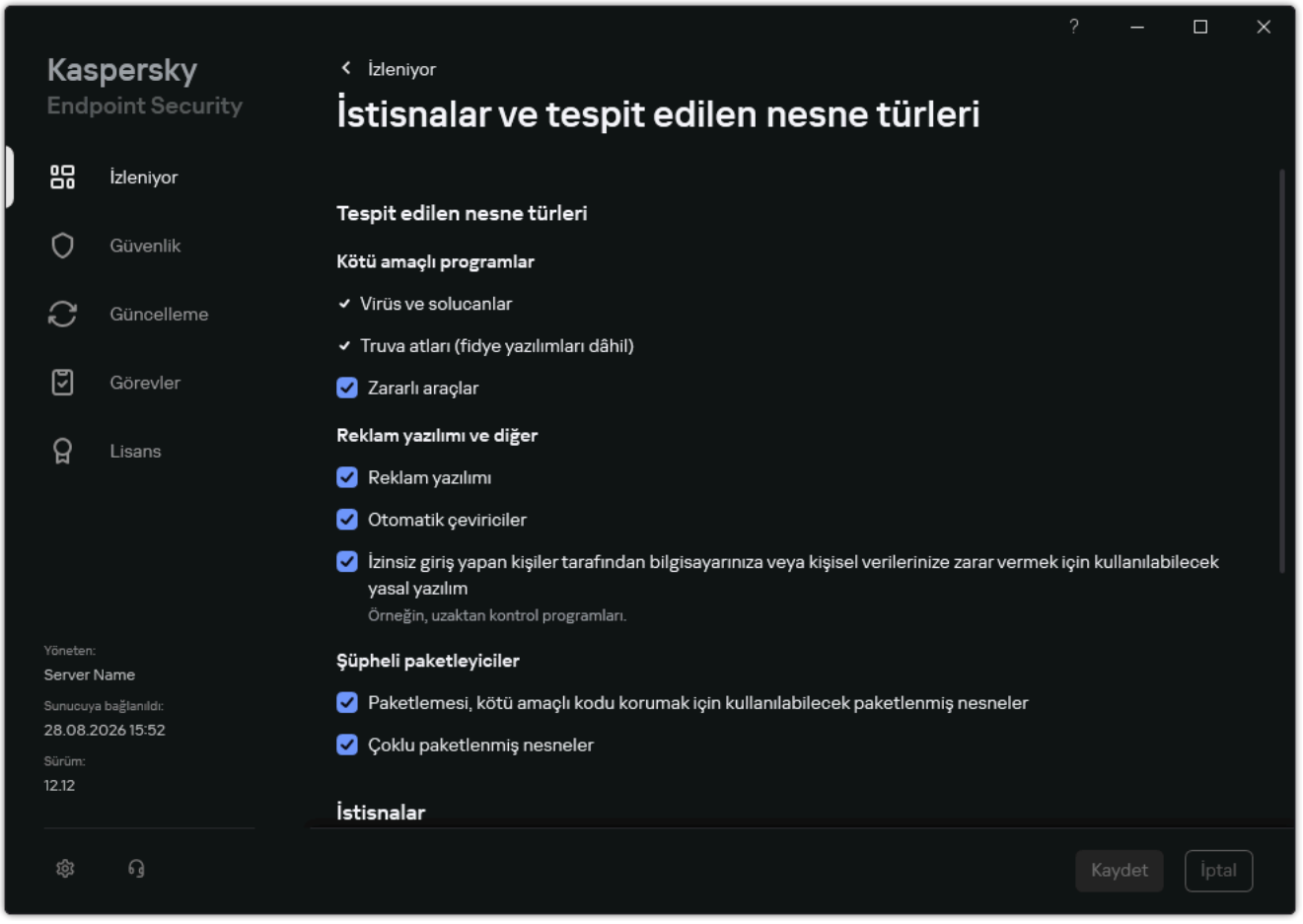
Web Console ve Cloud Console'da tespit edilebilir nesne türlerini seçme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Tespit Ayarları** bölümüne gidin.
5. **Diğer tür nesnelerin tespiti** bloğunda, Kaspersky Endpoint Security'nin tespit etmesini istediğiniz nesne türlerinin karşısındaki onay kutularını işaretleyin.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde algılanabilir nesne türlerini seçme

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
3. **Tespit edilen nesne türleri** bloğunda, Kaspersky Endpoint Security'nin tespit etmesini istediğiniz nesne türlerinin karşısındaki onay kutularını işaretleyin.
4. Değişikliklerinizi kaydedin.



Tespit edilen nesne türleri

Güvenilir uygulamalar listesini düzenleme

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 uygulama işlemi tarafından açılan, yürütülen veya kaydedilen nesneleri izler ve bunlar tarafından oluşturulan tüm uygulamaların ve ağ trafiğinin etkinliğini denetler. Bir uygulama güvenilir uygulamalar listesine eklendikten sonra, Kaspersky Endpoint Security uygulamanın etkinliğini izlemeyi durdurur.

Tarama istisnaları ve güvenilen uygulamalar arasındaki fark şudur: istisnalar için Kaspersky Endpoint Security'nin dosyaları taramaz, güvenilen uygulamalar için ise başlatılan işlemleri denetlemez. Güvenilir bir uygulama, tarama istisnalarına dahil olmayan bir klasörde zararlı bir dosya oluşturduğu takdirde, Kaspersky Endpoint Security dosyayı algılar ve tehdidi ortadan kaldırır. Klasör istisnalara eklenirse Kaspersky Endpoint Security bu dosyayı atlayacaktır.

Örneğin standart Microsoft Windows Not defteri uygulaması tarafından kullanılan nesnelerin güvenli olduğunu düşünüyorsanız yani bu uygulamaya güveniyorsanız Microsoft Windows Not Defteri'ni güvenilir uygulamaların listesine ekleyebilirsiniz, böylece bu uygulama tarafından kullanılan nesneler izlenmez. Bu, özellikle sunucu uygulamalarını kullanırken önemli olan bilgisayar performansını artıracaktır.

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.

Güvenilir uygulamalar, Kaspersky Endpoint Security ve diğer uygulamalar arasındaki uyumluluk sorunlarını önlemeye yardımcı olur (örneğin, üçüncü taraf bir bilgisayarın ağ trafiğinin Kaspersky Endpoint Security ve başka bir anti-virüs uygulaması tarafından iki kez taranması sorunu).

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.

Yönetim Konsolu'ndaki (MMC) güvenilir listeye bir uygulama nasıl eklenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Tarama istisnaları ve güvenilir uygulamalar** → **Güvenilir uygulamalar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, güvenilir uygulamaların listesini içeren bir pencere açar.
6. Şirketteki tüm bilgisayarlar için birleştirilmiş bir güvenilir uygulamalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki güvenilir uygulamalar listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki güvenilir uygulamalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin güvenilir uygulamalarının değiştirilmesi veya silinmesi mümkün değildir.

7. Kullanıcının yerel bir güvenilir uygulamalar listesi oluşturmasını sağlamak istiyorsanız, **Yerel güvenilir uygulamaların kullanımına izin ver** onay kutusunu seçin. Bu şekilde, bir kullanıcı, ilkede oluşturulan genel güvenilir uygulamalar listesine ek olarak kendi yerel güvenilir uygulamalar listesini de oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan güvenilir uygulamaların genel listesine erişebilir. Ayrıca, bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, uygulamanın kullanıcı arabirimindeki birleştirilmiş güvenilir uygulamalar listesini gizler.

8. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Güvenilir uygulamaları ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir güvenilir uygulama ekleyin.
   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir güvenilir uygulama ekler.
   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış güvenilir uygulamalar* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış güvenilir uygulamalar eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış güvenilir uygulamaları seçmelisiniz.
   - **Seçilen kategoriye yeni istisna**. Belirli bir kategoriye yeni bir güvenilir uygulama eklemek için bir kategori seçin.

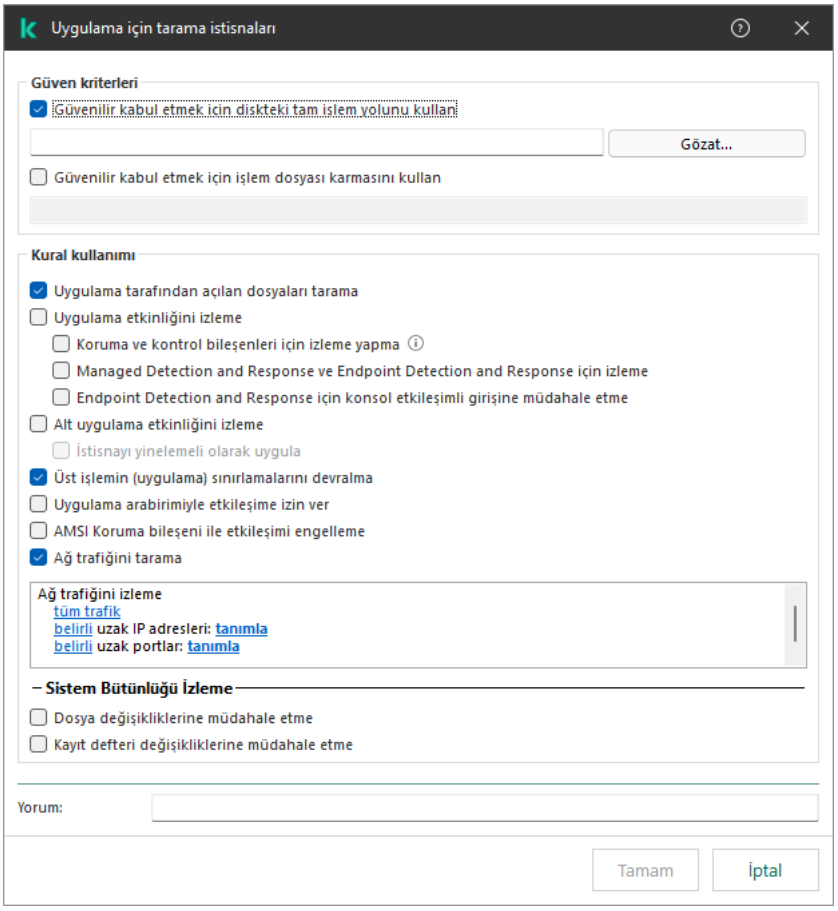
9. Güvenilirlik kriterlerini seçin:

   - **Güvenilir kabul etmek için diskteki tam işlem yolunu kullan**. Güvenilen uygulamanın yürütülebilir dosyasının yolunu girin.

     Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

     Kaspersky Endpoint Security, güvenilir bir uygulamanın dosya adını büyük/küçük harfe duyarlı olarak ele alır. Girdiğiniz dosya adının büyük/küçük harfleri yanlışsa Kaspersky Endpoint Security güvenilir uygulamayı tanımayacaktır.
   - **Güvenilir kabul etmek için işlem dosyası karmasını kullan**.

Kaspersky Endpoint Security, Kaspersky Security Center konsolunda bir güvenilir uygulamalar listesi oluştururken `%userprofile%` ortam değişkenini desteklemez. Girişi tüm kullanıcı hesaplarına uygulamak için * karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.



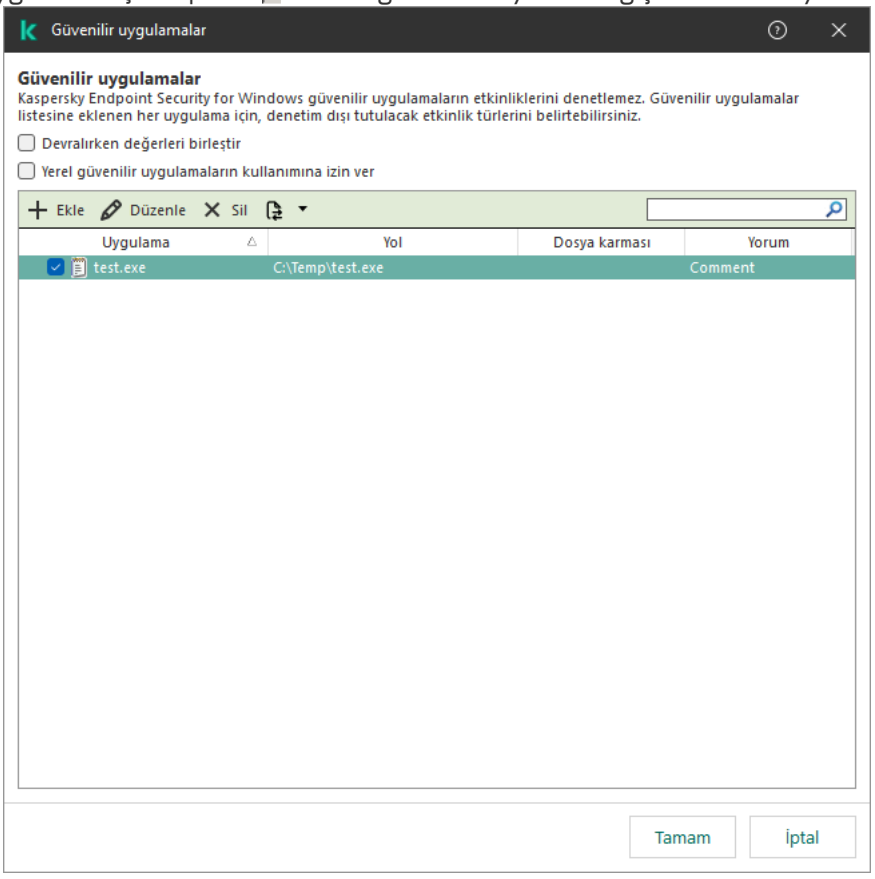
Güvenilir uygulama ayarları

10. Güvenilir uygulama için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

11. **Tamam**'a tıklayın.

    Yeni güvenilir uygulama listeye eklenecektir. Nesnenin yanındaki onay kutusunu kullanarak istediğiniz zaman bir uygulamayı güvenilir bölgeden hariç tutabilirsiniz.

12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.



Güvenilir uygulamaların listesi

Kaspersky Security Center Web Console'da bir uygulama güvenilir listeye nasıl eklenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenilir Bölge** bölümüne gidin.
5. Açılan pencerede **Uygulamalar** bağlantısına tıklayın.

   Bu, güvenilir uygulamaların listesini içeren bir pencere açar.
6. Şirketteki tüm bilgisayarlar için birleştirilmiş bir güvenilir uygulamalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki güvenilir uygulamalar listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki güvenilir uygulamalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin güvenilir uygulamalarının değiştirilmesi veya silinmesi mümkün değildir.
7. Kullanıcının yerel bir güvenilen uygulamalar listesi oluşturmasını sağlamak istiyorsanız **Yerel istisnaların kullanımına izin ver** onay kutusunu seçin. Bu şekilde, bir kullanıcı, ilkede oluşturulan genel güvenilir uygulamalar listesine ek olarak kendi yerel güvenilir uygulamalar listesini de oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan güvenilir uygulamaların genel listesine erişebilir. Ayrıca, bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, uygulamanın kullanıcı arabirimindeki birleştirilmiş güvenilir uygulamalar listesini gizler.

8. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Güvenilir uygulamaları ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir güvenilir uygulama ekleyin.
   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir güvenilir uygulama ekler.
   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış güvenilir uygulamalar* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış güvenilir uygulamalar eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış güvenilir uygulamaları seçmelisiniz.

   Belirli bir kategoriye yeni bir güvenilir uygulama eklemek için, o kategorinin yanındaki onay kutusunu seçin ve **Yeni istisna** seçeneğini seçin.

9. Güvenilirlik kriterlerini seçin:

   - **Dosya veya klasör yolu**. Güvenilen uygulamanın yürütülebilir dosyasının yolunu girin.

     Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

     Kaspersky Endpoint Security, güvenilir bir uygulamanın dosya adını büyük/küçük harfe duyarlı olarak ele alır. Girdiğiniz dosya adının büyük/küçük harfleri yanlışsa Kaspersky Endpoint Security güvenilir uygulamayı tanımayacaktır.

   - **Uygulama karması**.

   Kaspersky Endpoint Security, Kaspersky Security Center konsolunda güvenilen uygulamaların bir listesini oluştururken %userprofile% ortam değişkenini desteklemez. Girişi tüm kullanıcı hesaplarına uygulamak için `*` karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

10. Güvenilir uygulama için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

11. **Tamam**'a tıklayın.

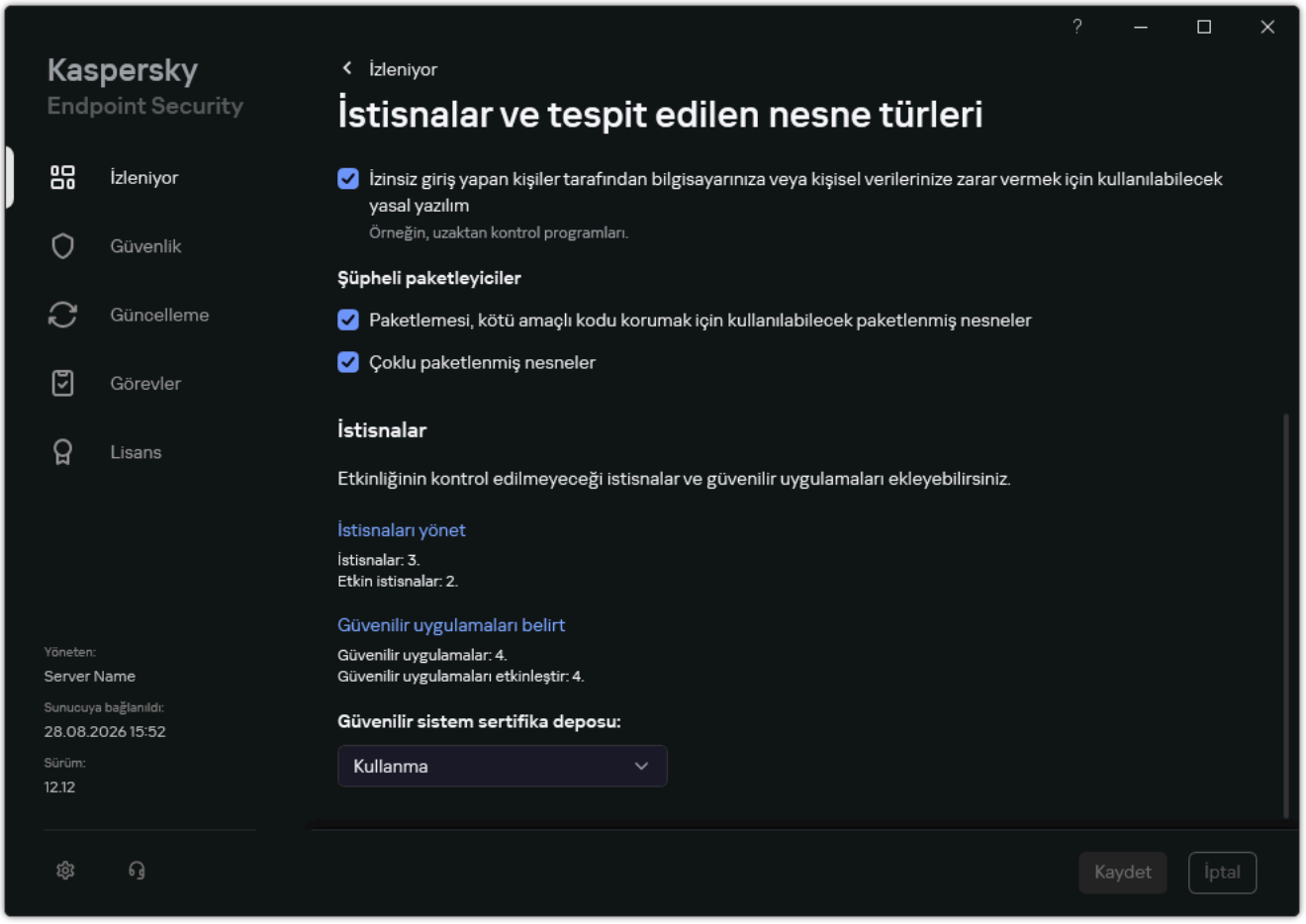
    Yeni güvenilir uygulama listeye eklenecektir. **Durum** sütunundaki onay kutusunu kullanarak istediğiniz zaman bir uygulamayı güvenilir bölgenin dışında bırakabilirsiniz.

12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabirimindeki güvenilenler listesine bir uygulama nasıl eklenir

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
3. **İstisnalar** bloğunda, **Güvenilir uygulamaları belirt** bağlantısına tıklayın.

Kaspersky Endpoint Security, güvenilir uygulamaların yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel güvenilir uygulamalar yasaklanmışsa (**Yerel güvenilir uygulamaların kullanımına izin ver** onay kutusunun işareti kaldırılmışsa), uygulamanın kullanıcı arabirimindeki birleştirilmiş güvenilir uygulamalar listesini gizler.



İstisna ayarları

4. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Güvenilir uygulamaları ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir güvenilir uygulama ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir güvenilir uygulama ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış güvenilir uygulamalar* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış güvenilir uygulamalar eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış güvenilir uygulamaları seçmelisiniz.

   Belirli bir kategoriye yeni bir güvenilir uygulama eklemek için, o kategorinin yanındaki onay kutusunu seçin ve **Yeni istisna** seçeneğini seçin.

5. Güvenilirlik kriterlerini seçin:

   - **Güvenilir kabul etmek için diskteki tam işlem yolunu kullan**. Güvenilen uygulamanın yürütülebilir dosyasının yolunu girin.

     Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

Kaspersky Endpoint Security, güvenilir bir uygulamanın dosya adını büyük/küçük harfe duyarlı olarak ele alır. Girdiğiniz dosya adının büyük/küçük harfleri yanlışsa Kaspersky Endpoint Security güvenilir uygulamayı tanımayacaktır.

- **Güvenilir kabul etmek için işlem dosyası karmasını kullan**.

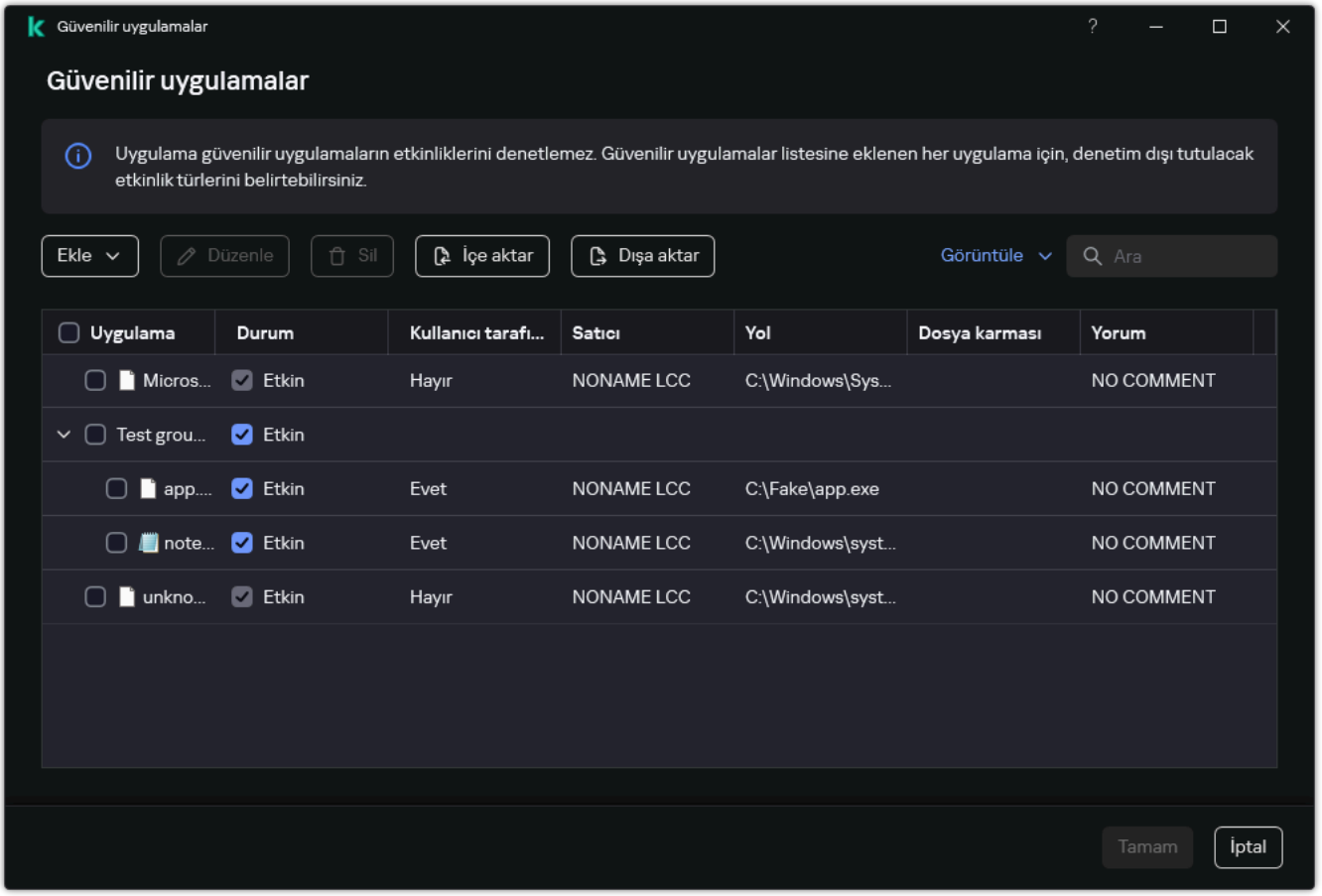
Kaspersky Endpoint Security, ortam değişkenlerini destekler ve uygulamanın yerel arabirimindeki yolu dönüştürür. Başka bir deyişle, `%userprofile%\Documents\File.exe` dosya yolunu girdiğinizde, uygulamanın yerel arabirimineFred123 kullanıcısı için bir `C:\Users\Fred123\Documents\File.exe` kaydı eklenir. Buna göre, Kaspersky Endpoint Security diğer kullanıcılar için `File.exe` güvenilir programını yoksayar. Girişi tüm kullanıcı hesaplarına uygulamak için `*` karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

6. Güvenilir uygulama özellikleri penceresinde, gelişmiş ayarları yapılandırın.

7. **Tamam**'a tıklayın.

   Yeni güvenilir uygulama listeye eklenecektir. **Durum** sütunundaki onay kutusunu kullanarak istediğiniz zaman bir uygulamayı güvenilir bölgenin dışında bırakabilirsiniz.

8. Değişikliklerinizi kaydedin.



Güvenilir uygulamaların listesi

Parametre	Açıklama
Uygulama tarafından açılan dosyaları tarama	Uygulama tarafından açılan tüm dosyalar Kaspersky Endpoint Security tarafından taramaların dışında tutulur. Örneğin, dosyaları yedeklemek için uygulamalar kullanıyorsanız, bu özellik Kaspersky Endpoint Security tarafından tüketilen kaynağın azaltılmasına yardımcı olur.
Uygulama etkinliğini izleme	Kaspersky Endpoint Security, uygulamanın işletim sistemindeki dosya ve ağ etkinliğini izlemez. Kaspersky Endpoint Security'nin farklı bileşenleri için uygulama etkinliği izlemeyi yapılandırabilirsiniz: • **Koruma ve kontrol bileşenleri için izleme yapma**. Uygulama etkinliği aşağıdaki bileşenler tarafından izlenir: Davranış Tespiti, Exploit Önleme, Sunucu Yetkisiz Erişim Önleme, Düzeltme Altyapısı ve Güvenlik Duvarı. • **Managed Detection and Response ve Endpoint Detection and Response için izleme**. Uygulama etkinliği yerleşik MDR aracısı ve yerleşik EDR (KATA) aracısı tarafından izlenir. • **Endpoint Detection and Response için konsol etkileşimli girişine müdahale etme**. Kaspersky Endpoint Security, konsolda uygulamanın yönetilmesiyle ilgili telemetri verileri göndermez. Telemetri verileri Kaspersky Anti Targeted Attack Platform (EDR) tarafından kullanılır.
Alt uygulama etkinliğini izleme	Kaspersky Endpoint Security, bu uygulama tarafından başlatılan uygulamaların dosya veya ağ etkinliklerini izlemez. İstisnayı yinelemeli olarak uygulayabilirsiniz. Böylece uygulama, tüm alt uygulama zincirinin etkinliklerini izlemez.
Üst işlemin (uygulama) sınırlamalarını devralma	Üst işlem için yapılandırılan kısıtlamalar Kaspersky Endpoint Security tarafından bir alt işleme uygulanmayacaktır. Üst işlem, kendisi için uygulama haklarının (Sunucu Yetkisiz Erişim Önleme) ve uygulama ağ kurallarının (Güvenlik Duvarı) yapılandırıldığı bir uygulama tarafından başlatılır.
Alt uygulama etkinliğini izleme	Kaspersky Endpoint Security, bu uygulama tarafından başlatılan uygulamaların dosya veya ağ etkinliklerini izlemez. İstisnayı yinelemeli olarak uygulayabilirsiniz. Böylece uygulama, tüm alt uygulama zincirinin etkinliklerini izlemez.
Uygulama arabirimiyle etkileşime izin ver	Kaspersky Endpoint Security Self-Defense, uzak bir bilgisayardan uygulama hizmetlerini yönetmeye yönelik tüm girişimleri engeller. Onay kutusu işaretlenirse uzaktan erişim uygulamasının Kaspersky Endpoint Security arabirimi aracılığıyla Kaspersky Endpoint Security ayarlarını yönetmesine izin verilir.
AMSI Koruma bileşeni ile etkileşimi engelleme	Kaspersky Endpoint Security, güvenilir uygulamanın AMSI Protection bileşeni tarafından taranacak nesnelere yönelik isteklerini izlemez.
Ağ trafiğini tarama	Uygulama tarafından başlatılan ağ trafiği, Kaspersky Endpoint Security tarafından taramaların dışında bırakılacaktır. Taramalardan ya tüm trafiği ya da yalnızca şifrelenmiş trafiği hariç tutabilirsiniz. Ayrı ayrı IP adreslerini ve port numaralarını da taramalardan hariç tutabilirsiniz. Kaspersky Endpoint Security 14.0 veya önceki sürümleri, güvenilir bir uygulama için yol yerine karma belirtildiğinde ağ trafiğinin hariç tutulmasını desteklemez.
Dosya değişikliklerine müdahale etme *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Kaspersky Endpoint Security, Sistem Bütünlüğü İzleme izleme kapsamındaki dosyalardaki değişiklikleri izlemez. Uygulama, istisna'yı tüm Sistem Bütünlüğü İzleme modlarına uygular: Gerçek Zamanlı Sistem Bütünlüğü İzleme ve İsteğe Bağlı Sistem Bütünlük Denetimi.
Kayıt defteri değişikliklerine müdahale etme *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Kaspersky Endpoint Security, Sistem Bütünlüğü İzleme izleme kapsamındaki kayıt defreti anahtarlarındaki değişiklikleri izlemez. Uygulama, istisna'yı tüm Sistem Bütünlüğü İzleme modlarına uygular: Gerçek Zamanlı Sistem Bütünlüğü İzleme ve İsteğe Bağlı Sistem Bütünlük Denetimi.
Yorum	Gerekirse, güvenilir uygulama için kısa bir yorum yazabilirsiniz. Yorumlar, güvenilir uygulamalar için aramayı ve sıralamayı basitleştirmeye yardımcı olur.
Durum	Güvenilir uygulamanın durumu: • **Etkin** durumu, uygulamanın güvenilir bölgede olduğu anlamına gelir. • **Etkin değil** durumu, uygulamanın güvenilir bölgenin dışında olduğu anlamına gelir.

Yerel bir güvenilir bölge oluşturma

Kullanıcı artık belirli bir bilgisayar için kendi yerel güvenilir bölgesini oluşturabilir. Bu şekilde, kullanıcı bir ilkedeki genel güvenilir bölgeye ek olarak kendi yerel istisnalar ve güvenilir uygulamalar listelerini oluşturabilir. Bir yönetici, ilke ayarlarında yerel istisnaların veya yerel güvenilir uygulamaların kullanımına izin verebilir veya bunları engelleyebilir. Bunu yapmak için ilkenin **İstisnalar** bölümündeki **Yerel istisnaların kullanılmasına izin ver** ve **Yerel güvenilir uygulamaların kullanımına izin ver** onay kutularını kullanın.

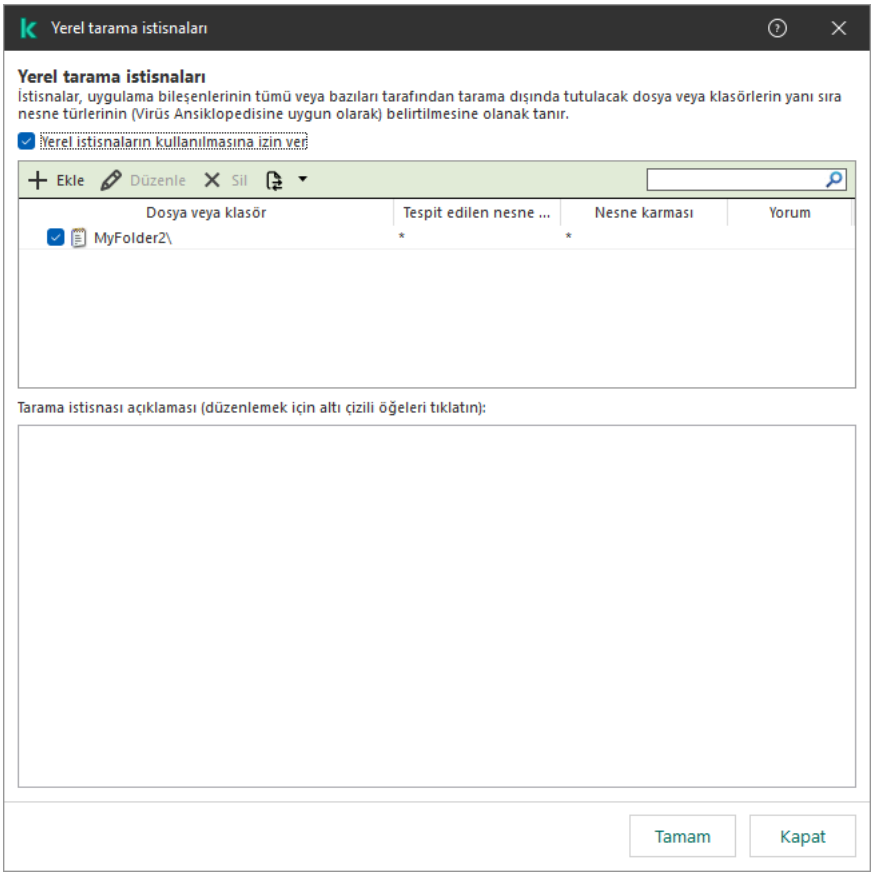
Bir yönetici tarafından yerel bir güvenilir bölge oluşturulmasına izin verilirse, kullanıcı uygulamanın kullanıcı arabiriminde kendi tarama istisnalarını ve güvenilir uygulamalarını ekleyebilir. Aynı zamanda, kullanıcının ilkede yapılandırılan güvenilen bölgedeki nesneleri değiştirme veya silme izinleri yoktur. Yönetici, tek bir bilgisayar için istisnaların eklenmesi gerekiyorsa Kaspersky Security Center konsolundaki liste öğelerini de görüntüleyebilir, ekleyebilir, değiştirebilir veya silebilir.

Kaspersky Endpoint Security, güvenilir bölgenin yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel tarama istisnaları ve güvenilir uygulamalar yasaklanmışsa, uygulamanın kullanıcı arabiriminde tarama istisnaları ve güvenilir uygulamalar listelerini gizler.

Yönetim Konsolu'nda (MMC) yerel güvenilir bölgeye nesne ekleme

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, **Cihazlar** sekmesini seçin.
4. İlke özellikleri penceresini açmak için çift tıklayın.
5. Bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
6. Bilgisayarda yüklü Kaspersky uygulamaları listesinde **Kaspersky Endpoint Security for Windows (14.2)** öğesini seçin ve çift tıklayarak uygulama özelliklerini açın.
7. Uygulama ayarları penceresinde, **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
8. **Tarama istisnaları ve güvenilir uygulamalar** → **Yerel tarama istisnaları** bloğunda, **Ayarlar** düğmesine tıklayın.

Bu, yerel istisnaların listesini içeren bir pencere açar.



Güvenilir bölge ayarları

9. Yerel tarama istisnalarının bir listesini yapın.

   Yerel tarama istisnaları oluşturma kuralları genel istisnalarla aynıdır. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

10. **Tarama istisnaları ve güvenilir uygulamalar** → **Yerel güvenilir uygulamalar** bloğunda, **Ayarlar** düğmesine tıklayın.

    Bu, yerel güvenilir uygulamaların listesini içeren bir pencere açar.

11. Yerel güvenilir uygulamaların bir listesini yapın.

    Uygulamaları yerel güvenilir uygulamalar listesine ekleme kuralları, genel listeye ekleme kurallarıyla aynıdır. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

12. Değişikliklerinizi kaydedin.

Kaspersky Security Center Web Console'da yerel güvenilen bölgeye nesne ekleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Bir kullanıcının engellenen bir eylemi gerçekleştirmesine izin vermek istediğiniz bilgisayarın adına tıklayın.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows**'a tıklayın.

   Bu, yerel uygulama ayarlarını açar.

5. **Uygulama ayarları** sekmesini seçin.

6. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
7. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Yerel tarama istisnaları** düğmesine tıklayın.
8. Yerel tarama istisnalarının bir listesini yapın.

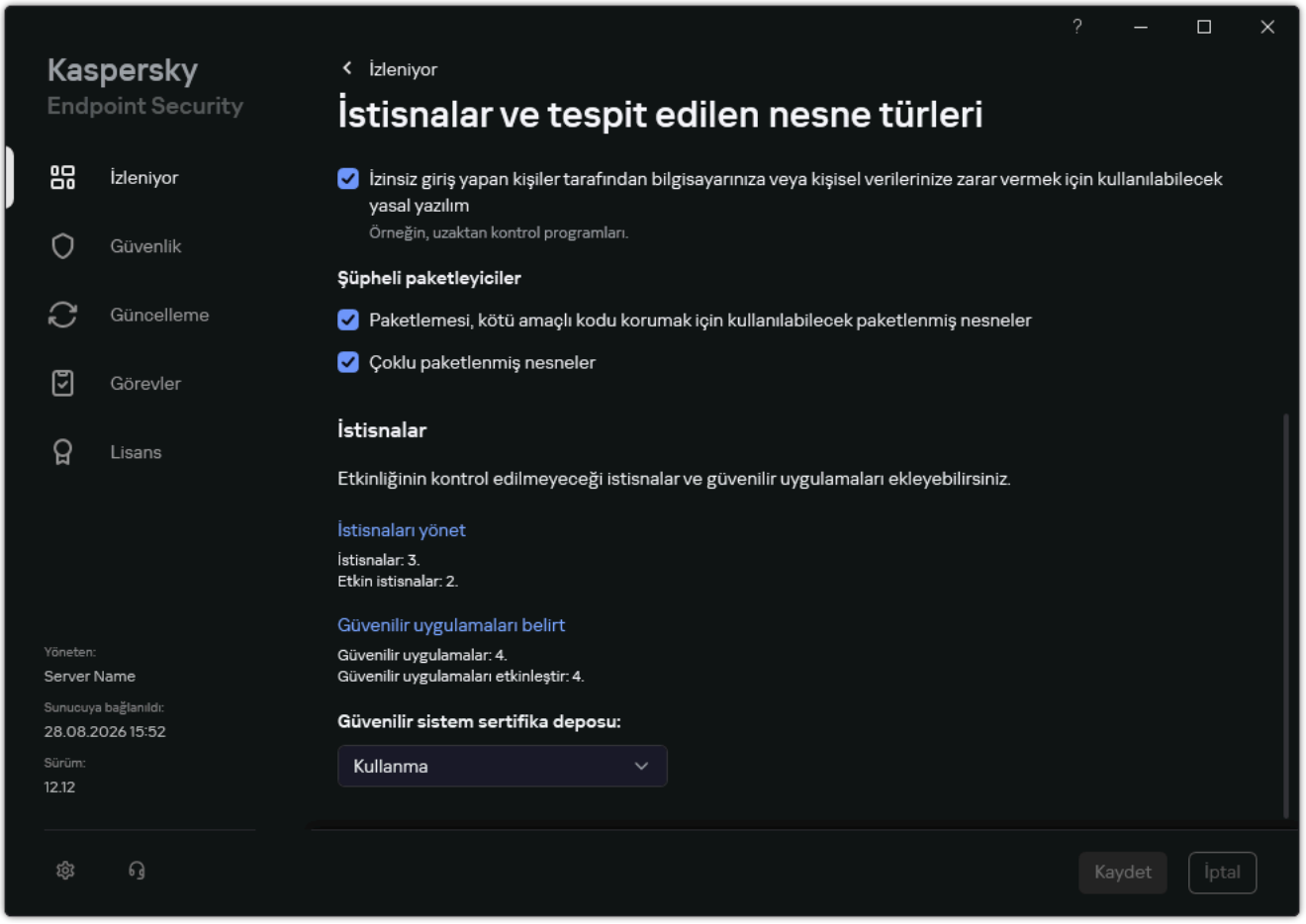
   Yerel istisnaların oluşturulmasına ilişkin kurallar genel istisnaların oluşturulmasına ilişkin kurallar ile aynıdır. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
9. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Yerel güvenilir uygulamalar** düğmesine tıklayın.
10. Yerel güvenilir uygulamaların bir listesini yapın.

    Uygulamaları yerel güvenilir uygulamalar listesine ekleme kuralları, genel listeye ekleme kurallarıyla aynıdır. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
11. Değişikliklerinizi kaydedin.

Uygulama arabiriminde yerel tarama istisnası nasıl oluşturulur

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
3. **İstisnalar** bloğunda, **İstisnaları yönet** bağlantısını tıklayın.

Kaspersky Endpoint Security, tarama istisnalarının yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel tarama istisnaları yasaklanmışsa (**Yerel istisnaların kullanılmasına izin ver** onay kutusunun işareti kaldırılmışsa) uygulamanın kullanıcı arabirimindeki tarama istisnaları listesini gizler.



İstisna ayarları

4. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Tarama istisnalarını ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir tarama istisnası ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir tarama istisnası ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış tarama istisnalarını* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış tarama istisnaları eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış tarama istisnalarını seçmelisiniz.

   Belirli bir kategoriye yeni bir tarama istisnası eklemek için, o kategorinin yanındaki onay kutusunu seçin ve **Yeni istisna** seçeneğini seçin.

5. Bir dosyayı veya klasörü taramaların dışında tutmak istiyorsanız, **Gözat** düğmesini tıklayarak dosyayı veya klasörü seçin.

Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler:

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

- İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

  Maskeleri dosya yolunun başında, ortasında veya sonunda kullanabilirsiniz. Örneğin, istisnalara tüm kullanıcılar için bir klasör eklemek istiyorsanız `?:\Users\*\Folder\` maskesini girin.

  Ağ klasörlerini hariç tutabilirsiniz. Bunu yapmak için ağ klasörünün yolunu manuel olarak girin (örneğin, `\\Network Share\*`).

6. Eğer taramalardan nesnenin belirli türünü dışlamak istiyorsanız, **Tespit edilen nesne türü** alanında Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Email-Worm`, `Rootkit` veya `RemoteAdmin`).

   Maskeleri `?` karakteri (herhangi bir tek karakteri değiştirir) ve `*` karakteri ile (herhangi bir sayıda karakteri değiştirir) kullanabilirsiniz. Örneğin, `Client*` maskesi belirtilirse, Kaspersky Endpoint Security, `Client-IRC`, `Client-P2P` ve `Client-SMTP` nesnelerini taramaların dışında tutar.

7. Tek bir dosyayı taramaların dışında tutmak istiyorsanız, **Nesne karması** alanına dosya karma değerini girin.

   Dosya değiştirilirse, dosya karması da değiştirilecektir. Böyle bir durumda, değiştirilen dosya istisnalara eklenmeyecektir.

8. **Koruma bileşenleri** bloğunda, tarama istisnasının uygulanmasını istediğiniz bileşenleri seçin.

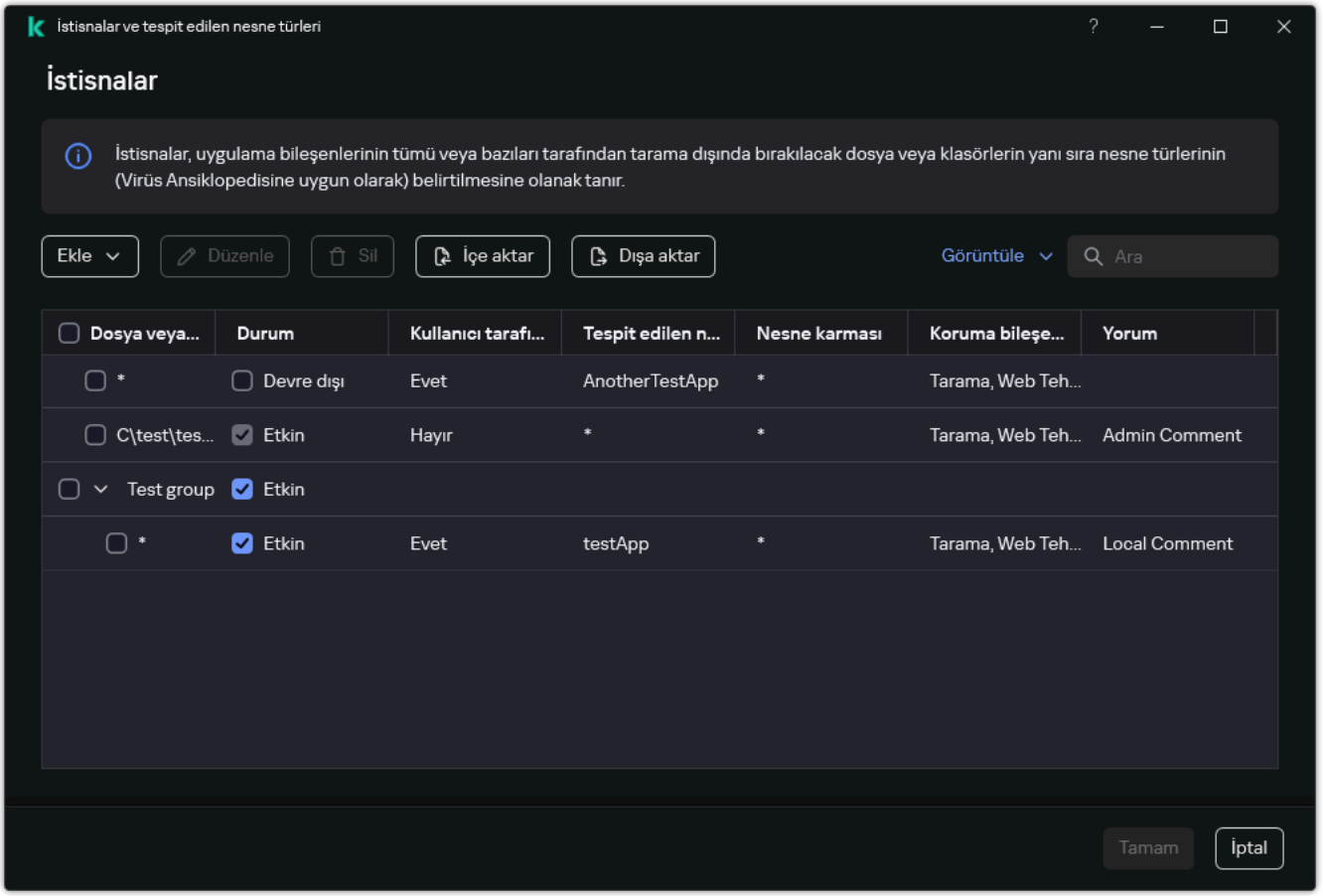
9. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

10. İstisna için **Etkin** durumu seçin.

11. **Ekle**'ye tıklayın.

    Yeni istisna listeye eklenecektir. **Durum** sütunundaki onay kutusunu kullanarak istediğiniz zaman istisnayı devre dışı bırakabilirsiniz.

12. Değişikliklerinizi kaydedin.

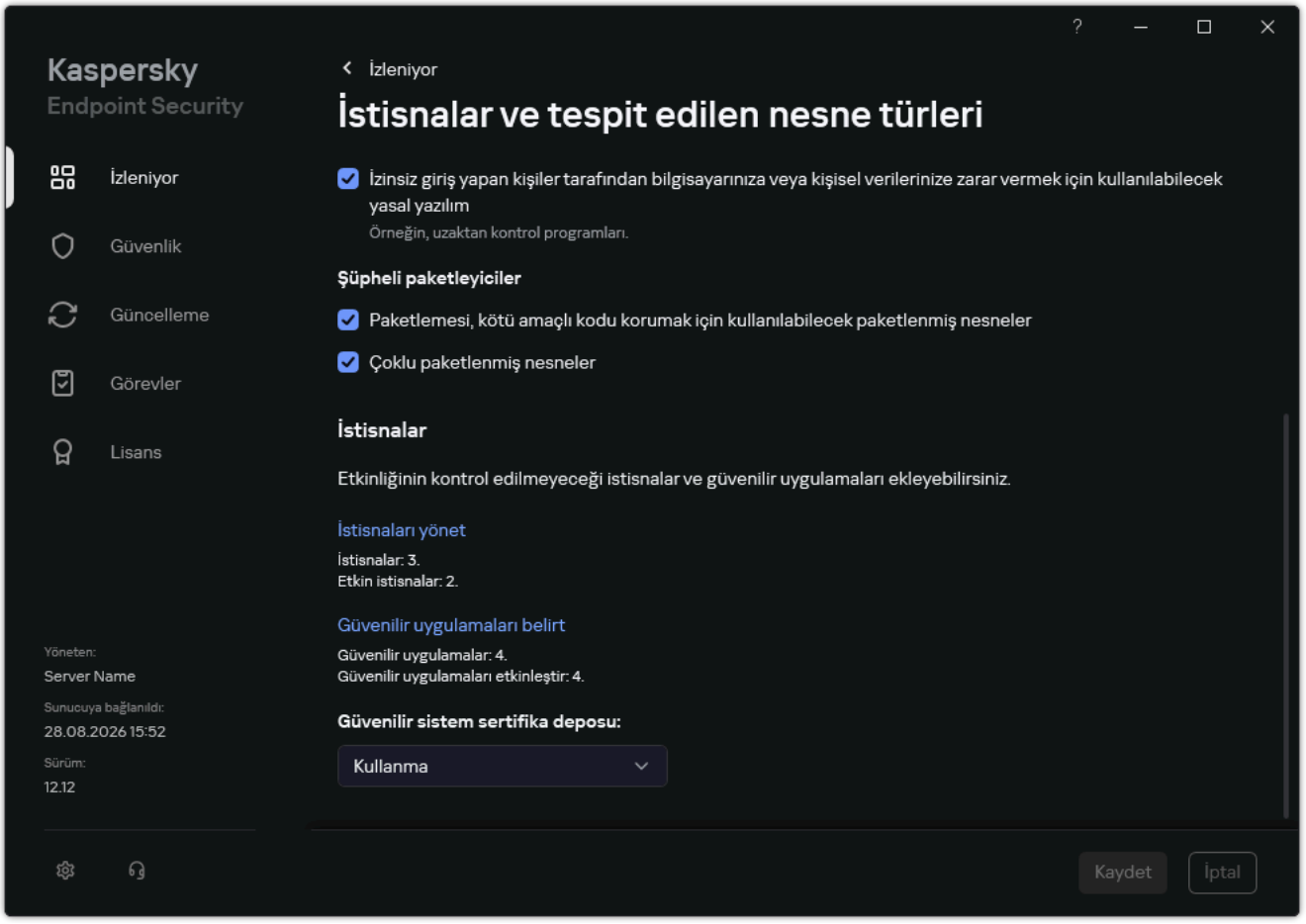


İstisnalar listesi

Uygulama arabirimindeki yerel güvenilen uygulamalar listesine bir uygulama ekleme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
3. **İstisnalar** bloğunda, **Güvenilir uygulamaları belirt** bağlantısına tıklayın.

Kaspersky Endpoint Security, güvenilir uygulamaların yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel güvenilir uygulamalar yasaklanmışsa (**Yerel güvenilir uygulamaların kullanımına izin ver** onay kutusunun işareti kaldırılmışsa), uygulamanın kullanıcı arabirimindeki birleştirilmiş güvenilir uygulamalar listesini gizler.



İstisna ayarları

4. **Ekle**'ye tıklayın ve bir eylem seçin:

   - **Kategori**. Güvenilir uygulamaları ayrı kategoriler halinde gruplayabilirsiniz. Yeni bir kategori oluşturmak için kategorinin adını girin ve kategoriye en az bir güvenilir uygulama ekleyin.

   - **Yeni istisna**. Kaspersky Endpoint Security, listenin köküne yeni bir güvenilir uygulama ekler.

   - **Listeden istisna seçin**. Kaspersky Endpoint Security'yi SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızlı bir şekilde yapılandırmak için uygulama *önceden tanımlanmış güvenilir uygulamalar* içerir. Ayrıca Citrix ve VMware sanal ortamlarında uygulama kurulumunu desteklemek için önceden tanımlanmış güvenilir uygulamalar eklenmiştir. Korunan sunucunun amacına bağlı olarak önceden tanımlanmış güvenilir uygulamaları seçmelisiniz.

   Belirli bir kategoriye yeni bir güvenilir uygulama eklemek için, o kategorinin yanındaki onay kutusunu seçin ve **Yeni istisna** seçeneğini seçin.

5. Güvenilirlik kriterlerini seçin:

   - **Güvenilir kabul etmek için diskteki tam işlem yolunu kullan**. Güvenilen uygulamanın yürütülebilir dosyasının yolunu girin.

     Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

Kaspersky Endpoint Security, güvenilir bir uygulamanın dosya adını büyük/küçük harfe duyarlı olarak ele alır. Girdiğiniz dosya adının büyük/küçük harfleri yanlışsa Kaspersky Endpoint Security güvenilir uygulamayı tanımayacaktır.

- **Güvenilir kabul etmek için işlem dosyası karmasını kullan**.

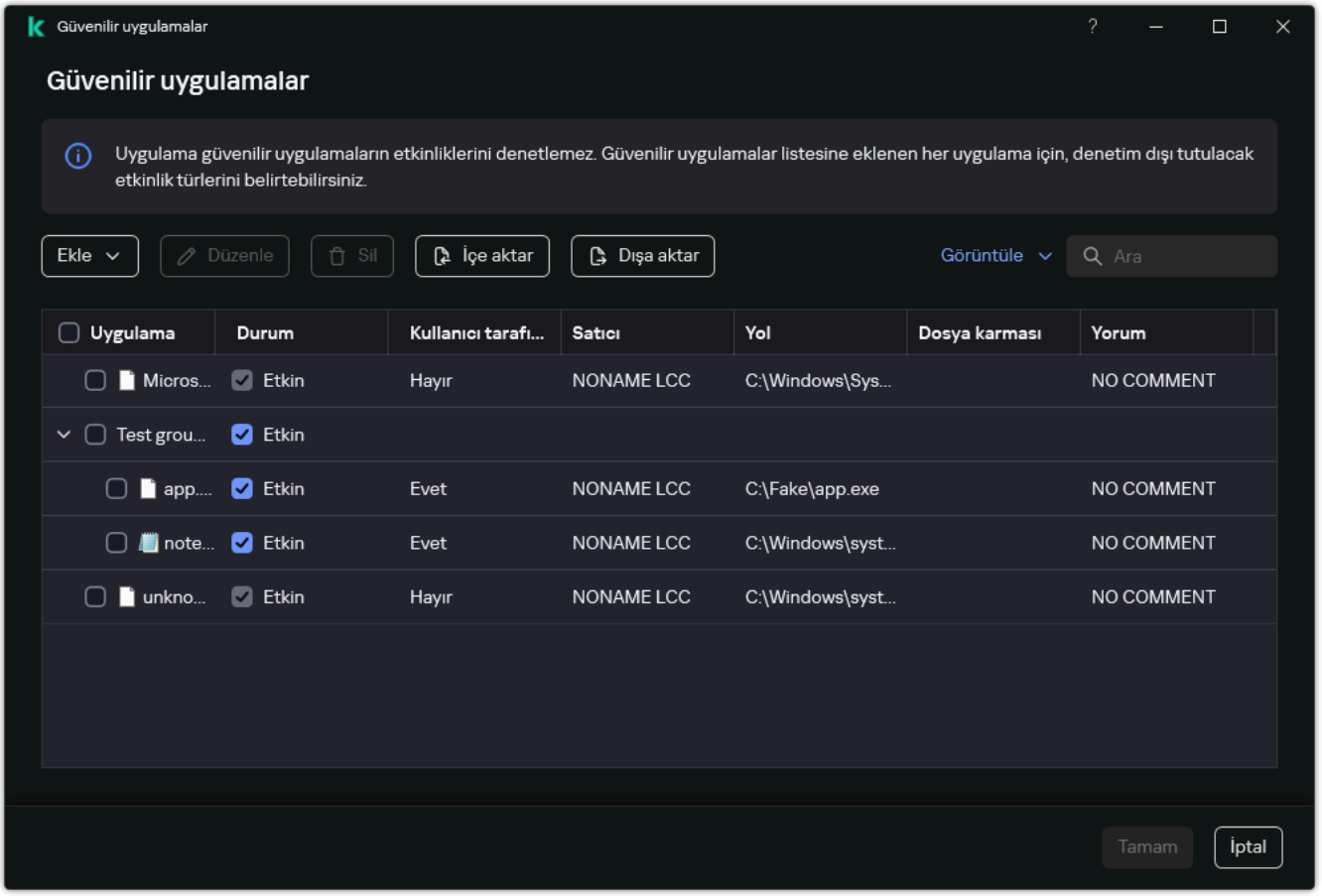
Kaspersky Endpoint Security, ortam değişkenlerini destekler ve uygulamanın yerel arabirimindeki yolu dönüştürür. Başka bir deyişle, `%userprofile%\Documents\File.exe` dosya yolunu girdiğinizde, uygulamanın yerel arabirimineFred123 kullanıcısı için bir `C:\Users\Fred123\Documents\File.exe` kaydı eklenir. Buna göre, Kaspersky Endpoint Security diğer kullanıcılar için `File.exe` güvenilir programını yoksayar. Girişi tüm kullanıcı hesaplarına uygulamak için `*` karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

6. Güvenilir uygulama özellikleri penceresinde, gelişmiş ayarları yapılandırın.

7. **Tamam**'a tıklayın.

   Yeni güvenilir uygulama listeye eklenecektir. **Durum** sütunundaki onay kutusunu kullanarak istediğiniz zaman bir uygulamayı güvenilir bölgenin dışında bırakabilirsiniz.

8. Değişikliklerinizi kaydedin.



Güvenilir uygulamaların listesi

Güvenilir bölge listesini dışa ve içe aktarma

Güvenilir bölge, Kaspersky Endpoint Security'nin etkin olduğunda izlemediği nesnelerin ve uygulamaların sistem yöneticisi tarafından yapılandırılan listesidir. Güvenilir bölge şu listelerden oluşur: *tarama istisnaları* ve *güvenilir uygulamalar*. Bu listeleri XML dosyalarına ve diğer biçimlere aktarabilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda dışlama eklemek için dosyayı değiştirebilirsiniz. İstisnalar listesini ve güvenilir uygulamalar listesini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

Uygulama, *istisnalar listesini* dışa ve içe aktarmak için şu biçimleri kullanır:

- XML, Yönetim Konsolu (MMC), Web Console ve Cloud Console'da mevcuttur.
- DAT, yalnızca Yönetim Konsolu'nda (MMC) içe aktarma için kullanılabilir. Bu biçimin amacı, uygulamanın eski sürümleriyle uyumluluğu korumaktır. İstisna listelerini Web Console'a taşımak için Yönetim Konsolu'nda (MMC) bir DAT dosyasını XML'e dönüştürebilirsiniz.
- CSV yalnızca uygulamanın yerel arabiriminde kullanılabilir.

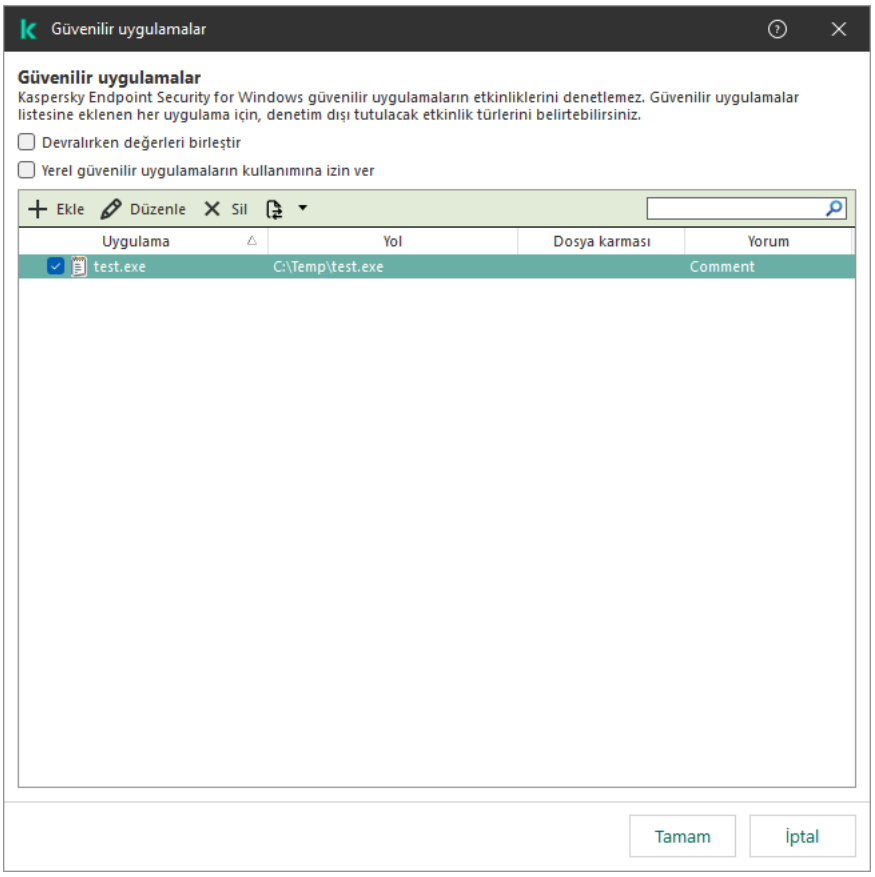
Kaspersky Endpoint Security, *güvenilir uygulamalar listesini* dışa ve içe aktarmak için XML biçimini kullanır.

Yönetim Konsolu'nda (MMC) güvenilir bölge nasıl dışarı ve içeri aktarılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
4. **Tarama istisnaları ve güvenilir uygulamalar** altında, dışarı veya içeri aktarmak istediğiniz güvenilen bölge bileşenini seçin: **Tarama istisnaları** veya **Güvenilir uygulamalar**.
5. **Ayarlar**'a tıklayın.
6. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
      Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.
   b. → **Dışa aktar** düğmesine tıklayın.
   c. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

d. Dosyaya kaydet.

Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır. Kaspersky Endpoint Security, istisnalar listesinin bir DAT dosyasına aktarılmasını da destekler.



Güvenilir uygulamaların listesi

7. İstisnalar listesini içe aktarmak için:

a. → **İçe aktar** düğmesine tıklayın.

b. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

c. Dosyayı aç.

Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler. Kaspersky Endpoint Security, bir DAT dosyasından istisnalar listesinin içe aktarılmasını da destekler.

8. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da güvenilir bölge nasıl dışa veya içe aktarılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenilir Bölge** bölümüne gidin.

5. Kurallar listesini dışa aktarmak için:

   a. **Kötü Amaçlı Yazılım Taraması** istisnaları bağlantısına tıklayın.

   b. Dışa aktarmak istediğiniz istisnaları seçin.

   c. → **Dışa aktar** düğmesine tıklayın.

      Kaspersky Endpoint Security, istisnalar listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

6. Güvenilir uygulamalar listesini dışa aktarmak için:

   a. Dışa aktarmak istediğiniz güvenilir uygulamaları seçin.

   b. → **Dışa aktar** düğmesine tıklayın.

      Kaspersky Endpoint Security, güvenilen uygulamaların listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.

7. İstisnalar listesini içe aktarmak için:

   a. **Kötü Amaçlı Yazılım Taraması** istisnaları bağlantısına tıklayın.

   b. → **İçe aktar** düğmesine tıklayın.

      Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.

   c. Dosyayı aç.

      Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

8. Güvenilir uygulamaların bir listesini içe aktarmak için:

   a. **Uygulamalar** bağlantısına tıklayın.

   b. → **İçe aktar** düğmesine tıklayın.

      Açılan pencerede, güvenilir uygulamalar listesini almak istediğiniz JSON dosyasını seçin.

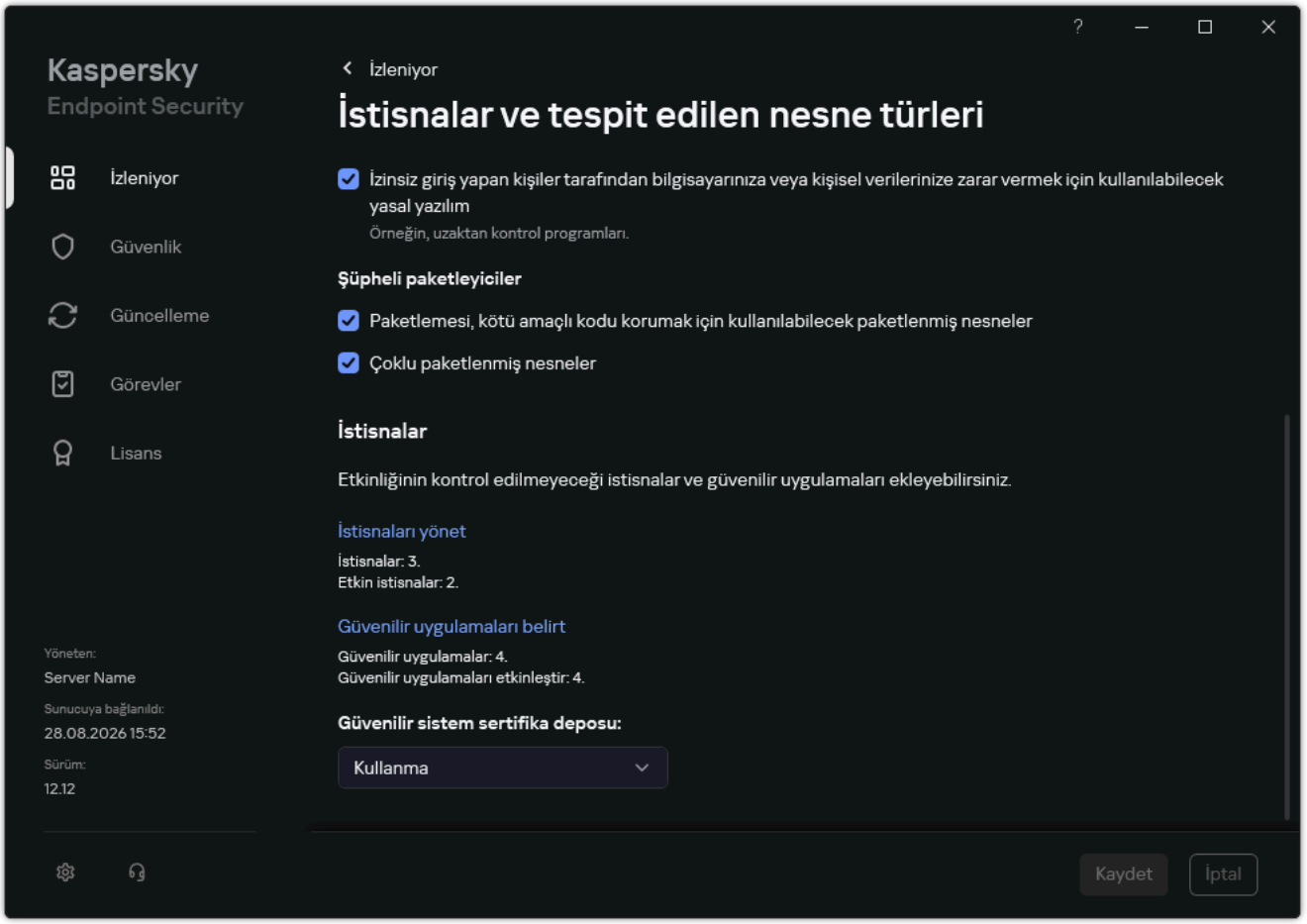
   c. Dosyayı aç.

      Bilgisayar zaten bir güvenilir uygulamalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.

9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde güvenilir bölge nasıl dışa veya içe aktarılır

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.

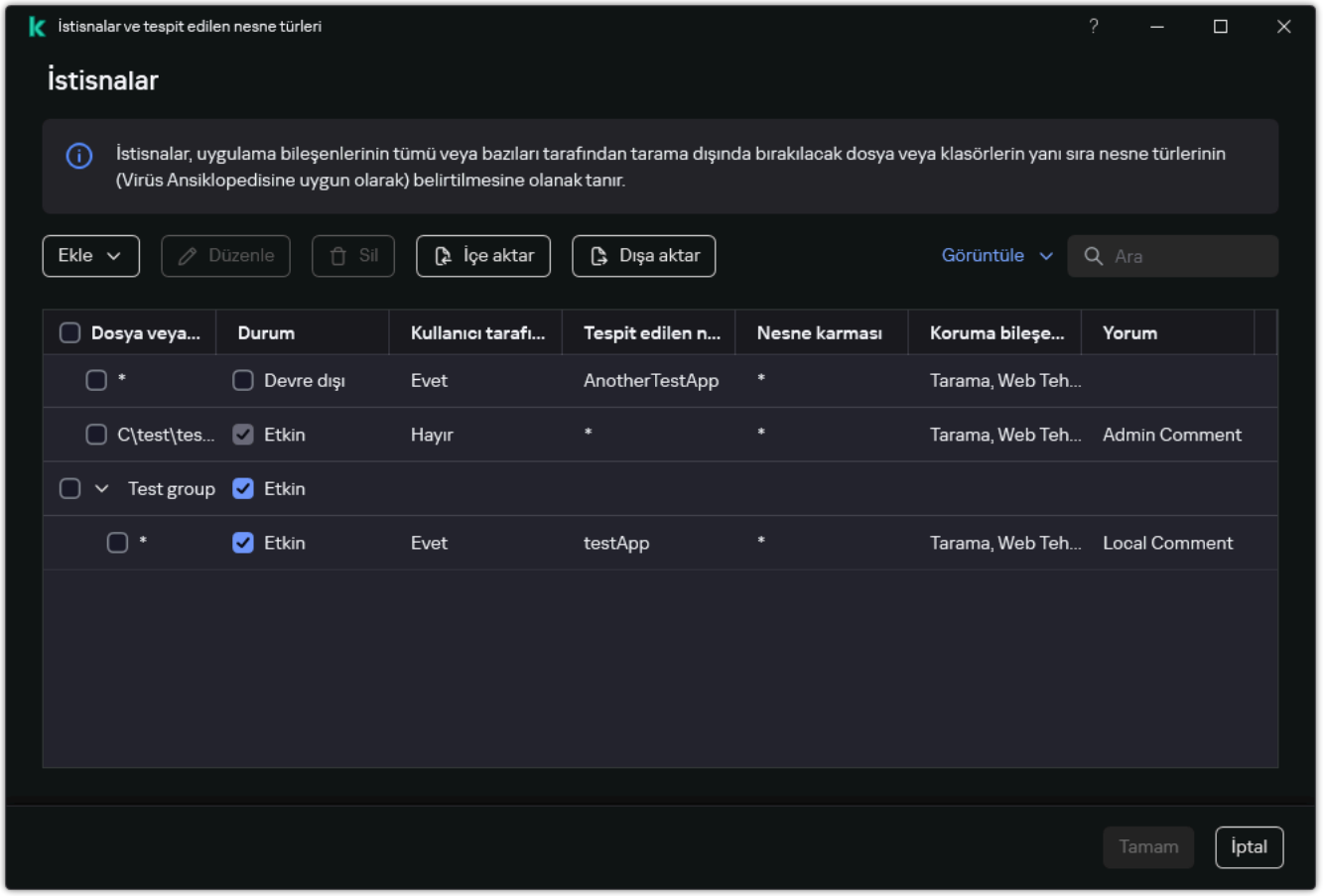


İstisna ayarları

3. Kurallar listesini dışa aktarmak için:
   a. **İstisnalar** bloğunda, **İstisnaları yönet** bağlantısını tıklayın.
   b. Dışa aktarmak istediğiniz istisnaları seçin.
   c. **Dışa aktar**'a tıklayın.
   d. Yalnızca seçili istisnaları veya tüm istisnalar listesini dışa aktarmak istediğinizi onaylayın.
   e. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz CSV dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

f. Dosyaya kaydet.

Kaspersky Endpoint Security, istisnalar listesinin tamamını CSV dosyasına aktarır.



İstisnalar listesi

4. Güvenilir uygulamalar listesini dışa aktarmak için:

a. **İstisnalar** bloğunda, **Güvenilir uygulamaları belirt** bağlantısına tıklayın.

b. Dışa aktarmak istediğiniz güvenilir uygulamaları seçin.

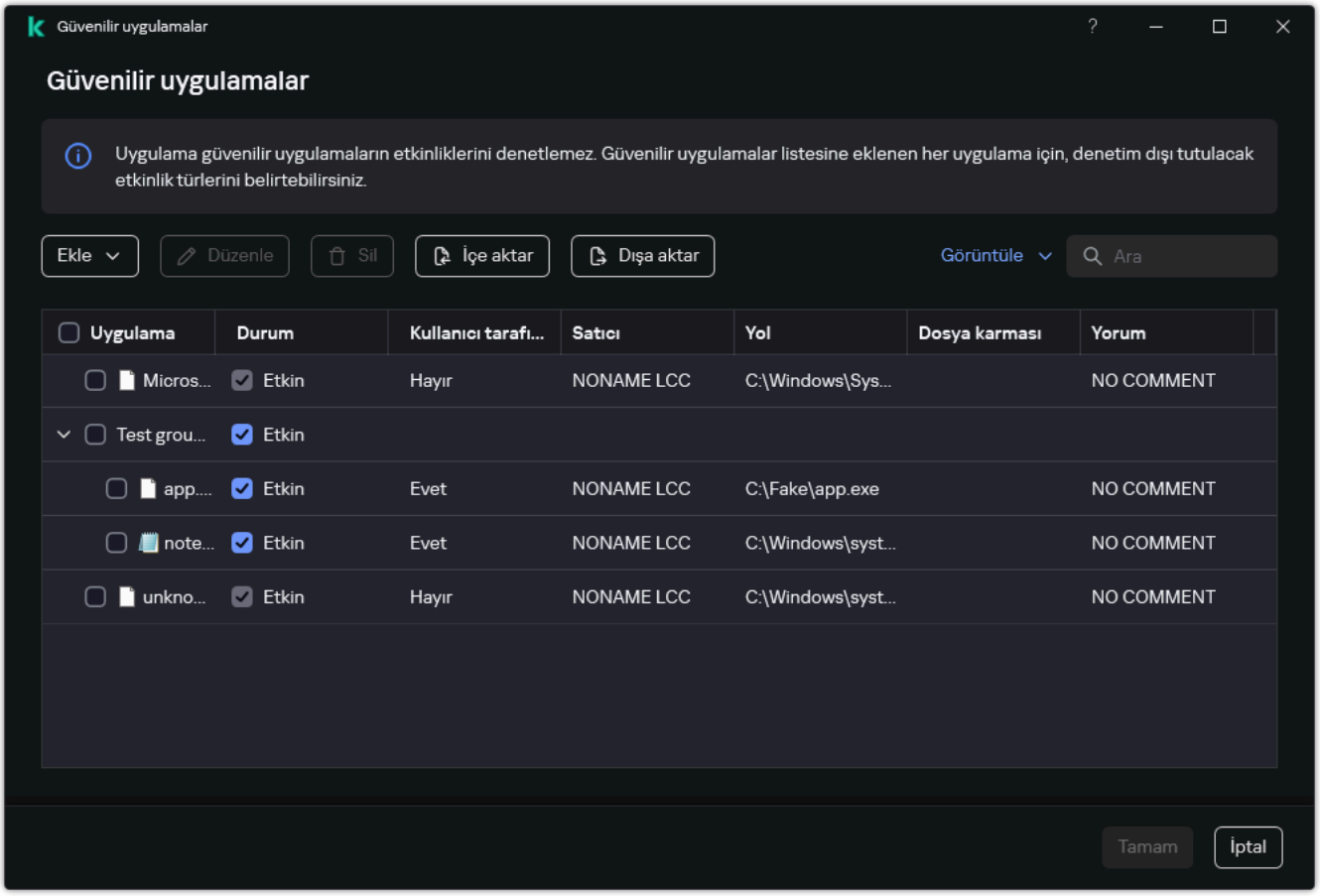
c. **Dışa aktar**'a tıklayın.

d. Yalnızca seçilen güvenilir uygulamaları mı dışa aktarmak yoksa tüm listeyi mi dışa aktarmak istediğinizi onaylayın.

e. Böylece açılan pencerede, güvenilir uygulamalar listesini dışa aktarmak istediğiniz XML dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

f. Dosyaya kaydet.

Kaspersky Endpoint Security, güvenilir uygulamalar listesinin tamamını XML dosyasına aktarır.



Güvenilir uygulamaların listesi

5. İstisnalar listesini içe aktarmak için:

a. **İstisnalar** bloğunda, **İstisnaları yönet** bağlantısını tıklayın.

b. **İçe aktar**'a tıklayın.

c. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz CSV dosyasını seçin.

d. Dosyayı aç.

Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye CSV dosyasından yeni girişler ekler.

6. Güvenilir uygulamaların bir listesini içe aktarmak için:

a. **İstisnalar** bloğunda, **Güvenilir uygulamaları belirt** bağlantısına tıklayın.

b. **İçe aktar**'a tıklayın.

c. Açılan pencerede, güvenilir uygulamalar listesini almak istediğiniz XML dosyasını seçin.

d. Dosyayı aç.

Bilgisayar zaten bir güvenilir uygulamalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

7. Değişikliklerinizi kaydedin.

Uygulamaları güvenilir bir dijital imza ile işleme

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.

Yönetim Konsolu (MMC) üzerinde güvenilen bir sistem sertifika deposunun kullanımını başlatma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
4. **Güvenilen sistem sertifika deposu** bloğunda, **Güvenilen sistem sertifika deposunu kullan** onay kutusunu seçin.
5. Açılır listeden hangi sistem deposunun Kaspersky Endpoint Security tarafından güvenilir olarak değerlendirilmesi gerektiğini seçin.
6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da güvenilir sistem sertifika deposu kullanımı nasıl başlatılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenilir Bölge** bölümüne gidin.
5. Açılan pencerede **Kök sertifikalar** bağlantısına tıklayın.
6. Açılan pencerede, **Güvenilir sistem sertifika deposunu kullan** onay kutusunu seçin.
7. Kaspersky Endpoint Security tarafından hangi sistem deposunun güvenilir olarak kabul edilmesi gerektiğini seçin.
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde güvenilir bir sistem sertifika deposunun kullanımı nasıl başlatılır

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.

3. **Güvenilir sistem sertifika deposu** açılır listesinden hangi sistem deposunun Kaspersky Endpoint Security tarafından güvenilir olarak değerlendirilmesi gerektiğini seçin.

4. Değişikliklerinizi kaydedin.

Ek. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, uygulamayı sanal ortamları korumak için Light Agent modunda yükleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir.

Önceden tanımlanmış istisnaları ve güvenilir uygulamaları aşağıdaki yollarla seçebilirsiniz:

- Uygulama yükleniyor.
  - Sihirbazı kullanarak uygulamayı yerel olarak yükleme
  - Kurulum paketi özellikleri
- İlkenin belirlenmesi.
  - Yeni ilke sihirbazı
  - İlke özellikleri: tarama istisnaları ve güvenilir uygulamalar

Microsoft SQL Server

Kaspersky Endpoint Security'yi bir SQL sunucusuna yüklerken, sunucunun çalışmasına müdahale edilmediğinden emin olmak için önceden tanımlanmış istisnalar ve güvenilir uygulamalardan bir güvenilir bölge oluşturmanız gerekir.

Önceden tanımlanmış tarama istisnaları

Yol	SQL sürümü
`%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA\*.mdf`	2012 2014 2016 2017 2019 2022
`%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?\*\Data\*.mdf`	2012
`%ProgramFiles%\Microsoft SQL Server\MSSQL.?\*\Data\*.mdf`	2012

Yol	SQL sürümü
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

Kaspersky Endpoint Security'yi bir Microsoft Exchange sunucusuna yüklerken, sunucunun çalışmasına müdahale edilmediğinden emin olmak için önceden tanımlanmış istisnalardan ve güvenilir uygulamalardan bir güvenilir bölge oluşturmanız gerekir.

Önceden tanımlanmış tarama istisnaları

Yol	Microsoft Exchange sürümü
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019

Yol	Microsoft Exchange sürümü
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Önceden tanımlanmış güvenilir uygulamalar

Yol	Microsoft Exchange sürümü
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Korumalı bilgisayarın işletim sisteminde Microsoft System Center Configuration Manager yüklüyse çözümün kararlı çalışmasını sağlamak için tarama istisnaları listesine önceden tanımlanmış bir istisna eklemeniz gerekir.

Önceden tanımlanmış tarama istisnaları

Yol	System Center Configuration Manager sürümü
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Kaspersky Endpoint Security'yi bir Citrix sanal ortamına yüklerken, sunucunun çalışmasına müdahale edilmediğinden emin olmak için önceden tanımlanmış istisnalardan ve güvenilir uygulamalardan bir güvenilir bölge oluşturmanız gerekir.

Önceden tanımlanmış tarama istisnaları

Yol
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf

Yol
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Önceden tanımlanmış güvenilir uygulamalar

Yol	Citrix Çözümü
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual Apps and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual Apps and Desktops

Yol	Citrix Çözümü
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual Apps and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual Apps and Desktops

Yol	Citrix Çözümü
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Workspace app
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Kaspersky Endpoint Security'yi bir VMware sanal ortamına yüklerken, sunucunun çalışmasına müdahale edilmediğinden emin olmak için önceden tanımlanmış güvenilir uygulamalardan bir güvenilir bölge oluşturmanız gerekir.

Önceden tanımlanmış güvenilir uygulamalar

Yol	VMware Çözümü
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon

Yol	VMware Çözümü
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Microsoft Windows Server'da veri tekilleştirme

Kaspersky Endpoint Security'nin yüklü olduğu Microsoft Windows Server işletim sisteminde veri tekilleştirme etkinse Kaspersky Endpoint Security'yi optimize etmek ve CPU yükünü azaltmak için önceden tanımlanmış güvenilir bir uygulamayı güvenilir uygulamalar listesine eklemeniz gerekir.

Önceden tanımlanmış güvenilir uygulamalar

Yol	Microsoft Windows Server sürümü
%SystemRoot%\system32\fsdmhost.exe	Desteklenen tüm sürümler

Yedeklemeyi Yönetme

Yedekleme depoları, temizleme esnasında silinen veya değiştirilen dosyaların yedek kopyalarını saklar. *Yedek kopya*, dosya temizlenmeden veya silinmeden önce oluşturulan bir dosya kopyasıdır. Dosyaların yedekleme kopyaları, özel bir biçimde saklanır ve bir tehdit oluşturmaz.

Dosyaların yedek kopyaları, `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasöründe saklanır.

Yönetici grubundaki kullanıcılara, bu klasör için tam erişim izni verilir. Hesabını Kaspersky Endpoint Security'yi yüklemek için kullanılan kullanıcıya, bu klasör için sınırlı erişim hakkı verilir.

Kaspersky Endpoint Security, dosyaların kopyalarının yedeklenmesine ilişkin kullanıcı erişim izinlerini yapılandırma özelliği sağlamaz.

Bazen temizleme işlemi sırasında dosyaların bütünlüğünü korumak mümkün değildir. Temizleme işleminden sonra temizlenen dosyadaki önemli bilgilere kısmen veya tamamen erişimi kaybederseniz dosyayı, yedekleme kopyasından orijinal klasörüne geri yüklemeyi deneyebilirsiniz.

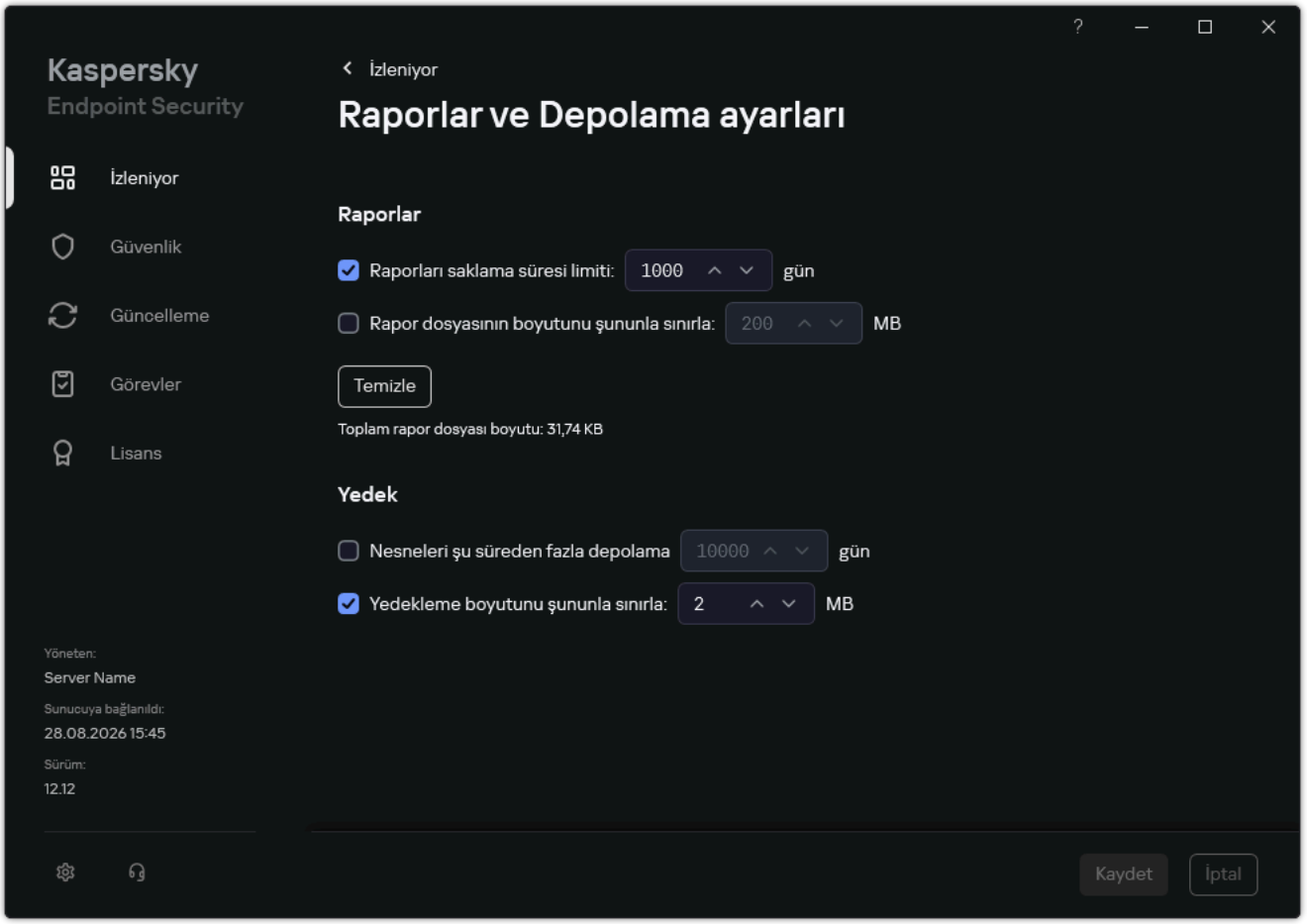
Kaspersky Endpoint Security, Kaspersky Security Center yönetimi kapsamında çalışıyorsa dosyaların yedek kopyaları Kaspersky Security Center Yönetim Sunucusuna iletilebilir. Kaspersky Security Center'da dosyaların yedek kopyalarını yönetme hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım sistemine bakın.

Yedekleme'deki dosyalar için maksimum depolama süresini yapılandırma

Yedekleme'de dosyaların kopyaları için varsayılan maksimum depolama süresi 30 gündür. Maksimum depolama süresinin sona ermesinin ardından Kaspersky Endpoint Security, en eski dosyaları Yedekleme'den siler.

Yedekleme'deki dosyalar için maksimum depolama süresini yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** bölümünden **Raporlar ve Depolama Alanı** seçimini yapın.



Yedekleme ayarları

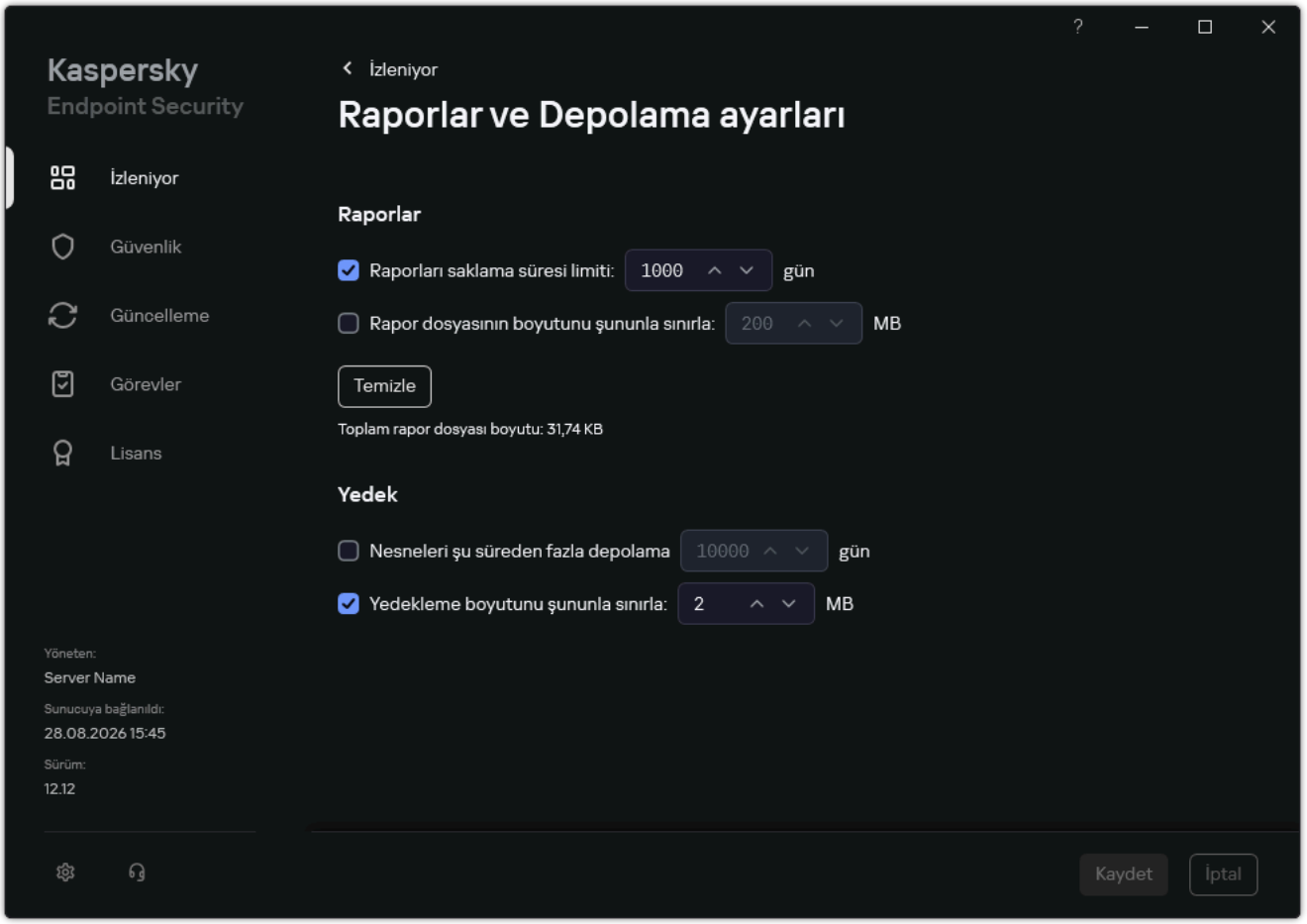
3. Yedekleme'deki dosyaların kopyalarının depolama dönemini sınırlamak istiyorsanız, **Yedek** bloğundaki **Nesneleri şu süreden fazla depolama**: **N gün** onay kutusunu seçin. Yedekleme'deki dosyalar için maksimum depolama süresini girin.
4. Değişikliklerinizi kaydedin.

Yedekleme için maksimum boyutu yapılandırma

Maksimum Yedekleme boyutunu belirtebilirsiniz. Yedekleme boyutu varsayılan olarak sınırsızdır. Kaspersky Endpoint Security, maksimum boyuta ulaşıldıktan sonra Yedekleme konumundan en eski dosyaları otomatik olarak siler.

Yedekleme'nin maksimum boyutunu yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** bölümünden **Raporlar ve Depolama Alanı** seçimini yapın.



Yedekleme ayarları

3. **Yedekleme** bloğunda, **Yedekleme boyutunu şununla sınırla**: **N MB** onay kutusunu seçin. Bu onay kutusu seçildiğinde maksimum depolama boyutu tanımlanan değerle sınırlanır. Varsayılan olarak, maksimum boyut 1024 MB'tır. Maksimum depolama boyutunu aşmamak için Kaspersky Endpoint Security, maksimum depolama dosyası boyutuna ulaşıldığında en eski dosyaları depolama alanından otomatik olarak siler.
4. Değişikliklerinizi kaydedin.

Yedekleme konumundan dosyaları geri yükleme

Dosyada zararlı kod tespit edilirse Kaspersky Endpoint Security dosyayı engeller, dosyaya *Virüslü değil* durumunu atar, dosyanın bir kopyasını Yedekleme'ye 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 özgün klasörüne geri yükleyebilirsiniz.

Bilgisayar yeniden başlatıldığında silinecek durumuna sahip dosyalar geri yüklenemez. Bilgisayarı yeniden başlatın, böylece dosya durumu *Temizlendi* veya *Silindi* olarak değişir. Temizlenen yedekleme kopyasından dosyayı özgün klasörüne geri yüklemek de mümkündür.

Windows Store uygulamasının parçası olan dosyadaki kötü amaçlı kod tespit edildiğinde Kaspersky Endpoint Security, Yedekleme konumuna taşımadan dosyayı hemen siler. Windows işletim sisteminin araçlarını kullanarak Windows Store uygulamasının bütünlüğünü geri yükleyebilirsiniz (Windows Store uygulamalarının geri yüklenmesiyle ilgili ayrıntılar için Windows yardım dosyaları bölümüne bakınız).

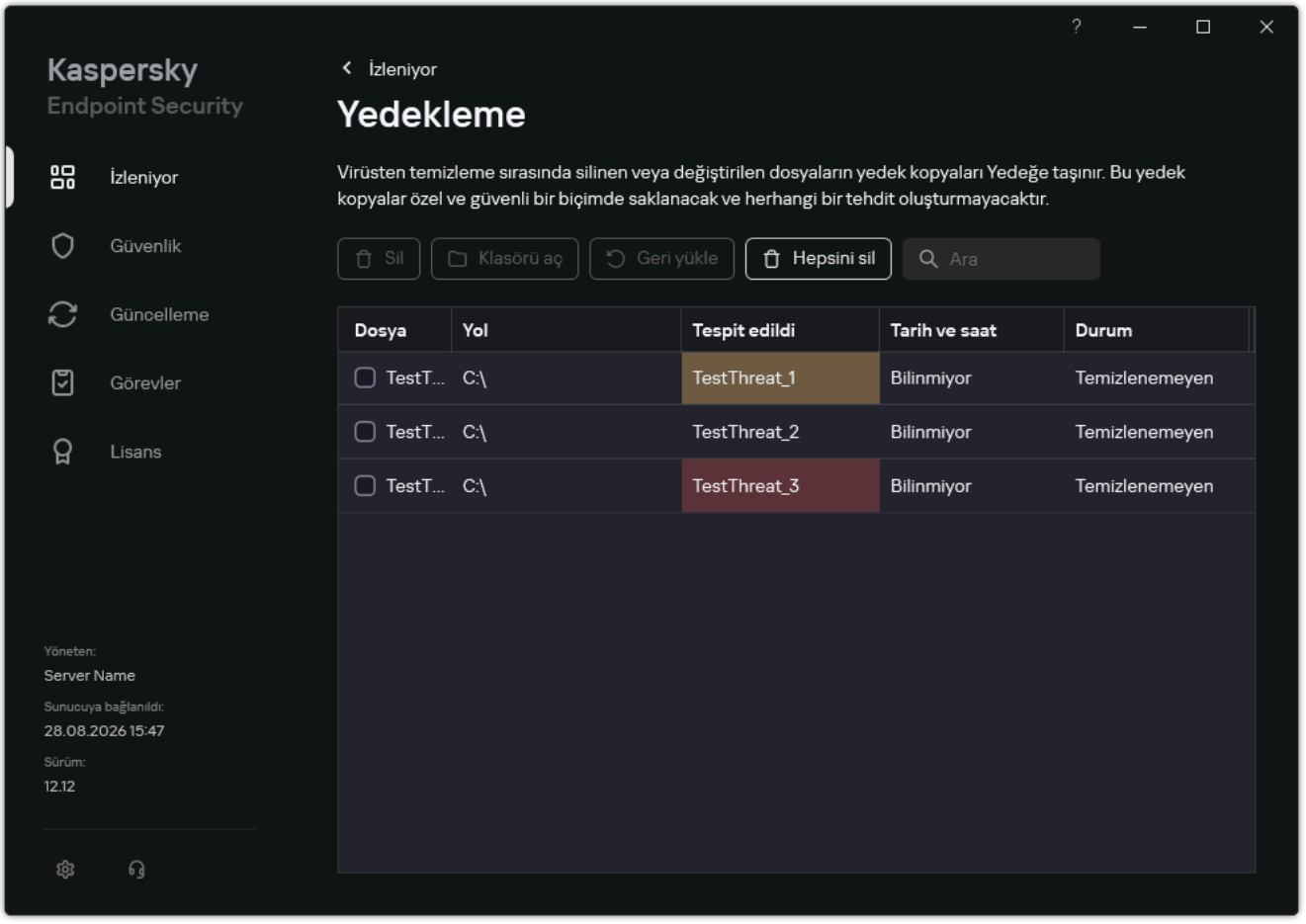
Dosyaların yedek kopyalarının grubu bir tablo olarak sunulmuştur. Dosyanın yedekleme kopyası için dosyanın orijinal klasörünün yolu görüntülenir. Dosyanın orijinal klasörünün yolunda kişisel veriler bulunabilir.

Aynı klasörde bulunan aynı ada ve farklı içeriğe sahip birkaç dosya Yedekleme'ye taşınırsa yalnızca Yedekleme klasörüne en son yerleştirilen dosya geri yüklenebilir.

Yedekleme konumundan dosyaları geri yüklemek için:

1. Ana uygulama penceresinin **İzleniyor** bölümünde, **Yedekleme** kutucuğuna tıklayın.
2. Bu, Yedekleme'deki dosyaların listesini açar; bu listede, geri yüklemek istediğiniz dosyaları seçin ve **Geri yükle**'ye tıklayın.

Kaspersky Endpoint Security, seçilen yedekleme kopyalarını orijinal klasörlerine geri yükler.



Yedekle

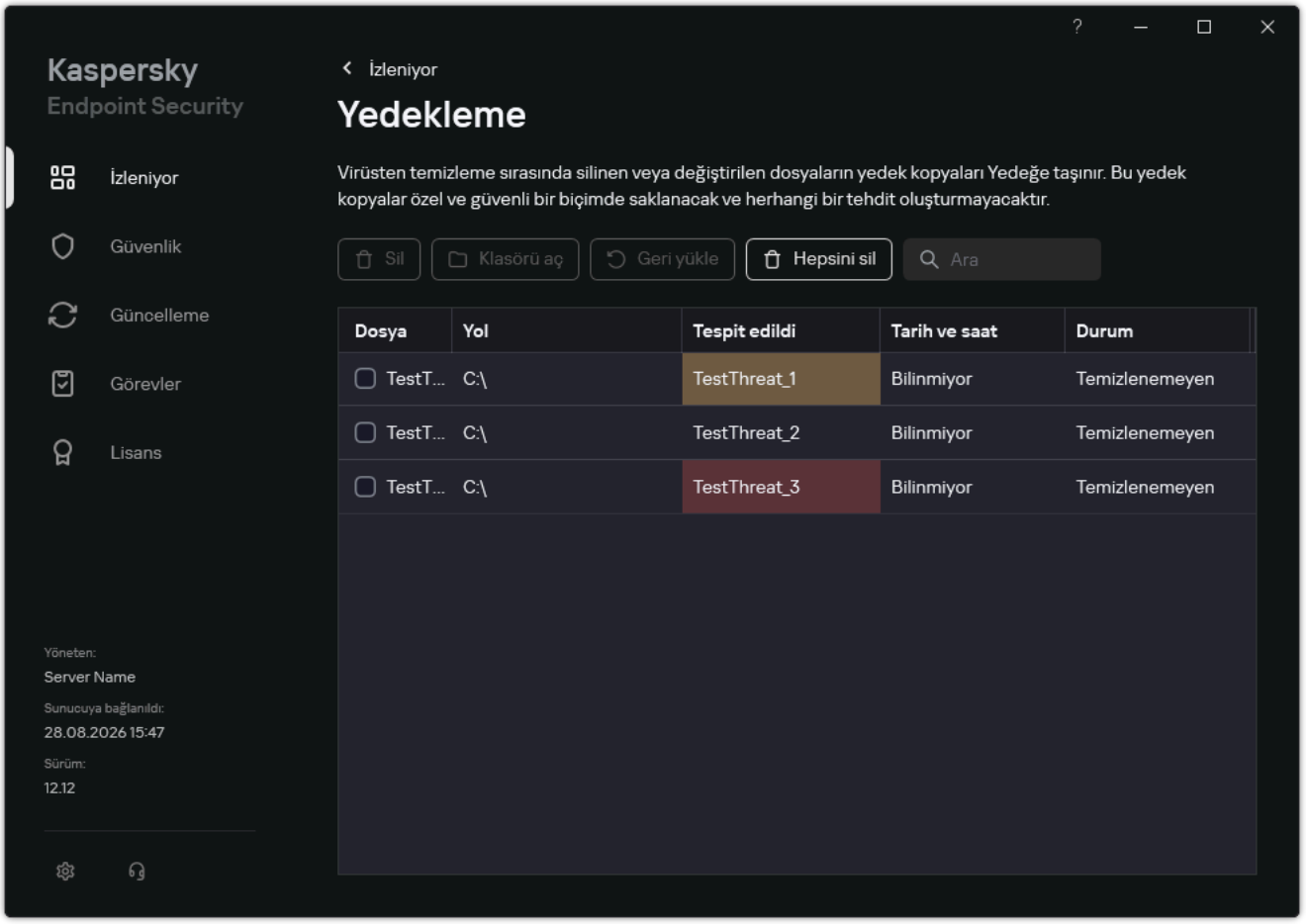
Yedekleme konumundan dosyaların yedekleme kopyalarını silme

Kaspersky Endpoint Security, uygulama ayarları bölümünde yapılandırılan depolama süresi geçtikten sonra her durumdaki dosyanın yedek kopyalarını Yedekleme'den otomatik olarak siler. Ayrıca bir dosyanın herhangi bir kopyasını Yedekten el ile de silebilirsiniz.

Yedekleme konumundan dosyaların yedekleme kopyalarını silmek için:

1. Ana uygulama penceresinin **İzleniyor** bölümünde, **Yedekleme** kutucuğuna tıklayın.
2. Bu, Yedekleme'deki dosyaların listesini açar; bu listede, Yedekten silmek istediğiniz dosyaları seçin ve **Sil**'e tıklayın.

Kaspersky Endpoint Security, Yedekleme konumundan seçilen dosyaların yedekleme kopyalarını siler.



Yedekle

Bildirim hizmeti

Kaspersky Endpoint Security'nin çalışması sırasında her tür olay gerçekleşir. Bu olayların bildirimleri tamamen bilgilendirme amaçlı olabilir ya da kritik bilgiler de içerebilir. Örneğin bildirimler veri tabanı ve uygulama modüllerinin güncellemesinin başarılı olduğu bilgisini verebilir ya da düzeltilmesi gereken bileşen hatalarını günlüğe kaydedebilir.

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 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. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
3. **Bildirimler** bloğunda **Bildirimleri yapılandır** düğmesine tıklayın.

   Kaspersky Endpoint Security bileşenleri ve görevleri pencerenin sol kısmında yer alır. Pencerenin sağ kısmında, seçilen bileşen veya görev için üretilen olaylar listelenir.

   Olaylar 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.
4. Pencerenin sol kısmında, olay günlüğü ayarlarını yapılandırmak istediğiniz bileşeni veya görevi seçin.

5. **Yerel rapora kaydet** ve **Windows Olay Günlüğüne kaydet** sütunlarında ilgili olayların karşısındaki onay kutularını işaretleyin.

   Yerel rapora kaydet sütununda onay kutuları seçilen olaylar, uygulama günlüklerinde görüntülenir. **Windows Olay Günlüğüne kaydet** sütununda onay kutularına sahip olaylar, `Application` kanalındaki Windows günlüklerinde görüntülenir.

6. Değişikliklerinizi kaydedin.

Bildirimlerin görüntülenmesini ve iletilmesini yapılandırma

Bildirimlerin görüntülenmesini ve iletilmesini yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
3. **Bildirimler** bloğunda **Bildirimleri yapılandır** düğmesine tıklayın.

   Kaspersky Endpoint Security bileşenleri ve görevleri pencerenin sol kısmında yer alır. Pencerenin sağ kısmında, seçilen bileşen veya görev için üretilen olaylar listelenir.

   Olaylar 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.

4. Pencerenin sol tarafında bildirimlerin iletimini yapılandırmak istediğiniz bileşeni veya görevi seçin.
5. **Ekran üzerinde bildir** sütununda ilgili 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 ilgili olayların yanındaki onay kutularını işaretleyin.

   E-posta bildirimi iletim ayarları yapılandırıldıysa seçilen olaylar hakkında bilgiler e-posta ile iletilir.

7. **Tamam**'a tıklayın.
8. E-posta bildirimlerini etkinleştirdiyseniz, e-posta teslimi için ayarları yapılandırın:

   a. **E-posta bildirimlerini yapılandır**'a tıklayın.

   b. **E-posta ile bildir** sütununda seçilen Kaspersky Endpoint Security olayları hakkındaki bilgilerin iletimini etkinleştirmek için **Olaylarla ilgili bildirimde bulun** onay kutusunu işaretleyin.

c. E-posta bildirimi iletim ayarlarını belirleyin.

d. **Tamam**'a tıklayın.

9. Değişikliklerinizi kaydedin.

Bildirim alanında uygulama durumu hakkında uyarıların görüntülenmesini yapılandırma

Bildirim alanında uygulama durumu uyarılarının görüntülenmesini yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
3. **Uygulamanın durumunu bildirim alanında göster** bloğunda, Microsoft Windows'un bildirim alanında bildirimlerini görmek istediğiniz olay kategorilerinin karşısındaki onay kutularını işaretleyin.
4. Değişikliklerinizi kaydedin.

Seçilen kategoriyle ilişkili bir olay gerçekleşirse bildirim alanında uygulama simgesi uyarının önem düzeyine bağlı olarak simgesine veya simgesine değişir.

Kullanıcılar ile yönetici arasında mesajlaşma

Uygulama Denetimi, Aygıt Denetimi, İnternet Denetimi ve Uyarlamalı Anomali Denetimi bileşenleri, Kaspersky Endpoint Security yüklü olan bilgisayarlara sahip LAN kullanıcılarının yöneticiye mesaj göndermesine olanak tanır.

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 Denetimi bir uygulamanın başlatılmasını engellemiştir.

  Engellenen bir uygulamanın başlatılmasına izin verme isteği için mesaj şablonu Kaspersky Endpoint Security arabiriminde Uygulama 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 Endpoint Security 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 Endpoint Security yüklü bilgisayarda bir Kaspersky Security Center ilkesi çalışıyorsa Kaspersky Security Center Yönetim Sunucusuna standart mesaj gönderilir.

  Bu durumda, Kaspersky Security Center olay deposundaki kullanıcı mesajları görüntülenebilir (aşağıdaki talimatlara bakın). Mesaj alanları Kaspersky Security Center ilkesinde tanımlanan şablondaki alanların değerleri ile doldurulmuştur.

- Kaspersky Endpoint Security yüklü bilgisayarda bir Kaspersky Security Center işyeri dışında 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 Sunucusuna 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 alanındaki bir kullanıcı mesajını görüntülemek için:

1. Kaspersky Security Center 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 **Olay seçimleri** açılır listesinden **Kullanıcı istekleri** seçimini yapın.

4. Yöneticiye gönderilen mesajı seçin.

5. Yönetim Konsolu çalışma alanının sağ tarafındaki **Olay özellikleri penceresini aç** düğmesine tıklayın.

Raporları yönetme

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, `C:\ProgramData\Kaspersky Lab\KES.14.2\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.

Rapordaki veriler tablo şeklinde sunulur. Her bir tablo satırı, ayrı bir olayla ilgili bilgiler 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 yanındaki ⊞ düğmesine tıklayın. 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 bileşenlerinin çalışması hakkında raporlar.
- Kaspersky Endpoint Security görev raporları.
- **Veri Şifreleme** raporu. Veri şifreleme ve şifre çözme sırasında oluşan olaylarla ilgili bilgi içerir.

Raporlarda aşağıdaki olay önem düzeyleri kullanılır:

ⓘ **Bilgilendirici mesajlar**. Normalde önemli bilgi içermeyen referans olaylardır.

⚠ **Uyarılar**. Kaspersky Endpoint Security'nin çalışmasında önemli durumları yansıttığı için dikkat edilmesi gereken olaylardır.

ⓘ **Kritik olaylar**. 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 ⊞ düğmesini kullanarak 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.

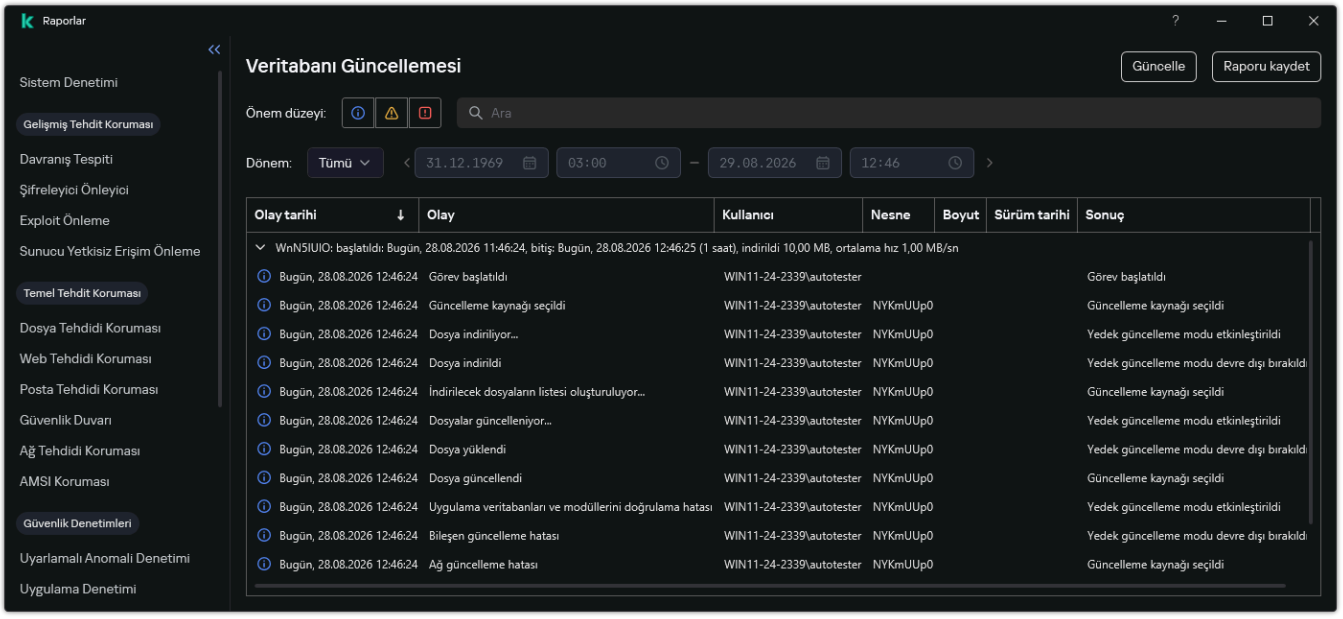
Kaspersky Endpoint Security, Kaspersky Security Center yönetimi altında çalışıyorsa, olaylar hakkındaki bilgiler Kaspersky Security Center Yönetim Sunucusu'na aktarılabilir (daha fazla bilgi için Kaspersky Security Center Yardımı 'na başvurun).

Raporları görüntüleme

Kullanıcı, raporları görüntüleyebiliyorsa raporlarda yansıtılan tüm olayları da görüntüleyebilir.

Raporları görüntülemek için:

1. Ana uygulama penceresinin **İzleniyor** bölümünde, **Raporlar** kutucuğuna tıklayın.



Raporlar

2. Bileşenler ve görevler listesinden bir bileşen veya görev seçin.

   Pencerenin sağ kısmında, Kaspersky Endpoint Security'nin seçili bileşeninin veya seçili görevinin çalışmasından kaynaklanan olay listesini içeren bir rapor görüntülenir. Rapordaki olayları, sütunlardan birinin hücrelerindeki değerlere göre sıralayabilirsiniz.

3. Bir etkinlik hakkındaki ayrıntılı bilgileri görüntülemek için raporda etkinliği seçin.

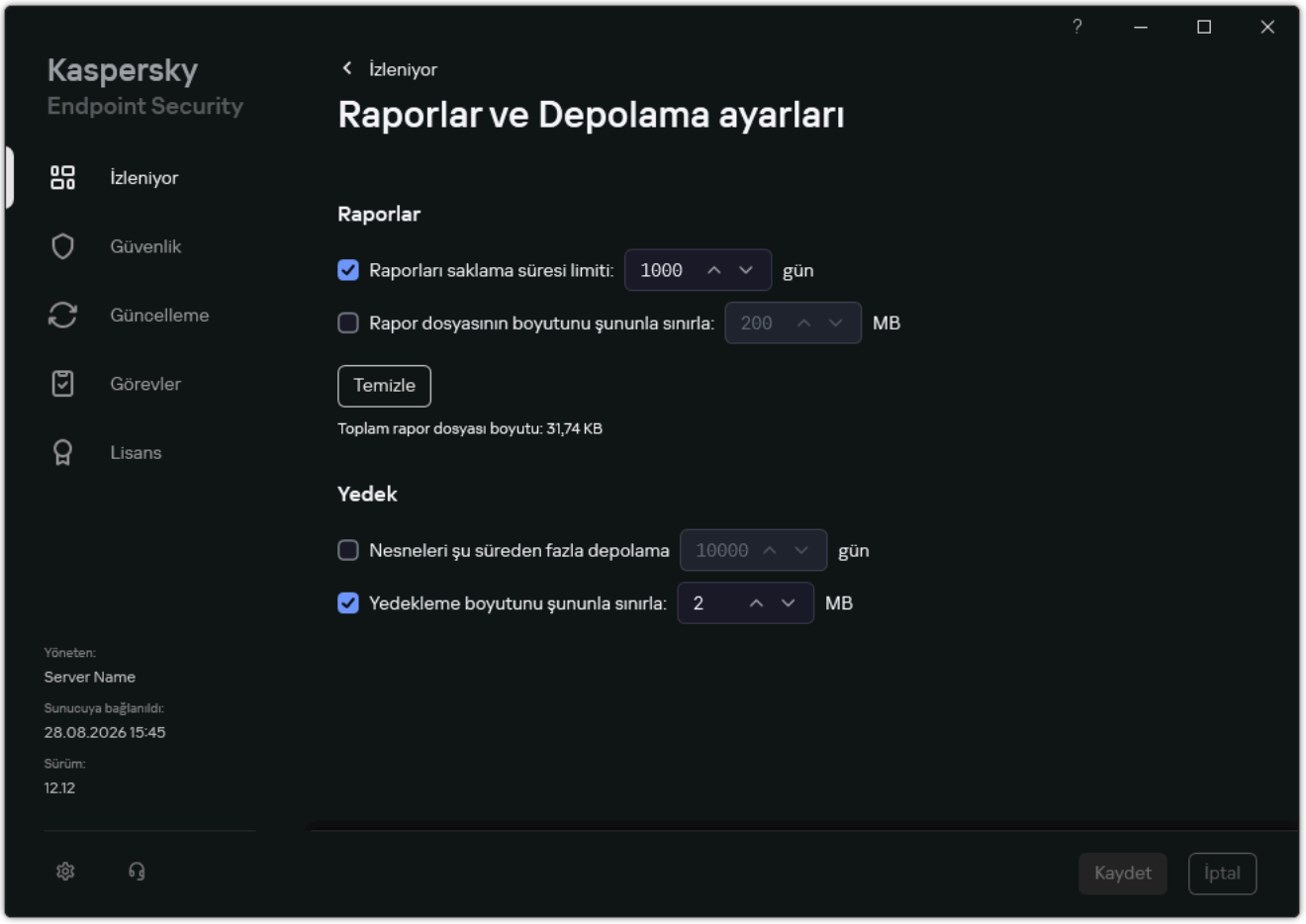
Pencerenin alt kısmında olay özetini içeren bir blok görüntülenir.

Maksimum rapor depolama süresini yapılandırma

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.

Maksimum rapor depolama süresini yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** bölümünden **Raporlar ve Depolama Alanı** seçimini yapın.



Rapor ayarları

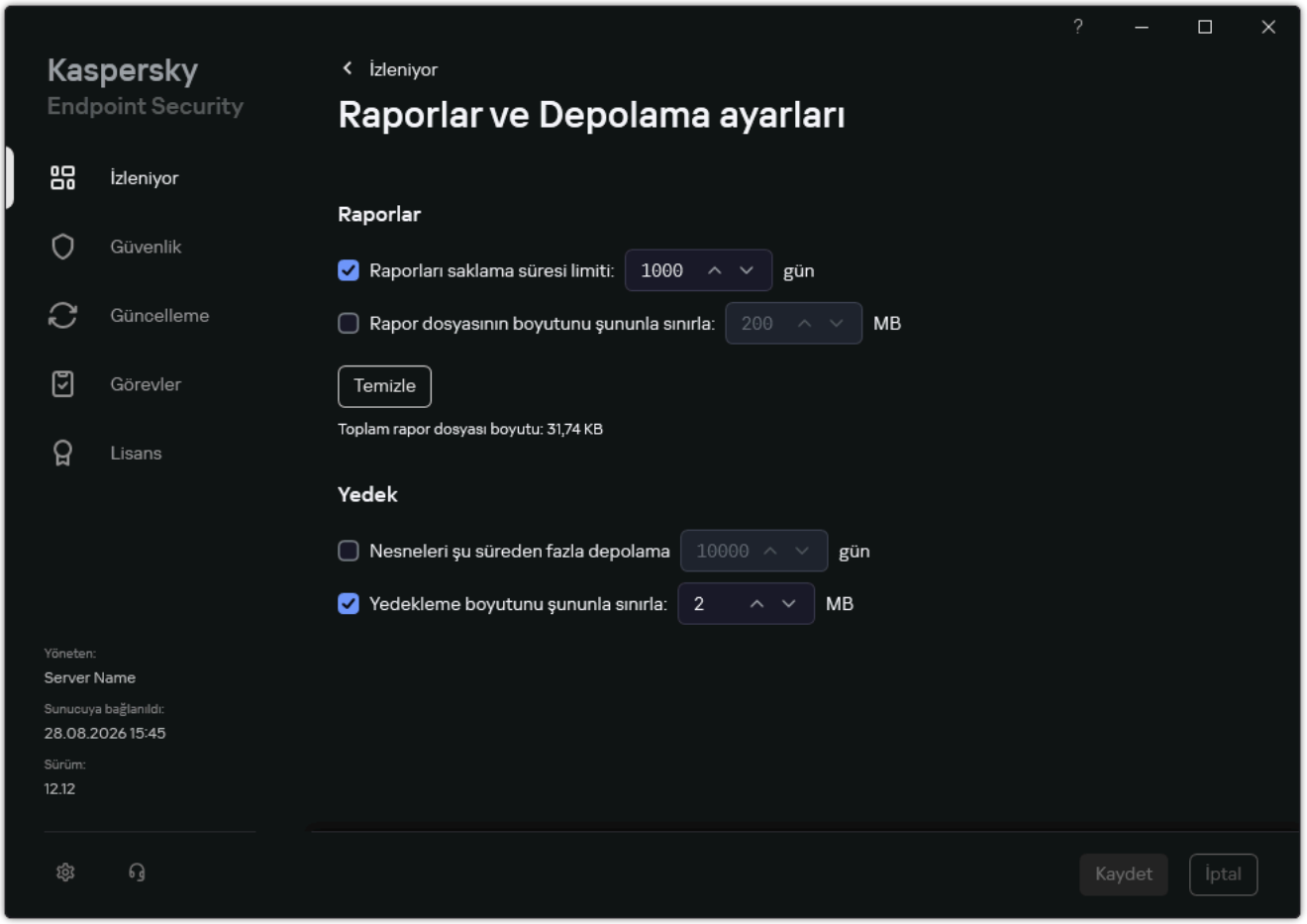
3. Rapor saklama süresini sınırlamak istiyorsanız, **Raporlar** bloğundaki **Raporları saklama süresi limiti: N gün** onay kutusunu seçin. Maksimum rapor depolama süresini tanımlama.
4. Değişikliklerinizi kaydedin.

Rapor dosyasının maksimum boyutunu yapılandırma

Raporu içeren dosyanın maksimum boyutunu belirtebilirsiniz. Öaksimum rapor dosyasının boyutu varsayılan olarak 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.

Maksimum rapor dosyası boyutunu yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** bölümünden **Raporlar ve Depolama Alanı** seçimini yapın.



Rapor ayarları

3. **Raporlar** bloğunda, bir rapor dosyasının boyutunu sınırlandırmak istiyorsanız, **Rapor dosyasının boyutunu şununla sınırla: N MB** onay kutusunu seçin. Rapor dosyasının maksimum boyutunu tanımlayın.
4. Değişikliklerinizi kaydedin.

Raporu dosya olarak kaydetme

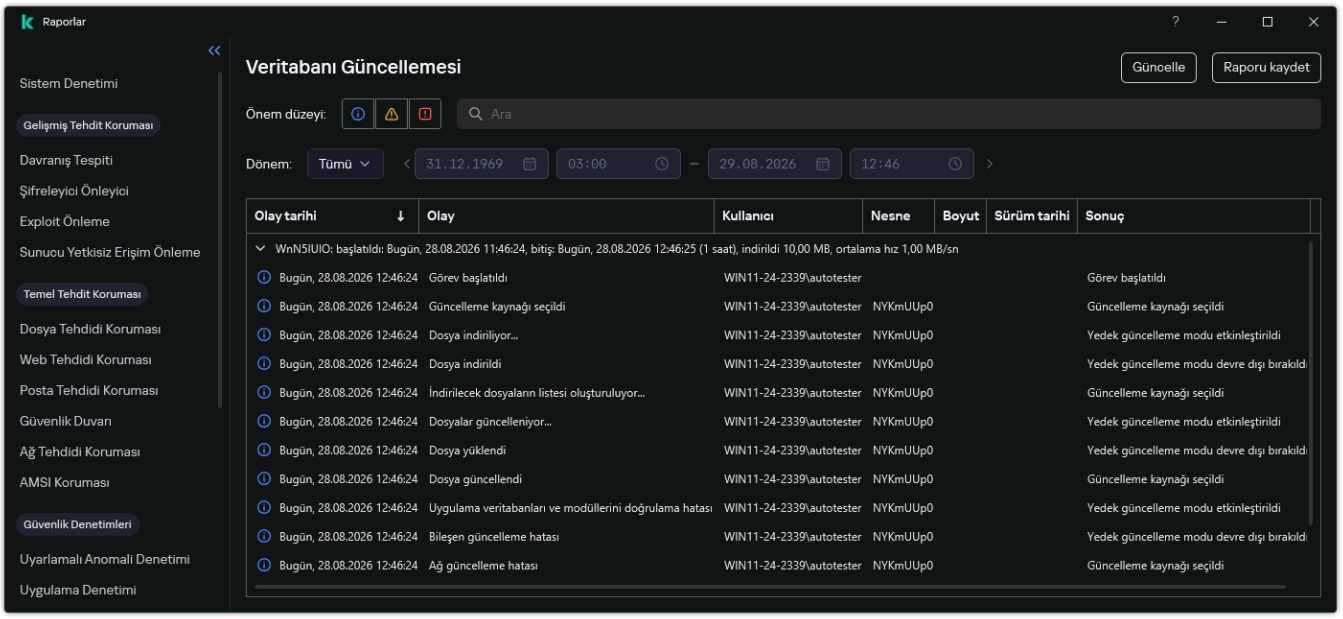
Kullanıcı, dosyaya kaydedilen bir rapordaki bilgilerin güvenliğini sağlamaktan ve özellikle de bu bilgilere erişimi denetlemekten ve kısıtlamaktan sorumludur.

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 penceresinin **İzleniyor** bölümünde, **Raporlar** kutucuğuna tıklayın.



Raporlar

2. Bir pencere açılır; bu pencereden bileşeni veya görevi seçin.

   Pencerenin sağında, Kaspersky Endpoint Security'nin seçilen bileşen veya görevinin çalışması sırasındaki olayların listesini içeren bir rapor görüntülenir.

3. Gerekirse rapordaki veri sunumunu aşağıdaki yöntemlerle değiştirebilirsiniz:

   - Olayları filtreleyerek
   - Olay araması yaparak
   - Sütunları yeniden düzenleyerek
   - Olayları sıralayarak

4. Pencerenin sağ üst kısmındaki **Raporu kaydet** düğmesine tıklayın.

5. Açılan pencerede, rapor dosyasının hedef klasörünü belirtin.

6. Rapor dosyasının adını girin.

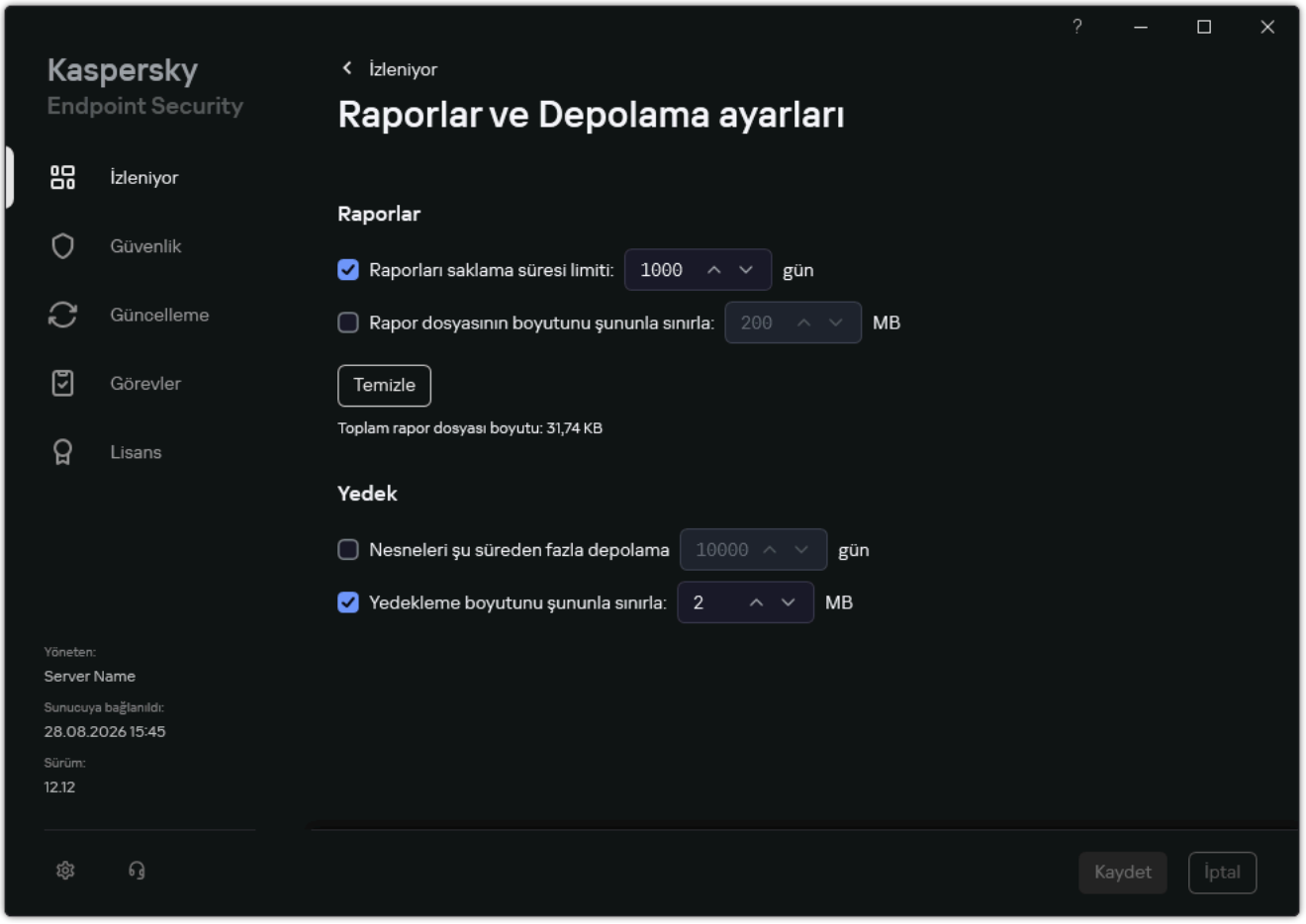
7. Gerekli rapor dosyası biçimini seçin: TXT veya CSV.

8. Değişikliklerinizi kaydedin.

Raporlar temizleniyor

Raporlardan bilgi çıkarmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** bölümünden **Raporlar ve Depolama Alanı** seçimini yapın.



Rapor ayarları

3. **Raporlar** bloğundan **Temizle** düğmesine tıklayın.
4. Parola koruması etkinse, Kaspersky Endpoint Security sizden kullanıcı hesabı kimlik bilgilerini isteyebilir. Kullanıcı gerekli izne sahip değilse uygulama, hesap kimlik bilgilerini ister.

Kaspersky Endpoint Security, tüm uygulama bileşenleri ve görevler için raporları silecektir.

Kaspersky Endpoint Security Kendini Koruma

Kendini Koruma, diğer uygulamaların Kaspersky Endpoint Security'nin çalışmasına müdahale edebilecek eylemler gerçekleştirmesini, örneğin, Kaspersky Endpoint Security'yi bilgisayardan kaldırılmasını, engeller. Kaspersky Endpoint Security için sunulan Kendini Koruma teknolojileri, işletim sisteminin 32 bit mi yoksa 64 bit mi olduğuna göre değişir (aşağıdaki tabloya bakınız). Kendini Koruma ayrıca Parola koruması ve Yönetim Sunucusu bağlantı koruması da içerir.

Parola koruması, kullanıcıların Kaspersky Endpoint Security'ye erişimlerini kendilerine verilen izinler kapsamında (uygulamadan çıkma izni gibi) kısıtlamanızı sağlar.

Yönetim Sunucusu bağlantı koruması, bilgisayarın güvenilmeyen bir sunucuya yetkisiz olarak yeniden bağlanmasını önler.

Kaspersky Endpoint Security Kendini Koruma teknolojileri

Teknoloji	Açıklama	x86 bilgisayar	x64 bilgisayar
Kendini Koruma mekanizması	Teknoloji, aşağıdaki uygulama bileşenlerine erişimi engeller: • Kaspersky Endpoint Security kurulum klasöründeki dosyalar ve uygulamanın diğer dosyaları; • Uygulamaya ait kayıtların bulunduğu kayıt defteri anahtarları; • Uygulamanın çalıştırdığı işlemler.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Teknoloji Kaspersky Endpoint Security'yi kötü amaçlı eylemlere karşı korur. AM-PPL teknolojisi hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin. AM-PPL teknolojisi Windows Server 2019 ve Windows 10 sürüm 1703 (RS2) veya üstü işletim sistemlerinde bulunur.	✓	✓
Harici yönetim koruma mekanizması	Bu teknoloji, diğer uygulamaların (örneğin TeamViewer veya RemotelyAnywhere) Kaspersky Endpoint Security'ye erişmesini engeller.	✓	– (Windows 7 hariç)

Kendini Koruma'yı etkinleştirme ve devre dışı bırakma

Kaspersky Endpoint Security, sabit sürücüdeki uygulama dosyalarının, bellek işlemlerinin ve sistem kayıt defterindeki girdilerin değiştirilmesini veya silinmesini önler.

Teknoloji, aşağıdaki uygulama bileşenlerine erişimi engeller:

- Kaspersky Endpoint Security kurulum klasöründeki dosyalar ve uygulamanın diğer dosyaları;
- Uygulamaya ait kayıtların bulunduğu kayıt defteri anahtarları;
- Uygulamanın çalıştırdığı işlemler.

Kendini savunma mekanizmaları, güvenilmeyen üst işlemler tarafından başlatılan Kaspersky Endpoint Security işlemlerine uygulanmaz.

Kaspersky Endpoint Security'nin Kendini Koruma mekanizması varsayılan olarak etkindir.

Yönetim Konsolu'nda (MMC) Kendini Korumayı etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar → Uygulama ayarları** öğesini seçin.
4. Kendini Koruma mekanizmasını etkinleştirmek veya devre dışı bırakmak için **Kendini Korumayı Etkinleştir** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

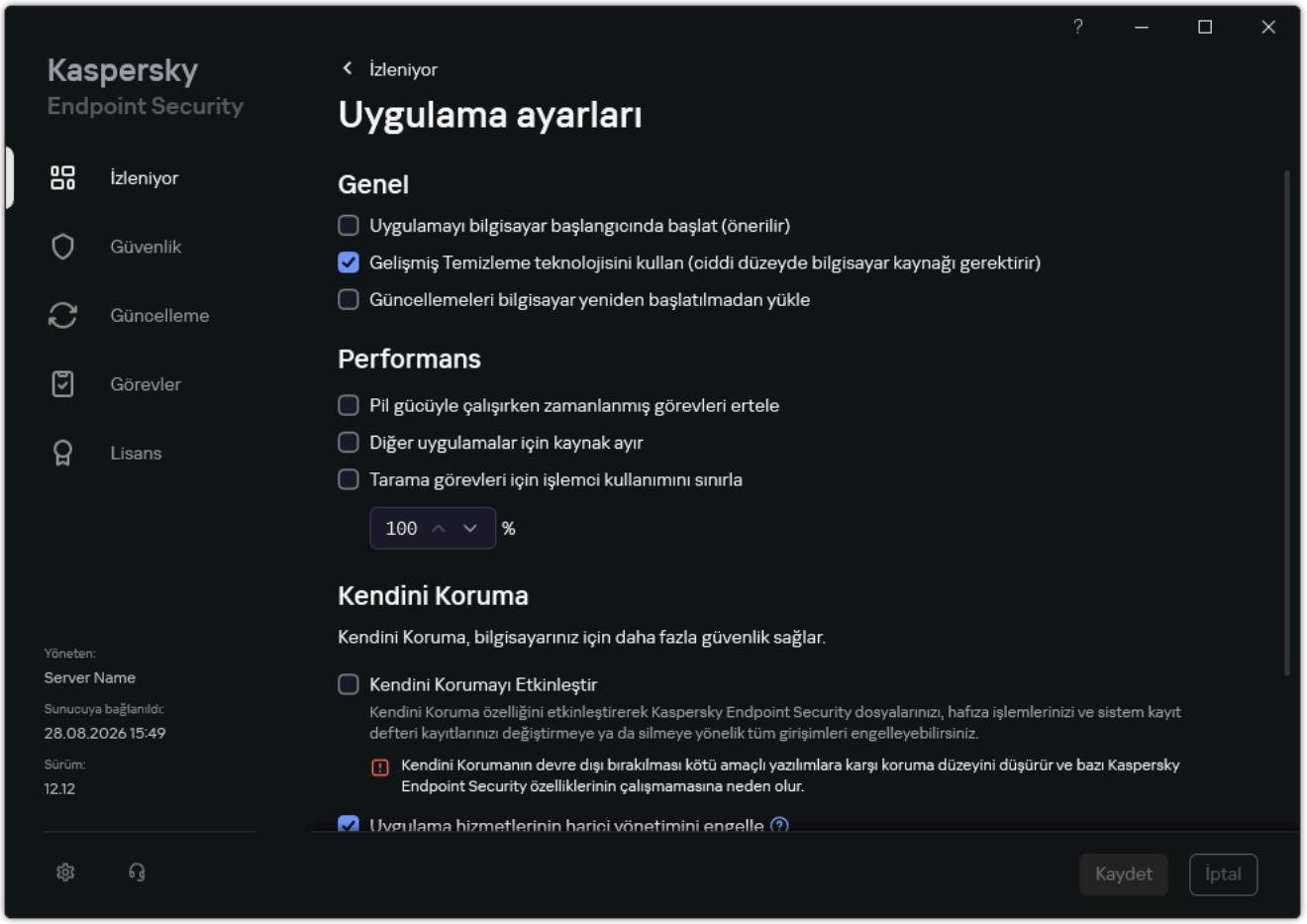
Web Console'da ve Cloud Console'da Kendini Korumayı etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar → Kendini Koruma** bölümüne gidin.
5. Kendini Koruma mekanizmasını etkinleştirmek veya devre dışı bırakmak için **Kendini Koruma ETKİN** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Kendini Korumayı etkinleştirme veya devre dışı bırakma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. Kendini Koruma mekanizmasını etkinleştirmek veya devre dışı bırakmak için **Kendini Korumayı Etkinleştir** onay kutusunu kullanın.
4. Değişikliklerinizi kaydedin.

AM-PPL desteğini etkinleştirme ve devre dışı bırakma

Kaspersky Endpoint Security, Microsoft'un Antimalware Protected Process Light teknolojisini (bundan sonra kısaca "AM-PPL" olarak anılacaktır) destekler. AM-PPL, Kaspersky Endpoint Security işlemlerini zararlı eylemlere karşı korur (örneğin uygulamanın sonlandırılması). AM-PPL sadece güvenilen işlemlerin çalışmasına izin verir. Kaspersky Endpoint Security işlemlerinin girişi Windows güvenlik gerekliliklerine uygun olarak yapıldı ve bu yüzden güvenilir statüsündeler. AM-PPL teknolojisi hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin. AM-PPL teknolojisi varsayılan olarak etkindir.

Kaspersky Endpoint Security'nin uygulama işlemlerini korumak üzere bütünleşik mekanizmaları vardır. AM-PPL desteği, işletim sistemine işlem güvenlik işlevleri atamanıza olanak tanır. Böylece uygulamanın hızını artırabilir ve bilgisayar kaynaklarının tüketimini azaltabilirsiniz.

AM-PPL teknolojisini sürekli kullanın. AM-PPL, işletim sistemi korumasının önemli bir bileşenidir. AM-PPL desteğini devre dışı bırakmak, Kaspersky Endpoint Security'nin bazı özelliklerinin çalışmamasına neden olabilir (örneğin, uygulamanın Windows Security Center) ile entegrasyonu). AM-PPL desteğinin devre dışı bırakılması, sorun giderme amacıyla yalnızca ayrı bir test ortamında izin verilir.

AM-PPL teknolojisi Windows Server 2019 ve Windows 10 sürüm 1703 (RS2) veya üstü işletim sistemlerinde bulunur.

AM-PPL teknolojisini etkinleştirmek veya devre dışı bırakmak için:

1. Uygulamanın Kendini Koruma mekanizmasını kapatın.

   Kendini Koruma mekanizması, AM-PPL durumlarının değiştirilmesi de dahil olmak üzere bilgisayar belleğindeki uygulama işlemlerinin değiştirilmesini ve silinmesini engeller.

2. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.

3. Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

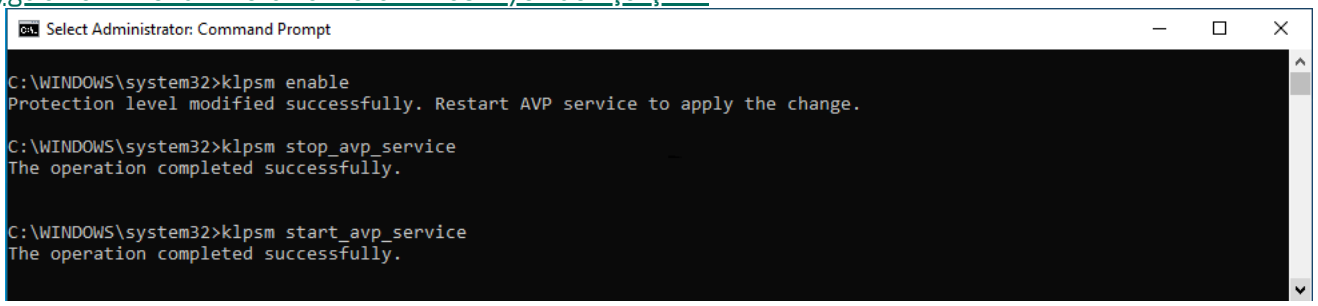
   Uygulama kurulumu sırasında yürütülebilir dosyanın yolunu %PATH% sistem değişkenine ekleyebilirsiniz.

4. Komut satırına şunu yazın:

   - `klpsm.exe enable` – AM-PPL teknolojisi desteğini etkinleştirir (aşağıdaki şekle bakın).
   - `klpsm.exe disable` – AM-PPL teknolojisi desteğini devre dışı bırakır.

5. Kaspersky Endpoint Security'yi yeniden başlatın.

6. Uygulamanın Kendini Koruma mekanizmasını yeniden çalıştırın.



AM-PPL teknolojisi desteğinin etkinleştirilmesi

Uygulama hizmetlerinin harici yönetime karşı korunması

Uygulama hizmetlerinin harici yönetime karşı korunması, kullanıcıların ve diğer uygulamaların Kaspersky Endpoint Security hizmetlerini durdurma girişimlerini engeller. Koruma, şu hizmetlerin çalışmasını sağlar:

- Kaspersky Endpoint Security Service (AVP.KES.14.2)
- Kaspersky Seamless Update Service hizmeti (AVPSUS.KES.14.2)

Komut satırını kullanarak uygulamadan çıkmak için Kaspersky Endpoint Security hizmetlerinin harici yönetime karşı korumasını devre dışı bırakın.

Uygulama hizmetlerinin dış yönetimine yalnızca AM-PPL teknolojisini desteklemeyen bilgisayarlarda veya teknolojinin devre dışı bırakıldığı bilgisayarlarda izin verebilirsiniz.

Yönetim Konsolu'nda (MMC) uygulama hizmetlerinin harici yönetime karşı korunmasını etkinleştirme veya devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
4. Kaspersky Endpoint Security hizmetlerinin harici yönetime karşı korumasını etkinleştirmek veya bu korumayı devre dışı bırakmak için **Uygulama hizmetlerinin harici yönetimini engelle** onay kutusunu kullanın.
5. Değişikliklerinizi kaydedin.

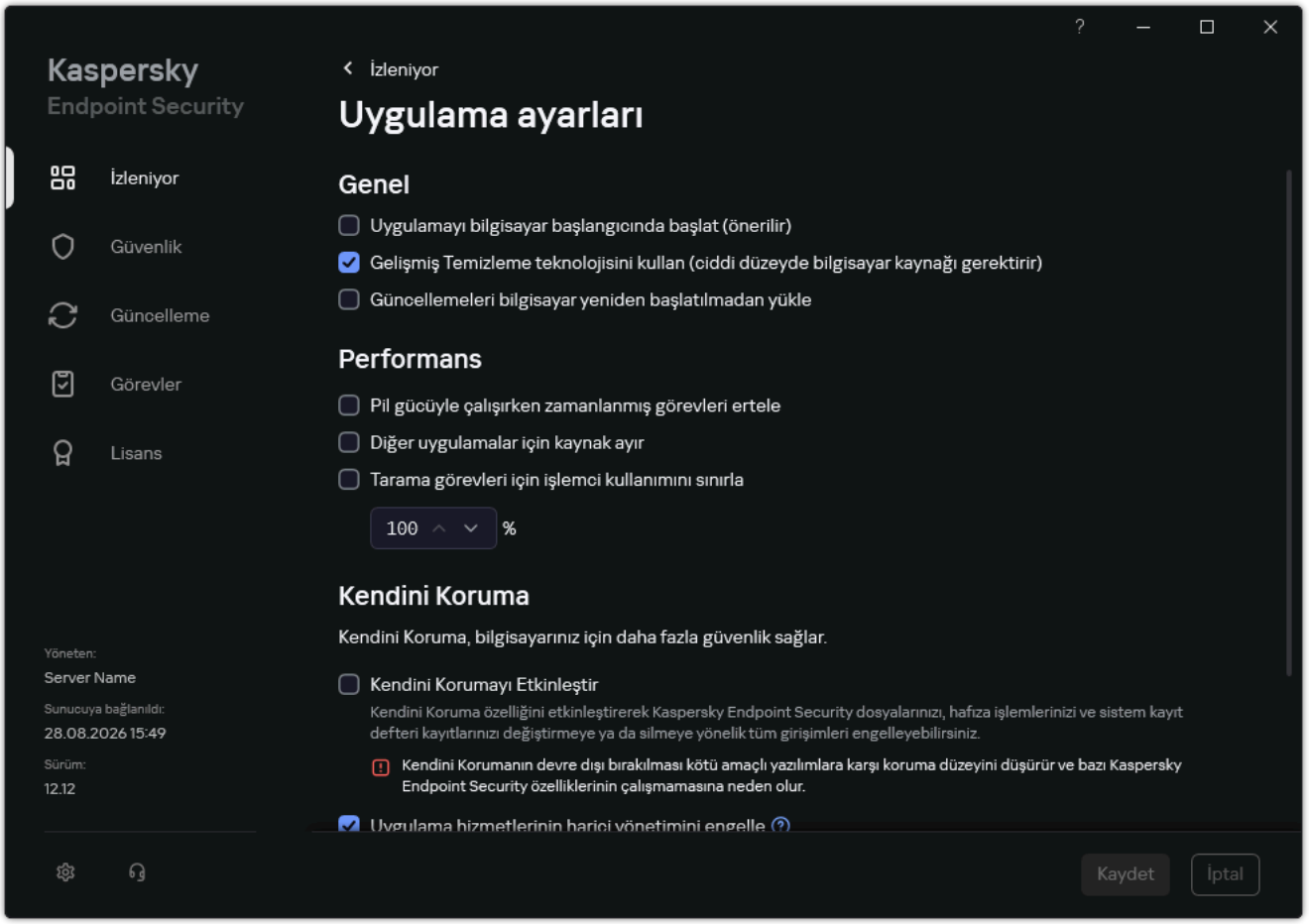
Web Console ve Cloud Console'da uygulama hizmetlerinin harici yönetime karşı korunmasını etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kendini Koruma** bölümüne gidin.
5. Kaspersky Endpoint Security hizmetlerinin harici yönetime karşı korumasını etkinleştirmek veya bu korumayı devre dışı bırakmak için **Uygulama hizmetlerinin harici yönetimini engelle** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde uygulama hizmetlerinin harici yönetime karşı korunmasını etkinleştirme veya devre dışı bırakma

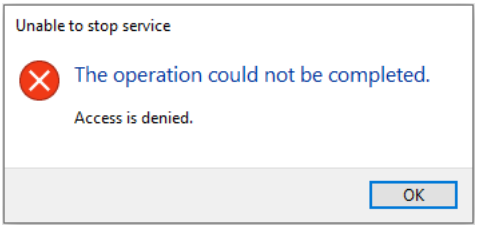
1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. Kaspersky Endpoint Security hizmetlerinin harici yönetime karşı korumasını etkinleştirmek veya bu korumayı devre dışı bırakmak için **Uygulama hizmetlerinin harici yönetimini engelle** onay kutusunu kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak, bir kullanıcı uygulama hizmetlerini durdurmaya çalıştığında, hata mesajı içeren bir sistem penceresi görüntülenir. Kullanıcı, uygulama hizmetlerini yalnızca Kaspersky Endpoint Security arabiriminden yönetebilir.



Uygulama hizmetleri erişim hatası

Uzaktan yönetim uygulamalarını destekleme

Harici yönetim koruması etkinken bazen uzak bir yönetim uygulaması kullanmanız gerekebilir.

Uzaktan yönetim uygulamalarının çalışmasını etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **İstisnalar ve tespit edilen nesne türleri** seçimini yapın.
3. **İstisnalar** bloğunda, **Güvenilir uygulamaları belirt** bağlantısına tıklayın.
4. Açılan pencerede **Ekle** düğmesine tıklayın.
5. Uzaktan yönetim uygulamasının yürütülebilir dosyasını seçin.

   Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.
6. **Kaspersky Endpoint Security arabirimi ile etkileşime izin ver** onay kutusunu işaretleyin.
7. Değişikliklerinizi kaydedin.

Parola koruması

Bilgisayar okuryazarlığı düzeyi farklı kullanıcılar aynı bilgisayarı kullanabilir. Kaspersky Endpoint Security'ye ve ayarlarına sınırsız erişiminiz varsa bilgisayar korumasının genel düzeyi düşebilir. Parola koruması, kullanıcıların Kaspersky Endpoint Security'ye erişimlerini kendilerine verilen izinler kapsamında (uygulamadan çıkma izni gibi) kısıtlamanızı sağlar.

Windows oturumunu başlatan kullanıcı (*oturum kullanıcısı*) eylemi gerçekleştirme iznine sahipse, Kaspersky Endpoint Security kullanıcı adı ve parola ya da bir geçici parola istemez. Kullanıcı, Kaspersky Endpoint Security erişimini verilen izinlere uygun olarak alır.

Oturum kullanıcısının bir eylemi gerçekleştirmek için izni yoksa, kullanıcı uygulamaya erişimi şu yollarla elde edebilir:

- Bir kullanıcı adı ve parola girmek.

  Bu yöntem, günlük işlemler için uygundur. Parola korumalı bir eylemi gerçekleştirmek için gerekli izne sahip etki alanı hesabınızın bilgilerini girmeniz gerekir. Bu durumda bilgisayar o etki alanında olmalıdır. Bilgisayar etki alanında değilse, KLAdmin hesabını ya da manuel olarak eklenen bir hesabı kullanabilirsiniz.

- Bir geçici parola girmek.

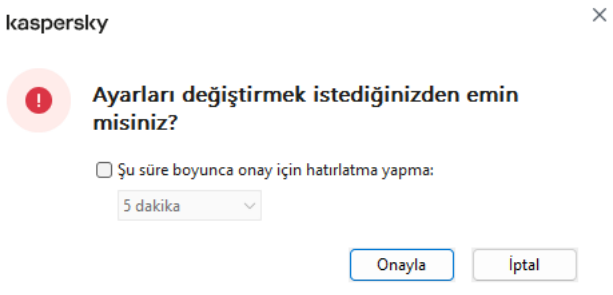
  Bu yöntem, kurumsal ağ dışındaki kullanıcıların engellenen eylemleri gerçekleştirebilmeleri (uygulamadan çıkmak gibi) amacıyla geçici izinler vermek için uygundur. Geçici parolanın süresi dolarsa veya oturum kapanırsa Kaspersky Endpoint Security, ayarları önceki değerlerine geri getirir.

- Belirteç.

  Bu yöntem, ayrıcalıklı kullanıcılar (örneğin teknik destek personeli) için uygundur. Belirteçle kimlik doğrulama, Active Directory'de akıllı kartla oturum açma modunun kullanılmasını sağlar. Bu, kuruluşun altyapısının güvenliğini artırır.

Kullanıcı, parola korumalı bir eylem gerçekleştirmeye çalıştığında Kaspersky Endpoint Security, kullanıcıdan kullanıcı adı ve parola, belirteç parolası veya geçici parola girmesini ister (aşağıdaki şekle bakın).

Parola girişi penceresinde, dilleri sadece **ALT+SHIFT** tuşlarına basarak değiştirebilirsiniz. Başka kısayollar, işletim sisteminde yapılandırılmış olsalar bile, dil değiştirmek için kullanılamaz.



Kaspersky Endpoint Security erişimi parola istemi

Kullanıcı adı ve parolası

Kaspersky Endpoint Security'ye erişmek için hesap kimlik bilgilerini girmeniz gerekir. Parola koruması aşağıdaki hesaplarda desteklenir:

- **KLAdmin**. Kaspersky Endpoint Security'ye sınırsız erişimi olan bir Yönetici hesabı. KLAdmin hesabının, parola korumalı tüm işlemleri gerçekleştirme izni bulunur. KLAdmin hesabının izinleri iptal edilemez. Parola korumasını etkinleştirdiğinizde Kaspersky Endpoint Security, KLAdmin hesabı için bir parola belirlemenizi ister.
- **Manuel olarak eklenen hesap**. Active Directory etki alanı dışındaki bir hesap. Yönetici parolasını paylaşmak istemiyorsanız KLAdmin yerine bu hizmet hesabını kullanabilirsiniz. Herhangi bir kullanıcı adı ve parola belirleyebilir ve bireysel izinleri yapılandırabilirsiniz.
- **Herkes grubu**. Kurumsal ağdaki tüm kullanıcıları içeren dahili bir Windows grubu. Herkes grubundaki kullanıcılar, kendilerine verilen izinler doğrultusunda uygulamaya erişebilir.
- **Kullanıcılar veya gruplar**. Her birinin izinlerini ayrı ayrı yapılandırabileceğiniz kullanıcı hesapları. Örneğin, bir eylem Herkes grubu için engellendiyse tek bir kullanıcının veya grubun bu eylemi gerçekleştirmesine izin verebilirsiniz.
- **Oturum kullanıcısı**. Windows oturumunu başlatan kullanıcının hesabı. Bir parola istendiğinde (**Parolayı bu oturum için kaydet** onay kutusu) başka bir oturum kullanıcısına geçiş yapabilirsiniz. Bu durumda Kaspersky Endpoint Security Windows oturumunu başlatan kullanıcının yerine hesap bilgileri girilen kullanıcıyı oturum kullanıcısı olarak değerlendirir.

Geçici parola

Kurumsal ağın dışındaki bir bilgisayar için Kaspersky Endpoint Security'ye geçici erişim vermek amacıyla geçici bir parola kullanılabilir. Yönetici, Kaspersky Security Center'daki bilgisayar özelliklerinde ayrı bir bilgisayar için geçici bir parola oluşturur. Yönetici, geçici parola ile koruma altına alınacak eylemleri seçer ve geçici parolanın geçerlilik dönemini belirler.

Belirteç

Kaspersky Endpoint Security işlevlerine erişmek için bağlı belirteçte depolanan sertifikalar listesinden uygun kullanıcı sertifikasını seçmeniz ve PIN'inizi girmeniz gerekir. Belirteç tabanlı kimlik doğrulama yalnızca Active Directory etki alanındaki kullanıcılar tarafından kullanılabilir. Yönetici, tek bir kullanıcı veya grup için izinleri yapılandırabilir. Belirteç tabanlı kimlik doğrulamanın çalışması için güvenilir bir PKI altyapısı dağıtmanız ve belirteci yönetmek üzere özel bir yazılım yüklemeniz gerekir.

Parola korumasını etkinleştir

Parola koruması, kullanıcıların Kaspersky Endpoint Security'ye erişimlerini kendilerine verilen izinler kapsamında (uygulamadan çıkma izni gibi) kısıtlamanızı sağlar.

Yönetim Konsolu'nda (MMC) Parola korumasını etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
4. **Parola koruması** bloğunda **Ayarlar** düğmesine tıklayın.
   Parola koruma ayarlarını içeren bir pencere açılır.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Parola korumasını etkinleştir** kutucuğunu işaretleyin.
6. **İzinler** bölümünden KLAdmin hesabını seçin.
7. Bir pencere açılır; bu pencerede **Parola**'ya tıklayın ve KLAdmin hesabı için bir parola belirleyin.
   KLAdmin hesabının, parola korumalı tüm işlemleri gerçekleştirme izni bulunur.

   KLAdmin hesabı parolanızı unuttuysanız parolayı ilke özelliklerinden sıfırlayabilirsiniz.
8. Hesap listesine geri dönün.
9. Kurumsal ağdaki tüm kullanıcıların izinlerini ayarlamak için:
   a. **İzinler** bölümünden "Herkes" grubunu seçin.
      Herkes grubu kurumsal ağdaki tüm kullanıcıları içeren dahili bir Windows grubudur.
   b. Açılan pencerede, kullanıcıların parola girmeden gerçekleştirebileceği eylemleri belirlemek için bu işlemlerin yanındaki onay kutularını seçin.
      Bir onay kutusunun işareti kaldırıldığında kullanıcıların eylemi gerçekleştirmesi engellenir. Örneğin, **Uygulamadan çık** izninin yanındaki onay kutusunun işareti kaldırıldığında yalnızca KLAdmin olarak ya da gerekli izne sahip kullanıcı olarak oturum açtığınızda veya geçici parola girdiğinizde uygulamadan çıkabilirsiniz.

Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları vardır. Kaspersky Endpoint Security'ye erişmek için tüm koşulların karşılandığından emin olun.

10. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Parola korumasını etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kendini Koruma** bölümüne gidin.
5. **Parola Koruması** bölümünde, bileşeni etkinleştirmek veya devre dışı bırakmak için **Parola Koruması ETKİN** anahtarını kullanın.
6. KLAdmin hesabının parolasını belirtin ve onaylayın.

   KLAdmin hesabının, parola korumalı tüm işlemleri gerçekleştirme izni bulunur.

   KLAdmin hesabı parolanızı unuttuysanız parolayı ilke özelliklerinden sıfırlayabilirsiniz.
7. Hesap listesine geri dönün.
8. Kurumsal ağdaki tüm kullanıcıların izinlerini ayarlamak için:

   a. Hesaplar tablosunda "Herkes" grubunu seçin.

   Herkes grubu kurumsal ağdaki tüm kullanıcıları içeren dahili bir Windows grubudur.

   b. Açılan pencerede, kullanıcıların parola girmeden gerçekleştirebileceği eylemleri belirlemek için bu işlemlerin yanındaki onay kutularını seçin.

   Bir onay kutusunun işareti kaldırıldığında kullanıcıların eylemi gerçekleştirmesi engellenir. Örneğin, **Uygulamadan çık** izninin yanındaki onay kutusunun işareti kaldırıldığında yalnızca KLAdmin olarak ya da gerekli izne sahip kullanıcı olarak oturum açtığınızda veya geçici parola girdiğinizde uygulamadan çıkabilirsiniz.

   Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları vardır. Kaspersky Endpoint Security'ye erişmek için tüm koşulların karşılandığından emin olun.
9. Değişikliklerinizi kaydedin.

Uygulama arabiriminde Parola korumasını etkinleştirme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Parola koruması** geçiş düğmesini kullanın.

4. KLAdmin hesabının parolasını belirtin ve onaylayın.

   KLAdmin hesabının, parola korumalı tüm işlemleri gerçekleştirme izni bulunur.

   Bilgisayar bir ilke kapsamında çalışıyorsa Yönetici ilke özelliklerinde KLAdmin hesabının parolasını sıfırlayabilir. Bilgisayar Kaspersky Security Center'a bağlı değilse ve KLAdmin hesabının parolasını unuttuysanız parolayı kurtaramazsınız.

5. Kurumsal ağdaki tüm kullanıcıların izinlerini ayarlamak için:

   a. Hesap tablosunda, Herkes grubunun izin listesini açmak için **Düzenle** düğmesine tıklayın.

      Herkes grubu kurumsal ağdaki tüm kullanıcıları içeren dahili bir Windows grubudur.

   b. Kullanıcıların parola girmeden gerçekleştirebileceği eylemleri belirlemek için bu işlemlerin yanındaki onay kutularını seçin.

      Bir onay kutusunun işareti kaldırıldığında kullanıcıların eylemi gerçekleştirmesi engellenir. Örneğin, **Uygulamadan çık** izninin yanındaki onay kutusunun işareti kaldırıldığında yalnızca KLAdmin olarak ya da gerekli izne sahip kullanıcı olarak oturum açtığınızda veya geçici parola girdiğinizde uygulamadan çıkabilirsiniz.

      Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları vardır. Kaspersky Endpoint Security'ye erişmek için tüm koşulların karşılandığından emin olun.

6. Değişikliklerinizi kaydedin.

Parola koruması etkinleştirildiğinde uygulama, kullanıcıların Kaspersky Endpoint Security'ye erişimlerini Herkes grubunda verilen izinlere göre kısıtlar. Herkes grubunda engellenmiş olan eylemleri, yalnızca KLAdmin hesabını veya gerekli izinlere sahip başka bir hesabı kullanıyorsanız ya da geçici parolayı girerseniz gerçekleştirebilirsiniz.

Sadece KLAdmin olarak oturum açtıysanız Parola korumasını devre dışı bırakabilirsiniz. Başka bir kullanıcı hesabı veya geçici parola kullanıyorsanız parola korumasını devre dışı bırakamazsınız.

Parola denetimi sırasında **Parolayı bu oturum için kaydet** onay kutusunu seçebilirsiniz. Bu durumda Kaspersky Endpoint Security, kullanıcı oturum sırasında başka bir parola korumalı eylem gerçekleştirmeye çalıştığında parola sormaz.

Ayrı ayrı kullanıcılara veya gruplara izinler verme

Parola koruması, Kaspersky Endpoint Security'ye bireysel Active Directory kullanıcı hesaplarına ve manuel olarak eklenen kullanıcı hesaplarına erişim izni verir.

Active Directory kullanıcı hesapları

Kaspersky Endpoint Security'ye Active Directory etki alanındaki tek tek kullanıcılara veya gruplara erişim izni verebilirsiniz. Örneğin, uygulamadan çıkış Herkes grubu için engellenmişse **Uygulamadan çık** iznini tek bir kullanıcıya verebilirsiniz. Sonuç olarak yalnızca o kullanıcı olarak veya KLAdmin olarak oturum açtığınızda uygulamadan çıkabilirsiniz.

Ancak bilgisayar etki alanı içinde ise uygulamaya erişim sağlamak için hesabı kimlik bilgilerini kullanabilirsiniz. Bilgisayar etki alanında değilse, KLAdmin hesabını ya da bir geçici parola kullanabilirsiniz.

Manuel olarak eklenen kullanıcı hesapları

Active Directory'de bulunmayan bir kullanıcı hesabı oluşturabilir ve bu kullanıcı hesabına özel izinler atayabilirsiniz. Yani, bir *hizmet kullanıcı hesabı* oluşturabilir ve bunu KLAdmin yerine kullanabilirsiniz. Bu şekilde, KLAdmin parolanızı diğer kullanıcılarla paylaşmanız veya yeni Active Directory kullanıcı hesapları oluşturmanız gerekmez. Herhangi bir kullanıcı adı ve parola belirleyebilirsiniz. Örneğin, hizmet kullanıcısı hesabına **Raporları görüntüle** izni verebilirsiniz. Sonuç olarak, raporların görüntülenmesi "Tümü" grubuna yasaklanmışsa, raporları hizmet kullanıcı hesabını veya KLAdmin kullanıcı hesabını kullanarak açabilirsiniz.

Ayrı ayrı kullanıcılara veya gruplara izinler verme

Yönetim Konsolu'nda (MMC) tek tek kullanıcılara veya gruplara izinler verme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
4. **Parola koruması** bloğunda **Ayarlar** düğmesine tıklayın.

   Parola koruma ayarlarını içeren bir pencere açılır.
5. Hesap tablosunda **Ekle**'ye tıklayın.

6. Eklemek istediğiniz kullanıcı hesabı türünü seçin:

   - **Active Directory'den bir kullanıcı / grup seçin** – Active Directory kullanıcı hesapları.

     Bir kullanıcı hesabı seçmek için **Seç**'e tıklayın. Active Directory'de bir kullanıcı veya grup seçin ve seçiminizi onaylayın.

   - Manuel olarak eklenen bir hizmet kullanıcı hesabı için **Manuel olarak bir kullanıcı / bir kullanıcı grubu ekleyin**.

     Bir hizmet kullanıcı hesabı eklemek için, bir kullanıcı adı ve bir parola girin (örneğin, SecureAdmin).

     İlke ayarlarında bir hizmet kullanıcı hesabı parolasını sıfırlayabilirsiniz. Hizmet kullanıcı hesabı parolası, KLAdmin parolası ile aynı şekilde sıfırlanmalıdır. Parola korumasi ayarlarının düzenlenmesine izin veriliyorsa ("kilit" açıksa) veya bilgisayarda herhangi bir ilke uygulanmıyorsa, uygulama arabiriminde hizmet kullanıcı hesabının parolasını sıfırlayabilirsiniz. Bunu yapmak için, KLAdmin parolasını kullanarak hizmet kullanıcı hesabı bilgilerindeki değişiklikleri onaylayın.

7. **İzinler** listesinde, seçilen kullanıcı veya grubun parola istenmeden gerçekleştirmesine izin verilecek eylemlerin yanındaki onay kutularını işaretleyin.

   Bir onay kutusunun işareti kaldırıldığında kullanıcıların eylemi gerçekleştirmesi engellenir. Örneğin, **Uygulamadan çık** izninin yanındaki onay kutusunun işareti kaldırıldığında yalnızca KLAdmin olarak ya da gerekli izne sahip kullanıcı olarak oturum açtığınızda veya geçici parola girdiğinizde uygulamadan çıkabilirsiniz.

   Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları vardır. Kaspersky Endpoint Security'ye erişmek için tüm koşulların karşılandığından emin olun.

8. Değişikliklerinizi kaydedin.

Web Console'da tek tek kullanıcılara veya gruplara izinler verme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Kendini Koruma** bölümüne gidin.
5. **Parola Koruması** bloğunda **Kullanıcı izinleri** bağlantısına tıklayın.

   Bu, Parola Etkinleştirme izinlerini vermek için formu açar.
6. **Ekle**'ye tıklayın.
7. Eklemek istediğiniz kullanıcı hesabı türünü seçin:

   - **Active Directory** - Active Directory kullanıcı hesapları arasından seçim yapın.

     Bir kullanıcı hesabı seçmek için **Düzenle**'ye tıklayın. Active Directory'de bir kullanıcı veya grup seçin ve seçiminizi onaylayın.

   - Manuel olarak eklenen bir hizmet kullanıcı hesabı için **manuel olarak ekle**.

     Bir hizmet kullanıcı hesabı eklemek için, bir kullanıcı adı ve bir parola girin (örneğin, SecureAdmin).

İlke ayarlarında bir hizmet kullanıcı hesabı parolasını sıfırlayabilirsiniz. Hizmet kullanıcı hesabı parolası, KL Admin parolası ile aynı şekilde sıfırlanmalıdır. Parola korumasi ayarlarının düzenlenmesine izin veriliyorsa ("kilit" açıksa) veya bilgisayarda herhangi bir ilke uygulanmıyorsa, uygulama arabiriminde hizmet kullanıcı hesabının parolasını sıfırlayabilirsiniz. Bunu yapmak için, KL Admin parolasını kullanarak hizmet kullanıcı hesabı bilgilerindeki değişiklikleri onaylayın.

8. **İzinler** listesinde, seçilen kullanıcı veya grubun parola istenmeden gerçekleştirmesine izin verilecek eylemlerin yanındaki onay kutularını işaretleyin.

   Bir onay kutusunun işareti kaldırıldığında kullanıcıların eylemi gerçekleştirmesi engellenir. Örneğin, **Uygulamadan çık** izninin yanındaki onay kutusunun işareti kaldırıldığında yalnızca KL Admin olarak ya da gerekli izne sahip kullanıcı olarak oturum açtığınızda veya geçici parola girdiğinizde uygulamadan çıkabilirsiniz.

   Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları vardır. Kaspersky Endpoint Security'ye erişmek için tüm koşulların karşılandığından emin olun.

9. **Ekle**'ye tıklayın.

10. Değişikliklerinizi kaydedin.

Uygulamanın arabiriminde tek tek kullanıcılara veya gruplara izinler verme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.

3. Hesap tablosunda **Ekle**'ye tıklayın.

4. Eklemek istediğiniz kullanıcı hesabı türünü seçin:

   - **Active Directory'den bir kullanıcı / grup seçin** – Active Directory kullanıcı hesapları.

     Bir kullanıcı hesabı seçmek için **Kullanıcı veya grup seçin**'e tıklayın. Active Directory'de bir kullanıcı veya grup seçin ve seçiminizi onaylayın.

   - Manuel olarak eklenen bir hizmet kullanıcı hesabı için **Manuel olarak bir kullanıcı ekleyin**.

     Bir hizmet kullanıcı hesabı eklemek için, bir kullanıcı adı ve bir parola girin (örneğin, SecureAdmin).

     İlke ayarlarında bir hizmet kullanıcı hesabı parolasını sıfırlayabilirsiniz. Hizmet kullanıcı hesabı parolası, KL Admin parolası ile aynı şekilde sıfırlanmalıdır. Parola korumasi ayarlarının düzenlenmesine izin veriliyorsa ("kilit" açıksa) veya bilgisayarda herhangi bir ilke uygulanmıyorsa, uygulama arabiriminde hizmet kullanıcı hesabının parolasını sıfırlayabilirsiniz. Bunu yapmak için, KL Admin parolasını kullanarak hizmet kullanıcı hesabı bilgilerindeki değişiklikleri onaylayın.

5. **İzinler** listesinde, seçilen kullanıcı veya grubun parola istenmeden gerçekleştirmesine izin verilecek eylemlerin yanındaki onay kutularını işaretleyin.

   Bir onay kutusunun işareti kaldırıldığında kullanıcıların eylemi gerçekleştirmesi engellenir. Örneğin, **Uygulamadan çık** izninin yanındaki onay kutusunun işareti kaldırıldığında yalnızca KL Admin olarak ya da gerekli izne sahip kullanıcı olarak oturum açtığınızda veya geçici parola girdiğinizde uygulamadan çıkabilirsiniz.

Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları vardır. Kaspersky Endpoint Security'ye erişmek için tüm koşulların karşılandığından emin olun.

6. Değişikliklerinizi kaydedin.

Sonuç olarak Herkes grubu için uygulamaya erişim sınırlandığında kullanıcılara, kendi kişisel izinlerine göre Kaspersky Endpoint Security'ye erişim izni verilir.

İzinler vermek için geçici parola kullanma

Kurumsal ağın dışındaki bir bilgisayar için Kaspersky Endpoint Security'ye geçici erişim vermek amacıyla geçici bir parola kullanılabilir. Bu, kullanıcının KLAdmin hesabı kimlik bilgilerini almadan engellenen bir eylem gerçekleştirmesini sağlamak için gereklidir. Geçici bir parola kullanmak için bilgisayar Kaspersky Security Center'a eklenmelidir.

Bir kullanıcının geçici bir parola kullanarak Yönetim Konsolu (MMC) aracılığıyla engellenen bir eylemi gerçekleştirmesine izin verme

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, **Cihazlar** sekmesini seçin.
4. İlke özellikleri penceresini açmak için çift tıklayın.
5. Bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
6. Bilgisayarda yüklü Kaspersky uygulamaları listesinde **Kaspersky Endpoint Security for Windows (14.2)** öğesini seçin ve çift tıklayarak uygulama özelliklerini açın.
7. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
8. **Parola koruması** bloğunda **Ayarlar** düğmesine tıklayın.
9. Açılan pencerede, **Geçici parola** bloğunda **Geçici parolaların listesi** düğmesine tıklayın.

   Geçici parolaların yönetimi penceresi açılır.
10. **Ekle**'ye tıklayın.
11. **Sona erme tarihi** alanında geçici parolanın süresinin dolacağı sona erme tarihini belirtin.
12. **Geçici parola kapsamı** tablosunda, geçici parola geçerli iken kullanıcı tarafından kullanılabilecek işlemlerin karşısındaki onay kutularını işaretleyin.
13. **Oluştur**'a tıklayın.

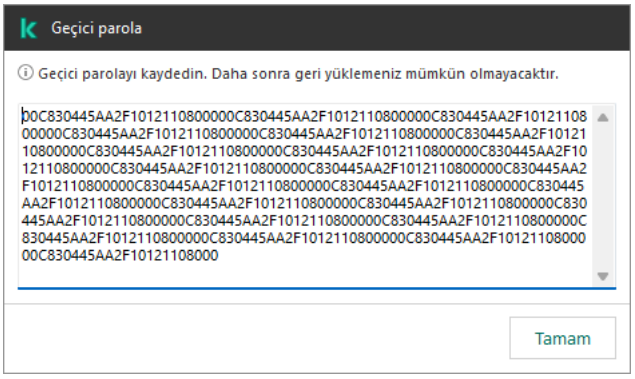
    Geçici parolayı içeren bir pencere açılır (aşağıdaki şekle bakın).
14. Parolayı kopyalayın ve kullanıcıya verin.

Bir kullanıcının geçici bir parola kullanarak Web Console ve Cloud Console aracılığıyla engellenen bir eylemi gerçekleştirmesine izin verme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Bir kullanıcının engellenen bir eylemi gerçekleştirmesine izin vermek istediğiniz bilgisayarın adına tıklayın.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows**'a tıklayın.

   Bu, yerel uygulama ayarlarını açar.
5. **Uygulama ayarları** sekmesini seçin.
6. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
7. **Geçici parolalar** bloğunda **Ekle** düğmesine tıklayın.
8. **Sona erme tarihi** alanında geçici parolanın süresinin dolacağı sona erme tarihini belirtin.
9. **Geçici parola kapsamı** tablosunda, geçici parola geçerli iken kullanıcı tarafından kullanılabilecek işlemlerin karşısındaki onay kutularını işaretleyin.
10. **Oluştur**'a tıklayın.

    Geçici parolayı içeren bir pencere açılır.
11. Parolayı kopyalayın ve kullanıcıya verin.



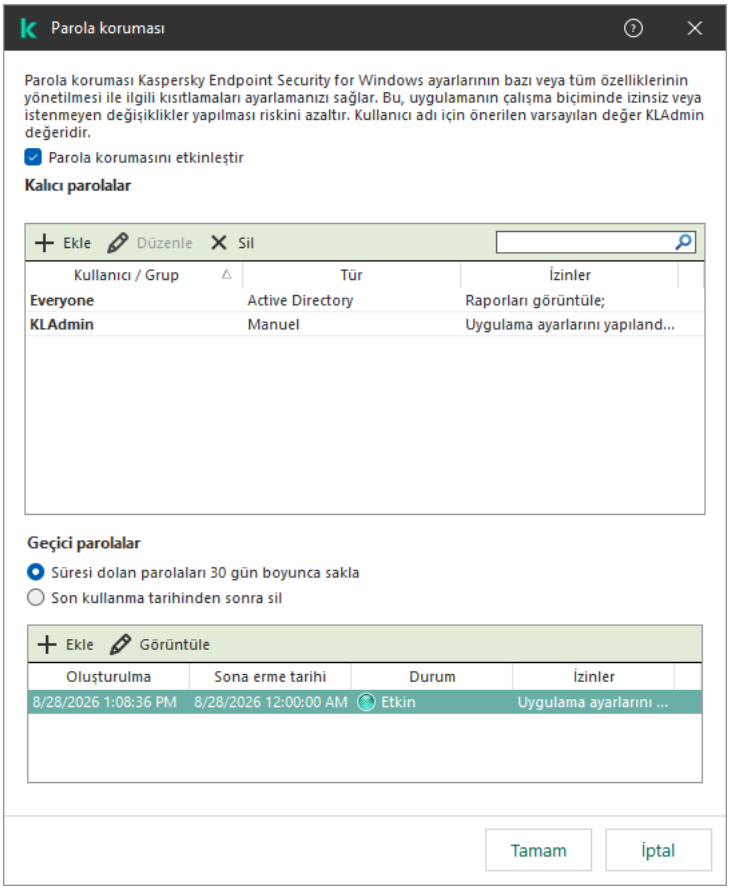
Geçici parola

Geçici parolanın iptal edilmesi

Kaspersky Endpoint Security for Windows, 12.9 sürümünden itibaren *Geçici Parolaların Yönetimi* işlevini içerir. Geçici parolaların yönetimi aşağıdaki eylemleri gerçekleştirmenizi sağlar:

- Parola geçmişini kaydetme (30 güne kadar).
- Geçici parola durumunu izleme: *Etkin*, *Süresi doldu*, *İptal edildi*.

- Geçici parolaları iptal edin.



Geçici parolaların yönetimi

Geçici parolaların yönetimi, parolanın durumunu günceller ve parolayı yalnızca bilgisayar Kaspersky Security Center ile senkronize edildikten sonra iptal eder.

Yönetim Konsolu (MMC) kullanılarak geçici parolanın iptal edilmesi

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, **Cihazlar** sekmesini seçin.
4. İlke özellikleri penceresini açmak için çift tıklayın.
5. Bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
6. Bilgisayarda yüklü Kaspersky uygulamaları listesinde **Kaspersky Endpoint Security for Windows (14.2)** öğesini seçin ve çift tıklayarak uygulama özelliklerini açın.
7. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
8. **Parola koruması** bloğunda **Ayarlar** düğmesine tıklayın.
9. Bu bir pencere açar; bu pencerede **Geçici parola** altında, süresi dolan parolalar için depolama ayarlarını yapılandırın.

10. **Geçici parolaların listesi** seçeneğine tıklayın.

    Geçici parolaların yönetimi penceresi açılır. Geçici parolaların yönetimi parolanın son kullanma tarihini, parolanın durumunu ve izinlerin listesini görüntüler.

11. İptal etmek istediğiniz etkin geçici parolayı seçin ve özelliklerini açmak için parolaya çift tıklayın.

12. Açılan pencerede **İptal et** düğmesine tıklayın.

13. Değişikliklerinizi kaydedin. İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın .

Web Console ve Cloud Console kullanılarak geçici parolanın iptal edilmesi

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.

2. Bir kullanıcının engellenen bir eylemi gerçekleştirmesine izin vermek istediğiniz bilgisayarın adına tıklayın.

3. **Uygulamalar** sekmesini seçin.

4. **Kaspersky Endpoint Security for Windows**'a tıklayın.

    Bu, yerel uygulama ayarlarını açar.

5. **Uygulama ayarları** sekmesini seçin.

6. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.

7. **Geçici parolalar** bölümünde, süresi dolan parolaların saklanmasını yapılandırın.

8. **Geçici parola** bağlantısına tıklayın.

    Geçici parolaların yönetimi penceresi açılır. Geçici parolaların yönetimi parolanın son kullanma tarihini, parolanın durumunu ve izinlerin listesini görüntüler.

9. İptal etmek istediğiniz etkin geçici parolayı seçin.

10. Açılan pencerede **Parolayı iptal et** düğmesine tıklayın.

11. Değişikliklerinizi kaydedin. İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın .

Sonuç olarak, Geçici parolaların yönetimi parolanın durumunu *İptal etme (bir ana bilgisayar ile senkronize etme)* olarak ayarlar. Bilgisayarı Kaspersky Security Center ile senkronize ettikten sonra, uygulama geçici parolayı iptal eder ve verilen izinleri hemen engeller.

Parola koruması izinlerinin özel boyutları

Parola koruması izinlerinin dikkate alınması gereken bazı önemli boyutları ve sınırlamaları vardır.

Uygulama ayarlarını yapılandır

Bir kullanıcının bilgisayarı bir ilkeye göre çalıştığında, ilkedeki tüm gerekli ayarların düzenlenebildiğinden emin olun (öznitelikleri açık).

Uygulamadan çık

Özel hususlar veya sınırlamalar yoktur.

Koruma bileşenlerini devre dışı bırak

- Herkes grubu için koruma bileşenlerini devre dışı bırakma izni vermek mümkün değildir. KLAdmin dışındaki kullanıcıların denetim bileşenlerini devre dışı bırakmasına izin vermek için Parola koruması ayarlarında **Koruma bileşenlerini devre dışı bırak** iznine sahip bir kullanıcı veya grup ekleyin.
- Bir kullanıcının bilgisayarı bir ilkeye göre çalıştığında, ilkedeki tüm gerekli ayarların düzenlenebildiğinden emin olun (öznitelikleri açık).
- Uygulama ayarlarında koruma bileşenlerini devre dışı bırakmak için bir kullanıcı **Uygulama ayarlarını yapılandır** iznine sahip olmalıdır.
- Bağlam menüsü (**Korumayı duraklat** menü öğesi kullanılarak) üzerinden koruma bileşenlerini devre dışı bırakmak için bir kullanıcı, **Denetim bileşenlerini devre dışı bırak** iznine ek olarak **Koruma bileşenlerini devre dışı bırak** iznine de sahip olmalıdır.

Denetim bileşenlerini devre dışı bırak

- Herkes grubu için denetim bileşenlerini devre dışı bırakma izni vermek mümkün değildir. KLAdmin dışındaki kullanıcıların denetim bileşenlerini devre dışı bırakmasına izin vermek için Parola koruması ayarlarında **Denetim bileşenlerini devre dışı bırak** iznine sahip bir kullanıcı veya grup ekleyin.
- Bir kullanıcının bilgisayarı bir ilkeye göre çalıştığında, ilkedeki tüm gerekli ayarların düzenlenebildiğinden emin olun (öznitelikleri açık).
- Uygulama ayarlarında denetim bileşenlerini devre dışı bırakmak için bir kullanıcı **Uygulama ayarlarını yapılandır** iznine sahip olmalıdır.
- Bağlam menüsü (**Korumayı duraklat** menü öğesi kullanılarak) üzerinden denetim bileşenlerini devre dışı bırakmak için bir kullanıcı **Koruma bileşenlerini devre dışı bırak** iznine ek olarak **Denetim bileşenlerini devre dışı bırak** iznine de sahip olmalıdır.

Kaspersky Security Center ilkesini devre dışı bırak

"Herkes" grubuna Kaspersky Security Center ilkesini devre dışı bırakma izni veremezsiniz. KLAdmin dışındaki kullanıcıların ilkeyi devre dışı bırakmasına izin vermek için Parola koruması ayarlarında **Kaspersky Security Center ilkesini devre dışı bırak** iznine sahip bir kullanıcı veya grup ekleyin.

Anahtarı kaldır

Özel hususlar veya sınırlamalar yoktur.

Uygulamayı kaldır/değiştir/geri yükle

"Tümü" grubu için uygulamanın kaldırılmasına, değiştirilmesine ve geri yüklenmesine izin verdiyseniz, kullanıcı bu işlemleri gerçekleştirmek istediğinde Kaspersky Endpoint Security bir parola istemez. Bu nedenle, etki alanı dışındaki kullanıcılar da dahil olmak üzere herhangi bir kullanıcı uygulamayı yükleyebilir, değiştirebilir veya geri yükleyebilir.

Şifrelenmiş sürücülerdeki verilere erişimi yeniden sağla

Yalnızca KLAdmin olarak oturum açtığınızda, şifrelenmiş sürücülerdeki verilere erişimi geri yükleyebilirsiniz. Bu eylemi gerçekleştirme izni başka bir kullanıcıya verilemez.

Raporları görüntüle

Özel hususlar veya sınırlamalar yoktur.

Yedekten geri yükle

Özel hususlar veya sınırlamalar yoktur.

Ayarları dışa aktar

Varsayılan olarak, "Tümü" grubuna uygulama ayarlarının dışa aktarılması reddedilir. KLAdmin kullanıcı hesabını kullanarak uygulama ayarlarını dışa aktarabilirsiniz. Uygulama ayarlarının dışa aktarılması, yalnızca uygulama arabiriminde Kaspersky Endpoint Security ayarlarını içeren bir yapılandırma dosyası oluşturmayı içerir. İzin, tarama dışlamaları, güvenilen web adresleri, güvenilen aygıtlar veya uygulama bileşenleri tarafından tutulan diğer listelerin dışa aktarılmasını kısıtlamaz.

KLAdmin parolasını sıfırlama

KLAdmin hesabı parolanızı unuttuysanız parolayı ilke özelliklerinden sıfırlayabilirsiniz. Parolayı uygulama arabiriminden sıfırlayamazsınız.

Bir geçici parola kullanarak parola korumalı eylemler gerçekleştirebilirsiniz. Bu durumda KLAdmin kimlik bilgilerini girmenize gerek yoktur.

Bilgisayar Kaspersky Security Center'a bağlı değilse ve KLAdmin hesabının parolasını unuttuysanız parolayı kurtaramazsınız.

KLAdmin hesabı parolasını Yönetim Konsolu (MMC) kullanarak sıfırlama

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
4. **Parola koruması** bloğunda **Ayarlar** düğmesine tıklayın.
5. Açılan pencerede, **Parola korumasını etkinleştir** kutucuğunu işaretleyin.
6. Değişikliklerinizi kaydedin.
7. **Parola korumasını etkinleştir** onay kutusunu tekrar işaretleyin.
8. **Tamam**'a tıklayın.
   Yönetici parolası penceresi açılır.
9. KLAdmin hesabının yeni parolasını belirtin ve onaylayın.
10. Değişikliklerinizi kaydedin.

KLAdmin hesabı parolasını Web Console ve Cloud Console'da sıfırlama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows 14.2** öğesine tıklayın.
   Bu, yerel uygulama ayarlarını açar.
5. **Uygulama ayarları** sekmesini seçin.
6. **Genel Ayarlar** → **Kendini Koruma** bölümüne gidin.
7. **Parola koruması** bölümünden **Parola koruması** anahtarını kapalı duruma getirin.
8. Değişikliklerinizi kaydedin.
9. **Parola koruması** anahtarını tekrar açık duruma getirin.

10. KLAdmin hesabının yeni parolasını belirtin ve onaylayın.

11. Değişikliklerinizi kaydedin.

Böylece, ilke uygulandıktan sonra KLAdmin hesabınızın parolası güncellenir.

Yönetim Sunucusu bağlantı koruması

Bilgisayarın Yönetim Sunucusuna bağlanması, Kaspersky Security Center'ın *Ağ Aracısı* bileşeni kullanılarak gerçekleştirilir. Bir saldırgan sunucu bağlantı ayarlarını değiştirmek için yeterli haklara sahip olduğunda, bilgisayarı güvenilmez bir sunucuya bağlama riski vardır. Bu, saldırganın kendi grup ilkelerini uygulamasına ve örneğin uygulamanın kendini savunmasını devre dışı bırakmasına olanak tanır. Kaspersky Endpoint Security, bir bilgisayarın farklı bir sunucuya yetkisiz olarak yeniden bağlanmasını önleyebilir. Sunucu bağlantısını korumak için, uygulama bir parola belirlemeyi ve Password-Based key Derivation Function (PBKDF2)'yi kullanmayı önerir. Sonuç olarak, uygulamaya parola olmadan erişim mümkün olmaz.

> Kaspersky Endpoint Security ve Ağ Aracısının yetkisiz erişime karşı kapsamlı bir şekilde korunmasını sağlamak için ek korumayı etkinleştirmenizi öneririz. Kaspersky Endpoint Security için Parola korumasının etkinleştirilmesini öneririz. Ağ Aracısını korumak için bir kaldırma parolası ayarlanmasını öneririz. Ağ Aracısının kaldırılmasına karşı koruma hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center Yardımı 'na başvurun.

Bilgisayarın Yönetim Sunucusuna bağlantısının yönetilmesi *Yönetim Sunucusu bağlantı koruması* görevi kullanılarak gerçekleştirilir. Görev şu işlemleri gerçekleştirmenize izin verir:

- Sunucu bağlantısını korumak için bir parola belirleyin.
- Parolayı değiştirin.
- Bilgisayarı farklı bir sunucuya yeniden bağlayın.
- Sunucu bağlantı korumasını devre dışı bırakın.

Yönetim Sunucusuna bağlanırken bilgisayarın kimlik doğrulaması

Bir parola belirledikten sonra, uygulama parolanın PBKDF2 dönüşümünü kullanarak bir veri dizisi oluşturur. Uygulama daha sonra bu veri dizisini Ağ Aracısı anahtarını kullanarak şifreler. Uygulama, sonraki bağlantılar için Yönetim Sunucusunun haklarını ve ayrıcalıklarını kontrol etmek amacıyla şifrelenmiş veri dizisini kullanır.

Daha sonra, bilgisayar Yönetim Sunucusuna yeniden bağlanmaya çalışıldığında, uygulama veri dizisinin şifresini Ağ Aracısı anahtarıyla çözer ve yerel kopyayla karşılaştırır. Eşleşmezlerse uygulamaya erişim kısıtlanır.

Yönetim Sunucusu bağlantı koruması

Yönetim Konsolu'nda (MMC) sunucu bağlantı koruması için parola belirleme

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Yönetim Sunucusu bağlantı koruması** seçimini yapın.

Adım 2. Yönetim Sunucusu bağlantısını koruma

Yönetim Sunucusu bağlantısını korumak için bir parola belirleyin:

1. **Yönetim Sunucusu bağlantı koruması** bölümünde **Bir parola ile koruyun** seçimini yapın.
2. **Yönetim Sunucusu** açılır listesinden **Yeni sunucu** seçimini yapın.
3. **Yönetim Sunucusuna bağlantı için parola** alanında, Yönetim Sunucusuna bağlanmak için bir parola belirleyin ve onaylayın.

   Bu parolayı unutursanız, bir görev kullanarak parolayı değiştirebilirsiniz.

4. Kaspersky Endpoint Security 12.7 veya uygulamanın önceki bir sürümü dağıtılmışsa, **Önceki uygulama sürümleri (12.7 ve daha düşük) için parola şifreleme uyumluluğunu etkinleştirin** onay kutusunu seçin.

   Kaspersky Endpoint Security 12.8 for Windows sürümünden itibaren uygulama daha güçlü parola şifrelemesi kullanır. Kaspersky Endpoint Security 12.8 veya sonraki bir sürümü kullanıyorsanız, bu onay kutusunun işaretini kaldırmanızı ve daha güçlü parola şifrelemesini kullanmanızı öneririz. Uygulamanın önceki sürümleri güçlü parola şifrelemesini desteklemez. Görevi çalıştırmak için onay kutusunu seçmelisiniz.

3. Adım. Görevi çalıştıracak hesabı seçme

Varsayılan hesap seçimini yapın. Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

4. Adım. Bir görev başlatma zamanlaması yapılandırma

Zamanlanmış başlatma bölümünde **Elle** seçimini yapın.

5. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Ana sunucu bağlantı parolası*.

6. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin ya da görevi manuel olarak çalıştırın. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console ve Cloud Console'da sunucu bağlantı koruması için parola belirleme

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Yönetim Sunucusu bağlantı koruması** seçimini yapın.

   c. **Görev adı** alanına, *Ana sunucu bağlantı parolası* gibi bir kısa açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Bir varsayılan kullanıcı hesabı seçin. Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Kaspersky Endpoint Security'nin **Yönetim Sunucusu bağlantı koruması** görevine tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. **Yönetim Sunucusu bağlantı koruması** bölümünde **Bir parola ile koruyun** seçimini yapın.

10. **Yönetim Sunucusuna bağlantı** açılır listesinden **Yeni parola** seçimini yapın.

11. **Yönetim Sunucusuna bağlantı için parola** alanında, Yönetim Sunucusuna bağlanmak için bir parola belirleyin ve onaylayın.

    Bu parolayı unutursanız, bir görev kullanarak parolayı değiştirebilirsiniz.

12. Kaspersky Endpoint Security 12.7 veya uygulamanın önceki bir sürümü dağıtılmışsa, **Önceki uygulama sürümleri (12.7 ve daha düşük) için parola şifreleme uyumluluğunu etkinleştirin** onay kutusunu seçin.

    Kaspersky Endpoint Security 12.8 for Windows sürümünden itibaren uygulama daha güçlü parola şifrelemesi kullanır. Kaspersky Endpoint Security 12.8 veya sonraki bir sürümü kullanıyorsanız, bu onay kutusunun işaretini kaldırmanızı ve daha güçlü parola şifrelemesini kullanmanızı öneririz. Uygulamanın önceki sürümleri güçlü parola şifrelemesini desteklemez. Görevi çalıştırmak için onay kutusunu seçmelisiniz.

13. Değişikliklerinizi kaydedin.

14. Görevin yanındaki onay kutusunu seçin.

15. **Başlat**'a tıklayın.

Görevin durumunu ve görevin başarıyla veya bir hatayla tamamlandığı aygıtların sayısını izleyebilirsiniz.

Bilgisayarı farklı bir Yönetim Sunucusuna yeniden bağlama

Bilgisayarın farklı bir Yönetim Sunucusuna yeniden bağlanması aşağıdaki adımları içerir:

1. Geçerli `[KSC1]` sunucusunun konsolunda, Ağ Aracısı için *Yönetim Sunucusunu Değiştir* görevini çalıştırın.

   Görevi çalıştırdıktan sonra bilgisayar yeni `[KSC2]` sunucusuna yeniden bağlanır.

   Bilgisayar `[KSC1]` sunucu konsolunda *Kritik* durumuyla görüntülenecektir. Uygulamayı ilkeler kullanarak yapılandırmak ya da görevleri bilgisayarda uzaktan çalıştırmak mümkündür.

2. Yeni `[KSC2]` sunucusunda, Kaspersky Endpoint Security için yeni bir *Yönetim Sunucusu bağlantı koruması* görevi oluşturun. Görev özelliklerinde, önceki sunucunun parolasını girin ve yeni sunucu için bir parola belirleyin.

   Yönetim Konsolu'nda (MMC) yeni bir sunucuya yeniden bağlanmak için yeni bir parola belirleme

   1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

      Görevler listesi açılır.

   2. **Yeni görev**'e tıklayın.

      Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Yönetim Sunucusu bağlantı koruması** seçimini yapın.

Adım 2. Yönetim Sunucusu bağlantısını koruma

Yeni Yönetim Sunucusuna bağlantıyı korumak için bir parola belirleyin:

1. **Yönetim Sunucusu bağlantı koruması** bölümünde **Bir parola ile koruyun** seçimini yapın.
2. **Yönetim Sunucusu** açılır listesinden **Başka bir sunucudan yeniden bağlan** seçimini yapın.
3. **Geçerli parola** alanına, daha önce kullanılan güvenilir sunucuya bağlantı için belirlenen parolayı girin.
4. **Yeni parola** alanında, yeni Yönetim Sunucusuna bağlanmak için bir parola belirleyin ve parolayı onaylayın.

   Bu parolayı unutursanız, bir görev kullanarak parolayı değiştirebilirsiniz.
5. Kaspersky Endpoint Security 12.7 veya uygulamanın önceki bir sürümü dağıtılmışsa, **Önceki uygulama sürümleri (12.7 ve daha düşük) için parola şifreleme uyumluluğunu etkinleştirin** onay kutusunu seçin.

   Kaspersky Endpoint Security 12.8 for Windows sürümünden itibaren uygulama daha güçlü parola şifrelemesi kullanır. Kaspersky Endpoint Security 12.8 veya sonraki bir sürümü kullanıyorsanız, bu onay kutusunun işaretini kaldırmanızı ve daha güçlü parola şifrelemesini kullanmanızı öneririz. Uygulamanın önceki sürümleri güçlü parola şifrelemesini desteklemez. Görevi çalıştırmak için onay kutusunu seçmelisiniz.

3. Adım. Görevi çalıştıracak hesabı seçme

Varsayılan hesap seçimini yapın. Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

4. Adım. Bir görev başlatma zamanlaması yapılandırma

Zamanlanmış başlatma bölümünde **Elle** seçimini yapın.

5. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Ana sunucu bağlantı parolası*.

6. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin ya da görevi manuel olarak çalıştırın. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console ve Cloud Console'da yeni bir sunucuya yeniden bağlanmak için yeni bir parola belirleme

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Yönetim Sunucusu bağlantı koruması** seçimini yapın.

   c. **Görev adı** alanına, *Ana sunucu bağlantı parolası* gibi bir kısa açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Bir varsayılan kullanıcı hesabı seçin. Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Kaspersky Endpoint Security'nin **Yönetim Sunucusu bağlantı koruması** görevine tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. **Yönetim Sunucusu bağlantı koruması** bölümünde **Bir parola ile koruyun** seçimini yapın.

10. **Yönetim Sunucusuna bağlantı** açılır listesinden **Başka bir sunucudan yeniden bağlan** seçimini yapın.

11. **Geçerli parola** alanına, daha önce kullanılan güvenilir sunucuya bağlantı için belirlenen parolayı girin.

12. **Yeni parola** alanında, yeni Yönetim Sunucusuna bağlanmak için bir parola belirleyin ve parolayı onaylayın.

    Bu parolayı unutursanız, bir görev kullanarak parolayı değiştirebilirsiniz.

13. Kaspersky Endpoint Security 12.7 veya uygulamanın önceki bir sürümü dağıtılmışsa, **Önceki uygulama sürümleri (12.7 ve daha düşük) için parola şifreleme uyumluluğunu etkinleştirin** onay kutusunu seçin.

    Kaspersky Endpoint Security 12.8 for Windows sürümünden itibaren uygulama daha güçlü parola şifrelemesi kullanır. Kaspersky Endpoint Security 12.8 veya sonraki bir sürümü kullanıyorsanız, bu onay kutusunun işaretini kaldırmanızı ve daha güçlü parola şifrelemesini kullanmanızı öneririz. Uygulamanın önceki sürümleri güçlü parola şifrelemesini desteklemez. Görevi çalıştırmak için onay kutusunu seçmelisiniz.

14. Değişikliklerinizi kaydedin.

15. Görevin yanındaki onay kutusunu seçin.

16. **Başlat**'a tıklayın.

    Görevin durumunu ve görevin başarıyla veya bir hatayla tamamlandığı aygıtların sayısını izleyebilirsiniz.

Görevi tamamladıktan sonra, yeni [KSC2] sunucusunun konsolunda bilgisayarın *Tamam* durumuna sahip olduğundan emin olun. Görevleri uzaktan çalıştırıp çalıştıramayacağınızı ve ilkeleri kullanarak uygulamayı yapılandırıp yapılandıramayacağınızı test edin.

Yönetim Sunucusu bağlantı parolasının sıfırlanması

Yönetim Sunucusu bağlantı parolasını unutmayız ya da parolanın ele geçirilmiş olması durumunda, parolayı görev özelliklerinden sıfırlayabilirsiniz. Ayrıca farklı Yönetim Sunucusu bağlantı koruma durumlarına sahip bir grup bilgisayar için parolayı sıfırlayabilir ve yeni bir parola belirleyebilirsiniz. Yani, bazı bilgisayarlarda koruma etkinleştirilmiş ve bazılarında devre dışı bırakılmışsa, görev tüm bilgisayarlar için bir parola belirler.

Yönetim Sunucusu bağlantı parolasını yalnızca bilgisayarın bağlı olduğu güvenilir sunucunun konsolundan sıfırlayabilirsiniz.

Yönetim Sunucusu bağlantı parolasını Yönetim Konsolu (MMC) kullanarak sıfırlama

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. **Yönetim Sunucusu bağlantı koruması** görevini seçin ve çift tıklayarak görev özelliklerini açın.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.
5. **Yönetim Sunucusu bağlantı koruması** bölümünde **Koru ve parolayı değiştir** seçimini yapın.
6. **Yönetim Sunucusuna bağlantı için parola** alanında, geçerli güvenilir sunucuya bağlanmak için bir parola belirleyin ve parolayı onaylayın.
7. Değişikliklerinizi kaydedin.
8. Görevi çalıştırın.

Yönetim Sunucusu bağlantı parolasını Web Console ve Cloud Console'da sıfırlama

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.
2. Kaspersky Endpoint Security'nin **Yönetim Sunucusu bağlantı koruması** görevine tıklayın.

   Görev özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yönetim Sunucusu bağlantı koruması** bölümünde **Koru ve parolayı değiştir** seçimini yapın.
5. **Yönetim Sunucusuna bağlantı için parola** alanında, geçerli güvenilir sunucuya bağlanmak için bir parola belirleyin ve parolayı onaylayın.
6. Değişikliklerinizi kaydedin.

7. Görevin yanındaki onay kutusunu seçin.
8. **Başlat**'a tıklayın.

Sonuç olarak, görev tamamlandıktan sonra Yönetim Sunucusu bağlantı parolası sıfırlanır.

Yönetim Sunucusu bağlantı korumasını devre dışı bırakma

Yönetim Sunucusu bağlantı korumasını yalnızca bilgisayarın bağlı olduğu güvenilir sunucunun konsolundan uzaktan devre dışı bırakabilirsiniz. Korumayı komut satırından yerel olarak devre dışı bırakmanız da mümkündür.

Yönetim Konsolu'nda (MMC) sunucu bağlantı korumasını devre dışı bırakma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Görevler**'i seçin.
3. **Yönetim Sunucusu bağlantı koruması** görevini seçin ve çift tıklayarak görev özelliklerini açın.
4. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.
5. **Yönetim Sunucusu bağlantı koruması** bölümünden **Korumayın** seçimini yapın.
6. Değişikliklerinizi kaydedin.
7. Görevi çalıştırın.
   Görevin durumunu ve görevin başarıyla veya bir hatayla tamamlandığı aygıtların sayısını izleyebilirsiniz.

Web Console ve Cloud Console'da sunucu bağlantı korumasını devre dışı bırakma

1. Web Console ana penceresinden **Görevler** seçimini yapın.
   Görevler listesi açılır.
2. Kaspersky Endpoint Security'nin **Yönetim Sunucusu bağlantı koruması** görevine tıklayın.
   Görev özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yönetim Sunucusu bağlantı koruması** bölümünde **Parola ile koruma** seçimini yapın.
5. Değişikliklerinizi kaydedin.
6. Görevin yanındaki onay kutusunu seçin.
7. **Başlat**'a tıklayın.
   Görevin durumunu ve görevin başarıyla veya bir hatayla tamamlandığı aygıtların sayısını izleyebilirsiniz.

Komut satırında sunucu bağlantı korumasını devre dışı bırakma

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

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Burada `<password>`, KL Admin kullanıcı hesabının ya da *Yönetim Sunucusu bağlantı koruması* görevinin parolasıdır. Parametre belirtilmezse Kaspersky Endpoint Security bir sonraki satırda parola girmenizi ister.

> Bu komutu yürütmek için Parola koruması etkinleştirilmelidir.

Örnek

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Veri Şifreleme

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. Kaspersky Endpoint Security Advanced Encryption Standard (AES) şifreleme algoritmasını kullanır.

Lisansın süresi sona erdiyse uygulama yeni verileri şifrelemez ve eski şifrelenmiş veriler şifrelenmiş olarak kalmaya ve kullanılabilir olmaya devam eder. Bu durumda, yeni verilerin şifrelenmesi uygulamanın şifrelemeye izin veren yeni bir lisans ile etkinleştirilmesini gerektirir.

Kaspersky Endpoint Security, Arm tabanlı bir bilgisayara yüklenmişse, yalnızca BitLocker Sürücü Şifreleme özelliği kullanılabilir. Uygulama, diğer veri şifreleme bileşenlerini desteklemez.

Lisansınızın süresi sona erdiyse veya Son Kullanıcı Lisans Sözleşmesi ihlal edildiyse lisans anahtarı, 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 sürücülerinde Dosya Düzeyinde 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 ilke 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.
- **Çıkarılabilir sürücüleri şifreleme**. 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.

- **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 paketler 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.

- **Tam Disk Şifreleme**. 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 Trusted Platform Module (TPM) bulunuyorsa BitLocker, şifrelenmiş sabit sürücüye erişim sağlayan kurtarma anahtarlarını bu modülü kullanarak depolar. Bilgisayar başlatıldığında BitLocker, Güvenilir Platform Modülü'nden sabit sürücü kurtarma anahtarlarını ister ve sürücünün kilidini kaldırır. Kurtarma anahtarlarına erişim için parola ve/veya PIN kodunun kullanımını yapılandırabilirsiniz.

  Varsayılan tam disk şifreleme kuralını belirtebilir ve şifreleme dışında tutulacak sabit sürücülerin bir listesini oluşturabilirsiniz. Kaspersky Security Center ilkesi uygulandıktan sonra Kaspersky Endpoint Security tam disk şifrelemesini kesime göre gerçekleştirir. Uygulama, sabit sürücülerin tüm mantıksal bölmelerini eşzamanlı olarak şifreler.

  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 hesaplarını yönet* görevini 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. Authentication Agent hesabının kullanıcı adı ve parolasını kullanarak işletim sisteminde otomatik olarak oturum açmanızı sağlayan Single Sign-On (SSO) teknolojisini de kullanabilirsiniz.

  > Bilgisayarı yedekleyip bilgisayar verilerini şifrelerseniz ve ardından bilgisayarın yedekleme 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 Yardım içeriğinden programın kullanımıyla ilgili daha fazla bilgi alabilirsiniz.

  Şifrelenmiş sabit sürücülere erişim sadece Kaspersky Endpoint Security'nin tam disk 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 bilgiler 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. Bu nedenle, dosyalar yeni bir aygıta yazıldığından ve aygıt **Sadece kullanılan disk alanını şifrele** işlevi etkin durumdayken düzenli olarak şifrelendiğinden tüm sektörler belirli bir süre sonra şifrelenir.

Dosyaların şifresini çözmek için gereken veriler, şifreleme zamanında bilgisayarı kontrol eden Kaspersky Security Center Yönetim Sunucusu tarafından sağlanır. Şifrelenmiş nesnelerin bulunduğu bilgisayar herhangi bir nedenle farklı bir Yönetim Sunucusu tarafından yönetildiyse, şifrelenmiş verilere aşağıdaki yollardan biriyle erişebilirsiniz:

- Aynı hiyerarşideki Yönetim Sunucuları:
  - Başka işlem yapmanız gerekmez. Kullanıcı şifrelenmiş nesnelere erişimi koruyacaktır. Şifreleme anahtarları tüm Yönetim Sunucularına dağıtılır.
- Ayrılmış Yönetim Sunucuları:
  - LAN yöneticisinden şifrelenmiş nesnelere erişim talep edin.
  - Şifrelenmiş cihazlardaki verileri Geri Yükleme Yardımcı Uygulamasını kullanarak geri yükleyin.
  - 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.

Şifrelenmiş verilere erişim olmadığında, şifrelenmiş verilerle çalışma için özel talimatları izleyin (Şifrelenmiş dosyalara yeniden erişim, Şifrelenmiş cihazlara erişim olmadığında şifrelenmiş cihazlarla çalışma).

Şifreleme işlevi sınırlamaları

Veri Şifreleme şu sınırlamalara sahiptir:

- Uygulama, şifreleme sırasında servis dosyaları oluşturur. Bunları kaydetmek için sabit sürücüdeki parçalanmamış kullanılabilir alanın yaklaşık %0,5'i gereklidir. Sabit sürücüde parçalanmamış yeterli kullanılabilir alan yoksa yeterli alan açılana kadar şifreleme başlamaz.
- Kaspersky Security Center Yönetim Konsolunda ve Kaspersky Security Center Web Console'da tüm veri şifreleme bileşenlerini yönetebilirsiniz. Kaspersky Security Center Cloud Console'da yalnızca Bitlocker'ı yönetebilirsiniz.
- Veri şifreleme sadece Kaspersky Endpoint Security, Kaspersky Security Center yönetim sistemi ya da Kaspersky Security Center Cloud Console (sadece BitLocker) ile birlikte kullanıldığında mevcuttur. Kaspersky Endpoint Security çevrimdışı modda kullanılırken Veri Şifreleme, Kaspersky Endpoint Security şifreleme anahtarlarını Kaspersky Security Center'da sakladığından mümkün değildir.

- Kaspersky Endpoint Security, Microsoft Windows for Servers çalıştıran bir bilgisayara yüklenirse sadece BitLocker Drive Encryption teknolojisini kullanan tam disk şifreleme mevcuttur. Kaspersky Endpoint Security, Windows for Workstations altında çalışan bir bilgisayara yüklenirse veri şifreleme işlevselliği tam olarak kullanılabilir.

- Kaspersky Endpoint Security, Arm tabanlı bir bilgisayara yüklenmişse, yalnızca BitLocker Sürücü Şifreleme teknolojisini kullanan Tam Disk Şifreleme özelliği kullanılabilir; diğer şifreleme bileşenleri desteklenmemektedir.

Kaspersky Disk Encryption teknolojisini kullanan tam disk şifreleme, donanım ve yazılım gereksinimlerini karşılamayan sabit sürücüler için kullanılamaz.

Kaspersky Endpoint Security ile Kaspersky Anti-Virus for UEFI arasında tam disk şifreleme işlevi uyumluluğu desteklenmemektedir. Kaspersky Anti-Virus for UEFI, işletim sistemi yüklenmeden önce başlatılır. Tam disk şifreleme kullanıldığında uygulama, bilgisayarda yüklü bir işletim sisteminin eksik olduğunu tespit eder. Sonuç olarak, Kaspersky Anti-Virus for UEFI'nin çalıştırılması bir hatayla sonuçlanır. Dosya Düzeyinde Şifreleme (FLE), Kaspersky Anti-Virus for UEFI için çalışmayı etkilemez.

Kaspersky Endpoint Security aşağıdaki yapılandırmaları destekler:

- HDD, SSD ve USB sürücüler.

  Kaspersky Disk Encryption (FDE) teknolojisi, SSD ile çalışmayı destekler ve ayrıca SSD sürücülerin performansını ve hizmet ömrünü korur.

- Veri yolu üzerinden bağlanan sürücüler: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- SD veya MMC veri yolu üzerinden bağlanan çıkarılabilir olmayan sürücüler.

- 512 bayt sektörlü sürücüler.

- 512 bayta öykünen 4096 bayt sektörlü sürücüler.

- Aşağıdaki bölüm türlerine sahip sürücüler: GPT, MBR ve VBR (çıkarılabilir sürücüler).

- UEFI 64 ve Legacy BIOS standardının yerleşik yazılımı.

- Secure Boot desteğine sahip UEFI standardının yerleşik yazılımı.

  Secure Boot, UEFI yükleyici uygulamaları ve sürücüleri için dijital imzaları doğrulamak üzere tasarlanmış bir teknolojidir. Secure Boot, imzalanmamış veya bilinmeyen yayıncılar tarafından imzalanmış UEFI uygulamalarının ve sürücülerinin başlatılmasını engeller. Kaspersky Disk Encryption (FDE), Secure Boot'u tamamen destekler. Kimlik Doğrulama Aracısı, bir Microsoft Windows UEFI Sürücü Yayıncısı sertifikası ile imzalanmıştır.

  Bazı cihazlarda (örneğin, Microsoft Surface Pro ve Microsoft Surface Pro 2), güncel olmayan bir dijital imza doğrulama sertifikaları listesi varsayılan olarak yüklenebilir. Sürücüyü şifrelemeden önce, sertifika listesini güncellemeniz gerekir.

- Hızlı Önyükleme desteğine sahip UEFI standardının yerleşik yazılımı.

  Hızlı Önyükleme, bilgisayarın daha hızlı başlamasına yardımcı olan bir teknolojidir. Hızlı Önyükleme teknolojisi etkinleştirildiğinde, normalde bilgisayar yalnızca işletim sistemini başlatmak için gereken minimum UEFI sürücülerini yükler. Fast Boot teknolojisi etkinleştirildiğinde, Kimlik Doğrulama Aracısı çalışırken USB klavyeler, fareler, USB belirteçleri, dokunmatik yüzeyler ve dokunmatik ekranlar çalışmayabilir.

Kaspersky Disk Encryption'ı (FDE) kullanmak için Hızlı Önyükleme teknolojisini devre dışı bırakmanız önerilir. Kaspersky Disk Encryption'ın (FDE) çalışmasını test etmek için FDE Test Yardımcı Programını kullanabilirsiniz.

Kaspersky Endpoint Security aşağıdaki yapılandırmaları desteklemez:

- Önyükleme yükleyicisi işletim sisteminden farklı bir sürücüde bulunmaktadır.
- Sistem UEFI 32 standardının gömülü yazılımını içermektedir.
- Sistem Intel® Hızlı Başlatma Teknolojisi devre dışı bırakıldığında bile hazırda bekleme bölümüne sahip Intel® Hızlı Başlatma Teknolojisi ve sürücülere sahiptir.
- 10 genişletilmiş bölümden daha fazla MBR biçiminde sürücüler.
- Sistem, sistem dışı bir sürücüde bulunan bir takas dosyasına sahiptir.
- Aynı anda yüklenen birden fazla işletim sistemini içeren çoklu önyükleme sistemi.
- Dinamik bölümler (sadece birincil bölümler desteklenmektedir).
- %0,5'ten daha az parçalanmamış disk alanı içeren sürücüler.
- 512 bayt veya 512 bayta öykünen 4096 bayttan farklı bir kesim boyutu içeren sürücüler.
- Karma sürücüler.
- Sistem, üçüncü taraf yükleyicilere sahiptir.
- Sıkıştırılmış NTFS dizinlerine sahip sürücüler.
- Kaspersky Disk Encryption (FDE) teknolojisi, diğer tam disk şifreleme teknolojileriyle (BitLocker, McAfee Drive Encryption ve WinMagic SecureDoc gibi) uyumsuzdur.
- Kaspersky Disk Encryption (FDE) teknolojisi, ExpressCache teknolojisiyle uyumlu değildir.
- Şifrelenmiş bir sürücüde bölümler oluşturulması, silinmesi ve değiştirilmesi desteklenmez. Veri kaybı yaşayabilirsiniz.
- Dosya sistemi biçimlendirmesi desteklenmez. Veri kaybı yaşayabilirsiniz.

  Kaspersky Disk Encryption (FDE) teknolojisi ile şifrelenmiş bir sürücüyü biçimlendirmeniz gerekiyorsa, sürücüyü Kaspersky Endpoint Security for Windows yüklü olmayan bir bilgisayarda biçimlendirin ve sadece tam disk şifrelemesi kullanın.

  Hızlı biçimlendirme seçeneğiyle biçimlendirilen şifrelenmiş bir sürücü, Kaspersky Endpoint Security for Windows yüklü bir bilgisayara bir sonraki bağlanışında, hatalı bir şekilde şifrelenmiş olarak tanımlanabilir. Kullanıcı verileri kullanılamaz.
- Kimlik Doğrulama Aracısı 100'den fazla hesabı desteklemez.
- Çoklu Oturum Açma teknolojisi, üçüncü taraf geliştiricilerin diğer teknolojileriyle uyumlu değildir.

- Kaspersky Disk Encryption (FDE) teknolojisi, aşağıdaki cihaz modellerinde desteklenmez:
  - Dell Latitude E6410 (UEFI modu)
  - HP Compaq nc8430 (Legacy BIOS modu)
  - Lenovo ThinkCentre 8811 (Legacy BIOS modu)
- Kimlik Doğrulama Aracısı, Legacy USB Support etkinleştirildiğinde USB belirteçleriyle çalışmayı desteklemez. Bilgisayarda yalnızca parola tabanlı kimlik doğrulama mümkün olacaktır.
- Legacy BIOS modunda bir sürücüyü şifrelerken, aşağıdaki cihaz modellerinde Legacy USB Support'u etkinleştirmeniz önerilir:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550
  - Lenovo ThinkPad L530

- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (anakart)

Şifreleme anahtarının uzunluğunu değiştirme (AES56 / AES256)

Kaspersky Endpoint Security, Gelişmiş Şifreleme Standardı (AES) şifreleme algoritmasını kullanır. Kaspersky Endpoint Security, AES şifreleme algoritmasını 256 veya 56 bitlik etkili bir anahtar uzunluğu ile kullanır. Veri şifreleme algoritması, dağıtım paketine dahil olan AES şifreleme kitaplığına bağlıdır: *Güçlü şifreleme (AES256)* veya *Hafif şifreleme (AES56)*. AES şifreleme kitaplığı uygulama ile birlikte yüklenir.

Şifreleme anahtarının uzunluğunun değiştirilmesi sadece Kaspersky Endpoint Security 11.2.0 veya üzeri ile mümkündür.

Şifreleme anahtarı uzunluğunun değiştirilmesi şu adımlardan oluşur:

1. Şifreleme anahtarının uzunluğunu değiştirmeye başlamadan önce Kaspersky Endpoint Security'nin daha önce şifrelediği nesnelerin şifresini çözün:
   a. Sabit sürücülerin şifresini çözün.
   b. Yerel sürücülerdeki dosyaların şifresini çözün.
   c. Çıkarılabilir sürücülerin şifresini çözün.

   Şifreleme anahtarı uzunluğunu değiştirdikten sonra, önceden şifrelenen nesneler kullanılamaz duruma gelir.
2. Kaspersky Endpoint Security'yi Kaldır.
3. Farklı bir şifreleme kitaplığı içeren Kaspersky Endpoint Security dağıtım paketinden Kaspersky Endpoint Security'yi yükleyin.

Şifreleme anahtarı uzunluğunu, uygulamayı güncelleyerek de değiştirmeniz mümkündür. Anahtar uzunluğu ancak şu koşullar sağlandığında bir uygulama güncellemesi aracılığıyla değiştirilebilir:

- Bilgisayarda Kaspersky Endpoint Security sürüm 10 Servis Paketi 2 veya üzeri yüklü ise.
- Veri şifreleme bileşenleri (Dosya Düzeyinde Şifreleme, Tam Disk Şifreleme) bilgisayara yüklenmez.

  Varsayılan olarak, veri şifreleme bileşenleri Kaspersky Endpoint Security'ye dahil değildir. BitLocker Management bileşeni, şifreleme anahtarının uzunluğunda değişimi etkilemez.

Şifreleme anahtarı uzunluğunu değiştirmek için dağıtım paketinden gerekli şifreleme kitaplığını içeren kes_win.msi veya setup_kes.exe dosyasını çalıştırın. Uygulamayı, kurulum paketini kullanarak uzaktan güncellemeniz de mümkündür.

Şifreleme anahtarının uzunluğunu, önce uygulamayı kaldırmadan, uygulamanın bilgisayarınızda kurulu olan sürümüne ait dağıtım paketini kullanarak değiştirmek mümkün değildir.

Kaspersky Disk Encryption

Kaspersky Disk Encryption, ARM tabanlı bilgisayarlarda desteklenmemektedir.

Kaspersky Disk Encryption sadece iş istasyonları için bir Windows işletim sistemi çalıştıran bilgisayarlarda kullanılabilir. Sunucular için olan bir Windows işletim sistemi çalıştıran bilgisayarlar için BitLocker Drive Encryption teknolojini kullanın.

Kaspersky Endpoint Security, FAT32, NTFS ve exFat dosya sistemlerinde tam disk şifrelemeyi destekler.

Tam disk şifrelemeye başlamadan önce uygulama, sistem sabit sürücüsünün Kimlik Doğrulama Aracısı veya 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 tam disk şifreleme, işletim sistemi yüklendikten ve 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 tam disk şifrelemeyi 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 tam disk şifrelemeden 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.

Tam disk şifreleme başladıktan sonra Kaspersky Endpoint Security sabit sürücülere yazılan tüm verileri şifreler.

Kullanıcı bilgisayarı tam disk şifreleme sırasında 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 tam disk şifrelemeyi sürdürür.

Tam disk şifreleme sırasında 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 tam disk şifrelemeyi sürdürür.

Tam disk şifreleme sırasında işletim sistemi uyku moduna geçerse Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı yüklenmeden işletim sistemi uyku modundan çıktığında tam disk 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.

  Sadece 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.

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.

SSD sürücü şifrelemesinin özel özellikleri

Uygulama, SSD sürücülerin, hibrit SSHD sürücülerin ve Intel Smart Response özelliğine sahip sürücülerin şifrelenmesini destekler. Uygulama, Intel Rapid Start özelliğine sahip sürücülerin şifrelenmesini desteklemez. Böyle bir sürücüyü şifrelemeden önce Intel Rapid Start özelliğini devre dışı bırakın.

SSD sürücüleri şifreleme şu özelliklere sahiptir:

- Bir SSD sürücüsü yeniyse ve hiçbir gizli veri içermiyorsa, yalnızca kullanılan alanın şifrelenmesini etkinleştirin. Bu, ilgili sürücü sektörlerinin üzerine yazmanıza izin verir.
- Bir SSD sürücüsü kullanılıyorsa ve sürücü üzerinde gizli veriler varsa, aşağıdaki seçeneklerden birini tercih edin:
  - SSD sürücüsünü tamamen silin (Güvenli Silme), işletim sistemini kurun ve yalnızca kullanılan alanı şifreleme seçeneği etkinleştirilmiş olarak SSD sürücüsünün şifrelemesini çalıştırın.
  - Yalnızca kullanılan alanı şifreleme seçeneği devre dışı bırakılarak SSD sürücüsünün şifrelemesini çalıştırın.

Bir SSD sürücüsünün şifrelenmesi, 5-10 GB boş alan gerektirir. Şifreleme yönetimi verilerini depolamak için boş alan gereksinimleri aşağıdaki tabloda verilmiştir.

Şifreleme yönetimi verilerini depolamak için boş alan gereksinimleri

SSD sürücü boyutu (GB)	SSD sürücüsünün birincil bölümünde boş alan (MB)	SSD sürücüsünün ikincil bölümünde boş alan (MB)
128	250	64
256	250	640
512	300	128

Kaspersky Disk Encryption'ı başlatma

Tam disk şifrelemeyi başlatmadan önce bilgisayarda virüs bulunmadığından emin olmanızı öneririz. Bunun için Tam Tarama veya Kritik Alanları Tarama görevini başlatın. Rootkit virüsü bulaşmış bir bilgisayarda tam disk şifreleme yapılması bilgisayarın çalışmamasına neden olabilir.

Disk şifreleme işlemine başlamadan önce Kimlik Doğrulama Aracısı hesaplarının ayarlarını kontrol etmelisiniz. Kimlik Doğrulama Aracısı, Kaspersky Disk Encryption (FDE) teknolojisi ile korunan sürücülerle çalışması gerekir. İşletim sistemi yüklenmeden önce kullanıcının Aracı ile kimlik doğrulamasını tamamlaması gerekir. Kaspersky Endpoint Security, bir sürücüyü şifrelemeden önce otomatik olarak Kimlik Doğrulama Aracısı hesapları oluşturmanıza izin verir. Kimlik Doğrulama Aracısı hesaplarının otomatik olarak oluşturulmasını Tam Disk Şifreleme ilkesi ayarlarından etkinleştirebilirsiniz (aşağıdaki talimatlara bakın). Ayrıca Çoklu Oturum Açma (SSO) teknolojisini de kullanabilirsiniz.

Kaspersky Endpoint Security, şu kullanıcı grupları için otomatik olarak Kimlik Doğrulama Aracısı hesapları oluşturmanıza izin verir:

- **Bilgisayardaki tüm hesaplar**. Bilgisayarda herhangi bir zamanda etkin olan tüm hesaplar.
- **Bilgisayardaki tüm etki alanı hesapları**. Bilgisayardaki bir etki alanına ait olan ve herhangi bir zamanda etkin olan tüm hesaplar.
- **Bilgisayardaki tüm yerel hesaplar**. Bilgisayarda herhangi bir zamanda etkin olan tüm yerel hesaplar.
- **Tek kullanımlık bir parolaya sahip hizmet hesabı**. Hizmet hesabı, örneğin kullanıcı parolasını unuttuğunda bilgisayara erişim sağlamak için gereklidir. Hizmet hesabını bir rezerve hesap olarak da kullanabilirsiniz. Hesabın adını girmelisiniz (varsayılan olarak, `ServiceAccount`). Kaspersky Endpoint Security otomatik olarak bir parola oluşturur. Parolayı Kaspersky Security Center konsolu üzerinde görüntüleyemezsiniz.
- **Yerel yönetici**. Kaspersky Endpoint Security, bilgisayarın yerel yöneticisi için bir Kimlik Doğrulama Aracısı kullanıcı hesabı oluşturur.
- **Bilgisayar yöneticisi**. Kaspersky Endpoint Security, bilgisayar yöneticisinin hesabı için bir Kimlik Doğrulama Aracısı kullanıcı hesabı oluşturur. Active Directory'deki bilgisayar özelliklerinde, hangi hesabın bilgisayar yöneticisi rolüne sahip olduğunu görebilirsiniz. Bilgisayar yöneticisi rolü varsayılan olarak tanımlanmamıştır, yani herhangi bir hesaba karşılık gelmez.
- **Etkin hesap**. Kaspersky Endpoint Security, disk şifrelemesi sırasında etkin olan hesap için otomatik olarak bir Kimlik Doğrulama Aracısı hesabı oluşturur.

Kimlik Doğrulama Aracısı hesaplarını yönet görevi, kullanıcı ayarlarını yapılandırmak için tasarlanmıştır. Yeni hesaplar eklemek, mevcut hesapların ayarlarını değiştirmek veya gerekirse hesapları kaldırmak için bu görevi kullanabilirsiniz. Bilgisayarlar için yerel görevler kullanabileceğiniz gibi, ayrı yönetim gruplarından bilgisayarlar ya da seçilen bilgisayarlar için grup görevleri de kullanabilirsiniz.

Kaspersky Disk Encryption bileşeni Yönetim Konsolu (MMC) üzerinden nasıl başlatılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
4. **Şifreleme teknolojisi** açılır listesinde **Kaspersky Disk Encryption** öğesini seçin.

   Kaspersky Disk Encryption teknolojisi, bilgisayarda BitLocker ile şifrelenen sabit sürücüler varsa kullanılamaz.

5. **Şifreleme modu** açılır listesinden **Tüm sabit sürücüleri şifrele** seçeneğini seçin.

Bilgisayarda birkaç işletim sistemi yüklüyse tüm sabit sürücüler şifrelendikten sonra yalnızca uygulamanın yüklü olduğu işletim sistemini yükleyebilirsiniz.

Sabit sürücülerin bir kısmını şifreleme dışında tutmak isterseniz bu sabit sürücülerin bir listesini oluşturun.

6. Gelişmiş Kaspersky Disk Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
7. Değişikliklerinizi kaydedin.

Kaspersky Disk Encryption bileşeni Web Console ve Cloud Console üzerinden nasıl çalıştırılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Tam Disk Şifreleme**'ye gidin.
5. **Kaspersky Disk Encryption** teknolojisini seçin.

   Kaspersky Disk Encryption teknolojisi, bilgisayarda BitLocker ile şifrelenen sabit sürücüler varsa kullanılamaz.

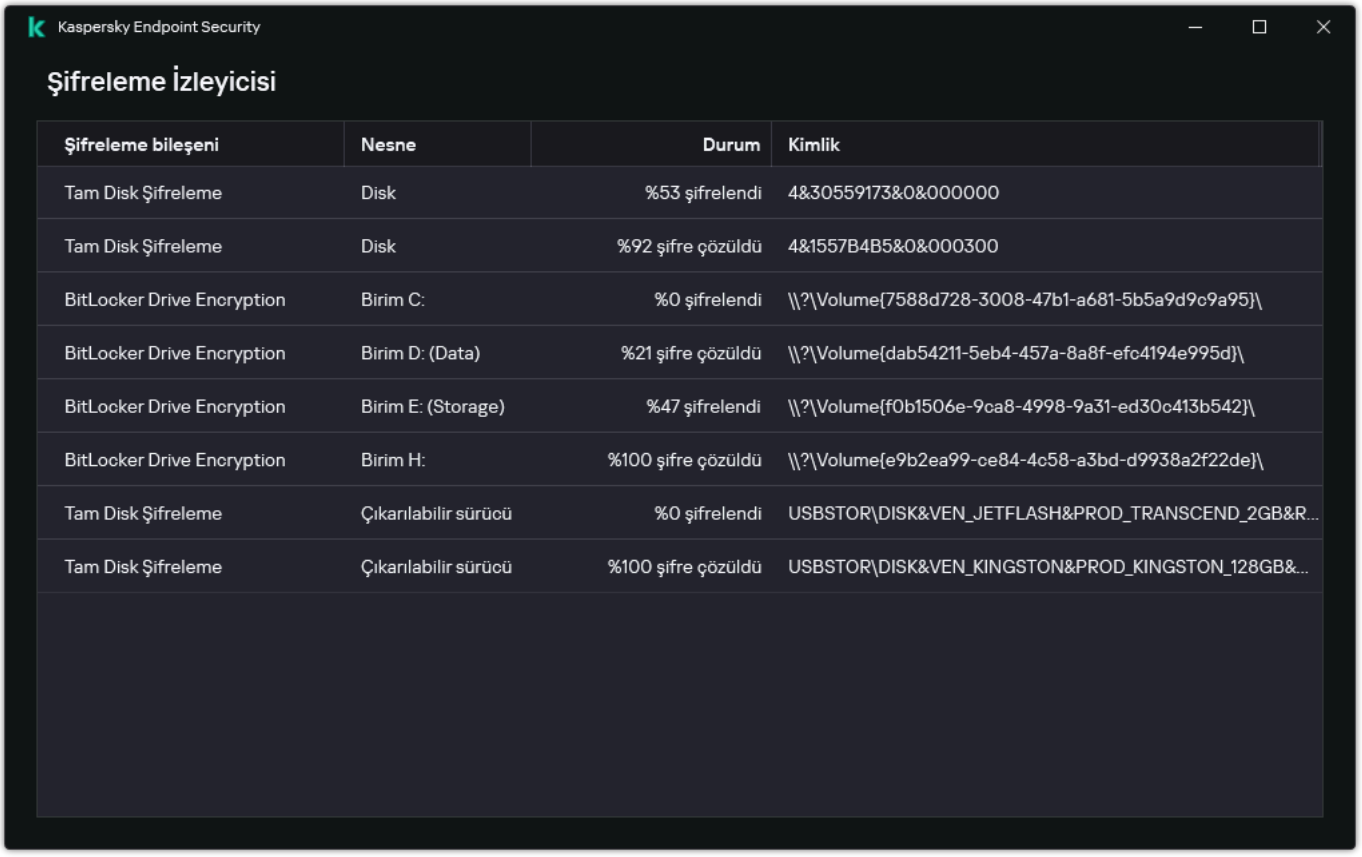
6. **Cihazlardaki eylem** bloğunda **Tüm sabit sürücüleri şifrele**'yi seçin.

   Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca şifreleme işleminin gerçekleştirildiği işletim sistemini yükleyebilirsiniz.

   Sabit sürücülerin bir kısmını şifreleme dışında tutmak isterseniz bu sabit sürücülerin bir listesini oluşturun.

7. Gelişmiş Kaspersky Disk Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
8. Değişikliklerinizi kaydedin.

Bir kullanıcının bilgisayarındaki disk şifreleme veya şifre çözme işlemini kontrol etmek için Şifreleme İzleyicisi aracını kullanabilirsiniz. Şifreleme İzleyicisi aracını ana uygulama penceresinden çalıştırabilirsiniz.



Şifreleme İzleyicisi

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.

Kaspersky Disk Encryption bileşeni ayarları

Parametre	Açıklama
Şifreleme sırasında kullanıcıları için Kimlik Doğrulama Aracısı hesaplarını otomatik olarak oluştur	Bu onay kutusu seçildiğinde, uygulama bilgisayardaki Windows kullanıcı hesapları listesine göre Kimlik Doğrulama Aracısı hesapları oluşturur. Kaspersky Endpoint Security varsayılan olarak, kullanıcının işletim sisteminde son 30 günde giriş yaptığı tüm yerel ve etki alanı hesaplarını kullanır.
Bu bilgisayardaki tüm kullanıcılar için giriş yapıldığında Kimlik Doğrulama Aracısı hesapları oluştur	Bu onay kutusu seçildiğinde, uygulama, Kimlik Doğrulama Aracısı'nı başlatmadan önce bilgisayardaki Windows kullanıcı hesapları hakkındaki bilgileri kontrol eder. Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı hesabı olmayan bir Windows kullanıcı hesabı tespit ettiğinde, uygulama şifrelenmiş sürücülere erişmek için yeni bir hesap oluşturacaktır. Yeni Kimlik Doğrulama Aracısı hesabı şu varsayılan ayarlara sahip olacaktır: yalnızca parola korumalı oturum açma ve ilk kimlik doğrulamada parola değişikliği. Bu nedenle, zaten şifrelenmiş sürücülere sahip bilgisayarlar için *Kimlik Doğrulama Aracısı hesaplarını yönet* görevini kullanarak Kimlik Doğrulama Aracısı hesaplarını manuel olarak eklemeniz gerekmez.
Kimlik Doğrulama Aracısı'na girilen kullanıcı adını kaydet	Onay kutusu işaretlenirse uygulama Kimlik Doğrulama Aracısı hesabının adını kaydeder. Aynı hesaptaki Kimlik Doğrulama Aracısı'nda yapacağınız bir sonraki yetkilendirme tamamlama girişiminde hesap adını girmeniz istenmeyecektir.

Parametre	Açıklama
Sadece kullanılan disk alanını şifrele (şifreleme süresini kısaltır)	Bu onay kutusu, şifreleme alanını yalnızca kullanılan sabit sürücü sektörleri ile sınırlayan seçeneği etkinleştirir/devre dışı bırakır. Bu sınır şifreleme süresini azaltmanızı sağlar. **Sadece kullanılan disk alanını şifrele (şifreleme süresini kısaltır)** özelliğinin şifrelemeyi başlattıktan sonra etkinleştirilmesi veya devre dışı bırakılması durumunda, sabit sürücülerin şifresi çözülene kadar bu ayar değiştirilmez. Şifrelemeyi başlatmadan önce onay kutusunu işaretlemeniz veya işaretini kaldırmanız gerekir. Onay kutusu işaretlenirse sabit sürücünün yalnızca dosyalar tarafından kullanılan bölümleri şifrelenir. Kaspersky Endpoint Security yeni eklenen verileri otomatik olarak şifreler. Onay kutusunun işareti kaldırılırsa daha önce silinen ve değiştirilen dosyaların kalan bölümleri de dahil olmak üzere tüm sürücü şifrelenir. Bu seçenek, verileri değiştirilmemiş veya silinmemiş yeni sabit sürücüler için önerilir. Şifrelemeyi zaten kullanımda olan bir sabit sürücüye uyguluyorsanız tüm sabit sürücünün şifrelenmesi önerilir. Bu, tüm verilerin, hatta potansiyel olarak kurtarılabilir silinmiş verilerin bile korunmasını sağlar. Varsayılan olarak, onay kutusu temizlenmiştir.
Legacy USB Support'u kullan (önerilmez)	Bu onay kutusu Legacy USB Support işlevselliğini etkinleştirir veya devre dışı bırakır. *Legacy USB Support*, **İşletim sistemi** başlatılmadan önce bilgisayarın önyükleme aşamasında (BIOS modu) USB aygıtlarını (güvenlik belirteci gibi) kullanmanıza imkan veren bir BIOS/UEFI işlevidir. Legacy USB Support, işletim sistemi başlatıldıktan sonra USB aygıtları için desteği etkilemez. Bu onay kutusu işaretlenirse bilgisayarın ilk başlatılması sırasında USB aygıtları için destek etkinleştirilir. Legacy USB Support işlevi etkinleştirildiğinde, Kimlik Doğrulama Aracısı BIOS modunda USB aracılığıyla belirteçlerle çalışmayı desteklemez. Bu seçeneği yalnızca donanım uyumluluk sorunu olduğunda ve yalnızca bu sorunun oluştuğu bilgisayarlar için kullanmanız önerilir.

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 Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
4. **Şifreleme teknolojisi** açılır listesinde **Kaspersky Disk Encryption** öğesini 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.
5. Şifreleme dışında tutulan sabit sürücülerin listesine sabit sürücüleri eklemek için:
   a. **Ekle**'ye tıklayın.
   b. Açılan pencerede **Aygıt adı**, **Bilgisayar**, **Disk türü**, **Kaspersky Disk Encryption** değerlerini belirtin.
   c. **Yenile**'ye 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.

6. Değişikliklerinizi kaydedin.

Şifreleme dışında tutulan sabit sürücülerin listesini içe/dışa aktarma

Sabit sürücü şifreleme istisnalarının listesini bir XML dosyasına verebilirsiniz. Daha sonra, örneğin, aynı türden çok sayıda dışlama eklemek için dosyayı değiştirebilirsiniz. İstisnalar listesini yedeklemek veya istisnaları farklı bir sunucuya taşımak için dışa aktarma/içe aktarma işlevini de kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) bir sabit sürücü şifreleme istisnaları listesinin dışa veya içer aktarılması

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
4. **Şifreleme teknolojisi** açılır listesinde **Kaspersky Disk Encryption** öğesini seçin.
   Şifreleme dışında tutulan sabit sürücülerin girişleri, **Aşağıdaki sabit sürücüleri şifreleme** tablosunda görülür.
5. İstisnalar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
      Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.
   b. → **Dışa aktar** düğmesine tıklayın.
   c. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
      Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.
6. Kurallar listesini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
   b. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.
   c. Dosyayı aç.
      Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.
7. Değişikliklerinizi kaydedin.

Web Console'da bir sabit sürücü şifreleme istisnaları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Tam Disk Şifreleme**'ye gidin.
   Kaspersky Disk Encryption teknolojisini seçin.
5. **İstisnalar** düğmesine tıklayın.
   İstisnalar listesi açılır.
6. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin.
   b. → **Dışa aktar** düğmesine tıklayın.
      Kaspersky Endpoint Security, istisnalar listesini varsayılan indirilenler klasöründeki bir JSON dosyasına aktarır.
7. İstisnalar listesini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
      Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz JSON dosyasını seçin.
   b. Dosyayı aç.
      Bilgisayar zaten bir istisnalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye JSON dosyasından yeni girişler ekler.
8. Değişikliklerinizi kaydedin.

Çoklu Oturum Açma (SSO) teknolojisini kullanma

Single Sign-On (SSO) teknolojisi, Kimlik Doğrulama Aracısı'nın kimlik bilgilerini kullanarak işletim sisteminde otomatik olarak oturum açmanızı sağlar. Bu, bir kullanıcının Windows'ta oturum açarken yalnızca bir kez parola girmesi gerektiği anlamına gelir (Kimlik Doğrulama Aracısı hesap parolası). Çoklu Oturum Açma teknolojisi, Windows hesabı parolası değiştirildiğinde Kimlik Doğrulama Aracısı hesap parolasını otomatik olarak güncellemenize de imkan verir.

Çoklu Oturum Açma teknolojisi kullanıldığında, Kimlik Doğrulama Aracısı Kaspersky Security Center'da belirlenmiş olan parola gücü gerekliliklerini yoksayar. Parolanızın gücü gerekliliklerini işletim sistemi ayarlarında belirleyebilirsiniz.

Çoklu Oturum Açma teknolojisini kullanma

Çoklu Oturum Açma teknolojisinin kullanımı Yönetim Konsolu'ndan (MMC) nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme → Ortak şifreleme ayarları** seçimini yapın.
4. **Parola ayarları** bloğunda **Ayarlar** düğmesine tıklayın.
5. Açılan pencerenin **Kimlik Doğrulama Aracısı** sekmesinden **Çoklu Oturum Açma (SSO) teknolojisi kullan** onay kutusunu işaretleyin.
6. Üçüncü taraf bir kimlik bilgisi sağlayıcı kullanıyorsanız **Üçüncü taraf kimlik bilgisi sağlayıcılarını sarmalayın** onay kutusunu seçin.
7. Değişikliklerinizi kaydedin.

Sonuç olarak, kullanıcının kimlik doğrulama prosedürünü Aracı ile sadece bir kez tamamlaması gerekir. Kimlik doğrulama prosedürü, işletim sisteminin yüklenmesi için gerekli değildir. İşletim sistemi otomatik olarak yüklenir.

Web Console'da Çoklu Oturum Açma kullanımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme → Tam Disk Şifreleme**'ye gidin.
5. **Kaspersky Disk Encryption** teknolojisini seçin.
6. **Parola ayarları** bloğunda, **Çoklu Oturum Açma (SSO) teknolojisi kullan** onay kutusunu işaretleyin.
7. Üçüncü taraf bir kimlik bilgisi sağlayıcı kullanıyorsanız **Üçüncü taraf kimlik bilgisi sağlayıcılarını sarmalayın** onay kutusunu seçin.
8. Değişikliklerinizi kaydedin.

Sonuç olarak, kullanıcının kimlik doğrulama prosedürünü Aracı ile sadece bir kez tamamlaması gerekir. Kimlik doğrulama prosedürü, işletim sisteminin yüklenmesi için gerekli değildir. İşletim sistemi otomatik olarak yüklenir.

Çoklu Oturum Açmanın çalışması için Windows hesabının parolası ile Kimlik Doğrulama Aracısı hesabının parolasının aynı olması gerekir. Parolalar eşleşmezse, kullanıcının kimlik doğrulama prosedürünü iki kez gerçekleştirmesi gerekir: Kimlik Doğrulama Aracısı arabiriminde ve işletim sistemi yüklenmeden önce. Parolaları senkronize etmek için bu eylemlerin yalnızca bir kez gerçekleştirilmesi gerekir. Bundan sonra, Kaspersky Endpoint Security Windows hesabının parolasını Kimlik Doğrulama Aracısı hesabının parolası ile değiştirir. Windows hesabı parolası değiştirildiğinde, uygulama, Kimlik Doğrulama Aracısı hesabının parolasını otomatik olarak güncelleyecektir.

Üçüncü taraf kimlik bilgileri sağlayıcıları

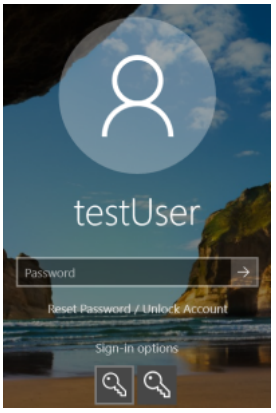
Kaspersky Endpoint Security, üçüncü taraf kimlik bilgisi sağlayıcı ADSelfService Plus'ı destekler.

Üçüncü taraf kimlik bilgisi sağlayıcılarıyla çalışırken, Kimlik Doğrulama Aracısı, işletim sistemi yüklenmeden önce parolayı yakalar. Bu, kullanıcının Windows'ta oturum açarken yalnızca bir kez parola girmesi gerektiği anlamına gelir. Kullanıcı Windows'ta oturum açtıktan sonra, örneğin kurumsal hizmetlerde kimlik doğrulama için üçüncü taraf bir kimlik bilgileri sağlayıcısının özelliklerini kullanabilir. Üçüncü taraf kimlik bilgileri sağlayıcıları, kullanıcıların kendi parolalarını bağımsız olarak sıfırlamalarına da olanak tanır. Bu durumda Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı parolasını otomatik olarak günceller.

Uygulama tarafından desteklenmeyen bir üçüncü taraf kimlik bilgisi sağlayıcısı kullanıyorsanız, Çoklu Oturum Açma teknolojisinin kullanıldığı işlemlerde bazı sınırlamalarla karşılaşabilirsiniz. Windows'ta oturum açarken, kullanıcıya iki profil sunulacaktır: sistem içi kimlik bilgileri sağlayıcısı ve üçüncü taraf kimlik bilgileri sağlayıcısı. Bu profillerin simgeleri aynı olacaktır (aşağıdaki resme bakın). Kullanıcı, aşağıdaki seçeneklerden biriyle devam etmeyi seçebilir:

- Kullanıcı *üçüncü taraf kimlik bilgileri sağlayıcısı* seçimini yaparsa Kimlik Doğrulama Aracısı parolayı Windows hesabıyla eşitlemez. Bu nedenle, kullanıcı Windows hesabı parolasını değiştirmişse Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı hesabı parolasını güncelleyemez. Dolayısıyla kullanıcının kimlik doğrulama prosedürünü iki kez gerçekleştirmesi gerekir: Kimlik Doğrulama Aracısı arabiriminde ve işletim sistemi yüklenmeden önce. Bu durumda kullanıcı, örneğin kurumsal hizmetlerde kimlik doğrulama için üçüncü taraf bir kimlik bilgileri sağlayıcısının özelliklerini kullanabilir.

- Kullanıcı *sistem içi kimlik bilgileri sağlayıcısı* seçimini yaparsa Kimlik Doğrulama Aracısı parolaları Windows hesabıyla eşitler. Bu durumda kullanıcı Windows'ta oturum açtıktan sonra, örneğin kurumsal hizmetlerde kimlik doğrulama için üçüncü taraf bir sağlayıcının özelliklerini kullanamaz.



Windows oturum açma için sistem kimlik doğrulama profili ve üçüncü taraf kimlik doğrulama profili

Kimlik Doğrulama Aracısı hesaplarını yönetme

Kimlik Doğrulama Aracısı, Kaspersky Disk Encryption (FDE) teknolojisi ile korunan sürücülerle çalışması gerekir. İşletim sistemi yüklenmeden önce kullanıcının Aracı ile kimlik doğrulamasını tamamlaması gerekir. *Kimlik Doğrulama Aracısı hesaplarını yönet* görevi, kullanıcı ayarlarını yapılandırmak için tasarlanmıştır. Bilgisayarlar için yerel görevler kullanabileceğiniz gibi, ayrı yönetim gruplarından bilgisayarlar ya da seçilen bilgisayarlar için grup görevleri de kullanabilirsiniz.

Kimlik Doğrulama Aracısı hesaplarını yönet görevinin başlatılması için bir zamanlama yapılandıramazsınız. Ayrıca bir görevi zorla durdurmak da mümkün değildir.

Yönetim Konsolu'nda (MMC) Kimlik Doğrulama Aracısı hesaplarını yönet görevi nasıl oluşturulur

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **Kimlik Doğrulama Aracısı hesaplarını yönet** seçimini yapın.

2. Adım. Bir Kimlik Doğrulama Aracısı hesap yönetim komutu seçme

Bir Kimlik Doğrulama Aracısı hesap yönetim komutları listesi oluşturun. Yönetim komutları ile Kimlik Doğrulama Aracısı hesapları için ekleme, değiştirme ve silme işlemlerini yapabilirsiniz (aşağıdaki talimatlara bakın). Sadece bir Kimlik Doğrulama Aracısı hesabına sahip olan kullanıcılar kimlik doğrulama prosedürünü tamamlayabilir, işletim sistemini yükleyebilir ve şifrelenmiş sürücüye erişim kazanabilir.

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Görev adını tanımlama

Görev için bir ad girin, örneğin *Yönetici Hesapları*.

5. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Böylece görev bilgisayarın bir sonraki başlatılmasında tamamlandıktan sonra, yeni kullanıcı kimlik doğrulama prosedürünü tamamlayabilir, işletim sistemini yükleyebilir ve şifrelenmiş sürücüye erişim kazanabilir.

Web Console'da Kimlik Doğrulama Aracısı hesaplarını yönet görevi nasıl oluşturulur

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
2. **Görev türü** açılır listesinde, **Kimlik Doğrulama Aracısı hesaplarını yönet**'i seçin.
3. **Görev adı** alanına *Yönetici hesapları* gibi kısa bir açıklama girin.
4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

2. Adım. Kimlik Doğrulama Aracısı hesaplarını yönetme

Bir Kimlik Doğrulama Aracısı hesap yönetim komutları listesi oluşturun. Yönetim komutları ile Kimlik Doğrulama Aracısı hesapları için ekleme, değiştirme ve silme işlemlerini yapabilirsiniz (aşağıdaki talimatlara bakın). Sadece bir Kimlik Doğrulama Aracısı hesabına sahip olan kullanıcılar kimlik doğrulama prosedürünü tamamlayabilir, işletim sistemini yükleyebilir ve şifrelenmiş sürücüye erişim kazanabilir.

3. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Görevler listesinde yeni bir görev görüntülenir.

Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçin ve **Başlat** düğmesine tıklayın.

Böylece görev bilgisayarın bir sonraki başlatılmasında tamamlandıktan sonra, yeni kullanıcı kimlik doğrulama prosedürünü tamamlayabilir, işletim sistemini yükleyebilir ve şifrelenmiş sürücüye erişim kazanabilir.

Bir Kimlik Doğrulama Aracısı hesabı eklemek için *Kimlik Doğrulama Aracısı hesaplarını yönet* görevine özel bir komut eklemeniz gerekir. Tüm bilgisayarlara bir yönetici hesabı eklemek gibi bir grup görevi kullanmak kullanışlı olabilir.

Kaspersky Endpoint Security, bir sürücüyü şifrelemeden önce otomatik olarak Kimlik Doğrulama Aracısı hesapları oluşturmanıza izin verir. Kimlik Doğrulama Aracısı hesaplarının otomatik olarak oluşturulmasını Tam Disk Şifreleme ilkesi ayarları'ndan etkinleştirebilirsiniz. Ayrıca Çoklu Oturum Açma (SSO) teknolojisini de kullanabilirsiniz.

Bir Kimlik Doğrulama Aracısı hesabı Yönetim Konsolu (MMC) aracılığıyla nasıl eklenir

1. *Kimlik Doğrulama Aracısı hesaplarını yönet* görevinin özelliklerini açın.
2. Görev özelliklerinden **Ayarlar** bölümünü seçin.
3. **Ekle → Hesap ekleme komutu**'na tıklayın.
4. Açılan penceredeki **Windows hesabı** alanında, Kimlik Doğrulama Aracısı hesabını oluşturmak için kullanılacak Microsoft Windows hesabının adını belirtin.
5. Windows hesabının adını manuel olarak girdiyseniz **İzin ver** düğmesine tıklayarak hesap güvenlik tanımlayıcısını (SID) tanımlayın.

   İzin ver düğmesine tıklayarak güvenlik tanımlayıcısını (SID) belirlememeyi tercih ederseniz bilgisayarda görev gerçekleştirildiğinde belirlenir.

   > Bir Windows hesabı güvenlik tanımlayıcısı tanımlamak, Windows hesabının adının doğru girildiğini doğrulamak için gereklidir. Windows hesabı bilgisayarda ya da güvenilir etki alanında yoksa, *Kimlik Doğrulama Aracısı hesaplarını yönet* görevi bir hata ile sonuçlanır.

6. Kimlik Doğrulama Aracısı için oluşturulmuş mevcut hesabın oluşturulan hesapla değiştirilmesini istiyorsanız **Mevcut hesabı 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, *Kimlik Doğrulama Aracısı hesaplarını yönet* yerel görevinin özelliklerinde bir Kimlik Doğrulama Aracısı hesabı oluşturma komutu eklerken kullanılamaz.

7. **Kullanıcı adı** alanına, şifrelenmiş sabit sürücülere erişim için kimlik doğrulama sırasında girilmesi gereken Kimlik Doğrulama Aracısı hesabının adını yazın.
8. 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. Kimlik Doğrulama Aracısı hesabı için bir parola belirleyin. Gerekirse, ilk kimlik doğrulamasından sonra kullanıcıdan yeni bir parola isteyebilirsiniz.
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. Bir akıllı kart ya da belirteç ile kimlik doğrulama için bir sertifika seçin.
10. Gerekirse **Komut açıklaması** alanına, komutu yönetmek için ihtiyaç duyduğunuz Kimlik Doğrulama Aracısı hesabının ayrıntılarını girin.
11. **Kimlik Doğrulama Aracısındaki doğrulamaya erişin** bloğunda, Kimlik Doğrulama Aracısında komutta belirtilen hesabı kullanan kullanıcı için kimlik doğrulama erişimini yapılandırın.
12. Değişikliklerinizi kaydedin.

Bir Kimlik Doğrulama Aracısı hesabı Web Console aracılığıyla nasıl eklenir

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Kimlik Doğrulama Aracısı hesaplarını yönet** görevine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. Kimlik Doğrulama Aracısı hesapları listesinde **Ekle** düğmesine tıklayın ve **Hesap ekle** komut türünü seçin.

5. Bir kullanıcı hesabı seçin. Etki alanı hesapları listesinden bir hesap seçebilir ya da hesap adını manuel olarak girebilirsiniz. Bir sonraki adıma geçin.

   Kaspersky Endpoint Security, hesabın güvenlik tanımlayıcısını (Security Identifier, SID) belirler. Bu, hesabı doğrulamak için gereklidir. Kullanıcı adını yanlış girdiyseniz, Kaspersky Endpoint Security görevi bir hata ile sonlandırır.

6. Kimlik Doğrulama Aracısı hesabı ayarlarını yapılandırın.

   - **Var olan hesabın yerine yeni bir Kimlik Doğrulama Aracısı hesabı oluştur**. Kaspersky Endpoint Security bilgisayardaki mevcut hesapları tarar. Bilgisayardaki ve görevdeki kullanıcı güvenlik tanımlayıcısı eşleşirse, Kaspersky Endpoint Security kullanıcı hesabı ayarlarını göreve uygun olarak değiştirir.

   - **Kullanıcı adı**. Kimlik Doğrulama Aracısı hesabının varsayılan kullanıcı adı, kullanıcının etki alanı adına karşılık gelir.

   - **Parola tabanlı kimlik doğrulamasına izin ver**. Kimlik Doğrulama Aracısı hesabı için bir parola belirleyin. Gerekirse, ilk kimlik doğrulamasından sonra kullanıcıdan yeni bir parola isteyebilirsiniz. Bu şekilde, her kullanıcı kendi benzersiz parolasına sahip olur. Ayrıca, ilkedeki Kimlik Doğrulama Aracısı hesabı için parola gücü gereklilikleri ayarlayabilirsiniz.

   - **Sertifika tabanlı kimlik doğrulamasına izin ver**. Bir akıllı kart ya da belirteç ile kimlik doğrulama için bir sertifika seçin. Böylece kullanıcının akıllı kart veya belirteç için parola girmesi gerekir.

   - **Şifrelenmiş verilere hesap erişimi**. Şifrelenmiş sürücüye kullanıcı erişimini yapılandırın. Örneğin Kimlik Doğrulama Aracısı hesabını silmek yerine kullanıcı kimlik doğrulamasını geçici olarak devre dışı bırakabilirsiniz.

   - **Yorum**. Gerekirse bir hesap açıklaması girin.

7. Değişikliklerinizi kaydedin.

8. Görevin yanındaki onay kutusunu seçin ve **Başlat** düğmesine tıklayın.

   Böylece görev bilgisayarın bir sonraki başlatılmasında tamamlandıktan sonra, yeni kullanıcı kimlik doğrulama prosedürünü tamamlayabilir, işletim sistemini yükleyebilir ve şifrelenmiş sürücüye erişim kazanabilir.

Kimlik Doğrulama Aracısı hesabının parolasını ve diğer ayarlarını değiştirmek için *Kimlik Doğrulama Aracısı hesaplarını yönet* görevine özel bir komut eklemeniz gerekir. Tüm bilgisayarlardaki yönetici belirteç sertifikasını değiştirmek gibi bir grup görevi kullanmak kullanışlı olabilir.

Bir Kimlik Doğrulama Aracısı hesabı Yönetim Konsolu (MMC) aracılığıyla nasıl değiştirilir

1. *Kimlik Doğrulama Aracısı hesaplarını yönet* görevinin özelliklerini açın.

2. Görev özelliklerinden **Ayarlar** bölümünü seçin.

3. **Ekle → Hesap düzenleme komutu**.

4. Açılan penceredeki **Windows hesabı** alanında, değiştirmek istediğiniz Microsoft Windows kullanıcı hesabının adını belirtin.

5. Windows hesabının adını manuel olarak girdiyseniz **İzin ver** düğmesine tıklayarak hesap güvenlik tanımlayıcısını (SID) tanımlayın.

   İzin ver düğmesine tıklayarak güvenlik tanımlayıcısını (SID) belirlememeyi tercih ederseniz bilgisayarda görev gerçekleştirildiğinde belirlenir.

   > Bir Windows hesabı güvenlik tanımlayıcısı tanımlamak, Windows hesabının adının doğru girildiğini doğrulamak için gereklidir. Windows hesabı bilgisayarda ya da güvenilir etki alanında yoksa, *Kimlik Doğrulama Aracısı hesaplarını yönet* görevi bir hata ile sonuçlanır.

6. **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.

7. Parola tabanlı kimlik doğrulaması ayarlarını düzenlenebilir hale getirmek için **Parola tabanlı kimlik doğrulaması ayarlarını değiştir** onay kutusunu işaretleyin.

8. 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. Kimlik Doğrulama Aracısı hesabı için bir parola belirleyin.

9. 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 doğrulaması yapıldıktan sonra parola değiştirme kuralını düzenle** onay kutusunu işaretleyin.

10. Kimlik Doğrulama Aracısı'nda kimlik doğrulama üzerine parola değiştirme ayarı değerini belirtin.

11. Bir belirteç veya akıllı kartın elektronik sertifikasına dayalı olarak kimlik doğrulaması ayarlarını düzenlenebilir yapmak için **Sertifika tabanlı kimlik doğrulaması ayarlarını değiştir** onay kutusunu seçin.

12. 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. Bir akıllı kart ya da belirteç ile kimlik doğrulama için bir sertifika 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 erişim kuralını düzenle** onay kutusunu işaretleyin.

15. Kimlik Doğrulama Aracısı'nda, kimlik doğrulama iletişim kutusunda erişim kuralını belirtin.

16. Değişikliklerinizi kaydedin.

Bir Kimlik Doğrulama Aracısı hesabı Web Console aracılığıyla nasıl değiştirilir

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Kimlik Doğrulama Aracısı hesaplarını yönet** görevine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. Kimlik Doğrulama Aracısı hesapları listesinde **Ekle** düğmesine tıklayın ve **Hesabı düzenle** komut türünü seçin.

5. Bir kullanıcı hesabı seçin. Etki alanı hesapları listesinden bir hesap seçebilir ya da hesap adını manuel olarak girebilirsiniz. Bir sonraki adıma geçin.

   Kaspersky Endpoint Security, hesabın güvenlik tanımlayıcısını (Security Identifier, SID) belirler. Bu, hesabı doğrulamak için gereklidir. Kullanıcı adını yanlış girdiyseniz, Kaspersky Endpoint Security görevi bir hata ile sonlandırır.

6. Düzenlemek istediğiniz ayarların yanındaki onay kutularını işaretleyin.

7. Kimlik Doğrulama Aracısı hesabı ayarlarını yapılandırın.

   - **Var olan hesabın yerine yeni bir Kimlik Doğrulama Aracısı hesabı oluştur**. Kaspersky Endpoint Security bilgisayardaki mevcut hesapları tarar. Bilgisayardaki ve görevdeki kullanıcı güvenlik tanımlayıcısı eşleşirse, Kaspersky Endpoint Security kullanıcı hesabı ayarlarını göreve uygun olarak değiştirir.

   - **Kullanıcı adı**. Kimlik Doğrulama Aracısı hesabının varsayılan kullanıcı adı, kullanıcının etki alanı adına karşılık gelir.

   - **Parola tabanlı kimlik doğrulamasına izin ver**. Kimlik Doğrulama Aracısı hesabı için bir parola belirleyin. Gerekirse, ilk kimlik doğrulamasından sonra kullanıcıdan yeni bir parola isteyebilirsiniz. Bu şekilde, her kullanıcı kendi benzersiz parolasına sahip olur. Ayrıca, ilkedeki Kimlik Doğrulama Aracısı hesabı için parola gücü gereklilikleri ayarlayabilirsiniz.

   - **Sertifika tabanlı kimlik doğrulamasına izin ver**. Bir akıllı kart ya da belirteç ile kimlik doğrulama için bir sertifika seçin. Böylece kullanıcının akıllı kart veya belirteç için parola girmesi gerekir.

   - **Şifrelenmiş verilere hesap erişimi**. Şifrelenmiş sürücüye kullanıcı erişimini yapılandırın. Örneğin Kimlik Doğrulama Aracısı hesabını silmek yerine kullanıcı kimlik doğrulamasını geçici olarak devre dışı bırakabilirsiniz.

   - **Yorum**. Gerekirse bir hesap açıklaması girin.

8. Değişikliklerinizi kaydedin.

9. Görevin yanındaki onay kutusunu seçin ve **Başlat** düğmesine tıklayın.

Bir Kimlik Doğrulama Aracısı hesabını silmek için *Kimlik Doğrulama Aracısı hesaplarını yönet* görevine özel bir komut eklemeniz gerekir. İşten ayrılan bir çalışanın hesabını silmek gibi bir grup görevi kullanmak kullanışlı olabilir.

Bir Kimlik Doğrulama Aracısı hesabı Yönetim Konsolu (MMC) aracılığıyla nasıl silinir

1. *Kimlik Doğrulama Aracısı hesaplarını yönet* görevinin özelliklerini açın.

2. Görev özelliklerinden **Ayarlar** bölümünü seçin.

3. **Ekle** → **Hesap silme komutu**'na tıklayın.

4. Açılan penceredeki **Windows hesabı** alanında, silmek istediğiniz Kimlik Doğrulama Aracısı hesabını oluşturmak için kullanılan Windows hesabının adını belirtin.

5. Windows hesabının adını manuel olarak girdiyseniz **İzin ver** düğmesine tıklayarak hesap güvenlik tanımlayıcısını (SID) tanımlayın.

   İzin ver düğmesine tıklayarak güvenlik tanımlayıcısını (SID) belirlememeyi tercih ederseniz bilgisayarda görev gerçekleştirildiğinde belirlenir.

Bir Windows hesabı güvenlik tanımlayıcısı tanımlamak, Windows hesabının adının doğru girildiğini doğrulamak için gereklidir. Windows hesabı bilgisayarda ya da güvenilir etki alanında yoksa, *Kimlik Doğrulama Aracısı hesaplarını yönet* görevi bir hata ile sonuçlanır.

6. Değişikliklerinizi kaydedin.

Bir Kimlik Doğrulama Aracısı hesabı Web Console aracılığıyla nasıl silinir

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **Kimlik Doğrulama Aracısı hesaplarını yönet** görevine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. Kimlik Doğrulama Aracısı hesapları listesinde **Ekle** düğmesine tıklayın ve **Hesabı kaldır** komut türünü seçin.

5. Bir kullanıcı hesabı seçin. Etki alanı hesapları listesinden bir hesap seçebilir ya da hesap adını manuel olarak girebilirsiniz.

6. Değişikliklerinizi kaydedin.

7. Görevin yanındaki onay kutusunu seçin ve **Başlat** düğmesine tıklayın.

   Böylece görev bilgisayarın bir sonraki başlatılmasında tamamlandıktan sonra, kullanıcı kimlik doğrulama prosedürünü tamamlayamaz ve işletim sistemini yükleyemez. Kaspersky Endpoint Security şifrelenmiş verilere erişimi reddedecektir.

Aracı ile kimlik doğrulamasını tamamlayabilecek ve işletim sistemini yükleyebilecek kullanıcıların listesini görüntülemek için yönetilen bilgisayarın özelliklerine gitmelisiniz.

Kimlik Doğrulama Aracısı hesaplarının listesi Yönetim Konsolu (MMC) aracılığıyla nasıl görüntülenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Konsol ağacında şunu seçin: **Cihazlar**.

3. İlke özellikleri penceresini açmak için çift tıklayın.

4. İstemci bilgisayar özellikleri penceresinde **Görevler** bölümünü seçin.

5. Görev listesinde, **Kimlik Doğrulama Aracısı hesaplarını yönet**'i seçin ve çift tıklayarak görev özelliklerini açın.

6. Görev özelliklerinden **Ayarlar** bölümünü seçin.

   Böylece bu bilgisayardaki Kimlik Doğrulama Aracısı hesaplarının bir listesine erişim sağlayabilirsiniz. Sadece listede yer alan kullanıcılar Aracı ile kimlik doğrulamasını tamamlayabilir ve işletim sistemini yükleyebilir.

1. Web Console'un ana penceresinde **Varlık yönetimi → Varlıklar (Cihazlar)** seçimini yapın.

2. Kimlik Doğrulama Aracısı hesapları listesini görüntülemek istediğiniz bilgisayarın adına tıklayın.

3. Bilgisayar özelliklerinde, **Görevler** sekmesini seçin.

4. Görev listesinde, **Kimlik Doğrulama Aracısı hesaplarını yönet**'i seçin.

5. Görev ayarlarından **Uygulama ayarları** sekmesini seçin.

Böylece bu bilgisayardaki Kimlik Doğrulama Aracısı hesaplarının bir listesine erişim sağlayabilirsiniz. Sadece listede yer alan kullanıcılar Aracı ile kimlik doğrulamasını tamamlayabilir ve işletim sistemini yükleyebilir.

Kimlik Doğrulama Aracısı ile belirteç ve akıllı kart kullanma

Şifrelenmiş sabit sürücülere erişirken kimlik doğrulama için bir belirteç veya akıllı kart kullanılabilir. Bunu yapmak için bir belirtecin veya akıllı kartın elektronik sertifika dosyasını *Kimlik Doğrulama Aracısı hesaplarını yönet* görevine eklemelisiniz.

Sadece 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.

Kaspersky Endpoint Security aşağıdaki belirteçler, akıllı kart okuyucular ve akıllı kartları destekler:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

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.
- Sertifika, en az 1024 bit uzunluğunda bir RSA anahtarı içerir.

Belirteç veya akıllı kartın elektronik sertifikası gereklilikleri karşılamadığı takdirde, bir Kimlik Doğrulama Aracısı hesabı oluşturmak için sertifika dosyasını komuta yükleyemezsiniz.

Sertifikanın `KeyUsage` parametresi, `keyEncipherment` veya `dataEncipherment` değerine sahip olmalıdır. `KeyUsage` parametresi sertifikanın parametresini belirler. Parametre farklı bir değere sahipse Kaspersky Security Center sertifika dosyasını indirir ancak bir uyarı görüntüler.

Kullanıcı bir belirteç veya akıllı kartı kaybetmişse yönetici, bir Kimlik Doğrulama Aracısı hesabı oluşturmak için belirteç veya akıllı kart elektronik sertifika dosyasını komuta eklemelidir. Kullanıcı daha sonra şifrelenmiş cihazlara erişim sağlama veya şifrelenen cihazlardaki verilerin kurtarılması prosedürlerini tamamlamalıdır.

Sabit sürücü şifresini çözme

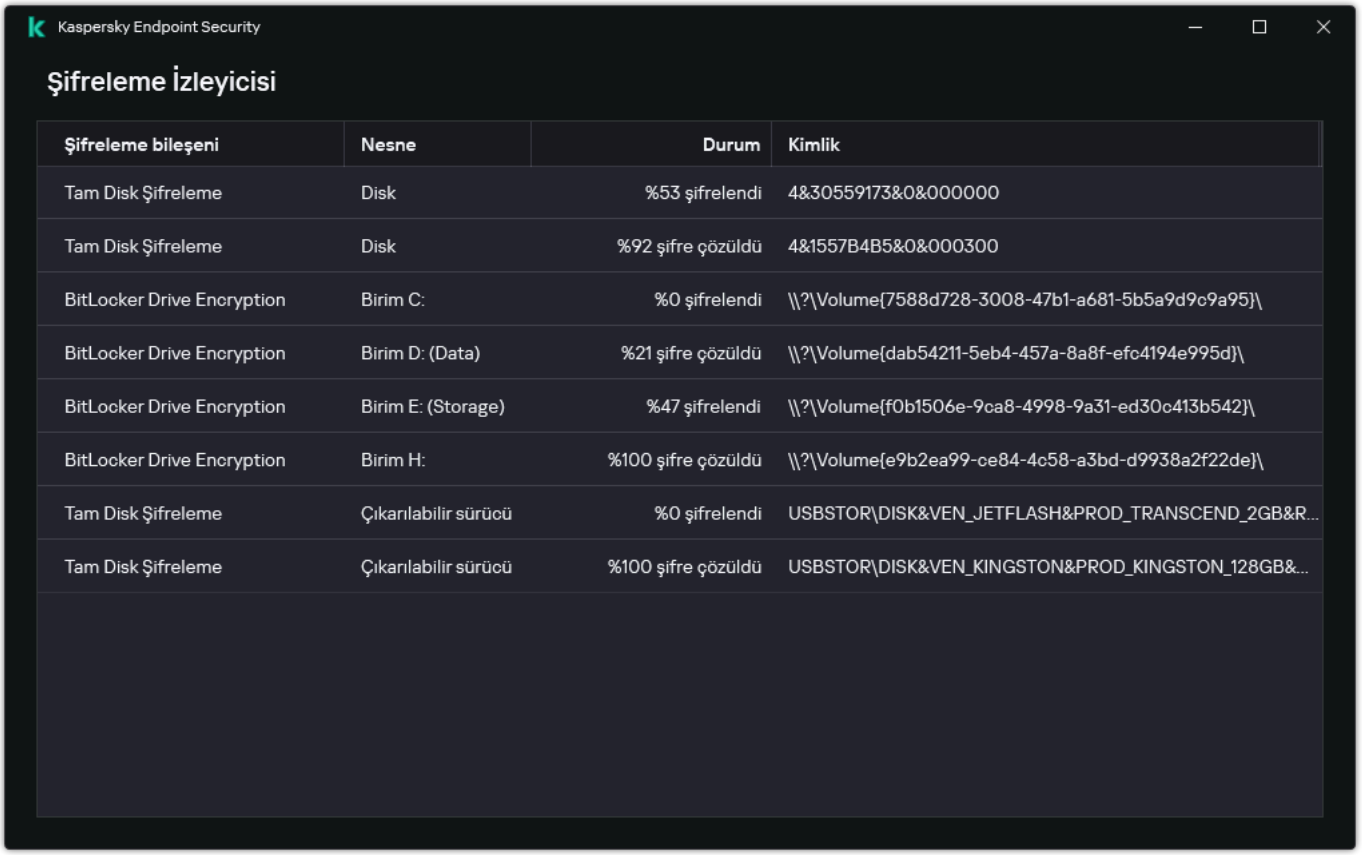
Veri şifrelemesine izin veren geçerli bir lisans olmasa dahi sabit sürücülerin şifresini çözebilirsiniz.

Sabit sürücülerin şifresini çözmek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
4. **Şifreleme teknolojisi** açılır listesinde, sabit sürücülerin şifrelendiği teknolojiyi seçin.
5. 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.
6. Değişikliklerinizi kaydedin.

Bir kullanıcının bilgisayarındaki disk şifreleme veya şifre çözme işlemini kontrol etmek için Şifreleme İzleyicisi aracını kullanabilirsiniz. Şifreleme İzleyicisi aracını ana uygulama penceresinden çalıştırabilirsiniz.



Şifreleme İzleyicisi

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.

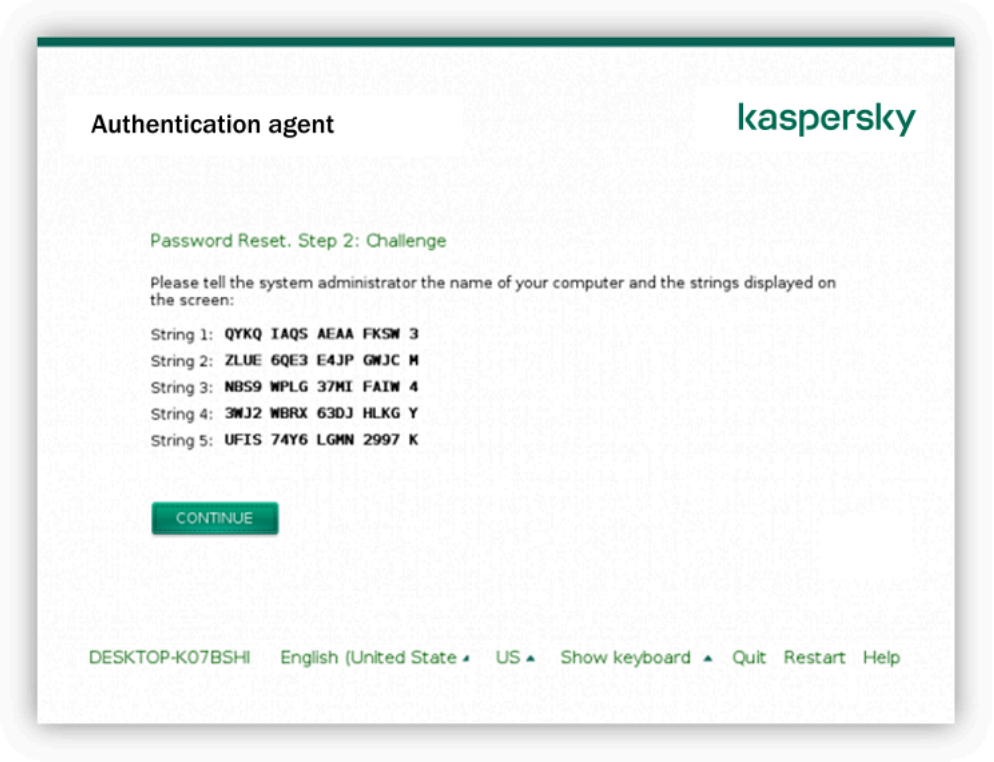
Kaspersky Disk Encryption teknolojisi tarafından korunan bir sürücüye yeniden erişim sağlamak

Bir kullanıcının Kaspersky Disk Encryption teknolojisi tarafından korunan bir sabit sürücüye erişim parolasını unutması halinde, kurtarma prosedürünü (İstek-Yanıt) yeniden başlatmanız gerekir. Ayrıca, bu özellik disk şifreleme ayarlarında etkinleştirildiği takdirde, sabit diske erişim elde etmek için hizmet hesabını kullanabilirsiniz.

Sistem sabit sürücüsüne yeniden erişim

Kaspersky Disk Encryption teknoloji tarafından korunan bir sistem sabit sürücüsüne yeniden erişim sağlamak için aşağıdaki adımlar uygulanmalıdır:

1. Kullanıcı yöneticiye istek bloklarını raporlar (aşağıdaki resme bakın).
2. Yönetici istek bloklarını Kaspersky Security Center'a girer, yanıt bloklarını alır ve yanıt bloklarını kullanıcıya raporlar.
3. Kullanıcı yanıt bloklarını Kimlik Doğrulama Aracısı'na girer ve sabit sürücüye erişim elde eder.



Kaspersky Disk Encryption teknolojisi tarafından korunan bir sistem sabit sürücüsüne yeniden erişim sağlamak

Kurtarma prosedürünü başlatmak için kullanıcının Kimlik Doğrulama Aracısı arabirimindeki **Parolanızı mı unuttunuz?** düğmesine tıklaması gerekir.

Yönetim Konsolu'nda (MMC) Kaspersky Disk Encryption teknoloji tarafından korunan bir sistem sabit sürücüsü için yanıt blokları nasıl alınır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Cihazlar**.
3. **Cihazlar** sekmesinde, şifrelenmiş verilere erişim talep eden kullanıcının bilgisayarını seçin ve bağlam menüsünü görüntülemek için sağ tıklayın.
4. İçerik menüsünde **Çevrimdışı modda erişim ver** seçeneğini belirleyin.
5. Bu işlem bir pencere açar; bu pencerede **Kimlik Doğrulama Aracısı** sekmesini seçin.
6. **Kullanılmakta olan şifreleme algoritması** bloğundan bir şifreleme algoritması seçin: **AES56** veya **AES256**.

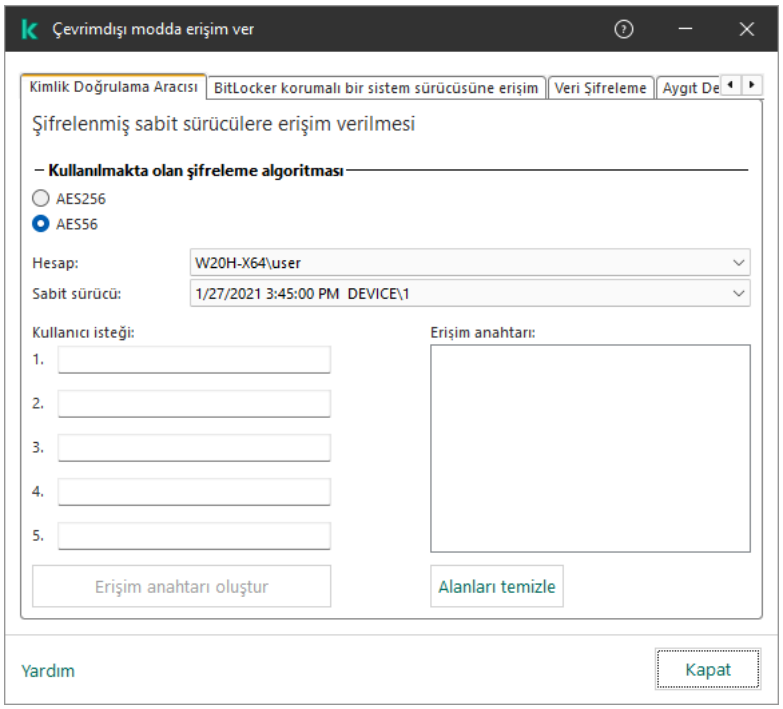
   Veri şifreleme algoritması, dağıtım paketine dahil olan AES şifreleme kitaplığına bağlıdır: *Güçlü şifreleme (AES256)* veya *Hafif şifreleme (AES56)*. AES şifreleme kitaplığı uygulama ile birlikte yüklenir.

7. **Hesap** açılır listesinden, sürücüye erişimi yeniden sağlama istediğini yapan Kimlik Doğrulama Aracısı hesap adını seçin.

8. **Sabit sürücü** açılır listesinde, erişimi kurtarmanız gereken şifrelenmiş sabit sürücüyü seçin.

9. **Kullanıcı isteği** bloğunda, kullanıcı tarafından belirtilen istek bloklarını girin.

Sonuç olarak, Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasının kurtarılması kullanıcı isteğine verilen yanıtın blokları, **Erişim anahtarı** alanında görüntülenir. Yanıt bloklarının içeriğini kullanıcıya aktarın.



Çevrimdışı modda erişim ver

Web Console'da Kaspersky Disk Encryption teknoloji tarafından korunan bir sistem sabit sürücüsü için yanıt blokları nasıl alınır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.

2. Sürücüsüne tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.

3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.

4. Açılan pencerede, **Kimlik Doğrulama Aracısı** bölümünü seçin.

5. **Hesap** açılır listesinde, Kimlik Doğrulama Aracısı hesabı adının ve parolasının kurtarılmasını isteyen kullanıcı için oluşturulan Kimlik Doğrulama Aracısı hesabının adını seçin.

6. Kullanıcıya aktarılan istek bloklarını girin.

Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasının kurtarılması kullanıcı isteğine verilen yanıtın blokları, pencerenin alt kısmında görüntülenir. Yanıt bloklarının içeriğini kullanıcıya aktarın.

Kurtarma prosedürünü tamamladıktan sonra, Kimlik Doğrulama Aracısı kullanıcıdan parolayı değiştirmesini ister.

Sistem dışı bir sabit sürücüye yeniden erişim

Kaspersky Disk Encryption teknoloji tarafından korunan bir sistem dışı sabit sürücüsüne yeniden erişim sağlamak için aşağıdaki adımlar uygulanmalıdır:

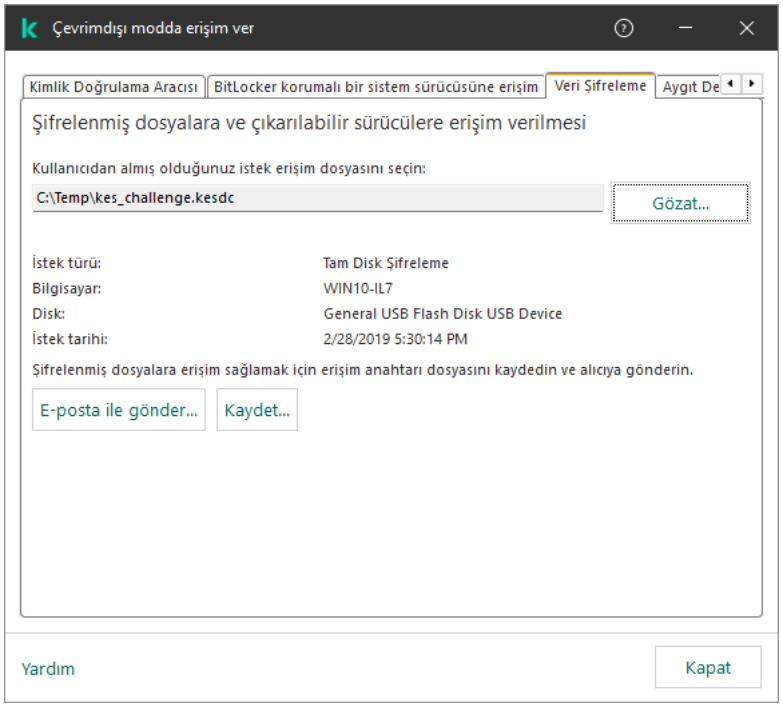
1. Kullanıcı yöneticiye bir istek erişim dosyası gönderir.
2. Yönetici istek erişim dosyasını Kaspersky Security Center'a ekler, bir istek erişim dosyası oluşturur ve bu dosyayı kullanıcıya gönderir.
3. Kullanıcı erişim anahtarını Kaspersky Endpoint Security'ye ekler ve sabit sürücüye erişim elde eder.

Kurtarma prosedürünü başlatmak için kullanıcının bir sabit sürücüye erişim girişiminde bulunması gerekir. Sonuç olarak, Kaspersky Endpoint Security bir istek erişim dosyası oluşturur (KESDC uzantılı bir dosya) ve kullanıcının bu dosyayı yöneticiye göndermesi gerekir, örneğin e-posta ile.

Yönetim Konsolu'nda (MMC) şifrelenmiş bir sistem dışı sabit sürücüye erişim nasıl sağlanır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Cihazlar**.
3. **Cihazlar** sekmesinde, şifrelenmiş verilere erişim talep eden kullanıcının bilgisayarını seçin ve bağlam menüsünü görüntülemek için sağ tıklayın.
4. İçerik menüsünde **Çevrimdışı modda erişim ver** seçeneğini belirleyin.
5. Bu işlem bir pencere açar; bu pencerede **Veri Şifreleme** sekmesini seçin.
6. **Veri Şifreleme** sekmesinde, **Gözat** düğmesine tıklayın.
7. İstek erişim dosyası seçme penceresinde, kullanıcıdan alınan dosyanın yolunu belirdin.

Kullanıcının isteğiyle ilgili bilgiler görüntülenir. Kaspersky Security Center bir anahtar dosyası oluşturur. Oluşturulan şifrelenmiş dosya erişim anahtar dosyasını kullanıcıya e-posta ile gönderin. Yahut erişim dosyasını kaydedin ve transfer içi mevcut yöntemlerden birini kullanın.



Çevrimdışı modda erişim ver

Web Console'da bir şifrelenmiş sistem dışı sabit sürücü erişim anahtar dosyası nasıl alınır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Verilerine tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.
3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.
4. **Veri Şifreleme**'yi seçin.
5. **Dosya seç** düğmesine tıklayın ve kullanıcıdan aldığınız istek erişim dosyasını (KESDC uzantılı bir dosya) seçin.

   Web Console, istekle ilgili bilgileri görüntüler. Bu bilgiler arasında kullanıcının dosyaya erişim isteği yaptığı bilgisayarın adı da yer alır.
6. **Anahtarı kaydet** düğmesine tıklayın ve şifrelenmiş veri erişim anahtarı dosyasının (KESDR uzantılı bir dosya) kaydedileceği bir klasör seçin.

Sonuç olarak, kullanıcıya aktarmanız gereken şifrelenmiş verilere erişim anahtarını alırsınız.

Kimlik Doğrulama Aracısı hizmet hesabıyla oturum açma

Kaspersky Endpoint Security, bir sürücüyü şifrelerken bir Kimlik Doğrulama Aracısı hizmet hesabı eklemenize izin verir. Hizmet hesabı, örneğin kullanıcı parolasını unuttuğunda bilgisayara erişim sağlamak için gereklidir. Hizmet hesabını bir rezerve hesap olarak da kullanabilirsiniz. Bir hesap eklemek için disk şifreleme ayarları bölümünden bir hizmet hesabı seçin ve kullanıcı hesabının adını girin (varsayılan olarak, `ServiceAccount`). Aracıyı kullanarak kimlik doğrulaması yapmak için tek kullanımlık bir parolaya ihtiyacınız olacaktır.

Yönetim Konsolu'nda (MMC) tek kullanımlık parola nasıl bulunur

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Cihazlar**.
3. İlke özellikleri penceresini açmak için çift tıklayın.
4. İstemci bilgisayar özellikleri penceresinde **Görevler** bölümünü seçin.
5. Görev listesinde, **Kimlik Doğrulama Aracısı hesaplarını yönet**'i seçin ve çift tıklayarak görev özelliklerini açın.
6. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.
7. Hesaplar listesinden Kimlik Doğrulama Aracısı hizmet hesabını seçin (örneğin, `WIN10-USER\ServiceAccount`).
8. **Eylem** açılır listesinden **Hesabı görüntüle** seçimini yapın.
9. Hesap özelliklerinden **İlk parolayı göster** onay kutusunu seçin.
10. Hizmet hesabıyla oturum açmak için tek kullanımlık parolayı kopyalayın.

Web Console'da tek kullanımlık parola nasıl bulunur

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Kimlik Doğrulama Aracısı hesapları listesini görüntülemek istediğiniz bilgisayarın adına tıklayın.
   Bu, bilgisayar özelliklerini açar.
3. Bilgisayar özelliklerinde, **Görevler** sekmesini seçin.
4. Görev listesinde, **Kimlik Doğrulama Aracısı hesaplarını yönet**'i seçin.
5. Görev ayarlarından **Uygulama ayarları** sekmesini seçin.
6. Hesaplar listesinden Kimlik Doğrulama Aracısı hizmet hesabını seçin (örneğin, `WIN10-USER\ServiceAccount`).
7. Hesap özelliklerinden **Parolayı göster** onay kutusunu seçin.
8. Hizmet hesabıyla oturum açmak için tek kullanımlık parolayı kopyalayın.

Kaspersky Endpoint Security, bir kullanıcı hizmet hesabıyla her kimlik doğrulama gerçekleştirdiğinde, parolayı otomatik olarak günceller. Aracıyı kullanarak kimlik doğrulaması yaptıktan sonra Windows hesabı parolasını girmeniz gerekir. Hizmet hesabıyla oturum açarken SSO teknolojisini kullanamazsınız.

İşletim sistemini güncelleme

Tam Disk Şifreleme (FDE) tarafından korunan bir bilgisayarın işletim sisteminin güncellenmesi için dikkate alınması gereken bazı özel durumlar vardır. İşletim sistemini şöyle güncelleyin: önce bir bilgisayar üzerindeki işletim sistemini güncelleyin ve ardından küçük bir grup bilgisayardaki işletim sistemi güncelleyin, son olarak da ağdaki tüm bilgisayarların işletim sistemlerini güncelleyin.

Kaspersky Disk Encryption teknolojisini kullanıyorsanız Kimlik Doğrulama Aracısı işletim sistemi başlatılmadan önce yüklenmiştir. Kullanıcı, Kimlik Doğrulama Aracısı'nı kullanarak sisteme giriş yaparak şifrelenmiş sürücülere erişebilir. Bundan sonra işletim sistemi yüklemeye başlar. Kaspersky Disk Encryption teknolojisi kullanılarak korunan bir bilgisayarda bir işletim sistemi güncellemesi başlatırsanız, İşletim Sistemi Güncelleme Sihirbazı Kimlik Doğrulama Aracısı'nı kaldıracaktır. Bunun sonucunda, işletim sistemi yükleyicisi şifrelenmiş sürücüye erişim sağlayamayacağından bilgisayar kilitlenebilir.

İşletim sistemi güncellemesinin özellikleri:

- **WSUS aracılığıyla işletim sistemini güncelleme**. İşletim sistemini normal şekilde güncelleyebilirsiniz.
- **İşletim Sistemini ISO'dan Güncelleme**. İşletim sistemini güncellemek için Kaspersky disk şifreleme sürücülerinin bulunduğu klasörü belirtmeniz gerekir. Uygulama sürücüleri otomatik olarak ayrı bir klasöre kopyalar. Aşağıdakileri uygulayın:

  1. ISO görüntüsünü bağlayın.
  2. Sistem güncellemesinin kurulumunu şu anahtarla başlatın:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

Otomatik işletim sistemi güncellemesi yalnızca bilgisayar Windows 10 1607 (RS1) veya üstünü çalıştırıyorsa kullanılabilir. İşletim sisteminin önceki sürümlerini yükseltmek için önce diskin şifresini çözmeniz, bir işletim sistemi yükseltmesi gerçekleştirmeniz ve ardından diski şifrelemeniz önerilir.

BitLocker Drive Encryption teknolojisini kullanıyorsanız Windows 10'u güncellemek için sabit sürücülerin şifresini çözmenize gerek yoktur. BitLocker hakkında daha fazla bilgi için lütfen Microsoft web sitesini ziyaret edin.

Şifreleme işlevselliğini güncelleme hatalarını ortadan kaldırma

Tam Disk Şifreleme, uygulamanın önceki bir sürümü Kaspersky Endpoint Security for Windows 14.2 for Windows sürümüne yükseltildiğinde güncellenir.

Tam Disk Şifreleme işlevselliğinin güncellenmesi işlemi başlatılırken aşağıdaki hatalar oluşabilir:

- Güncelleme başlatılamıyor.
- Aygıt Kimlik Doğrulama Aracısı ile uyumsuz.

Yeni uygulama sürümünde Tam Disk Şifreleme işlevselliğinin güncelleme işlemini başlattığınızda oluşan hataları ortadan kaldırmak için:

1. Sabit sürücülerin şifresini çözün.
2. Bir kez daha sabit sürücüleri şifreleyin.

Tam Disk Şifreleme işlevselliğinin güncellemesi sırasında aşağıdaki hatalar oluşabilir:

- Güncelleme tamamlanamıyor.
- Tam Disk Şifreleme yükseltmesini geri alma işlemi bir hatayla tamamlandı.

Tam Disk Şifreleme işlevselliğinin güncellenmesi işlemi sırasında oluşan hataları ortadan kaldırmak için

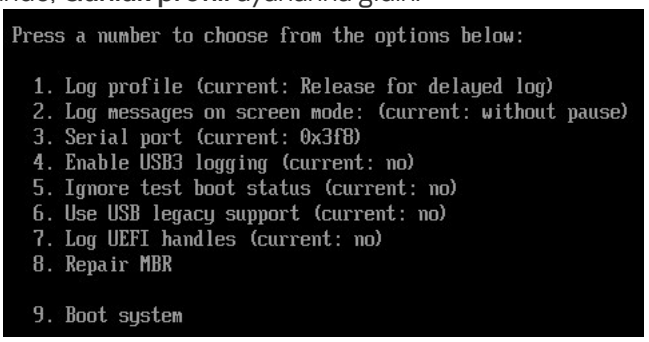
Geri Yükleme Yardımcı Programını kullanarak şifrelenmiş cihazlara erişimi geri yükleyin.

Kimlik Doğrulama Aracısını İzleme

Uygulama, Kimlik Doğrulama Aracısı'nın işlemleri hakkında hizmet bilgisini ve Kimlik Doğrulama Aracısı ile kullanıcının yaptığı işlemler hakkındaki bilgiyi izleme dosyasına kaydeder.

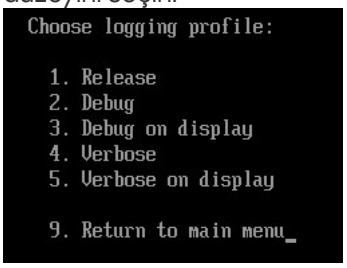
Kimlik Doğrulama Aracısı izlemesini etkinleştirmek için:

1. Kaspersky Endpoint Security izlemesini etkinleştirin.
2. Bilgisayarı yeniden başlat.
3. Şifrelenmiş sabit sürücüye sahip bir bilgisayar açılır açılmaz Kimlik Doğrulama Aracısı ayarlarını yapılandırmak amacıyla pencere açmak için **F3** tuşuna basın.
4. FDE önyükleyici başlatıldıktan sonra, **KES (FDE <sürüm>)** önyükleme yöneticisini seçin.
5. Önyükleme yöneticisi menüsünde, **Günlük profili** ayarlarına gidin.



Önyükleme yöneticisi menüsü

6. Günlük profili ayarları penceresinde izleme düzeyini seçin:



Kimlik Doğrulama Aracısı izleme düzeyleri

- **Bırak**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı olayları hakkında izleme dosyasına bilgi kaydetmez.
- **Hata ayıklama**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgileri izleme dosyasına kaydeder.

- **Ekranda hata ayıklama**. 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 portu üzerinden aktarır.

  Şifrelenmiş sabit sürücülü bir bilgisayar COM portu üzerinden başka bir bilgisayara bağlanırsa Kimlik Doğrulama Aracısı olayları söz konusu diğer bilgisayardan incelenebilir.

- **Ayrıntılı**. 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** seçeneğinin düzeyi ile karşılaştırıldığında bu seçenek altındaki giriş ayrıntılarının düzeyi daha yüksektir. Yüksek düzeyde giriş ayrıntıları Kimlik Doğrulama Aracısı ve işletim sisteminin açılışını yavaşlatabilir.

- **Ekranda ayrıntılı bilgi**. 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 portu üzerinden aktarır.

  > **Ekranda hata ayıklama** seçeneğinin düzeyi ile karşılaştırıldığında bu seçenek altındaki giriş ayrıntılarının düzeyi daha yüksektir. Yüksek düzeyde giriş ayrıntıları Kimlik Doğrulama Aracısı ve işletim sisteminin açılışını yavaşlatabilir.

Bir izleme düzeyi seçtikten sonra, önyükleme yöneticisi menüyü tekrar görüntüler.

7. Önyükleme yöneticisi menüsünde **Önyükleme sistemi** seçimini yapın.

   FDE önyükleyici, Kimlik Doğrulama Aracısını başlatır.

   Sorunu yeniden oluşturun.

   Bilgisayarda şifrelenmiş sabit sürücüler varsa veya tam disk şifreleme sırasında, veriler Kimlik Doğrulama Aracısı izleme dosyasına kaydedilir.

8. İzleme işlemini durdurmak için Destek Araçları penceresine geri dönün ve izlemeyi devre dışı bırakın.

Sonuç olarak, `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasöründe Kimlik Doğrulama Aracısı KES.SRV çalışma iz dosyaları oluşturulur. 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 yardım metinlerini düzenleme

> Kimlik Doğrulama Aracısı'nın yardım mesajlarını düzenlemeden önce lütfen önyükleme ortamında desteklenen karakterlerin listesini gözden geçirin (aşağıya bakın).

Kimlik Doğrulama Aracısı yardım mesajlarını düzenlemek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Ortak şifreleme ayarları** seçimini yapın.

4. **Şablonlar** bloğunda, **Yardım** düğmesine tıklayın.

5. Açılan pencerede şunları yapın:

   - 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.

6. Yardım mesajlarını düzenleyin.

   Orijinal metni geri yüklemek isterseniz **Varsayılan olarak** düğmesine tıklayın.

   > 16 satır veya daha az yardım metni girebilirsiniz. Satır en fazla 64 karakter uzunluğunda olabilir.

7. Değişikliklerinizi kaydedin.

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'nın çalışması test edildikten sonra kalan nesnelerin ve verilerin kaldırılması

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 şu yöntemleri kullanarak 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 Geri Yükleme Yardımcı Programı'nı kullanmak için:

1. Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyası olan fdert.exe isimli dosyayı çalıştırın. Bu dosya, Kaspersky Endpoint Security tarafından oluşturulur.
2. Geri Yükleme Yardımcı Programı penceresinde gerekli aygıtı seçin.
3. **Tara**'ya tıklayın.
4. Sistem sabit sürücüsünü tanıladıktan sonra, Kimlik Doğrulama Aracısı'nın test işleminden kalan nesneler ve veriler olduğunu belirten bir mesaj alırsanız **AA nesnelerini ve verilerini sil** düğmesine tıklayın.

   AA nesnelerini ve verilerini sil düğmesi, yalnızca Kimlik Doğrulama Aracısı'nın test işleminin ardından kalan nesneler ve veriler algılanırsa kullanılabilir.

Kimlik Doğrulama Aracısı ile uygulama uyumsuzluğu hakkındaki bilgileri kaldırmak için

komut satırına `avp pbatestreset` komutunu yazın.

BitLocker Management

BitLocker, Windows işletim sistemlerinde yerleşik olarak bulunan bir şifreleme teknolojisidir. Kaspersky Endpoint Security, Kaspersky Next altyapısını kullanarak Bitlocker'ı kontrol etmenizi ve yönetmenizi sağlar. BitLocker mantıksal birimleri şifreler. BitLocker, çıkarılabilir sürücülerin şifrelenmesi için kullanılamaz. BitLocker hakkında daha ayrıntılı bilgi için Microsoft belgelerine bakın.

BitLocker diski şifrelerken önyükleme yükleyicisini ve diğer yardımcı dosyaları system partition içeriğine yerleştirir. Bu bölüm şifrelenmemiştir. İşletim sistemi, Windows kurulumu sırasında sistem bölümünü otomatik olarak oluşturur. Windows'u yüklemeden önce disk tamamen bölümlenmişse, işletim sistemi bir sistem bölümü oluşturamaz. Bu durumda, BitLocker disk şifrelemesini başlattığınızda, işletim sistemi diski yeniden bölümlendirmenizi ve bir sistem bölümü oluşturmanızı ister. Bir sistem bölümü oluşturduktan sonra, işletim sistemi BitLocker şifrelemesini başlatır.

BitLocker şifreleme algoritması, dağıtım paketinde bulunan AES kütüphanesi sürümüne (AES256 veya AES56) bağlı değildir. Şifreleme, işletim sisteminin yerleşik şifreleme kütüphanesini kullanır.

Varsayılan olarak, uygulama daha önce hiç şifrelenmemiş cihazları şifrelemek için 256 bitlik etkin anahtar uzunluğuna sahip BitLocker şifreleme algoritmasını kullanır. Uygulama kurulmadan önce şifrelenmiş bir cihazda, şifreleme algoritması farklı olabilir. Şifreleme algoritmasının seçilmesiyle ilgili ayrıntılar için Microsoft Teknik Destek web sitesine bakın. 12.9 sürümünden itibaren, Kaspersky Endpoint Security, daha önce üçüncü taraf uygulamalar tarafından şifrelenmiş cihazların orijinal kurtarma anahtarını Kaspersky Security Center'a gönderir.

BitLocker, güvenilir bir platform modülü kullanarak erişim anahtarlarının güvenli bir şekilde saklanmasını sağlar. Bir *Trusted Platform Module (TPM)* güvenlikle ilgili temel işlevleri (örneğin şifreleme anahtarlarını saklamak için) sağlamak üzere geliştirilmiş bir mikroçiptir. Bir Güvenilir Platform Modülü genellikle bilgisayarın ana kartına yüklenmiştir ve donanım veri yolu aracılığıyla tüm diğer sistem bileşenleri ile etkileşim halindedir. TPM, başlatma öncesi sistem bütünlüğü doğrulaması sağladığından, BitLocker erişim anahtarlarını depolamanın en güvenli yolu TPM kullanmaktır. Bir bilgisayardaki sürücüleri TPM olmadan da şifreleyebilirsiniz. Bu durumda erişim anahtarı bir parola ile şifrelenecektir. BitLocker şu kimlik doğrulama yöntemlerini kullanır:

- TPM.
- TPM ve PIN.
- Parola.

Sistem sabit sürücüsünü şifreledikten sonra, işlem sistemini önyüklemek için kullanıcının BitLocker kimlik doğrulamasını gerçekleştirmesi gerekir. Kimlik doğrulamasından sonra BitLocker kullanıcının oturum açmasına izin verir. BitLocker çoklu oturum açma (SSO) desteği sunmaz.

Bir sürücüyü şifreledikten sonra, BitLocker bir kurtarma anahtarı oluşturur. Kaspersky Endpoint Security, kurtarma anahtarını Kaspersky Security Center'a gönderir, böylece mesela bir kullanıcı parolasını unuttuysa diske erişimi geri yükleyebilirsiniz.

Bir kullanıcı bir diski BitLocker ile şifrelediğinde, Kaspersky Endpoint Security kurtarma anahtarını ve disk şifrelemeyle ilgili bilgileri Kaspersky Security Center'a gönderir.

Windows grup ilkeleri kullanıyorsanız ilke ayarlarından BitLocker yönetimini kapatın. Windows ilke ayarları Kaspersky Endpoint Security'nin ilke ayarları ile çakışabilir. Bir sürücüyü şifrelerken hatalar meydana gelebilir.

BitLocker Drive Encryption'ı başlatma

Tam disk şifrelemeyi başlatmadan önce bilgisayarda virüs bulunmadığından emin olmanızı öneririz. Bunun için Tam Tarama veya Kritik Alanları Tarama görevini başlatın. Rootkit virüsü bulaşmış bir bilgisayarda tam disk şifreleme yapılması bilgisayarın çalışmamasına neden olabilir.

Windows tabanlı işletim sistemlerinde sunucular için BitLocker Drive Encryption kullanmak için, BitLocker Drive Encryption bileşeninin yüklenmesi gerekebilir. Bileşeni, işletim sistemi araçlarını kullanarak yükleyin (Rol ve Bileşen Ekle Sihirbazı). BitLocker Drive Encryption kurulumu hakkında daha fazla bilgi için Microsoft belgelerine bakın.

BitLocker Drive Encryption bileşeni Yönetim Konsolu (MMC) üzerinden nasıl başlatılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
4. **Şifreleme teknolojisi** açılır listesinde **BitLocker Drive Encryption** öğesini seçin.
5. **Şifreleme modu** açılır listesinden **Tüm sabit sürücüleri şifrele** seçeneğini seçin.

   Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca şifreleme işleminin gerçekleştirildiği işletim sistemini yükleyebilirsiniz.

6. Gelişmiş BitLocker Drive Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
7. Değişikliklerinizi kaydedin.

BitLocker Sürücü Şifrelemesini Web Console'da çalıştırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Tam Disk Şifreleme**'ye gidin.
5. **BitLocker Disk Şifrelemesi** teknolojisini seçin.

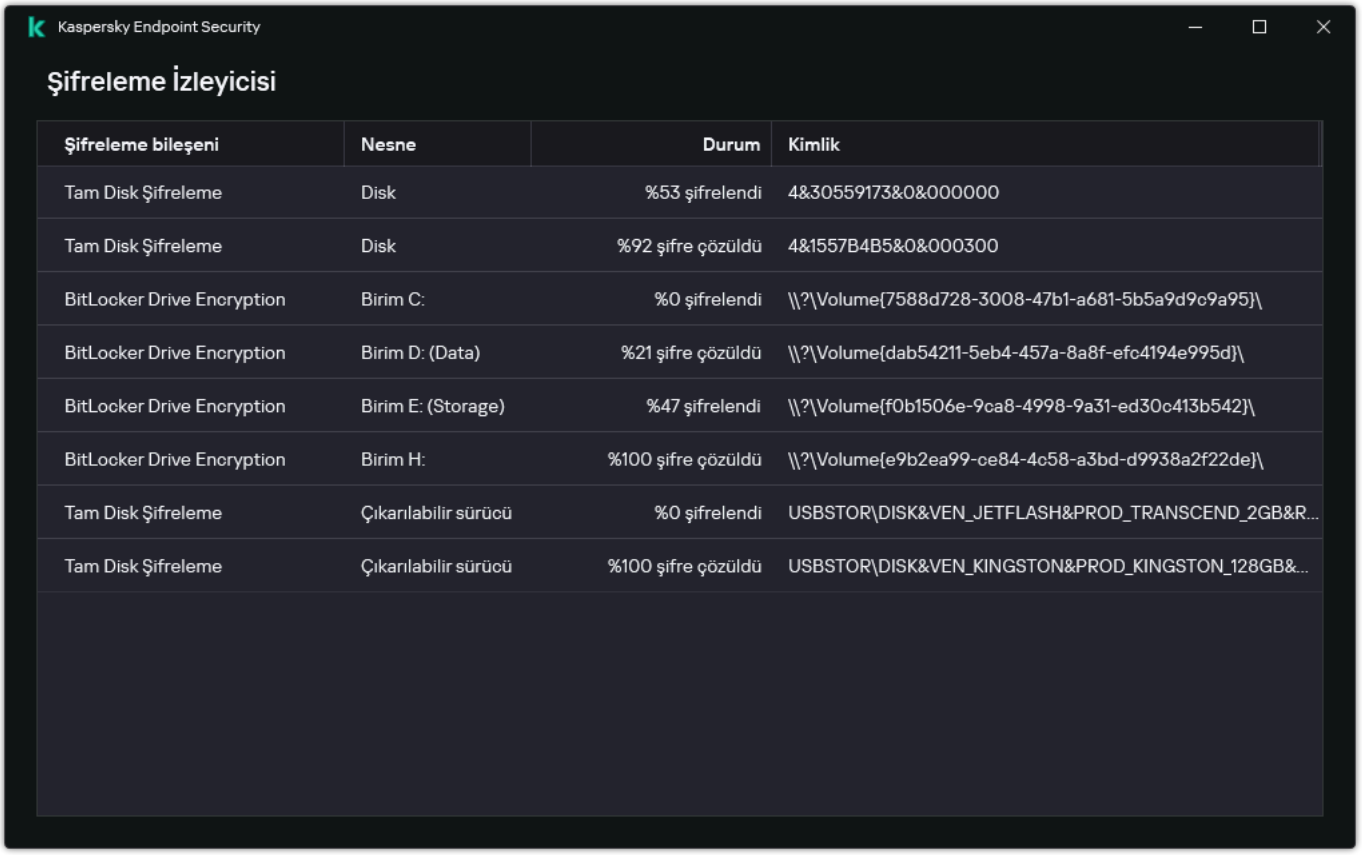
6. **Cihazlardaki eylem** bloğunda **Tüm sabit sürücüleri şifrele**'yi seçin.

Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca şifreleme işleminin gerçekleştirildiği işletim sistemini yükleyebilirsiniz.

7. Gelişmiş BitLocker Drive Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).

8. Değişikliklerinizi kaydedin.

Bir kullanıcının bilgisayarındaki disk şifreleme veya şifre çözme işlemini kontrol etmek için Şifreleme İzleyicisi aracını kullanabilirsiniz. Şifreleme İzleyicisi aracını ana uygulama penceresinden çalıştırabilirsiniz.



Şifreleme İzleyicisi

İlke uygulandıktan sonra uygulama, kimlik doğrulama ayarlarına bağlı olarak aşağıdaki sorguları görüntüler:

- Sadece TPM. Kullanıcının giriş yapmasına gerek yoktur. Bilgisayar yeniden başlatıldığında disk şifrelenecektir.
- TPM + PIN / Parola. TPM modülü varsa bir PIN kodu istem penceresi görüntülenir. TPM modülü yoksa önyükleme öncesi kimlik doğrulaması için bir parola istem penceresi görürsünüz.
- Sadece parola. Önyükleme öncesi kimlik doğrulaması için bir parola istem penceresi görürsünüz.

Federal Bilgi İşleme standart uyumluluk modu, bilgisayar işletim sistemi için etkinse Windows 8'de ve işletim sisteminin önceki sürümlerinde kurtarma anahtarı dosyasını kaydetmek için bir depolama aygıtı bağlama isteği görüntülenir. Tek bir depolama aygıtına birden fazla kurtarma anahtarı kaydedebilirsiniz.

Bir parola ya da PIN ayarladıktan sonra, BitLocker şifrelemeyi tamamlamak için sizden bilgisayarınızı yeniden başlatmanızı isteyecektir. Bundan sonra kullanıcının BitLocker kimlik doğrulama prosedürünü tamamlaması gerekir. Kimlik doğrulama prosedüründen sonra kullanıcı sisteme giriş yapmalıdır. İşletim sistemi yüklendikten sonra, BitLocker şifrelemeyi tamamlayacaktır.

Şifreleme anahtarlarına erişim yoksa kullanıcı, yerel ağ yöneticisinden bir kurtarma anahtarı sağlamasını isteyebilir (kurtarma anahtarı önceden bir depolama aygıtına kaydedilmediyse veya kaybolduysa).

BitLocker Drive Encryption bileşeni ayarları

Parametre	Açıklama
Tabletlerde önyükleme öncesi klavye gerektiren BitLocker kimlik doğrulaması kullanımını etkinleştir	Platform önyükleme öncesi giriş özelliğine sahip olmasa bile (örneğin, tabletlerde dokunmatik ekran klavyeleri ile) önyükleme öncesi ortamda veri girişi gerektiren kimlik doğrulamasının kullanılması. Tablet bilgisayarların dokunmatik ekranı önyükleme ortamında kullanılamaz. Tablet bilgisayarlarda BitLocker kimlik doğrulamasını tamamlamak için kullanıcının USB klavye gibi bir aygıt bağlaması gerekir. Onay kutusu işaretlenirse önyükleme girişi gerektiren kimlik doğrulamasının kullanılmasına izin verilir. Bu ayarın yalnızca dokunmatik ekran klavyelerine ek olarak USB klavye gibi önyükleme öncesi ortamda alternatif veri giriş araçlarına sahip cihazlar için kullanılması önerilir. Bu kutu işaretlenmemişse, tabletlerde BitLocker Drive Encryption kullanmak mümkün olmaz.
Donanım şifrelemesi kullan (Windows 8 ve sonraki sürümler)	Onay kutusu işaretlenirse uygulama, donanım şifrelemesi uygular. Bu, şifreleme hızını artırmanızı ve daha az bilgisayar kaynağı kullanmanızı sağlar.
Sadece kullanılan disk alanını şifrele (Windows 8 ve sonraki sürümler)	Bu onay kutusu, şifreleme alanını yalnızca kullanılan sabit sürücü sektörleri ile sınırlayan seçeneği etkinleştirir/devre dışı bırakır. Bu sınır şifreleme süresini azaltmanızı sağlar. **Sadece kullanılan disk alanını şifrele (şifreleme süresini kısaltır)** özelliğinin şifrelemeyi başlattıktan sonra etkinleştirilmesi veya devre dışı bırakılması durumunda, sabit sürücülerin şifresi çözülene kadar bu ayar değiştirilmez. Şifrelemeyi başlatmadan önce onay kutusunu işaretlemeniz veya işaretini kaldırmanız gerekir. Onay kutusu işaretlenirse sabit sürücünün yalnızca dosyalar tarafından kullanılan bölümleri şifrelenir. Kaspersky Endpoint Security yeni eklenen verileri otomatik olarak şifreler. Onay kutusunun işareti kaldırılırsa daha önce silinen ve değiştirilen dosyaların kalan bölümleri de dahil olmak üzere tüm sürücü şifrelenir. Bu seçenek, verileri değiştirilmemiş veya silinmemiş yeni sabit sürücüler için önerilir. Şifrelemeyi zaten kullanımda olan bir sabit sürücüye uyguluyorsanız tüm sabit sürücünün şifrelenmesi önerilir. Bu, tüm verilerin, hatta potansiyel olarak kurtarılabilir silinmiş verilerin bile korunmasını sağlar. Varsayılan olarak, onay kutusu temizlenmiştir.

Parametre	Açıklama
Kimlik doğrulama yöntemi	**Sadece parola (Windows 8 ve sonraki sürümler)** Bu seçenek işaretlenirse, kullanıcı şifrelenmiş bir sürücüye erişmeye çalıştığında Kaspersky Endpoint Security kullanıcıdan bir parola ister. Bu seçenek, Güvenilir Platform Modülü (TPM) kullanılmadığında seçilebilir. **Güvenilir platform modülü (TPM)** Bu seçenek işaretlenirse BitLocker, Güvenilir Platform Modülü'nü (TPM) kullanır. Bir *Trusted Platform Module (TPM)* güvenlikle ilgili temel işlevleri (örneğin şifreleme anahtarlarını saklamak için) sağlamak üzere geliştirilmiş bir mikroçiptir. Bir Güvenilir Platform Modülü genellikle bilgisayarın ana kartına yüklenmiştir ve donanım veri yolu aracılığıyla tüm diğer sistem bileşenleri ile etkileşim halindedir. Windows 7 veya Windows Server 2008 R2 çalıştıran bilgisayarlar için sadece bir TPM modülü kullanarak şifreleme kullanılabilir. Bir TPM modülü yüklü değilse, BitLocker şifrelemesi mümkün değildir. Bu bilgisayarlarda parola kullanımı desteklenmez. Güvenilir Platform Modülü ile donatılmış bir aygıt, yalnızca aygıtla şifresi çözülebilen şifreleme anahtarları oluşturabilir. Güvenilir Platform Modülü şifreleme anahtarlarını kendi kök depolama anahtarı ile şifreler. Kök depolama anahtarı, Güvenilir Platform Modülü'nde saklanır. Bu, şifreleme anahtarlarını ele geçirmek için yapılan girişimlere karşı ek bir koruma düzeyi sağlar. Bu eylem varsayılan olarak seçilmiştir. Şifreleme anahtarına erişim için ek bir koruma katmanı ayarlayabilir ve anahtarı bir parola veya PIN ile şifreleyebilirsiniz: • **TPM için PIN Kullan**. Bu onay kutusu işaretlendiğinde, kullanıcı Güvenilir Platform Modülünde (TPM) depolanan bir şifreleme anahtarına erişim sağlamak için bir PIN kodu kullanabilir. Bu onay kutusu işaretlenmezse, kullanıcıların PIN kodu kullanması yasaklanır. Şifreleme anahtarına erişmek için kullanıcının parola girmesi gerekir. • **Güvenilir platform modülü (TPM) veya TPM kullanılamıyorsa parola**. Bu seçenek tercih edilirse, Güvenilir Platform Modülü (TPM) mevcut olmadığında kullanıcı şifreleme anahtarlarına erişim elde etmek için bir parola kullanabilir. Bu onay kutusu işaretlenmemişse ve TPM kullanılabilir değilse, tam disk şifreleme başlamaz. Seçilen kimlik doğrulama yöntemi, parola veya PIN gereklilikleri belirlenerek yapılandırılmalıdır: • **Minimum PIN uzunluğu (karakter)** (varsayılan değer 6'dır). • **Minimum parola uzunluğu (karakter)** (varsayılan değer 8'dir). • **Depolanan maksimum parola/PIN sayısı** (varsayılan değer 5'tir). • **TPM için parola/PIN geçerlilik süresini sınırla (gün)** (varsayılan olarak devre dışıdır). • **Gelişmiş PIN (harfler ve rakamlar) kullan**. *Genişletilmiş PIN* sayısal karakterlere ek olarak büyük ve küçük Latin harfleri, özel karakterler ve boşluklar gibi diğer karakterlerin kullanılmasına da izin verir. Varsayılan olarak devre dışıdır.
Kurtarma anahtarını otomatik olarak yeniden oluştur (gün)	BitLocker tarafından korunan bir sürücüye erişimi geri yüklemek için parolayı otomatik olarak güncelleyin. Bu onay kutusu işaretlendiğinde, kurtarma anahtarı parolasının geçerlilik süresini belirtin. Bu, kurtarma anahtarı parolasının yeniden kullanılmasını önlemeye yardımcı olur.

BitLocker tarafından korunan bir sürücünün şifresinin çözülmesi

Kullanıcılar, bir diskin şifresini işletim sistemini kullanarak çözebilir (*BitLocker'ı Kapat* işlevi). Bundan sonra, Kaspersky Endpoint Security, kullanıcıdan diski tekrar şifrelemesini ister. Kaspersky Endpoint Security, ilkede disk şifre çözmeyi etkinleştirmediyseniz, diskin şifrelenmesini isteyecektir.

BitLocker tarafından korunan bir sürücünün şifresi Yönetim Konsolu (MMC) kullanılarak nasıl çözülür

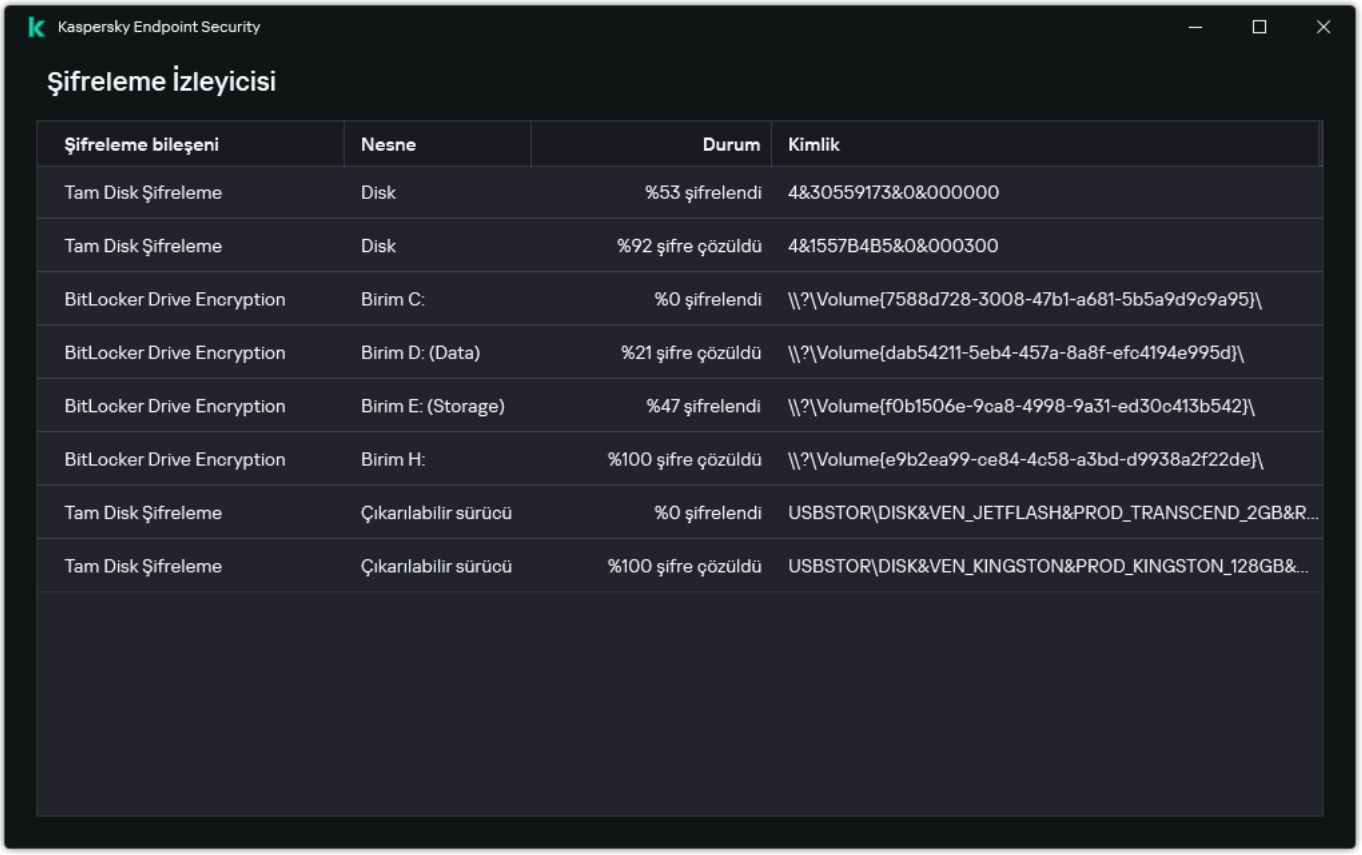
1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
4. **Şifreleme teknolojisi** açılır listesinde **BitLocker Drive Encryption** öğesini seçin.

5. **Şifreleme modu** açılır listesinden **Tüm sabit sürücülerin şifresini çöz** seçeneğini seçin.
6. Değişikliklerinizi kaydedin.

BitLocker ile şifrelenmiş bir sabit sürücünün şifresini Web Console ve Cloud Console aracılığıyla çözme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Tam Disk Şifreleme**'ye gidin.
5. **BitLocker Disk Şifrelemesi** teknolojisini seçin.
6. **Cihazlardaki eylem** bloğunda, **Tüm sabit sürücülerin şifresini çöz**'ü seçin.
7. Değişikliklerinizi kaydedin.

Bir kullanıcının bilgisayarındaki disk şifreleme veya şifre çözme işlemini kontrol etmek için Şifreleme İzleyicisi aracını kullanabilirsiniz. Şifreleme İzleyicisi aracını ana uygulama penceresinden çalıştırabilirsiniz.



Şifreleme İzleyicisi

BitLocker tarafından korunan bir sürücüye erişimi geri yükleme

Bir kullanıcının BitLocker tarafından şifrelenmiş bir sabit sürücüye erişim parolasını unutması halinde, kurtarma prosedürünü (İstek-Yanıt) başlatmanız gerekir.

Bilgisayarın işletim sisteminde Federal Bilgi İşleme standart (FIPS) uyumluluk modu etkinse, Windows 8 sonraki sürümlerde kurtarma anahtarı dosyası şifreleme öncesinde çıkarılabilir sürücüye kaydedilir. Sürücüye tekrar erişim sağlamak için çıkarılabilir sürücüyü takın ve ekrandaki talimatları izleyin.

BitLocker tarafından şifrelenmiş bir sabit sürücüye erişimi tekrar sağlamak için şu adımları uygulayın:

1. Kullanıcı, yöneticiye kurtarma anahtarı kimliğini söyler (aşağıdaki şekle bakın).
2. Yönetici, kurtarma anahtarının kimliğini, Kaspersky Security Center'ın bilgisayar özelliklerinde doğrular. Kullanıcının sunduğu kimlik ile bilgisayar özelliklerinde görüntülenen kimlik eşleşmelidir.
3. Kurtarma anahtarı kimliği eşleşirse, yönetici kullanıcıya kurtarma anahtarını sunar ya da bir kurtarma anahtarı dosyası gönderir.

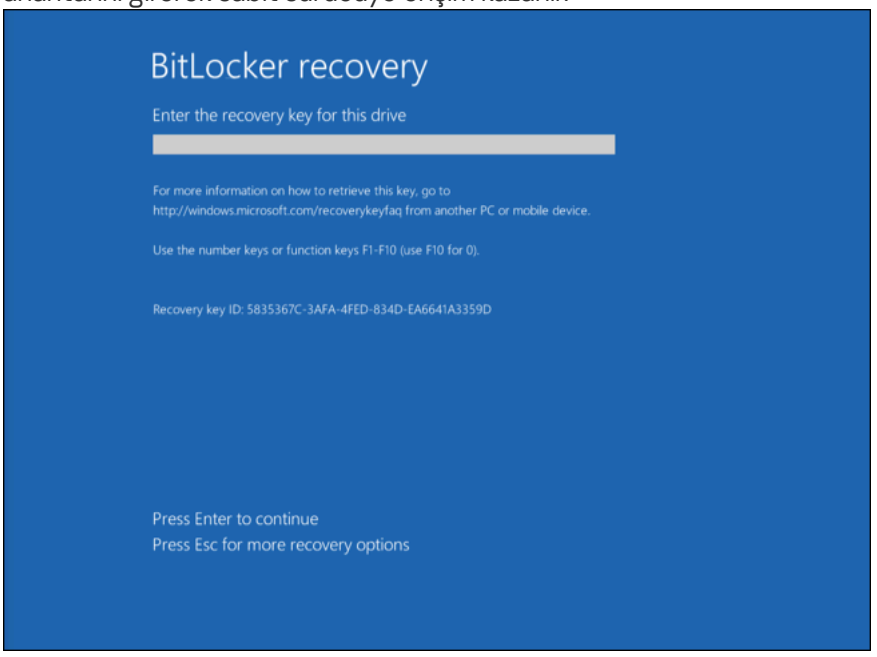
   Şu işletim sistemlerini çalıştıran bilgisayarlar için bir kurtarma anahtarı dosyası kullanılır:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   Diğer tüm işletim sistemleri için bir kurtarma anahtarı kullanılır.

   Kurtarma anahtarı parolasının yeniden kullanılmasını önlemek için, ilke ayarlarında otomatik parola güncellemesini yapılandırabilirsiniz.

4. Kullanıcılar kurtarma anahtarını girerek sabit sürücüye erişim kazanır.



BitLocker tarafından şifrelenen bir sabit sürücüye erişimi geri yükleme

Bir sistem sürücüsüne yeniden erişim

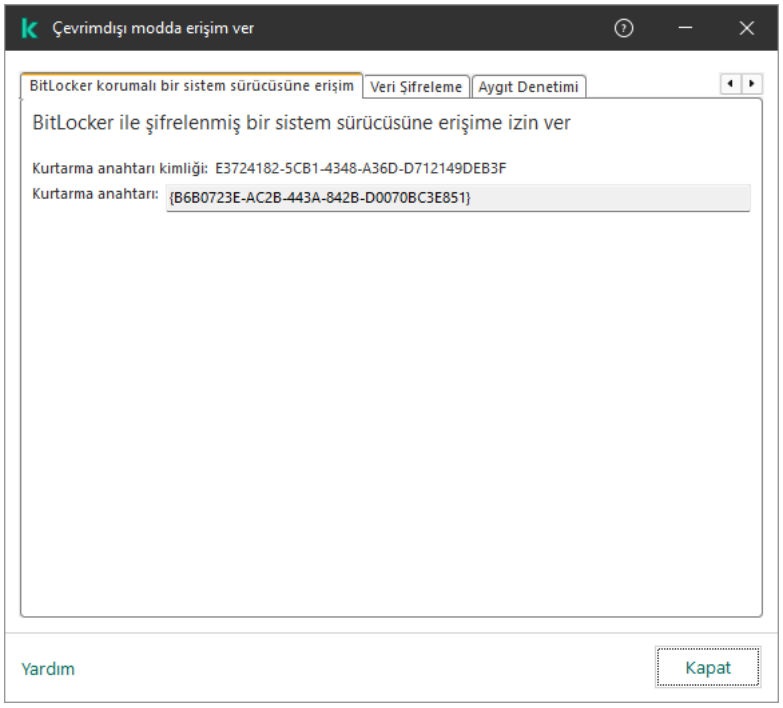
Kurtarma prosedürünü başlatmak için kullanıcının önyükleme kimlik doğrulaması aşamasında **Esc** tuşuna basması gerekir.

BitLocker tarafından şifrelenmiş bir sistem sürücüsü için kurtarma anahtarı Yönetim Konsolu'nda (MMC) nasıl görüntülenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Yönetilen cihazlar**.
3. **Cihazlar** sekmesinde, şifrelenmiş verilere erişim talep eden kullanıcının bilgisayarını seçin ve bağlam menüsünü görüntülemek için sağ tıklayın.
4. İçerik menüsünde **Çevrimdışı modda erişim ver** seçeneğini belirleyin.
5. Bu işlem bir pencere açar; bu pencerede, **BitLocker ile korunan sistem sürücüsüne erişim** sekmesini seçin.
6. 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.

Böylece kullanıcıya aktarılacak kurtarma anahtarına ya da kurtarma anahtarının dosyasına erişim kazanmış olursunuz.



BitLocker ile şifrelenen bir sürücüye erişimin geri yüklenmesi

BitLocker tarafından şifrelenmiş bir sistem sürücüsü için kurtarma anahtarı Web Console ve Cloud Consola'da nasıl görüntülenir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Sürücüsüne tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.
3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.
4. Açılan pencereden **BitLocker** bölümünü seçin.
5. Kurtarma anahtarı kimliğini doğrulayın. Kullanıcı tarafından sunulan kimlik ile bilgisayar ayarlarında görüntülenen kimlik eşleşmelidir.

   Kimlikler eşleşmezse bu anahtar belirtilen sistem sürücüsüne erişimin geri yüklenmesi için geçerli değildir. Seçilen bilgisayarın adının kullanıcı bilgisayarının adı ile eşleştiğinden emin olun.

6. **Anahtarı al**'a tıklayın.

Böylece kullanıcıya aktarılacak kurtarma anahtarına ya da kurtarma anahtarının dosyasına erişim kazanmış olursunuz.

İşletim sistemi yüklendikten sonra, Kaspersky Endpoint Security kullanıcıdan parolayı veya PIN kodunu değiştirmesini ister. Yeni bir parola veya PIN kodu belirledikten sonra, BitLocker yeni bir kurtarma anahtarı oluşturur ve anahtarı Kaspersky Security Center'a gönderir. Sonuç olarak, kurtarma anahtarı ve kurtarma anahtarı dosyası güncellenecektir. Kullanıcının parolayı değiştirmemesi halinde, işletim sisteminin bir sonraki yüklemesinde eski kurtarma anahtarını kullanabilirsiniz.

Windows 7 bilgisayarlar, parolanın veya PIN kodunun değiştirilmesine izin vermez. Kurtarma anahtarı girildikten ve işletim sistemi yüklendikten sonra, Kaspersky Endpoint Security kullanıcıdan parolayı veya PIN kodunu değiştirmesini istemez. Bu nedenle, yeni bir parola veya PIN kodu belirlemek mümkün değildir. Bu sorun, işletim sisteminden kaynaklanmaktadır. Devam etmek için sabit sürücüyü yeniden şifrelemeniz gerekir.

Sistem dışı bir sürücüye yeniden erişim

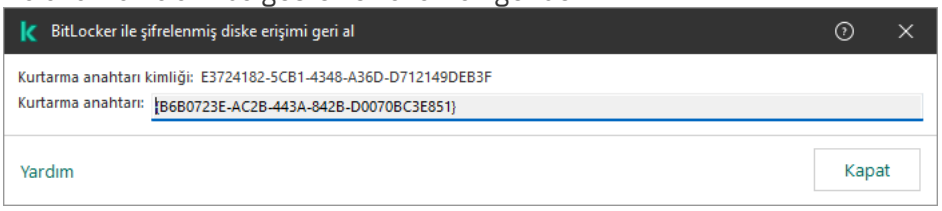
Kurtarma prosedürünü başlatmak için kullanıcının, sürücüye erişim sağlayan penceredeki **Parolanızı mı unuttunuz?** düğmesine tıklaması gerekir. Şifrelenmiş sürücüye erişim kazandıktan sonra kullanıcı, BitLocker ayarlarından, Windows kimliklik doğrulaması sırasında sürücünün kilidinin otomatik olarak kaldırılmasını etkinleştirebilir.

BitLocker tarafından şifrelenmiş bir sistem dışı sürücü için kurtarma anahtarı Yönetim Konsolu'nda (MMC) nasıl görüntülenir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Gelişmiş → Veri şifreleme ve koruma → Şifrelenmiş sürücüler** klasörünü seçin.
3. Çalışma alanında, bir erişim anahtarı dosyası oluşturmak istediğiniz şifrelenmiş aygıtı seçin, ardından aygıtın içerik menüsünden **Kaspersky Endpoint Security'da aygıta erişim al**'a tıklayın.
4. 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.

5. Kullanıcıya **Kurtarma anahtarı** alanında gösterilen anahtarı gönderin.



BitLocker ile şifrelenen bir sürücüye erişimin geri yüklenmesi

BitLocker tarafından şifrelenmiş bir sistem sürücüsü için kurtarma anahtarı Web Console ve Cloud Console'da nasıl görüntülenir

1. Web Console'un ana penceresinden **İşlemler → Veri şifreleme ve koruma → Şifrelenmiş sürücüler**'ı seçin.
2. Sürücüsüne tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.

3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.

   Bu, bir aygıta erişim verecek Sihirbazı başlatılır.

4. Bir aygıta erişim kazanmak için Sihirbazın talimatlarını uygulayın:

   a. **Kaspersky Endpoint Security for Windows** eklentisini seçin.

   b. Kurtarma anahtarı kimliğini doğrulayın. Kullanıcı tarafından sunulan kimlik ile bilgisayar ayarlarında görüntülenen kimlik eşleşmelidir.

   > Kimlikler eşleşmezse bu anahtar belirtilen sistem sürücüsüne erişimin geri yüklenmesi için geçerli değildir. Seçilen bilgisayarın adının kullanıcı bilgisayarının adı ile eşleştiğinden emin olun.

   c. **Anahtarı al**'a tıklayın.

Böylece kullanıcıya aktarılacak kurtarma anahtarına ya da kurtarma anahtarının dosyasına erişim kazanmış olursunuz.

Yazılımı güncellemek için BitLocker korumasını duraklatma

İşletim sistemini güncellemek, işletim sistemi için güncelleme paketleri yüklemek veya BitLocker koruması açıkken diğer yazılımları güncellemek için bir dizi özel husus vardır. Güncellemeler yüklenirken bilgisayarın birden fazla kez yeniden başlatılması gerekebilir. Her yeniden başlatmanın ardından kullanıcının BitLocker kimlik doğrulamasını tamamlaması gerekir. Güncellemelerin doğru yüklendiğinden emin olmak için BitLocker kimlik doğrulamasını geçici olarak kapatabilirsiniz. Bu durumda disk şifrelenmiş kalır ve kullanıcı sistemde oturum açtıktan sonra verilere erişebilir. BitLocker kimlik doğrulamasını yönetmek için *BitLocker Koruma Yönetimi* görevini kullanabilirsiniz. BitLocker kimlik doğrulaması gerektirmeyen bilgisayarlar için yeniden başlatma sayısını belirtmek için bu görevi kullanabilirsiniz. Bu şekilde, güncellemeler yüklendikten ve *BitLocker Koruma Yönetimi* görevi tamamlandıktan sonra BitLocker kimlik doğrulaması otomatik olarak etkinleştirilir. BitLocker kimlik doğrulamasını istediğiniz zaman etkinleştirebilirsiniz.

Yönetim Konsolu (MMC) kullanılarak BitLocker koruması nasıl duraklatılır

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (14.2) → **BitLocker Koruma Yönetimi** seçimini yapın.

2. Adım. BitLocker Koruma Yönetimi

BitLocker kimlik doğrulamasını yapılandırın. BitLocker korumasını duraklatmak için **BitLocker kimlik doğrulamasının atlanmasına geçici olarak izin ver** seçimini yapın ve BitLocker kimlik doğrulaması olmadan yeniden başlatma sayısını girin (1 ila 15 kez). Gerekirse, görev için bir sona erme tarihi ve saati girin. Belirtilen zamanda görev otomatik olarak kapatılır ve bilgisayar yeniden başlatıldığında kullanıcının BitLocker kimlik doğrulamasını tamamlaması gerekir.

3. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

4. Adım. Görev adını tanımlama

Görevin adını girin, örneğin *Windows 10'a yükseltme*.

5. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

Web Console kullanılarak BitLocker koruması nasıl duraklatılır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Genel görev ayarlarını yapılandırma

Genel görev ayarlarını yapılandırın:

1. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
2. **Görev türü** açılır listesinden **BitLocker Koruma Yönetimi** seçimini yapın.
3. **Görev adı** alanına, *Windows 10'a yükseltme* gibi bir kısa açıklama girin.
4. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

2. Adım. BitLocker Koruma Yönetimi

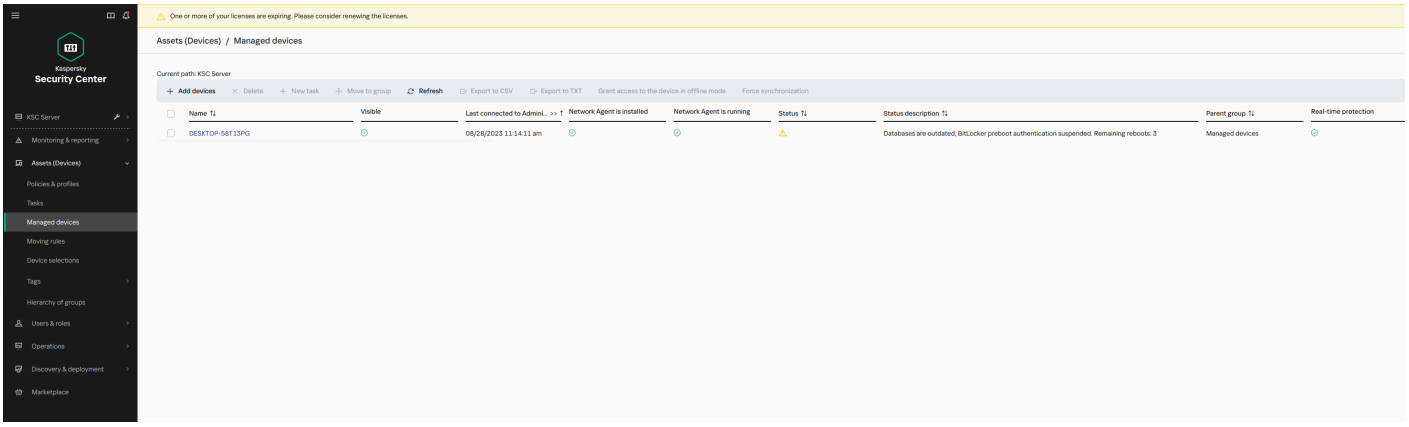
BitLocker kimlik doğrulamasını yapılandırın. BitLocker korumasını duraklatmak için **BitLocker kimlik doğrulamasının atlanmasına geçici olarak izin ver** seçimini yapın ve BitLocker kimlik doğrulaması olmadan yeniden başlatma sayısını girin (1 ila 15 kez). Gerekirse, görev için bir sona erme tarihi ve saati girin. Belirtilen zamanda görev otomatik olarak kapatılır ve bilgisayar yeniden başlatıldığında kullanıcının BitLocker kimlik doğrulamasını tamamlaması gerekir.

3. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Görevler listesinde yeni bir görev görüntülenir.

Bir görevi çalıştırmak için göreve ilişkin onay kutusunu seçin ve **Başlat** düğmesine tıklayın.

Sonuç olarak, görev çalışırken, bilgisayarın bir sonraki yeniden başlatılmasından sonra BitLocker kullanıcıdan kimlik doğrulaması istemez. Bilgisayarın BitLocker kimlik doğrulaması olmadan her yeniden başlatılmasından sonra, Kaspersky Endpoint Security karşılık gelen bir olay oluşturur ve kalan yeniden başlatma sayısını kaydeder. Kaspersky Endpoint Security daha sonra olayı yönetici tarafından izlenmek üzere Kaspersky Security Center'a gönderir. Kalan yeniden başlatma sayısını Kaspersky Security Center konsolunun **Yönetilen cihazlar** klasöründeki cihaz durumu açıklamasında da görüntüleyebilirsiniz.



Yönetilen cihazların listesi

Belirtilen yeniden başlatma sayısına veya görevin sona erme tarihine ulaşıldığında, BitLocker kimlik doğrulaması otomatik olarak açılır. Verilere erişmek için kullanıcının BitLocker kimlik doğrulamasını tamamlaması gerekir.

Windows 7 çalıştıran bilgisayarlarda, BitLocker bilgisayar yeniden başlatmalarını sayamaz. Windows 7 bilgisayarlarda, yeniden başlatmaları sayma işlemi Kaspersky Endpoint Security tarafından gerçekleştirilir. Bu nedenle, her yeniden başlatma sonrasında BitLocker kimlik doğrulamasını otomatik olarak açmak için Kaspersky Endpoint Security başlatılmalıdır.

BitLocker kimlik doğrulamasını önceden açmak için *BitLocker Koruma Yönetimi* görev özellikleri açın ve **Önyükleme öncesinde her seferinde kimlik doğrulama iste** seçimini yapın.

Yerel bilgisayar sürücülerinde Dosya Düzeyinde Şifreleme

Arm tabanlı bilgisayarlarda dosya şifreleme özelliği desteklenmemektedir.

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

Dosya şifreleme şu özel özelliklere sahiptir:

- 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 veya yeniden yönlendirilen klasörlerin önceden tanımlanmış klasörlerindeki dosyaları şifrelemez veya şifresini çözmez.
- Kaspersky Endpoint Security, değiştirilmesi işletim sistemine ve yüklü uygulamalara zarar verebilecek dosyaları şifrelemez. Örneğin içe içe geçmiş klasörlerin olduğu aşağıdaki dosya ve klasörler şifrelemeden istisnalar listesindedir:
  - %WINDIR%;
  - %PROGRAMFILES% ve %PROGRAMFILES(X86)%;
  - Windows kayıt defteri dosyaları.

  Şifreleme istisnaları listesi görüntülenemez veya düzenlenemez. Şifreleme istisnaları listesindeki dosyalar ve klasörler şifreleme listesine eklenebilir ancak dosya şifreleme sırasında şifrelenmez.

Yerel bilgisayar sürücülerindeki dosyaları şifreleme

Kaspersky Endpoint Security, OneDrive bulut depolama alanında veya adları OneDrive olan diğer klasörlerde bulunan dosyaları şifrelemez. Kaspersky Endpoint Security, şifrelenmiş dosyalar şifre çözme kuralına eklenmemişse, bu dosyaların OneDrive klasörlerine eklenmesini de engeller.

Yerel sürücülerdeki dosyaları şifrelemek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme → Dosya Düzeyinde Şifreleme** seçimini yapın.
4. **Şifreleme modu** açılır listesinden **Kurallara göre** seçimini yapın.
5. **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.
      - **Belgeler**. İşletim sisteminin standart *Belgeler* klasörü ve onun alt klasörleri.
      - **Sık Kullanılanlar**. İşletim sisteminin standart *Sık Kullanılanlar* klasörü ve onun alt klasörleri.
      - **Masaüstü**. İşletim sisteminin standart *Masaüstü* klasörü ve onun alt klasörleri.
      - **Geçici dosyalar**. Bilgisayara yüklenmiş uygulamaların çalışmasıyla ilgili geçici dosyalar. Örneğin Microsoft Office uygulamaları, belgelerin yedek kopyalarını içeren geçici dosyalar oluşturur.

        Veri kaybına neden olabileceğinden, geçici dosyaları şifrelemeniz önerilmez. Örneğin, Microsoft Word, bir belgeyi işlerken geçici dosyalar oluşturur. Geçici dosyalar şifrelenmiş ancak orijinal dosya şifrelenmemişse, kullanıcı belgeyi kaydetmeye çalıştığında *Erişim Reddedildi* hatası alabilir. Microsoft Word dosyayı ayrıca kaydedebilir, ancak bir dahaki sefere belgeyi açmak mümkün olmayacaktır, yani veriler kaybolacaktır.

      - **Outlook dosyaları**. Outlook posta istemcisinin çalışmasıyla ilgili dosyalar: veri dosyaları (PST), çevrimdışı veri dosyaları (OST), çevrimdışı adres defteri dosyaları (OAB) ve kişisel adres defteri dosyaları (PAB).

   b. Şifreleme kuralının manuel olarak girilen klasör yolunu eklemek için **Özel klasör** öğesini seçin.

      Bir klasör yolu yazarken şu kurallara uyun:

      - Bir ortam değişkeni kullanın (örneğin `%FOLDER%\UserFolder\`). Bir ortam değişkenini sadece bir kez ve yolun başında kullanabilirsiniz.
      - Göreli yollar kullanmayın.
      - `*` ve `?` karakterlerini kullanmayın.
      - UNC yollarını kullanmayın.
      - Ayırıcı karakter olarak `;` veya `,` kullanın.

c. Bir şifreleme kuralına tek tek dosya uzantıları eklemek için **Uzantıya göre dosyalar** öğesini seçin. Kaspersky Endpoint Security bilgisayarın tüm yerel sürücülerindeki belirtilen uzantılara sahip dosyaları şifreler.

d. Bir şifreleme kuralına dosya uzantıları grubunu eklemek için **Uzantı gruplarına göre dosyalar** öğesini seçin (örneğin *Microsoft Office belgeleri*). Kaspersky Endpoint Security, bilgisayarın tüm yerel sürücülerindeki uzantı gruplarında belirtilen uzantılara sahip dosyaları şifreler.

6. Değişikliklerinizi kaydedin.

İlke uygulanır uygulanmaz Kaspersky Endpoint Security, şifreleme kuralında yer alan ve şifre çözme kuralında yer almayan dosyaları şifreler.

Dosya şifreleme şu özel özelliklere sahiptir:

- Aynı dosya hem şifreleme kuralı hem de şifre çözme kuralı olarak eklenirse Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:
  - Dosya şifrelenmemişse, Kaspersky Endpoint Security bu dosyayı şifrelemez.
  - Dosya şifrelenmişse, Kaspersky Endpoint Security bu dosyanın şifresini çözer.
- Yeni dosyalar şifreleme kuralını sağlıyorsa Kaspersky Endpoint Security bunları şifrelemeye devam eder. Örneğin şifrelenmemiş bir dosya, siz özelliklerini (yolunu veya uzantısını) değiştirdiğinizde dosya şifreleme kuralının kriterini karşılayabilir. Kaspersky Endpoint Security bu dosyayı şifreler.
- Kullanıcı tarafından özellikleri şifreleme kuralı kriterlerini karşılayan yeni bir dosya oluşturulduğunda Kaspersky Endpoint Security, açılır açılmaz dosyayı şifreler.
- Kaspersky Endpoint Security, kapatılana kadar açık dosyaların şifrelemesini erteler.
- Şifrelenmiş bir dosyayı yerel sürücüdeki başka bir klasöre taşırsanız bu klasörün şifreleme kuralında yer alıp almadığına bakılmaksızın dosya şifreli olarak kalır.
- Bir dosyanın şifresini çözer ve şifreleme kuralında yer almayan başka bir yerel klasöre kopyalarsanız, dosyanın kopyası şifrelenebilir. Kopyalanan dosyanın şifrelenmesini engellemek isterseniz hedef klasör için bir şifreleme kuralı oluşturun.

Uygulamalar için şifreli dosyaya erişim kuralları oluşturma

Varsayılan olarak, tüm uygulamalar şifrelenmiş dosyalarla şifresi çözülmüş durumda çalışır. Belirli uygulamaları sık kullanıyorsanız (örneğin, tarayıcılar veya metin düzenleyiciler), bilgileri korumak için şifreli dosya erişim kuralları oluşturabilirsiniz.

Microsoft Internet Explorer ve Microsoft Edge tarayıcıları için bir şifrelenmiş dosya erişim kuralı oluşturmanızı öneririz. Bu tarayıcıların çalışma şekli nedeniyle, bir web sitesine (örneğin bulut depolama) şifrelenmiş bir dosya yüklerseniz, dosyanın şifresi otomatik olarak çözülür. Bu bir veri sızıntısına neden olabilir. Bu tarayıcıları kullanarak şifrelenmiş bir dosya yüklemek mümkün değildir. **Sadece şifrelenmiş metne sahip şifrelenmiş dosyalara erişim ver** kuralını ayarlamanızı öneririz. Diğer tarayıcılar (Google Chrome gibi) için bir kural oluşturmanıza gerek yoktur.

Uygulamalar için şifrelenmiş dosyaya erişim kuralları oluşturmak amacıyla:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme** seçimini yapın.
4. **Şifreleme modu** açılır listesinden **Kurallara göre** seçimini yapın.

   Erişim kuralları sadece **Kurallara göre** modundayken uygulanır. **Kurallara göre** modunda erişim kurallarını uyguladıktan sonra **Değiştirmeden bırak** moduna geçerseniz Kaspersky Endpoint Security tüm erişim kurallarını yoksayar. Tüm uygulamaların tüm şifrelenmiş dosyalara erişimi olacaktır.

5. Pencerenin sağ kısmında, **Uygulamalar için kurallar** sekmesini seçin.
6. Uygulamaları sadece Kaspersky Security Center listesinden seçmek isterseniz, **Ekle** düğmesine tıklayın ve açılır listeden **Kaspersky Security Center listesinden uygulamalar** öğesini seçin.
   a. Tablodaki uygulamalar listesini daraltmak için filtreler belirtin. Bunu yapmak için **Uygulama**, **Satıcı** ve **Eklendiği dönem** parametrelerinin tüm değerlerini belirtin ve **Grup** bloğundaki tüm onay kutularını işaretleyin.
   b. **Yenile**'ye tıklayın.
   c. Tabloda, uygulanan filtrelerle eşleşen uygulamalar listelenir.
   d. **Uygulama** sütununda, şifrelenmiş dosya erişim kurallarını oluşturmak istediğiniz uygulamaların karşısındaki onay kutularını işaretleyin.
   e. **Uygulamalar için kural** açılır listesinde, uygulamaların şifrelenmiş dosyalara erişimini belirleyecek olan kuralı seçin.
   f. **Daha önce seçilen uygulamalar için işlemler** açılır listesinden, bu uygulamalar için daha önceden oluşturulan şifrelenmiş dosya erişim kurallarına Kaspersky Endpoint Security tarafından uygulanacak eylemi seçin.

   Uygulamalar için şifrelenen dosya erişim kuralının ayrıntıları, **Uygulamalar için kurallar** sekmesindeki tabloda görülür.
7. Uygulamaları manuel olarak seçmek isterseniz **Ekle** düğmesine tıklayın ve açılır listeden **Özel uygulamalar** öğesini seçin.
   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, uygulamaların şifrelenmiş dosyalara erişimini belirleyecek olan kuralı seçin.

   Uygulamalar için şifrelenen dosya erişim kuralının ayrıntıları, **Uygulamalar için kurallar** sekmesindeki tabloda görülür.
8. Değişikliklerinizi kaydedin.

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 şifrelemesini yapılandırmak için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme** seçimini yapın.
4. **Şifreleme modu** açılır listesinden **Kurallara göre** seçimini yapın.

   Şifreleme kuralları yalnızca **Kurallara göre** modundayken uygulanır. **Kurallara göre** modunda şifreleme kurallarını uyguladıktan sonra **Değiştirmeden bırak** moduna geçerseniz Kaspersky Endpoint Security tüm şifreleme kurallarını yoksayar. Önceden şifrelenmiş dosyalar şifrelenmiş olarak kalır.

5. Pencerenin sağ kısmında, **Uygulamalar için kurallar** sekmesini seçin.
6. Uygulamaları sadece Kaspersky Security Center listesinden seçmek isterseniz, **Ekle** düğmesine tıklayın ve açılır listeden **Kaspersky Security Center listesinden uygulamalar** öğesini seçin.

   a. Tablodaki uygulamalar listesini daraltmak için filtreler belirtin. Bunu yapmak için **Uygulama**, **Satıcı** ve **Eklendiği dönem** parametrelerinin tüm değerlerini belirtin ve **Grup** bloğundaki tüm onay kutularını işaretleyin.

   b. **Yenile**'ye tıklayın.

      Tabloda, uygulanan filtrelerle eşleşen uygulamalar listelenir.

   c. **Uygulama** sütununda, şifrelemek istediğiniz dosyaları oluşturan uygulamaların yanındaki onay kutularını seçin.

   d. **Uygulamalar için kural** açılır listesinde, **Oluşturulan tüm dosyaları şifrele** seçeneğini belirleyin.

   e. **Daha önce seçilen uygulamalar için işlemler** açılır listesinden, bu uygulamalar için daha önceden oluşturulan dosya şifreleme kurallarına Kaspersky Endpoint Security tarafından uygulanacak eylemi seçin.

Seçilen uygulamalar tarafından oluşturulan veya değiştirilen dosyalar için şifreleme kuralı hakkında bilgi, **Uygulamalar için kurallar** sekmesindeki tabloda görüntülenir.

7. Uygulamaları manuel olarak seçmek isterseniz **Ekle** düğmesine tıklayın ve açılır listeden **Özel uygulamalar** öğesini seçin.

   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, **Oluşturulan tüm dosyaları şifrele** seçeneğini belirleyin.

   Seçilen uygulamalar tarafından oluşturulan veya değiştirilen dosyalar için şifreleme kuralı hakkında bilgi, **Uygulamalar için kurallar** sekmesindeki tabloda görüntülenir.

8. Değişikliklerinizi kaydedin.

Şifre çözme kuralı oluşturma

Bir şifre çözme kuralı oluşturmak için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme → Dosya Düzeyinde Şifreleme** seçimini yapın.
4. **Şifreleme modu** açılır listesinden **Kurallara göre** seçimini yapın.
5. **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.

   b. Şifre çözme kuralının manuel olarak girilen klasör yolunu eklemek için **Özel klasör** öğesini seçin.

   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.

   d. Bir şifre çözme kuralına dosya uzantıları grubunu eklemek için **Uzantı gruplarına göre dosyalar** öğesini seçin (örneğin *Microsoft Office belgeleri*). Kaspersky Endpoint Security, bilgisayarın tüm yerel sürücülerindeki uzantı gruplarında belirtilen uzantılara sahip dosyaları şifrelemez.

6. Değişikliklerinizi kaydedin.

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 Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme** seçimini yapın.
4. Pencerenin sağ kısmında, **Şifreleme** sekmesini seçin.
5. Şifresini çözmek istediğiniz dosya ve klasörleri şifreleme listesinden kaldırın. Bunun için dosyaları seçin ve **Sil** düğmesinin bağlam menüsündeki **Kuralı silin ve dosyaların şifresini çözün** öğesini seçin.

   Şifreleme listesinden kaldırılan dosya ve klasörler otomatik olarak şifre çözme listesine eklenir.
6. Dosya şifre çözme listesi oluşturma.
7. Değişikliklerinizi kaydedin.

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

Kurumsal ağ dışındaki kullanıcılara dosyalar gönderirken verilerinizi korumak için şifrelenmiş paketler kullanabilirsiniz. Şifrelenmiş paketler, e-posta istemcileri doysa boyutu kısıtlamalarına sahip olduğundan, çıkarılabilir sürücülerdeki büyük dosyaların gönderilmesinde kullanışlı olabilir.

Şifrelenmiş paketler oluşturmadan önce, Kaspersky Endpoint Security kullanıcıdan bir parola isteyecektir. Verileri güvenli bir şekilde korumak için parola güvenliği denetimini etkinleştirebilir ve parola güvenliği gerekliliklerini belirleyebilirsiniz. Böylece kullanıcıların `1234` gibi basit ve kısa parolalar oluşturması engellenir.

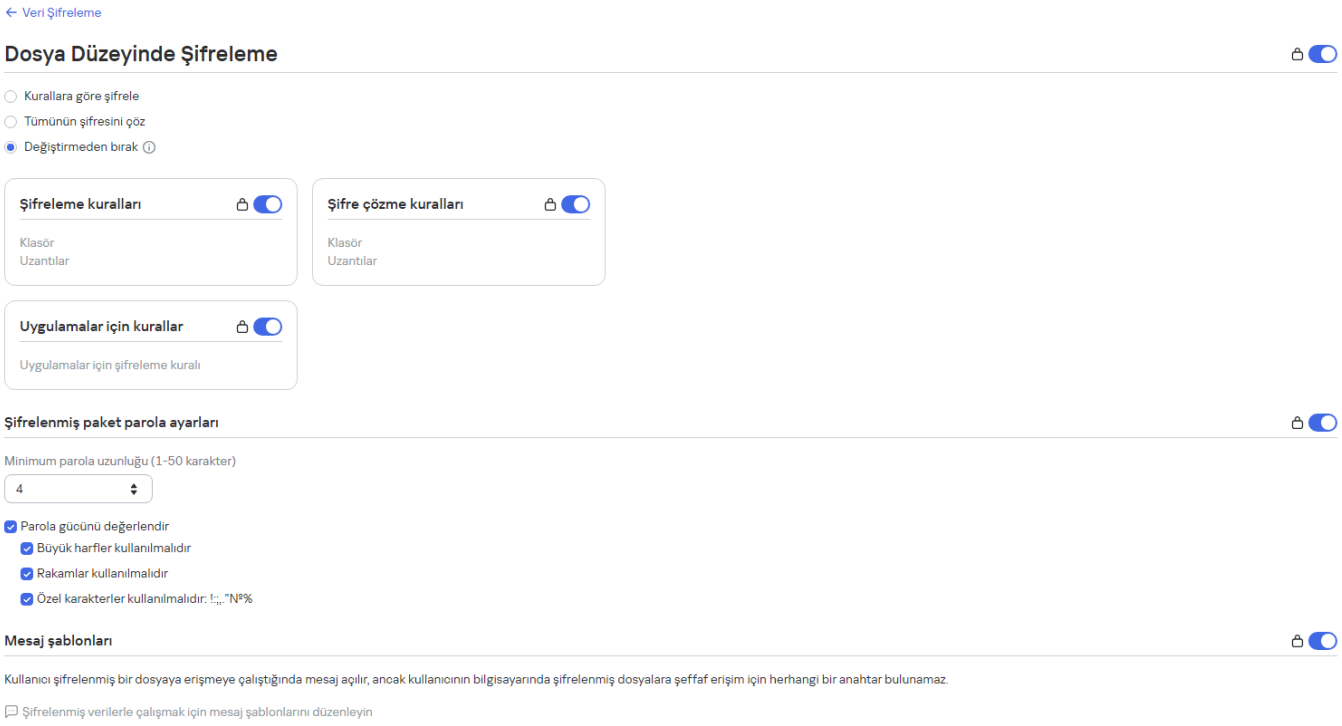
Yönetim Konsolu'nda (MMC) şifrelenmiş arşivler oluştururken parola güvenliği denetimi nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Ortak şifreleme ayarları** seçimini yapın.
4. **Parola ayarları** bloğunda **Ayarlar** düğmesine tıklayın.
5. Bu işlem bir pencere açar; bu pencerede **Şifrelenmiş paketler** sekmesini seçin.
6. Şifrelenmiş paketleri oluştururken parola karmaşıklığı ayarlarını yapılandırın.

Web Console'da yeni bir şifrelenmiş paket oluştururken parola güvenliği denetimi nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme**'ye gidin.
5. **Şifrelenmiş paket parola ayarları** bloğunda, şifrelenmiş paketler oluştururken gerekli olan parola gücü ölçütlerini yapılandırın.



Dosya Şifreleme ayarları

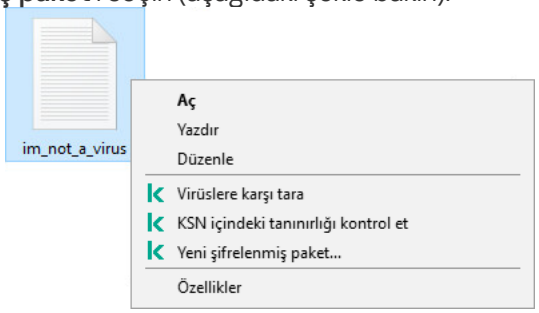
Dosya Düzeyinde Şifrelemenin kullanılabildiği Kaspersky Endpoint Security yüklü bilgisayarlarda şifrelenmiş paketler oluşturabilirsiniz.

İçeriği OneDrive bulut depolama ortamında bulunan şifrelenmiş pakete bir dosya eklerken Kaspersky Endpoint Security, dosyanın içeriğini indirip şifreleme yapar.

Şifrelenmiş bir paket oluşturmak için:

1. Herhangi bir dosya yöneticisinden, şifrelenmiş paketi eklemek istediğiniz dosyaları veya klasörleri seçin. İçerik menüsünü açmak için sağ tıklayın.

2. İçerik menüsünde, **Yeni şifrelenmiş paket**'i seçin (aşağıdaki şekle bakın).



Şifrelenmiş bir paket oluşturma

3. Açılan pencerede parolayı belirleyin ve onaylayın.

   Parola, ilkede belirtilmiş olan karmaşıklık kriterlerini karşılamalıdır.

4. **Oluştur**'a tıklayın.

Şifrelenmiş paket oluşturma işlemi başlar. Kaspersky Endpoint Security, şifrelenmiş bir paket oluşturduğunda dosyaları sıkıştırmaz. İşlem tamamlandığında, seçilen hedef klasörde kendini açabilen parola korumalı bir arşiv (.exe uzantısına sahip bir yürütülebilir dosya –) oluşturulur.

Şifrelenmiş bir paketteki dosyalara erişmek için çift tıklayarak Paket Açma Sihirbazını başlatın ve ardından parolayı girin. Parolanızı unutur ya da kaybederseniz parolayı kurtarmak ve şifrelenmiş paketteki dosyalara erişmek mümkün olmaz. Şifrelenmiş paketi tekrar oluşturabilirsiniz.

Şifrelenmiş dosyalara yeniden erişim sağlama

Dosyalar şifrelendiğinde, Kaspersky Endpoint Security şifrelenmiş dosyalara doğrudan erişim için gerekli bir şifreleme 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.

Şifrelenmiş 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 şifrelenmiş görünür.

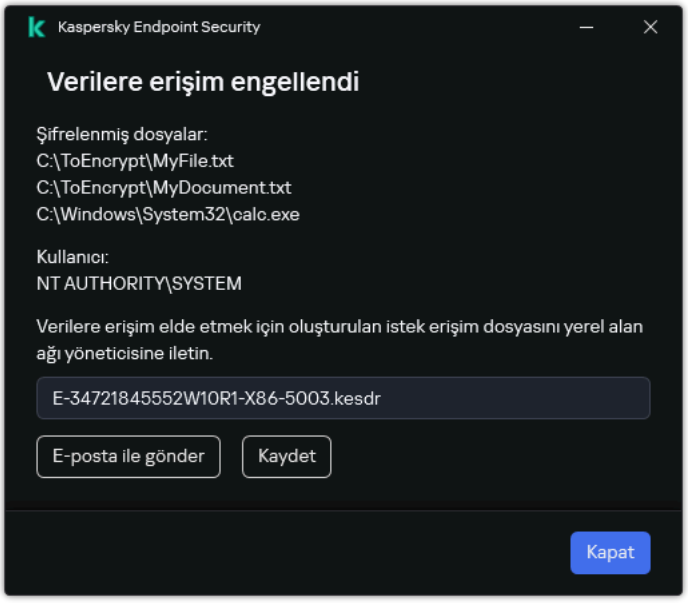
Kullanıcı, şifrelenmiş dosyalarla aşağıdaki durumlarda çalışabilir:

- Dosyalar Kaspersky Endpoint Security yüklü bir bilgisayarda oluşturulmuş şifrelenmiş paketlerin içindedir.
- Dosyalar taşınabilir moda izin verilmiş çıkarılabilir sürücülerde saklanmaktadır.

Şifrelenmiş dosyalara erişim sağlamak için kullanıcının kurtarma prosedürünü (İstek-Yanıt).

Şifrelenmiş dosyalara erişimi yeniden sağlamak için aşağıdaki adımlar uygulanmalıdır:

1. Kullanıcı yöneticiye bir istek erişim dosyası gönderir (aşağıdaki resme bakın).
2. Yönetici istek erişim dosyasını Kaspersky Security Center'a ekler, bir istek erişim dosyası oluşturur ve bu dosyayı kullanıcıya gönderir.
3. Kullanıcı erişim anahtarını Kaspersky Endpoint Security'ye ekler ve dosyalara erişim kazanır.



Şifrelenmiş dosyalara yeniden erişim sağlama

Kurtarma prosedürünü başlatmak için kullanıcının bir dosyaya erişim girişiminde bulunması gerekir. Sonuç olarak, Kaspersky Endpoint Security bir istek erişim dosyası oluşturur (KESDC uzantılı bir dosya) ve kullanıcının bu dosyayı yöneticiye göndermesi gerekir, örneğin e-posta ile.

Kaspersky Endpoint Security, bilgisayarın sürücüsünde (yerel veya çıkarılabilir sürücü) saklanan tüm şifrelenmiş dosyalara erişim için bir istek erişim dosyası oluşturur.

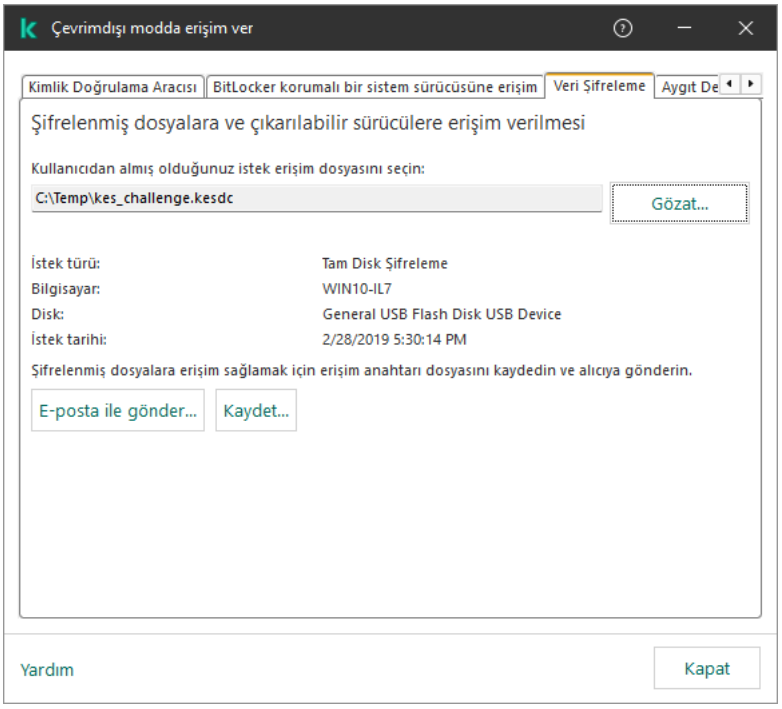
Yönetim Konsolu'nda (MMC) şifrelenmiş verilere erişim anahtarı dosyası nasıl elde edilir

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Cihazlar**.
3. **Cihazlar** sekmesinde, şifrelenmiş verilere erişim talep eden kullanıcının bilgisayarını seçin ve bağlam menüsünü görüntülemek için sağ tıklayın.
4. İçerik menüsünde **Çevrimdışı modda erişim ver** seçeneğini belirleyin.
5. Bu işlem bir pencere açar; bu pencerede **Veri Şifreleme** sekmesini seçin.

6. **Veri Şifreleme** sekmesinde, **Gözat** düğmesine tıklayın.

7. İstek erişim dosyası seçme penceresinde, kullanıcıdan alınan dosyanın yolunu belirdin.

Kullanıcının isteğiyle ilgili bilgiler görüntülenir. Kaspersky Security Center bir anahtar dosyası oluşturur. Oluşturulan şifrelenmiş dosya erişim anahtar dosyasını kullanıcıya e-posta ile gönderin. Yahut erişim dosyasını kaydedin ve transfer içi mevcut yöntemlerden birini kullanın.



Çevrimdışı modda erişim ver

Web Console'da bir şifrelenmiş verilere erişim anahtarı dosyası nasıl alınır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.

2. Verilerine tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.

3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.

4. **Veri Şifreleme**'yi seçin.

5. **Dosya seç** düğmesine tıklayın ve kullanıcıdan aldığınız istek erişim dosyasını (KESDC uzantılı bir dosya) seçin.

   Web Console, istekle ilgili bilgileri görüntüler. Bu bilgiler arasında kullanıcının dosyaya erişim isteği yaptığı bilgisayarın adı da yer alır.

6. **Anahtarı kaydet** düğmesine tıklayın ve şifrelenmiş veri erişim anahtarı dosyasının (KESDR uzantılı bir dosya) kaydedileceği bir klasör seçin.

Sonuç olarak, kullanıcıya aktarmanız gereken şifrelenmiş verilere erişim anahtarını alırsınız.

Şifrelenmiş verilere erişim anahtarı dosyası alındıktan sonra, kullanıcı dosyanın üzerine çift tıklayarak dosyayı çalıştırmalıdır. Sonuç olarak, Kaspersky Endpoint Security sürücüde saklanan tüm şifrelenmiş dosyalara erişim verir. Diğer sürücülerde saklanan şifrelenmiş dosyalara erişmek istiyorsanız her bir sürücü için ayrı bir erişim anahtarı dosyası almanız gerekir.

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. Veriler şifrelenirken bilgisayarı denetleyen Kaspersky Security Center Yönetim Sunucusu ve bilgisayar arasında bir bağlantı kurun.

Şifrelenmiş verilere erişim, işletim sistemi hatasından önce uygulanan aynı koşullarda sağlanır.

Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenleme

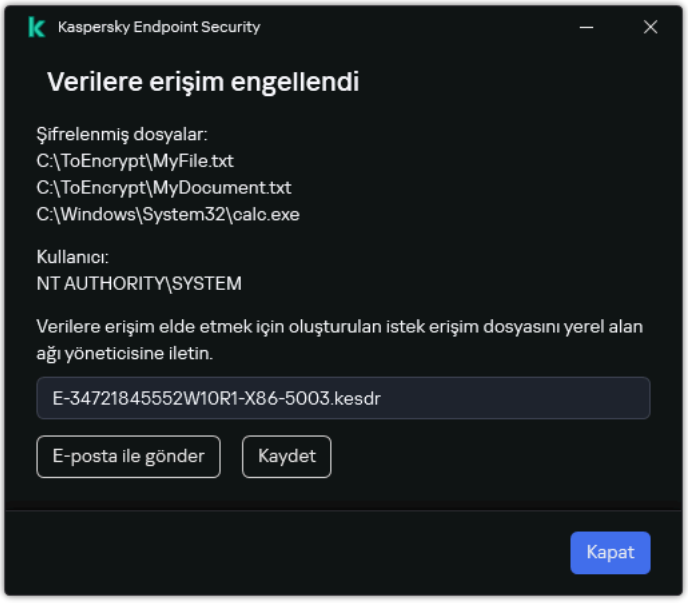
Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenlemek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Ortak şifreleme ayarları** seçimini yapın.
4. **Şablonlar** bloğunda, **Şablonlar** düğmesine tıklayın.
5. Açılan pencerede şunları yapın:
   - Kullanıcı mesajı şablonunu düzenlemek isterseniz **Kullanıcı mesajı** sekmesini seçin. Şifreli dosyalara erişim için bilgisayarda anahtar bulunmadığında şifreli bir dosyaya kullanıcı erişim sağlamaya çalıştığında aşağıdaki pencere açılır. **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. Şifrelenmiş dosyalara erişim izni verildikten sonra kullanıcı bu mesajı alır.
6. Mesaj şablonlarını düzenleyin.

   Şablon metnine bir değişken eklemek için, imleci istediğiniz konuma getirin, **Değişken**'e tıklayın ve mevcut seçenekler listesinden gerekli değişkeni seçin.

   Varsayılan olarak düğmesini kullanarak varsayılan şablon metnini geri yükleyebilirsiniz.

7. Değişikliklerinizi kaydedin.



Şifrelenmiş dosyalara yeniden erişim sağlama

Çıkarılabilir sürücüleri şifreleme

Arm tabanlı bilgisayarlarda çıkarılabilir sürücülerin şifrelenmesi desteklenmemektedir.

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

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.

Çıkarılabilir sürücülerdeki verileri korumak için şu şifreleme türlerini kullanabilirsiniz:

- Full Disk Encryption (FDE).

  Dosya sistemi de dahil olmak üzere çıkarılabilir sürücünün tamamının şifrelenmesidir.

  Kurumsal ağın dışındaki şifrelenmiş verilere erişim mümkün değildir. Bundan başka, eğer bilgisayar Kaspersky Security Center'a bağlı değilse (örneğin bir konuk bilgisayarda) kurumsal ağ içindeki verilere erişmek mümkün olmaz.

- File Level Encryption (FLE).

  Sadece bir çıkarılabilir bir sürücüdeki dosyaların şifrelenmesidir. Dosya sistemi değişmez.

Çıkarılabilir sürücülerdeki dosyaların şifrelenmesi, *taşınabilir mod* adlı özel bir mod kullanılarak kurumsal ağın dışındaki verilere erişim imkanı sağlar.

Şifreleme sırasında Kaspersky Endpoint Security bir ana anahtar oluşturur. Kaspersky Endpoint Security ana anahtarı şu veri havuzlarına kaydeder:

- Kaspersky Security Center.
- Kullanıcının bilgisayarı.

  Ana anahtar, kullanıcının gizli anahtarı kullanılarak şifrelenir.
- Çıkarılabilir sürücü.

  Ana anahtar, Kaspersky Security Center'ın genel anahtarı ile şifrelenir.

Şifreleme tamamlandıktan sonra, kurumsal ağ içinde çıkarılabilir sürücü üzerinde verilere, sanki şifrelenmemiş normal bir çıkarılabilir sürücü üzerindeymiş gibi erişilebilir.

Şifrelenmiş verilere erişim

Şifrelenmiş verilere sahip bir çıkarılabilir sürücü bağlandığında, Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

1. Kullanıcının bilgisayarındaki yerel depolama alanında bir ana anahtar arar.

   Bir ana anahtar bulunursa kullanıcı çıkarılabilir sürücüldeki verilere erişim kazanır.

   Ana anahtar bulunmazsa, Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

   a. Kaspersky Security Center'a bir istek gönderir.

      İstek alındıktan sonra, Kaspersky Security Center ana anahtarı içeren bir yanıt gönderir.

   b. Kaspersky Endpoint Security ana anahtarı, şifrelenmiş çıkartılabilir sürücü ile gerçekleştirilecek daha sonraki işlemler için kullanıcının bilgisayarındaki yerel depolama alanına kaydeder.
2. Verilerin şifresini çözer.

Çıkarılabilir sürücü şifrelemesinin özel özellikleri

Çıkarılabilir sürücüleri şifreleme şu özelliklere sahiptir:

- Belirli bir grup yönetilen bilgisayar için kaldırılabilir sürücü şifreleme ön ayarlarına sahip ilke 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 dosyaları şifrelemez / şifresini çözmez.

- 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

Çıkarılabilir sürücüleri şifrelemeyi başlatma

Bir çıkarılabilir sürücünün şifresini çözmek için bir politika kullanabilirsiniz. Belirli bir yönetim grubu için çıkarılabilir sürücü şifrelemesi için tanımlanmış ayarlara sahip bir ilke oluşturulur. Bu nedenle çıkarılabilir sürücülerde veri şifresi çözmenin sonucu, çıkarılabilir sürücünün bağlandığı bilgisayara bağlıdır.

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.

Çıkarılabilir bir sürücüdeki dosyaları şifrelemeden önce, sürücünün biçimlendirildiğinden ve üzerinde gizli bölümler (EFI sistem bölümü gibi) olmadığından emin olun. Sürücü biçimlendirilmemişse ya da gizli bölümler içeriyorsa, dosya şifreleme bir hata ile başarısız olabilir.

Çıkarılabilir sürücüleri şifrelemek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
4. **Şifreleme modu** açılır listesinden, Kaspersky Endpoint Security'nin çıkarılabilir sürücülerde gerçekleştirmesini istediğiniz varsayılan eylemi seçin:
   - **Çıkarılabilir sürücünün tamamını şifrele** (FDE). Kaspersky Endpoint Security, bir çıkarılabilir sürücünün içeriğini sektör sektör şifreler. Sonuç olarak uygulama sadece çıkartılabilir sürücüde saklanan dosyaları değil, çıkartılabilir sürücüdeki dosya adları ve klasör yapıları da dahil olmak üzere dosya sistemlerini de şifreler.
   - **Tüm dosyaları şifrele** (FLE). Kaspersky Endpoint Security, çıkarılabilir sürücülerde saklanan tüm dosyaları şifreler. Uygulama, dosya ve klasör yapıları dahil olmak üzere çıkarılabilir sürücülerin dosya sistemlerini şifrelemez.
   - **Sadece yeni dosyaları şifrele** (FLE). Kaspersky Endpoint Security sadece çıkartılabilir sürücülere eklenmiş olan ya da çıkartılabilir sürücülerde saklanan ve Kaspersky Security Center ilkesinin son uygulanma tarihinden sonra değiştirilen dosyaları şifreler.

   Kaspersky Endpoint Security, zaten şifrelenmiş olan bir çıkarılabilir sürücüyü şifrelemez.

5. Çıkarılabilir sürücülerin şifrelenmesi için taşınabilir modu kullanmak isterseniz **Taşınabilir mod** onay kutusunu seçin.

   Taşınabilir mod, çıkarılabilir sürücülerde, kurumsal bir ağın dışındaki verilere erişebilmenizi sağlayan bir dosya şifreleme modudur (FLE). Taşınabilir mod ayrıca Kaspersky Endpoint Security yüklü olmayan bilgisayarlarda şifrelenmiş verilerle çalışmanıza olanak tanır.

6. Yeni bir çıkartılabilir sürücüyü şifrelemek isterseniz **Sadece kullanılan disk alanını şifrele** onay kutusunu seçmeniz önerilir. Bu onay kutusunun işareti kaldırılırsa, Kaspersky Endpoint Security silinen veya değiştirilen dosyaların artık parçaları da dahil olmak üzere tüm dosyaları şifreler.

7. Çıkarılabilir sürücüler için şifrelemeyi teker teker yapılandırmak isterseniz şifreleme kuralları tanımayın.

8. Çevrimdışı modda çıkartılabilir sürücülerde tam disk şifrelemesi kullanmak isterseniz **Çevrimdışı modda çıkarılabilir sürücülerin şifrelenmesine izin ver** onay kutusunu seçin.

   Çevrimdışı şifreleme modu, Kaspersky Security Center ile bağlantı olmadığında çıkarılabilir sürücülerin şifrelenmesidir (FDE). Şifreleme sırasında Kaspersky Endpoint Security ana anahtarı sadece kullanıcının bilgisayarına kaydeder. Kaspersky Endpoint Security ana anahtarı Kaspersky Endpoint Security'ye bir sonraki senkronizasyon sırasında gönderir.

   > Ana anahtarın kaydedildiği bilgisayar bozulur ve veriler Kaspersky Security Center'a gönderilmezse, çıkartılabilir sürücüye erişim sağlamak mümkün olmaz.

   Çevrimdışı modda çıkarılabilir sürücülerin şifrelenmesine izin ver onay kutusunun işareti kaldırılırsa ve Kaspersky Security Center ile bağlantı kurulmamışsa, çıkartılabilir sürücü şifrelemesi mümkün değildir.

9. Değişikliklerinizi kaydedin.

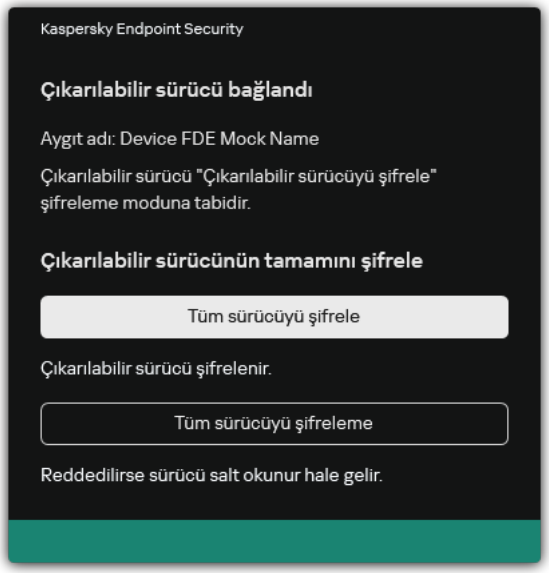
İlke uygulandıktan sonra, kullanıcı bir çıkartılabilir sürücü bağladığında ya da bir çıkartılabilir sürücü zaten bağlı ise, Kaspersky Endpoint Security kullanıcıdan şifreleme işlemini onaylamasını ister (aşağıdaki resme bakın).

Uygulama şu işlemleri gerçekleştirmenize izin verir:

- Kullanıcı şifreleme isteğini onayladığında, Kaspersky Endpoint Security verileri şifreler.
- Kullanıcının şifreleme isteğini reddetmesi halinde, Kaspersky Endpoint Security verileri değiştirmez ve bu çıkarılabilir sürücü için salt okunur erişim atar.
- Kullanıcının şifreleme isteğine cevap vermemesi halinde, Kaspersky Endpoint Security verileri değiştirmez ve bu çıkarılabilir sürücü için salt okunur erişim atar. Daha sonra bir ilke uygulandığında ya da bu çıkarılabilir sürücünün bir sonraki bağlanışında uygulama tekrar onay ister.

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. Veri şifreleme işlemi, çıkartılabilir sürücü bu bilgisayara tekrar bağlandığında devam edecektir.

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.



Çıkartılabilir sürücü şifreleme isteği

Çıkarılabilir sürücülere şifreleme kuralı ekleme

Çıkarılabilir sürücülere şifreleme kuralı eklemek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
4. **Ekle** düğmesine tıklayın ve açılır listeden aşağıdakilerden birini seçin:
   - Aygıt Denetimi bileşeninin güvenilir aygıtlar listesindeki çıkarılabilir sürücüler için şifreleme kuralları eklemek isterseniz **Bu ilkenin güvenilir aygıtlar listesinden** seçeneğini seçin.
   - Kaspersky Security Center listesindeki çıkarılabilir sürücülere şifreleme kuralları eklemek isterseniz **Kaspersky Security Center aygıt listesinden** seçeneğini seçin.
5. **Seçili aygıtlar için şifreleme modu** açılır listesinde, Kaspersky Endpoint Security tarafından seçilen çıkarılabilir sürücülerde kayıtlı dosyalara uygulanacak eylemi seçin.

6. 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.

7. 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 bilgiler 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 şifrele** modunda bir ilke uygulandıktan sonra, dosyalar tarafından kullanılmayan sektörler yine de şifrelenmez.

8. **Daha önce seçilmiş aygıtlar için işlemler** 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 **Yenile**'yi seçin.

9. Değişikliklerinizi kaydedin.

Çıkarılabilir sürücüler için eklenen şifreleme kuralları, kuruluş içindeki herhangi bir bilgisayara bağlı olan çıkarılabilir sürücülere uygulanacaktır.

Çıkarılabilir sürücüler için şifreleme kuralları listesini dışa ve içe aktarma

Çıkarılabilir sürücü şifreleme kurallarının listesini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin, aynı tür çıkarılabilir sürücüler için çok sayıda kural eklemek üzere dosyayı değiştirebilirsiniz. Kural listesini yedeklemek veya kuralları farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

Yönetim Konsolu'nda (MMC) çıkarılabilir sürücü şifreleme kuralları listesini dışa aktarma ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimini yapın.
5. **Seçili xcihazlar için şifreleme kuralları** bloğunda, **<N> kuralları** bağlantısına tıklayın.

   Bu, çıkarılabilir sürücüler için şifreleme kurallarının bir listesini açar.

6. Çıkarılabilir sürücüler için şifreleme kuralları listesini dışa aktarmak için:

   a. Düzenlemek istediğiniz kuralları seçin.

   b. **Dışa aktar**'a tıklayın.

   c. Yalnızca seçili kuralları veya tüm listeyi dışa aktarmak istediğinizi onaylayın.

   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, kural listesini varsayılan indirilenler klasöründeki bir XML dosyasına aktarır.

7. Kurallar listesini içe aktarmak için:

   a. **İçe aktar** bağlantısına tıklayın.

      Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   b. Dosyayı aç.

      Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

8. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinden **Veri Şifreleme → Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.

4. Çıkarılabilir sürücüler için şifreleme kuralları listesini dışa aktarmak için:

   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla port seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

      Herhangi bir kural seçmezseniz, Kaspersky Endpoint Security tüm istisnaları dışa aktaracaktır.

   b. **Dışa aktar** bağlantısına tıklayın.

   c. Açılan pencerede, kurallar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   d. Dosyaya kaydet.

      Kaspersky Endpoint Security, kurallar listesini XML dosyasına aktarır.

5. Çıkarılabilir sürücüler için şifreleme kuralları listesini içe aktarmak için:

   a. **İçe aktar** bağlantısına tıklayın.

      Açılan pencerede, kurallar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   b. Dosyayı aç.

      Bilgisayar zaten bir kurallar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

6. Değişikliklerinizi kaydedin.

Çıkarılabilir sürücülerdeki şifreli dosyalara erişim için taşınabilir mod

Taşınabilir mod, çıkarılabilir sürücülerde, kurumsal bir ağın dışındaki verilere erişebilmenizi sağlayan bir dosya şifreleme modudur (FLE). Taşınabilir mod ayrıca Kaspersky Endpoint Security yüklü olmayan bilgisayarlarda şifrelenmiş verilerle çalışmanıza olanak tanır.

Taşınabilir mod, aşağıdaki durumlarda kullanmak için uygundur:

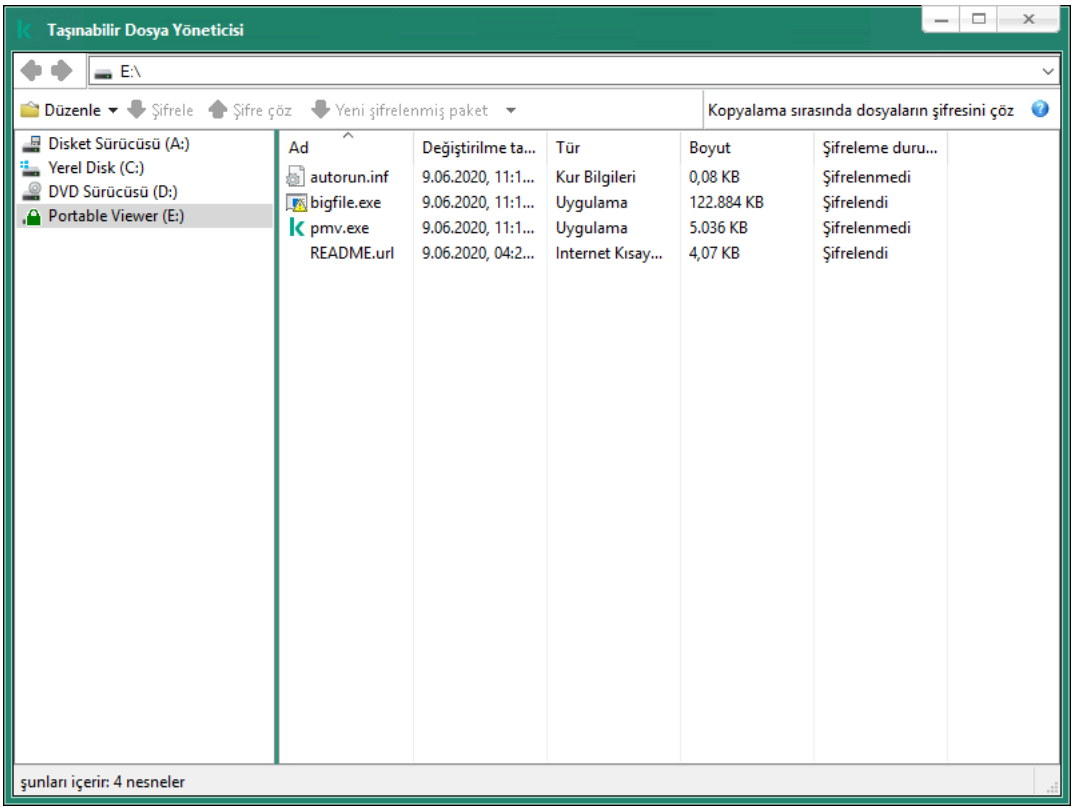
- Bilgisayar ile Kaspersky Security Center Yönetim Sunucusu arasında bağlantı olmadığında.
- Kaspersky Security Center Yönetim Sunucusunun değişimi ile altyapı değiştiğinde.
- Kaspersky Endpoint Security bilgisayarda yüklü olmadığında.

Taşınabilir Dosya Yöneticisi

Taşınabilir modda çalışmak için Kaspersky Endpoint Security bir çıkarılabilir sürücüye *Taşınabilir Dosya Yöneticisi* adlı özel bir şifreleme modülü yükler. Taşınabilir Dosya Yöneticisi, Kaspersky Endpoint Security bilgisayarda yüklü olmadığında şifrelenmiş verilerle çalışmak için bir arabirim sunar (aşağıdaki şekle bakın). Kaspersky Endpoint Security bilgisayarınızda yüklü ise şifrelenmiş çıkarılabilir sürücülerle her zamanki dosya yöneticinizi (örneğin Gezgin) kullanarak çalışabilirsiniz.

Taşınabilir Dosya Yöneticisi, dosyaları şifrelemek için bir çıkartılabilir sürücü üzerinde bir anahtar saklar. Bu anahtar kullanıcı parolası ile şifrelenmiştir. Kullanıcı, dosyaları bir çıkartılabilir sürücü üzerinde şifrelemeden önce bir parola ayarlar.

Bir çıkartılabilir sürücü Kaspersky Endpoint Security yüklü olmayan bir bilgisayara bağlandığında, Taşınabilir Dosya Yöneticisi otomatik olarak başlatılır. Bilgisayarda uygulamaların otomatik başlatılması devre dışı bırakılmışsa Taşınabilir Dosya Yöneticisini manuel olarak başlatın. Bunu yapmak için çıkartılabilir sürücüde saklanan pmv.exe isimli dosyayı çalıştırın.



Taşınabilir Dosya Yöneticisi

Şifrelenmiş dosyalarla çalışmak için taşınabilir mod desteği

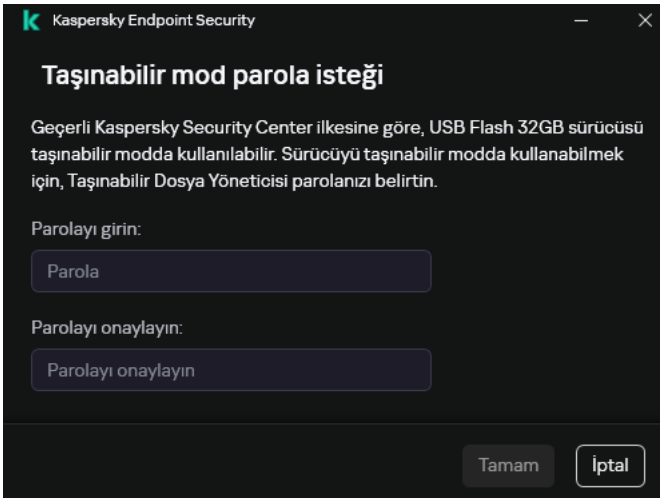
Yönetim Konsolu'nda (MMC) çıkarılabilir sürücüler üzerindeki şifrelenmiş dosyalarla çalışmak için taşınabilir mod desteği nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
4. **Seçili aygıtlar için şifreleme modu** açılır listesinden **Tüm dosyaları şifrele** veya **Sadece yeni dosyaları şifrele** seçimini yapın.

   Taşınabilir mod sadece Dosya Düzeyinde Şifreleme (FLE) ile kullanılabilir. Tam Disk Şifreleme. (FDE) için taşınabilir mod desteğini etkinleştirmek mümkün değildir.

5. **Taşınabilir mod** onay kutusunu seçin.
6. Gerekirse, çıkartılabilir sürücüler için tek tek şifreleme kuralları ekleyebilirsiniz.
7. Değişikliklerinizi kaydedin.
8. İlkeyi uyguladıktan sonra çıkarılabilir sürücüyü bilgisayara bağlayın.
9. Çıkarılabilir sürücü şifreleme işlemini onaylayın.

Bu, Taşınabilir Dosya Yöneticisi için bir parola oluşturabileceğiniz pencereyi açar.



Taşınabilir mod parola isteği

10. Güç gereksinimlerini karşılayan bir şifre belirleyin ve onaylayın.
11. Değişikliklerinizi kaydedin.

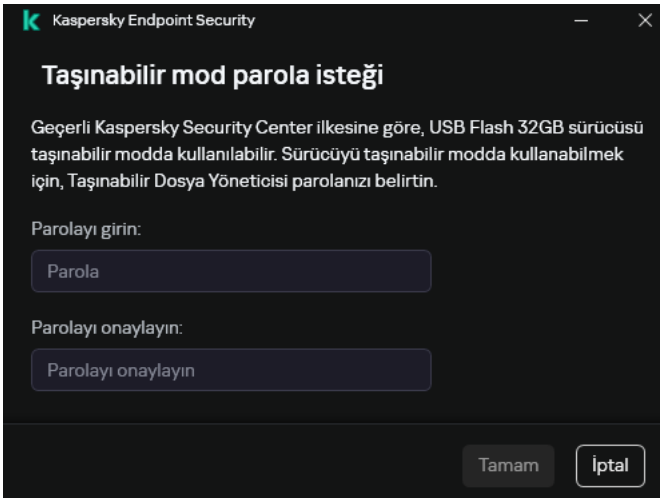
Web Console'da çıkarılabilir sürücüler üzerindeki şifrelenmiş dosyalarla çalışırken taşınabilir mod desteği nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimini yapın.
5. **Varsayılan eylem** bloğunda, **Tüm dosyaları şifrele** veya **Sadece yeni dosyaları şifrele** seçimini yapın.

   Taşınabilir mod sadece Dosya Düzeyinde Şifreleme (FLE) ile kullanılabilir. Tam Disk Şifreleme. (FDE) için taşınabilir mod desteğini etkinleştirmek mümkün değildir.

6. **Taşınabilir mod** onay kutusunu seçin.
7. Gerekirse, çıkartılabilir sürücüler için tek tek şifreleme kuralları ekleyebilirsiniz.
8. Değişikliklerinizi kaydedin.
9. İlkeyi uyguladıktan sonra çıkarılabilir sürücüyü bilgisayara bağlayın.
10. Çıkarılabilir sürücü şifreleme işlemini onaylayın.

Bu, Taşınabilir Dosya Yöneticisi için bir parola oluşturabileceğiniz pencereyi açar.



Taşınabilir mod parola isteği

11. Güç gereksinimlerini karşılayan bir şifre belirleyin ve onaylayın.

12. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Security, çıkarılabilir sürücülerdeki dosyaları şifreleyecektir. Şifrelenmiş dosyalarla çalışmak için kullanılan Taşınabilir Dosya Yöneticisi ayrıca çıkarılabilir sürücüye de eklenecektir. Çıkarılabilir sürücü üzerinde zaten şifrelenmiş dosyalar varsa, Kaspersky Endpoint Security bunları kendi anahtarını kullanarak tekrar şifreleyecektir. Böylece kullanıcının çıkarılabilir sürücü üzerindeki tüm dosyalara taşınabilir modda erişmesi mümkün olur.

Bir çıkarılabilir sürücüdeki şifrelenmiş dosyalara erişme

Bir çıkartılabilir sürücüdeki dosyaları taşınabilir mod desteği ile şifreledikten sonra şu dosya erişim yöntemleri kullanılabilir:

- Kaspersky Endpoint Security bilgisayarda yüklü olmadığında, Taşınabilir Dosya Yöneticisi sizden bir parola girmenizi ister. Bilgisayarı her yeniden başlattığınızda ya da çıkartılabilir sürücüyü her bağladığınızda parolayı girmeniz gerekir.

- Bilgisayar kurumsal ağın dışında ve Kaspersky Endpoint Security bilgisayara yüklüyse, uygulama parola girmenizi ister ya da dosyalara erişim için yöneticiye bir istek gönderir. Bir çıkartılabilir sürücüdeki dosyalara erişim kazandıktan sonra, Kaspersky Endpoint Security gizli anahtarı bilgisayarın anahtar deposuna kaydeder. Böylece gelecekten dosyalara bir parola girmeden ya da yöneticiye sormadan erişmek mümkün olur (aşağıdaki resme bakın).

- Bilgisayar kurumsal ağın içinde ve Kaspersky Endpoint Security bilgisayarda yüklü ise cihaza bir parola girmeden erişim sağlanır. Kaspersky Endpoint Security, bilgisayarın bağlı olduğu Kaspersky Security Center Yönetim Sunucusundan gizli anahtarı alır.



Bir çıkarılabilir sürücüdeki şifrelenmiş dosyalara erişme

Taşınabilir modda çalışmak için parolanın kurtarılması

Taşınabilir modda çalışmak için gerekli parolayı unutursanız, çıkarılabilir sürücüyü kurumsal ağda yer alan ve Kaspersky Endpoint Security yüklü bir bilgisayara bağlamanız gerekir. Gizli anahtar bilgisayarın anahtar deposunda ya da Yönetim Sunucusunda saklandığından, dosyalara erişim alırsınız. Dosyalarda yeni bir parola ile şifreleme ve şifre çözme yapın.

Bir çıkarılabilir sürücüyü başka bir ağdaki bir bilgisayara bağlarken taşınabilir modun özellikleri

Bilgisayar kurumsal ağın dışında ve Kaspersky Endpoint Security bilgisayarda yüklü ise cihaza şu yöntemlerle erişim sağlanır:

- **Parola tabanlı erişim**

  Parolayı girdikten sonra, çıkarılabilir sürücüdeki dosyaları görüntüleyebilir, değiştirebilir ve kaydedebilirsiniz (*saydam erişim*). Çıkarılabilir sürücüleri şifreleme ilke ayarlarında şu parametreler yapılandırılmışsa, Kaspersky Endpoint Security bir çıkarılabilir sürücü için bir salt okunur erişim hakkı ayarlayabilir:

  - Taşınabilir mod desteği devre dışı.
  - **Tüm dosyaları şifrele** veya **Sadece yeni dosyaları şifrele** modu seçilidir.

  Diğer tüm durumlarda, çıkarılabilir sürücüye tam erişim elde edersiniz (okuma/yazma izni). Dosya ekleme ve silme yapabilirsiniz.

  Çıkarılabilir sürücü bilgisayara bağlı olsa bile çıkarılabilir sürücü erişim izinlerini değiştirebilirsiniz. Çıkarılabilir sürücü erişim izinleri değiştirilirse, Kaspersky Endpoint Security dosyalara erişimi engelleyecek ve sizden parolayı tekrar girmenizi isteyecektir.

  Parolayı girdikten sonra, çıkarılabilir sürücü için şifreleme ilkesi ayarlarını uygulayamazsınız. Bu durumda, çıkarılabilir sürücüdeki dosyaların şifresini çözmek veya yeniden şifrelemek mümkün değildir.

- **Yöneticiden dosyalara erişim isteyin**

Taşınabilir modda çalışmak için gereken parolayı unutursanız, dosyalara erişmek için yöneticiden izin isteyin. Kullanıcının dosyalara erişmek için yöneticiye bir istek erişim dosyası (KESDC uzantılı bir dosya) göndermesi gerekir. Örneğin, kullanıcı istek erişim dosyasını e-posta ile gönderebilir. Yönetici bir şifrelenmiş verilere erişim dosyası (KESDR uzantılı bir dosya) gönderir.

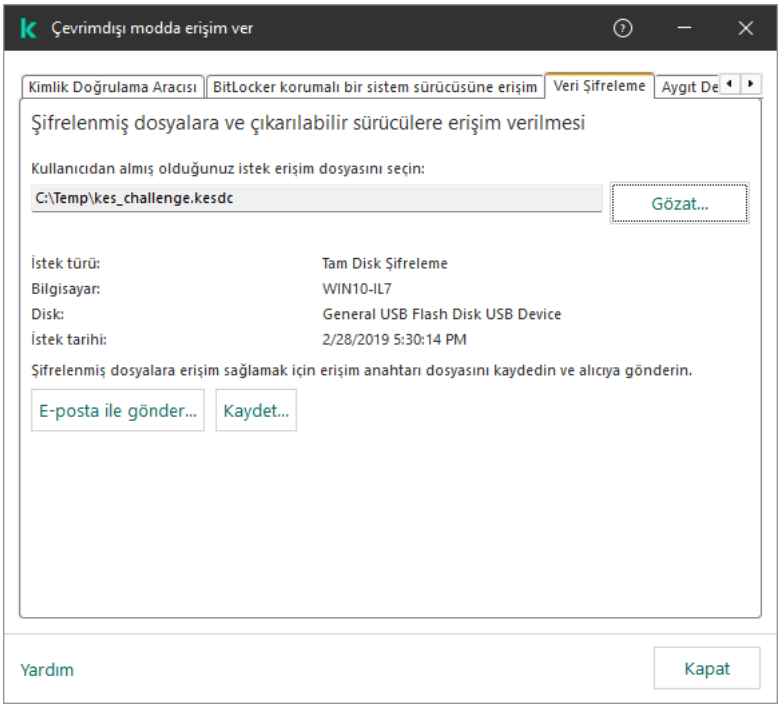
İstek-Yanıt parola kurtarma prosedürünü tamamladıktan sonra, çıkarılabilir sürücüdeki dosyalara saydam erişim ve çıkarılabilir sürücüye tam erişim (okuma/yazma izni) alırsınız.

Örneğin, çıkarılabilir bir sürücü şifreleme ilkesini uygulayabilir ve dosyaların şifresini çözebilirsiniz. Parolayı kurtardıktan sonra veya ilke güncelleştirildiğinde, Kaspersky Endpoint Security değişiklikleri onaylamanızı ister.

Yönetim Konsolu'nda (MMC) bir şifrelenmiş verilere erişim dosyası nasıl alınır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Cihazlar**.
3. **Cihazlar** sekmesinde, şifrelenmiş verilere erişim talep eden kullanıcının bilgisayarını seçin ve bağlam menüsünü görüntülemek için sağ tıklayın.
4. İçerik menüsünde **Çevrimdışı modda erişim ver** seçeneğini belirleyin.
5. Bu işlem bir pencere açar; bu pencerede **Veri Şifreleme** sekmesini seçin.
6. **Veri Şifreleme** sekmesinde, **Gözat** düğmesine tıklayın.
7. İstek erişim dosyası seçme penceresinde, kullanıcıdan alınan dosyanın yolunu belirdin.

Kullanıcının isteğiyle ilgili bilgiler görüntülenir. Kaspersky Security Center bir anahtar dosyası oluşturur. Oluşturulan şifrelenmiş dosya erişim anahtar dosyasını kullanıcıya e-posta ile gönderin. Yahut erişim dosyasını kaydedin ve transfer içi mevcut yöntemlerden birini kullanın.



Çevrimdışı modda erişim ver

Web Console'da bir şifrelenmiş verilere erişim dosyası nasıl alınır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Verilerine tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.
3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.
4. **Veri Şifreleme**'yi seçin.
5. **Dosya seç** düğmesine tıklayın ve kullanıcıdan aldığınız istek erişim dosyasını (KESDC uzantılı bir dosya) seçin.

   Web Console, istekle ilgili bilgileri görüntüler. Bu bilgiler arasında kullanıcının dosyaya erişim isteği yaptığı bilgisayarın adı da yer alır.
6. **Anahtarı kaydet** düğmesine tıklayın ve şifrelenmiş veri erişim anahtarı dosyasının (KESDR uzantılı bir dosya) kaydedileceği bir klasör seçin.

Sonuç olarak, kullanıcıya aktarmanız gereken şifrelenmiş verilere erişim anahtarını alırsınız.

Çıkarılabilir sürücülerin şifresini çözme

Bir çıkarılabilir sürücünün şifresini çözmek için bir politika kullanabilirsiniz. Belirli bir yönetim grubu için çıkarılabilir sürücü şifrelemesi için tanımlanmış ayarlara sahip bir ilke oluşturulur. Bu nedenle çıkarılabilir sürücülerde veri şifresi çözmenin sonucu, çıkarılabilir sürücünün bağlandığı bilgisayara bağlıdır.

Çıkarılabilir sürücülerin şifresini çözmek için:

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
4. Çıkarılabilir sürücülerde kayıtlı tüm şifrelenmiş dosyaların şifresini çözmek isterseniz, **Şifreleme modu** açılır listesinde **Çıkarılabilir sürücünün tamamının şifresini çöz** seçeneğini seçin.
5. 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 düzenle** düğmesine tıklayın.
   c. **Bir kural düzenle** düğmesinin bağlam menüsünden **Çıkarılabilir sürücünün tamamının şifresini çöz**'ü seçin.
6. Değişikliklerinizi kaydedin.

Sonuç olarak, bir kullanıcı bir çıkarılabilir sürücüye bağlanırsa ya da zaten bağlı ise, Kaspersky Endpoint Security bu çıkartılabilir sürücünün şifresini çözer. Uygulama kullanıcıya şifre çözme işleminin biraz zaman alabileceği uyarısında bulunur. 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. Veri şifresini çözme işlemi, çıkartılabilir sürücü bilgisayara tekrar bağlandığında devam edecektir.

Bir çıkarılabilir sürücü 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.

Veri şifreleme ayrıntılarını görüntüleme

Şifreleme veya şifre çözme devam ederken Kaspersky Endpoint Security, Kaspersky Security Center'ın istemci bilgisayarlarına uygulanan şifreleme parametrelerinin durumu hakkında bilgi aktarır.

Şifreleme durumunu görüntüleme

Veri şifrelemesini izlemek için duruma bakabilirsiniz. Kaspersky Endpoint Security şu şifreleme durumlarını atar:

- **İlkeye uymuyor; kullanıcı tarafından iptal edildi**. Kullanıcı veri şifrelemeyi iptal etti.
- **Bir hata nedeniyle ilkeye uymuyor**. Veri şifreleme hatası, örneğin bir lisans eksik.
- **İlke uygulanıyor; yeniden başlatma gerekli**. Bilgisayarda veri şifreleme devam ediyor. Veri şifrelemeyi tamamlamak için bilgisayarı yeniden başlatın.
- **Hiçbir şifreleme ilkesi belirtilmemiş**. İlke ayarlarında veri şifreleme kapalı.
- **Desteklenmiyor**. Veri şifreleme bileşenleri bilgisayarda yüklü değil.
- **İlke uygulanıyor**. Bilgisayarda veri şifreleme ve/veya şifre çözme devam ediyor.

Bilgisayar verilerinin şifreleme durumunu görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Yönetilen cihazlar**.
3. Çalışma alanındaki **Cihazlar** sekmesinde, kaydırma çubuğunu sonuna kadar sağa sürükleyin. **Şifreleme durumu** sütunu görüntülenmiyorsa, Kaspersky Security Center konsol ayarlarında bu sütunu ekleyin.

   Şifreleme durumu sütununda, seçilen yönetim grubundaki bilgisayarların şifreleme durumu görüntülenir. Bu durum, bilgisayarın yerel sürücülerindeki dosya şifreleme ve tam disk şifreleme hakkındaki bilgilere göre oluşturulur.
4. Bilgisayar için veri şifreleme durumu **İlke uygulanıyor** olduğunda, şifreleme ilerleme panelini takip edebilirsiniz:
   a. **İlke uygulanıyor** durumuna çift tıklayarak bilgisayarın özelliklerini açın.
   b. Bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
   c. Bilgisayarda yüklü Kaspersky uygulamaları listesinden **Kaspersky Endpoint Security for Windows** seçimini yapın.
   d. **İstatistikler**'e tıklayın.
   e. **Cihazların şifrelenmesi** bölümünde veri şifrelemenin anlık ilerlemesini yüzde olarak görebilirsiniz.

Kaspersky Security Center panolarındaki şifreleme istatistiklerini görüntüleme

Kaspersky Security Center panolarındaki şifreleme durumunu görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **Yönetim Sunucusu** düğümünü seçin.
3. Yönetim Konsolu ağacının sağındaki çalışma alanında **İstatistikler** sekmesini seçin.
4. Veri şifreleme istatistiklerini içeren ayrıntılar alanlarının bulunduğu yeni bir sayfa oluşturun. Bunun için:
   a. **İstatistikler** sekmesinde, **Görünümü özelleştir** düğmesine tıklayın.
   b. Açılan pencerede **Ekle** düğmesine tıklayın.
   c. Bu bir pencere açar; bu penceredeki **Genel** bölümüne sayfanın adını girin.
   d. **Bilgi bölmeleri** bölümünde **Ekle** düğmesine tıklayın.
   e. **Koruma durumu** grubunda açılan yeni pencerede **Cihazların şifrelenmesi** öğesini seçin.
   f. **Tamam**'a tıklayın.
   g. Gerekirse ayrıntılar bölmesinin ayarlarını düzenleyin. Bunu yapmak için **Görüntüle** ve **Cihazlar** bölümlerini kullanın.
   h. **Tamam**'a tıklayın.
   i. Talimatların d – h adımlarını tekrarlayın; Yeni bilgi bölmesi penceresinin **Koruma durumu** bölümünden **Çıkarılabilir sürücülerin şifrelenmesi** öğesini seçin.

      Bilgi bölmeleri listesinde, eklenen ayrıntılar alanları görüntülenir.
   j. **Tamam**'a tıklayın.

      Önceki adımda oluşturulan ayrıntılar alanlarının olduğu sayfanın adı **Sayfalar** listesinde görülür.
   k. **Kapat** düğmesine tıklayın.
5. **İstatistikler** sekmesinde, talimatların önceki adımlarında oluşturulan sayfayı açın.

Bilgisayarların ve çıkarılabilir sürücülerin şifreleme durumunu görüntüleyen ayrıntılar alanları açılır.

Yerel bilgisayar sürücülerinde dosya şifreleme hatalarını görüntüleme

Yerel bilgisayar sürücülerinde dosya şifreleme hatalarını görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında şunu seçin: **Yönetilen cihazlar**.
3. **Cihazlar** sekmesinde, listeden bilgisayarın adını seçin ve sağ tıklayarak bağlam menüsünü açın.
4. Bilgisayarın bağlam menüsünden **Özellikler** öğesini seçin. Açılan pencereden **Koruma** bölümünü seçin.
5. **Veri şifreleme hatalarını görüntüle** penceresini açmak için **Veri şifreleme hataları** bağlantısına tıklayın.

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

Kaspersky Security Center, veri şifreleme raporları oluşturmanıza olanak tanır:

- **Yönetilen cihazların şifreleme durumları hakkında rapor**. Rapor, bilgisayarın şifreleme durumunun şifreleme ilkesine uyup uymadığına ilişkin bilgiler içerir.
- **Yığın depolama cihazlarının şifreleme durumu hakkında rapor**. Rapor, harici cihazların ve depolama cihazlarının şifreleme durumu hakkında bilgi içerir.
- **Şifrelenmiş sürücülere erişim haklarına yönelik rapor**. Rapor, şifrelenmiş sürücülere erişimi olan hesapların durumu hakkında bilgi içerir.
- **Dosya şifreleme hataları hakkında rapor**. Rapor, bilgisayarlarda veri şifreleme veya şifre çözme görevlerinin yürütülmesi sırasında oluşan hatalar hakkında bilgi içerir.
- **Şifrelenmiş dosyalara erişimin engellenmesi hakkında rapor**. Rapor, şifrelenmiş dosyalara erişmesi engellenen uygulamalar hakkında bilgi içerir.

Veri şifreleme raporunu görüntülemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Raporlar** sekmesini seçin.
3. **Yeni rapor şablonu** düğmesine tıklayın.

   Yeni Rapor Şablonu Sihirbazı başlatılır.

4. Rapor Şablonu Sihirbazı talimatlarını uygulayın. **Diğer** bölümünde **Rapor şablon türünü seçme** penceresinden veri şifreleme raporlarından birini seçin.

   Yeni Rapor Şablonu Sihirbazı ile işlemi tamamladıktan sonra yeni rapor şablonu **Raporlar** sekmesindeki tabloda görünür.

5. Talimatların önceki adımlarında oluşturulan rapor şablonunu seçin.

6. Şablonun bağlam menüsünden **Raporu göster**'i seçin.

Rapor üretme işlemi başlar. Rapor yeni bir pencerede görüntülenir.

Şifrelenmiş cihazlara erişim olmadığında şifrelenmiş cihazlarla çalışma

Şifrelenmiş cihazlara erişim sağlama

Bir kullanıcının şifrelenmiş cihazlara 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 cihazlara erişim aşağıdaki şekilde elde edilebilir:

1. Kullanıcı kesdc uzantılı bir istek erişim dosyasını oluşturmak için Kaspersky Endpoint Security uygulamasının arabirimini 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 cihazlarla çalışmak için Şifrelenmiş Aygıt Geri Yükleme Yardımcı Uygulaması (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 şifrelenmiş cihazlara erişimi geri yüklemek için gereken veriler bir süredir kullanıcı bilgisayarının belleğinde şifrelenmemiş biçimde bulunuyor. Bu tür verilere yetkisiz erişim riskini azaltmak için şifrelenmiş cihazlara erişimi güvenilir bilgisayarlarda geri yüklemeniz önerilir.

Şifrelenmiş cihazlardaki dosyalar aşağıdaki şekilde elde edilebilir:

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 bozulmuş kullanıcı geri yükleme prosedürünü bir istek erişim dosyası kullanarak tamamlamalıdır.

Şifrelenmiş cihazlarda veriler geri yüklenmeden önce Kaspersky Security Center ilkesinin iptal edilmesi veya bu işlemin gerçekleştirileceği bilgisayarda Kaspersky Security Center ilke ayarlarındaki şifrelemenin devre dışı bırakılması önerilir. Bu şekilde aygıtın yeniden şifrelenmesi önlenir.

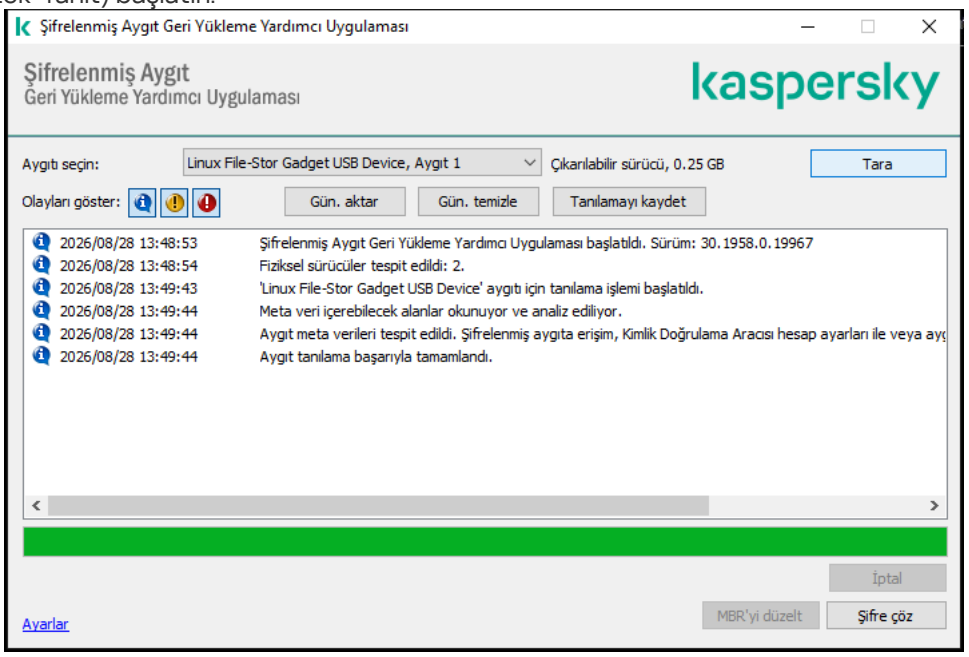
FDERT Geri Yükleme Yardımcı Uygulamasını kullanarak veri kurtarma

Sabit sürücüde arıza olursa sistem çökebilir. Böyle bir durumda, Kaspersky Disk Encryption teknolojisi tarafından korunan veriler kullanılamaz. Verilerin şifresini çözüp onları yeni bir sürücüye kopyalayabilirsiniz.

Kaspersky Disk Encryption teknoloji tarafından korunan bir sürücüde veri kurtarma yapmak için aşağıdaki adımlar uygulanmalıdır:

1. Bir bağımsız Geri Yükleme Yardımcı Programı oluşturun (aşağıdaki resme bakın).
2. Kaspersky Endpoint Security şifreleme bileşenleri yüklü olmayan bir bilgisayara bir sürücü bağlayın.
3. Geri Yükleme Yardımcı Programı'nı çalıştırın ve sabit sürücüde tanılama yapın.

4. Sürücüdeki verilere erişin. Bunu yapmak için Kimlik Doğrulama Aracısının kimlik bilgilerini girin ya da kurtarma prosedürünü (İstek-Yanıt) başlatın.



FDERT Geri Yükleme Yardımcı Programı

Bağımsız bir geri yükleme yardımcı programı oluşturmak

Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyasını oluşturmak için:

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Açılan pencerede **Şifrelenmiş aygıtı geri yükle** düğmesine tıklayın.

   Şifrelenmiş Aygıt Geri Yükleme Yardımcı Uygulaması başlatılır.
3. Geri Yükleme Yardımcı Programı penceresinde **Bağımsız Geri Yükleme Yardımcı Programı Oluştur** düğmesine tıklayın.
4. Bağımsız Geri Yükleme Yardımcı Programı'nı bilgisayarın belleğine kaydedin.

Sonuç olarak, Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyası (fdert.exe) belirtilen klasöre kaydedilir. Kaspersky Endpoint Security şifreleme bileşenleri olmayan bir bilgisayara Geri Yükleme Yardımcı Programı'nı kopyalayın. Bu şekilde sürücünün yeniden şifrelenmesi önlenir.

Geri Yükleme Yardımcı Programı kullanılarak şifrelenmiş cihazlara erişimi geri yüklemek için gereken veriler bir süredir kullanıcı bilgisayarının belleğinde şifrelenmemiş biçimde bulunuyor. Bu tür verilere yetkisiz erişim riskini azaltmak için şifrelenmiş cihazlara erişimi güvenilir bilgisayarlarda geri yüklemeniz önerilir.

Bir sabit sürücüdeki verileri kurtarma

Geri Yükleme Yardımcı Programını kullanarak şifrelenmiş aygıtlara erişimi geri yüklemek için:

1. Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyası olan fdert.exe isimli dosyayı çalıştırın. Bu dosya, Kaspersky Endpoint Security tarafından oluşturulur.

2. Geri Yükleme Yardımcı Programı penceresinden erişimin geri yüklenmesine istediğiniz şifrelenmiş aygıtı 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 var Geri Yükleme Yardımcı Programı aygıtın kilidini kaldırmanızı ister. Aygıtın kilidinin kaldırılması şifresini çözmese de, kilidinin kaldırılmasından dolayı aygıt doğrudan erişilebilir hale gelir. Bilgisayarın Kaspersky Endpoint Security şifreleme işlevselliğine erişimi yoksa Geri Yükleme Yardımcı Programı aygıtın şifresini çözmenizi ister.

4. Tanı bilgilerini içe aktarmak isterseniz **Tanılamayı kaydet** düğmesine tıklayın.

   Yardımcı program, tanılama bilgilerini içeren dosyaları bir arşive kaydeder.

5. 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 kaldırmak veya şifresini çözmek için gereken bilgileri alma işlemini hızlandırabilir.

6. Teşhis sonuçlarına göre **Kilidi kaldır** veya **Şifre çöz** düğmesine tıklayın.

7. Bir Kimlik Doğrulama Aracısı hesabı kullanarak verileri geri yüklemek isterseniz **Kimlik Doğrulama Aracısı hesap ayarlarını kullan** seçeneğini seçin ve Kimlik Doğrulama Aracısı'nın kimlik bilgilerini girin.

   Bu yöntem, yalnızca bir sistem sabit sürücüsündeki verileri geri yüklerken mümkündür. Sistem sabit sürücüsü bozuksa ve Kimlik Doğrulama Aracısı hesabı verileri kaybolduysa şifrelenmiş bir aygıttaki verileri geri yüklemek için kurumsal LAN yöneticinizden bir erişim anahtarı edinmelisiniz.

8. Kurtarma prosedürünü başlatmak isterseniz şunları yapın:

   a. **Aygıt erişim anahtarını manuel olarak belirle** seçeneğini seçin.

   b. **Erişim anahtarını al** düğmesine tıklayın ve istek erişim dosyasını (FDERTC uzantılı bir dosya) bilgisayarın belleğine kaydedin.

   c. İstek erişim dosyasını kurumsal LAN yöneticisine gönderin.

      Erişim anahtarını almayana kadar **Aygıt erişim anahtarını al** penceresini kapatmayın. Bu pencere tekrar açıldığında, yönetici tarafından daha önce oluşturulmuş olan erişim anahtarını uygulayamazsınız.

   d. Kurumsal LAN yöneticisi tarafından oluşturulup size gönderilen istek erişim dosyasını (FDERTR uzantılı bir dosya) alın ve kaydedin (aşağıdaki talimatlara bakın).

   e. Erişim dosyasını **Aygıt erişim anahtarını al** penceresinden indirin.

9. Bir cihazın şifresini çözüyorsanız ek şifre çözme ayarları yapılandırmanız gerekir:

    - Şifresi çözülecek alanı belirleyin:

        - 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 alanı belirleyin.

    - Şifresi çözülmüş verileri yazmak için konumu seçin:

        - Orijinal aygıttaki verilerin şifresi çözülmüş verilerle yeniden yazılmasını istiyorsanız **Disk görüntü dosyasının şifresini çöz** onay kutusunun işaretini kaldırın.

        - Şifresi çözülmüş verilerin orijinal olarak şifrelenen verilerden ayrı olarak kaydedilmesini istiyorsanız **Disk görüntü dosyasının şifresini çöz** onay kutusunu işaretleyin ve VHD dosyasının kaydedileceği yolu belirtmek üzere **Gözat** düğmesini kullanın.

10. **Tamam**'a tıklayın.

Aygıt kilidi kaldırma / şifre çözme işlemi başlar.

Yönetim Konsolu'nda (MMC) bir şifrelenmiş verilere erişim dosyası nasıl oluşturulur

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacında, **Gelişmiş → Veri şifreleme ve koruma → Şifrelenmiş sürücüler** klasörünü seçin.

3. Çalışma alanında, bir erişim anahtarı dosyası oluşturmak istediğiniz şifrelenmiş aygıtı seçin, ardından aygıtın içerik menüsünden **Kaspersky Endpoint Security'da aygıta erişim al**'a tıklayın.

    Erişim isteği dosyasının hangi bilgisayar için oluşturulduğundan emin değilseniz Yönetim Konsolu ağacında, **Gelişmiş → Veri şifreleme ve koruma** klasörünü seçin ve çalışma alanında **Kaspersky Endpoint Security'deki cihaz şifreleme anahtarını al**'a tıklayın.

4. Açılan pencerede, kullanılacak şifreleme algoritmasını seçin: AES256 veya AES56.

    Veri şifreleme algoritması, dağıtım paketine dahil olan AES şifreleme kitaplığına bağlıdır: *Güçlü şifreleme (AES256)* veya *Hafif şifreleme (AES56)*. AES şifreleme kitaplığı uygulama ile birlikte yüklenir.

5. Bir pencere açmak için **Gözat**'a tıklayın; bu pencerede, kullanıcıdan almış olduğunuz fdertc uzantılı istek dosyasının yolunu belirtin.

6. **Kilidi aç**'a tıklayın.

Kullanıcının isteğiyle ilgili bilgiler görüntülenir. Kaspersky Security Center bir anahtar dosyası oluşturur. Oluşturulan şifrelenmiş dosya erişim anahtar dosyasını kullanıcıya e-posta ile gönderin. Yahut erişim dosyasını kaydedin ve transfer içi mevcut yöntemlerden birini kullanın.

Web Console'da bir şifrelenmiş verilere erişim dosyası nasıl oluşturulur

1. Web Console'un ana penceresinden **İşlemler → Veri şifreleme ve koruma → Şifrelenmiş sürücüler**'ı seçin.

2. Sürücüsünde veri kurtarma yapmak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.

3. **Cihaza çevrimdışı modda erişim izni ver**'e tıklayın.

   Bu, bir aygıta erişim verecek Sihirbazı başlatılır.

4. Bir aygıta erişim kazanmak için Sihirbazın talimatlarını uygulayın:

   a. Kaspersky Endpoint Security for Windows eklentisini seçin.

   b. Kullanılacak şifreleme algoritmasını seçin: AES256 veya AES56.

      Veri şifreleme algoritması, dağıtım paketine dahil olan AES şifreleme kitaplığına bağlıdır: *Güçlü şifreleme (AES256)* veya *Hafif şifreleme (AES56)*. AES şifreleme kitaplığı uygulama ile birlikte yüklenir.

   c. Kullanıcıdan alınan istek erişim dosyasını seçin (FDERTC uzantılı bir dosya).

   d. Şifrelenmiş veri erişim anahtarı dosyasını (FDERTR uzantılı bir dosya) kaydetmek için bir klasör seçin.

Sonuç olarak, kullanıcıya aktarmanız gereken şifrelenmiş verilere erişim anahtarını alırsınız.

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. Şifrelenmiş Aygıt Geri Yükleme Yardımcı Uygulaması 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 (ör. Microsoft TechNet kaynağı).

Detection and Response çözümleri

Kaspersky Detection and Response çözümleri, bir kuruluşun altyapısının farklı seviyelerindeki gelişmiş tehditleri ve saldırı göstergelerini tespit etmeye yönelik güvenlik sistemleridir. Tespit ve Müdahale çözümleri tespit edilen tehdit hakkında bilgi sağlar ve Tehdit Müdahale eylemlerinin yönetilmesine olanak tanır.

Bu amaçla, Detection and Response çözümü şunları yapar:

- Bir bilgisayarın, sunucunun veya diğer cihazların çalışması hakkında bilgi almak (telemetri).
- Tehditleri tespit etmek için bilgileri otomatik olarak analiz etmek.
- Analiz ve Tehdit Yanıtı eylemlerini seçmek için tehdit geliştirme zincirinin sütunları olarak uyarı ayrıntılarını oluşturmak.
- Tehdit Yanıtı eylemlerini gerçekleştirmek (örneğin, bilgisayarın ağ izolasyonu).

Kaspersky Endpoint Security, Detection and Response çözümlerini yerleşik bir aracı kullanarak destekler. Yerleşik aracı, çözüm sunucularına telemetri gönderir ve Tehdit Yanıtı eylemlerini gerçekleştirir. Yerleşik aracı şunları destekler:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) sürüm 7.1 veya öncesi
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Kaspersky Endpoint Security ile Detection and Response çözümünü çeşitli yapılandırmalarla kullanabilirsiniz, örneğin [EDR Optimum+MDR].

MDR ve EDR Optimum lisanslama

Kaspersky Endpoint Security, Kaspersky Managed Detection and Response (MDR) ve Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) çözümlerinin işlevselliğini destekler. Kaspersky Endpoint Security'yi bu çözümlerle birlikte çeşitli yapılandırmalarda kullanabilir ve özel gereksinimlerinizi karşılayan özel bir koruma sistemi oluşturabilirsiniz. Bunu yapmak için, çözümlerin her biri için bir lisans satın almanız gerekir. Lisans, tek bir çözümü (örneğin sadece MDR Eklentisi) veya [EDR Optimum+MDR] Eklentisi gibi birkaç çözümü kullanma hakkını kapsayabilir.

MDR ve EDR Optimum aşağıdaki lisanslama yöntemlerini destekler:

- MDR ve EDR Optimum işlevselliği, Kaspersky Endpoint Security for Windows lisansına dahildir.

  Bu işlevsellik, Kaspersky Endpoint Security for Windows etkinleştirildikten hemen sonra kullanılabilir. Yalnızca bir anahtar eklemeniz gerekir.

- MDR veya EDR Optimum için ayrı lisanslar vardır (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  İşlevsellik, MDR Eklentisi, EDR Optimum Eklentisi veya [EDR Optimum+MDR] Eklentisi için ayrı bir anahtar eklendikten sonra kullanılabilir olacaktır. Sonuç olarak, bilgisayara iki anahtar eklenir: Kaspersky Endpoint Security için bir anahtar ve MDR veya EDR Optimum için bir anahtar. Kaspersky Endpoint Security anahtarı ilk eklenecek anahtar olmalıdır.

Kaspersky Endpoint Security, MDR ve EDR Optimum lisanslaması için yalnızca bir *etkin anahtar* eklenmesine izin verir. Bu nedenle, bu çözümlerin her ikisini de etkinleştirmeniz gerekiyorsa, her çözüm için ayrı bir anahtar yerine bir [EDR Optimum+MDR] Add-on anahtarı eklemeniz gerekir. Ayrıca bir *rezerve anahtar* da ekleyebilirsiniz.

MDR'yi dağıtırken bir BLOB dosyası kullandıysanız, MDR'yi etkinleştirmek için ayrı bir anahtara ihtiyacınız yoktur. BLOB dosyası zaten lisans bilgilerini içerir.

Çözümlerin ilk kez lisanslaması

MDR ve EDR Optimum ilk kez dağıtıldığında, çözümler Kaspersky Endpoint Security uygulamasıyla aynı şekilde etkinleştirilir. *Anahtar ekle* görevini kullanarak bir anahtar ekleyebilir veya otomatik anahtar dağıtım işlevini kullanabilirsiniz. Lisans anahtarı uygulamaya ikinci bir etkin anahtar olarak veya ilgili onay kutusunu seçerseniz rezerve anahtar olarak eklenir.

Bir lisanstan diğerine geçiş

Kuruluşunuzda bu çözümlerden biri zaten kullanılıyorsa ve ilgili anahtar uygulamaya eklenmişse, yeni yapılandırmanın lisanslanmasıyla ilgili bazı özel hususlar vardır. Farklı bir lisansa geçerken, uygulama yeni anahtarı uygulamaya eklemez, bunun yerine mevcut anahtarı yeni anahtarla değiştirir. Bunun nedeni, uygulamanın MDR ve EDR Optimum'u etkinleştirmek için yalnızca bir anahtar eklemesine izin veren kısıtlamadır.

Örneğin, kuruluşunuzda [EDR Optimum+MDR] çözümünün kurulu olduğunu ve MDR Eklentisinin yapılandırmasına geçmeye karar verdiğinizi varsayalım. Yeni yapılandırmaya geçmek için [EDR Optimum+MDR] Add-on anahtarını MDR Eklentisinin anahtarıyla değiştirmeniz gerekir.

EDR Optimum ve MDR için ayrı bir lisans ([EDR Optimum+MDR] Eklentisi) artık mevcut değildir. Bu çözümlerin her ikisini de kullanmak istiyorsanız, MDR'yi bir BLOB dosyası kullanarak ve EDR Optimum'u bir lisans anahtarıyla etkinleştirmeniz gerekir.

Otomatik anahtar dağıtım özelliği ile uygulama, aynı sayıda çözümü kapsayan lisans anahtarlarını reddeder. Yani, bir EDR Optimum Eklenti anahtarı eklediyseniz, bu anahtarı bir MDR Eklenti anahtarıyla değiştiremezsiniz. Ancak, EDR Optimum Eklenti anahtarını bir [EDR Optimum+MDR] Eklenti anahtarı ile değiştirebilirsiniz. Uygulama ayrıca bir MDR Eklenti anahtarını bir EDR Eklenti anahtarıyla değiştirmeye çalışırsanız anahtarları reddeder. Bir anahtarı değiştirmek için *Anahtar ekle* görevini çalıştırabilirsiniz. *Anahtar ekle* görevi, lisans anahtarlarının herhangi bir sayıda çözümle değiştirilmesine olanak tanır.

Bir [EDR Optimum+MDR] Add-on rezerve anahtarı eklediyseniz, bir EDR Optimum Eklentisi veya MDR Eklentisi için bir etkin anahtarı doğru şekilde eklemek için, önce rezerve anahtarını bir EDR Optimum Eklentisi veya MDR Eklentisi anahtarıyla değiştirmeniz veya alternatif olarak rezerve anahtarını kaldırmanız ve ardından etkin anahtarı değiştirmeniz gerekir.

Üçüncü taraf EDR çözümleriyle uyumluluk

Kaspersky Endpoint Security'yi, iş istasyonlarını ve sunucuları üçüncü taraf EDR çözümleriyle birlikte korumak için kullanabilirsiniz. Hatalı pozitif sonuçları ortadan kaldırmak için, Kaspersky Endpoint Security ve Network Agent'ın yürütülebilir dosyalarını üçüncü taraf EDR çözümünüzün güvenilir bölgelerine eklemenizi öneririz.

Üçüncü taraf EDR çözümleriyle uyumluluk için güvenilir bölge

	Kaspersky Endpoint Security for Windows	Kaspersky Security Center Network Agent
Çalışma klasörü	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Yürütülebilir dosyalar	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent, gelişmiş tehditleri tespit etmek için uygulama ile diğer Kaspersky çözümleri (örneğin Kaspersky Sandbox) arasında etkileşimi destekler. Kaspersky çözümleri, Kaspersky Endpoint Agent'ın belirli sürümleri ile uyumludur.

Kaspersky Endpoint Agent'ı Kaspersky çözümlerinin bir parçası olarak kullanmak için bu çözümleri karşılık gelen bir lisans anahtarıyla etkinleştirmeniz gerekir.

Kullandığınız yazılım çözümüne dahil olan Kaspersky Endpoint Agent ve bağımsız çözüm hakkında eksiksiz bilgi almak için lütfen ilgili ürünün Yardım Kılavuzuna bakın:

- Kaspersky Anti Targeted Attack Platform Yardım
- Kaspersky Sandbox Yardım
- Kaspersky Endpoint Detection and Response Optimum Yardım
- Kaspersky Managed Detection and Response Yardım

Kaspersky Endpoint Security 11.2.0 - 11.8.0 sürümleri için dağıtım kiti Kaspersky Endpoint Agent'ı içerir. Kaspersky Endpoint Security for Windows'u yüklerken Kaspersky Endpoint Agent'ı seçebilirsiniz. Sonuç olarak, bilgisayarınıza iki uygulama yüklenecektir: KEA ve KES. Kaspersky Endpoint Security 11.9.0'da Kaspersky Endpoint Agent dağıtım paketi artık Kaspersky Endpoint Security dağıtım kitinin bir parçası değildir.

KEA sürümlerinin (KES'in bir parçası olarak) KES sürümleriyle uyumu

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky, tüm Detection and Response işlemlerini Kaspersky Endpoint Agent yerine Kaspersky Endpoint Security bütünleşik aracısıyla çalışmaya geçiriyor. Kaspersky, bu çözümler için kademeli olarak destek ekliyor ve Kaspersky Endpoint Agent'ı kullanımdan kaldırıyor (aşağıdaki tabloya bakın). Uygulama, 12.1 sürümünden itibaren tüm Detection and Response çözümlerini desteklemektedir. Ayrıca, 12.1 sürümünden itibaren uygulama artık Kaspersky Endpoint Agent ile uyumlu değildir ve bu iki uygulamanın aynı bilgisayara aynı anda yüklenmesi artık mümkün değildir.

Kaspersky Endpoint Security sürümü	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (Endpoint Detection and Response Expert bileşeni)	Kaspersky Anti Targeted Attack Platform (Network Detection and Response Expert bileşeni)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent
12.6	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**

[KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi

Kaspersky Endpoint Security, Detection and Response çözümleriyle çalışmak için bütünleşik aracılara sahiptir. Bu çözümlerle çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok. Kaspersky Endpoint Agent yüklü bilgisayarlara Kaspersky Endpoint Security dağıttığınızda, Detection and Response çözümleri Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır.

Kaspersky Endpoint Security 11.2.0 - 11.8.0 sürümleri için dağıtım kiti Kaspersky Endpoint Agent'ı içerir. Kaspersky Endpoint Security for Windows'u yüklerken Kaspersky Endpoint Agent'ı seçebilirsiniz. Sonuç olarak, bilgisayarınıza iki uygulama yüklenecektir: KEA ve KES. Kaspersky Endpoint Security 11.9.0'da Kaspersky Endpoint Agent dağıtım paketi artık Kaspersky Endpoint Security dağıtım kitinin bir parçası değildir.

[KES+KEA] yapılandırmasını [KES+bütünleşik aracı]'ya aktarmak şu adımları içerir:

1. **Kaspersky Security Center'a yükseltme**

   Kullanıcı bilgisayarlarındaki Ağ Aracısı ve Web Console dahil tüm Kaspersky Security Center bileşenlerini sürüm 13.2 veya üstüne yükseltin.

2. **Kaspersky Endpoint Security web eklentisini yükseltme**

   Kaspersky Security Center Web Console'da, Kaspersky Endpoint Security web eklentisini 11.7.0 veya daha yüksek bir sürüme sürümüne yükseltin. EDR Optimum ve Kaspersky Sandbox bileşenlerini yönetmek için mutlaka Web Console kullanmanız gerekir.

Kaspersky Anti Targeted Attack Platform (EDR)'yi kullanmak için Kaspersky Endpoint Security sürüm 12.1 veya üstü için bir web eklentisine ihtiyacınız olacaktır.

Kaspersky Anti Targeted Attack Platform (NDR)'yi kullanmak için Kaspersky Endpoint Security sürüm 12.7 veya üstü için bir web eklentisine ihtiyacınız olacaktır.

3 İlkelerin ve görevlerin taşınması

Kaspersky Endpoint Agent ayarlarını Kaspersky Endpoint Security for Windows'a taşımak için Kaspersky Endpoint Agent İlke ve Görev Geçiş Sihirbazını kullanın.

Bu, yeni bir Kaspersky Endpoint Security ilkesi oluşturur. Yeni ilke *Etkin değil* durumundadır. İlkeyi uygulamak için ilke özelliklerini açın, Kaspersky Security Network Bildirimi'ni kabul edin ve durumu *Etkin* olarak ayarlayın.

4 Lisanslama işlevleri

Kaspersky Endpoint Security for Windows ve Kaspersky Endpoint Agent'ı etkinleştirmek için ortak bir Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security lisansı kullanıyorsanız, EDR Optimum işlevi uygulama 11.7.0 sürümüne yükseltildikten sonra otomatik olarak etkinleştirilecektir. Başka bir şey yapmanız gerekmez.

EDR Optimum işlevini etkinleştirmek için bağımsız bir Kaspersky Endpoint Detection and Response Optimum Eklentisi lisansı kullanıyorsanız, EDR Optimum Eklentisi anahtarının Kaspersky Security Center veri havuzuna eklendiğinden ve otomatik lisans anahtarı dağıtım işlevinin etkinleştirildiğinden emin olmalısınız. EDR Optimum işlevi, uygulamayı 11.7.0 sürümüne yükselttikten sonra otomatik olarak etkinleştirilir.

Kaspersky Endpoint Agent'ı etkinleştirmek için Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security lisansı ve Kaspersky Endpoint Security for Windows'u etkinleştirmek için farklı bir lisans kullanıyorsanız, Kaspersky Endpoint Security for Windows anahtarını, ortak Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security anahtarıyla değiştirmelisiniz. Anahtarı, *Anahtar ekle* görevini kullanarak değiştirebilirsiniz.

Kaspersky Sandbox işlevini etkinleştirmeniz gerekmez. Kaspersky Sandbox işlevi, Kaspersky Endpoint Security for Windows'u yükseltip etkinleştirdikten hemen sonra kullanılabilir.

Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olarak Kaspersky Endpoint Security'yi etkinleştirmek için yalnızca Kaspersky Anti Targeted Attack Platform lisansı kullanılabilir. EDR (KATA) işlevi, uygulamayı 12.1 sürümüne yükselttikten sonra otomatik olarak etkinleştirilir. Başka bir şey yapmanız gerekmez.

5 Kaspersky Endpoint Security uygulamasını yükseltme

Uygulamayı yükseltmek ve EDR Optimum ve Kaspersky Sandbox işlevselliğini taşımak için bir uzaktan yükleme görevi önerilir.

Uygulamayı bir uzaktan yükleme görevi kullanarak yükseltmek için şu ayarları düzenlemeniz gerekir:

- Kurulum paketinin ayarlarında Detection and Response çözümleri için bileşenleri seçin.
- Kurulum paketinin ayarlarında Kaspersky Endpoint Agent bileşenini hariç tut (Kaspersky Endpoint Security for Windows sürüm 11.2.0 - 11.8.0 için).
- Kaspersky Endpoint Agent'a erişimi kısıtlamak için Parola Koruması etkinleştirilmişse, *Uygulamayı uzaktan yükle* görevinin ayarlarına uygulama kaldırma parolasını girin. Kaspersky Security Center Linux 15.1 ile başlayarak kaldırma parolasını girebilirsiniz.

Uygulamayı, şu yöntemleri kullanarak da güncellemeniz mümkündür:

- Kaspersky güncelleme hizmetini kullanma (Sorunsuz Güncelleme – SMU).
- Kurulum Sihirbazını kullanarak yerel olarak.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent uygulamasının yüklü olduğu bir bilgisayarda uygulama yükseltilirken, bileşenlerin otomatik olarak seçilmesini destekler. Bileşenlerin otomatik seçimi, uygulamayı yükselten kullanıcı hesabının izinlerine bağlıdır.

Kaspersky Endpoint Security'yi sistem hesabı (SYSTEM) altındaki EXE veya MSI dosyasını kullanarak yükseltiyorsanız, Kaspersky Endpoint Security, Kaspersky çözümlerinin geçerli lisanslarına erişim kazanır. Dolayısıyla, bilgisayarda örneğin Kaspersky Endpoint Agent yüklü ve EDR Optimum çözümü etkinleştirildiyse, Kaspersky Endpoint Security yükleyicisi bileşen setini otomatik olarak yapılandırır ve EDR Optimum bileşenini seçer. Bu, Kaspersky Endpoint Security'nin bütünleşik aracıyı kullanmaya geçmesini sağlar ve Kaspersky Endpoint Agent'ı kaldırır. MSI yükleyicisinin sistem hesabı (SYSTEM) altında çalıştırılması genellikle Kaspersky güncelleme hizmeti (SMU) aracılığıyla yükseltme yapılırken ya da Kaspersky Security Center aracılığıyla bir yükleme paketi dağıtılırken gerçekleştirilir.

Kaspersky Endpoint Security'yi ayrıcalıklı olmayan bir kullanıcı hesabı altında bir MSI dosyası kullanarak yükseltiyorsanız, Kaspersky Endpoint Security'nin Kaspersky çözümlerinin geçerli lisanslarına erişimi olmaz. Bu durumda Kaspersky Endpoint Security, bileşenleri Kaspersky Endpoint Agent yapılandırmasına göre otomatik olarak seçer. Bundan sonra, Kaspersky Endpoint Security' bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

6. **Bilgisayarı yeniden başlat**

   Uygulamayı yerleşik aracıyla yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatın. Uygulamayı yükseltirken, yükleyici bilgisayar yeniden başlatılmadan önce Kaspersky Endpoint Agent'ı kaldırır. Bilgisayar yeniden başlatıldıktan sonra yükleyici yerleşik aracıyı ekler. Bu, Kaspersky Endpoint Security'nin bilgisayar yeniden başlatılana kadar EDR ve Kaspersky Sandbox işlevlerini yerine getirmeyeceği anlamına gelir.

7. **Kaspersky Endpoint Detection and Response Optimum ve Kaspersky Sandbox'ın durumunu kontrol etme**

   Yükseltmeden sonra bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

   - Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
   - *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin.
   - Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.

   - *Uygulama bileşenlerinin durumu hakkında rapor* seçeneğini kullanarak EDR Optimum işlevselliğinin etkinleştirildiğinden emin olun. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, EDR Optimum'un otomatik lisans anahtarı dağıtım işlevinin açık olduğundan emin olun.

Kaspersky Endpoint Agent için İlke ve Görev Geçişi

Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş için bir sihirbaz içerir. Şu çözümler için ilke ve görev ayarlarını taşıyabilirsiniz:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş sihirbazı yalnızca Web Console ve Cloud Console'da çalışır. Yönetim Konsolu'nda (MMC), standart Kaspersky Security Center İlke ve Görev Geçiş Sihirbazını kullanarak yalnızca Kaspersky Anti Targeted Attack Platform (EDR) çözümü için ayarları taşıyabilirsiniz.

Kaspersky Endpoint Agent'ı önce bir bilgisayarda Kaspersky Endpoint Security'ye geçirmeniz, sonra bunu bir grup bilgisayarda yapmanız ve ardından geçişi kuruluşun tüm bilgisayarlarında tamamlamanız önerilir.

İlke ve görev ayarlarını Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçirmek için,

Web Console ana penceresinde, **İşlemler** → **Kaspersky Endpoint Agent'tan Geçiş** seçimini yapın.

Böylece ilke ve görev geçiş sihirbazı çalıştırılır. Sihirbazın talimatlarını uygulayın.

1. Adım. İlke geçişi

Geçiş Sihirbazı, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent ilkelerinin ayarlarını birleştiren yeni bir ilke oluşturur. İlke listesinden, ayarlarını Kaspersky Endpoint Security ilkesiyle birleştirmek istediğiniz Kaspersky Endpoint Agent ilkelerini seçin. Ayarları birleştirmek istediğiniz Kaspersky Endpoint Security ilkesini seçmek için Kaspersky Endpoint Agent ilkesine tıklayın. Doğru ilkeleri seçtiğinizden emin olun ve sonraki adıma geçin.

2. Adım. Görev geçişi

Geçiş Sihirbazı, Kaspersky Endpoint Security için yeni görevler oluşturur. Görev listesinden, Kaspersky Endpoint Security ilkesi için oluşturmak istediğiniz Kaspersky Endpoint Agent görevlerini seçin. Sihirbaz, Kaspersky Endpoint Detection and Response ve Kaspersky Sandbox görevlerini destekler. Bir sonraki adıma geçin.

3. Adım Sihirbazı tamamlama

Sihirbazı tamamlayın. Sonuç olarak, sihirbaz şunları yapar:

- Yeni bir Kaspersky Endpoint Security ilkesi oluşturur.

  İlke, Kaspersky Endpoint Security'den ve Kaspersky Endpoint Agent'tan gelen ayarları birleştirir. Bu ilkeye *<Kaspersky Endpoint Security ilke adı> & <Kaspersky Endpoint Agent ilke adı>* adı verilir. Yeni ilke *Etkin değil* durumundadır. Devam etmek için Kaspersky Endpoint Agent ve Kaspersky Endpoint Security ilkelerinin durumlarını *Etkin değil* olarak değiştirtin ve yeni birleştirilmiş ilkeyi etkinleştirin.

  Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçiş yapıldıktan sonra, lütfen yeni ilkenin Yönetim Sunucusu kurulumuna veri aktarımı (karantina dosyası verileri ve tehdit geliştirme zinciri verileri) işlevine sahip olduğundan emin olun. bir Kaspersky Endpoint Agent ilkesinden veri aktarımı parametresi değerleri taşınmaz.

Kaspersky Endpoint Agent'tan Kaspersky Anti Targeted Attack Platform (EDR) çözümü için Kaspersky Endpoint Security'ye geçiş yaparken, bilgisayarı Central Node sunucularına bağlana sırasında hatalarla karşılaşabilirsiniz. Bunun nedeni, Web Console geçiş sihirbazının şu ilke ayarlarını atlaması ve bunları geçirmemesidir:

- Ayarlar değişiklik yasağı **KATA sunucularına bağlantı** ("kilit").

  Varsayılan olarak ayarlar değiştirilebilir ("kilit" açıktır). Bu nedenle ayarlar bilgisayarda uygulanmaz. Ayarların değiştirilmesi yasaklanmalı ve "kilit" kapatılmalıdır.

- Kripto konteyneri.

  Central Node sunucularına bağlanmak için iki yönlü kimlik doğrulama kullanıyorsanız, kripto konteynerini yeniden eklemeniz gerekir. Geçiş sihirbazı sunucunun TLS sertifikasının geçişini doğru şekilde gerçekleştirir.

Yönetim Konsolu (MMC) içeriğinde bulunan İlke ve Görev Geçiş Sihirbazı, Kaspersky Anti Targeted Attack Platform (EDR) çözümü için tüm ayarların geçişini gerçekleştirir.

- Yeni Kaspersky Endpoint Security görevleri oluşturur.

  Yeni görevler, Kaspersky Endpoint Detection and Response ve Kaspersky Sandbox için Kaspersky Endpoint Agent görevlerinin kopyalarıdır. Aynı zamanda, Sihiirbaz Kaspersky Endpoint Agent görevlerini değiştirmeden bırakır.

Yönetim Konsolu'nda (MMC) ilke ve görev ayarlarını Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye taşıma (yalnızca KATA (EDR) için)

1. Yönetim Konsolu'nda, Yönetim Sunucusunu seçin ve içerik menüsünü açmak için sağ tıklayın.
2. **Tüm görevler → İlke ve görevler toplu dönüştürme sihirbazı** seçimini yapın.

İlkeler ve Görevler Toplu Dönüştürme Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. İlke ve görevlerini dönüştürmeniz gereken uygulamayı seçme

Bu adımda Kaspersky Endpoint Security for Windows'u seçmeniz gerekir. Bir sonraki adıma geçin.

2. Adım. İlkelerin dönüştürülmesi

Geçiş Sihirbazı, Kaspersky Endpoint Agent ilke ayarlarının taşınacağı yeni bir Kaspersky Endpoint Security ilkesi oluşturur. İlkeler listesinden, ayarlarını Kaspersky Endpoint Security ilkesine aktarmak istediğiniz Kaspersky Endpoint Agent ilkelerini seçin. Bir sonraki adıma geçin.

Geçiş Sihirbazı ilkeleri dönüştürmeye başlayacaktır. İlke dönüştürme sırasında Geçiş Sihirbazı, Kaspersky Security Network Bildirimi kabul etmenizi ister. Yeni ilkeler *<İlke adı> (dönüştürülmüş)* şeklinde adlandırılır.

3. Adım. Görevlerin dönüştürülmesi

Bu adımı atlayın. Sihirbaz, yalnızca Kaspersky Endpoint Detection and Response Optimum ve Kaspersky Sandbox görevlerini destekler. Bu bileşenlerin yönetimi yalnızca Web Console'da mevcuttur. Bir sonraki adıma geçin.

4. Adım Sihirbazı tamamlama

Sihirbazı tamamlayın. Sihirbazın sonucunda yeni bir Kaspersky Endpoint Security ilkesi oluşturulacaktır.

Endpoint Detection and Response Agent (EDR Agent)

Kaspersky Endpoint Security 12.3 for Windows'tan başlayarak, uygulama Endpoint Detection and Response Agent (EDR Agent) yapılandırmasını içerir. *Endpoint Detection and Response Agent*, Kaspersky'nin aşağıdaki Detection and Response çözümlerini desteklemek için kuruluşun BT altyapısındaki bireysel iş istasyonlarına ve sunuculara yüklenen bir uygulamadır:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (12.6 sürümünden itibaren)
- Kaspersky Anti Targeted Attack Platform (NDR) (12.7 sürümünden itibaren)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (12.11 sürümünden itibaren)

EDR Agent, Kaspersky Endpoint Detection and Response Expert (cloud) çözümüyle entegrasyonu desteklemez.

EDR Agent bu bilgisayarlarda çalışan işlemleri, açık ağ bağlantılarını ve değiştirilen dosyaları sürekli olarak izler. Uygulamanın koruma ve kontrol bileşenleri EDR Agent için mevcut değildir.

EDR Agent üçüncü taraf EPP uygulamalarıyla uyumludur. Bu, Kaspersky'nin Detection and Response özelliğinin yanı sıra üçüncü taraf altyapı güvenlik araçlarını da kullanmanıza olanak tanır.

EDR Agent'ı dağıtmak için bilgisayarda Ağ Aracısı yüklü olmalı ve bilgisayar Kaspersky Security Center konsoluna eklenmelidir. EDR Agent'ın Kaspersky Security Center ile etkileşimini etkinleştirmek için Kaspersky Endpoint Security for Windows yönetim eklentisini yüklemeniz gerekir. EDR Agent ayarlarını bir grup ilkesi kullanarak belirleyebilirsiniz. EDR Agent'ı entegre etmek için, entegrasyonu uygun ilke bölümlerinde yapılandırmanız gerekir.

Kaspersky Detection and Response çözümlerini desteklemek için aşağıdaki Kaspersky uygulamaları altyapıya yüklenmelidir:

	• Ağ Aracısı • EDR Agent
Endpoint	
	Kaspersky Endpoint Security for Windows Yönetim Eklentisi
Kaspersky Security Center	

Detection and Response çözümleri: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

EDR Agent'ı Yükleme

Kaspersky Endpoint Security, Kaspersky Detection and Response çözümleri için Endpoint Detection and Response Agent (EDR Agent) yapılandırmasında aynı şekilde yüklenir.

EDR Agent bilgisayara şu yollardan biri kullanılarak yüklenebilir:

- Kaspersky Security Center kullanarak uzaktan.
- Kurulum Sihirbazını kullanarak yerel olarak.
- Komut satırında yerel olarak (yalnızca KATA (EDR) ve EDR Expert (on-premises) için).

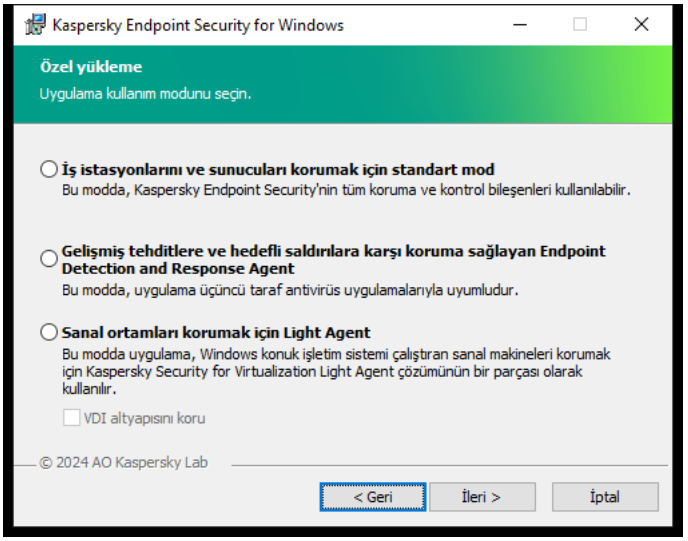
EDR Agent'ı yüklemek için yükleme paketi ayarlarında veya Kurulum Sihirbazı sırasında uygun yapılandırmayı seçmelisiniz.

Kurulum Sihirbazı kullanılarak EDR Agent kurulumu

1. Dağıtım noktası klasörünü kullanıcının bilgisayarına kopyalayın.
2. setup_kes.exe dosyasını çalıştırın.

   Kurulum Sihirbazı başlatılır.

Kaspersky Endpoint Security yapılandırması



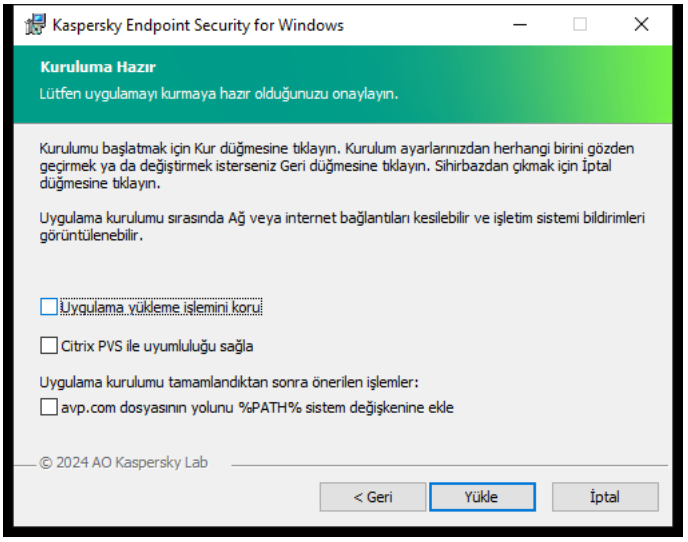
Uygulama yapılandırmasının seçilmesi

Endpoint Detection and Response Agent yapılandırmasını seçin. Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.

Kaspersky Endpoint Security bileşenleri

Kurmak istediğiniz bileşenleri seçin. Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz. Bunu yapmak için, Kurulum Sihirbazını tekrar çalıştırmanız ve kullanılabilir bileşenleri değiştirmeyi seçmeniz gerekir.

Gelişmiş ayarlar



Gelişmiş uygulama kurulum ayarları

Uygulama yükleme işlemini koru. Kurulum koruması, dağıtım paketinin zararlı programlarla değiştirilmesine karşı koruma, Kaspersky Endpoint Security yükleme klasörüne erişimi engelleme ve uygulama anahtarlarını içeren sistem kayıt defteri bölümüne erişimi engellemeyi içerir. Ancak, uygulama yüklenemiyorsa (örneğin, Windows Remote Desktop yardımıyla uzaktan yükleme gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız önerilir.

Citrix PVS ile uyumluluğu sağla. Kaspersky Endpoint Security'yi sanal bir makineye yüklemek için Citrix Provisioning Services desteğini etkinleştirebilirsiniz.

avp.com dosyasının yolunu %PATH% sistem değişkenine ekle. Komut satırı arabiriminin uygun kullanımı için kurulum yolunu %PATH% değişkenine ekleyebilirsiniz.

EDR Agent'ı komut satırında yükleme (yalnızca KATA (EDR) ve EDR Expert (on-premises) 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 /pSTANDALONEMODE=1 [/s]
```

veya

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

Sonuç olarak, Kaspersky Anti Targeted Attack Platform (EDR) veya Kaspersky Endpoint Detection and Response Expert (on-premises) ile entegrasyon için EDR Agent uygulaması bilgisayara yüklenir. `status` komutunu kullanarak uygulamanın yüklenip yüklenmediğini ve uygulama ayarlarını kontrol edebilirsiniz.

Yönetim Konsolu (MMC) kullanılarak EDR Agent kurulumu

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacından **Gelişmiş** → **Uzaktan kurulum** → **Kurulum paketleri** klasörünü seçin.

   Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.
3. Kurulum paketinin özelliklerini açın.

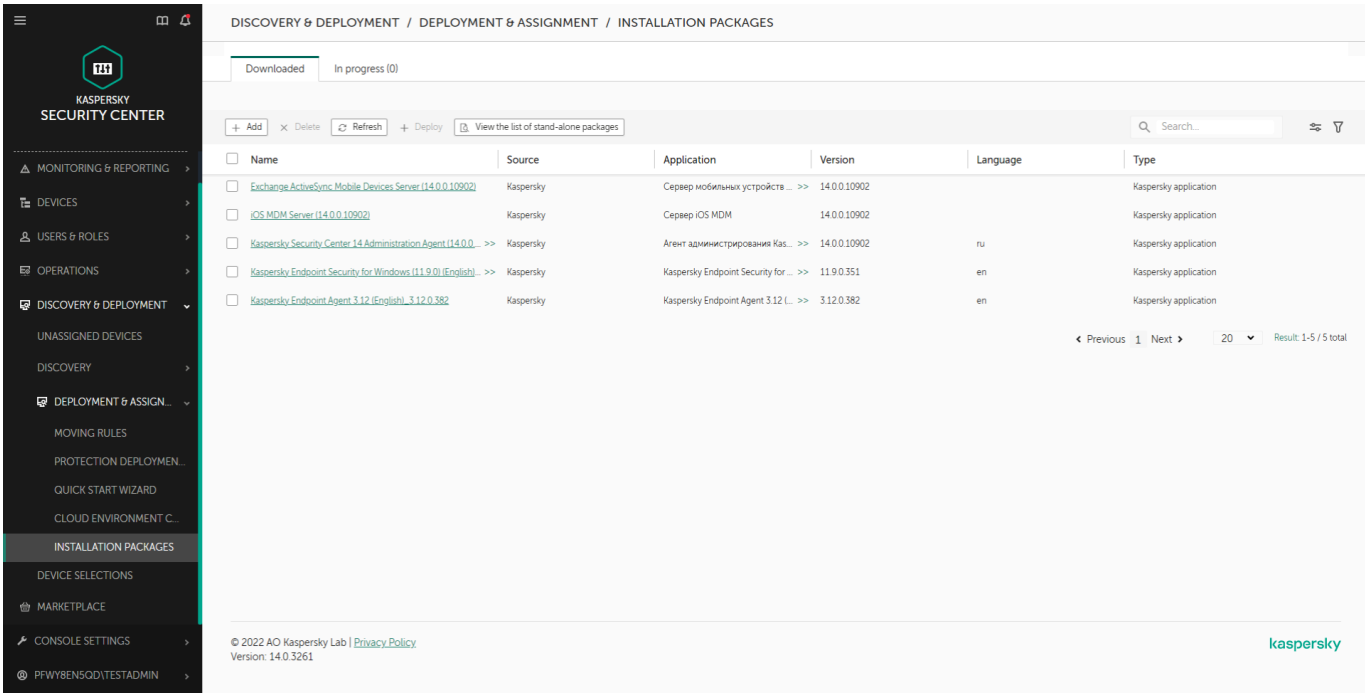
   Gerekirse yeni bir kurulum paketi oluşturun.
4. **Koruma bileşenleri** bölümüne gidin.
5. **Gelişmiş tehditlere ve hedefli saldırılara karşı koruma sağlayan Endpoint Detection and Response Agent** yapılandırmasını seçin. Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.
6. Kurmak istediğiniz bileşenleri seçin.

   Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz.
7. Değişikliklerinizi kaydedin.
8. Bir uzaktan kurulum görevi oluşturun. Görev özelliklerinde, oluşturduğunuz yükleme paketini seçin.

Web Console. kullanılarak EDR Agent kurulumu

1. Web Console'un ana penceresinden **Keşif ve dağıtım** → **Dağıtım ve atama** → **Kurulum paketleri** seçimini yapın.

Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.



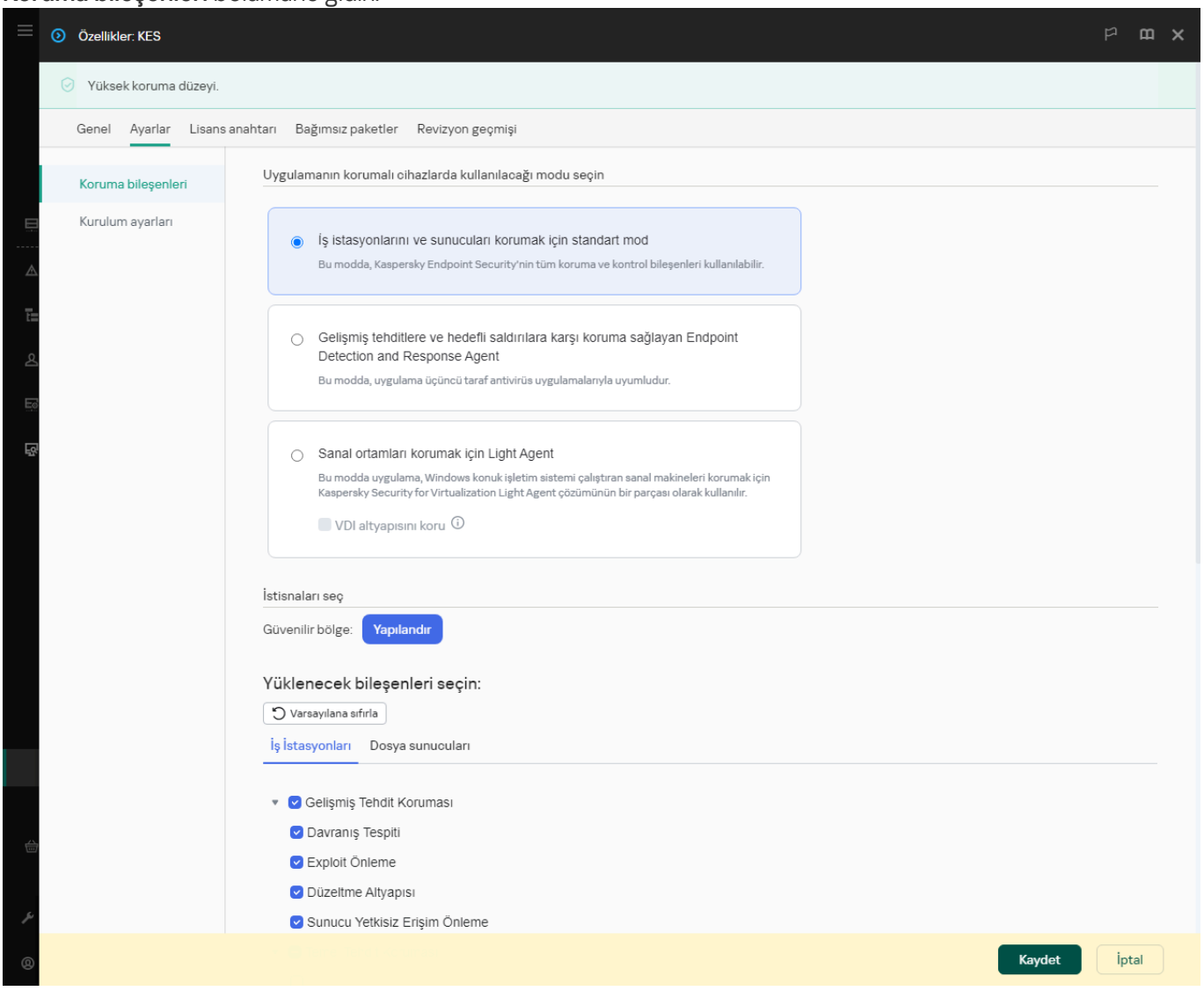
Kurulum paketlerinin listesi

2. Kurulum paketinin özelliklerini açın.

   Gerekirse yeni bir kurulum paketi oluşturun.

3. **Ayarlar** sekmesini seçin.

4. **Koruma bileşenleri** bölümüne gidin.



Kurulum paketine dahil olan bileşenler

5. **Endpoint Detection and Response Agent** yapılandırmasını seçin. Bu yapılandırmada, yalnızca Detection and Response çözümlerine destek sağlayan bileşenleri yükleyebilirsiniz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ve KUMA. Bu yapılandırma, kuruluşunuzda Kaspersky Detection and Response çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.

6. Kurmak istediğiniz bileşenleri seçin.

   Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz.

7. Değişikliklerinizi kaydedin.

8. Bir uzaktan kurulum görevi oluşturun. Görev özelliklerinde, oluşturduğunuz yükleme paketini seçin.

Sonuç olarak, EDR Agent kullanıcının bilgisayarına yüklenir. Uygulamanın arabirimini kullanabilirsiniz, bildirim alanında uygulamanın bir simgesi görüntülenir .

Kaspersky Security Center'da, EDR Agent yapılandırmasında yüklü uygulamanın bulunduğu bilgisayar *Kritik* durumuna - sahiptir. Bilgisayar, Dosya Tehdidi Koruması bileşeni eksik olduğu için bu duruma sahiptir. Herhangi bir işlem yapmanıza gerek yoktur.

Yükleyici bilgisayarda uyumsuz yazılım bulduğu için EDR Agent'ı üçüncü taraf EPP uygulaması olan bir bilgisayara yükleyemediyseniz, uyumsuz yazılım kontrolünü atlayabilirsiniz.



EDR Agent'ın ana penceresi

Şimdi Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) veya Kaspersky Anti Targeted Attack (NDR) çözümü ile entegrasyonu yapılandırmanız gerekir. Ayrıca uygulamanın gelişmiş ayarlarını belirleyebilir ve örneğin güvenilir bir bölge oluşturabilir veya uygulamanın arabirimini gizleyebilirsiniz. Aşağıdaki bölümlerdeki ayarlar kullanılabilir:

- Kaspersky Security Network
- Uygulama Ayarları
- Ağ ayarları
- İstisnalar
- Raporlar

- Arabirim
- Ayarları yönet

EDR Agent'ı MDR ile entegre etme

EDR Agent, kuruluşun BT altyapısındaki iş istasyonlarına ve sunuculara yüklenir. EDR Agent verileri işler ve Kaspersky Security Network akışları üzerinden Kaspersky Managed Detection and Response'a gönderir.

Kaspersky Managed Detection and Response bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için yeni bir güvenli bağlantı, yani bir *arka plan bağlantısı* kurmanız şarttır. Kaspersky Managed Detection and Response, çözümün dağıtımını yaparken, sizden bir arka plan bağlantısı kurmanızı ister. Arka plan bağlantısının kurulduğundan emin olun.

Web Console'da bir arka plan bağlantısı kurma

1. Web Console ana penceresinden **Ayarlar** → **Tümleştirme** seçimini yapın.
2. **Tümleştirme** bölümüne gidin.
3. **Tümleştirme için bir arka plan bağlantısı Etkin** iki durumlu düğmesini açık duruma getirin.
4. Değişikliklerinizi kaydedin.

Kaspersky Managed Detection and Response ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Managed Detection and Response bileşenini yükleme**

   MDR bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken seçebilirsiniz.

   > Managed Detection and Response bileşenini bilgisayarı yeniden başlatmadan *Uygulama bileşenlerini değiştir* görevini kullanarak yüklemek için görev ayarlarındaki **Uyumsuz üçüncü taraf uygulamaları denetle** seçeneğini devre dışı bırakmanız gerekir.

2. **Kaspersky Private Security Network'ü yapılandırma**

   > Kaspersky Security Center Cloud Console kullanıyorsanız bu adımı atlayın. Kaspersky Security Center Cloud Console, Kaspersky Private Security Network'ü, MDR eklentisi yüklenirken otomatik olarak yapılandırır.

   Kaspersky Private Security Network (KPSN), Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür.

   Yönetim Sunucusu özelliklerine Kaspersky Security Network yapılandırma dosyasını yükleyin. Kaspersky Security Network yapılandırma dosyası, MDR yapılandırma dosyasının ZIP arşivinde bulunur. ZIP arşivini Kaspersky Managed Detection and Response Konsolunda bulabilirsiniz. Kaspersky Private Security Network yapılandırılmasıyla ilgili ayrıntılar için lütfen Kaspersky Security Center Yardım içeriğine bakın. Kaspersky Security Network yapılandırma dosyasını bilgisayara komut satırından da yükleyebilirsiniz (aşağıdaki talimatlara bakın).

Kaspersky Private Security Network komut satırından nasıl yapılandırılır

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

   ```
   avp.com KSN /private <file name>
   ```

   burada `<file name>` Kaspersky Private Security Network ayarlarını içeren yapılandırma dosyasının (PKCS7 veya PEM dosya biçiminde) adıdır.

   Örnek:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Sonuç olarak Kaspersky Endpoint Security, dosyaların, uygulamaların ve web sitelerinin tanınırlığını belirlemek için Kaspersky Private Security Network'ü kullanacaktır. İlke ayarlarının **Kaspersky Security Network** bölümü şu çalışma durumunu gösterecektir: *Altyapı: Kaspersky Private Security Network*.

Managed Detection and Response bileşeninin çalışması için genişletilmiş KSN modunu etkinleştirmeniz gerekir.

3 Kaspersky Managed Detection and Responseu etkinleştirme

Kaspersky Endpoint Security for Windows 12.10 sürümünden itibaren, Managed Detection and Response işlevini etkinleştirmek için etkinleştirme koduna alternatif olarak bir anahtar dosyası da kullanabilirsiniz.

MDR (Kaspersky Managed Detection and Response Eklentisi) için ayrı bir lisans satın almanız gerekir.

Kaspersky Managed Detection and Response Eklentisi için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir. Bağımsız Managed Detection and Response işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

MDR işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

4 Managed Detection and Response bileşenini etkinleştirme

BLOB yapılandırma dosyasını Kaspersky Endpoint Security ilkesine yükleyin (aşağıdaki talimatlara bakın). BLOB dosyası, istemci kimliğini ve Kaspersky Managed Detection and Response lisansı hakkındaki bilgileri içerir. BLOB dosyası, MDR yapılandırma dosyasının ZIP arşivinde bulunur. ZIP arşivini Kaspersky Managed Detection and Response Konsolunda bulabilirsiniz. Bir BLOB dosyası hakkında ayrıntılı bilgi için lütfen Kaspersky Yönetilen Algılama ve Yanıt Yardım içeriğine bakın.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, geçerli bir lisansınız varsa BLOB dosyası eklemek Kaspersky Managed Detection and Response için kiracı olmadan isteğe bağlıdır.

Managed Detection and Response, Yönetim Konsolu (MMC) ile nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** seçimini yapın.
4. **Managed Detection and Response (Industrial CyberSecurity)** onay kutusunu seçin.

5. **Ayarlar** bloğunda, **Yükle**'a tıklayın ve Kaspersky Managed Detection and Response Konsolu'nda alınan BLOB dosyasını seçin. Dosya P7 uzantısına sahiptir.

   Varsayılan olarak, kullanıcının uygulama ayarlarını yönetmesine izin verilir ("asma kilit" açık durumdadır). İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın.

6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Managed Detection and Response bileşeni nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Managed Detection and Response** bölümüne gidin.
5. **Managed Detection and Response ETKİN** geçiş düğmesini açık duruma getirin.
6. **Yükle**'ye tıklayın ve Kaspersky Managed Detection and Response Konsolu'nda elde edilen BLOB dosyasını seçin. Dosya P7 uzantısına sahiptir.

   Varsayılan olarak, kullanıcının ilke ayarlarını yönetmesine izin verilir ("asma kilit" açık durumdadır). İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın.
7. Değişikliklerinizi kaydedin.

Managed Detection and Response bileşeni komut satırından nasıl etkinleştirilir

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

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

   Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Uygulama ayarlarını yapılandır** izninin olması gerekir.

Sonuç olarak Kaspersky Endpoint Security BLOB dosyasını doğrular. BLOB dosya doğrulaması, dijital imzanın ve lisans süresinin kontrol edilmesini kapsar. BLOB dosyası başarıyla doğrulanırsa Kaspersky Endpoint Security dosyayı indirir ve Kaspersky Security Center ile bir sonraki senkronizasyon sırasında dosyayı bilgisayara gönderir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Managed Detection and Response** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

5 Telemetri almak için uygulamanın diğer bileşenlerini yapılandırma

Managed Detection and Response bileşeninin çalışması için şu bileşenleri etkinleştirmeniz gerekir:

- Kaspersky Security Network (genişletilmiş mod).
- Davranış Tespiti.
- Exploit Önleme.
- Web Tehdidi Koruması.
- Posta Tehdidi Koruması.
- Dosya Tehdidi Koruması.
- Ağ Tehdidi Koruması.
- Güvenlik Duvarı.
- AMSI Koruması.
- Arka plan taraması.

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Managed Detection and Response** bölümüne gidin.
5. **Managed Detection and Response ETKİN** geçiş düğmesini açık duruma getirin.
6. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** seçimini yapın.
4. **Managed Detection and Response (Industrial CyberSecurity)** onay kutusunu seçin.
5. Değişikliklerinizi kaydedin.

EDR Agent'ı EDR (KATA) ile entegre etme

EDR Agent, kuruluşun BT altyapısındaki iş istasyonlarına ve sunuculara yüklenir. Bu bilgisayarlarda EDR Agent işlemleri, açık ağ bağlantılarını ve değiştirilen dosyaları sürekli olarak izler ve izleme verilerini Central Node bileşeniyle sunucuya gönderir.

EDR (KATA) ile entegre etmek için Endpoint Detection and Response (KATA) bileşenini etkinleştirmeniz ve EDR Agent'ı yapılandırmanız gerekir.

Endpoint Detection and Response (KATA) bileşeninin çalışması için şu şartlar sağlanmalıdır:

- Kaspersky Anti Targeted Attack Platform sürümleri 5.0–7.1.
- Kaspersky Security Center sürüm 14.2 veya üstü. Kaspersky Security Center'ın önceki sürümlerinde Endpoint Detection and Response (KATA) özelliğini etkinleştirmek mümkün değildir.

https://www.youtube.com/watch?v=cZzgtBoeC7k

Endpoint Detection and Response ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Endpoint Detection and Response (KATA)'yı etkinleştirme**

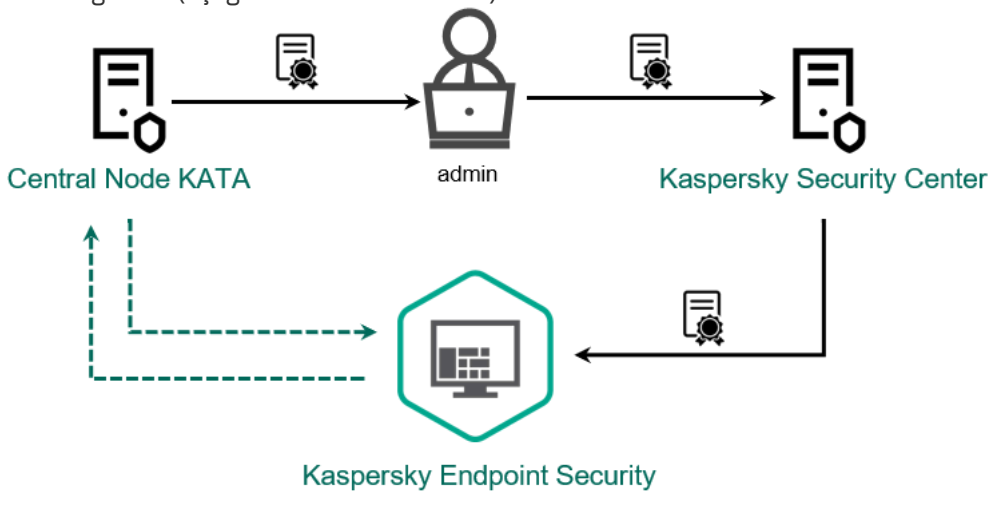
   EDR (KATA) (Kaspersky Endpoint Detection and Response (KATA) Eklentisi) için ayrı bir lisans satın almanız gerekir.

   Kaspersky Endpoint Detection and Response (KATA) için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir hale gelir. Bağımsız Endpoint Detection and Response (KATA) işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   EDR (KATA) işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

2. **Central Node'a bağlanma**

   Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security ile Central Node bileşeni arasında güvenilir bir bağlantı kurulmasını gerektirir. Güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası kullanmanız gerekir. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Ardından TLS sertifikasını Kaspersky Endpoint Security'ye eklemeniz gerekir (aşağıdaki talimatlara bakın).



Kaspersky Endpoint Security'ye TLS sertifikası ekleme

Kaspersky Endpoint Security varsayılan olarak yalnızca Central Node'un TLS sertifikasını kontrol eder. Bağlantıyı daha güvenli hale getirmek için, bilgisayarın Central Node üzerinde doğrulanmasını da etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu doğrulamayı etkinleştirmek için Central Node ve Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı açmanız gerekir. İki yönlü kimlik doğrulamayı kullanmak için ayrıca bir kripto konteynere ihtiyacınız olacaktır. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).

Yönetim Konsolu (MMC) kullanılarak bir Kaspersky Endpoint Security bilgisayarı Central Node'a nasıl bağlanır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Detection and Response → Endpoint Detection and Response Expert (on-premises)** seçimini yapın.
5. **Endpoint Detection and Response Expert (on-premises)** onay kutusunu seçin.
6. **Sunucu bağlantı ayarları** seçeneğine tıklayın.
7. Sunucu bağlantısını yapılandırın:
   - **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener.
   - **Sunucu TLS sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).
   - **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

     Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
8. **Tamam**'a tıklayın.
9. Central Node sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

   Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

10. Gerekirse telemetriyi yapılandırın.

11. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console kullanılarak bir Kaspersky Endpoint Security bilgisayarı Central Node'a nasıl bağlanır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (on-premises)** bölümüne gidin.

5. **Endpoint Detection and Response Expert (on-premises) ETKİN** iki durumlu düğmesini açık duruma getirin.

6. EDR'yi (KATA) yapılandırmak için çözümler listesinden **Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi)** seçimini yapın.

7. **Bağlantı ayarları** seçeneğine tıklayın.

8. Sunucu bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener.

   - **Sunucu sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım'daki talimatlara bakın).

   - **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

     Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

9. **Tamam**'a tıklayın.

10. Central Node sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

    Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

11. Gerekirse telemetriyi yapılandırın.

12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Sonuç olarak, bilgisayar Kaspersky Anti Targeted Attack Platform konsoluna eklenir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Endpoint Detection and Response Expert (on-premises)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

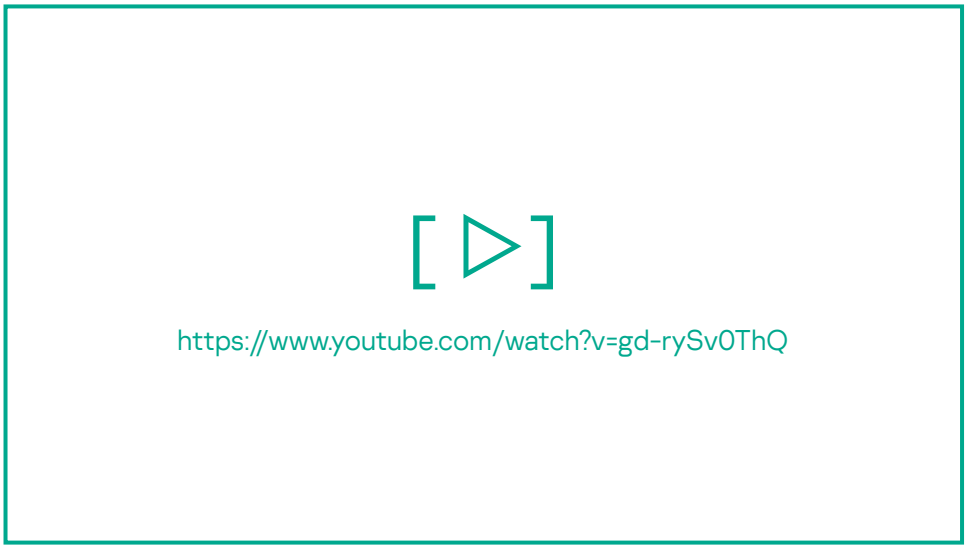
EDR Agent'ı NDR (KATA) ile entegre etme

EDR Agent, kuruluşun BT altyapısındaki iş istasyonlarına ve sunuculara yüklenir. Bu bilgisayarlarda EDR Agent işlemleri, açık ağ bağlantılarını ve değiştirilen dosyaları sürekli olarak izler ve izleme verilerini Central Node bileşeniyle sunucuya gönderir.

NDR (KATA) ile entegre etmek için Network Detection and Response (KATA) bileşenini etkinleştirmeniz ve EDR Agent'ı yapılandırmanız gerekir.

Network Detection and Response (KATA) bileşeninin çalışması için şu şartlar sağlanmalıdır:

- Kaspersky Anti Targeted Attack Platform sürüm 7.0 veya üzeri.
- Kaspersky Security Center sürüm 14.2 veya üstü. Kaspersky Security Center'ın önceki sürümlerinde Network Detection and Response (KATA) özelliğini etkinleştirmek mümkün değildir.



https://www.youtube.com/watch?v=gd-rySv0ThQ

Network Detection and Response (KATA) ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Network Detection and Response (KATA)'yı etkinleştirme**

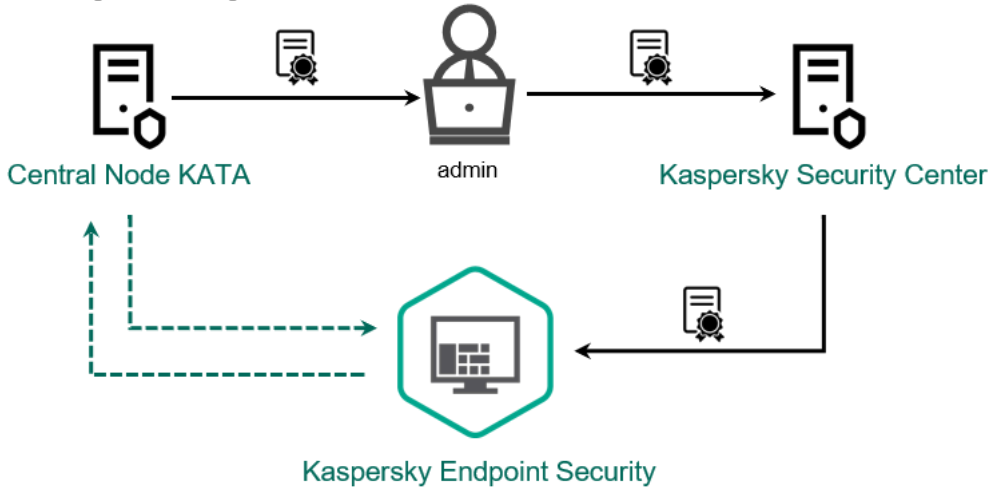
   NDR (KATA) (Kaspersky Network Detection and Response (KATA) Eklentisi) için ayrı bir lisans satın almanız gerekir.

   Kaspersky Network Detection and Response (KATA) için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir hale gelir. Bağımsız Network Detection and Response (KATA) işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   NDR (KATA) işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

2. **Central Node'a bağlanma**

Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security ile Central Node bileşeni arasında güvenilir bir bağlantı kurulmasını gerektirir. Güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası kullanmanız gerekir. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Ardından TLS sertifikasını Kaspersky Endpoint Security'ye eklemeniz gerekir (aşağıdaki talimatlara bakın).



Kaspersky Endpoint Security'ye TLS sertifikası ekleme

Kaspersky Endpoint Security varsayılan olarak yalnızca Central Node'un TLS sertifikasını kontrol eder. Bağlantıyı daha güvenli hale getirmek için, bilgisayarın Central Node üzerinde doğrulanmasını da etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu doğrulamayı etkinleştirmek için Central Node ve Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı açmanız gerekir. İki yönlü kimlik doğrulamayı kullanmak için ayrıca bir kripto konteynere ihtiyacınız olacaktır. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).

Yönetim Konsolu (MMC) kullanılarak bir Kaspersky Endpoint Security bilgisayarı Central Node'a nasıl bağlanır

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Detection and Response → Network Detection and Response (KATA)** seçimini yapın.
4. **Network Detection and Response (KATA)** onay kutusunu seçin.
5. **Bağlantı ayarları** seçeneğine tıklayın.
6. Sunucu bağlantısını yapılandırın:
   - **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener.
   - **Sunucu sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).

- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

7. **Tamam**'a tıklayın.
8. Central Node sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.
9. Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
10. Gerekirse telemetriyi yapılandırın.
11. Değişikliklerinizi kaydedin.

Web Console kullanılarak bir Kaspersky Endpoint Security bilgisayarı Central Node'a nasıl bağlanır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Network Detection and Response (KATA)** bölümüne gidin.
5. **Network Detection and Response (KATA) ETKİN** iki durumlu düğmesini açık duruma getirin.
6. **Bağlantı ayarları** seçeneğine tıklayın.
7. Sunucu bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener.
   - **Sunucu sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım'daki talimatlara bakın).

- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

8. **Tamam**'a tıklayın.
9. Central Node sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.
10. Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
11. Gerekirse telemetriyi yapılandırın.
12. Değişikliklerinizi kaydedin.

Sonuç olarak, bilgisayar Kaspersky Anti Targeted Attack Platform konsoluna eklenir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Network Detection and Response (KATA)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

EDR Agent'ı EDR Expert (on-premises) ile entegre etme

EDR Agent, kuruluşun BT altyapısındaki iş istasyonlarına ve sunuculara yüklenir. Bu bilgisayarlarda EDR Agent işlemleri, açık ağ bağlantılarını ve değiştirilen dosyaları sürekli olarak izler ve izleme verilerini EDR Expert (on-premises) sunucusuna gönderir.

EDR Expert (on-premises) ile entegre etmek için Endpoint Detection and Response Expert (on-premises) bileşenini etkinleştirmeniz ve EDR Agent'ı yapılandırmanız gerekir.

Endpoint Detection and Response Expert (on-premises) ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Kaspersky Endpoint Detection and Response Expert (on-premises) ürününün etkinleştirilmesi**

   EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) Eklentisi) için ayrı bir lisans satın almanız gerekir.

   Kaspersky Endpoint Detection and Response Expert (on-premises) için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir hale gelir. Bağımsız Endpoint Detection and Response Expert (on-premises) işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   EDR Expert (on-premises) işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

2. **Telemetri toplama sunucusuna ve yanıt sunucusuna bağlanma**

Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Security ile iki sunucu arasında güvenilir bir bağlantı gerektirir:

- Bir *telemetri toplama sunucusu*, SIEM çözümünün bir parçası olan ve bilgisayarda meydana gelen olaylarla ilgili bilgileri toplayan, normalleştiren, ilişkilendiren, analiz eden ve depolayan bir sunucudur.
- Bir *yanıt sunucusu*, verileri almak ve taramak, nesnelerin davranışlarını incelemek ve bu tür çalışmaların sonuçlarını yayınlamak için kullanılan bir sunucudur.

Güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası kullanmanız gerekir. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Ardından TLS sertifikasını Kaspersky Endpoint Security'ye eklemeniz gerekir (aşağıdaki talimatlara bakın).

Varsayılan olarak, Kaspersky Endpoint Security yalnızca sunucuların TLS sertifikasını kontrol eder. Bağlantıyı daha güvenli hale getirmek için, ek olarak sunucudaki bilgisayarın doğrulanmasını etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu doğrulamayı etkinleştirmek için sunucu ve Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı açmanız gerekir. İki yönlü kimlik doğrulamayı kullanmak için ayrıca bir kripto konteynere ihtiyacınız olacaktır. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).

Web Console kullanarak bir Kaspersky Endpoint Security bilgisayarını EDR Expert'e (on-premises) bağlama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (on-premises)** bölümüne gidin.
5. **Endpoint Detection and Response Expert (on-premises) ETKİN** iki durumlu düğmesini açık duruma getirin.
6. EDR Expert (on-premises) ürününü yapılandırmak için çözümler listesinden **Endpoint Detection and Response Expert (sürüm 8.0 veya üstü)** seçeneğini seçin.
7. *Telemetri toplama sunucuları* bağlantısını yapılandırın:

   a. **Telemetri toplama sunucularına bağlantı** bloğunda **Bağlantı ayarları** bağlantısına tıklayın.

   b. Telemetri toplama sunucuları bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır.
   - **Sunucu sertifikası**. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).

- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ile sunucu arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için sunucu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto kabı almanız ve kripto kabını korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Sunucu ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto kapsayıcı yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

c. **Tamam**'a tıklayın.

d. Telemetri toplama sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

Birden fazla telemetri toplama sunucusu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

e. Gerekirse telemetriyi yapılandırın.

8. *Yanıt sunucuları* bağlantısını yapılandırın:

a. **Yanıt sunucularına bağlantı** bloğunda, **Senkronizasyon isteğini sunucuya her (dk)** gönder ayarını yapılandırın. Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında Kaspersky Endpoint Security tehdit yanıtı görevlerini alır ve görev sonuçlarını gönderir.

b. **Bağlantı ayarları** bağlantısına tıklayın.

c. Yanıt sunucuları bağlantısını yapılandırın:

- **Zaman aşımı (sn)**. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır.

- **Sunucu sertifikası**. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).

- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ile sunucu arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için sunucu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto kabı almanız ve kripto kabını korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Sunucu ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto kapsayıcı yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

d. **Tamam**'a tıklayın.

e. Yanıt sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

Birden fazla yanıt sunucusu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Sonuç olarak, bilgisayar Open Single Management Platform'a (OSMP) eklenir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Endpoint Detection and Response Expert (on-premises)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

Üçüncü taraf EPP uygulamalarla uyumluluk

EDR Agent, Kaspersky Detection and Response çözümlerinin işlevselliğini destekler. EDR Agent için koruma ve kontrol bileşenleri mevcut değildir. Bu yapılandırma, üçüncü taraf EPP uygulamalarının yüklenmesine ve Kaspersky Detection and Response çözümlerinin kuruluşun altyapısında dağıtılmasına olanak tanır.

EDR Agent, aşağıdaki satıcıların EPP uygulamaları ile uyumludur:

- **Dr.Web**

  EDR Agent, Dr.Web Agent for Windows sürüm 13 ve Dr.Web Server (x64) 13.0.0.10200 ile uyumludur.

- **Dallas Lock**

  EDR Agent, Dallas Lock 8.0-C sürüm 843.2 ile uyumludur.

  > EDR Agent'in Dallas Lock yazılımının yüklü olduğu bir bilgisayarda çalışması için Güvenlik Duvarı modülünün ayarlarında Kaspersky harici hizmetlerine bağlantıya izin vermeniz gerekir.

- **Secret Net Studio**

  EDR Agent, Secret Net Studio sürüm 8.11 (20851) ile uyumludur.

  > Uygulama, Secret Net Studio'nun Antivirüs bileşeniyle birlikte dağıtıldığı bir bilgisayara yüklenemez. Birlikte çalışabilirliği mümkün kılmak için Antivirüs bileşenini Secret Net Studio'dan kaldırmalısınız.

- **Trend Micro**

  EDR Agent, Trend Micro Vision One (Security Agent sürüm 14.0.20731 dahil) ile uyumludur.

  EDR Agent, Trend Micro Deep Security sürüm 20.0.3-18160 (Security Agent dahil) ile uyumludur.

- **Windows Defender**

- **Sophos**

  EDR Agent, Sophos Intercept X sürüm 2024.1.2 (Endpoint Agent dahil) ve Sophos Core Agent sürüm 2026.2.1.3 ile uyumludur.

- **Bitdefender**

  EDR Agent, Bitdefender Endpoint Security Tools sürüm 8.26.7.647 ile uyumludur.

- **ESET**

  EDR Agent, ESET Endpoint Security sürüm 13.0.2044.0 ve ESET Management Agent sürüm 13.2.1189.0 ile uyumludur.

Arm64 için Windows 11 çalıştıran bilgisayarlarda, EDR Agent Bitdefender Endpoint Security Tools ile uyumlu değildir.

Uygulamalar şu sırayla yüklenmelidir: önce EPP uygulamasını, ardından Kaspersky Security Center Network Agent'ı, ardından EDR Agent'ı yükleyin. Bu gereklidir çünkü EPP uygulamasının yükleyicisi EDR Agent ve Network Agent'ı uyumsuz yazılım olarak algılayıp kaldırabilir. Üçüncü taraf EPP uygulaması güncellendikten sonra EDR Agent ve Network Agent'ın çalışması da kontrol edilmelidir, çünkü yükleyici bilgisayarı uyumsuz yazılımlar için yeniden tarayabilir ve uygulamaları kaldırabilir.

Yükleyici bilgisayarda uyumsuz yazılım bulduğu için EDR Agent'ı üçüncü taraf EPP uygulaması olan bir bilgisayara yükleyemediyseniz, uyumsuz yazılım kontrolünü atlayabilirsiniz.

Managed Detection and Response

Kaspersky Endpoint Security for Windows, Managed Detection and Response çözümü ile entegrasyonu destekler. *Kaspersky Managed Detection and Response (MDR)* çözümü, altyapınızdaki güvenlik olaylarını otomatik olarak algılar ve analiz eder. MDR bunu yapmak için uç noktalardan alınan telemetri verilerini ve makine öğrenimini kullanır. MDR, olay verilerini Kaspersky uzmanlarına gönderir. Uzmanlar daha sonra olayı işleyebilir ve mesela antivirüs veritabanlarına yeni bir giriş ekleyebilir. Alternatif olarak, uzmanlar olayın işlenmesiyle ilgili önerilerde bulunabilir ve mesela bilgisayarın ağdan izole edilmesini önerebilir. Çözümün nasıl çalıştığı hakkında ayrıntılı bilgi için lütfen Kaspersky Managed Detection and Response Yardım içeriğine bakın.

MDR ile entegrasyon için Kaspersky Endpoint Security yapılandırmaları

MDR ile çalışmak için aşağıdaki yapılandırmalar kullanılabilir:

- **[KES+yerleşik aracı]**. Bu yapılandırmada, Kaspersky Endpoint Security hem bilgisayarın güvenliğini sağlayan uygulama hem de MDR ile çalışma uygulaması olarak görev yapar.
- **[üçüncü taraf EPP+EDR Agent]**. Bu yapılandırmada, BT altyapısının güvenliği üçüncü taraf Endpoint Protection Platform (EPP) tarafından sağlanır. MDR ile etkileşim, Endpoint Detection and Response Agent (EDR Agent) yapılandırmasında Kaspersky Endpoint Security tarafından sağlanır. EDR Agent bu yapılandırmada üçüncü taraf EPP uygulamalarıyla uyumludur.

Yerleşik aracının MDR ile entegrasyonu

Kaspersky Managed Detection and Response ile entegrasyonu ayarlamak için Managed Detection and Response bileşenini etkinleştirmeniz ve Kaspersky Endpoint Security'yi yapılandırmanız gerekir.

Kaspersky Managed Detection and Response bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için yeni bir güvenli bağlantı, yani bir *arka plan bağlantısı* kurmanız şarttır. Kaspersky Managed Detection and Response, çözümün dağıtımını yaparken, sizden bir arka plan bağlantısı kurmanızı ister. Arka plan bağlantısının kurulduğundan emin olun.

Web Console'da bir arka plan bağlantısı kurma

1. Web Console ana penceresinden **Ayarlar** → **Tümleştirme** seçimini yapın.
2. **Tümleştirme** bölümüne gidin.
3. **Tümleştirme için bir arka plan bağlantısı Etkin** iki durumlu düğmesini açık duruma getirin.
4. Değişikliklerinizi kaydedin.

Kaspersky Managed Detection and Response ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Managed Detection and Response bileşenini yükleme**

   MDR bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken seçebilirsiniz.

   > Managed Detection and Response bileşenini bilgisayarı yeniden başlatmadan *Uygulama bileşenlerini değiştir* görevini kullanarak yüklemek için görev ayarlarındaki **Uyumsuz üçüncü taraf uygulamaları denetle** seçeneğini devre dışı bırakmanız gerekir.

2. **Kaspersky Private Security Network'ü yapılandırma**

   > Kaspersky Security Center Cloud Console kullanıyorsanız bu adımı atlayın. Kaspersky Security Center Cloud Console, Kaspersky Private Security Network'ü, MDR eklentisi yüklenirken otomatik olarak yapılandırır.

   Kaspersky Private Security Network (KPSN), Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür.

   Yönetim Sunucusu özelliklerine Kaspersky Security Network yapılandırma dosyasını yükleyin. Kaspersky Security Network yapılandırma dosyası, MDR yapılandırma dosyasının ZIP arşivinde bulunur. ZIP arşivini Kaspersky Managed Detection and Response Konsolunda bulabilirsiniz. Kaspersky Private Security Network yapılandırılmasıyla ilgili ayrıntılar için lütfen Kaspersky Security Center Yardım içeriğine bakın. Kaspersky Security Network yapılandırma dosyasını bilgisayara komut satırından da yükleyebilirsiniz (aşağıdaki talimatlara bakın).

   Kaspersky Private Security Network komut satırından nasıl yapılandırılır

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

      ```
      avp.com KSN /private <file name>
      ```

      burada `<file name>` Kaspersky Private Security Network ayarlarını içeren yapılandırma dosyasının (PKCS7 veya PEM dosya biçiminde) adıdır.

      Örnek:
      ```
      avp.com KSN /private C:\kpsn_config.pkcs7
      ```

Sonuç olarak Kaspersky Endpoint Security, dosyaların, uygulamaların ve web sitelerinin tanınırlığını belirlemek için Kaspersky Private Security Network'ü kullanacaktır. İlke ayarlarının **Kaspersky Security Network** bölümü şu çalışma durumunu gösterecektir: *Altyapı: Kaspersky Private Security Network*.

Managed Detection and Response bileşeninin çalışması için genişletilmiş KSN modunu etkinleştirmeniz gerekir.

3 Kaspersky Managed Detection and Responseu etkinleştirme

Kaspersky Endpoint Security for Windows 12.10 sürümünden itibaren, Managed Detection and Response işlevini etkinleştirmek için etkinleştirme koduna alternatif olarak bir anahtar dosyası da kullanabilirsiniz.

Kaspersky Managed Detection and Response aşağıdaki lisanslama yöntemlerini destekler:

- Managed Detection and Response işlevselliği, Kaspersky Endpoint Security for Windows lisansına dahildir.

  Bu işlevsellik, Kaspersky Endpoint Security for Windows etkinleştirildikten hemen sonra kullanılabilir.

- MDR (Kaspersky Managed Detection and Response Eklentisi) için ayrı bir lisans kullanılır.

  Kaspersky Managed Detection and Response Eklentisi için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir. Sonuç olarak bilgisayara iki anahtar eklenir: Kaspersky Endpoint Security için bir anahtar ve Kaspersky Managed Detection and Response için bir anahtar.

  Bağımsız Managed Detection and Response işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

MDR işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

4 Managed Detection and Response bileşenini etkinleştirme

BLOB yapılandırma dosyasını Kaspersky Endpoint Security ilkesine yükleyin (aşağıdaki talimatlara bakın). BLOB dosyası, istemci kimliğini ve Kaspersky Managed Detection and Response lisansı hakkındaki bilgileri içerir. BLOB dosyası, MDR yapılandırma dosyasının ZIP arşivinde bulunur. ZIP arşivini Kaspersky Managed Detection and Response Konsolunda bulabilirsiniz. Bir BLOB dosyası hakkında ayrıntılı bilgi için lütfen Kaspersky Yönetilen Algılama ve Yanıt Yardım içeriğine bakın.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, geçerli bir lisansınız varsa BLOB dosyası eklemek Kaspersky Managed Detection and Response için kiracı olmadan isteğe bağlıdır.

Managed Detection and Response, Yönetim Konsolu (MMC) ile nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** seçimini yapın.
4. **Managed Detection and Response (Industrial CyberSecurity)** onay kutusunu seçin.

5. **Ayarlar** bloğunda, **Yükle**'a tıklayın ve Kaspersky Managed Detection and Response Konsolu'nda alınan BLOB dosyasını seçin. Dosya P7 uzantısına sahiptir.

   Varsayılan olarak, kullanıcının uygulama ayarlarını yönetmesine izin verilir ("asma kilit" açık durumdadır). İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın.

6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Managed Detection and Response bileşeni nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Managed Detection and Response** bölümüne gidin.
5. **Managed Detection and Response ETKİN** geçiş düğmesini açık duruma getirin.
6. **Yükle**'ye tıklayın ve Kaspersky Managed Detection and Response Konsolu'nda elde edilen BLOB dosyasını seçin. Dosya P7 uzantısına sahiptir.

   Varsayılan olarak, kullanıcının ilke ayarlarını yönetmesine izin verilir ("asma kilit" açık durumdadır). İlkeyi bilgisayarlara uygulamak için asma kilitleri kapatın.
7. Değişikliklerinizi kaydedin.

Managed Detection and Response bileşeni komut satırından nasıl etkinleştirilir

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

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

   Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Uygulama ayarlarını yapılandır** izninin olması gerekir.

Sonuç olarak Kaspersky Endpoint Security BLOB dosyasını doğrular. BLOB dosya doğrulaması, dijital imzanın ve lisans süresinin kontrol edilmesini kapsar. BLOB dosyası başarıyla doğrulanırsa Kaspersky Endpoint Security dosyayı indirir ve Kaspersky Security Center ile bir sonraki senkronizasyon sırasında dosyayı bilgisayara gönderir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Managed Detection and Response** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

5 **Telemetri almak için uygulamanın diğer bileşenlerini yapılandırma**

Managed Detection and Response bileşeninin çalışması için şu bileşenleri etkinleştirmeniz gerekir:

- Kaspersky Security Network (genişletilmiş mod).
- Davranış Tespiti.
- Exploit Önleme.
- Web Tehdidi Koruması.
- Posta Tehdidi Koruması.
- Dosya Tehdidi Koruması.
- Ağ Tehdidi Koruması.
- Güvenlik Duvarı.
- AMSI Koruması.
- Arka plan taraması.

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Managed Detection and Response** bölümüne gidin.
5. **Managed Detection and Response ETKİN** geçiş düğmesini açık duruma getirin.
6. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinden **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** seçimini yapın.
4. **Managed Detection and Response (Industrial CyberSecurity)** onay kutusunu seçin.
5. Değişikliklerinizi kaydedin.

MDR için KEA'dan KES'e Geçiş Kılavuzu

Kaspersky Endpoint Security for Windows, Kaspersky Managed Detection and Response çözümü için yerleşik bir aracı içerir. MDR ile çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok. Tüm Kaspersky Endpoint Agent işlevleri Kaspersky Endpoint Security tarafından gerçekleştirilecektir.

Kaspersky Endpoint Agent yüklü bilgisayarlara Kaspersky Endpoint Security dağıttığınızda, Kaspersky Managed Detection and Response çözümü Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır. Kaspersky Endpoint Security'yi 11.6.0 veya daha üst bir sürüme güncellediğinizde sistemde aynı davranış ortaya çıkar.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent ile uyumlu değildir. Bu uygulamaların her ikisini de aynı bilgisayara yükleyemezsiniz.

Kaspersky Endpoint Security'nin Kaspersky Managed Detection and Response'un bir parçası olarak çalışması için şu koşulların karşılanması gerekir:

- Kaspersky Security Center sürüm 13.2 veya üstü (Network Agent dahil). Kaspersky Security Center'ın önceki sürümlerinde Managed Detection and Response özelliğini etkinleştirmek mümkün değildir.
- Kaspersky Security Center Web Console ile Yönetim Sunucusu arasında bir arka plan bağlantısı kuruldu. MDR bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için yeni bir güvenli bir bağlantı, yani bir *arka plan bağlantısı* kurmanız da şarttır.

MDR için [KES+KEA] yapılandırmasını [KES+yerleşik aracı]'ya taşıma adımları

1. **Kaspersky Endpoint Security Management Eklentisini Yükseltme**

   MDR bileşeni, Kaspersky Endpoint Security Management Plug-in sürüm 11.6 veya üstü kullanılarak yönetilebilir. Kullandığınız Kaspersky Security Center konsolunun türüne bağlı olarak, Yönetim Konsolu (MMC)'deki yönetim eklentisini veya Web Console'daki web eklentisini güncelleyin.

2. **İlkelerin ve görevlerin taşınması**

   Kaspersky Endpoint Agent ayarlarını Kaspersky Endpoint Security for Windows'a aktarın. Aşağıdaki seçenekler kullanılabilir:

   - Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş için bir sihirbaz. Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş sihirbazı yalnızca Web Console'da çalışır

     Web Console'da Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye ilke ve görev ayarlarını taşıma

     Web Console ana penceresinde, **İşlemler** → **Kaspersky Endpoint Agent'tan Geçiş** seçimini yapın.

     Böylece ilke ve görev geçiş sihirbazı çalıştırılır. Sihirbazın talimatlarını uygulayın.

     1. Adım. İlke geçişi

     Geçiş Sihirbazı, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent ilkelerinin ayarlarını birleştiren yeni bir ilke oluşturur. İlke listesinden, ayarlarını Kaspersky Endpoint Security ilkesiyle birleştirmek istediğiniz Kaspersky Endpoint Agent ilkelerini seçin. Ayarları birleştirmek istediğiniz Kaspersky Endpoint Security ilkesini seçmek için Kaspersky Endpoint Agent ilkesine tıklayın. Doğru ilkeleri seçtiğinizden emin olun ve sonraki adıma geçin.

2. Adım. Görev geçişi

Geçiş Sihirbazı MDR görevlerini desteklemez. Bu adımı atlayın.

3. Adım Sihirbazı tamamlama

Sihirbazı tamamlayın. Sihirbazın sonucunda yeni bir Kaspersky Endpoint Security ilkesi oluşturulacaktır. İlke, Kaspersky Endpoint Security'den ve Kaspersky Endpoint Agent'tan gelen ayarları birleştirir. Bu ilkeye *<Kaspersky Endpoint Security ilke adı> & <Kaspersky Endpoint Agent ilke adı>* adı verilir. Yeni ilke *Etkin değil* durumundadır. Devam etmek için Kaspersky Endpoint Agent ve Kaspersky Endpoint Security ilkelerinin durumlarını *Etkin değil* olarak değiştirtin ve yeni birleştirilmiş ilkeyi etkinleştirin.

- Standart bir İlke ve görevler toplu dönüştürme sihirbazı. İlke ve görevler toplu dönüştürme sihirbazı yalnızca Yönetim Konsolu'nda (MMC) kullanılabilir. İlke ve görevler toplu dönüştürme sihirbazı hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

3 MDR işlevselliğinin lisanslanması

Kaspersky Managed Detection and Response çözümünün bir parçası olarak Kaspersky Endpoint Security'yi etkinleştirmek için ayrı bir Kaspersky Managed Detection and Response Eklentisi lisansına ihtiyacınız vardır. Anahtarı, *Anahtar ekle* görevini kullanarak ekleyebilirsiniz. Sonuç olarak, uygulamaya iki anahtar eklenecektir: *Kaspersky Endpoint Security* ve *Kaspersky Managed Detection and Response*.

4 Kaspersky Endpoint Security uygulamasını Yükleme/Yükseltme

Bir uygulama kurulumu veya yükseltmesi sırasında MDR işlevselliğini taşımak için uzaktan kurulum görevinin kullanılması önerilir. Bir uzaktan kurulum görevi oluştururken, kurulum paketi ayarlarında MDR bileşenini seçmeniz gerekir.

Uygulamayı, şu yöntemleri kullanarak da güncellemeniz mümkündür:

- Kaspersky güncelleme hizmetini kullanma.
- Kurulum Sihirbazını kullanarak yerel olarak.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent uygulamasının yüklü olduğu bir bilgisayarda uygulama yükseltilirken, bileşenlerin otomatik olarak seçilmesini destekler. Bileşenlerin otomatik seçimi, uygulamayı yükselten kullanıcı hesabının izinlerine bağlıdır.

Kaspersky Endpoint Security'yi sistem hesabı (SYSTEM) altındaki EXE veya MSI dosyasını kullanarak yükseltiyorsanız, Kaspersky Endpoint Security, Kaspersky çözümlerinin geçerli lisanslarına erişim kazanır. Dolayısıyla, bilgisayarda Kaspersky Endpoint Agent yüklü ve MDR çözümü etkinleştirilmişse, Kaspersky Endpoint Security yükleyicisi bileşen setini otomatik olarak yapılandırır ve MDR bileşenini seçer. Bu, Kaspersky Endpoint Security'nin bütünleşik aracıyı kullanmaya geçmesini sağlar ve Kaspersky Endpoint Agent'ı kaldırır. MSI yükleyicisinin sistem hesabı (SYSTEM) altında çalıştırılması genellikle Kaspersky güncelleme hizmeti aracılığıyla yükseltme yapılırken ya da Kaspersky Security Center aracılığıyla bir yükleme paketi dağıtılırken gerçekleştirilir.

Kaspersky Endpoint Security'yi ayrıcalıklı olmayan bir kullanıcı hesabı altında bir MSI dosyası kullanarak yükseltiyorsanız, Kaspersky Endpoint Security'nin Kaspersky çözümlerinin geçerli lisanslarına erişimi olmaz. Bu durumda Kaspersky Endpoint Security, Kaspersky Endpoint Agent'ın bir dizi bileşenini temel alarak bileşenleri otomatik olarak seçer. Bundan sonra, Kaspersky Endpoint Security' bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

Kaspersky Endpoint Security, bilgisayar yeniden başlatılmadan yükseltme yapılmasını destekler. İlke özelliklerinde uygulama yükseltme modunu seçebilirsiniz.

5. **Uygulama çalışmasının kontrolü**

   Uygulama yükleme veya yükseltmesi sonrasında bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

   - Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
   - *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, yerleşik aracı işlevselliğini etkinleştirdiğinizden emin olun.
   - Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows, artık Kaspersky Endpoint Detection and Response Optimum çözümü için yerleşik bir aracıya sahip (bundan böyle "EDR Optimum" olarak anılacaktır). 11.8.0 sürümünden itibaren, Kaspersky Endpoint Security for Windows artık Kaspersky Endpoint Detection and Response Expert çözümü (bundan böyle "EDR Expert" olarak anılacaktır) için yerleşik bir aracıya sahip. *Kaspersky Endpoint Detection and Response*, kurumsal BT altyapısını gelişmiş siber tehditlere karşı korumaya yönelik bir çözüm yelpazesidir. Çözümlerin işlevselliği, yeni açıklar, fidye yazılımı, dosyasız saldırılar ve yasal sistem araçlarını kullanan yöntemler dahil olmak üzere gelişmiş saldırılara karşı koymak için tehditlerin otomatik olarak algılanması ile bu tehditlere yanıt verme yeteneğini birleştirir. EDR Expert, EDR Optimum'a göre daha fazla tehdit izleme ve tehdit yanıtı işlevselliği sunar. Çözümlerin ayrıntıları için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

Tehdit İstihbarat araçları

Kaspersky Endpoint Detection and Response, aşağıdaki Threat Intelligence araçlarını kullanır:

- Dosyaların ve internet adreslerinin tanınırlığı hakkında bilgi içeren ve görüntüleyen Kaspersky Threat Intelligence Portal ile entegrasyon.
- Kaspersky Tehditler veritabanı.
- Kaspersky bilgi bankasından gerçek zamanlı dosya, web sitesi ve yazılım tanınırlık bilgilerine erişim sağlayan Kaspersky Security Network (bundan böyle "KSN" olarak anılacaktır) bulut hizmeti altyapısı. Kaspersky Security Network'ten gelen verilerin kullanılması Kaspersky uygulamalarının tehditlerle karşılaştığında verdiği tepki süresini kısaltır ve bazı koruma bileşenlerinin performansını iyileştirerek hatalı pozitif sonuç riskini azaltır.
- Tespit edilwn dosyaları yalıtılmış bir ortamda çalıştırmanıza ve tanınırlıklarını kontrol etmenize olanak tanıyan Cloud Sandbox teknolojisi.

Çözümün çalışma prensibi

Kaspersky Endpoint Detection and Response, tehdit gelişimini inceleyip analiz eder ve *güvenlik personeli* ya da *Yönetici* tarafından zamanında yanıt verilebilmesini sağlamak için potansiyel saldırı hakkındaki gerekli bilgileri sağlar. Kaspersky Endpoint Detection and Response uyarı ayrıntılarını ayrı bir pencerede görüntüler. *Uyarı*, kurumsal BT altyapısında uygulamanın olağandışı veya şüpheli olarak tanımladığı ve kurumsal BT altyapısı için bir güvenlik tehdidi oluşturabilecek bir olaydır. *Uyarı Ayrıntıları*, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

Kaspersky Endpoint Security'nin önceki sürümleri için destek

Kaspersky Endpoint Detection and Response Optimum ile birlikte çalışabilirlik için Kaspersky Endpoint Security 11.2.0–11.6.0 kullanıyorsanız, uygulama Kaspersky Endpoint Agent'ı içerir. Kaspersky Endpoint Security'yi Kaspersky Endpoint Agent ile birlikte yükleyebilirsiniz. Kaspersky Endpoint Security 11.9.0'da Kaspersky Endpoint Agent dağıtım paketi artık Kaspersky Endpoint Security dağıtım kitinin bir parçası değildir.

Kaspersky Endpoint Detection and Response Expert çözümü, Kaspersky Endpoint Agent ile birlikte çalışabilirliği desteklemez. Kaspersky Endpoint Detection and Response Expert çözümü, yerleşik aracılı (sürüm 11.8.0 ve üstü) Kaspersky Endpoint Security'yi kullanır.

Yerleşik aracının EDR Optimum/EDR Expert ile entegrasyonu

Kaspersky Endpoint Detection and Response ile entegrasyonu kurmak için Endpoint Detection and Response Optimum bileşenini ya da Endpoint Detection and Response Expert (cloud) bileşenini eklemeli ve Kaspersky Endpoint Security'yi yapılandırmalısınız.

Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) ve Endpoint Detection and Response Expert (on-premises) bileşenleri birbirleriyle uyumlu değildir.

Endpoint Detection and Response bileşeninin çalışması için şu şartlar sağlanmalıdır:

- Kaspersky Security Center sürüm 13.2 veya üstü. Kaspersky Security Center'ın önceki sürümlerinde Endpoint Detection and Response özelliğini etkinleştirmek mümkün değildir.
- Kaspersky Endpoint Detection and Response yönetim eklentisi.

  Kaspersky Endpoint Security sürüm 12.6'dan itibaren uyarı ayrıntılarının görüntülenmesi Kaspersky Endpoint Security yönetim eklentisinden EDR yönetim eklentisine taşınmıştır. EDR yönetim eklentisi, Windows, Mac ve Linux işletim sistemlerinde aracılarla çalışmak için tek bir eklentidir. Artık EDR Optimum ile çalışırken, tehdit yanıt görevleri oluşturmak için Kaspersky Endpoint Security yönetim eklentisine ve uyarı ayrıntılarını görüntülemek için EDR yönetim eklentisine ihtiyacınız olacak.
- Kaspersky Endpoint Security'nin bir parçası olan Endpoint Detection and Response Optimum bileşeni, Kaspersky Endpoint Detection and Response Optimum 2.0 çözümüyle etkileşimi destekler. Kaspersky Endpoint Detection and Response Optimum sürüm 1.0 ile etkileşim desteklenmez.

- EDR Optimum, Kaspersky Security Center Web Console ve Kaspersky Security Center Cloud Console'da yönetilebilir.

  EDR Expert özellikleri, yalnızca Kaspersky Security Center Cloud Console kullanılarak yönetilebilir. Bu işlevselliği Yönetim Konsolu'nu (MMC) kullanarak yönetemezsiniz.

- Uygulama etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.
- Endpoint Detection and Response bileşeni açık olmalıdır.
- Endpoint Detection and Response bileşeninin bağlı olduğu uygulama bileşenleri etkin ve çalışır durumda olmalıdır. Endpoint Detection and Response aşağıdaki bileşenlere bağlıdır:
  - Dosya Tehdidi Koruması.
  - Web Tehdidi Koruması.
  - Posta Tehdidi Koruması.
  - Exploit Önleme.
  - Davranış Tespiti.
  - Sunucu Yetkisiz Erişim Önleme.
  - Düzeltme Altyapısı.
  - Uyarlamalı Anomali Denetimi.

Kaspersky Endpoint Detection and Response ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Endpoint Detection and Response bileşenlerini yükleme**

   Yükleme veya yükseltme sırasında ya da *Uygulama bileşenlerini değiştir* görevini kullanarak Endpoint Detection and Response Optimum bileşenini veya Endpoint Detection and Response Expert (cloud) bileşenini seçebilirsiniz.

   > Uygulamayı yeni bileşenlerle yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatmanız gerekir.

2. **Kaspersky Endpoint Detection and Response'u etkinleştirme**

   Kaspersky Endpoint Detection and Response'u kullanmak için aşağıdaki yöntemlerle bir lisans alabilirsiniz:

   - Endpoint Detection and Response işlevselliği, Kaspersky Endpoint Security for Windows lisansına dahildir.

     Bu işlevsellik, Kaspersky Endpoint Security for Windows etkinleştirildikten hemen sonra kullanılabilir.

   - EDR Optimum veya EDR Expert (Kaspersky Endpoint Detection and Response Eklentisi) için ayrı bir lisans satın almak.

     Kaspersky Endpoint Detection and Response için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir hale gelir. Sonuç olarak bilgisayara iki anahtar eklenir: Kaspersky Endpoint Security için bir anahtar ve Kaspersky Endpoint Detection and Response için bir anahtar.

     Bağımsız Endpoint Detection and Response işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   EDR Optimum veya EDR Expert işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

EDR Optimum Son Kullanıcı Lisans Sözleşmesi hakkında daha fazla bilgi almak için Kaspersky Endpoint Detection and Response Optimum Yardım içeriğine bakın.

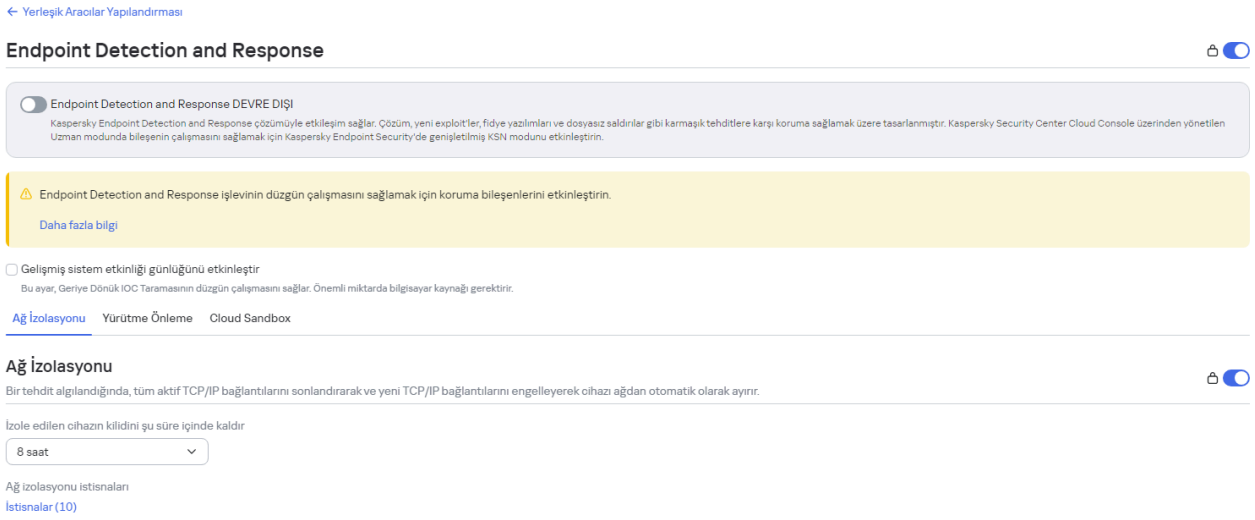
3 Endpoint Detection and Response bileşenlerini etkinleştirme

Kaspersky Endpoint Security for Windows ilke ayarlarından bileşeni etkinleştirebilir veya devre dışı bırakabilirsiniz.

Web Console'da Endpoint Detection and Response bileşenini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.
5. **Endpoint Detection and Response ETKİN** iki durumlu düğmesini açık duruma getirin.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.



EDR entegrasyon ayarları

Kaspersky Endpoint Detection and Response bileşeni etkinleştirilir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Endpoint Detection and Response Optimum** veya **Endpoint Detection and Response Expert (cloud)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

4 Yönetim Sunucusu'na veri aktarımı etkinleştirilme

Tüm Endpoint Detection and Response özelliklerini etkinleştirmek için, aşağıdaki veri türleri için veri aktarımı etkinleştirilmelidir:

- Karantina dosyası verileri.

  Veriler, bir bilgisayarda karantinaya alınan dosyalar hakkında Web Console aracılığıyla bilgi almak için gereklidir. Örneğin, Web Console'da analiz için karantinadan bir dosya indirebilirsiniz.

- Tehdit gelişim zinciri verileri.

  Veriler, bir bilgisayarda tespit edilen tehditler hakkında Web Console üzerinden bilgi almak için gereklidir. Web Console'da uyarı ayrıntılarını görüntüleyebilir ve müdahale eylemleri gerçekleştirebilirsiniz.

Web Console'da Yönetim Sunucusu'na veri aktarımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.
5. **Yönetim Sunucusu'na Veri Aktarımı** bloğunda, **Gelişmiş ayarlar** bağlantısını tıklayın.
6. Açılan pencerede aşağıdaki onay kutularını işaretleyin:
   - **Karantina dosyaları hakkında**.
   - **Bir tehdit geliştirme zinciri hakkında**.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Güvenlik ihlali göstergelerini (standart görev) tara

Güvenlik İhlali Göstergesi (IOC) bilgisayara yetkisiz erişimi (verilerin ele geçirilmesi) gösteren bir nesne veya etkinlik hakkında bir dizi veridir. Örneğin, sistemde oturum açmaya yönelik birçok başarısız girişim, bir Güvenlik İhlali Göstergesi oluşturabilir. *IOC Taraması* görevi, bilgisayarda güvenlik ihlali göstergelerini bulmaya ve tehdit yanıtı önlemleri almaya olanak verir.

Kaspersky Endpoint Security, IOC dosyaları kullanarak güvenlik ihlali göstergelerini arar. *IOC dosyaları*, uygulamanın bir algılamayı saymak için eşleştirmeye çalıştığı gösterge gruplarını içeren dosyalardır. IOC dosyaları OpenIOC standardına uygun olmalıdır.

IOC Taraması görevi çalışma modu

Kaspersky Endpoint Detection and Response, risk altındaki verileri tespit etmek için standart IOC Scan görevleri oluşturmanıza izin verir. *Standart IOC tarama görevi* Web Console'da manuel olarak oluşturulan ve yapılandırılan bir grup veya yerel görevdir. Görevler, kullanıcı tarafından hazırlanan IOC dosyaları kullanılarak çalıştırılır. Manuel olarak bir güvenlik ihlali göstergesi eklemek istiyorsanız lütfen IOC dosyaları için gereklilikleri okuyun.

Aşağıdaki bağlantıya tıklayarak indirebileceğiniz dosyada, OpenIOC standardının IOC terimlerinin tam listesini içeren bir tablo bulunur.

IOC_TERMS.XLSX DOSYASINI İNDİRİN

Kaspersky Endpoint Security, uygulama Kaspersky Sandbox çözümünün bir parçası olarak kullanıldığında bağımsız IOC Taraması görevlerini de destekler.

IOC dosyası oluşturma

Kaspersky Endpoint Security 12.10 for Windows ile başlayarak, IOC dosyalarını doğrudan görev ayarlarından oluşturabilirsiniz. Bir IOC dosyası oluşturmak için, güvenlik ihlallerinin bir listesini içeren bir TXT dosyası hazırlamanız gerekir. Güvenlik ihlali olarak aşağıdaki nesnelerin listelerini ekleyebilirsiniz:

- Dosya karmaları (MD5 / SHA256).

  Uygulama, FileItem/Md5sum veya FileItem/Sha256sum tarama kapsamına sahip bir IOC dosyası hazırlar.

- IP adresleri (IPv4, IPv6).

  Uygulama, PortItem/RemoteIP tarama kapsamına sahip bir IOC dosyası hazırlar.

- DNS adları.

  Uygulama, DnsEntryItem/RecordName tarama kapsamına sahip bir IOC dosyası hazırlar.

Web Console'da IOC dosyası oluşturma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. **IOC Taraması** görevini seçin.

   Görev özellikleri penceresi açılır. Gerekirse **IOC Taraması** görevi oluşturun.

3. **Uygulama ayarları** sekmesini seçin.

4. **Tehdit Taraması** bölümüne gidin.

5. **IOC dosyalarını yeniden tanımla**'ya tıklayın.

6. Bu, bir IOC dosyası oluşturmak için formu açar:

   a. **IOC dosyası kaynağı** bölümünden **Dosyadan oluştur** seçimini yapın.

   b. IOC dosyası için bir ad girin.

   c. Güvenlik ihlallerinin bir listesini içeren bir TXT dosyası seçin.

   d. IOC dosyasının türünü seçin: **DNS adları**, **Dosya karmaları**, **IP adresleri**.

   e. **Yükle** seçeneğine tıklayın.

   Kaspersky Endpoint Security, IOC dosyalarını IOC koleksiyonuna ekler. Gerekirse, IOC dosyalarını geçici olarak görev kapsamı dışında bırakabilirsiniz.

7. Değişikliklerinizi kaydedin.

Bir IOC Taraması görevi oluşturma

IOC Taraması görevlerini manuel olarak oluşturabilirsiniz:

- Uyarı ayrıntılarında (sadece EDR Optimum için).

  Uyarı Ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

- Görev Sihirbazını Kullanma.

Taranan bilgisayarlarda Kaspersky Endpoint Detection and Response Expert (on-premises) veya Kaspersky Endpoint Detection and Response Expert (cloud) ile entegrasyon yapılandırılmışsa *IOC Taraması* grup görevi çalıştırılamaz. Bu durumda, ele geçirilme göstergelerini aramak için *IOC Taraması* yanıt eylemini kullanmanızı öneririz. Daha fazla ayrıntı için Kaspersky Endpoint Detection and Response Expert (on-premises) yardımına başvurun.

EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.

Bir IOC Taraması görevi oluşturmak için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **IOC Taraması**'nı seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. Bir sonraki adıma geçin.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

   Sistem hesabı (SYSTEM), ağ sürücülerinde *IOC Taraması* görevini gerçekleştirme iznine sahip değildir. Görevi bir ağ sürücüsü için çalıştırmak istiyorsanız, o sürücüye erişimi olan bir kullanıcının hesabını seçin.

Ağ sürücülerindeki bağımsız IOC Taraması görevleri için görev özelliklerinden bu sürücüye erişimi olan kullanıcı hesabını manuel olarak seçmeniz gerekir.

6. Sihirbazı tamamlayın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. **Tehdit Taraması** bölümüne gidin.

10. Güvenlik ihlallerini aramak için IOC dosyalarını yükleyin.

    IOC dosyalarını yükledikten sonra uygulama, denetimi geçemeyen ihlallerin listesi de dahil olmak üzere dosya hakkında özet bilgiler görüntüler. IOC dosyalarını yükledikten sonra, dosyaları yerleşik düzenleyicide doğrudan görev özelliklerinde manuel olarak düzenleyebilirsiniz. Kaspersky Endpoint Security, OpenIOC 1.1 standardıyla uyumlu IOC dosyalarının düzenlenmesini destekler. OpenIOC sürüm 1.0 ile uyumlu IOC dosyalarının içeriğini değiştirmek mümkün değildir.

    Kaspersky Endpoint Security, IOC dosyalarını IOC koleksiyonuna ekler. Gerekirse, IOC dosyalarını geçici olarak görev kapsamı dışında bırakabilirsiniz.

    Görevi çalıştırdıktan sonra IOC dosyalarının eklenmesi veya kaldırılması önerilmez. Bu, görevin önceki çalıştırmaları için IOC tarama sonuçlarının yanlış görüntülenmesine neden olabilir. Yeni IOC dosyalarına göre güvenlik ihlali göstergelerini aramak için yeni görevler eklemeniz önerilir.

11. **Gerekirse, Geriye Dönük IOC Taraması** onay kutusunu seçin. *Geriye Dönük IOC Taraması*, Kaspersky Endpoint Security'nin belirli bir zaman dilimine ait verileri kullanarak ihlal göstergelerini taradığı *IOC Taraması* görevinin bir modudur. Bu mod, ağ etkinliği, işlemler, dosyalar ve diğer telemetri verileri gibi korunan bilgisayarın telemetri verilerini kullanarak güvenlik ihlali göstergelerini aramaya yöneliktir. Kaspersky Endpoint Security, bilgisayardaki işletim sistemi günlükleri ve tarayıcı günlüklerindeki verileri analiz eder. Retrospektif IOC Taraması şu tarayıcıların günlüklerini analiz eder: Google Chrome, Mozilla Firefox, Microsoft Edge (sürüm 79 veya üstü).

12. IOC tespit edildiğinde uygulanacak eylem:

    - **Cihazı ağdan izole et**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security tehdidin yayılmasını önlemek için bilgisayarı ağdan izole eder. İzolasyonun süresini Endpoint Detection and Response bileşen ayarları bölümünde yapılandırabilirsiniz.

      Bu onay kutusunun işareti kaldırılırsa, görevi manuel olarak çalıştırdıktan sonra bilgisayarı ağdan izole edebilirsiniz. *IOC Taraması* görevi bir IOC tespit ederse, bilgisayarı doğrudan IOC'den ağdan izole edebilirsiniz (*IOC Taraması* özellikleri → **Uygulama ayarları** → **IOC Taraması sonuçları** görevi). Kaspersky Endpoint Security ayrıca ek ayarların hemen yönetilmesini sağlar: Ağ izolasyonu devre dışı bırakma süresi ve Ağ izolasyonu istisnaları.

    - **Kopyayı Karantinaya taşı, nesneyi sil**. Bu seçenek tercihe dildiğinde, Kaspersky Endpoint Security bilgisayardaki kötü amaçlı nesneyi siler. Kaspersky Endpoint Security, nesneyi silmeden önce nesnenin daha sonra geri yüklenmesi gerekebileceği ihtimaline karşı bir yedek kopya oluşturur. Kaspersky Endpoint Security, yedek kopyayı Karantinaya taşır.

Bu onay kutusunun işareti kaldırılırsa, görevi manuel olarak çalıştırdıktan sonra dosyayı manuel olarak karantinaya alabilirsiniz. *IOC Taraması* görevi verileri tehlikeye atabilecek bir dosya tespit ederse, bu dosyayı doğrudan IOC Taraması sonuçlarından karantinaya alabilirsiniz (**Uygulama ayarları → IOC Taraması sonuçları**). Sonuç olarak Kaspersky Endpoint Security, algılanan dosyanın önceden ayarlanmış verileriyle görev oluşturma sihirbazını başlatır. Yalnızca ek görev ayarlarını yönetmeniz, örneğin görev zamanlamasını ayarlamanız gerekir.

Gerekirse **Sistem için kritik nesnelere uygula** onay kutusunu seçin. System Critical Object'ler (SCO'lar), işletim sisteminin çalışması için gereken dosyaları içerir.

SCO dosyalarına eylem uygulamanızı önermeyiz. Bu, işletim sisteminin kararsız hâle gelmesine veya önyükleme yapamamasına neden olabilir.

- **Kritik Alanları Taramayı çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Critical Areas Scan* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.

13. **Gelişmiş** bölümüne gidin.

14. Görevin bir parçası olarak analiz edilmesi gereken veri türlerini (IOC belgeleri) seçin.

Kaspersky Endpoint Security, *IOC Taraması* görevindeki veri türlerini (IOC belgeleri), yüklenen IOC dosyalarının içeriğine göre otomatik olarak seçer. Veri türlerinin seçiminin kaldırılması önerilmez.

Şu veri türleri için tarama kapsamlarını ayrıca yapılandırabilirsiniz:

- **Dosyalar - FileItem**. Ön tanımlı kapsamlar kullanarak bir IOC tarama kapsamı ayarlayın.

  Varsayılan olarak, Kaspersky Endpoint Security, yalnızca İndirilenler klasörü, masaüstü, geçici işletim sistemi dosyalarını içeren klasör gibi bilgisayarın önemli alanlarında IOC'ler için tarama yapar. Tarama kapsamını manuel olarak da ekleyebilirsiniz.

- **Windows olay günlüğü - EventLogItem**. Olayların günlüğe kaydedileceği zaman aralığını girin. Ayrıca IOC taraması için hangi Windows olay günlüklerinin kullanılması gerektiğini seçebilirsiniz. Varsayılan olarak şu olay günlükleri seçilir: uygulama olay günlüğü, sistem olay günlüğü ve güvenlik olay günlüğü.

  EventLogItem\source IOC terimi için olayın XML şemasındaki **Sağlayıcı Adı** değerini kullanın.

- **Windows kayıt defteri - RegistryItem**. Kayıt defterinde IOC Taraması kapsamını yapılandırın.

  Kaspersky Endpoint Security varsayılan olarak bir dizi kayıt defteri anahtarını tarar.

15. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

16. Görev zamanlamasını yapılandırın.

Wake-on-LAN bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

17. Değişikliklerinizi kaydedin.

18. Görevin yanındaki onay kutusunu seçin.

19. **Başlat**'a tıklayın.

    Sonuç olarak Kaspersky Endpoint Security, bilgisayardaki güvenlik ihlali göstergelerini arar. Görevin sonuçlarını **Sonuçlar** bölümündeki görev özelliklerinden izleyebilirsiniz. Algılanan güvenlik ihlali göstergeleri hakkındaki bilgileri görev özelliklerinde görüntüleyebilirsiniz: **Uygulama ayarları → IOC Taraması sonuçları**. IOC Taraması sonuçlarında, tespit edilen dosyayı manuel olarak karantinaya alabilir veya bilgisayarı ağdan izole edebilirsiniz.

Kaspersky Endpoint Security, aynı IOC dosyası için oluşturulan kayıtlar arasında yinelenenleri arar ve görev sonuçlarında yalnızca benzersiz kayıtları tutar. Yinelenen kayıtlar, karşılaştırılan tüm alanlarda aynı değerlere sahip olan aynı türdeki kayıtlardır. Uygulama ayrıca bir veya daha fazla alanda değer yoksa kayıt oluşturmayabilir (aşağıdaki tabloya bakın).

Tür	Karşılaştırılan alanlar	Kayıt oluşturmama koşulu
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• FullPath, Md5sum, Sha256sum alanlarının değerlerinin olmaması. • FullPath alanının değerinin olmaması ve Md5sum, Sha256sum alanlarının değerlerinin aynı olması.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Şu alanlardan en az birinin değerinin olmaması: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	startTime veya PID alanının değerinin olmaması.

Uyarı Ayrıntıları penceresi aynı alan değerlerine sahip RegistryItem kayıtlarını görüntüleyebilir. Bu tür kayıtlar yinelenmez çünkü arabirimde görüntülenmeyen Metin alanının farklı değerlerine sahiptirler.

IOC taraması sonuçları 30 gün boyunca saklanır. Bu süre sonrasında Kaspersky Endpoint Security en eski kayıtları otomatik olarak siler.

IOC Taraması için genişletilmiş telemetri

Geriye dönük IOC taraması için bilgisayarda genişletilmiş telemetriyi etkinleştirmenizi öneririz. Genişletilmiş telemetri, IOC tespitinin doğruluğunu artırır, ancak bilgisayarın daha fazla kaynağını kullanır.

Genişletilmiş telemetri aşağıdaki ek terimlerin desteğini içerir:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified

- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Genişletilmiş telemetri devre dışı bırakılırsa Kaspersky Endpoint Security, algılanan ihlal göstergeleri hakkındaki bilgileri döndürebilir.

Genişletilmiş telemetriyi etkinleştirmek için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.
5. **Gelişmiş sistem etkinliği günlüğünü etkinleştir** onay kutusunu seçin.
6. Değişikliklerinizi kaydedin.

Dosyayı Karantinaya taşı

Kaspersky Endpoint Detection and Response tehditlere tepki verirken *Dosyayı Karantinaya taşı* görevleri oluşturabilir. Bu, tehdidin sonuçlarını en aza indirmek için gereklidir. *Karantina* bilgisayardaki özel bir yerel depolama alanıdır. Kullanıcı, bilgisayar için tehlikeli olduğunu düşündüğü dosyaları karantinaya alabilir. Karantinaya alınan dosyalar şifrelenmiş bir durumda saklanır ve cihazın güvenliğini tehdit etmez. Kaspersky Endpoint Security, Karantinayı yalnızca Kaspersky Detection and Response çözümleriyle entegre edildiğinde kullanır. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantina'nın yönetimi hakkında ayrıntılar için lütfen Kaspersky Sandbox Yardım, Kaspersky Endpoint Detection and Response Optimum Yardım, Kaspersky Endpoint Detection and Response Expert Yardım, Kaspersky Anti Targeted Attack Platform Yardım ve Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım belgelerine bakın.

Dosyayı Karantinaya taşı görevlerini şu yöntemlerle oluşturabilirsiniz:

- Uyarı ayrıntılarında (sadece EDR Optimum için).

  Uyarı Ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

- Görev Sihirbazını Kullanma.

  Dosya yolunu veya karmasını (SHA256 veya MD5) ya da hem dosya yolunu hem de dosya karmasını girmelisiniz.

- *IOC Taraması* görev ayarları.

  IOC Taraması görevi verileri tehlikeye atabilecek bir dosya tespit ederse, bu dosyayı doğrudan IOC Taraması sonuçlarından karantinaya alabilirsiniz (**Uygulama ayarları → IOC Taraması sonuçları**). Sonuç olarak Kaspersky Endpoint Security, algılanan dosyanın önceden ayarlanmış verileriyle görev oluşturma sihirbazını başlatır. Yalnızca ek görev ayarlarını yönetmeniz, örneğin görev zamanlamasını ayarlamanız gerekir.

Dosyayı Karantinaya taşı görevi şu sınırlamalara sahiptir:

1. Dosya boyutu 100 MB'ı geçemez.
2. Kaspersky Endpoint Security for Windows'un çalışması için gereken dosyaları silemezsiniz:
   - Kaspersky Endpoint Security for Windows'un Kendini Savunma teknolojisi kapsamındaki dosyalar
   - Kaspersky tarafından dijital olarak imzalanmış dosyalar
3. EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.
4. *Dosyayı Karantinaya taşı* görevinin bir sonucu olarak karantinaya alınan bir nesneyi tarayamazsınız.

Bir Dosyayı Karantinaya taşı görevi oluşturmak için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.
2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
   b. **Görev türü** açılır listesinde, **Dosyayı Karantinaya taşı** seçimini yapın.
   c. **Görev adı** alanına kısa bir açıklama girin.
   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri**'ye tıklayın.
5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri**'ye tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.
6. **Son** düğmesine tıklayarak sihirbazı sonlandırın.

   Görevler listesinde yeni bir görev görüntülenir.
7. Yeni göreve tıklayın.

   Görev özellikleri penceresi açılır.
8. **Uygulama ayarları** sekmesini seçin.

9. Gerekirse **Sistem için kritik nesnelere uygula** onay kutusunu seçin.

   System Critical Object'ler (SCO'lar), işletim sisteminin çalışması için gereken dosyaları içerir.

   SCO dosyalarına eylem uygulamanızı önermeyiz. Bu, işletim sisteminin kararsız hâle gelmesine veya önyükleme yapamamasına neden olabilir.

10. Dosya listesinden **Ekle**'ye tıklayın.

    Dosya ekleme sihirbazı başlatılır.

11. Dosyayı eklemek için dosyanın tam yolunu veya hem dosya karmasını hem de yolu girmelisiniz.

    Dosya bir ağ sürücüsünde bulunuyorsa, sürücü harfini değil `\\` ile başlayan dosya yolunu girin. Örneğin, `\\server\shared_folder\file.exe`. Dosya yolu bir ağ sürücüsü harfi içeriyorsa, bir *Dosya bulunamadı* hatası alabilirsiniz.

12. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

13. Görev zamanlamasını yapılandırın.

    Wake-on-LAN bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

14. Değişikliklerinizi kaydedin.

15. Görevin yanındaki onay kutusunu seçin.

16. **Başlat**'a tıklayın.

    Sonuç olarak Kaspersky Endpoint Security, dosyayı Karantinaya alır.

Dosya farklı bir işlem tarafından kilitlenmişse görev Tamamlandı olarak görüntülenir ancak dosyanın kendisi yalnızca bilgisayar yeniden başlatıldıktan sonra karantinaya alınır. Bilgisayarı yeniden başlattıktan sonra dosyanın silindiğini onaylayın.

Dosya farklı bir işlem tarafından kilitlenirse göre: *Tamamlandı* olarak görüntülenir ancak dosyanın kendisi yalnızca bilgisayar yeniden başlatıldıktan sonra karantinaya alınır. Bilgisayarı yeniden başlattıktan sonra dosyanın silindiğini onaylayın.

Dosyayı Karantinaya taşı görevi, çalışır durumdaki yürütülebilir bir dosyayı karantinaya almaya çalışıyorsanız *Erişim reddedildi* hatasını verebilir. Dosya için bir işlemi sonlandır görevi oluşturun ve tekrar deneyin.

Dosyayı Karantinaya taşı görevi, çok büyük bir dosyayı karantinaya almaya çalışıyorsanız *Karantina depolamasında yeterli alan yok* hatası ile sonlanabilir. Karantinayı boşaltın ya da Karantina boyutunu artırın. Ardından tekrar deneyin.

Bir dosyayı Karantinadan geri yükleyebilir veya Karantinayı Console'u kullanarak boşaltabilirsiniz. Komut satırını kullanarak bilgisayarda yerel olarak nesneleri geri yükleyebilirsiniz.

Dosyayı al

Kullanıcı bilgisayarlarından dosyalar alabilirsiniz. Örneğin, üçüncü taraf bir uygulama tarafından oluşturulan bir olay günlüğü dosyasını almayı yapılandırabilirsiniz. Görevin yürütülmesi sonucunda dosyanın bir kopyası Karantinaya kaydedilir. *Karantina* bilgisayardaki özel bir yerel depolama alanıdır. Bu dosyayı, Web Console kullanarak Karantinadan bilgisayarınıza indirebilirsiniz (**İşlemler** → **Veri havuzları** → **Karantina**). Kullanıcının bilgisayarında, dosya orijinal klasöründe kalır.

Dosya boyutu 2 GB'ı geçemez.

EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.

Bir Dosyayı al görevi oluşturmak için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.
   Görevler listesi açılır.
2. **Ekle**'ye tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.
   b. **Görev türü** açılır listesinde, **Dosyayı al**'ı seçin.
   c. **Görev adı** alanına kısa bir açıklama girin.
   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri**'ye tıklayın.
5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri**'ye tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Son** düğmesine tıklayarak sihirbazı sonlandırın.
   Görevler listesinde yeni bir görev görüntülenir.
7. Yeni göreve tıklayın.
   Görev özellikleri penceresi açılır.
8. **Uygulama ayarları** sekmesini seçin.

9. Dosya listesinden **Ekle**'ye tıklayın.

   Dosya ekleme sihirbazı başlatılır.

10. Dosyayı eklemek için dosyanın tam yolunu veya hem dosya karmasını hem de yolu girmelisiniz.

    Dosya bir ağ sürücüsünde bulunuyorsa, sürücü harfini değil `\\` ile başlayan dosya yolunu girin. Örneğin, `\\server\shared_folder\file.exe`. Dosya yolu bir ağ sürücüsü harfi içeriyorsa, bir *Dosya bulunamadı* hatası alabilirsiniz.

11. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

12. Görev zamanlamasını yapılandırın.

    Wake-on-LAN bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. Değişikliklerinizi kaydedin.

14. Görevin yanındaki onay kutusunu seçin.

15. **Başlat**'a tıklayın.

    Sonuç olarak, Kaspersky Endpoint Security dosyanın bir kopyasını oluşturur ve bu kopyayı Karantinaya taşır. Dosyayı Web Console'daki Karantinadan indirebilirsiniz.

Dosyayı sil

Dosyayı sil görevini kullanarak dosyaları uzaktan silebilirsiniz. Örneğin, tehditlere yanıt verirken bir dosyayı uzaktan silebilirsiniz.

Kaspersky Endpoint Security for Windows'un çalışması için gereken dosyaları silemezsiniz:

- Kaspersky Endpoint Security for Windows'un Kendini Savunma teknolojisi kapsamındaki dosyalar
- Kaspersky tarafından dijital olarak imzalanmış dosyalar

EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.

Bir Dosyayı sil görevi oluşturmak için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Dosyayı sil**'i seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri**'ye tıklayın.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri**'ye tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Son** düğmesine tıklayarak sihirbazı sonlandırın.
   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.
   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. Dosyayı eklemek için dosyanın tam yolunu veya hem dosya karmasını hem de yolu girmelisiniz.

   Dosya bir ağ sürücüsünde bulunuyorsa, sürücü harfini değil `\\` ile başlayan dosya yolunu girin. Örneğin, `\\server\shared_folder\file.exe`. Dosya yolu bir ağ sürücüsü harfi içeriyorsa, bir *Dosya bulunamadı* hatası alabilirsiniz.

10. Gerekirse **Sistem için kritik nesnelere uygula** onay kutusunu seçin.
    System Critical Object'ler (SCO'lar), işletim sisteminin çalışması için gereken dosyaları içerir.

    SCO dosyalarına eylem uygulamanızı önermeyiz. Bu, işletim sisteminin kararsız hâle gelmesine veya önyükleme yapamamasına neden olabilir.

11. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

12. Görev zamanlamasını yapılandırın.

    Wake-on-LAN bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. Değişikliklerinizi kaydedin.

14. Görevin yanındaki onay kutusunu seçin.

15. **Başlat**'a tıklayın.

Böylece Kaspersky Endpoint Security dosyayı bilgisayardan siler. Dosya farklı bir işlem tarafından kilitlenirse göre:

Bitti olarak görüntülenir ancak dosyanın kendisi yalnızca bilgisayar yeniden başlatıldıktan sonra silinir. Bilgisayarı yeniden başlattıktan sonra dosyanın silindiğini onaylayın.

Dosyayı sil görevi, çalışır durumdaki yürütülebilir bir dosyayı silmeye çalışıyorsanız *Erişim reddedildi veya dosya bulunamadı* hatasını verebilir. Dosya için bir işlemi sonlandır görevi oluşturun ve tekrar deneyin.

İşlem başlangıcı

İşlem başlangıcı görevini kullanarak dosyaları uzaktan çalıştırabilirsiniz. Örneğin, bilgisayar yapılandırma dosyasını oluşturan bir yardımcı programı uzaktan çalıştırabilirsiniz. Ardından, oluşturulan dosyayı Kaspersky Security Center Web Console'da almak için *Dosyayı al* görevini kullanabilirsiniz.

EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.

Bir İşlem başlangıcı görevi oluşturmak için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **İşlem başlangıcı** seçimini yapın.

   c. **Görev adı** alanına kısa bir açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri**'ye tıklayın.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri**'ye tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Son** düğmesine tıklayarak sihirbazı sonlandırın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.

8. Görev özellikleri penceresi açılır.

9. **Uygulama ayarları** sekmesini seçin.

10. İşlem başlangıcı komutunu girin.

Bilgisayarın yapılandırmasıyla ilgili bilgileri geçerli klasördeki (varsayılan olarak) `conf.txt` adlı bir dosyaya kaydeden bir yardımcı program (`utility.exe`) çalıştırmak istediğinizi varsayalım. Yardımcı program `C:\Users\admin\Diagnostic\` klasöründedir. Yapılandırma dosyasını `C:\Users\admin\Documents\Configuration` klasörüne kaydetmelisiniz. Aşağıdaki değerleri girin:

- **Yürütülebilir komut** - `C:\Users\admin\Diagnostic\utility.exe`
- **Komut satırı argümanları (isteğe bağlı)** - `/R conf.txt`
- **Çalışma klasörü yolu (isteğe bağlı)** - `C:\Users\admin\Documents\Configuration`

11. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.
12. Görev zamanlamasını yapılandırın.

    Wake-on-LAN bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. Değişikliklerinizi kaydedin.
14. Görevin yanındaki onay kutusunu seçin.
15. **Başlat**'a tıklayın.

    Sonuç olarak Kaspersky Endpoint Security, komutu sessiz modda çalıştırır ve işlemi başlatır. Görevin sonuçlarını **Yürütme sonuçları** bölümündeki görev özelliklerinden izleyebilirsiniz.

İşlemi sonlandır

İşlemi sonlandır görevini kullanarak işlemleri uzaktan sonlandırabilirsiniz. Örneğin, *İşlem başlangıcı* görevi kullanılarak başlatılan bir internet hız testi uzaktan sonlandırabilirsiniz.

Bir dosyanın çalışmasını yasaklamak istiyorsanız Yürütme önleme bileşenini yapılandırabilirsiniz. Yürütülebilir dosyaların, komut dosyalarının, ofis dosyalarının yürütülmesini yasaklayabilirsiniz.

İşlemi sonlandır görevi aşağıdaki şu sahiptir:

Kaspersky Endpoint Security for Windows'un çalışması için gereken dosya işlemlerini sonlandıramazsınız:

- Kaspersky Endpoint Security for Windows'un Kendini Savunma teknolojisi kapsamındaki dosyalar
- Kaspersky tarafından dijital olarak imzalanmış dosyalar

EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.

Bir İşlemi sonlandır görevi oluşturmak için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. **Ekle**'ye tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows 14.2** seçimini yapın.

   b. **Görev türü** açılır listesinde, **İşlemi sonlandır**'ı seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

   d. **Görevin atanacağı cihazlar** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri**'ye tıklayın.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri**'ye tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Son** düğmesine tıklayarak sihirbazı sonlandırın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. Gerekirse **Sistem için kritik nesnelere uygula** onay kutusunu seçin.

   System Critical Object'ler (SCO'lar), işletim sisteminin çalışması için gereken dosyaları içerir.

   SCO dosyalarına eylem uygulamanızı önermeyiz. Bu, işletim sisteminin kararsız hâle gelmesine veya önyükleme yapamamasına neden olabilir.

10. İşlemi tamamlamak için sonlandırmak istediğiniz dosyayı seçmelisiniz. Aşağıdaki yöntemlerden biriyle bir dosya seçebilirsiniz:

    - Dosyanın tam adını girin.
    - Dosyanın karmasını ve dosyanın yolunu girin.
    - Sürecin PID'sini girin (yalnızca yerel görevler için).
    - Dosya bir ağ sürücüsünde bulunuyorsa, sürücü harfini değil `\\` ile başlayan dosya yolunu girin. Örneğin, `\\server\shared_folder\file.exe`. Dosya yolu bir ağ sürücüsü harfi içeriyorsa, bir *Dosya bulunamadı* hatası alabilirsiniz.

Dosya bir ağ sürücüsünde bulunuyorsa, sürücü harfini değil `\\` ile başlayan dosya yolunu girin. Örneğin, `\\server\shared_folder\file.exe`. Dosya yolu bir ağ sürücüsü harfi içeriyorsa, bir *Dosya bulunamadı* hatası alabilirsiniz.

11. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

12. Görev zamanlamasını yapılandırın.

    Wake-on-LAN bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. **Kaydet**'e tıklayın.

14. Görevin yanındaki onay kutusunu seçin.

15. **Başlat**'a tıklayın.

    Böylece Kaspersky Endpoint Security bilgisayardaki işlemi sonlandırır. Örneğin bir GAME uygulaması çalışıyorsa ve game.exe işlemini sonlandırırsanız, uygulama veri kaydı yapılmadan kapanır. Görevin sonuçlarını **Sonuçlar** bölümündeki görev özelliklerinden izleyebilirsiniz.

Yürütme önleme

Yürütme önleme, yürütülebilir dosyaların ve komut dosyalarının çalıştırılmasının yanı sıra ofis biçimindeki dosyaların açılmasının yönetilmesine de olanak tanır. Bu şekilde, örneğin güvenli olmadığını düşündüğünüz uygulamaların yürütülmesini engelleyebilirsiniz. Sonuç olarak, tehdidin yayılması durdurulabilir. Yürütme önleme bir ofis dosyası uzantıları grubunu ve bir komut dizisi yorumlayıcısı grubunu destekler.

Yürütme önleme kuralı

Yürütme önleme, dosyalara kullanıcı erişimini yürütme önleme kuralları aracılığıyla yönetir. *Yürütme önleme kuralı* bir nesne yürütmesine tepki verirken, örneğin nesne yürütmesini engellerken, uygulamanın dikkate aldığı bir dizi kriterdir. Uygulama, dosyaları yollarına veya MD5 ve SHA256 karma algoritmaları kullanılarak hesaplanan sağlama toplamlarına göre tanımlar.

Yürütme önleme kuralları oluşturabilirsiniz:

- Uyarı ayrıntılarında (sadece EDR Optimum için).

  Uyarı Ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

- Bir grup ilkesi veya yerel uygulama ayarları kullanma.

  Dosya yolunu veya karmasını (SHA256 ya da MD5) ya da klasör yolunu ve dosya karmasını girmelisiniz.

Yürütme önleme yönetimini, komut satırı ile yerel olarak da yönetebilirsiniz.

Yürütme önleme şu sınırlamalara sahiptir:

1. Önleme kuralları CD'lerdeki ya da ISO görüntülerindeki dosyaları kapsamaz. Uygulama, bu dosyaların yürütülmesini veya açılmasını engellemez.
2. Kaspersky Endpoint Security for Windows'un çalışması için gereken dosyalara önleme kuralı uygulayamazsınız:
   - Kaspersky Endpoint Security for Windows'un Kendini Savunma teknolojisi kapsamındaki dosyalar
   - Kaspersky tarafından dijital olarak imzalanmış dosyalar
3. Sistem kararsızlığına neden olabileceği için 5000'den fazla çalışma önleme kuralının oluşturulması önerilmez.

Yürütme önleme kuralı modları

Yürütme önleme bileşeni iki modda çalışabilir:

- **Sadece istatistikler**

  Bu modda Kaspersky Endpoint Security, Windows olay günlüğü ve Kaspersky Security Center ile önleme kuralı kriterleriyle eşleşen yürütülebilir nesneleri veya açık belgeleri yürütme girişimleri hakkında bir olay yayınlar, ancak nesneyi veya belgeyi yürütme veya açma girişimini engellemez. Varsayılan olarak bu mod seçilidir.

- **Etkin**

  Bu modda, uygulama, engelleme kuralı kriterlerine uyan nesnelerin yürütülmesini veya belgelerin açılmasını engeller. Uygulama ayrıca Windows olay günlüğüne ve Kaspersky Security Center olay günlüğüne nesneleri çalıştırma veya belgeleri açma girişimleri hakkında bir olay yayınlar.

Yürütme önleme yönetimi

Bileşen ayarlarını yalnızca Web Console'da yapılandırabilirsiniz.

Yürütmeyi önlemek için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.
5. **Yürütme Önleme** sekmesini seçin.
6. **Yürütme Önleme ETKİN** iki durumlu düğmesini açık duruma getirin.

7. **Yasak nesnenin yürütülmesi veya açılması ile ilgili eylem** bloğundan bileşen çalışma modunu seçin:

   - **Engelle ve olay günlüğüne ekle**. Bu modda, uygulama, engelleme kuralı kriterlerine uyan nesnelerin yürütülmesini veya belgelerin açılmasını engeller. Uygulama ayrıca Windows olay günlüğüne ve Kaspersky Security Center olay günlüğüne nesneleri çalıştırma veya belgeleri açma girişimleri hakkında bir olay yayınlar.

     Gerekirse **Sistem için kritik nesnelere uygula** onay kutusunu seçin. System Critical Object'ler (SCO'lar), işletim sisteminin çalışması için gereken dosyaları içerir.

     > SCO dosyalarına eylem uygulamanızı önermeyiz. Bu, işletim sisteminin kararsız hâle gelmesine veya önyükleme yapamamasına neden olabilir.

   - **Olay günlüğüne ekle**. Bu modda Kaspersky Endpoint Security, Windows olay günlüğü ve Kaspersky Security Center ile önleme kuralı kriterleriyle eşleşen yürütülebilir nesneleri veya açık belgeleri yürütme girişimleri hakkında bir olay yayınlar, ancak nesneyi veya belgeyi yürütme veya açma girişimini engellemez. Varsayılan olarak bu mod seçilidir.

8. Bir yürütme önleme kuralları listesi oluşturun:

   a. **Ekle**'ye tıklayın.

   b. Bu bir pencere açar; bu pencereye yürütme önleme kuralının adını girin (örneğin, *Uygulama A*).

   c. **Tür** açılır listesinden engellemek istediğiniz nesneyi seçin: **Yürütülebilir dosya**, **Komut dizisi**, **Microsoft Office belgesi**.

      Yanlış bir nesne türü seçerseniz Kaspersky Endpoint Security dosyayı veya komut dosyasını engellemez.

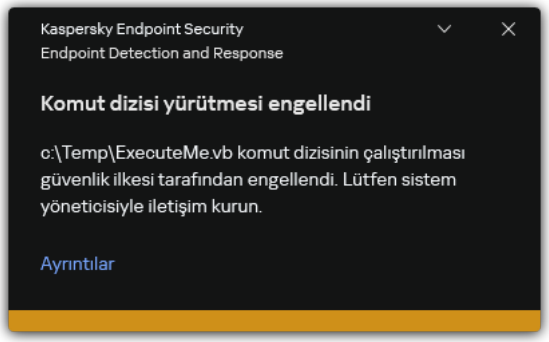
   d. Dosyayı eklemek için dosyanın karmasını (SHA256 ya da MD5), dosyanın tam yolunu ya da karmayı ve klasör yolunu girmelisiniz.

      > Dosya bir ağ sürücüsünde bulunuyorsa, sürücü harfini değil `\\` ile başlayan dosya yolunu girin. Örneğin, `\\server\shared_folder\file.exe`. Dosya yolu bir ağ sürücüsü harfi içeriyorsa Kaspersky Endpoint Security dosyayı veya komut dosyasını engellemez.

      Yürütme önleme bir ofis dosyası uzantıları grubunu ve bir komut dizisi yorumlayıcısı grubunu destekler.

9. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security nesnelerin yürütülmesini engeller: yürütülebilir dosyaları ve komut dizilerini çalıştırma, ofis biçimindeki dosyaları açma. Bununla birlikte, örneğin, komut dizisinin çalıştırılması engellenmiş olsa bile, bir komut dizisini bir metin düzenleyicide açabilirsiniz. Bir nesnenin yürütülmesini engellendiğinde, bildirimler uygulama ayarlarında etkinleştirildiyse Kaspersky Endpoint Security standart bir bildirim görüntüler (aşağıdaki şekle bakın).



Yürütme önleme bildirimi

Bilgisayar ağ izolasyonu

Bilgisayar ağı izolasyonu, bir güvenlik ihlali göstergesinin (IOC) algılanmasına yanıt olarak bir bilgisayarın ağdan otomatik olarak izole edilmesine olanak tanır, bu *otomatik mod* olarak adlandırılır. Tespit edilen tehdidi araştırırken Ağ izolasyonunu manuel olarak açabilirsiniz - bu *manuel mod* olarak adlandırılır.

Ağ izolasyonu açıldığında, uygulama tüm etkin bağlantıları keser ve aşağıdaki istisnalar hariç olmak üzere bilgisayardaki tüm yeni TCP/IP ağ bağlantılarını engeller:

- Ağ izolasyonu istisnalarında listelenen bağlantılar.
- Kaspersky Endpoint Security hizmetleri tarafından başlatılan bağlantılar.
- Kaspersky Security Center Ağ Aracısı tarafından başlatılan bağlantılar.
- Uygulama Light Agent modunda kullanılıyorsa SVM ve Entegrasyon Sunucusuna bağlantılar.
- Uygulamayı Kaspersky Managed Detection and Response ile entegre ederken KSN ile kurulan bağlantılar.

Bileşen ayarlarını yalnızca Web Console'da yapılandırabilirsiniz.

Otomatik Ağ izolasyonu modu

Bir IOC algılamasına yanıt olarak Ağ izolasyonunu otomatik olarak açılacak şekilde yapılandırabilirsiniz. Otomatik Ağ izolasyonu modunu bir grup ilkesiyle yapılandırabilirsiniz.

Bir IOC algılamasına yanıt olarak Ağ izolasyonunu otomatik olarak açılacak şekilde yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **IOC Taraması** görevine tıklayın.

   Görev özellikleri penceresi açılır.

   Gerekirse *IOC Taraması* görevi oluşturun.

3. **Uygulama ayarları** sekmesini seçin.

4. **Yanıt ayarları** bölümünü seçin.

5. **IOC algılandığında yanıt eylemlerini yapılandır** bloğunda **Uyarı ve yanıt** seçeneğini belirleyin ve **Cihazı ağdan izole et** onay kutusunu seçin.

6. Değişikliklerinizi kaydedin.

Sonuç olarak, bir IOC tespit edildiğinde uygulama, tehdidin yayılmasını önlemek için bilgisayarı ağdan izole eder.

Otomatik Ağ izolasyonunu belirli bir süre sonra devre dışı bırakılacak şekilde yapılandırabilirsiniz. Uygulama varsayılan olarak açılmasının üzerinden 8 saat geçtikten sonra Ağ izolasyonunu kapatır. Ağ izolasyonunu manuel olarak da kapatabilirsiniz (aşağıdaki talimatlara bakın). Ağ izolasyonunu kapattıktan sonra, bilgisayar Ağı kısıtlamaları olmadan kullanabilir.

Otomatik modda bir bilgisayarın ağ izolasyonunu kapatmak için gecikme süresi yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

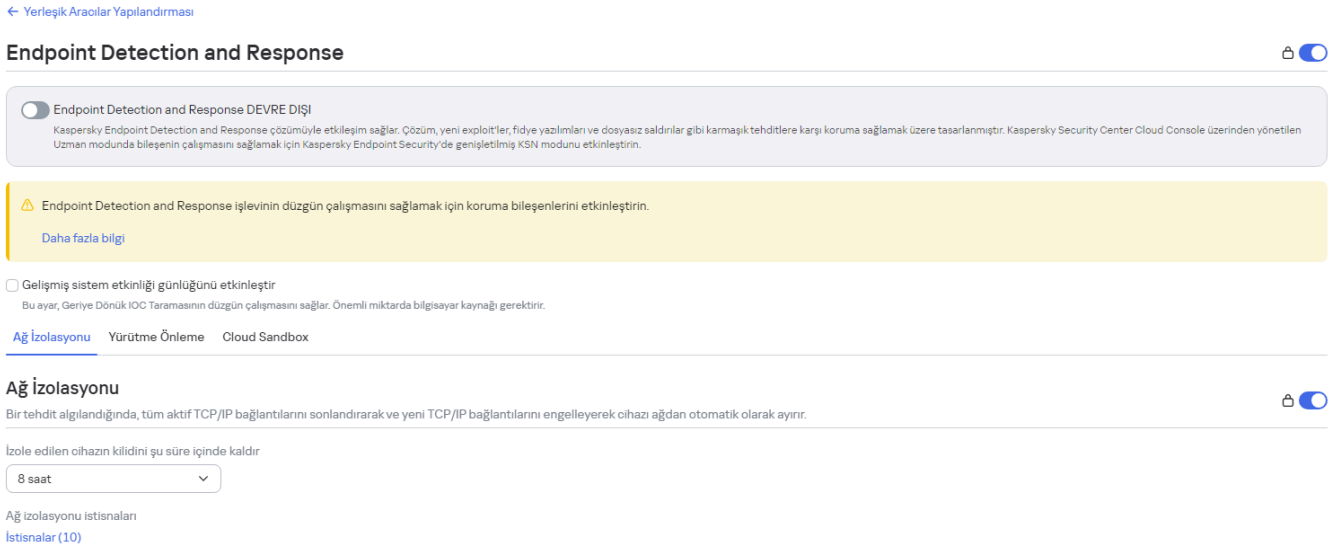
3. **Uygulama ayarları** sekmesini seçin.

4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.

5. **Ağ İzolasyonu** sekmesini seçin.

6. Ağ izolasyonunu kapatma gecikme süresini seçin.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.



EDR entegrasyon ayarları

Manuel Ağ izolasyonu modu

Ağ izolasyonunun manuel olarak açıp kapatılması mümkündür. Kaspersky Security Center konsolundaki bilgisayar özelliklerini kullanarak manuel Ağ izolasyonu modunu yapılandırabilirsiniz.

Ağ izolasyonunu açabilirsiniz:

- Uyarı ayrıntılarında (sadece EDR Optimum için).

  Uyarı Ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

- Yerel uygulama ayarlarını kullanma.

- *IOC Taraması* görev ayarları.

  IOC Taraması görevi bir IOC tespit ederse, bilgisayarı doğrudan IOC'den ağdan izole edebilirsiniz (*IOC Taraması* özellikleri → **Uygulama ayarları** → **IOC Taraması sonuçları** görevi). Kaspersky Endpoint Security ayrıca ek ayarların hemen yönetilmesini sağlar: Ağ izolasyonu devre dışı bırakma süresi ve Ağ izolasyonu istisnaları.

Bir bilgisayarın ağ izolasyonunu manuel olarak açma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.

   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows 14.2** öğesine tıklayın.

   Bu, yerel uygulama ayarlarını açar.
5. **Uygulama ayarları** sekmesini seçin.
6. **Detection and Response** → **Endpoint Detection and Response** bölümüne gidin.
7. **Ağ izolasyonu** bloğundan **Bilgisayarı ağdan izole et** seçeneğine tıklayın.

Otomatik Ağ izolasyonunu belirli bir süre sonra devre dışı bırakılacak şekilde yapılandırabilirsiniz. Uygulama varsayılan olarak açılmasının üzerinden 8 saat geçtikten sonra Ağ izolasyonunu kapatır. Ağ izolasyonunu kapattıktan sonra, bilgisayar Ağı kısıtlamaları olmadan kullanabilir.

Manuel modda bir bilgisayarın ağ izolasyonunu kapatmak için gecikme süresi yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.

   Bu, bilgisayar özelliklerini açar.
3. **Görevler** sekmesini seçin.

   Bu, bilgisayarda kullanılabilir olan görevlerin listesini görüntüler.

4. **Ağ izolasyonu** görevini seçin.
5. **Uygulama ayarları** sekmesini seçin.
6. Bir pencere açılır, bu pencerede Ağ izolasyonunu kapatma gecikmesini seçin.
7. Değişikliklerinizi kaydedin.

Bir bilgisayarın ağ izolasyonunu manuel olarak kapatma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows 14.2** öğesine tıklayın.
   Bu, yerel uygulama ayarlarını açar.
5. **Uygulama ayarları** sekmesini seçin.
6. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.
7. **Ağ izolasyonu** bloğundan **Ağdan izole edilmiş bilgisayarın kilidini kaldır** seçeneğine tıklayın.

Ağ izolasyonunu, komut satırı ile yerel olarak da kaldırabilirsiniz.

Windows için Kaspersky Endpoint Security 12.10 ile başlayarak, uyarı ayrıntılarında Ağ İzolasyonunu yönetebilirsiniz. Ek olarak, uyarı ayrıntılarında bilgisayar Ağ İzolasyonu zaman periyodunu belirleyebilirsiniz. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

Ağ izolasyonu istisnaları

Ağ izolasyonu istisnalarını yapılandırabilirsiniz. Ağ izolasyonu açıkken bilgisayarda kurallarla eşleşen ağ bağlantıları engellenmez.

Ağ izolasyonu istisnalarını yapılandırmak için bir *standart ağ profilleri* listesi kullanabilirsiniz. Varsayılan olarak, istisnalar, DNS/DHCP sunucusu ve DNS/DHCP istemci rollerine sahip cihazların kesintisiz çalışmasını sağlayan kuralları barındıran ağ profillerini içerir. İsterseniz standart ağ profillerinin ayarlarını değiştirebilir ya da istisnaları manuel olarak tanımlayabilirsiniz (aşağıdaki talimatlara bakın).

İlke özelliklerinde belirtilen istisnalar, yalnızca algılanan bir tehdide yanıt olarak Ağ izolasyonu otomatik olarak açılırsa uygulanır. Bilgisayar özelliklerinde belirtilen istisnalar, yalnızca Kaspersky Security Center konsolundaki bilgisayar özelliklerinde veya uyarı ayrıntılarında Ağ izolasyonu manuel olarak açılırsa uygulanır.

Etkin bir ilke, bu parametreler farklı kullanım senaryolarına sahip olduğundan, bilgisayar özelliklerinde yapılandırılan Ağ izolasyonundan hariç tutma istisnalarının uygulanmasını engellemez.

Otomatik modda ağ izolasyonu istisnası ekleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.
5. **Ağ İzolasyonu** sekmesini seçin.
6. **Ağ izolasyonu istisnaları** bloğundan, **İstisnalar**'a tıklayın.
7. Böylece bir pencere açılır; bu pencereden **Ekle** → **Profilden ekle** seçeneklerine tıklayın ve istisnaları yapılandırma için standart ağ profillerini seçin.

   Profildeki ağ izolasyonu istisnaları, Ağ izolasyonu istisnaları listesine eklenir. Ağ bağlantılarının özelliklerini görüntüleyebilirsiniz. Gerekirse ağ bağlantısı ayarlarını değiştirebilirsiniz.
8. Gerekirse, manuel olarak bir Ağ izolasyonu istisnası ekleyin. Bunu yapmak için, istisnalar listesinin bulunduğu pencerede **Ekle** → **Ekle** seçeneklerine tıklayın ve ağ bağlantısı ayarlarını manuel olarak düzenleyin.
9. Değişikliklerinizi kaydedin.

Manuel modda ağ izolasyonu istisnası ekleme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.

   Bu, bilgisayar özelliklerini açar.
3. **Görevler** sekmesini seçin.

   Bu, bilgisayarda kullanılabilir olan görevlerin listesini görüntüler.
4. **Ağ izolasyonu** görevini seçin.
5. **Uygulama ayarları** sekmesini seçin.
6. Bir pencere açılır, bu pencerede **İstisnalar**'a tıklayın.
7. Böylece bir pencere açılır; bu pencereden **Profilden ekle**'ye tıklayın ve istisnaları yapılandırma için standart ağ profillerini seçin.

   Profildeki ağ izolasyonu istisnaları, Ağ izolasyonu istisnaları listesine eklenir. Ağ bağlantılarının özelliklerini görüntüleyebilirsiniz. Gerekirse ağ bağlantısı ayarlarını değiştirebilirsiniz.
8. Gerekirse, manuel olarak bir Ağ izolasyonu istisnası ekleyin. Bunu yapmak için, istisnalar listesinin bulunduğu pencerede **Ekle**'ye tıklayın ve ağ bağlantısı ayarlarını manuel olarak düzenleyin.
9. Değişikliklerinizi kaydedin.

Ağ izolasyonu istisnasını, komut satırı ile yerel olarak da görüntüleyebilirsiniz. Bu durumda bilgisayar izole edilmelidir.

Windows için Kaspersky Endpoint Security 12.10 ile başlayarak, uyarı ayrıntılarına Ağ izolasyonu İstisnalarını ekleyebilirsiniz. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

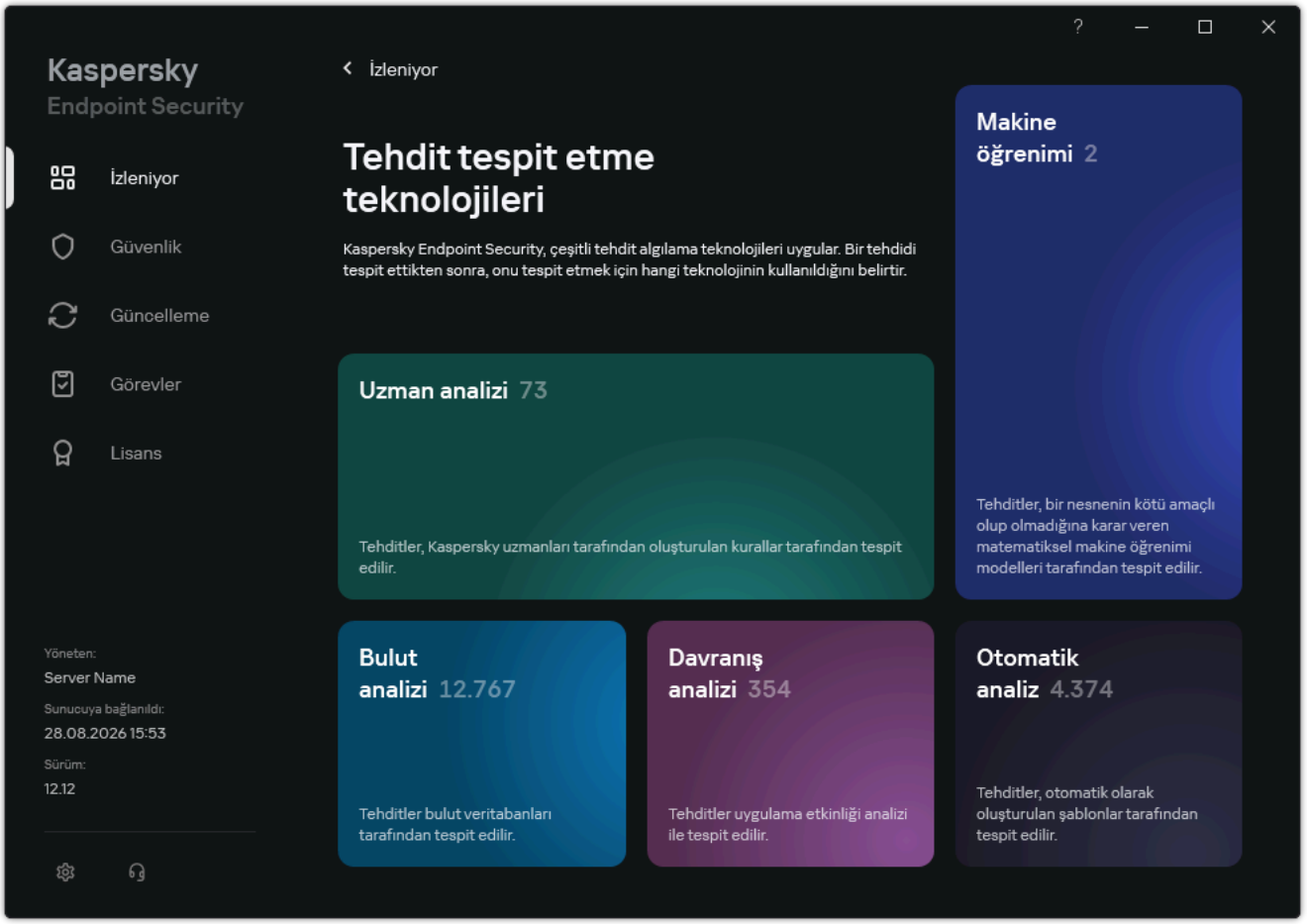
Cloud Sandbox

Cloud Sandbox bir bilgisayardaki gelişmiş tehditleri tespit etmenizi sağlayan bir teknolojidir. Kaspersky Endpoint Security, tespit edilen dosyaları analiz edilmek üzere otomatik olarak Cloud Sandbox'a iletir. Cloud Sandbox, kötü amaçlı etkinlikleri belirlemek için bu dosyaları yalıtılmış bir ortamda çalıştırır ve tanınırlıklarına göre karar verir. Bu dosyalardaki veriler daha sonra Kaspersky Security Network'e gönderilir. Bu nedenle, Cloud Sandbox kötü amaçlı bir dosya algıladığında, Kaspersky Endpoint Security bu dosyanın algılandığı tüm bilgisayarlarda bu tehdidi ortadan kaldırmak üzere uygun eylemi gerçekleştirir.

Cloud Sandbox'un çalışması için Kaspersky Security Network kullanımını etkinleştirmeniz gerekir.

Kaspersky Private Security Network kullanıyorsanız Cloud Sandbox teknolojisi kullanılamaz.

Cloud Sandbox teknolojisi kalıcı olarak etkinleştirilir ve kullandıkları lisans türünden bağımsız olarak tüm Kaspersky Security Network kullanıcıları tarafından kullanılabilir. Endpoint Detection and Response Optimum çözümünü zaten dağıttıysanız Cloud Sandbox tarafından algılanan tehditler için ayrı bir sayaç etkinleştirebilirsiniz. Algılanan tehditleri analiz ederken istatistik oluşturmak için bu sayacı kullanabilirsiniz. Kaspersky Endpoint Security, Kaspersky Security Center konsolundaki *Tehdit raporunda* Cloud Sandbox tehdit algılama teknolojisini gösterir.



Tehdit sayaçları

Cloud Sandbox sayacını etkinleştirmek için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response** bölümüne gidin.
5. **Cloud Sandbox** sekmesini seçin.
6. **Cloud Sandbox ETKİN** düğmesini açık konumuna getirin.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Bir tehdit olduğunda Kaspersky Endpoint Security, **Tehdit tespit etme teknolojileri** altındaki ana uygulama penceresinde yer alan Cloud Sandbox'u kullanarak algılanan tehditler için sayacı etkinleştirir. Kaspersky Endpoint Security, Kaspersky Security Center konsolundaki *Tehdit raporunda* Cloud Sandbox tehdit tespit etme teknolojisini de gösterecek.

Endpoint Detection and Response ilke bölümü

EDR Optimum için KEA'dan KES'e Geçiş Kılavuzu

Kaspersky Endpoint Security for Windows, artık Kaspersky Endpoint Detection and Response Optimum çözümü için yerleşik bir aracıya sahip. EDR Optimum ile çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok. Tüm Kaspersky Endpoint Agent işlevleri Kaspersky Endpoint Security tarafından gerçekleştirilecektir.

Kaspersky Endpoint Agent yüklü bilgisayarlara Kaspersky Endpoint Security dağıttığınızda, Kaspersky Endpoint Detection and Response Optimum çözümü Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır. Kaspersky Endpoint Security'yi 11.7.0 veya daha üst bir sürüme güncellediğinizde sistemde aynı davranış ortaya çıkar.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent ile uyumlu değildir. Bu uygulamaların her ikisini de aynı bilgisayara yükleyemezsiniz.

Kaspersky Endpoint Security'nin Kaspersky Endpoint Detection and Response Optimum bir parçası olarak çalışması için şu koşulların karşılanması gerekir:

- Kaspersky Endpoint Detection and Response Optimum sürüm 2.0 veya üstü.
- Kaspersky Security Center sürüm 13.2 veya üstü (Network Agent dahil). Kaspersky Security Center'ın önceki sürümlerinde EDR Optimum özelliğini etkinleştirmek mümkün değildir.
- EDR Optimum özellikleri, yalnızca Kaspersky Security Center Web Console kullanılarak yönetilebilir.

- Yönetim Sunucusu'na veri aktarımı etkinleştirildi. Veriler, bir bilgisayarda karantinaya alınan dosyalar hakkında Web Console aracılığıyla bilgi almak için gereklidir.
- Kaspersky Security Center Web Console ile Yönetim Sunucusu arasında bir arka plan bağlantısı kuruldu. EDR Optimum bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için yeni bir güvenli bir bağlantı, yani bir *arka plan bağlantısı* kurmanız da şarttır.

EDR Optimum için [KES+KEA] yapılandırmasını [KES+yerleşik aracı]'ya taşıma adımları

1. **Kaspersky Endpoint Security web eklentisini yükseltme**

   EDR Optimum bileşeni, Kaspersky Endpoint Security Web Eklentisi sürüm 11.7.0 veya üstü kullanılarak yönetilebilir.

2. **İlkelerin ve görevlerin taşınması**

   Kaspersky Endpoint Agent ayarlarını Kaspersky Endpoint Security for Windows'a aktarın. Bunu yapmak için Web Console'daki Kaspersky Endpoint Agent'tan geçiş sihirbazını kullanın.

   Web Console'da Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye ilke ve görev ayarlarını taşıma

   Web Console ana penceresinde, **İşlemler** → **Kaspersky Endpoint Agent'tan Geçiş** seçimini yapın.

   Böylece ilke ve görev geçiş sihirbazı çalıştırılır. Sihirbazın talimatlarını uygulayın.

   1. Adım. İlke geçişi

   Geçiş Sihirbazı, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent ilkelerinin ayarlarını birleştiren yeni bir ilke oluşturur. İlke listesinden, ayarlarını Kaspersky Endpoint Security ilkesiyle birleştirmek istediğiniz Kaspersky Endpoint Agent ilkelerini seçin. Ayarları birleştirmek istediğiniz Kaspersky Endpoint Security ilkesini seçmek için Kaspersky Endpoint Agent ilkesine tıklayın. Doğru ilkeleri seçtiğinizden emin olun ve sonraki adıma geçin.

   2. Adım. Görev geçişi

   Geçiş Sihirbazı, Kaspersky Endpoint Security için yeni görevler oluşturur. Görev listesinden, Kaspersky Endpoint Security ilkesi için oluşturmak istediğiniz Kaspersky Endpoint Agent görevlerini seçin. Bir sonraki adıma geçin.

   3. Adım Sihirbazı tamamlama

   Sihirbazı tamamlayın. Sonuç olarak, sihirbaz şunları yapar:

   - Yeni bir Kaspersky Endpoint Security ilkesi oluşturur.

İlke, Kaspersky Endpoint Security'den ve Kaspersky Endpoint Agent'tan gelen ayarları birleştirir. Bu ilkeye *<Kaspersky Endpoint Security ilke adı> & <Kaspersky Endpoint Agent ilke adı>* adı verilir. Yeni ilke *Etkin değil* durumundadır. Devam etmek için Kaspersky Endpoint Agent ve Kaspersky Endpoint Security ilkelerinin durumlarını *Etkin değil* olarak değiştirtin ve yeni birleştirilmiş ilkeyi etkinleştirin.

Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçiş yapıldıktan sonra, lütfen yeni ilkenin Yönetim Sunucusu kurulumuna veri aktarımı (karantina dosyası verileri ve tehdit geliştirme zinciri verileri) işlevine sahip olduğundan emin olun. bir Kaspersky Endpoint Agent ilkesinden veri aktarımı parametresi değerleri taşınmaz.

- Yeni Kaspersky Endpoint Security görevleri oluşturur.

  Yeni görevler, Kaspersky Endpoint Agent görevlerinin kopyalarıdır. Aynı zamanda, Sihiirbaz Kaspersky Endpoint Agent görevlerini değiştirmeden bırakır.

3. **EDR Optimum işlevselliğinin lisanslanması**

Kaspersky Endpoint Security for Windows ve Kaspersky Endpoint Agent'ı etkinleştirmek için ortak bir Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security lisansı kullanıyorsanız, EDR Optimum işlevi uygulama sürüm 11.7.0 veya üstüne yükseltildikten sonra otomatik olarak etkinleştirilecektir. Başka bir şey yapmanız gerekmez.

EDR Optimum işlevini etkinleştirmek için bağımsız bir Kaspersky Endpoint Detection and Response Optimum Eklentisi lisansı kullanıyorsanız, EDR Optimum anahtarının Kaspersky Security Center veri havuzuna eklendiğinden ve otomatik lisans anahtarı dağıtım işlevinin etkinleştirildiğinden emin olmalısınız. EDR Optimum işlevi, uygulamayı sürüm 11.7.0 veya üstüne yükselttikten sonra otomatik olarak etkinleştirilir.

Kaspersky Endpoint Agent'ı etkinleştirmek için Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security lisansı ve Kaspersky Endpoint Security for Windows'u etkinleştirmek için farklı bir lisans kullanıyorsanız, Kaspersky Endpoint Security for Windows anahtarını, ortak Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security anahtarıyla değiştirmelisiniz. Anahtarı, *Anahtar ekle* görevini kullanarak değiştirebilirsiniz.

4. **Kaspersky Endpoint Security uygulamasını Yükleme/Yükseltme**

Bir uygulama kurulumu veya yükseltmesi sırasında EDR Optimum işlevselliğini taşımak için uzaktan kurulum görevinin kullanılması önerilir. Bir uzaktan kurulum görevi oluştururken, kurulum paketi ayarlarında EDR Optimum bileşenini seçmeniz gerekir.

Uygulamayı, şu yöntemleri kullanarak da güncellemeniz mümkündür:

- Kaspersky güncelleme hizmetini kullanma.
- Kurulum Sihirbazını kullanarak yerel olarak.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent uygulamasının yüklü olduğu bir bilgisayarda uygulama yükseltilirken, bileşenlerin otomatik olarak seçilmesini destekler. Bileşenlerin otomatik seçimi, uygulamayı yükselten kullanıcı hesabının izinlerine bağlıdır.

Kaspersky Endpoint Security'yi sistem hesabı (SYSTEM) altındaki EXE veya MSI dosyasını kullanarak yükseltiyorsanız, Kaspersky Endpoint Security, Kaspersky çözümlerinin geçerli lisanslarına erişim kazanır. Dolayısıyla, bilgisayarda örneğin Kaspersky Endpoint Agent yüklü ve EDR Optimum çözümü etkinleştirildiyse, Kaspersky Endpoint Security yükleyicisi bileşen setini otomatik olarak yapılandırır ve EDR Optimum bileşenini seçer. Bu, Kaspersky Endpoint Security'nin bütünleşik aracıyı kullanmaya geçmesini sağlar ve Kaspersky Endpoint Agent'ı kaldırır. MSI yükleyicisinin sistem hesabı (SYSTEM) altında çalıştırılması genellikle Kaspersky güncelleme hizmeti aracılığıyla yükseltme yapılırken ya da Kaspersky Security Center aracılığıyla bir yükleme paketi dağıtılırken gerçekleştirilir.

Kaspersky Endpoint Security'yi ayrıcalıklı olmayan bir kullanıcı hesabı altında bir MSI dosyası kullanarak yükseltiyorsanız, Kaspersky Endpoint Security'nin Kaspersky çözümlerinin geçerli lisanslarına erişimi olmaz. Bu durumda Kaspersky Endpoint Security, bileşenleri Kaspersky Endpoint Agent yapılandırmasına göre otomatik olarak seçer. Bundan sonra, Kaspersky Endpoint Security' bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

Kaspersky Endpoint Security, bilgisayar yeniden başlatılmadan yükseltme yapılmasını destekler. İlke özelliklerinde uygulama yükseltme modunu seçebilirsiniz.

5. **Uygulama çalışmasının kontrolü**

   Uygulama yükleme veya yükseltmesi sonrasında bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

   - Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
   - *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, yerleşik aracı işlevselliğini etkinleştirdiğinizden emin olun.
   - Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.

Kaspersky Sandbox



Kaspersky Endpoint Security for Windows artık Kaspersky Sandbox çözümüyle entegrasyon için yerleşik bir aracı içeriyor. *Sandbox* bileşeni bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Sandbox Yardım ve Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Yerleşik aracının Kaspersky Sandbox ile entegrasyonu

Sandbox bileşeninin eklenmesi Kaspersky Sandbox ile entegrasyon için gereklidir. Sandbox bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken seçebilirsiniz.

Bileşeni kullanmak için aşağıdaki koşulların karşılanması gerekir:

- Kaspersky Security Center 13.2. Eski Kaspersky Security Center sürümleri, tehdit yanıtı için bağımsız IOC Taraması görevlerinin oluşturulmasına izin vermez.
- Bileşen yalnızca Web Console kullanılarak yönetilebilir. Bu bileşeni Yönetim Konsolu'nu (MMC) kullanarak yönetemezsiniz.
- Uygulama etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.
- Yönetim Sunucusu'na veri aktarımı etkinleştirildi.

  Kaspersky Sandbox'un tüm özelliklerini kullanmak için karantina dosyası veri aktarımının etkinleştirildiğinden emin olun. Veriler, bir bilgisayarda karantinaya alınan dosyalar hakkında Web Console aracılığıyla bilgi almak için gereklidir. Örneğin, Web Console'da analiz için karantinadan bir dosya indirebilirsiniz.

Web Console'da Yönetim Sunucusu'na veri aktarımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.
5. **Yönetim Sunucusu'na veri aktarımı** bloğundan **Karantina dosyaları hakkında** onay kutusunu işaretleyin.
6. Değişikliklerinizi kaydedin.

- Kaspersky Security Center Web Console ile Yönetim Sunucusu arasında bir arka plan bağlantısı kuruldu

  Kaspersky Sandbox'un bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için yeni bir güvenli bir bağlantı, yani bir *arka plan bağlantısı* kurmanız da şarttır. Kaspersky Security Center'ın diğer Kaspersky çözümleriyle entegre edilmesi hakkında ayrıntılı bilgi almak için Kaspersky Security Center Yardım içeriğine bakın.

  Web Console'da bir arka plan bağlantısı kurma

  1. Web Console ana penceresinden **Ayarlar** → **Tümleştirme** seçimini yapın.
  2. **Tümleştirme** bölümüne gidin.
  3. **Tümleştirme için bir arka plan bağlantısı Etkin** iki durumlu düğmesini açık duruma getirin.
  4. Değişikliklerinizi kaydedin.

  Kaspersky Security Center Web Console ile Yönetim Sunucusu arasında bir arka plan bağlantısı kurulmazsa, Tehdit Yanıtının bir parçası olarak bağımsız IOC taraması görevleri oluşturulamaz.

- Sandbox sunucusuyla güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Daha sonra bir ilke kullanarak sertifikayı bilgisayara eklemeniz gerekir. Sertifikayı Sandbox sunucusuna da eklemeniz gerekir.

  > Kripto konteyneri kullanarak iki yönlü kimlik doğrulama Kaspersky Sandbox için kullanılamaz.

  Komut satırı üzerinden Web Console'a yerel olarak bir TLS sertifikası ekleyebilirsiniz.

- Kaspersky Sandbox bileşeni etkinleştirilmelidir.
- Sandbox'un çalışmasını sağlayan uygulama bileşenleri etkin ve çalışır durumdadır. Aşağıdaki bileşenler Sandbox'un çalışmasını sağlar:
  - Dosya Tehdidi Koruması.
  - Sunucu Yetkisiz Erişim Önleme.
  - Güvenlik Duvarı.

- AMSI Koruması.
- Arka plan taraması.

Kaspersky Sandbox ile entegrasyonu etkinleştirmek veya devre dışı bırakmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Sandbox** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sandbox ile entegrasyon ETKİN** iki durumlu düğmesini kullanın.
6. **Entegrasyon modu** bloğunda, bileşen çalışma modunu seçin: **Kaspersky Sandbox**.
7. **Bağlantı ayarları** bağlantısına tıklayın.

   Sandbox sunucusu bağlantı ayarları penceresi açılır.
8. **Sunucu TLS sertifikası** bloğundan **Yükle**'ye tıklayın ve TLS sertifika dosyasını seçin.

   Kaspersky Endpoint Security, bir Sandbox sunucusu için yalnızca bir TLS sertifikasına sahip olabilir. Daha önce bir TLS sertifikası eklediyseniz, o sertifika iptal edilir. Yalnızca son eklenen sertifika kullanılır.
9. Sandbox sunucuları için gelişmiş bağlantı ayarlarını yapılandırın:

   - **Zaman aşımı (ms)**. Sandbox sunucusu için bağlantı zaman aşımı. Yapılandırılan zaman aşımı süresi geçtikten sonra Kaspersky Endpoint Security bir sonraki sunucuya bir istek gönderir. Bağlantı hızınız düşükse veya bağlantı dengesizse sunucu için bağlantı zaman aşımını artırabilirsiniz. Önerilen istek zaman aşımı 0,5 saniye veya daha kısadır.
   - **İstek kuyruğu**. İstek kuyruğu klasörünün boyutu. Sandbox'ta tarama için birden fazla nesne gönderirken Kaspersky Endpoint Security bir istek kuyruğu oluşturur. İstek kuyruğu klasörünün boyutu varsayılan olarak 100 MB ile sınırlandırılmıştır. Maksimum boyuta ulaşıldıktan sonra, Sandbox kuyruğa yeni isteklerin eklenmesini durdurur ve ilgili olayı Kaspersky Security Center'a gönderir. İstek kuyruğu klasörünün boyutunu sunucu yapılandırmanıza göre yapılandırabilirsiniz.
10. **Sandbox sunucularına bağlantı** bloğunda, **Ekle** düğmesine tıklayın.
11. Bir pencere açılır; bu pencerede, Sandbox sunucusunun adresini (IPv4, IPv6, DNS) ve portu girin.

    Sanal görüntüleri dağıtma ve Sandbox sunucularını yapılandırma hakkında ayrıntılar için Kaspersky Sandbox Yardım içeriğine bakın.
12. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security TLS dosyasını doğrular. Sertifika başarıyla doğrulanırsa Kaspersky Endpoint Security sertifika dosyasını Kaspersky Security Center ile bir sonraki senkronizasyon sırasında bilgisayara yükler. İki TLS sertifikası eklemeniz durumunda, Kaspersky Sandbox güvenilir bir bağlantı kurmak için en son sertifikayı kullanır. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Sandbox** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecek.

Kaspersky Sandbox ile entegrasyonu Web Konsolu'nda veya Komut satırını kullanarak yerel olarak etkinleştirebilir veya devre dışı bırakabilirsiniz.

Kaspersky Endpoint Security, Kaspersky Sandbox bileşeninin işleyişiyle ilgili bilgileri bir rapora kaydeder. Bu rapor hatalar hakkında bilgiler de içerir. Açıklaması `Error code: XXX` biçimi ile uyumlu bir hata alırsanız (örneğin, `0xa67b01f4`) Teknik Destek ile iletişim kurun.

Güvenlik ihlali göstergelerini tarayın (bağımsız görev)

Güvenlik İhlali Göstergesi (IOC) bilgisayara yetkisiz erişimi (verilerin ele geçirilmesi) gösteren bir nesne veya etkinlik hakkında bir dizi veridir. Örneğin, sistemde oturum açmaya yönelik birçok başarısız girişim, bir Güvenlik İhlali Göstergesi oluşturabilir. *IOC Taraması* görevi, bilgisayarda güvenlik ihlali göstergelerini bulmaya ve tehdit yanıtı önlemleri almaya olanak verir.

Kaspersky Endpoint Security, IOC dosyaları kullanarak güvenlik ihlali göstergelerini arar. *IOC dosyaları*, uygulamanın bir algılamayı saymak için eşleştirmeye çalıştığı gösterge gruplarını içeren dosyalardır. IOC dosyaları OpenIOC standardına uygun olmalıdır. Kaspersky Endpoint Security, Kaspersky Sandbox için otomatik olarak IOC dosyaları oluşturur.

IOC Taraması görevi çalışma modu

Uygulama, Kaspersky Sandbox için bağımsız IOC taraması görevleri oluşturur. *Bağımsız IOC taraması görevi*, Kaspersky Sandbox tarafından algılanan bir tehdide tepki verirken otomatik olarak oluşturulan bir grup görevidir. Kaspersky Endpoint Security, IOC dosyasını otomatik olarak oluşturur. Özel IOC dosyaları desteklenmez. Görevler, oluşturma zamanından 30 gün sonra otomatik olarak silinir. Bağımsız IOC tarama görevleri hakkında daha fazla ayrıntı için Kaspersky Sandbox Yardım içeriğine bakın.

IOC Taraması görev ayarları

Kaspersky Sandbox, tehditlere tepki verirken otomatik olarak *IOC Taraması* görevleri oluşturabilir ve çalıştırabilir.

Ayarları sadece Web Console'da yapılandırabilirsiniz.

Kaspersky Sandbox'un tüm bağımsız IOC Taraması görevlerinin çalışabilmesi için Kaspersky Security Center 13.2 gereklidir.

IOC Taraması görevinin ayarlarını değiştirmek için:

1. Web Console ana penceresinden **Görevler** seçimini yapın.

   Görevler listesi açılır.

2. Kaspersky Endpoint Security'nin **IOC Taraması** görevine tıklayın.

   Görev özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **IOC Taraması ayarları** bölümüne gidin.

5. IOC tespit edildiğinde uygulanacak eylem:

   - **Kopyayı Karantinaya taşı, nesneyi sil**. Bu seçenek tercihe dildiğinde, Kaspersky Endpoint Security bilgisayardaki kötü amaçlı nesneyi siler. Kaspersky Endpoint Security, nesneyi silmeden önce nesnenin daha sonra geri yüklenmesi gerekebileceği ihtimaline karşı bir yedek kopya oluşturur. Kaspersky Endpoint Security, yedek kopyayı Karantinaya taşır.

   - **Kritik Alanları Taramayı çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Critical Areas Scan* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.

   - **Sadece bilgisayar boştayken çalıştır**. Bilgisayar kaynakları meşgul olduğunda görevin başlatılması ertelenir. Kaspersky Endpoint Security, bilgisayar kilitliyse veya ekran koruyucu açıksa tarama görevini başlatır. Görevin yürütülmesini, örneğin bilgisayarın kilidini açarak durdurduysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır. Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.

6. Değişikliklerinizi kaydedin.

Görevin sonuçlarını **Sonuçlar** bölümündeki görev özelliklerinden izleyebilirsiniz. Algılanan güvenlik ihlali göstergeleri hakkındaki bilgileri görev özelliklerinde görüntüleyebilirsiniz: **Uygulama ayarları** → **IOC Taraması sonuçları**.

IOC taraması sonuçları 30 gün boyunca saklanır. Bu süre sonrasında Kaspersky Endpoint Security en eski kayıtları otomatik olarak siler.

Kaspersky Sandbox için KEA'dan KES'e Geçiş Kılavuzu

Kaspersky Endpoint Security for Windows artık Kaspersky Sandbox çözümü için yerleşik bir aracı içerir. Kaspersky Sandbox ile çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok. Tüm Kaspersky Endpoint Agent işlevleri Kaspersky Endpoint Security tarafından gerçekleştirilecektir.

Kaspersky Endpoint Agent yüklü bilgisayarlara Kaspersky Endpoint Security dağıttığınızda, Kaspersky Sandbox çözümü Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır. Kaspersky Endpoint Security'yi 11.7.0 veya daha üst bir sürüme güncellediğinizde sistemde aynı davranış ortaya çıkar.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent ile uyumlu değildir. Bu uygulamaların her ikisini de aynı bilgisayara yükleyemezsiniz.

Kaspersky Endpoint Security'nin Kaspersky Sandbox'un bir parçası olarak çalışması için şu koşulların karşılanması gerekir:

- Kaspersky Sandbox sürüm 2.0 veya üstü.

- Kaspersky Security Center sürüm 13.2 veya üstü (Network Agent dahil). Kaspersky Security Center'ın önceki sürümlerinde Kaspersky Sandbox özelliğini etkinleştirmek mümkün değildir.

- Kaspersky Sandbox, yalnızca Kaspersky Security Center Web Console kullanılarak yönetilebilir.
- Yönetim Sunucusu'na veri aktarımı etkinleştirildi. Veriler, bir bilgisayarda karantinaya alınan dosyalar hakkında Web Console aracılığıyla bilgi almak için gereklidir.
- Kaspersky Security Center Web Console ile Yönetim Sunucusu arasında bir arka plan bağlantısı kuruldu. Kaspersky Sandbox'un bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için yeni bir güvenli bir bağlantı, yani bir *arka plan bağlantısı* kurmanız da şarttır.

Kaspersky Sandbox için [KES+KEA] yapılandırmasını [KES+yerleşik aracı]'ya taşıma adımları

1. **Kaspersky Endpoint Security web eklentisini yükseltme**

   Kaspersky Sandbox bileşeni, Kaspersky Endpoint Security Web Eklentisi sürüm 11.7.0 veya üstü kullanılarak yönetilebilir.

2. **İlkelerin ve görevlerin taşınması**

   Kaspersky Endpoint Agent ayarlarını Kaspersky Endpoint Security for Windows'a aktarın. Bunu yapmak için Web Console'daki Kaspersky Endpoint Agent'tan geçiş sihirbazını kullanın.

   Web Console'da Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye ilke ve görev ayarlarını taşıma

   Web Console ana penceresinde, **İşlemler** → **Kaspersky Endpoint Agent'tan Geçiş** seçimini yapın.

   Böylece ilke ve görev geçiş sihirbazı çalıştırılır. Sihirbazın talimatlarını uygulayın.

   1. Adım. İlke geçişi

   Geçiş Sihirbazı, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent ilkelerinin ayarlarını birleştiren yeni bir ilke oluşturur. İlke listesinden, ayarlarını Kaspersky Endpoint Security ilkesiyle birleştirmek istediğiniz Kaspersky Endpoint Agent ilkelerini seçin. Ayarları birleştirmek istediğiniz Kaspersky Endpoint Security ilkesini seçmek için Kaspersky Endpoint Agent ilkesine tıklayın. Doğru ilkeleri seçtiğinizden emin olun ve sonraki adıma geçin.

   2. Adım. Görev geçişi

   Geçiş Sihirbazı, Kaspersky Endpoint Security için yeni görevler oluşturur. Görev listesinden, Kaspersky Endpoint Security ilkesi için oluşturmak istediğiniz Kaspersky Endpoint Agent görevlerini seçin. Bir sonraki adıma geçin.

   3. Adım Sihirbazı tamamlama

   Sihirbazı tamamlayın. Sonuç olarak, sihirbaz şunları yapar:

   - Yeni bir Kaspersky Endpoint Security ilkesi oluşturur.

İlke, Kaspersky Endpoint Security'den ve Kaspersky Endpoint Agent'tan gelen ayarları birleştirir. Bu ilkeye *<Kaspersky Endpoint Security ilke adı> & <Kaspersky Endpoint Agent ilke adı>* adı verilir. Yeni ilke *Etkin değil* durumundadır. Devam etmek için Kaspersky Endpoint Agent ve Kaspersky Endpoint Security ilkelerinin durumlarını *Etkin değil* olarak değiştirtin ve yeni birleştirilmiş ilkeyi etkinleştirin.

Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçiş yapıldıktan sonra, lütfen yeni ilkenin Yönetim Sunucusu kurulumuna veri aktarımı (karantina dosyası verileri ve tehdit geliştirme zinciri verileri) işlevine sahip olduğundan emin olun. bir Kaspersky Endpoint Agent ilkesinden veri aktarımı parametresi değerleri taşınmaz.

- Yeni Kaspersky Endpoint Security görevleri oluşturur.

  Yeni görevler, Kaspersky Endpoint Agent görevlerinin kopyalarıdır. Aynı zamanda, Sihiirbaz Kaspersky Endpoint Agent görevlerini değiştirmeden bırakır.

3 Kaspersky Sandbox işlevselliğini lisanslama

Kaspersky Sandbox çözümünün bir parçası olarak Kaspersky Endpoint Security'yi etkinleştirmek için ayrı bir Kaspersky Sandbox Eklentisi lisansına ihtiyacınız vardır. Anahtarı, *Anahtar ekle* görevini kullanarak ekleyebilirsiniz. Sonuç olarak, uygulamaya iki anahtar eklenecektir: *Kaspersky Endpoint Security* ve *Kaspersky Sandbox*.

4 Kaspersky Endpoint Security uygulamasını Yükleme/Yükseltme

Bir uygulama kurulumu veya yükseltmesi sırasında Kaspersky Sandbox işlevselliğini taşımak için uzaktan kurulum görevinin kullanılması önerilir. Bir uzaktan kurulum görevi oluştururken, kurulum paketi ayarlarında Kaspersky Sandbox bileşenini seçmeniz gerekir.

Uygulamayı, şu yöntemleri kullanarak da güncellemeniz mümkündür:

- Kaspersky güncelleme hizmetini kullanma.
- Kurulum Sihirbazını kullanarak yerel olarak.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent uygulamasının yüklü olduğu bir bilgisayarda uygulama yükseltilirken, bileşenlerin otomatik olarak seçilmesini destekler. Bileşenlerin otomatik seçimi, uygulamayı yükselten kullanıcı hesabının izinlerine bağlıdır.

Kaspersky Endpoint Security'yi sistem hesabı (SYSTEM) altındaki EXE veya MSI dosyasını kullanarak yükseltiyorsanız, Kaspersky Endpoint Security, Kaspersky çözümlerinin geçerli lisanslarına erişim kazanır. Dolayısıyla, bilgisayarda örneğin Kaspersky Endpoint Agent yüklü ve Kaspersky Sandbox çözümü etkinleştirildiyse, Kaspersky Endpoint Security yükleyicisi bileşen setini otomatik olarak yapılandırır ve Kaspersky Sandbox bileşenini seçer. Bu, Kaspersky Endpoint Security'nin bütünleşik aracıyı kullanmaya geçmesini sağlar ve Kaspersky Endpoint Agent'ı kaldırır. MSI yükleyicisinin sistem hesabı (SYSTEM) altında çalıştırılması genellikle Kaspersky güncelleme hizmeti aracılığıyla yükseltme yapılırken ya da Kaspersky Security Center aracılığıyla bir yükleme paketi dağıtılırken gerçekleştirilir.

Kaspersky Endpoint Security'yi ayrıcalıklı olmayan bir kullanıcı hesabı altında bir MSI dosyası kullanarak yükseltiyorsanız, Kaspersky Endpoint Security'nin Kaspersky çözümlerinin geçerli lisanslarına erişimi olmaz. Bu durumda Kaspersky Endpoint Security, bileşenleri Kaspersky Endpoint Agent yapılandırmasına göre otomatik olarak seçer. Bundan sonra, Kaspersky Endpoint Security' bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

Kaspersky Endpoint Security, bilgisayar yeniden başlatılmadan yükseltme yapılmasını destekler. İlke özelliklerinde uygulama yükseltme modunu seçebilirsiniz.

5 Uygulama çalışmasının kontrolü

Uygulama yükleme veya yükseltmesi sonrasında bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

- Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
- *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, yerleşik aracı işlevselliğini etkinleştirdiğinizden emin olun.
- Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security for Windows, Kaspersky Anti Targeted Attack Platform çözümü ile çalışmayı destekler. *Kaspersky Anti Targeted Attack Platform* hedeflenen saldırılar, gelişmiş sürekli tehditler (APT), sıfır gün saldırıları ve diğer karmaşık tehditleri zamanında tespit etmek üzere tasarlanmış bir çözümdür. Kaspersky Anti Targeted Attack Platform üç işlevsel birim içerir:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Tüm işlevsel birimleri veya tek tek işlevsel birimleri ayrı ayrı satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın. Uygulama, EDR, NDR bileşenleri için yerleşik aracılar içerir. Uygulama ayrıca KATA'nın bir parçası olan Sandbox bileşeni ile çalışmayı da desteklemektedir.

Tehdit İstihbarat araçları

Kaspersky Endpoint Detection and Response, aşağıdaki Threat Intelligence araçlarını kullanır:

- Dosyaların ve internet adreslerinin tanınırlığı hakkında bilgi içeren ve görüntüleyen Kaspersky Threat Intelligence Portal ile entegrasyon.
- Kaspersky Tehditler veritabanı.
- Kaspersky bilgi bankasından gerçek zamanlı dosya, web sitesi ve yazılım tanınırlık bilgilerine erişim sağlayan Kaspersky Security Network (bundan böyle "KSN" olarak anılacaktır) bulut hizmeti altyapısı. Kaspersky Security Network'ten gelen verilerin kullanılması Kaspersky uygulamalarının tehditlerle karşılaştığında verdiği tepki süresini kısaltır ve bazı koruma bileşenlerinin performansını iyileştirerek hatalı pozitif sonuç riskini azaltır.

Çözümün çalışma prensibi

Kaspersky Endpoint Security, kurumsal BT altyapısındaki bilgisayarlara yüklenir ve süreçleri, açık ağ bağlantılarını ve değiştirilmekte olan dosyaları sürekli olarak izler. Bilgisayardaki olaylarla ilgili bilgiler (telemetri verileri) Kaspersky Anti Targeted Attack Platform sunucusuna gönderilir. Bu durumda, Kaspersky Endpoint Security ayrıca uygulama tarafından keşfedilen tehditler ve bu tehditlerin işlenmesinden elde edilen sonuçlar hakkında Kaspersky Anti Targeted Attack Platform sunucusuna bilgiler gönderir.

EDR (KATA) ve NDR (KATA) entegrasyonu Kaspersky Security Center konsolunda yapılandırılır. Yerleşik aracı daha sonra Kaspersky Anti Targeted Attack Platform konsolu kullanılarak yönetilir; buna görevleri çalıştırma, karantinaya alınan nesneleri yönetme, raporları görüntüleme ve diğer eylemler dahildir.

EDR/NDR (KATA) ile çalışmak için Kaspersky Endpoint Security yapılandırmaları

EDR/NDR (KATA) ile çalışmak için şu yapılandırmalar kullanılabilir:

- **[KES+yerleşik aracı]**. Bu yapılandırmada, Kaspersky Endpoint Security hem bilgisayarın güvenliğini sağlayan uygulama hem de EDR/NDR (KATA) ile çalışma uygulaması olarak görev yapar. EDR (KATA) için yerleşik aracı, Kaspersky Endpoint Security 12.1 for Windows veya sonraki sürümlerde mevcuttur. NDR (KATA) için yerleşik aracı, Kaspersky Endpoint Security 12.7 for Windows veya sonraki sürümlerde mevcuttur.

- **[üçüncü taraf EPP+EDR Agent]**. Bu yapılandırmada, BT altyapısının güvenliği üçüncü taraf Endpoint Protection Platform (EPP) tarafından sağlanır. EDR/NDR (KATA) ile etkileşim, Endpoint Detection and Response Agent (EDR Agent) yapılandırmasında Kaspersky Endpoint Security tarafından sağlanır. EDR Agent bu yapılandırmada üçüncü taraf EPP uygulamalarıyla uyumludur. EDR (KATA) için EDR Agent, Kaspersky Endpoint Security 12.3 for Windows veya sonraki sürümlerde mevcuttur. NDR (KATA) için EDR Agent, Kaspersky Endpoint Security 12.7 for Windows veya sonraki sürümlerde mevcuttur.

Kaspersky Endpoint Security'nin önceki sürümleri için destek

Kaspersky Anti Targeted Attack Platform (EDR) ile birlikte çalışabilirlik için Kaspersky Endpoint Security 11.2.0 - 11.8.0 kullanıyorsanız, uygulama Kaspersky Endpoint Agent'ı içerir. Kaspersky Endpoint Security'yi Kaspersky Endpoint Agent ile birlikte yükleyebilirsiniz.

Kaspersky Endpoint Security 11.9.0 - 12.0 kullanıyorsanız Kaspersky Endpoint Agent'ı ayrı olarak yüklemeniz gerekir çünkü Kaspersky Endpoint Security 11.9.0'dan itibaren Kaspersky Endpoint Agent dağıtım paketi artık Kaspersky Endpoint Security dağıtım kitinin bir parçası değildir.

Yerleşik aracının EDR/NDR (KATA) ile entegrasyonu

EDR/NDR (KATA) ile entegrasyon için ilgili bileşeni eklemeniz gerekir: Endpoint Detection and Response (KATA) veya Network Detection and Response (KATA). Uygulamayı yüklerken veya yükseltirken EDR/NDR (KATA) ile entegrasyon için bileşenleri seçebilir, ayrıca *Uygulama bileşenlerini değiştir* görevini kullanabilirsiniz.

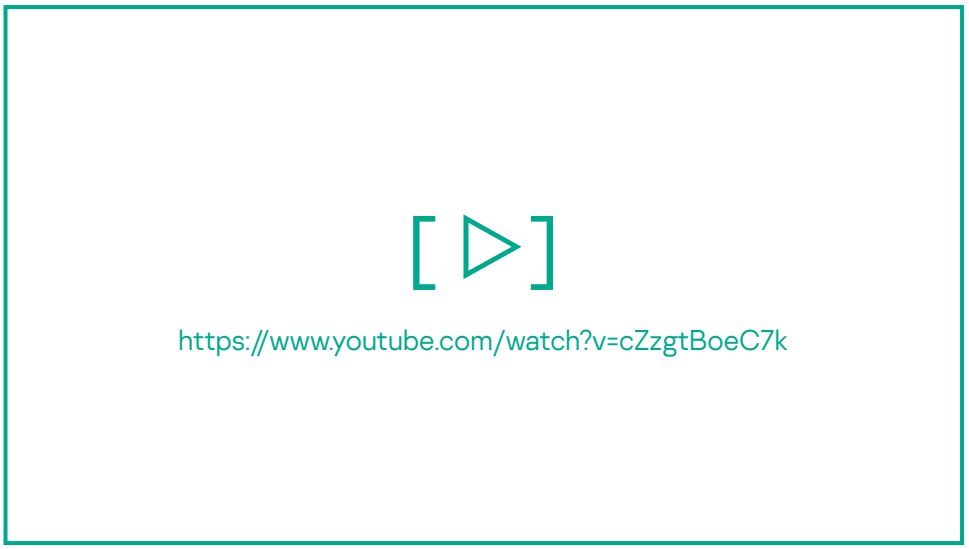
Kaspersky Endpoint Security for Windows sürüm 12.11'den itibaren, EDR (KATA) bileşeni **Endpoint Detection and Response Expert (sürüm 8.0 veya üstü)** olarak yeniden adlandırılmıştır. Uygulamanın bu sürümünde bileşen, Kaspersky Anti Targeted Attack Platform 7.1 ve önceki sürümlerinin yanı sıra Kaspersky Endpoint Detection and Response Expert (on-premises) ile uyumludur.

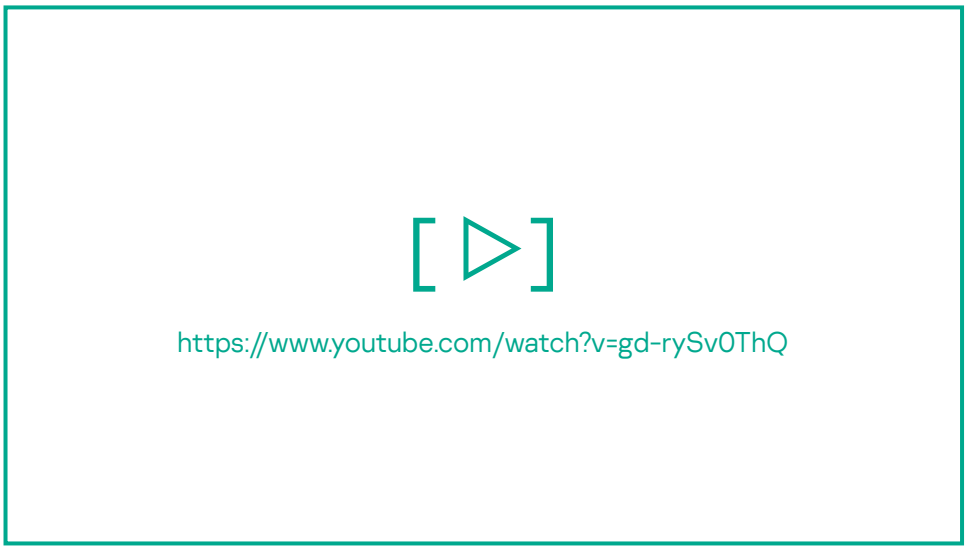
Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) ve Endpoint Detection and Response Expert (on-premises) bileşenleri birbirleriyle uyumlu değildir.

EDR/NDR (KATA) kullanmak için aşağıdaki koşulların karşılanması gerekir:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform sürümleri 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform sürüm 7.0 veya üzeri.
- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 veya üstü. KATA'nın Kaspersky Endpoint Security'nin farklı sürümleriyle uyumluluğu hakkında daha fazla bilgi için Kaspersky Anti Targeted Attack Platform Yardımı'na bakın.
- NDR (KATA): Kaspersky Endpoint Security for Windows 12.7 veya üstü.
- Kaspersky Security Center sürüm 14.2 veya üstü. Kaspersky Security Center'ın önceki sürümlerinde EDR/NDR (KATA) entegrasyon işlevselliğini etkinleştirmek mümkün değildir.
- Uygulama etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.
- Endpoint Detection and Response (KATA) ve Network Detection and Response (KATA) bileşenleri etkinleştirilir.
- EDR/NDR (KATA)'nin çalışmasını sağlayan uygulama bileşenleri etkin ve çalışır durumdadır. Aşağıdaki bileşenler EDR/NDR (KATA)'nin çalışmasını sağlar:
  - Dosya Tehdidi Koruması.
  - Web Tehdidi Koruması.
  - Posta Tehdidi Koruması.
  - Exploit Önleme.
  - Davranış Tespiti.
  - Sunucu Yetkisiz Erişim Önleme.
  - AMSI Koruması.

- Arka plan taraması.
- Kaspersky Security Network.





Endpoint Detection and Response ile entegrasyon aşağıdaki adımlardan oluşur:

1. **Endpoint Detection and Response (KATA) ve Network Detection and Response (KATA) bileşenlerini yükleme**

   EDR (KATA) ve NDR (KATA) bileşenlerini yükleme veya yükseltme sırasında seçebileceğiniz gibi *Uygulama bileşenlerini değiştir* görevini kullanarak da seçebilirsiniz.

   > Uygulamayı yeni bileşenlerle yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatmanız gerekir.

2. **Endpoint Detection and Response (KATA) ve Network Detection and Response (KATA) etkinleştirme**

   EDR (KATA) ve NDR (KATA) için ayrı bir lisans satın almanız gerekir (örneğin, Kaspersky Endpoint Detection and Response (KATA) Eklentisi).

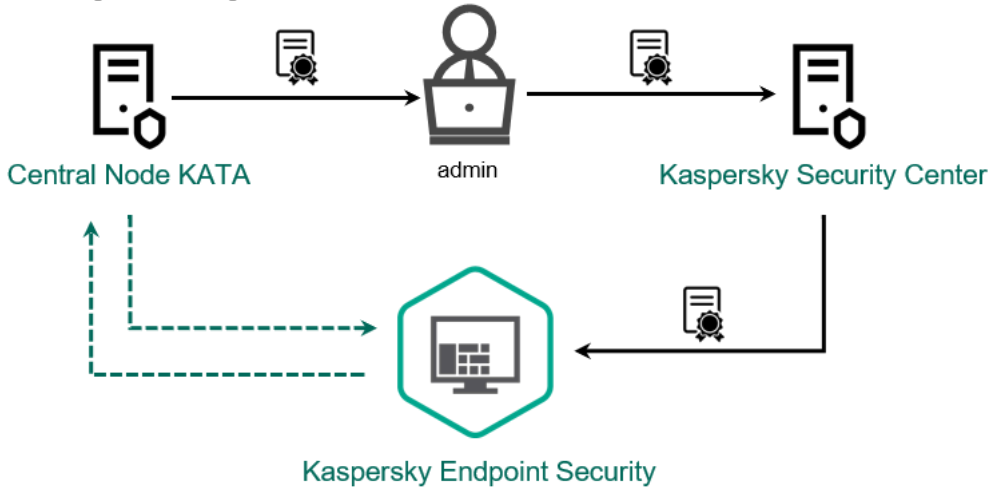
   İşlevsellik, EDR (KATA) ve NDR (KATA) işlevselliğini kapsayan ayrı bir anahtar eklendikten sonra kullanılabilir hale gelir. Sonuç olarak, bilgisayara birden fazla anahtar eklenir: Kaspersky Endpoint Security için bir anahtar ve Kaspersky Endpoint Detection and Response (KATA) ve Network Detection and Response (KATA) için anahtarlar.

   Bağımsız EDR (KATA) ve NDR (KATA) işlevleri için lisanslama, Kaspersky Endpoint Security lisanslamasıyla aynıdır.

   Hem EDR (KATA) hem de NDR (KATA) işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

3. **Central Node'a bağlanma**

Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security ile Central Node bileşeni arasında güvenilir bir bağlantı kurulmasını gerektirir. Güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası kullanmanız gerekir. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Ardından TLS sertifikasını Kaspersky Endpoint Security'ye eklemeniz gerekir (aşağıdaki talimatlara bakın).



Kaspersky Endpoint Security'ye TLS sertifikası ekleme

Kaspersky Endpoint Security varsayılan olarak yalnızca Central Node'un TLS sertifikasını kontrol eder. Bağlantıyı daha güvenli hale getirmek için, bilgisayarın Central Node üzerinde doğrulanmasını da etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu doğrulamayı etkinleştirmek için Central Node ve Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı açmanız gerekir. İki yönlü kimlik doğrulamayı kullanmak için ayrıca bir kripto konteynere ihtiyacınız olacaktır. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).

Yönetim Konsolu (MMC) kullanılarak bir Kaspersky Endpoint Security bilgisayarı Central Node'a nasıl bağlanır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Detection and Response** öğesini seçin ve yapılandırmak istediğiniz bileşeni seçin: **Endpoint Detection and Response Expert (on-premises)** veya **Network Detection and Response (KATA)**.
5. İlgili onay kutusunu seçin: **Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi)** veya **Network Detection and Response (KATA)**.
6. **Sunucu bağlantı ayarları** seçeneğine tıklayın.
7. Sunucu bağlantısını yapılandırın:
   - **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener.
   - **Sunucu TLS sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).

- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

8. **Tamam**'a tıklayın.
9. Central Node sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

   Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
10. Gerekirse telemetriyi yapılandırın.
11. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console kullanılarak bir Kaspersky Endpoint Security bilgisayarı Central Node'a nasıl bağlanır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** bölümüne gidin ve yapılandırmak istediğiniz bileşeni seçin: **Endpoint Detection and Response Expert (on-premises)** veya **Network Detection and Response (KATA)**.
5. İlgili geçiş düğmesini açın: **Endpoint Detection and Response Expert (on-premises) ETKİN** veya **Network Detection and Response (KATA) ETKİN**.
6. EDR'yi (KATA) yapılandırmak için çözümler listesinden **Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi)** seçimini yapın.
7. **Bağlantı ayarları** seçeneğine tıklayın.
8. Sunucu bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener.
   - **Sunucu sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın).

- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

9. **Tamam**'a tıklayın.
10. Central Node sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

    Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
11. Gerekirse telemetriyi yapılandırın.
12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Komut satırı üzerinden yerel olarak da bir TLS sertifikası ekleyebilirsiniz.

Sonuç olarak, bilgisayar Kaspersky Anti Targeted Attack Platform konsoluna eklenir. *Uygulama bileşenlerinin durumu hakkında rapor* görüntüleyerek bileşenlerin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bileşenlerin çalışma durumunu da görüntüleyebilirsiniz. Kaspersky Endpoint Security bileşenleri listesine **Endpoint Detection and Response Expert (sürüm 8.0 veya üstü)** ve **Network Detection and Response (KATA)** bileşenleri eklenecektir.

Kaspersky Security Center konsolundaki bileşenlerin durumunu bilgisayar özelliklerindeki **Bileşenler** bölümünden kontrol edebilirsiniz. Konsolda bileşenin durumunu kontrol ederken aşağıdakileri göz önünde bulundurun. Bileşen yüklü değilse ve işlevsellik lisansınız kapsamında değilse konsolda **Yüklü değil** yerine **Lisansla desteklenmiyor** durumu görüntülenir.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, EDR (KATA) bileşeninin durumunu Kaspersky Security Center Yönetim Konsolu'nda (MMC) izleyebilirsiniz. Bileşenin mevcut durumu bilgisayar özelliklerinde **Endpoint Sensor durumu** sütununda görüntülenir (*Çalışıyor*, *Başlatılıyor*, *Durduruldu*, *Duraklatıldı*, *Başarısız oldu*, *Bilinmiyor*). Web Console Endpoint Sensor'un durumunu göstermez.

EDR (KATA) telemetrisini yapılandırma

Telemetri, korunan bilgisayarda meydana gelen olayların bir listesidir. Kaspersky Endpoint Security, telemetri verilerini analiz eder ve senkronizasyon sırasında Kaspersky Anti Targeted Attack Platform'a gönderir. Telemetri olayları sunucuya neredeyse sürekli olarak ulaşır. Kaspersky Endpoint Security, şu koşullardan herhangi biri karşılandığında sunucu ile senkronizasyonu başlatır:

- Senkronizasyon aralığı sona erdi.
- Arabellekteki olay sayısı üst sınırı aşıyor.

Bu nedenle, varsayılan olarak, uygulama her 30 saniyede bir veya tampon bellekte 1024 olay biriktiğinde senkronize olur. Kaspersky Endpoint Security ilkesinde senkronizasyon davranışını yapılandırabilir ve ağ yükünüze uyacak optimum değerleri seçebilirsiniz (aşağıdaki talimatlara bakın).

Kaspersky Endpoint Security ile sunucu arasında bağlantı yoksa uygulama yeni olayları kuyruğa alır. Bağlantı yeniden sağlandığında, Kaspersky Endpoint Security sıraya alınan olayları sunucuya uygun sırayla gönderir. Sunucunun aşırı yüklenmesini önlemek için Kaspersky Endpoint Security bazı olayları atlayabilir. Bunu etkinleştirmek için, örneğin saat başına maksimum olay değerini ayarlamak için olay iletim ayarlarını optimize edebilirsiniz (aşağıdaki talimatlara bakın).

Kaspersky Anti Targeted Attack Platform'u telemetri de kullanan başka bir çözümle birlikte kullanıyorsanız, KATA (EDR) için telemetriyi kapatabilirsiniz (aşağıdaki talimatlara bakın). Bu, bu çözümler için sunucu yükünü optimize etmenizi sağlar. Örneğin, Managed Detection and Response çözümüne ve KATA'ya (EDR) sahipseniz, MDR telemetrisini kullanabilir ve KATA'da (EDR) Tehdit Müdahalesi görevleri oluşturabilirsiniz.

Yönetim Konsolu'nda (MMC) telemetri yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Detection and Response** öğesini seçin ve yapılandırmak istediğiniz bileşeni seçin: **Endpoint Detection and Response Expert (on-premises)** veya **Network Detection and Response (KATA)**.
5. **KATA sunucusuna her (dakika) senkronizasyon isteği gönder** ayarını yapılandırın. Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.
6. **KATA'ya telemetri gönder** onay kutusunun seçili olduğundan emin olun.
7. Gerekirse, **Veri iletim ayarları** bloğundaki sunucu ayarlarıyla senkronizasyonu yapılandırın:
   - **Maksimum olay iletim gecikmesi (sn)**. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
   - **Paket başına maksimum olay sayısı**. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır.
8. Gerekirse, **Talep daraltma** bloğunda **Talep daraltmayı etkinleştir** onay kutusunu seçin.

   Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur.
9. Olayları sunucuya göndermek için optimizasyon ayarlarını yapılandırın:
   - **Saat başına maksimum olay sayısı**. Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir.
   - **Olay sınırı aşım yüzdesi**. Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.
10. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da telemetri yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (on-premises)** bölümüne gidin.
5. EDR'yi (KATA) yapılandırmak için çözümler listesinden **Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi)** seçimini yapın.
6. **Veri iletim ayarları** bloğunda **Telemetriyi KATA sunucularına gönder** onay kutusunun seçili olduğundan emin olun.
7. **Sunucusuna her (dakika) senkronizasyon isteği gönder** ayarını yapılandırın. Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.
8. **KATA sunucularına telemetri gönder** onay kutusunun seçili olduğundan emin olun.
9. Gerekirse, **Veri iletim ayarları** bloğundaki sunucu ayarlarıyla senkronizasyonu yapılandırın:

   - **Maksimum olay iletim gecikmesi (sn)**. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
   - **Paket başına maksimum olay sayısı**. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır.
10. Gerekirse, **Talep daraltma** bloğunda **Talep daraltmayı etkinleştir** onay kutusunu seçin.

    Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur.
11. Olayları sunucuya göndermek için optimizasyon ayarlarını yapılandırın:

    - **Saat başına maksimum olay sayısı**. Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir.
    - **Olay sınırı aşım yüzdesi**. Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.
12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **KATA entegrasyonu** → **Telemetri istisnaları** bölümüne gidin.
5. **Veri iletim ayarları** bölümünde, **İstisnaları kullan** onay kutusunu seçin.
6. **Ekle**'ye tıklayın ve istisnaları yapılandırın:

   Kriterler mantıksal *AND* ile birleştirilir.

   - **Yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. İstisnanın çalışması için dosyanın yolu belirtilmelidir.
   - **Komut satırı**. Nesneyi çalıştırmak için kullanılan komut.
   - **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri.
     VersionInfo kaynağı hakkında daha ayrıntılı bilgi için lütfen Microsoft web sitesini ziyaret edin.
   - **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri.
   - **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri.
   - **MD5**. Dosyanın MD5 karması.
   - **SHA256**. Dosyanın SHA256 karması.
   - **Olay türleri**. İstisnanın çalışması için en az bir olay türü seçmelisiniz.
7. Değişikliklerinizi kaydedin.

1. Kaspersky Security Center Yönetim Konsolu ağacında **Görevler** seçimini yapın.
   Görevler listesi açılır.
2. **Yeni görev**'e tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

1. **Kaspersky Endpoint Security for Windows (14.2)** → **Güncellemeyi geri al** seçimini yapın.

2. Adım. Görevin atanacağı cihazları seçme

Görevin gerçekleştirileceği bilgisayarları seçin. Aşağıdaki seçenekler kullanılabilir:

- Görevi bir yönetim grubuna atayın. Bu durumda, görev önceden oluşturulan bir yönetim grubuna dahil edilen bilgisayarlara atanır.
- Yönetim Sunucusu tarafından ağda *atanmamış cihazlar* olarak tespit edilmiş bilgisayarları seçin. Belirli cihazlar, yönetim gruplarındaki cihazları ve atanmamış cihazları içerebilir.
- Aygıt adreslerini manuel olarak belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Bir görev başlatma zamanlaması yapılandırma

Görev zamanlamasını örneğin manuel olarak yapılandırın.

4. Adım. Görev adını tanımlama

Görev için bir ad girin.

7. Adım. Görev oluşturmayı tamamlama

Sihirbazı tamamlayın. Gerekirse, **Sihirbazı tamamladıktan sonra görevi çalıştır** onay kutusunu işaretleyin. Görevin ilerleme durumunu görev özelliklerinden izleyebilirsiniz.

EDR (KATA) telemetri istisnaları

Performansı artırmak ve Telemetri sunucusuna veri iletimini optimize etmek için telemetri istisnalarını yapılandırabilirsiniz. Örneğin, bireysel uygulamalar için ağ iletişim verilerini göndermemeyi seçebilirsiniz.

Yönetim Konsolu'nda (MMC) nasıl bir telemetri istisnası oluşturulur

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
4. **Telemetri ayarları** → **EDR (KATA) / NDR (KATA) telemetri** bloğunda, **Ayarlar** düğmesine tıklayın.

5. Açılan pencerede telemetri istisnalarını yapılandırın (aşağıdaki tabloya bakın).

   Uygulama, istisna koşullarını mantıksal VE ile birleştirir. Bir kural oluşturmak için, **Tam yol** alanında bir değer belirtmeniz ve **Aşağıdaki etkinlik türleri için kullan** listesinde en az bir olay türü seçmeniz gerekir.

6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir telemetri istisnası oluşturma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Telemetri Ayarlarıı** bölümüne gidin.

5. **EDR (KATA) / NDR (KATA) telemetri** sekmesini seçin.

6. Açılan pencerede telemetri istisnalarını yapılandırın (aşağıdaki tabloya bakın).

   Uygulama, istisna koşullarını mantıksal VE ile birleştirir. Bir kural oluşturmak için **Tam yol** alanında bir değer belirtmeniz ve en az bir olay türü seçmeniz gerekir.

7. Değişikliklerinizi kaydedin.

Parametre	Açıklama
Hariç tutulan süreçler	**Gönderilecek telemetri boyutunu optimize et**. Kaspersky Endpoint Security, iletilen veri miktarını optimize etmeye ve telemetriden belirli kodlara sahip olayları hariç tutmaya olanak tanır: Microsoft SMB protokolü, WinRM hizmeti ve Ağ Aracısının klnagent.exe işlemi için kod 102 (temel iletişimler) ve 8 (işlemin ağ etkinliği) ve ayrıca her tür ağ protokolü için ağ paketi türleri hakkında genişletilmiş bilgiler. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir. **Aşağıdaki etkinlik türleri için kullan**: • **Dosya değişikliği**. • **Ağ olayları**. • **İşlem: konsol etkileşimli girişi**. • **Modül yüklendi**. • **Kayıt defteri değiştirildi**. • **DNS günlükleri**. • **Süreç erişimi**. • **Kod ekleme**. • **WMI sorgusu**. • **Pipe**. • **LDAP**. • **AMSI**.
Hariç tutulan ağ iletişimleri	**Kural adı**. **Yön**. **İletişim kuralı**. **Ham soket**. **Protokol numarası**. **TLS sertifikası**. **Yerel port veya aralık**. **Uzak port veya aralık**. **Yerel adres**. Kaspersky Endpoint Security'nin telemetriyi ağ trafiğinin dışında tuttuğu bilgisayarın ağ adresi. **Uzak adres**. Kaspersky Endpoint Security'nin telemetriyi ağ trafiğinin dışında tuttuğu bilgisayarın ağ adresi. IP adresleri için yalnızca IPv4 biçimi desteklenir. **Uygulamalar**. Kaspersky Endpoint Security'nin EDR telemetrisini ağ trafiğinin dışında bıraktığı uygulamaların yürütülebilir dosyalar listesi.

Parametre	Açıklama
Hariç tutulan dosya işlemleri	**Kural adı**. **Dosya adı ya da maskesi**. Bir dosya veya klasörün adı ya da maskesi; Kaspersky Endpoint Security, bu dosya veya klasöre erişildiğinde istisna kuralını uygular. Kaspersky Endpoint Security, bir maske girerken `*` ve `?` karakterlerini destekler. **İşlem türü**. **Önceki yol**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.
Hariç tutulan DNS işlemleri	**Kural adı**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir. **DNS**: • **DNS sunucusu IP adresi**. • **Sorgu seçenekleri**. • **Durum**. • **Etki alanı adı**. • **Ayar tipi kimliği**. • **Yanıt verileri**.

Parametre	Açıklama
Hariç tutulan LDAP işlemleri	**Kural adı**. **LDAP arama kapsamı**. **Filtre**. **LDAP nesneleri araması için ayırt edici ad**. **Nesne öznitelikleri**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.
Hariç tutulan süreç erişim sorguları	**Kural adı**. **İşlem türü**. **Sürece erişim talep edildi**. **Çağrı yığını izi**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem**, **Ana işlem**, **Hedef işlemin dosyası**, **Kaynak işleme ait tanıtıcı** ve **Hedef işleme ait tanıtıcı**. • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Kural tetikleme kriterlerini ve bu kuralın kullanılacağı olay türlerini belirtin**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.

Parametre	Açıklama
Hariç tutulan kod eklemeleri	**Kural adı**. **Erişim yöntemi**. **Çağrı yığını**. **Değiştirilmiş komut satırı**. **Ekleme adresi**. **Eklenen DLL adı**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.
Hariç tutulan WMI sorguları	**Kural adı**. **WMI işlem türü**. **Uzak sorgu**. **WMI komutunu çalıştıran bilgisayarın adı**. **WMI kullanıcı hesabı**. **Çalıştırılan WMI komutu**. **WMI ad alanı**. **WMI olay tüketici filtresi**. **Oluşturulan WMI olay tüketicisinin adı**. **WMI olay tüketicisi kaynak kodu**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.

Parametre	Açıklama
Hariç tutulan pipe işlemleri	**Kural adı**. **Pipe adı**. **İşlem türü**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.
Hariç tutulan kayıt defteri değişiklikleri	**Kural adı**. **İşlem türü**. **Yol**. **Değer adı**. **Değer**. **Kayıt dosyasının tam adı**. Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir. **İşlem** ve **Ebeveyn işlemi**: • **Tam yol**. Adı ve uzantısı dahil olmak üzere dosyanın tam yolu. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. • **Komut satırı metni**. Dosyayı çalıştırmak için kullanılan komut. • **Açıklama**. RT_VERSION (VersionInfo) kaynağından alınan FileDescription parametresinin değeri. • **Orijinal dosya adı**. RT_VERSION (VersionInfo) kaynağından alınan OriginalFilename parametresinin değeri. • **Sürüm**. RT_VERSION (VersionInfo) kaynağından alınan FileVersion parametresinin değeri. • **Dosya sağlama toplamları**. MD5 ve SHA256. Bir dosyayı manuel olarak da seçebilirsiniz, böylece uygulama seçilen dosyadaki alanları otomatik olarak dolduracaktır. 64 bit işletim sistemlerinde, uygulama yürütülebilir dosya parametre alanlarını `C:\windows\syswow64` klasöründeki aynı yürütülebilir dosyanın 32 bit sürümünün özelliklerinden gelen verilerle doldurduğundan, `C:\windows\system32` klasöründeki bir işlemin yürütülebilir dosyasının 64 bit sürümünün parametrelerini manuel olarak girmeniz gerekir. Örneğin, `C:\windows\system32\cmd.exe`'yi seçtiğinizde, eklenti `C:\windows\syswow64\cmd.exe` parametrelerini görüntüler. Bu tür davranışlar işletim sisteminin özellikleri tarafından belirlenir.
Cihazlarla yapılan hariç tutma işlemleri	**Kural adı**. **Aygıt türü**. **Cihaz Kimliği**. **Aygıt adı**.

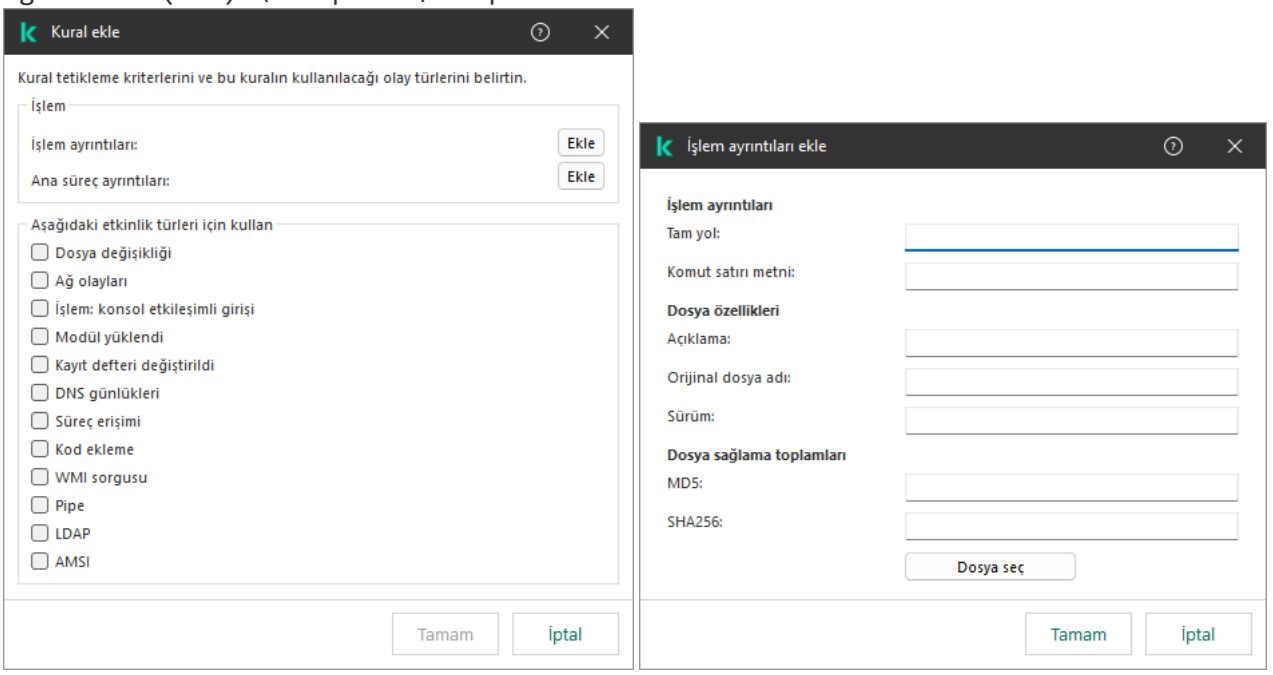
Örnek 1. Hariç tutulan süreçler

Üçüncü taraf uygulama (işlem) olaylarını telemetriden hariç tutmak için, **Hariç tutulan işlemler** sekmesinde EDR telemetri istisnaları penceresini açın ve uygulamanın yürütülebilir dosyasını ekleyin.

Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir.

Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. Örneğin:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Bir süreci hariç tutma

Örnek 1. Dosya değişikliği

Notepad++ uygulamasında sık sık komut dosyaları düzenliyorsanız ve ilgili komut dosyaları için değişiklik olaylarını hariç tutmak istiyorsanız, Notepad++ yürütülebilir dosyasını telemetri istisnalarına ekleyin.

Ayarları aşağıdaki gibi belirleyin:

- **Tam yol**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Aşağıdaki etkinlik türleri için kullan**: Dosya değişikliği.

Örnek 2. Ağ olayları

Uzak bir sunucudaki dosyaları yönetmek için WinSCP uygulamasını kullanıyorsanız ve ağ olaylarını hariç tutmak istiyorsanız, WinSCP yürütülebilir dosyasını telemetri istisnalarına ekleyin.

Ayarları aşağıdaki gibi belirleyin:

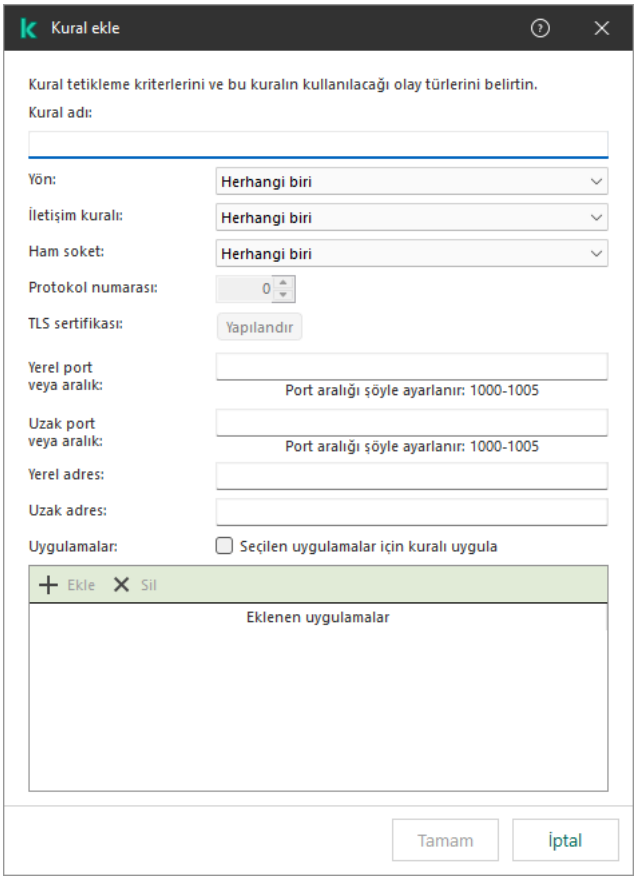
- **Tam yol**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (optional).
- **Aşağıdaki etkinlik türleri için kullan**: Ağ olayları.

Örnek 2. Hariç tutulan ağ iletişimleri

Uzak hizmet bağlantı olaylarını telemetriden hariç tutmak için, **Hariç tutulan ağ iletişimleri** sekmesinde EDR telemetri istisnaları penceresini açın ve bağlantı ayarlarını ekleyin: protokol, port, yön, IP adresi, TLS sertifikası ve diğerleri.

Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir.

Bir alt ağ adresi belirtemezsiniz (örneğin, 10.28.0.0/24). Uygulama yalnızca bir IP adresi belirtilmesine izin verir (örneğin, 10.28.0.105).



Ağ iletişiminin hariç tutulması

Kurumsal bir web sunucusu kullanıyorsanız ve bu web sunucusuna bağlanırken tarayıcı olaylarını hariç tutmak istiyorsanız, sunucunun IP adresini ve tarayıcının yürütülebilir dosyasını telemetri istisnalarına ekleyin.

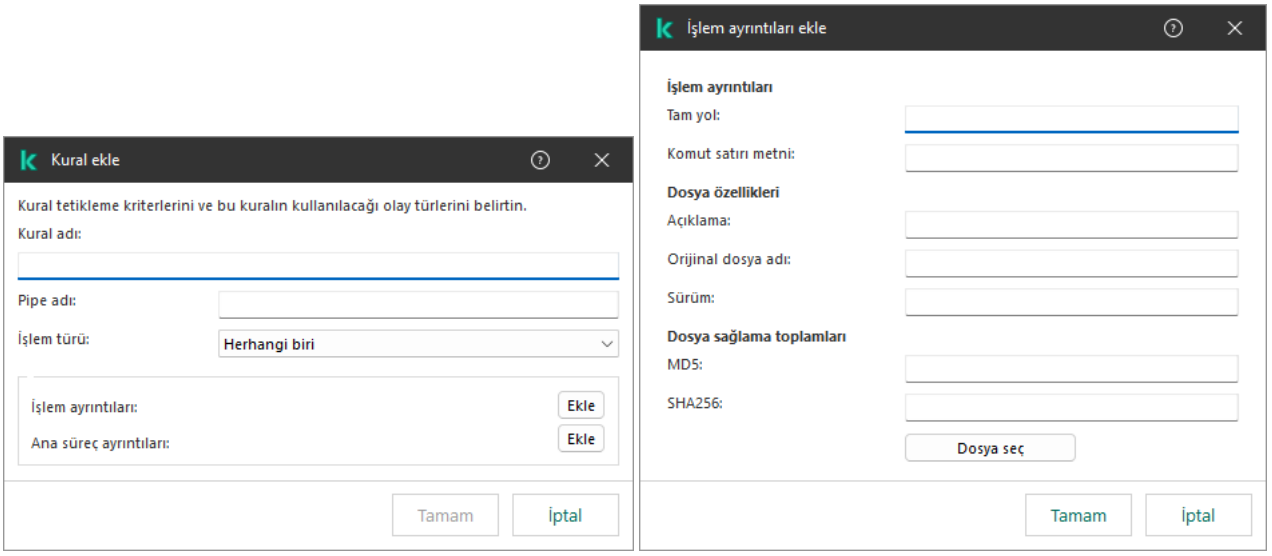
Ayarları aşağıdaki gibi belirleyin:

- **İletişim kuralı**: TKP.
- **Uzak port veya aralık**: 443.
- **Uzak adres**: 10.28.0.105.
- **Uygulamalar**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Örnek 3. Hariç tutulan dosya işlemleri

Güvenilen dosyalarla yapılan işlemleri içeren olayları telemetri dışında tutmak için **Hariç tutulan dosya işlemleri** sekmesindeki EDR telemetri istisnaları penceresini açın ve güvenilen dosyayı ekleyin.

Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir.



Dosya işlemlerinin hariç tutulması

Bir uygulama bir günlüğe yazıyorsa ve günlük dosyası değişiklik olaylarını hariç tutmak istiyorsanız, günlük dosyasını ve uygulamanın yürütülebilir dosyasını telemetriden ekleyin.

Ayarları aşağıdaki gibi belirleyin:

- **Dosya adı veya maskesi**: `C:\Apache24\logs\error.log`.
- **İşlem türü**: Dosya değişikliği.
- **Tam yol**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Örnek 4. Hariç tutulan kayıt defteri değişiklikleri

Kayıt defteri, değişiklik olaylarını telemetriden hariç tutmak için **Hariç tutulan kayıt defteri değişiklikleri** sekmesinde EDR telemetri hariç tutmaları penceresini açın ve bir kayıt defteri anahtarı ekleyin.

Kaspersky Endpoint Security, kural tetikleme kriterlerini mantıksal bir VE ile birleştirir.

Bir uygulama kayıt defteri değerlerini sık sık değiştiriyorsa ve bu kayıt defteri değişiklik olaylarını telemetriden hariç tutmak istiyorsanız, kayıt defteri anahtarını ve uygulamanın yürütülebilir dosyasını telemetri istisnalarına ekleyin.

Ayarları aşağıdaki gibi belirleyin:

- **İşlem türü**: Değiştir.
- **Yol**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Tam yol**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform, Sandbox (KATA Sandbox) bileşenini içerir. *Sandbox* bir bilgisayardaki gelişmiş tehditleri tespit etmenizi sağlayan bir teknolojidir. Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

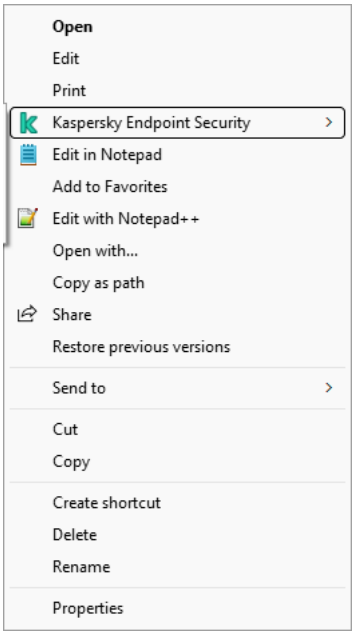
KATA Sandbox'ın etkinleştirilmesi için, KATA veya KEDR işlevselliğini içeren bir lisans anahtarına ihtiyacınız vardır. Kullanılabilir işlevler hakkında ayrıntılar için Kaspersky Anti Targeted Attack Platform Yardım bölümüne bakın.

KATA Sandbox, şu modlarda dosya taramasına izin verir:

- *Manuel*. Kullanıcı, bağlam menüsünden dosyayı tarama için manuel olarak gönderir (**Sandbox'a Gönder**). Sandbox'a bir dosya gönderirken, uygulama antivirüs veritabanlarını kullanarak dosyayı tarar.
- *Otomatik*. Uygulama nesneleri otomatik olarak algılar ve tarama için Sandbox'a gönderir.

Dosya Sandbox'a gönderildikten sonra, dosya kullanıcı tarafından erişilebilir durumda kalır. Kaspersky Endpoint Security ilgili olayı günlüğe kaydeder ve olayı Kaspersky Security Center'a ve Kaspersky Anti Targeted Attack Platform konsoluna gönderir. Sandbox kötü amaçlı etkinlik tespit ederse Kaspersky Endpoint Security otomatik olarak bir Tehdit Yanıt eylemi gerçekleştirir (örneğin, nesneyi siler ve bir Kritik Alanları Tarama başlatır).

KATA Sandbox'ın manuel modda çalışması için Kaspersky Anti Targeted Attack Platform 7.0 veya üstü sürümünün kurulması gerekir. KATA Sandbox'ın otomatik modda çalışması için Kaspersky Anti Targeted Attack Platform 8.0 veya üstü sürümünün kurulması gerekir.



Bağlam menüsünden KATA Sandbox'ta tarama

Yerleşik aracının KATA Sandbox ile entegrasyonu

Sandbox bileşeninin eklenmesi KATA Sandbox ile entegrasyon için gereklidir. Sandbox bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken seçebilirsiniz.

Dosyaları taramaya göndermek için KATA Sandbox ile entegrasyonu etkinleştirmeli ve çözümün içinde yer alan bir Central Node sunucusu eklemelisiniz. Bileşen yalnızca Kaspersky Security Center Web Console kullanılarak yönetilebilir. Bu bileşeni Yönetim Konsolu'nu (MMC) kullanarak yönetemezsiniz.

KATA Sandbox ile entegrasyonu etkinleştirmek veya devre dışı bırakmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Sandbox** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sandbox ile entegrasyon ETKİN** iki durumlu düğmesini kullanın.

6. KATA Sandbox çalışma modunu seçin:

   - **Manuel**. Kullanıcı, bağlam menüsünden dosyayı tarama için manuel olarak gönderir (**Sandbox'a Gönder**).
   - **Otomatik**. Uygulama nesneleri otomatik olarak algılar ve tarama için Sandbox'a gönderir.
   - **Birleştirilmiş**.

7. **Bağlantı ayarları** bağlantısına tıklayın.

8. Central Node sunucusu bağlantı ayarlarını yapılandırın:

   - **Zaman aşımı (ms)**. Central Node sunucusu için bağlantı zaman aşımı. Yapılandırılan zaman aşımı süresi geçtikten sonra Kaspersky Endpoint Security bir sonraki sunucuya bir istek gönderir. Bağlantı hızınız düşükse veya bağlantı dengesizse sunucu için bağlantı zaman aşımını artırabilirsiniz. Önerilen istek zaman aşımı 0,5 saniye veya daha kısadır.
   - **İstek kuyruğu**. İstek kuyruğu klasörünün boyutu. Sandbox'ta tarama için birden fazla nesne gönderirken Kaspersky Endpoint Security bir istek kuyruğu oluşturur. İstek kuyruğu klasörünün boyutu varsayılan olarak 100 MB ile sınırlandırılmıştır. Maksimum boyuta ulaşıldıktan sonra, Sandbox kuyruğa yeni isteklerin eklenmesini durdurur ve ilgili olayı Kaspersky Security Center'a gönderir. İstek kuyruğu klasörünün boyutunu sunucu yapılandırmanıza göre yapılandırabilirsiniz.
   - **Sunucu TLS sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Daha sonra bir ilke kullanarak sertifikayı bilgisayara eklemeniz gerekir. Sertifikayı Central Node sunucusuna da eklemeniz gerekir.
   - **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.

9. **Sandbox sunucularına bağlantı** bloğunda, **Ekle** düğmesine tıklayın.

10. Bir pencere açılır; bu pencerede, Central Node sunucusunun adresini (IPv4, IPv6, DNS) ve portu girin.

    Sanal görüntüleri dağıtma ve Central Node sunucularını yapılandırma hakkında ayrıntılar için Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

11. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

    Sonuç olarak, Sandbox bileşeni etkinleştirilir. *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Sandbox** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecek.

Tehdit Yanıtı eylemlerini yapılandırma

Sandbox kötü amaçlı etkinlik tespit ederse Kaspersky Endpoint Security otomatik olarak bir Tehdit Yanıt eylemi gerçekleştirir (örneğin, nesneyi siler ve bir Kritik Alanları Tarama başlatır).

Tehdit Yanıtı eylemlerini yapılandırmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Sandbox** bölümüne gidin.
5. **Tehdit algılandığında yapılacak eylem** bloğunda gereken eylemi seçin:

   - **Kopyayı Karantinaya taşı, nesneyi sil**. Bu seçenek tercihe dildiğinde, Kaspersky Endpoint Security bilgisayardaki kötü amaçlı nesneyi siler. Kaspersky Endpoint Security, nesneyi silmeden önce nesnenin daha sonra geri yüklenmesi gerekebileceği ihtimaline karşı bir yedek kopya oluşturur. Kaspersky Endpoint Security, yedek kopyayı Karantinaya taşır.
   - **Kritik Alanları Taramayı çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Critical Areas Scan* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.
   - **IOC Taraması görevi oluştur**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security otomatik olarak *IOC Taraması görevi (otonom IOC tarama görevi) oluşturur*. Bu görev için çalışma modunu, tarama kapsamını ve IOC algılandığında gerçekleştirilecek eylemi yapılandırabilirsiniz (*Kopyasını Karantinaya taşı, nesneyi sil* veya *Kritik Alanları Taramayı Çalıştır*). *IOC Taraması* görevinin diğer ayarları değiştirmek için görev ayarlarına gidin.
6. Gerekirse, **IOC Taraması kapsamı** bloğunda *IOC Taraması* görev ayarlarını yapılandırın.

   - **Kritik dosya alanları**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security yalnızca bilgisayarın kritik dosya alanlarında bir IOC taraması gerçekleştirir: çekirdek belleği ve önyükleme kesimleri.
   - **Bilgisayarın sistem sürücüsündeki dosya alanları**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security bilgisayarın sistem sürücüsünde bir IOC taraması gerçekleştirir.
7. Gerekirse, **IOC Taraması görevini çalıştır** bloğunda *IOC Taraması* görev ayarlarını yapılandırın.

   - **Manuel**. *IOC Taraması* görevini sizin için uygun olan bir zamanda manuel olarak başlatabileceğiniz çalıştırma modu.
   - **Otomatik**. Kaspersky Endpoint Security'nin *IOC Taraması* görevini bir tehdit algılandıktan sonra otomatik olarak çalıştırdığı çalışma modudur.
   - **Sadece bilgisayar boştayken çalıştır**. Kaspersky Endpoint Security'nin *IOC Taraması* görevini ekran koruyucu etkin ya da ekran kilitli olduğunda çalıştırdığı çalıştırma modudur. Kullanıcı bilgisayarın kilidini açarsa Kaspersky Endpoint Security görevi duraklatır. Bu, görevin tamamlanmasının birkaç gün sürebileceği anlamına gelir.
8. *IOC Taraması* için gelişmiş görev ayarlarını yapılandırın.
9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

EDR (KATA) için KEA'dan KES'e Geçiş Kılavuzu

Kaspersky Endpoint Security for Windows, 12.1 sürümünden itibaren Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olarak Kaspersky Endpoint Detection and Response bileşenini yönetmek için yerleşik bir aracı içerir. EDR (KATA) ile çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok. Tüm Kaspersky Endpoint Agent işlevleri Kaspersky Endpoint Security tarafından gerçekleştirilecektir. Kaspersky Anti Targeted Attack Platform sunucuları üzerindeki yük aynı kalacaktır.

Kaspersky Endpoint Agent yüklü bilgisayarlara Kaspersky Endpoint Security dağıttığınızda, Kaspersky Anti Targeted Attack Platform (EDR) çözümü Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır. Kaspersky Endpoint Security'yi 12.1 veya üstü sürümlere güncellediğinizde sistemde aynı davranış ortaya çıkar.

> Kaspersky Endpoint Security, Kaspersky Endpoint Agent ile uyumlu değildir. Bu uygulamaların her ikisini de aynı bilgisayara yükleyemezsiniz.

Kaspersky Endpoint Security'nin Endpoint Detection and Response'un (KATA) bir parçası olarak çalışması için şu koşulların karşılanması gerekir:

- Kaspersky Anti Targeted Attack Platform sürüm 5.0 veya üzeri.
- Kaspersky Security Center sürüm 14.2 veya üstü (Network Agent dahil). Kaspersky Security Center'ın önceki sürümlerinde Endpoint Detection and Response (KATA) özelliğini etkinleştirmek mümkün değildir.

EDR (KATA) için [KES+KEA] yapılandırmasını [KES+yerleşik aracı]'ya taşıma adımları

1. **Kaspersky Endpoint Security Management Eklentisini Yükseltme**

   EDR (KATA) bileşeni, Kaspersky Endpoint Security Management Plug-in sürüm 12.1 veya üstü kullanılarak yönetilebilir. Kullandığınız Kaspersky Security Center konsolunun türüne bağlı olarak, Yönetim Konsolu (MMC)'deki yönetim eklentisini veya Web Console'daki web eklentisini güncelleyin.

2. **İlkelerin ve görevlerin taşınması**

   Kaspersky Endpoint Agent ayarlarını Kaspersky Endpoint Security for Windows'a aktarın. Aşağıdaki seçenekler kullanılabilir:

   - Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş için bir sihirbaz. Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş sihirbazı yalnızca Web Console'da çalışır

     Web Console'da Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye ilke ve görev ayarlarını taşıma

     Web Console ana penceresinde, **İşlemler** → **Kaspersky Endpoint Agent'tan Geçiş** seçimini yapın.

     Böylece ilke ve görev geçiş sihirbazı çalıştırılır. Sihirbazın talimatlarını uygulayın.

1. Adım. İlke geçişi

Geçiş Sihirbazı, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent ilkelerinin ayarlarını birleştiren yeni bir ilke oluşturur. İlke listesinden, ayarlarını Kaspersky Endpoint Security ilkesiyle birleştirmek istediğiniz Kaspersky Endpoint Agent ilkelerini seçin. Ayarları birleştirmek istediğiniz Kaspersky Endpoint Security ilkesini seçmek için Kaspersky Endpoint Agent ilkesine tıklayın. Doğru ilkeleri seçtiğinizden emin olun ve sonraki adıma geçin.

2. Adım. Görev geçişi

Geçiş Sihirbazı EDR (KATA) görevlerini desteklemez. Bu adımı atlayın.

3. Adım Sihirbazı tamamlama

Sihirbazı tamamlayın. Sihirbazın sonucunda yeni bir Kaspersky Endpoint Security ilkesi oluşturulacaktır. İlke, Kaspersky Endpoint Security'den ve Kaspersky Endpoint Agent'tan gelen ayarları birleştirir. Bu ilkeye *<Kaspersky Endpoint Security ilke adı> & <Kaspersky Endpoint Agent ilke adı>* adı verilir. Yeni ilke *Etkin değil* durumundadır. Devam etmek için Kaspersky Endpoint Agent ve Kaspersky Endpoint Security ilkelerinin durumlarını *Etkin değil* olarak değiştirtin ve yeni birleştirilmiş ilkeyi etkinleştirin.

Web Console'daki geçiş sihirbazı şu ilke ayarlarını atlar ve bunları taşımaz:

- Ayarların değiştirilmesi yasağı **Bağlantı ayarları** ("kilit").

  Varsayılan olarak ayarlar değiştirilebilir ("kilit" açıktır). Bu nedenle ayarlar bilgisayarda uygulanmaz. Ayarların değiştirilmesi yasaklanmalı ve "kilit" kapatılmalıdır.

- Kripto konteyneri.

  Central Node sunucularına bağlanmak için iki yönlü kimlik doğrulama kullanıyorsanız, kripto konteynerini yeniden eklemeniz gerekir.

Geçiş Sihirbazı bu ayarları taşımadığından, bilgisayarı Central Node sunucularına bağlarken hatalarla karşılaşabilirsiniz. Hataları düzeltmek için ilke özelliklerine gitmeniz ve bağlantı ayarlarını yapılandırmanız gerekir.

- Standart bir İlke ve görevler toplu dönüştürme sihirbazı. İlke ve görevler toplu dönüştürme sihirbazı yalnızca Yönetim Konsolu'nda (MMC) kullanılabilir. İlke ve görevler toplu dönüştürme sihirbazı hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

Kaspersky Endpoint Security'nin sunucularda düzgün çalıştığından emin olmak için, sunucunun çalışması için önemli olan dosyaların güvenilir bölgeye eklenmesi önerilir. SQL sunucuları için MDF ve LDF veritabanı dosyalarını eklemelisiniz. Microsoft Exchange sunucuları için CHK, EDB, JRS, LOG ve JSL dosyaları eklemelisiniz. Maskeler kullanabilirsiniz, örneğin, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir.

EDR telemetri istisnaları Kaspersky Endpoint Agent ilkesinden Kaspersky Endpoint Security ilkesine aktarılmaz. Kaspersky Endpoint Security'nin kendi istisna araçları vardır - güvenilir uygulamalar. Kaspersky Endpoint Security'nin çalışması, bireysel EDR telemetri istisnalarının olmaması, Kaspersky Endpoint Agent ile karşılaştırıldığında bilgisayarınızda herhangi bir ek yüke neden olmayacak şekilde optimize edilmiştir. Kaspersky Endpoint Security telemetriyi yalnızca EDR (KATA) için değil, aynı zamanda uygulama koruma bileşenlerinin çalışması için de kullanır. Bu nedenle, bireysel EDR telemetri istisnalarının aktarılmasına gerek yoktur. Bilgisayar performansında bir düşüş yaşamanız durumunda, uygulamanın çalışmasını kontrol edin (bkz. 7. adım Performansı kontrol etme).

3 EDR (KATA) işlevselliğinin lisanslanması

Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olarak Kaspersky Endpoint Security'yi etkinleştirmek için ayrı bir Kaspersky Endpoint Detection and Response (KATA) Eklentisi lisansına ihtiyacınız vardır. Anahtarı, *Anahtar ekle* görevini kullanarak ekleyebilirsiniz. Sonuç olarak, uygulamaya iki anahtar eklenecektir: *Kaspersky Endpoint Security* ve *Kaspersky Endpoint Detection and Response (KATA)*.

Daha önce EDR Optimum veya EDR Expert özellikleri etkinleştirilen bilgisayarlarda Kaspersky Endpoint Detection and Response (KATA) Eklentisi lisanslanması aşağıdaki özel hususları içerir:

- Kaspersky Endpoint Security'yi EDR Optimum veya EDR Expert özellikleriyle lisanslamak için bir *anahtar dosyası* kullanıyorsanız, Kaspersky Endpoint Detection and Response (KATA) Eklentisi için ayrı bir anahtar ekleyemezsiniz. Lisanslama için bir etkinleştirme kodu kullanmaya geçebilir veya Kaspersky Endpoint Security ve EDR özelliklerini etkinleştirmek için yeni bir anahtar dosyası almak üzere hizmet sağlayıcınızla iletişime geçebilirsiniz. Hizmet sağlayıcı lisanslama için bir veya daha fazla anahtar dosya sağlayacaktır.

- Kaspersky Endpoint Security'yi EDR Optimum veya EDR Expert özellikleri olmadan lisanslamak için bir *anahtar dosyası* kullanıyorsanız, anahtar dosyalarının yeniden düzenlenmesine gerek kalmadan Kaspersky Endpoint Detection and Response (KATA) Eklentisi için ayrı bir anahtar ekleyebilirsiniz.

- Lisanslama için bir *etkinleştirme kodu* kullanıyorsanız, Kaspersky etkinleştirme sunucusu anahtarları otomatik olarak yeniden yayınlayacak ve EDR (KATA) özellikleri otomatik olarak kullanılabilir hale gelecektir. Bu durumda, EDR Optimum ve EDR Expert devre dışı bırakılacaktır.

- Kaspersky Endpoint Security, en fazla iki etkin anahtar eklemenize olanak tanır: Kaspersky Endpoint Security anahtarı ve Eklenti türü anahtar. Ayrıca iki adede kadar rezerve anahtar ekleyebilirsiniz. Bir Kaspersky Endpoint Security rezerve anahtarı ve bir Eklenti türü rezerve anahtar.

4 Kaspersky Endpoint Security uygulamasını Yükleme/Yükseltme

Bir uygulama kurulumu veya yükseltmesi sırasında EDR (KATA) işlevselliğini taşımak için uzaktan kurulum görevinin kullanılması önerilir. Bir uzaktan kurulum görevi oluştururken, kurulum paketi ayarlarında EDR (KATA) bileşenini seçmeniz gerekir.

Uygulamayı, şu yöntemleri kullanarak da güncellemeniz mümkündür:

- Kaspersky güncelleme hizmetini kullanma.

- Kurulum Sihirbazını kullanarak yerel olarak.

Kaspersky Endpoint Security, Kaspersky Endpoint Agent uygulamasının yüklü olduğu bir bilgisayarda uygulama yükseltilirken, bileşenlerin otomatik olarak seçilmesini destekler. Bileşenlerin otomatik seçimi, uygulamayı yükselten kullanıcı hesabının izinlerine bağlıdır.

Kaspersky Endpoint Security'yi sistem hesabı (SYSTEM) altındaki EXE veya MSI dosyasını kullanarak yükseltiyorsanız, Kaspersky Endpoint Security, Kaspersky çözümlerinin geçerli lisanslarına erişim kazanır. Dolayısıyla, bilgisayarda Kaspersky Endpoint Agent yüklü ve EDR (KATA) çözümü etkinleştirilmişse, Kaspersky Endpoint Security yükleyicisi bileşen setini otomatik olarak yapılandırır ve EDR (KATA) bileşenini seçer. Bu, Kaspersky Endpoint Security'nin bütünleşik aracıyı kullanmaya geçmesini sağlar ve Kaspersky Endpoint Agent'ı kaldırır. MSI yükleyicisinin sistem hesabı (SYSTEM) altında çalıştırılması genellikle Kaspersky güncelleme hizmeti aracılığıyla yükseltme yapılırken ya da Kaspersky Security Center aracılığıyla bir yükleme paketi dağıtılırken gerçekleştirilir.

Kaspersky Endpoint Security'yi ayrıcalıklı olmayan bir kullanıcı hesabı altında bir MSI dosyası kullanarak yükseltiyorsanız, Kaspersky Endpoint Security'nin Kaspersky çözümlerinin geçerli lisanslarına erişimi olmaz. Bu durumda Kaspersky Endpoint Security, Kaspersky Endpoint Agent'ın bir dizi bileşenini temel alarak bileşenleri otomatik olarak seçer. Bundan sonra, Kaspersky Endpoint Security' bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

Kaspersky Endpoint Security, bilgisayar yeniden başlatılmadan yükseltme yapılmasını destekler. İlke özelliklerinde uygulama yükseltme modunu seçebilirsiniz.

5 Uygulama çalışmasının kontrolü

Uygulama yükleme veya yükseltmesi sonrasında bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

- Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
- *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, yerleşik aracı işlevselliğini etkinleştirdiğinizden emin olun.
- Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.

6 Kaspersky Anti Targeted Attack Platform sunucusuna bağlantıyı yapılandırma

Kaspersky Anti Targeted Attack Platform sunucusuna bağlantıyı kontrol edin. Bunun için:

1. Geçerli bir sertifikanız olup olmadığını kontrol edin.
2. Sunucu bağlantı ayarlarını kontrol edin.
3. Olay günlüğünü kontrol edin.

   Sunucuyla bir bağlantı kurulursa, uygulama *EDR Expert sunucusuna bağlantı başarılı* olayını gönderir. Başarılı bir bağlantı olayı ve bağlantı hataları içeren hiçbir olay yoksa, olay günlüğü ayarlarını kontrol edin ve Endpoint Detection and Response (KATA) için olay gönderimini etkinleştirin.

Sunucu bağlantı durumu, Kaspersky Security Center konsolundaki bilgisayar durumunu etkilemez. Bu nedenle, sunucuyla bağlantı yoksa, bilgisayar yine de *Tamam* durumuna sahip olabilir. Sunucuyla bağlantıyı doğrulamak için olay günlüğünü kontrol edin.

7 Performans kontrolü

Bir uygulamayı yükledikten veya güncelledikten sonra bilgisayarınızın performansı yavaşladıysa, veri aktarımını optimize edebilirsiniz. Bunun için:

1. EDR (KATA) bileşenini devre dışı bırakın ve performans düşüşünün EDR (KATA) kaynaklı olup olmadığını kontrol edin.
2. Güvenilir uygulamalar için, konsol giriş işlemlerinde telemetri toplamayı kapatın (varsayılan olarak etkindir).
3. Bilgisayar performansını düşüren uygulamaları güvenilir uygulamalar listesine ekleyin.
4. Kaspersky Teknik Destek ile iletişim kurun. Destek uzmanları, Kaspersky Anti Targeted Attack Platform'da telemetri filtrelemeyi yapılandırmanıza yardımcı olacaktır. Bu sayede trafik miktarı azalacaktır. Bilgisayarınızın performansı belirli bir uygulamadan etkileniyorsa, bu uygulamanın dağıtım paketini isteğe ekleyin.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Detection and Response Expert (on-premises) çözümüyle entegrasyonu destekler. *Kaspersky Endpoint Detection and Response Expert (on-premises)*, bir kuruluşun çoğu siber risk türüne karşı savunma yapmasını ve en önemli tehdit yayılma senaryolarını kapsamasını sağlayan Kaspersky uygulamalarını içeren kurumsal bir siber güvenlik çözümüdür. EDR Expert (on-premises) bileşenleri, Açık Tek Yönetim Platformu (OSMP) üzerinde dağıtılır. Bu platform, platformlar arası senaryoları tek bir arabirimde çalıştırır ve Kaspersky uygulamalarının üçüncü taraf uygulamalarla entegre edilerek kapsamlı bir güvenlik sistemine dönüştürülmesini sağlar.

Çözümün merkezi unsurlarından biri *SIEM*'dir. SIEM, tüm bileşenlerden gelen olayları izler ve satıcı ve kullanıcı tanımlı kuralları kullanarak bu olayları birbiriyle ilişkilendirir. EDR Expert (on-premises), saldırıları otomatik olarak tespit etmek için kurumsal altyapıdan alınan günlükleri ve telemetriyi inceler ve Kaspersky uygulamalarından ve üçüncü taraf bilgi güvenliği ürünlerinden gelen olaylar dahil olmak üzere EDR Expert (on-premises) içinde toplanan tüm olayları birleştiren birleşik bir araştırma grafiği kullanarak olayların araştırılmasını sağlar.

Gelişmiş olaylara müdahale etmek için EDR Expert (on-premises), önceden ayarlanmış ve kullanıcı tanımlı senaryolar kullanır. Üçüncü taraf uygulamalardan gelen yanıt eylemlerini ve birden fazla uygulamayı içeren yanıt senaryolarını da kullanabilirsiniz.

Tehdit İstihbarat araçları

Kaspersky Endpoint Detection and Response, aşağıdaki Threat Intelligence araçlarını kullanır:

- Dosyaların ve internet adreslerinin tanınırlığı hakkında bilgi içeren ve görüntüleyen Kaspersky Threat Intelligence Portal ile entegrasyon.
- Kaspersky Tehditler veritabanı.
- Kaspersky bilgi bankasından gerçek zamanlı dosya, web sitesi ve yazılım tanınırlık bilgilerine erişim sağlayan Kaspersky Security Network (bundan böyle "KSN" olarak anılacaktır) bulut hizmeti altyapısı. Kaspersky Security Network'ten gelen verilerin kullanılması Kaspersky uygulamalarının tehditlerle karşılaştığında verdiği tepki süresini kısaltır ve bazı koruma bileşenlerinin performansını iyileştirerek hatalı pozitif sonuç riskini azaltır.

Çözümün çalışma prensibi

Kaspersky Endpoint Security, kurumsal BT altyapısındaki bilgisayarlara yüklenir ve süreçleri, açık ağ bağlantılarını ve değiştirilmekte olan dosyaları sürekli olarak izler.

VDI altyapısında standart modda kurulduğunda Kaspersky Endpoint Security, EDR Expert (on-premises) ile entegrasyonu destekler. Ancak, uygulamanın diğer işlevlerinin çalışabilirliği garanti edilmez. VDI altyapısındaki sanal makineleri korumak için Kaspersky Endpoint Security'yi Light Agent modunda kullanmanızı öneririz.

Bilgisayardaki olaylarla ilgili bilgiler (telemetri), EDR Expert (on-premises) sunucusuna gönderilir. Bu durumda, Kaspersky Endpoint Security ayrıca uygulama tarafından keşfedilen tehditler ve bu tehditlerin işlenmesinden elde edilen sonuçlar hakkında bilgiler gönderir.

EDR Expert (on-premises) entegrasyonu, Kaspersky Security Center konsolunda yapılandırılır. Yerleşik aracı daha sonra görevleri çalıştırma, karantinaya alınan nesneleri yönetme, raporları görüntüleme ve diğer eylemler dahil olmak üzere Open Single Management Platform (OSMP) kullanılarak yönetilir.

EDR Expert (on-premises) ile çalışmaya yönelik Kaspersky Endpoint Security yapılandırmaları

EDR Expert (on-premises) ile çalışmak için aşağıdaki yapılandırmalar kullanılabilir:

- **[KES+yerleşik aracı]**. Bu yapılandırmada Kaspersky Endpoint Security, hem bilgisayarın güvenliğini sağlayan uygulama hem de EDR Expert (on-premises) ile çalışmaya yönelik uygulama olarak görev yapar. EDR Expert (on-premises) için yerleşik aracı, Kaspersky Endpoint Security 12.11 for Windows veya sonraki sürümlerde kullanılabilir.
- **[üçüncü taraf EPP+EDR Agent]**. Bu yapılandırmada, BT altyapısının güvenliği üçüncü taraf Endpoint Protection Platform (EPP) tarafından sağlanır. EDR Expert (on-premises) ile etkileşim, Endpoint Detection and Response Agent (EDR Agent) yapılandırmasında Kaspersky Endpoint Security tarafından sağlanır. EDR Agent bu yapılandırmada üçüncü taraf EPP uygulamalarıyla uyumludur. EDR Expert (on-premises) için EDR Agent, Kaspersky Endpoint Security 12.11 for Windows veya sonraki sürümlerde kullanılabilir.

Yerleşik aracının EDR Expert (on-premises) ile entegrasyonu

Kaspersky Endpoint Detection and Response Expert (on-premises) çözümüyle entegrasyon sağlamak için Endpoint Detection and Response Expert (on-premises) bileşenini eklemeniz ve Kaspersky Endpoint Security'yi yapılandırmanız gerekir.

Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) ve Endpoint Detection and Response Expert (on-premises) bileşenleri birbirleriyle uyumlu değildir.

Endpoint Detection and Response Expert (on-premises) bileşeninin çalışması için şu koşulların karşılanması gerekir:

- OSMP (Open Single Management Platform) yüklendi.
- Uygulama etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.

- Endpoint Detection and Response Expert (on-premises) bileşeni açık olmalıdır.
- EDR Expert (on-premises) ürününün çalışmasını sağlayan uygulama bileşenleri etkin ve çalışır durumda olmalıdır. Aşağıdaki bileşenler EDR Expert (on-premises) ürününün çalışmasını sağlar:
  - Dosya Tehdidi Koruması.
  - Web Tehdidi Koruması.
  - Posta Tehdidi Koruması.
  - Exploit Önleme.
  - Davranış Tespiti.
  - Sunucu Yetkisiz Erişim Önleme.
  - Düzeltme Altyapısı.
  - Uyarlamalı Anomali Denetimi.

EDR Expert (on-premises) entegrasyonunu ayarlama aşağıdaki adımları içerir:

1. **EDR Expert (on-premises) bileşeninin yüklenmesi**

   EDR Expert (on-premises) bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanarak seçebilirsiniz.

   > Uygulamayı yeni bileşenle yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatmanız gerekir.

2. **Kaspersky Endpoint Detection and Response Expert (on-premises) ürününün etkinleştirilmesi**

   EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) Eklentisi) için ayrı bir lisans satın almanız gerekir.

   Kaspersky Endpoint Detection and Response Expert (on-premises) için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir hale gelir. Sonuç olarak bilgisayara iki anahtar eklenir: Kaspersky Endpoint Security için bir anahtar ve Kaspersky Endpoint Detection and Response Expert (on-premises) için bir anahtar.

   Bağımsız Endpoint Detection and Response Expert (on-premises) işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   EDR Expert (on-premises) işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

3. **Telemetri toplama sunucusuna ve yanıt sunucusuna bağlanma**

   Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Security ile iki sunucu arasında güvenilir bir bağlantı gerektirir:

   - Bir *telemetri toplama sunucusu*, SIEM çözümünün bir parçası olan ve bilgisayarda meydana gelen olaylarla ilgili bilgileri toplayan, normalleştiren, ilişkilendiren, analiz eden ve depolayan bir sunucudur.
   - Bir *yanıt sunucusu*, verileri almak ve taramak, nesnelerin davranışlarını incelemek ve bu tür çalışmaların sonuçlarını yayınlamak için kullanılan bir sunucudur.

Güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası kullanmanız gerekir. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Ardından TLS sertifikasını Kaspersky Endpoint Security'ye eklemeniz gerekir (aşağıdaki talimatlara bakın).

Varsayılan olarak, Kaspersky Endpoint Security yalnızca sunucuların TLS sertifikasını kontrol eder. Bağlantıyı daha güvenli hale getirmek için, ek olarak sunucudaki bilgisayarın doğrulanmasını etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu doğrulamayı etkinleştirmek için sunucu ve Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı açmanız gerekir. İki yönlü kimlik doğrulamayı kullanmak için ayrıca bir kripto konteynere ihtiyacınız olacaktır. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).

Web Console kullanarak bir Kaspersky Endpoint Security bilgisayarını EDR Expert'e (on-premises) bağlama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (on-premises)** bölümüne gidin.
5. **Endpoint Detection and Response Expert (on-premises) ETKİN** iki durumlu düğmesini açık duruma getirin.
6. EDR Expert (on-premises) ürününü yapılandırmak için çözümler listesinden **Endpoint Detection and Response Expert (sürüm 8.0 veya üstü)** seçeneğini seçin.
7. *Telemetri toplama sunucuları* bağlantısını yapılandırın:

   a. **Telemetri toplama sunucularına bağlantı** bloğunda **Bağlantı ayarları** bağlantısına tıklayın.

   b. Telemetri toplama sunucuları bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır.
   - **Sunucu sertifikası**. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).
   - **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ile sunucu arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için sunucu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto kabı almanız ve kripto kabını korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Sunucu ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto kapsayıcı yüklemeniz gerekir.

     Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

c. **Tamam**'a tıklayın.

d. Telemetri toplama sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

Birden fazla telemetri toplama sunucusu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

e. Gerekirse telemetriyi yapılandırın.

8. *Yanıt sunucuları* bağlantısını yapılandırın:

a. **Yanıt sunucularına bağlantı** bloğunda, **Senkronizasyon isteğini sunucuya her (dk)** gönder ayarını yapılandırın. Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında Kaspersky Endpoint Security tehdit yanıtı görevlerini alır ve görev sonuçlarını gönderir.

b. **Bağlantı ayarları** bağlantısına tıklayın.

c. Yanıt sunucuları bağlantısını yapılandırın:

- **Zaman aşımı (sn)**. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır.
- **Sunucu sertifikası**. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).
- **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ile sunucu arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için sunucu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto kabı almanız ve kripto kabını korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Sunucu ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto kapsayıcı yüklemeniz gerekir.

  Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

d. **Tamam**'a tıklayın.

e. Yanıt sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için portu belirtin.

Birden fazla yanıt sunucusu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Bileşen durumunu *Uygulama bileşenlerinin durumu raporu* aracılığıyla kontrol edebilirsiniz. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Endpoint Detection and Response Expert (on-premises)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

EDR Expert (on-premises) telemetri ayarlarını yapılandırma

Telemetri, korunan bilgisayarda meydana gelen olayların bir listesidir. Kaspersky Endpoint Security telemetri verilerini analiz eder ve senkronizasyon sırasında telemetri toplama sunucularına gönderir. Aktarılan telemetri olayları hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğine bakın.

Telemetri olayları sunucuya neredeyse sürekli olarak ulaşır. Kaspersky Endpoint Security, şu koşullardan herhangi biri karşılandığında sunucu ile senkronizasyonu başlatır:

- Senkronizasyon aralığı sona erdi.
- Arabellekteki olay sayısı üst sınırı aşıyor.

Bu nedenle, varsayılan olarak, uygulama her 30 saniyede bir veya tampon bellekte 1024 olay biriktiğinde senkronize olur. Kaspersky Endpoint Security ilkesinde senkronizasyon davranışını yapılandırabilir ve ağ yükünüze uyacak optimum değerleri seçebilirsiniz (aşağıdaki talimatlara bakın).

Kaspersky Endpoint Security ile sunucu arasında bağlantı yoksa uygulama yeni olayları kuyruğa alır. Bağlantı yeniden sağlandığında, Kaspersky Endpoint Security sıraya alınan olayları sunucuya uygun sırayla gönderir. Sunucunun aşırı yüklenmesini önlemek için Kaspersky Endpoint Security bazı olayları atlayabilir. Bunu etkinleştirmek için, örneğin saat başına maksimum olay değerini ayarlamak için olay iletim ayarlarını optimize edebilirsiniz (aşağıdaki talimatlara bakın).

Telemetri ayarlarını yapılandırmak için şu adımları uygulayın:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (on-premises)** bölümüne gidin.
5. EDR Expert (on-premises) ürününü yapılandırmak için çözümler listesinden **Endpoint Detection and Response Expert (sürüm 8.0 veya üstü)** seçeneğini seçin.
6. **Veri iletim ayarları** bloğunda **Telemetri verilerini telemetri toplama sunucularına gönder** onay kutusunun seçili olduğundan emin olun.
7. Gerekirse, **Telemetriyi yalnızca IOA ile gönder** onay kutusunu seçin. *Saldırı Göstergesi (IOA)*, hedefli bir saldırıyı işaret edebilecek sistemdeki şüpheli davranışların açıklamasını içeren bir kuraldır. Uygulama, sistemdeki devam eden davranışları bu kurallarla karşılaştırır ve hedefli bir saldırıyı gösteren olayları günlüğe kaydeder. Uygulama, bu tür olayların gerçek zamanlı olarak izlenmesini sağlayan *akış tarama* teknolojisini kullanır.
8. Gerekirse, **Veri iletim ayarları** bloğundaki sunucu ayarlarıyla senkronizasyonu yapılandırın:
   - **Maksimum olay iletim gecikmesi (sn)**. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
   - **Paket başına maksimum olay sayısı**. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır.

9. Gerekirse, **Talep daraltma** bloğunda **Talep daraltmayı etkinleştir** onay kutusunun işaretini kaldırın.

   Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur. Bu seçenek varsayılan olarak etkindir.

10. Olayları sunucuya göndermek için optimizasyon ayarlarını yapılandırın:

    - **Saat başına maksimum olay sayısı**. Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir.

    - **Olay sınırı aşım yüzdesi**. Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.

11. **Yanıt sunucularına bağlantı** bloğunda, **Senkronizasyon isteğini sunucuya her (dk) gönder** parametresini yapılandırın.

12. Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.

13. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

EDR Expert (on-premises) telemetri istisnaları

Performansı artırmak ve telemetri toplama sunucusuna veri iletimini optimize etmek için telemetri istisnaları ekleyebilirsiniz. Örneğin, bireysel uygulamalar için ağ iletişim verilerini göndermemeyi seçebilirsiniz.

> Çok fazla kural kullanmak Telemetri toplama sunucusu üzerindeki yükü artırabilir ve bilgisayar performansını düşürebilir. Sadece gerekli kuralları eklemenizi öneririz.

Web Console'da ve Cloud Console'da bir telemetri istisnası oluşturmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Telemetri Ayarları** bölümüne gidin.

5. **EDR Expert (on-premises) telemetri** sekmesini seçin.

6. **Genel istisnalar** bloğunda **Ekle** düğmesine tıklayın.

   İstisna kuralı ekle penceresi açılır.

7. Gerekirse kuralın durumunu değiştirin. Varsayılan olarak, kural etkindir.

8. Kural için bir ad girin.

9. Kural tetiklendiğinde gerçekleştirilecek eylemi seçin:

   - **Toplama**. Filtrelenen olay, gönderilen telemetri verilerinden hariç tutulacaktır.

   - **IOA'yı hariç tut**. IOA kuralı tetikleme olayı, gönderilen telemetri verilerinden hariç tutulacaktır.

10. **IOA'yı hariç tut** seçeneği işaretliyse, istisna listesine eklenecek IOA kurallarını belirtin:

    - **Tümünü hariç tut**. Belirtilen koşul karşılandığında, uygulama tüm IOA kurallarına göre oluşturulan olayları telemetri verilerinden hariç tutacaktır.

    - **GUID'ye göre hariç tut**. IOA kuralının GUID'sini belirtin. Burada, `,` kullanarak birden fazla GUID belirtebilirsiniz. IOA kuralları hakkında daha fazla ayrıntı için lütfen EDR Expert (on-premises) Yardım bölümüne bakın.

11. Filtreleme koşulunu belirtin:

    a. Filtreleme için kullanılacak alan adını seçin.

    b. Bir operatör seçin (aşağıdaki tabloya bakın) ve olaydaki alan değerinin karşılaştırılacağı değeri belirtin.

Koşullu operatörlerin listesi

Operatör	Açıklama
<	Alan değeri, koşulda belirtilen değerden küçükse, olay filtrelenerek çıkarılır.
≤	Alan değeri, koşulda belirtilen değerden küçük veya ona eşitse, olay filtrelenerek çıkarılır.
=	Alanın değeri koşulda belirtilen değerle aynıysa, olay filtrelenerek çıkarılır.
≥	Alanın değeri, koşulda belirtilen değerden büyük veya ona eşitse, olay filtrelenerek çıkarılır.
>	Alan değeri, koşulda belirtilen değerden büyükse, olay filtrelenerek çıkarılır.
≠	Alanın değeri koşulda belirtilen değerle aynı değilse, olay filtrelenerek dışarıda bırakılır.
şuna benziyor	Alan değeri, koşulda belirtilen maskeyle eşleşirse, olay filtrelenerek çıkarılır. Uygulama, maske girerken `*` ve `?` karakterlerini destekler:
şuna benzemiyor	Alan değeri, koşulda belirtilen maskeyle eşleşmezse, olay filtrelenerek çıkarılır. Uygulama, maske girerken `*` ve `?` karakterlerini destekler:
şunlardan biri	Alan değeri, koşulda belirtilen listedeki değerlerden biriyle eşleşirse, olay filtrelenmiş sayılır.
hiçbiri	Alan değeri, koşulda belirtilen listedeki değerlerin hiçbiriyle eşleşmezse, olay filtrelenmiş sayılır.
şunlardan birine benziyor	Alan değeri, koşulda belirtilen maskelerden biriyle eşleşirse, olay filtrelenerek çıkarılır. Uygulama, maske girerken * ve ? karakterlerini destekler.
şunlardan birine benzemiyor	Alan değeri, koşulda belirtilen maskelerden hiçbiriyle eşleşmezse, olay filtrelenerek çıkarılır. Uygulama, maske girerken * ve ? karakterlerini destekler.
var	Koşulda belirtilen alan olayda varsa, olay filtrelenerek çıkarılır.
yok	Koşulda belirtilen alan olayda yoksa, olay filtrelenerek çıkarılır.
contains	Koşulda belirtilen değer alan değerinde bulunuyorsa, olay filtrelenerek çıkarılacaktır.
şuna eşittir	Alanın değeri koşulda belirtilen değerle aynıysa, olay filtrelenerek çıkarılır. Tarama işleminin büyük/küçük harf duyarlılığı yoktur.
bitsel VE	Alan değeri ile koşulda belirtilen değer arasındaki bitsel VE (&) operatörünün sonucu 1 ise, olay filtrelenerek dışarıda bırakılır.

12. Gerekirse, birden fazla filtre koşulu ve koşul grubu ekleyerek karmaşık filtre kriterleri oluşturabilirsiniz. Ayrıca, bir koşul grubuna iç içe geçmiş koşullar ve koşul grupları da ekleyebilirsiniz. Aşağıdaki operatörleri kullanabilirsiniz:

    - **VE**, filtrenin belirtilen tüm koşulları karşılayan olayları seçtiği anlamına gelir.
    - **VEYA**, filtrenin belirtilen koşullardan birini karşılayan olayları seçtiği anlamına gelir.
    - **DEĞİL** (bu operatörü kullanmak için **Öncesine DEĞİL ekle** seçeneğini seçin), filtrenin belirtilen koşullardan hiçbirine uymayan olayları seçtiği anlamına gelir.

    Koşullar ve birinci düzey koşul grupları **VE** operatörüyle birleştirilir.

13. Bilgisayarınızda Open Single Management Platform (OSMP) çalışıyorsa, oluşturduğunuz filtreleme kuralını tarayabilirsiniz. Tarama işlemini başlatmak için **Kuralı kontrol et** düğmesine tıklayın.

    Açılan pencerede, oluşturulan kural ile filtrelenmiş olayların bir tablosu görüntülenecektir. Daha fazla ayrıntı için lütfen EDR Expert (on-premises) Yardım bölümüne bakın.

14. Gerekirse, **Tüm olay türleri** bölümünde olay türüne göre telemetri istisnaları ekleyin.

    a. Olay türünün adı üzerine tıklayın.

    b. Açılan pencerede, **Manuel olarak kur** düğmesine tıklayın.

    c. Gerekirse, **Olay gönder** anahtarını kullanarak seçilen olay türü için telemetri iletimini yapılandırın. Varsayılan olarak, tüm olay türleri için telemetri iletimi etkindir.

    d. **İstisna kuralları** bloğunda, **Ekle** düğmesine tıklayın.

    İstisna kuralı ekle penceresi açılır.

    e. Eklediğiniz her kural için 7 ila 13. adımlarda açıklanan işlemleri gerçekleştirin.

15. Bazı olay türleri için, toplanan telemetri verilerini genişletmek amacıyla dahil etme kuralları da ekleyebilirsiniz:

    a. **Dahil etme kuralları** bloğunda, **Ekle** düğmesine tıklayın.

    Dahil etme kuralları ekle penceresi açılır.

    b. Kural için bir ad girin.

    c. **Koşul** bölümünde, görüntülenen alanlara değerleri girin. Kullanılabilir alanların türü, seçilen olaya bağlıdır.

    İstisna kuralları, dahil etme kurallarına göre önceliklidir.

16. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

EDR Expert (on-premises) olay filtrelerini dışa ve içe aktarma

İstisna listesini bir JSON dosyasına aktarabilirsiniz. Daha sonra, dosyayı değiştirerek örneğin çok sayıda olay kimliği ekleyebilirsiniz. Ayrıca, dışa aktarma/içe aktarma işlevini kullanarak olay filtrelerini yedekleyebilir veya listeyi farklı bir sunucuya taşıyabilirsiniz.

Çok fazla kural kullanmak Telemetri toplama sunucusu üzerindeki yükü artırabilir ve bilgisayar performansını düşürebilir. Sadece gerekli kuralları eklemenizi öneririz.

Yönetim Konsolu'nda (MMC) olay filtrelerini dışa ve içe aktarma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Telemetri ayarları** → **EDR Expert (on-premises) telemetri** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Olay filtrelerini dışa aktarmak için:
   a. **Dışa aktar**'a tıklayın.
      Açılan pencerede, olay filtrelerini dışa aktarmak istediğiniz JSON dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   b. Dosyaya kaydet.
      Kaspersky Endpoint Security, olay filtrelerini JSON dosyasına aktarır.
7. Olay filtrelerini içe aktarmak için:
   a. **İçe aktar**'a tıklayın.
   b. Açılan pencerede, olay filtrelerini içe aktarmak istediğiniz JSON dosyasını seçin.
   c. Dosyayı aç.
      Bilgisayarda olay filtreleme kuralları zaten mevcutsa, Kaspersky Endpoint Security bunları içe aktarırken değiştirir.
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da olay filtrelerini dışa ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Telemetri Ayarları** bölümüne gidin.

5. **EDR Expert (on-premises) telemetri** sekmesini seçin.

6. Olay filtrelerini dışa aktarmak için:

   a. **Dışa aktar**'a tıklayın.

   b. Açılan pencerede, olay filtrelerini dışa aktarmak istediğiniz JSON dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   c. Dosyaya kaydet.

   Kaspersky Endpoint Security, olay filtrelerini JSON dosyasına aktarır.

7. Olay filtrelerini içe aktarmak için:

   a. **İçe aktar**'a tıklayın.

   b. Açılan pencerede, olay filtrelerini içe aktarmak istediğiniz JSON dosyasını seçin.

   c. Olay filtreleme kurallarının nasıl içe aktarılmasını istediğinizi seçin: mevcut kurallara ekleyerek veya mevcut kuralları atıp yenileriyle değiştirerek.

   d. Dosyayı aç.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Ayrıca komut satırını kullanarak da olay filtrelerini dışa veya içe aktarabilirsiniz.

EDR Expert (on-premises) ve EDR (KATA) ile entegrasyonu yapılandırmak için ilke profillerini kullanırken dikkat edilmesi gereken özel noktalar

Tek bir ilke kapsamında, belirli yönetim grupları için EDR (KATA) ile ve diğerleri için EDR Expert (on-premises) ile entegrasyonu yapılandırmak üzere ilke profillerini kullanmanız gerekir. EDR (KATA) entegrasyon ayarlarını ilke özelliklerinde yapılandırmanız gerekir; seçilen yönetim grupları için EDR Expert (on-premises) entegrasyonu ise ilke profili özelliklerinde yapılandırılmalıdır.

EDR Expert (on-premises) ile entegrasyonu yapılandırmak için ilke profillerini kullanmanın aşağıdaki sınırlamaları vardır:

- İlke özelliklerinde EDR Expert (on-premises) ile entegrasyonu yapılandırırsanız bu ayarlar tüm yönetim grupları için geçerli olur; ilke profillerindeki entegrasyon ayarları uygulanmaz.
- EDR Expert (on-premises) ile entegrasyonu yapılandırmak için ilke profillerini kullanırken, ilkeleri yönetmek üzere Yönetim Konsolu'nu (MMC) kullanamazsınız. İlke özelliklerini Yönetim Konsolu'nda açtığınızda, ilke profillerindeki EDR Expert (on-premises) entegrasyon ayarlarının üzerine ilkedeki ayarlar yazılır ve bu da bileşenin hatalı çalışmasına neden olur. Aşağıdaki talimatlara göre Endpoint Detection and Response Expert (on-premises) bileşen ayarlarını sıfırlamanız gerekir.
- EDR Expert (on-premises) ile entegrasyonu yapılandırmak için ilke profillerini kullanırken alt ilkeleri kullanamazsınız.

Web eklentisinin önceki bir sürümünde yapılandırılmış bir ilkeniz zaten varsa, EDR Expert (on-premises) entegrasyon ayarlarını ilke profillerinden yönetilen cihazlara uygulamak için Endpoint Detection and Response Expert (on-premises) bileşeninin ayarlarını sıfırlamanız gerekir.

Bileşen ayarlarını sıfırlamak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (on-premises)** bölümüne gidin.
5. İşletim modunu **Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi)** seçeneğinden **Endpoint Detection and Response Expert (sürüm 8.0 veya üzeri) modu** seçeneğine değiştirin.
6. Tekrar **Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi)** moduna geçin.
7. Değişikliklerinizi kaydedin.

Endpoint Detection and Response Expert (cloud)

Kaspersky Endpoint Security ile Kaspersky Endpoint Detection and Response Expert (cloud) arasındaki entegrasyon geçici olarak kullanılamamaktadır. Bu işlevselliğin 2026 yılı sonuna kadar desteklenmesi planlanmaktadır. Uygulama güncellemelerinden ve yeni özelliklerden haberdar olmak için Sürüm Notlarımızı takip edin.



Kaspersky Endpoint Security, Kaspersky Endpoint Detection and Response Expert (cloud) çözümüyle entegrasyonu destekler. *Kaspersky Endpoint Detection and Response Expert (cloud)*, bir kuruluşun çoğu siber risk türüne karşı savunma yapmasını ve en önemli tehdit yayılma senaryolarını kapsamasına olanak tanıyan Kaspersky uygulamalarını içeren bulut tabanlı bir siber güvenlik çözümüdür. EDR Expert (cloud) bileşenleri Open Single Management Platform (OSMP) üzerinde dağıtılır. Bu platform, platformlar arası senaryoları tek bir arabirimde çalıştırır ve Kaspersky uygulamalarının üçüncü taraf uygulamalarla entegre edilerek kapsamlı bir güvenlik sistemine dönüştürülmesini sağlar.

Çözümün merkezi unsurlarından biri *SIEM*dir. SIEM, tüm bileşenlerden gelen olayları izler ve satıcı ve kullanıcı tanımlı kuralları kullanarak bu olayları birbiriyle ilişkilendirir. EDR Expert (cloud), saldırıları otomatik olarak tespit etmek için kurumsal altyapıdan alınan günlüklere ve telemetriye bakar ve Kaspersky uygulamalarından ve üçüncü taraf bilgi güvenliği ürünlerinden gelen olaylar da dahil olmak üzere EDR Expert'te (cloud) toplanan tüm olayları birleştiren birleşik bir araştırma grafiği kullanarak olayların araştırılmasına olanak tanır.

Gelişmiş olaylara müdahale için EDR Expert (cloud) önceden ayarlanmış ve kullanıcı tanımlı senaryolar kullanır. Üçüncü taraf uygulamalardan gelen yanıt eylemlerini ve birden fazla uygulamayı içeren yanıt senaryolarını da kullanabilirsiniz.

Tehdit İstihbarat araçları

Kaspersky Endpoint Detection and Response, aşağıdaki Threat Intelligence araçlarını kullanır:

- Dosyaların ve internet adreslerinin tanınırlığı hakkında bilgi içeren ve görüntüleyen Kaspersky Threat Intelligence Portal ile entegrasyon.
- Kaspersky Tehditler veritabanı.
- Kaspersky bilgi bankasından gerçek zamanlı dosya, web sitesi ve yazılım tanınırlık bilgilerine erişim sağlayan Kaspersky Security Network (bundan böyle "KSN" olarak anılacaktır) bulut hizmeti altyapısı. Kaspersky Security Network'ten gelen verilerin kullanılması Kaspersky uygulamalarının tehditlerle karşılaştığında verdiği tepki süresini kısaltır ve bazı koruma bileşenlerinin performansını iyileştirerek hatalı pozitif sonuç riskini azaltır.

Çözümün çalışma prensibi

Kaspersky Endpoint Security, kurumsal BT altyapısındaki bilgisayarlara yüklenir ve süreçleri, açık ağ bağlantılarını ve değiştirilmekte olan dosyaları sürekli olarak izler.

Bilgisayardaki olaylar hakkındaki bilgiler (telemetri) EDR Expert (cloud) sunucusuna gönderilir. Bu durumda, Kaspersky Endpoint Security ayrıca uygulama tarafından keşfedilen tehditler ve bu tehditlerin işlenmesinden elde edilen sonuçlar hakkında bilgiler gönderir.

EDR Expert (cloud) entegrasyonu Kaspersky Security Center konsolunda yapılandırılır. Yerleşik aracı daha sonra görevleri çalıştırma, karantinaya alınan nesneleri yönetme, raporları görüntüleme ve diğer eylemler dahil olmak üzere Open Single Management Platform (OSMP) kullanılarak yönetilir.

Yerleşik aracının EDR Expert (cloud) ile entegrasyonu

Kaspersky Endpoint Detection and Response (cloud) çözümüyle entegrasyonu kurmak için, Endpoint Detection and Response Expert (cloud) bileşenini yüklemeniz ve Kaspersky Endpoint Security yapılandırmasını tamamlamanız gerekir.

> Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) ve Endpoint Detection and Response Expert (on-premises) bileşenleri birbirleriyle uyumlu değildir.

EDR Expert (cloud) çalışma koşulları

EDR Expert (cloud) uygulamasının çalışabilmesi için aşağıdaki koşulların sağlanması gerekir:

- Kaspersky Endpoint Detection and Response Expert (cloud) altyapısı bölgenizde kullanılabilir. Bölgenizde EDR Expert (cloud) altyapısının kullanılabilirliği hakkında bilgi almak için lütfen Teknik Destek ile iletişime geçin.
- OSMP (Open Single Management Platform) yüklendi.

- Kaspersky Endpoint Security standart modda yüklü.
- Kaspersky Endpoint Security uygulaması etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.
- Kaspersky Endpoint Detection and Response Expert (cloud) Veri İşleme Sözleşmesinin şartlarını kabul edilmelidir.
- Endpoint Detection and Response Expert (cloud) bileşeni etkinleştirilmiş olmalıdır.
- EDR Expert (cloud) ürününün çalışmasını sağlayan uygulama bileşenleri etkin ve çalışır durumda olmalıdır:
  - Dosya Tehdidi Koruması.
  - Web Tehdidi Koruması.
  - Posta Tehdidi Koruması.
  - Exploit Önleme.
  - Davranış Tespiti.
  - Sunucu Yetkisiz Erişim Önleme.
  - Düzeltme Altyapısı.
  - Uyarlamalı Anomali Denetimi.

EDR Expert (cloud) ile entegrasyon adımları

EDR Expert (cloud) Entegrasyonunun kurulması aşağıdaki adımları içerir:

1. **Endpoint Detection and Response Expert (cloud) bileşenini yükleme**

   Yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken Endpoint Detection and Response Expoert (cloud) bileşenini seçebilirsiniz.

   > Uygulamayı yeni bileşenle yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatmanız gerekir.

2. **Kaspersky Endpoint Detection and Response Expert (cloud) ürününün etkinleştirilmesi**

   Kaspersky Endpoint Detection and Response Expert (cloud) için ayrı bir lisans satın almanız gerekir.

   Kaspersky Endpoint Detection and Response Expert (cloud) için ayrı bir anahtar eklendikten sonra bu işlev kullanılabilir hale gelir. Sonuç olarak bilgisayara iki anahtar eklenir: Kaspersky Endpoint Security için bir anahtar ve Kaspersky Endpoint Detection and Response Expert (cloud) için bir anahtar.

   Bağımsız Endpoint Detection and Response Expert (cloud) işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   EDR Expert (cloud) işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

3. **Telemetri toplama sunucusuna ve yanıt sunucusuna bağlanma**

Kaspersky Endpoint Detection and Response Expert (cloud), Kaspersky Endpoint Security ile iki sunucu arasında güvenilir bir bağlantı gerektirir:

- Bir *telemetri toplama sunucusu*, SIEM çözümünün bir parçası olan ve bilgisayarda meydana gelen olaylarla ilgili bilgileri toplayan, normalleştiren, ilişkilendiren, analiz eden ve depolayan bir sunucudur.
- Bir *yanıt sunucusu*, verileri almak ve taramak, nesnelerin davranışlarını incelemek ve bu tür çalışmaların sonuçlarını yayınlamak için kullanılan bir sunucudur.

Web Console kullanılarak bir Kaspersky Endpoint Security bilgisayarı EDR Expert'e (cloud) ürününü bağlama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (cloud)** bölümüne gidin.
5. **Endpoint Detection and Response Expert (cloud) DEVRE DIŞI** anahtarını kullanarak bileşeni etkinleştirin.
6. Mevcut ilke bir alt ilke ise ve üst ilke EDR Expert (cloud) entegrasyon ayarlarında değişiklik yapılmasını engelliyorsa (kapalı "kilit" simgesi), **Devralma** bölümünden ayar devralma özelliğini yapılandırabilirsiniz:
   - **Bağlantı ayarlarını ilkeden devral** (varsayılan değer). Bağlantı ayarları üst ilkeye göre belirlenecektir. Ayarları düzenleyemezsiniz.
   - **Özel bağlantı ayarları kullanın**. Bağlantı ayarlarını manuel olarak yapılandırabilirsiniz.
7. **Yanıt Sunucusu** sekmesi, otomatik olarak alınan yanıt sunucusunun tam etki alanı adını ve portunu gösterir. Altyapınızdaki güvenlik ilkesi EDR Expert (cloud) sunucularına doğrudan bağlanmanıza izin vermiyorsa, bir TCP tüneli üzerinden bağlantı kurabilirsiniz:
   a. **Yanıt için TCP tüneli kullan** onay kutusunu işaretleyin.
   b. Tünele bağlanmak için sunucu adresini (IPv4, IPv6) ve portu belirtin.
8. Gerekirse, **Sunucuya her (dakika) senkronizasyon isteği gönder** alanından sunucuya senkronizasyon taleplerinin gönderilme sıklığını ayarlayın. Senkronizasyon sırasında Kaspersky Endpoint Security tehdit yanıtı görevlerini alır ve görev sonuçlarını gönderir.
9. **Telemetri toplama sunucusu** sekmesine gidin.

10. Telemetri toplama sunucusu bağlantı ayarlarını yapılandırın:

    a. **Düzenle** bağlantısına tıklayın.

    b. Açılan pencerede listeden telemetri toplama sunucusunu seçin. KUMA toplayıcı, EDR Expert (cloud) uygulamasında telemetri toplama sunucusu olarak görev yapar. Daha fazla ayrıntı için lütfen Kaspersky Unified Monitoring and Analysis Platform Yardım bölümüne bakın.

    Telemetri toplama sunucusuna bağlanırken bir hata oluşursa farklı bir sunucu seçin. Telemetri toplama sunucusuna bağlanamıyorsanız, lütfen Teknik Destek ile iletişime geçin.

    c. Gerekirse, yanıt sunucusu için yaptığınız gibi telemetri toplama sunucusuna TCP tüneli üzerinden bağlantı yapılandırabilirsiniz.

11. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Bileşen durumunu *Uygulama bileşenlerinin durumu raporu* aracılığıyla kontrol edebilirsiniz. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Endpoint Detection and Response Expert (cloud)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

EDR Expert (cloud) telemetri ayarlarını yapılandırma

Telemetri, korunan bilgisayarda meydana gelen olayların bir listesidir. Kaspersky Endpoint Security telemetri verilerini analiz eder ve senkronizasyon sırasında telemetri toplama sunucularına gönderir. Telemetri olayları sunucuya neredeyse sürekli olarak ulaşır. Kaspersky Endpoint Security, şu koşullardan herhangi biri karşılandığında sunucu ile senkronizasyonu başlatır:

- Senkronizasyon aralığı sona erdi.
- Arabellekteki olay sayısı üst sınırı aşıyor.

Bu nedenle, varsayılan olarak, uygulama her 30 saniyede bir veya tampon bellekte 1024 olay biriktiğinde senkronize olur. Kaspersky Endpoint Security ilkesinde senkronizasyon davranışını yapılandırabilir ve ağ yükünüze uyacak optimum değerleri seçebilirsiniz (aşağıdaki talimatlara bakın).

Kaspersky Endpoint Security ile sunucu arasında bağlantı yoksa uygulama yeni olayları kuyruğa alır. Bağlantı yeniden sağlandığında, Kaspersky Endpoint Security sıraya alınan olayları sunucuya uygun sırayla gönderir. Sunucunun aşırı yüklenmesini önlemek için Kaspersky Endpoint Security bazı olayları atlayabilir. Bunu etkinleştirmek için, örneğin saat başına maksimum olay değerini ayarlamak için olay iletim ayarlarını optimize edebilirsiniz (aşağıdaki talimatlara bakın).

Telemetri ayarlarını yapılandırmak için şu adımları uygulayın:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Aracılar Yapılandırması** → **Endpoint Detection and Response Expert (cloud)** bölümüne gidin.
5. Açılan pencerede, **Veri iletim ayarları** sekmesini seçin.
6. **Telemetri gönderme ETKİN** onay kutusunun seçili olduğundan emin olun.

7. Gerekirse **Yalnızca IOA ile telemetri gönder** işlevini etkinleştirin. *Saldırı Göstergesi (IOA)*, hedefli bir saldırıyı işaret edebilecek sistemdeki şüpheli davranışların açıklamasını içeren bir kuraldır. Uygulama, sistemdeki devam eden davranışları bu kurallarla karşılaştırır ve hedefli bir saldırıyı gösteren olayları günlüğe kaydeder. Uygulama, bu tür olayların gerçek zamanlı olarak izlenmesini sağlayan *akış tarama* teknolojisini kullanır. Varsayılan olarak, işlev devre dışıdır.

8. Gerekirse, sunucu senkronizasyon ayarlarını yapılandırın:

   - **Maksimum olay iletim gecikmesi (sn)**. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.

   - **Paket başına maksimum olay sayısı**. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır.

9. **Talep daraltma** sekmesine gidin.

10. Gerekirse **Talep daraltma ETKİN** geçiş düğmesini kullanarak talep daraltmasını devre dışı bırakın.

    Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur. Bu seçenek varsayılan olarak etkindir.

11. Olayları sunucuya göndermek için optimizasyon ayarlarını yapılandırın:

    - **Saat başına maksimum olay sayısı**. Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir.

    - **Olay sınırı aşım yüzdesi (%)**. Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.

12. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

EDR Expert (cloud) telemetri istisnaları

Performansı artırmak ve telemetri toplama sunucusuna veri iletimini optimize etmek için telemetri istisnaları ekleyebilirsiniz. Örneğin, bireysel uygulamalar için ağ iletişim verilerini göndermemeyi seçebilirsiniz.

Çok fazla kural kullanmak Telemetri toplama sunucusu üzerindeki yükü artırabilir ve bilgisayar performansını düşürebilir. Sadece gerekli kuralları eklemenizi öneririz.

Web Console'da ve Cloud Console'da bir telemetri istisnası oluşturmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi → İlkeler** sekmesini seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Telemetri Ayarları** bölümüne gidin.

5. **EDR Expert (cloud) telemetri** sekmesini seçin.

6. **Genel istisnalar** bloğunda **Ekle** düğmesine tıklayın.
   İstisna kuralı ekle penceresi açılır.

7. Gerekirse kuralın durumunu değiştirin. Varsayılan olarak, kural etkindir.

8. Kural için bir ad girin.

9. Kural tetiklendiğinde gerçekleştirilecek eylemi seçin:

   - **Toplama**. Filtrelenen olay, gönderilen telemetri verilerinden hariç tutulacaktır.
   - **IOA'yı hariç tut**. IOA kuralı tetikleme olayı, gönderilen telemetri verilerinden hariç tutulacaktır.

10. **IOA'yı hariç tut** seçeneği işaretliyse, istisna listesine eklenecek IOA kurallarını belirtin:

    - **Tümünü hariç tut**. Belirtilen koşul karşılandığında, uygulama tüm IOA kurallarına göre oluşturulan olayları telemetri verilerinden hariç tutacaktır.
    - **GUID'ye göre hariç tut**. IOA kuralının GUID'sini belirtin. Burada, `,` kullanarak birden fazla GUID belirtebilirsiniz. IOA kuralları hakkında daha fazla ayrıntı için lütfen EDR Expert (cloud) Yardım bölümüne bakın.

11. Filtreleme koşulunu belirtin:

    a. Filtreleme için kullanılacak alan adını seçin.

    b. Bir operatör seçin (aşağıdaki tabloya bakın) ve olaydaki alan değerinin karşılaştırılacağı değeri belirtin.

Koşullu operatörlerin listesi

Operatör	Açıklama
<	Alan değeri, koşulda belirtilen değerden küçükse, olay filtrelenerek çıkarılır.
≤	Alan değeri, koşulda belirtilen değerden küçük veya ona eşitse, olay filtrelenerek çıkarılır.
=	Alanın değeri koşulda belirtilen değerle aynıysa, olay filtrelenerek çıkarılır.
≥	Alanın değeri, koşulda belirtilen değerden büyük veya ona eşitse, olay filtrelenerek çıkarılır.
>	Alan değeri, koşulda belirtilen değerden büyükse, olay filtrelenerek çıkarılır.
≠	Alanın değeri koşulda belirtilen değerle aynı değilse, olay filtrelenerek dışarıda bırakılır.
şuna benziyor	Alan değeri, koşulda belirtilen maskeyle eşleşirse, olay filtrelenerek çıkarılır. Uygulama, maske girerken `*` ve `?` karakterlerini destekler:
şuna benzemiyor	Alan değeri, koşulda belirtilen maskeyle eşleşmezse, olay filtrelenerek çıkarılır. Uygulama, maske girerken `*` ve `?` karakterlerini destekler:
şunlardan biri	Alan değeri, koşulda belirtilen listedeki değerlerden biriyle eşleşirse, olay filtrelenmiş sayılır.
hiçbiri	Alan değeri, koşulda belirtilen listedeki değerlerin hiçbiriyle eşleşmezse, olay filtrelenmiş sayılır.
şunlardan birine benziyor	Alan değeri, koşulda belirtilen maskelerden biriyle eşleşirse, olay filtrelenerek çıkarılır. Uygulama, maske girerken * ve ? karakterlerini destekler.
şunlardan birine benzemiyor	Alan değeri, koşulda belirtilen maskelerden hiçbiriyle eşleşmezse, olay filtrelenerek çıkarılır. Uygulama, maske girerken * ve ? karakterlerini destekler.
var	Koşulda belirtilen alan olayda varsa, olay filtrelenerek çıkarılır.
yok	Koşulda belirtilen alan olayda yoksa, olay filtrelenerek çıkarılır.

Operatör	Açıklama
contains	Koşulda belirtilen değer alan değerinde bulunuyorsa, olay filtrelenerek çıkarılacaktır.
şuna eşittir	Alanın değeri koşulda belirtilen değerle aynıysa, olay filtrelenerek çıkarılır. Tarama işleminin büyük/küçük harf duyarlılığı yoktur.
bitsel VE	Alan değeri ile koşulda belirtilen değer arasındaki bitsel VE (&) operatörünün sonucu 1 ise, olay filtrelenerek dışarıda bırakılır.

12. Gerekirse, birden fazla filtre koşulu ve koşul grubu ekleyerek karmaşık filtre kriterleri oluşturabilirsiniz. Ayrıca, bir koşul grubuna iç içe geçmiş koşullar ve koşul grupları da ekleyebilirsiniz. Aşağıdaki operatörleri kullanabilirsiniz:

    - **VE**, filtrenin belirtilen tüm koşulları karşılayan olayları seçtiği anlamına gelir.
    - **VEYA**, filtrenin belirtilen koşullardan birini karşılayan olayları seçtiği anlamına gelir.
    - **DEĞİL** (bu operatörü kullanmak için **Öncesine DEĞİL ekle** seçeneğini seçin), filtrenin belirtilen koşullardan hiçbirine uymayan olayları seçtiği anlamına gelir.

    Koşullar ve birinci düzey koşul grupları **VE** operatörüyle birleştirilir.

13. Oluşturduğunuz filtreleme kuralını taramak için **Kuralı kontrol et** düğmesine tıklayın.

    Açılan pencerede, oluşturulan kural ile filtrelenmiş olayların bir tablosu görüntülenecektir. Daha fazla ayrıntı için lütfen EDR Expert (cloud) Yardım bölümüne bakın.

14. Gerekirse, **Tüm olay türleri** bölümünde olay türüne göre telemetri istisnaları ekleyin.

    a. Olay türünün adı üzerine tıklayın.

    b. Açılan pencerede, **Manuel olarak kur** düğmesine tıklayın.

    c. Gerekirse, **Olay gönder** anahtarını kullanarak seçilen olay türü için telemetri iletimini yapılandırın. Varsayılan olarak, tüm olay türleri için telemetri iletimi etkindir.

    d. **İstisna kuralları** bloğunda, **Ekle** düğmesine tıklayın.

    İstisna kuralı ekle penceresi açılır.

    e. Eklediğiniz her kural için 7 ila 13. adımlarda açıklanan işlemleri gerçekleştirin.

15. Bazı olay türleri için, toplanan telemetri verilerini genişletmek amacıyla dahil etme kuralları da ekleyebilirsiniz:

    a. **Dahil etme kuralları** bloğunda, **Ekle** düğmesine tıklayın.

    Dahil etme kuralları ekle penceresi açılır.

    b. Kural için bir ad girin.

    c. **Koşul** bölümünde, görüntülenen alanlara değerleri girin. Kullanılabilir alanların türü, seçilen olaya bağlıdır.

    İstisna kuralları, dahil etme kurallarına göre önceliklidir.

16. İlkeyi bilgisayarlara uygulamak için asma kilitlerin kapalı olduğundan emin olun (🔒) ve değişikliklerinizi kaydedin.

EDR Expert (cloud) olay filtrelerini dışa veya içe aktarma

İstisna listesini bir JSON dosyasına aktarabilirsiniz. Daha sonra, dosyayı değiştirerek örneğin çok sayıda olay kimliği ekleyebilirsiniz. Ayrıca, dışa aktarma/içe aktarma işlevini kullanarak olay filtrelerini yedekleyebilir veya listeyi farklı bir sunucuya taşıyabilirsiniz.

Çok fazla kural kullanmak Telemetri toplama sunucusu üzerindeki yükü artırabilir ve bilgisayar performansını düşürebilir. Sadece gerekli kuralları eklemenizi öneririz.

Web Console'da olay filtrelerini dışa ve içe aktarmak için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Telemetri Ayarlarıı** bölümüne gidin.
5. **EDR Expert (cloud) telemetri** sekmesini seçin.
6. Olay filtrelerini dışa aktarmak için:
   a. **Dışa aktar**'a tıklayın.
   b. Açılan pencerede, olay filtrelerini dışa aktarmak istediğiniz JSON dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   c. Dosyaya kaydet.

      Kaspersky Endpoint Security, olay filtrelerini JSON dosyasına aktarır.
7. Olay filtrelerini içe aktarmak için:
   a. **İçe aktar**'a tıklayın.
   b. Açılan pencerede, olay filtrelerini içe aktarmak istediğiniz JSON dosyasını seçin.
   c. Olay filtreleme kurallarının nasıl içe aktarılmasını istediğinizi seçin: mevcut kurallara ekleyerek veya mevcut kuralları atıp yenileriyle değiştirerek.
   d. Dosyayı aç.
8. İlkeyi bilgisayarlara uygulamak için asma kilitlerin kapalı olduğundan emin olun (🔒) ve değişikliklerinizi kaydedin.
   1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
   2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

      İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Telemetri Ayarları** bölümüne gidin.

5. **EDR Expert (cloud) telemetri** sekmesini seçin.

6. Olay filtrelerini dışa aktarmak için:

   a. **Dışa aktar**'a tıklayın.

   b. Açılan pencerede, olay filtrelerini dışa aktarmak istediğiniz JSON dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   c. Dosyaya kaydet.

   Kaspersky Endpoint Security, olay filtrelerini JSON dosyasına aktarır.

7. Olay filtrelerini içe aktarmak için:

   a. **İçe aktar**'a tıklayın.

   b. Açılan pencerede, olay filtrelerini içe aktarmak istediğiniz JSON dosyasını seçin.

   c. Olay filtreleme kurallarının nasıl içe aktarılmasını istediğinizi seçin: mevcut kurallara ekleyerek veya mevcut kuralları atıp yenileriyle değiştirerek.

   d. Dosyayı aç.

8. İlkeyi bilgisayarlara uygulamak için asma kilitlerin kapalı olduğundan emin olun (🔒) ve değişikliklerinizi kaydedin.

Karantinayı Yönetme

Karantina bilgisayardaki özel bir yerel depolama alanıdır. Kullanıcı, bilgisayar için tehlikeli olduğunu düşündüğü dosyaları karantinaya alabilir. Karantinaya alınan dosyalar şifrelenmiş bir durumda saklanır ve cihazın güvenliğini tehdit etmez. Kaspersky Endpoint Security, Karantinayı yalnızca Kaspersky Detection and Response çözümleriyle entegre edildiğinde kullanır. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantina'nın yönetimi hakkında ayrıntılar için lütfen Kaspersky Sandbox Yardım, Kaspersky Endpoint Detection and Response Optimum Yardım, Kaspersky Endpoint Detection and Response Expert Yardım, Kaspersky Anti Targeted Attack Platform Yardım ve Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım belgelerine bakın.

Kaspersky Endpoint Security, dosyaları karantinaya almak için sistem hesabını (SYSTEM) kullanır.

Karantina ayarlarını sadece Kaspersky Security Center Konsolu üzerinden yapılandırabilirsiniz. Karantinaya alınan nesneleri yönetmek (geri yükleme, silme, ekleme vb.) için Kaspersky Security Center Konsolunu da kullanabilirsiniz. Yerel olarak, bilgisayarda yalnızca komut satırını kullanarak nesneyi geri yükleyebilirsiniz.

Maksimum Karantina boyutunu yapılandırma

Karantina boyutu varsayılan olarak 1024 MB ile sınırlandırılmıştır. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security dosya göndermeyi durdurur ve *Karantina depolamasında yeterli alan yok* olayını oluşturur. Karantinada disk alanı bitmesini önlemek için, Kaspersky Endpoint Security'nin *Karantina depolama alanı neredeyse doldu* olayı oluşturduğu bir eşik değeri ayarlayabilirsiniz. Karantinaya alınan dosyaların otomatik olarak silinmesi için saklama süresi yapılandırılamaz.

Kuruluşunuzda Kaspersky Anti Targeted Attack Platform (EDR) çözümü kullanılıyorsa, Karantina boyutunu artırmanızı öneririz. Bir YARA taraması yaparken, uygulama büyük bir bellek dökümü ile karşılaşabilir. Bellek dökümünün boyutu Karantina boyutunu aştığı takdirde, YARA taraması bir hatayla tamamlanır ve bellek dökümü karantinaya alınmaz. Karantina boyutunu bilgisayarın RAM'inin toplam boyutuna eşit olacak şekilde ayarlamanızı (örneğin, 8 GB) veya Karantina boyut sınırını devre dışı bırakmanızı öneririz.

Yönetim Konsolu'nda (MMC) maksimum karantina boyutunu yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.
4. **Karantina** bloğundan Karantina boyutunu yapılandırın:
   - **Karantina boyutunu şununla sınırla: N MB**. Bu onay kutusu seçildiğinde maksimum Karantina boyutu tanımlanan değerle sınırlanır. Varsayılan olarak, maksimum boyut 1024 MB'tır. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security *Karantina depolamasında yeterli alan yok* olayını Kaspersky Security Center'a gönderir ve olayı Windows Olay Günlüğünde yayınlar. Bu arada uygulama yeni nesneleri karantinaya almayı durdurur. Karantiyanı manuel olarak boşaltmanız gerekir.

     Onay kutusunun işareti kaldırıldığında, Karantina boyutu kullanılabilir boş disk alanı ile olur.
   - **Karantina depolamasının boyutu şu yüzdeye ulaştığında bildirim yap: yüzde N**. Karantinanın eşik değeri. Örneğin, Karantina eşiğini %50 olarak ayarlayabilirsiniz. Karantina eşiğe ulaştığında, Kaspersky Endpoint Security ilgili olayı Kaspersky Security Center'a gönderir ve olayı Windows Olay Günlüğünde yayınlar. Bu arada uygulama yeni nesneleri karantinaya almaya devam eder.

     Bu onay kutusunun işaretini kaldırırsanız, uygulama karantina eşiğine ulaşıldığında olaylar oluşturmaz.
5. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da maksimum Karantina boyutunu yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Raporlar ve Depolama Alanı** bölümüne gidin.

5. **Karantina** bloğundan Karantina boyutunu yapılandırın:

   - **Karantina boyutunu şununla sınırla**. Bu onay kutusu işaretlendiğinde, Karantina boyutu belirtilen değerle sınırlandırılır. Onay kutusunun işareti kaldırıldığında, Karantina boyutu kullanılabilir boş disk alanı ile olur. Bu, YARA taraması için gerekli olabilir çünkü uygulama büyük bir bellek döküm dosyası kaydedebilir.

   - **Karantina maksimum boyutu (MB)**. Bu onay kutusu seçildiğinde maksimum Karantina boyutu tanımlanan değerle sınırlanır. Varsayılan olarak, maksimum boyut 1024 MB'tır. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security *Karantina depolamasında yeterli alan yok* olayını Kaspersky Security Center'a gönderir ve olayı Windows Olay Günlüğünde yayınlar. Bu arada uygulama yeni nesneleri karantinaya almayı durdurur. Karantiyanı manuel olarak boşaltmanız gerekir.

     Onay kutusunun işareti kaldırıldığında, Karantina boyutu kullanılabilir boş disk alanı ile olur.

   - **Karantina depolamasının boyutu şu seviyeye ulaştığında bildirim yap (%)**. Karantinanın eşik değeri. Örneğin, Karantina eşiğini %50 olarak ayarlayabilirsiniz. Karantina eşiğe ulaştığında, Kaspersky Endpoint Security ilgili olayı Kaspersky Security Center'a gönderir ve olayı Windows Olay Günlüğünde yayınlar. Bu arada uygulama yeni nesneleri karantinaya almaya devam eder.

6. Değişikliklerinizi kaydedin.

Karantinaya alınan dosyalarla ilgili verileri Kaspersky Security Center'a gönderme

Web Console'da karantinaya alınan nesnelerle eylemler gerçekleştirmek için karantinaya alınan dosya verilerinin Yönetim Sunucusu'na gönderilmesini etkinleştirmeniz gerekir. Örneğin, Web Console'da analiz için karantinadan bir dosya indirebilirsiniz. Karantinaya alınan dosya verilerinin gönderilmesi, tüm Kaspersky Sandbox ve Kaspersky Endpoint Detection and Response işlevlerinin çalışması için etkinleştirilmelidir.

Yönetim Konsolu'nda (MMC) karantinaya alınan dosya verilerinin aktarımı nasıl etkinleştirilir

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.
4. **Yönetim Sunucusu'na veri aktarımı** bloğunda, **Ayarlar** düğmesine tıklayın.
5. Açılan pencerede, **Karantina dosyaları** kutucuğunu işaretleyin.
6. Değişikliklerinizi kaydedin.

Web Console'da karantinaya alınan dosya verilerinin aktarımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **KSC Entegrasyonu** bölümüne gidin.

5. **Yönetim Sunucusu'na veri aktarımı** bloğundan **Karantina dosyaları hakkında** onay kutusunu işaretleyin.

6. Değişikliklerinizi kaydedin.

Sonuç olarak, bilgisayarınızda karantinaya alınan dosyaların bir listesini Kaspersky Security Center Konsolunda görüntüleyebilirsiniz. Karantinaya alınan nesneleri yönetmek (geri yükleme, silme, ekleme vb.) için Kaspersky Security Center Konsolunu kullanabilirsiniz. Karantina ile çalışmak hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

Dosyaları Karantinadan geri yükleme

Varsayılan olarak, Kaspersky Endpoint Security, dosyaları orijinal klasörlerine geri yükler. Hedef klasör silinmişse veya kullanıcının bu klasöre erişim hakları yoksa, uygulama dosyayı `%DataRoot%\QB\Restored` klasörüne konumlandırır. Bundan sonra dosyayı manuel olarak hedef klasöre taşımalısınız.

Dosyaları Karantinadan geri yüklemek için:

1. Web Console ana penceresinden **İşlemler** → **Veri havuzları** → **Karantina** seçimini yapın.

2. Bu, Karantinadaki dosyaların listesini açar; bu listede, geri yüklemek istediğiniz dosyaları seçin ve **Geri yükle**'ye tıklayın.

   Kaspersky Endpoint Security bu dosyayı geri yükler. Hedef klasörde zaten aynı ada sahip bir dosya varsa, uygulama dosyanın geri yüklenmesini iptal eder. Uygulama, dosyayı geri yükledikten sonra dosyanın bir kopyasını Karantinaya kaydeder. Dosyayı silmek için Karantinayı el ile temizlemeniz gerekir.

EDR eylemlerinin izlenmesi

Kaspersky Endpoint Security for Windows 12.9, EDR eylem izleme merkezini sunar. *EDR eylem izleme merkezi*, tüm Kaspersky Detection and Response çözümleri için Tehdit Yanıtı geçmişini görüntüleyebileceğiniz bir konsoldur. Kuruluşunuzda birden fazla Detection and Response uygulaması varsa (örneğin, EDR Optimum ve MDR), Kaspersky Endpoint Security tüm çözümler için Tehdit Yanıtı geçmişini görüntüler. Bu, ayrı bir bilgisayarda Detection and Response çözümlerinin performansını analiz etmenize ve bu çözümlerin ayarlarını optimize etmenize olanak tanır.

İzleme merkezi aşağıdaki bilgileri sağlar:

- Tehdit Yanıtı görevleri hakkında bilgi (örneğin, *İşlemi sonlandır* görevi)
- Ağ izolasyonu ve Yürütme önleme kurallarındaki değişiklikler

Tehdit yanıtı bir ağ paylaşımına erişimle ilgili bir hatayla karşılaşırsa, bu hata görüntülenen Tehdit Yanıtı geçmişinden çıkarılır.

EDR eylem izleme merkezine gitmek için:

1. Web Console'un ana penceresinde **Varlık yönetimi** → **Varlıklar (Cihazlar)** seçimini yapın.

2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.

   Bu, bilgisayar özelliklerini açar.

3. **Uygulamalar** sekmesini seçin.

4. **Kaspersky Endpoint Security for Windows 14.2** öğesine tıklayın.

   Bu, yerel uygulama ayarlarını açar.

5. **Uygulama ayarları** sekmesini seçin.

6. **Detection and Response** → **Yanıt geçmişi** bölümüne gidin.

EDR eylem izleme merkezi konsolu açılır. Tehdit Yanıtı görev durumlarını, görev süresini, kural değişikliklerini ve başlatıcı ayrıntılarını görüntülemek için bu konsolu kullanabilirsiniz.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows, Kaspersky Unified Monitoring and Analysis Platform çözümünü destekler. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)*, kurumların BT altyapısı için bir güvenlik bilgi ve olay yönetimi (SIEM) çözümüdür. KUMA, güvenlik tehditlerinin zarar vermeden önce tespit edilmesini, analiz edilmesini ve etkilerinin azaltılmasını sağlar.

Kaspersky Endpoint Security, kurumsal BT altyapısındaki bilgisayarlara yüklenir ve süreçleri, açık ağ bağlantılarını ve değiştirilmekte olan dosyaları sürekli olarak izler. Bilgisayardaki olaylarla ilgili bilgiler (telemetri) Kaspersky Unified Monitoring and Analysis Platform (KUMA) sunucusuna gönderilir. KUMA, konsolunda olayları Windows olay günlüğüne benzer şekilde işaretlemeden bir liste olarak görüntüler.

Kaspersky Endpoint Security, KUMA için bir aracının tüm işlevlerini sağlamaz. Uygulama, KUMA'ya yalnızca işaretleme olmadan olay gönderir. Tüm KUMA işlevlerine erişim sağlamak için bir lisans satın almanız ve çözümü KUMA Yönetici kılavuzuna uygun olarak dağıtmanız gerekir.

Kaspersky Endpoint Security'nin KUMA ile Entegrasyonu

KES'in KUMA ile entegrasyonunu ayarlamak için aşağıdaki adımlar uygulanır:

1. KUMA konsolunda bir toplayıcı ekleyin.
2. KUMA konsolunda, toplayıcının KES'ten olayları alması için bir bağlayıcı yapılandırın.
3. KUMA konsolunda iki yönlü kimlik doğrulamayı etkinleştirin (isteğe bağlı).
4. Kaspersky Endpoint Security for Windows ilkesinde, KES'i KUMA'ya bağlama ayarlarını yapılandırın.
5. KUMA konsolunda, KES'ten gelen olayların doğru kiracıya ulaştığından ve doğru korelasyon kuralları tarafından işlendiğinden emin olun.

KES'in KUMA ile entegrasyonuna hazırlık

KUMA'yı kullanmak için aşağıdaki koşulların karşılanması gerekir:

- Kaspersky Security Center sürüm 14.2 veya üstü. Kaspersky Security Center'ın önceki sürümlerinde KUMA entegrasyon işlevselliğini etkinleştirmek mümkün değildir.
- Uygulama etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.
- KUMA entegrasyon bileşeni etkinleştirilmelidir.

KES'in KUMA ile entegrasyonuna hazırlık aşağıdaki adımları içerir:

1. **KUMA entegrasyon bileşeninin kurulumu**

   KUMA entegrasyon bileşenini, uygulamanın yüklenmesi veya yükseltilmesi sırasında ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken seçebilirsiniz.

   Uygulamayı yeni bileşenle yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatmanız gerekir.

2. **KUMA etkinleştirmesi**

   Kaspersky Endpoint Security uygulama lisansına (örneğin, Kaspersky Endpoint Security for Business Standard) ek olarak, Kaspersky Endpoint Security'nin KUMA ile entegrasyonu için ayrı bir lisansa ihtiyacınız vardır (Kaspersky Endpoint Security for Windows KUMA Entegrasyon Eklentisi).

   Uygulamayı EDR Agent modunda yüklüyorsanız Kaspersky Endpoint Security'yi KUMA ile entegre etmek için bir lisansa ve bir Kaspersky Anti Targeted Attack Platform (KATA) lisansına veya bir Kaspersky Managed Detection and Response (MDR) lisansına ihtiyacınız vardır. EDR Agent'ı yalnızca KUMA için dağıtamazsınız.

   İşlevsellik, ayrı KUMA anahtarı eklendikten sonra kullanılabilir hale gelir. Sonuç olarak, Kaspersky Endpoint Security'nin KUMA ile entegrasyonu için bilgisayarda başka bir etkin anahtar olacaktır.

   Bağımsız KUMA işlevselliği için lisanslama, Kaspersky Endpoint Security'nin lisanslaması ile aynıdır.

   KUMA işlevselliğinin lisansa dahil edildiğinden ve uygulamanın yerel arabiriminde çalıştığından emin olun.

KES'i KUMA'ya bağlama

Kaspersky Endpoint Security uygulamasına sahip bilgisayarı KUMA çözümüne bağlamak için:

1. KUMA konsolunda, **tcp**, **udp** veya **http** türünde konektörlere sahip bir toplayıcı ekleyin ve bağlantının temel ağ ayarlarını belirtin. Konektörleri yönetme hakkında ayrıntılı bilgi için lütfen Kaspersky Unified Monitoring and Analysis Platform Yardım bölümüne bakın.
2. Kaspersky Endpoint Security ilkesinde, KUMA toplayıcı adreslerini ekleyin ve bağlantının ağ ayarlarını belirtin.

Yönetim Konsolu (MMC) kullanılarak bir Kaspersky Endpoint Security bilgisayarı KUMA'ya nasıl bağlanır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **KUMA Entegrasyonu** seçin.
5. **KUMA Entegrasyonu** onay kutusunu seçin.
6. **Entegrasyon ayarları** bloğunda, **$IsKUMATelemetry ? "Windows olaylarının bir KUMA sunucusuna aktarımını etkinleştir": "Windows olaylarının bir SIEM sunucusuna aktarımını etkinleştir"** onay kutusunu seçin.

7. KUMA sunucuları ekleyin:

   a. **Ekle**'ye tıklayın.

      Bu, KUMA sunucuları ekleyebileceğiniz formu açar.

   b. KUMA sunucusuna bağlanmak için protokolü seçin: **HTTP / HTTPS**, **TCP**, **UDP**.

      Kaspersky Endpoint Security'de toplayıcıya bağlanmak için kullanılan protokol, KUMA'daki konektör türüyle eşleşmelidir: **http**, **tcp** veya **udp**.

      > UDP protokolü kullanılırken protokolün doğasında bulunan trafik kaybı nedeniyle veriler kaybolabilir.

   c. Sunucu adresini (IPv4, IPv6, FQDN) ve sunucuya bağlanmak için kullanılacak portu girin (varsayılan olarak 443 numaralı port belirtilir).

      Sunucu adresini girerken şunları dikkate alın:

      - **TCP**:
        - **TLS'siz**. Sunucunun IP adresini veya FQDN'sini belirtebilirsiniz.
        - **TLS ile**. Sunucunun yalnızca FQDN'sini belirtmeniz gerekir.
      - **HTTP / HTTPS**:
        - **TLS'siz**. Sunucu adresinde HTTP protokolünü açıkça belirtmeniz gerekir (örneğin, `http://server.com` veya `http://10.10.10.100`).
        - **TLS ile**. Protokolü belirtmeniz gerekmez (örneğin, `https://server.com` veya `server.com`).
      - **UDP**. UDP protokolü TLS şifrelemesini desteklemez. Sunucunun IP adresini veya FQDN'sini belirtebilirsiniz.

      Sunucu adresini KUMA konsolundaki konektör özelliklerinde görüntüleyebilirsiniz. KUMA konektörleri hakkında daha fazla bilgi için Kaspersky Unified Monitoring and Analysis Platform Yardım bölümüne bakın.

   d. **Tamam**'a tıklayın.

   Kaspersky Endpoint Security, listedeki ilk KUMA sunucusuna bağlanır. Bağlantı başarısız olursa Kaspersky Endpoint Security listedeki ikinci KUMA sunucusuna bağlanır ve bu böyle devam eder.

8. Gerekirse, **Veri iletim ayarları** bloğunda **Maksimum olay iletim gecikmesi (sn)** ayarını yapılandırın. Belirtilen süre dolduğunda, Kaspersky Endpoint Security aynı toplayıcıya bağlanmayı dener veya birden fazla toplayıcı varsa listedeki bir sonraki toplayıcıya bağlanır. Varsayılan değer ayarı 30 saniyedir.

9. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console kullanılarak bir Kaspersky Endpoint Security bilgisayarı KUMA'ya nasıl bağlanır

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Yerleşik Ajanlar Yapılandırması** → **KUMA Entegrasyonu** bölümüne gidin.

5. **KUMA Entegrasyonu ETKİN** geçişini açın.

6. KUMA sunucuları ekleyin:

   a. **Ekle**'ye tıklayın.

   Bu, KUMA sunucuları ekleyebileceğiniz formu açar.

   b. KUMA sunucusuna bağlanmak için protokolü seçin: **HTTP/HTTPS**, **TCP**, **UDP**.

   Kaspersky Endpoint Security'de toplayıcıya bağlanmak için kullanılan protokol, KUMA'daki konektör türüyle eşleşmelidir: **http**, **tcp** veya **udp**.

   > UDP protokolü kullanılırken protokolün doğasında bulunan trafik kaybı nedeniyle veriler kaybolabilir.

   c. Sunucu adresini (IPv4, IPv6, FQDN) ve sunucuya bağlanmak için kullanılacak portu girin (varsayılan olarak 443 numaralı port belirtilir).

   Sunucu adresini girerken şunları dikkate alın:

   - **TCP**:
     - **TLS'siz**. Sunucunun IP adresini veya FQDN'sini belirtebilirsiniz.
     - **TLS ile**. Sunucunun yalnızca FQDN'sini belirtmeniz gerekir.
   - **HTTP/HTTPS**:
     - **TLS'siz**. Sunucu adresinde HTTP protokolünü açıkça belirtmeniz gerekir (örneğin, `http://server.com` veya `http://10.10.10.100`).
     - **TLS ile**. Protokolü belirtmeniz gerekmez (örneğin, `https://server.com` veya `server.com`).
   - **UDP**. UDP protokolü TLS şifrelemesini desteklemez. Sunucunun IP adresini veya FQDN'sini belirtebilirsiniz.

   Sunucu adresini KUMA konsolundaki konektör özelliklerinde görüntüleyebilirsiniz. KUMA konektörleri hakkında daha fazla bilgi için Kaspersky Unified Monitoring and Analysis Platform Yardım bölümüne bakın.

   d. **Tamam**'a tıklayın.

   Kaspersky Endpoint Security, listedeki ilk KUMA sunucusuna bağlanır. Bağlantı başarısız olursa Kaspersky Endpoint Security listedeki ikinci KUMA sunucusuna bağlanır ve bu böyle devam eder.

7. Gerekirse, **Sunucu bağlantı ayarları** bloğunda **Olayları gönderirken maksimum gecikme (sn)** ayarını yapılandırın. Belirtilen süre dolduğunda, Kaspersky Endpoint Security aynı toplayıcıya bağlanmayı dener veya birden fazla toplayıcı varsa listedeki bir sonraki toplayıcıya bağlanır. Varsayılan değer ayarı 30 saniyedir.

8. Değişikliklerinizi kaydedin.

KUMA entegrasyonunun KUMA konsolunda doğru yapılandırıldığını doğrulayabilirsiniz (ayrıntılar için Kaspersky Unified Monitoring and Analysis Platform Yardım bölümüne bakın). Kaspersky Security Center konsolunda *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek bileşenin çalışma durumunu kontrol edin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **KUMA Entegrasyonu** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecek.

KES ile KUMA arasında güvenilir bağlantı kurma

Kaspersky Endpoint Security ile tcp veya http türünde bir konektöre sahip KUMA toplayıcısı arasında güvenilir bir bağlantı kurabilirsiniz. udp türündeki bir konektörle güvenilir bağlantı kurulamaz.

Güvenilir bir bağlantı kurmak için konektör ayarlarında bir TLS modu yapılandırmanız gerekir. Aşağıdaki TLS modları kullanılabilir:

- **Devre dışı**: TLS şifrelemesi kullanmayın. Bu seçenek varsayılan olarak seçilidir.
- **Etkin**: TLS şifrelemesi kullanın, ancak sertifika doğrulaması yapmayın.
- **İstemci kimlik doğrulamalı özel PFX**: PFX gizli dizisiyle TLS şifrelemesi kullanın. Bu modda istemcinin kimliği bir sertifikayla doğrulanır.

Kaspersky Endpoint Security, **Özel PFX** TLS modunu desteklemez. KES ile KUMA'yı PFX kullanarak entegre ederken parola ile kullanıcı kimlik doğrulaması gerekir.

Güvenilir bir bağlantı yapılandırmak için bir TLS sertifikasına, yani *mikro hizmet için CA sertifikasına* ihtiyacınız vardır. KUMA konsolundan bir TLS sertifikası alabilirsiniz. TLS sertifikalarını indirme hakkında ayrıntılar için lütfen Kaspersky Unified Monitoring and Analysis Platform Yardım bölümüne bakın. Ardından TLS sertifikasını Kaspersky Endpoint Security'ye eklemeniz gerekir (aşağıdaki talimatlara bakın).

Bağlantıyı daha güvenli hale getirmek için bilgisayarın KUMA'da ek kimlik doğrulamasını etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu kimlik doğrulamayı etkinleştirmek için harici bir sertifika yetkilisinde kripto konteyner oluşturmanız gerekir. *Kripto konteyner*, PKCS#12 biçiminde bir sertifika ve özel anahtar içeren PFX arşividir. Ardından KUMA ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz (TLS modu: **İstemci kimlik doğrulamalı özel PFX**), Kaspersky Endpoint Security'de iki yönlü kimlik doğrulamayı etkinleştirmeniz ve hem KUMA konsoluna hem de Kaspersky Endpoint Security'ye bir PFX arşivi eklemeniz gerekir.

Yönetim Konsolu'nda (MMC) KES ile KUMA arasında güvenilir bağlantı yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **KUMA Entegrasyonu** seçin.
5. **KUMA Entegrasyonu** onay kutusunu seçin.
6. **KUMA sunucularına bağlanma ayarları** bloğunda **TLS şifrelemesi kullan** onay kutusunu seçin.

7. Güvenilir bağlantıyı yapılandırın:

   a. **KUMA sunucularına bağlantı için ayarlar**'a tıklayın.

   b. Sunucu bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. KUMA sunucusundan yanıt beklemek için maksimum süre (varsayılan değer 5 saniyedir). Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir KUMA sunucusuna bağlanmayı dener.
   - **Sunucu TLS sertifikası**. KUMA sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Unified Monitoring and Analysis Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Unified Monitoring and Analysis Platform Yardım bölümündeki talimatlara bakın).

     Güvenilir bir bağlantı kurmak için KUMA konsolunda **Etkin** TLS modunu seçmeniz gerekir.
   - **İki yönlü kimlik doğrulama kullan**. KES ile KUMA arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulama kullanmak için KUMA konsolundaki bağlayıcı ayarlarında **İstemci kimlik doğrulamalı özel PFX** TLS modunu seçmelisiniz (Kaspersky Unified Monitoring and Analysis Platform Yardım bölümündeki bağlayıcı ayarlarına bakın). Ardından bir sunucu sertifikası indirmeli ve kripto konteyneri korumak için bir parola belirlemelisiniz.

     > Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

   c. **Tamam**'a tıklayın.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da KES ile KUMA arasında güvenilir bağlantı yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerleşik Ajanlar Yapılandırması** → **KUMA Entegrasyonu** bölümüne gidin.
5. **KUMA Entegrasyonu ETKİN** geçişini açın.
6. **Sunucu bağlantı ayarları** bölümünde **TLS şifrelemesi kullan** anahtarını açın.

7. Güvenilir bağlantıyı yapılandırın:

   a. **Bağlantı ayarları** seçeneğine tıklayın.

   b. Sunucu bağlantısını yapılandırın:

   - **Zaman aşımı (sn)**. KUMA sunucusundan yanıt beklemek için maksimum süre (varsayılan değer 5 saniyedir). Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir KUMA sunucusuna bağlanmayı dener.
   - **Sunucu TLS sertifikası**. KUMA sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Unified Monitoring and Analysis Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Unified Monitoring and Analysis Platform Yardım bölümündeki talimatlara bakın).

     Güvenilir bir bağlantı kurmak için KUMA konsolunda **Etkin** TLS modunu seçmeniz gerekir.
   - **İki yönlü kimlik doğrulama kullan**. KES ile KUMA arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulama kullanmak için KUMA konsolundaki bağlayıcı ayarlarında **İstemci kimlik doğrulamalı özel PFX** TLS modunu seçmelisiniz (Kaspersky Unified Monitoring and Analysis Platform Yardım bölümündeki bağlayıcı ayarlarına bakın). Ardından bir sunucu sertifikası indirmeli ve kripto konteyneri korumak için bir parola belirlemelisiniz.

     > Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

   c. **Tamam**'a tıklayın.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

KUMA sunucusuna telemetri gönderiminin etkinleştirilmesi

Varsayılan olarak, KUMA sunucusuna olay gönderme özelliği devre dışıdır. KUMA'nın düzgün çalışmasını sağlamak için telemetri gönderimini etkinleştirmeniz gerekir. Standart günlükler arasından bir olay kaynağı seçebilirsiniz: *Uygulama*, *Güvenlik* veya *Sistem*.

Yönetim Konsolu'nda (MMC) KUMA'ya telemetri gönderimini etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Telemetri ayarları** → **KUMA telemetri** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Olay kaynağı olarak kullanmak istediğiniz olay günlüklerini seçin: *Uygulama*, *Güvenlik* veya *Sistem*.

   Standart günlüklerin yanı sıra, üçüncü taraf bir uygulamanın günlüğünü de belirtebilirsiniz.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da KUMA'ya telemetri gönderimini etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Telemetri Ayarlarıı** bölümüne gidin.
5. **KUMA telemetri** sekmesini seçin.
6. Olay kaynağı olarak kullanmak istediğiniz olay günlüklerini seçin: *Uygulama*, *Güvenlik* veya *Sistem*.
   Standart günlüklerin yanı sıra, üçüncü taraf bir uygulamanın günlüğünü de belirtebilirsiniz.
7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

KUMA'ya gönderilecek olayları filtreleme

Varsayılan olarak, KUMA sunucusuna olay gönderme özelliği devre dışıdır. KUMA'nın düzgün çalışmasını sağlamak için telemetri gönderimini etkinleştirmeniz gerekir. Standart günlükler arasından bir olay kaynağı seçebilirsiniz: *Uygulama*, *Güvenlik* veya *Sistem*. KUMA sunucusuna veri iletimini iyileştirmek ve optimize etmek için, telemetriye bireysel olayları manuel olarak ekleyebilir veya hariç tutabilirsiniz. Örneğin, Sysmon olaylarını hariç tutabilirsiniz.

Yönetim Konsolu'nda KUMA'ya gönderilecek olayların listesini oluşturma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Telemetri ayarları** → **KUMA telemetri** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, KUMA'ya gönderilecek olay filtrelerini yapılandırın.
   Standart *Application*, *Security*, *System* günlükleri için olay filtrelemesi yapılandırabilir ya da manuel olarak başka bir günlük ekleyebilirsiniz:
   a. Günlük özelliklerini açın veya **Ekle** düğmesine tıklayın ve günlük adını girin.
   b. Bir olay gönderme modu seçin:
   - **Tüm olayları gönder**. Bu modda, uygulama, istisna kurallarına eklenen olaylar hariç, Windows günlüğündeki tüm olayları gönderir.
   - **Yalnızca seçilen etkinlikleri gönder**. Bu modda, uygulama yalnızca dahil etme kurallarına eklenen olayları gönderir.

c. İlgili olay gönderme modu için istisna kuralı veya dahil etme kuralları listeleri oluşturun.

Kural eklemek için, Windows olay günlüğünde olayın kimliğini belirtmeniz gerekir. Bir kuralda birden fazla olay kimliği listeleyebilirsiniz. Birden fazla olay kimliği belirtmek için virgül karakteri (,) kullanın.

d. Gerekirse, günlük adının yanındaki onay kutusunu işaretleyerek olay günlüğünü etkinleştirin.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da KUMA'ya gönderilecek olayların listesini oluşturma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Telemetri Ayarları** bölümüne gidin.
5. **KUMA telemetri** sekmesini seçin.
6. Açılan pencerede, KUMA'ya gönderilecek olay filtrelerini yapılandırın.

Standart *Application*, *Security*, *System* günlükleri için olay filtrelemesi yapılandırabilir ya da manuel olarak başka bir günlük ekleyebilirsiniz:

a. Günlük özelliklerini açın veya **Ekle** düğmesine tıklayın ve günlük adını girin.

b. Bir olay gönderme modu seçin:

- **Tüm olayları gönder**. Bu modda, uygulama, istisna kurallarına eklenen olaylar hariç, Windows günlüğündeki tüm olayları gönderir.
- **Yalnızca seçilen etkinlikleri gönder**. Bu modda, uygulama yalnızca dahil etme kurallarına eklenen olayları gönderir.

c. İlgili olay gönderme modu için istisna kuralı veya dahil etme kuralları listeleri oluşturun.

Kural eklemek için, Windows olay günlüğünde olayın kimliğini belirtmeniz gerekir. Bir kuralda birden fazla olay kimliği listeleyebilirsiniz. Birden fazla olay kimliği belirtmek için virgül karakteri (,) kullanın.

d. Gerekirse, günlük adının yanındaki anahtarı kullanarak olay günlüğünü etkinleştirin.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

KUMA olay filtrelerini dışa ve içe aktarma

İstisna listesini bir JSON dosyasına aktarabilirsiniz. Daha sonra, dosyayı değiştirerek örneğin çok sayıda olay kimliği ekleyebilirsiniz. Ayrıca, dışa aktarma/içe aktarma işlevini kullanarak olay filtrelerini yedekleyebilir veya listeyi farklı bir sunucuya taşıyabilirsiniz.

Çok fazla kural kullanmak KUMA sunucusundaki yükü artırabilir ve bilgisayar performansını düşürebilir. Sadece gerekli kuralları eklemenizi öneririz.

Yönetim Konsolu'nda (MMC) olay filtrelerini dışa ve içe aktarma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar ve nesne türleri** öğesini seçin.
5. **Telemetri ayarları** → **KUMA telemetri** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Olay filtrelerini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz olay günlüklerini filtrelerle seçin.
   b. → **Dışa aktar** düğmesine tıklayın.
   c. Açılan pencerede, olay filtrelerini dışa aktarmak istediğiniz JSON dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   d. Dosyaya kaydet.
      Kaspersky Endpoint Security, olay filtrelerini JSON dosyasına aktarır.
7. Olay filtrelerini içe aktarmak için:
   a. → **İçe aktar** düğmesine tıklayın.
   b. Açılan pencerede, olay filtrelerini içe aktarmak istediğiniz JSON dosyasını seçin.
   c. Dosyayı aç.
      Bilgisayarda olay filtreleme kuralları zaten mevcutsa, Kaspersky Endpoint Security bunları içe aktarırken değiştirir.
8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da olay filtrelerini dışa ve içe aktarma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler** sekmesini seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Telemetri Ayarları** bölümüne gidin.
5. **KUMA telemetri** sekmesini seçin.
6. Olay filtrelerini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz olay günlüklerini filtrelerle seçin.
   b. → **Dışa aktar** düğmesine tıklayın.

c. Açılan pencerede, olay filtrelerini dışa aktarmak istediğiniz JSON dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

d. Dosyaya kaydet.

Kaspersky Endpoint Security, olay filtrelerini JSON dosyasına aktarır.

7. Olay filtrelerini içe aktarmak için:

a. → **İçe aktar** düğmesine tıklayın.

b. Açılan pencerede, olay filtrelerini içe aktarmak istediğiniz JSON dosyasını seçin.

c. Dosyayı aç.

Bilgisayarda olay filtreleme kuralları zaten mevcutsa, Kaspersky Endpoint Security bunları içe aktarırken değiştirir.

8. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Ayrıca komut satırını kullanarak da olay filtrelerini dışa veya içe aktarabilirsiniz.

KSWS'den KES'e Geçiş Kılavuzu

Kaspersky Endpoint Security, 11.8.0 sürümünden itibaren Kaspersky Security for Windows Server (KSWS) çözümünün temel işlevlerini destekler. *Kaspersky Security for Windows Server*, Microsoft Windows işletim sistemlerini çalıştıran sunucuları ve ağa bağlı depoları, sunucuların ve ağa bağlı depoların dosya alışverişi sırasında maruz kaldığı virüslere ve diğer bilgisayar güvenliği tehditlerine karşı korur. Çözümün nasıl çalıştığı hakkında ayrıntılı bilgi için lütfen Kaspersky Security for Windows Server Yardım içeriğine bakın. Kaspersky Endpoint Security 11.8.0 ile başlayarak Kaspersky Security for Windows Server'dan Kaspersky Endpoint Security for Windows'a geçebilir ve iş istasyonları ile sunucuları korumak için tek bir çözüm kullanabilirsiniz.

Yazılım gereksinimleri

KSWS'den KES'e geçişi başlatmadan önce sunucunuzun Kaspersky Endpoint Security for Windows'un donanım ve yazılım gereksinimlerini karşıladığından emin olun. Desteklenen işletim sistemi sürümlerinin listesi KES ve KSWS için farklıdır. Örneğin KES, Windows Server 2003 çalıştıran sunucuları desteklemez.

KSWS'den KES'e geçiş için minimum yazılım gereksinimleri:

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Kaspersky Security for Windows Server'ın daha önceki bir sürümünü yüklediyseniz, uygulamayı en son sürüme yükseltmenizi öneririz. İlke ve görevler dönüştürme sihirbazı, Kaspersky Security for Windows Server'ın önceki sürümlerini desteklemez.
- Kaspersky Security Center 14.2

  Kaspersky Security Center'ın daha eski bir sürümü kuruluysa, onu 14.2 veya sonraki bir sürüme güncelleyin. Kaspersky Security Center'ın bu sürümünde, İlke ve görevler toplu dönüştürme sihirbazı, ilkeleri bir ilke yerine bir profile taşımanıza olanak tanır. Kaspersky Security Center'ın bu sürümünde, İlke ve görevler toplu dönüştürme sihirbazı, daha geniş bir ilke ayarları yelpazesini taşımanıza da olanak tanır.
- Kaspersky Endpoint Agent 3.10.

  Kaspersky Endpoint Agent'ın daha eski bir sürümünü yüklediyseniz, uygulamayı en son sürüme yükseltmenizi öneririz. Kaspersky Endpoint Security, Kaspersky Endpoint Agent 3.10'dan başlayarak bir [KSWS KEA] yapılandırmasının [KES bütünleşik aracı]'ya taşınmasını destekler.

Geçiş önerileri

KSWS'den KES'e geçerken aşağıdaki önerilere uyun:

- KSWS'den KES'e geçiş zamanını önceden planlayın. Hafta sonu gibi sunucuların en hafif yük altında çalıştığı bir zaman seçin.
- Geçiş sonrasında, uygulama bileşenlerini kademeli olarak açın. Yani, örneğin, yalnızca Dosya Tehdidi Koruması bileşenini etkinleştirerek başlayın, ardından diğer koruma bileşenlerini etkinleştirin, ardından kontrol bileşenlerini etkinleştirin ve bu şekilde devam edin. Her adımda, uygulamanın doğru çalıştığından emin olmalı ve sunucunun performansını izlemelisiniz. KES'in mimarisi KSWS'den farklıdır, bu nedenle işletim sistemi de farklı davranabilir.

- Geçişi kademeli olarak gerçekleştirin. Önce tek bir sunucuyu, ardından birden fazla sunucuyu geçirin, daha sonra kuruluşun tüm sunucularında geçişi gerçekleştirin.
- Farklı sunucu türlerini ayrı ayrı geçirin. Yani, örneğin, önce veritabanı sunucularını, ardından posta sunucularını vb. geçirin.
- Yüksek yüklü sunuculara geçiş bazı özel hususları içerir.

Geçiş adımları

KSWS'den KES'e geçiş yarı otomatik olarak gerçekleştirilir. Bu, uygulamaların farklı mimarileri nedeniyle gereklidir. İlke ayarlarını taşımak için, İlke ve görevler toplu dönüştürme sihirbazını (geçiş sihirbazı) çalıştırmalısınız. İlke ayarlarını taşıdıktan sonra, geçiş sihirbazının otomatik olarak taşıyamayacağı ayarları (örneğin, Parola koruma ayarları) elle yapılandırmanız gerekir. Geçiş sonrasında, geçiş sihirbazının tüm ayarları doğru bir şekilde taşıyıp taşımadığını kontrol etmeniz de önerilir.

KSWS'den KES'e aşağıdaki sırayla geçiş yapın:

1. **KSWS görevlerini ve ilkelerini taşıyın**

   İlkeleri ve görevleri taşıdıktan sonra, ek yapılandırma adımları gerçekleştirmeniz gerekir. Ayrıca, KSWS'den geçiş yaptıktan sonra Kaspersky Endpoint Security'nin gerekli güvenlik seviyesini sağladığından emin olmanızı öneririz.

   > Kaspersky Security for Windows Server için İlke ve görevler toplu dönüştürme sihirbazı yalnızca Yönetim Konsolu'nda (MMC) kullanılabilir. İlke ve görev ayarlarının geçişi Web Console ve Kaspersky Security Center Cloud Console'da gerçekleştirilemez.

2. **Kaspersky Endpoint Security'yi yükleyin**

   Kaspersky Endpoint Security'yi şu şekillerde yükleyebilirsiniz:

   - KSWS'yi kaldırdıktan sonra KES'i yüklemek (önerilir).

     > Kavremover yardımcı programı KSWS yönetimini desteklemez.

   - KES'in KSWS'nin üzerine yüklemek.

3. **KES'i bir KSWS anahtarıyla etkinleştirme**

4. **Geçişten sonra uygulamanın çalışır durumda olduğunu onaylayın**

   KSWS'den KES'e geçiş yaptıktan sonra uygulamanın doğru çalıştığından emin olun. Konsoldaki sunucunun durumunu kontrol edin (*Tamam* olmalıdır). Uygulama için herhangi bir hata rapor edilmediğinden emin olun, ayrıca Yönetim Sunucusuna son bağlantı zamanını, son veritabanı güncelleme zamanını ve sunucu koruma durumunu kontrol edin.

   > İstisna listelerinin, güvenilir uygulamaların, güvenilir web adreslerinin, Uygulama Denetimi kurallarının geçişine özellikle dikkat edin.

KSWS ve KES bileşenlerinin benzerliği

KSWS'den KES'e geçiş yapılırken, bileşen seti yalnızca uygulama yerel olarak yüklenirken taşınır.

Kaspersky Security for Windows Server ve Kaspersky Endpoint Security for Windows bileşenlerinin benzerliği

Kaspersky Security for Windows Server bileşeni	Kaspersky Endpoint Security for Windows bileşeni
Basic functionality	Uygulama çekirdeği
Log Inspection	Günlük Denetimi
Device Control	Aygıt Denetimi
Firewall Management	*(desteklenmiyor)* KSWS Güvenlik Duvarı işlevleri, sistem düzeyindeki Güvenlik Duvarı tarafından gerçekleştirilir. KES'te, Güvenlik Duvarı işlevinden ayrı bir bileşen sorumludur. Geçiş tamamlandıktan sonra, Kaspersky Endpoint Security Güvenlik Duvarını yapılandırabilirsiniz.
File Integrity Monitor	Sistem Bütünlüğü İzleme
Exploit Prevention	Exploit Önleme
System Tray Icon	*(desteklenmiyor)* Uygulama arabirimi ayarları bölümünde kullanıcı etkileşimini yapılandırabilirsiniz.
Integration with Kaspersky Security Center	Ağ Aracısı Bağlayıcısı
Endpoint Agent	*(desteklenmiyor)* Kaspersky Endpoint Security 11.9.0'da Kaspersky Endpoint Agent dağıtım paketi artık Kaspersky Endpoint Security dağıtım kitinin bir parçası değildir. Kaspersky Endpoint Agent dağıtım paketini ayrıca indirmeniz gerekir.
Network Threat Protection	Ağ Tehdidi Koruması
Anti-Cryptor	Davranış Tespiti
Anti-Cryptor for NetApp	*(desteklenmiyor)*
Traffic Security	Web Tehdidi Koruması Posta Tehdidi Koruması İnternet Denetimi
On-Demand Scan	Uygulama çekirdeği
ICAP Network Storage Protection	*(desteklenmiyor)* Kaspersky Endpoint Security, Ağa Bağlı Depolamalar Koruması bileşenlerini desteklemez. Bu bileşenlere ihtiyacınız varsa Kaspersky Security for Windows Server'ı kullanmaya devam edebilirsiniz.
RPC Network Storage Protection	*(desteklenmiyor)* Kaspersky Endpoint Security, Ağa Bağlı Depolamalar Koruması bileşenlerini desteklemez. Bu bileşenlere ihtiyacınız varsa Kaspersky Security for Windows Server'ı kullanmaya devam edebilirsiniz.
Real-Time File Protection	Dosya Tehdidi Koruması
Script Monitoring	*(desteklenmiyor)* Komut Dizisi İzleme, diğer bileşenler tarafından gerçekleştirilir, örneğin, AMSI Koruması.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Uygulama Denetimi
Performance counters	*(desteklenmiyor)*

KSWS ve KES ayarlarının benzerliği

KES, ilkeleri ve görevleri taşırken, KSWS ayarlarına göre yapılandırılır. KSWS'nin sahip olmadığı uygulama bileşenlerinin ayarları varsayılan değerlere ayarlanır.

Application settings

Scalability, interface and scanning settings

Uygulama ayarları Kaspersky Endpoint Security for Windows'ta desteklenmez.

Uygulama Ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Scalability settings	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm iş süreçlerini yönetir.
Show System Tray Icon	*(geçiş gerçekeşmez)* Bir istemci bilgisayarında, varsayılan olarak Kaspersky Endpoint Security'nin ana penceresi ve Windows bildirim alanındaki simge vardır. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile işlemler gerçekleştirebilir. Kaspersky Endpoint Security ayrıca uygulama simgesinin üzerinde bildirimler görüntüler. Uygulama arabirimi ayarları bölümünde kullanıcı etkileşimini yapılandırabilirsiniz.
Restore file attributes after scanning	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, bir dosyayı taradıktan sonra dosya özniteliklerini otomatik olarak geri yükler.
Limit CPU usage for scanning threads	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tarama yaparken işlemci kullanımını sınırlamaz. Görevi, bilgisayar minimum yük altında çalışırken çalışacak şekilde yapılandırabilirsiniz.
Folder for temporary files created during scanning	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, geçici dosyaları `C:\Windows\Temp` klasörüne yerleştirir.
HSM system settings	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, HSM sistemlerini desteklemez.

Security and reliability

KSWS güvenlik ayarları, **Genel Ayarlar** bölümünün, **Uygulama ayarları** ve **Arabirim** alt bölümlerine taşındı.

Uygulama güvenlik ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Protect application processes from external threats	**Kendini Korumayı Etkinleştir** (**Uygulama ayarları** alt bölümü)
Apply password protection	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, yerleşik bir Parola koruması özelliğine sahiptir (**Arabirim** alt bölümüne bakın).
Perform task recovery	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security *Kötü Amaçlı Yazılım Taraması* görevlerini yalnızca otomatik olarak geri yükler. Kaspersky Endpoint Security, diğer görevleri bir zamanlamaya göre çalıştırır.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Do not start scheduled scan tasks	**Pil gücüyle çalışırken zamanlanmış görevleri ertele** (**Uygulama ayarları** alt bölümü)
Stop current scan tasks	*(geçiş gerçekleşmez)* Bilgisayar bir UPS tarafından çalıştırıldığında, Kaspersky Endpoint Security halihazırda çalışmakta olan tarama görevlerini durdurmaz.

Connection settings

Yönetim Sunucusu etkileşim ayarları, **Genel Ayarlar** bölümünün **Ağ ayarları** ve **Uygulama ayarları** alt bölümlerine taşınır.

Yönetim Sunucusu etkileşim ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Proxy server settings	**Proxy sunucusu ayarları** (**Ağ ayarları** alt bölümü)
Do not use proxy server for local addresses	**Yerel adresler için proxy sunucusunu atla** (**Ağ ayarları** alt bölümü)
Proxy server authentication settings	**Proxy sunucusu kimlik doğrulamasını kullan** (**Ağ ayarları** alt bölümü) Proxy sunucusu kimlik doğrulama parolası taşınmaz. Bir ilke taşındıktan sonra parolanın manuel olarak girilmesi gerekir.
Use Kaspersky Security Center as a proxy server when activating the application	**Etkinleştirme için proxy sunucusu olarak Kaspersky Security Center'ı kullan** (**Uygulama ayarları** alt bölümü)

Run local system tasks

Kaspersky Endpoint Security, Kaspersky Security for Windows Server'ın yerel sistem görevlerini çalıştırma ayarlarını yok sayar. **Yerel Görevler**, **Görev yönetimi** bölümünden yerel KES görevlerinin kullanımını yapılandırabilirsiniz. bu görevlerin özelliklerinde *Kötü Amaçlı Yazılım Taraması* ve *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevlerinin çalıştırılması için bir zamanlama da yapılandırabilirsiniz.

Supplementary

Trusted zone

KSWS güvenilir bölge ayarları, **Genel Ayarlar** bölümünün **İstisnalar** alt bölümüne taşındı.

Güvenilir bölge ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Object to scan (Exclusions)	**Tarama istisnaları** (Tarama istisnaları) Nesneleri seçmek için KSWS ve KES tarafından kullanılan yöntemler farklıdır. KES, geçiş sırasında, tek tek dosyalar veya dosya/klasör yolları olarak tanımlanan istisnaları destekler. KSWS'nin önceden tanımlanmış bir alan veya bir komut dosyası URL'si olarak yapılandırılmış istisnaları varsa, bu tür istisnalar taşınmaz. Geçiş işleminden sonra bu tür istisnaları manuel olarak eklemelisiniz. Önceden tanımlanmış alanlar olarak istisnalar, *Kötü Amaçlı Yazılım Taraması* görev ayarlarında yapılandırılmalıdır. Web Tehdidi Koruması için güvenilir web adreslerine komut dosyası web adresleri olarak istisnalar eklenmelidir.
Apply also to subfolders (Exclusions)	**Alt klasörleri dahil et** (Tarama istisnaları)

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Objects to detect (Exclusions)	**Tespit edilen nesne türü** (Tarama istisnaları)
Exclusion usage scope (Exclusions)	**Koruma bileşenleri** (Tarama istisnaları) KSWS'de en az bir bileşen seçildiği takdirde KES, istisnaları tüm uygulama bileşenlerine uygular.
Comment (Exclusions)	**Yorum** (Tarama istisnaları)
Trusted process (Trusted process)	**Güvenilir uygulamalar** Güvenilir süreç/uygulama seçim yöntemleri KSWS ve KES'te farklıdır. Geçiş sırasında KES, yürütülebilir dosyanın yolu veya maskesi olarak yapılandırılan güvenilir uygulamaları destekler. KSWS'nin dosya karması olarak yapılandırılmış güvenilen süreçleri varsa, bu tür güvenilir süreçler taşınmaz. Geçiş işleminden sonra bu tür güvenilir işlemleri manuel olarak eklemeniz gerekir.
Do not check file backup operations (Trusted process)	**Uygulama etkinliğini izleme** (Güvenilir uygulamalar)

Removable drives scan

Çıkarılabilir Sürücü Tarama ayarları, **Yerel Görevler** bölümünün **Çıkarılabilir Sürücü Taraması** alt bölümüne taşındı.

Çıkarılabilir Sürücü Taraması ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Scan removable drives on connection via USB	**Çıkarılabilir sürücü bağlantısında yapılacak eylem**
Scan removable drives if its stored data volume does not exceed (MB)	**En büyük çıkarılabilir sürücü boyutu**
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Çıkarılabilir sürücü bağlantısında yapılacak eylem**: • **Maksimum koruma**. • **Önerilen**. KSWS güvenlik düzeyleri, şu KES tarama modlarına karşılık gelir: • Maximum protection – Maksimum koruma • Recommended – Önerilen • Maximum performance – Önerilen

User permissions for application management

Kaspersky Endpoint Security, uygulama yönetimi ve uygulama hizmeti yönetimi için kullanıcı erişim izinlerinin atanmasını desteklemez. Uygulamayı Kaspersky Security Center'da yönetmek için kullanıcılar ve kullanıcı grupları için erişim ayarlarını yapılandırabilirsiniz.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security, uygulama yönetimi ve uygulama hizmeti yönetimi için kullanıcı erişim izinlerinin atanmasını desteklemez. Uygulamayı Kaspersky Security Center'da yönetmek için kullanıcılar ve kullanıcı grupları için erişim ayarlarını yapılandırabilirsiniz.

Storages

KSWS depolama ayarları **Genel Ayarlar** bölümünün **Raporlar ve Depolama Alanı** alt bölümüne ve **Temel Tehdit Koruması** bölümünün **Ağ Tehdidi Koruması** alt bölümüne taşındı.

Depolama ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Backup folder	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, dosyaların yedek kopyalarını `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasörüne kaydeder.
Maximum Backup size (MB)	**Yedekleme boyutunu şununla sınırla**: **N MB** (**Genel Ayarlar** → **Raporlar ve Depolama Alanı** bölümü)
Threshold value for space available (MB)	*(geçiş gerçekeşmez)* Eşiğin %50'si dolduğunda, Kaspersky Endpoint Security *Karantina depolama alanı neredeyse doldu* olayını günlüğe kaydeder.
Target folder for restoring objects	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, dosyaları orijinal klasörlerine geri yükler.
Quarantine folder	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, dosyaların yedek kopyalarını `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasörüne kaydeder.
Maximum Quarantine size (MB)	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, muhtemelen virüslü nesneleri depolamak için Yedeklemeyi kullanır. Kaspersky Endpoint Security, geçiş sırasında Karantina ayarlarını yok sayar.
Threshold value for space available (MB)	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, muhtemelen virüslü nesneleri depolamak için Yedeklemeyi kullanır. Kaspersky Endpoint Security, geçiş sırasında Karantina ayarlarını yok sayar.
Target folder for restoring objects	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, dosyaları orijinal klasörlerine geri yükler.
Unblock automatically in N	**Saldırıda bulunan cihazları şu kadar süre için engelle N dk** (**Temel Tehdit Koruması** → **Ağ Tehdidi Koruması** bölümü)

Real-time server protection

Real-Time File Protection

KSWS Gerçek Zamanlı Dosya Koruma ayarları, **Temel Tehdit Koruması** bölümünün **Dosya Tehdidi Koruması** alt bölümüne taşındı.

Gerçek Zamanlı Dosya Koruma ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Tarama modu**: • **Akıllı mod**. • **Yürütme durumunda**. • **Erişim durumunda**. • **Erişim ve değiştirme durumunda**
Deeper analysis of launching processes	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, yalnızca bir analiz modunu, yani Optimal modunu destekler.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Sezgisel analiz**: • **Hızlı tarama**. • **Normal tarama**. • **Ayrıntılı tarama**
Apply Trusted Zone	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, güvenilir bölgeyi tüm bileşenlere uygular. İstisnaları güvenilir bölge ayarlarında yapılandırabilirsiniz.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Use KSN for protection	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm uygulama bileşenleri için KSN kullanır.
Block access to network shared resources for the hosts that show malicious activity	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, kötü amaçlı etkinlik gösteren ana bilgisayarlar için ağ paylaşımlı kaynaklara erişimi varsayılan olarak engeller.
Launch critical areas scan when active infection is detected	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, etkin bir virüs tespit edildiğinde kritik alanları tarama görevini başlatmaz.
Use Kaspersky Sandbox for protection	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security nesneleri tarama için varsayılan olarak Kaspersky Sandbox'a gönderir.
Protection scope	**Koruma kapsamı**
Schedule settings	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Dosya Tehdidi Korumasını duraklatmak için kendi zamanlamasını kullanır.

KSN Usage

Kaspersky Security Network için KSWS ayarları, **Gelişmiş Tehdit Koruması** bölümü, Kaspersky Security Network alt bölümüne taşındı.

Kaspersky Security Network ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Kaspersky Security Network Bildirimi** Kaspersky Endpoint Security, uygulama yüklendiğinde, yeni bir ilke oluşturulduğunda veya Kaspersky Security Network kullanımı etkinleştirildiğinde Kaspersky Security Network Bildirimi için onay ister.
Send data about scanned files	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, KSN etkinse taranan dosyalar hakkındaki verileri otomatik olarak gönderir.
Send data about requested URLs	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, KSN etkinse, istenen URL'lerle ilgili verileri otomatik olarak gönderir.
Send Kaspersky Security Network statistics	**Genişletilmiş KSN modunu etkinleştir**
Accept the terms of the Kaspersky Managed Protection Statement	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, KMP hizmetini içermez.
Action to perform on KSN untrusted objects	*(geçiş gerçekeşmez)* Koruma bileşeni ayarlarında ve Tarama görevi ayarlarında, Tehdit algılandığında yapılacak eylemi yapılandırabilirsiniz.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(geçiş gerçekeşmez)* Koruma bileşeni ayarlarında ve Tarama görevi ayarlarında, büyük dosya tarama kısıtlamalarını yapılandırabilirsiniz.
Use Kaspersky Security Center as KSN Proxy	**Yönetim Sunucusunu KSN proxy sunucusu olarak kullanma**
Schedule settings	*(geçiş gerçekeşmez)* Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

Traffic Security

KSWS Trafik Güvenliği ayarları, **Temel Tehdit Koruması** bölümü, Web Tehdidi Koruması ve Posta Tehdidi Koruması alt bölümü; **Güvenlik Denetimleri** bölümü, İnternet Denetimi alt bölümü; **Genel Ayarlar** bölümü, Ağ ayarları alt bölümüne taşınmıştır.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Apply URL-based rules	**İnternet Denetimi** (**İnternet Denetimi** alt bölüm) URL tabanlı kurallar Kaspersky Endpoint Security'deki ayrı kurallara taşındı.
Apply certificate-based rules	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, sertifika tabanlı kuralları desteklemez.
Apply rules for web traffic category control	**İnternet Denetimi** (**İnternet Denetimi** alt bölüm) İnternet trafiği kategorisi denetimi için engelleme kuralları, Kaspersky Endpoint Security'deki tek bir engelleme kuralına taşındı. Kaspersky Endpoint Security, kategori denetimi için izin verme kurallarını yok sayar. KSWS ve KES kategorilerinin benzerlikleri aşağıda listelenmiştir.
Allow access if the web page can not be categorized	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, web sayfası kategorize edilemiyorsa erişime izin verir.
Allow access to legitimate web resources that can be used to damage a protected device	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, korunan cihaza zarar vermek için kullanılabilecek meşru web kaynaklarına erişime izin verir.
Allow access to legitimate advertisement	*(geçiş gerçekeşmez)* İnternet Denetimi ayarlarında *Reklam pencereleri* web kaynağı kategorisini kullanarak meşru reklamlara erişimi yönetebilirsiniz.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security yalnızca Driver Interceptor modunu destekler.
ICAP-service connection settings	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, ICAP Ağ Depolama Korumasını desteklemez.
Check safe connections through the HTTPS protocol	**Şifrelenmiş bağlantıları tara** / **Şifrelenmiş bağlantıları her zaman tara** modu (**Ağ ayarları** alt bölümü)
Use TLS protocol version	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, aşağıdaki protokoller üzerinden iletilen şifrelenmiş ağ trafiğini tarar: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Ek olarak SSL 2.0 bağlantılarını şifreli bağlantılar tarama ayarlarında engelleyebilirsiniz.
Do not trust web-servers with invalid certificate	**Adres** (**Ağ ayarları** alt bölümü)
Intercept ports (Interception area)	**İzlenen portlar** (**Ağ ayarları** alt bölümü) Geçiş sırasında KES, **Kaspersky tarafından önerilen listeden uygulamalar için tüm portları izle** ve **Belirtilen uygulamalar için tüm portları izle** onay kutularını temizler.
Exclude ports (Interception area)	*(geçiş gerçekeşmez)*
Exclude IP addresses (Interception area)	**Güvenilir adresleri yapılandır** (**Ağ ayarları** alt bölümü)
Exclude processes (Interception area)	**Güvenilir uygulamaları yapılandır** (**Ağ ayarları** alt bölümü) Taşıma sırasında KES, güvenilir uygulama için şu ayarları yapılandırır: • **Ağ trafiğini tarama** onay kutusu seçilidir. KES, herhangi bir uzak IP adresi ve portu için ağ trafiğini taramaz. • Güvenilir uygulama ayarlarındaki diğer onay kutuları temizlenir.
Security port	*(geçiş gerçekeşmez)*
Use malicious URL database to scan web links	**Web adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et** (**Web Tehdidi Koruması** alt bölümü)
Use anti-phishing database to scan web pages	**Web adresini kimlik avı internet adresleri veritabanıyla karşılaştırarak kontrol et** (**Web Tehdidi Koruması** alt bölümü)
Use KSN for protection	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm uygulama bileşenleri için KSN kullanır.
Use Trusted Zone	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, güvenilir bölgeyi tüm bileşenlere uygular. İstisnaları güvenilir bölge ayarlarında yapılandırabilirsiniz.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Use heuristic analyzer	**Sezgisel analiz kullan** (**Web Tehdidi Koruması** ve **Posta Tehdidi Koruması** alt bölümleri)
Security level	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Web Tehdidi Koruması ve Posta Tehdidi Koruması bileşenleri için kendi güvenlik düzeylerine sahiptir. Kaspersky Endpoint Security, varsayılan olarak önerilen güvenlik düzeyini ayarlar.
Enable mail threat protection	**Posta Tehdidi Koruması** (**Posta Tehdidi Koruması** alt bölümü) **Microsoft Outlook uzantısını bağla** **Sadece gelen mesajlar** (Koruma kapsamı) **Alırken tara** (E-posta koruması)
Schedule settings	*(geçiş gerçekeşmez)* Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

Exploit Prevention

KSWS Exploit Önleme ayarları, **Gelişmiş Tehdit Koruması** bölümü, **Exploit Önleme** alt bölümüne taşındı.

Exploit Önleme ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Exploit algılandığında**: • **Engelle**. • **Bilgilendir**.
Notify about abused processes via Terminal Service	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security terminal hizmetlerini desteklemez.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, hassas işlemlerde exploit yaşanmasını sürekli olarak önler.
Protected processes	**Sistem işlemleri bellek korumasını etkinleştir** Kaspersky Endpoint Security korunan işlemlerin seçilmesini desteklemez. Yalnızca sistem işlemleri bellek korumasını etkinleştirebilirsiniz.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, mevcut tüm exploit önleme tekniklerini uygular.

Network Threat Protection

KSWS Ağ Tehdidi Koruması ayarları, **Temel Tehdit Koruması** bölümü, **Ağ Tehdidi Koruması** alt bölümüne taşındı.

Ağ Tehdidi Koruması ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Ağ Tehdidi Koruması** **Pass-through** modu seçildiğinde, Ağ Tehdidi Koruması devre dışı bırakılır. **Only inform about network attacks** modu veya **Block connections when attack is detected** modu seçildiğinde, Ağ Tehdidi Koruması etkinleştirilir. Kaspersky Endpoint Security her zaman **Block connections when attack is detected** modunda çalışır.
Do not stop traffic analysis when the task is not running	*(geçiş gerçekeşmez)* Bu bileşen etkinleştirildiğinde, Kaspersky Endpoint Security trafiği sürekli olarak analiz eder.
Do not control excluded IP addresses	**İstisnalar**
Schedule settings	*(geçiş gerçekeşmez)* Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

Script Monitoring

Kaspersky Endpoint Security Komut Dizisi İzleme bileşenini desteklemez. Komut Dizisi İzleme, diğer bileşenler tarafından gerçekleştirilir, örneğin, AMSI Koruması.

Website categories

Kaspersky Endpoint Security, Kaspersky Security for Windows Server'ın tüm kategorilerini desteklemez. Kaspersky Endpoint Security'de var olmayan kategoriler taşınmaz. Dolayısıyla, desteklenmeyen kategorilere sahip web kaynağı sınıflandırma kuralları taşınmaz.

Web sitesi kategorileri

Kaspersky Security for Windows Server kategorileri	Kaspersky Endpoint Security for Windows kategorileri
Wargaming	Video oyunları
Abortion	*(geçiş gerçekeşmez)*
Lotteries (extended)	Kumar, piyango, çekiliş
Alcohol	Alkol, tütün, uyuşturucu
Anonymous proxy servers	IP gizleyiciler
Anorexia	*(geçiş gerçekeşmez)*
Rentals for real estate	*(geçiş gerçekeşmez)*
Audio, video and software	Yazılım, ses, video
Banks	Bankalar
Blogs	Bloglar
Military	Silahlar, patlayıcı maddeler, askeri
For children	*(geçiş gerçekeşmez)*
Discrimination	Şiddet, hoşgörüsüzlük
Home and family	*(geçiş gerçekeşmez)*
Hosting and domain services	İnternet iletişimleri
Pets and animals	*(geçiş gerçekeşmez)*
Law and politics	Bölgesel yasalarca yasaklandı
Restricted by Roskomnadzor (RF)	Rusya Federasyonu yasaları uyarınca yasaktır
Restricted by Federal Law 436 (RF)	Rusya Federasyonu yasaları uyarınca yasaktır
Restricted by RF legislation	Rusya Federasyonu yasaları uyarınca yasaktır
Restricted by global legislation	Bölgesel yasalarca yasaklandı
Adult dating	Yetişkinlere yönelik içerik
Internet services	*(geçiş gerçekeşmez)*
Sex shops	Yetişkinlere yönelik içerik
Information technologies	*(geçiş gerçekeşmez)*
Casinos, card games	Kumar, piyango, çekiliş
Books and writing	*(geçiş gerçekeşmez)*
Computer games	Video oyunları
Health and beauty	*(geçiş gerçekeşmez)*
Culture and society	*(geçiş gerçekeşmez)*
LGBT	Yetişkinlere yönelik içerik
Lotteries	Kumar, piyango, çekiliş
Medicine	*(geçiş gerçekeşmez)*

Kaspersky Security for Windows Server kategorileri	Kaspersky Endpoint Security for Windows kategorileri
Fashion	*(geçiş gerçekeşmez)*
Music	*(geçiş gerçekeşmez)*
Drugs	Alkol, tütün, uyuşturucu
Violence	Şiddet, hoşgörüsüzlük
Discontent	*(geçiş gerçekeşmez)*
Illegal drugs	Alkol, tütün, uyuşturucu
Hate and discrimination	Şiddet, hoşgörüsüzlük
Obscene vocabulary	Küfür, müstehcenlik
Lingerie	Yetişkinlere yönelik içerik
News	Haber medyası
Nudism	Yetişkinlere yönelik içerik
Education	*(geçiş gerçekeşmez)*
Online shopping	Çevrimiçi mağazalar
All communication media	İnternet iletişimleri
Payment by credit cards	Ödeme sistemleri
Online shopping (own payment system)	Çevrimiçi mağazalar
Online encyclopedias	*(geçiş gerçekeşmez)*
Online banking	Bankalar
Weapons	Silahlar, patlayıcı maddeler, askeri
Fishing and hunting	*(geçiş gerçekeşmez)*
Payment systems	Ödeme sistemleri
Job search	İş arama
Search engines	*(geçiş gerçekeşmez)*
Police decision (JP)	Japon Polisi tarafından yasaklandı
Trusted by KPSN	*(geçiş gerçekeşmez)*
Untrusted by KPSN	*(geçiş gerçekeşmez)*
Porn	Yetişkinlere yönelik içerik
Media hosting and streaming	Haber medyası
Web Mail	Web tabanlı e-posta
Traveling	*(geçiş gerçekeşmez)*
TV and radio	Haber medyası
Teasers and ads services	Reklam pencereleri
Religion	Dinler, dini dernekler
Restaurants, cafe and food	*(geçiş gerçekeşmez)*
Dating sites	Arkadaşlık siteleri
Sex education	Yetişkinlere yönelik içerik
Social networks	Sosyal ağlar
Sport	*(geçiş gerçekeşmez)*
Betting	Kumar, piyango, çekiliş
Suicide	Şiddet, hoşgörüsüzlük
Tobacco	Alkol, tütün, uyuşturucu

Kaspersky Security for Windows Server kategorileri	Kaspersky Endpoint Security for Windows kategorileri
Torrents	Torrentler
Mentioned in Federal list of extremists (RF)	Rusya Federasyonu yasaları uyarınca yasaktır
File sharing	Dosya paylaşımı
Pharmacy	*(geçiş gerçekeşmez)*
Hobby and entertainment	*(geçiş gerçekeşmez)*
Chats and forums	Sohbetler, forumlar, anlık ileti
Schools and universities pages	*(geçiş gerçekeşmez)*
Astrology and esoterica	*(geçiş gerçekeşmez)*
Extremism and racism	Şiddet, hoşgörüsüzlük
E-commerce	Çevrimiçi mağazalar
Erotic	Yetişkinlere yönelik içerik
Humor	*(geçiş gerçekeşmez)*

Local activity control

Applications Launch Control

KSWS Uygulama Denetimi ayarları, **Güvenlik Denetimleri** bölümünün **Uygulama Denetimi** alt bölümüne taşındı.

Uygulama Başlatma Denetimi ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Operation mode: • **Statistics only** • **Active**	**Eylem** (Uygulama Denetimi): • **Kuralı test et**. • **Kuralları uygula**
Repeat action taken for the first file launch on all the subsequent launches for this file	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, her çalışma girişiminde uygulamayı tarar.
Deny the command interpreters launch with no command to execute	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Uygulama Denetimi tarafından yasaklanmadıysa komut yorumlayıcılarının çalıştırılmasına izin verir.
Rules	**Uygulama Denetimi kuralları** *(sınırlamalarla desteklenir)* Kaspersky Endpoint Security 11.11.0, Uygulama Başlatma Denetimi kurallarının taşınması için destek sunar. Uygulama Başlatma Denetimi kuralı geçiş işlevinin bazı sınırlamaları vardır. Varsayılan olarak, KSWS Uygulamaları Başlatma Denetimi iki kural içerir: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** En az bir kaynak KSWS kuralı **Allow** türüne sahipse yazın, geçiş sırasında KES yeni bir izin kuralı oluşturur, **Güvenilir kök sertifikaları olan uygulamalar**. Yani KES Uygulama Denetimi, güvenilir komut dosyalarının, MSI paketlerinin ve yürütülebilir dosyaların çalıştırılmasına izin vermek için tek bir kural kullanır. Her iki kaynak KSWS kuralın da **Deny** türüne sahip olduğunda, KES, güvenilir kök sertifikaları olan uygulamaları yönetmek için kurallar eklemez.
Apply rules to executable files	*(geçiş gerçekeşmez)* Kural uygulama kapsamı, KES Uygulama Denetimi ayarlarında yapılandırılamaz. KES Uygulama Denetimi, tüm dosya türlerine kurallar uygular: yürütülebilir dosyalar, komut dosyaları ve MSI paketleri. Tüm dosya türleri KSWS'de kural uygulama kapsamına dahil edilmişse, KES, geçiş sırasında KSWS kurallarını taşır. Bazı dosya türleri KSWS'de kural uygulama kapsamından çıkarılırsa, geçiş sırasında KES ayrıca KSWS kurallarını da taşır, ancak **Kuralı test et** Uygulama Denetimi eylemi olarak seçilir.
Monitor loading of DLL modules	**DLL modüllerinin yüklenmesini izle (sistem yükünü önemli ölçüde artırır)**

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Apply rules to scripts and MSI packages	*(geçiş gerçekleşmez)* Kural uygulama kapsamı, KES Uygulama Denetimi ayarlarında yapılandırılamaz. KES Uygulama Denetimi, tüm dosya türlerine kurallar uygular: yürütülebilir dosyalar, komut dosyaları ve MSI paketleri. Tüm dosya türleri KSWS'de kural uygulama kapsamına dahil edilmişse, KES, geçiş sırasında KSWS kurallarını taşır. Bazı dosya türleri KSWS'de kural uygulama kapsamından çıkarılırsa, geçiş sırasında KES KSWS kurallarını taşır, ancak **Kuralı test et** Uygulama Denetimi eylemi olarak seçilir.
Deny applications untrusted by KSN	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, uygulamaların tanınırlığını dikkate almaz ve uygulamaların kurallara uygun olarak çalıştırılmasına izin verir veya vermez.
Allow applications trusted by KSN	Geçiş sırasında KES, yeni bir izin verme kuralı ekler. **Diğer Yazılımlar\KSN'deki tanınırlığına göre güvenilir uygulamalar**, KL kategorisi, kural tetikleme koşulu olarak belirtilir.
Users and / or user groups allowed to run applications trusted by KSN	**Diğer Yazılımlar\KSN'deki tanınırlığına göre güvenilir uygulamalar** KL kategorisini içeren bir Uygulama Denetimi izin verme kuralındaki **Kullanıcılar ve hakları**
Automatically allow software distribution via applications and packages listed	KSWS ve KES'te Yazılım Dağıtım Kontrolü farklı şekilde çalışır. Geçiş sırasında KES, otomatik yazılım dağıtımına izin verilen uygulamalar için yeni izin kuralları ekler. Dosya karması, kural tetikleme koşulu olarak belirlenir.
Always allow software distribution via Windows Installer	KSWS ve KES'te Yazılım Dağıtım Kontrolü farklı şekilde çalışır. Geçiş sırasında KES, otomatik yazılım dağıtımına izin verilen uygulamalar için yeni izin kuralları ekler (**Software distribution applications and packages allowed**). Dosya karması, kural tetikleme koşulu olarak belirlenir. Hesap özelliklerinde **Güvenilir Güncelleyiciler** onay kutusu seçilir.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(geçiş gerçekleşmez)*
Software distribution applications and packages allowed	KSWS ve KES'te Yazılım Dağıtım Kontrolü farklı şekilde çalışır. Geçiş sırasında KES, otomatik yazılım dağıtımına izin verilen uygulamalar için yeni izin kuralları ekler. Dosya karması, kural tetikleme koşulu olarak belirlenir. Hesap özelliklerinde **Güvenilir Güncelleyiciler** onay kutusu seçilir.
Schedule settings	*(geçiş gerçekleşmez)* KSWS ayarlarında bileşen için bir zamanlama yapılandırılırsa, Uygulama Denetimi bileşeni geçiş sırasında etkinleştirilir. KSWS ayarlarında bileşen için bir zamanlama yapılandırılmamışsa, geçiş sırasında Uygulama Denetimi devre dışı bırakılır. Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

Device Control

KSWS Cihaz Kontrolü ayarları, **Güvenlik Denetimleri** bölümünün **Aygıt Denetimi** alt bölümüne taşındı.

Aygıt Denetimi ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Operation mode: • **Active** • **Statistics only**	*(geçiş gerçekleşmez)* Uygulama Denetimi, *Active* modda çalışır. Aygıt bağlantı istatistikleri sürekli olarak Denetim tarafından sağlanır.
Allow using all external devices when the Device Control task is not running	*(geçiş gerçekleşmez)* Aygıt Denetimi, Kaspersky Endpoint Security çalışırken her zaman açıktır.
Device Control rules	**Güvenilir aygıtlar** Kaspersky Endpoint Security, geçiş sırasında KSWS kurallarını yok sayar.
Schedule settings	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security belirli aygıtlara erişim elde etmek için kendi zamanlamasını kullanır.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security, Ağa Bağlı Depolamalar Koruması bileşenlerini desteklemez. Bu bileşenlere ihtiyacınız varsa Kaspersky Security for Windows Server'ı kullanmaya devam edebilirsiniz.

ICAP Network Storage Protection

Kaspersky Endpoint Security, Ağa Bağlı Depolamalar Koruması bileşenlerini desteklemez. Bu bileşenlere ihtiyacınız varsa Kaspersky Security for Windows Server'ı kullanmaya devam edebilirsiniz.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security, NetApp için Şifreleyici Önleyici'yi desteklemez. Şifreleyici Önleyici işlevselliği, Davranış Tespiti gibi diğer uygulama bileşenleri tarafından sağlanır.

Network activity control

Firewall Management

Kaspersky Endpoint Security, KSWS Güvenlik Duvarı Yönetimini desteklemez. KSWS Güvenlik Duvarı işlevleri, sistem düzeyindeki Güvenlik Duvarı tarafından gerçekleştirilir. Geçiş tamamlandıktan sonra, Kaspersky Endpoint Security Güvenlik Duvarını yapılandırabilirsiniz.

Anti-Cryptor

Ağ Şifreleyici Önleyici ayarları, **Gelişmiş Tehdit Koruması** bölümünün **Davranış Tespiti** alt bölümüne taşındı.

Şifreleyici Önleyici ayarları

KSWS ayarları	KES ayarları
Operation mode: • **Statistics only** • **Active**	**Paylaşılan klasörlerin dış şifrelemesi algılandığında**: • **Bilgilendir**. • **Engelle**.
Heuristic analyzer	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Davranış Tespiti için Sezgisel Analiz kullanmaz.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, korunan bilgisayarın tüm paylaşılan ağ klasörlerinin şifrelenmesini engeller.
Exclusions	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Davranış Tespiti bileşeni için kendi istisnalarına sahiptir. Geçiş işleminden sonra istisnaları manuel olarak ekleyebilirsiniz.
Schedule settings	*(geçiş gerçekeşmez)* Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

System Inspection

File Integrity Monitor

Dosya Bütünlük İzleyicisi ayarları KSWS'den **Güvenlik Denetimleri** bölümünün **Sistem Bütünlüğü İzleme** alt bölümüne taşınır.

Dosya Bütünlük İzleyicisi ayarları

KSWS ayarları	KES ayarları
Log information about file operations that appear during the monitor interruption period	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, izleme kesintisi süresi boyunca gerçekleştirilen dosya işlemleri için olayları günlüğe kaydetmez.
Block attempts to compromise the USN log	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, USN günlüğünün güvenliğini aşma girişimlerini engellemez.
Monitoring scope	**İzleme kapsamı** → **Dosya** *(sınırlamalarla desteklenir)* Devre dışı bırakılan izleme kapsamı kayıtları KES'e taşınmaz. Kaspersky Endpoint Security, izleme kapsamına yalnızca etkinleştirilmiş kayıtları ekler.
Trusted users	**Güvenilir kullanıcılar ve/veya kullanıcı grupları**
File operation markers	**Dosya işlemi işaretleyicileri**
Calculate checksum for the file if possible	**Karma**
Exclusions	**İstisnalar** → **Dosya**

Log Inspection

KSWS Günlük Denetimi ayarları, **Güvenlik Denetimleri** bölümünün **Güvenlik Denetimleri** alt bölümüne taşındı.

Günlük Denetimi ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Apply custom rules for log inspection	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, etkinleştirilmiş tüm özel kuralları uygular.
Custom rules	**Özel kurallar** **A service was installed in the system (for Server 2003 OS)** önceden tanımlanmış kuralı KES'e taşınmaz.
Apply predefined rules for log inspection	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, etkinleştirilmiş tüm önceden tanımlanmış kuralları uygular.
Predefined rules	**Önceden tanımlanmış kurallar**
Password brute-force detection	**Deneme yanılma saldırısı tespiti**
Network logon detection	**Ağ oturum açma tespiti**
Exclusions (IP addresses)	**İstisnalar** (IP adresi)
Exclusions (users)	**İstisnalar** (Kullanıcılar)
Schedule settings	*(geçiş gerçekeşmez)* Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

Logs and notifications

Task logs

KSWS Günlükleri ayarları, **Genel Ayarlar** bölümünün, Arabirim ve Raporlar ve Depolama alt bölümlerine taşındı.

Günlük ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Event logging	**Bildirimler** (**Arabirim** alt bölümü)
Logs folder	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, raporları `C:\ProgramData\Kaspersky Lab\KES.14.2\Report` klasörüne kaydeder.
Remove task logs older than N day(s)	*(geçiş gerçekleşmez)* KES raporları için saklama süresini **Genel Ayarlar**, **Raporlar ve Depolama Alanı** bölümünden yapılandırabilirsiniz.
Remove from the audit log events N day(s)	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, sistem denetim raporları dahil olmak üzere tüm raporlara raporları depolama sınırlamaları uygular.
SIEM Integration	*(geçiş gerçekleşmez)* Kaspersky Security Center'da SIEM entegrasyonunu yapılandırabilirsiniz.

Event notifications

KSWS Bildirim ayarları, **Genel Ayarlar** bölümünün Arabirim alt bölümüne taşındı.

Bildirim ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Notifications	**Bildirimler**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security bildirim metninin değiştirilmesini desteklemez. Kaspersky Endpoint Security, standart bildirimler görüntüler.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Yalnızca e-posta bildirim ayarları Kaspersky Endpoint Security'ye taşınır – **E-posta bildirim ayarları** (**Bildirimler** bloğu). Diğer yöneticileri bilgilendirme yöntemleri desteklenmez.
Application database is out of date	**Veritabanları güncellenmediyse "Veritabanları güncel değil" bildirimini gönder**
Application database is extremely out of date	**Veritabanları güncellenmediyse "Veritabanları son derece eski" bildirimini gönder**
Critical areas scan has not been performed for a long time	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, üç gün sonra, bir eksik Kritik Alanlar Taraması olayı oluşturur.

Interaction with Administration Server

KSWS Yönetim Sunucusu etkileşim ayarları, **Genel Ayarlar** bölümünün Raporlar ve Depolama Alanı alt bölümüne taşındı.

Yönetim Sunucusu etkileşim ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Quarantined files	**Karantina dosyaları**
Backed up files	**Yedekleme dosyaları**
Blocked hosts	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, engellenen ana bilgisayarlarla ilgili verileri otomatik olarak gönderir.

Tasks

Activating the application

Kaspersky Endpoint Security *Application activation* görevini desteklemez (KSWS). Bir *Anahtar ekle* görevi (KES) oluşturabilir, Yükleme paketine bir lisans anahtarı ekleyebilir veya otomatik lisans anahtarı dağıtımını etkinleştirebilirsiniz.

Copying Updates

Copying Updates görev ayarları (KSWS) *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevine (KES) taşındı.

Güncellemeleri Kopyalama görev ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Güncelleme kaynağı**: • **Kaspersky Security Center**. • **Kaspersky güncelleme sunucuları**. • **Kullanıcı tarafından belirtilen**
Use Kaspersky update servers if specified servers are not available	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Kaspersky güncelleme sunucuları da dahil olmak üzere birden fazla güncelleme kaynağı seçilmesine izin verir. İlk güncelleme kaynağı kullanılabilir olmadığında, Kaspersky Endpoint Security, listedeki diğer bir kaynaktan güncellemeler almanızı sağlar.
Use proxy server settings to connect to Kaspersky update servers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.
Use proxy server settings to connect to other servers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, veritabanı güncellemelerini ve uygulama modüllerinin kritik güncellemelerini tek bir paket olarak kopyalar.
Folder for local storage of copied updates	**Güncellemeleri klasöre kopyala**

Baseline File Integrity Monitor

Baseline File Integrity Monitor görev ayarları (KSWS) *Sistem Bütünlük Denetimi* görevine ve **Güvenlik Denetimleri** ilke bölümünün **Sistem Bütünlüğü İzleme** alt bölümüne taşındı.

Temel Dosya Bütünlüğü İzleme görev ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Hash calculation algorithm: • **MD5** • **SHA256**.	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, sağlama toplamı hesaplaması için SHA256 algoritmasını kullanır.
Scan scope	**İzleme kapsamı** (**Sistem Bütünlüğü İzleme** alt bölümü)

Database Update

Database Update görev ayarları (KSWS) *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevine (KES) taşındı.

Veritabanı Güncellemesi görevi ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Güncelleme kaynağı**: • **Kaspersky Security Center**. • **Kaspersky güncelleme sunucuları**. • **Kullanıcı tarafından belirtilen**
Use Kaspersky update servers if specified servers are not available	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Kaspersky güncelleme sunucuları da dahil olmak üzere birden fazla güncelleme kaynağı seçilmesine izin verir. İlk güncelleme kaynağı kullanılabilir olmadığında, Kaspersky Endpoint Security, listedeki diğer bir kaynaktan güncellemeler almanızı sağlar.
Use proxy server settings to connect to Kaspersky update servers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.
Use proxy server settings to connect to other servers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.
Lower the load on the disk I/O	*(geçiş gerçekeşmez)*

Software modules updates

Software Modules Update görev ayarları (KSWS) *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevine (KES) taşındı.

Yazılım Modülleri Güncellemesi görev ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Güncelleme kaynağı**: • **Kaspersky Security Center**. • **Kaspersky güncelleme sunucuları**. • **Kullanıcı tarafından belirtilen**
Use Kaspersky update servers if specified servers are not available	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Kaspersky güncelleme sunucuları da dahil olmak üzere birden fazla güncelleme kaynağı seçilmesine izin verir. İlk güncelleme kaynağı kullanılabilir olmadığında, Kaspersky Endpoint Security, listedeki diğer bir kaynaktan güncellemeler almanızı sağlar.
Use proxy server settings to connect to Kaspersky update servers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.
Use proxy server settings to connect to other servers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Copy and install critical software modules updates	**Kritik ve onaylı güncelleştirmeleri yükle**
Only check for critical software updates available	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, uygulama modülleri için kritik güncellemelerin kullanılabilirliğini sürekli olarak denetler.
Allow operating system restart	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, kullanıcıdan bilgisayarı yeniden başlatmak için izin ister.
Receive information about available scheduled software modules updates	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, yazılım modülü güncellemeleriyle ilgili bildirimleri görüntüler.

Rollback of Application Database Update

Rollback of Application Database Update görev ayarları (KSWS) *Güncellemeyi geri al* görevine (KES) taşındı. Yeni *Güncellemeyi geri al* görevi (KES) bir görev başlatma zamanlamasına sahiptir - *Elle*.

On-Demand Scan

On-Demand Scan görev ayarları (KSWS) *Kötü Amaçlı Yazılım Taraması* görevine (KES) taşındı.

Virüs Taraması görev ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Scan scope	**Tarama kapsamı**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Güvenlik düzeyi**: • **Yüksek**. • **Önerilen**. • **Düşük**. KSWS ve KES'de güvenlik düzeyi ayarları farklıdır.
Objects to scan: • **All objects** • **Objects scanned by format** • **Objects scanned according to list of extensions specified in anti-virus database** • **Objects scanned by specified list of extensions**	**Dosya türleri**: • **Tüm dosyalar**. • **Biçime göre taranan dosyalar**. • **Uzantıya göre taranan dosyalar** Kaspersky Endpoint Security, özel uzantı listeleri oluşturmaya izin vermez. Kaspersky Endpoint Security, **Objects scanned by specified list of extensions** değerini **Uzantıya göre taranan dosyalar** değeri ile değiştirir.
Subfolders	**Alt klasörleri dahil et**
Subfiles	*(geçiş gerçekeşmez)*
Scan disk boot sectors and MBR	*(geçiş gerçekeşmez)*
Scan alternate NTFS streams	*(geçiş gerçekeşmez)*
Scan only new and modified files	**Sadece yeni ve değiştirilmiş dosyaları tara**
Scan of compound objects: • **All archives** • **All SFX archives** • **All email databases** • **All packed objects** • **All plain email** • **All embedded OLE objects**	**Birleşik dosyaları tara**: • **Arşivleri tara**. • **Parola korumalı arşivleri tara**. • **Dağıtım paketlerini tara**. • **E-posta biçimindeki dosyaları tara**. • **Microsoft Office biçimlerindeki dosyaları tara**
Action to perform on infected and other objects: • **Disinfect** • **Disinfect. Remove if disinfection fails** • **Remove** • **Perform recommended action** • **Notify only**	**Tehdit algılandığında yapılacak eylem**: • **Temizle; temizleme başarısız olursa sil**. • **Temizle; temizleme başarısız olursa bildir**. • **Bilgilendir**.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Action to perform on probably infected objects: • **Quarantine** • **Remove** • **Perform recommended action** • **Notify only**	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, herhangi bir tehdit tespit edildiğinde eylemi uygular.
Perform actions depending on the type of object detected	*(geçiş gerçekeşmez)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(geçiş gerçekeşmez)*
Exclude files	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, güvenilir bölgeyi tüm bileşenlere uygular. İstisnaları güvenilir bölge ayarlarında yapılandırabilirsiniz.
Do not detect	*(geçiş gerçekeşmez)*
Stop scanning if it takes longer than N sec	**Bu süreden daha uzun süreyle taranan dosyaları atla**: **N sn**
Do not scan compound objects larger than N MB	**Büyük bileşik dosya paketlerini açma**
Use iSwift technology	**iSwift Teknolojisi**
Use iChecker technology	**iChecker Teknolojisi**
Action on the offline files: • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, çevrimdışı dosyaları bütünüyle tarar.

Application Integrity Check

Application Integrity Control görev ayarları (KSWS) *Uygulama Bütünlüğü Kontrolü* görevine (KES) taşındı.

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security *Applications Launch Control Generator* görevini desteklemez. Uygulama Denetimi ayarlarında kurallar oluşturabilirsiniz.

Rule Generator for Device Control

Kaspersky Endpoint Security *Rule Generator for Device Control* görevini desteklemez. Aygıt Denetimi ayarlarında erişim kuralları oluşturabilirsiniz.

KSWS bileşenlerini taşıma

Yerel kurulumdan önce Kaspersky Endpoint Security, bilgisayarda Kaspersky uygulamalarının var olup olmadığını denetler. Bilgisayarda Kaspersky Security for Windows Server kuruluysa, KES kurulu olan KSWS bileşenlerini algılar ve kurulum için aynı bileşenleri seçer.

KSWS'nin sahip olmadığı KES bileşenleri şu şekilde kurulur:

- AMSI Koruması, Sunucu Yetkisiz Erişim Önleme ve Düzeltme Altyapısı varsayılan ayarlarla yüklenir.
- BadUSB Saldırısı Önleme, Uyarlamalı Anomali Denetimi, Veri Şifreleme, Detection and Response bileşenleri yok sayılır.

Uzaktan kurulduğunda, KES uygulaması kurulu KSWS bileşenleri kümesini yok sayar. Yükleyici, yükleme paketinin özelliklerindee seçtiğiniz bileşenleri yükler. Kaspersky Endpoint Security yüklendikten ve ilkeler ile görevler taşındıktan sonra KES ayarları KSWS ayarlarına uygun olarak yapılandırılır.

KSWS görevlerini ve ilkelerini taşıma

KSWS ilke ve görev ayarlarını şu yollarla geçirebilirsiniz:

- İlke ve Görevleri Toplu Dönüştürme Sihirbazını kullanarak (bundan böyle Geçiş Sihirbazı olarak anılacaktır).

  > KSWS için Geçiş Sihirbazı yalnızca Yönetim Konsolu'nda (MMC) bulunur. İlke ve görev ayarlarının geçişi Web Console ve Cloud Console'da gerçekleştirilemez.

  Toplu dönüştürme sihirbazı, Kaspersky Security Center'ın farklı sürümleri için farklı şekilde çalışır. Çözümü 14.2 veya daha yüksek bir sürüme yükseltmenizi öneririz. Kaspersky Security Center'ın bu sürümünde, İlke ve görevler toplu dönüştürme sihirbazı, ilkeleri bir ilke yerine bir profile taşımanıza olanak tanır. Kaspersky Security Center'ın bu sürümünde, İlke ve görevler toplu dönüştürme sihirbazı, daha geniş bir ilke ayarları yelpazesini taşımanıza da olanak tanır.

- Kaspersky Endpoint Security for Windows için Yeni İlke Sihirbazını Kullanma.

  Yeni İlke Sihirbazı, bir KSWS ilkesine dayalı olarak bir KES ilkesi oluşturmanıza olanak tanır.

KSWS ilke geçiş prosedürleri, Geçiş Sihirbazı ve Yeni İlke Sihirbazı kullanıldığında farklıdır.

İlke ve görevler toplu dönüştürme sihirbazı

Geçiş sihirbazı, KES ilke ayarları yerine KSWS ilke ayarlarını ilke profiline aktarır. *İlke profili*, bilgisayarın yapılandırılmış etkinleştirme kurallarını karşılaması durumunda bilgisayarda etkinleştirilen bir ilke ayarları kümesidir. `UpgradedFromKSWS` cihaz etiketi, ilke profilinin tetikleme kriteri olarak seçilir. Kaspersky Security Center, uzaktan yükleme görevini kullanarak KSWS'nin üzerine KES yüklediğiniz tüm bilgisayarlara otomatik olarak `UpgradedFromKSWS` etiketini ekler. Farklı bir yükleme yöntemi seçtiyseniz etiketi cihazlara elle atayabilirsiniz.

Bir cihaza etiket eklemek için:

1. Sunucular için yeni bir etiket oluşturun — `UpgradedFromKSWS`.

   Cihazlar için etiketler oluşturmak hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

2. Kaspersky Security Center konsolunda yeni bir yönetim grubu oluşturun ve etiketi atamak istediğiniz sunucuları bu gruba ekleyin.

   Seçim aracını kullanarak sunucuları gruplandırabilirsiniz. Seçimlerle çalışmak hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

3. Kaspersky Security Center konsolunda yönetim grubunun tüm sunucularını seçin, seçilen sunucuların özelliklerini açın ve etiketi atayın.

Birden fazla KSWS ilkesinin geçişini gerçekleştiriyorsanız, her ilke tek bir kapsayıcı ilke içinde bir profile dönüştürülür. KSWS ilkesi zaten profiller içeriyorsa, bu profiller de profiller olarak geçirilir. Sonuç olarak, tüm KSWS ilkelerine karşılık gelen profilleri içeren tek bir ilke elde edersiniz.

KSWS ilke ayarlarını taşımak için İlke ve Görevler Toplu Dönüştürme Sihirbazını kullanma

1. Yönetim Konsolu'nda, Yönetim Sunucusunu seçin ve içerik menüsünü açmak için sağ tıklayın.
2. **Tüm görevler → İlke ve görevler toplu dönüştürme sihirbazı** seçimini yapın.

İlkeler ve Görevler Toplu Dönüştürme Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. İlke ve görevlerini dönüştürmeniz gereken uygulamayı seçme

Bu adımda Kaspersky Endpoint Security for Windows'u seçmeniz gerekir. Bir sonraki adıma geçin.

2. Adım. İlkelerin dönüştürülmesi

Geçiş sihirbazı, bir KES ilkesi içinde KSWS ilke profilleri oluşturur. İlke profillerine dönüştürmek istediğiniz Kaspersky Security for Windows Server ilkelerini seçin. Bir sonraki adıma geçin.

Geçiş Sihirbazı ilkeleri dönüştürmeye başlayacaktır. Yeni ilke profillerinin adları, orijinal KSWS ilkelerine karşılık gelir.

3. Adım. İlke geçiş raporu

Geçiş sihirbazı bir ilke taşıma raporu oluşturur. İlke geçiş raporu, ilkelerin dönüştürüldüğü tarih ve saati, orijinal KSWS ilkesinin adını, hedef KES ilkesinin adını ve yeni ilke profilinin adını içerir.

4. Adım. Görevlerin dönüştürülmesi

Geçiş Sihirbazı, Kaspersky Endpoint Security for Windows için yeni görevler oluşturur. Görev listesinden, Kaspersky Endpoint Security için oluşturmak istediğiniz KSWS görevlerini seçin. Yeni görevler *<KSWS görev adı> (dönüştürülmüş)* şeklinde adlandırılır. Bir sonraki adıma geçin.

5. Adım Sihirbazı tamamlama

Sihirbazı tamamlayın. Sonuç olarak, sihirbaz şunları yapar:

- Kaspersky Endpoint Security ilkesine yeni ilke profilleri eklenir.

  İlke, Kaspersky Security for Windows Server ayarlarını içeren profilleri içerir. Yeni ilke *Etkin* durumundadır. Sihirbaz, KSWS ilkelerini değiştirmeden bırakır.

- Yeni Kaspersky Endpoint Security görevleri oluşturur.

  Yeni görevler, KSWS görevlerinin kopyalarıdır. Sihirbaz, KSWS görevlerini değiştirmeden bırakır.

KSWS ayarlarını içeren yeni ilke profili *UpgradedFromKSWS <Kaspersky Security for Windows Server ilkesinin adı>* olarak adlandırılacaktır. Geçiş sihirbazı, profil özelliklerinde tetikleme kriteri olarak `UpgradedFromKSWS` cihaz etiketini otomatik olarak seçer. Böylece ilke profilindeki ayarlar sunuculara otomatik olarak uygulanır.

KSWS ilkesine dayalı bir ilke oluşturma sihirbazı

Bir KSWS ilkesine dayalı olarak bir KES ilkesi oluşturulduğunda, sihirbaz ayarları uygun şekilde yeni ilkeye aktarır. Yani, bir KES ilkesi bir KSWS ilkesine karşılık gelecektir. Sihirbaz, ilkeyi bir profile dönüştürmez.

KSWS ilke ayarlarını taşımak için Yeni İlke Sihirbazı nasıl kullanılır

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 seçin.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. **Yeni ilke** üzerine tıklayın.

   İlke Sihirbazı başlatılır.
5. İlke Sihirbazı talimatlarını uygulayın.

Adım 1. Grup ilkesi oluşturmak için uygulamayı seçme

Kaspersky Endpoint Security for Windows (14.2) uygulamasını seçin.

Adım 2. Grup ilkesini adlandırma

Grup ilkesi için bir ad girin; örneğin, *Ofis için İlke*.

Uygulamanın önceki bir sürümü için ilke ayarlarını kullan onay kutusunu seçin. **Göz at**'a tıklayın ve KSWS ilkesini seçin.

Adım 3. Kaspersky Security Network'e katılma

Lütfen Kaspersky Security Network (KSN) Bildirimi şartlarını okuyun ve kabul edin.

4. Adım Bilgisayarlarda uygulama kullanım modunun seçilmesi

Ana bilgisayarları korumak için standart mod seçimini yapın. Kaspersky Endpoint Security, tüm uygulama modları ve işletim sistemi türleri için ortak bir ilke sağlar.

> Farklı modlar ve işletim sistemi türleri için farklı ilkeler kullanmanızı öneririz.

5. Adım. Ayarları içe aktarma

> Bu adım, 4. adımda manuel ilke yapılandırmasını seçmeniz durumunda kullanılabilir.

Kaspersky Endpoint Security ayarlarından yola çıkarak bir ilke oluşturabilirsiniz. CFG yapılandırma dosyası. Yeni ilke sihirbazı, şifrelenmiş yapılandırma dosyalarını desteklemez. Yapılandırma dosyasını dışa aktarırken dosya şifreleme adımını atlayın.

Bir uygulama CFG yapılandırma dosyası içe aktarılırken sihirbaz tüm ilke ayarlarına erişemez. Örneğin, uygulama ayarlarında ilke profilleri eksik olabilir. Tüm ayarları ve profilleri ilkeye aktarmak istiyorsanız, bir KLP dosyasından başka bir ilkeyi içe aktarabilirsiniz.

> Bir yapılandırma dosyası içe aktarılırken, Kaspersky Endpoint Security kripto konteyner parolalarını aktarmaz. Sunuculara bağlanırken iki aşamalı kimlik doğrulama kullanıyorsanız, kripto konteyner parolalarını baştan belirlemeniz gerekir.

6. - 10. adım. İlke ayarlarını yapılandırma

> Bu adım, 4. adımda manuel ilke yapılandırmasını seçmeniz durumunda kullanılabilir.

İlke ayarlarını yönetmek için aşağıdaki adımları izleyin.

11. Adım. Güvenilen bölgeyi yapılandırma

Güvenilen bölgeyi yapılandırın. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar ekleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar da Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında Light Agent modunda hızlı bir şekilde yapılandırmanıza yardımcı olabilir.

12. Adım. İlke durumunu seçme

- **Etkin**. İlke bir sonraki senkronizasyondan sonra bilgisayarda etkin ilke olarak kullanılır.

  Bir etkin ilkenin ayarları, senkronizasyon sırasında istemci bilgisayara kaydedilir. Bir bilgisayarda aynı anda birden çok ilke uygulayamazsınız, bu nedenle her bir grupta yalnızca bir ilke etkin durumda olabilir.

- **Etkin değil**. Yedek ilke. Gerekli olduğunda etkin olmayan bir ilke etkin duruma geçebilir.

  Sınırsız sayıda etkin olmayan ilke oluşturabilirsiniz. Etkin olmayan bir ilke, ağdaki bilgisayarların uygulama ayarlarını etkilemez. Etkin olmayan ilkeler, virüs saldırısı gibi acil durumlara yöneliktir. Flash sürücüler üzerinden bir saldırı olursa flash sürücülere erişimi engelleyen bir ilkeyi etkinleştirebilirsiniz. Bu durumda, etkin ilke otomatik olarak etkin olmayan duruma geçer.

- **İşyeri dışında**. İlke, bir bilgisayar kuruluş ağından ayrıldığında etkinleştirilir.

Sihirbazı tamamlayın.

Geçiş sonrasında ilkelerde ve görevlerde ek yapılandırma

KSWS ve KES farklı bileşen setlerine ve ilke ayarlarına sahiptir, bu nedenle geçişten sonra ilke ayarlarının kurumsal güvenlik gereksinimlerinizi karşıladığını doğrulamanız gerekir.

Şu temel ilke ayarlarını kontrol edin:

- Parola koruması. KSWS Parola koruma ayarlarının geçişi yapılmaz. Kaspersky Endpoint Security, yerleşik bir Parola koruması özelliğine sahiptir. Eğer gerekliyse, Parola korumasını açın ve bir parola belirleyin.

- Güvenilir bölge. Nesneleri seçmek için KSWS ve KES tarafından kullanılan yöntemler farklıdır. KES, geçiş sırasında, tek tek dosyalar veya dosya/klasör yolları olarak tanımlanan istisnaları destekler. KSWS'nin önceden tanımlanmış bir alan veya bir komut dosyası URL'si olarak yapılandırılmış istisnaları varsa, bu tür istisnalar taşınmaz. Geçiş işleminden sonra bu tür istisnaları manuel olarak eklemelisiniz.

  > Kaspersky Endpoint Security'nin sunucularda düzgün çalıştığından emin olmak için, sunucunun çalışması için önemli olan dosyaların güvenilir bölgeye eklenmesi önerilir. SQL sunucuları için MDF ve LDF veritabanı dosyalarını eklemelisiniz. Microsoft Exchange sunucuları için CHK, EDB, JRS, LOG ve JSL dosyaları eklemelisiniz. Maskeler kullanabilirsiniz, örneğin, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir.

- Güvenlik Duvarı. KSWS Güvenlik Duvarı işlevleri, sistem düzeyindeki Güvenlik Duvarı tarafından gerçekleştirilir. KES'te, Güvenlik Duvarı işlevinden ayrı bir bileşen sorumludur. Geçiş tamamlandıktan sonra, Kaspersky Endpoint Security Güvenlik Duvarını yapılandırabilirsiniz.

- Kaspersky Security Network. Kaspersky Endpoint Security, bileşenler için KSN'nin ayrı olarak yapılandırılmasını desteklemez. Kaspersky Endpoint Security, tüm uygulama bileşenleri için KSN kullanır. KSN'yi kullanmak için Kaspersky Security Network Bildirimi'nin yeni hüküm ve koşullarını kabul etmeniz gerekir.

- İnternet Denetimi. İnternet trafiği kategorisi denetimi için engelleme kuralları, Kaspersky Endpoint Security'deki tek bir engelleme kuralına taşındı. Kaspersky Endpoint Security, kategori denetimi için izin verme kurallarını yok sayar. Kaspersky Endpoint Security, Kaspersky Security for Windows Server'ın tüm kategorilerini desteklemez. Kaspersky Endpoint Security'de var olmayan kategoriler taşınmaz. Dolayısıyla, desteklenmeyen kategorilere sahip web kaynağı sınıflandırma kuralları taşınmaz. Gerekirse İnternet Denetimi kuralları ekleyin.

- Proxy sunucusu. Proxy sunucusu bağlantı parolası taşınmaz. Proxy sunucusuna bağlanmak için kullanılacak parolayı elle girin.

- Bileşenlerin ayrı zamanlamaları. Kaspersky Endpoint Security, ayrı bileşenler için zamanlama yapılandırmayı desteklemez. Bileşenler, Kaspersky Endpoint Security çalışırken her zaman açıktır.

- Bileşenler seti. Kullanılabilir Kaspersky Endpoint Security özellikleri, işletim sisteminin türüne bağlıdır: iş istasyonu veya sunucu. Örneğin, sunucularda şifreleme araçları dışında yalnızca BitLocker Drive Encryption kullanılabilir.

- özniteliği. Özniteliğinin durumu taşınmaz. Özniteliği varsayılan değere sahip olacaktır. Varsayılan olarak, yeni ilkedeki hemen hemen tüm ayarlarda, alt ilkelerdeki ve yerel uygulama arabirimindeki ayarların değiştirilmesi için uygulanan bir yasak vardır. Öznitelik, **Managed Detection and Response (Industrial CyberSecurity)** bölümündeki ve **Kullanıcı desteği** ayar grubundaki (**Arabirim** bölümü) ilke ayarları için değerine sahiptir. Gerekirse, ana ilkeden ayar devralmayı yapılandırabilirsiniz.

- Etkin tehditlerle çalışma. Gelişmiş Temizleme, iş istasyonları ve sunucular için farklı çalışır. *Kötü Amaçlı Yazılım Taraması* görev ayarlarında ve uygulama ayarlarında gelişmiş temizlemeyi yapılandırabilirsiniz.

- Uygulamayı yükseltme. Büyük güncellemeleri ve yamaları yeniden başlatmadan yüklemek için uygulama yükseltme modunu değiştirmeniz gerekir. Varsayılan olarak, Uygulama güncellemelerini yeniden başlatmadan yükleme özelliği devre dışıdır.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security, Detection and Response çözümleriyle çalışmak için bütünleşik bir aracıya sahiptir. Gerekirse Kaspersky Endpoint Agent ilke ayarlarını Kaspersky Endpoint Security ilkesine aktarın.

- *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevleri. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevinin ayarlarının doğru şekilde taşındığından emin olun. KES, KSWS'nin üç görevi yerine tek bir KES görevi kullanır. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevlerini optimize edebilir ve gereksiz görevleri kaldırabilirsiniz.

- Diğer görevler. Uygulama Denetimi, Aygıt Denetimi ve Dosya Bütünlük İzleyicisi bileşenleri, KSWS ve KES'te farklı çalışır. KES *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control* görevlerini kullanmaz. Bu nedenle, bu görevler taşınmaz. Geöiş sonrasında, Dosya Bütünlük İzleyicisi, Uygulama Denetimi, Aygıt Denetimi bileşenlerini yapılandırabilirsiniz.

KSWS güvenilir bölgesini taşıma

Güvenilir bölge, Kaspersky Endpoint Security'nin etkin olduğunda izlemediği nesnelerin ve uygulamaların sistem yöneticisi tarafından yapılandırılan listesidir. Güvenilir bölge nesnelerini KSWS'den KES'e taşımak için *İlkeler ve Görevler Toplu Dönüştürme Sihirbazı* ya da *KSWS politikasına dayalı yeni bir KES politikası oluşturma sihirbazı* kullanılabilir. KSWS ve KES farklı bileşen setlerine ve özelliklere sahiptir, bu nedenle geçişten sonra istisnaların kurumsal güvenlik gereksinimlerinizi karşıladığını doğrulamanız gerekir. Güvenilir bölgeye istisna ekleme yöntemleri de KES ve KSWS için farklıdır. Taşıma Sihirbazı, tüm KSWS istisnalarını taşımak için araçlara sahip değildir. Bu, taşımadan sonra KSWS istisnalarından bazılarını manuel olarak eklemeniz gerektiği anlamına gelir.

Kaspersky Endpoint Security'nin sunucularda düzgün çalıştığından emin olmak için, sunucunun çalışması için önemli olan dosyaların güvenilir bölgeye eklenmesi önerilir. SQL sunucuları için MDF ve LDF veritabanı dosyalarını eklemelisiniz. Microsoft Exchange sunucuları için CHK, EDB, JRS, LOG ve JSL dosyaları eklemelisiniz. Maskeler kullanabilirsiniz, örneğin, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir.

KES ve KSWS güvenilir bölge oluşturma yöntemleri.

KSWS		KES
Object to scan		
• Predefined scope	*(geçiş gerçekeşmez)*	
• Disk, folder or network location	→	**Dosya veya klasör**
• File	→	**Dosya veya klasör**
• Script file or web address	*(geçiş gerçekeşmez)*	
Detected object	→	**Tespit edilen nesne türü**
Trusted processes	→	**Güvenilir uygulamalar**

Taranan nesnelerin taşınması

Özelliklerinde **Object to scan** yöntemi seçili olan KSWS istisnaları, bazı sınırlamalarla birlikte, özelliklerinde **Dosya veya klasör** yöntemi seçili olan KES istisnalarına taşınır. Bir istisnanın taşınması nesne seçim yöntemine bağlıdır:

- Predefined scope - *geçiş gerçekeşmez*.

  Geçiş işleminden sonra bu tür istisnaları manuel olarak eklemelisiniz. Önceden tanımlanmış alanlar olarak istisnalar, *Kötü Amaçlı Yazılım Taraması* görev ayarlarında yapılandırılmalıdır.

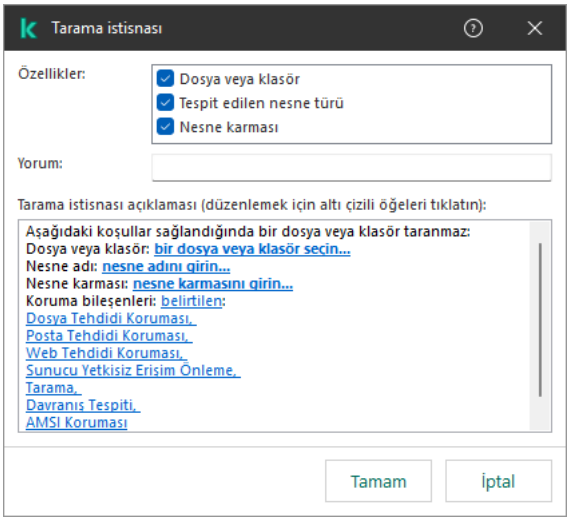
- Disk, folder or network location - özelliklerinde "Dosya veya klasör" yöntemi seçili olan KES istisnalarına taşı.

- File - özelliklerinde "Dosya veya klasör" yöntemi seçili olan KES istisnalarına taşı.

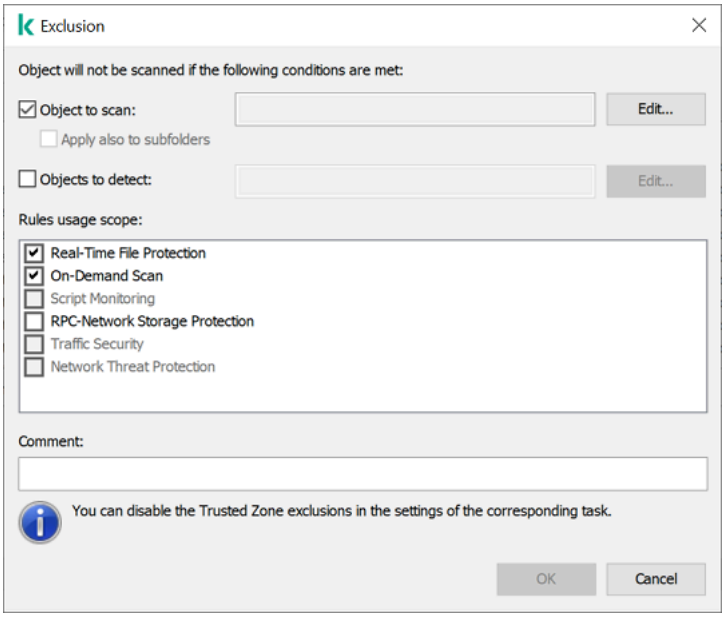
- Script file or web address - *geçiş gerçekeşmez*.

  Geçiş işleminden sonra bu tür istisnaları manuel olarak eklemelisiniz. Web Tehdidi Koruması için güvenilir web adreslerine komut dosyası web adresleri olarak istisnalar eklenmelidir.

Taranan nesne için **Apply also to subfolders** onay kutusu seçiliyse, bu ayar KES istisnalarına taşınır (**Alt klasörleri dahil et** onay kutusu).



KES istisna ayarları



KSWS istisna ayarları

Tespit edilen nesnelerin taşınması

Özelliklerinde **Detected object** yöntemi seçili olan KSWS istisnaları, özelliklerinde **Tespit edilen nesne türü** yöntemi seçili olan KES istisnalarına taşınır. Kaspersky Ansiklopedisinin sınıflandırmasına göre tespit edilen nesnenin adı (örneğin `Email-Worm`, `Rootkit` veya `RemoteAdmin`). Kaspersky Endpoint Security, soru işareti `?` (herhangi bir tek karakterle eşleşir) ve yıldız işareti `*` (herhangi bir karakter dizisiyle eşleşir) içeren maskeleri destekler.

İstisna kullanım kapsamının taşınması

Bir istisnanın kullanım kapsamı, istisnanın uygulandığı bir dizi bileşendir. KES ve KSWS farklı bileşen setlerine sahiptir, bu nedenle Taşıma Sihirbazı istisna kullanım kapsamını taşımaz. Bu nedenle, KSWS kullanım kapsamında en az bir bileşen seçilirse, KES istisnayı tüm uygulama bileşenlerine uygular.

KSWS kullanım kapsamını güvenilir bölge ayarlarında ve ayrıca KSWS koruma bileşenlerinin ayarlarında yapılandırabilirsiniz. Bunu yapmak için ilkenin karşılık gelen bölümünde **Apply Trusted Zone** onay kutusunu seçebilir veya temizleyebilirsiniz. KES koruma bileşenlerinin ayarlarında böyle bir onay kutusu bulunmaz. Bu, bireysel bileşen ayarlarındaki güvenilir bölge durumunun geçiş sırasında kaybolacağı anlamına gelir. Geçişi tamamladıktan sonra, KES ilkesindeki güvenilir bölge ayarlarında istisnanın geçerli olduğu bileşenleri seçin.

Açıklamaları taşıma

KSWS güvenilir bölgesinden gelen açıklamalar değişiklik yapılmadan KES istisna açıklamalarına taşınır.

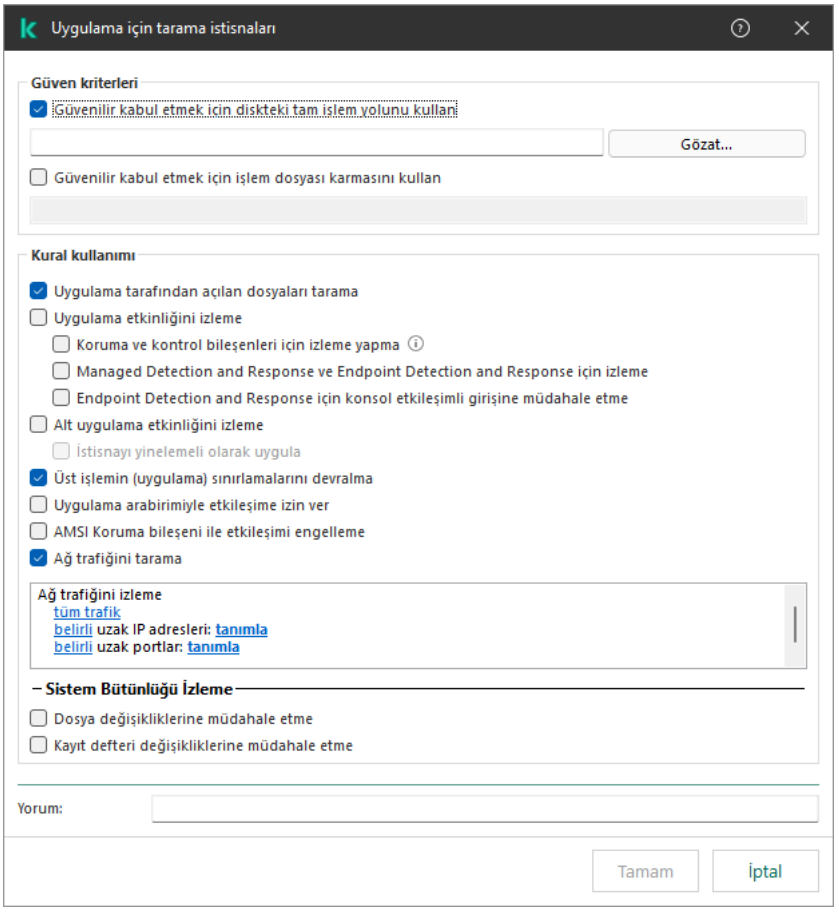
Güvenilir işlemlerin taşınması

KSWS güvenilir süreçleri bazı sınırlamalarla KES güvenilir süreçlerine taşınır. Güvenilir işlemlerin taşınması nesne seçim yöntemine bağlıdır:

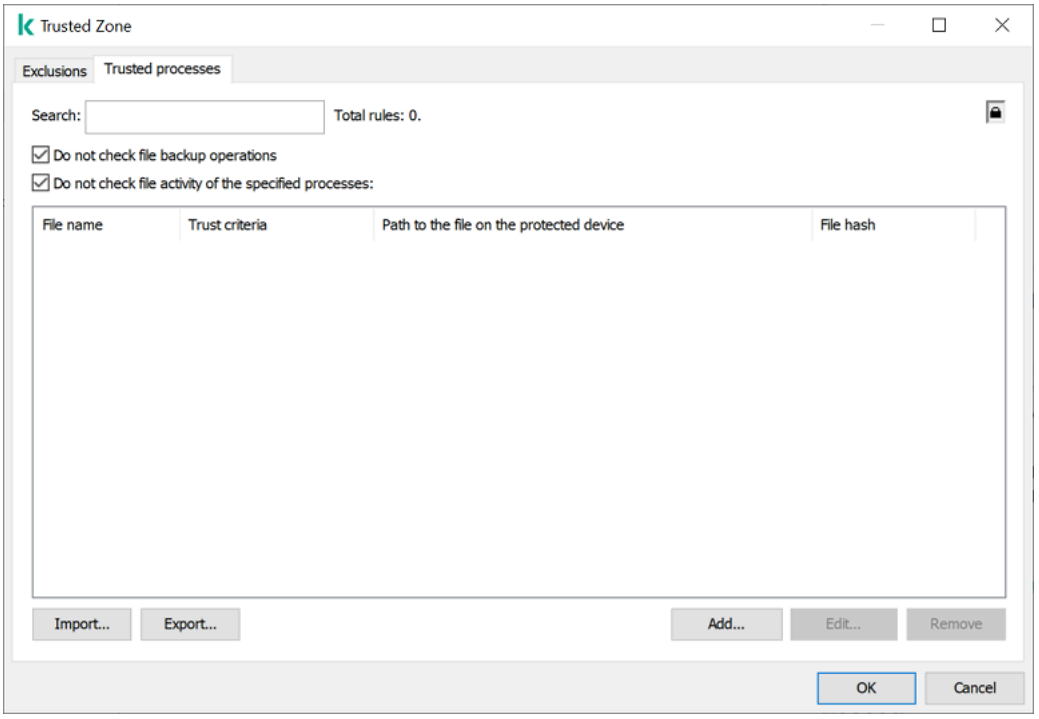
- Path to the file on the protected device - KES'in güvenilir uygulamalarına taşınır.
- File hash - *geçiş gerçekeşmez*.

KSWS'nin dosya karması olarak yapılandırılmış güvenilen süreçleri varsa, bu tür güvenilir süreçler taşınmaz. Geçiş işleminden sonra bu tür güvenilir işlemleri manuel olarak eklemeniz gerekir.

Güvenilir işlem ayarlarında **Do not check file backup operations** onay kutusu seçiliyse, bu ayar KES güvenilir uygulamalarına taşınır (**Uygulama etkinliğini izleme** onay kutusu).



KES güvenilir uygulama ayarları



KSWS güvenilir işlem ayarları

KSWS Uygulamaları Başlatma Denetimi kurallarını taşıma

KSWS Uygulamaları Başlatma Denetimi varsayılan olarak bloktur. Yani, Uygulama Başlatma Denetimi, kurallarda izin verilen uygulamalar olarak belirtilmeyen tüm uygulamaları otomatik olarak engeller. Bu nedenle KES Uygulama Denetimi için geçiş sihirbazı, varsayılan blok ilkesine karşılık gelen **İzin verilenler listesi** kontrol modunu otomatik olarak ayarlar.

Kuralları KSWS'den KES'e taşımak için *İlkeler ve Görevler Toplu Dönüştürme Sihirbazı* ya da *KSWS politikasına dayalı yeni bir KES politikası oluşturma sihirbazı* kullanılabilir.

Uygulama Başlatma Denetimi modunun taşınması

KSWS Uygulama Başlatma Denetimi modu KES Uygulama Denetimine aşağıdaki şekilde taşınır:

- **Statistics only** → **Kuralı test et**;
- **Active** → **Kuralları uygula**.

KSWS Uygulamaları Başlatma Denetimi kurallarını taşıma için önceden tanımlanmış kurallar

Varsayılan olarak, KSWS Uygulamaları Başlatma Denetimi iki kural içerir:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Önceden tanımlanmış kurallar, güvenilir bir kök sertifika tarafından imzalanmış *komut dosyaları*, *MSI paketleri* ve *yürütülebilir dosyaların* çalıştırılmasına izin verir. En az bir önceden tanımlanmış KSWS kuralı **Allow** türüne sahipse yazın, geçiş sihirbazı yeni bir izin kuralı oluşturur, **Güvenilir kök sertifikaları olan uygulamalar**. Yani KES Uygulama Denetimi, güvenilir komut dosyalarının, MSI paketlerinin ve yürütülebilir dosyaların çalıştırılmasına izin vermek için tek bir kural kullanır.

KSWS ön tanımlı kurallarının her ikisi de **Deny** türüne sahipse, KES önceden tanımlanmış kuralları yok sayar.

KSWS Uygulamaları Başlatma Denetimi kurallarını taşıma için özel kurallar

KSWS Uygulamaları Başlatma Denetimi kuralları, dosyaların aşağıdaki kriterlere uygun olarak yürütülmesini düzenler:

- dijital sertifikalı imza;
- SHA256 hash;
- dosya yolu.

Kurallar KSWS ve KES'de farklı şekilde oluşturulur, bu nedenle geçiş sihirbazı KSWS kurallarındaki koşulları ve istisnaları içeren *uygulama kategorileri* oluşturur ve bu uygulama kategorilerini KES kurallarına ekler. Sihirbaz, uygulama kategorilerinde **Sertifika**, **Klasör yolu** ve **Dosya karması** koşullarını kullanır. Yeni uygulama kategorileri Kaspersky Security Center Yönetim Konsolu'nda **Uygulama yönetimi → Uygulama kategorileri** bölümünde mevcuttur.

Geçiş sihirbazı KSWS kurallarını türe ve kullanıcıya göre gruplar. Ardından, sihirbaz KSWS kurallarından koşullar ve istisnalar içeren uygulama kategorileri oluşturur ve uygulama kategorilerini yeni KES kurallarına ekler. Sihirbaz, KES kurallarının **Açıklama** alanında KSWS kurallarının adlarını belirtir.

KSWS Uygulamaları Başlatma Denetimi gelişmiş ayarlarını taşıma

KSWS Uygulamaları Başlatma Denetimi ve KES Uygulama Denetimi için çalışma prensipleri farklıdır, bu nedenle geçiş sihirbazı ayarların bir alt kümesini aktarabilir.

Uygulama Başlatma Denetimi ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Repeat action taken for the first file launch on all the subsequent launches for this file	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, her çalışma girişiminde uygulamayı tarar.
Deny the command interpreters launch with no command to execute	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Uygulama Denetimi tarafından yasaklanmadıysa komut yorumlayıcılarının çalıştırılmasına izin verir.
Apply rules to executable files	*(geçiş gerçekeşmez)* Kural uygulama kapsamı, KES Uygulama Denetimi ayarlarında yapılandırılamaz. KES Uygulama Denetimi, tüm dosya türlerine kurallar uygular: yürütülebilir dosyalar, komut dosyaları ve MSI paketleri. Tüm dosya türleri KSWS'de kural uygulama kapsamına dahil edilmişse, KES, geçiş sırasında KSWS kurallarını taşır. Bazı dosya türleri KSWS'de kural uygulama kapsamından çıkarılırsa, geçiş sırasında KES ayrıca KSWS kurallarını da taşır, ancak **Kuralı test et** Uygulama Denetimi eylemi olarak seçilir.
Monitor loading of DLL modules	**DLL modüllerinin yüklenmesini izle (sistem yükünü önemli ölçüde artırır)**
Apply rules to scripts and MSI packages	*(geçiş gerçekeşmez)* Kural uygulama kapsamı, KES Uygulama Denetimi ayarlarında yapılandırılamaz. KES Uygulama Denetimi, tüm dosya türlerine kurallar uygular: yürütülebilir dosyalar, komut dosyaları ve MSI paketleri. Tüm dosya türleri KSWS'de kural uygulama kapsamına dahil edilmişse, KES, geçiş sırasında KSWS kurallarını taşır. Bazı dosya türleri KSWS'de kural uygulama kapsamından çıkarılırsa, geçiş sırasında KES KSWS kurallarını taşır, ancak **Kuralı test et** Uygulama Denetimi eylemi olarak seçilir.
Deny applications untrusted by KSN	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, uygulamaların tanınırlığını dikkate almaz ve uygulamaların kurallara uygun olarak çalıştırılmasına izin verir veya vermez.
Allow applications trusted by KSN	Geçiş sırasında KES, yeni bir izin verme kuralı ekler. **Diğer Yazılımlar\KSN'deki tanınırlığına göre güvenilir uygulamalar**, KL kategorisi, kural tetikleme koşulu olarak belirtilir.
Users and / or user groups allowed to run applications trusted by KSN	**Diğer Yazılımlar\KSN'deki tanınırlığına göre güvenilir uygulamalar** KL kategorisini içeren bir Uygulama Denetimi izin verme kuralındaki **Kullanıcılar ve hakları**
Automatically allow software distribution via applications and packages listed	KSWS ve KES'te Yazılım Dağıtım Kontrolü farklı şekilde çalışır. Geçiş sırasında KES, otomatik yazılım dağıtımına izin verilen uygulamalar için yeni izin kuralları ekler. Dosya karması, kural tetikleme koşulu olarak belirlenir.
Always allow software distribution via Windows Installer	KSWS ve KES'te Yazılım Dağıtım Kontrolü farklı şekilde çalışır. Geçiş sırasında KES, otomatik yazılım dağıtımına izin verilen uygulamalar için yeni izin kuralları ekler (**Software distribution applications and packages allowed**). Dosya karması, kural tetikleme koşulu olarak belirlenir. Hesap özelliklerinde **Güvenilir Güncelleyiciler** onay kutusu seçilir.

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(geçiş gerçekeşmez)*
Software distribution applications and packages allowed	KSWS ve KES'te Yazılım Dağıtım Kontrolü farklı şekilde çalışır. Geçiş sırasında KES, otomatik yazılım dağıtımına izin verilen uygulamalar için yeni izin kuralları ekler. Dosya karması, kural tetikleme koşulu olarak belirlenir. Hesap özelliklerinde **Güvenilir Güncelleyiciler** onay kutusu seçilir.
Schedule settings	*(geçiş gerçekeşmez)* KSWS ayarlarında bileşen için bir zamanlama yapılandırılırsa, Uygulama Denetimi bileşeni geçiş sırasında etkinleştirilir. KSWS ayarlarında bileşen için bir zamanlama yapılandırılmamışsa, geçiş sırasında Uygulama Denetimi devre dışı bırakılır. Bileşen için ayrı bir program yapılandırmak mümkün değildir. Bileşen, Kaspersky Endpoint Security çalışırken her zaman açıktır.

KSWS yerine KES'i yükleme

Kaspersky Endpoint Security'yi şu şekillerde yükleyebilirsiniz:

- KSWS'yi kaldırdıktan sonra KES'i yüklemek (önerilir).
- KES'in KSWS'nin üzerine yüklemek.

Kaspersky Security for Windows Server'ı kaldırma

Uygulamayı, *Uygulamayı uzaktan kaldır* görevi ile ya da sunucu üzerinden yerel olarak kaldırabilirsiniz. KSWS'yi kaldırdıktan sonra sunucuyu yeniden başlatmanız gerekebilir. Kaspersky Endpoint Security'yi yeniden başlatma yapmadan yüklemek istiyorsanız lütfen Kaspersky Security for Windows Server'ın tamamen kaldırıldığından emin olun. Uygulama tamamen kaldırılmadığı takdirde, Kaspersky Endpoint Security'nin yüklenmesi sunucunun hatalı çalışmasına neden olabilir. Kavremover yardımcı programını kullandıysanız uygulamanın tamamen kaldırıldığından emin olmanız da önerilir. Kavremover yardımcı programı KSWS yönetimini desteklemez.

KSWS'ye erişimi kısıtlamak için Parola Koruması etkinleştirilmişse, KES kurulum paketi ayarlarına kaldırma parolasını girin.

KSWS kaldırıldıktan sonra, mevcut yöntemlerden herhangi birini kullanarak Kaspersky Endpoint Security for Windows'u yükleyin.

Kaspersky Endpoint Security'yi yükleme

KES'i uzaktan kurduğunuzda, kurulum paketi özelliklerinde seçtiğiniz bileşenler sunucuya yüklenir. Kurulum paketi özelliklerinde varsayılan bileşenleri seçmenizi öneririz. KES'i KSWS'nin üzerine kurarken yeniden başlatma gerekli değildir.

Yerel kurulumdan önce Kaspersky Endpoint Security, bilgisayarda Kaspersky uygulamalarının var olup olmadığını denetler. Bilgisayarda Kaspersky Security for Windows Server kuruluysa, KES kurulu olan KSWS bileşenlerini algılar ve kurulum için aynı bileşenleri seçer. KES'i KSWS'nin üzerine kurarken yeniden başlatma gerekli değildir.

KSWS'nin üzerine KES kurulumu başarısız olursa, kurulumu geri alabilirsiniz. Kurulumu geri aldıktan sonra, sunucuyu yeniden başlatmanız ve tekrar denemeniz önerilir.

KSWS ayarları ve görevleri, Kaspersky Endpoint Security for Windows yüklendiğinde taşınmaz. Ayarları ve görevleri taşımak için İlke ve Görevler Toplu Dönüştürme Sihirbazı'nı çalıştırın.

Yüklü bileşenlerin listesini uygulama arabiriminin **Güvenlik** bölümünde `status` kodunu kullanarak ya da bilgisayar özelliklerinde Kaspersky Security Center konsolundan kontrol edebilirsiniz. *Uygulama bileşenlerini değiştirmeyi* kullanarak kurulumdan sonra bileşen setini değiştirebilirsiniz.

[KSWS+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi

Kaspersky Endpoint Security for Windows'un EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA ve MDR'nin bir parçası olarak kullanılmasını desteklemek için uygulamaya yerleşik bir aracı eklendi. Bu çözümlerle çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok.

KSWS'den KES'e geçiş sırasında EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA ve MDR çözümleri Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır.

[KSWS+KEA] yapılandırmasını [KES+bütünleşik aracı]'ya aktarmak şu adımları içerir:

1. **KSWS'den KES'e geçiş**

   KSWS'den KES'e geçiş, Kaspersky Security for Windows Server yerine Kaspersky Endpoint Security'nin kurulmasını içerir.

   Yöneticiler genellikle KSWS'ye ve KEA'ya erişimi kısıtlamak için Parola korumasını etkinleştirir. Kaspersky Security Center Linux 15.1'den başlamak üzere, *Uygulamayı uzaktan yükle* görev ayarlarında uygulama kaldırma parolasını girebilirsiniz. Görev yalnızca bir kaldırma parolası girilmesine izin verir. Yani KSWS ve KEA için aynı parola ayarlanırsa KSWS ve KEA uygulamaları başarıyla kaldırılır. Parolalar farklıysa uygulamalardan birinin kaldırılması erişim hatasıyla başarısız olur. Geçişi tamamlamak için, *Uygulamayı uzaktan yükle* görevinin ayarlarında parolasını giremediğiniz uygulama için Parola Korumasını devre dışı bırakmanız gerekir.

   Geçişi gerçekleştirmek için, Kaspersky Endpoint Security'nin bir parçası olarak Algılama ve Yanıt çözümlerini desteklemek için gereken bileşenleri seçmelisiniz. Uygulamayı yükledikten sonra Kaspersky Endpoint Security, bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

2. **İlkelerin ve görevlerin taşınması**

[KSWS+KEA] ilke ve görevlerini [KES+bütünleşik aracı]'ya aktarmak şu adımları içerir:

1. İlke ve Görevler Toplu Dönüştürme Sihirbazını (yalnızca Yönetim Konsolu'nda (MMC) kullanılabilir) kullanarak ilkeleri ve görevleri KSWS'den KES'e aktarma.

   Sonuç olarak, KES ilkesine *UpgradedFromKSWS <Kaspersky Security for Windows Server ilkesinin adı>* adına sahip bir ilke profili eklenir. Yeni KES görevleri de *<KSWS görev adı> (dönüştürülmüş)* adlarıylla oluşturulur.

2. Kaspersky Endpoint Agent'tan geçiş sihirbazını kullanarak ilkeleri ve görevleri KEA'dan KES'e aktarma (yalnızca Web Console ve Cloud Console'da mevcuttur).

   Sonuç olarak, *<Kaspersky Endpoint Security ilkesinin adı> ve <Kaspersky Endpoint Agent ilkesinin adı>* adıyla yeni bir ilke oluşturulur. Yeni görevler ve KES görevleri de oluşturulur.

3 Lisanslama işlevleri

Kaspersky Endpoint Security for Windows ve Kaspersky Endpoint Agent'ı etkinleştirmek için ortak bir Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security lisansı kullanıyorsanız, EDR Optimum işlevi uygulama 11.7.0 sürümüne yükseltildikten sonra otomatik olarak etkinleştirilecektir. Başka bir şey yapmanız gerekmez.

EDR Optimum işlevini etkinleştirmek için bağımsız bir Kaspersky Endpoint Detection and Response Optimum Eklentisi lisansı kullanıyorsanız, EDR Optimum Eklentisi anahtarının Kaspersky Security Center veri havuzuna eklendiğinden ve otomatik lisans anahtarı dağıtım işlevinin etkinleştirildiğinden emin olmalısınız. EDR Optimum işlevi, uygulamayı 11.7.0 sürümüne yükselttikten sonra otomatik olarak etkinleştirilir.

Kaspersky Endpoint Agent'ı etkinleştirmek için Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security lisansı ve Kaspersky Endpoint Security for Windows'u etkinleştirmek için farklı bir lisans kullanıyorsanız, Kaspersky Endpoint Security for Windows anahtarını, ortak Kaspersky Endpoint Detection and Response Optimum veya Kaspersky Optimum Security anahtarıyla değiştirmelisiniz. Anahtarı, *Anahtar ekle* görevini kullanarak değiştirebilirsiniz.

Kaspersky Sandbox işlevini etkinleştirmeniz gerekmez. Kaspersky Sandbox işlevi, Kaspersky Endpoint Security for Windows'u yükseltip etkinleştirdikten hemen sonra kullanılabilir.

Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olarak Kaspersky Endpoint Security'yi etkinleştirmek için yalnızca Kaspersky Anti Targeted Attack Platform lisansı kullanılabilir. EDR (KATA) işlevi, uygulamayı 12.1 sürümüne yükselttikten sonra otomatik olarak etkinleştirilir. Başka bir şey yapmanız gerekmez.

4 Kaspersky Endpoint Detection and Response Optimum ve Kaspersky Sandbox'ın durumunu kontrol etme

Yükseltmeden sonra bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

- Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
- *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin.
- Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.

Uygulama bileşenlerinin durumu hakkında rapor seçeneğini kullanarak EDR Optimum işlevselliğinin etkinleştirildiğinden emin olun. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, EDR Optimum'un otomatik lisans anahtarı dağıtım işlevinin açık olduğundan emin olun.

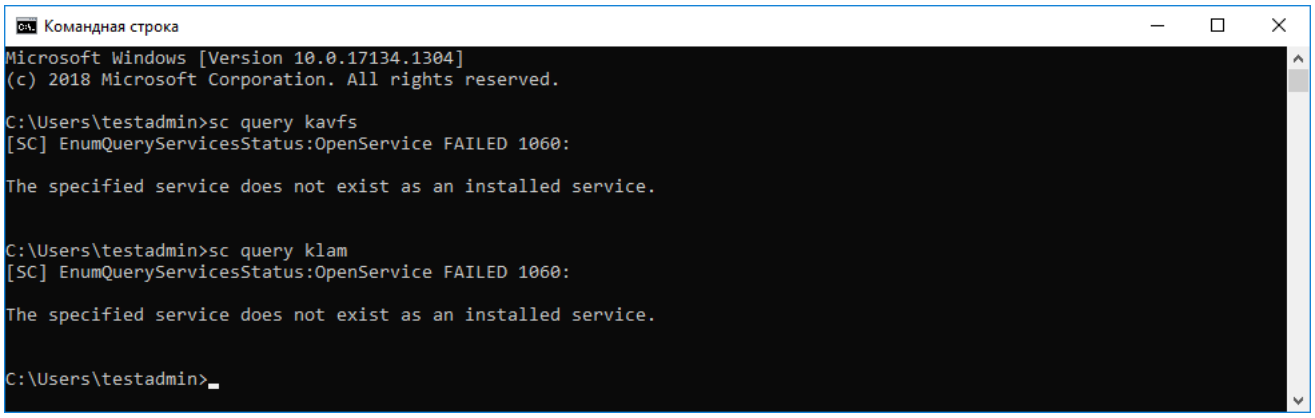
Kaspersky Security for Windows Server'ın başarıyla kaldırıldığından emin olma

Kaspersky Security for Windows Server'ın tamamen kaldırıldığından emin olun:

- `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` klasörü mevcut değil.
- Şu hizmetler mevcut değil:
  - Kaspersky Security Service (KAVFS)
  - Kaspersky Security Management hizmeti (KAVFSGT)
  - Kaspersky Security Exploit Prevention hizmeti (KAVFSSLP)
  - Kaspersky Security Script Checker hizmeti (KAVFSSCS)

  Çalışan hizmetleri Görev Yöneticisinde veya `sc query` komutunu vererek kontrol edebilirsiniz (aşağıdaki şekle bakın).
- Şu sürücüler mevcut değildir:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

Yüklü sürücüleri `C:\Windows\System32\drivers` klasöründen veya `sc query` komutunu vererek kontrol edebilirsiniz. Bir hizmet veya sürücü eksikse şu yanıtı alırsınız:



Kaspersky Security for Windows Server hizmetlerinin ve sürücülerinin başarıyla kaldırıldığından emin olma

Uygulama veya sürücü dosyaları sunucuda kalırsa, ilgili dosyaları elle silin. Kaspersky Security for Windows Server hizmetleri sunucuda hala çalışıyorsa, hizmetleri elle olarak durdurun (`sc stop`) ve silin (`sc delete`). klam.sys sürücüsünü durdurmak için `fltmc unload klam` komutunu kullanın.

KES'i bir KSWS anahtarıyla etkinleştirme

Uygulamayı yükledikten sonra, Kaspersky Security for Windows Server (KSWS) lisans anahtarı kullanarak Kaspersky Endpoint Security for Windows'u (KES) etkinleştirebilirsiniz. Geçişten sonraki etkinleştirme süreci, KSWS etkinleştirme yöntemine bağlıdır (aşağıdaki tabloya bakın).

Kaspersky Endpoint Security, *Kaspersky Security for Storage lisansını* desteklemez. Bu lisansla çalışmak için Kaspersky Security for Windows Server kullanmanız gerekir.

KES'i KSWS anahtarı ile etkinleştirmek için yalnızca etkinleştirme kodunu kullanabilirsiniz. Uygulamayı etkinleştirmek için bir anahtar dosyası kullanıyorsanız Kaspersky Endpoint Security anahtar dosyası için Teknik Destek ile iletişime geçmeniz gerekir.

Kaspersky Endpoint Security for Windows'u Kaspersky Security for Windows Server anahtarıyla etkinleştirme

Kaspersky Security for Windows Server etkinleştirme yöntemi	Kaspersky Endpoint Security for Windows anahtar geçişi.
KSWS lisans anahtarının bilgisayarlara otomatik dağıtımı.	KSWS lisans anahtarı özelliklerinde otomatik anahtar dağıtımı etkinleştirildiğinde, KES, KSWS anahtarı ile otomatik olarak etkinleştirilir.
KSWS anahtarı bir görev tarafından eklenir.	KSWS uygulamanız görev kullanılarak etkinleştirildiyse, KSWS'den geçiş sırasında KSWS lisans anahtarı silinir. Bu durumda uygulamayı yeniden etkinleştirmeniz gerekir. Örneğin, Kaspersky Endpoint Security for Windows yükleme paketine bir lisans anahtarı ekleyebilirsiniz.
KSWS anahtarı, uygulama arabirimine yerel olarak eklenir.	KSWS uygulamanız Uygulama Etkinleştirme Sihirbazı kullanılarak yerel olarak etkinleştirildiyse, KSWS'den geçiş sırasında KSWS lisans anahtarı silinir. Bu durumda uygulamayı yeniden etkinleştirmeniz gerekir. Örneğin, Kaspersky Endpoint Security for Windows yükleme paketine bir lisans anahtarı ekleyebilirsiniz.
KSWS anahtarı kurulum paketine eklenir.	KSWS uygulamanız kurulum paketinde gelen anahtar kullanılarak etkinleştirildiyse, KSWS'den geçiş sırasında KSWS lisans anahtarı silinir. Bu durumda uygulamayı yeniden etkinleştirmeniz gerekir. Örneğin, Kaspersky Endpoint Security for Windows yükleme paketine bir lisans anahtarı ekleyebilirsiniz.

Kaspersky Security for Windows Server etkinleştirme yöntemi	Kaspersky Endpoint Security for Windows anahtar geçişi.
Amazon Web Services'de (AWS) ücretli sanal makine görüntüsü (Amazon Machine Image - AMI).	Kaspersky Security Center'ı Amazon Web Services'te (AWS) ücretli bir sanal makine görüntüsü (Amazon Makine Görüntüsü - AMI) olarak satın aldıysanız KES'i etkinleştirmeniz gerekmez. Bu durumda Kaspersky Security Center, uygulamaya zaten eklenmiş olan AWS aboneliğini kullanır.
Kendi lisansınızla hazır ücretsiz Kaspersky Security Center görüntüsü (Kendi Lisansını Getir - KLG modeli).	Bir bulut ortamında (Kendi Lisansını Getir – KLG modeli) kendi lisansınızla birlikte kullanıma hazır ücretsiz bir Kaspersky Security Center görüntüsü kullanıyorsanız, mevcut herhangi bir yöntemi kullanarak uygulamayı etkinleştirmeniz gerekir. Bir Kaspersky Hybrid Cloud Security lisansına ihtiyacınız olacak.

Yüksek yüklü sunucuların geçişi için dikkat edilmesi gereken özel hususlar

Yüksek yüke sahip sunucularda performansı izlemek ve hataları önlemek önemlidir. Kaspersky Endpoint Security for Windows'a geçiş yaptıktan sonra, diğer bileşenlere göre önemli sunucu kaynakları kullanan uygulama bileşenlerini geçici olarak devre dışı bırakmanızı öneririz. Sunucunun normal çalıştığından emin olduktan sonra uygulama bileşenlerini tekrar açabilirsiniz.

Yüksek yüke sahip sunucular için geçişin aşağıdaki şekilde yapılmasını öneriyoruz:

1. Varsayılan ayarlarla bir Kaspersky Endpoint Security ilkesi oluşturun.

   Varsayılan ayarlar optimum olarak kabul edilir. Kaspersky uzmanları tarafından bu ayarlar tavsiye edilmektedir. Varsayılan ayarlar, önerilen koruma düzeyini ve optimum kaynak kullanımını sağlar.

2. İlke ayarlarında aşağıdaki bileşenleri kapatın: Ağ Tehdidi Koruması, Davranış Tespiti, Exploit Önleme, Düzeltme Altyapısı, Uygulama Denetimi.

   Kuruluşunuzda Kaspersky Managed Detection and Response (MDR) çözümü dağıtılmışsa BLOB yapılandırma dosyasını Kaspersky Endpoint Security ilkesine yükleyin.

3. Kaspersky Security for Windows Server'ı sunucudan kaldırın.

4. Kaspersky Endpoint Security for Windows'u varsayılan bileşen seti ile yükleyin.

   Kuruluşunuzda Detection and Response çözümleri dağıtılmışsa, kurulum paketinin özelliklerinden ilgili bileşenleri seçin.

5. Uygulamanın ayarlarını kontrol edin:

   - Uygulama, KSWS lisans anahtarı ile etkinleştirilir.
   - Yeni ilke uygulanır. Önceden seçilen bileşenler devre dışı bırakılır.

6. Sunucunun çalıştığından emin olun. Kaspersky Endpoint Security for Windows'un sunucu kaynaklarının %1'inden fazlasını kullanmadığından emin olun.

7. Gerekirse, tarama istisnaları oluşturun, güvenilir uygulamalar ekleyin, güvenilir web adreslerinin bir listesini oluşturun.

8. Davranış Tespiti, Exploit Önleme, Düzeltme Altyapısı bileşenlerini açın. Kaspersky Endpoint Security for Windows'un sunucu kaynaklarının %1'inden fazlasını kullanmadığından emin olun.

9. Ağ Tehdidi Koruması bileşenini açın. Kaspersky Endpoint Security for Windows'un sunucu kaynaklarının %2'inden fazlasını kullanmadığından emin olun.

10. Kural testi modunda Uygulama Denetimi bileşenini açın.

11. Uygulama Denetiminin çalıştığından emin olun. Gerekirse, yeni Uygulama Denetimi kuralları ekleyin ve Uygulama Denetiminin çalıştığını onayladıktan sonra kural test modunu kapatın.

KSWS'den KES'e geçiş yaptıktan sonra uygulamanın doğru çalıştığından emin olun. Konsoldaki sunucunun durumunu kontrol edin (*Tamam* olmalıdır). Uygulama için herhangi bir hata rapor edilmediğinden emin olun, ayrıca Yönetim Sunucusuna son bağlantı zamanını, son veritabanı güncelleme zamanını ve sunucu koruma durumunu kontrol edin.

Uygulamayı Server Core modunda bir sunucuda yönetme

Server Core modundaki bir sunucu GUI'ye sahip değildir. Bu nedenle, uygulamayı yalnızca Kaspersky Security Center konsolunu kullanarak uzaktan veya komut satırından yerel olarak yönetebilirsiniz.

Uygulamayı Kaspersky Security Center konsolunu kullanarak yönetme

Uygulamayı Kaspersky Security Center konsolunu kullanarak yüklemek, normal şekilde yüklemekten farklı değildir. Bir kurulum paketi oluştururken, uygulamayı etkinleştirmek için bir lisans anahtarı ekleyebilirsiniz. Bir Kaspersky Endpoint Security for Windows anahtarı veya bir Kaspersky Security for Windows Server anahtarı kullanabilirsiniz.

Server Core modundaki bir sunucuda, şu uygulama bileşenleri kullanılamaz: Web Tehdidi Koruması, Posta Tehdidi Koruması, İnternet Denetimi, BadUSB Saldırısı Önleme, Dosya Düzeyinde Şifreleme (FLE), Kaspersky Disk Encryption (FDE).

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. Uygulama, kullanıcıdan sunucuyu yeniden başlatmasını isteyen bir pencere görüntüleyemez. Sunucuyu yeniden başlatmanın gerekliliği hakkında Kaspersky Security Center konsolundaki raporlardan bilgi edinebilirsiniz.

Uygulamayı Server Core modundaki bir sunucuda yönetmek, bir bilgisayarı yönetmekten farklı değildir. Uygulamayı yapılandırmak için ilkeleri ve görevleri kullanabilirsiniz.

Uygulamayı Server Core modundaki bir sunucuda yönetmek, aşağıdaki özel hususları içerir:

- Server Core modundaki bir sunucuda bir grafik kullanıcı arabirimi yoktur. Kaspersky Endpoint Security bu nedenle kullanıcıya Gelişmiş Temizlemenin gerekli olduğunu bildiren bir uyarı görüntülemez. Bir tehdidi temizlemek için uygulama ayarlarından Gelişmiş Temizleme teknolojisini etkinleştir ve *Kötü Amaçlı Yazılım Taraması* görev ayarlarından Gelişmiş Temizlemeyi derhal çalıştır seçimini yapın. Ardından *Kötü Amaçlı Yazılım Taraması* görevini başlatmalısınız.

- BitLocker Drive Encryption, yalnızca Güvenilir Platform Modülü (TPM) ile kullanılabilir. Uygulama, önyükleme öncesi kimlik doğrulaması için parola istemi penceresini görüntüleyemediğinden, şifreleme için bir PIN/parola kullanılamaz. İşletim sisteminde Federal Bilgi İşleme standardı (FIPS) uyumluluk modu etkinse, sürücüyü şifrelemeye başlamadan önce şifreleme anahtarını kaydetmek için çıkarılabilir bir sürücü bağlayın.

Uygulamanın komut satırından yönetimi

Bir grafik kullanıcı arabirimi kullanamadığınızda, Kaspersky Endpoint Security'yi komut satırından yönetebilirsiniz.

Uygulamayı Server Core modundaki bir sunucuya kurmak için şu komutu çalıştırın:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Uygulamayı etkinleştirmek için şu komutu çalıştırın:

```
avp.com license /add <activation code or key file>
```

Uygulama profili durumlarını kontrol etmek için şu komutu çalıştırın:

```
avp.com status
```

Uygulama yönetimi komutlarının listesini görüntülemek için şu komutu çalıştırın:

```
avp.com help
```

[KSWS+KEA] uygulamasının [KES+ bütünleşik aracı]'ya geçişi

Kaspersky Security for Windows Server'dan (KSWS) Kaspersky Endpoint Security'ye (KES) geçerken, sunucu korumasını yapılandırmak ve performansı optimize etmek için aşağıdaki önerileri kullanabilirsiniz. Burada tek bir kuruluş için bir geçiş örneğine bakacağız.

Kuruluşun altyapısı

Şirket aşağıdaki ekipmana sahiptir:

- Kaspersky Security Center 14.2

  Yönetici, Kaspersky çözümlerini Yönetim Konsolu'nu (MMC) kullanarak yönetir. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) da kullanılmaktadır

  Kaspersky Security Center'da, kuruluşun sunucularını içeren üç yönetim grubu oluşturulmuştur: SQL sunucuları için iki yönetim grubu ve Microsoft Exchange sunucuları için bir yönetim grubu. Her yönetim grubu kendi politikası tarafından yönetilir. Kuruluştaki tüm sunucular için *Database Update* ve *On-demand scan* görevleri oluşturulmuştur.

  KSWS etkinleştirme anahtarı Kaspersky Security Center'a eklenmiştir. Otomatik anahtar dağıtımı etkinleştirilmiştir.

- Kaspersky Security for Windows Server 11.0.1 ve Kaspersky Endpoint Agent 3.11 yüklü SQL sunucuları vardır. SQL sunucuları iki kümede birleştirilmiştir.

  KSWS, *SQL_Policy(1)* ve *SQL_Policy(2)* politikaları tarafından yönetilmektedir. Ayrıca *Database Update*, *On-demand scan* görevleri oluşturulmuştur.

- Kaspersky Security for Windows Server 11.0.1 ve Kaspersky Endpoint Agent 3.11 yüklü bir Microsoft Exchange sunucusu vardır.

  KSWS, *Exchange_Policy* politikası tarafından yönetilmektedir. Ayrıca *Database Update*, *On-demand scan* görevleri oluşturulmuştur.

Geçişi planlama

Geçiş şu adımları içerir:

1. İlkeler ve Görevler Toplu Dönüştürme Sihirbazını kullanarak KSWS görevlerini ve ilkelerini taşıma.
2. İlkeler ve Görevler Toplu Dönüştürme Sihirbazını kullanarak Kaspersky Endpoint Agent ilkesini taşıma.
3. Yeni ilkenin özelliklerinde, ilke profillerini etkinleştirmek için etiketleri kullanma.
4. KSWS yerine KES'i yükleme.
5. EDR Optimum'u etkinleştirme.
6. KES'in çalıştığını doğrulama.

Geçiş senaryosu, başlangıçta SQL sunucularının bir kümesinde gerçekleştirilir. Ardından, diğer SQL sunucuları kümesinde geçiş senaryosu gerçekleştirilir. Daha sonra Microsoft Exchange üzerinde geçiş senaryosu gerçekleştirilir.

İlkeler ve Görevler Toplu Dönüştürme Sihirbazını kullanarak KSWS görevlerini ve ilkelerini taşıma

KSWS görevlerini geçirmek için İlkeler ve Görevler Toplu Dönüştürme Sihirbazı (taşıma sihirbazı) kullanılabilir. Sonuç olarak, *SQL_Policy(1)*, *SQL_Policy(2)* ve *Exchange_Policy* ilkeleri yerine, sırasıyla SQL ve Microsoft Exchange sunucuları için üç profil içeren tek bir ilke elde edersiniz. KSWS ayarlarını içeren yeni ilke profili *UpgradedFromKSWS <Kaspersky Security for Windows Server ilkesinin adı>* olarak adlandırılacaktır. Geçiş sihirbazı, profil özelliklerinde tetikleme kriteri olarak `UpgradedFromKSWS` cihaz etiketini otomatik olarak seçer. Böylece ilke profilindeki ayarlar sunuculara otomatik olarak uygulanır.

İlkeler ve Görevler Toplu Dönüştürme Sihirbazını kullanarak Kaspersky Endpoint Agent ilkesini taşıma

Kaspersky Endpoint Agent ilkelerini taşımak için İlkeler ve Görevler Toplu Dönüştürme Sihirbazı kullanılabilir. Kaspersky Endpoint Agent için İlke ve Görev Geçiş Sihirbazı yalnızca Web Konsolunda mevcuttur.

Yeni ilkenin özelliklerinde, ilke profillerini etkinleştirmek için etiketleri kullanma

Profil etkinleştirme koşulu olarak daha önce atadığınız cihaz etiketini seçin. İlke özelliklerini açın ve profil etkinleştirme koşulu olarak *İlke profili etkinleştirme için genel kurallar* seçimini yapın.

KSWS yerine KES'i yükleme

KES'i yüklemeden önce, KSWS ilke özelliklerinde Parola korumasını devre dışı bırakmalısınız.

KES'in yüklenmesi şu adımları içerir:

1. Kurulum paketini hazırlayın. Kurulum paketi özelliklerinde Kaspersky Endpoint Security for Windows 12.0 dağıtım kitini ve varsayılan bileşen setini seçin.
2. SQL sunucusu yönetim gruplarından biri için *Uygulamayı uzaktan yükle* görevi oluşturun.
3. Görev özelliklerinde, kurulum paketini ve lisans anahtarı dosyasını seçin.
4. Görev başarıyla tamamlanana kadar bekleyin.
5. Kalan yönetim grupları için KES kurulumunu tekrarlayın.

Kaspersky Security Center, KES yüklemesi tamamlandıktan sonra konsoldaki bilgisayar adlarına otomatik olarak `UpgradedFromKSWS` etiketini ekler.

KES kurulumunu kontrol etmek için *Koruma dağıtımı raporunu* kullanabilirsiniz. Cihaz durumunu da kontrol edebilirsiniz. Uygulama aktivasyonunu onaylamak için *Lisans anahtarı kullanım raporunu* kullanabilirsiniz.

EDR Optimum'u etkinleştirme

EDR Optimum işlevini, bağımsız bir Kaspersky Endpoint Detection and Response Optimum Eklentisi lisansı kullanarak etkinleştirebilirsiniz. EDR Optimum anahtarının Kaspersky Security Center deposuna eklendiğini ve otomatik lisans anahtarı dağıtım işlevinin etkinleştirildiğini onaylamanız gerekir.

EDR Optimum aktivasyonunu kontrol etmek için *Uygulama bileşenlerinin durumu hakkında rapor*'u kullanabilirsiniz.

KES'in çalıştığını doğrulama

KES'in çalıştığını doğrulamak için kontrol gerçekleştirebilir ve herhangi bir hata raporlanmadığını görebilirsiniz. Cihaz durumu *Tamam* olmalıdır. Güncelleme ve kötü amaçlı yazılım tarama görevleri başarıyla tamamlandı.

Sanal makineleri korumak için Light Agent modu

Sürüm 12.8'den itibaren Kaspersky Endpoint Security for Windows'u Kaspersky Security for Virtualization Light Agent'ın bir parçası olarak kullanabilirsiniz. *Kaspersky Security for Virtualization Light Agent*, sanal makinelerin çeşitli bilgi güvenliği tehditlerine, ağ saldırılarına ve kimlik avı saldırılarına karşı kapsamlı bir şekilde korunmasını sağlayan entegre bir çözümdür. Bu çözümü kullanmak için uygulamayı Light Agent modunda yüklemeniz gerekir.

Arm tabanlı sanal makinelerde Kaspersky Endpoint Security'nin Light Agent modunda kurulumu desteklenmemektedir.

Kaspersky Endpoint Security'yi, 6.2 sürümünden itibaren Kaspersky Security for Virtualization Light Agent'ın bir parçası olarak Light Agent modunda kullanabilirsiniz.

Light Agent'ı başlattığınızda, sanal makine SVM (Secure Virtual Machine) ile bir bağlantı kurar ve bu bağlantıyı sürdürür. SVM üzerinde bir Protection Server dağıtılır. *Protection Server*, dosyaları virüslere ve diğer kötü amaçlı yazılımlara karşı tarayan, anti-virüs veritabanlarını güncelleyen ve lisans anahtarlarını yöneten Kaspersky Security for Virtualization Light Agent çözüm bileşenidir. Light Agent, taranması gereken dosyaları veya dosya parçalarını SVM'ye gönderir. Tarama sonuçları Light Agent'ın yüklü olduğu tüm sanal makineler için kullanılabilir (SharedCache teknolojisi). Bu teknoloji çözümün verimliliğini artırır ve tehditlere daha hızlı yanıt verilmesini sağlar.

Kuruluşun altyapısı, Light Agent yüklü birçok sanal makine ve birçok SVM içerebilir. Entegrasyon Sunucusu, sanal makineler ile SVM'ler arasındaki etkileşimi yönetir. *Entegrasyon Sunucusu*, kullanılabilir SVM'lerin listesini oluşturan ve bu verileri Light Agent'lara aktaran, SVM'lerin Light Agent'lar tarafından keşfedilmesine katılan, Light Agent'lar ile SVM'ler arasındaki bağlantıyı koruyan ve diğer işlevleri yerine getiren Kaspersky Security for Virtualization Light Agent çözümünün bir bileşenidir.

Hafif Ajan modu için özel hususlar

Kaspersky Endpoint Security ilkelerini ve görevlerini kullanarak Kaspersky Endpoint Security'yi Standart modda ve Light Agent modunda yönetebilirsiniz. Light Agent modunda uygulamanın bazı bileşenleri ve özellikleri kullanılamaz.

Veritabanlarını ve uygulama yazılım modüllerini güncelleme

Light Agent modundaki Kaspersky Endpoint Security, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak çalışırken uygulamanın ihtiyaç duyduğu özel kötü amaçlı yazılım veritabanlarını kullanır. Kaspersky Endpoint Security, veritabanlarını ve uygulama modülü güncellemelerini Protection Server'dan alır.

Korumalı sanal makinelerdeki veritabanları ve modüller, SVM'deki bir klasörün güncelleme kaynağı olarak belirtildiği özel bir *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi kullanılarak güncellenir. Light Agent, *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini otomatik olarak çalıştırır. Farklı bir güncelleme kaynağı seçemez, görev zamanını yapılandıramaz veya görevi kaldıramazsınız.

En son kötü amaçlı yazılım veritabanı güncellemesinin geri alınması da Protection Server tarafında gerçekleştirilir. SVM'deki veritabanları ve uygulama modülleri güncellemesinin geri alınmasından sonra, korunan sanal makinede özel bir yerel *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevi başlatılır. Bu görev, Light Agent'ın önceki kötü amaçlı yazılım veritabanı setini kullanmaya geri dönmesini sağlar.

Light Agent modundaki Kaspersky Endpoint Security, *Güncellemeyi geri al* görevini desteklemez.

Light Agent'ı etkinleştirme

Uygulamayı etkinleştirmek için Light Agent'ın bağlı olduğu SVM'ye bir lisans anahtarı eklemeniz gerekir. Ayrıca uygulamayı etkinleştirmenize gerek yoktur.

Light Agent modu için diğer özel hususlar

- Uygulama için bir ilke oluştururken, Light Agent modunu seçmenizi öneririz. Bu modda, Yeni İlke Sihirbazı sizden SVM bağlantısını yapılandırmanızı ister. Bu ayarlar uygulamanın Light Agent modunda çalışması için gereklidir.
- Light Agent modunda Veri Şifreleme bileşenlerini ve Uyarlamalı Anomali Denetimi'ni yükleyemezsiniz. Bileşen kümesi ayrıca konuk işletim sisteminin türüne de bağlıdır: iş istasyonu veya sunucu.
- Light Agent, Kaspersky Endpoint Detection and Response Expert ve Kaspersky Endpoint Detection and Response Expert (bulut) çözümleriyle entegrasyonu desteklemez.
- Light Agent'ı Yönetim Konsolu (MMC) ve Kaspersky Security Center Web Console'dan yönetebilirsiniz. Kaspersky Security Center Cloud Console'da Light Agent'ı yönetmek mümkün değildir.
- VDI sanal makinelerindeki uygulama bileşenleri kümesinin değiştirilmesi desteklenmez.
- Kaspersky Endpoint Security, KSN sunucularıyla bir KSN proxy sunucusu aracılığıyla iletişim kurar. KSN ile doğrudan iletişim desteklenmez.
- Kaspersky Security Network'ün bulut modu desteklenmez.
- Entegrasyon Sunucusu (VIIS), Protection Server (SVM) ve KSN sunucularına bağlanırken uygulama proxy sunucusunun kullanılması desteklenmez.

Sanal makinenin ön yapılandırması

Kaspersky Endpoint Security'yi sanal platform teknolojisini kullanan bir sanal makineye yükleyebilirsiniz. Kaspersky Endpoint Security VMware, Microsoft Hyper-V, Citrix sanal platformlarını destekler. Kurulumdan önce, sanal makinelerin ön yapılandırmasını gerçekleştirmelisiniz.

Citrix App Layering teknolojisi ile uyumluluk

Geçici sanal makinelerin durumunu kaydetmek için Full User Layer kullanmayı düşünüyorsanız, sanal makine şablonuna yüklemeden önce şunları yapmanız gerekir:

1. C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt dosyasını oluşturun ve dosyaya aşağıdaki istisnaları ekleyin:
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. İşletim sisteminin kayıt defterinde HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr anahtarında MiniFilterBypass adında yeni bir DWORD değeri oluşturun ve bunu 1 olarak ayarlayın.
3. İşletim sisteminin kayıt defterinde HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd anahtarında ExcludeKey adında yeni bir MULTI_SZ değeri oluşturun ve bunu \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab olarak ayarlayın.
4. Sanal makineyi yeniden başlatın.

Citrix App Layering kullanan bir altyapıdaki sanal makinelere kurulum için aşağıdakileri yapmanız gerekir:

1. Kaspersky Security Center Administration Agent ve Kaspersky Endpoint Security for Windows'u Uygulama Katmanındaki sanal makine şablonuna yükleyin.
2. Birden fazla katmandan oluşan bir sanal makine görüntüsü oluşturun.
3. Oluşturulan görüntüyü Citrix App Layering çözümünü destekleyen hiper yöneticilere dağıtın.
4. Oluşturulan görüntüden geçici sanal makinelerin oluşturulmasını yapılandırın.

Citrix App Layering ile birlikte antivirüs yazılımının yüklenmesi hakkında ayrıntılar için lütfen Citrix App Layering belgelerine bakın.

Citrix Provisioning (Citrix Provisioning Services) teknolojisi ile uyumluluk

Uygulamanın Citrix Provisioning teknolojisi (Citrix Provisioning Services) ile uyumlu olduğundan emin olmak için:

- Sanal makinede Citrix Provisioning Target Device yazılımı yüklüyse, Kaspersky Endpoint Security uygulamasını yüklemeden önce bunu kaldırmanız gerekir (ayrıntılar için lütfen Citrix teknik destek web sitesini ziyaret edin). Uygulamayı yükledikten sonra Citrix Provisioning Target Device'ı tekrar yüklemeniz gerekir. İşletim sisteminin yükseltilmesi de dahil olmak üzere uygulamayı geri yüklerken Citrix Provisioning Target Device'ı da yeniden yüklemeniz gerekir.

İşletim sisteminin yükseltilmesi aşağıdaki adımlardan oluşur:

1. Citrix Provisioning Target Device'ı silin.
2. İşletim sistemini yükseltin.
3. Sanal makineyi başlattıktan sonra Kaspersky Endpoint Security uygulamasının çalışır durumda olduğundan ve düzgün çalıştığından emin olun.
4. Citrix Provisioning Target Device'ı yeniden yükleyin.

- Uygulamayı Kurulum Sihirbazı'nı kullanarak veya Kaspersky Security Center'ı kullanarak uzaktan yüklerken, **Citrix PVS ile uyumluluğu sağla** onay kutusunu işaretlemeniz gerekir.

Omnissa App Volumes teknolojisi ile uyumluluk

Sanal makine şablonuna yüklemeden önce, %SVAgent%\Config\Custom\snapvol.cfg dosyasını oluşturmalı ve aşağıdaki istisnaları eklemelisiniz:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Ayrıntılar için lütfen Omnissa belgelerine başvurun.

Light Agent'ı Yükleme

Arm tabanlı sanal makinelerde Kaspersky Endpoint Security'nin Light Agent modunda kurulumu desteklenmemektedir.

Light Agent modunda uygulamanın yüklenmesi Standart moddakiyle aynıdır. Light Agent'ı bir sanal makineye yüklemeden önce Kaspersky Security Center Network Agent'ın yüklü olduğundan emin olmalısınız. *Ağ Aracısı*, Yönetim Sunucusu ile bir sanal makine arasındaki etkileşimi kolaylaştırır.

Light Agent bir sanal makineye aşağıdaki yollardan biriyle yüklenebilir:

- Kaspersky Security Center kullanarak uzaktan.
- Kurulum Sihirbazını kullanarak yerel olarak.
- Komut satırını kullanarak yerel olarak.

Light Agent'ı yüklemek için yükleme paketi ayarlarında veya Kurulum Sihirbazı sırasında uygun yapılandırmayı seçmelisiniz.

Light Agent'ı bir sunucuya yüklerken, gelişmiş koruma bileşenleri (Davranış Tespiti, Exploit önleme, Düzeltme Altyapısı) uygulamanın varsayılan yapılandırmasından hariç tutulur. Varsayılan uygulama ayarları, önerilen koruma düzeyini ve sunucu kaynaklarının en uygun şekilde kullanılmasını sağlar. Light Agent'ı bir iş istasyonuna yüklerken, gelişmiş koruma bileşenleri uygulamanın varsayılan yapılandırmasına dahil edilir.

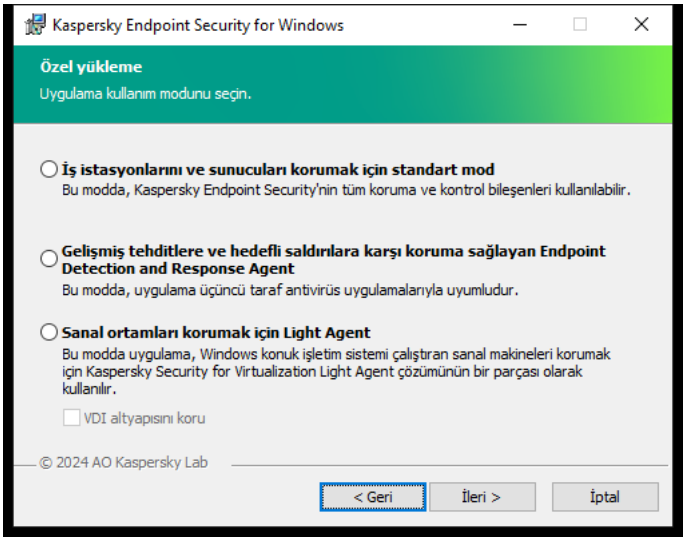
Light Agent'ı yüklerken, ilgili sanal ortam için önceden tanımlanmış istisnaları ve güvenilir uygulamaları seçmenizi öneririz. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar, uygulamayı hızlı bir şekilde kurmanıza ve sanal ortam uyumluluk sorunlarından kaçınmanıza yardımcı olur. Ayrıca ilkede, kurulumdan sonra önceden tanımlanmış tarama istisnalarını ve güvenilir uygulamaları yapılandırabilirsiniz.

Kurulum Sihirbazı kullanılarak Light Agent kurulumu

1. Dağıtım kiti klasörünü sanal makineye kopyalayın.
2. setup_kes.exe dosyasını çalıştırın.

   Kurulum Sihirbazı başlatılır.

Kaspersky Endpoint Security yapılandırması



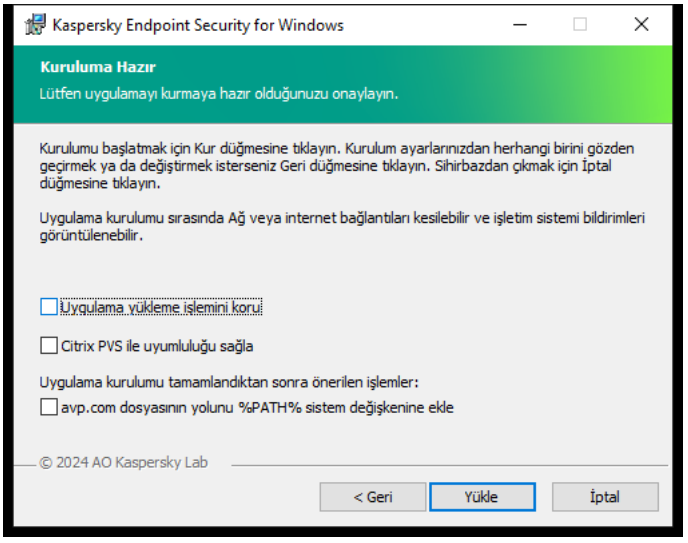
Uygulama yapılandırmasının seçilmesi

Sanal ortamları korumak için Light Agent yapılandırmasını seçin. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.

Kaspersky Endpoint Security bileşenleri

Yüklemek istediğiniz bileşenleri seçin (aşağıdaki şekle bakın). Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz. Bunu yapmak için, Kurulum Sihirbazını tekrar çalıştırmanız ve kullanılabilir bileşenleri değiştirmeyi seçmeniz gerekir.

Gelişmiş ayarlar



Gelişmiş uygulama kurulum ayarları

Uygulama yükleme işlemini koru. Kurulum koruması, dağıtım paketinin zararlı programlarla değiştirilmesine karşı koruma, Kaspersky Endpoint Security yükleme klasörüne erişimi engelleme ve uygulama anahtarlarını içeren sistem kayıt defteri bölümüne erişimi engellemeyi içerir. Ancak, uygulama yüklenemiyorsa (örneğin, Windows Remote Desktop yardımıyla uzaktan yükleme gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız önerilir.

Citrix PVS ile uyumluluğu sağla. Kaspersky Endpoint Security'yi sanal bir makineye yüklemek için Citrix Provisioning Services desteğini etkinleştirebilirsiniz.

avp.com dosyasının yolunu %PATH% sistem değişkenine ekle. Komut satırı arabiriminin uygun kullanımı için kurulum yolunu %PATH% değişkenine ekleyebilirsiniz.

Komut satırını kullanarak Light Agent nasıl yüklenir

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 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
```

veya

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
```

`VDI` seçeneği, VDI (Virtual Desktop Infrastructure) koruma modunu etkinleştirir. VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur. Varsayılan olarak, VDI koruma modu devre dışıdır.

Sonuç olarak, Light Agent sanal makineye varsayılan bileşen kümesiyle yüklenir. setup.ini dosyasını kullanarak bileşen setini düzenleyebilir ve gelişmiş ayarları belirleyebilirsiniz. Kurulum ayarlarını komut satırında da belirleyebilirsiniz.

Light Agent'ı Yönetim Konsolu (MMC) kullanarak yükleme

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacından **Gelişmiş** → **Uzaktan kurulum** → **Kurulum paketleri** klasörünü seçin.

   Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.
3. Kaspersky Endpoint Security for Windows yükleme paketinin özelliklerini açın.

   Gerekirse yeni bir kurulum paketi oluşturun.
4. **Ayarlar** bölümüne gidin.
5. **Sanal ortamları korumak için Light Agent** yapılandırmasını seçin. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.
6. Kurmak istediğiniz bileşenleri seçin.

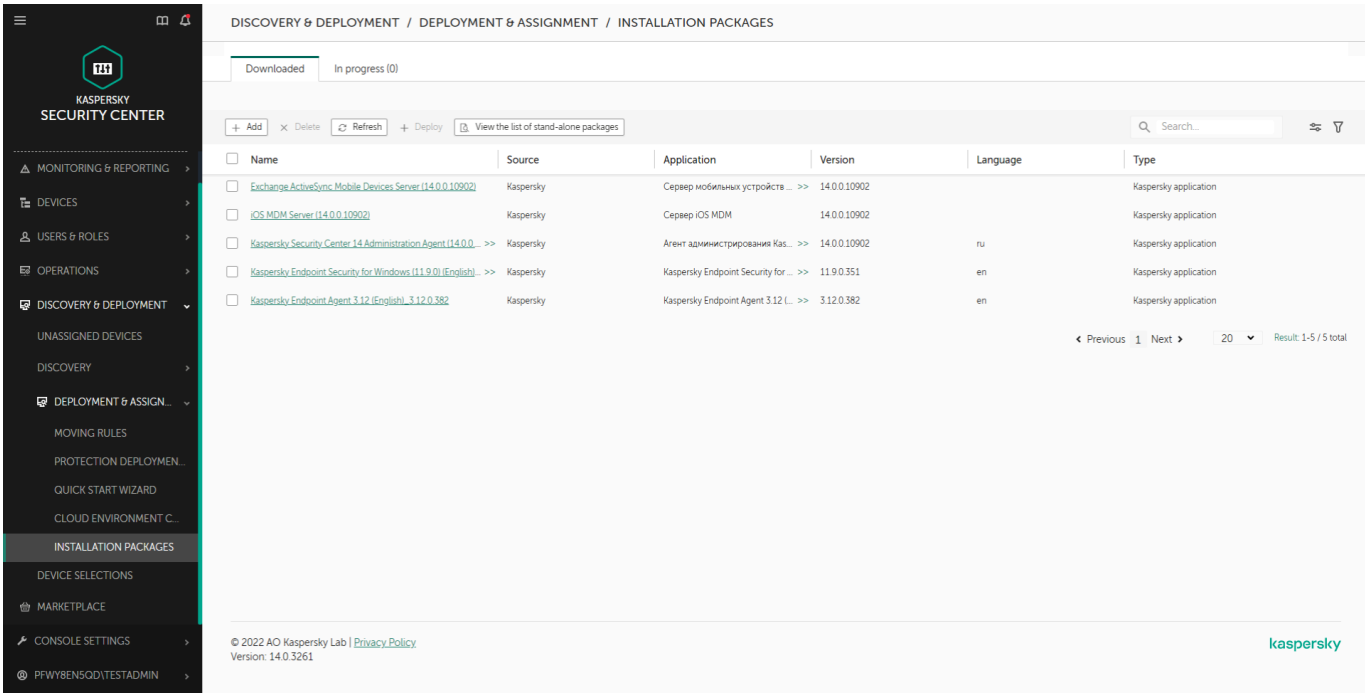
   Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz.
7. Güvenilen bölgeyi yapılandırın. Uygulamayı yüklediğiniz sanal ortam için önceden tanımlanmış tarama istisnalarını ve güvenilir uygulamaları seçin.

   Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar, uygulamayı hızlı bir şekilde kurmanıza ve sanal ortam uyumluluk sorunlarından kaçınmanıza yardımcı olur.
8. Değişikliklerinizi kaydedin.
9. Bir uzaktan kurulum görevi oluşturun. Görev özelliklerinde, oluşturduğunuz yükleme paketini seçin.

Web Console. kullanılarak Light Agent kurulumu

1. Web Console'un ana penceresinden **Keşif ve dağıtım** → **Dağıtım ve atama** → **Kurulum paketleri** seçimini yapın.

Böylece Kaspersky Security Center'dan indirilen kurulum paketlerinin bir listesi açılır.



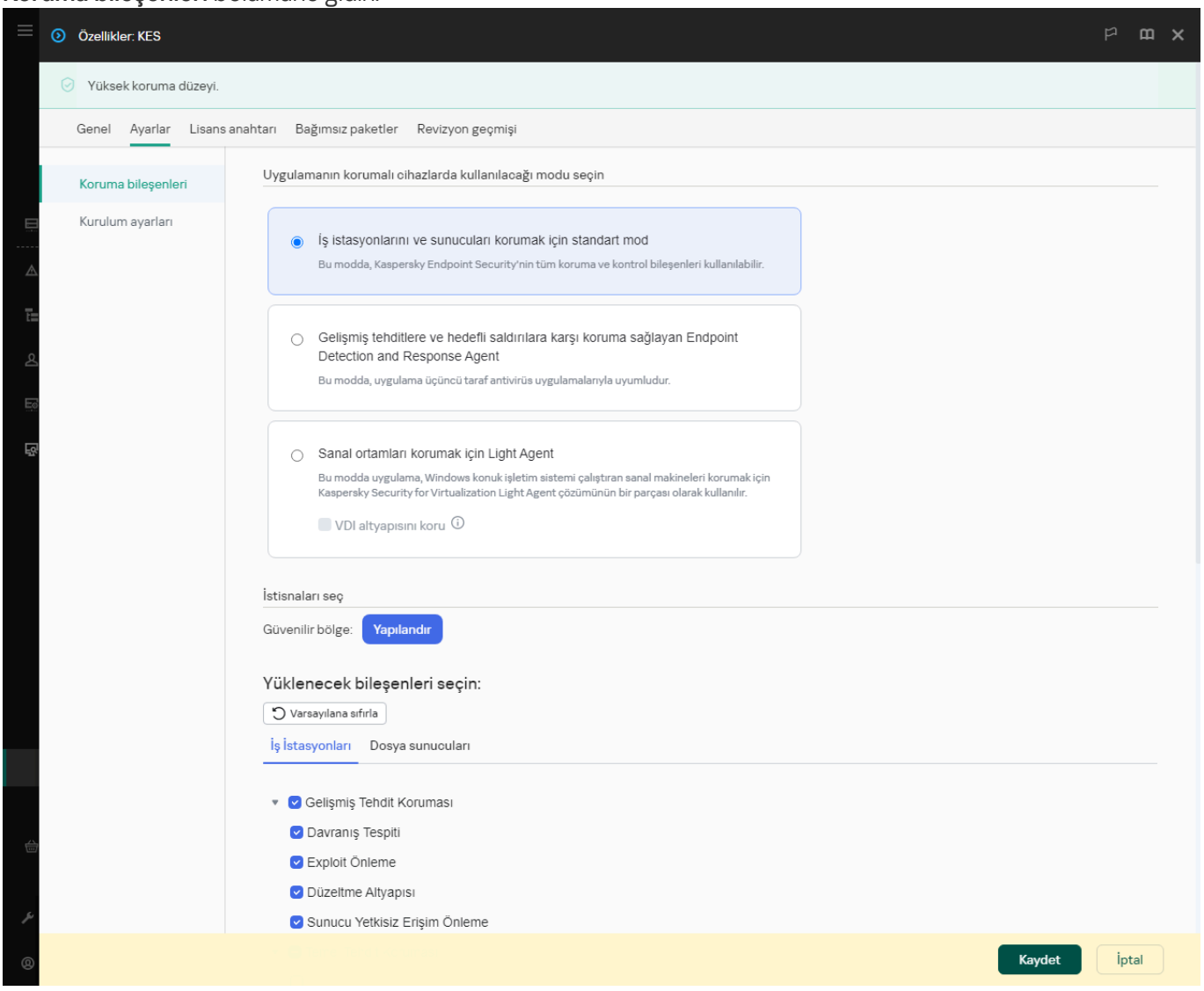
Kurulum paketlerinin listesi

2. Kaspersky Endpoint Security for Windows yükleme paketinin özelliklerini açın.

   Gerekirse yeni bir kurulum paketi oluşturun.

3. **Ayarlar** sekmesini seçin.

4. **Koruma bileşenleri** bölümüne gidin.



Kurulum paketine dahil olan bileşenler

5. **Sanal ortamları korumak için Light Agent** yapılandırmasını seçin. Bu yapılandırma, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılan uygulama için tasarlanmıştır. cLight Agent, çözüm kullanılarak korunması gereken her sanal makineye yüklenmelidir. Bu yapılandırmada Veri Şifreleme bileşenlerini veya Uyarlanabilir Anomali Denetimini kullanamazsınız. Light Agent'ı *kalıcı olmayan sanal makineler* oluşturmak için kullanılacak bir sanal makine şablonuna yüklüyorsanız, **VDI altyapısını koru** onay kutusunu seçin (VDI, Virtual Desktop Infrastructure anlamına gelir). VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. Bu modda, Light Agent sanal makinenin yeniden başlatılmasını gerektiren uygulama güncellemelerini reddeder. Light Agent, yeniden başlatma gerektiren uygulama güncellemeleri alırken, korunan sanal makinelerin şablonunun güncellenmesi gerektiğiyle ilgili bir olay oluşturur.

6. Kurmak istediğiniz bileşenleri seçin.

   Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz.

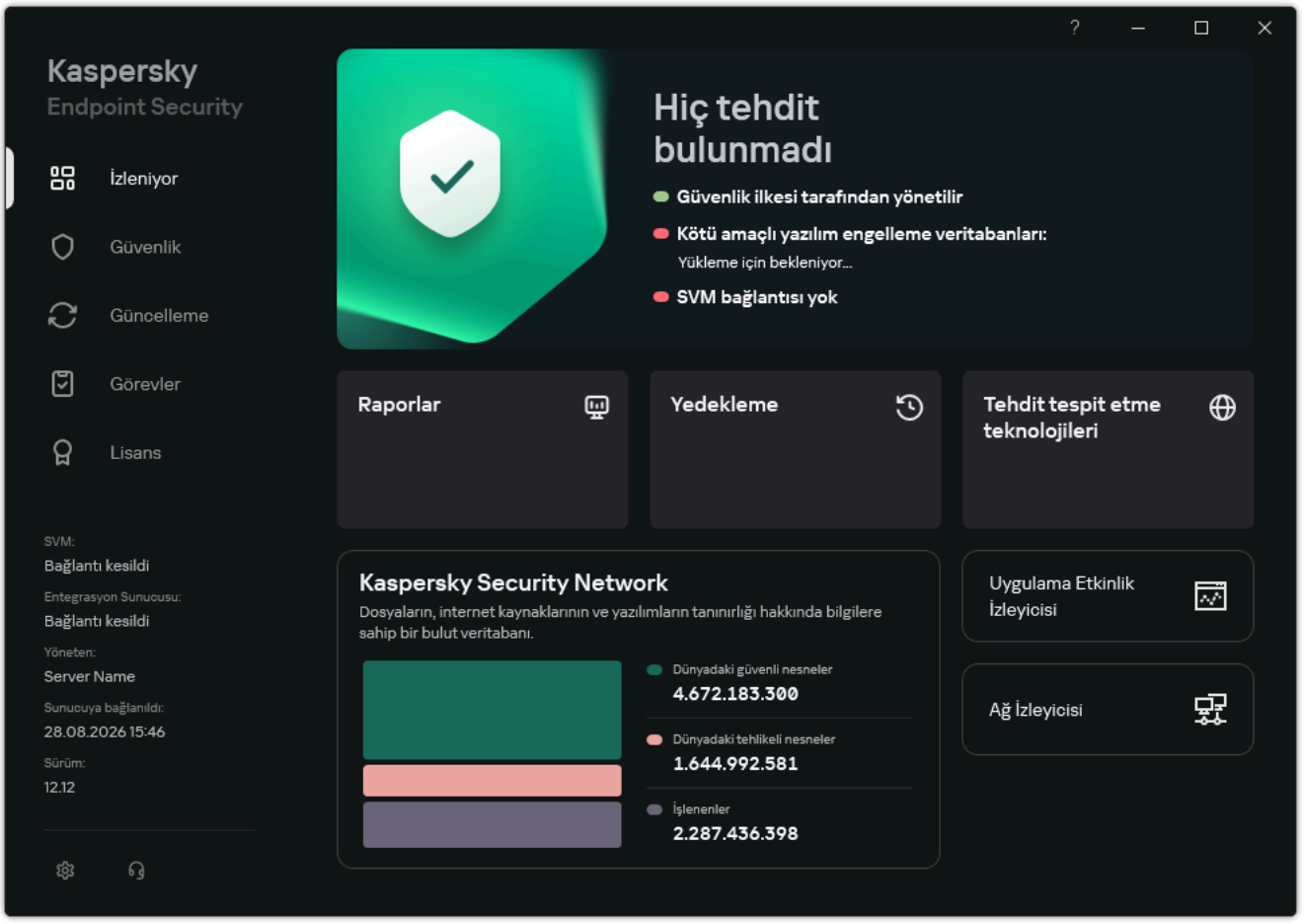
7. Güvenilen bölgeyi yapılandırın. Uygulamayı yüklediğiniz sanal ortam için önceden tanımlanmış tarama istisnalarını ve güvenilir uygulamaları seçin.

   Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar, uygulamayı hızlı bir şekilde kurmanıza ve sanal ortam uyumluluk sorunlarından kaçınmanıza yardımcı olur.

8. Değişikliklerinizi kaydedin.

9. Bir uzaktan kurulum görevi oluşturun. Görev özelliklerinde, oluşturduğunuz yükleme paketini seçin.

Sonuç olarak, Light Agent sanal makineye yüklenir. Uygulamanın arabirimini kullanabilirsiniz, bildirim alanında uygulamanın bir simgesi görüntülenir . Şimdi Light Agent'ın SVM ile bağlantısını yapılandırmanız gerekir.



Light Agent'ın ana penceresi

Light Agent'ı SVM'ye bağlama

Kaspersky Security for Virtualization Light Agent çözümü, Light Agent ve SVM'nin sürekli iletişim halinde olmasını gerektirir. Bu, Light Agent tarafından gönderilen dosyaları virüslere ve diğer kötü amaçlı yazılımlara karşı taramak için gereklidir. SVM bağlantısı olmadan, Light Agent tarama için dosya gönderemez. Bağlantı beş dakikadan uzun süre kurulamazsa tarama bir hata ile sonlandırılır.

Bir Light Agent'ın bir SVM'ye bağlanması şu adımları içerir:

1. Light Agent kullanılabilir SVM'lerin listesini alır.
2. Light Agent, SVM seçim algoritmasına göre bağlantı için en uygun olan kullanılabilir bir Protection Server (SVM) belirler.
3. Light Agent ek SVM bağlantı ayarlarını kontrol eder: etiketler, bağlantı koruma durumu, lisans kapsamındaki uygulama işlevselliği.
4. Light Agent'ı SVM'ye bağlama.

Light Agent'ın SVM'ye olan bağlantısının durumu hakkında Kaspersky Endpoint Security'den veya uygulama komutunu kullanarak bilgi alabilirsiniz. Uygulama, Light Agent'ın SVM bağlantısı kesildiğinde veya kurulduğunda bir olay oluşturur ve bu olayları Kaspersky Security Center'a gönderir. SVM keşfi için bir Entegrasyon Sunucusu kullanıyorsanız, SVM'nin durumu ve bağlı Light Agent'ların sayısı hakkında Entegrasyon Sunucusu Konsolu'ndan bilgi alabilirsiniz. SVM durum izleme hakkında ayrıntılar için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

SVM keşfi

Light Agent için SVM keşfi yöntemlerinden birini seçebilirsiniz:

- Entegrasyon Sunucusunu (VIIS) kullanma.

  Entegrasyon Sunucusu, Kaspersky Security for Virtualization Light Agent'ın sanal altyapıyla etkileşim kurmasını sağlayan ve bağlantı kurulabilecek SVM'lerin listesini oluşturan çözüm bileşenidir. Light Agent, Entegrasyon Sunucusu ile bir bağlantı kurar ve SVM adreslerinin listesini alır.

  Entegrasyon Sunucusu, SVM'ler arasındaki yükü otomatik olarak dengelediği, kullanılabilir SVM'ler hakkında bilgi aldığı, bu bilgileri analiz ettiği ve Light Agent'lara bağlantı için en uygun Koruma Sunucularının (SVM'lerin) listesini sağladığı için özellikle büyük sanal altyapılarda kullanışlıdır.

  Light Agent'ın SVM'lerin bir listesini alabilmesi için, yalnızca Entegrasyon Sunucusunun adresini girmeniz gerekir.

- Entegrasyon Sunucularından oluşan bir yüksek kullanılabilirlik kümesi kullanma.

  Entegrasyon Sunucularından oluşan bir yüksek kullanılabilirlik kümesinin dağıtımı, Kaspersky Security for Virtualization Light Agent 6.4 sürümünden itibaren kullanılabilir. Entegrasyon Sunucularından oluşan yüksek kullanılabilirlik kümesi, birincil Entegrasyon Sunucusu arızalandığında SVM'lerin ve Light Agent'ların yedek Entegrasyon Sunucusuna devredilmesi sayesinde sanal ortamın kesintisiz korunmasını sağlar. Özel bir küme bileşeni olan *yük dengeleyici*, sunucuların yük devretme işleminden sorumludur. Entegrasyon Sunucularından oluşan yüksek kullanılabilirlik kümesi hakkında ayrıntılı bilgi için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

  Light Agent'ın SVM listesini alabilmesi için yük dengeleyicinin yüklü olduğu cihazın adresini girmeniz gerekir.

- SVM adreslerinin listesini kullanarak.

  Light Agent'ın bağlanmasını istediğiniz SVM'leri tek tek belirtmeniz gerekiyorsa, manuel olarak bir liste hazırlayabilirsiniz.

  Light Agent'ın bağlanabileceği kullanılabilir SVM'lerin adreslerini listelemeniz gerekir.

Yönetim Konsolu'nda (MMC) Light Agent tarafından SVM keşfini yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde, **Light Agent modu** → **SVM keşfi ayarları** seçimini yapın.

5. Bir SVM keşfi yöntemi seçin.

   - **Entegrasyon Sunucusunu Kullan**. Altyapınıza bağlı olarak Entegrasyon Sunucusuna bağlantı ayarlarını girin:

     - **Tek Entegrasyon Sunucusu**. Entegrasyon Sunucusu bağlantı ayarlarını girin: cihazın IPv4 adresi veya tam etki alanı adı (FQDN).

     - **Entegrasyon Sunucularından oluşan yüksek kullanılabilirlik kümesi**. Kümenin parçası olan yük dengeleyicinin IP adresini ve bağlantı noktasını girin.

   - **SVM adreslerinin özel bir listesini kullan**. Light Agent'ın bağlanabileceği SVM'lerin bir listesini oluşturun. IPv4 biçiminde IP adresini veya SVM'nin tam etki alanı adını (FQDN) belirtin. Her liste öğesi yeni bir satıra yazılmalı veya önceki öğeden noktalı virgül (**;**) karakteri ile ayrılmalıdır.

     SVM adresleri listesinde, yalnızca tek bir IP adresiyle eşleşen tam etki alanı adlarını (FQDN) belirtin. Birden fazla IP adresine karşılık gelen tam nitelikli bir alan adı kullanmak çözümde hatalara yol açabilir.

6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Web Console'da Light Agent tarafından SVM keşfi yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Light Agent modu** → **SVM keşfi ayarları** seçeneğine gidin.

5. Bir SVM keşfi yöntemi seçin.

   - **Entegrasyon Sunucusunu Kullan**. Altyapınıza bağlı olarak Entegrasyon Sunucusuna bağlantı ayarlarını girin:

     - **Tek Entegrasyon Sunucusu**. Entegrasyon Sunucusu bağlantı ayarlarını girin: cihazın IPv4 adresi veya tam etki alanı adı (FQDN).

     - **Entegrasyon Sunucularından oluşan yüksek kullanılabilirlik kümesi**. Kümenin parçası olan yük dengeleyicinin IP adresini ve bağlantı noktasını girin.

   - **SVM adreslerinin özel bir listesini kullan**. Light Agent'ın bağlanabileceği SVM'lerin bir listesini oluşturun. IPv4 biçiminde IP adresini veya SVM'nin tam etki alanı adını (FQDN) belirtin. Her liste öğesi yeni bir satıra yazılmalı veya önceki öğeden noktalı virgül (**;**) karakteri ile ayrılmalıdır.

     SVM adresleri listesinde, yalnızca tek bir IP adresiyle eşleşen tam etki alanı adlarını (FQDN) belirtin. Birden fazla IP adresine karşılık gelen tam nitelikli bir alan adı kullanmak çözümde hatalara yol açabilir.

6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde Light Agent tarafından SVM keşfi yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Light Agent modu** altında **SVM keşfi ayarları** kutucuğuna tıklayın.
3. Bir SVM keşfi yöntemi seçin.
   - **Entegrasyon Sunucusunu Kullan**. Altyapınıza bağlı olarak Entegrasyon Sunucusuna bağlantı ayarlarını girin:
     - **Tek Entegrasyon Sunucusu**. Entegrasyon Sunucusu bağlantı ayarlarını girin: cihazın IPv4 adresi veya tam etki alanı adı (FQDN).
     - **Entegrasyon Sunucularından oluşan yüksek kullanılabilirlik kümesi**. Kümenin parçası olan yük dengeleyicinin IP adresini ve bağlantı noktasını girin.
   - **SVM adreslerinin özel bir listesini kullan**. Light Agent'ın bağlanabileceği SVM'lerin bir listesini oluşturun. IPv4 biçiminde IP adresini veya SVM'nin tam etki alanı adını (FQDN) belirtin. Her liste öğesi yeni bir satıra yazılmalı veya önceki öğeden noktalı virgül (**;**) karakteri ile ayrılmalıdır.

     SVM adresleri listesinde, yalnızca tek bir IP adresiyle eşleşen tam etki alanı adlarını (FQDN) belirtin. Birden fazla IP adresine karşılık gelen tam nitelikli bir alan adı kullanmak çözümde hatalara yol açabilir.
4. Değişikliklerinizi kaydedin.

Light Agent için SVM seçim algoritmasını yapılandırma

Kuruluşun altyapısı, Light Agent'ların bağlanabileceği birden fazla dağıtılmış SVM'ye sahip olabilir. Sanal altyapının ağ ve kaynakları üzerindeki yükü dengelemek için Light Agent'ları SVM'ler arasında dağıtmanız gerekir.

SVM seçim algoritmaları

Light Agent'lar bağlantı kurmak için şu SVM seçim algoritmalarını kullanabilir: Standart algoritma (varsayılan) ve Genişletilmiş algoritma.

Standart algoritma	Genişletilmiş algoritma
Bu algoritma kullanılırsa, yükleme ve başlatma sonrasında sanal makinedeki Light Agent, Light Agent'a göre *yerel* olan bir SVM'ye bağlanmayı seçer. Bağlantı için uygun yerel SVM bulunamazsa, Light Agent, SVM'nin sanal altyapıdaki konumuna bakılmaksızın, en az sayıda Light Agent'ın bağlı olduğu bir SVM seçer. SVM üzerindeki Protection Server için büyük altyapı koruma modu etkinleştirildiyse uygulama, SVM'nin Light Agent'a göre yerel olup olmadığını belirlemez. Bu durumda, genişletilmiş SVM seçim algoritmasının kullanılması ve SVM bulma yöntemi olarak Entegrasyon Sunucusunun seçilmesi önerilir. Bir SVM'nin Light Agent için yerel kabul edilip edilmemesi sanal altyapının türüne bağlıdır.	Bu algoritma uygulanırsa aşağıdaki SVM seçim ayarlarını tanımlayabilirsiniz: • bağlantı için SVM'leri seçerken altyapıdaki SVM konumunun dikkate alınıp alınmayacağı veya yok sayılıp sayılmayacağı • SVM konumu dikkate alınıyorsa, SVM'nin Light Agent'a göre yerelliğini belirleme yöntemi Light Agent'lar altyapıdaki SVM'lerin konumunu yok sayarsa Light Agent'lar bağlantı için kullanılabilir tüm SVM'lere bağlanabilir. Light Agent'ların altyapıdaki SVM'lerin konumunu dikkate alması gerekiyorsa SVM'nin Light Agent'a göre yerelliği belirlenirken dikkate alınacak SVM yolu türünü seçmeniz gerekir. Bir SVM'nin Light Agent için yerel kabul edilip edilmeyeceği sanal altyapının türüne bağlıdır. Light Agent'lar bağlanacakları SVM'yi seçerken altyapıdaki SVM'lerin konumunu dikkate alırsa, Light Agent'lar yalnızca yerel olan SVM'lere bağlanabilir. Örneğin SVM yolu türü olarak bir hiper yönetici kümesi belirtirseniz, bu hiper yönetici kümesinde dağıtılmış tüm SVM'ler Light Agent için yerel kabul edilir ve Light Agent yalnızca bu SVM'lerden birine bağlanabilir. Light Agent'ın çalıştığı aynı kümede bağlantı için kullanılabilir SVM yoksa Light Agent bir SVM'ye bağlanmaz. SVM'leri seçerken Light Agent'lar, Light Agent'ların bağlantı için kullanılabilir SVM'ler arasında eşit şekilde dağıtılmasını sağlamak için bağlı Light Agent sayısını da dikkate alır. Light Agent genişletilmiş SVM seçim algoritmasını kullanıyorsa, SVM bulma yöntemi SVM adres listesi olarak ayarlanmışsa ve SVM'de büyük altyapı koruma modu etkinleştirilmişse Light Agent'ın bu SVM'ye bağlanması yalnızca SVM yolu yok sayılırsa mümkündür.
Basis Dynamix Enterprise	
Basis Dynamix Enterprise tabanlı bir sanal altyapıda, Light Agent için yerel kabul edilen SVM, Light Agent yüklü sanal makineyle aynı düğümde dağıtılmış olan SVM'dir.	Basis Dynamix Enterprise tabanlı bir sanal altyapıda bir SVM, aşağıdaki durumlardan herhangi birinde Light Agent için yerel kabul edilebilir: • Bir SVM, Light Agent yüklü sanal makineyle aynı düğümde dağıtılmıştır. • Bir SVM, Light Agent yüklü sanal makineyle aynı bölgede dağıtılmıştır. • Bir SVM, Light Agent yüklü sanal makineyle aynı veri merkezinde dağıtılmıştır.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ve Basis Dynamix Standard	
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda, Light Agent için yerel kabul edilen SVM, Light Agent yüklü sanal makineyle aynı hiper yönetici üzerinde dağıtılmış olan SVM'dir.	Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda bir SVM, aşağıdaki durumlardan herhangi birinde Light Agent için yerel kabul edilebilir: • Bir SVM, Light Agent yüklü sanal makineyle aynı hiper yönetici üzerinde dağıtılmıştır. • Bir SVM, Light Agent yüklü sanal makineyle aynı hiper yönetici kümesinde dağıtılmıştır. • Bir SVM, Light Agent yüklü sanal makineyle aynı veri merkezinde dağıtılmıştır.
OpenStack ve VK Private Cloud SVM	

Standart algoritma	Genişletilmiş algoritma
OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda, Entegrasyon Sunucusu yapılandırma dosyası appsettings.json içindeki `HypervisorSpecificSettings:Openstack` bölümünde yer alan `StandardAlgorithmSvmLocality` parametresini kullanarak Light Agent'a göre SVM yerelliğinin nasıl belirleneceğini belirtebilirsiniz. Entegrasyon Sunucusunun sürümüne bağlı olarak dosya aşağıdaki yollardan birinde bulunur: • /var/opt/kaspersky/viis/common/ Linux tabanlı Entegrasyon Sunucusu için • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ Windows tabanlı Entegrasyon Sunucusu için `StandardAlgorithmSvmLocality` parametresi aşağıdaki değerleri alabilir: • `ServerGroup` – bu değer seçilirse SVM, Light Agent yüklü sanal makineyle aynı sunucu grubu içinde bulunuyorsa Light Agent için yerel kabul edilir. Bu değer varsayılan olarak kullanılır. • `Project` – bu değer seçilirse SVM, Light Agent yüklü sanal makineyle aynı OpenStack projesi içinde dağıtılmışsa Light Agent için yerel kabul edilir. • `AvailabilityZone` – bu değer seçilirse SVM, Light Agent yüklü sanal makineyle aynı kullanılabilirlik bölgesi içinde bulunuyorsa Light Agent için yerel kabul edilir.	OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda bir SVM, aşağıdaki durumlardan herhangi birinde Light Agent için yerel kabul edilebilir: • Bir SVM, Light Agent yüklü sanal makineyle aynı sunucu grubunda bulunur. • Bir SVM, Light Agent yüklü sanal makineyle aynı OpenStack projesi içinde dağıtılmıştır. • Bir SVM, Light Agent yüklü sanal makineyle aynı kullanılabilirlik bölgesinde bulunur.

SVM bağlantı algoritmalarına ek olarak, Light Agent'ların SVM'lere bağlantısını etiketler kullanarak düzenleyebilirsiniz.

SVM seçim algoritmasını yapılandırma

Yönetim Konsolu'nda (MMC) Light Agent için SVM seçim algoritmasını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde, **Light Agent modu** → **SVM seçim algoritması** öğesini seçin.
4. Algoritmayı seçin:
   - **Standart SVM seçim algoritmasını kullan**. Light Agent, aynı hiper yöneticide dağıtılmış SVM'leri seçer.
   - **Genişletilmiş SVM seçim algoritmasını kullan**. Light Agent, seçilen SVM yolu türünde (varsayılan olarak **Hiper Yönetici**) dağıtılan SVM'leri seçer.
5. Gerekirse genişletilmiş SVM seçim algoritması için SVM yollarını seçin:
   - **Hiper Yönetici**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):
     - SVM'ler, Light Agent yüklü sanal makineyle aynı hiper yönetici üzerinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).
     - SVM, Light Agent yüklü sanal makineyle aynı sunucu grubunda bulunur (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).
     - SVM, Light Agent yüklü sanal makineyle aynı düğümde bulunur (Basis Dynamix Enterprise sanal altyapısında).

     Light Agent yüklü sanal makinenin bulunduğu aynı hiper yönetici üzerinde veya aynı sunucu grubunda bağlantı için kullanılabilir SVM yoksa Light Agent SVM'ye bağlanmaz.

- **Küme**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):

  - SVM'ler, Light Agent yüklü sanal makineyle aynı hiper yönetici kümesinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).

  - SVM'ler, Light Agent yüklü sanal makineyle aynı OpenStack projesi içinde dağıtılmıştır (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı bölgede bulunur (Basis Dynamix Enterprise sanal altyapısında).

  Light Agent yüklü sanal makinenin bulunduğu aynı hiper yönetici kümesinde veya aynı OpenStack projesi içinde bağlantı için kullanılabilir SVM yoksa Light Agent SVM'ye bağlanmaz.

- **Veri merkezi**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):

  - SVM'ler, Light Agent yüklü sanal makineyle aynı veri merkezinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).

  - SVM'ler, Light Agent yüklü sanal makineyle aynı kullanılabilirlik bölgesinde bulunur (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı veri merkezinde bulunur (Basis Dynamix Enterprise sanal altyapısında).

  Light Agent içeren sanal makinenin bulunduğu aynı veri merkezinde veya Kullanılabilirlik Bölgesinde bağlantı için kullanılabilir SVM yoksa, Light Agent SVM'ye bağlanmaz.

- **Yoksay**. Light Agent, Protection Server'a bağlanmak için SVM yolunu yok sayar. Light Agent'lar diğer kriterleri de dikkate alır: etiketler, bir SVM'ye bağlı Light Agent'ların sayısı vb.

6. Değişikliklerinizi kaydedin.

Web Console'da Light Agent için SVM seçim algoritması yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Light Agent modu** → **SVM seçim algoritması** menüsüne gidin.

5. Algoritmayı seçin:

   - **Standart SVM seçim algoritmasını kullan**. Light Agent, aynı hiper yöneticide dağıtılmış SVM'leri seçer.

   - **Genişletilmiş SVM seçim algoritmasını kullan**. Light Agent, seçilen SVM yolu türünde (varsayılan olarak **Hiper Yönetici**) dağıtılan SVM'leri seçer.

6. Gerekirse genişletilmiş SVM seçim algoritması için SVM yollarını seçin:

- **Hiper Yönetici**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):

  - SVM'ler, Light Agent yüklü sanal makineyle aynı hiper yönetici üzerinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı sunucu grubunda bulunur (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı düğümde bulunur (Basis Dynamix Enterprise sanal altyapısında).

  Light Agent yüklü sanal makinenin bulunduğu aynı hiper yönetici üzerinde veya aynı sunucu grubunda bağlantı için kullanılabilir SVM yoksa Light Agent SVM'ye bağlanmaz.

- **Küme**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):

  - SVM'ler, Light Agent yüklü sanal makineyle aynı hiper yönetici kümesinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).

  - SVM'ler, Light Agent yüklü sanal makineyle aynı OpenStack projesi içinde dağıtılmıştır (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı bölgede bulunur (Basis Dynamix Enterprise sanal altyapısında).

  Light Agent yüklü sanal makinenin bulunduğu aynı hiper yönetici kümesinde veya aynı OpenStack projesi içinde bağlantı için kullanılabilir SVM yoksa Light Agent SVM'ye bağlanmaz.

- **Veri merkezi**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):

  - SVM'ler, Light Agent yüklü sanal makineyle aynı veri merkezinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).

  - SVM'ler, Light Agent yüklü sanal makineyle aynı kullanılabilirlik bölgesinde bulunur (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı veri merkezinde bulunur (Basis Dynamix Enterprise sanal altyapısında).

  Light Agent içeren sanal makinenin bulunduğu aynı veri merkezinde veya Kullanılabilirlik Bölgesinde bağlantı için kullanılabilir SVM yoksa, Light Agent SVM'ye bağlanmaz.

- **Yoksay**. Light Agent, Protection Server'a bağlanmak için SVM yolunu yok sayar. Light Agent'lar diğer kriterleri de dikkate alır: etiketler, bir SVM'ye bağlı Light Agent'ların sayısı vb.

7. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arayüzünde Light Agent için SVM seçim algoritmasını yapılandırma

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Light Agent modu** altında **SVM keşfi ayarları** kutucuğuna tıklayın.
3. Algoritmayı seçin:
   - **Standart SVM seçim algoritmasını kullan**. Light Agent, aynı hiper yöneticide dağıtılmış SVM'leri seçer.
   - **Genişletilmiş SVM seçim algoritmasını kullan**. Light Agent, seçilen SVM yolu türünde (varsayılan olarak **Hiper Yönetici**) dağıtılan SVM'leri seçer.
4. Gerekirse genişletilmiş SVM seçim algoritması için SVM yollarını seçin:
   - **Hiper Yönetici**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):
     - SVM'ler, Light Agent yüklü sanal makineyle aynı hiper yönetici üzerinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).
     - SVM, Light Agent yüklü sanal makineyle aynı sunucu grubunda bulunur (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).
     - SVM, Light Agent yüklü sanal makineyle aynı düğümde bulunur (Basis Dynamix Enterprise sanal altyapısında).

     Light Agent yüklü sanal makinenin bulunduğu aynı hiper yönetici üzerinde veya aynı sunucu grubunda bağlantı için kullanılabilir SVM yoksa Light Agent SVM'ye bağlanmaz.
   - **Küme**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):
     - SVM'ler, Light Agent yüklü sanal makineyle aynı hiper yönetici kümesinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).
     - SVM'ler, Light Agent yüklü sanal makineyle aynı OpenStack projesi içinde dağıtılmıştır (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).
     - SVM, Light Agent yüklü sanal makineyle aynı bölgede bulunur (Basis Dynamix Enterprise sanal altyapısında).

     Light Agent yüklü sanal makinenin bulunduğu aynı hiper yönetici kümesinde veya aynı OpenStack projesi içinde bağlantı için kullanılabilir SVM yoksa Light Agent SVM'ye bağlanmaz.

- **Veri merkezi**. Light Agent, bağlanmak üzere şu kriterleri karşılayan bir SVM seçer (sanal altyapının türüne bağlı olarak):

  - SVM'ler, Light Agent yüklü sanal makineyle aynı veri merkezinde dağıtılmıştır (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer veya Basis Dynamix Standard tabanlı bir sanal altyapıda).

  - SVM'ler, Light Agent yüklü sanal makineyle aynı kullanılabilirlik bölgesinde bulunur (OpenStack veya VK Private Cloud platformunda çalışan bir sanal altyapıda).

  - SVM, Light Agent yüklü sanal makineyle aynı veri merkezinde bulunur (Basis Dynamix Enterprise sanal altyapısında).

  Light Agent içeren sanal makinenin bulunduğu aynı veri merkezinde veya Kullanılabilirlik Bölgesinde bağlantı için kullanılabilir SVM yoksa, Light Agent SVM'ye bağlanmaz.

- **Yoksay**. Light Agent, Protection Server'a bağlanmak için SVM yolunu yok sayar. Light Agent'lar diğer kriterleri de dikkate alır: etiketler, bir SVM'ye bağlı Light Agent'ların sayısı vb.

5. Değişikliklerinizi kaydedin.

Light Agent'ların bağlantılarını SVM'lere dağıtma (etiketler)

Birden fazla Light Agent bir SVM'ye bağlanabilir. Light Agent bağlantılarını dengelemek için ayrı bir SVM listesi belirleyebilirsiniz. SVM keşfi için bir Entegrasyon sunucusu kullanıyorsanız, SVM'lere Light Agent bağlantılarını dengelemek için *etiketleri* kullanabilirsiniz. Yani, bir Light Agent için, bir etiket kullanarak bağlanmak üzere bir SVM listesi atayabilirsiniz. Bunu yapmak için Light Agent'a bir etiket atamanız ve bu etiketi SVM ayarlarında belirtmeniz gerekir. SVM ayarlarında etiket belirleme hakkında ayrıntılar için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

Örnek: Kaspersky Endpoint Detection and Response Optimum çözümü, belirlenen sanal makine ana bilgisayarları için altyapınızda dağıtılır. Bu durumda, EDR Optimum (EDR Optimum Eklentisi) lisans anahtarı eklenmiş SVM'lere bağlanmasını sağlamak için Light Agent'a `[EDROptimum]` etiketini atayabilirsiniz. Sonuç olarak, Light Agent ile sanal makinede EDR Optimum işlevselliğini kullanabilirsiniz. Light Agent'ı EDR Optimum lisans anahtarı olmayan bir SVM'ye bağlarken Kaspersky Endpoint Detection and Response Optimum işlevi kullanılamaz.

Yönetim Konsolu'nda (MMC) bir Light Agent'a SVM bağlantı etiketi atama

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Light Agent modu** → **SVM bağlantı etiketi** öğesini seçin.

4. **Bağlantı etiketini kullan** onay kutusunu seçin ve bir bağlantı etiketi girin.

   Bir etiket için 255 karakter uzunluğuna kadar bir metin girebilirsiniz. `;` karakterleri dışında herhangi bir karakteri kullanabilirsiniz.

5. Değişikliklerinizi kaydedin.

Web Console'da bir Light Agent'a SVM bağlantı etiketi atama

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Light Agent modu** → **SVM bağlantı etiketi** seçeneğine gidin.
5. **Bağlantı etiketini kullan** onay kutusunu seçin ve bir bağlantı etiketi girin.

   Bir etiket için 255 karakter uzunluğuna kadar bir metin girebilirsiniz. `;` karakterleri dışında herhangi bir karakteri kullanabilirsiniz.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde bir Light Agent'a SVM bağlantı etiketi atama

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Light Agent modu** altında **SVM bağlantı etiketi** kutucuğuna tıklayın.
3. **Bağlantı etiketini kullan** onay kutusunu seçin ve bir bağlantı etiketi girin.

   Bir etiket için 255 karakter uzunluğuna kadar bir metin girebilirsiniz. `;` karakterleri dışında herhangi bir karakteri kullanabilirsiniz.
4. Değişikliklerinizi kaydedin.

Light Agent ve SVM arasındaki bağlantının korunması

Light Agent'lar ve Protection Server arasındaki bağlantının şifrelenmesini yapılandırabilirsiniz. Bunu yapmak için, SVM'deki Protection Server ayarlarında ve Light Agent ayarlarında Light Agent ile Protection Server arasındaki veri kanalının şifrelenmesini etkinleştirmeniz gerekir.

Bağlantı korumasının etkin olduğu bir Light Agent, yalnızca Light Agent ile Protection Server arasındaki veri kanalının şifrelemesinin etkin olduğu SVM'lere bağlanabilir. Bağlantı korumasının devre dışı bırakıldığı bir Light Agent, yalnızca kanal şifrelemesinin devre dışı bırakıldığı SVM'lere bağlanabilir veya Protection Server ile Light Agent arasında güvenli olmayan bir bağlantıya izin verilir.

Protection Server'da bağlantı korumasını yapılandırma hakkında ayrıntılar için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

Bağlantının şifreleme kullanılarak korunması, Kaspersky Security for Virtualization Light Agent'ın performansını düşürebilir.

Yönetim Konsolu'nda (MMC) bir Light Agent'ta bağlantı korumasını yapılandırma

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde, **Light Agent modu** → **Bağlantı koruması** seçeneğini kullanın.
4. **Light Agent ve Protection Server arasındaki veri kanalını şifrele** onay kutusunu seçin.
5. Değişikliklerinizi kaydedin.

Web Console'da bir Light Agent'ta bağlantı koruması yapılandırma

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Light Agent modu** → **Bağlantı koruması** seçeneğine gidin.
5. **Light Agent ve Protection Server arasındaki veri kanalını şifrele** onay kutusunu seçin.
6. İlkeyi bilgisayarlara uygulamak için kapatın. Kilit simgesine tıklayın ve değişikliklerinizi kaydedin.

Uygulama arabiriminde bir Light Agent'ta bağlantı koruması yapılandırma

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Light Agent modu** altındaki **Bağlantı koruması** kutucuğuna tıklayın.
3. **Light Agent ve Protection Server arasındaki veri kanalını şifrele** onay kutusunu seçin.
4. Değişikliklerinizi kaydedin.

Light Agent'ı etkinleştirme

Kaspersky Endpoint Security, sanal ortamları korumak için Light Agent modunda kullanılıyorsa uygulamayı ayrıca etkinleştirmeniz gerekmez. Uygulamayı etkinleştirmek için SVM'ye bir lisans anahtarı eklemeniz gerekir. Kaspersky Security Center konsolundaki özel görevi kullanarak SVM'ye bir lisans anahtarı ekleyebilirsiniz. Light Agent arayüzünde lisans anahtarlarını yönetemezsiniz, ancak lisans bilgilerini görüntüleyebilirsiniz (aşağıdaki şekle bakın). Light Agent lisans bilgilerini komut satırından da görüntüleyebilirsiniz (aşağıdaki talimatlara bakın). Light Agent bu bilgiyi SVM'den alır. Çözümü etkinleştirme ve lisans anahtarlarını yönetme hakkında ayrıntılar için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

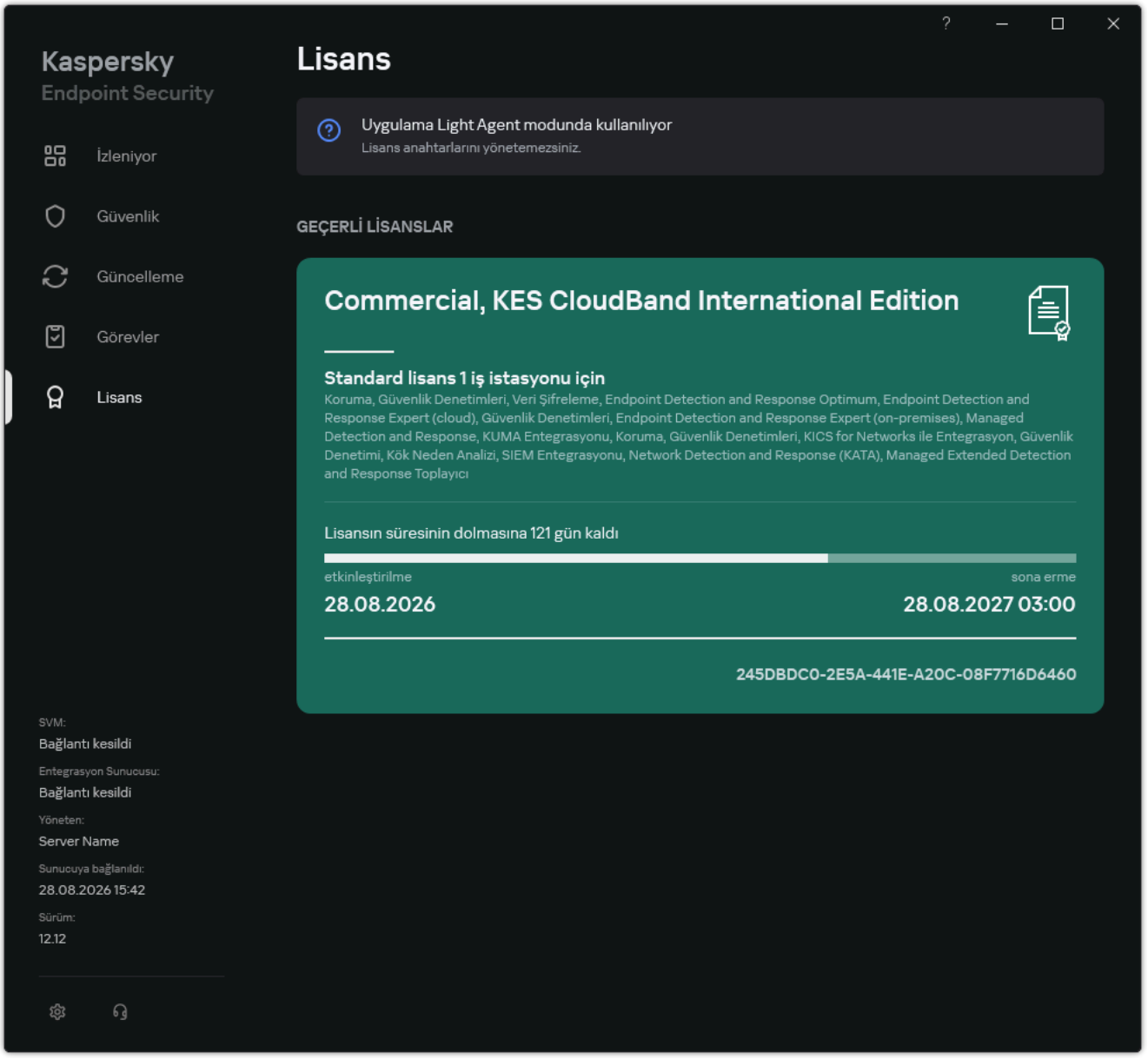
Light Agent lisans bilgilerini görüntülemek için:

1. Komut satırı yorumlayıcısını (cmd) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

3. Aşağıdaki komutu çalıştırın:

```
avp.com LICENSE /CHECK
```

Sonuç olarak, Kaspersky Endpoint Security lisans bilgilerini görüntüler: Light Agent'ın bağlı olduğu SVM'nin adresi, lisansın sona ermesine kalan gün sayısı ve diğer bilgiler. Light Agent'ı etkinleştirirken herhangi bir sorunla karşılaşırsanız lütfen Teknik Destek Bilgi Bankasına bakın.



Lisanslama penceresi

KSVLA Light Agent'tan KES Light Agent'a Geçiş Kılavuzu

Kaspersky Security for Virtualization 5.2 Light Agent, Windows 5.2 için Light Agent bileşenini içerir (bundan sonra "KSVLA Light Agent" olarak da anılacaktır). Kaspersky Security for Virtualization Light Agent 6.2'de, Light Agent bileşeni olarak Light Agent modunda Kaspersky Endpoint Security kullanılır. Çözümü sürüm 6.2'ye güncellemek için KSVLA Light Agent 5.2'den Kaspersky Endpoint Security in Light Agent moduna (bundan sonra "KES Light Agent" olarak da anılacaktır) geçiş yapmanız gerekir. Kaspersky Security for Virtualization Light Agent çözümünün sürümünü güncelleme hakkında ayrıntılar için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

Yazılım gereksinimleri

KSVLA Light Agent'tan KES Light Agent'a geçişe başlamadan önce sanal makinenizin Kaspersky Endpoint Security for Windows'un donanım ve yazılım gereksinimlerini karşıladığından emin olun. Desteklenen işletim sistemi sürümlerinin listesi KES ve KSWS için farklıdır. Örneğin KES, Windows Server 2003 çalıştıran sunucuları desteklemez.

KSVLA Light Agent'tan KES Light Agent'a geçiş için minimum yazılım gereksinimleri:

- Kaspersky Endpoint Security for Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (Koruma Sunucusu ve Entegrasyon Sunucusu bileşenleri dahil).
- Kaspersky Security Center 14.2

  Kaspersky Security Center'ın daha eski bir sürümü kuruluysa, onu 14.2 veya sonraki bir sürüme güncelleyin. Kaspersky Security Center'ın bu sürümünde, İlke ve görevler toplu dönüştürme sihirbazı, ilkeleri bir ilke yerine bir profile taşımanıza olanak tanır. Kaspersky Security Center'ın bu sürümünde, İlke ve görevler toplu dönüştürme sihirbazı, daha geniş bir ilke ayarları yelpazesini taşımanıza da olanak tanır.

Geçiş adımları

KSVLA Light Agent'tan KES Light Agent'a geçiş yarı otomatik olarak gerçekleştirilir. Bu, uygulamaların farklı mimarileri nedeniyle gereklidir.

KSVLA Light Agent'tan KES Light Agent'a aşağıdaki sırayla geçiş yapın:

1. **KSVLA Light Agent görevlerini ve ilkelerini taşıma**

   İlke ayarlarını taşımak için, İlke ve görevler toplu dönüştürme sihirbazını (geçiş sihirbazı) çalıştırmalısınız. İlke ayarlarını geçirdikten sonra, geçiş sihirbazının otomatik olarak geçiremediği ayarları (örneğin, veritabanı güncelleştirme ayarları) manuel olarak yapılandırmanız gerekir. Geçiş sonrasında, geçiş sihirbazının tüm ayarları doğru bir şekilde taşıyıp taşımadığını kontrol etmeniz de önerilir.

   KSVLA Light Agent'a erişimi kısıtlamak için Parola koruması etkinleştirilmişse, KES Light Agent'ı yüklemeden önce, KSVLA Light Agent ilkesinde Parola korumasını devre dışı bırakmanız gerekir. KES Light Agent yükleme paketi ayarlarında kaldırma parolasını giremezsiniz. KSVLA Light Agent'ın üzerine KES Light Agent'ın kurulumunu tamamladıktan sonra, KES ilkesinde Parola korumasını etkinleştirmeniz gerekir.

2. **Kaspersky Endpoint Security'yi Light Agent modunda yükleme**

   KES Light Agent'ı aşağıdaki şekillerde yükleyebilirsiniz:

   - KSVLA Light Agent'ı kaldırdıktan sonra KES Light Agent'ı yükleme (önerilir)
   - KES Light Agent'ı KSVLA Light Agent'ın üzerine yükleme

3. **Geçişten sonra uygulamanın çalışır durumda olduğunu onaylayın**

   KSVLA Light Agent'tan KES Light Agent'a geçiş yaptıktan sonra uygulamanın doğru çalıştığından emin olun. Dönüştürülen politikayı etkinleştirin. Kaspersky Security Center konsolunda sanal makinenin durumunu kontrol edin (*Tamam* olmalıdır). Uygulama için herhangi bir hata rapor edilmediğinden emin olun, ayrıca SVM'ye son bağlantı zamanını ve sanal makine koruma durumunu kontrol edin. Lisans anahtarı SVM'ye eklendiği için Light Agent'ı etkinleştirmeniz gerekmez.

KSVLA Light Agent yerine KES Light Agent'ı yükleme

KES Light Agent'ı aşağıdaki şekillerde yükleyebilirsiniz:

- KSVLA Light Agent'ı kaldırdıktan sonra KES Light Agent'ı yükleme (önerilir)
- KES Light Agent'ı KSVLA Light Agent'ın üzerine yükleme

KSVLA Işık Ajanını Çıkarma

Uygulamayı uzaktan yükle görevini kullanarak uygulamayı uzaktan, sanal makinede yerel olarak veya sanal makine şablonunda kaldırabilirsiniz. KSVLA Light Agent'ı kaldırdıktan sonra sanal makineyi yeniden başlatmanız gerekebilir.

KSVLA Light Agent'ı kaldırdıktan sonra, uygun herhangi bir yöntem kullanarak KES Light Agent'ı yükleyin.

Kaspersky Endpoint Security'yi yükleme

> KSVLA Light Agent'a erişimi kısıtlamak için Parola koruması etkinleştirilmişse, KES Light Agent'ı yüklemeden önce, KSVLA Light Agent ilkesinde Parola korumasını devre dışı bırakmanız gerekir. KES Light Agent yükleme paketi ayarlarında kaldırma parolasını giremezsiniz. KSVLA Light Agent'ın üzerine KES Light Agent'ın kurulumunu tamamladıktan sonra, KES ilkesinde Parola korumasını etkinleştirmeniz gerekir.

Kaspersky Endpoint Security'yi yüklerken, **Sanal ortamları korumak için Light Agent** modunu seçmelisiniz. KES Light Agent'ı bir sanal makineye yüklemeden önce, yükleyici KSVLA Light Agent'ı uyumsuz yazılım olarak algılar ve kaldırır. KSVLA Light Agent yapılandırmasının taşınması desteklenmez. Yani, KES Light Agent'ı yüklediğinizde, yüklenecek bileşen seti yükleme paketi özelliklerinde veya yükleme sihirbazında yaptığınız seçime göre belirlenir. KSVLA Light Agent'ı kaldırdıktan sonra sanal makineyi yeniden başlatmanız gerekir.

KES Light Agent'ı yüklediğinizde KSVLA Light Agent'ın ayarları ve görevleri taşınmaz. Ayarları ve görevleri taşımak için İlke ve Görevler Toplu Dönüştürme Sihirbazı'nı çalıştırın.

Yüklü bileşenlerin listesini uygulama arabiriminin **Güvenlik** bölümünde `status` kodunu kullanarak ya da bilgisayar özelliklerinde Kaspersky Security Center konsolundan kontrol edebilirsiniz. *Uygulama bileşenlerini değiştirmeyi* kullanarak kurulumdan sonra bileşen setini değiştirebilirsiniz.

KSVLA Light Agent ve KES Light Agent bileşenlerinin yazışmaları

KSVLA Light Agent ve KES Light Agent'ın bileşen setleri hemen hemen aynıdır. KES Light Agent, KSVLA Light Agent'tan daha fazla ayara sahiptir. Geçişten sonra yeni ayarlar varsayılan değerlere sahip olur.

KSVLA Light Agent ve KES Light Agent bileşenlerinin yazışmaları

Light Agent 5.2	KES Light Agent
Scan kernel	Uygulama çekirdeği
File Anti-Virus	Dosya Tehdidi Koruması
Mail Anti-Virus	Posta Tehdidi Koruması
Web Anti-Virus	Web Tehdidi Koruması
Firewall	Güvenlik Duvarı
Network Attack Blocker	Ağ Tehdidi Koruması
Application Privilege Control	Sunucu Yetkisiz Erişim Önleme
Applications Launch Control	Uygulama Denetimi
Web Control	İnternet Denetimi
Device Control	Aygıt Denetimi
System Watcher	Kaspersky Endpoint Security'de bu bileşen şu bileşenlere ayrılmıştır: • Exploit Önleme • Davranış Tespiti • Düzeltme Altyapısı
System Integrity Monitoring	Sistem Bütünlüğü İzleme
Integration with Kaspersky Endpoint Agent	*(desteklenmiyor)* Kaspersky Endpoint Security for Windows 11.9.0 sürümünden itibaren Kaspersky Endpoint Agent dağıtım paketi artık dağıtım kitinin bir parçası değildir.
AMSI Protection	AMSI Koruması

KSVLA Light Agent görevlerini ve ilkelerini geçirme

KSVLA Light Agent ilkelerinin ve görevlerinin ayarlarını, İlkeler ve Görevler Toplu Dönüştürme Sihirbazını (bundan böyle "Geçiş Sihirbazı" olarak da anılacaktır) kullanarak geçirebilirsiniz.

KSVLA Light Agent için Geçiş Sihirbazı yalnızca Yönetim Konsolu'nda (MMC) bulunur. İlke ve görev ayarlarının geçişi Web Console ve Cloud Console'da gerçekleştirilemez.

İlkelerin ve görevlerin geçirilmesinde aşağıdaki özel hususlar dikkate alınmalıdır:

- Yeni bir ilke *<İlke> (dönüştürülmüş)* adına sahiptir.
- Yeni ilke *Etkin olmayan ilke* durumundadır.
- Ayarları değiştirme yasağı ("asma kilit") taşınmamıştır. Taşıma Sihirbazı varsayılan değerleri ayarlar.
- İlke profilleri taşınmaz. İlke profillerini manuel olarak eklemeniz gerekir.

- Güvenilir bölge yönetimi iyileştirildi. KSVLA Light Agent'ta, önceden tanımlanmış istisnaları yalnızca bir ilke oluştururken ekleyebilirsiniz. Daha sonra, ilke özelliklerinde daha önce eklenmiş önceden tanımlanmış istisnaları yapılandırabilir veya istisnaları manuel olarak ekleyebilirsiniz. İlke özelliklerine önceden tanımlanmış istisnalar ekleyemezsiniz. KES Light Agent'ta önceden tanımlanmış istisnalar hem ilke oluşturma sırasında hem de oluşturulan ilkelerin özelliklerinde kullanılabilir. Kurulum paketinde önceden tanımlanmış istisnaları da seçebilirsiniz.

- Kaspersky Endpoint Security'deki uygulama kullanıcı arabiriminin yapılandırması yükleyiciden ilkeye taşındı. Örneğin, uygulamanın kullanıcı arabirimini gizlemeniz gerekiyorsa, ilke ayarlarını kullanın.

- Kaspersky Endpoint Security ve KSVLA Light Agent'ta hak tabanlı erişim denetimini (RBAC) yapılandırmaya yönelik işlevsellik kümeleri farklıdır. Fonksiyonel alanlara kullanıcı erişim haklarını sıfırdan yapılandırmanız gerekir.

KSVLA Light Agent ilke ayarlarını taşımak için İlkeler ve Görevler Toplu Dönüştürme Sihirbazını kullanma

1. Yönetim Konsolu'nda, Yönetim Sunucusunu seçin ve içerik menüsünü açmak için sağ tıklayın.

2. **Tüm görevler → İlke ve görevler toplu dönüştürme sihirbazı** seçimini yapın.

   İlkeler ve Görevler Toplu Dönüştürme Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. İlke ve görevlerini dönüştürmeniz gereken uygulamayı seçme

Bu adımda Kaspersky Endpoint Security for Windows'u seçmeniz gerekir. Bir sonraki adıma geçin.

2. Adım. İlkelerin dönüştürülmesi

Dönüştürmek istediğiniz Kaspersky Security for Virtualization 5.2 Light Agent for Windows ilkesini seçin. Bir sonraki adıma geçin.

Geçiş Sihirbazı ilkeleri dönüştürmeye başlayacaktır. Dönüşüm sırasında, Taşıma Sihirbazı KSN Bildirimi koşullarını kabul etmenizi ister. Yeni bir ilke *<İlke> (dönüştürülmüş)* adına sahiptir.

3. Adım. Görevlerin dönüştürülmesi

Geçiş Sihirbazı, Kaspersky Endpoint Security for Windows için yeni görevler oluşturur. Görev listesinden, Kaspersky Endpoint Security için oluşturmak istediğiniz KSVLA Light Agent görevlerini seçin. Yeni görevler *<Görev adı> (dönüştürülmüş)* şeklinde adlandırılır. Bir sonraki adıma geçin.

4. Adım Sihirbazı tamamlama

Sihirbazı tamamlayın.

Bir ilkeyi geçirdikten sonra ilkenin özelliklerini açmanız, ayarlarını kontrol etmeniz ve ilkeyi kaydetmeniz gerekir. Bu adımları tamamlamazsanız, KES Light Agent dönüştürülen ilkeyi yok sayabilir.

Light Agent'ın SVM bağlantı ayarları, istisna listeleri, güvenilen uygulamalar, güvenilir web adresleri, Uygulama Kontrol kurallarının taşınmasına özellikle dikkat edin.

KSVLA Light Agent+KEA] yapılandırmasını [KES Light Agent+yerleşik aracı] yapılandırmasına taşıma

Kaspersky Endpoint Security for Windows'un EDR (KATA), EDR Optimum, Kaspersky Sandbox'ın bir parçası olarak kullanılmasını desteklemek için uygulamaya yerleşik bir aracı eklendi. Bu çözümlerle çalışmak için artık ayrı bir Kaspersky Endpoint Agent uygulamasına ihtiyacınız yok.

KSVLA Light Agent'tan KES Light Agent'a geçiş sırasında EDR (KATA), EDR Optimum, Kaspersky Sandbox çözümleri Kaspersky Endpoint Security yerleşik aracılarıyla çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır.

KSVLA Light Agent'tan KES Light Agent'a geçiş yapmadan önce, Protection Server ve Entegrasyon sunucusu dahil olmak üzere tüm Kaspersky Security for Virtualization bileşenlerini sürüm 6.2'ye güncellemeniz gerekir. Kaspersky Security for Virtualization Light Agent çözümünün sürümünü güncelleme hakkında ayrıntılar için Kaspersky Security for Virtualization Light Agent Yardım içeriğine bakın.

[KSVLA Light Agent+KEA] yapılandırmasını [KES Light Agent+bütünleşik aracı]'ya aktarmak şu adımları içerir:

1. **İlkelerin ve görevlerin taşınması**

   KSVLA Light Agent+KEA] ilke ve görevlerinin [KES Light Agent+yerleşik aracı]'ya taşınması şu adımları içerir:

   1. İlke ve Görevler Toplu Dönüştürme Sihirbazını (yalnızca Yönetim Konsolu'nda (MMC) kullanılabilir) kullanarak ilkeleri ve görevleri KSVLA Light Agent'tan KES Light Agent'a aktarma.

      Sonuç olarak, *<İlke> (dönüştürülmüş)* adıyla yeni bir ilke oluşturulur. Yeni KES görevleri de *<Görev adı> (dönüştürülmüş)* adlarıyla oluşturulur.

   2. Kaspersky Endpoint Agent'tan geçiş sihirbazını kullanarak ilkeleri ve görevleri KEA'dan KES'e aktarma (yalnızca Web Console ve Cloud Console'da mevcuttur).

      Sonuç olarak, *<Kaspersky Endpoint Security ilkesinin adı> ve <Kaspersky Endpoint Agent ilkesinin adı>* adıyla yeni bir ilke oluşturulur. Yeni görevler ve KES görevleri de oluşturulur.

2. **KSVLA Light Agent'tan KES Light Agent'a geçiş**

   KSVLA Light Agent'tan KES Light Agent'a geçiş, KSVLA Light Agent yerine KES Light Agent'ın yüklenmesini içerir.

Yöneticiler genellikle KEA ve KSVLA Light Agent'a erişimi kısıtlamak için Parola korumasını etkinleştirir. KEA kaldırma parolasını yalnızca *Uygulamayı uzaktan yükle* görevinin özelliklerine girebilirsiniz. Geçiş için KSVLA Light Agent için Parola korumasını devre dışı bırakmanız gerekir.

Geçişi gerçekleştirmek için, Kaspersky Endpoint Security'nin bir parçası olarak Algılama ve Yanıt çözümlerini desteklemek için gereken bileşenleri seçmelisiniz. Uygulamayı yükledikten sonra Kaspersky Endpoint Security, bütünleşik aracıyı kullanmaya geçer ve Kaspersky Endpoint Agent'ı kaldırır.

3. **Lisanslama işlevleri**

   Uygulama Light Agent modunda kullanılıyorsa, uygulamayı etkinleştirmeniz gerekmez. Uygulamayı etkinleştirmek için SVM'ye bir lisans anahtarı eklemeniz gerekir. SVM'ye ek işlevleri (örneğin EDR Optimum) etkinleştirmek için lisans anahtarını da eklemeniz gerekir. Yani, geçişin bir parçası olarak işlevsellik lisanslaması otomatik olarak gerçekleşir.

4. **Kaspersky Endpoint Detection and Response Optimum ve Kaspersky Sandbox'ın durumunu kontrol etme**

   Yükseltmeden sonra bilgisayarın Kaspersky Security Center konsolunda *Kritik* durumu görülüyorsa:

   - Bilgisayarda Ağ Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
   - *Uygulama bileşenlerinin durumu hakkında rapor*'u görüntüleyerek yerleşik aracının durumunu denetleyin. Bir bileşenin durumu *Yüklü değil* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin.
   - Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Bildirimi'ni kabul ettiğinizden emin olun.
   - *Uygulama bileşenlerinin durumu hakkında rapor* seçeneğini kullanarak EDR Optimum işlevselliğinin etkinleştirildiğinden emin olun. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, EDR Optimum'un otomatik lisans anahtarı dağıtım işlevinin açık olduğundan emin olun.
   - Sanal makinenin SVM'ye bağlantı durumunu kontrol edin. Light Agent'ın SVM'ye olan bağlantısının durumu hakkında Kaspersky Endpoint Security'den veya uygulama komutunu kullanarak bilgi alabilirsiniz.

Uygulamanın komut satırından yönetimi

Kaspersky Endpoint Security'yi komut satırından yönetebilirsiniz. `avp.com HELP` komutunu çalıştırarak uygulama yönetimi için kullanılabilecek komutların listesini görebilirsiniz. Belirli bir komutun söz dizimi hakkında bilgi almak için `avp.com HELP <command>` komutunu girin.

Komutta özel karakterler atlatılmalıdır. `&`, `|`, `(`, `)`, `<`, `>`, `^` karakterlerini atlamak için `^` kaçış karakterini kullanın (örneğin `&` karakterini kullanmak için `^&` girin). `%` karakterini atlatmak için `%%` girin.

`1` değerinin alternatifleri, `yes`, `on`, `enable`, `enabled` ve `true` seçenekleridir. `0` değerinin alternatifleri, `no`, `off`, `disable`, `disabled` ve `false` seçenekleridir.

Setup. Uygulama yükleniyor

Uygulamanın komut satırından yüklenmesi aşağıdaki adımları içerir:

1. **Dağıtım paketi seçme**

   Kaspersky, farklı yerelleştirmeler için farklı CPU mimarileriyle uyumlu ve çeşitli şifreleme modülleri içeren dağıtım paketleri sunar.

   Dağıtım kiti aşağıdaki dağıtım paketlerini içerir:

   - **AES256**

     Bu dağıtım paketi, x86/x64 mimarisine sahip bilgisayarlara kurulmak üzere tasarlanmıştır. Bu dağıtım paketi, 256 bit etkin anahtar uzunluğuna sahip AES (Advanced Encryption Standard) şifreleme algoritmasını uygulayan şifreleme araçlarını içerir.

   - **AES56**

     Bu dağıtım paketi, x86/x64 mimarisine sahip bilgisayarlara kurulmak üzere tasarlanmıştır. Bu dağıtım paketi, 56 bit etkin anahtar uzunluğuna sahip AES şifreleme algoritmasını kullanan şifreleme araçlarını içerir.

   - **Arm64**

     Bu dağıtım paketi, Arm tabanlı bilgisayarlara kurulmak üzere tasarlanmıştır. Bu dağıtım paketi, sunuculara kurulmak üzere tasarlanmamıştır.

2. **Uygulamanın dağıtım paketini bilgisayarın depolama alanına aktarma**

   Dağıtım paketi, EXE formatında kendiliğinden açılan bir arşivdir. Dağıtım paketinin içeriğini görüntülemek için arşivi ayrı bir klasöre açmanız gerekir. Uygulamayı yüklemek için bases.cab dosyası da dahil olmak üzere dağıtım paketindeki tüm dosyalara ihtiyacınız vardır.

3. **Kurulum komutunu çalıştırma**

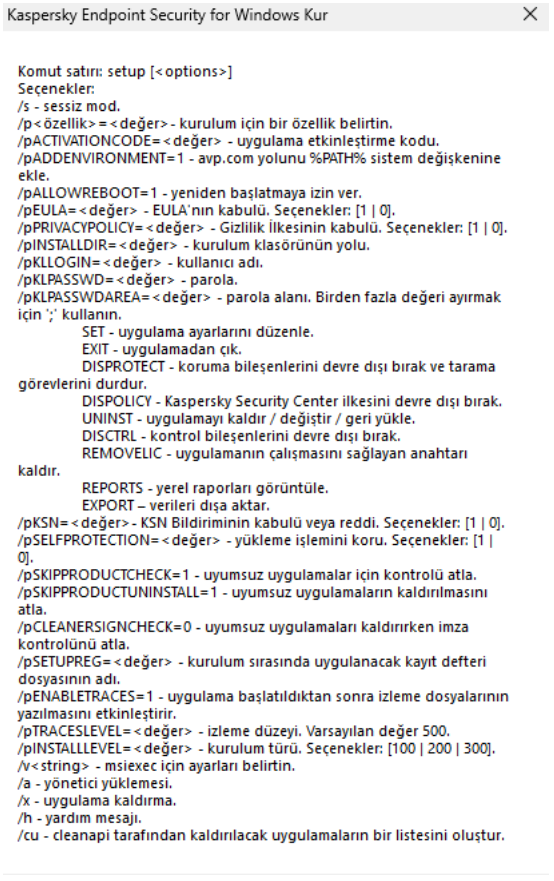
   Kaspersky Endpoint Security, komut satırından aşağıdaki modlardan birinde yüklenebilir:

   - Uygulama Kurulum Sihirbazı'nı kullanarak etkileşimli modda.

   - Sessiz modda. Sessiz modda yüklemenin başlatılmasının ardından yükleme işlemine müdahale etmeniz gerekmez (sessiz kurulum). Sessiz modda uygulamayı yüklemek için `/s` ve `/qn` anahtarlarını kullanın.

Uygulamanın sessiz modda yüklenmesi öncesinde, lütfen Son Kullanıcı Lisans Sözleşmesi'ni ve Gizlilik İlkesi'nin metnini açın ve okuyun. Son Kullanıcı Lisans Sözleşmesi ve Gizlilik İlkesi'nin metni Kaspersky Endpoint Security dağıtım kitinde mevcuttur. Uygulamanın yükleme işlemine ancak Son Kullanıcı Lisans Sözleşmesi'nin hükümlerini ve koşullarını tam olarak okuduysanız, anladıysanız ve kabul ettiyseniz, verilerinizin Gizlilik İlkesi 'ne (üçüncü taraf ülkeler dahil) işleneceğini ve iletileceğini anlıyor ve kabul ediyorsanız ve Gizlilik İlkesi'ni tamamen okuyup anladıysanız devam edebilirsiniz. Son Kullanıcı Lisans Sözleşmesi'nin ve Gizlilik İlkesi'nin hükümlerini ve koşullarını kabul etmiyorsanız lütfen Kaspersky Endpoint Security'yi yüklemeyin ve kullanmayın.

`/h` komutunu çalıştırarak uygulama yüklemesi için kullanılabilecek komutların listesini görebilirsiniz. Kurulum komut sözdizimi hakkında yardım almak için `setup_kes.exe /h` yazın. Sonuç olarak, yükleyici komut seçeneklerinin açıklamasını içeren bir pencere görüntüler (aşağıdaki şekle bakın).



Kurulum komut seçeneklerinin açıklaması

Uygulamayı yüklemek veya uygulamanın önceki bir 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] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

veya

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

Bunun sonucunda uygulama bilgisayara yüklenir. `status` komutunu kullanarak uygulamanın yüklenip yüklenmediğini ve uygulama ayarlarını kontrol edebilirsiniz.

Uygulama kurulum ayarları

`EULA=1`	Son Kullanıcı Lisans Sözleşmesi koşullarının kabulü. 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=1`	Gizlilik İlkesi'nin kabul edilmesi. 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 (KSN) 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.
`CONFIGPATH=<path to the configuration file>`	Uygulamanın önceden tanımlanmış ayarlarla yüklenmesi. Bunu yapmak için Kaspersky Endpoint Security ayarlarını tanımlayan bir dosya yüklemeniz gerekir. Uygulamanın yerel arabiriminde bir yapılandırma dosyası oluşturabilirsiniz.
`ALLOWREBOOT=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.
`SKIPPRODUCTCHECK=1`	Yüklü yazılım kontrolünü devre dışı bırakın. Uyumluluk sorunlarına neden olabilecek yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında yer alır. Bu parametre için herhangi bir değer ayarlanmazsa ve listeden bir yazılım tespit edilirse Kaspersky Endpoint Security kurulumu sonlandırılır.
`SKIPPRODUCTUNINSTALL=1`	Tespit edilen yazılımın incompatible.txt listesinden otomatik olarak kaldırılmasını devre dışı bırakın. Bu parametre için herhangi bir değer ayarlanmazsa Kaspersky Endpoint Security, uyumluluk sorunlarına neden olabilecek yazılımı kaldırmaya çalışır. Kaspersky Endpoint Security, msiexec yükleyicisi kullanılarak yüklendiğinde, yazılımların otomatik olarak kaldırılması etkinleştirilemez. Uyumluluk sorunlarına neden olabilecek yazılımları otomatik olarak kaldırmak için setup_kes.exe dosyasını kullanın.

`CLEANERSIGNCHECK=0|1`	incompatible.txt listesinden tespit edilen yazılım dosyalarının dijital imzalarının doğrulanması. Kaspersky Endpoint Security, yazılımı kaldırmak için yazılım yükleyici dosyasını çalıştırır. Yükleyici dosyasının dijital imzası yoksa Kaspersky Endpoint Security dosyayı güvenilmez olarak değerlendirir ve potansiyel olarak zararlı kodların çalışmasını önlemek için yazılımın kaldırılmasını durdurur. Uygulama, algılanan yazılım dosyasının dijital imzasını doğrulayamazsa Kaspersky Endpoint Security yüklemesi bir hata ile durdurulur. Varsayılan değer, yazılım yükleme yöntemine bağlı olarak farklıdır: • `0` dijital imza doğrulamasının devre dışı olduğu anlamına gelir (Kaspersky Security Center aracılığıyla dağıtıldıysa varsayılan değerdir). • `1` dijital imza doğrulamanın etkinleştirildiği anlamına gelir (uygulama yerel olarak kuruluyorsa varsayılan değerdir).
`STANDALONEMODE=1`	Kaspersky Endpoint Detection and Response (KATA) veya Kaspersky Endpoint Detection and Response Expert (on-premises) çözümleriyle entegrasyon için uygulamayı Endpoint Detection and Response Agent (EDR Agent) yapılandırmasında yükleme. Bu yapılandırma, kuruluşunuzda Kaspersky Endpoint Detection and Response sınıfı çözümünün yanı sıra bir üçüncü taraf Endpoint Protection Platform (EPP) dağıtılmış ise gereklidir. Bu, Endpoint Detection and Response Agent yapılandırmasındaki Kaspersky Endpoint Security'yi üçüncü taraf EPP uygulamalarıyla uyumlu hale getirir.
`KLLOGIN`	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için kullanıcı adını ayarlayın (Parola koruması bileşeni). Kullanıcı adı, `KLPASSWD` ve `KLPASSWDAREA` parametreleriyle birlikte ayarlanır. KLAdmin kullanıcı adı varsayılan olarak kullanılır.
`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 çık. • `DISPROTECT` – Koruma bileşenlerini devre dışı bırakma ve tarama görevlerini durdurma. • `DISPOLICY` – Kaspersky Security Center ilkesini devre dışı bırak. • `UNINST` – Uygulamayı bilgisayardan kaldırma. • `DISCTRL` – Denetim bileşenlerini devre dışı bırakma. • `REMOVELIC` – anahtarın kaldırılması. • `REPORTS` – raporların görüntülenmesi. • `EXPORT` – uygulama ayarlarını dışa aktarma. Örneğin, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`. KLAdmin hesabının, parola korumalı tüm işlemleri gerçekleştirme izni bulunur. Bu nedenle, KLAdmin hesabı için parola alanının yapılandırılması mümkün değildir. KLAdmin hesabı için parola kapsamını yapılandırmaya çalışırsanız, uygulama "Herkes" grubu için belirtilen eylemleri yasaklar.
`PROTECTOSSERVICES`	İşletim sistemi hizmetlerinin işlevselliğinin korunması. İşletim sistemi hizmetleri koruması, üçüncü taraf uygulamaların işletim sistemi hizmetlerinin çalışmasını engellemesini önler. Bu tür hizmetler arasında, örneğin, uygulama otomatik başlatma hizmeti bulunur. • `1` işletim sistemi hizmetlerinin korunmasının etkinleştirildiği anlamına gelir (varsayılan değer). • `0` işletim sistemi hizmetlerinin korunmasının devre dışı olduğu anlamına gelir.
`ENABLETRACES`	Uygulama izlemeyi etkinleştirme veya devre dışı bırakma. Kaspersky Endpoint Security başladıktan sonra, iz dosyalarını `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasörüne kaydeder. Kullanılabilir değerler: • `1` – izleme etkinleştirildi. • `0` – izleme devre dışı bırakıldı (varsayılan değer).
`TRACESLEVEL`	İzlerin ayrıntı düzeyi. Kullanılabilir değerler: • `100` (kritik). Sadece önemli hatalarla ilgili mesajlar. • `200` (yüksek). Önemli hatalar dahil tüm hatalarla ilgili mesajlar. • `300` (tanısal). Tüm hataların yanı sıra uyarılarla ilgili mesajlar. • `400` (önemli). Tüm hata mesajları, uyarılar ve ek bilgiler. • `500` (normal). Tüm hatalar ve uyarıların yanı sıra uygulamanın normal moddaki çalışmasıyla ilgili ayrıntılı bilgiler hakkında mesajlar (varsayılan). • `600` (düşük). Tüm mesajlar.

ENABLEAZURESUPPORT	Azure WVD uyumluluk modunu etkinleştirme veya devre dışı bırakma. Kullanılabilir değerler: • 1 – Azure WVD uyumluluk modu etkinleştirilir. • 0 – Azure WVD uyumluluk modu devre dışı bırakılır (varsayılan değer). Bu özellik, Kaspersky Anti Targeted Attack Platform konsolunda Azure sanal makine durumunun doğru görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensor ID) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensor ID atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensor ID değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir.
AMPPL	AM-PPL teknolojisini (Antimalware Protected Process Light) kullanan Kaspersky Endpoint Security işlemlerinin korumasını etkinleştirir veya devre dışı bırakır. AM-PPL teknolojisi hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin. AM-PPL teknolojisi Windows Server 2019 ve Windows 10 sürüm 1703 (RS2) veya üstü işletim sistemlerinde bulunur. Kullanılabilir değerler: • 1 – AM-PPL teknolojisini kullanan Kaspersky Endpoint Security işlemlerinin koruması etkin. • 0 – AM-PPL teknolojisini kullanan Kaspersky Endpoint Security işlemlerinin koruması devre dışı.
UPGRADEMODE	Uygulama yükseltme modu: • Seamless, uygulamayı bilgisayarı yeniden başlatarak yükseltmek anlamına gelir (varsayılan değer). • Force, uygulamayı yeniden başlatma yapmadan yükseltmek anlamına gelir. 11.10.0 sürümünden itibaren, uygulamayı yeniden başlatma yapmadan yükseltebilirsiniz. Uygulamanın önceki bir sürümünü yükseltmek için bilgisayarı yeniden başlatmanız gerekir. Ayrıca 11.11.0 sürümünden itibaren yamaları yeniden başlatma yapmadan da yükleyebilirsiniz. Kaspersky Endpoint Security'yi yüklerken yeniden başlatma gerekli değildir. Böylece uygulamanın yükseltme modu uygulama ayarlarında belirtilecektir. Bu parametreyi uygulama ayarlarında veya ilkede değiştirebilirsiniz. Önceden yüklenmiş bir uygulamayı yükseltirken, komut satırı parametresinin önceliği, uygulama ayarlarında veya setup.ini dosyasında belirtilen parametrenin önceliğinden daha düşüktür. Örneğin, komut satırında Force güncelleme modu ve uygulama ayarlarında Seamless modu belirtilmişse, yükseltme bilgisayarın yeniden başlatılmasıyla birlikte yüklenir (Seamless).
RESTAPI	REST API aracılığıyla uygulamanın yönetilmesi. Uygulamayı REST API aracılığıyla yönetmek için kullanıcı adı belirlemeniz gerekir (RESTAPI_User parametresi). Kullanılabilir değerler: • 1 – REST API aracılığıyla yönetime izin verilir. • 0 – REST API aracılığıyla yönetim engellenir (varsayılan değer). Uygulamayı REST API aracılığıyla yönetmek için, yönetim sistemleri kullanılarak yönetime izin verilmiş olmalıdır. Bunu yapmak için AdminKitConnector=1 parametre ayarını yapın. Uygulamayı REST API aracılığıyla yönetiyorsanız, uygulamayı Kaspersky yönetim sistemlerini kullanarak yönetmek imkansızdır.
RESTAPI_User	Uygulamanın REST API aracılığıyla yönetilmesi için kullanılan Windows etki alanının kullanıcı adı. Uygulamanın REST API aracılığıyla yönetilmesi izni sadece bu kullanıcıya verilir. Kullanıcı adını şu biçime göre girin <DOMAIN>\<UserName> (örneğin, RESTAPI_User=COMPANY\Administrator). REST API ile çalışmak üzere sadece bir kullanıcı seçebilirsiniz. Bir kullanıcı adı eklemek, uygulamanın REST API aracılığıyla yönetilmesi için bir ön şarttır.
RESTAPI_Port	Uygulamanın REST API aracılığıyla yönetilmesi için kullanılan port. Varsayılan olarak 6782 portu kullanılır. Portun boş olduğundan emin olun.
RESTAPI_Certificate	İstekleri tanımlama için sertifika (örneğin, RESTAPI_Certificate=C:\cert.pem). Kaspersky Endpoint Security'nin REST istemcisiyle güvenli etkileşimi, istek tanımlaması yapılandırılmasını gerektirir. Bunu yapmak için bir sertifika yüklemeniz ve ardından her isteğin yükünü imzalamanız gerekir.
ADMINKITCONNECTOR	Yönetim sistemlerini kullanarak uygulama yönetimi. Yönetim sistemlerine örnek olarak Kaspersky Security Center verilebilir. Kaspersky yönetim sistemlerine ek olarak üçüncü taraf çözümler de kullanabilirsiniz. Kaspersky Endpoint Security bu amaçla bir API sunar. Kullanılabilir değerler: • 1 – yönetim sistemlerinin yardımıyla uygulama yönetimine izin verilir (varsayılan değer). • 0 – uygulama yönetimine sadece yerel arabirim üzerinden izin verilir.

`EnableUniqueSensorID`	Uygulamanın yüklenmesi veya güncellenmesi sırasında benzersiz bir bilgisayar tanımlayıcısı (Sensor ID) oluşturma. Sensor ID, Kaspersky Anti Targeted Attack Platform çözümünde sunucuya telemetri gönderen bilgisayarları tanımlamak için kullanılır. Sensor ID oluşturulurken uygulama, anakart seri numarası gibi bilgisayarın yapılandırmasını dikkate alan bir algoritma kullanır. Bazı durumlarda, örneğin uygulama sanal bir ortamda kullanılırken, Sensor ID çoğaltılabilir. Sonuç olarak, Kaspersky Anti Targeted Attack Platform telemetrinin gönderildiği bilgisayarı tanımlayamaz. Benzersiz bir Sensor ID oluşturmak için `EnableUniqueSensorID=1` parametresini ayarlamanız gerekir. Sonuç olarak, uygulama Sensor ID'yi oluşturmak için bilgisayarla ilgili diğer verileri dikkate alan farklı bir algoritma kullanacaktır. Bu, benzersiz bir Sensor ID sağlar. Varsayılan olarak parametre ayarlanmamıştır. Uygulama, aşağıdaki durumlarda Sensor ID'yi devralır: • uygulama sürümünün güncellenmesi; • [KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi. Uygulama onarımının bir parçası olarak, yükleyici Sensor ID değerini devralmaya çalışır. Sensor ID geri yüklenemiyorsa, uygulama yeni bir Sensor ID oluşturur.
`SKIPKB5007186CHECK=1`	KB5007186 yüklü işletim sistemi güncelleştirmesi için denetimi devre dışı bırakma. Uygulamayı yüklemeden önce, yükleyici yüklü işletim sistemi güncellemelerini kontrol eder. KB5007186 güncellemesi, uygulama için sorunlara neden olabilecek işletim sistemi güncellemeleri listesinde yer alır. Ayrıntılı bilgi için Teknik Destek Bilgi Tabanına bakın. Bu nedenle, bu güncelleme tespit edilirse yükleyici yüklemeyi iptal eder. Kuruluma devam etmek için `SKIPKB5007186CHECK=1` ayarını yapın.

Örnek

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

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

Kaspersky Endpoint Security yüklendikten sonra, setup.ini dosyasında bir etkinleştirme kodu sunmadığınız sürece deneme lisansı etkinleştirilir. Deneme lisansı genellikle kısa sürelidir. Deneme lisansının süresi sona erdiğinde tüm Kaspersky Endpoint Security özellikleri devre dışı bırakılır. Uygulamayı kullanmaya devam etmek için Uygulama Etkinleştirme Sihirbazını ya da özel bir komut kullanarak uygulamayı bir ticari lisans ile etkinleştirmelisiniz.

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

- setup.ini – uygulama yüklemesinin genel ayarları.

  setup.ini dosyasından ayarları uygulamak için bu dosyayı Kaspersky Endpoint Security dağıtım paketini içeren klasöre yerleştirin.

- install.cfg – Kaspersky Endpoint Security işleminin ayarları

  install.cfg yapılandırma dosyasındaki ayarları uygulamak için, şu uygulama yükleme komutunda dosyanın yolunu belirtmeniz gerekir: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – kayıt defteri anahtarı.

  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.reg dosyasından ayarları uygulamak için bu dosyayı Kaspersky Endpoint Security dağıtım paketini içeren klasöre yerleştirin. setup.reg dosyasını farklı bir klasöre de koyabilirsiniz. Bunu yaparsanız, aşağıdaki uygulama yükleme komutunda dosyanın yolunu belirtmeniz gerekir: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Uygulamayı kaldırma

Kaspersky Endpoint Security, komut satırından aşağıdaki modlardan birinde kaldırılabilir:

- Uygulama Kurulum Sihirbazı'nı kullanarak etkileşimli modda.
- Sessiz modda. Sessiz modda kaldırmanın başlatılmasının ardından kaldırma işlemine müdahale etmeniz gerekmez (sessiz kaldırma). Uygulamayı sessiz modda kaldırmak için `/s` ve `/qn` anahtarlarını kullanın.

Uygulamayı sessiz modda kaldırmak için:

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

   - Kaldırma işlemi parola korumalı değilse:

     ```
     setup_kes.exe /s /x
     ```

     veya

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` uygulamanın benzersiz kimliğidir. Teknik Destek Bilgi Bankasını veya aşağıdaki komutu kullanarak uygulamanın GUID'ini bulabilirsiniz:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Kaldırma işlemi parola korumalı ise:

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     veya

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Uygulama tarafından taranan ve Yedekleme'ye yerleştirilen dosyaları kaydetmek için `SAVEQB` parametresini de kullanabilirsiniz. Dosyaların yedek kopyaları, `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasöründe saklanır. Varsayılan olarak, dosyaları Yedeklemeye kaydetme devre dışıdır (`SAVEQB=0`).

Örnek

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Uygulamanın kurtarılması

Kurtarma sırasında uygulama, uygulama yükleme işleminin bir parçası olarak oluşturulan tüm hasarlı uygulama modüllerinin ve sistem kayıt defteri anahtarlarının bütünlüğünü kontrol eder ve geri yükler.

Kaspersky Endpoint Security, aşağıdaki modlardan birinde komut satırından kurtarılabilir:

- Uygulama Kurulum Sihirbazı'nı kullanarak etkileşimli modda.
- Sessiz modda. Kurtarma işlemini sessiz modda başlattıktan sonra, kurtarma işlemine müdahale etmeniz gerekmez.

Kaspersky Endpoint Security yükleyicisi kurtarma modunda çalışıyorsa ve uygulamanın kurtarılması gerekmiyorsa, yükleyici hiçbir değişiklik yapmaz.

Kaspersky Endpoint Security yükleyicisi kurtarma modunda çalışıyorsa ve uygulama yüklenmemişse, yükleyici yükleme işlemini başlatır.

Uygulamayı sessiz modda kurtarmak için:

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

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` uygulamanın benzersiz kimliğidir. Teknik Destek Bilgi Bankasını veya aşağıdaki komutu kullanarak uygulamanın GUID'ini bulabilirsiniz:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Kurtarma işlemi parola korumalı ise:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Örnek

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

AVP komutları

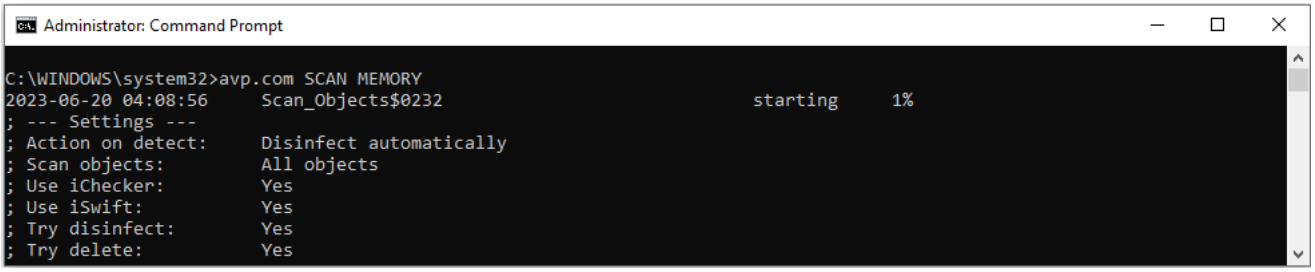
Kaspersky Endpoint Security'yi komut satırından yönetmek için:

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

   Uygulama kurulumu sırasında yürütülebilir dosyanın yolunu %PATH% sistem değişkenine ekleyebilirsiniz.
3. Komutu çalıştırmak için aşağıdaki şablonu kullanın:

```
avp.com <command> [options]
```

Böylece Kaspersky Endpoint Security, komutu yürütecektir (aşağıdaki şekle bakın).



Uygulamanın komut satırından yönetimi

SCAN. Kötü Amaçlı Yazılım Taraması

Kötü Amaçlı Yazılım Taraması görevini çalıştırma.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Tarama kapsamı	
`<files to scan>`	Dosyalar ve klasörlerin boşlukla ayrılmış bir listesi. Uzun yollar çift tırnak işareti içine alınmalıdır. Kısa yolların (MS-DOS biçimi) çift tırnak işareti içine alınmasına gerek yoktur. Örneğin: • `"C:\Program Files (x86)\Example Folder"` – uzun yol. • `C:\PROGRA~2\EXAMPL~1` – kısa yol.

`/ALL`	*Kötü Amaçlı Yazılım Taraması* görevini çalıştır. Kaspersky Endpoint Security aşağıdaki nesneleri tarar: • Çekirdek Belleği • İşletim sistemi açılışında yüklenen nesneler • Önyükleme kesimleri • İşletim sistemi yedekleme • Tüm sabit ve çıkarılabilir sürücüler Kaspersky Endpoint Security for Windows 12.12'de e-posta, uygulama tarama kapsamından çıkarılmıştır. Gelen ve giden e-posta mesajlarının taranması, Posta Tehdit Koruması bileşeni tarafından gerçekleştirilir. Yönetim eklentisinin önceki bir sürümünü kullanıyorsanız, ilke e-postayı içerse bile uygulama e-postayı tarama kapsamı dışında bırakır.
`/MEMORY`	Çekirdek belleği tara
`/STARTUP`	İşletim sistemi başlatılırken yüklenen Nesneleri tara
`/REMDRIVES`	Çıkarılabilir sürücüleri tara.
`/FIXDRIVES`	Sabit sürücüleri tara.
`/NETDRIVES`	Ağ sürücülerini tara.
`/QUARANTINE`	Kaspersky Endpoint Security Yedeklemesindeki dosyaları tara.
`/@:<file list.lst>`	Bir listedeki dosyaları ve klasörleri tara. Listedeki her dosya yeni bir satırda olmalıdır. Uzun yollar çift tırnak işareti içine alınmalıdır. Kısa yolların (MS-DOS biçimi) çift tırnak işareti içine alınmasına gerek yoktur. Örneğin: • `"C:\Program Files (x86)\Example Folder"` – uzun yol. • `C:\PROGRA~2\EXAMPL~1` – kısa yol.

Tehdit algılandığında yapılacak eylem	
`/i0`	**Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
`/i1`	**Temizle; temizleme başarısız olursa bildir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme başarısız olursa Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
`/i2`	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler. Bu eylem varsayılan olarak seçilmiştir.
`/i3`	**Temizleme başarısız olursa sil**. Ayrıca virüslü dosya temizlenemez veya silinemezse birleşik dosyaları da (örneğin, arşivler) sil.
`/i4`	**Sil**. Ayrıca virüslü dosya silinemezse birleşik dosyaları da (örneğin, arşivler) sil.

Dosya türleri	
`/fe`	**Uzantıya göre taranan dosyalar** Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Dosya biçimi daha sonra dosyanın uzantısına göre belirlenir.
`/fi`	**Biçime göre taranan dosyalar**. Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Bir dosyada kötü amaçlı kod taraması yapmadan önce dosyanın iç başlığı, dosyanın biçimini (örneğin, .txt, .doc veya .exe) belirlemek için analiz edilir. Tarama ayrıca belirli dosya uzantılarına sahip dosyaları arar.
`/fa`	**Tüm dosyalar**. Bu ayar etkinleştirilirse uygulama, tüm dosyaları istisnasız (tüm formatları ve uzantıları) olarak kontrol eder. Bu varsayılan ayardır.

Tarama istisnaları	
`-e:a`	RAR, ARJ, ZIP, CAB, LHA, JAR ve ICE arşivleri tarama kapsamında değildir.

`-e:<file mask>`	Dosya maskesiyle eşleşen dosyalar tarama kapsamında değildir. Örneğin: • "`*.exe`" maskesi, exe uzantısı olan tüm dosya yollarını içerir. • `example*` maskesi, EXAMPLE adlı tüm dosya yollarını içerir.
`-e:<seconds>`	Tarama işlemi belirtilen süre sınırını (saniye cinsinden) aşan dosyalar tarama kapsamında değildir.
`-es:<megabytes>`	Boyutları belirtilen boyut sınırını (megabayt cinsinden) aşan dosyalar tarama kapsamında değildir.

Olayları bir rapor dosyası moduna kaydetme (yalnızca Tarama, Güncelleme ve Geri alma profilleri için)	
`/R:<report file>`	Yalnızca önemli olayları rapor dosyasına kaydet.
`/RA:<report file>`	Tüm olayları bir rapor dosyasına kaydet.

Tarama teknolojileri	
`/iChecker=on|off`	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).
`/iSwift=on|off`	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.

Gelişmiş ayarlar	
`/C:<file with scan settings>`	*Kötü Amaçlı Yazılım Taraması* görevi ayarları içeren dosya. Dosya manuel olarak oluşturulmalı ve TXT biçiminde kaydedilmelidir. Dosyada şu içerikler olabilir: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Örnek

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Veritabanlarını ve uygulama yazılım modüllerini güncelleme

Veritabanlarının ve uygulama modüllerinin güncellemesi görevini çalıştırma.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

Komut söz dizimi

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Güncelleme görevi ayarları	
`local`	Uygulama yüklendikten sonra otomatik olarak oluşturulan *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevinin başlatılması. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevinin ayarlarını, yerel uygulama arabiminde veya Kaspersky Security Center konsolunda değiştirebilirsiniz. Bu ayar yapılandırılmazsa Kaspersky Endpoint Security, varsayılan ayarlarla veya komutta belirtilen ayarlarla *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini başlatır. *Veritabanlarının ve uygulama modüllerinin güncellemesi* görev ayarlarını aşağıdaki gibi yapılandırabilirsiniz: • `UPDATE` varsayılan ayarlarla *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini başlatır: güncelleme kaynağı Kaspersky güncelleme sunucularıdır, hesap Sistemdir ve diğer varsayılan ayarlar kullanılır. • `UPDATE local` kurulum sonrasında otomatik olarak oluşturulan *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini (önceden tanımlanmış görev) başlatır. • `UPDATE <update settings>` *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini manuel olarak tanımlanmış ayarlarla başlatır (aşağıya bakınız).

Güncelleme kaynağı	
`"<update source>"`	HTTP veya FTP sunucusunun veya güncelleme paketi içeren paylaşılan klasörün adresi. Sadece bir güncelleme kaynağı belirleyebilirsiniz. Güncelleme kaynağı belirtilmezse, Kaspersky Endpoint Security varsayılan kaynağı, yani Kaspersky güncelleme sunucularını kullanır.

Olayları bir rapor dosyası moduna kaydetme (yalnızca Tarama, Güncelleme ve Geri alma profilleri için)	
`/R:<report file>`	Yalnızca önemli olayları rapor dosyasına kaydet.
`/RA:<report file>`	Tüm olayları bir rapor dosyasına kaydet.

Gelişmiş ayarlar	
`/C:<file with update settings>`	*Veritabanlarının ve uygulama modüllerinin güncellemesi* görev ayarlarına sahip dosya. Dosya manuel olarak oluşturulmalı ve TXT biçiminde kaydedilmelidir. Dosyada şu içerikler olabilir: `["<update source>"] [/R[A]:<report file>]`.

Örnek

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Son güncellemeyi geri alma

Son anti-virüs veritabanı güncellemesini geri alma. 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 sürümüne geri almanıza olanak tanır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

Komut söz dizimi

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Olayları bir rapor dosyası moduna kaydetme (yalnızca Tarama, Güncelleme ve Geri alma profilleri için)	
`/R:<report file>`	Yalnızca önemli olayları rapor dosyasına kaydet.
`/RA:<report file>`	Tüm olayları bir rapor dosyasına kaydet.

Örnek

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. İzleme

İz dosyaları, uygulama kullanımda olduğu sürece bilgisayarda saklanır ve uygulama kaldırıldığında kalıcı olarak silinir. Kimlik Doğrulama Aracısının iz dosyaları hariç iz dosyaları `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasöründe saklanır. Varsayılan olarak izleme devre dışı bırakılmıştır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

İzleme düzeyi	
`<tracing level>`	İzlerin ayrıntı düzeyi. Kullanılabilir değerler: • `100` (kritik). Sadece önemli hatalarla ilgili mesajlar. • `200` (yüksek). Önemli hatalar dahil tüm hatalarla ilgili mesajlar. • `300` (tanısal). Tüm hataların yanı sıra uyarılarla ilgili mesajlar. • `400` (önemli). Tüm hata mesajları, uyarılar ve ek bilgiler. • `500` (normal). Tüm hatalar ve uyarıların yanı sıra uygulamanın normal moddaki çalışmasıyla ilgili ayrıntılı bilgiler hakkında mesajlar (varsayılan). • `600` (düşük). Tüm mesajlar.

Gelişmiş ayarlar	
`all`	Bir komutu `file` and `mem` parametreleri ile çalıştırın.
`file`	Bir izleme dosyasını kaydedin (boyut sınırı yoktur).
`rot`	Boyutları ve sayıları sınırlı dosya kümelerine izleri kaydedin ve maksimum boyuta ulaşıldığında eski dosyaların üzerine yazın.
`mem`	İzleri döküm dosyalarına kaydedin.

Örnek

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Bir profilin başlatılması

Bir profilin başlatılması (örneğin, bir veritabanı güncellemesinin başlatılması veya bir koruma bileşeninin etkinleştirilmesi).

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com START <profile> [/R[A]:<report file>]
```

Profil	
`<profile>`	Profil adı. *Profil* bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Kullanılabilir profillerin listesini `HELP START` komutunu çalıştırarak görebilirsiniz.

Olayları bir rapor dosyası moduna kaydetme (yalnızca Tarama, Güncelleme ve Geri alma profilleri için)	
`/R:<report file>`	Yalnızca önemli olayları rapor dosyasına kaydet.
`/RA:<report file>`	Tüm olayları bir rapor dosyasına kaydet.

Örnek

```
avp.com START Scan_Objects
```

STOP. Profili durdurma

Profil yürütmeyi durdurma (örneğin, Çıkarılabilir Sürücü Taramasını durdurma veya bir koruma bileşenini devre dışı bırakma).

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcı **Koruma bileşenlerini devre dışı bırak** ve **Denetim bileşenlerini devre dışı bırak** izinlerine sahip olmalıdır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Profil adı. *Profil* bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Kullanılabilir profillerin listesini `HELP STOP` komutunu çalıştırarak görebilirsiniz.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

STATUS. Profil durumu

Uygulama profilleri için durum bilgierinin görüntülenmesi (örneğin, `running` veya `completed`). Kullanılabilir profillerin listesini `HELP STATUS` komutunu çalıştırarak görebilirsiniz.

Kaspersky Endpoint Security, servis profillerinin durumu hakkındaki bilgileri de görüntüler. Kaspersky Teknik Destek ile iletişim kurarken servis profillerinin durumu hakkındaki bilgiler gerekebilir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com STATUS [<profile>]
```

Komutu bir profil olmadan girerseniz Kaspersky Endpoint Security, uygulamanın tüm profillerinin durumunu görüntüler.

STATISTICS. Profil işlem istatistikleri

Bir uygulama profili için istatistiklerin görüntülenmesi (örneğin, tarama süresi veya tespit edilen tehditlerin sayısı). Kullanılabilir profillerin listesini `HELP STATISTICS` komutunu çalıştırarak görebilirsiniz.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com STATISTICS <profile>
```

RESTORE. Yedekleme konumundan dosyaları geri yükleme

Bir dosyayı Yedekleme'den orijinal klasörüne geri yükleme. Belirtilen yolda aynı ada sahip bir dosya zaten varsa, uygulama dosyayı değiştirmek için onay isteyecektir. Geri yüklenen dosya orijinal adı değiştirilmeden kopyalanır.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Yedekten geri yükle** izninin olması gerekir.

Yedekleme depoları, temizleme esnasında silinen veya değiştirilen dosyaların yedek kopyalarını saklar. *Yedek kopya*, dosya temizlenmeden veya silinmeden önce oluşturulan bir dosya kopyasıdır. Dosyaların yedekleme kopyaları, özel bir biçimde saklanır ve bir tehdit oluşturmaz.

Dosyaların yedek kopyaları, `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasöründe saklanır.

Yönetici grubundaki kullanıcılara, bu klasör için tam erişim izni verilir. Hesabını Kaspersky Endpoint Security'yi yüklemek için kullanılan kullanıcıya, bu klasör için sınırlı erişim hakkı verilir.

Kaspersky Endpoint Security, dosyaların kopyalarının yedeklenmesine ilişkin kullanıcı erişim izinlerini yapılandırma özelliği sağlamaz.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Gelişmiş ayarlar	
`/REPLACE`	Var olan bir dosyanın üzerine yaz.
`<file name>`	Geri yüklenecek dosyanın adı.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Uygulama ayarlarını dışa aktarma

Kaspersky Endpoint Security ayarlarını bir dosyaya dışa aktarma Komut yalnızca ayarları aktarmak istediğiniz dosyanın adını içeriyorsa, uygulama dosyayı aşağıdaki gibi yerleştirir:

- avp.com yolu %PATH% sistem değişkenine eklenirse, uygulama dosyayı `C:\Windows\SysWOW64` klasörüne yerleştirir.
- Komutu uygulama yükleme klasöründen çalıştırırsanız, uygulamanın kendini koruması uygulama klasöründe yeni bir dosya oluşturulmasını engellediğinden dışa aktarma başarısız olur. Uygulama ayarlarını bir dosyaya aktarmak için dosya yolunu girin.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Ayarları dışa aktar** izninin olması gerekir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Profil adı. *Profil* bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Kullanılabilir profillerin listesini `HELP EXPORT` komutunu çalıştırarak görebilirsiniz.

Dışa aktarılacak dosya	
`<file name>`	Uygulama ayarlarının dışa aktarılacağı dosyanın adı. Dosya yolunu da girebilirsiniz. Kaspersky Endpoint Security ayarlarını DAT veya CFG yapılandırma dosyası, TXT metin dosyası veya XML belgesine dışa aktarabilirsiniz.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Uygulama ayarlarını içe aktarma

Kaspersky Endpoint Security ayarlarını `EXPORT` komutuyla oluşturulan bir dosyadan içe aktarma.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Uygulama ayarlarını yapılandır** izninin olması gerekir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

İçe aktarılacak dosya	
`<file name>`	Uygulama ayarlarının içe aktarılacağı dosyanın adı. Kaspersky Endpoint Security ayarlarını DAT veya CFG yapılandırma dosyası, TXT metin dosyası veya XML belgesinden içe aktarabilirsiniz.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Anahtar dosyasını uygulama

Kaspersky Endpoint Security'yi bir anahtar dosyası kullanarak etkinleştirme. Uygulama zaten etkinleştirilmişse anahtar rezerve anahtar olarak eklenir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

Komut söz dizimi

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Anahtar dosyası	
`<file name>`	Anahtar dosyası adı.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Kullanıcı hesabı kimlik bilgileri. Bu kimlik bilgilerinin yalnızca Parola koruması etkinleştirildiğinde girilmesi gerekir.

Örnek

```
avp.com ADDKEY file.key
```

LICENSE. Lisanslama

Kaspersky Endpoint Security, EDR Optimum veya EDR Expert (Kaspersky Endpoint Detection and Response Eklentisi) lisans anahtarlarını yönetme.

Bu komutu yürütmek ve bir lisans anahtarını kaldırmak için Parola koruması etkinleştirilmelidir. Kullanıcının **Anahtarı kaldır** izninin olması gerekir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

Komut söz dizimi

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

İşlem	
`/ADD <file name>`	Kaspersky Endpoint Security'yi bir anahtar dosyası kullanarak etkinleştirme. Uygulama zaten etkinleştirilmişse anahtar rezerve anahtar olarak eklenir.
`/ADD <activation code>`	Bir etkinleştirme kodu kullanarak Kaspersky Endpoint Security'yi etkinleştirin. Uygulama zaten etkinleştirilmişse anahtar rezerve anahtar olarak eklenir.
`/REFRESH`	Kaspersky Endpoint Security lisansının durumunu güncelleyin. Uygulama, Kaspersky etkinleştirme sunucularından güncel lisans durumu bilgilerini alır.
`/REFRESH <license ID>`	Lisans kimliğini kullanarak lisansların durumunu güncelleyin. Bu komutu kullanarak EDR Eklentisi, MDR Eklentisi, KUMA Eklentisi veya diğer lisansların durumunu güncelleyebilirsiniz. Lisans kimliğini lisans sertifikasından alabilirsiniz. Uygulama, Kaspersky etkinleştirme sunucularından güncel lisans durumu bilgilerini alır.
`/CHECK`	Lisans bilgilerini alın. Kaspersky Endpoint Security, rezerve anahtarlar, EDR Eklentisi, MDR Eklentisi, KUMA Eklentisi anahtarları ve diğer anahtarlar dahil olmak üzere eklenen tüm lisans anahtarları hakkında bilgi görüntüler. Kaspersky Endpoint Security aşağıdaki lisans bilgilerini gösterir: • lisans adı; • lisans tanımlayıcısı; • Uygulamanın Light Agent modunda yüklendiği sanal makinenin bağlı olduğu Protection Server'ın (SVM) adresi; • lisans türü: deneme, ticari, beta, abonelik; • uygulama etkinleştirme tarihi ve saati; • lisansın sona erme tarihi ve saati; • lisansın sona ermesine kalan gün sayısı.
`/CHECK <license ID>`	Kimliğe göre lisans bilgilerini al. Lisans bilgilerini almak için bu komutu kullanabilirsiniz. Lisans kimliğini lisans sertifikasından alabilirsiniz.

`/DEL /login=<user name> /password=<password>`	Uygulamanın lisans anahtarını kaldırın. Rezerve anahtar da kaldırılacaktır.
`/DEL <license ID> /login= <user name> /password= <password>`	Lisans kimliğini kullanarak anahtarı silin. Bu komutu kullanarak EDR Eklentisi, MDR Eklentisi, KUMA Eklentisi veya diğer lisanslardan bir anahtarı silebilirsiniz. Lisans kimliğini lisans sertifikasından alabilirsiniz.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Örnek

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Lisans satın alma

Lisansınızı satın almak veya yenilemek için Kaspersky web sitesini açma.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

PBATESTRESET. Diski şifrelemeden önce disk denetimi sonuçlarını sıfırlama

Hem Kaspersky Disk Encryption hem de BitLocker Drive Encryption teknolojileri dahil olmak üzere Tam Disk Şifreleme (FDE) için uyumluluk denetimi sonuçlarını sıfırlama.

Tam Disk Şifrelemeyi çalıştırmadan önce uygulama, bir dizi kontrol gerçekleştirerek bilgisayarın şifrelenebileceğini doğrular. Bilgisayar Tam Disk Şifrelemeyi desteklemezse, Kaspersky Endpoint Security uyumsuzluk hakkındaki bilgileri günlüğe kaydeder. Sonraki şifreleme denemenizde uygulama bu kontrolü gerçekleştirmez ve şifrelemenin gerçekleştirilemeyeceğini size bildirir. Bilgisayarın donanım yapılandırması değiştirildiyse uygulamanın daha önceden günlüğe kaydettiği uyumluluk kontrolü sonuçları, sistem sabit sürücüsünün Kaspersky Disk Encryption ve BitLocker Drive Encryption teknolojileriyle uyumluluğunun yeniden kontrol edilmesi için sıfırlanmalıdır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

EXIT. Uygulamadan çıkış

Kaspersky Endpoint Security'den çıkış. Uygulama, bilgisayarın RAM'inden kaldırılacaktır.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Uygulamadan çık** izninin olması gerekir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. İlkeyi devre dışı bırakma

Bilgisayardaki Kaspersky Security Center ilkesini devre dışı bırakma. İlkede kapalı bir kilit içeren ayarlar da dahil olmak üzere tüm Kaspersky Endpoint Security ayarları yapılandırılabilir ( ).

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Kaspersky Security Center ilkesini devre dışı bırak** izninin olması gerekir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. İlkeyi etkinleştirme

Bilgisayardaki Kaspersky Security Center ilkesini etkinleştirme. Uygulama ayarları ilkeye göre yapılandırılır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

DISABLE. Korumayı devre dışı bırakma

Kaspersky Endpoint Security lisansı sona eren bir bilgisayardaki Dosya Tehdidi Korumasını devre dışı bırakma. Uygulamanın etkinleştirilmediği ya da geçerli bir lisansa sahip olmayan bir bilgisayarda bu komut çalıştırılamaz.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

SPYWARE. Casus yazılım algılama

Casus yazılım tespitini yönetme. Varsayılan olarak casus yazılım algılama etkindir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com SPYWARE on|off
```

KSN. KSN / KPSN arasında geçiş yapma

Dosyaların veya İnternet sitelerinin tanınırlığını belirlemek için bir Kaspersky çözümü seçme. Kaspersky Endpoint Security, Kaspersky tanınırlık veritabanlarıyla çalışmak için şu altyapı çözümlerini destekler:

- *Kaspersky Security Network (KSN)*, çoğu Kaspersky uygulaması tarafından kullanılan çözümdür. KSN katılımcıları Kaspersky'denbilgiler alır ve kullanıcının bilgisayarında tespit edilen nesneler hakkındaki Kaspersky bilgilerini, Kaspersky analistleri tarafından ek analize tabi tutulması ve tanınırlık ve istatistiksel veritabanlarına dahil edilmesi için gönderir.
- *Kaspersky Private Security Network (KPSN),* Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür. KPSN, aşağıdaki sebeplerden herhangi birinden ötürü Kaspersky Security Network'e katılamayan kurumsal müşteriler için tasarlanmıştır:
  - Yerel iş istasyonları İnternet'e bağlı değildir.
  - Verilerin ülke ya da kurumsal LAN dışına aktarılması yasalarca yasaklanmış ya da kurumsal güvenlik politikaları nedeniyle kısıtlanmıştır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

Komut söz dizimi

```
avp.com KSN /global | /private <file name>
```

Kaspersky Security Network yapılandırma dosyası	
`<file name>`	Kaspersky Private Security Network ayarlarını içeren yapılandırma dosyasının adı. Bu dosya PKCS7 veya PEM uzantısına sahiptir.

Örnek

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Örnek

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Sunucu bağlantı korumasını devre dışı bırakma

Bilgisayarın Yönetim Sunucusu bağlantısındaki parolayı kaldıran *Yönetim Sunucusu bağlantı koruması* görevini çalıştırma. Böylece, görev Yönetim Sunucusu bağlantısının korunmasını devre dışı bırakmış olur.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Parola	
`/password=<password>`	KL Admin kullanıcı hesabının parolası veya *Yönetim Sunucusu bağlantı koruması* görevinden gelen parola. Parametre belirtilmezse Kaspersky Endpoint Security bir sonraki satırda parola girmenizi ister.

KESCLI komutları

KESCLI komutları, OPSWAT bileşeni kullanılarak bilgisayar korumasının durumu hakkında bilgi almanızı ve *Kötü Amaçlı Yazılım Taraması* ve *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevleri gibi standart görevleri gerçekleştirmenizi sağlar.

KESCLI komutlarının listesini `kescli --help` komutunu ya da `kescli -h` kısaltılmış komutunu kullanarak görüntüleyebilirsiniz.

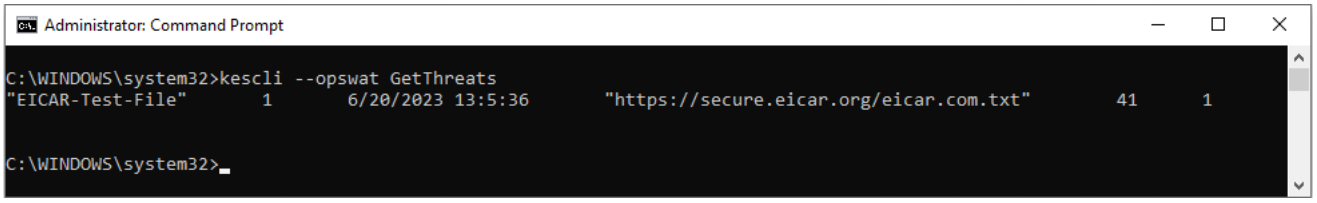
Kaspersky Endpoint Security'yi komut satırından yönetmek için:

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

   Uygulama kurulumu sırasında yürütülebilir dosyanın yolunu %PATH% sistem değişkenine ekleyebilirsiniz.
3. Komutu çalıştırmak için aşağıdaki şablonu kullanın:

   ```
   kescli <komut> [options]
   ```

   Böylece Kaspersky Endpoint Security, komutu yürütecektir (aşağıdaki şekle bakın).



Uygulamanın komut satırından yönetimi

Scan. Kötü Amaçlı Yazılım Taraması

Kötü Amaçlı Yazılım Taraması (Tam Tarama) görevini çalıştırma.

Görevi çalıştırmak için yönetici Yerel görevlerin kullanılmasına izin vermelidir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Kötü Amaçlı Yazılım Taraması görevinin tamamlanma durumunu `GetScanState` komutunu kullanarak kontrol edebilir, `GetLastScanTime` komutunu kullanarak da son taramanın tamamlandığı tarihi ve saati görüntüleyebilirsiniz.

Tarama kapsamı	
`<scan scope>`	`;`-dosyaların ve klasörlerin boşlukla ayrılmış bir listesi. Örneğin, `"C:\Program Files (x86)\Example Folder"`.

Tehdit algılandığında yapılacak eylem	
`0`	**Bilgilendir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
`1`	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler. Bu eylem varsayılan olarak seçilmiştir.

Örnek

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Tarama tamamlanma durumu

Kötü Amaçlı Yazılım Taraması (*Tam Tarama*) görevinin tamamlanma durumu hakkındaki bilgileri görüntüleme:

- `1` – tarama devam ediyor.
- `0` – tarama çalışmıyor.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat GetScanState
```

GetLastScanTime. Taramanın tamamlanma süresinin belirlenmesi

Son *Kötü Amaçlı Yazılım Taraması* (*Tam Tarama*) görevinin tamamlanmasının tarihi ve saati hakkında bilgileri görüntüleme.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat GetLastScanTime
```

GetThreats. Tespit edilen tehditler hakkında veriler alma

Tespit edilen tehditlerin bir listesini görüntüleme (*Tehdit raporu*). Bu rapor, rapor oluşturmadan önceki son 30 gün boyunca gerçekleşen tehditler ve virüs aktivitesi hakkında bilgi içerir.

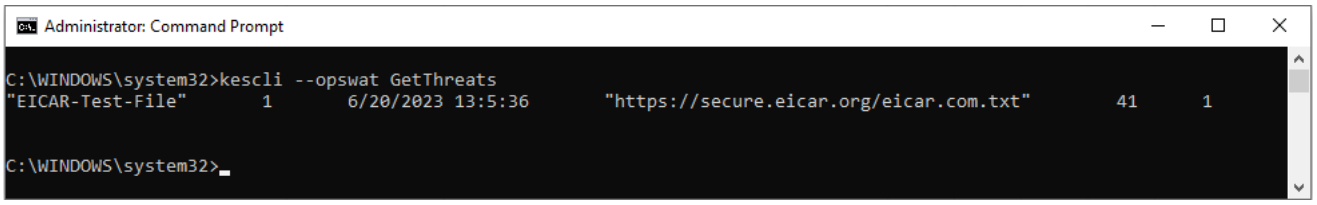
Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat GetThreats
```

Bu komut çalıştırıldığında, Kaspersky Endpoint Security şu biçimde bir yanıt gönderir:

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



Uygulamanın komut satırından yönetimi

Nesne türü	
0	Bilinmiyor (Unknown).
1	Virüsler (Virware).
2	Truva atı programları (Trojware).
3	Kötü amaçlı programlar (Malware).
4	Reklam programları (Adware).
5	Otomatik çevirici programları (Pornware).
6	Bir siber suçlu tarafından kullanıcının bilgisayarına veya verilerine zarar vermek için kullanılabilecek uygulamalar (Riskware).
7	Paketlenme yöntemi kötü amaçlı kodu korumak için kullanılabilecek paketlenmiş nesneler (Packed).
20	Bilinmeyen nesneler (Xfiles).
21	Bilinen uygulamalar (Software).
22	Gizlenmiş dosyalar (Hidden).
23	İlgilenilmesi gereken uygulamalar (Pupware).
24	Kuraldışı davranışlar (Anomaly).
30	Belirlenmemiş (Undetect).
40	Reklam şeritleri (Banner).
50	Ağ saldırısı (Attack).
51	Kayıt defteri erişimi (Registry).
52	Şüpheli etkinlik (Suspicion).
60	Zayıf noktalar (Vulnerability).
70	Kimlik Avı (Phishing).
80	İstenmeyen e-posta eki (Attachment).
90	Kaspersky Security Network tarafından tespit edilen zararlı yazılım (Urgent).
100	Bilinmeyen bağlantı (Suspic URL).
110	Diğer zararlı yazılımlar (Behavioral).

Tehdit algılandığında yapılacak eylem	
`0`	Bilinmiyor (`unknown`).
`1`	Çözümlenen tehditler (`ok`).
`2`	Virüs bulaşmış ancak temizlenmemiş durumdaki nesne (`infected`).
`5`	Bir arşivde yer alan ve temizlenmemiş durumdaki nesne (`archive`).
`9`	Temizlenmiş nesne (`disinfected`).
`10`	Temizlenmemiş nesne (`not disinfected`).
`11`	Silinmiş nesne (`deleted`).
`13`	Nesnenin bir yedek kopyası oluşturuldu (`backupped`).
`15`	Nesne Yedeklemeye taşındı (`quarantined`).
`23`	Nesne bilgisayar yeniden başlatıldığında silindi (`delete on reboot`).
`25`	Nesne bilgisayar yeniden başlatıldığında temizlendi (`disinfect on reboot`).
`29`	Nesne bir kullanıcı tarafından Yedeklemeye taşındı (`added by user`).
`30`	Nesne istisnalara eklendi (`added to exclude`).
`31`	Nesne bilgisyar yeniden başlatıldığında Yedeklemeye taşındı (`quarantine on reboot`).
`36`	Hatalı pozitif (`false alarm`).
`38`	İşlem sonlandırıldı (`terminated`).
`40`	Nesne tespit edilmedi (`not found`).
`41`	Tehdit çözüme kavuşturulamadı (`untreatable`).
`42`	Nesne eski durumuna getirildi (`rolled back`).
`43`	Nesne tehdit etkinliğinin bir sonucu olarak oluşturuldu (`produced by threat`).
`44`	Nesne bilgisayar yeniden başlatıldığında eski durumuna getirildi (`roll back on reboot`).
`0xffffffff`	Nesne işlenmedi (`discarded`).

Tehdit tehlike düzeyi	
`0`	Bilinmiyor
`1`	Yüksek
`2`	Normal tarama
`4`	Düşük
`8`	Bilgiler (*Düşük* üstü)

UpdateDefinitions. Veritabanlarını ve uygulama yazılım modüllerini güncelleme

Veritabanlarının ve uygulama modüllerinin güncellemesi görevini çalıştırma. Kaspersky Endpoint Security varsayılan kaynağı kullanır: Kaspersky güncelleme sunucuları.

Görevi çalıştırmak için yönetici Yerel görevlerin kullanılmasına izin vermelidir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

> Uygulama Light Agent modunda yüklenmişse bu komut çalıştırılamaz.

Komut söz dizimi

```
kescli --opswat UpdateDefinitions
```

`GetDefinitionsetState` komutunu kullanarak geçerli antivirüs veritabanlarının yayınlanma tarihini ve saatini görüntüleyebilirsiniz.

GetDefinitionState. Veritabanlarının son güncellenme tarih ve saatinin belirlenmesi

Kullanılan anti-virüs veritabanlarının son güncelleme tarihi ve saati hakkında bilgi görüntülenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat GetDefinitionState
```

EnableRTP. Koruma etkinleştiriliyor

Bilgisayarda, Kaspersky Endpoint Security güvenlik koruma bileşenlerini etkinleştirme: Dosya Tehdidi Koruması, Web Tehdidi Koruması, Posta Tehdidi Koruması, Ağ Tehdidi Koruması, Sunucu Yetkisiz Erişim Önleme.

> Koruma bileşenlerini etkinleştirmek için yönetici, ilgili ilke ayarlarının değiştirilebildiğinden emin olmalıdır (özellikler açık).

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat EnableRTP
```

Sonuç olarak, uygulama ayarlarının değiştirilmesini Parola koruması ile yasaklamış olsanız bile koruma bileşenleri etkinleştirilir.

Dosya Tehdidi Korumasının çalışma durumunu `GetRealTimeProtectionState` komutu ile kontrol edebilirsiniz.

GetRealTimeProtectionState. Dosya Tehdidi Koruması durumu

Dosya Tehdit Koruması bileşeninin durumu hakkında bilgileri görüntüleme:

- `1` – bileşen etkinleştirilmiş.
- `0` – bileşen devre dışı.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Disk şifreleme durumu

Disk şifreleme durumu hakkındaki bilgileri görüntüleme:

- `1` diskin Kaspersky veya BitLocker disk şifreleme teknolojisi ile korunduğu anlamına gelir.
- `0` diskin şifrelenmediği anlamına gelir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --opswat GetEncryptionState
```

Version. Uygulama sürümünün tanımlanması

Kaspersky Endpoint Security for Windows sürümünü görüntüleme.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.

Komut söz dizimi

```
kescli --Version
```

`-v` kısaltılmış komutunu kullanmanız mümkündür.

Detection and Response komutları

Detection and Response çözümlerinin (örneğin, Kaspersky Sandbox veya Kaspersky Endpoint Detection and Response Optimum) yerleşik işlevlerini yönetmek için komut satırını kullanabilirsiniz. Kaspersky Security Center konsolunu kullanarak yönetim mümkün değilse Detection and Response çözümlerini yönetebilirsiniz. `HELP` komutunu çalıştırarak uygulama yönetimi için kullanılabilecek komutların listesini görebilirsiniz. Belirli bir komutun söz dizimi hakkında bilgi almak için `HELP <command>` komutunu girin.

Komut satırını kullanarak Detection and Response çözümlerinin yerleşik özelliklerini yönetmek için:

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.
3. Komutu çalıştırmak için aşağıdaki şablonu kullanın:

   ```
   avp.com <command> [options]
   ```

   Böylece Kaspersky Endpoint Security, komutu yürütecektir.

SANDBOX. Sandbox'ı Yönetme

Sandbox bileşenini yönetme komutları:

- Sandbox bileşenini etkinleştirme veya devre dışı bırakma.

  Sandbox bileşenleri, Kaspersky Sandbox çözümü ve Kaspersky Anti Targeted Attack Platform'un bir parçası olan KATA Sandbox bileşeni ile etkileşim sağlar.

- Kaspersky Sandbox bileşenini yapılandırma:

  - Bilgisayarı Sandbox sunucularına bağlama.

    Sunucular, taranması gereken nesneleri çalıştırmak için Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini kullanır. Bir IP adresi (IPv4 veya IPv6) veya bir tam etki alanı adı girebilirsiniz. Sanal görüntüleri dağıtma ve Sandbox sunucularını yapılandırma hakkında ayrıntılar için Kaspersky Sandbox Yardım ve Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

  - Sunucusu için bağlantı zaman aşımını yapılandırma.

    Sandbox sunucusu (Kaspersky Sandbox için) veya Central Node sunucusu (KATA için) için bağlantı zaman aşımı. Yapılandırılan zaman aşımı süresi geçtikten sonra Kaspersky Endpoint Security bir sonraki sunucuya bir istek gönderir. Bağlantı hızınız düşükse veya bağlantı dengesizse sunucu için bağlantı zaman aşımını artırabilirsiniz. Önerilen istek zaman aşımı 0,5 saniye veya daha kısadır.

  - Bilgisayar ve sunucuları arasında güvenilir bir bağlantı yapılandırma.

    Sandbox sunucusu (Kaspersky Sandbox için) veya Central Node sunucusu (KATA için) ile güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Daha sonra bir ilke kullanarak sertifikayı bilgisayara eklemeniz gerekir. Ayrıca sertifikayı Sandbox sunucusuna (Kaspersky Sandbox için) veya Central Node sunucusuna (KATA için) eklemeniz gerekir.

- Entegrasyon modunu yapılandırma.

  Sandbox'ın bir parçası olan bir çözüm seçmeniz gerekiyor; yani Kaspersky Sandbox veya KATA Sandbox. *Kaspersky Sandbox*, Kaspersky'nin bağımsız bir Detection and Response çözümüdür. *KATA Sandbox*, Kaspersky Anti Targeted Attack Platform çözümünün bir bileşenidir. KATA Sandbox ile entegre edildiğinde, bileşen aşağıdaki modlarda çalışabilir:

  - **Manuel**. Kullanıcı, bağlam menüsünden dosyayı tarama için manuel olarak gönderir (**Sandbox'a Gönder**).
  - **Otomatik**. Uygulama nesneleri otomatik olarak algılar ve tarama için Sandbox'a gönderir.
  - **Birleştirilmiş**.

- Bileşenin geçerli ayarlarının görüntülenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

İşlem	
`stop`	Sandbox bileşenini devre dışı bırak.
`start`	Sandbox bileşenini etkinleştir.

`set`	Sandbox bileşenini yapılandırın. Şu ayarları yapılandırabilirsiniz:
	• Sandbox sunucuları ekle (`--servers`)
	• Bir TLS sertifikası ekleyin (`--pinned-certificate`)
	• Bir kripto-konteyner ekleme (`--client-certificate`)
	• Kripto konteyner için bir şifre belirleyin (`--client-certificate-password`);
	• Sunucusu bağlantı zaman aşımını ayarla (`--timeout`)
	• Bir entegrasyon modu seçin (`--mode`):
	  • `KSB` – Kaspersky Sandbox ile Entegrasyon;
	  • `KATAManual` – KATA Sandbox ile manuel entegrasyon;
	  • `KATAAuto` – KATA Sandbox ile otomatik entegrasyon;
	  • `KATAFull` – KATA Sandbox ile birleştirilmiş entegrasyon.

`show`	Bileşenin geçerli ayarlarını görüntüleyin. Aşağıdaki yanıtı alırsınız:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. Yürütme önleme yönetimi

Yürütme engelleme bileşeninin devre dışı bırakılması veya yürütme engelleme kuralları listesi de dahil olmak üzere bileşenin geçerli ayarlarının görüntülenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com prevention disable
```

```
avp.com prevention /show
```

`prevention /show` komutunu yürüttükten sonra şu yanıtı alırsınız:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Komut dönüş değerleri:

- `-1`, bilgisayarda yüklü olan Kaspersky sürümü tarafından komutun desteklenmediği anlamına gelir.
- `0`, komutun başarıyla yürütüldüğü anlamına gelir.
- `1`, komuta zorunlu bir bağımsız değişkenin iletilmediği anlamına gelir.
- `2`, genel bir hata oluştuğu anlamına gelir.

- 4, bir sözdizimi hatası olduğu anlamına gelir.
- 9 – yanlış işlem (örneğin, bileşen zaten devre dışıyken devre dışı bırakma girişimi).

ISOLATION. Ağ izolasyonunu yönetme

Bilgisayarın Ağ izolasyonunun devre dışı bırakılması veya bileşenin mevcut ayarlarının görüntülenmesi. Bileşen ayarlarında istisnalara eklenen ağ bağlantılarının bir listesi de yer alır.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

`stat` komutunu çalıştırdığınızda şu yanıt alınır: `Network isolation on|off`.

RESTORE. Dosyaları Karantinadan geri yükleme

Bir dosyayı Karantinadan orijinal klasörüne geri yükleme. *Karantina* bilgisayardaki özel bir yerel depolama alanıdır. Kullanıcı, bilgisayar için tehlikeli olduğunu düşündüğü dosyaları karantinaya alabilir. Karantinaya alınan dosyalar şifrelenmiş bir durumda saklanır ve cihazın güvenliğini tehdit etmez. Kaspersky Endpoint Security, Karantinayı yalnızca Kaspersky Detection and Response çözümleriyle entegre edildiğinde kullanır. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantina'nın yönetimi hakkında ayrıntılar için lütfen Kaspersky Sandbox Yardım, Kaspersky Endpoint Detection and Response Optimum Yardım, Kaspersky Endpoint Detection and Response Expert Yardım, Kaspersky Anti Targeted Attack Platform Yardım ve Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım belgelerine bakın.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Yedekten geri yükle** izninin olması gerekir.

Nesne, sistem hesabı (SYSTEM) altında karantinaya alınır.

Dosyaları Karantinadan geri yüklemek aşağıdaki özel hususları içerir:

- Hedef klasör silinmişse veya kullanıcının bu klasöre erişim hakları yoksa, uygulama dosyayı `%DataRoot%\QB\Restored` klasörüne konumlandırır. Bundan sonra dosyayı manuel olarak hedef klasöre taşımalısınız.
- Uygulama, geri yüklenen dosyanın adını büyük/küçük harfe duyarlı olarak işler. Dosya adını girerken durumu gözlemlemezseniz, uygulama dosyayı geri yüklemez.

- Hedef klasörde zaten aynı ada sahip bir dosya varsa, uygulama dosyanın geri yüklenmesini iptal eder.
- KATA (EDR) çözümünü kullanıyorsanız, uygulama dosyayı geri yükledikten sonra dosyanın bir kopyasını Karantinaya kaydeder. Karantiyanı manuel olarak temizleyebilirsiniz. EDR Optimum ve EDR Expert çözümlerinde, uygulama dosyayı geri yükledikten sonra siler.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Gelişmiş ayarlar	
`/REPLACE`	Var olan bir dosyanın üzerine yaz.
`<file name>`	Geri yüklenecek dosyanın adı.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Komut dönüş değerleri:

- `-1`, bilgisayarda yüklü olan Kaspersky sürümü tarafından komutun desteklenmediği anlamına gelir.
- `0`, komutun başarıyla yürütüldüğü anlamına gelir.
- `1`, komuta zorunlu bir bağımsız değişkenin iletilmediği anlamına gelir.
- `2`, genel bir hata oluştuğu anlamına gelir.
- `4`, bir sözdizimi hatası olduğu anlamına gelir.

IOCSCAN. Güvenlik ihlali göstergeleri (IOC) için tara

IOC Taraması görevini çalıştırma. *Güvenlik İhlali Göstergesi (IOC)* bilgisayara yetkisiz erişimi (verilerin ele geçirilmesi) gösteren bir nesne veya etkinlik hakkında bir dizi veridir. Örneğin, sistemde oturum açmaya yönelik birçok başarısız girişim, bir Güvenlik İhlali Göstergesi oluşturabilir. *IOC Taraması* görevi, bilgisayarda güvenlik ihlali göstergelerini bulmaya ve tehdit yanıtı önlemleri almaya olanak verir.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

IOC Taraması, IOC dosyalarında açıklanan risk göstergeleri ile 128 eşleşmeden sonra iptal edilir. Bu, IOC Taraması görev raporundaki giriş sayısını sınırlandırarak analiz edilmesini kolaylaştırmak ve çok sayıda eşleşme oluşturabilecek kesin olmayan bir şekilde formüle edilmiş risk göstergeleri nedeniyle raporda aşırı doluluk oluşmasını önlemek için gereklidir.

Komut söz dizimi

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off] [/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC dosyaları	
`<full path to the IOC file>`	Tarama için kullanmak istediğiniz IOC dosyasının tam yolu. Boşluklarla ayrılmış birden IOC dosyası belirtebilirsiniz. IOC dosyasının tam yolu, `/path` argümanı olmadan girilmelidir. Örneğin, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Tarama için kullanmak istediğiniz IOC dosyalarının bulunduğu klasörün yolu. *IOC dosyaları*, uygulamanın bir algılamayı saymak için eşleştirmeye çalıştığı gösterge gruplarını içeren dosyalardır. IOC dosyaları OpenIOC standardına uygun olmalıdır. Örneğin, `C:\Users\Admin\Desktop\IOC`

IOC taraması için veri türü	
`/process=on|off`	IOC taramasını gerçekleştirirken işlem verilerini analiz et (ProcessItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security taramayı gerçekleştirirken bilgisayarda çalışan işlemleri analiz etmez. IOC dosyası, ProcessItem IOC belgesinin IOC terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security işlem verilerini ancak, ProcessItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/hint=<full path to the executable file of the process|full path to the file>`	IOC taraması gerçekleştirirken dosya verilerini analiz et (ProcessItem ve FileItem terimleri). Aşağıdaki yöntemlerden biriyle bir dosya seçebilirsiniz: • `<full path to the executable file of the process>` – ProcessItem terimi; • `<full path to the file>` – FileItem terimi.
`/registry=on|off`	Bir IOC taraması gerçekleştirirken Windows kayıt defteri verilerini analiz et (RegistryItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, Windows kayıt defterini taramaz. IOC dosyası, RegistryItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security Windows kayıt defterini ancak, RegistryItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder. RegistryItem veri türü için Kaspersky Endpoint Security bir kayıt defteri anahtarları grubunu tarar.
`/dnsentry=on|off`	IOC taraması gerçekleştirirken yerel DNS önbelleğindeki kayıtlarla ilgili verileri analiz et (DnsEntryItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, yerel DNS önbelleğini taramaz. IOC dosyası, DnsEntryItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security DNS önbelleğini ancak, DnsEntryItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/arpentry=on|off`	IOC taraması gerçekleştirirken ARP tablosundaki kayıtlarla ilgili verileri analiz et (ArpEntryItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, ARP tablosunu taramaz. IOC dosyası, ArpEntryItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security ARP tablosunu ancak, ArpEntryItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.

`/ports=on|off`	IOC taraması gerçekleştirilirken dinleme için açık olan portlar hakkındaki verileri analiz et (PortItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, cihazdaki etkin bağlantılar tablosunu taramaz. IOC dosyası, PortItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security etkin bağlantılar tablosunu ancak, PortItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/services=on|off`	IOC taraması gerçekleştirilirken cihaza yüklenen hizmetlerle ilgili verileri analiz et (ServiceItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, cihaza yüklenen hizmetlerle ilgili verileri taramaz. IOC dosyası, ServiceItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security hizmet verilerini ancak, ServiceItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/system=on|off`	IOC taramasını gerçekleştirirken ortam verilerini analiz et (SystemInfoItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, ortam verilerini analiz etmez. IOC dosyası, SystemInfoItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security ortam verilerini ancak, SystemInfoItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/users=on|off`	IOC taramasını gerçekleştirirken kullanıcılar hakkındaki verileri analiz et (UserItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, sistemde oluşturulan kullanıcılar hakkındaki verileri analiz etmez. IOC dosyası, UserItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security sistemde oluşturulan kullanıcılar hakkındaki verileri ancak UserItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/volumes=on|off`	IOC taramasını gerçekleştirirken birimlerle ilgili verileri analiz et (VolumeItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, cihaza yüklenen birimlerle ilgili verileri taramaz. IOC dosyası, VolumeItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security birim verilerini ancak, VolumeItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/eventlog=on|off`	IOC taraması gerçekleştirirken Windows olay günlüğündeki kayıtlarla ilgili verileri analiz et (EventLogItem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security, Windows olay günlüğündeki kayıtları taramaz. IOC dosyası, EventLogItem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security Windows olay günlüğünü ancak, EventLogItem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder. EventLogItem\source IOC terimi için olayın XML şemasındaki **Sağlayıcı Adı** değerini kullanın.
`/datetime=<event publication date>`	İlgili IOC belgesi için IOC tarama kapsamını belirlerken, olayın Windows olay günlüğünde yayınlandığı tarihi dikkate alın. Bir IOC taraması gerçekleştirirken, Kaspersky Endpoint Security, belirtilen saat ve tarihten görevin çalıştırıldığı zamana kadar geçen süre boyunca yayınlanan Windows olay günlüğü girişlerini tarar. Kaspersky Endpoint Security, bağımsız argümanın değeri olarak olay yayın tarihinin belirtilmesine izin verir. Tarama, yalnızca belirtilen tarihten sonra ve tarama çalıştırılmadan önce Windows olay günlüğünde yayınlanan olaylar için gerçekleştirilir. Argüman belirtilmediği takdirde, Kaspersky Endpoint Security olayları yayın tarihinden bağımsız olarak tarar. `TaskSettings::BaseSettings::EventLogItem::datetime` ayarı düzenlenemez. Bu ayar, yalnızca EventLogItem IOC belgesi, tarama için sağlanan IOC dosyasında açıklandığında kullanılır.
`/channel=<list of channels>`	IOC taraması yapmak istediğiniz kanal adlarının listesi (günlük). Argümen belirtildiği takdirde, Kaspersky Endpoint Security belirtilen günlüklerde yayınlanan kayıtları tarar. IOC belgesi, açıklanan EventLogItem terimine sahip olmalıdır. Günlüğün adı, günlüğün özelliklerinde (Full Name parametresi) veya olay özelliklerinde (olayın xml şemasındaki (`<Channel></Channel>` parametresi) belirtilen günlüğün (kanalın) adına göre bir dize olarak belirtilir. Boşluklarla ayrılmış birden çok kanal belirtebilirsiniz. Kaspersky Endpoint Security, argüman belirtilmediği takdirde, `Application`, `System`, `Security` kanalları için kayıtları tarar.

`/files=on|off`	IOC taraması gerçekleştirirken dosya verilerini analiz et (Fileltem terimi). Argümanın değeri `off` olduğunda, Kaspersky Endpoint Security verileri analiz etmez. IOC dosyası, Fileltem IOC belgesi terimlerini içeriyorsa bunlar yoksayılır (eşleşme olmadığı algılanır). Argüman belirtilmediği takdirde, Kaspersky Endpoint Security dosya verilerini ancak, Fileltem IOC belgesi tarama için sağlanan IOC dosyasında açıklanmışsa analiz eder.
`/drives=<all|system|critical|custom>`	Fileltem IOC belgesi için verileri analiz ederken IOC tarama kapsamını ayarlayın. Tarama kapsamı için aşağıdaki değerleri ayarlayabilirsiniz: • Mevcut tüm dosya kapsamları için `<all>`. • İşletim sisteminin kurulu olduğu klasörlerdeki dosyalar için `<system>`. • Kullanıcı ve sistem klasörlerindeki geçici dosyalar için `<critical>`. • Kullanıcı tanımlı kapsamlardaki dosyalar için `<custom>` (`/scope=<list of folders to scan>`). Argüman belirtilmezse tarama kritik alanlar için yapılır.
`/excludes=<list of exclusions>`	Fileltem IOC belgesi için verileri analiz ederken istisna kapsamını ayarlayın. Boşluklarla ayrılmış birden çok yol belirtebilirsiniz.
`/scope=<list of folders to scan>`	Fileltem IOC belgesi için verileri analiz ederken kullanıcı tanımlı IOC tarama kapsamı (`/drives=custom`). Boşluklarla ayrılmış birden çok yol belirtebilirsiniz.
`/retro /<number of days>`	*Geriye Dönük IOC Taraması*, Kaspersky Endpoint Security'nin belirli bir zaman dilimine ait verileri kullanarak ihlal göstergelerini taradığı *IOC Taraması* görevinin bir modudur. Bu mod, ağ etkinliği, işlemler, dosyalar ve diğer telemetri verileri gibi korunan bilgisayarın telemetri verilerini kullanarak güvenlik ihlali göstergelerini aramaya yöneliktir. Zaman aralığını 1 ila 14 gün arasında ayarlayabilirsiniz. Varsayılan olarak, uygulama bir gün boyunca ihlal göstergelerini tarar.
`/network=on|off`	Ağ verilerinin analizi (Networkltem terimi).
`/url=on|off`	Tarayıcı günlüklerindeki verilerin analizi (UrlHistoryItem terimi). Retrospektif IOC Taraması şu tarayıcıların günlüklerini analiz eder: Google Chrome, Mozilla Firefox, Microsoft Edge (sürüm 79 veya üstü).
`/email`	Posta nesnelerinin analizi (Emailltem terimi).
`/route`	Yönlendirme ve yönlendirme tablolarının analizi (RouteEntryItem terimi).

Komut dönüş değerleri:

- `-1`, bilgisayarda yüklü olan Kaspersky sürümü tarafından komutun desteklenmediği anlamına gelir.
- `0`, komutun başarıyla yürütüldüğü anlamına gelir.
- `1`, komuta zorunlu bir bağımsız değişkenin iletilmediği anlamına gelir.
- `2`, genel bir hata oluştuğu anlamına gelir.
- `4`, bir sözdizimi hatası olduğu anlamına gelir.

Komut başarıyla yürütüldüyse (dönüş değeri `0`) ve yol boyunca güvenlik ihlali göstergeleri algılandıysa, Kaspersky Endpoint Security aşağıdaki görev sonucu bilgilerini komut satırına gönderir:

`Uuid`	IOC dosya yapısının başlığından IOC dosyasının kimliği (`<ioc id="">` etiketi)
`Name`	IOC dosya yapısının başlığından IOC dosyasının açıklaması (`<description></description>` etiketi)
`Matched Indicator Items`	Eşleşen tüm göstergelerin kimliklerinin listesi.
`Matched objects`	Bir eşleşme bulunan her IOC belgesi için veriler.

MDRLICENSE. MDR etkinleştirmesi

Managed Detection and Response'u etkinleştirmek için BLOB yapılandırma dosyasını ekleme. BLOB dosyası, istemci kimliğini ve Kaspersky Managed Detection and Response lisansı hakkındaki bilgileri içerir. BLOB dosyası, MDR yapılandırma dosyasının ZIP arşivinde bulunur. ZIP arşivini Kaspersky Managed Detection and Response Konsolunda bulabilirsiniz. Bir BLOB dosyası hakkında ayrıntılı bilgi için lütfen Kaspersky Yönetilen Algılama ve Yanıt Yardım içeriğine bakın.

Bir BLOB dosyasıyla işlem yapmak için yönetici ayrıcalıkları gerekir. İlkede Managed Detection and Response ayarları da düzenlenebilir olmalıdır ( ).

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

İşlem	
`/ADD <file name>`	Kaspersky Managed Detection and Response ile entegrasyon için BLOB yapılandırma dosyasını uygulayın (P7 dosya biçimi). Yalnızca bir tane BLOB dosyası uygulayabilirsiniz. Bilgisayara zaten bir BLOB dosyası eklenmişse dosya değiştirilecektir.
`/DEL`	BLOB yapılandırma dosyasını silin.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Örnek

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. EDR (KATA) entegrasyonu

Endpoint Detection and Response bileşenini (KATA) yönetmek için komutlar:

- EDR (KATA) bileşeninin etkinleştirilmesi veya devre dışı bırakılması.

  EDR bileşeni (KATA), Kaspersky Anti Targeted Attack Platform çözümü ile birlikte çalışabilirlik sağlar.

- Kaspersky Anti Targeted Attack Platform sunucularına bağlantıyı yapılandırma.
- Bileşenin geçerli ayarlarının görüntülenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

İşlem	
`stop`	EDR (KATA) bileşenini devre dışı bırakın.
`start`	EDR (KATA) bileşenini etkinleştirin.
`set`	EDR (KATA) bileşenini yapılandırın. Şu ayarları yapılandırabilirsiniz: • Central Node sunucuları ekleyin (`servers=<server address>:<port>`) • Bir TLS sertifikası ekleyin (`server-certificate=<path to the TLS certificate>`) • Central Node sunucusu bağlantı zaman aşımını ayarlayın (`/timeout=<Central Node server connection timeout (s)>`) • Central Node sunucusu ile senkronizasyon süresini ayarlayın (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Bileşenin geçerli ayarlarını görüntüleyin.

EDRExpertOnPrem. EDR Expert (on-premises) entegrasyonu

Kaspersky Endpoint Detection and Response Expert (on-premises) entegrasyonunu yapılandırmak için yerleşik aracıyı yönetme komutları:

- Yerleşik EDR Expert (on-premises) aracısını etkinleştirme veya devre dışı bırakma.
- EDR Expert (on-premises) sunucuları için bağlantı ayarlarını yapılandırma.
- Yerleşik aracının geçerli ayarlarının görüntülenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

İşlem	Açıklama
`stop`	Yerleşik EDR Expert (on-premises) aracısını devre dışı bırakın.
`start`	Yerleşik EDR Expert (on-premises) aracısını etkinleştirin.

`set`	Yerleşik EDR Expert (on-premises) aracısını yapılandırın.
	Yanıt sunucuları için aşağıdaki bağlantı ayarlarını yapılandırabilirsiniz:
	• `servers=<server address>:<port>`. Yanıt sunucusu adresi (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. İki yönlü kimlik doğrulama için bir kripto konteyneri kullanın. *Kripto konteyner*, PKCS#12 biçiminde bir sertifika ve özel anahtar içeren PFX arşividir. Bu kimlik doğrulamayı etkinleştirmek için harici bir sertifika yetkilisinde kripto konteyner oluşturmanız gerekir.
	• `timeout=<server connection timeout (s)>`. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır.
	• `sync-period=<server synchronization period (min)>`. Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında Kaspersky Endpoint Security tehdit yanıtı görevlerini alır ve görev sonuçlarını gönderir.
	Telemetri toplama sunucuları için aşağıdaki bağlantı ayarlarını yapılandırabilirsiniz:
	• `telemetry-servers=<server address:port>`. Telemetri toplama sunucusu adresi (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. İki yönlü kimlik doğrulama için bir kripto konteyneri kullanın. *Kripto konteyner*, PKCS#12 biçiminde bir sertifika ve özel anahtar içeren PFX arşividir. Bu kimlik doğrulamayı etkinleştirmek için harici bir sertifika yetkilisinde kripto konteyner oluşturmanız gerekir.
	• `telemetry-timeout=<server connection timeout (s)>`. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır.
	• `events-send-period=<seconds>`. Olayları gönderirken maksimum gecikme. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
	• `events-limit=<0|1>`. İsteklerin sayısını sınırlayın. Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur.
	• `events-per-hour=<number of events>`. Saat başına maksimum olay sayısı Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir.
	• `max-packet-length=<number of packets>`. Maksimum paket uzunluğu. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır.
	• `telemetry-only-tagged-events=<0|1>`. Yalnızca IOA içeren telemetrinin gönderilmesi. *Saldırı Göstergesi (IOA)*, hedefli bir saldırıyı işaret edebilecek sistemdeki şüpheli davranışların açıklamasını içeren bir kuraldır. Uygulama, sistemdeki devam eden davranışları bu kurallarla karşılaştırır ve hedefli bir saldırıyı gösteren olayları günlüğe kaydeder. Uygulama, bu tür olayların gerçek zamanlı olarak izlenmesini sağlayan *akış tarama* teknolojisini kullanır.
	Aşağıdaki genel ayarları yapılandırabilirsiniz:
	• `mode=EDRKATA | EDRExpertOnPrem`. Çözümler arasında geçiş yapma:
	  • `EDRKATA`. Endpoint Detection and Response Expert (sürüm 7.1 veya öncesi).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (sürüm 8.0 veya üstü). Varsayılan değer.
	• `login=<user name> password=<password>`. Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

`show`	Bileşenin geçerli ayarlarını görüntüleyin.

KUMA. KUMA Entegrasyonu

Yerleşik KUMA ajanı yönetmek için komutlar:

- KUMA entegrasyonunu etkinleştirme veya devre dışı bırakma.

  Yerleşik KUMA aracısı, Kaspersky Unified Monitoring and Analysis Platform çözümüyle birlikte çalışabilirlik sağlar.

- Kaspersky Unified Monitoring and Analysis Platform sunucularına bağlantıyı yapılandırma.

- Bileşenin geçerli ayarlarının görüntülenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

İşlem	
`stop`	KUMA entegrasyonunu devre dışı bırakın.
`start`	KUMA entegrasyonunu etkinleştirin.
`set`	Yerleşik KUMA aracısını yapılandırın. Şu ayarları yapılandırabilirsiniz: • KUMA sunucuları ekleyin (`/servers=<protocol>://<server address>:<port>`) Uygulama şu sunucu bağlantı protokollerini destekler: `tcp`, `udp`, `http`, `https`. • Bir TLS sertifikası ekleyin (`/server-certificate=<path to the TLS certificate>`) • Sunucusu bağlantı zaman aşımını ayarla (`/timeout=<KUMA server connection timeout (s)>`) • Bir kripto-konteyner ekleme (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Olay iletim gecikmesini yapılandırın (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Bileşenin geçerli ayarlarını görüntüleyin.

Kimlik Doğrulama	
`/login=<user name> /password=<password>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. YARA Taramasını Çalıştırma

YARA Taramasını Çalıştır görevini çalıştırma. Uygulama, YARA kuralları veritabanlarını kullanarak kurumsal BT altyapısına yönelik hedefli saldırıların göstergelerini bulmak için dosyaları ve nesneleri tarar. *YARA kuralları*, Kaspersky Endpoint Security'nin nesneleri taramak için kullandığı, kurumsal BT altyapısına yönelik saldırıların ve izinsiz girişlerin imzalarının tanımlamalarıdır.

Bir YARA taraması çalıştırmak için kuralları tanımlayan YARA dosyaları hazırlamanız gerekir. YARA dosyalarını oluştururken aşağıdaki gereksinimleri göz önünde bulundurun:

- Kaspersky Endpoint Security, güvenlik ihlali göstergelerini tanımlamak için YARA 4.2.3 açık standardını izleyen .YARA ve .YAR uzantılı YARA dosyalarını destekler.
- Görev için yalnızca YARA kuralları içeren dosyalar belirtilebilir. *YARA Taramasını Çalıştır* görevi diğer kural türlerini desteklemez.
- Kaspersky Endpoint Security'nin desteklemediği YARA dosyalarını eklediyseniz veya kurallar söz dizimi hataları içeriyorsa, görev ilgili hata mesajıyla iptal edilir.
- Tek bir görevde kullanılan tüm YARA dosyalarının tanımlayıcıları benzersiz olmalıdır. Aynı tanımlayıcıya sahip YARA dosyaları olduğunda, bu görev yürütme sonuçlarını etkileyebilir.
- Bir YARA taraması, YARA kurallarında açıklanan göstergelerle 128 eşleşmeden sonra iptal edilir. Bu, YARA tarama raporundaki girdilerin sayısını sınırlandırarak analiz edilmesini kolaylaştırmak ve çok fazla sayıda eşleşme oluşturabilecek kesin olmayan bir şekilde formüle edilmiş YARA kuralları nedeniyle raporda aşırı doluluk oluşmasını önlemek için gereklidir.

Kaspersky, YARA dosyası başına bir kural oluşturulmasını önerir. Bu, tarama sonuçlarını daha okunabilir hale getirir.

YARA taraması önemli miktarda zaman alabilir. Sürücü boyutuna, görev ayarlarına ve diskteki nesne sayısına bağlı olarak, bir YARA taraması birkaç dakikadan birkaç saate kadar sürebilir. Uygulama bir ilerleme göstergesi görüntülemez. Bir YARA taramasını durdurmak veya iptal etmek mümkün değildir. YARA taramasının sonuçları elde edilene kadar beklemeniz tavsiye edilir.

Komut söz dizimi

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA dosyaları	
`<full path to the YARA file>`	Tarama için kullanmak istediğiniz YARA dosyasının tam yolu. Birden fazla YARA dosyasının yolunu boşluklarla ayırarak belirtebilirsiniz. `/path=<path to the folder with YARA files>` değeri belirtilmemişse zorunlu parametre. Örnek: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`

`/path=<path to the folder with YARA files>`	Tarama işlemi için kullanmak istediğiniz YARA dosyalarının bulunduğu klasörün tam yolu. `<full path to the YARA file>` değeri belirtilmemişse zorunlu parametre. Örnek: `/path=C:\Users\Admin\Desktop\YARA`

Gelişmiş ayarlar	
`/fastScan=<on|off>`	Hızlı YARA Taraması. Uygulama, her nesne için tespit edilen göstergenin bir olayını günlüğe kaydeder. Uygulama ayrıca günlükte tespit edilen göstergelerin kopyalarını da gizler. Hızlı YARA Taraması, büyük dosyaların daha hızlı taranmasını sağlar. Bu ayar belirtilmezse, uygulama standart bir YARA taraması gerçekleştirir. Bu modda, uygulama tespit edilen göstergelerin kopyalarını günlüğe kaydeder.
`/maxRules=<maximum number of scan rules>`	Ulaşıldığında uygulamanın YARA taramasını durdurmasına neden olan benzersiz tetiklenen kural sayısının üst sınırı. Bu ayarın değeri belirtilmezse veya `0` belirtilirse, uygulama YARA taramasını sınırlama olmaksızın gerçekleştirir.
`/timeOut=<stop scan after the specified time in seconds>`	Bir YARA taramasının saniye cinsinden ne kadar sürebileceği. Bu süre dolduğunda, uygulama YARA taramasını durdurur. Bu ayarın değeri belirtilmezse veya `0` belirtilirse, uygulama YARA taramasını sınırlama olmaksızın gerçekleştirir.
`/recursive=<on|off>`	Bu seçenek, `/scanFolders` Özel Tarama kapsamındaki alt klasörlerin özyinelemeli bir taramasını başlatır.
`/scanFolders=<list of folders to be scanned>`	Bu komut, belirtilen klasörler listesindeki dosyalar için bir YARA taraması başlatır. Boşluklarla ayrılmış birden fazla değer belirtebilirsiniz. Kaspersky Endpoint Security, klasör yolu maskesini girerken `*` ve `?` karakterlerini destekler. Bu ayar belirtilmezse, uygulama ağ paylaşımları, bulut sürücüleri ve çıkarılabilir medya hariç tüm yerel disklerde bir YARA taraması gerçekleştirir.
`/scanMemory=<on|off>`	Çalışan tüm işlemlerin belleğini tarayın.
`/scanProcess=<process name>`	Belleği yalnızca belirtilen işlemler için tarayın. İşlemlerin yürütülebilir dosyalarının tam yollarını boşluklarla ayırarak belirtin. Bir maske girmek için `*` ve `?` karakterlerini de kullanabilirsiniz.
`/maxSize=<file size in bytes>`	YARA taraması için dosya boyutunu sınırlayın. Uygulama daha büyük dosyaları atlar.
`/includes=<list of objects to be scanned>>`	Tarama kapsamının düzenlenmesi. Boşluklarla ayrılmış birden fazla değer belirtebilirsiniz. Aşağıdaki değerler kullanılabilir: • Dosya adı • Dosya uzantısı Tarama kapsamı, `/scanFolders` parametresi ile belirtilmelidir. Örnek: `/scanFolders C:\*.* /includes=*.exe *.dll` – uygulama, C sürücüsündeki tüm .EXE ve .DLL uzantılı dosyaları tarar.
`/excludes=<list of objects to be scanned>`	YARA taramasından dosyaları hariç tutulur. Boşluklarla ayrılmış birden fazla değer belirtebilirsiniz. Aşağıdaki değerler kullanılabilir: • Dosya yolu • Dosya yolunun maskesi İstisnalar, `/scanFolders` parametresiyle belirtilmelidir. Örnek: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – uygulama, readme.txt dosyasını, C:\trusted klasöründeki tüm dosyaları ve C sürücüsünün kök klasöründe bulunan .XML uzantılı tüm dosyaları atlar.
`/scanAutoruns=<on|off>`	Otomatik çalıştırma noktası nesnelerinin YARA taraması.
`/excludeAutoruns=<list of autorun point areas to skip>`	Otomatik çalıştırma noktası nesnelerini tarama kapsamı dışında bırakma. İşlemlerin yürütülebilir dosyalarının tam yollarını boşluklarla ayırarak belirtin. Bir maske girmek için `*` ve `?` karakterlerini de kullanabilirsiniz.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Bir klasörün yolunu belirtirseniz, uygulama tarama sonuçlarını belirtilen yolda yara_<bilgisayar adı>_<tarama tamamlanma zamanı>.txt adlı bir dosyaya kaydeder. Belirli bir TXT dosyasının yolunu belirtirseniz, uygulama tarama sonuçlarını bu dosyaya kaydeder. Örneğin: `/logFolder=C:\test` veya `/logFolder=C:\test\abc.txt`. Tarama sonuçları, `/logFolder` seçeneğinin belirtilip belirtilmediğine bakılmaksızın komut satırına yazdırılır.

Komut dönüş değerleri:

- `-1`, bilgisayarda yüklü olan Kaspersky sürümü tarafından komutun desteklenmediği anlamına gelir.
- `0`, komutun başarıyla yürütüldüğü anlamına gelir.
- `1`, komuta zorunlu bir bağımsız değişkenin iletilmediği anlamına gelir.
- `2`, genel bir hata oluştuğu anlamına gelir.
- `4`, bir sözdizimi hatası olduğu anlamına gelir.
- `5` parametrede belirtilen YARA kurallarına sahip bir veya daha fazla dosyanın bulunamadığı anlamına gelir.

Komut başarıyla yürütüldüyse (dönüş değeri `0`) ve yol boyunca güvenlik ihlali göstergeleri algılandıysa, Kaspersky Endpoint Security aşağıdaki görev sonucu bilgilerini komut satırına gönderir:

`Started at <time>` `Finished at <time>`	Bir taramanın başlangıç ve bitiş saatleri.
`Host name: <computer name>`	Nesnenin tespit edildiği bilgisayarın adı.
`Result: <error>`	Görev yürütülürken meydana gelen hatanın hata kodu. Herhangi bir hata yoksa, uygulama `0x00000000` çıktısını verir.
`Comment: <comment text>`	Görev yürütülürken meydana gelen hatanın hata açıklaması. Örneğin, `Operation timeout`.
`Object Name:` veya `Process:` (işlemci belleğini tararken)	YARA kuralının tetiklendiği nesnenin veya işlemin adı.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	YARA kuralının tetiklendiği nesnenin karma değerleri.
`Rule Name`	Tetiklenen YARA kuralının adı.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	YARA kuralında belirtilen meta veriler.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Nesne içinde YARA kuralının koşullarını karşılayan eşleşmeler bulundu:
	• Eşleşme tespit edildiği işlem belleği veya dosyadaki kaydırma (`Offset`).
	• YARA kuralındaki eşleşen dizenin adı (`String name`).
	• İşlem belleğinde veya dosyada bulunan eşleşen dize (`String data`).

TELEMETRİ FİLTRELERİ. KUMA'ya gönderilecek olayları filtreleme

Varsayılan olarak, KUMA sunucusuna olay gönderme özelliği devre dışıdır. KUMA'nın düzgün çalışmasını sağlamak için telemetri gönderimini etkinleştirmeniz gerekir. Standart günlükler arasından bir olay kaynağı seçebilirsiniz: *Uygulama*, *Güvenlik* veya *Sistem*. KUMA sunucusuna veri iletimini iyileştirmek ve optimize etmek için, telemetriye bireysel olayları manuel olarak ekleyebilir veya hariç tutabilirsiniz. Örneğin, Sysmon olaylarını hariç tutabilirsiniz.

İstisna listesini komut satırından bir JSON dosyasına aktarabilirsiniz.

Komut yalnızca ayarları aktarmak istediğiniz dosyanın adını içeriyorsa, uygulama dosyayı aşağıdaki gibi yerleştirir:

- avp.com yolu %PATH% sistem değişkenine eklenirse, uygulama dosyayı `C:\Windows\SysWOW64` klasörüne yerleştirir.
- Komutu uygulama yükleme klasöründen çalıştırırsanız, uygulamanın kendini koruması uygulama klasöründe yeni bir dosya oluşturulmasını engellediğinden dışa aktarma başarısız olur. Uygulama ayarlarını bir dosyaya aktarmak için dosya yolunu girin.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

İşlem	
`export`	KUMA'ya gönderilecek etkinlik filtrelerini dışa aktarma.
`import`	KUMA'ya gönderilecek etkinlik filtrelerini içe aktarma. Bilgisayarda olay filtreleme kuralları zaten mevcutsa, Kaspersky Endpoint Security bunları içe aktarırken değiştirir.

Dışa veya içe aktarma dosyası	
`<file name>`	KUMA'ya gönderilecek olay filtrelerinin bulunduğu dosyanın adı. Dosya yolunu da girebilirsiniz. KUMA'ya göndermek için filtreleri bir JSON dosyasına aktarabilirsiniz.

Light Agent yönetim komutları

Uygulamayı komut satırında sanal ortamları korumak için Light Agent'ta yönetebilirsiniz. Kaspersky Security Center konsolunu kullanarak yönetim mümkün değilse uygulamayı Light Agent modunda yönetebilirsiniz. `HELP` komutunu çalıştırarak uygulama yönetimi için kullanılabilecek komutların listesini görebilirsiniz. Belirli bir komutun söz dizimi hakkında bilgi almak için `HELP <command>` komutunu girin.

Uygulamayı komut satırından Light Agent modunda yönetmek için:

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin.
3. Komutu çalıştırmak için aşağıdaki şablonu kullanın:

   ```
   avp.com <command> [options]
   ```

   Böylece Kaspersky Endpoint Security, komutu yürütecektir.

Light Agent modunda yüklenen uygulama, Standart modda yüklenen uygulamanın neredeyse tüm AVP komutlarını destekler. Light Agent modunda, anti-virüs veritabanı güncelleme görevleri ve lisans anahtarı yönetimi görevleri sınırlıdır.

KSVLAINFO. Light Agent modunun belirlenmesi

Light Agent modunun belirlenmesi.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com KSVLAINFO
```

Komut aşağıdaki bilgileri konsola çıktı olarak verir:

- Sanal ortamları korumak için Light Agent modu: etkin veya devre dışı.

  Light Agent modu etkinleştirilirse uygulama, Kaspersky Security for Virtualization Light Agent çözümünün bir parçası olarak kullanılır.

- VDI koruma modu: etkin veya devre dışı.

  VDI koruma modu, Kaspersky Endpoint Security'nin kalıcı olmayan sanal makinelerdeki performansını optimize etmeye yardımcı olur. VDI koruma modu etkinleştirilirse, korumalı sanal makinenin yeniden başlatılmasını gerektiren güncelleştirmeler kalıcı olmayan sanal makinelere yüklenmez. Yeniden başlatma gerektiren güncellemeleri alırken, kalıcı olmayan bir sanal makineye yüklenen Light Agent, Kaspersky Security Center'a korunan sanal makine şablonunun güncellenmesi gerektiğini bildiren bir mesaj gönderir.

- Korunan sanal makinenin türü: kalıcı veya kalıcı olmayan.

- Korunan sanal makinenin sanal altyapıdaki rolü: sunucu veya iş istasyonu.

- Tanımlayıcı: UUID.

VIISINFO. Entegrasyon Sunucusuna Light Agent bağlantısının durumu

Entegrasyon Sunucusuna Light Agent bağlantısı hakkındaki bilgileri görüntüleme.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com VIISINFO
```

Komut aşağıdaki bilgileri konsola çıktı olarak verir:

- Light Agent'ın bağlı olduğu Entegrasyon Sunucusunun adresi ve bağlantı noktası.
- Entegrasyon Sunucusu bağlantı durumu.
- Light Agent'ın Entegrasyon Sunucusuna son bağlantısının tarih ve saati.

SVMINFO. Light Agent'ın Protection Server ile bağlantısının durumu

Light Agent'ın Protection Server'a bağlantısı hakkındaki bilgileri görüntüleme.

Komutu çalıştırmak için Kaspersky Endpoint Security yürütülebilir dosyasının bulunduğu klasöre gidin. Ayrıca yürütülebilir dosya yolunu %PATH% sistem değişkenine ekleyebilir ve uygulama klasörüne gitmeden komutu çalıştırabilirsiniz.

Komut söz dizimi

```
avp.com SVMINFO
```

Komut aşağıdaki bilgileri konsola çıktı olarak verir:

- Light Agent'ın bağlı olduğu SVM'nin adresi ve SVM'nin Light Agent'a göre sanal altyapıdaki konumu: yerel veya yerel olmayan.
- Light Agent'ın kullandığı SVM keşfi yöntemi: bir Entegrasyon Sunucusu kullanarak veya özel bir SVM adresleri listesi kullanarak.
- SVM keşfi yöntemi olarak SVM adres listesi seçilmişse SVM adreslerinin listesi.
- Light Agent'ı SVM'ye bağlamak için etiket.
- SVM seçim algoritması: standart veya genişletilmiş. Genişletilmiş SVM seçim algoritması kullanılıyorsa, sanal altyapıdaki SVM yolu türü de görüntülenir.
- Light Agent ile Protection Server arasındaki bağlantının koruma durumu.

Hata kodları

Uygulama ile komut satırından çalışılırken hatalar meydana gelebilir. Hatalar meydana geldiğinde, Kaspersky Endpoint Security bir hata mesajı görüntüler, örneğin `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security ayrıca bir kod biçiminde ek bilgiler de gösterebilir, örneğin, `error=8947906D` (aşağıdaki tabloya bakın).

Hata kodları

Hata kodu	Açıklama
`09479001`	Bu anahtar zaten kullanımda
`0947901D`	Lisansın süresi sona erdi. Veritabanı güncellemeleri kullanılamıyor

Hata kodu	Açıklama
89479002	Anahtar bulunamadı
89479003	Dijital imza yok ya da bozulmuş.
89479004	Veriler bozuk.
89479005	Anahtar dosyası bozuk
89479006	Lisansın süresi sona erdi
89479007	Anahtar dosyası belirtilmedi
89479008	Geçersiz anahtar dosyası
89479009	Veri kaydedilemedi
8947900A	Veri okunamadı
8947900B	G/Ç hatası
8947900C	Veritabanları bulunamadı
8947900E	Lisanslama kitaplığı yüklenmedi.
8947900F	Veritabanları bozuk veya manuel olarak güncellenmiş
89479010	Veritabanları bozulmuş
89479011	Bir rezerve anahtar eklemek için geçersiz bir anahtar dosyası kullanılamaz
89479012	Sistem hatası
89479013	Anahtar reddedilenler listesi bozuk
89479014	Dosya imzası, Kaspersky'nin dijital imzası ile eşleşmiyor
89479015	Bir deneme lisansı anahtarı ticari lisans anahtarı olarak kullanamaz.
89479016	Uygulamanın beta sürümünü kullanmak için beta lisansı gerekiyor
89479017	Anahtar dosyası bu uygulama ile uyumlu değil. Kaspersky Endpoint Security for Windows'u başka bir uygulamanın anahtar dosyasıyla etkinleştirmek mümkün değildir. Lütfen yüklü uygulamayı kontrol edin
89479018	Lisans anahtarı Kaspersky tarafından engellendi
89479019	Uygulama zaten bir deneme lisansı altında kullanılmış. Deneme lisansı için tekrar anahtar eklenemez
8947901A	Anahtar dosyası bozuk
8947901B	Dijital imza yok, bozulmuş ya da Kaspersky dijital imzası ile uyuşmuyor.
8947901C	İlgili ticari olmayan lisans sona ermişse, anahtar eklenemez
8947901E	Anahtar dosyasının oluşturulduğu ya da kullanıldığı tarih geçersiz. Lütfen sistem tarihini kontrol edin
8947901F	Deneme lisansı için bir anahtar eklenemiyor: deneme lisansı için ek bir anahtar zaten aktif.
89479020	Anahtar reddedilenler listesi bozuk veya eksik
89479021	Güncelleme açıklaması eksik veya bozuk
89479022	Anahtar bu uygulama için uygun değil
89479023	Bir rezerve anahtar eklemek için geçersiz bir anahtar dosyası kullanılamaz
89479025	Etkinleştirme sunucusu isteği gönderilemedi. Olası nedenler: İnternet bağlantısı hatası ya da etkinleştirme sunucusundaki geçici sorunlar. Uygulamayı daha sonra (1 ila 2 saat içinde) etkinleştirme kodu ile etkinleştirmeyi deneyin. Bu hata tekrar meydana gelirse internet sağlayıcınızla iletişim kurun
89479026	İstek, hatalı etkinleştirme kodunu içeriyor
89479027	Yanıt durumu alınamıyor
89479028	Geçici dosya kaydedilirken hata meydana geldi
89479029	Hatalı etkinleştirme kodu girilmiş veya bilgisayarda geçersiz sistem tarihi ayarlanmış. Lütfen bilgisayarınızdaki sistem tarihini kontrol edin.
8947902A	Anahtar bu uygulama ile uyumlu değil veya lisansın süresi doldu

Hata kodu	Açıklama
8947902B	Anahtar dosyası alınamadı Yanlış etkinleştirme kodu girildi
8947902C	Etkinleştirme sunucusu 400 hatası verdi
8947902D	Etkinleştirme sunucusu 401 hatası verdi
8947902E	Etkinleştirme sunucusu 403 hatası verdi
8947902F	Etkinleştirme sunucusunda gerekli kaynak yok. Etkinleştirme kodu 404 hatası verdi. İnternet bağlantı ayarlarınızı denetleyin
89479030	Etkinleştirme sunucusu 405 hatası verdi
89479031	Etkinleştirme sunucusu 406 hatası verdi
89479032	Proxy kimlik doğrulaması gerekiyor. Lütfen ağ ayarlarınızı kontrol edin
89479033	İstek zaman aşımına uğradı
89479034	Etkinleştirme sunucusu 409 hatası verdi
89479035	Etkinleştirme sunucusunda gerekli kaynak yok. Etkinleştirme kodu 410 hatası verdi. İnternet bağlantı ayarlarınızı denetleyin
89479036	Etkinleştirme sunucusu 411 hatası verdi
89479037	Etkinleştirme sunucusu 412 hatası verdi
89479038	Etkinleştirme sunucusu 413 hatası verdi
89479039	Etkinleştirme sunucusu 414 hatası verdi
8947903A	Etkinleştirme sunucusu 415 hatası verdi
8947903C	Dahili sunucu hatası
8947903D	İşlevsellik desteklenmiyor
8947903E	Geçersiz ağ geçidi yanıtı. Lütfen ağ ayarlarınızı kontrol edin
8947903F	Kaynak geçici olarak kullanılamıyor
89479040	Ağ geçidi yanıtı zaman aşımına uğradı. Lütfen ağ ayarlarınızı kontrol edin
89479041	İletişim kuralı sunucu tarafından desteklenmiyor
89479043	Bilinmeyen HTTP hatası
89479044	Geçersiz kaynak kimliği
89479046	Geçersiz URL
89479047	Geçersiz hedef klasörü
89479048	Bellek atama hatası
89479049	Parametreler ANSI dizisine (URL, klasör, aracı) dönüştürülürken hata ortaya çıktı
8947904A	Çalışan dizi oluşturulurken hata ortaya çıktı
8947904B	Çalışan dizi zaten çalışıyor
8947904C	Çalışan dizi çalışmıyor
8947904D	Anahtar dosyası etkinleştirme sunucusunda bulunamadı
8947904E	Anahtar engellendi
8947904F	Etkinleştirme sunucusu iç hatası
89479050	Etkinleştirme isteğinde yeterli veri yok
89479053	Eklenen anahtar ile ilgili lisansın süresi zaten dolmuş
89479054	Bilgisayarda geçersiz sistem tarihi ayarlanmış. Lütfen sistem tarih değerini kontrol edin
89479055	Deneme lisansının süresi doldu
89479056	Uygulama etkinleştirme süresi doldu
89479057	Belirtilen kod için uygulama etkinleştirme sınırı aşıldı

Hata kodu	Açıklama
89479058	Etkinleştirme prosedürü bir sistem hatası ile tamamlandı
89479059	Bir deneme lisansı anahtarı ticari lisans anahtarı olarak kullanamaz.
8947905C	Etkinleştirme kodu gerekli
89479062	Etkinleştirme sunucusuna bağlanamıyor
89479064	Etkinleştirme sunucusu kullanılamıyor. Lütfen İnternet bağlantı ayarlarınızı kontrol edin ve etkinleştirmeyi tekrar deneyin
89479065	Lisansın süresi sona erdi
89479066	Etkin anahtar, süresi dolmuş bir anahtar ile değiştirilemez
89479067	İlgili lisans geçerli lisanstan önce sona eriyorsa bir rezerve anahtar eklenemez.
89479068	Güncellenmiş abonelik anahtarı eksik
8947906A	Geçersiz etkinleştirme kodu
8947906B	Anahtar zaten etkin
8947906C	Etkin ve rezerve anahtarlara karşılık gelen lisans türleri eşleşmiyor
8947906D	Bileşen lisans tarafından desteklenmiyor
8947906E	Abonelik anahtarı rezerve anahtar olarak eklenemiyor
89479213	Taşıma katmanı genel hatası
89479214	Etkinleştirme sunucusuna bağlanılamadı
89479215	Geçersiz web adresi biçimi
89479216	Proxy sunucusu adresi dönüştürme başarısız
89479217	Sunucu adresi dönüştürülemedi. Lütfen internet bağlantısı ayarlarını kontrol edin
89479218	Sunucu bağlantı girişimi başarısız oldu
89479219	Erişim uzaktan reddedildi
8947921A	İşlem zaman aşımına uğradı
8947921B	HTTP isteğini göndermede hata
8947921C	SSL bağlantısı hatası
8947921D	İşlem geri arama ile durduruldu
8947921E	Çok sayıda yönlendirme
8947921F	Alıcı denetimi başarısız
89479220	Sunucudan boş yanıt
89479221	Verileri gönderirken hata
89479222	Verileri almada hata
89479223	SSL sertifikası ile ilgili sorun
89479224	SSL şifreleme ile ilgili sorun
89479225	SSL sertifika merkezi ile ilgili sorun
89479226	Ağ paketinin geçersiz içeriği
89479227	Hesap erişimi reddedildi
89479228	Geçersiz SSL sertifika dosyası
89479229	SSL bağlantısı sona erdirilemiyor
8947922A	Yinelenen hata
8947922B	İptal edilen sertifikalara sahip geçersiz bir dosya
8947922C	SSL sertifika isteği hatası

Hata kodu	Açıklama
89479401	Bilinmeyen sunucu hatası
89479402	Dahili sunucu hatası
89479403	Girilen etkinleştirme kodu için herhangi bir anahtar yok
89479404	Etkin anahtar engellendi
89479405	Etkinleştirme isteğinin gerekli parametreleri eksik
89479406	Geçersiz istemci numarası veya parolası
89479407	Geçersiz etkinleştirme kodu
89479408	Etkinleştirme kodu bu uygulamayla uyumlu değil. Kaspersky Endpoint Security for Windows'u başka bir uygulama için olan etkinleştirme koduyla etkinleştirmek mümkün değildir. Lütfen yüklü uygulamayı kontrol edin
89479409	Etkinleştirme kodu gerekli
8947940B	Etkinleştirme süresi doldu
8947940C	Bu kodla yapılabilecek etkinleştirme sayısı aşıldı
8947940D	Geçersiz istek kimliği biçimi
8947940E	Etkinleştirme kodu zaten kullanımda
8947940F	Etkinleştirme kodu yenileme başarısız
89479410	Etkinleştirme kodu bu bölgede geçersizdir
89479411	Bu etkinleştirme kodu uygulamanın bu yerelleştirmesi için kullanılamaz.
89479412	Etkinleştirme kodu, bu uygulamanın yeni sürümü için tasarlanmıştır. Uygulamanın yüklü sürümünü etkinleştirmek için farklı bir etkinleştirme kodu alın
89479413	Etkinleştirme sunucusu 643 hatası verdi
89479414	Etkinleştirme sunucusu 644 hatası verdi
89479415	Etkinleştirme sunucusu 645 hatası verdi
89479416	Etkinleştirme sunucusu 646 hatası verdi
89479417	Etkinleştirme sunucusu sürümü 1.0 gerekli
89479418	Etkinleştirme kodunun biçimi yanlış
89479419	Bilgisayar saati, etkinleştirme sunucu saati ile senkronize değil
8947941A	Yanlış uygulama sürümü
8947941B	Abonelik süresi sona erdi
8947941C	Etkinleştirme sayısı geçildi
8947941D	Geçersiz etiket imzası
8947941E	Ek kullanıcı verileri gerekli
8947941F	Veri doğrulama başarısız
89479420	Abonelik etkin değil
89479421	Etkinleştirme sunucusu bakımda
89479501	Beklenmeyen hata
89479502	Geçersiz parametre aktarıldı. Örneğin etkinleştirme sunucusu adreslerinin boş bir listesi.
89479503	Geçersiz etkinleştirme kodu (geçersiz karma)
89479504	Geçersiz kullanıcı kimliği
89479505	Geçersiz kullanıcı parolası
89479506	Etkinleştirme sunucusundan geçersiz yanıt

Hata kodu	Açıklama
89479507	Etkinleştirme isteği kesintiye uğratıldı
89479509	Etkinleştirme sunucusu boş bir iletme listesi getirdi

Ek. Uygulama profilleri

Profil bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Profiller uygulamanın komut satırından yönetimi için kullanılır. Profilleri `START`, `STOP`, `STATUS`, `STATISTICS` ve `EXPORT` komutlarını çalıştırmak için kullanabilirsiniz. Profilleri kullanarak uygulama ayarlarını yapılandırabilir (örneğin, `STOP DeviceControl`) veya görevleri çalıştırabilirsiniz (örneğin, `START Scan_My_Computer`).

Aşağıdaki profiller kullanılabilir:

- `AdaptiveAnomaliesControl` – Uyarlamalı Anomali Denetimi
- `AMSI` – AMSI Koruması.
- `AntiCryptor`
- `BehaviorDetection` – Davranış Tespiti.
- `DeviceControl` – Aygıt Denetimi
- `EntAppControl` – Uygulama Kontrolü
- `File_Monitoring` veya `FM` – Dosya Tehdidi Koruması
- `Firewall` veya `FW` – Güvenlik Duvarı
- `HIPS` – Sunucu Yetkisiz Erişim Önleme.
- `IDS` – Ağ Tehdidi Koruması
- `IntegrityCheck` – Bütünlük denetimi
- `LogInspector` – Günlük Denetimi
- `Mail_Monitoring` veya `EM` – Posta Tehdidi Koruması
- `Rollback` – Güncelleme geri alma (uygulama Light Agent modunda yüklüyse profil uygulanamaz)
- `Scan_ContextScan` – Bağlam menüsünden tarama
- `Scan_IdleScan` – Arka plan taraması
- `Scan_Memory` – Çekirdek bellek taraması
- `Scan_My_Computer` – Tam tarama
- `Scan_Objects` – Özel tarama

- `Scan_Qscan` – İşletim sistemi başlatılırken yüklenen nesneleri tarama
- `Scan_Removable_Drive` – Çıkarılabilir sürücü taraması
- `Scan_Startup` veya `STARTUP` – Kritik Alanları Tarama
- `Updater` – Güncelle (uygulama Light Agent modunda yüklenmişse profil uygulanamaz)
- `Web_Monitoring` veya `WM` – Web Tehdidi Koruması
- `WebControl` – İnternet Denetimi

Kaspersky Endpoint Security, servis profillerini de destekler. Kaspersky Teknik Destek ile iletişim kurarken servis profilleri gerekebilir.

REST API aracılığıyla uygulamanın yönetilmesi

Kaspersky Endpoint Security, üçüncü taraf çözümler kullanarak uygulama ayarlarını yapılandırmanıza, bir tarama gerçekleştirmenize, antivirüs veritabanlarını güncellemenize ve diğer görevleri gerçekleştirmenize izin verir. Kaspersky Endpoint Security bu amaçla bir API sunar. Kaspersky Endpoint Security REST API, HTTP üzerinden çalışır ve bir dizi talep/yanıt yönteminden meydana gelir. Başka bir deyişle, Kaspersky Endpoint Security'yi yerel uygulama arabirimini ya da Kaspersky Security Center Yönetim Konsolu'nu kullanarak değil de, bir üçüncü taraf yazılımı üzerinden yönetebilirsiniz.

REST API'yi kullanmaya başlamak için Kaspersky Endpoint Security REST API desteği ile yüklenmelidir. REST istemcisi ve Kaspersky Endpoint Security aynı bilgisayara kurulmalıdır.

Kaspersky Endpoint Security ile REST istemcisi arasında güvenli etkileşim sağlamak için:

- REST istemcisi geliştiricisinin önerine göre REST istemcisinin izinsiz erişime karşı korumasını yapılandırın. Kısıtlı Erişim Denetim Listesinin (DACL) yardımıyla, REST istemcisi yazmaya karşı klasör korumasını yapılandırın.
- REST istemcisini çalıştırmak için yönetici haklarına sahip ayrı bir hesap kullanın. Bu hesap için sistemde etkileşimli oturum açmayı reddedin.

Uygulama REST API aracılığıyla http://127.0.0.1 veya http://localhost üzerinden yönetilir. Kaspersky Endpoint Security'nin REST API aracılığıyla uzaktan yönetilmesi mümkün değildir.

REST API DOKÜMANTASYONUNU AÇIN

REST API aracılığıyla uygulamanın yüklenmesi

Uygulamayı REST API aracılığıyla yönetmek için Kaspersky Endpoint Security REST API desteği ile yüklenmelidir. Kaspersky Endpoint Security'yi REST API aracılığıyla yönetirseniz, uygulamayı Kaspersky Security Center'ı kullanarak yönetemezsiniz.

Uygulamayı REST API desteği ile yüklemek için hazırlık

Kaspersky Endpoint Security'nin REST istemcisiyle güvenli etkileşimi, istek tanımlaması yapılandırılmasını gerektirir. Bunu yapmak için bir sertifika yüklemeniz ve ardından her isteğin yükünü imzalamanız gerekir.

Bir sertifika oluşturmak için örneğin OpenSSL kullanabilirsiniz.

Örnek:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Anahtar uzunluğu 2048 bit veya daha fazla olan RSA şifreleme algoritmasını kullanın.

Sonuç olarak, bir `cert.pem` sertifikası ve bir `key.pem` özel anahtarı elde edilir.

Uygulamayı REST API desteği ile yüklemek

Kaspersky Endpoint Security'yi REST API desteği ile yüklemek için:

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security sürüm 11.2.0 veya üzeri için dağıtım paketini içeren klasöre gidin.
3. Kaspersky Endpoint Security'yi şu ayarlarla yükleyin:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Uygulamanın REST API aracılığıyla yönetilmesi için kullanıcı adı. Kullanıcı adını şu biçime göre girin `<DOMAIN>\<UserName>` (örneğin, `RESTAPI_User=COMPANY\Administrator`). Uygulamayı REST API aracılığıyla sadece bu hesaptan yönetebilirsiniz. REST API ile çalışmak üzere sadece bir kullanıcı seçebilirsiniz.

   - `RESTAPI_Port=<port>`

     Uygulamanın REST API aracılığıyla yönetilmesi için kullanılan port. Varsayılan olarak 6782 portu kullanılır. Portun boş olduğundan emin olun. İsteğe bağlı parametre.

   - `RESTAPI_Certificate=<path to certificate>`

     İstekleri tanımlama için sertifika (örneğin, `RESTAPI_Certificate=C:\cert.pem`).

     Uygulamayı yükledikten sonra sertifikayı yükleyebilir veya sertifikayı sertifikanın süresi dolduktan sonra güncelleyebilirsiniz.

     REST API istek tanımlaması için sertifika nasıl yüklenir

     1. Kaspersky Endpoint Security Kendini Koruma'yı devre dışı bırakma

        Kendini Koruma mekanizması, sabit sürücüdeki uygulama dosyalarının, bellekteki işlemlerin ve sistem kayıt defterindeki girişlerin değiştirilmesini veya silinmesini önler.

     2. REST API ayarlarını içeren kayıt defteri anahtarına gidin
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Sertifikanın yolunu girin, örneğin, `Certificate = C:\Folder\cert.pem`.
     4. Kaspersky Endpoint Security Kendini Koruma'yı etkinleştirin.
     5. Uygulamayı yeniden başlatın.

   - `AdminKitConnector=1`

     Yönetim sistemlerini kullanarak uygulama yönetimi. Yönetime varsayılan olarak izin verilir.

   REST API ile çalışmak üzere ayarları tanımlamak için setup.ini dosyasını da kullanabilirsiniz.

   Örnek:
   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
   /pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
   ```

Böylece uygulamayı REST API aracılığıyla yönetebilirsiniz. Çalışmayı doğrulamak için bir GET isteği kullanarak REST API dokümantasyonunu açın.

Örnek:

```
GET http://localhost:6782/kes/v1/api-docs
```

Uygulamayı REST API desteğiyle yüklediğinizde, Kaspersky Endpoint Security web kaynaklarına erişmek için İnternet Denetimi ayarlarında otomatik olarak bir izin kuralı oluşturur (*REST API için Hizmet Kuralı*). Bu kural, REST istemcisinin her zaman Kaspersky Endpoint Security'ye erişmesine izin vermek için gereklidir. Örneğin, internet kaynaklarına kullanıcı erişimini kısıtladıysanız bu, REST API aracılığıyla uygulamanın yönetilmesini etkilemeyecektir. Kuralı silmemenizi ya da *REST API için Hizmet Kuralı* ayarlarını değiştirmemenizi öneririz. Kuralı sildiyseniz, Kaspersky Endpoint Security, uygulamayı yeniden başlattıktan sonra kuralı geri yükler.

API ile çalışmak

Parola koruması kullanarak REST API aracılığıyla uygulamaya erişimi kısıtlamak mümkün değildir. Örneğin bir kullanıcı REST API aracılığıyla korumayı devre dışı bırakmaz. Parola korumasını REST API aracılığıyla yapılandırabilir ve uygulamaya kullanıcı erişimini yerel arabirimden kısıtlayabilirsiniz.

Uygulamayı REST API aracılığıyla yönetmek için REST istemcisini, REST API desteğine sahip uygulamayı kurarken belirttiğiniz hesabın altında çalıştırmalısınız. REST API ile çalışmak üzere sadece bir kullanıcı seçebilirsiniz.

REST API DOKÜMANTASYONUNU AÇIN

REST API aracılığıyla uygulamanın yönetilmesi şu adımlardan meydana gelir:

1. Uygulama ayarlarının geçerli değerleri. Bunu yapmak için bir GET isteği gönderin.

   Örnek:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Uygulama, ayarların yapısı ve değerleri ile bir yanıt gönderecektir. Kaspersky Endpoint Security XML ve JSON biçimlerini destekler.

   Örnek:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Uygulama ayarlarını düzenleyin. GET isteğine yanıt olarak alınan ayarlar yapısını kullanın.

   Örnek:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Uygulama ayarlarını (yük) bir JSON dosyasına (payload.json) kaydedin.

5. JSON dosyasını PKCS7 biçiminde imzalayın.

   Örnek:

   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

Sonuç olarak, isteğiniz yükünü içeren imzalı bir dosya elde edersiniz (`signed_payload.pem`).

6. Uygulama ayarlarını düzenleyin. Bunu yapmak için bir POST isteği gönderin ve istek yükünü içeren imzalı dosyayı ekleyin (`signed_payload.pem`).

Uygulama, yeni ayarları uygular ve uygulama yapılandırma sonuçlarını içeren bir yanıt gönderir (bu yanıt boş olabilir). Bir GET isteği kullanarak ayarların güncellendiğini doğrulayabilirsiniz.

Uygulama hakkında bilgi kaynakları

Bu bölümde, uygulama hakkında bilgi kaynakları açıklanmıştır.

Meselenizin önemine ve aciliyetine bağlı olarak en uygun bilgi kaynağını seçebilirsiniz.

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 Forumda tartışılması

Sorunuza acil bir yanıt gerekmiyorsa Forumumuzda Kaspersky uzmanlarıyla ve diğer kullanıcılarla tartışabilirsiniz.

Forumda var olan başlıkları görebilir, kendi yorumlarınızı gönderebilir, yeni başlıklar açabilirsiniz.

Teknik Destek ile irtibat kurma

Belgelerde veya Kaspersky Endpoint Security hakkındaki diğer bilgi kaynaklarında sorununuza bir çözüm bulamazsanız Teknik Destek ile iletişim kurmanızı öneririz. Teknik Destek, Kaspersky Endpoint Security'yi yükleme ve kullanmayla ilgili sorularınızı yanıtlayacaktır.

Kaspersky, uygulamanın yaşam döngüsü boyunca Kaspersky Endpoint Security için destek sağlar (uygulama yaşam döngüsü sayfasına bakın). Teknik Destek ile irtibat kurmadan önce lütfen destek kurallarını okuyun.

Teknik Destek ile aşağıdaki yollardan biriyle irtibat kurabilirsiniz:

- Teknik destek İnternet sitesini ziyaret ederek
- Kaspersky Teknik Destek'e Kaspersky CompanyAccount portalından bir talep göndererek

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 ve uygulama bileşenlerinin çalışmasıyla ilgili ayrıntılı raporlar hakkında ek bilgi isteyebilir.

Tanılama yaparken Teknik Destek uzmanları aşağıdakileri yaparak uygulama ayarlarını değiştirmenizi isteyebilirler:

- Genişletilmiş tanılama bilgileri alan işlevi etkinleştirerek.
- Standart kullanıcı arabirimi üzerinden erişilemeyen özel ayarları değiştirerek uygulamanın ayrı bileşenlerini yapılandırın.
- Tanılama bilgilerinin depolama 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 vb.) sağlayacak ve hata ayıklama amacıyla kullanılan verilerin kapsamı hakkında sizi bilgilendirecektir. Genişletilmiş tanılama bilgileri, kullanıcının bilgisayarına kaydedilir. Veriler otomatik olarak Kaspersky'ye iletilmez.

Yukarıda sıralanan işlemler yalnızca Teknik Destek uzmanlarının gözetimi altında, onların talimatlarını izleyerek yapılmalıdır. Uygulama ayarlarını kendi başınıza Çevrimiçi Yardım veya Teknik Destek önerilerinde açıklanmayan şekillerde değiştirmek, işletim sisteminin yavaşlamasına ve çökmesine neden olabilir, bilgisayarınızın koruma düzeyini düşürebilir ve işlenen bilgilerin kullanılabilirliğine ve bütünlüğüne zarar verebilir.

İz dosyalarının içeriği ve depolanması

Bilgisayarınızda yer alan bilgilerin güvenliğinden bizzat siz sorumlusunuz. Özellikle verilerin Kaspersky'ye gönderilmeden önce izlemeye ve verilere erişimin sınırlandırılmasına daha fazla dikkat etmelisiniz.

İz dosyaları, uygulama kullanımda olduğu sürece bilgisayarda saklanır ve uygulama kaldırıldığında kalıcı olarak silinir.

Kimlik Doğrulama Aracısının iz dosyaları hariç iz dosyaları `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasöründe saklanır.

İz dosyaları şu şekilde adlandırılır: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

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.

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.
- Bilgisayara kurulu olan donanım üzerindeki veriler (BIOS/UEFI üretici yazılımı verileri gibi). Kaspersky Disk Encryption uygulanırken bu veriler iz dosyalarına yazılır.
- Açık olarak iletildiyse kullanıcı adı ve parola. Bu veriler, İnternet trafiği taraması sırasında iz dosyalarına kaydedilebilir.
- 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, port, 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.
- Ağ trafiği verileri. Trafik izleme bileşenleri (İnternet Denetimi gibi) etkinse bu veriler iz dosyalarına yazılır.
- Kaspersky sunucularından alınan veriler (antivirüs veritabanlarının sürümü gibi).
- Kaspersky Endpoint Security bileşenlerinin durumları ve çalışma verileri.
- Uygulamadaki kullanıcı etkinliği verileri.
- İşletim sistemi olayları.

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.

Performans iz dosyalarının içeriği

Performans iz dosyaları şu şekilde adlandırılır: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Performans iz dosyaları, genel verilere ek olarak işlemci üzerindeki yük, işletim sisteminin ve uygulamaların yükleme süresi hakkında bilgiler ve çalışan işlemler hakkında bilgiler içerir.

AMSI Koruması bileşeni 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

Uygulama web eklentisinin iz dosyaları, Kaspersky Security Center Web Console'un dağıtıldığı bilgisayarda, `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs` dizininde depolanır.

Uygulama web eklentisinin iz dosyaları şu şekilde adlandırılır: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Web Console, kurulumdan sonra verileri yazmaya başlar ve Web Console kaldırıldıktan sonra iz dosyalarını siler.

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 değiştir* 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

Kimlik Doğrulama Aracısı iz dosyası System Volume Information klasöründe saklanır ve şu şekilde adlandırılır: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

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.

Uygulama çalışmasını izleme

Uygulama izleme, uygulama tarafından gerçekleştirilen işlemlerin ayrıntılı bir kaydı ve uygulamanın çalışması sırasında meydana gelen olaylar hakkındaki mesajlardır. İzleme işlemi sırasında uygulama, farklı uygulama bileşenlerinin çalışmasıyla ilgili verileri içeren bir dizi dosya oluşturur (örneğin, SRV.log, WD.log ve diğerleri).

Uygulama izleme, Kaspersky Teknik Desteğin denetimi altında gerçekleştirilmelidir.

Uygulama izi dosyası oluşturmak için:

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Açılan pencerede **Destek Araçları** düğmesine tıklayın.
3. Uygulamanın çalışmasının izlenmesini etkinleştirmek veya devre dışı bırakmak için **Uygulama izlemeyi etkinleştir** geçiş düğmesini kullanın.
4. **İzleme** açılır listesinden bir uygulama izleme modu seçin:
   - **Boyut sınırlaması ile**. Boyutları ve sayıları sınırlı dosya kümelerine izleri kaydedin ve maksimum boyuta ulaşıldığında eski dosyaların üzerine yazın. Bu mod seçildiğinde, dönüş için maksimum dosya kümesi sayısını ve her dosya kümesi için maksimum boyutu tanımlayabilirsiniz.

     Uygulama varsayılan olarak beş küme izleme dosyası kaydeder. Her bir dosya kümesinin boyutu 3072 MB'dir. Bu şekilde, izleme dosyalarını kaydetmek için 15 GB boş disk alanına ihtiyacınız vardır.
   - **Sınırlamalar olmadan**. Bir izleme dosyasını kaydedin (boyut sınırı yoktur).
5. **Düzey** açılır listesinde izleme düzeyini seçin:
   - **Normal** seçeneği, iz dosyasının tüm hatalar ve uyarılarla ilgili mesajların yanı sıra uygulamanın normal çalışmasına ilişkin bilgileri de kaydetmesi anlamına gelir (varsayılan ayar).
   - **Ayrıntılar** seçeneği, iz dosyasının uygulamanın çalışmasıyla ilgili tüm bilgileri kaydetmesi anlamına gelir.

Uygulama izleme ayarlarını komut satırından yönetiyorsanız, ek izleme düzeyleri de kullanılabilir. Gerekli izleme düzeyini bir Teknik Destek uzmanına danışmanız önerilir. Teknik Destek'e danışamazsanız izleme düzeyini **Normal**'e ayarlayın.

Komut satırında uygulama izleme etkinleştirilmişse ve izleme düzeyi **Normal** veya **Ayrıntılar** dışında bir değer olarak ayarlanmışsa, **Düzey** açılır listesi **Normal** olarak ayarlanır.

6. İzleme sürecini durdurmak için **Destek Araçları** penceresine dönün ve izlemeyi devre dışı bırakın.

setup.ini dosyasını kullanarak veya uygulamayı komut satırından yüklerken de iz dosyaları oluşturabilirsiniz.

Sonuç olarak, `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasöründe uygulama çalışma izleri dosyaları oluşturulur. İz dosyaları oluşturulduktan sonra bu dosyaları Kaspersky Teknik Desteğine gönderin.

Kaspersky Endpoint Security, uygulama kaldırıldığında izleme dosyalarını otomatik olarak siler. Dosyaları manuel olarak da silebilirsiniz. Bunu yapmak için izlemeyi devre dışı bırakarak uygulamayı durdurmanız gerekir.

Uygulama performansı izleme

Kaspersky Endpoint Security, uygulamanın kullanımı sırasında meydana gelen bilgisayar çalışma sorunları hakkında bilgiler almanıza izin verir. Örneğin uygulamanın yüklenmesinden sonra işlerim sisteminin yüklenmesinde meydana gelen gecikmeler hakkında bilgi alabilirsiniz. Bunu yapmak için Kaspersky Endpoint Security performans iz dosyaları oluşturur. *Performans izleme*, Kaspersky Endpoint Security'nin performans sorunlarını tanılamak amacıyla uygulama tarafından gerçekleştirilen eylemlerin günlüğe kaydedilmesidir. Kaspersky Endpoint Security bilgileri almak için Windows Olay İzleme (ETW) hizmetini kullanır. Kaspersky Endpoint Security sorunlarının tanılanmasından ve bu sorunlar için sebeplerin tespit edilmesinden Kaspersky Teknik desteği sorumludur.

Uygulama izleme, Kaspersky Teknik Desteğin denetimi altında gerçekleştirilmelidir.

Bir performans izi dosyası oluşturmak için:

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Açılan pencerede **Destek Araçları** düğmesine tıklayın.
3. Performans işleminin izlenmesini etkinleştirmek veya devre dışı bırakmak için **Performans izlemeyi etkinleştir** geçiş düğmesini kullanın.
4. **İzleme** açılır listesinden bir uygulama izleme modu seçin:
   - **Boyut sınırlaması ile**. Boyutları ve sayıları sınırlı dosyalara izleri kaydedin ve maksimum boyuta ulaşıldığında eski dosyaların üzerine yazın. Bu mod seçilirse, her dosya için maksimum boyutu belirleyebilirsiniz.
   - **Sınırlamalar olmadan**. Bir izleme dosyasını kaydedin (boyut sınırı yoktur).
5. **Düzey** açılır listesinde izleme düzeyini seçin:
   - **Hafif**. Kaspersky Endpoint Security performansla ilgili en önemli işletim sistemi işlemlerini analiz eder.
   - **Ayrıntılı**. Kaspersky Endpoint Security performansla ilgili tüm işletim sistemi işlemlerini analiz eder.

6. **İzleme türü** açılır listesinden şu izleme türünü seçin:

   - **Temel bilgiler**. Kaspersky Endpoint Security işletim sistemi çalışırken işlemleri analiz eder. Tarayıcıdan İnternete erişememe gibi bir sorun işletim sistemi yüklendikten sonra da yaşanmaya devam ediyorsa bu izleme türünü seçin.

   - **Yeniden başlatmada**. Kaspersky Endpoint Security sadece işletim sistemi yüklenirken işlemleri analiz eder. İşletim sistemi yüklendikten sonra, Kaspersky Endpoint Security izlemeyi durdurur. Sorun işletim sisteminin yüklenmesinde gecikmeyle alakalı ise bu izleme türünü seçin.

7. Bilgisayarı yeniden başlatarak sorunun tekrar ortaya çıkmasını sağlamaya çalışın.

8. İzleme sürecini durdurmak için Destek Araçları penceresine dönün ve izlemeyi devre dışı bırakın.

   Sonuç olarak, `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasöründe bir performans iz dosyası oluşturulur. İz dosyası oluşturulduktan sonra bu dosyayı Kaspersky Teknik Desteğine gönderin.

Döküm yazımı

Döküm dosyası, döküm dosyası oluşturulduğu anda Kaspersky Endpoint Security işlemlerinin çalışma belleği hakkındaki tüm bilgileri içerir.

> Kaydedilen döküm dosyaları gizli bilgiler içerebilir. Verilere erişimi kontrol etmek için döküm dosyalarının güvenliğini ayrı olarak sağlamalısınız.

Döküm dosyaları, uygulama kullanımda olduğu sürece bilgisayarda saklanır ve uygulama kaldırıldığında kalıcı olarak silinir. Döküm dosyaları `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` klasöründe saklanır.

Yönetim Konsolu'nda (MMC) döküm yazımını etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.

2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.

4. **Hata ayıklama bilgileri** bloğunda **Ayarlar** düğmesine tıklayın.

5. Açılan pencerede, uygulama döküm yazımını etkinleştirmek veya devre dışı bırakmak için **Döküm yazımını etkinleştir** onay kutusunu kullanın.

6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da döküm yazımını etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel Ayarlar** → **Teknik Destek** bölümüne gidin.

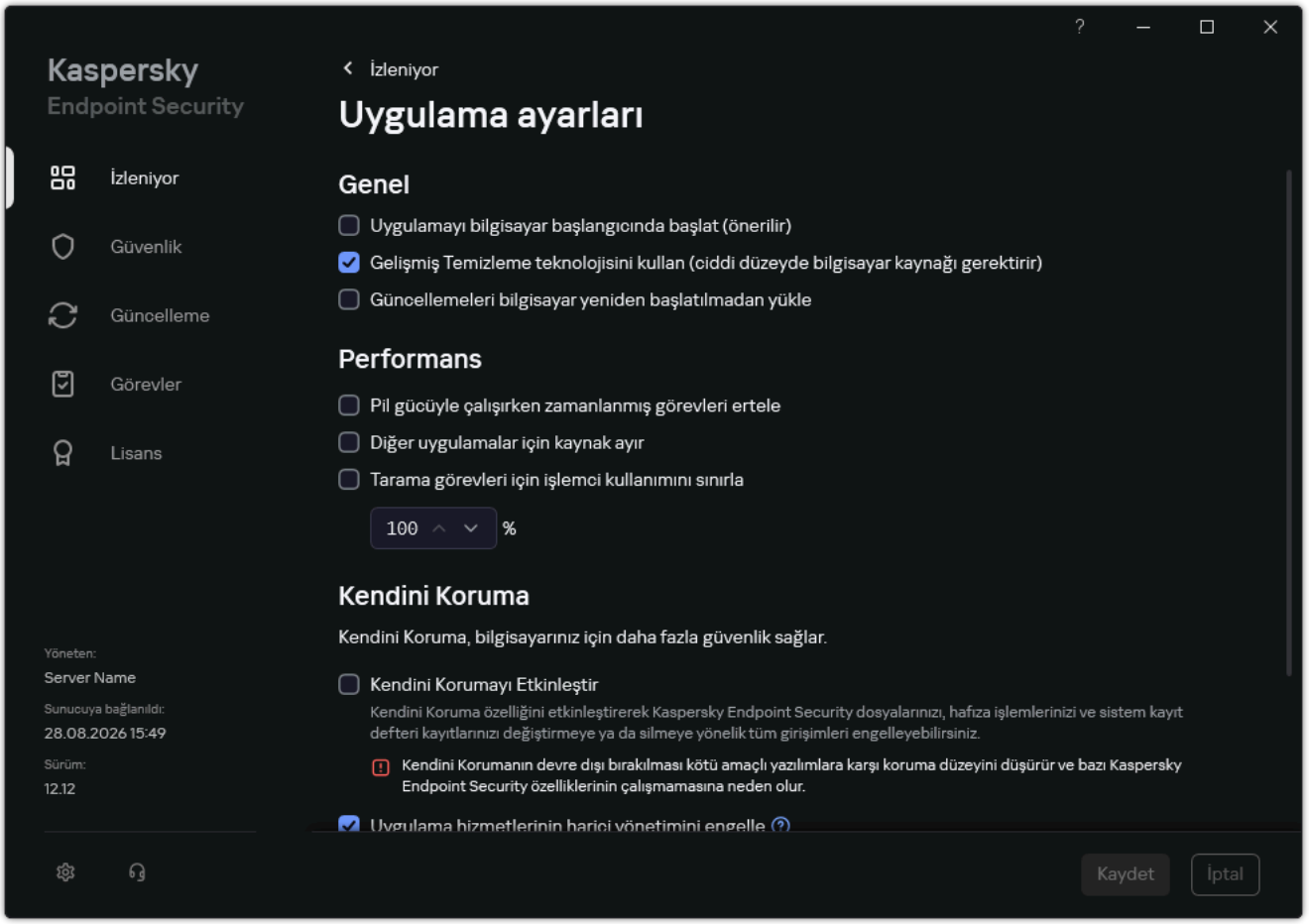
5. **Hata ayıklama bilgileri** bloğunda, uygulama döküm yazımını etkinleştirmek veya devre dışı bırakmak için **Döküm yazımı ETKİN** onay kutusunu kullanın.

6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde döküm yazımını etkinleştirme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. **Hata ayıklama bilgileri** bloğunda, uygulama döküm yazımını etkinleştirmek veya devre dışı bırakmak için **Döküm yazımını etkinleştir** onay kutusunu kullanın.

4. Değişikliklerinizi kaydedin.

Döküm dosyalarını ve iz dosyalarını koruma

Döküm dosyaları ve iz dosyaları işletim sistemi hakkında bilgiler içerir ve kullanıcı verilerini de içerebilir. Bu tür verilere yetkisiz erişimin engellenmesi için döküm dosyaları ve iz 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 iz dosyalarının yazılmasına izin veren kullanıcı tarafından erişilebilir.
- İz dosyalarına sadece sistem yöneticisi ve yerel yönetici tarafından erişilebilir.

Yönetim Konsolu'nda (MMC) döküm dosyalarının ve izleme dosyalarının korunmasını etkinleştirme

1. Kaspersky Security Center Yönetim Konsolu ağacında **İlkeler** seçimini yapın.
2. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
3. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
4. **Hata ayıklama bilgileri** bloğunda **Ayarlar** düğmesine tıklayın.
5. Açılan pencerede, dosya korumasını etkinleştirmek veya devre dışı bırakmak için **Bellek dökümü ve iz dosyaları korumasını etkinleştir** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

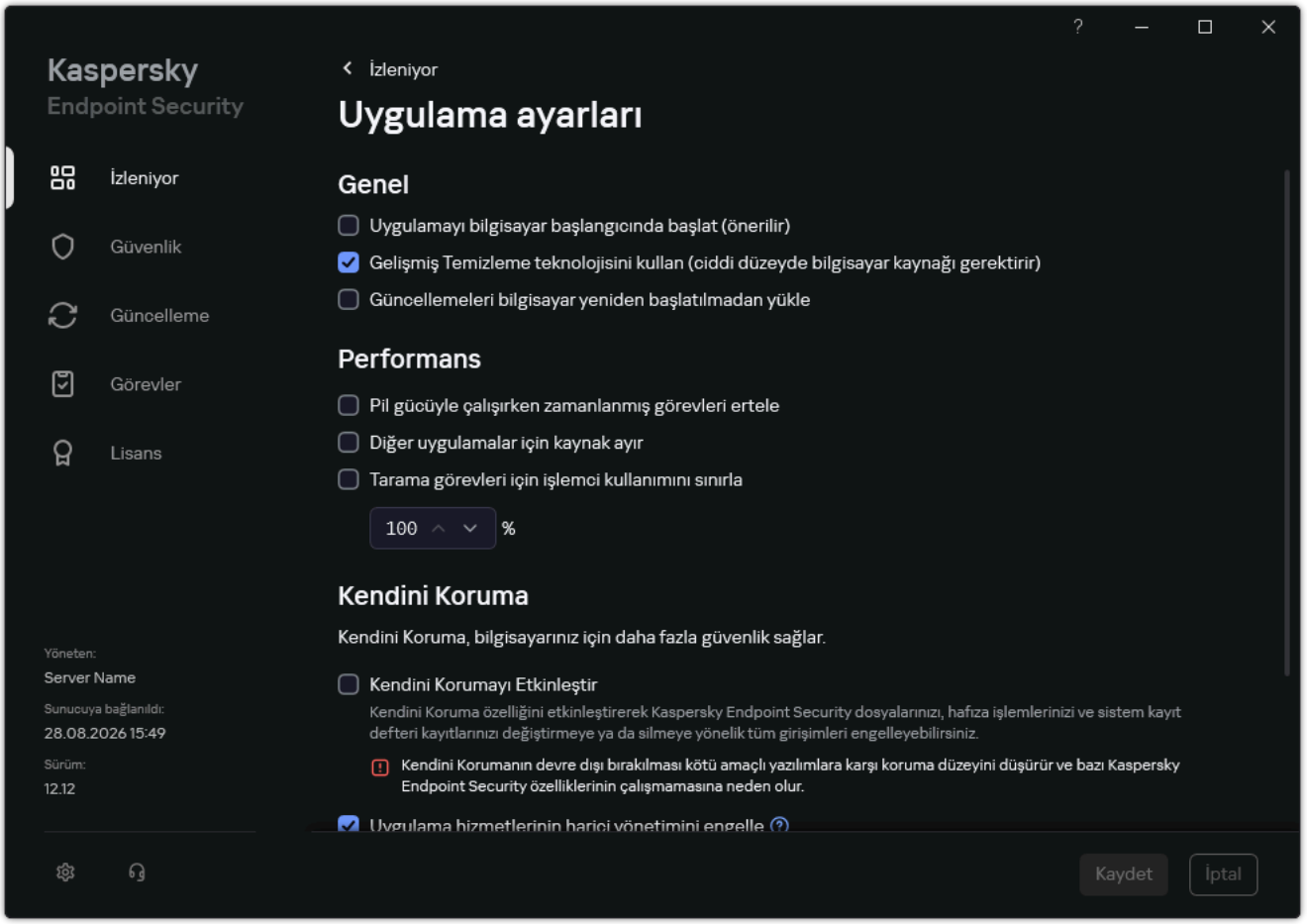
Web Console ve Cloud Console'da döküm dosyalarının ve izleme dosyalarının korunmasını etkinleştirme

1. Web Console'un ana penceresinde **Varlık yönetimi** → **İlkeler**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Teknik Destek** bölümüne gidin.
5. **Hata ayıklama bilgileri** bloğunda, dosya korumasını etkinleştirmek veya devre dışı bırakmak için **Bellek dökümü ve iz dosyaları koruması ETKİN** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Uygulama arabiriminde döküm dosyalarının ve izleme dosyalarının korunmasını etkinleştirme

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.



Kaspersky Endpoint Security for Windows ayarları

3. **Hata ayıklama bilgileri** bloğunda, dosya korumasını etkinleştirmek veya devre dışı bırakmak için **Bellek dökümü ve iz dosyaları korumasını etkinleştir** onay kutusunu kullanın.
4. Değişikliklerinizi kaydedin.

Koruma etkinken yazılan döküm dosyaları ve iz dosyaları bu işlev devre dışı bırakıldıktan sonra bile korunur.

İşletim sistemi verilerini alma (Kaspersky Get System Info)

Kaspersky Endpoint Security uygulaması yüklendikten sonra işletim sistemi veya bir uygulama düzgün çalışmayabilir. Uygulama ile bilgisayar bileşenlerinin yazılımları veya sürücüleri arasında bir çakışma vardır.

Kaspersky Teknik Destek, sorunun nedenini belirlemek için Kaspersky Sistem Bilgisi AI yardımcı programından (bundan sonra GSI olarak anılacaktır) bir rapor ister. Yardımcı programın kullanımı hakkında ayrıntılar için Kaspersky Bilgi Bankası'na bakın.

Sınırlamalar ve uyarılar

Kaspersky Endpoint Security'de, uygulamanın çalışması için kritik olmayan bazı sınırlamalar vardır.

Uygulama yükleniyor

- Microsoft Windows 10, Microsoft Windows Server 2016 ve Microsoft Windows Server 2019 işletim sistemleri desteği hakkındaki ayrıntılar için lütfen Teknik Destek Bilgi Bankası'na bakın.
- Microsoft Windows 11 ve Microsoft Windows Server 2022 işletim sistemleri desteği hakkındaki ayrıntılar için lütfen Teknik Destek Bilgi Bankası'na bakın.
- Uygulama, virüs bulaşmış bir bilgisayara yüklendikten sonra, kullanıcıyı bilgisayar taraması çalıştırma ihtiyacı konusunda bilgilendirmez. Uygulamayı etkinleştirirken sorunlarla karşılaşabilirsiniz. Bu sorunları çözmek için bir Kritik Alanları Tarama başlatın.
- Setup.ini ve setup.reg dosyalarında ASCII olmayan karakterler (örneğin, Rusça harfler) kullanılıyorsa, dosyayı notepad.exe kullanarak düzenlemeniz ve UTF-16LE kodlamasını kullanarak kaydetmeniz önerilir. Diğer kodlamalar desteklenmez.
- Uygulama, kurulum paketi ayarlarında uygulama yükleme yolunu belirtirken ASCII olmayan karakterlerin kullanılmasını desteklemez.
- Uygulama ayarları bir CFG dosyasından içe aktarıldığında, Kaspersky Security Network'e katılımı tanımlayan ayarın değeri uygulanmaz. Ayarları içe aktardıktan sonra, lütfen Kaspersky Security Network Bildirimi metnini okuyun ve Kaspersky Security Network'e katılmak için rızanızı onaylayın. Bildirim metnini uygulama arabiriminde veya uygulama dağıtım kitini içeren klasörde bulunan ksn_*.txt dosyasında okuyabilirsiniz.
- Şifrelemeyi (FLE veya FDE) veya Aygıt Denetimi bileşenini kaldırmak ve sonra yeniden yüklemek isterseniz, yeniden yüklemeden önce sistemi yeniden başlatmanız gerekir.
- Microsoft Windows 10 işletim sistemini kullanırken, Dosya Düzeyinde Şifreleme (FLE) bileşenini kaldırdıktan sonra sistemi yeniden başlatmanız gerekir.
- Uygulama bileşenlerini teker teker kaldırırken (örneğin, *Uygulama bileşenlerini değiştirme* görevi kullanılarak), bilgisayarın yeniden başlatılması gerekebilir.
- *Uygulama bileşenlerini değiştirme* görevinin özelliklerinde, kurulum modunu değiştirirken (**Ayrı mod** / **Birleştirilmiş mod**), bileşen kümesinin modlar arasında senkronizasyonu desteklenmez. Uygulama, siz görev özelliklerini yeniden açtıktan sonra bileşen setini modlar arasında senkronize eder.
- Uygulamanın yüklenmesi, *Bilgisayarınızda adı eksik veya okunamayan bir uygulamanın yüklü olduğunu* belirten bir hatayla sona erebilir. Bu, uyumsuz uygulamaların veya bunların parçalarının bilgisayarınızda kaldığı anlamına gelir. Uyumsuz uygulamaların kalıntılarını kaldırmak için Kaspersky CompanyAccount aracılığıyla Kaspersky Teknik Destek'e durumun ayrıntılı bir açıklamasını içeren bir talep gönderin.
- Kaspersky Endpoint Security'nin kaldırılmasını iptal ettiyseniz, bilgisayarı yeniden başlattıktan sonra uygulama kurtarmayı başlatın.
- Uygulama, Microsoft .NET Framework 4.0 veya sonraki bir sürümünü gerektirir. Microsoft .NET Framework 4.6.1'de güvenlik açıkları vardır. Microsoft .NET Framework 4.6.1 kullanıyorsanız, güvenlik güncellemelerini yüklemeniz gerekir. Microsoft .NET Framework güvenlik güncellemeleriyle ilgili ayrıntılar için Microsoft Teknik Destek web sitesine bakın.

- Uygulama, bir sunucu işletim sisteminde Kaspersky Endpoint Agent bileşeni seçilerek başarısız bir şekilde kurulursa ve *Windows Installer Düzenleyicisi Hatası* penceresi görüntülenirse, Microsoft destek web sitesindeki talimatlara bakın.

- Uygulama etkileşimli olmayan modda yerel olarak yüklenmişse, yüklü bileşenleri değiştirmek için sağlanan setup.ini dosyasını kullanın.

- Windows 7'nin bazı yapılandırmalarında Kaspersky Endpoint Security for Windows yüklendikten sonra, Windows Defender çalışmaya devam eder. Sistem performansının düşmesini önlemek için Windows Defender'ı manuel olarak devre dışı bırakmanız önerilir.

- Kaspersky Endpoint Security for Windows'u Kaspersky Security for Windows Server (KSWS) ve Windows Defender uygulamalarının yüklü olduğu bir sunucuya yüklerken sistemi yeniden başlatmanız gerekir. Sistemi yeniden başlatmadan uygulama yüklemeyi etkinleştirmiş olsanız bile, sistemin yeniden başlatılması gerekir. Windows Defender for Windows Server, Kaspersky Endpoint Security for Windows ile uyumlu olmayan yazılımlar listesine dahil edilmiştir. Uygulamayı yüklemeden önce, yükleyici Windows Defender for Windows Server'ı kaldırır. Uyumsuz yazılımın kaldırılması, sistemin yeniden başlatılmasını gerektirir.

- Kaspersky Endpoint Security for Windows'u (KES) Kaspersky Security for Windows Server (KSWS) yüklü bir sunucuya yüklemeden önce KSWS Parola Korumasını kapatmanız gerekir. KSWS'den KES'e geçiş yaptıktan sonra, uygulama ayarlarında Parola Korumasını etkinleştirin.

- Uygulamayı Veeam Backup & Replication yazılımının kurulu olduğu Windows 7 veya Windows Server 2008 R2 çalıştıran bilgisayarlara yüklemek için bilgisayarınızı yeniden başlatmanız ve yüklemeyi tekrar çalıştırmanız gerekebilir.

- Kaspersky Small Office Security'den (KSOS) Parola Koruması etkinleştirilmiş Kaspersky Endpoint Security'ye (KES) geçiş, KSOS yapı 21.16.*.*'dan itibaren kullanılabilir. KSOS'un önceki sürümlerini taşımak için Parola Korumasını devre dışı bırakmanız veya KSOS'u manuel olarak kaldırmanız gerekir. Parola Koruması devre dışı bırakılarak KSOS'tan KES'e geçiş doğru şekilde gerçekleştirilir.

- Kaspersky Endpoint Security'yi önyüklenebilir bir çıkarılabilir sürücüye yükleyemezsiniz. Yükleme sırasında Kaspersky Endpoint Security bir hata mesajı görüntüler: *Geçersiz bir klasör veya sürücü seçtiniz. Uygulama yerel bir sabit sürücüye yüklenmelidir*. Uygulamayı üçüncü taraf araçlar kullanarak çıkarılabilir bir sürücüye yüklemeyi başarırsanız, bu, önyükleme işlemi sırasında işletim sisteminin çökmesine (BSOD) neden olabilir. Bu, Kaspersky Endpoint Security'nin Windows To Go ve benzeri çözümleri desteklemediği anlamına gelir. Bir bilgisayarı çıkarılabilir bir sürücüden taramak için ücretsiz Kaspersky Rescue Disk uygulamasını kullanabilirsiniz.

- Çok kullanıcılı RDP oturumları olan bir terminal sunucusuna ağ bileşenleriyle birlikte Kaspersky Endpoint Security'yi yüklemek, bazı özel noktalara dikkat edilmesini gerektirir. İşletim sistemi, Yönetici oturumu sona erdikten sonra tüm kullanıcı oturumlarının sona ermesini zorlar. Terminal sunucusuna bağlanmak için sunucuyu yeniden başlatmanız veya sisteme yerel olarak oturum açmanız gerekir. Bu tür davranışları Windows işletim sisteminin çalışma biçimi belirler.

- Kaspersky Endpoint Security for Windows (yapı 12.11.0.2004) ve Kaspersky Endpoint Security for Linux (yapı 12.4.0.1354) web eklentileri Kaspersky Security Center 16.0 veya Kaspersky Security Center 16.1'de yüklüyse, Kaspersky Endpoint Security for Windows web eklentisinin 12.11.0.6004 sürümüne güncellenmesi Kaspersky Endpoint Security for Linux ilkelerinde sorunlara yol açabilir.

  Olası çözüm: **Ayarlar** → **Web eklentileri** penceresine gidin ve Kaspersky Endpoint Security for Windows web eklentisini, Kaspersky Endpoint Security for Linux web eklentisini ve Unified Protection and Management Plug-in'i listeden kaldırın. Ardından önce Kaspersky Endpoint Security for Linux web eklentisini, sonra da Kaspersky Endpoint Security for Windows web eklentisini yükleyin.

- Web Console'da, Kaspersky Endpoint Security 12.11 for Windows'un kurulum paketi özelliklerinde bileşen listesi yanlış görüntüleniyor. Ayrı bir bileşen olan Şifreleyici Önleyici, uygulamanın bu sürümünde mevcut değildir. Paylaşılan klasörlerin harici şifreleme işlevine karşı korunması Davranış Tespiti bileşenine dahildir. Windows için Kaspersky Endpoint Security 12.12'de bu işlev ayrı bir bileşendir. Aynı zamanda, Yönetim Konsolu'nda (MMC) bileşenlerin listesi doğru şekilde görüntülenir.

- Web eklentisinin 7.0 veya sonraki bir sürümü kullanıldığında, Kaspersky Endpoint Security 14.1 ve önceki sürümlerin kurulum paketi özelliklerinde varsayılan olarak kurulmak üzere seçilen bileşenlerin listesi yanlış görüntülenir. Kurulum paketi oluşturulurken bu liste değiştirilmezse uygulama, ilgili sürüm için belirtilen varsayılan bileşen kümesiyle yüklenir.

Uygulamayı yükseltme

- 11.0.0 sürümünden itibaren, Kaspersky Endpoint Security for Windows MMC eklentisini önceki eklenti sürümünün üzerine yükleyebilirsiniz. Önceki bir eklenti sürümüne dönmek için, var olan eklentiyi silin ve eklentinin önceki bir sürümünü yükleyin.

- Kaspersky Endpoint Security 11.0.0 veya 11.0.1 for Windows'u yükseltirken, *Veritabanlarının ve uygulama modüllerinin güncellemesi*, *Kritik Alanları Tarama*, *Özel Tarama* ve *Uygulama Bütünlüğü Kontrolü* görevleri için yerel görev zamanlama ayarları kaydedilmez.

- Windows 10 sürüm 1903 ve 1909 çalıştıran bilgisayarlarda, Kaspersky Endpoint Security 10 for Windows Service Pack 2 Bakım Sürümü 3 (derleme 10.3.3.275), Service Pack 2 Bakım Sürümü 4 (derleme 10.3.3.304), Dosya Düzeyinde Şifreleme (FLE) bileşeninin yüklü olduğu 11.0.0 ve 11.0.1, bir hatayla sona erebilir. Bunun nedeni, Windows 10 sürüm 1903 ve 1909'da Kaspersky Endpoint Security for Windows'un bu sürümlerinde dosya şifrelemenin desteklenmemesidir. Bu yükseltmeyi yüklemeden önce, dosya şifreleme bileşenini kaldırmanız önerilir.

- Uygulama, Microsoft .NET Framework 4.0 veya sonraki bir sürümünü gerektirir. Microsoft .NET Framework 4.6.1'de güvenlik açıkları vardır. Microsoft .NET Framework 4.6.1 kullanıyorsanız, güvenlik güncellemelerini yüklemeniz gerekir. Microsoft .NET Framework güvenlik güncellemeleriyle ilgili ayrıntılar için Microsoft Teknik Destek web sitesine bakın.

- Kaspersky Endpoint Security'yi yükseltirken uygulama, Kaspersky Security Network Bildirimi kabul edilene kadar KSN'nin kullanımını devre dışı bırakır. Ayrıca, bilgisayar durumu Kaspersky Security Center'da *Kritik* olarak değiştirilebilir; *KSN sunucuları kullanılabilir değil* olayı alınır. Kaspersky Managed Detection and Response bileşenini kullandığınızda, çözüm çalıştırıldığında ihlaller hakkında olaylar alırsınız. Kaspersky Managed Detection and Response bileşeninin çalışması için KSN'nin kullanılması gereklidir. Kaspersky Endpoint Security, yöneticinin KSN kullanım şartlarını kabul ettiği ilkeyi uyguladıktan sonra KSN kullanımını etkinleştirilir. Kaspersky Security Network Bildirimi kabul edildikten sonra, Kaspersky Endpoint Security çalışmasına devam eder.

- Kaspersky Endpoint Security'yi yeniden başlatma yapmadan 11.10.0 veya sonraki bir sürüme yükselttikten sonra, bilgisayarda iki Kaspersky Endpoint Security uygulaması kurulu olacaktır. Uygulamanın önceki sürümünü manuel olarak kaldırmayın. Bilgisayar yeniden başlatıldığında önceki sürüm otomatik olarak kaldırılacaktır.

- Microsoft Windows 11 çalıştıran bir bilgisayarda Kaspersky Endpoint Security'yi yükselttikten sonra, dosya içerik menüsü hem önceki hem de yeni uygulama sürümleri için öğeler görüntüleyebilir. Dosya içerik menüsünün doğru çalıştığından emin olmak için bilgisayarınızı iki kez yeniden başlatın.

- Uygulamanın Kendini Koruma özelliği kapatılırsa ve tüm ağ bağdaştırıcıları durdurulursa, uygulamanın ağ bileşenleri uygulama yükseltmesinin sona ermesi ile bilgisayarın yeniden başlatılması arasında çalışmayacaktır. Uygulamanın ağ bileşenleri arasında Web Tehdidi Koruması, Posta Tehdidi Koruması, Ağ Tehdidi Koruması, Güvenlik Duvarı, Sunucu İzinsiz Girişi Önleme ve İnternet Denetimi bulunmaktadır. Uygulamanın düzgün çalışması için bilgisayarı yeniden başlatın.

- BadUSB Saldırısı Önleme bileşeni, uygulama yükseltmesinin sona ermesi ile bilgisayarın yeniden başlatılması arasında çalışmaz. Uygulamanın düzgün çalışması için bilgisayarı yeniden başlatın.

- Önceki yükseltme işlemi tamamlanmamışsa, uygulama yükseltilemez. Uygulamanın düzgün çalışması için bilgisayarı yeniden başlatın.
- Uygulama Kaspersky Endpoint Security 11 for Windows'tan önceki sürümlerden yükseltildikten sonra bilgisayarın yeniden başlatılması gerekir.
- Kaspersky Security Center Cloud Console kullanarak Kaspersky Endpoint Security'yi yönetiyorsanız, uygulamayı yerel olarak güncellemek mümkün değildir. Uygulamayı yerel olarak güncellerken, Kaspersky Security Center Cloud Console için Veri İşleme Sözleşmesini kabul etmek mümkün değildir.

Arm mimarisi desteği

- Arm tabanlı sanal makinelerde Kaspersky Endpoint Security'nin Light Agent modunda kurulumu desteklenmemektedir.
- Kaspersky Disk Encryption, ARM tabanlı bilgisayarlarda desteklenmemektedir.
- Arm tabanlı bilgisayarlarda dosya şifreleme özelliği desteklenmemektedir.
- Arm tabanlı bilgisayarlarda çıkarılabilir sürücülerin şifrelenmesi desteklenmemektedir.
- Arm64 için Windows 11 çalıştıran bilgisayarlarda, EDR Agent Bitdefender Endpoint Security Tools ile uyumlu değildir.
- Ses sinyali koruma özelliği ve web kamerası erişim koruma özelliği, Arm tabanlı bilgisayarlarda desteklenmemektedir.
- Arm tabanlı bilgisayarlarda, Posta Tehdidi Koruması uzantısı Outlook 2016, Outlook 2021, Outlook 2024 ve Arm64 için Outlook 365'in 32 bit ve 64 bit sürümlerini destekler.
- Kaspersky Endpoint Security, Arm mimarisine yönelik nesneleri Kaspersky Sandbox'a göndermez.
- Arm tabanlı bilgisayarlarda yazdırma denetimi desteklenmemektedir.
- Arm tabanlı bilgisayarlarda, *IOC Taraması* yalnızca aşağıdaki posta istemcilerinden gelen e-posta dosyalarını destekler: Outlook 2016 ile Outlook 2021, 2024 ve 365'in 32 bit ve 64 bit sürümleri (Arm64 için).
- Arm64 için Windows 11 çalıştıran bilgisayarlarda, işletim sistemi belirteçte geçerli bir sertifika algılayamadığı için belirteç tabanlı kimlik doğrulama kullanılamayabilir. Bu davranış, işletim sisteminin belirteç yazılımıyla etkileşim biçiminden kaynaklanır. Örneğin işletim sisteminde, belirtecin çalışması için gereken sürücüler bulunmayabilir. Bu durumda Kaspersky Endpoint Security de belirteç tabanlı kimlik doğrulamayı (Parola Koruması) desteklemez. Kullanıcı kimlik bilgileri gibi diğer kimlik doğrulama yöntemlerini kullanabilirsiniz.

Sunucu platformları için destek

- *Veri tekilleştirmenin* etkin olduğu sunucularda fsdmhost.exe dosyasını güvenilir uygulamalar listesine eklemeniz gerekir. Bu, uygulamanın performansının optimize edilmesine ve işlemcinin aşırı yüklenmesinin önlenmesine yardımcı olur.
- ReFS dosya sistemi kısıtlamalar ile desteklenmektedir:
  - Kaspersky Endpoint Security, tehdit temizleme olaylarını hatalı şekilde işleyebilir. Örneğin, uygulama kötü amaçlı bir dosyayı silmişse, rapor Nesne işlenmedi girdisine sahip olabilir. Aynı anda, Kaspersky Endpoint Security, uygulama ayarlarına göre tehditleri temizler. Kaspersky Endpoint Security ayrıca aynı nesne için *Nesne yeniden başlatmada temizlenecek* olayının bir kopyasını oluşturabilir.
  - Dosya Tehdidi Koruması bazı tehditleri atlayabilir. Aynı zamanda, Kötü Amaçlı Yazılım Taraması düzgün çalışır.

- *Kötü Amaçlı Yazılım Taraması* görevi başlatıldıktan sonra, iChecker ile eklenen istisnalar sunucu yeniden başlatıldığında sıfırlanır.
- iSwift teknolojisi desteklenmemektedir. Kaspersky Endpoint Security, iSwift teknolojisi kullanılarak eklenen tarama istisnalarını dikkate almaz.
- Kaspersky Endpoint Security, eğer meicar.exe dosyası Kaspersky Endpoint Security yüklenmeden önce de bilgisayarda varsa, eicar.com ve susp-eicar.com dosyalarını tespit etmez.
- Kaspersky Endpoint Security, tehdit temizleme bildirimlerini hatalı şekilde görüntüleyebilir. Örneğin, uygulama önceden temizlenmiş bir tehdit için bir tehdit bildirimi görüntüleyebilir.

- Dosya Düzeyinde Şifreleme (FLE) ve Kaspersky Disk Encryption (FDE) teknolojileri sunucu platformlarında desteklenmez. Aynı zamanda Kaspersky Endpoint Security, veri şifreleme olaylarını hatalı şekilde işleyebilir.
- Sunucu işletim sistemlerinde, gelişmiş temizleme ihtiyacına ilişkin herhangi bir uyarı görüntülenmez.
- Microsoft Windows Server 2008 desteği artık devam ettirilmeyecek. Uygulamanın, Microsoft Windows Server 2008 işletim sistemini çalıştıran bir bilgisayara yüklenmesi desteklenmez.
- Microsoft Data Protection Manager (DPM) dağıtılmış bir sunucuya yüklenen Kaspersky Endpoint Security, DPM'nin arızalanmasına neden olabilir. Bu durum DPM işlemindeki sınırlamalarla ilgilidir. Arızaları ortadan kaldırmak için Dosya Tehdidi Koruması bileşeni için istisnalara yerel sunucu sürücüleri ve *Kötü Amaçlı Yazılım Taraması* görevleri eklemelisiniz.
- Server Core modu sınırlamalarla desteklenir:
  - Yerel grafik kullanıcı arabirimi kullanılamaz; buna bildirimler, açılır bildirimler ve diğer arabirim denetimleri dahildir. Uygulama, aşağıdaki pencereler de dahil olmak üzere bilgi istemi pencerelerini görüntüleyemez:
    - Uygulama sürümü ve modül yükseltme için onay sor.
    - Bilgisayarı yeniden başlatmayı sor.
    - Proxy sunucusu kimlik doğrulama bilgilerini sor;
    - Bir cihaza erişim kazanmayı soru (Cihaz Denetimi).
  - Şu bileşenler mevcut değildir: Web Tehdidi Koruması, Posta Tehdidi Koruması, İnternet Denetimi, BadUSB Saldırısı Önleme.
  - Köprüleme Önleme mevcut değildir.
  - Kaspersky Security Network Bildirimi yalnızca Kaspersky Security Center konsolundaki uygulama ilkesinde kabul edilebilir.
  - BitLocker Drive Encryption, yalnızca Güvenilir Platform Modülü (TPM) ile kullanılabilir. Uygulama, önyükleme öncesi kimlik doğrulaması için parola istemi penceresini görüntüleyemediğinden, şifreleme için bir PIN/parola kullanılamaz. İşletim sisteminde Federal Bilgi İşleme standardı (FIPS) uyumluluk modu etkinse, sürücüyü şifrelemeye başlamadan önce şifreleme anahtarını kaydetmek için çıkarılabilir bir sürücü bağlayın.

Sanal platformlar için destek

- Hyper-V sanal makinelerde tam disk şifreleme (FDE) desteklenmez.
- Citrix sanal platformlarında tam disk şifreleme (FDE) desteklenmez.

- Windows 10 Enterprise çoklu oturum ve Windows 11 Enterprise çoklu oturum işletim sistemleri bazı sınırlamalarla desteklenir:
  - Kaspersky Endpoint Security, tıpkı sunuculardaki etkin tehditleri temizlerken olduğu gibi, etkin tehditleri kullanıcıyı bilgilendirmeden temizler. İşletim sistemi çoklu oturum modunda çalışmaya devam ettiğinden, tehdit anında çözülmediği takdirde diğer etkin kullanıcılar verilerini kaybedebilir.
  - Tam disk şifreleme (FDE) desteklenmez.
  - BitLocker yönetimi desteklenmez.
  - Kaspersky Endpoint Security'nin çıkarılabilir sürücülerle kullanımı desteklenmez. Microsoft Azure altyapısı, çıkarılabilir sürücüleri ağ sürücüleri olarak tanımlar.
- Citrix sanal platformlarında dosya düzeyinde şifrelemenin (FLE) yüklenmesi ve kullanılması desteklenmez.
- Kaspersky Endpoint Security for Windows ile Citrix PVS uyumluluğunu desteklemek için, **Citrix PVS ile uyumluluğu sağla** seçeneği etkinleştirilmiş olarak kurulum gerçekleştirin. Bu seçenek Kurulum Sihirbazı'nda veya /pCITRIXCOMPATIBILITY=1 `/pCITRIXCOMPATIBILITY=1` kullanılarak etkinleştirilebilir. Uzaktan kurulum durumunda, KUD dosyası aşağıdaki parametre eklenerek düzenlenmelidir: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Klonlamaya başlamadan önce, vDisk kullanan sanal makineleri klonlamak için Kendini Korumayı devre dışı bırakmanız gerekir.
- Önceden yüklenmiş Kaspersky Endpoint Security for Windows ve Kaspersky Security Center Network Agent ile Citrix XenDesktop ana görüntüsü için bir şablon makine hazırlarken yapılandırma dosyasına aşağıdaki istisna türlerini ekleyin:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Citrix XenDesktop ile ilgili ayrıntılar için Citrix Destek web sitesini ziyaret edin.
- Bazı durumlarda, çıkarılabilir bir sürücünün güvenli bir şekilde bağlantısını kesme denemesi, bir VMware ESXi hiper yöneticisine dağıtılmış bir sanal makinede başarısız olabilir. Cihazın bağlantısını güvenli bir şekilde kesmeyi bir kez daha deneyin.
- Kaspersky Endpoint Security VMware ESXi hiper yöneticisi ile aşağıdaki sınırlamalarla uyumludur:
  - Kaspersky Endpoint Security, Guest Introspection sürücüleriyle (vnetWFP.sys, vnetFLT.sys ve diğerleri) uyumsuz olabilir. Uyumsuzluğu gidermek için sürücüleri en son sürüme güncelleyin veya sürücüleri kaldırın.
  - Bazı durumlarda, bir sanal makinedeki çıkarılabilir bir diski güvenli bir şekilde kaldırma girişimi başarısız olabilir. Cihazın bağlantısını güvenli bir şekilde kesmeyi bir kez daha deneyin.
- Citrix VDA aracısı bulunan sanal makinelere Kaspersky Endpoint Security'yi yüklemek, uyumluluk hatasıyla sonuçlanabilir. Bunun nedeni, Citrix Provisioning Services ile antivirüs çözümleri arasındaki uyumluluğun sınırlı olmasıdır. Antivirüs çözümlerini Citrix Provisioning Services ile kullanmaya ilişkin en iyi uygulamalar için Citrix destek web sitesine bakın.
- Kaspersky Endpoint Security, sürücü Citrix hipervizörü üzerindeki bir sanal makineye bağlıysa, çıkarılabilir sürücünün taramasını atlar (*Çıkarılabilir Sürücüler Taraması* görevi). Bu tür cihazlarda, işletim sistemi bağlı çıkarılabilir sürücüyü bir ağ sürücüsü olarak algılar. Bu tür durumlarda *Özel Tarama* görevini kullanabilirsiniz. Uygulamanın standart modda ve Light Agent modunda çalışması aynıdır.

- Kaspersky Endpoint Security, Citrix App Layering teknolojisini kullanan bir altyapıdaki sanal makineye yüklenmişse uygulama tarafından virüs bulaşmış olarak algılanan ve *Nesne yeniden başlatıldığında silinecek* durumuna sahip dosyalar, sanal makine yeniden başlatıldığında otomatik olarak silinmez.

  Bu tür dosyaları silmek için User Layer öğesini içeren VHDX dosyasını Citrix App Layering yöneticisinin bilgisayarına bağlamanız ve bağlanan diskte Kötü Amaçlı Yazılım Taraması çalıştırmanız gerekir.

- Kaspersky Endpoint Security yüklü bir sanal makinenin Altın Görüntü anlık görüntüsünü oluşturmadan önce sanal makineyi kapatmanız ve "soğuk" bir anlık görüntü oluşturmanız önerilir. Sanal makine çalışırken ("sıcak") bir anlık görüntü oluşturursanız uygulamanın doğru çalışacağı garanti edilmez.

Kaspersky Security Center ile uyumluluk

- Kaspersky Security Center Web Console sürüm 14.1 ve önceki sürümlerinde, Günlük Denetimi ve Dosya Bütünlük İzleyicisi bileşenlerinin işlevsel alanlarının adları, Yönetim Sunucusu özelliklerinin kullanıcı erişim izinleri ayarları bölümünde doğru şekilde görüntülenmez.

- Uygulama onarıldıktan sonra, bilgisayarın Yönetim Sunucusuna olan bağlantısının koruması devre dışı bırakılır. Uygulamayı onardıktan sonra, *Yönetim Sunucusu bağlantı koruması* görevini tekrar çalıştırın.

- Kaspersky Security Center Yönetim Konsolu'nda, **Kullanıcı veya kullanıcı grubu seçin** penceresi, Kaspersky Security Center kullanıcı listesinden yalnızca ilk 50.000 kullanıcıyı gösterir. Daha fazla bilgi için bkz. Kaspersky Security Center Yardım.

- Kaspersky Security Center Yönetim Konsolu'nda yönetilen cihazları ararken, **Uygulama bileşenleri** sekmesinde aynı uygulama bileşeninin adının birden fazla varyantı aynı anda görüntülenebilir; buna Kaspersky Endpoint Security'nin eski sürümlerine ait adlar da dahildir. Bazı bileşenlerin adları da tekrarlanabilir.

  Parça bazında arama yapmak için, görüntülenen seçeneklerden birini seçmeniz yeterlidir. Cihaz bulma hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun.

- Kaspersky Endpoint Security for Windows web eklentisinin 12.11 veya sonraki bir sürümünün ve Birleşik Koruma ve Yönetim Eklentisi'nin yüklü olduğu Kaspersky Security Center Web Console 15.1 Güncelleme 2'de, ilkenin profil etkinleştirme koşulları çalışmaz. Kaspersky Security Center, profil etkinleştirme koşullarını karşılayan yeni cihazları konsola eklemez.

Lisanslama

- *Verileri almada hata* sistem mesajı görüntülenirse, etkinleştirmeyi gerçekleştirdiğiniz bilgisayarın ağ erişimine sahip olduğunu doğrulayın veya Kaspersky Security Center Etkinleştirme Proxy'si aracılığıyla etkinleştirme ayarlarını yapılandırın.

- Uygulama arabiriminde, lisans sona erme tarihi bilgisayarın yerel saatinde görüntülenir.

- Uygulamanın, sabit olmayan İnternet erişimine sahip bir bilgisayara gömülü anahtar dosyasıyla yüklenmesi, uygulamanın etkinleştirilmediğini veya lisansın bileşen çalışmasına izin vermediğini belirten olayların geçici olarak görüntülenmesine neden olabilir. Bu durum, yükleme işlemi sırasında uygulamanın ilk olarak gömülü deneme lisansını etkinleştirmesinden kaynaklanmaktadır. İnternet erişimi gerektirir.

- Deneme süresi boyunca, stabil olmayan İnternet erişimine sahip bir bilgisayara herhangi bir uygulama yükseltmesinin veya yamanın yüklenmesi, uygulamanın etkinleştirilmediğini belirten olayların geçici olarak görüntülenmesine neden olabilir. Bu durum, güncelleme yükleme işlemi sırasında uygulamanın ilk olarak yerleşik deneme lisansını etkinleştirmesinden kaynaklanmaktadır. İnternet erişimi gerektirir.

- Uygulama kurulumu sırasında deneme lisansı otomatik olarak etkinleştirildiyse ve daha sonra uygulama, lisans bilgileri kaydedilmeden kaldırıldıysa, uygulama yeniden yüklendiğinde deneme lisansıyla otomatik olarak etkinleştirilmeyecektir. Bu durumda uygulamayı elle etkinleştirin.

- Kaspersky Security Center sürüm 11 ve Kaspersky Endpoint Security sürüm 14.2 kullanıyorsanız, bileşen performans raporları düzgün çalışmayabilir. Lisansınızın kapsamında yer almayan Kaspersky Endpoint Security bileşenlerini kurduysanız, Ağ Aracısı bileşen durumu hatalarını Windows Olay Günlüğü'ne gönderebilir. Hataları önlemek için lisansınızın kapsamında olmayan bileşenleri kaldırın.

Posta Tehdidi Koruması

- E-postaları Microsoft Outlook için Posta Tehdidi Koruması uzantısıyla tararken Exchange Server Önbellekli Modu'nu (Use Cached Exchange Mode) kullanmanızı öneririz.

- Kaspersky Endpoint Security, Microsoft Outlook posta istemcisinin 64 bit sürümünü desteklemiyor. Bu, bilgisayarda Microsoft Outlook'un 64 bit sürümü yüklüyse, tarama kapsamına posta dahil edilse bile Kaspersky Endpoint Security'nin Microsoft Outlook dosyalarını (PST ve OST dosyaları) taramayacağı anlamına gelir.

- Kaspersky Endpoint Security, Microsoft Outlook Yeni Posta istemcisini desteklemez.

- Posta Tehdidi Koruması tarafından algılanan tehditlerin temizlenmesini devre dışı bıraktıysanız ve Outlook posta kutunuza virüslü bir e-posta geldiyse Web Tehdidi Koruması, Exchange sunucusuyla MAPI üzerinden iletişimi engelleyebilir. Bunun üzerine Web Tehdidi Koruması bir tehdit algılama olayı oluşturur ve bunu Kaspersky Security Center'a gönderir. Bilgisayar ile Exchange sunucusu arasındaki bağlantıyı yeniden kurmak için virüslü e-postayı Outlook posta kutusundan elle silmeniz gerekir.

  Bilgisayarı yeniden başlatmadan uygulama sürümünü güncellediğinizde Posta Tehdidi Koruması'nın koruma düzeyi geçici olarak (en fazla bir dakika boyunca) düşer. Uygulama güncellenirken Outlook posta kutunuza virüslü bir e-posta gelirse Web Tehdidi Koruması, Exchange sunucusuyla MAPI üzerinden bağlantıyı da engeller. Bağlantıyı yeniden kurmak için virüslü e-postayı Outlook posta kutusundan silin.

Düzeltme Altyapısı

- Uygulama yalnızca NTFS veya FAT32 dosya sistemi olan aygıtlardaki dosyaları geri yükler.

- Uygulama, boyutu 100 MB'a kadar olan dosyaları kurtarır.

- Uygulama yalnızca aşağıdaki uzantıları olan dosyaları geri yükleyebilir: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.

- Ağ sürücülerinde veya yeniden yazılabilir CD'lerde/DVD'lerde yer alan dosyalar geri yüklenemez.

- Encryption File System (EFS) ile şifrelenmiş dosyalar geri yüklenemez. EFS işlemleri hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin.

- Uygulama, işletim sistemi çekirdeği düzeyindeki işlemler tarafından gerçekleştiren dosyalarda yapılan değişiklikleri izlemez.

- Bir ağ paketi kuralı veya uygulama ağı kuralı DNS adlarını belirtiyorsa, Kaspersky Endpoint Security bu kaynakların IP adreslerini belirlemek için DNS sunucusuna istek gönderebilir. Güvenlik Duvarı, ağ etkinliğini izlemek için IP adreslerini kullanır. Bu nedenle uygulama DNS adlarını IP adreslerine çözümler. Kurallarda DNS adlarının yalnızca LAN bilgisayarları veya dahili hizmetler için kullanılması önerilir.

- Tüm IPv6 adreslerine yönelik bir kural belirtmek için ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff adres aralığını ekleyin. Güvenlik Duvarı ::/0 maskesini desteklemez.

- Paketlerin veya bağlantıların yerel adres, fiziksel arabirim ve paket yaşam süresine (TTL) göre filtrelenmesi aşağıdaki durumlarda desteklenir:

  - TCP ve UDP ve paket kuralları için uygulama kurallarında giden paketler veya bağlantılar için yerel adrese göre.

  - Uygulama engelleme kurallarında ve paket kurallarında gelen paketler veya bağlantılar için (UDP hariç) yerel adrese göre.

  - Gelen veya giden paketler için blok paket kurallarında yaşam süresi (TTL) paketine göre.

  - Gelen ve giden paketler veya paket kurallarındaki bağlantılar için ağ arabiriminde göre.

- İzin verilen bir paket kuralı için bir ağ bağdaştırıcısı veya paket yaşam süresi (TTL) yapılandırdıysanız, bu kuralın önceliği bir engelleme uygulama kuralından daha düşüktür. Diğer bir deyişle, bir uygulama için ağ etkinliği engellenmişse (örneğin, uygulama *Yüksek Kısıtlamalı* güvenilirlik grubundaysa), bu ayarlarla bir paket kuralı kullanarak uygulamanın ağ etkinliğine izin veremezsiniz. Diğer tüm durumlar için bir paket kuralının önceliği, bir uygulama ağ kuralından daha yüksektir.

- Güvenlik Duvarı paket kurallarını içe aktarma yapılırken, Kaspersky Endpoint Security kural adlarını değiştirebilir. Uygulama, kuralları aynı genel parametre gruplarıyla belirler: protokol, yön, uzak ve yerel portlar, paket yaşam süresi (TTL). Bu genel parametreler grubu birden çok kural için aynı olduğunda, uygulama bu kurallara aynı adı atar veya bu ada bir parametre etiketi ekler. Böylece Kaspersky Endpoint Security'nin tüm paket kurallarını içe aktarır ancak aynı genel ayarlara sahip kuralların adı değiştirilebilir.

- Bir ağ kuralında uygulama olay raporlamasını etkinleştirdiyseniz, uygulamayı farklı bir güvenilirlik grubuna taşıma sırasında, bu güvenilirlik grubunun kısıtlamaları uygulanmaz. Bu nedenle, uygulama Güvenilir güvenilirlik grubundaysa, ağ kısıtlaması olmayacaktır. Ardından bu uygulama için olay raporlamayı etkinleştirin ve onu *Güvenilmeyen* güvenilirlik grubuna taşıyın. Güvenlik Duvarı bu uygulama için ağ kısıtlamaları uygulamaz. Öncelikle uygulamayı uygun güvenilirlik grubuna taşımanızı ve olay raporlamayı etkinleştirmenizi öneririz. Bu yöntem uygun değilse, uygulama için ağ kuralı ayarlarındaki kısıtlamaları manuel olarak da yapılandırabilirsiniz. Kısıtlamalar sadece başvurunun yerel arabirimi için geçerlidir. Uygulamanın ilke içindeki güvenilirlik grupları arasında taşınması düzgün şekilde çalışır.

- Güvenlik Duvarı ve Yetkisiz Erişim Önleme bileşenlerinin ortak ayarları vardır: uygulama hakları ve korunan kaynaklar. Güvenlik Duvarı için bu ayarları değiştirmeniz halinde, Kaspersky Endpoint Security yeni ayarları Yetkisiz Erişim Önleme bileşenine otomatik olarak uygular. Güvenlik Duvarı ilkesinin genel ayarlarında değişiklik yapılmasına izin verdiğinizi varsayalım (asma kilit açık durumda); bu durumda Yetkisiz Erişim Önleme ayarları da düzenlenebilir olacaktır.

- Kaspersky Endpoint Security 11.6.0 veya önceki sürümlerde bir ağ paketi kuralı tetiklendiğinde, Güvenlik Duvarı raporundaki **Uygulama adı** sütununda her zaman *Kaspersky Endpoint Security* değeri görüntülenir. Ayrıca Güvenlik Duvarı, bağlantıyı tüm uygulamalar için paket düzeyinde engeller. Bu davranış Kaspersky Endpoint Security 11.7.0 ve sonrası için değiştirilmiştir. Güvenlik duvarı raporuna **Kural türü** sütunu eklendi. Bir ağ paketi kuralı tetiklendiğinde, **Uygulama adı** sütunundaki değer boş kalır.

- Güvenlik Duvarı kullanarak tüm ağ etkinliklerini yasakladıysanız, Ağ Tehdidi Koruması bileşeni Port Tarama türünde bir saldırı algılayabilir. Bunun nedeni, uygulamanın ağdaki şüpheli etkinlikleri tespit etmek için Güvenlik Duvarından önce Ağ Tehdidi Korumasını başlatması olabilir.

BadUSB Saldırısı Önleme

- Kaspersky Endpoint Security, bilgisayar kilitlendiğinde USB aygıtı kilidinin zaman aşımını (örneğin geçen ekran kilitleme süresini) sıfırlar. Bu durumda üst üste birkaç kez yanlış bir USB aygıtı yetkilendirme kodu girilir ve uygulama USB aygıtını kilitlenirse, Kaspersky Endpoint Security bilgisayarın kilidi açıldıktan sonra tekrar yetkilendirme denemesi yapmanıza izin verir. Bu durumda, Kaspersky Endpoint Security USB aygıtını BadUSB Saldırısı Önleme bileşeni ayarlarında belirtilen süre boyunca kilitlemez.

- Kaspersky Endpoint Security bilgisayar koruması duraklatıldığında USB aygıtının kilitleme zaman aşımını sıfırlar. Bu durumda üst üste birkaç kez yanlış bir USB aygıtı yetkilendirme kodu girilir ve uygulama USB aygıtını kilitlenirse, Kaspersky Endpoint Security bilgisayar koruması sürdürüldüğünde tekrar yetkilendirme denemesi yapmanıza izin verir. Bu durumda, Kaspersky Endpoint Security USB aygıtını BadUSB Saldırısı Önleme bileşeni ayarlarında belirtilen süre boyunca kilitlemez.

Kaspersky Security Network

- Kaspersky Endpoint Security, sunucunun adresi Latin olmayan harfler (ASCII olmayan semboller) içeriyorsa KSN Proxy'ye bağlanırken (KSN Proxy bağlantı ayarlarında **HTTPS kullan** onay kutusu seçili) HTTPS'yi desteklemez.

- Kaspersky Security Center'da, küresel Kaspersky Security Network'ü kullanmaktan özel Kaspersky Security Network'ü (KPSN) kullanmaya geçerken veya tam tersi, Kaspersky Security Network'e katılma seçeneği belirtilen ürünün ilkesinde devre dışı bırakılır. Ayarları içe aktardıktan sonra, lütfen Kaspersky Security Network Bildirimi metnini dikkatlice okuyun ve KSN'ye katılmak için rızanızı onaylayın. Bildirim metnini uygulama arabiriminde veya ürün ilkesini düzenlerken okuyabilirsiniz.

- Kaspersky Endpoint Security 12.9 for Windows' ile başlayarak, KPSN'den global KSN'ye geçerken Kaspersky Security Network Bildirimini kabul ettiğinizi yeniden onaylamanız gerekir. Bunu yapmak için, ilke özelliklerinde veya uygulama arabiriminde Kaspersky Security Network kullanımını etkinleştirmeniz ve Kaspersky Security Network Bildirimini kabul ettiğinizi onaylamanız gerekir. Global KSN'yi zaten kullandıysanız, önce KSN Kullanımını devre dışı bırakmalı, ardından yeniden etkinleştirmeli ve Kaspersky Security Network Bildirimini kabul ettiğinizi onaylamalısınız. Kaspersky Security Network Bildirimini kabul etmediğiniz takdirde, uygulama Kaspersky Security Network verilerine erişemeyecektir.

- Kaspersky Endpoint Security, tarama amacıyla Kaspersky Security Network'e metin dosyalarını (TXT, CSV, LOG ve makro içermeyen DOCX dosyaları gibi) göndermez. Uygulama, KSN için tehdit oluşturabilecek dosyaları tarama amacıyla gönderir. Bu dosyalar arasında yürütülebilir dosyalar veya yürütülebilir kod içerebilen dosyalar (örneğin DOCX dosyalarındaki makrolar) bulunur. Uygulamanın diğer bileşenleri metin dosyalarını taramaktan sorumludur. Ayrıca, bir metin dosyasının güvenilirliğini dosya bağlam menüsünden manuel olarak da kontrol edebilirsiniz. Bir metin dosyası *Güvenilmez (Kaspersky Security Network)* güvenilirliğine sahipse, uygulama tespit edilen tehditler için tanımlanan eylemi yok sayar.

Uygulama Denetimi

- Uygulama Denetimi kurallarıyla çalışırken, Kaspersky Endpoint Security'nin minimum donanım gereksinimlerini karşılayan ve Microsoft Windows 10 üzerinde çalışan bir bilgisayarda çalıştırılması koşuluyla, farklı kategorilerdeki uygulamalar için toplam 100.000'den fazla dahil etme ve hariç tutma koşulu eklemeniz önerilmez.

- Kaspersky Security Center Web Console'da Uygulama Denetimi kuralları ile çalışırken yalnızca ZIP biçimli arşivler desteklenir. RAR veya 7z gibi diğer biçimlerdeki arşivler desteklenmez. Yönetim Konsolu'nda (MMC) Uygulama Denetimi kuralları ile çalışıyorsanız böyle bir kısıtlama yoktur.

- Kaspersky Security Center Web Konsolu'nda Uygulama Kontrolü kuralları ile çalışırken, yüklenen bir dosyanın desteklenen maksimum boyutu 104 MB'dir. Yönetim Konsolu'nda (MMC) Uygulama Denetimi kuralları ile çalışıyorsanız böyle bir kısıtlama yoktur.

- Microsoft Windows 10'da uygulama reddedilenler listesi modunda çalışırken, engelleme kuralları hatalı şekilde uygulanabilir ve bu da kurallarda belirtilmeyen uygulamaların engellenmesine neden olabilir.

- Kaspersky Endpoint Security'yi yükseltirken *önceden tanımlanmış yeni Uygulama denetimi kuralları* eklediyseniz, bu kuralları uygulamanın önceki sürümlerine uygulayamazsınız.

- İleri web uygulamaları (PWA), Uygulama Denetimi bileşeni tarafından engellendiğinde, appManifest.xml, raporda engellenen uygulama olarak gösterilir.

- Standart Notepad uygulaması Windows 11 için bir Uygulama Denetimi kuralına eklenirken, uygulamanın yolunun belirtilmesi önerilmez. Windows 11 çalıştıran bilgisayarlarda, işletim sistemi `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` klasöründe bulunan Metro Notepad'i kullanır. İşletim sisteminin önceki sürümlerinde, Notepad şu klasörlerde yer alıyordu:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Uygulama Denetimi kuralına Notepad eklenirken, örneğin, çalışan uygulamanın özelliklerinden uygulama adını ve dosya karmasını belirtebilirsiniz.

- KSWS ilkesini KES ilke profiline geçirirken, İlke ve görevler toplu dönüştürme sihirbazı (Taşıma Sihirbazı), kategori adları şu yasak karakterleri içeriyorsa uygulama kategorilerini yeniden adlandırır: `'` `*` `<` `>` `?` `\` `:` `|`. Geçiş Sihirbazı bu karakterleri `_` karakterleriyle değiştirir. Örneğin, `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` uygulama kategorisi `KSWS_Everyone_[C61F-3B7C-4D89-96A1]` olarak yeniden adlandırılır.

Aygıt Denetimi

- Kaspersky Endpoint Security, harici cihaz bağlantı ve bağlantı kesme olaylarını günlüğe kaydedebilir. Windows hizmetleri, aygıtları bağlamak veya bağlantılarını kesmek için sistem kullanıcı hesabını kullanır. Bu, hangi kullanıcının cihazı bağladığını veya bağlantısını kestiğini bilmeyi imkansız hale getirir. Kaspersky Endpoint Security, olayda SYSTEM kullanıcı hesabını belirtir.

- Güvenilir listesine eklenen Yazıcı aygıtlarına erişim, aygıt ve veri yolu engelleme kuralları tarafından engellenir.

- MTP aygıtları için, işletim sisteminin yerleşik Microsoft sürücülerini kullanıyorsanız Okuma, Yazma ve Bağlanma işlemlerinin denetlenmesi desteklenir. Bir kullanıcı, bir aygıtla çalışmak için özel bir sürücü yüklerse (örneğin, iTunes veya Android Hata Ayıklama Köprüsü'nün parçası olarak), Okuma ve Yazma işlemlerinin denetlenmesi çalışmayabilir.

- MTP aygıtlarıyla çalışırken, cihaz yeniden bağlandıktan sonra erişim kuralları değiştirilir.

- Aygıt Denetimi bileşeni, bir aygıtın bağlanması ve bağlantısının kesilmesi, bir aygıttan bir dosyanın okunması, bir aygıta bir dosyanın yazılması ve diğer olaylar gibi izlenen aygıtlarla ilgili olayları kaydeder. Kaspersky Endpoint Security, bağlantı kesme olaylarını yalnızca şu aygıt türleri için kaydeder: Taşınabilir aygıtlar (MTP), Çıkarılabilir sürücüler, Disketler, CD/DVD sürücüleri. Diğer cihaz türleri için uygulama bağlantı kesme olaylarını kaydetmez. Uygulama, tüm aygıt türleri için bir cihazı bilgisayara bağlama işlemini kaydeder.

- Güvenilir listesine model maskesine göre bir cihaz ekliyorsanız ve kimliğe dahil olan ancak model adında bulunmayan karakterleri kullanıyorsanız, bu cihazlar eklenmez. Bir iş istasyonunda, bu cihazlar bir kimlik maskesine göre güvenilenler listesine eklenecektir.

- Uygulama bilgisayar yeniden başlatılmadan yükseltildiğinde, Aygıt Denetimi yeniden bağlanan aygıtlara erişim kuralları uygulamaz. Ancak, cihaz yükseltmeden önce bağlanmışsa, Aygıt Denetimi kuralları doğru şekilde uygular. Uygulamanın yeniden bağlanan cihazlarla düzgün çalışması için bilgisayarı yeniden başlatın.

- Kaspersky Endpoint Security sürüm 12.0 yüklü bilgisayarlarda, bilgisayara Kaspersky Endpoint Security sürüm 12.1 ilkesi uygulanmışsa **Ağ yazıcıları** aygıt türü için yazıcı erişimine **İzin ver ve günlüğe kaydetme** modu **Bağlantı veriyoluna bağlıdır** adlandırılır. Bu modlarda uygulama aynı eylemleri gerçekleştirir. Kaspersky Endpoint Security sürüm 12.1'de, ağ yazıcıları için erişim modu doğru şekilde **İzin ver ve günlüğe kaydetme** olarak adlandırılmıştır.

- Kaspersky Endpoint Security for Windows 12.0 ile başlayarak, uygulama yazıcılar için yazdırma kurallarının yapılandırılmasına izin verir (yazdırma kontrolü). Yazdırma denetimli uygulamayı yükledikten veya uygulamayı yazdırma denetimli bir sürüme yükselttikten sonra bilgisayarı yeniden başlatmanız gerekir. Bilgisayar yeniden başlatılana kadar Kaspersky Endpoint Security yazdırma kurallarını uygulamaz ve yalnızca yazıcılara erişimi denetleyebilir. Bilgisayarın yeniden başlatılması kuruluşunuzdaki iş akışlarını olumsuz etkiliyorsa, yalnızca spoolsv hizmetini (Yazdırma Biriktiricisi) yeniden başlatabilirsiniz. Arm tabanlı bilgisayarlarda yazdırma denetimi desteklenmemektedir.

- Kaspersky Endpoint Security for Windows sürüm 12.0'dan itibaren uygulama tarafından WPA3 protokolü, **Wi-Fi** tipi cihazlar için desteklenmektedir. Bir bilgisayara Kaspersky Endpoint Security sürüm 12.2 ilkesi uygulanırsa, Kaspersky Endpoint Security sürüm 11.11.0 ve önceki sürümlere sahip bilgisayarlarda WPA2 protokolü seçilir; 12.0 ila 12.1 sürümleri için WPA2/WPA3 seçilir; 12.2 ve sonraki sürümler için WPA3 seçilir.

- Apple cihazları, taşınabilir aygıtlar (MTP) ve iTunes aygıtları olarak sınıflandırılır. İşletim sistemi Apple aygıtının bağlantısını yanlış tanımlayabilir ve Apple aygıtını taşınabilir bir aygıt (MTP) olarak belirleyemez. Bu nedenle Apple aygıtı dosya yöneticisinde kullanılamaz, ancak iTunes uygulamasında erişilebilir olacaktır. Sonuç olarak Kaspersky Endpoint Security, Apple aygıtına erişimi yalnızca iTunes uygulamasında denetler. Apple aygıtınıza taşınabilir aygıt (MTP) olarak erişmek için Aygıt Yöneticisine gitmeniz ve Apple Mobil Aygıt USB Sürücüsünü USB Denetleyicileri listesinden kaldırmanız gerekir. Bilgisayar yeniden başlatıldıktan sonra, işletim sistemi Apple aygıtını taşınabilir aygıt (MTP) ve iTunes aygıtı olarak tanımlayacaktır. Kaspersky Endpoint Security, hem iTunes uygulamasında hem de dosya yöneticisinde aygıta erişimi kontrol edecektir.

- Kaspersky Endpoint Security 12.3 for Windows'ta, **Bluetooth** cihaz türü için erişim ayarları farklıdır. Uygulamanın önceki sürümünde **Bağlantı veriyoluna bağlıdır** değerini belirttiyseniz, uygulamayı 12.3 sürümüne yükselttikten sonra yapılandırılan değer **İzin ver ve günlüğe kaydetme** olarak değişir. Bu, cihazın davranışını değiştirmez.

- Aygıt Denetimi, Bluetooth cihazlarını yalnızca Microsoft Windows Bluetooth yığını aracılığıyla destekler. Aygıt Denetimi üçüncü taraf Bluetooth yığınlarıyla yanlış çalışabilir.

- Bluetooth cihazı Cihaz Sınıfını (COD) gizler veya taklit ederse, Aygıt Denetimi yanlış çalışabilir.

- Belirli Realtek Bluetooth dongle sürücülerine sahip Windows 7 veya Windows 8 bilgisayarlarda, Bluetooth cihazlarının yalnızca giriş cihazları (HID sınıfı) olarak bağlanmasına izin vermek mümkün olmayabilir. Yani, uygulama ayarlarında Bluetooth cihazlarına erişimi yasaklar ve giriş cihazlarını istisnalara eklerseniz, Aygıt Denetimi bunun yerine tüm Bluetooth cihazlarına erişimi engelleyebilir.

İnternet Denetimi

- OGV ve WEBM formatları desteklenmemektedir.
- RTMP protokolü desteklenmemektedir.
- İnternet Denetimi yalnızca WSL1'i destekler. Uygulama WSL2 trafiğini kontrol etmez.

Uyarlamalı Anomali Denetimi

- Etkinliğe göre otomatik olarak istisnaların oluşturulması önerilir. Elle bir dışlama eklerken, hedef nesneyi belirtirken yolun başlangıcına `*` karakterini ekleyin.
- Örneklemde adı 260 karakterden uzun tek bir olay bile varsa **Tetiklenen Uyarlamalı Anomali Denetimi kuralları raporu** oluşturulamaz.
- Bir nesnenin veya işlemin özelliklerinin değeri 256 karakterden fazla ise (örneğin hedef nesneye yol) Uyarlamalı Anomali Denetimi Kural Tetikleme havuzundan istisnalar eklemesi desteklenmez. İlke ayarlarından bir istisnayı manuel olarak ekleyebilirsiniz. Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor bölümüne de bir istisna ekleyebilirsiniz.
- Kaspersky Security Center 15.1, belirli bir kural için **Uyarlamalı Anomali Denetimi kuralları durum raporu** hakkında ayrıntılı rapor oluşturamıyor.
- Uyarlamalı Anomali Denetimi kuralları yalnızca web eklentisinin kurulum diliyle eşleşen dilde kullanılabilir. Arayüz dilini değiştirirseniz Web Konsolu boş bir kural listesi görüntüler. Kurallara erişmek için arayüz dilini yeniden web eklentisinin kurulum diline değiştirin.

Sürücü Şifreleme (FDE)

- Kaspersky Disk Encryption, ARM tabanlı bilgisayarlarda desteklenmemektedir.
- BitLocker Drive Encryption, Windows Home işletim sistemini çalıştıran bilgisayarlarda desteklenmemektedir.
- BitLocker Sürücü Şifrelemesi kullanılırken kullanıcı, Windows API'sini kullanarak kimlik doğrulama parolasını manuel olarak değiştirebilir. Bu gibi durumlarda BitLocker, Kaspersky Endpoint Security ilkesinde belirlenen parola gereksinimlerini yok sayar. Başka bir deyişle, kullanıcı istediği herhangi bir parolayı ayarlayabilir.
- Uygulamayı yükledikten sonra, sabit sürücü şifrelemesinin düzgün çalışması için işletim sistemini yeniden başlatmanız gerekir.
- Kimlik Doğrulama Aracısı hiyeroglifleri veya `|` ve `\` özel karakterleri desteklemiyor.
- Şifreleme sonrasında optimum bilgisayar performansı için işlemcinin AES-NI komut kümesini (Intel Advanced Encryption Standard New Instructions) desteklemesi gerekir. İşlemci AES-NI desteği sunmuyorsa bilgisayar performansı düşebilir.
- Uygulama bu tür aygıtlara erişim izni vermeden önce şifrelenmiş aygıtlara erişmeye çalışan işlemler olduğunda, uygulama bu tür işlemlerin sonlandırılması gerektiğini belirten bir uyarı gösterir. İşlemler sonlandırılamazsa, şifrelenmiş aygıtları yeniden bağlayın.
- Sabit sürücülerin benzersiz kimlikleri, aygıt şifreleme istatistiklerinde ters formatta görüntülenir.
- Aygıtların şifrelenirken biçimlendirilmesi önerilmez.
- Birden çok çıkarılabilir sürücü aynı anda bir bilgisayara bağlandığında, şifreleme ilkesi yalnızca bir çıkarılabilir sürücüye uygulanabilir. Çıkarılabilir aygıtlar yeniden bağlandığında, şifreleme ilkesi doğru şekilde uygulanır.

- Büyük ölçüde parçalanmış bir sabit sürücüde şifreleme başlatılamayabilir. Sabit sürücüyü birleştirme.

- Sabit sürücüler şifrelendiğinde, şifreleme görevinin başladığı andan Microsoft Windows 7/8/8.1/10 çalıştıran bir bilgisayarın ilk kez yeniden başlatılmasına kadar ve sabit sürücü şifrelemesinin yüklenmesinin ardından Microsoft Windows 8/8.1/10 işletim sisteminin ilk yeniden başlatılmasına kadar hazırda bekletme engellenir. Sabit sürücülerin şifresi çözüldüğünde, önyükleme sürücüsünün şifresinin tamamen çözüldüğü andan işletim sisteminin ilk yeniden başlatılmasına kadar hazırda bekletme engellenir. Microsoft Windows 8/8.1/10'da Hızlı Başlangıç seçeneği etkinleştirildiğinde, hazırda bekletme modunun engellenmesi, işletim sistemini kapatmanızı önler.

- Windows 7 bilgisayarlar, disk BitLocker teknolojisi ile şifrelendiğinde kurtarma sırasında parolanın değiştirilmesine izin vermez. Kurtarma anahtarı girildikten ve işletim sistemi yüklendikten sonra, Kaspersky Endpoint Security kullanıcıdan parolayı veya PIN kodunu değiştirmesini istemez. Bu nedenle, yeni bir parola veya PIN kodu belirlemek mümkün değildir. Bu sorun, işletim sisteminden kaynaklanmaktadır. Devam etmek için sabit sürücüyü yeniden şifrelemeniz gerekir.

- Ek sağlayıcılar etkinken xbootmgr.exe aracının kullanılması önerilmez. Örneğin, Dağıtıcı, Ağ veya Sürücüler.

- Kaspersky Endpoint Security for Windows yüklü bir bilgisayarda şifrelenmiş çıkarılabilir bir sürücünün biçimlendirilmesi desteklenmez.

- FAT32 dosya sistemiyle şifrelenmiş çıkarılabilir bir sürücünün biçimlendirilmesi desteklenmez (sürücü şifrelenmiş olarak görüntülenir). Bir sürücüyü biçimlendirmek için sürücüyü NTFS dosya sistemine yeniden biçimlendirin.

- Şifrelenmiş bir bilgisayarda birden çok indirme aracısı bir arada bulunamaz.

- Önyüklenebilir bir GPT diskinin görüntüsünü şifrelenmemiş bir durumda geri yükleme girişimi, işletim sistemini çalışmaz hale getirebilir. Bunu önlemek için aşağıdaki önerileri uygulayın:

  - Görüntüyü yedekten geri yüklemeden önce diskin şifresini tamamen çözün.

  - Görüntüyü oluştururken sektör sektör kopyalamayı kullanın.

  - Görüntüyü geri yüklemeden önce şifrelenmiş diskin ilk sektörlerindeki verileri silin ve diski yeniden başlatın.

- Aşağıdaki koşulların tümü aynı anda karşılandığında, daha önce farklı bir bilgisayarda şifrelenmiş çıkarılabilir bir sürücüye erişmek imkansızdır:

  - Kaspersky Security Center sunucusuna bağlantı yok.

  - Kullanıcı, yeni bir belirteç veya parola ile yetkilendirme yapmaya çalışıyor.

  Benzer bir durum meydana gelirse bilgisayarı yeniden başlatın. Bilgisayar yeniden başlatıldıktan sonra şifrelenmiş çıkarılabilir sürücüye erişim verilecektir.

- USB aygıtlarının Kimlik Doğrulama Aracısı tarafından keşfedilmesi, BIOS ayarlarında USB için xHCI modu etkinleştirildiğinde desteklenmeyebilir.

- En sık kullanılan verileri önbelleğe almak için kullanılan bir aygıtın SSD bölümü için Kaspersky Disk Şifreleme (FDE), SSHD aygıtları için desteklenmez.

- UEFI modunda çalışan 32 bit Microsoft Windows 8/8.1/10 işletim sistemlerinde sabit sürücülerin şifrelenmesi desteklenmez.

- Şifresi çözülmüş bir sabit sürücüyü yeniden şifrelemeden önce bilgisayarı yeniden başlatın.

- Sabit sürücü şifrelemesi, Kaspersky Anti-Virus for UEFI ile uyumlu değildir. Kaspersky Anti-Virus for UEFI kurulu olan bilgisayarlarda sabit sürücü şifrelemesinin kullanılması önerilmez.

- Microsoft hesaplarına dayalı Kimlik Doğrulama Aracısı hesaplarının oluşturulması aşağıdaki sınırlamalarla desteklenir:

  - Çoklu Oturum Açma teknolojisi desteklenmez.

  - Son N gün içinde sistemde oturum açan kullanıcılar için hesap oluşturma seçeneği seçilirse, Kimlik Doğrulama Aracısı hesaplarının otomatik olarak oluşturulması desteklenmez.

- Bir Kimlik Doğrulama Aracısı hesabının adı `<domain>/<Windows account name>` biçimine sahipse, bilgisayar adını değiştirdikten sonra, bu bilgisayarın yerel kullanıcıları için oluşturulan hesapların adlarını da değiştirmeniz gerekir. Örneğin, `Ivanov` bilgisayarında `Ivanov` yerel kullanıcısı var olduğunu ve kullanıcı için `Ivanov/Ivanov` adıyla bir Kimlik Doğrulama Aracısı hesabı oluşturulduğunu hayal edin. Bilgisayar adı `Ivanov`, `Ivanov-PC` ile değiştirilmişse, Kimlik Doğrulama Aracısı hesabının adını `Ivanov` kullanıcısı için `Ivanov/Ivanov`'dan `Ivanov-PC/Ivanov`'a değiştirmeniz gerekir. Doğrulama Aracısı'nın hesap yönetim görevini kullanarak hesap adını değiştirebilirsiniz. Hesabın adı değiştirilmeden önce, eski ad (örneğin `Ivanov/Ivanov`) kullanılarak önyükleme ortamında kimlik doğrulama mümkündür.

- Bir kullanıcının Kaspersky Disk Encryption teknolojisi kullanılarak şifrelenmiş bir bilgisayara yalnızca bir belirteç kullanarak erişmesine izin verilirse ve bu kullanıcının erişim kurtarma prosedürünü tamamlaması gerekiyorsa, bu kullanıcıya şifrelenmiş bilgisayara erişim geri yüklendikten sonra bu bilgisayara parola tabanlı erişim verildiğinden emin olun. Erişimi geri yüklerken kullanıcının belirlediği parola kaydedilmeyebilir. Bu durumda, kullanıcının, bilgisayarın bir sonraki yeniden başlatılışında şifrelenmiş bilgisayara erişimi geri yükleme prosedürünü yeniden tamamlaması gerekecektir.

- FDE Kurtarma Aracı kullanılarak bir sabit sürücünün şifresini çözerken, kaynak aygıttaki verilerin şifresi çözülen verilerle üzerine yazılması durumunda şifre çözme işlemi bir hatayla sona erebilir. Sabit sürücüdeki verilerin bir kısmı şifrelenmiş kalacaktır. FDE Kurtarma Aracını kullanırken, şifresi çözülmüş verileri cihaz şifre çözme ayarlarında bir dosyaya kaydetme seçeneğinin seçilmesi önerilir.

- Kimlik Doğrulama Aracısı parolası değiştirilmişse, *Parolanız başarıyla değiştirildi. Tamam'a tıklayın* metnini içeren bir mesaj görüntülenir ve kullanıcı bilgisayarı yeniden başlatırsa, yeni parola kaydedilmez. Eski parola, önyükleme ortamında sonraki kimlik doğrulama için kullanılmalıdır.

- Disk şifreleme, Intel Rapid Start teknolojisiyle uyumlu değildir.

- Disk şifreleme, ExpressCache teknolojisiyle uyumlu değildir.

- Bazı durumlarda, FDE Kurtarma Aracı kullanılarak şifrelenmiş bir sürücünün şifresini çözmeye çalışırken, araç "İstek-Yanıt" prosedürü tamamlandıktan sonra cihaz durumunu hatalı bir şekilde "şifrelenmemiş" olarak algılar. Aracın günlüğünde, cihazın şifresinin başarıyla çözüldüğünü belirten bir olay görüntülenir. Bu durumda, cihazın şifresini çözmek için veri kurtarma prosedürünü yeniden başlatmanız gerekir.

- Kaspersky Endpoint Security for Windows eklentisi Web Console'da güncellendikten sonra, istemci bilgisayar özellikleri Web Console hizmeti yeniden başlatılıncaya kadar BitLocker kurtarma anahtarını göstermez.

- Tam disk şifreleme desteğinin diğer sınırlamalarını ve kısıtlamalarla sabit sürücü şifrelemesinin desteklendiği cihazların bir listesini görmek için lütfen Teknik Destek Bilgi Tabanına bakın.

Dosya Düzeyinde Şifreleme (FLE)

- Arm tabanlı bilgisayarlarda dosya şifreleme özelliği desteklenmemektedir.

- Microsoft Windows yerleşik işletim sistemlerinde dosya ve klasör şifreleme özelliği desteklenmemektedir.

- Uygulamayı yükledikten sonra, dosya ve klasör şifrelemenin düzgün çalışması için işletim sistemini yeniden başlatmanız gerekir.

- Uygulama yalnızca NTFS ve FAT32 dosya sistemlerine sahip cihazlarda dosya şifrelemeyi destekler. Şifrelenmiş bir dosya desteklenmeyen bir dosya sistemine (örneğin exFAT) sahip bir aygıta aktarılırsa, bu aygıttaki dosya şifrelenmez ve değiştirilmesi mümkün olur.

- Şifrelenmiş bir dosya, kullanılabilir şifreleme işlevi olan bir bilgisayarda depolanırsa ve dosyaya şifrelemenin olmadığı bir bilgisayardan erişirseniz, bu dosyaya doğrudan erişim sağlanacaktır. Kullanılabilir şifreleme işlevi olan bir bilgisayardaki bir ağ klasöründe depolanan şifrelenmiş bir dosya, şifreleme işlevi olmayan bir bilgisayara şifresi çözülmüş biçimde kopyalanır.

- Dosyaları Kaspersky Endpoint Security for Windows ile şifrelemeden önce Encrypting File System ile şifrelenmiş dosyaların şifresini çözmeniz önerilir.

- Bir dosya şifrelendikten sonra boyutu 4 KB artar.

- Bir dosya şifrelendikten sonra, dosya özelliklerinde *Arşiv* özniteliği ayarlanır.

- Şifresi çözülen dosya, örneğin çıkarılabilir medyaya kopyalanırken dosya şifreli kalabilir. Bu durum, dosya yöneticisi (örneğin explorer.exe) şifrelenmiş dosyaya erişim sağlamaya çalıştığında, dosyanın karmasını işlemin özel bir listesine kaydetmesi nedeniyle meydana gelebilir. Dosyanın şifresini çözdükten sonra, dosya yöneticisi dosyaya erişmeye çalıştığında, işlem listede dosyanın karmasını arar. Karma bulunursa Kaspersky Endpoint Security dosyayı şifreli olarak bırakır. Bunu önlemek için işlem listesini temizlemeniz gerekir. İşletim sistemi, işlem listesini doldukça otomatik olarak temizler. Listeyi manuel olarak da temizleyebilirsiniz. Bunu yapmak için bilgisayarı yeniden başlatabilir, dosyaya erişim sağlamak için kullandığınız işlemi yeniden başlatabilir (örneğin, explorer.exe) veya şifrelenmiş dosyaya erişim için kullanmadığınız farklı bir dosya yöneticisi kullanabilirsiniz.

- Şifrelenmiş bir arşivden paketi açılmış bir dosya, bilgisayarınızda zaten var olan bir dosya ile aynı ada sahipse, şifrelenmiş bir arşivden çıkarılmış olan yeni dosya, bu dosyanın üzerine yazılacaktır. Kullanıcıya üzerine yazma işlemi hakkında bilgi verilmez.

- Şifrelenmiş bir arşivi açmadan önce, paketten çıkarılmış dosyaları yerleştirmek için yeterli boş disk alanınız olduğundan emin olun. Yeterli disk alanınız yoksa, arşiv açma işlemi tamamlanabilir ancak dosyalar bozulabilir. Bu durumda, Kaspersky Endpoint Security'nin herhangi bir hata mesajı göstermemesi mümkündür.

- Taşınabilir Dosya Yöneticisi arabirimi, çalışması sırasında ortaya çıkan hatalarla ilgili mesajları görüntülemez.

- Kaspersky Endpoint Security for Windows, Dosya Düzeyinde Şifreleme bileşeninin yüklü olduğu bir bilgisayarda Taşınabilir Dosya Yöneticisini başlatmaz.

- Aşağıdaki şartlar aynı anda sağlandığında, bir çıkarılabilir sürücüye erişmek için Taşınabilir Dosya Yöneticisi'ni kullanamazsınız:

  - Kaspersky Security Center'a bağlantı yok;

  - Kaspersky Endpoint Security for Windows bilgisayarda yüklü olduğunda;

  - Bilgisayarda veri şifreleme (FDE veya FLE) gerçekleştirilmemiş.

  Taşınabilir Dosya Yöneticisi parolasını bilseniz bile erişim mümkün olmaz.

- Dosya şifreleme kullanıldığında, uygulama Sylpheed posta istemcisiyle uyumlu değildir.

- Kaspersky Endpoint Security for Windows bazı uygulamalarda, şifrelenmiş dosyalara erişim kısıtlaması kurallarını desteklemez. Bunun nedeni, bazı dosya işlemlerinin üçüncü taraf bir uygulama tarafından gerçekleştirilmesidir. Örneğin, dosya kopyalama, uygulamanın kendisi tarafından değil, dosya yöneticisi tarafından gerçekleştirilir. Bu şekilde, Outlook posta istemcisinin şifrelenmiş dosyalara erişimi reddedilirse, Kaspersky Endpoint Security, kullanıcı dosyaları pano aracılığıyla veya sürükle ve bırak işlevini kullanarak e-posta mesajına kopyaladıysa posta istemcisinin şifrelenmiş dosyaya erişmesine izin verir. Kopyalama işlemi, şifrelenmiş dosyalara erişim kısıtlama kurallarının belirtilmediği, yani erişime izin verilen bir dosya yöneticisi tarafından gerçekleştirilir.

- Çıkarılabilir sürücüler taşınabilir mod desteğiyle şifrelendiğinde, parola yaşı kontrolü devre dışı bırakılamaz.

- Sayfa dosyası ayarlarının değiştirilmesi desteklenmez. İşletim sistemi, belirtilen parametre değerleri yerine varsayılan değerleri kullanır.

- Şifrelenmiş çıkarılabilir sürücülerle çalışırken güvenli kaldırma kullanın. Çıkarılabilir sürücü güvenli bir şekilde çıkarılmazsa veri bütünlüğünü garanti edemeyiz.

- Dosyalar şifrelendikten sonra, şifrelenmemiş orijinalleri güvenli bir şekilde silinir.

- Client-Side Caching (CSC) kullanılarak çevrimdışı dosyaların senkronizasyonu desteklenmez. Çevrimdışı dosyaların şifrelenmesi veya sunucular için SMB üzerinden Branch Caching teknolojisi de desteklenmez. Grup ilkesi düzeyinde paylaşılan kaynakların çevrimdışı yönetiminin yasaklanması önerilir. Çevrimdışı modda olan dosyalar düzenlenebilir. Senkronizasyondan sonra, çevrimdışı bir dosyada yapılan değişiklikler kaybolabilir.

- Sistem sabit sürücüsünün kök dizininde şifrelenmiş bir arşiv oluşturulmasını desteklenmez.

- Ağ üzerinden şifrelenmiş dosyalara erişirken sorunlarla karşılaşabilirsiniz. Dosyaları farklı bir kaynağa taşımanız veya dosya sunucusu olarak kullanılan bilgisayarın aynı Kaspersky Security Center Yönetim Sunucusu tarafından yönetildiğinden emin olmanız önerilir.

- Klavye düzeninin değiştirilmesi, şifrelenmiş, kendi kendine açılan bir arşivin parola giriş penceresinin takılmasına neden olabilir. Bu sorunu çözmek için parola giriş penceresini kapatın, işletim sisteminizdeki klavye düzenine geçin ve şifrelenmiş arşivin parolasını yeniden girin.

- Dosya şifreleme, bir diskte birden çok bölüm bulunan sistemlerde kullanıldığında, pagefile.sys dosyasının boyutunu otomatik olarak belirleyen seçeneği kullanmanız önerilir. Bilgisayar yeniden başlatıldıktan sonra pagefile.sys dosyası disk bölümleri arasında taşınabilir.

- *Belgelerim* klasöründeki dosyalar dahil olmak üzere dosya şifreleme kurallarını uyguladıktan sonra, şifreleme uygulanan kullanıcıların şifrelenmiş dosyalara başarıyla erişebildiğinden emin olun. Bunu yapmak için, Kaspersky Security Center bağlantısı mevcut olduğunda her bir kullanıcının sistemde oturum açmasını sağlayın. Bir kullanıcı, Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara erişmeye çalışırsa, sistem kilitlenebilir.

- Sistem dosyaları bir şekilde dosya düzeyinde şifreleme kapsamına dahil edilirse, bu dosyaları şifrelerken ortaya çıkan hatalarla ilgili olaylar raporlarda görünebilir. Bu olaylarda belirtilen dosyalar aslında şifrelenmez.

- Pico işlemleri desteklenmez.

- Büyük/küçük harfe duyarlı yollar desteklenmez. Şifreleme kuralları veya şifre çözme kuralları uygulandığında, ürün olaylarındaki yollar küçük harfle görüntülenir.

- Başlangıçta sistem tarafından kullanılan dosyaların şifrelenmesi önerilmez. Bu dosyalar şifrelenmişse, Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara erişme girişimi, sistemin takılmasına veya şifrelenmemiş dosyalara erişim isteklerine neden olabilir.

- Kullanıcılar, dosyadan belleğe eşleme yöntemini (WordPad veya FAR gibi) ve büyük dosyalarla çalışmak için tasarlanmış uygulamaları (Notepad ++ gibi) kullanan uygulamalar aracılığıyla FLE kuralları altında ağ üzerinden bir dosyayla birlikte çalışırsa, dosya şifrelenmemiş biçimde, bulunduğu bilgisayardan ona erişme yeteneği olmadan süresiz olarak engellenebilir.

- Kaspersky Endpoint Security, OneDrive bulut depolama alanında veya adları OneDrive olan diğer klasörlerde bulunan dosyaları şifrelemez. Kaspersky Endpoint Security, şifrelenmiş dosyalar şifre çözme kuralına eklenmemişse, bu dosyaların OneDrive klasörlerine eklenmesini de engeller.

- Dosya düzeyinde şifreleme bileşeni yüklendiğinde, kullanıcıların ve grupların yönetimi WSL (Windows Subsystem for Linux) modunda çalışmaz.

- Dosya düzeyinde şifreleme bileşeni yüklendiğinde, dosyaları yeniden adlandırmak ve silmek için POSIX (Portable Operating System Interface) desteklenmez.

- Veri kaybına neden olabileceğinden, geçici dosyaları şifrelemeniz önerilmez. Örneğin, Microsoft Word, bir belgeyi işlerken geçici dosyalar oluşturur. Geçici dosyalar şifrelenmiş ancak orijinal dosya şifrelenmemişse, kullanıcı belgeyi kaydetmeye çalıştığında *Erişim Reddedildi* hatası alabilir. Microsoft Word dosyayı ayrıca kaydedebilir, ancak bir dahaki sefere belgeyi açmak mümkün olmayacaktır, yani veriler kaybolacaktır. Veri kaybını önlemek için, geçici dosyalar klasörünü şifreleme kurallarının dışında tutmanız gerekir.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- *Dosyayı karantinaya taşı* görevinin bir sonucu olarak karantinaya alınan bir nesneyi tarayamazsınız.

- 4 MB üzeri bir Alternate Data Stream (ADS) karantinaya almak mümkün değildir. Kaspersky Endpoint Security bu büyüklükteki ADS'leri kullanıcıya bildirim yapmadan atlar.

- Kaspersky Endpoint Security, görev özelliklerindeki klasör yolu bir sürücü harfi ile başlıyorsa ağ sürücülerinde *IOC Taraması* görevlerini desteklemez. Kaspersky Endpoint Security ağ sürücülerindeki *IOC Taraması* görevleri için sadece UNC yolu biçimini destekler. Örneğin, `\\server\shared_folder`.

- EmailItem terimlerini kullanan *IOC Taraması* görevinin düzgün çalışması için, Kaspersky Endpoint Security web eklentisinin en son sürüme güncellenmesi gerekir.

- Arm tabanlı bilgisayarlarda, *IOC Taraması* yalnızca aşağıdaki posta istemcilerinden gelen e-posta dosyalarını destekler: Outlook 2016 ile Outlook 2021, 2024 ve 365'in 32 bit ve 64 bit sürümleri (Arm64 için).

- Yapılandırma dosyasında Kaspersky Sandbox ile entegrasyon ayarı etkinleştirildiğinde, bir uygulama yapılandırma dosyasının içe aktarılması hata ile sonuçlanır. Uygulama ayarlarını dışa aktarmadan önce Kaspersky Sandbox'ı devre dışı bırakın. Ardından dışa aktarma/içe aktarma prosedürünü gerçekleştirin. Yapılandırma dosyasını içe aktardıktan sonra Kaspersky Sandbox'ı etkinleştirin.

- KLP dosyasından ilke içe aktarılırken, Kaspersky Detection and Response Expert Sözleşmesi'nin hüküm ve koşullarının kabul edilmesini belirleyen parametre değeri uygulanmaz. Sonuç olarak, ilke içe aktarıldıktan sonra Kaspersky Endpoint Security, EDR Agent işlevlerini gerçekleştirmez. EDR Agent'ın çalışması için ilkeyi açın, herhangi bir parametreyi değiştirin ve ilke ayarlarını kaydedin.

- *IOC Taraması* görevi çalıştırılırken bir güvenlik ihlali göstergesi algılandığında, uygulama sadece FileItem terimi için bir dosyayı karantinaya alır. Bir dosyanın başka terimler için karantinaya alınması desteklenmez.

- Uyarı ayrıntılarını yönetmek için Kaspersky Endpoint Security for Windows web eklentisi 11.7.0 veya üzeri gereklidir. Endpoint Detection and Response çözümleri (EDR Optimum ve EDR Expert) ile çalışılırken uyarı ayrıntıları gereklidir. Algılama, sadece Kaspersky Security Center Web Console ve Kaspersky Security Center Cloud Console'da mevcuttur.

- [KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi yapılandırması, bir Kaspersky Endpoint Agent uygulama kaldırma hatası ile sonuçlanabilir. Uygulama kaldırma hatası, Kaspersky Endpoint Agent'ın en son sürümü yüklendiğinde düzelir. Kaspersky Endpoint Agent'ı kaldırmak için bilgisayarı yeniden başlatın ve bir uygulama kaldırma görevi oluşturun.

- [KES+KEA+yerleşik aracı] yapılandırması desteklenmez. Bu tür bir yapılandırma, uygulamalarla kuruluşunuzda dağıtılan Detection and Response çözümü arasındaki etkileşimi bozar. Ayrıca, Kaspersky Endpoint Agent ve yerleşik aracının aynı bilgisayarda kullanılması telemetrinin tekrarlanmasına ve bilgisayar ile ağ üzerindeki yükün artmasına neden olabilir. [KES + yerleşik aracı] yapılandırmasına geçtikten sonra Kaspersky Endpoint Agent'ın bilgisayardan kaldırıldığından emin olun. Geçişten sonra Kaspersky Endpoint Agent çalışmaya devam ederse uygulamayı manuel olarak kaldırın (örneğin, *Uygulamayı uzaktan kaldır* görevini kullanarak).

  Yükleyici, Kaspersky Endpoint Agent'ı Kaspersky Endpoint Security ve yerleşik aracının yüklü olduğu bir bilgisayara dağıtmanıza olanak tanır. Kaspersky Endpoint Agent ve yerleşik aracı, *Uygulama bileşenlerini değiştirme* görevinin bir sonucu olarak tek bir bilgisayara da yüklenebilir. Davranış, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent sürümlerine bağlıdır.

- Uygulama, uyarı ayrıntıları oluştururken, değiştirilen dosyaların karmaları da dahil olmak üzere tespit edilen tehdit hakkında bilgi sağlar. Kaspersky Endpoint Security, uyarı ayrıntılarını oluştururken dosyanın karmasını hesaplar. Dosya değiştirme olayı oluşturulduğunda dosyanın orijinal karmasının, uyarı ayrıntıları oluşturulduğunda hesaplanan karma ile aynı olmayabileceğini göz önünde bulundurun.

- Yerleşik aracı EDR (KATA), bilgisayar yeniden başlatıldıktan sonra, izolasyon süresi dolmuş olsa bile bilgisayarın ağ izolasyonunu devam ettirir. Tekrarlanan bilgisayar izolasyonunu önlemek için Kaspersky Anti Targeted Attack Platform konsolunda ağ izolasyonunu kapatmanız gerekir.

- Ağ izolasyonu bittikten sonra uygulamayı yükseltmenizi öneririz. Kaspersky Endpoint Security yükseltildikten sonra Ağ izolasyonu durdurulabilir.

- EDR (KATA), EDR Optimum ve EDR Expert için yerleşik aracılar birbirleriyle uyumlu değildir. Bu nedenle, Kaspersky Endpoint Security'yi farklı EDR işlevleriyle etkinleştirdiyseniz EDR yerleşik aracısının bağımsız bir Kaspersky Endpoint Detection and Response eklenti lisansıyla etkinleştirilmesi atlanabilir. Örneğin, Kaspersky Endpoint Security'yi [KES+EDR Optimum] lisansı ile etkinleştirdiyseniz EDR (KATA) yerleşik aracısının tek başına bir lisansla etkinleştirilmesi atlanır.

- Kaspersky Endpoint Security sürüm 12.1'de, yerleşik EDR (KATA) aracısı *NTFS meta dosyalarını al* görevi için şu meta dosyalarını desteklemez: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Bu meta dosyalar için destek Kaspersky Endpoint Security sürüm 12.2'ye eklenmiştir.

- Kaspersky Endpoint Agent'tan Kaspersky Anti Targeted Attack Platform (EDR) çözümü için Kaspersky Endpoint Security'ye geçiş yaparken, bilgisayarı Central Node sunucularına bağlana sırasında hatalarla karşılaşabilirsiniz. Bunun nedeni, Web Console geçiş sihirbazının şu ilke ayarlarını atlaması ve bunları geçirmemesidir:

  - Ayarların değiştirilmesi yasağı **Bağlantı ayarları** ("kilit").

    Varsayılan olarak ayarlar değiştirilebilir ("kilit" açıktır). Bu nedenle ayarlar bilgisayarda uygulanmaz. Ayarların değiştirilmesi yasaklanmalı ve "kilit" kapatılmalıdır.

  - Kripto konteyneri.

    Central Node sunucularına bağlanmak için iki yönlü kimlik doğrulama kullanıyorsanız, kripto konteynerini yeniden eklemeniz gerekir. Geçiş sihirbazı sunucunun TLS sertifikasının geçişini doğru şekilde gerçekleştirir.

  Yönetim Konsolu (MMC) içeriğinde bulunan İlke ve Görev Geçiş Sihirbazı, Kaspersky Anti Targeted Attack Platform (EDR) çözümü için tüm ayarların geçişini gerçekleştirir.

- Uygulama, Kaspersky Managed Detection and Response çözümünü desteklemek için Endpoint Detection and Response Agent modunda yüklendiğinde uygulama Kaspersky Security Center ile hiçbir bağlantısı olmadan etkinleştirme durumu hatalı görüntüleniyor. BLOB dosyası indirildikten sonra, Windows görev çubuğu bildirim alanında yanlış bir durum görüntüleniyor: *Uygulama etkinleştirilmemiş*. Ancak, uygulama arabirimi etkinleştirme durumunu doğru şekilde görüntülüyor. Uygulamanın düzgün çalışması için bilgisayarı yeniden başlatın.

- Kaspersky Endpoint Security, EDR (KATA) bileşenini veya Endpoint Sensor (desteklenmiyor) kullanarak Kaspersky Anti Targeted Attack Platform çözümü ile entegrasyona izin verir. Kaspersky Anti Targeted Attack Platform ile etkileşim kurmak için bileşenlerden yalnızca birini kullanabileceğinizi unutmayın. Bileşenin durumunu görüntülemek için Yönetim Konsolu'nda (MMC) bilgisayar özelliklerini açın, **Uygulamalar** bölümünde Kaspersky Endpoint Security for Windows'un özelliklerini açın ve **Bileşenler** bölümüne gidin. Kaspersky Anti Targeted Attack Platform ile etkileşim için bileşen durumunun görüntülenmesinde aşağıdaki özel hususlar geçerlidir:

  - Yönetim eklentisi 12.0 ve önceki sürümler için uygulama **Endpoint Sensor** için güncel durumu görüntüler. Kaspersky Endpoint Security 12.0 ve önceki sürümlerde EDR (KATA) bileşeni yoktur. EDR (KATA) bileşeni 12.1 sürümünde tanıtılmıştır.

  - Yönetim eklentisi 12.1 ve sonraki sürümler için uygulama, **Endpoint Detection and Response (KATA)** genel durumunu görüntüler; bu, Endpoint Sensor durumu veya EDR (KATA) bileşen durumu anlamına gelebilir. Bu, kullanıcının bilgisayarında yüklü olan uygulamanın sürümüne ve Kaspersky Anti Targeted Attack Platform ile etkileşim kurmak için kullanabileceğiniz kullanılabilir bileşenlere bağlıdır.

- Kaspersky Endpoint Security sürüm 12.6 ve üzeri sürümlerden başlayarak, Kaspersky Security Center Web Console sürüm 14.2 ve daha alt sürümler bilgisayar özelliklerinde **Endpoint Detection and Response (KATA)** bileşeninin adını doğru şekilde görüntülemez. Uygulama, **Endpoint Detection and Response (KATA)** bileşeni yerine **Endpoint Detection and Response Expert (KATA EDR)** bileşeninin adını görüntüler. Bileşenlerin listesini görüntülemek için Web Console'da bilgisayar özelliklerini açın, **Uygulamalar** bölümünde Kaspersky Endpoint Security for Windows'un özelliklerini açın ve **Bileşenler** bölümüne gidin. Kaspersky Security Center Web Console sürüm 15.1 ve üzeri sürümlerden itibaren, uygulama bileşen adını doğru şekilde görüntüler.

- Kaspersky Endpoint Detection and Response yönetim eklentisi, Web Console sürüm 14.0–14.2'de yüklü olan sürüm 15.3'e güncellenirken uyarı ayrıntıları yanlış görüntüleniyor. Uyarı ayrıntılarının düzgün çalışması için Kaspersky Security Center Yönetim Sunucusunu yeniden başlatın.

- Kaspersky Endpoint Detection and Response yönetim eklentisi sürüm 15.4 ve sonrası, Kaspersky Security Center sürüm 14.0'ı desteklemez. Yönetim eklentisini güncelledikten sonra uyarı ayrıntıları yanlış görüntüleniyor.

- Kaspersky Extended Detection and Response (XDR) sürüm 1.4 sınıfı çözümler, Kaspersky Endpoint Security for Windows web eklentisi sürüm 12.12 veya üstünü desteklemez. Mevcut web eklentisi sürümünü bırakabilir ya da XDR çözümünü 2.0 veya sonraki bir sürüme güncelleyebilirsiniz.

- Kaspersky Endpoint Security, Arm mimarisine yönelik nesneleri Kaspersky Sandbox'a göndermez.

- Kaspersky Endpoint Security, toplamda en fazla 10.000 adet EDR Expert (on-premises) dahil etme ve hariç tutma olay filtreleme kuralını destekler.

- Depolanan filtreleme kuralları için desteklenen sınır aşılırsa, EDR Expert (on-premises) olay filtreleme kuralları ilkeden Kaspersky Endpoint Security sürüm 14.0 veya daha eski bir sürümünü çalıştıran yönetilen cihazlara iletilmeyecektir. Uygulama buna ilişkin bir uyarı gösterecektir.

- Kaspersky Endpoint Security for Windows 12.11–14.1 sürümleri, aşağıdaki EDR Expert (on-premises) telemetri olaylarını desteklemez:

  - LDAP Attribute Change

  - GPO Change

- SCCM Local Config Mismatch
- SCCM Config Change
- SCCM Deployment Task
- Smb Connection Open

Kaspersky Endpoint Security, 14.2 sürümünden itibaren LDAP Attribute Change hariç tüm bu EDR Expert (on-premises) telemetri olaylarını destekler.

Diğer sınırlamalar

- Windows işletim sistemleri, sürüm 11 24H2'den başlayarak UDP Receive Segment Coalescing Offload (URO) teknolojisini desteklemektedir. Bilgisayarda uyumlu bir ağ kartı ve sürücüleri yüklüyse teknoloji varsayılan olarak etkindir. Bir kullanıcının bilgisayarında URO'nun devre dışı bırakılması uygulamanın performansını önemli ölçüde düşürebilir.
- Kaspersky Endpoint Security, WSL alt sistemini (Windows Subsystem for Linux) kısıtlamalarla destekler:
  - WSL 1. Uygulama, ağ trafiğini izler ve HTTP / HTTPS üzerinden tehditleri algılar. Kaspersky Endpoint Security'nin güvenli HTTPS bağlantılarını taramak için kendi sertifikasını kullanması nedeniyle, bazı üçüncü taraf uygulamaların çalışması kesintiye uğrayabilir.
  - WSL 2. Uygulama WSL 2'yi desteklememektedir.
- 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. Antivirüs veritabanlarını güncelledikten veya uygulama modülü güncellemelerini uyguladıktan sonra uygulamayı işlevsel duruma geri getirmeye çalışır.
- Güvenilir listesine eklenen web adresleri yanlış işlenebilir.
- Kaspersky Security Center konsolunda, **Gelişmiş** → **Veri havuzları** → **Etkin tehditler** klasöründen bir dosyayı diske kaydedemezsiniz. Dosyayı kaydetmek için virüslü dosyayı dezenfekte etmeniz gerekir. Temizleme sırasında, uygulama dosyanın bir kopyasını Backup klasörüne kaydeder. Şimdi dosyayı **Gelişmiş** → **Veri havuzları** → **Yedekle** klasöründen diske kaydedebilirsiniz.
- Yönetim Sunucusuna veri aktarımı ayarlarının kalıtımı (**Genel Ayarlar** → **Raporlar ve Depolama Alanı** → **Yönetim Sunucusu'na veri aktarımı**) diğer ayarların kalıtımından farklıdır. İlkede veri aktarım ayarlarının değiştirilmesine izin verdiyseniz ("kilit" açık), bu ayarlar daha önce tanımlanmamışsa konsoldaki yerel bilgisayar özelliklerinde varsayılan değerlere sıfırlanacaktır. Bu ayarlar daha önce tanımlanmışsa, değerleri geri yüklenir. Bir ilke silinirken, ayarlar aynı şekilde devralınır. Bu durumlarda, yerel bilgisayar özelliklerindeki diğer ayarlar ilkeden devralınır.
- Kaspersky Endpoint Security, RFC 2616, RFC 7540, RFC 7541, RFC 7301 standartlarıyla uyumlu HTTP trafiğini izler. Kaspersky Endpoint Security tarafından, HTTP trafiğinde başka bir veri alışverişi biçimi tespit edilmesi durumunda, uygulama internetten zararlı dosyaların indirilmesini önlemek için bu bağlantıyı engeller.
- Kaspersky Endpoint Security, QUIC iletişim kuralı üzerinden iletişimi engeller. Tarayıcılar, tarayıcıda QUIC desteğinin etkinleştirilmiş olup olmadığından bağımsız olarak standart taşıma iletişim kuralını (TLS veya SSL) kullanır.

- Üçüncü taraf yazılımlar Libcurl kütüphanesi ile çalıştığında TLS bağlantı hataları oluşabilir. Bu, Kaspersky Endpoint Security'nin şifrelenmiş bağlantıları taramak için kullandığı Kaspersky sertifikasıyla ilgili olabilir. Çalışmaya devam etmek için, üçüncü taraf yazılımlar için sertifika doğrulamayı devre dışı bırakabilir (önerilmez) veya cURL sertifika deposuna bir Kaspersky sertifika gövdesi ekleyebilirsiniz. Ayrıntılı bilgi için Kaspersky Bilgi Bankası'na bakın.

- Kaspersky Endpoint Security for Windows ilk kez başlatıldığında, dijital olarak imzalanmış bir uygulama geçici olarak yanlış gruba yerleştirilebilir. Dijital olarak imzalanan uygulama daha sonra doğru gruba yerleştirilecektir.

- Üçüncü taraf yazılım tarafından engellenen zararlı bir nesnenin yeniden taranması sırasında, tehdit yeniden algılandığında kullanıcı bilgilendirilmez. Tehdit yeniden algılama olayı, uygulama raporunda ve Kaspersky Security Center raporunda görüntülenir.

- Kaspersky Security Center cihaz şifreleme raporu, sunucu platformlarında veya Aygıt Denetimi bileşeninin yüklü olmadığı iş istasyonlarında, Microsoft BitLocker kullanılarak şifrelenen cihazlar hakkında bilgi içermeyecektir.

- Kaspersky Security Center Web Console'da tüm rapor girişlerini görüntülemek mümkün değildir. Web Console'da, sadece raporlarda görüntülenen girişlerin sayısını değiştirebilirsiniz. Kaspersky Security Center Web Console varsayılan olarak 1000 rapor girişi görüntüler. Yönetim Konsolu (MMC) için tüm rapor girişlerinin görüntülenmesini etkinleştirebilirsiniz.

- Kaspersky Security Center Console'da, 1000 rapor girişinden fazlasını görüntülemek üzere ayar yapmak mümkün değildir. 1000'den daha yüksek bir değer ayarlamanız durumunda, Kaspersky Security Center Console sadece 1000 rapor girişi görüntüleyecektir.

- Bir ilke hiyerarşisi kullanılırken, bir alt ilkedeki Çıkarılabilir Sürücülerin Şifrelenmesi bölümünün ayarlarına, üst ilke bu ayarların değiştirilmesini yasaklaması durumunda düzenleme için erişilebilir.

- Paylaşılan klasörlerin dış şifrelemeye karşı korunması için istisnaların düzgün çalışmasını sağlamak için işletim sistemi ayarlarında Denetim Oturumu Açma özelliğini etkinleştirmelisiniz.

- Paylaşılan klasör koruması etkinleştirilirse, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Windows başlatılmadan önce başlatılan her uzaktan erişim oturumu için paylaşılan klasörleri şifreleme girişimlerini izler, uzaktan erişim oturumunun başlatıldığı bilgisayarın olup olmadığı da dahil hariç tutmalara eklendi. Kaspersky Endpoint Security for Windows'un, istisnalara eklenen ve Kaspersky Endpoint Security for Windows başlatılmadan önce başlatılan bir bilgisayardan başlatılan uzaktan erişim oturumları için paylaşılan klasörleri şifreleme girişimlerini izlemesini istemiyorsanız, sonlandırın ve yeniden uzaktan erişim oturumunu kurun veya Kaspersky Endpoint Security for Windows yazılımının kurulu olduğu bilgisayarı yeniden başlatın.

- Güncelleme görevi belirli bir kullanıcı hesabının izinleriyle çalıştırılırsa, yetki gerektiren bir kaynaktan güncelleme yapılırken ürün yamaları indirilmeyecektir.

- Uygulama, yetersiz sistem performansı nedeniyle başlatılamayabilir. Bu sorunu çözmek için Ready Boot seçeneğini kullanın veya hizmetleri başlatmak için işletim sistemi zaman aşımını artırın.

- Uygulama Windows'ta Safe Mode ile çalışamaz.

- Uygulamayı yükledikten sonra ilk yeniden başlatmaya kadar Ses Denetiminin çalışacağını garanti edemeyiz.

- Yönetim Konsolu'nda (MMC), uygulama izinleri yapılandırma penceresindeki Yetkisiz Erişim Önleme ayarlarında **Kaldır** düğmesi kullanılamaz. Bir uygulamayı, uygulamanın içerik menüsü aracılığıyla bir güvenilirlik grubundan kaldırabilirsiniz.

- Uygulamanın yerel arabiriminde, Yetkisiz Erişim Önleme ayarlarında, bilgisayarın bir ilke tarafından yönetilip yönetilmediğini görüntülemek için uygulama izinleri ve korunan kaynaklar görüntülenmez. Kaydırma, arama, filtreleme ve diğer pencere kontrolleri kullanılamaz. Kaspersky Security Center Console'daki ilke özelliklerinden uygulama izinlerini görüntüleyebilirsiniz.

- Döndürülmüş iz dosyaları etkinleştirildiğinde, AMSI bileşeni ve Outlook eklentisi için hiçbir iz oluşturulmaz.
- Windows Server 2008'de performans izleri manuel olarak toplanamaz.
- "Yeniden Başlatma" izleme türü için performans izleri desteklenmez.
- Pico işlemleri için döküm günlüğü desteklenmez.
- **Sistem hizmetlerinin harici yönetimini devre dışı bırak** seçeneğinin kapatılması, `AMPPL=1` parametresiyle yüklenen uygulamanın hizmetini durdurmanıza izin vermez (varsayılan olarak, parametre değeri Windows 10RS2 işletim sisteminden başlayarak `1` olarak ayarlanmıştır. sistem sürümü). `1` değerli `AMPPL` parametresi, ürün hizmeti için Koruma Süreçleri teknolojisinin kullanılmasını sağlar.
- Bir klasörü için özel bir tarama çalıştırmak için, özel taramayı başlatan kullanıcının bu klasörün özniteliklerini okuma izinlerine sahip olması gerekir. Aksi takdirde, özel klasör taraması imkansız olacak ve bir hata ortaya çıkacaktır.
- Bir ilkede tanımlanan bir tarama kuralı sonunda `\` karakteri olmayan bir yol içerdiğinde, örneğin `C:\folder1\folder2`, tarama `C:\folder1\` yolu için çalıştırılacaktır.
- Yazılım kısıtlama ilkeleri kullanıyorsanız (Software Restriction Policies, SRP), bilgisayar yüklemede başarısız olabilir (siyah ekran). Arızaları önlemek için SRP özelliklerinde uygulama kitaplıklarının kullanımına izin vermeniz gerekir. SRP özelliklerinde,khkum.dll dosyası için **Kısıtlanmamış** güvenlik düzeyi kuralını ekleyin (**Yeni Karma Kuralı** menü öğesi). Dosya `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\` klasöründe bulunur. Bu yöntemi seçtiyseniz, Kaspersky Endpoint Security için *Güncelleme* görevi ayarlarında **Uygulama modüllerinin güncellemelerini indir** onay kutusunun işaretini kaldırmanız gerekir. SRP hakkında ayrıntılar için Microsoft belgelerine bakın.

  Ayrıca SRP'yi devre dışı bırakabilir ve uygulama kullanımını kontrol etmek için Kaspersky Endpoint Security'nin Uygulama Denetimi bileşenini kullanabilirsiniz.
- Bilgisayar, DriverLoadPolicy parametresi 8 olarak ayarlanmış Windows Grup İlkesi Nesnesi (Group Policy Object, GPO) altındaki bir etki alanına aitse (Good only), Kaspersky Endpoint Security yüklü bilgisayarın yeniden başlatılması BSOD'ye neden olur. Bir hatayı önlemek için, Grup İlkesindeki Early Launch Antimalware (ELAM) parametresi 1 (Good and unknown) olarak ayarlanmalıdır. ELAM ayarları ilkede şunun altında bulunur: **Bilgisayar Yapılandırması → Yönetim Şablonları → Sistem → Erken Başlatma Kötü Amaçlı Yazılımdan Koruma**.
- Rest API aracılığıyla Outlook eklenti ayarlarının yönetimi desteklenmez.
- Belirli bir kullanıcı için görev çalıştırma ayarları, bir yapılandırma dosyası aracılığıyla cihazlar arasında aktarılamaz. Ayarlar bir yapılandırma dosyasından uygulandıktan sonra, kullanıcı adını ve parolayı elle belirtin.
- Bir güncelleme yükledikten sonra, bütünlük denetimi görevi, güncellemeyi uygulamak için sistem yeniden başlatılıncaya kadar çalışmaz.
- Döndürülmüş izleme düzeyi, uzaktan tanılama yardımcı programı aracılığıyla değiştirildiğinde, Kaspersky Endpoint Security for Windows, izleme düzeyi için hatalı şekilde boş bir değer görüntüler. Ancak, izleme dosyaları doğru izleme düzeyine göre yazılır. Döndürülen izleme düzeyi uygulamanın yerel arabirimi aracılığıyla değiştirildiğinde, izleme düzeyi doğru şekilde değiştirilir, ancak uzaktan tanılama yardımcı programı, yardımcı program tarafından en son tanımlanan izleme düzeyini hatalı şekilde görüntüler. Bu, yöneticinin geçerli izleme düzeyi hakkında güncel bilgilere sahip olmamasına neden olabilir ve bir kullanıcı uygulamanın yerel arabiriminde izleme düzeyini manuel olarak değiştirirse, ilgili bilgiler izlerde bulunmayabilir.
- Yerel arabirimde, Parola koruması ayarları yönetici hesabının adının değiştirilmesine izin vermez (varsayılan olarak KLAdmin). Yönetici hesabının adını değiştirmek için Parola korumasını devre dışı bırakmanız, ardından Parola korumasını etkinleştirmeniz ve yönetici hesabı için yeni bir ad belirlemeniz gerekir.

- Kaspersky Endpoint Security uygulaması, bir Windows Server 2019 sunucusuna yüklendiğinde Docker ile uyumlu değildir. Docker kapsayıcılarını Kaspersky Endpoint Security içeren bir bilgisayara dağıtmak çökmeye (BSOD) neden olur.

- Kaspersky Endpoint Security, SQL Server DBMS'nin bir sunucusuna kurulursa uygulama, istekleri sunucunun örneğine gönderir. Bu, SQL Server Agent'ın işlerini taramak ve kötü amaçlı işlerin çalışmasını önlemek için gereklidir. Kaspersky Endpoint Security, işleri taramak için SQL Server kullanıcı hesabını kullanır. Uygulama, sistem belleğini tararken ve anti-virüs veritabanlarını güncelledikten sonra sunucuya istek gönderir.

- Kaspersky Endpoint Security ve Secret Net Studio yazılımının uyumluluğu sınırlıdır:

  - Kaspersky Endpoint Security uygulaması, Secret Net Studio yazılımının Antivirüs bileşeniyle uyumlu değildir.

    Uygulama, Secret Net Studio'nun Antivirüs bileşeniyle birlikte dağıtıldığı bir bilgisayara yüklenemez. Birlikte çalışabilirliği mümkün kılmak için Antivirüs bileşenini Secret Net Studio'dan kaldırmalısınız.

  - Kaspersky Endpoint Security uygulaması, Secret Net Studio yazılımının Disk koruma ve veri şifreleme bileşeniyle uyumlu değildir.

    Uygulama, Secret Net Studio'nun Disk koruma ve veri şifreleme bileşeniyle birlikte dağıtıldığı bir bilgisayara yüklenemez. Birlikte çalışabilirliği mümkün kılmak için Disk koruma ve veri şifreleme bileşenini Secret Net Studio'dan kaldırmalısınız.

  - Secret Net Studio, Kaspersky Endpoint Security'nin Dosya Düzeyinde Şifreleme (FLE) bileşeniyle uyumlu değildir.

    Kaspersky Endpoint Security'yi Dosya Düzeyinde Şifreleme (FLE) bileşeniyle birlikte yüklediğinizde, Secret Net Studio çalışırken hatalar verebilir. Birlikte çalışabilirliği sağlamak için Dosya Düzeyinde Şifreleme (FLE) bileşenini Kaspersky Endpoint Security'den kaldırmanız gerekir.

- Sistem Bütünlüğü İzleme kurallarını içe aktarırken, uygulama kuralın kimliğini ve adını kontrol eder. Kural kimlikleri aynıysa Kaspersky Endpoint Security mevcut kuralları yeni kuralla değiştirir. Kuralları dışa aktarırken, uygulama otomatik olarak kimlikler atar. Örneğin, dışa aktarılan kural XML dosyalarını manuel olarak düzenlediyseniz, aynı kimliklere sahip kurallar mevcut olabilir. Kural kimlikleri benzersiz ancak kural adları aynıysa Kaspersky Endpoint Security, kuralın adına `(1)` ve benzerlerini ekler.

- Kaspersky Endpoint Security for Windows sürüm 12.11'den itibaren, Web Console'da alt grupta açık olan üst ilkenin ayarlarını görüntülemek mümkün değildir. Web Console ayrıca bir uyarı görüntüler: *Bu ilke devralınmıştır. İlke ayarlarını yalnızca oluşturulduğu yönetim grubunda düzenleyebilirsiniz.*

- Yönetim Konsolu'nda (MMC) 256 karakterden uzun açılır bildirimler görüntülenmez.

- İlkedeki ve kurulum paketindeki bileşen adları farklı olabilir. Örneğin, Endpoint Detection and Response Expert (on-premises) uygulamasının adı Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) veya Kaspersky Anti Targeted Attack Platform Integration olarak belirlenebilir. Bileşen adları, uygulamanın sürümüne göre de farklılık gösterebilir.

Sözlük

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.

Antivirüs veritabanları

Antivirüs veritabanlarının yayınlandığı tarih itibarıyla Kaspersky tarafından bilinen bilgisayar güvenliği tehditleri hakkında bilgiler içeren veritabanları. Antivirüs veritabanı imzaları, taranan nesnelerdeki kötü amaçlı kodların algılanmasına yardımcı olur. Antivirüs 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, kullanıcı adı, parola ve bağlantı noktasının İnternet kaynağı adresinin metin gösteriminin dışında tutulması; ayrıca, İnternet kaynağı adresinin büyük harflerden küçük harflere değiştirilmesi).

Koruma bileşenlerinin çalışmasıyla ilgili olarak, İnternet kaynağı adreslerinin normalleştirilmesinin amacı, fiziksel olarak eşdeğerken 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.

Cloud Discovery

Cloud Discovery, bulut hizmetlerine kullanıcı erişimini yönetir. Bulut hizmetleri arasında örneğin Microsoft Teams, Salesforce ve Microsoft Office 365 yer alır. Bulut hizmetleri kategoriler halinde gruplandırılmıştır, örneğin *Dosya paylaşımı*, *Mesajlaşma Uygulamaları*, *E-posta*.

E-dolandırıcılık web adreslerinin veritabanı

Kaspersky uzmanlarının kimlik avı ile ilgili olduğunu tespit ettiği web adreslerinin bir listesi. Veritabanı düzenli olarak güncellenir ve Kaspersky uygulama dağıtım kitinin bir parçasıdır.

Entegrasyon Sunucusu

Kaspersky Endpoint Security for Virtualization Light Agent bileşeni. Kaspersky Endpoint Security bileşenleri ile sanal altyapı arasında etkileşim kurar.

Etkin anahtar

Uygulama tarafından kullanılmakta olan bir anahtar.

Görev

Kaspersky uygulaması tarafından görev olarak gerçekleştirilen işlevler, örneğin: Gerçek Zamanlı Dosya Koruma, Tam Aygıt Tarama, Veritabanı Güncellemesi.

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.

IOC

Güvenlik İhlali Göstergesi. Kötü amaçlı bir nesne veya etkinlik hakkında bir dizi veri.

IOC dosyası

Uygulamanın bir algılamayı saymak için eşleştirmeye çalıştığı bir dizi güvenlik ihlali göstergesi (IOC) içeren bir dosya. Tarama sonucunda nesne için birden fazla IOC dosyasıyla tam eşleşme bulunursa, algılama olasılığı daha yüksek olabilir.

Kerberos kimlik doğrulaması

Güvenilir olmayan ağlar üzerinden iletişim kurmaya izin veren, aralarında bir bağlantı kurmadan önce istemci ve sunucu tarafından karşılıklı kimlik doğrulama mekanizması. Bu mekanizma, kullanıcının güvenilir bir kimlik doğrulama merkezinden aldığı bir bilete dayanır.

Kimlik Doğrulama Aracısı

Şifrelenen sabit sürücülere erişim sağlamak ve önyüklenebilir sabit sürücü şifrelendikten sonra işletim sistemini yüklemek için kimlik doğrulama işlemini tamamlamanızı sağlayan arabirimdir.

Koruma kapsamı

Çalışıyorken Temel Tehdit Koruması tarafından sürekli olarak taranan nesneler. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir.

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent bileşeni. Korunması gereken her sanal makineye yüklenir.

Lisans Sertifikası

Kaspersky'nin anahtar dosyası veya etkinleştirme kodu ile birlikte kullanıcıya aktardığı bir belge. Kullanıcıya verilen lisans hakkında bilgi içerir.

Maske

Joker karakterler kullanarak bir dosya adının ve uzantısının temsilidir.

Dosya maskeleri, joker karakterler de dahil olmak üzere dosya adlarında izin verilen tüm karakterleri içerebilir:

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.

- İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir. ** maskesi sadece tarama istisnaları oluştururken kullanılabilir.

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını 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.

OpenIOC

XML tabanlı ve 500'den fazla farklı Güvenlik İhlali Göstergesini içeren Açık Güvenlik İhlali Göstergeleri (IOC) açıklamaları standardı.

Sertifika veren

Sertifikayı düzenleyen sertifikalandırma merkezi.

SVM

Güvenli sanal makine - tarama sunucusu hizmetinin (Protection Server, Kaspersky Endpoint Security for Virtualization Light Agent'ın bir bileşeni) yüklü olduğu özel bir sanal makine.

Tarama kapsamı

Bir tarama görevi yürütülürken Kaspersky Endpoint Security tarafından taranan nesneler.

Taşınabilir Dosya Yöneticisi

Bu, bilgisayarda şifreleme işlevi bulunmadığında çıkarılabilir sürücülerde 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.

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 kodların izinsiz giriş riski vardır.

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.

Yanlış alarm

Kaspersky uygulaması bir dosyanın imzası bir virüsünkine benzediği için virüslü olmayan bir dosyayı virüslü olarak rapor ettiğinde yanlış alarm oluşur.

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.

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.

Ekler

Bu bölümde, belgenin gövdesini destekleyen bilgiler yer alır.

Ek 1. Uygulama Ayarları

Kaspersky Endpoint Security'yi yapılandırmak için bir ilke, görevler veya uygulama arabirimini kullanabilirsiniz. Uygulama bileşenleri hakkında ayrıntılı bilgi ilgili bölümlerde verilmiştir.

Dosya Tehdidi Koruması

Dosya Tehdidi Koruması bileşeni, bir bilgisayar dosya sistemine bulaşmasını önlemenizi sağlar. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni bilgisayarın RAM'inde kalıcı olarak bulunur ve açılan, kaydedilen veya çalıştırılan tüm dosyaları gerçek zamanlı olarak tarar. Bu bileşen, bağlı sürücüler de dahil olmak üzere tüm bilgisayar sürücülerindeki dosyaları tarar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Bileşen, kullanıcı veya uygulama tarafından erişilen dosyaları tarar. Zararlı bir nesnenint epsit edilmesi durumunda Kaspersky Endpoint Security dosyanın çalışmasını engeller. Uygulama bundan sonra zararlı dosyayı Dosya Tehdidi Koruması bileşeninin ayarlarına göre temizler veya siler.

OneDrive bulut depolama alanında bulunan bir dosyaya erişmeye çalışırken, Kaspersky Endpoint Security dosya içeriğini indirir ve tarar.

Dosya Tehdidi Koruması bileşeni ayarları

Parametre	Açıklama
Güvenlik düzeyi *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Dosya Tehdidi Koruması için Kaspersky Endpoint Security, farklı ayar grupları uygulayabilir. Uygulamada saklanan bu ayar kümelerine *güvenlik seviyeleri* denir: • **Yüksek**. Bu dosya güvenlik düzeyi seçildiğinde Dosya Tehdidi Koruması bileşeni açılan, kaydedilen ve başlatılan tüm dosyaların en sıkı denetimini gerçekleştirir. Dosya Tehdidi Koruması bileşeni, bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde bulunan tüm dosya türlerini tarar. Ayrıca arşivleri, kurulum paketlerini ve gömülü OLE nesnelerini de tarar. • **Önerilen**. Kaspersky Lab uzmanları bu dosya güvenlik düzeyini önerir. Dosya Tehdidi Koruması bileşeni, bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde bulunan yalnızca belirtilen dosya biçimlerini ve gömülü OLE nesnelerini tarar. Dosya Tehdidi Koruması bileşeni, arşivleri veya kurulum paketlerini taramaz. • **Düşük**. Bu dosya güvenliği düzeyi ayarları maksimum tarama hızı sağlar. Dosya Tehdidi Koruması bileşeni bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde yalnızca belirtilen uzantılara sahip dosya türlerini tarar. Dosya Tehdidi Koruması bileşeni birleşik dosyaları taramaz.
Dosya türleri *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	**Tüm dosyalar**. Bu ayar etkinleştirilirse Kaspersky Endpoint Security, tüm dosyaları istisnasız (tüm formatları ve uzantıları) olarak kontrol eder. **Biçime göre taranan dosyalar**. Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Bir dosyada kötü amaçlı kod taraması yapmadan önce dosyanın iç başlığı, dosyanın biçimini (örneğin, .txt, .doc veya .exe) belirlemek için analiz edilir. Tarama ayrıca belirli dosya uzantılarına sahip dosyaları arar. **Uzantıya göre taranan dosyalar** Bu ayar etkinleştirildiğinde, uygulama sadece virüs bulaşabilecek dosyaları tarar. Dosya biçimi daha sonra dosyanın uzantısına göre belirlenir.
Tarama kapsamı	Dosya Tehdidi Koruması bileşeni tarafından taranan nesneleri içerir. Bir tarama nesnesi, bir sabit sürücü, çıkarılabilir sürücü, ağ sürücüsü, klasör, dosya veya bir maske ile tanımlanmış birden fazla dosya olabilir. Varsayılan olarak Dosya Tehdidi Koruması bileşeni, herhangi bir sabit sürücüde, çıkarılabilir sürücülerde veya ağ sürücülerinde başlatılan dosyaları tarar. Bu nesneler için koruma kapsamı değiştirilemez ya da silinemez. Yalnızca bir nesneyi (çıkarılabilir sürücüler gibi) taramaların dışında bırakabilirsiniz.

Parametre	Açıklama
Makine öğrenimi ve imza analizi *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Makine öğrenimi ve imza analizi yöntemi, bilinen tehditlerin açıklamalarını ve etkisiz duruma getirme yollarını içeren Kaspersky Endpoint Security veritabanlarını kullanır. Bu yöntemi kullanan koruma kabul edilebilir en düşük güvenlik düzeyini sağlar. Kaspersky uzmanları makine öğreniminin ve imza analizinin her zaman etkin olmasını önerir.
Sezgisel analiz *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	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. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
Tehdit algılandığında yapılacak eylem	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama dosyayı siler. **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse, uygulama algılanan virüslü dosyayı otomatik olarak temizlemeye çalışır. Temizleme başarısız olursa, uygulama bu dosyayı engeller. **Engelle**. Bu seçenek seçildiğinde, uygulama virüs bulaşmış dosyayı temizlemeye veya silmeye çalışmadan otomatik olarak engeller. Uygulama, virüslü bir dosyayı temizlemeye veya silmeye başlamadan önce, dosyayı geri yüklemeniz gerekip gerekmediğini veya ileride temizlenebileceğini düşünerek dosyanın bir yedekleme kopyasını oluşturur.
Sadece yeni ve değiştirilmiş dosyaları tara	Yalnızca yeni dosyaları ve en son tarandıklarından beri değiştirilmiş dosyaları tarar. Bu yardım, bir taramanın süresini kısaltır. Bu mod hem basit hem bileşik dosyalara uygulanır.
Arşivleri tara	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Dağıtım paketlerini tara	Üçüncü taraf uygulamaların dağıtım paketlerinin taranması.
Microsoft Office biçimlerindeki dosyaları tara	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.
E-posta biçimindeki dosyaları tara	E-posta biçimindeki dosyaları tarar. Uygulama MSG ve EML dosyalarını tarar. E-posta biçimindeki dosyalar da OLE nesnelerini ve MHT dosyalarını içerir. Kaspersky Endpoint Security, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük e-posta biçimlerindeki dosyaları tarar.
Büyük bileşik dosya paketlerini açma	Bu onay kutusu işaretlendiğinde, uygulama boyutları belirtilen değeri aşan birleşik dosyaları taramaz. Bu onay kutusu işaretlenmediğinde, uygulama her boyuttaki birleşik dosyaları tarar. Uygulama, onay kutusunun seçili olup olmadığından bağımsız olarak arşivlerden çıkarılan büyük dosyaları tarar.

Parametre	Açıklama
Bileşik dosyaları arka planda çıkart	Onay kutusu işaretlenirse, uygulama bu dosyalar taranmadan önce belirtilen değerden daha büyük bileşik dosyalara erişim sağlar. Bu durumda, Kaspersky Endpoint Security arka planda bileşik dosyaları açar ve tarar. Uygulama sadece bu dosyaları paketinden çıkardıktan ve taradıktan sonra bu değerden küçük bileşik dosyalara erişim sağlar. Onay kutusu işaretlenmediğinde, uygulama bileşik dosyalara yalnızca herhangi bir boyuttaki dosyaları açıp taradıktan sonra erişim sağlar.
Tarama modu *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Kaspersky Endpoint Security, kullanıcı, işletim sistemi veya kullanıcı hesabı altında çalışan bir uygulama tarafından erişilen dosyaları tarar. **Akıllı mod**. Bu modda, Dosya Tehdidi Koruması bir nesneyi o nesnede yapılan eylemlerin çözümlemesine dayalı olarak tarar. Örneğin, bir Microsoft Office belgesi ile çalışırken Kaspersky Endpoint Security dosyayı ilk açıldığında ve son kapandığında tarar. Dosyanın üzerine yazan ara işlemler taranmasına neden olmaz. **Erişim ve değiştirme durumunda** Bu modda, Dosya Tehdidi Koruması nesneleri açma veya değişiklik yapma girişimi olduğunda tarar. **Erişim durumunda**. Bu modda, Dosya Tehdidi Koruması nesneleri yalnızca onları açma girişimi olduğunda tarar. **Yürütme durumunda**. Bu modda Dosya Tehdidi Koruması nesneleri yalnızca onları çalıştırma girişimi olduğunda tarar.
iSwift teknolojisini kullan *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.
iChecker teknolojisini kullan *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Bu teknoloji belli dosyaları taramadan dışlayarak tarama hızını artırmaya olanak verir. Dosyalar, Kaspersky Endpoint Security veritabanlarının yayın tarihini, dosyanın son taranma tarihini ve tarama ayarlarında yapılan tüm değişiklikleri dikkate alan özel bir algoritma kullanılarak taramaların dışında tutulur. iChecker Teknolojisi için sınırlamalar vardır: büyük dosyalarla çalışmaz ve yalnızca uygulamanın tanıdığı yapıdaki dosyalara uygulanır (örneğin; EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP ve RAR).
Dosya Tehdidi Korumasını Duraklat *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Bu, belirtilen zamanda veya belirtilen uygulamalarla çalışırken Dosya Tehdidi Korumasının çalışmasını geçici ve otomatik olarak duraklatır.
Windows kapsayıcılarında yürütülen dosya işlemlerinin taranması	Bir kapsayıcı içinde bir tehdit algılanırsa, uygulama Dosya Tehdit Koruması bileşeni için seçilen eylemi uygular. **Temizleme başarısız olursa kapsayıcıyı durdur**. Uygulama, algılanan nesne için yeterli okuma ve yazma haklarına sahip olmayabilir. Bu durumda, tespit edilen nesnenin temizlenmesi veya silinmesi mümkün değildir. Bu onay kutusu işaretlendiğinde, uygulama algılanan nesneyi engeller ve kapsayıcıyı durdurur. Bu onay kutusunun işareti kaldırıldığında, uygulama yalnızca algılanan nesneyi engeller. **Windows kapsayıcılarında yürütülen dosya işlemlerini tarama**. Onay kutusu işaretlendiğinde, uygulama kapsayıcı yalnızca kapsayıcı başlangıcında tarar. Onay kutusunun işareti kaldırıldığında, uygulama kapsayıcıyı gerçek zamanlı olarak sürekli tarar.

Web Tehdidi Koruması

Web Tehdidi Koruması bileşeni, internetten zararlı dosyaların indirilmesini önler ve ayrıca zararlı ve kimlik avı amaçlı web sitelerine bağlantıyı engeller. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Kaspersky Endpoint Security sadece HTTP, HTTPS ve FTP trafiğini tarar. Kaspersky Endpoint Security URL'leri ve IP adreslerini tarar.

Tehdit Korumasını kullanmak için uygulamanın ilk yapılandırmasını tamamlamanız gerekir:

- HTTPS trafiğini izlemek için şifreli bağlantı taramasını etkinleştirin (varsayılan olarak etkindir).
- Kaspersky Endpoint Security'nin izlemesi gereken portları seçin (varsayılan olarak uygulama tüm portları izler).
- Kaspersky Endpoint Security'nin trafiğini izlemesini istediğiniz uygulamaları seçin. Çoğu tarayıcı Kaspersky tarafından önerilen uygulamalar listesinde zaten vardır. Eğer tarayıcınız listede yoksa manuel olarak ekleyin.
- Web trafiğine bir web sayfası etkileşim komut dosyası enjekte etmenizi öneririz (varsayılan olarak komut dosyası enjeksiyonu devre dışıdır). Bu komut dosyası, uygulama olay günlüğü, işletim sistemi olay günlüğü ve raporlar için Web Tehdidi Koruması olaylarının kaydını sağlar.

Bir kullanıcı kötü amaçlı veya kimlik avı yapan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller ve bir uyarı gösterir.

Web Tehdidi Koruması bileşeni ayarları

Parametre	Açıklama
Güvenlik düzeyi *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Uygulama, Web Tehdidi Koruması için farklı ayar grupları uygulayabilir. Uygulamada saklanan bu ayar kümelerine *güvenlik seviyeleri* denir: • **Yüksek**. Web Tehdidi Koruması bileşeninin, bir bilgisayarın HTTP ve FTP yoluyla aldığı web trafiğinin maksimum taramasını gerçekleştirdiği güvenlik düzeyi. Web Tehdidi Koruması, uygulama veritabanlarının tam setini kullanarak tüm İnternet trafiği nesnelerini ayrıntılı olarak tarar ve mümkün olan en ayrıntılı sezgisel analizi gerçekleştirir. • **Önerilen**. Uygulamanın performansı ve İnternet trafiği güvenliği arasında en iyi dengeyi sağlayan güvenlik düzeyidir. Web Tehdidi Koruması bileşeni, normal tarama düzeyinde sezgisel analiz yapar. Bu İnternet trafiği güvenlik düzeyi Kaspersky uzmanları tarafından önerilir. • **Düşük**. Bu İnternet trafiği güvenlik düzeyinin ayarları, en yüksek İnternet trafiğin tarama hızını sağlar. Web Tehdidi Koruması bileşeni, hızlı tarama düzeyinde sezgisel analiz yapar.
Tehdit algılandığında yapılacak eylem	**Engelle**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Web Tehdidi Koruması bileşeni nesneye erişimi engeller ve tarayıcıda bir mesaj görüntüler. **Bilgilendir**. Bu seçenek işaretlenir ve İnternet trafiğinde virüslü bir nesne tespit edilirse, Kaspersky Endpoint Security bu nesnenin bilgisayara indirilmesine izin verir ancak nesneyi virüslü nesne hakkında etkin tehditler listesine ekler.
Web adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Kötü amaçlı web adresleri veritabanına dahil edilip edilmediğini belirlemek için bağlantıların taranması, red listesine alınmış web sitelerini izlemenize olanak tanır. Kaspersky tarafından güncellenen kötü amaçlı web adreslerinin veritabanı, uygulama kurulum paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri sırasında güncellenir.
Sezgisel analiz kullan *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	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. Virüs ve tehdit oluşturan diğer uygulamalar için web trafiği tarandığında, sezgisel çözümleyici yürütülebilir dosyalarda talimatları uygular. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
Web adresini kimlik avı internet adresleri veritabanıyla karşılaştırarak kontrol et *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	E-dolandırıcılık web adreslerinin veritabanı, e-dolandırıcılık saldırıları başlatmak için kullanılan halihazırda bilinen web sitelerinin web adreslerini içerir. Kaspersky, kimlik avı bağlantılarından oluşan veritabanını, Anti-Phishing Çalışma Grubu olarak da bilinen uluslararası kuruluştan alınan adreslerle destekler. E-dolandırıcılık adresleri veritabanı, uygulama yükleme paketinde bulunur ve Kaspersky Endpoint Security veritabanı güncellemeleri ile tamamlanmaktadır.
Güvenilir adreslerin web trafiğini tarama	Bu seçenekt ercih edildiğinde, Web Tehdidi Koruması bileşeni, adresleri güvenilir internet adresleri listesinde bulunan web sayfalarının veya web sitelerinin içeriğini taramaz. İnternet sayfasının/İnternet sitesinin hem tam adresini hem de adres maskesini güvenilir internet adresleri listesine ekleyebilirsiniz. Ayrıca şifrelenmiş bağlantılar için genel bir istisna listesi oluşturabilirsiniz. Bu durumda, Kaspersky Endpoint Security, Web Tehdidi Koruması, Posta Tehdidi Koruması, İnternet Denetimi bileşenleri işlerini yaparken güvenilir internet adreslerinin HTTPS trafiğini taramaz.

Posta Tehdidi Koruması

Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarının eklerinde virüsler ve diğer tehditler için tarama yapar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar.

Posta Tehdidi Koruması hem gelen hem de giden mesajları tarayabilir. Uygulama, aşağıdaki posta istemcilerinde POP3, SMTP, IMAP ve NNTP'yi destekler:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Mozilla Thunderbird, MyOffice Mail ve R7-Office Organizer posta istemcilerindeki trafiği taramak için Kaspersky sertifikasını sertifika deposuna eklemeniz ve kendi sertifika deposunu seçmeniz gerekir.

Posta Tehdidi Koruması, diğer protokolleri ve posta istemcilerini desteklemez.

Posta Tehdidi Koruması her zaman mesajlara *protokol düzeyinde* erişim sağlayamayabilir (örneğin, Microsoft Exchange çözümünü kullanırken). Bu nedenle Posta Tehdidi Koruması, Microsoft Office Outlook için uzantı içerir. Uzantı, mesajların *posta istemcisi düzeyinde* taranmasına izin verir. Posta Tehdidi Koruması eklentisi, Outlook 2010, 2013, 2016, 2019, 2021, 2024 ve 365'in 32 bit ve 64 bit sürümlerini destekler. Arm tabanlı bilgisayarlarda, Posta Tehdidi Koruması uzantısı Outlook 2016, Outlook 2021, Outlook 2024 ve Arm64 için Outlook 365'in 32 bit ve 64 bit sürümlerini destekler.

Posta Tehdidi Koruması bileşeni, posta istemcisi bir tarayıcıda açıldığında mesajları taramaz.

Bir ekte kötü amaçlı bir dosya algılandığında, Kaspersky Endpoint Security mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.

Posta Tehdidi Koruması bileşeni ayarları

Parametre	Açıklama
Güvenlik düzeyi *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	Uygulama, Posta Tehdidi Koruması için farklı ayar grupları uygulayabilir. Uygulamada saklanan bu ayar kümelerine *güvenlik seviyeleri* denir: • **Yüksek**. Bu e-posta güvenlik düzeyi seçildiğinde Posta Tehdidi Koruması bileşeni e-posta mesajlarını en kapsamlı şekilde tarar. Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarını tarar ve derin sezgisel analiz gerçekleştirir. Yüksek riskli ortamlar için Yüksek posta güvenlik düzeyi önerilir. Merkezi e-posta koruması tarafından korunmayan bir ev ağından bağlanılan ücretsiz bir e-posta hizmeti bağlantısı böyle bir ortama örnektir. • **Önerilen**. Uygulamanın performansı ve e-posta güvenliği arasında en iyi dengeyi sağlayan e-posta güvenlik düzeyidir. Posta Tehdidi Koruması bileşeni, gelen ve giden e-posta mesajlarını tarar ve orta düzeyde sezgisel analiz yapar. Bu e-posta trafiği güvenlik düzeyi Kaspersky uzmanları tarafından önerilmektedir. • **Düşük**. Bu e-posta güvenlik düzeyi seçildiğinde Posta Tehdidi Koruması bileşeni, yalnızca gelen e-posta mesajlarını tarar, hafif sezgisel analiz gerçekleştirir ve e-posta mesajlarına eklenen arşivleri taramaz. Bu e-posta güvenlik düzeyinde, Posta Tehdidi Koruması bileşeni e-posta mesajlarını maksimum hızla tarar ve işletim sistemi kaynaklarını minimum seviyede kullanır. Düşük e-posta güvenlik düzeyinin, iyi korunmuş bir ortamda kullanılması önerilir. Bu tip bir çevreye örnek olarak merkezi e-posta güvenliği içeren bir kurumsal LAN gösterilebilir.

Parametre	Açıklama
Tehdit algılandığında yapılacak eylem	**Temizle; temizleme başarısız olursa sil**. Gelen veya giden bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse uygulama virüslü nesneyi siler. Uygulama, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*. **Temizle; temizleme başarısız olursa engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edildiğinde, uygulama tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler. **Engelle**. Gelen bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Giden bir mesajda virüs bulaşmış bir nesne tespit edilirse, uygulama mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.
Koruma kapsamı *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	*Koruma kapsamı*, bileşenin çalıştırıldığında denetlediği nesneleri içerir: gelen ve giden mesajlar veya sadece gelen mesajlar. Bilgisayarlarınızı korumak için yalnızca gelen mesajları taramanız gerekir. Etkilenen dosyaların arşivlere gönderilmesini önlemek için giden mesajların taranmasını açabilirsiniz. Ses ve video dosyaları gibi belirli biçimlerde dosyaların gönderilmesini önlemek istiyorsanız, giden mesajların taranmasını da açabilirsiniz.
POP3, SMTP, NNTP ve IMAP trafiğini tara	POP3, SMTP, NNTP ve IMAP iletişim kuralları aracılığıyla aktarılan trafiğin Posta Tehdit Koruması bileşeni tarafından taranması.
Microsoft Outlook uzantısını bağla	Bu onay kutusu işaretlenirse POP3, SMTP, NNTP, IMAP iletişim kuralları yoluyla iletilen e-posta mesajlarının taranması, Microsoft Outlook'a entegre uzantıda etkinleştirilir. Posta Microsoft Outlook uzantısı kullanılarak taranıyorsa, Cached Exchange Mode kullanılması önerilir. Önbelleklenmiş Exchange modu ve nasıl kullanıldığıyla ilgili öneriler hakkında daha ayrıntılı bilgi için Microsoft Bilgi Bankası 'na bakın.
Sezgisel analiz *(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)*	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. Kötü amaçlı kod için dosyaları tararken, sezgisel çözümleyici yürütülebilir dosyalardaki talimatları yürütür. Sezgisel çözümleyici tarafından yürütülen talimatların sayısı, sezgisel çözümleyici için belirtilen seviyeye bağlıdır. Sezgisel analiz düzeyi, yeni tehditler için aramanın bütünlüğü, işletim sisteminin kaynakları üzerindeki yük ve sezgisel analizin süresi arasında denge sağlar.
Ekli arşivleri tara	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar. Tarama sırasında uygulama mesaj metninde bir arşiv parolası tespit ederse, bu parola arşivin içeriğini kötü amaçlı uygulamalara karşı taramak için kullanılır. Bu durumda şifre kaydedilmez. Bir arşiv tarama sırasında açılır. Çıkarma işlemi sırasında bir uygulama hatası oluşursa, şu yola kaydedilen paketten çıkarılmış dosyaları manuel olarak silebilirsiniz: %systemroot%\temp. Dosyalarda PR öneki bulunur.
Microsoft Office biçimlerindeki ekli dosyaları tara	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.
Şundan büyük arşivleri tarama: N MB	Bu onay kutusu işaretlenirse Posta Tehdidi Koruması bileşeni, boyutları belirtilen değeri aşarsa e-posta mesajlarına eklenen arşivleri tarama kapsamının dışında tutar. Onay kutusunun işareti kaldırılırsa Posta Tehdidi Koruması bileşeni, herhangi bir boyuttaki e-posta eki arşivlerini tarar.
Arşivleri kontrol süresini şununla sınırla: N saniye	Onay kutusu işaretlenirse e-posta mesajlarına ekli arşivleri taramak için ayrılan süre belirtilen süreyle sınırlandırılır.
Ek filtresi	Ek filtresi, giden e-posta mesajlarına uygulanmaz. **Filtrelemeyi devre dışı bırak**. Bu seçenek tercih edilirse Posta Tehdidi Koruması bileşeni e-posta mesajlarına eklenen dosyaları filtrelemez. **Seçili türlerdeki ekleri yeniden adlandır**. Bu seçenek seçilmişse, Posta Tehdidi Koruması bileşeni, belirtilen türdeki ekli dosyalarda bulunan son uzantı karakterini alt çizgi karakteriyle değiştirir (örneğin attachment.doc_). Bu nedenle, dosyayı açmak için kullanıcının dosyayı yeniden adlandırması gerekir. **Seçili türlerdeki ekleri sil**. Bu seçenek tercih edilirse Posta Tehdidi Koruması bileşeni, belirtilen türlerin ekli dosyalarını e-posta mesajlarından siler. Dosya maskelerinin listesinde, ekli dosyaların türlerini belirleyerek bunları e-posta mesajlarından silebilir veya yeniden adlandırabilirsiniz.

Ağ Tehdidi Koruması

Ağ Tehdidi Koruması bileşeni (Ayrıca Intrusion Detection System, IDS olarak da adlandırılır), ağ saldırılarının karakteristik aktiviteleri için gelen ağ trafiğini izler. Uygulama kullanıcının bilgisayarına gerçekleştirilen bir ağ saldırısı tespit ederse, saldıran bilgisayarla ağ bağlantısını engeller. Şu anda bilinen ağ saldırısı türlerinin açıklamaları ve bunlara karşı koyma yolları, uygulama veritabanlarında sunulmaktadır. Ağ Tehdidi Koruması bileşeninin tespit ettiği ağ saldırıları listesi, veritabanı ve uygulama modülü güncellemeleri sırasında güncellenir.

Ağ Tehdidi Koruması bileşeni ayarları

Parametre	Açıklama
Port tarama ve ağ taşma olaylarına saldırı olarak davran	*Ağ Taşma*, bir kuruluşun ağ kaynaklarına (web sunucuları gibi) yapılan bir saldırıdır. Bu saldırıda, ağ kaynaklarının bant genişliğini aşırı yüklemek için çok sayıda istek gönderimi yapılır. Bu olduğunda, kullanıcılar kuruluşun ağ kaynaklarına erişim sağlayamaz. *Port Tarama* saldırısı, bilgisayardaki UDP portlarının, TCP portlarının ve ağ hizmetlerini taramaktan oluşur. Bu saldırı, saldırganın daha tehlikeli ağ saldırıları gerçekleştirmeden önce bilgisayarın güvenlik açığı düzeyini belirlemesine olanak tanır. Port Tarama sayesinde saldırgan aynı zamanda bilgisayardaki işletim sistemini tanımlayabilir ve bu işletim sistemi için uygun ağ saldırılarını seçebilir. Bu onay kutusu işaretlenirse Kaspersky Endpoint Security bu saldırıları tespit etmek için ağ trafiğini izler. Bir saldırı tespit edilirse, uygulama kullanıcıyı bilgilendirir ve ilgili olayı Kaspersky Security Center'a gönderir. Uygulama, zamanında tehdit yanıt eylemleri için gerekli olan saldıran bilgisayar hakkında bilgi sağlar. İzin verilen uygulamalardan bazılarının bu tür saldırılar için tipik olan işlemleri gerçekleştirmesi durumunda, bu tür saldırıların algılanmasını devre dışı bırakabilirsiniz. Bu, yanlış alarmların önlenmesine yardımcı olacaktır.
Saldırıda bulunan cihazları şu kadar süre için engelle N dk	Bu seçenek etkinleştirilirse, Ağ Tehdidi Koruması bileşeni saldıran bilgisayarı engellenenler listesine ekler. Bu, Ağ Tehdidi Koruması bileşeninin saldırgan bir bilgisayarın ağ bağlantısını, ilk ağ saldırısı denemesinden sonra belirli bir süre boyunca engellediği anlamına gelir. Bu engelleme aynı adresten gelecekteki olası ağ saldırılarına karşı kullanıcının bilgisayarını otomatik olarak korur. Saldıran bir bilgisayarın engelleme listesinde geçirmesi gereken minimum süre bir dakikadır. Maksimum süre 999 dakikadır. Ağ İzleyicisi aracı penceresinde engelleme listesini görüntüleyebilirsiniz. Kaspersky Endpoint Security, uygulama yeniden başlatıldığında ve Ağ Tehdidi Koruması ayarları değiştirildiğinde engelleme listesini temizler.
İstisnalar	Liste, Ağ Tehdidi Koruması'nın ağ saldırılarını engellemediği IP adreslerini içerir. Port ve iletişim kuralı belirtilmiş bir IP adresi ekleyebilirsiniz. Uygulama, istisnalar listesinde bulunan IP adreslerinden gelen ağ saldırılarına ilişkin bilgileri günlüğe kaydetmez.
MAC kafesleme koruması	*MAC kafesleme saldırısı*, bir ağ aygıtının (ağ kartı) MAC adresini değiştirmeye çalışır. Böylece saldırgan bir aygıta gönderilen verileri başka bir aygıta yönlendirerek bu verilere erişim sağlayabilir. Kaspersky Endpoint Security, MAC Aldatma saldırılarını engellemenizi ve bu saldırılar hakkında bildirimler almanızı sağlar.

Güvenlik Duvarı

Güvenlik Duvarı bileşeni, internet veya yerel ağ üzerinde çalışırken bir bilgisayara yetkisiz bağlantıları engeller. Güvenlik Duvarı aynı zamanda bilgisayardaki uygulamaların ağ etkinliklerini de denetler. Bu, kurumsal LAN'ınızı kimlik hırsızlığı ve diğer saldırılara karşı korumanızı sağlar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve önceden tanımlanmış *ağ kuralları* yardımıyla bilgisayar koruması sağlar.

Kaspersky Security Center ile etkileşim için Ağ Aracısı kullanılır. Güvenlik duvarı, uygulamanın ve Ağ Aracısının çalışması için gereken ağ kurallarını otomatik olarak oluşturur. Sonuç olarak, Güvenlik Duvarı bilgisayarda birkaç port açar. Hangi portların açılacağı bilgisayarın rolüne bağlıdır (örneğin, dağıtım noktası). Bilgisayarda açılacak portlar hakkında daha fazla bilgi edinmek için Kaspersky Security Center Yardım içeriğine bakın.

Ağ kuralları

Ağ kurallarını şu düzeylerde yapılandırabilirsiniz:

- *Ağ paketi kuralları*. Ağ paketi kuralları, uygulamaya bakılmaksızın ağ paketlerine sınırlamalar getirir. Bu kurallar, seçilen veri iletişim kuralının belirli portları yoluyla gelen ve giden ağ trafiğini sınırlar. Kaspersky Endpoint Security'nin, Kaspersky uzmanları tarafından önerilen izinlere sahip önceden tanımlanmış ağ paketi kuralları vardır.

- *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.

Uygulamaların işletim sistemi kaynaklarına, işlemlerine ve kişisel verilere kontrollü erişimi, Sunucu Yetkisiz Erişim Önleme bileşeni tarafından *uygulama hakları* kullanılarak sağlanır.

Uygulamanın ilk başlatılması sırasında, Güvenlik Duvarı şu eylemleri gerçekleştirir:

1. İndirilen anti virüs veritabanlarını kullanarak uygulamanın güvenliğini kontrol eder.

2. Kaspersky Security Network'teki uygulamanın güvenliğini denetler.

   Güvenlik Duvarının daha etkin çalışmasını sağlamak için Kaspersky Security Network'e katılmanız önerilir.

3. Uygulamayı güven gruplarından birine sokar: *Güvenilir*, *Düşük Kısıtlamalı*, *Yüksek Kısıtlamalı*, *Güvenilmez*.

   Güvenilirlik grubu, Kaspersky Endpoint Security'nin uygulama etkinliğini denetlerken uyguladığı hakları tanımlar. Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, bu uygulamanın bilgisayar için oluşturduğu tehdidin seviyesine göre yerleştirir.

   Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, Güvenlik Duvarı ve Sunucu Yetkisiz Erişim Önleme bileşenleri için yerleştirir. Güven grubunu sadece Güvenlik Duvarı ya da Sunucu Yetkisiz Erişim Önleme için değiştiremezsiniz.

   KSN'ye katılmayı reddederseniz ya da ağ bağlantısı olmazsa, Kaspersky Endpoint Security uygulamayı Sunucu Yetkisiz Erişim Önleme bileşeninin ayarlarına göre bir güven grubuna yerleştirir. KSN'den uygulamanın saygınlığı alındıktan sonra, güven grubu otomatik olarak değiştirilebilir.

4. Güven grubuna bağlı olarak uygulamanın ağ etkinliklerini engeller. Örneğin *Yüksek Kısıtlamalı* güven grubundaki uygulamaların herhangi bir ağ bağlantısını kullanmasına izin verilmez.

Uygulamanın bir sonraki başlatılmasında, Kaspersky Endpoint Security uygulamanın bütünlüğünü kontrol eder. Uygulama değişmediyse bileşen, geçerli ağ kurallarını kullanır. Uygulama değiştirildiyse Kaspersky Endpoint Security ilk kez başlatılıyormuş gibi uygulamayı analiz eder.

Ağ Kuralı Öncelikleri

Her kuralın bir önceliği vardır. Bir kural listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Ağ etkinliğinin birkaç kurala eklenmesi halinde, Güvenlik Duvarı ağ etkinliğini en yüksek önceliğe sahip kurala göre düzenler.

Ağ paketi kuralları, uygulamalar için ağ kurallarından daha yüksek bir 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 belirli bir şekilde çalışır. Uygulamalar için ağ kuralı, ağ durumuna dayalı erişim kurallarını içerir: *Ortak ağ*, *Yerel ağ*, *Güvenilir ağ*. 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 türleri

Güvenlik Duvarı, ağ bağlantısının türüne bağlı olarak ağ etkinliklerini kontrol etmenize olanak tanır. Kaspersky Endpoint Security ağ bağlantısı türünü bilgisayarın işletim sisteminden alır. İşletim sistemindeki ağ bağlantısının türü, bağlantının ayarlanması sırasında kullanıcı tarafından ayarlanır. Kaspersky Endpoint Security ayarlarından ağ bağlantısı türünü değiştirebilirsiniz. Güvenlik Duvarı ağ etkinliklerini işletim sistemindeki ağ türüne göre değil Kaspersky Endpoint Security ayarlarındaki ağ durumuna göre izleyecektir.

Aşağıdaki ağ bağlantısı türleri mevcuttur:

- **Ortak ağ**. Ağ antivirüs uygulamaları, güvenlik duvarları veya filtreler tarafından korunmaz (bir kafedeki Wi-Fi gibi). 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 internete *Ortak ağ* türünü atar. İnternetin türünü değiştiremezsiniz.

- **Yerel ağ**. Bu bilgisayardaki dosyalara ve yazıcılara kısıtlı erişime sahip kullanıcılar için olan ağdır (bir kurumsal LAN veya ev ağı gibi).

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

Güvenlik duvarı bileşeni ayarları

Parametre	Açıklama
Paket kuralları	Ağ paketi kurallarının listesini içeren tablodur. Ağ paketi kuralları, uygulamaya bakılmaksızın ağ paketlerine sınırlamalar getirilmesini sağlar. Bu kurallar, seçilen veri iletişim kuralının belirli portları yoluyla gelen ve giden ağ trafiğini sınırlar. Tabloda, Microsoft Windows işletim sistemlerinde çalışan bilgisayarların ağ trafiğini en iyi seviyede korumak için Kaspersky tarafından önerilen önceden yapılandırılmış ağ paketi kuralları listelenmektedir. Güvenlik duvarı, her ağ paketi kuralının yürütülme önceliğini belirler. Güvenlik duvarı, ağ paketi kurallarını, ağ paketi kuralları listesindeki görünüm sırasına göre yukarıdan aşağıya doğru işler. Güvenlik duvarı, ağ bağlantısı için uygun olan en üstteki ağ paket kuralını bulur ve bunu, ağ etkinliğine izin vererek veya engelleyerek uygular. Güvenlik duvarı bundan sonra bu ağ bağlantısı için diğer tüm ağ paket kurallarını yoksayar. Ağ paketi kuralları, uygulamalar için ağ kurallarından daha yüksek bir önceliğe sahiptir.
Kullanılabilir ağlar	Bu tablo, Güvenlik Duvarı'nın bilgisayarda tespit ettiği ağ bağlantıları hakkında bilgi içerir. *Ortak ağ* durumu, varsayılan olarak internete atanır. İnternet'in durumunu değiştiremezsiniz.
Uygulamalar için kurallar	**Uygulama**. Güvenlik Duvarı bileşeni tarafından denetlenen uygulamaların tablosu. Uygulamalar güven gruplarına atanmıştır. Bir güvenilirlik grubu, uygulamaların ağ etkinliğini denetlerken Kaspersky Endpoint Security tarafından kullanılan hakları tanımlar. Bir ilkenin etkisi altındaki bilgisayarlara yüklenmiş tüm uygulamaların yer aldığı tek bir listeden bir uygulama seçebilir ve uygulamayı bir güven grubuna ekleyebilirsiniz. **Ağ kuralları**. Bir güven grubunun parçası olan uygulamalar için ağ kuralları tablosudur. Güvenlik Duvarı, uygulamaların ağ etkinliğini bu kurallara göre düzenler. Tablo, Kaspersky uzmanları tarafından önerilen önceden tanımlanmış ağ kurallarını görüntüler. Bu ağ kuralları, Windows tabanlı işletim sistemlerini çalıştıran bilgisayarların ağ trafiğini optimum bir şekilde korumak amacıyla eklenmiştir. Önceden tanımlanmış ağ kurallarını silmek mümkün değildir.

BadUSB Saldırısı Önleme

Bazı virüsler, işletim sistemini USB aygıtını bir klavye gibi algılayacak şekilde kandırmak için USB aygıtların üretici yazılımını değiştirir. Sonuç olarak virüs, örneğin zararlı yazılım indirmek için kullanıcı hesabınız altında komutlar yürütebilir.

BadUSB Saldırısı Önleme bileşeni, klavyeye öykünen virüslü USB aygıtların bilgisayara bağlanmasını engeller.

Bilgisayara bir USB cihazı bağlandığında ve işletim sistemi tarafından klavye olarak algılandığında, uygulama kullanıcıdan uygulama tarafından üretilen sayısal bir kodu bu klavyeyi ya da varsa Ekran Klavyesini kullanarak girmesini ister (aşağıdaki şekle bakın). Bu işlem, klavye yetkilendirme olarak bilinir.

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 klavye yetkilendirmenin tekrarlanması gerekmez.

Yetkilendirilen klavye bilgisayarın farklı bir USB portuna bağlandığında, uygulama bu klavyenin yetkilendirilmesi için bir istem görüntüler.

Sayısal kod yanlış girildiyse uygulama yeni bir kod üretir. Sayısal kodun girişmesi için deneme sayısını yapılandırabilirsiniz. Sayısal kod birkaç kez yanlış girilirse veya klavye yetkilendirme penceresi kapatılırsa (aşağıdaki şekle bakın), uygulama bu klavyeden giriş yapılmasını engeller. USB aygıtı engelleme süresi dolduğunda ya da işletim sistemi yeniden başlatıldığında, uygulama kullanıcıdan yeniden klavye yetkilendirme yapmasını ister.

Uygulama yetkilendirilmiş bir klavyenin kullanımına izin verir ve yetkilendirilmemiş bir klavyeyi engeller.



Klavye yetkilendirme

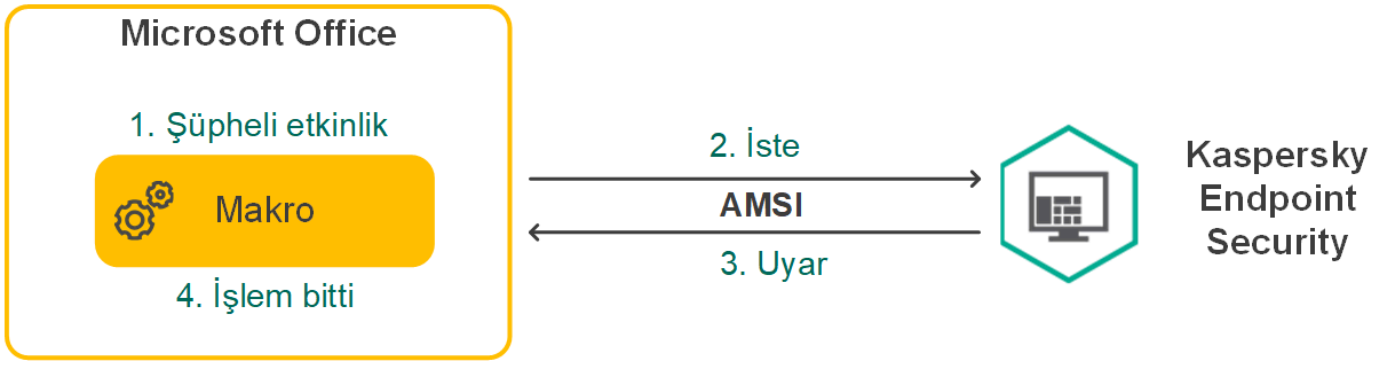
BadUSB Saldırısı Önleme bileşeni ayarları

Parametre	Açıklama
USB cihazlarının kimlik doğrulaması için Ekran Klavyesinin kullanımını yasakla	Anahtar açık durumda ise, uygulama bir yetkilendirme kodunun girilemediği bir USB cihazının yetkilendirilmesi için Ekran Klavyesinin kullanımını engeller.
USB cihazlarının kimlik doğrulaması için barkod kullanımını yasakla	Bu anahtar etkinleştirilirse, uygulama barkod tarayıcı kimlik doğrulama bildiriminde barkodu göstermez.
Maksimum sayıda USB cihazı doğrulama girişimi	Yetkilendirme kodunun belirtilen sayıda yanlış girilmesi durumunda USB cihazı otomatik olarak bloke edilir. Geçerli değerler 1 ila 10 arasındadır. Örneğin, yetkilendirme kodunu girmek için beş denemeye izin verirseniz, uygulama beşinci başarısız denemeden sonra USB cihazını engeller. Kaspersky Endpoint Security, USB cihazı için engelleme süresini görüntüler. Bu süre dolduktan sonra, yetkilendirme kodunu girmek için yine beş deneme hakkınız vardır.
Maksimum girişim sayısına ulaşılırken zaman aşımı	Yetkilendirme kodunu girmek için belirtilen sayıda başarısız denemeden sonra USB cihazı engelleme süresi. Geçerli değerler 1 ila 180 (dakika) arasındadır.

AMSI Koruması

AMSI Koruması bileşeni, Microsoft'un Antimalware Scan Interface işlevini desteklemeyi amaçlamaktadır. *Antimalware Scan Interface (AMSI)*, AMSI destekli üçüncü taraf uygulamaların, bu nesneleri ek bir tarama için Kaspersky Endpoint Security'ye göndermesine ve bu nesnelerin tarama sonuçlarını almasına (örneğin PowerShell komut dizileri) olanak tanır. Üçüncü taraf uygulamalarına örnek olarak Microsoft Office uygulamaları verilebilir (aşağıdaki resme bakın). AMSI hakkında ayrıntılar için lütfen Microsoft belgelerine bakın.

AMSI Koruması yalnızca bir tehdidi tespit edebilir ve tespit edilen tehditle ilgili bilgilendirme yapar. Bir üçüncü taraf uygulaması, bir tehdit bildirimi aldıktan sonra, kötü niyetli eylemlere izin vermez (örneğin, eylemi sonlandırır).



AMSI çalışma örneği

AMSI Koruması bileşeni, üçüncü taraf uygulamadan gelen bir isteği reddedebilir (örneğin bu uygulama, belirtilen bir aralıktaki maksimum istek sayısını aşıyorsa). Kaspersky Endpoint Security, üçüncü taraf bir uygulamadan gelen talebin reddedilmesine ilişkin bilgileri Yönetim Sunucusuna iletir. AMSI Koruma bileşeni, AMSI Koruma bileşeniyle sürekli entegrasyon etkin durumda olan üçüncü taraf uygulamalarından gelen istekleri reddetmez.

AMSI Koruması, iş istasyonları ve sunucular için aşağıdaki işletim sistemlerinde kullanılabilir:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise çoklu oturum
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise çoklu oturum
- Windows Server 2016 Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2019 Essentials / Standard / Datacenter (Server Core modu dahil)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Server Core modu dahil)
- Windows Server 2025 Standard / Datacenter

AMSI Koruması ayarları

Parametre	Açıklama
Arşivleri tara	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE ve diğer arşiv biçimleri taranır. Uygulama, arşivleri sadece uzantıya göre değil biçime göre de tarar. Arşivleri kontrol ederken, uygulama özyinelemeli bir paket açma işlemi gerçekleştirir. Bu, çok seviyeli arşivlerin (arşiv içinde arşiv) içindeki tehditlerin tespit edilmesini sağlar.
Dağıtım paketlerini tara	Üçüncü taraf uygulamaların dağıtım paketlerinin taranması.
Microsoft Office biçimlerindeki dosyaları tara	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office biçimindeki dosyalar da OLE nesnelerini içerir. Uygulama, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.
Büyük bileşik dosya paketlerini açma	Bu onay kutusu işaretlendiğinde, uygulama boyutları belirtilen değeri aşan birleşik dosyaları taramaz. Bu onay kutusu işaretlenmediğinde, uygulama her boyuttaki birleşik dosyaları tarar. Uygulama, onay kutusunun seçili olup olmadığından bağımsız olarak arşivlerden çıkarılan büyük dosyaları tarar.

Exploit Önleme

Exploit Önleme bileşeni, yönetici ayrıcalıklarını kullanmak ya da zararlı etkinlikler gerçekleştirmek amacıyla bilgisayardaki zayıf noktalardan faydalanan program kodunu tespit eder. Örneğin istismarcılar bir arabellek taşması saldırısı kullanabilir. İstismarcı bunu yapmak için savunmasız bir uygulamaya büyük miktarda veri gönderimi yapar. Bu verileri işleyen savunmasız uygulama da zararlı kodları çalıştırır. Bu saldırının sonucunda istismarcı zararlı bir yazılımın izinsiz yüklemesini başlatabilir. Yürütülebilir bir dosyanın hassas bir uygulama tarafından çalıştırılması girişimi kullanıcı tarafından gerçekleştirilmediyse Kaspersky Endpoint Security, bu dosyanın çalıştırılmasını engeller ve kullanıcıyı bilgilendirir.

Exploit Önleme bileşeni ayrıca bilgisayarın güvenliğini tehdit edebilecek uygulamaların işlemleri için ağ portlarını izler. Uygulama, anti-virüs veritabanları ile bu tür işlemler hakkında bilgi alır.

Exploit Önleme bileşeni ayarları

Parametre	Açıklama
Exploit algılandığında	**Engelle**. Bu öğe işaretliyse Kaspersky Endpoint Security, bir açıktan yararlanma tespit ettiğinde bu açıktan yararlanma işlemlerini engeller ve bu açıktan yararlanma hakkında bilgileri içeren bir günlük girişi yapar. **Bilgilendir**. Bu öğe seçiliyse ve Kaspersky Endpoint Security exploit tespit ederse exploit hakkında bilgileri içeren bir olayı günlüğe kaydeder ve bu exploit hakkında bilgileri etkin tehditler listesine ekler.
Sistem işlemleri bellek korumasını etkinleştir	Bu iki durumlu düğme açılırsa Kaspersky Endpoint Security, sistem işlem belleğine erişim girişiminde bulunan dış işlemleri engeller.

Davranış Tespiti

Davranış Tespiti bileşeni, bilgisayarınızdaki uygulamaların işlemleriyle ilgili veriler toplar ve bu bilgileri, performanslarını iyileştirmek için diğer koruma bileşenlerine sağlar. Davranış Tespiti bileşeni, uygulamalar için Davranış Akışı İmzalarından (BSS) yararlanır. Uygulama etkinliğinin bir davranış akımı imzasıyla eşleşmesi halinde Kaspersky Endpoint Security seçili duyarlı işlemi gerçekleştirir. Davranış akışı imzalarına dayanan Kaspersky Endpoint Security işlevi, bilgisayarınız için ileriye dönük etkili koruma sağlar.

Davranış Tespiti bileşeni ayrıca bilgisayarın güvenliğini tehdit edebilecek uygulamaların işlemleri için ağ portlarını izler. Uygulama, anti-virüs veritabanları ile bu tür işlemler hakkında bilgi alır.

Davranış Tespiti bileşeni ayarları

Parametre	Açıklama
Kötü amaçlı yazılım etkinliği tespit edildiğinde gerçekleştirilecek eylem	**Sil**. Bu seçenek seçilirse Kaspersky Endpoint Security, zararlı yazılım etkinliği tespit edildiğinde zararlı uygulamanın yürütülebilir dosyasını siler ve dosyanın bir yedekleme kopyasını Yedekleme'de oluşturur. **Engelle**. Bu seçenek seçilirse Kaspersky Endpoint Security, zararlı yazılımların etkinlikleri tespit edildiğinde bu uygulamayı sonlandırır. **Bilgilendir**. Bu seçenek işaretlenmiş ve uygulamanın zararlı yazılım etkinliği tespit edilirse Kaspersky Endpoint Security uygulamayı sonlandırmaz ama bu uygulamanın zararlı yazılım etkinliği hakkındaki bilgileri etkin tehditler listesine ekler.

Sunucu Yetkisiz Erişim Önleme

Sunucu Yetkisiz Erişim Önleme bileşeni, uygulamaların işletim sistemi için tehlikeli olabilecek işlemler yapmasını engeller ve işletim sistemi kaynaklarına ve kişisel verilere erişim üzerinde denetim sağlar. Bileşen, anti-virüs veritabanları ve Kaspersky Security Network bulut hizmetinin yardımıyla bilgisayar koruması sağlar.

Bileşen, *uygulama haklarını* kullanarak uygulamaların çalışmasını denetler. Uygulama hakları şu erişim parametrelerini kapsar:

- İşletim sistemi kaynaklarına erişim (örneğin seçeneklerin, kayıt defteri anahtarlarının otomatik başlatılması)
- Kişisel verilere erişim (örneğin, dosyalar ve uygulamalar)

Uygulamaların ağ etkinliği, *ağ kuralları* kullanılarak Güvenlik Duvarı bileşeni tarafından kontrol edilir.

Uygulamanın ilk başlatılması sırasında, Sunucu Yetkisiz Erişim Önleme bileşeni şu eylemleri gerçekleştirir:

1. İndirilen anti virüs veritabanlarını kullanarak uygulamanın güvenliğini kontrol eder.
2. Kaspersky Security Network'teki uygulamanın güvenliğini denetler.

   Sunucu Yetkisiz Erişim Önleme bileşeninin daha etkin çalışmasını sağlamak için Kaspersky Security Network'e katılmanız önerilir.

3. Uygulamayı güven gruplarından birine sokar: *Güvenilir*, *Düşük Kısıtlamalı*, *Yüksek Kısıtlamalı*, *Güvenilmez*.

   Güvenilirlik grubu, Kaspersky Endpoint Security'nin uygulama etkinliğini denetlerken uyguladığı hakları tanımlar. Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, bu uygulamanın bilgisayar için oluşturduğu tehdidin seviyesine göre yerleştirir.

   Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, Güvenlik Duvarı ve Sunucu Yetkisiz Erişim Önleme bileşenleri için yerleştirir. Güven grubunu sadece Güvenlik Duvarı ya da Sunucu Yetkisiz Erişim Önleme için değiştiremezsiniz.

   KSN'ye katılmayı reddederseniz ya da ağ bağlantısı olmazsa, Kaspersky Endpoint Security uygulamayı Sunucu Yetkisiz Erişim Önleme bileşeninin ayarlarına göre bir güven grubuna yerleştirir. KSN'den uygulamanın saygınlığı alındıktan sonra, güven grubu otomatik olarak değiştirilebilir.

4. Uygulama eylemlerini güven grubuna göre engeller. Örneğin, *Yüksek Kısıtlamalı* güven grubundan olan uygulamaların işletim sistemi modüllerine erişimi reddedilir.

Uygulamanın bir sonraki başlatılmasında, Kaspersky Endpoint Security uygulamanın bütünlüğünü kontrol eder. Uygulama değişmediyse bileşen, geçerli uygulama haklarını kullanır. Uygulama değiştirildiyse Kaspersky Endpoint Security ilk kez başlatılıyormuş gibi uygulamayı analiz eder.

Parametre	Açıklama
Uygulama hakları	Sunucu Yetkisiz Erişim Önleme bileşeni tarafından izlenen uygulamaların tablosu. Uygulamalar güven gruplarına atanmıştır. Güvenilirlik grubu, Kaspersky Endpoint Security'nin uygulama etkinliğini denetlerken uyguladığı hakları tanımlar. Bir ilkenin etkisi altındaki bilgisayarlara yüklenmiş tüm uygulamaların yer aldığı tek bir listeden bir uygulama seçebilir ve uygulamayı bir güven grubuna ekleyebilirsiniz. Uygulama erişim hakları şu tablolarda sunulur: • **Dosya ve sistem kayıt defteri**. Güvenilirlik grubuna ait uygulamalar için işletim sistemi kaynakları ve kişisel veriler için erişim hakları tablosu. • **Haklar**. Güvenilirlik grubuna ait uygulamalar için işletim sisteminin işlemlerine ve kaynaklarına yönelik erişim hakları tablosu. • **Ağ kuralları**. Bir güven grubunun parçası olan uygulamalar için ağ kuralları tablosudur. Bu kurallara uygun olarak Güvenlik Duvarı, uygulamaların ağ etkinliğini düzenler. Tablo, Kaspersky uzmanları tarafından önerilen önceden tanımlanmış ağ kurallarını görüntüler. Bu ağ kuralları, Windows tabanlı işletim sistemlerini çalıştıran bilgisayarların ağ trafiğini optimum bir şekilde korumak amacıyla eklenmiştir. Önceden tanımlanmış ağ kurallarını silmek mümkün değildir.
Korunan kaynaklar	Bu tablo, kategorilere ayrılan bilgisayar kaynaklarını içerir. Sunucu Yetkisiz Erişim Önleme bileşeni diğer uygulamalar tarafından tablodaki kaynaklara yapılan erişim girişimlerini izler. Kaynak; bir kayıt kategorisi, dosya veya klasör ya da kayıt defteri anahtarı olabilir.
Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güven grubu	Kaspersky Endpoint Security'nin, Kaspersky Endpoint Security başlatılmadan önce başlatılan uygulamaları yerleştireceği bir güvenilirlik grubu.
KSN'den eskiden bilinmeyen uygulamalar için kuralları güncelle	Onay kutusu işaretlenirse Sunucu Yetkisiz Erişim Önleme bileşeni, Kaspersky Security Network veritabanını kullanarak önceden bilinmeyen uygulamaların haklarını günceller.
Dijital olarak imzalanmış uygulamalara güven	Bu onay kutusu işaretlenirse Sunucu Yetkisiz Erişim Önleme bileşeni, güvenilir satıcıların dijital imzalı uygulamalarını *Güvenilir* gruba yerleştirir. *Güvenilir satıcılar*, Kaspersky'nin güvendiği yazılım satıcılarıdır. Güvenilir sertifika deposuna manuel olarak da satıcı sertifikası ekleyebilirsiniz. Onay kutusunun işareti kaldırılırsa Sunucu Yetkisiz Erişim Önleme bileşeni, bu tür uygulamaları güvenilir kabul etmez ve onların güvenilirlik gruplarını belirlemek için başka parametreler kullanır.
Şundan daha uzun bir süredir başlatılmayan uygulamaların kurallarını sil: N gün (1 - 90 arası)	Bu onay kutusu işaretlenirse, aşağıdaki koşullar yerine getirildiğinde Kaspersky Endpoint Security uygulama hakkındaki bilgileri (güvenilirlik grubu ve erişim hakları) otomatik olarak siler: • Uygulamayı manuel olarak bir güvenilirlik grubuna koydunuz veya erişim haklarını yapılandırdınız. • Uygulama, belirlenen süre içinde başlamadı. Bir uygulamanın güven grubu ve hakları otomatik olarak belirlenirse, Kaspersky Endpoint Security 30 gün sonra bu uygulama hakkındaki bilgileri siler. Uygulama bilgileri için saklama süresini değiştirmek veya otomatik silmeyi kapatmak mümkün değildir. Bu uygulamayı bir sonraki başlatışınızda, Kaspersky Endpoint Security uygulamayı ilk kez başlatılıyormuş gibi analiz eder.
Diğer gruplara dahil olmayan uygulamalar için güvenilirlik grubu	Bu açılır listedeki öğeler, Kaspersky Endpoint Security'nin bilinmeyen bir uygulamayı hangi güvenilirlik grubuna atayacağını belirler. Aşağıdaki öğelerden birini seçebilirsiniz: • **Düşük Kısıtlamalı**. • **Yüksek Kısıtlamalı**. • **Güvenilmez**.

Düzeltme Altyapısı

Düzeltme Altyapısı, Kaspersky Endpoint Security' bileşeninin işletim sisteminde zararlı yazılımların gerçekleştirdiği etkinlikleri geri almasını sağlar.

Kaspersky Endpoint Security, işletim sistemindeki zararlı yazılım etkinliğini geri alırken aşağıdaki zararlı yazılım türlerine işlem yapar:

- **Dosya etkinliği**

  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

  - Zararlı yazılımlar tarafından oluşturulan yürütülebilir dosyaları (ağ sürücüleri hariç tüm ortamlardakileri) siler.
  - Zararlı yazılımların sızdığı programlar tarafından oluşturulmuş yürütülebilir dosyaları siler.
  - Zararlı yazılımlar tarafından değiştirilmiş veya silinmiş dosyaları geri yükler.

  Dosya kurtarma özelliğinin bazı sınırlamaları vardır.

- **Kayıt defteri etkinliği**

  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

  - Zararlı yazılımlar tarafından oluşturulmuş kayıt defteri anahtarlarını siler.
  - Zararlı yazılımlar tarafından değiştirilmiş veya silinmiş kayıt defteri anahtarlarını geri yüklemez.

- **Sistem etkinliği**

  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

  - Zararlı yazılımlar tarafından başlatılmış işlemleri sonlandırır.
  - Zararlı uygulamaların girdiği işlemleri sonlandırır.
  - Zararlı yazılımlar tarafından durdurulan işlemleri sürdürmez.

- **Ağ etkinliği**

  Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

  - Zararlı yazılımların ağ etkinliğini engeller.
  - Zararlı yazılımların sızdığı işlemlerin ağ etkinliğini engeller.

Zararlı yazılım eylemlerini geri alma işlemi Dosya Tehdidi Koruması veya Davranış Tespiti bileşeni tarafından ya da kötü amaçlı yazılım 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.

Kaspersky Security Network



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.

KSN işlevselliği ABD'de yazılımda kullanılabilir olmayabilir.

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. Kaspersky Security Network'e katılıyorsanız, KSN hizmetleri Kaspersky Endpoint Security'ye taranan web adreslerinin itibarı hakkında bilgi ve taranan dosyaların kategorisi ve tanınırlığı hakkında bilgi sağlar. KSN'ye erişim ayarları hakkında daha fazla ayrıntı için Kaspersky Security Center Yardım bölümüne bakın.

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.

KSN'ye katılım sırasında oluşturulan istatistiksel bilgilerin Kaspersky'ye gönderilmesi ve bu bilgilerin depolanması ve imhası hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Network Bildirimi'ne ve Kaspersky web sitesi'ne başvurun. Kaspersky Security Network Bildirimi metnine sahip ksn_<dil kodu>.txt dosyası dağıtım kitinde mevcuttur.

Kaspersky tanınırlık veritabanlarının altyapısı

Kaspersky Endpoint Security, Kaspersky tanınırlık veritabanlarıyla çalışmak için şu altyapı çözümlerini destekler:

- *Kaspersky Security Network (KSN)*, çoğu Kaspersky uygulaması tarafından kullanılan çözümdür. KSN katılımcıları Kaspersky'denbilgiler alır ve kullanıcının bilgisayarında tespit edilen nesneler hakkındaki Kaspersky bilgilerini, Kaspersky analistleri tarafından ek analize tabi tutulması ve tanınırlık ve istatistiksel veritabanlarına dahil edilmesi için gönderir.

- *Kaspersky Private Security Network (KPSN),* Kaspersky Endpoint Security veya diğer Kaspersky uygulamaları yüklü bilgisayarların kullanıcılarının kendi bilgisayarlarından Kaspersky'ye veri gönderimi yapmadan Kaspersky tanınırlık veritabanlarına ve diğer istatistiksel verilere erişim elde etmelerini sağlayan bir çözümdür. KPSN, aşağıdaki sebeplerden herhangi birinden ötürü Kaspersky Security Network'e katılamayan kurumsal müşteriler için tasarlanmıştır:

    - Yerel iş istasyonları İnternet'e bağlı değildir.

Verilerin ülke ya da kurumsal LAN dışına aktarılması yasalarca yasaklanmış ya da kurumsal güvenlik politikaları nedeniyle kısıtlanmıştır.

Parametre	Açıklama
Genişletilmiş KSN modunu etkinleştir	*Genişletilmiş KSN modu*, Kaspersky Endpoint Security'nin Kaspersky'ye daha fazla veri gönderdiği bir moddur. Kaspersky Endpoint Security, KSN'yi iki durumlu düğmenin konumundan bağımsız olarak tehditleri algılamak için kullanır.
Bulut modunu etkinleştir	*Bulut modu*, Kaspersky Endpoint Security'nin anti-virüs veritabanlarının daha basit bir sürümünü kullandığı uygulama çalışma moduna karşılık gelir. Kaspersky Security Network, uygulamanın basit anti-virüs veritabanlarını kullanarak çalışmasını destekler. Anti-virüs veritabanlarının basit sürümü ile kullanılan RAM miktarı, normal veritabanları ile kullanılan RAM miktarının yaklaşık olarak yarısıdır. Kaspersky Security Network'e katılmazsanız ya da bulut modu devre dışı bırakılırsa, Kaspersky Endpoint Security Kaspersky sunucularından anti-virüs veritabanlarının en son sürümünü indirir. İki durumlu düğme açılırsa Kaspersky Endpoint Security, anti-virüs veritabanlarının basit sürümünü kullanır, bu da işletim sistemi kaynaklarındaki yükü azaltır. Kaspersky Endpoint Security, onay kutusu seçildikten sonra bir sonraki güncellemede anti-virüs veritabanlarının basit sürümünü indirir. İki durumlu düğme kapatılırsa Kaspersky Endpoint Security anti-virüs veritabanlarının tam sürümünü kullanır. Kaspersky Endpoint Security, onay kutusu işaretinin kaldırılmasından bir sonraki güncellemede anti-virüs veritabanlarının tam sürümünü indirir.
KSN sunucuları kullanılamadığında bilgisayarın durumu *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu açılır listedeki öğeler, KSN sunucularının kullanılabilir olmadığı durumlarda bir bilgisayarın Kaspersky Security Center'daki durumunu belirler.
Yönetim Sunucusunu KSN proxy sunucusu olarak kullanma *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Onay kutusu işaretlenirse Kaspersky Endpoint Security, KSN Proxy hizmetini kullanır. KSN Proxy hizmeti ayarlarını Yönetim Sunucusu özelliklerinden yapılandırabilirsiniz.
KSN proxy sunucusu kullanılamıyorsa Kaspersky Security Network sunucularını kullan *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Onay kutusu işaretlenirse Kaspersky Endpoint Security, KSN Proxy hizmeti kullanılabilir olmadığında KSN sunucularını kullanır. KSN sunucuları hem Kaspersky'nin tarafında hem de üçüncü taraflar tarafında bulunabilir (Kaspersky Private Security Network kullanıldığında).

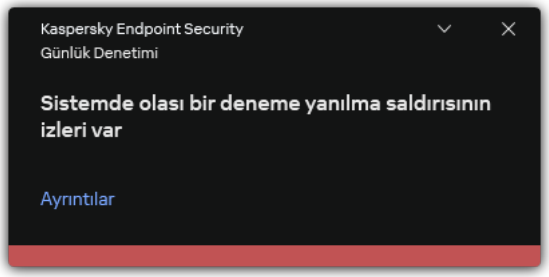
Günlük Denetimi

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

Günlük Denetimi, Windows olay günlüğü analizine göre korunan ortamın bütünlüğünü izler. Uygulama, sistemde tipik olmayan davranış belirtilerini tespit ettiğinde, bu davranış bir siber saldırı girişiminin göstergesi olabileceğinden yöneticiyi bilgilendirir.

Kaspersky Endpoint Security, Windows olay günlüklerini analiz eder ve kurallara uygun olarak ihlali tespit eder. Bileşen, önceden tanımlanmış kuralları içerir. Önceden tanımlanmış kurallar, sezgisel analiz tarafından desteklenir. Ayrıca kendi kurallarınızı ekleyebilirsiniz (özel kurallar). Bir kural tetiklendiğinde, uygulama, *Kritik* durumuna sahip bir olay oluşturur (aşağıdaki şekle bakın).

Günlük Denetimini kullanmak istiyorsanız, denetim ilkesinin güvenlik ayarlarının yapılandırıldığından ve sistemin ilgili olayları günlüğe kaydettiğinden emin olun (ayrıntılar için bkz. Microsoft teknik destek web sitesi.).



Günlük Denetimi bildirimi

Günlük Denetimi ayarları

Parametre	Açıklama
Önceden tanımlanmış kurallar	Günlük Denetimi kurallarının listesi. Önceden tanımlanmış kurallar, korunan bilgisayardaki anormal etkinlik şablonlarını içerir. Anormal etkinlik, saldırı girişimi anlamına gelebilir.
Özel kurallar	Kullanıcı tarafından eklenen Günlük Denetimi kurallarının listesi. Kendi Günlük Denetimi kuralı tetikleme kriterlerinizi belirleyebilirsiniz. Bunu yapmak için bir olay kimliği girmeli ve bir olay kaynağı seçmelisiniz. Standart günlükler arasından bir olay kaynağı seçebilirsiniz: *Uygulama*, *Güvenlik* veya *Sistem*. Ayrıca bir üçüncü taraf uygulamasının günlüğünü de belirtebilirsiniz.

Şifreleyici Önleyici

Şifreleyici Önleyici bileşeni paylaşılan klasörlerdeki etkinliği analiz eder. Bu etkinlik, dış şifreleme için tipik olan bir davranış akışı imzasıyla eşleşirse Kaspersky Endpoint Security seçili eylemi gerçekleştirir.

Kaspersky Endpoint Security, yalnızca NTFS dosya sistemine sahip olan ve EFS sistemi tarafından şifrelenmemiş ortamlarda bulunan dosyaların dış şifrelemesini önler.

Parametre	Açıklama
Ad veya IP adresine göre istisnalar	**Ad veya IP adresine göre istisnalar**. Paylaşılan klasörleri şifreleme girişimlerinin izlenmediği bilgisayarların listesidir. Paylaşılan klasörlerin dış şifrelemeye karşı korunmasından gelen bilgisayarlar istisnaları listesini uygulamak için Windows güvenlik denetleme ilkesinde Oturum Açı Denetlemeyi etkinleştirmeniz gerekir. Oturum Açı Denetle varsayılan olarak devre dışıdır. Windows güvenlik denetleme ilkesi hakkında daha ayrıntılı bilgi için lütfen Microsoft İnternet sitesini ziyaret edin. **Maskeye göre istisnalar**. Koruma kapsamı istisnaları. Bir klasörü koruma kapsamından çıkarmak, kuruluşunuz paylaşılan klasörleri kullanarak dosya alışverişi yaparken veri şifreleme kullanıyorsa hatalı pozitiflerin miktarını azaltabilir. Örneğin, Davranış Tespiti, kullanıcı paylaşılan bir klasörde ENC uzantılı dosyalarla çalıştığında hatalı pozitif sonuçlara neden olabilir. Bu etkinlik türü, dış şifreleme için tipik olan bir davranış kalıbıyla eşleşir. Verileri korumak için paylaşılan bir klasörde şifrelenmiş dosyalarınız varsa o klasörü istisnalara ekleyin. Maskeler kullanarak: • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir. • İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir. • `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.
Tehdit algılandığında yapılacak eylem	• **Bilgilendir**. Bu seçenek belirlenirse, paylaşılan klasörlerdeki dosyaları değiştirme girişimi algılandığında Kaspersky Endpoint Security, bu girişim hakkındaki bilgileri etkin tehditler listesine ekler, yerel uygulama arabirimi raporlarına bir giriş ekler ve tespit edilen algılanan kötü amaçlı etkinlikle ilgili bilgileri Kaspersky Security Center'a gönderir. • **Bağlantıyı şu kadar süre engelle (dk)**: **N dk**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security paylaşılan klasörlerdeki dosyaları değiştirme girişimi algıladığında, kötü amaçlı etkinliği başlatan oturum için dosya değiştirme erişimini engeller ve değiştirilen dosyaların yedek kopyalarını oluşturur. Düzeltme Altyapısı bileşeni etkinse ve **Bağlantıyı şu kadar süre engelle (dk)**: **N dk** seçeneği belirlenmişse değiştirilen dosyalar yedek kopyalarından geri yüklenir.
Koruma kapsamı	*Koruma kapsamı*, Kaspersky Endpoint Security'nin dosya etkinliğini izlediği paylaşılan klasörlere giden yolların bir listesidir. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. Varsayılan olarak, uygulama paylaşılan klasörleri otomatik olarak tanımlar ve tüm klasörlerdeki dosya etkinliğini izler.

İnternet Denetimi

İnternet Denetimi, web kaynaklarına kullanıcı erişimini yönetir. Böylece trafiğin azaltılmasına ve çalışma zamanının daha verimli kullanılmasına yardımcı olur. Bir kullanıcı İnternet Denetimi tarafından kısıtlanan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller veya bir uyarı gösterir (aşağıdaki şekle bakın).

İnternet Denetimini kullanmak için uygulamanın ilk yapılandırmasını tamamlamanız gerekir:

- HTTPS trafiğini izlemek için şifreli bağlantı taramasını etkinleştirin (varsayılan olarak etkindir).
- Kaspersky Endpoint Security'nin izlemesi gereken portları seçin (varsayılan olarak uygulama tüm portları izler).
- Kaspersky Endpoint Security'nin trafiğini izlemesini istediğiniz uygulamaları seçin. Çoğu tarayıcı Kaspersky tarafından önerilen uygulamalar listesinde zaten vardır. Eğer tarayıcınız listede yoksa manuel olarak ekleyin.
- Web trafiğine bir web sayfası etkileşim komut dosyası enjekte etmenizi öneririz (varsayılan olarak komut dosyası enjeksiyonu devre dışıdır). Bu komut dosyası, uygulama olay günlüğü, işletim sistemi olay günlüğü ve raporlar için İnternet Denetimi olaylarının kaydını sağlar.

İnternet sitelerine erişimi yönetme yöntemleri

İnternet Denetimi, şu yöntemleri kullanarak web sitelerine erişimi yapılandırır:

- **Web sitesi kategorisi**. Web siteleri, Kaspersky Security Network bulut hizmeti, sezgisel analiz ve bilinen web siteleri veritabanını (uygulama veritabanlarının içindedir) kullanarak kategorize eder. Örneğin, kullanıcı erişimini *Sosyal ağlar* kategorisiyle veya diğer kategorilerle kısıtlayabilirsiniz.
- **Veri tipi**. Örneğin, bir web sitesindeki verilere kullanıcı erişimini kısıtlayabilir ve görüntüleri gizleyebilirsiniz. Kaspersky Endpoint Security veri türünü uzantısına göre değil dosya biçimine göre belirler.

  > Kaspersky Endpoint Security arşivlerin içindeki dosyaları taramaz. Örneğin resim dosyaları bir arşivin içindeyse, Kaspersky Endpoint Security bu dosyanın türünü *Grafikler* olarak değil *Arşivler* veri tipi olarak belirler.

- **Tek tek adresler**. Bir web adresi girebilir ya da maskeler kullanabilirsiniz.

Web sitelerine erişimi düzenlemek için birkaç yöntemi aynı anda kullanmak mümkündür. Örneğin *Ofis uygulama dosyaları* veri türüne erişimi sadece *Web tabanlı e-posta* web sitesi kategorisi için kısıtlayabilirsiniz.

Web sitesi erişim kuralları

İnternet Denetimi, *erişim kuralları* kullanarak web sitelerine kullanıcı erişimini düzenler. Bir web sitesi erişim kuralı için şu gelişmiş ayaları yapılandırabilirsiniz:

- Kuralın uygulanacağı kullanıcılar.

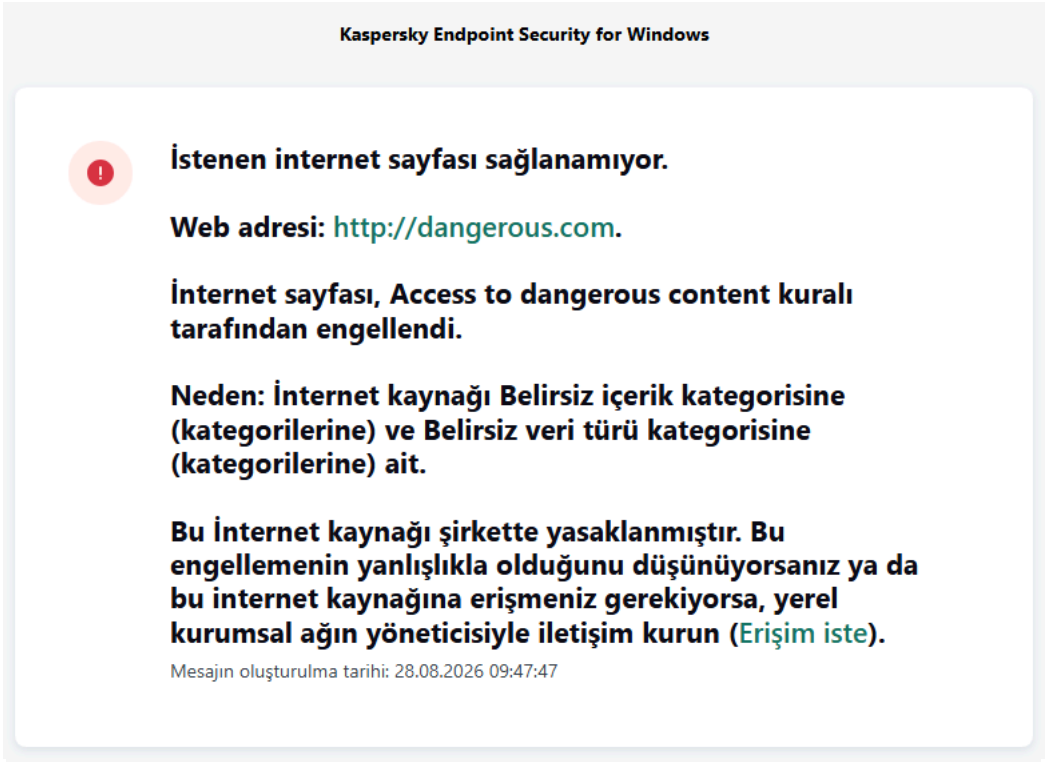
  Örneğin BT departmanı hariç olmak üzere şirketin tüm çalışanlarının bir tarayıcı üzerinden İnternete erişmesini kısıtlayabilirsiniz.

- Kural zamanlaması.

  Örneğin sadece çalışma saatleri içinde bir tarayıcıdan İnternete erişimi kısıtlayabilirsiniz.

Erişim kuralı öncelikleri

Her kuralın bir önceliği vardır. Bir kural listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Bir web sitesinin birden fazla kurala eklenmesi durumunda, İnternet Denetimi web sitesine erişimi en yüksek önceliğe sahip kurala göre düzenler. Örneğin Kaspersky Endpoint Security bir kurumsal portalı bir sosyal ağ olarak tanımlayabilir. Sosyal ağlara erişimi kısıtlarken kurumsal web portalına erişim sağlamak için iki kural oluşturun: *Sosyal ağlar* web sitesi kategorisi için bir kural ve kurumsal web postalı için bir kural. Kurumsal web portalına erişim kuralı, sosyal ağlara erişim kuralından daha yüksek önceliğe sahip olmalıdır.





İnternet Denetimi mesajları

İnternet Denetimi bileşen ayarları

Parametre	Açıklama
İnternet kaynaklarına erişim kuralları	İnternet kaynağı erişim kurallarını içeren liste. Her kuralın bir önceliği vardır. Bir kural listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Bir web sitesinin birden fazla kurala eklenmesi durumunda, İnternet Denetimi web sitesine erişimi en yüksek önceliğe sahip kurala göre düzenler.
Varsayılan kural	*Varsayılan kural*, herhangi başka bir kuralın kapsamında bulunmayan internet kaynaklarına erişim kuralıdır. Aşağıdaki seçenekler kullanılabilir: • Yasaklı web siteleri için reddedilenler listesi modu olarak da bilinen **Kurallar listesi dışında tümüne izin ver**. • İzin verilen web siteleri için izin verilenler listesi modu olarak da bilinen **Kurallar listesi dışında her şeyi reddet**.

Parametre	Açıklama
Kural uygulandıktan sonra etkin kullanıcı oturumlarını sonlandır	Onay kutusu işaretlendiğinde, İnternet Denetimi, ilke uygulandıktan hemen sonra engellenen web kaynaklarına olan bağlantıyı sonlandırır. Tarayıcı web sayfasından veri indirmeyi derhal durdurur. Web sayfasını yenilediğinizde veya yasaklanmış başka bir web sayfasına gittiğinizde, uygulama bir uyarı görüntüler. İnternet Denetimi, yalnızca internet tarayıcılarında internet kaynaklarının bağlantısının hemen kesilmesini sağlar. Diğer uygulamalar için İnternet Denetimi yalnızca yeni bağlantıları kısıtlar. Onay kutusunun işareti kaldırılırsa, İnternet Denetimi yalnızca yasaklanmış web kaynaklarına yeni bağlantıları kısıtlar. İnternet Denetimi etkin bağlantıları sonlandırmaz.
Şablonlar	**Uyarı**. Giriş alanı, istenmeyen bir İnternet kaynağına erişme girişimleri hakkında uyarı amaçlı bir kural tetiklendiğinde görüntülenen mesaj şablonundan oluşur. **Engelleme hakkında mesaj**. Giriş alanı, bir İnternet kaynağına erişimi engelleyen bir kural tetiklenirse görüntülenen mesajın şablonunu içerir. **Yöneticiye mesaj**. Kullanıcının engellemenin bir hata olduğunu değerlendirmesi halinde LAN yöneticisine gönderilecek mesaj şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için web sayfası erişimini engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir. Mesaj şablonlarını yönetmek için özel değişkenler sağlanır (örneğin, `%USER_NAME%`). Değişkenler, tek bir mesaj şablonunun farklı bilgisayarlar için kullanılmasına olanak tanır.
İzin verilen sayfaların açılması için günlük kaydı tut	Kaspersky Endpoint Security, izin verilenler de dahil olmak üzere tüm web sitelerine yapılan ziyaretlerin verilerini günlük dosyası olarak saklar. Kaspersky Endpoint Security, olayları Kaspersky Security Center'a, Kaspersky Endpoint Security'nin yerel günlük kaydına ve Windows Olay günlüğüne gönderir. Kullanıcı İnternet etkinliklerini izlemek için etkinliklerin kaydedilmesi için ayarları yapılandırmanız gerekir. İzleme işlevini destekleyen tarayıcılar: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Kullanıcı etkinliği izleme diğer tarayıcılarda çalışmaz. Kullanıcı İnternet etkinliklerinin izlenmesi, HTTPS trafiğinin şifresini çözerken daha fazla bilgisayar kaynağının kullanılmasını gerektirebilir.

Aygıt Denetimi

Aygıt Denetimi, bilgisayara yüklenen veya bağlanan aygıtlara (örneğin sabit sürücüler, kameralar veya Wi-Fi modülleri) kullanıcı erişimini yönetir. Bu, bu tür cihazlar bağlandığında bilgisayarı enfeksiyondan korumanıza ve veri kaybını veya veri sızıntılarını önlemenize olanak tanır.

Aygıt Denetimi etkinleştirilirse, uygulama bağlı cihazlar hakkındaki bilgileri Kaspersky Security Center'a aktarır. Bağlı cihazların listesini Kaspersky Security Center'daki **Gelişmiş** → **Veri havuzları** → **Donanım** klasöründe görüntüleyebilirsiniz.

Cihaz erişim düzeyleri

Aygıt Denetimi aşağıdaki düzeylerde erişimi denetler:

- **Aygıt türü**. Örneğin yazıcılar, çıkarılabilir sürücüler ve CD/DVD sürücüleri.

Aygıt erişimini aşağıdaki şekilde yapılandırabilirsiniz:

- İzin ver – .
- Engelle – .
- Kurallara göre (yalnızca yazıcılar ve taşınabilir cihazlar) – .
- Bağlantı veriyoluna bağlıdır (Wi-Fi hariç) – .
- İstisnalarla engelle (yalnızca Wi-Fi) - .

- **Bağlantı veri yolları**. *Bağlantı veri yolu*, bilgisayara aygıtları (örneğin USB veya FireWire) bağlamak için kullanılan bir arabirimdir. Cihaz tipi için **Bağlantı veriyoluna bağlıdır** modu seçilirse, uygulama bağlantı arabirimine (örneğin USB) bağlı olarak cihaza erişime izin verir veya erişimi reddeder.

  Aygıt erişimini aşağıdaki şekilde yapılandırabilirsiniz:

  - İzin ver – .
  - Engelle – .

- **Güvenilir aygıtlar**. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

  Güvenilir aygıtları aşağıdaki verilere göre ekleyebilirsiniz:

  - **Kimliğe göre aygıtlar**. Her cihazın benzersiz bir tanımlayıcısı (Hardware ID veya HWID) vardır. Bu kimliği, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. Cihaz kimliği örneği: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Birkaç belirli cihazı eklemek istiyorsanız cihazları kimliğe göre eklemek uygundur.
  - **Modele göre aygıtlar**. Her cihazın bir Vendor ID (VID) ve bir Product ID (PID) vardır. Bu kimlikleri, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. VID ve PID girme şablonu: `VID_1234&PID_5678`. Kuruluşunuzda belirli bir model cihazlar kullanıyorsanız cihazları modele göre eklemek uygundur. Böylece bu model tüm cihazları ekleyebilirsiniz.
  - **Kimlik maskesine göre aygıtlar**. Benzer kimliklere sahip birden fazla cihaz kullanıyorsanız, cihazları güvenilir listeye maskeler kullanarak ekleyebilirsiniz. `*` karakteri herhangi bir karakter kümesinin yerini alır. Kaspersky Endpoint Security, bir maske girişi yapılırken `?` karakterinin kullanımını desteklemez. Örneğin, `WDC_C*`.
  - **Model maskesine göre aygıtlar**. Benzer VID veya PID sahibi birden fazla aygıt kullanıyorsanız (örneğin aynı üreticinin aygıtları) maskeler kullanarak güvenilir listeye aygıt ekleyebilirsiniz. `*` karakteri herhangi bir karakter kümesinin yerini alır. Kaspersky Endpoint Security, bir maske girişi yapılırken `?` karakterinin kullanımını desteklemez. Örneğin, `VID_05AC&PID_*`.

Aygıt Denetimi, *erişim kuralları* kullanarak aygıtlara kullanıcı erişimini düzenler. Aygıt Denetimi, aygıt bağlantısı/aygıt bağlantının kesilmesi olaylarını kaydetmenize de izin verir. Olayları kaydetmek için olayların kaydını bir ilke içinde yapılandırmanız gerekir.

Bir aygıta erişim bağlantı veri yoluna bağlıysa (durumu) Kaspersky Endpoint Security, aygıt bağlantısı/aygıt bağlantısının kesilmesi olaylarını kaydetmez. Kaspersky Endpoint Security'nin aygıt bağlantısı/aygıt bağlantısının kesilmesi olaylarını kaydetmesini etkinleştirmek için ilgili aygıt türüne erişime izin verin (durumu) veya aygıtı güvenilir listeye ekleyin.

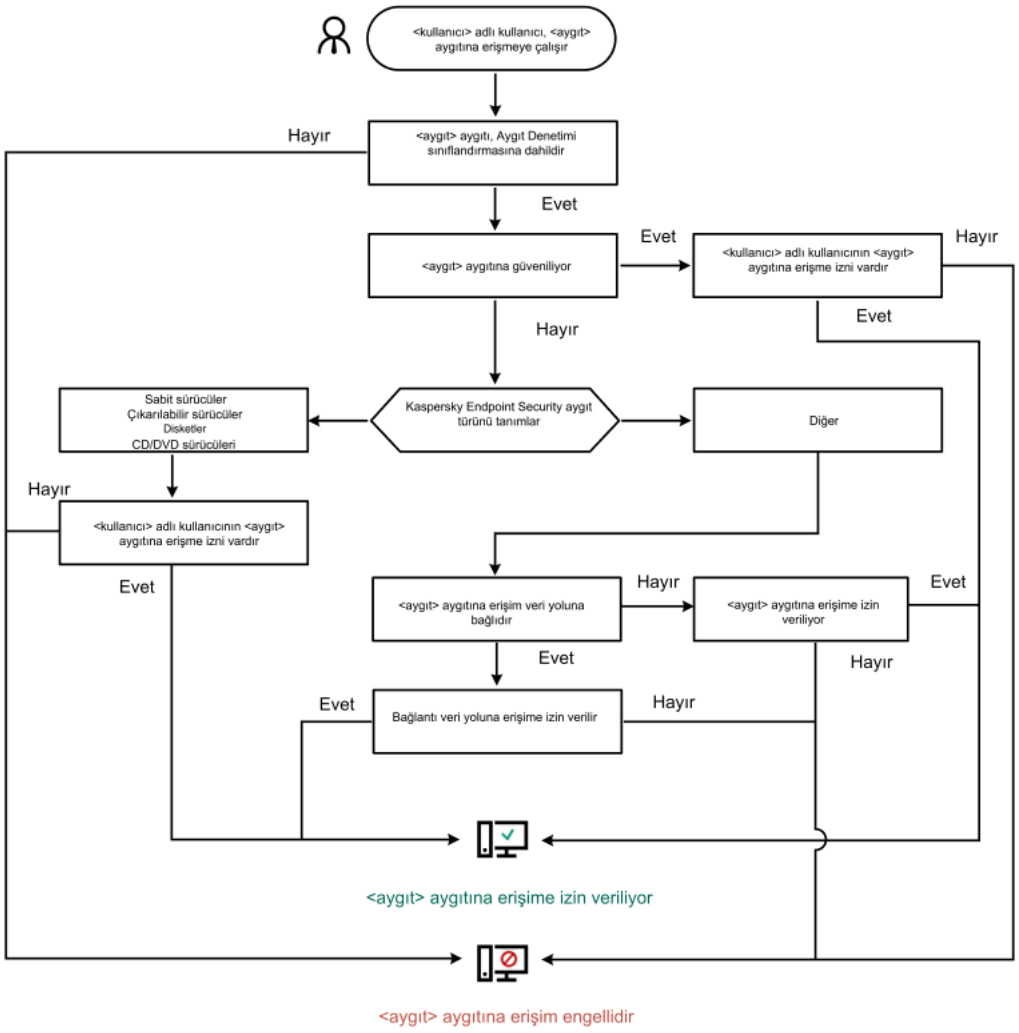
Aygıt Denetimi tarafından engellenen bir aygıt bilgisayara bağlandığında, Kaspersky Endpoint Security erişimi engeller ve bir bildirim gösterir (aşağıdaki şekle bakın).



Aygıt Denetimi bildirimi

Aygıt Denetimi işlem algoritması

Kaspersky Endpoint Security, kullanıcı aygıtı bilgisayara bağladıktan sonra aygıta erişime izin verip vermeyeceği hakkında bir karar verir (aşağıdaki resme bakın).



Aygıt Denetimi işlem algoritması

Bir cihaz bağlı ve erişim iznine sahipse erişim kuralını düzenleyebilir ve erişimini engelleyebilirsiniz. Bu durumda, bir kişinin bu aygıta bir sonraki bağlanma denemesinde (örneğin klasör ağacını görüntülemek ya da yazma veya okuma işlemleri gerçekleştirmek), 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 Denetimi bileşeni ayarları

Parametre	Açıklama
Geçici erişim isteğine izin ver *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Onay kutusu işaretlenirse **Erişim iste** düğmesi Kaspersky Endpoint Security'nin yerel arabirim aracılığıyla etkinleşir. Bu düğmeyi kullanarak, kullanıcı engellenen bir aygıta geçici erişim isteyebilir.
Aygıtlar ve Wi-Fi ağları	Bu tabloda, kendi erişim durumları da dahil olmak üzere Aygıt Denetimi bileşeninin sınıflandırmasına göre tüm olası aygıt türleri yer alır.
Bağlantı veri yolları	Kendi erişim durumları da dahil olmak üzere Aygıt Denetimi bileşeninin sınıflandırmasına göre tüm geçerli bağlantı veri yollarını içeren bir liste. Kaspersky Endpoint Security, **Bağlantı veriyoluna bağlıdır** modu seçilirse bağlantı veriyolunun türüne bağlı olarak cihazlara erişime izin verir veya erişimi reddeder.
Güvenilir aygıtlar	Bu aygıtlara erişim verilmiş güvenilir aygıtlar ve kullanıcılar listesi.
Devralırken değerleri birleştir *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu, Kaspersky Security Center'ın üst ve alt ilkelerindeki güvenilen cihazların listesini birleştirir. Listeleri birleştirmek için, alt ilke, Kaspersky Security Center'ın üst ilkesinin ayarlarını devralacak şekilde yapılandırılmalıdır. Onay kutusu seçiliyse, Kaspersky Security Center üst ilkesindeki liste öğeleri alt ilkelerde görüntülenir. Bu şekilde, örneğin, tüm kuruluş için birleştirilmiş bir güvenilir cihazlar listesi oluşturabilirsiniz. Bir alt ilkedeki devralınan liste öğeleri silinemez veya düzenlenemez. Devralma sırasında birleştirilen güvenilir aygıtlar listesindeki öğeler yalnızca üst ilkede silinebilir ve düzenlenebilir. Daha düşük düzey alt ilkelerdeki liste öğelerini ekleyebilir, düzenleyebilir veya silebilirsiniz. Alt ve üst ilke listelerindeki öğeler eşleşirse, bu öğeler üst ilkenin aynı öğesi olarak görüntülenir. Onay kutusu seçilmezse, Kaspersky Security Center ilkelerinin ayarlarını devralırken liste öğeleri birleştirilmez. Bu işlevsellik aynı zamanda ilke profillerindeki listelerin birleştirilmesine de olanak tanır. Listeleri birleştirmek için, en yüksek öncelikli profilde, ayarların daha düşük öncelikli bir profilden devralınmasını etkinleştirin. İlke profili öncelikleri hakkında daha fazla ayrıntı için lütfen Kaspersky Security Center Yardımı 'na başvurun.
Köprüleme Önleme	Köprüleme Önleme, bir bilgisayar için aynı anda birden fazla ağ bağlantısının kurulmasını engelleyerek ağ köprülerinin oluşturulmasını önler. Bu, bir kurumsal ağı korunmasız, yetkisiz ağlar üzerinden gelen saldırılara karşı korumanızı sağlar. Köprüleme Önleme, aygıtların önceliklerine göre birden fazla bağlantının korumasını engeller. Bir aygıt listenin ne kadar üst sırasında yer alıyorsa o kadar yüksek önceliğe sahiptir. Etkin bir bağlantı ve yeni bir bağlantı aynı türdense (örneğin Wi-Fi), Kaspersky Endpoint Security etkin olan bağlantıyı engeller ve yeni bağlantının kurulmasına izin verir. Etkin bir bağlantı ile yeni bir bağlantı farklı türlerdeyse (örneğin bir ağ bağdaştırıcısı ve Wi-Fi), Kaspersky Endpoint Security daha düşük önceliğe sahip olan bağlantıyı engeller ve daha yüksek önceliğe sahip olan bağlantıya izin verir. Köprüleme Önleme şu aygıt türleriyle çalışmayı destekler: ağ bağdaştırıcısı, Wi-Fi ve modem.
Mesaj şablonları	**Engelleme hakkında mesaj**. Bir kullanıcı engellenen bir cihaza erişmeyi denediğinde görüntülenen mesajın şablonu. Bu mesaj aynı zamanda bir kullanıcı bu kullanıcı için engellenmiş olan cihaz içeriğinde bir işlem gerçekleştirmeyi denediğinde de görüntülenir. **Yöneticiye mesaj**. Kullanıcı cihaza erişimin yanlışlıkla engellendiğine veya cihaz içeriği ile ilgili bir işlemin yanlışlıkla yasaklandığına inandığında LAN yöneticisine gönderilecek mesaj için bir şablon. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yöneticiye aygıta erişimin engellenmesine yönelik mesaj**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

Uygulama Denetimi

Uygulama Denetimi, kullanıcıların bilgisayarlarındaki uygulamaların başlatılmasını yönetir. Böylece uygulamalar kullanılırken bir kurumsal güvenlik ilkesi uygulamak mümkün olur. Uygulama Denetimi ayrıca uygulamalara erişimi kısıtlayarak bilgisayara virüs bulaşma riskini azaltır.

Uygulama Denetimi yapılandırması şu adımlardan oluşur:

1. Uygulama kategorileri oluşturma.

   Yönetici tarafından yönetilmek istenen uygulama kategorileri oluşturur. Uygulama kategorileri, yönetim gruplarından bağımsız olarak kurumsal ağdaki tüm bilgisayarlar içindir. Bir kategori oluşturmak için şu kriterleri kullanabilirsiniz: KL kategorisi (örneğin, *Tarayıcılar* veya başka bir kategori), dosya karması, uygulama satıcısı ve diğer kriterler.

2. Uygulama Denetimi kuralları oluşturma.

   Yönetici, yönetim grubu için ilkede Uygulama Denetimi kuralları oluşturur. Kural uygulama kategorilerini ve şu kategorilerdeki uygulamaların başlatma durumlarını içerir: engellenen veya izin verilen. Yönetici birçok kural oluşturabilir. Bir uygulama birden fazla kuralın kriterleriyle eşleşebilir. Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Kaspersky Endpoint Security, bir uygulamanın her başlatıldığında bir kuralla eşleşip eşleşmediğini kontrol eder. Kaspersky Endpoint Security, uygulamayı tüm Uygulama Denetimi kurallarıyla sıralı olarak eşleştirir.

3. Uygulama Denetimi modunu seçme.

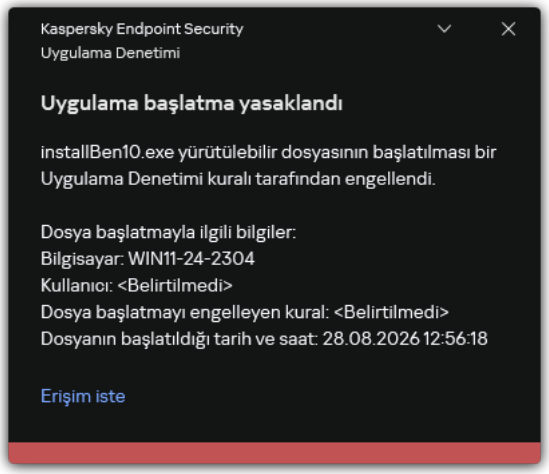
   Yönetici, şu kuralların herhangi birine dahil olmayan uygulamalarla çalışmak için mod seçimi yapar (uygulama reddedilenler ve izin verilenler listesi).

Bir kullanıcı yasaklanmış bir uygulamayı başlatmayı denediğinde, Kaspersky Endpoint Security uygulamanın başlatılmasını engeller ve bir bildirim görüntüler (aşağıdaki resme bakın).

Uygulama Denetimi yapılandırmasının kontrolü için bir *test modu* sunulur. Bu modda, Kaspersky Endpoint Security şunları yapar:

- Yasaklanmış olanlar da dahil olmak üzere uygulamaların başlatılmasına izin verir.
- Yasaklanmış bir uygulamanın başlatılması hakkında bir bildirim gösterir ve bilgileri kullanıcının bilgisayarındaki rapora ekler.

- Yasaklanan uygulamaların başlatılması hakkındaki bilgileri Kaspersky Security Center'a gönderir.



Uygulama Denetimi bildirimi

Uygulama Denetimi işletim modları

Uygulama Denetimi bileşeni iki modda çalışır:

- **Reddedilenler listesi**. Bu modda Uygulama Denetimi, Uygulama Denetimi kurallarında yasaklanan uygulamalar hariç olmak üzere tüm uygulamaların kullanıcılar tarafından başlatılmasına izin verir.

  Uygulama Denetimi'nin bu modu varsayılan olarak etkindir.

- **İzin verilenler listesi**. Bu modda Uygulama Denetimi, kullanıcıların Uygulama Denetimi izin ver kurallarında izin verilen ve yasaklanmamış uygulamalar haricinde herhangi bir uygulamayı başlatmasını engeller.

  Uygulama Denetimi izin ver kuralları tamamen yapılandırılırsa bileşen, işletim sisteminin ve kullanıcıların çalışmalarında güvendiği güvenilir uygulamaların çalışmasına izin verirken, LAN yöneticisi tarafından doğrulanmamış tüm yeni uygulamaların başlatılmasını engeller.

  Uygulama denetimi kurallarını izin verilenler listesi modunda yapılandırma hakkında öneriler'i okuyabilirsiniz.

Uygulama Denetimi, Kaspersky Endpoint Security yerel arabirimi ve Kaspersky Security Center kullanılarak 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.

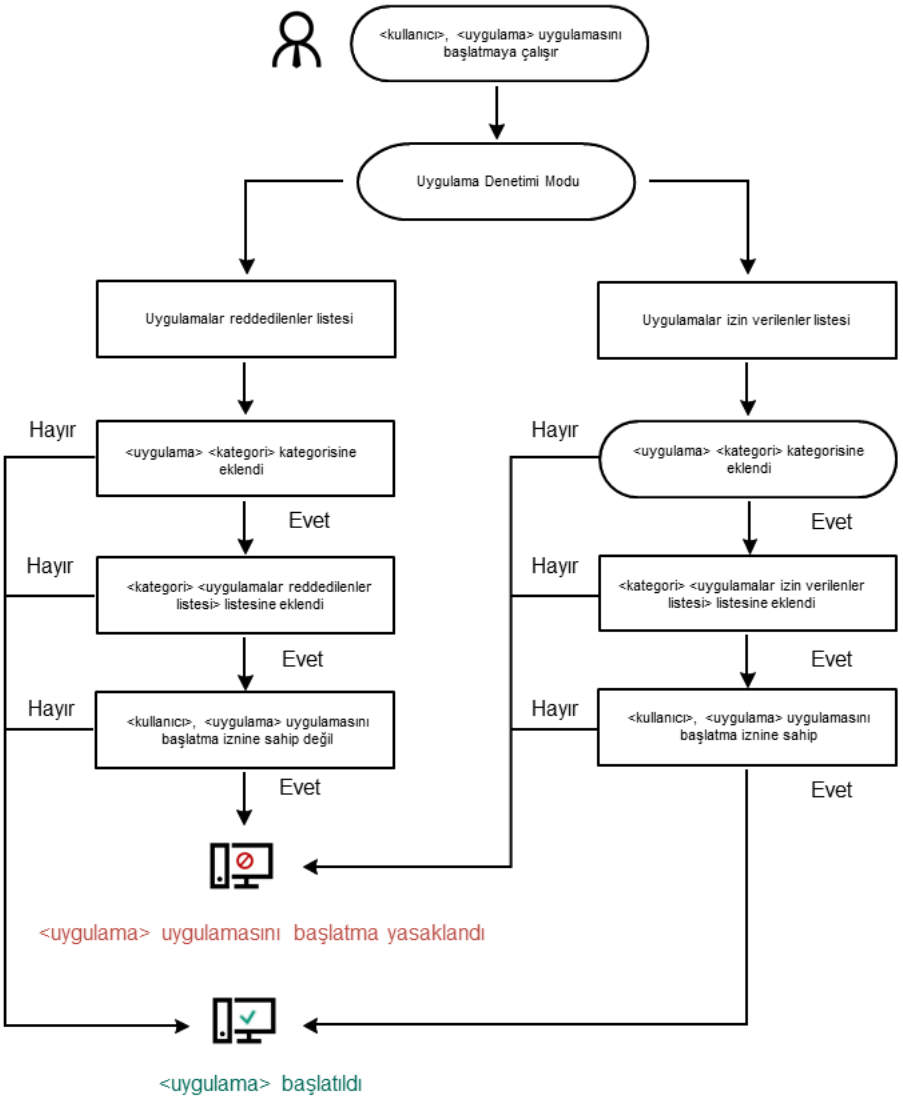
  Kaspersky Security Center Yönetim Konsolunda oluşturulan Uygulama Denetimi kuralları, Kaspersky Endpoint Security yerel arabiriminde olduğu gibi dahil etme ve hariç tutma koşullarına değil, özel uygulama kategorilerine dayanır.

- Kurumsal LAN bilgisayarlarına yüklenen uygulamalar hakkında bilgi toplama.

Uygulama Denetimi bileşeninin çalışmasını yapılandırmak için Kaspersky Security Center'ı kullanmanın önerilmesinin nedeni budur.

Uygulama Denetimi işlem algoritması

Kaspersky Endpoint Security, bir uygulamanın başlatılması hakkında karar vermek için bir algoritma kullanır (aşağıdaki resme bakın).



Uygulama Denetimi işlem algoritması

Parametre	Açıklama
Kurallar tarafından engellenen uygulamaları başlatma eylemi	**Kuralları uygula** Kaspersky Endpoint Security, uygulamaların başlatılmasını seçilen moda göre yönetir. **Kuralı test et**. Kaspersky Endpoint Security, geçerli Uygulama Denetimi modunda engellenen bir uygulamanın başlatılmasına izin verir ancak uygulamanın başlatılmasıyla ilgili bilgileri rapora kaydeder.
Uygulama Başlatma Denetimi modu	Aşağıdaki seçeneklerden birini seçebilirsiniz: • **Reddedilenler listesi**. Bu seçenek belirlenirse Uygulama Denetimi engelleme kurallarının koşullarının yerine getirildiği durumlar haricinde, Uygulama Denetimi tüm kullanıcıların herhangi bir uygulamayı başlatmasına izin verir. • **İzin verilenler listesi**. Bu seçenek belirlenirse Uygulama Denetimi izin verme kuralları koşullarının yerine getirildiği durumlar haricinde, Uygulama Denetimi tüm kullanıcıların herhangi bir uygulamayı başlatmasını engeller. **İzin verilenler listesi** modu seçildiğinde, otomatik olarak iki Uygulama Denetimi kuralı oluşturulur: • **Altın İmaj**. • **Güvenilir Güncelleyiciler**. Otomatik olarak oluşturulan kuralları silemez ya da ayarlarını düzenleyemezsiniz. Bu kuralları etkinleştirebilir veya devre dışı bırakabilirsiniz.
DLL modüllerinin yüklenmesini izle	Onay kutusu işaretlenirse, kullanıcılar uygulamaları başlatmaya çalıştığında Kaspersky Endpoint Security, DLL modüllerinin yüklenmesini denetler. DLL modülü ve DLL modülünü yükleyen uygulama hakkında bilgi, rapora kaydedilir. DLL modüllerinin ve sürücülerin yüklenmesine ilişkin denetimi etkinleştirirken, Uygulama Denetimi ayarlarındaki kurallardan varsayılan **Altın İmaj** kuralının ya da "**Altın İmaj\Güvenilir Sertifikalar**" KL kategorisini içeren başka bir kuralın etkinleştirildiğinden ve bu kuralın güvenilir DLL modüllerinin ve sürücülerin Kaspersky Endpoint Security başlatılmadan önce yüklenmesini sağladığından emin olun. **Altın İmaj** kuralı devre dışı bırakıldığında DLL modüllerinin ve sürücülerinin yükleme denetiminin etkinleştirilmesi, işletim sisteminde kararsızlığa neden olabilir. Kaspersky Endpoint Security, yalnızca onay kutusu seçildikten sonra yüklenen DLL modüllerini ve sürücüleri izler. Kaspersky Endpoint Security başlatılmadan önce, uygulamanın yüklenenler de dahil olmak üzere tüm DLL modüllerini ve sürücüleri izlemesi için bilgisayarın yeniden başlatılması önerilir.
Sıkı dijital imza doğrulaması kullanın	Bir Uygulama Denetimi kuralı için tetikleyici koşul olarak bir sertifika seçebilirsiniz. Bu onay kutusu seçilirse Kaspersky Endpoint Security, kuralları yalnızca güvenilir sistem sertifika deposundaki sertifikalarla imzalanmış uygulamalara uygular. Böyle bir sertifika ile imzalanmış uygulamalar, örneğin *Kötü Amaçlı Yazılım Taraması* görevi gibi koruma bileşenleri tarafından da güvenilir olarak kabul edilir. Ancak, bir Uygulama Denetimi kuralında farklı bir depodan sertifika belirtirseniz Kaspersky Endpoint Security böyle bir kuralı uygulamaz. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security, kuralları Windows Güvenilir Kök Sertifika Deposundaki bir sertifika tarafından imzalanmış uygulamalara uygular. Bu tür uygulamalar güvenilir bölgenin bir parçası değildir. Koruma bileşenleri bu tür uygulamaların etkinliğini izler.
Uygulama engelleme hakkında mesaj şablonları	**Engelleme hakkında mesaj**. Uygulamanın başlatılmasını engelleyen bir Uygulama Denetimi kuralı tetiklendiğinde görüntülenen mesajın şablonunu içerir. **Yöneticiye mesaj**. Kullanıcının bir uygulamanın yanlışlıkla engellendiğine inanması durumunda kullanıcının şirket LAN yöneticisine gönderebileceği mesajın şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için uygulama başlatmasını engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

Uyarlamalı Anomali Denetimi

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

Uyarlamalı Anomali Denetimi bileşeni, şirketin ağındaki bilgisayarlarda tipik olarak görülmeyen eylemleri izler ve engeller. Uyarlamalı Anomali Denetimi, tipik olmayan davranışı izlemek için kurallar dizisi kullanır (örneğin, *Microsoft PowerShell'in Office uygulamasından başlatılması* kuralı). Kurallar, Kaspersky uzmanları tarafından zararlı etkinliğin tipik senaryolarına dayanarak oluşturulur. Uyarlamalı Anomali Denetiminin her bir kuralı nasıl ele aldığını yapılandırabilirsiniz (örneğin, belirli iş akışı görevlerini otomatikleştiren PowerShell komut dizilerinin yürütülmesine izin vermek). Kaspersky Endpoint Security, uygulama veritabanlarıyla birlikte kurallar dizisini de günceller. Kurallar dizisinde yapılan güncellemeler elle onaylanmalıdır.

Uyarlamalı Anomali Denetimi ayarları

Uyarlamalı Anomali Denetimini yapılandırma işlemi şu adımlardan oluşur:

1. Uyarlamalı Anomali Denetimi eğitimi.

   Uyarlamalı Anomali Denetimini etkinleştirmenizin ardından kurallar *eğitim modunda* çalışır. Eğitim sırasında Uyarlamalı Anomali Denetimi, kural tetiklemeyi izler ve tetikleme etkinliklerini Kaspersky Security Center'a gönderir. Her kuralın kendi eğitim modu süresi vardır. Eğitim modunun süresi Kaspersky uzmanları tarafından belirlenir. Normalde eğitim modu iki hafta boyunca etkindir.

   Bir kural eğitim boyunca hiç tetiklenmezse Uyarlamalı Anomali Denetimi bu kuralla ilgili eylemleri tipik değil olarak ele alır. Kaspersky Endpoint Security bu kuralla ilgili tüm eylemleri engeller.

   Eğitim sırasında bir kural tetiklendiyse Kaspersky Endpoint Security, etkinlikleri kural tetikleme raporunda ve **Akıllı Eğitim durumundaki kural tetikleyicileri** veri havuzunda günlüğe kaydeder.

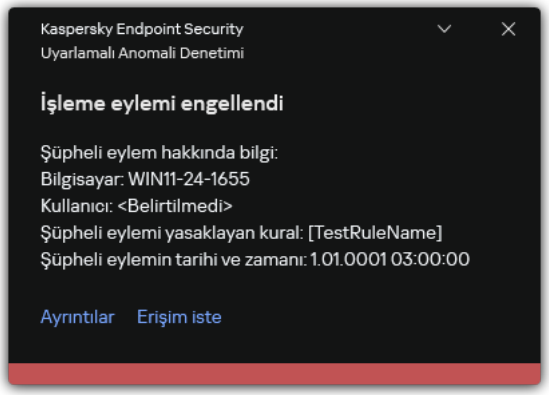
2. Kural tetikleme raporunu analiz etme.

   Yönetici, kural tetikleme raporunu veya **Akıllı Eğitim durumundaki kural tetikleyicileri** veri havuzunun içeriğini analiz eder. Ardından yönetici, kural tetiklendiğinde Uyarlamalı Anomali Denetiminin davranışını seçebilir: engelleme veya izin verme. Yönetici ayrıca kuralın nasıl çalıştığını izlemeye devam edebilir ve eğitim modunun süresini uzatabilir. Yönetici hiçbir eylemde bulunmazsa uygulama da eğitim modunda çalışmaya devam eder. Eğitim modu süresi yeniden başlatılır.

Uyarlamalı Anomali Denetimi aşağıdaki kanallar aracılığıyla gerçek zamanlı olarak yapılandırılır:

- Uyarlamalı Anomali Denetimi, eğitim modunda hiç tetiklenmeyen kurallarla ilgili eylemleri otomatik olarak engellemeye başlar.
- Kaspersky Endpoint Security yeni kurallar ekler veya kullanılmayan kuralları kaldırır.
- Yönetici, kural tetikleme raporunu ve **Akıllı Eğitim durumundaki kural tetikleyicileri** veri havuzunun içeriğini gözden geçirdikten sonra Uyarlamalı Anomali Denetiminin çalışmasını yapılandırır. Kuralların tetiklenmesiyle ilgili raporu ve **Akıllı Eğitim durumundaki kural tetikleyicileri** deposunun içeriğini kontrol etmenizi öneririz.

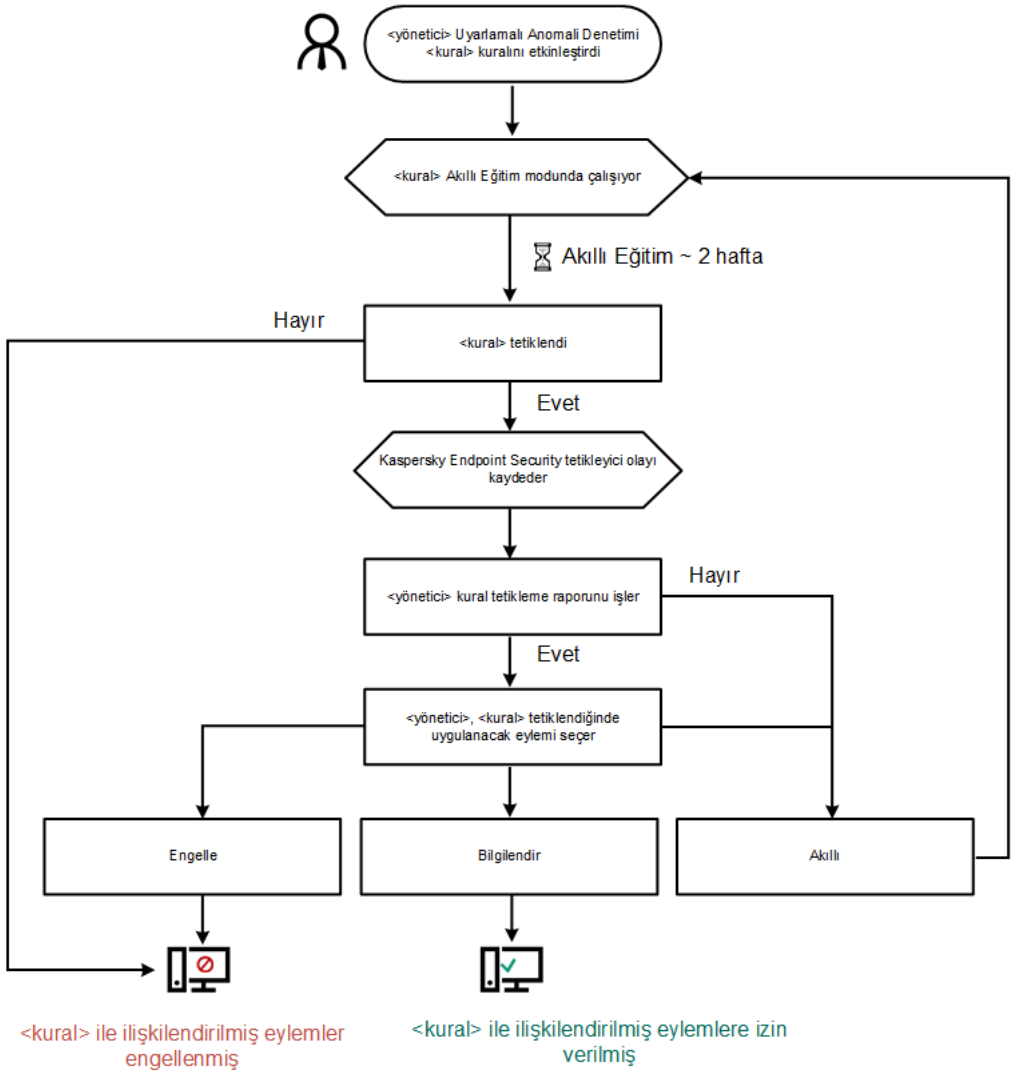
Zararlı bir uygulama eylemde bulunmaya çalıştığında Kaspersky Endpoint Security, eylemi engeller ve bir bildirim gösterir (aşağıdaki resme bakın).



Uyarlamalı Anomali Denetimi bildirimi

Uyarlamalı Anomali Denetimi çalışma algoritması

Kaspersky Endpoint Security, bir kuralla ilgili eyleme izin verilip verilmeyeceğini aşağıdaki algoritmaya (aşağıdaki resme bakın) göre belirler.



Uyarlamalı Anomali Denetimi çalışma algoritması

Parametre	Açıklama
Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu rapor Uyarlamalı Anomali Denetimi algılama kurallarının durumu hakkında bilgiler içerir (örneğin, *Devre dışı* veya *Engelle*). Rapor, tüm yönetim grupları için oluşturulur.
Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu rapor, Uyarlamalı Anomali Denetimi kullanılarak tespit edilen tipik olmayan eylemler hakkında bilgi içerir. Rapor, tüm yönetim grupları için oluşturulur.
Kurallar	Uyarlamalı Anomali Denetimi kuralları tablosu. Kurallar, Kaspersky uzmanları tarafından zararlı etkinliğin tipik senaryolarına dayanarak oluşturulur.
Şablonlar	**Engelleme hakkında mesaj**. Tipik olmayan bir eylemi engelleyen bir Uyarlamalı Anomali Denetimi kuralı tetiklendiğinde kullanıcıya gösterilecek mesajın şablonu. **Yöneticiye mesaj**. Kullanıcı, engelleme işleminin bir hata olduğunu düşünüyorsa yerel kurumsal ağ yöneticisine gönderebileceği mesaj şablonu. Kullanıcı erişim sağlama talebinde bulunduktan sonra Kaspersky Endpoint Security, Kaspersky Security Center'a bir olay gönderir: **Yönetici için uygulama etkinliği engelleme mesajı**. Olay açıklaması, değiştirilen değişkenlerle birlikte yöneticiye bir mesaj içerir. Bu olayları Kaspersky Security Center konsolunda, önceden tanımlanmış olay seçimi **Kullanıcı isteklerini** kullanarak görüntüleyebilirsiniz. Kuruluşunuzda Kaspersky Security Center dağıtılmamışsa veya Yönetim Sunucusuna bağlantı yoksa, uygulama belirtilen e-posta adresine yöneticiye bir mesaj gönderir.

Sistem Bütünlüğü İzleme

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

Kaspersky Endpoint Security for Windows, 12.6 sürümünden itibaren Dosya Bütünlük İzleyicisi bileşeni yerine Sistem Bütünlüğü İzleme bileşenini içerir. Sistem Bütünlüğü İzleme bileşeni, Dosya Bütünlük İzleyicisinin tüm işlevlerini içerir ve ayrıca kayıt defteri değişikliklerini ve harici cihazların bağlantısını izlemeye izin verir.

Sistem Bütünlüğü İzleme bileşeni, işletim sisteminde bilgisayar güvenliği ihlallerine işaret edebilecek değişiklikleri izler. Bu tür değişiklikler tespit edildiğinde, Kaspersky Endpoint Security ilgili olayları oluşturur ve yöneticiyi uyarır. Sistem Bütünlüğü İzleme gerçek zamanlı modda çalışabilir ve ayrıca talep üzerine sistem bütünlüğü kontrolleri gerçekleştirebilir.

Gerçek Zamanlı Sistem Bütünlüğü İzleme

Gerçek zamanlı modda, Sistem Bütünlüğü İzleme, bileşenin kapsamına (*izleme kapsamı*) dahil ettiğiniz nesnelerdeki değişiklikleri izler. Sistem Bütünlüğü İzleme, bu tür nesnelere yetkisiz erişimin gerçek zamanlı olarak engellenmesine de olanak tanır.

İsteğe Bağlı Sistem Bütünlük Denetimi

İsteğe Bağlı Sistem Bütünlük Denetimi, manuel olarak veya bir zamanlamaya göre çalıştırabileceğiniz bir görevdir. *Sistem Bütünlük Denetimi* görevini çalıştırmak için bileşenin kapsamını (*izleme kapsamı*) yapılandırmanız ve bir temel oluşturmanız gerekir. *Temel*, uygulamanın mevcut durumla karşılaştırırken referans olarak kullandığı, sistemdeki nesnelerin kaydedilmiş bir durumudur.

Sistem Bütünlüğü İzleme ayarları

Parametre	Açıklama
Engelleme kuralları için çalışma modu	• **Engelle**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarlarıyla yapılan eylemleri engeller ve ilgili bir olay oluşturur. • **Bilgilendir**. Bu modda, Sistem Bütünlüğü İzleme, izleme kapsamındaki dosyalar ve kayıt defteri anahtarları ile eylemlere izin verir ve ilgili bir olay oluşturur.
Gerçek Zamanlı Sistem Bütünlüğü İzleme	Gerçek zamanlı modda, Sistem Bütünlüğü İzleme, bileşenin kapsamına (*izleme kapsamı*) dahil ettiğiniz nesnelerdeki değişiklikleri izler. Sistem Bütünlüğü İzleme, bu tür nesnelere yetkisiz erişimin gerçek zamanlı olarak engellenmesine de olanak tanır.
Cihazları izle	Sistem Bütünlüğü İzleme, harici cihazların bağlantısını ve bağlantısının kesilmesini izler.
Dosyaları ve kayıt defterini izle	Sistem Bütünlüğü İzleme dosyalar, klasörler ve kayıt defterindeki değişiklikleri izler.
Sistem Bütünlük Denetimi	İsteğe Bağlı Sistem Bütünlük Denetimi, manuel olarak veya bir zamanlamaya göre çalıştırabileceğiniz bir görevdir. *Sistem Bütünlük Denetimi* görevini çalıştırmak için bileşenin kapsamını (*izleme kapsamı*) yapılandırmanız ve bir temel oluşturmanız gerekir. *Temel*, uygulamanın mevcut durumla karşılaştırırken referans olarak kullandığı, sistemdeki nesnelerin kaydedilmiş bir durumudur.

Endpoint Sensor

Endpoint Sensor, Kaspersky Endpoint Security 11.4.0 sürümünde mevcut değildir.

Kaspersky Security Center Web Console ve Kaspersky Security Center Yönetim Konsolu üzerinden Endpoint Sensor'u yönetebilirsiniz. Kaspersky Security Center Cloud Console üzerinden Endpoint Sensor'u yönetmek mümkün değildir.

Endpoint Sensor, Kaspersky Anti Targeted Attack Platform ile etkileşim için tasarlanmıştır. *Kaspersky Anti Targeted Attack Platform* hedeflenen saldırılar, gelişmiş sürekli tehditler (APT), sıfır gün saldırıları ve diğer karmaşık tehditleri zamanında tespit etmek üzere tasarlanmış bir çözümdür. Kaspersky Anti Targeted Attack Platform üç işlevsel birim içerir:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Tüm işlevsel birimleri veya tek tek işlevsel birimleri ayrı ayrı satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Endpoint Sensor yönetimi şu kısıtlamalara tabidir:

- Bilgisayarda Kaspersky Endpoint Security 11.0.0 ila 11.3.0 sürümler yüklü ise bir ilkede Endpoint Sensor ayarlarını yapılandırabilirsiniz. İlke kullanarak Endpoint Sensor ayarlarını yapılandırmak hakkında daha fazla bilgi almak için önceki Kaspersky Endpoint Security sürümlerinin yardım makalelerine bakın.
- Bilgisayarda Kaspersky Endpoint Security sürüm 11.4.0 ve üzeri yüklü ise, Endpoint Sensor ayarlarını ilkede yapılandıramazsınız.

Endpoint Sensor istemci bilgisayarlarda kurulur. Bu bilgisayarlarda bileşen işlemleri, etkin ağ bağlantılarını ve değiştirilen dosyaları sürekli olarak izler. Endpoint Sensor, bilgileri KATA sunucusuna iletir.

Bileşen işlevselliği aşağıdaki işletim sistemlerinde kullanılabilir:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-bit).

KATA işlemleri hakkında ayrıntılı bilgi için Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Sandbox

Kaspersky Endpoint Security for Windows artık Kaspersky Sandbox çözümüyle entegrasyon için yerleşik bir aracı içeriyor. *Sandbox* bileşeni bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Sandbox Yardım ve Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Kaspersky Endpoint Security for Windows, 12.7 sürümünden itibaren Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olan Sandbox bileşenini destekliyor. Kaspersky Sandbox çözümünün aksine, KATA Sandbox bileşeni dosyaları yalnızca otomatik olarak değil, aynı zamanda dosya bağlam menüsünden manuel olarak da tarayabilmektedir.

KATA Sandbox'ın dağıtılması için Kaspersky Anti Targeted Attack Platform 7.0 veya üstü gerekir.

Bileşen yalnızca Kaspersky Security Center Web Console kullanılarak yönetilebilir. Bu bileşeni Yönetim Konsolu'nu (MMC) kullanarak yönetemezsiniz.

Sandbox bileşen ayarları

Parametre	Açıklama
Entegrasyon modu	**Kaspersky Sandbox**. Kaspersky Sandbox çözümü ile entegrasyon. Uygulama, Kaspersky Sandbox'ta taranacak dosyaları yalnızca otomatik modda gönderir. **KATA Sandbox**. Kaspersky Anti Targeted Attack Platform çözümünün Sandbox bileşeniyle entegrasyon. Tarama için dosya gönderme modunu seçebilirsiniz: • **Manuel**. Kullanıcı, bağlam menüsünden dosyayı tarama için manuel olarak gönderir (**Sandbox'a Gönder**). • **Otomatik**. Uygulama nesneleri otomatik olarak algılar ve tarama için Sandbox'a gönderir. • **Birleştirilmiş**.
Sunucu bağlantı ayarları	**Zaman aşımı (ms)**. Sandbox sunucusu (Kaspersky Sandbox için) veya Central Node sunucusu (KATA için) için bağlantı zaman aşımı. Yapılandırılan zaman aşımı süresi geçtikten sonra Kaspersky Endpoint Security bir sonraki sunucuya bir istek gönderir. Bağlantı hızınız düşükse veya bağlantı dengesizse sunucu için bağlantı zaman aşımını artırabilirsiniz. Önerilen istek zaman aşımı 0,5 saniye veya daha kısadır. **İstek kuyruğu**. İstek kuyruğu klasörünün boyutu. Sandbox'ta tarama için birden fazla nesne gönderirken Kaspersky Endpoint Security bir istek kuyruğu oluşturur. İstek kuyruğu klasörünün boyutu varsayılan olarak 100 MB ile sınırlandırılmıştır. Maksimum boyuta ulaşıldıktan sonra, Sandbox kuyruğa yeni isteklerin eklenmesini durdurur ve ilgili olayı Kaspersky Security Center'a gönderir. İstek kuyruğu klasörünün boyutunu sunucu yapılandırmanıza göre yapılandırabilirsiniz. **Sunucu TLS sertifikası**. Sandbox sunucusu (Kaspersky Sandbox için) veya Central Node sunucusu (KATA için) ile güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Daha sonra bir ilke kullanarak sertifikayı bilgisayara eklemeniz gerekir. Ayrıca sertifikayı Sandbox sunucusuna (Kaspersky Sandbox için) veya Central Node sunucusuna (KATA için) eklemeniz gerekir. **İki yönlü kimlik doğrulama kullan** (yalnızca KATA Sandbox için). Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir.
Sandbox sunucularına bağlantı	**Kaspersky Sandbox**. Sandbox sunucusu bağlantı ayarları. Sunucular, taranması gereken nesneleri çalıştırmak için Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini kullanır. Bir IP adresi (IPv4 veya IPv6) veya bir tam etki alanı adı girebilirsiniz. **KATA Sandbox**. Central Node sunucusu bağlantı ayarları. Central Node tarama için en uygun ayarları seçer ve Sandbox sunucuları arasında yükü dengeler.
Tehdit algılandığında yapılacak eylem	**Kopyayı Karantinaya taşı, nesneyi sil**. Bu seçenek tercihe dildiğinde, Kaspersky Endpoint Security bilgisayardaki kötü amaçlı nesneyi siler. Kaspersky Endpoint Security, nesneyi silmeden önce nesnenin daha sonra geri yüklenmesi gerekebileceği ihtimaline karşı bir yedek kopya oluşturur. Kaspersky Endpoint Security, yedek kopyayı Karantinaya taşır. **Kritik Alanları Taramayı çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Critical Areas Scan* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar. **IOC Taraması görevi oluştur**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security otomatik olarak *IOC Taraması* görevi *(otonom IOC tarama görevi) oluşturur*. Bu görev için çalışma modunu, tarama kapsamını ve IOC algılandığında gerçekleştirilecek eylemi yapılandırabilirsiniz (*Kopyasını Karantinaya taşı, nesneyi sil* veya *Kritik Alanları Taramayı Çalıştır*). *IOC Taraması* görevinin diğer ayarları değiştirmek için görev ayarlarına gidin.
IOC Taraması kapsamı	**Kritik dosya alanları**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security yalnızca bilgisayarın kritik dosya alanlarında bir IOC taraması gerçekleştirir: çekirdek belleği ve önyükleme kesimleri. **Bilgisayarın sistem sürücüsündeki dosya alanları**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security bilgisayarın sistem sürücüsünde bir IOC taraması gerçekleştirir.

Parametre	Açıklama
IOC Taraması görevini çalıştır	**Manuel**. *IOC Taraması* görevini sizin için uygun olan bir zamanda manuel olarak başlatabileceğiniz çalıştırma modu. **Otomatik**. Kaspersky Endpoint Security'nin *IOC Taraması* görevini bir tehdit algılandıktan sonra otomatik olarak çalıştırdığı çalışma modudur. **Sadece bilgisayar boştayken çalıştır**. Kaspersky Endpoint Security'nin *IOC Taraması* görevini ekran koruyucu etkin ya da ekran kilitli olduğunda çalıştırdığı çalıştırma modudur. Kullanıcı bilgisayarın kilidini açarsa Kaspersky Endpoint Security görevi duraklatır. Bu, görevin tamamlanmasının birkaç gün sürebileceği anlamına gelir.

Managed Detection and Response

Kaspersky Endpoint Security for Windows, Managed Detection and Response çözümü ile entegrasyonu destekler. *Kaspersky Managed Detection and Response (MDR)* çözümü, altyapınızdaki güvenlik olaylarını otomatik olarak algılar ve analiz eder. MDR bunu yapmak için uç noktalardan alınan telemetri verilerini ve makine öğrenimini kullanır. MDR, olay verilerini Kaspersky uzmanlarına gönderir. Uzmanlar daha sonra olayı işleyebilir ve mesela antivirüs veritabanlarına yeni bir giriş ekleyebilir. Alternatif olarak, uzmanlar olayın işlenmesiyle ilgili önerilerde bulunabilir ve mesela bilgisayarın ağdan izole edilmesini önerebilir. Çözümün nasıl çalıştığı hakkında ayrıntılı bilgi için lütfen Kaspersky Managed Detection and Response Yardım içeriğine bakın.

Managed Detection and Response ayarları

Parametre	Açıklama
MDR yapılandırma dosyası	BLOB dosyası, istemci kimliğini ve Kaspersky Managed Detection and Response lisansı hakkındaki bilgileri içerir. BLOB dosyası, MDR yapılandırma dosyasının ZIP arşivinde bulunur. ZIP arşivini Kaspersky Managed Detection and Response Konsolunda bulabilirsiniz. Bir BLOB dosyası hakkında ayrıntılı bilgi için lütfen Kaspersky Yönetilen Algılama ve Yanıt Yardım içeriğine bakın.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows, artık Kaspersky Endpoint Detection and Response Optimum çözümü için yerleşik bir aracıya sahip (bundan böyle "EDR Optimum" olarak anılacaktır). 11.8.0 sürümünden itibaren, Kaspersky Endpoint Security for Windows artık Kaspersky Endpoint Detection and Response Expert çözümü (bundan böyle "EDR Expert" olarak anılacaktır) için yerleşik bir aracıya sahip. *Kaspersky Endpoint Detection and Response*, kurumsal BT altyapısını gelişmiş siber tehditlere karşı korumaya yönelik bir çözüm yelpazesidir. Çözümlerin işlevselliği, yeni açıklar, fidye yazılımı, dosyasız saldırılar ve yasal sistem araçlarını kullanan yöntemler dahil olmak üzere gelişmiş saldırılara karşı koymak için tehditlerin otomatik olarak algılanması ile bu tehditlere yanıt verme yeteneğini birleştirir. EDR Expert, EDR Optimum'a göre daha fazla tehdit izleme ve tehdit yanıtı işlevselliği sunar. Çözümlerin ayrıntıları için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

Kaspersky Endpoint Detection and Response, tehdit gelişimini inceleyip analiz eder ve *güvenlik personeli* ya da *Yönetici* tarafından zamanında yanıt verilebilmesini sağlamak için potansiyel saldırı hakkındaki gerekli bilgileri sağlar. Kaspersky Endpoint Detection and Response uyarı ayrıntılarını ayrı bir pencerede görüntüler. *Uyarı*, kurumsal BT altyapısında uygulamanın olağandışı veya şüpheli olarak tanımladığı ve kurumsal BT altyapısı için bir güvenlik tehdidi oluşturabilecek bir olaydır. *Uyarı Ayrıntıları*, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Uyarı ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Uyarı ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

Endpoint Detection and Response Optimum bileşenini Web Console ve Cloud Console'dan yapılandırabilirsiniz. Endpoint Detection and Response Expert (cloud) bileşeninin ayarlarına yalnızca Cloud Console üzerinden erişilebilir.

Parametre	Açıklama
Gelişmiş sistem etkinliği günlüğünü etkinleştir	Genişletilmiş telemetri, IOC tespitinin doğruluğunu artırır, ancak bilgisayarın daha fazla kaynağını kullanır. Geriye dönük IOC taraması için bilgisayarda genişletilmiş telemetriyi etkinleştirmenizi öneririz. *Geriye Dönük IOC Taraması*, Kaspersky Endpoint Security'nin belirli bir zaman dilimine ait verileri kullanarak ihlal göstergelerini taradığı *IOC Taraması* görevinin bir modudur. Bu mod, ağ etkinliği, işlemler, dosyalar ve diğer telemetri verileri gibi korunan bilgisayarın telemetri verilerini kullanarak güvenlik ihlali göstergelerini aramaya yöneliktir. Genişletilmiş telemetri devre dışı bırakılırsa Kaspersky Endpoint Security, algılanan ihlal göstergeleri hakkındaki bilgileri döndürebilir.
Ağ İzolasyonu	Tespit edilen tehditlere yanıt olarak bilgisayarın ağdan otomatik olarak izole edilmesidir. Ağ izolasyonu açıldığında, uygulama tüm etkin bağlantıları keser ve bilgisayardaki tüm yeni TCP/IP bağlantılarını engeller. Uygulama yalnızca aşağıdaki bağlantıları etkin bırakır: • Ağ izolasyonu istisnalarında listelenen bağlantılar. • Kaspersky Endpoint Security hizmetleri tarafından başlatılan bağlantılar. • Kaspersky Security Center Ağ Aracısı tarafından başlatılan bağlantılar.
İzole edilmiş cihazın kilidini otomatik olarak aç (saat)	Ağ izolasyonu belirli bir süre sonra otomatik olarak veya manuel olarak kapatılabilir. Varsayılan olarak Kaspersky Endpoint Security Ağ izolasyonunu, izolasyonun başlamasından 5 saat sonra kapatır.
Ağ izolasyonu istisnaları	Ağ izolasyonundan istisna kurallarının listesi. Ağ izolasyonu açıkken bilgisayarlarda kurallarla eşleşen ağ bağlantıları engellenmez. Ağ izolasyonu istisnalarını yapılandırmak için bir *standart ağ profilleri* listesi kullanabilirsiniz. Varsayılan olarak, istisnalar, DNS/DHCP sunucusu ve DNS/DHCP istemci rollerine sahip cihazların kesintisiz çalışmasını sağlayan kuralları barındıran ağ profillerini içerir. İsterseniz standart ağ profillerinin ayarlarını değiştirebilir ya da istisnaları manuel olarak tanımlayabilirsiniz. İlke özelliklerinde belirtilen istisnalar, yalnızca algılanan bir tehdide yanıt olarak Ağ izolasyonu otomatik olarak açılırsa uygulanır. Bilgisayar özelliklerinde belirtilen istisnalar, yalnızca Kaspersky Security Center konsolundaki bilgisayar özelliklerinde veya uyarı ayrıntılarında Ağ izolasyonu manuel olarak açılırsa uygulanır.
Yürütme Önleme	Yürütülebilir dosyaların ve komut dosyalarının yürütülmesini ve ofis dosyalarının açılmasını kontrol edin. Örneğin, seçilen bilgisayarda güvenli olmadığı düşünülen uygulamaların yürütülmesini engelleyebilirsiniz. Yürütme önleme bir ofis dosyası uzantıları grubunu ve bir komut dizisi yorumlayıcısı grubunu destekler. Yürütme önleme bileşenini kullanmak için yürütme önleme kuralları eklemeniz gerekir. *Yürütme önleme kuralı* bir nesne yürütmesine tepki verirken, örneğin nesne yürütmesini engellerken, uygulamanın dikkate aldığı bir dizi kriterdir. Uygulama, dosyaları yollarına veya MD5 ve SHA256 karma algoritmaları kullanılarak hesaplanan sağlama toplamlarına göre tanımlar.
Yasak nesnenin yürütülmesi veya açılması ile ilgili eylem	**Engelle ve olay günlüğüne ekle**. Bu modda, uygulama, engelleme kuralı kriterlerine uyan nesnelerin yürütülmesini veya belgelerin açılmasını engeller. Uygulama ayrıca Windows olay günlüğüne ve Kaspersky Security Center olay günlüğüne nesneleri çalıştırma veya belgeleri açma girişimleri hakkında bir olay yayınlar. **Olay günlüğüne ekle**. Bu modda Kaspersky Endpoint Security, Windows olay günlüğü ve Kaspersky Security Center ile önleme kuralı kriterleriyle eşleşen yürütülebilir nesneleri veya açık belgeleri yürütme girişimleri hakkında bir olay yayınlar, ancak nesneyi veya belgeyi yürütme veya açma girişimini engellemez. Varsayılan olarak bu mod seçilidir.
Yürütme önleme kuralları	*Yürütme önleme kuralı* bir nesne yürütmesine tepki verirken, örneğin nesne yürütmesini engellerken, uygulamanın dikkate aldığı bir dizi kriterdir. Uygulama, dosyaları yollarına veya MD5 ve SHA256 karma algoritmaları kullanılarak hesaplanan sağlama toplamlarına göre tanımlar.
Cloud Sandbox	*Cloud Sandbox* bir bilgisayardaki gelişmiş tehditleri tespit etmenizi sağlayan bir teknolojidir. Kaspersky Endpoint Security, tespit edilen dosyaları analiz edilmek üzere otomatik olarak Cloud Sandbox'a iletir. Cloud Sandbox, kötü amaçlı etkinlikleri belirlemek için bu dosyaları yalıtılmış bir ortamda çalıştırır ve tanınırlıklarına göre karar verir. Bu dosyalardaki veriler daha sonra Kaspersky Security Network'e gönderilir. Bu nedenle, Cloud Sandbox kötü amaçlı bir dosya algıladığında, Kaspersky Endpoint Security bu dosyanın algılandığı tüm bilgisayarlarda bu tehdidi ortadan kaldırmak üzere uygun eylemi gerçekleştirir. Cloud Sandbox teknolojisi kalıcı olarak etkinleştirilir ve kullandıkları lisans türünden bağımsız olarak tüm Kaspersky Security Network kullanıcıları tarafından kullanılabilir. Bu onay kutusu seçildiğinde, Kaspersky Endpoint Security, Cloud Sandbox'u kullanılarak, ana uygulama penceresinde **Tehdit tespit etme teknolojileri** altında algılanan tehditler için sayacı etkinleştirir. Kaspersky Endpoint Security, uygulama olaylarında ve Kaspersky Security Center konsolundaki *Tehdit raporunda* Cloud Sandbox tespit etme teknolojisini de gösterecek.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Detection and Response Expert (on-premises) çözümüyle entegrasyonu destekler. *Kaspersky Endpoint Detection and Response Expert (on-premises)*, bir kuruluşun çoğu siber risk türüne karşı savunma yapmasını ve en önemli tehdit yayılma senaryolarını kapsamasını sağlayan Kaspersky uygulamalarını içeren kurumsal bir siber güvenlik çözümüdür. EDR Expert (on-premises) bileşenleri, Açık Tek Yönetim Platformu (OSMP) üzerinde dağıtılır. Bu platform, platformlar arası senaryoları tek bir arabirimde çalıştırır ve Kaspersky uygulamalarının üçüncü taraf uygulamalarla entegre edilerek kapsamlı bir güvenlik sistemine dönüştürülmesini sağlar.

Çözümün merkezi unsurlarından biri *SIEM*dir. SIEM, tüm bileşenlerden gelen olayları izler ve satıcı ve kullanıcı tanımlı kuralları kullanarak bu olayları birbiriyle ilişkilendirir. EDR Expert (on-premises), saldırıları otomatik olarak tespit etmek için kurumsal altyapıdan alınan günlükleri ve telemetriyi inceler ve Kaspersky uygulamalarından ve üçüncü taraf bilgi güvenliği ürünlerinden gelen olaylar dahil olmak üzere EDR Expert (on-premises) içinde toplanan tüm olayları birleştiren birleşik bir araştırma grafiği kullanarak olayların araştırılmasını sağlar.

Gelişmiş olaylara müdahale etmek için EDR Expert (on-premises), önceden ayarlanmış ve kullanıcı tanımlı senaryolar kullanır. Üçüncü taraf uygulamalardan gelen yanıt eylemlerini ve birden fazla uygulamayı içeren yanıt senaryolarını da kullanabilirsiniz.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows, Kaspersky Anti Targeted Attack Platform (EDR (KATA)) çözümünün bir parçası olarak Kaspersky Endpoint Detection and Response bileşeni ile çalışmayı destekliyor. *Kaspersky Anti Targeted Attack Platform* hedeflenen saldırılar, gelişmiş sürekli tehditler (APT), sıfır gün saldırıları ve diğer karmaşık tehditleri zamanında tespit etmek üzere tasarlanmış bir çözümdür. Kaspersky Anti Targeted Attack Platform üç işlevsel birim içerir:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Tüm işlevsel birimleri veya tek tek işlevsel birimleri ayrı ayrı satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Kaspersky Endpoint Security, kurumsal BT altyapısındaki bilgisayarlara yüklenir ve süreçleri, açık ağ bağlantılarını ve değiştirilmekte olan dosyaları sürekli olarak izler. Bilgisayardaki olaylarla ilgili bilgiler (telemetri verileri) Kaspersky Anti Targeted Attack Platform sunucusuna gönderilir. Bu durumda, Kaspersky Endpoint Security ayrıca uygulama tarafından keşfedilen tehditler ve bu tehditlerin işlenmesinden elde edilen sonuçlar hakkında Kaspersky Anti Targeted Attack Platform sunucusuna bilgiler gönderir.

EDR (KATA) ve NDR (KATA) entegrasyonu Kaspersky Security Center konsolunda yapılandırılır. Yerleşik aracı daha sonra Kaspersky Anti Targeted Attack Platform konsolu kullanılarak yönetilir; buna görevleri çalıştırma, karantinaya alınan nesneleri yönetme, raporları görüntüleme ve diğer eylemler dahildir.

Parametre	Açıklama
Telemetri toplama sunucularına bağlantı	Bir *telemetri toplama sunucusu*, SIEM çözümünün bir parçası olan ve bilgisayarda meydana gelen olaylarla ilgili bilgileri toplayan, normalleştiren, ilişkilendiren, analiz eden ve depolayan bir sunucudur. Telemetri toplama sunucularına (KUMA) bağlanmak için aşağıdakileri yapılandırın: • **Zaman aşımı (sn)**. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır. • **Sunucu sertifikası**. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). • **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ile sunucu arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için sunucu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto kabı almanız ve kripto kabını korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Sunucu ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto kapsayıcı yüklemeniz gerekir. Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
Adres ve **Port** (telemetri toplama sunucuları)	Telemetri toplama sunucularına bağlanmak için ayarlar. Bir IP adresi (IPv4 veya IPv6) girebilirsiniz. Birden fazla telemetri toplama sunucusu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
Telemetri toplama sunucularına telemetri gönderme	Bu işlev KATA sunucusuna telemetri gönderimini tamamen kapatmanızı sağlar. Örneğin Kaspersky Anti Targeted Attack Platform'u telemetri de kullanan başka bir çözümle birlikte kullanıyorsanız, KATA (EDR) için telemetri gönderimini kapatabilirsiniz. Bu, bu çözümler için sunucu yükünü optimize etmenizi sağlar. Managed Detection and Response çözümüne ve KATA'ya (EDR) sahipseniz, MDR telemetrisini kullanabilir ve KATA'da (EDR) Tehdit Müdahalesi görevleri oluşturabilirsiniz. • **Telemetriyi yalnızca IOA ile gönder**. Bu, telemetriyi optimize etmeyi ve yalnızca IOA ile telemetri göndermeyi sağlar. *Saldırı Göstergesi (IOA)*, hedefli bir saldırıyı işaret edebilecek sistemdeki şüpheli davranışların açıklamasını içeren bir kuraldır. Uygulama, sistemdeki devam eden davranışları bu kurallarla karşılaştırır ve hedefli bir saldırıyı gösteren olayları günlüğe kaydeder. Uygulama, bu tür olayların gerçek zamanlı olarak izlenmesini sağlayan *akış tarama* teknolojisini kullanır. • **Maksimum olay iletim gecikmesi (sn)**. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir. • **İletim başına olay paketi sayısını sınırlayın**. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır. Bu fonksiyon, sunucu ile senkronizasyondan önce olayların tamponlanmasını devre dışı bırakmayı sağlar.
Talep daraltmayı etkinleştir	Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur. Telemetri ayarlarını yapılandırın: • **Saat başına maksimum olay sayısı**. Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir. • **Olay sınırı aşım yüzdesi**. Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.
Sunucuya her (dakika) senkronizasyon isteği gönder	Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.

Parametre	Açıklama
Yanıt sunucularına bağlantı	Bir *yanıt sunucusu*, verileri almak ve taramak, nesnelerin davranışlarını incelemek ve bu tür çalışmaların sonuçlarını yayınlamak için kullanılan bir sunucudur. Yanıt sunucularının bağlantısı için şu yapılandırmaları yapın: • **Zaman aşımı (sn)**. Maksimum sunucu yanıt zaman aşımı. Zaman aşımı dolduğunda, Kaspersky Endpoint Security farklı bir sunucuya bağlanmaya çalışır. • **Sunucu sertifikası**. Sunucuya güvenilir bir bağlantı kurmak için TLS sertifikası. Açık Tek Yönetim Platformu'nda bir TLS sertifikası alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). • **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ile sunucu arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için sunucu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto kabı almanız ve kripto kabını korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Açık Tek Yönetim Platformu'nda bir kripto konteyneri alabilirsiniz (Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım içeriğindeki talimatlara bakın). Sunucu ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto kapsayıcı yüklemeniz gerekir.
Adres ve **Port** (yanıt sunucuları)	Yanıt sunucularına bağlanmak için ayarlar. Bir IP adresi (IPv4 veya IPv6) girebilirsiniz. Birden fazla telemetri toplama sunucusu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

Endpoint Detection and Response (KATA) ayarları

Parametre	Açıklama
Sunucuya her (dakika) senkronizasyon isteği gönder	Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.
KATA sunucularına bağlantı	Merkezi Düğüm sunucu bağlantısı için aşağıdakileri yapılandırın: • **Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener. • **Sunucu sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). • **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir. Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
Adres ve **Port** (KATA sunucuları)	Kaspersky Anti Targeted Attack Platform sunucularına bağlanma ayarları. Bağlanılacak Merkezi Düğüm sunucusunun IP adresini (IPv4 veya IPv6) ve portunu girin. Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
KATA'ya telemetri gönder	Bu işlev KATA sunucusuna telemetri gönderimini tamamen kapatmanızı sağlar. Örneğin Kaspersky Anti Targeted Attack Platform'u telemetri de kullanan başka bir çözümle birlikte kullanıyorsanız, KATA (EDR) için telemetri gönderimini kapatabilirsiniz. Bu, bu çözümler için sunucu yükünü optimize etmenizi sağlar. Managed Detection and Response çözümüne ve KATA'ya (EDR) sahipseniz, MDR telemetrisini kullanabilir ve KATA'da (EDR) Tehdit Müdahalesi görevleri oluşturabilirsiniz. Telemetri ayarlarını yapılandırın: • **Maksimum olay iletim gecikmesi (sn)**. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir. • **Paket başına maksimum olay sayısı**. Tampon olaylarla dolduğunda uygulama sunucu ile senkronize olur. Varsayılan ayar 1024 olaydır.

Parametre	Açıklama
Talep daraltmayı etkinleştir	Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur. Telemetri ayarlarını yapılandırın: • **Saat başına maksimum olay sayısı**. Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir. • **Olay sınırı aşım yüzdesi**. Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows, Kaspersky Anti Targeted Attack Platform (EDR (KATA)) çözümünün bir parçası olarak Kaspersky Network Detection and Response bileşeniyle çalışmayı destekler. *Kaspersky Anti Targeted Attack Platform* hedeflenen saldırılar, gelişmiş sürekli tehditler (APT), sıfır gün saldırıları ve diğer karmaşık tehditleri zamanında tespit etmek üzere tasarlanmış bir çözümdür. Kaspersky Anti Targeted Attack Platform üç işlevsel birim içerir:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Tüm işlevsel birimleri veya tek tek işlevsel birimleri ayrı ayrı satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Kaspersky Endpoint Security, kurumsal BT altyapısındaki bilgisayarlara yüklenir ve süreçleri, açık ağ bağlantılarını ve değiştirilmekte olan dosyaları sürekli olarak izler. Bilgisayardaki olaylarla ilgili bilgiler (telemetri verileri) Kaspersky Anti Targeted Attack Platform sunucusuna gönderilir. Bu durumda, Kaspersky Endpoint Security ayrıca uygulama tarafından keşfedilen tehditler ve bu tehditlerin işlenmesinden elde edilen sonuçlar hakkında Kaspersky Anti Targeted Attack Platform sunucusuna bilgiler gönderir.

EDR (KATA) ve NDR (KATA) entegrasyonu Kaspersky Security Center konsolunda yapılandırılır. Yerleşik aracı daha sonra Kaspersky Anti Targeted Attack Platform konsolu kullanılarak yönetilir; buna görevleri çalıştırma, karantinaya alınan nesneleri yönetme, raporları görüntüleme ve diğer eylemler dahildir.

Network Detection and Response (KATA) parametreleri

Parametre	Açıklama
Sunucu bağlantı ayarları	**Zaman aşımı (sn)**. Maksimum Central Node sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Central Node sunucusuna bağlanmayı dener. **Sunucu TLS sertifikası**. Central Node sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Anti Targeted Attack Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). **İki yönlü kimlik doğrulama kullan**. Kaspersky Endpoint Security ve Central Node sunucusu arasında güvenli bir bağlantı kurarken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulamayı kullanmak için Central Node sunucusu ayarlarında iki yönlü kimlik doğrulamayı etkinleştirmeniz, ardından bir kripto konteyneri almanız ve kripto konteynerini korumak için bir parola belirlemeniz gerekir. Bir *kripto konteyner*, sertifika ve özel anahtar içeren bir PFX arşividir. Kaspersky Anti Targeted Attack Platform konsolundan bir kripto konteyner alabilirsiniz (Kaspersky Anti Targeted Attack Platform Yardım 'daki talimatlara bakın). Central Node ayarlarını yapılandırdıktan sonra, Kaspersky Endpoint Security ayarlarında iki yönlü kimlik doğrulamayı da etkinleştirmeniz ve parola korumalı bir kripto konteyneri yüklemeniz gerekir. Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.

Parametre	Açıklama
Adres ve **Port**	Kaspersky Anti Targeted Attack Platform sunucularına bağlanma ayarları. Bağlanılacak Merkezi Düğüm sunucusunun IP adresini (IPv4 veya IPv6) ve portunu girin. Birden fazla Central Node sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.
NDR sunucusuna her (dakika) senkronizasyon isteği gönder	Sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.
Maksimum olay iletim gecikmesi (sn)	Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
Talep daraltmayı etkinleştir	Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Bu işlev etkinleştirilirse uygulama olay iletimini kısıtlar. Olay sayısı yapılandırılan sınırları aşarsa Kaspersky Endpoint Security olay gönderimini durdurur.
Saat başına maksimum olay sayısı	Uygulama telemetri veri akışını analiz eder ve olay akışı yapılandırılmış olay/saat sınırını aşarsa olayların gönderilmesini kısıtlar. Kaspersky Endpoint Security bir saat sonra olayları göndermeye devam eder. Varsayılan ayar saatte 3000 olaydır. Uygulama bir sunucuya kurulursa, telemetri veri akışı daha yüksek olur. Sunucular için bu değerin saatte 60.000 olaya çıkarılması önerilir.
Olay sınırı aşım yüzdesi	Uygulama, olayları türlerine göre sıralar (örneğin, "kayıt defterindeki değişiklikler" olayları) ve aynı türdeki olayların toplam olay sayısına oranı yüzde olarak yapılandırılan sınırı aşarsa olayların iletimini sınırlar. Kaspersky Endpoint Security, diğer olayların toplam olay sayısına oranı tekrar yeterince büyük olduğunda olayları göndermeye devam eder. Varsayılan ayar %15'tir.

KUMA Entegrasyonu

Kaspersky Endpoint Security for Windows, Kaspersky Unified Monitoring and Analysis Platform çözümünü destekler. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)*, kurumların BT altyapısı için bir güvenlik bilgi ve olay yönetimi (SIEM) çözümüdür. KUMA, güvenlik tehditlerinin zarar vermeden önce tespit edilmesini, analiz edilmesini ve etkilerinin azaltılmasını sağlar.

KUMA entegrasyon ayarları

Parametre	Açıklama
Olayları gönderirken maksimum gecikme (saniye)	Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
KUMA sunucularına bağlantı	**Zaman aşımı (sn)**. KUMA sunucusundan yanıt beklemek için maksimum süre (varsayılan değer 5 saniyedir). Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir KUMA sunucusuna bağlanmayı dener. **Sunucu sertifikası**. KUMA sunucusu ile güvenilir bir bağlantı kurmak için TLS sertifikası. Kaspersky Unified Monitoring and Analysis Platform konsolundan bir TLS sertifikası alabilirsiniz (Kaspersky Unified Monitoring and Analysis Platform Yardım bölümündeki talimatlara bakın). KUMA konsolunda bir güvenilir bağlantı kurmak için tcp ayarlarında **With verification** TLS modu seçimini yapmalısınız (Kaspersky Unified Monitoring and Analysis Platform Yardımında tcp tipi bağlayıcı ayarlarına bakın). **İki yönlü kimlik doğrulama kullan**. KES ile KUMA arasında güvenli bir bağlantı kurulurken iki yönlü kimlik doğrulama. İki yönlü kimlik doğrulama kullanmak için KUMA konsolundaki bağlayıcı ayarlarında **İstemci kimlik doğrulamalı özel PFX** TLS modunu seçmelisiniz (Kaspersky Unified Monitoring and Analysis Platform Yardım bölümündeki bağlayıcı ayarlarına bakın). Ardından bir sunucu sertifikası indirmeli ve kripto konteyneri korumak için bir parola belirlemelisiniz. Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
KUMA sunucuları	Kaspersky Unified Monitoring and Analysis Platform sunucularına bağlantı ayarları. Bir IP adresi (IPv4 veya IPv6) girebilirsiniz. Birden fazla KUMA sunucu adresi ekleyebilirsiniz. Kaspersky Endpoint Security, ilk IP adresini kullanarak sunucuya bağlanmaya çalışır. Bağlantı kurulamazsa, Kaspersky Endpoint Security listedeki ikinci IP adresini kullanarak bağlanmayı dener ve bu şekilde devam eder.

Tam Disk Şifreleme

Bir şifreleme teknolojisi seçebilirsiniz: Kaspersky Disk Encryption veya BitLocker Drive Encryption (bundan sonra "BitLocker" olarak ifade edilecektir).

Kaspersky Disk Encryption

Kaspersky Disk Encryption, ARM tabanlı bilgisayarlarda desteklenmemektedir.

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 hesaplarını yönet* görevini 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. Authentication Agent hesabının kullanıcı adı ve parolasını kullanarak işletim sisteminde otomatik olarak oturum açmanızı sağlayan Single Sign-On (SSO) teknolojisini de kullanabilirsiniz.

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.

  Sadece 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.

BitLocker Drive Encryption.

BitLocker, Windows işletim sistemlerinde yerleşik olarak bulunan bir şifreleme teknolojisidir. Kaspersky Endpoint Security, Kaspersky Next altyapısını kullanarak Bitlocker'ı kontrol etmenizi ve yönetmenizi sağlar. BitLocker mantıksal birimleri şifreler. BitLocker, çıkarılabilir sürücülerin şifrelenmesi için kullanılamaz. BitLocker hakkında daha ayrıntılı bilgi için Microsoft belgelerine bakın.

BitLocker diski şifrelerken önyükleme yükleyicisini ve diğer yardımcı dosyaları system partition içeriğine yerleştirir. Bu bölüm şifrelenmemiştir. İşletim sistemi, Windows kurulumu sırasında sistem bölümünü otomatik olarak oluşturur. Windows'u yüklemeden önce disk tamamen bölümlenmişse, işletim sistemi bir sistem bölümü oluşturamaz. Bu durumda, BitLocker disk şifrelemesini başlattığınızda, işletim sistemi diski yeniden bölümlendirmenizi ve bir sistem bölümü oluşturmanızı ister. Bir sistem bölümü oluşturduktan sonra, işletim sistemi BitLocker şifrelemesini başlatır.

BitLocker, güvenilir bir platform modülü kullanarak erişim anahtarlarının güvenli bir şekilde saklanmasını sağlar. Bir *Trusted Platform Module (TPM)* güvenlikle ilgili temel işlevleri (örneğin şifreleme anahtarlarını saklamak için) sağlamak üzere geliştirilmiş bir mikroçiptir. Bir Güvenilir Platform Modülü genellikle bilgisayarın ana kartına yüklenmiştir ve donanım veri yolu aracılığıyla tüm diğer sistem bileşenleri ile etkileşim halindedir. TPM, başlatma öncesi sistem bütünlüğü doğrulaması sağladığından, BitLocker erişim anahtarlarını depolamanın en güvenli yolu TPM kullanmaktır. Bir bilgisayardaki sürücüleri TPM olmadan da şifreleyebilirsiniz. Bu durumda erişim anahtarı bir parola ile şifrelenecektir. BitLocker şu kimlik doğrulama yöntemlerini kullanır:

- TPM.
- TPM ve PIN.
- Parola.

Sistem sabit sürücüsünü şifreledikten sonra, işlem sistemini önyüklemek için kullanıcının BitLocker kimlik doğrulamasını gerçekleştirmesi gerekir. Kimlik doğrulamasından sonra BitLocker kullanıcının oturum açmasına izin verir. BitLocker çoklu oturum açma (SSO) desteği sunmaz.

Bir sürücüyü şifreledikten sonra, BitLocker bir kurtarma anahtarı oluşturur. Kaspersky Endpoint Security, kurtarma anahtarını Kaspersky Security Center'a gönderir, böylece mesela bir kullanıcı parolasını unuttuysa diske erişimi geri yükleyebilirsiniz.

Bir kullanıcı bir diski BitLocker ile şifrelediğinde, Kaspersky Endpoint Security kurtarma anahtarını ve disk şifrelemeyle ilgili bilgileri Kaspersky Security Center'a gönderir.

Windows grup ilkeleri kullanıyorsanız ilke ayarlarından BitLocker yönetimini kapatın. Windows ilke ayarları Kaspersky Endpoint Security'nin ilke ayarları ile çakışabilir. Bir sürücüyü şifrelerken hatalar meydana gelebilir.

Kaspersky Disk Encryption bileşeni ayarları

Parametre	Açıklama
Şifreleme modu	**Tüm sabit sürücüleri şifrele**. Bu seçenek seçilirse, ilke uygulandığında uygulama tüm sabit sürücüleri şifreler. Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca uygulamanın yüklü olduğu işletim sistemini yükleyebilirsiniz. **Tüm sabit sürücülerin şifresini çöz**. Bu seçenek seçilirse, ilke uygulandığında uygulama önceden şifrelenmiş tüm sabit sürücülerin şifresini çözer. **Değiştirmeden bırak**. Bu öğe seçilirse ilke uygulandığında uygulama sürücüleri önceki durumunda bırakır. Sürücü şifreliyse şifrelenmiş olarak kalır. Sürücü şifresi çözülmüşse şifresi çözülmüş olarak kalır. Bu öğe varsayılan olarak seçilmiştir.
Şifreleme sırasında, Windows kullanıcıları için otomatik olarak Kimlik Doğrulama Aracısı hesapları oluştur	Bu onay kutusu seçildiğinde, uygulama bilgisayardaki Windows kullanıcı hesapları listesine göre Kimlik Doğrulama Aracısı hesapları oluşturur. Kaspersky Endpoint Security varsayılan olarak, kullanıcının işletim sisteminde son 30 günde giriş yaptığı tüm yerel ve etki alanı hesaplarını kullanır.

Parametre	Açıklama
Kimlik Doğrulama Aracısı hesabı oluşturma ayarları	**Bilgisayardaki tüm hesaplar**. Bilgisayarda herhangi bir zamanda etkin olan tüm hesaplar. **Bilgisayardaki tüm etki alanı hesapları**. Bilgisayardaki bir etki alanına ait olan ve herhangi bir zamanda etkin olan tüm hesaplar. **Bilgisayardaki tüm yerel hesaplar**. Bilgisayarda herhangi bir zamanda etkin olan tüm yerel hesaplar. **Tek kullanımlık bir parolaya sahip hizmet hesabı**. Hizmet hesabı, örneğin kullanıcı parolasını unuttuğunda bilgisayara erişim sağlamak için gereklidir. Hizmet hesabını bir rezerve hesap olarak da kullanabilirsiniz. Hesabın adını girmelisiniz (varsayılan olarak, `ServiceAccount`). Kaspersky Endpoint Security otomatik olarak bir parola oluşturur. Parolayı Kaspersky Security Center konsolu üzerinde görüntüleyemezsiniz. **Yerel yönetici**. Kaspersky Endpoint Security, bilgisayarın yerel yöneticisi için bir Kimlik Doğrulama Aracısı kullanıcı hesabı oluşturur. **Bilgisayar yöneticisi**. Kaspersky Endpoint Security, bilgisayar yöneticisinin hesabı için bir Kimlik Doğrulama Aracısı kullanıcı hesabı oluşturur. Active Directory'deki bilgisayar özelliklerinde, hangi hesabın bilgisayar yöneticisi rolüne sahip olduğunu görebilirsiniz. Bilgisayar yöneticisi rolü varsayılan olarak tanımlanmamıştır, yani herhangi bir hesaba karşılık gelmez. **Etkin hesap**. Kaspersky Endpoint Security, disk şifrelemesi sırasında etkin olan hesap için otomatik olarak bir Kimlik Doğrulama Aracısı hesabı oluşturur.
Bu bilgisayardaki tüm kullanıcılar için giriş yapıldığında Kimlik Doğrulama Aracısı hesapları oluştur	Bu onay kutusu seçildiğinde, uygulama, Kimlik Doğrulama Aracısı'nı başlatmadan önce bilgisayardaki Windows kullanıcı hesapları hakkındaki bilgileri kontrol eder. Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı hesabı olmayan bir Windows kullanıcı hesabı tespit ettiğinde, uygulama şifrelenmiş sürücülere erişmek için yeni bir hesap oluşturacaktır. Yeni Kimlik Doğrulama Aracısı hesabı şu varsayılan ayarlara sahip olacaktır: yalnızca parola korumalı oturum açma ve ilk kimlik doğrulamada parola değişikliği. Bu nedenle, zaten şifrelenmiş sürücülere sahip bilgisayarlar için *Kimlik Doğrulama Aracısı hesaplarını yönet* görevini kullanarak Kimlik Doğrulama Aracısı hesaplarını manuel olarak eklemeniz gerekmez.
Kimlik Doğrulama Aracısı'na girilen kullanıcı adını kaydet	Onay kutusu işaretlenirse uygulama Kimlik Doğrulama Aracısı hesabının adını kaydeder. Aynı hesaptaki Kimlik Doğrulama Aracısı'nda yapacağınız bir sonraki yetkilendirme tamamlama girişiminde hesap adını girmeniz istenmeyecektir.
Sadece kullanılan disk alanını şifrele (şifreleme süresini kısaltır)	Bu onay kutusu, şifreleme alanını yalnızca kullanılan sabit sürücü sektörleri ile sınırlayan seçeneği etkinleştirir/devre dışı bırakır. Bu sınır şifreleme süresini azaltmanızı sağlar. **Sadece kullanılan disk alanını şifrele (şifreleme süresini kısaltır)** özelliğinin şifrelemeyi başlattıktan sonra etkinleştirilmesi veya devre dışı bırakılması durumunda, sabit sürücülerin şifresi çözülene kadar bu ayar değiştirilmez. Şifrelemeyi başlatmadan önce onay kutusunu işaretlemeniz veya işaretini kaldırmanız gerekir. Onay kutusu işaretlenirse sabit sürücünün yalnızca dosyalar tarafından kullanılan bölümleri şifrelenir. Kaspersky Endpoint Security yeni eklenen verileri otomatik olarak şifreler. Onay kutusunun işareti kaldırılırsa daha önce silinen ve değiştirilen dosyaların kalan bölümleri de dahil olmak üzere tüm sürücü şifrelenir. Bu seçenek, verileri değiştirilmemiş veya silinmemiş yeni sabit sürücüler için önerilir. Şifrelemeyi zaten kullanımda olan bir sabit sürücüye uyguluyorsanız tüm sabit sürücünün şifrelenmesi önerilir. Bu, tüm verilerin, hatta potansiyel olarak kurtarılabilir silinmiş verilerin bile korunmasını sağlar. Varsayılan olarak, onay kutusu temizlenmiştir.
Legacy USB Support'u kullan (önerilmez)	Bu onay kutusu Legacy USB Support işlevselliğini etkinleştirir veya devre dışı bırakır. *Legacy USB Support*, **İşletim sistemi** başlatılmadan önce bilgisayarın önyükleme aşamasında (BIOS modu) USB aygıtlarını (güvenlik belirteci gibi) kullanmanıza imkan veren bir BIOS/UEFI işlevidir. Legacy USB Support, işletim sistemi başlatıldıktan sonra USB aygıtları için desteği etkilemez. Bu onay kutusu işaretlenirse bilgisayarın ilk başlatılması sırasında USB aygıtları için destek etkinleştirilir. Legacy USB Support işlevi etkinleştirildiğinde, Kimlik Doğrulama Aracısı BIOS modunda USB aracılığıyla belirteçlerle çalışmayı desteklemez. Bu seçeneği yalnızca donanım uyumluluk sorunu olduğunda ve yalnızca bu sorunun oluştuğu bilgisayarlar için kullanmanız önerilir.
Parola ayarları	Kimlik Doğrulama Aracısı hesap parolası gücü ayarları. Çoklu Oturum Açma teknolojisi kullanıldığında, Kimlik Doğrulama Aracısı Kaspersky Security Center'da belirlenmiş olan parola gücü gerekliliklerini yoksayar. Parolanızın gücü gerekliliklerini işletim sistemi ayarlarında belirleyebilirsiniz.

Parametre	Açıklama
Çoklu Oturum Açma (SSO) teknolojisi kullan	SSO teknolojisi, şifrelenmiş sabit sürücülere erişim sağlamak ve işletim sisteminde oturum açmak için aynı hesap kimlik bilgilerinin kullanılmasına imkan tanır. Onay kutusu işaretlenirse şifrelenmiş sabit sürücülere erişmek ve ardından işletim sisteminde otomatik olarak oturum açmak için hesap kimlik bilgilerini girmeniz gerekir. Onay kutusunun işareti kaldırılırsa şifrelenmiş sabit sürücülere erişmek ve ardından işletim sisteminde oturum açmak için şifrelenmiş sabit sürücüler ve işletim sistemi kullanıcı hesabı kimlik bilgilerine erişmek üzere kimlik bilgilerini ayrı olarak girmeniz gerekir.
Üçüncü taraf kimlik bilgisi sağlayıcılarını sarmalayın	Kaspersky Endpoint Security, üçüncü taraf kimlik bilgisi sağlayıcı ADSelfService Plus'ı destekler. Üçüncü taraf kimlik bilgisi sağlayıcılarıyla çalışırken, Kimlik Doğrulama Aracısı, işletim sistemi yüklenmeden önce parolayı yakalar. Bu, kullanıcının Windows'ta oturum açarken yalnızca bir kez parola girmesi gerektiği anlamına gelir. Kullanıcı Windows'ta oturum açtıktan sonra, örneğin kurumsal hizmetlerde kimlik doğrulama için üçüncü taraf bir kimlik bilgileri sağlayıcısının özelliklerini kullanabilir. Üçüncü taraf kimlik bilgileri sağlayıcıları, kullanıcıların kendi parolalarını bağımsız olarak sıfırlamalarına da olanak tanır. Bu durumda Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı parolasını otomatik olarak günceller. Uygulama tarafından desteklenmeyen bir üçüncü taraf kimlik bilgisi sağlayıcısı kullanıyorsanız, Çoklu Oturum Açma teknolojisinin kullanıldığı işlemlerde bazı sınırlamalarla karşılaşabilirsiniz.
Yardım	**Kimlik Doğrulama**. Hesap bilgileri girilirken Kimlik Doğrulama Aracısı penceresinde görüntülenen yardım metni. **Parolayı değiştir**. Kimlik Doğrulama Aracısı hesabı için parola değiştirilirken Kimlik Doğrulama Aracısı penceresinde görüntülenen yardım metni. **Parolayı kurtar**. Kimlik Doğrulama Aracısı hesabı için parola kurtarılırken Kimlik Doğrulama Aracısı penceresinde görüntülenen yardım metni.

BitLocker Drive Encryption bileşeni ayarları

Parametre	Açıklama
Şifreleme modu	**Tüm sabit sürücüleri şifrele**. Bu seçenek seçilirse, ilke uygulandığında uygulama tüm sabit sürücüleri şifreler. Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca uygulamanın yüklü olduğu işletim sistemini yükleyebilirsiniz. **Tüm sabit sürücülerin şifresini çöz**. Bu seçenek seçilirse, ilke uygulandığında uygulama önceden şifrelenmiş tüm sabit sürücülerin şifresini çözer. **Değiştirmeden bırak**. Bu öğe seçilirse ilke uygulandığında uygulama sürücüleri önceki durumunda bırakır. Sürücü şifreliyse şifrelenmiş olarak kalır. Sürücü şifresi çözülmüşse şifresi çözülmüş olarak kalır. Bu öğe varsayılan olarak seçilmiştir.
Tabletlerde önyükleme öncesi klavye gerektiren BitLocker kimlik doğrulaması kullanımını etkinleştir	Platform önyükleme öncesi giriş özelliğine sahip olmasa bile (örneğin, tabletlerde dokunmatik ekran klavyeleri ile) önyükleme öncesi ortamda veri girişi gerektiren kimlik doğrulamasının kullanılması. Tablet bilgisayarların dokunmatik ekranı önyükleme ortamında kullanılamaz. Tablet bilgisayarlarda BitLocker kimlik doğrulamasını tamamlamak için kullanıcının USB klavye gibi bir aygıt bağlaması gerekir. Onay kutusu işaretlenirse önyükleme girişi gerektiren kimlik doğrulamasının kullanılmasına izin verilir. Bu ayarın yalnızca dokunmatik ekran klavyelerine ek olarak USB klavye gibi önyükleme öncesi ortamda alternatif veri giriş araçlarına sahip cihazlar için kullanılması önerilir. Bu kutu işaretlenmemişse, tabletlerde BitLocker Drive Encryption kullanmak mümkün olmaz.
Donanım şifrelemesi kullan (Windows 8 ve sonraki sürümler)	Onay kutusu işaretlenirse uygulama, donanım şifrelemesi uygular. Bu, şifreleme hızını artırmanızı ve daha az bilgisayar kaynağı kullanmanızı sağlar.

Parametre	Açıklama
Sadece kullanılan disk alanını şifrele (Windows 8 ve sonraki sürümler)	Bu onay kutusu, şifreleme alanını yalnızca kullanılan sabit sürücü sektörleri ile sınırlayan seçeneği etkinleştirir/devre dışı bırakır. Bu sınır şifreleme süresini azaltmanızı sağlar. **Sadece kullanılan disk alanını şifrele (şifreleme süresini kısaltır)** özelliğinin şifrelemeyi başlattıktan sonra etkinleştirilmesi veya devre dışı bırakılması durumunda, sabit sürücülerin şifresi çözülene kadar bu ayar değiştirilmez. Şifrelemeyi başlatmadan önce onay kutusunu işaretlemeniz veya işaretini kaldırmanız gerekir. Onay kutusu işaretlenirse sabit sürücünün yalnızca dosyalar tarafından kullanılan bölümleri şifrelenir. Kaspersky Endpoint Security yeni eklenen verileri otomatik olarak şifreler. Onay kutusunun işareti kaldırılırsa daha önce silinen ve değiştirilen dosyaların kalan bölümleri de dahil olmak üzere tüm sürücü şifrelenir. Bu seçenek, verileri değiştirilmemiş veya silinmemiş yeni sabit sürücüler için önerilir. Şifrelemeyi zaten kullanımda olan bir sabit sürücüye uyguluyorsanız tüm sabit sürücünün şifrelenmesi önerilir. Bu, tüm verilerin, hatta potansiyel olarak kurtarılabilir silinmiş verilerin bile korunmasını sağlar. Varsayılan olarak, onay kutusu temizlenmiştir.
Kimlik doğrulama yöntemi	**Sadece parola (Windows 8 ve sonraki sürümler)** Bu seçenek işaretlenirse, kullanıcı şifrelenmiş bir sürücüye erişmeye çalıştığında Kaspersky Endpoint Security kullanıcıdan bir parola ister. Bu seçenek, Güvenilir Platform Modülü (TPM) kullanılmadığında seçilebilir. **Güvenilir platform modülü (TPM)** Bu seçenek işaretlenirse BitLocker, Güvenilir Platform Modülü'nü (TPM) kullanır. Bir *Trusted Platform Module (TPM)* güvenlikle ilgili temel işlevleri (örneğin şifreleme anahtarlarını saklamak için) sağlamak üzere geliştirilmiş bir mikroçiptir. Bir Güvenilir Platform Modülü genellikle bilgisayarın ana kartına yüklenmiştir ve donanım veri yolu aracılığıyla tüm diğer sistem bileşenleri ile etkileşim halindedir. Windows 7 veya Windows Server 2008 R2 çalıştıran bilgisayarlar için sadece bir TPM modülü kullanarak şifreleme kullanılabilir. Bir TPM modülü yüklü değilse, BitLocker şifrelemesi mümkün değildir. Bu bilgisayarlarda parola kullanımı desteklenmez. Güvenilir Platform Modülü ile donatılmış bir aygıt, yalnızca aygıtla şifresi çözülebilen şifreleme anahtarları oluşturabilir. Güvenilir Platform Modülü şifreleme anahtarlarını kendi kök depolama anahtarı ile şifreler. Kök depolama anahtarı, Güvenilir Platform Modülü'nde saklanır. Bu, şifreleme anahtarlarını ele geçirmek için yapılan girişimlere karşı ek bir koruma düzeyi sağlar. Bu eylem varsayılan olarak seçilmiştir. Şifreleme anahtarına erişim için ek bir koruma katmanı ayarlayabilir ve anahtarı bir parola veya PIN ile şifreleyebilirsiniz: • **TPM için PIN Kullan**. Bu onay kutusu işaretlendiğinde, kullanıcı Güvenilir Platform Modülünde (TPM) depolanan bir şifreleme anahtarına erişim sağlamak için bir PIN kodu kullanabilir. Bu onay kutusu işaretlenmezse, kullanıcıların PIN kodu kullanması yasaklanır. Şifreleme anahtarına erişmek için kullanıcının parola girmesi gerekir. • **Güvenilir platform modülü (TPM) veya TPM kullanılamıyorsa parola**. Bu seçenek tercih edilirse, Güvenilir Platform Modülü (TPM) mevcut olmadığında kullanıcı şifreleme anahtarlarına erişim elde etmek için bir parola kullanabilir. Bu onay kutusu işaretlenmemişse ve TPM kullanılabilir değilse, tam disk şifreleme başlamaz. Seçilen kimlik doğrulama yöntemi, parola veya PIN gereklilikleri belirlenerek yapılandırılmalıdır: • **Minimum PIN uzunluğu (karakter)** (varsayılan değer 6'dır). • **Minimum parola uzunluğu (karakter)** (varsayılan değer 8'dir). • **Depolanan maksimum parola/PIN sayısı** (varsayılan değer 5'tir). • **TPM için parola/PIN geçerlilik süresini sınırla (gün)** (varsayılan olarak devre dışıdır). • **Gelişmiş PIN (harfler ve rakamlar) kullan**. *Genişletilmiş PIN* sayısal karakterlere ek olarak büyük ve küçük Latin harfleri, özel karakterler ve boşluklar gibi diğer karakterlerin kullanılmasına da izin verir. Varsayılan olarak devre dışıdır.
Kurtarma anahtarını otomatik olarak yeniden oluştur (gün)	BitLocker tarafından korunan bir sürücüye erişimi geri yüklemek için parolayı otomatik olarak güncelleyin. Bu onay kutusu işaretlendiğinde, kurtarma anahtarı parolasının geçerlilik süresini belirtin. Bu, kurtarma anahtarı parolasının yeniden kullanılmasını önlemeye yardımcı olur.

Dosya Düzeyinde Şifreleme

Arm tabanlı bilgisayarlarda dosya şifreleme özelliği desteklenmemektedir.

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

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 ilke 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.

Dosya şifreleme şu özel özelliklere sahiptir:

- 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 veya yeniden yönlendirilen klasörlerin önceden tanımlanmış klasörlerindeki dosyaları şifrelemez veya şifresini çözmez.
- Kaspersky Endpoint Security, değiştirilmesi işletim sistemine ve yüklü uygulamalara zarar verebilecek dosyaları şifrelemez. Örneğin içe içe geçmiş klasörlerin olduğu aşağıdaki dosya ve klasörler şifrelemeden istisnalar listesindedir:
  - %WINDIR%;
  - %PROGRAMFILES% ve %PROGRAMFILES(X86)%;
  - Windows kayıt defteri dosyaları.

  Şifreleme istisnaları listesi görüntülenemez veya düzenlenemez. Şifreleme istisnaları listesindeki dosyalar ve klasörler şifreleme listesine eklenebilir ancak dosya şifreleme sırasında şifrelenmez.

Dosya Düzeyinde Şifreleme bileşeni ayarları

Parametre	Açıklama
Şifreleme modu	**Değiştirmeden bırak**. Bu öğe seçilirse Kaspersky Endpoint Security dosyaları ve klasörleri şifrelemeden veya şifrelerini çözmeden bırakır. **Kurallara göre**. Bu öğe seçilirse, Kaspersky Endpoint Security dosyaları ve klasörleri şifreleme kurallarına göre şifreler, dosyaların ve klasörlerin şifresini çözme kurallarına göre şifresini çözer ve uygulamaların şifrelenmiş dosyalara erişimini uygulama kurallarına göre düzenler. **Tümünün şifresini çöz**. Bu öğe seçilirse Kaspersky Endpoint Security tüm şifrelenmiş dosyaların ve klasörlerin şifrelerini çözer.

Parametre	Açıklama
Şifreleme	Bu sekmede, yerel sürücüler üzerinde saklanan dosyalar için şifreleme kuralları yer alır. Dosyaları şu şekilde ekleyebilirsiniz: • **Ön tanımlı klasörler**. Kaspersky Endpoint Security şu alanları eklemenize izin verir: **Belgeler**. İşletim sisteminin standart *Belgeler* klasörü ve onun alt klasörleri. **Sık Kullanılanlar**. İşletim sisteminin standart *Sık Kullanılanlar* klasörü ve onun alt klasörleri. **Masaüstü**. İşletim sisteminin standart *Masaüstü* klasörü ve onun alt klasörleri. **Geçici dosyalar**. Bilgisayara yüklenmiş uygulamaların çalışmasıyla ilgili geçici dosyalar. Örneğin Microsoft Office uygulamaları, belgelerin yedek kopyalarını içeren geçici dosyalar oluşturur. **Outlook dosyaları**. Outlook posta istemcisinin çalışmasıyla ilgili dosyalar: veri dosyaları (PST), çevrimdışı veri dosyaları (OST), çevrimdışı adres defteri dosyaları (OAB) ve kişisel adres defteri dosyaları (PAB). • **Özel klasör**. Klasörün yolunu yazabilirsiniz. Bir klasör yolu yazarken şu kurallara uyun: Bir ortam değişkeni kullanın (örneğin `%FOLDER%\UserFolder\`). Bir ortam değişkenini sadece bir kez ve yolun başında kullanabilirsiniz. Göreli yollar kullanmayın. `*` ve `?` karakterlerini kullanmayın. UNC yollarını kullanmayın. Ayırıcı karakter olarak `;` veya `,` kullanın. • **Uzantıya göre dosyalar**. Listeden uzantı grupları seçebilirsiniz, örneğin *Arşivler* uzantı grubu. Ayrıca dosya uzantısını manuel olarak eklemeniz de mümkündür.
Şifre çözme	Bu sekmede, yerel sürücüler üzerinde saklanan dosyalar için şifre çözme kuralları yer alır.
Uygulamalar için kurallar	Bu sekmede, uygulamalar için şifrelenmiş dosya erişim kuralları ve tek tek uygulamalar tarafından oluşturulan veya değiştirilen dosyalar için şifreleme kuralları içeren bir tablo görüntülenir.
Şifrelenmiş paketler	Şifrelenmiş paketler oluşturma sırasında karşılanması gereken parola güvenliği gereklilikleri.

Çıkarılabilir sürücüleri şifreleme

Arm tabanlı bilgisayarlarda çıkarılabilir sürücülerin şifrelenmesi desteklenmemektedir.

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

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.

Çıkarılabilir sürücülerdeki verileri korumak için şu şifreleme türlerini kullanabilirsiniz:

- Full Disk Encryption (FDE).

  Dosya sistemi de dahil olmak üzere çıkarılabilir sürücünün tamamının şifrelenmesidir.

  Kurumsal ağın dışındaki şifrelenmiş verilere erişim mümkün değildir. Bundan başka, eğer bilgisayar Kaspersky Security Center'a bağlı değilse (örneğin bir konuk bilgisayarda) kurumsal ağ içindeki verilere erişmek mümkün olmaz.

- File Level Encryption (FLE).

  Sadece bir çıkarılabilir bir sürücüdeki dosyaların şifrelenmesidir. Dosya sistemi değişmez.

Çıkarılabilir sürücülerdeki dosyaların şifrelenmesi, *taşınabilir mod* adlı özel bir mod kullanılarak kurumsal ağın dışındaki verilere erişim imkanı sağlar.

Şifreleme sırasında Kaspersky Endpoint Security bir ana anahtar oluşturur. Kaspersky Endpoint Security ana anahtarı şu veri havuzlarına kaydeder:

- Kaspersky Security Center.
- Kullanıcının bilgisayarı.

  Ana anahtar, kullanıcının gizli anahtarı kullanılarak şifrelenir.
- Çıkarılabilir sürücü.

  Ana anahtar, Kaspersky Security Center'ın genel anahtarı ile şifrelenir.

Şifreleme tamamlandıktan sonra, kurumsal ağ içinde çıkarılabilir sürücü üzerinde verilere, sanki şifrelenmemiş normal bir çıkarılabilir sürücü üzerindeymiş gibi erişilebilir.

Şifrelenmiş verilere erişim

Şifrelenmiş verilere sahip bir çıkarılabilir sürücü bağlandığında, Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

1. Kullanıcının bilgisayarındaki yerel depolama alanında bir ana anahtar arar.

   Bir ana anahtar bulunursa kullanıcı çıkarılabilir sürücüldeki verilere erişim kazanır.

   Ana anahtar bulunmazsa, Kaspersky Endpoint Security aşağıdaki eylemleri gerçekleştirir:

   a. Kaspersky Security Center'a bir istek gönderir.

      İstek alındıktan sonra, Kaspersky Security Center ana anahtarı içeren bir yanıt gönderir.

   b. Kaspersky Endpoint Security ana anahtarı, şifrelenmiş çıkartılabilir sürücü ile gerçekleştirilecek daha sonraki işlemler için kullanıcının bilgisayarındaki yerel depolama alanına kaydeder.
2. Verilerin şifresini çözer.

Çıkarılabilir sürücü şifrelemesinin özel özellikleri

Çıkarılabilir sürücüleri şifreleme şu özelliklere sahiptir:

- Belirli bir grup yönetilen bilgisayar için kaldırılabilir sürücü şifreleme ön ayarlarına sahip ilke 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 dosyaları şifrelemez / şifresini çözmez.

- 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

Çıkarılabilir sürücülerin bileşen ayarlarının şifrelenmesi

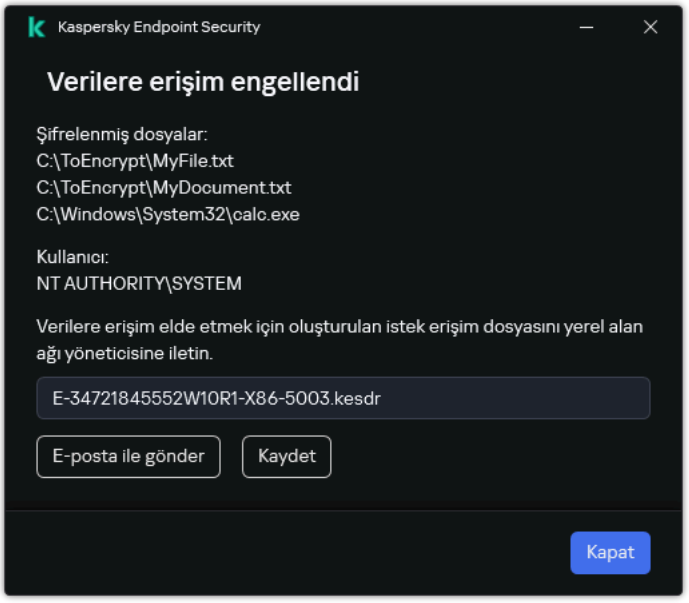
Parametre	Açıklama
Şifreleme modu	**Çıkarılabilir sürücünün tamamını şifrele**. Bu öğe seçilirse çıkarılabilir sürücüler için belirtilen şifreleme ayarlarıyla birlikte ilke uygulanırken Kaspersky Endpoint Security, çıkarılabilir sürücüleri dosya sistemleri de dahil olmak üzere kesim kesim şifreler. **Tüm dosyaları şifrele**. Bu öğe seçilirse çıkarılabilir sürücüler için belirtilen şifreleme ayarlarıyla birlikte ilke uygulanırken Kaspersky Endpoint Security, çıkarılabilir sürücülerde depolanan tüm dosyaları şifreler. Kaspersky Endpoint Security şifrelenmiş dosyaları tekrar şifrelemez. Klasör yapısı ve şifrelenmiş dosyaların adları da dahil olmak üzere, çıkarılabilir bir sürücünün dosya sisteminin içeriği şifrelenmez ve erişilebilir kalır. **Sadece yeni dosyaları şifrele**. Bu öğe seçilirse çıkarılabilir sürücüler için belirtilen şifreleme ayarlarıyla birlikte ilke uygulanırken Kaspersky Endpoint Security, yalnızca Kaspersky Security Center ilkesi en son uygulandıktan sonra çıkarılabilir sürücülere eklenen veya sürücülerde değiştirilen dosyaları şifreler. Bu şifreleme modu, çıkarılabilir bir sürücü hem kişisel hem de iş amaçlı kullanıldığında uygundur. Bu şifreleme modu, tüm eski dosyaları değiştirmeden bırakmanıza ve kullanıcının Kaspersky Endpoint Security'nin yüklü olduğu ve şifreleme işlevselliğinin etkinleştirilmiş olduğu bir iş bilgisayarında oluşturduğu dosyaları şifrelemenize olanak tanır. Sonuç olarak kişisel dosyalara erişim, şifreleme işlevselliği etkinleştirilmiş olarak Kaspersky Endpoint Security'nin bilgisayara yüklenip yüklenmediğine bakılmaksızın her zaman etkindir. **Çıkarılabilir sürücünün tamamının şifresini çöz**. Bu öğe seçilirse çıkarılabilir sürücüler için belirtilen şifreleme ayarlarıyla birlikte ilke uygulanırken Kaspersky Endpoint Security, çıkarılabilir sürücülerde depolanan tüm şifreli dosyaların ve daha önce şifrelenmişse çıkarılabilir sürücülerin dosya sistemlerinin şifresini çözer. **Değiştirmeden bırak**. Bu öğe seçilirse ilke uygulandığında uygulama sürücüleri önceki durumunda bırakır. Sürücü şifreliyse şifrelenmiş olarak kalır. Sürücü şifresi çözülmüşse şifresi çözülmüş olarak kalır. Bu öğe varsayılan olarak seçilmiştir.
Taşınabilir mod	Bu onay kutusu, kurumsal ağın dışındaki bilgisayarlardaki çıkarılabilir sürücüde depolanan dosyalara erişimi mümkün kılan bir çıkarılabilir sürücünün hazırlanmasını etkinleştirir/devre dışı bırakır. Bu onay kutusu işaretlenirse Kaspersky Endpoint Security, ilkenin uygulanması üzerine çıkarılabilir bir sürücüdeki dosyaları şifrelemeden önce kullanıcıdan bir parola belirlemesini ister. Parola, kurumsal ağın dışındaki bilgisayarlardaki çıkarılabilir bir sürücüde şifrelenmiş dosyalara erişmek için gereklidir. Parolanın gücünü yapılandırabilirsiniz. Taşınabilir mod **Tüm dosyaları şifrele** veya **Sadece yeni dosyaları şifrele** modları için kullanılabilir.
Sadece kullanılan disk alanını şifrele	Bu onay kutusu, yalnızca kullanılan disk kesimlerinin şifrelendiği şifreleme modunu etkinleştirir/devre dışı bırakır. Bu mod, verileri değiştirilmemiş veya silinmemiş yeni sürücüler için önerilir. Onay kutusu işaretlenirse sürücünün yalnızca dosyalar tarafından kullanılan bölümleri şifrelenir. Kaspersky Endpoint Security yeni eklenen verileri otomatik olarak şifreler. Onay kutusu işaretlenmezse daha önce silinen ve değiştirilen dosyaların kalan bölümleri de dahil olmak üzere tüm sürücü şifrelenir. Sadece kullanılan alanın şifrelenmesi özelliği, yalnızca **Çıkarılabilir sürücünün tamamını şifrele** modu için kullanılabilir. Şifreleme başladıktan sonra **Sadece kullanılan disk alanını şifrele** işlevinin etkinleştirilmesi/devre dışı bırakılması, bu ayarı değiştirmez. Şifrelemeyi başlatmadan önce onay kutusunu işaretlemeniz veya işaretini kaldırmanız gerekir.

Özel kurallar	Bu tablo özel şifreleme kuralları tanımlanmış aygıtları içerir. Çıkarılabilir sürücüler için şu yöntemleri kullanarak şifreleme kuralları oluşturabilirsiniz:
	• Aygıt Denetimi için güvenilir aygıtlar listesinden bir çıkarılabilir sürücü ekleyin.
	• Bir çıkarılabilir sürücüyü manuel olarak ekleyin:
	  • Cihaz kimliğine göre (Hardware ID veya HWID)
	  • Cihaz modeline göre: Vendor ID (VID) ve Product ID (PID)

Parametre	Açıklama
Çevrimdışı modda çıkarılabilir sürücülerin şifrelenmesine izin ver	Bu onay kutusu işaretlenirse Kaspersky Endpoint Security, Kaspersky Security Center ile bağlantı kurulmasa bile çıkarılabilir sürücüleri şifreler. Bu durumda, çıkarılabilir sürücülerin şifresini çözmek için gereken veriler, çıkarılabilir sürücünün bağlı olduğu bilgisayarın sabit sürücüsünde saklanır ve Kaspersky Security Center'a iletilmez. Onay kutusu işaretlenmezse Kaspersky Endpoint Security, Kaspersky Security Center ile bağlantı olmadığında çıkarılabilir sürücüleri şifrelemez.
Şifreleme parolası ayarları / Taşınabilir Dosya Yöneticisi	Taşınabilir Dosya Yöneticisi için parola gücü ayarları.

Şablonlar (veri şifreleme)

Veri şifreleme sonrasında, Kaspersky Endpoint Security tüm verilere erişimi kısıtlayabilir; örneğin kuruluşun altyapısındaki bir değişikliğe ve Kaspersky Security Center Yönetim Sunucusu'ndaki bir değişikliğe bağlı olarak. Bir kullanıcının şifrelenmiş verilere erişimi yoksa, kullanıcı yöneticiden verilere erişim isteyebilir. Başka bir deyişle, kullanıcının yöneticiye bir istek erişim dosyası göndermesi gerekir. Kullanıcının bundan sonra yöneticiden aldığı yanıt dosyasını Kaspersky Endpoint Security'ye yüklemesi gerekir. Kaspersky Endpoint Security, yöneticiden e-posta ile alınan verilere erişim istemenize olanak tanır.



Şifrelenmiş verilere erişim isteme

Şifrelenmiş verilere erişim olmadığında raporlama yapmak için bir şablon sunulur. Kullanıcı kolaylığı için şu alanları doldurabilirsiniz:

- **Bitiş**. Veri şifreleme özellikleri için haklara sahip olan yönetim grubunun e-posta adresini girin.
- **Konu**. Şifrelenmiş dosyalara erişim için yapılan istekle birlikte e-postanın konusunu girin. Örneğin mesajları filtrelemek için etiketleri ekleyebilirsiniz.
- **Kullanıcı mesajı**. Gerekirse mesajın içeriğini değiştirin. Gerekli verileri almak için değişkenler kullanabilirsiniz, örneğin, %USER_NAME% değişkeni.

İstisnalar

Güvenilir bölge, Kaspersky Endpoint Security'nin etkin olduğunda izlemediği nesnelerin ve uygulamaların sistem yöneticisi tarafından yapılandırılan listesidir.

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. Bir yönetici, bir kullanıcının belirli bir bilgisayar için kendi yerel güvenilir bölgesini oluşturmasına da izin verebilir. Bu şekilde, kullanıcılar bir ilkedeki genel güvenilen bölgeye ek olarak kendi yerel istisnalar ve güvenilir uygulamalar listelerini oluşturabilir.

Kaspersky Endpoint Security 12.5 for Windows ile başlayarak, EDR telemetrisini güvenilir bölgeye ekleyebilirsiniz. Bu, uygulamanın Kaspersky Anti Targeted Attack Platform (EDR) çözümü için telemetri toplama sunucusuna gönderdiği verilerin optimize edilmesini sağlar.

Kaspersky Endpoint Security 12.6 for Windows sürümünden itibaren, tarama istisnaları ve güvenilir uygulamalar güvenilen bölgeye eklenir. Önceden tanımlanmış tarama istisnaları ve güvenilir uygulamalar Kaspersky Endpoint Security'nin SQL sunucularında, Microsoft Exchange sunucularında ve System Center Configuration Manager'da hızla yapılandırılmasına yardımcı olur. Bu, sunucularda uygulama için manuel olarak güvenilir bir bölge ayarlamanıza gerek olmadığı anlamına gelir.

Kaspersky Endpoint Security 12.8 for Windows ile başlayarak, uygulamayı sanal ortamları korumak için Light Agent modunda yükleyebilirsiniz. Önceden tanımlanmış tarama istisnaları ve güvenilen uygulamalar, Kaspersky Endpoint Security'yi Citrix ve VMware sanal ortamlarında hızla yapılandırmanıza yardımcı olabilir.

Tarama istisnaları

Tarama istisnası, Kaspersky Endpoint Security'nin belirli bir nesnede virüsleri ve diğer tehditleri taramaması için karşılanması gereken koşullar kümesidir. Tarama istisnaları, suçlular tarafından bir bilgisayara veya kullanıcı verilerine zarar vermek için kullanılabilecek yasal yazılımların güvenli bir şekilde kullanılmasını mümkün kılar. Bu tür uygulamaların mutlaka zararlı bir amacı yoktur ancak bilgisayar korsanları tarafından istismar edilebilirler. Saldırganların bilgisayarın veya kullanıcı verilerinin güvenliğini tehlikeye atmak için kullanabileceği meşru uygulamalar hakkında ayrıntılı bilgi edinmek için lütfen Kaspersky Ansiklopedisi web sitesini ziyaret edin.

Bu uygulamalar, Kaspersky Endpoint Security tarafından engellenebilir. Uygulamaların engellenmesini önlemek için kullanılan uygulamaların tarama istisnalarını yapılandırabilirsiniz. Bunun için Kaspersky IT 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 IT 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.
- *Kötü Amaçlı Yazılım Taraması* görevi

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 uygulama işlemi tarafından açılan, yürütülen veya kaydedilen nesneleri izler ve bunlar tarafından oluşturulan tüm uygulamaların ve ağ trafiğinin etkinliğini denetler. Bir uygulama güvenilir uygulamalar listesine eklendikten sonra, Kaspersky Endpoint Security uygulamanın etkinliğini izlemeyi durdurur.

Tarama istisnaları ve güvenilen uygulamalar arasındaki fark şudur: istisnalar için Kaspersky Endpoint Security'nin dosyaları taramaz, güvenilen uygulamalar için ise başlatılan işlemleri denetlemez. Güvenilir bir uygulama, tarama istisnalarına dahil olmayan bir klasörde zararlı bir dosya oluşturduğu takdirde, Kaspersky Endpoint Security dosyayı algılar ve tehdidi ortadan kaldırır. Klasör istisnalara eklenirse Kaspersky Endpoint Security bu dosyayı atlayacaktır.

Örneğin standart Microsoft Windows Not defteri uygulaması tarafından kullanılan nesnelerin güvenli olduğunu düşünüyorsanız yani bu uygulamaya güveniyorsanız Microsoft Windows Not Defteri'ni güvenilir uygulamaların listesine ekleyebilirsiniz, böylece bu uygulama tarafından kullanılan nesneler izlenmez. Bu, özellikle sunucu uygulamalarını kullanırken önemli olan bilgisayar performansını artıracaktır.

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.

Güvenilir uygulamalar, Kaspersky Endpoint Security ve diğer uygulamalar arasındaki uyumluluk sorunlarını önlemeye yardımcı olur (örneğin, üçüncü taraf bir bilgisayarın ağ trafiğinin Kaspersky Endpoint Security ve başka bir anti-virüs uygulaması tarafından iki kez taranması sorunu).

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.

Parametre	Açıklama

Tespit edilen nesne türleri

Kaspersky Endpoint Security, yapılandırılmış uygulama ayarlarından bağımsız olarak her zaman virüsleri, solucanları ve Truva atlarını tespit eder ve engeller. Bilgisayara çok büyük zarar verebilirler.

- **Virüs ve solucanlar**

  Alt kategori: Virüs ve solucanlar (Viruses_and_Worms)

  Tehlike düzeyi: Yüksek

  Klasik virüs ve solucanlar, kullanıcılar tarafından yetkilendirilmeyen eylemleri gerçekleştirir. Kendi kendilerini çoğaltabilme kabiliyetine sahip kopyalarını oluşturabilirler.

  Klasik virüs

  Klasik bir virüs bilgisayara sızdığında, bir dosyaya bulaşır, etkinleşir, kötü amaçlı eylemleri gerçekleştirir ve kendi kopyalarını diğer dosyalara ekler.

  Klasik bir virüs, yalnızca bilgisayarın yerel kaynakları üzerinde çoğalır; kendi başına diğer bilgisayarlara giremez. Virüs, başka bir bilgisayara yalnızca paylaşımlı bir klasörde veya takılı bir CD'de bulunan bir dosyaya kendi kopyasını eklerse veya kullanıcı virüslü dosya ekli bir e-posta mesajını iletirse geçebilir.

  Klasik virüs kodu, bilgisayarların, işletim sistemlerinin ve uygulamaların çeşitli alanlarına girebilir. Ortama bağlı olarak virüsler, *dosya virüslerine*, *önyükleme virüslerine*, *komut dizisi virüslerine* ve *makro virüslerine* ayrılır.

  Virüsler, çeşitli teknikler kullanarak dosyalara bulaşabilir. *Overwriting* virüsler kodlarını bulaştıkları dosyanın kodunun üzerine yazarak dosyanın içeriğini silerler. Virüslü dosya çalışmaz ve geri yüklenemez. *Parasitic* virüsler dosyaları değiştirerek tamamen veya kısmen işlevsel hale getirir. *Companion* dosyaları değiştirmez, bunun yerine kopyalar oluşturur. Virüslü bir dosya açıldığında, dosyanın (aslında bir virüs olan) kopyası başlatılır. Şu virüs türleriyle de karşılaşılmaktadır: *Link virüsleri*, *OBJ virüsleri*, *LIB virüsleri*, *kaynak kodu* virüsleri ve daha pek çok tür

  Worm

  Klasik virüslerde olduğu gibi, solucan kodu da bilgisayara sızdıktan sonra etkinleşir ve kötü amaçlı eylemler gerçekleştirir. Solucanların bu şekilde adlandırılmalarının nedeni, bir bilgisayardan diğerine "gezinme" kabiliyetleri ve kullanıcının izni olmaksızın çok sayıda veri kanalı üzerinden kopyalarını yaymalarıdır.

  Çeşitli solucan türleri arasında ayrım yapmaya izin veren ana özellik, yayılma biçimleridir. Aşağıdaki tabloda, yayılma biçimlerine göre sınıflandırılan çeşitli solucan türlerine genel bir bakış sağlanmaktadır.

  Solucanların yayılma biçimleri

Tür	Ad	Açıklama
Email-Worm	Email-Worm	E-posta yoluyla yayılır. Virüslü bir e-posta mesajı, bir solucan kopyasına sahip bir dosya veya hacklenmiş ya da özellikle bu amaç için oluşturulmuş bir İnternet sitesine yüklenen bir dosyanın bağlantısını içerir. Eklenen dosyayı açtığınızda solucan etkinleştirilir. Bağlantıya tıklayıp, dosyayı indirip açtığınızda, solucan da kötü amaçlı eylemlerini gerçekleştirmeye başlar. Bundan sonra kendi kopyalarını yaymaya, diğer e-posta adreslerini aramaya ve virüslü mesajlar göndermeye devam eder.
IM-Worm	Anlık Mesajlaşma istemcisi solucanları	Anlık ileti uygulamaları aracılığıyla yayılır. Genellikle bu tür solucanlar, kullanıcının iletişim listelerini kullanarak bir İnternet sitesindeki solucanın bir kopyasıyla bir dosyaya bağlantı içeren mesajlar gönderir. Kullanıcı dosyayı indirip açtığında solucan etkinleşir.
IRC-Worm	İnternet sohbeti solucanları	Gerçek zamanlı olarak İnternet üzerinden diğer insanlarla iletişim kurmaya izin veren hizmet sistemlerinden Internet Relay Chats aracılığıyla yayılır. Bu solucanlar, bir İnternet sohbetinde kendilerinin bir kopyası veya bir dosya bağlantısı içeren bir dosya yayınlar. Kullanıcı dosyayı indirip açtığında solucan etkinleşir.
Net-Worm	Ağ solucanları	Bu solucanlar, bilgisayar ağları üzerinden yayılır. Diğer solucan türlerinden farklı olarak, tipik bir ağ solucanı kullanıcının katılımı olmadan yayılır. Yerel ağlarda zayıf noktalara sahip programlar bulunan bilgisayarları tarar. Bunun için solucan kodunu veya bir bölümünü içeren özel olarak oluşturulmuş bir ağ paketi (açık bırakıcı) gönderir. Ağda "hassas" bir bilgisayar varsa, bu ağ paketini alır. Solucan bilgisayara tamamen girdiğinde etkinleşir.
P2P-Worm	Dosya paylaşımı ağ solucanları	Eşdüzey dosya paylaşım ağları üzerinden yayılır. Bir P2P ağına sızmak için solucan genellikle kullanıcının bilgisayarında bulunan bir dosya paylaşım klasörüne kendisini kopyalar. P2P ağı, bu dosyayla ilgili bilgileri görüntüler, böylece kullanıcı ağdaki virüslü dosyayı başka herhangi bir dosya gibi "bulabilir" ve ardından dosyayı indirip açabilir. Daha karmaşık solucanlar belirli bir P2P ağının ağ iletişim kuralını taklit eder: arama sorgularına olumlu tepki verirler ve indirmek için kopyalarını sunarlar.
Worm	Solucanların diğer türleri	Solucanların diğer türleri aşağıdakileri içerir: • Kendi kopyalarını ağ kaynaklarına yayan solucanlar. İşletim sisteminin işlevlerini kullanarak, etkin ağ klasörlerini tarar, İnternet'teki bilgisayarlara bağlanır ve disk sürücülerine tam erişim elde etmeye çalışırlar. Daha önce açıklanan solucan türlerinden farklı olarak diğer solucan türleri kendi başlarına değil, kullanıcı tarafından solucanın kopyasını içeren bir dosya açıldığında etkinleşir. • Yayılmak için önceki tabloda açıklanan yöntemlerin hiçbirini kullanmayan solucanlar (örneğin, cep telefonlarından yayılanlar).

- **Truva atları (fidye yazılımı dahil)**;

  Alt kategori: Truva atları

  Tehlike düzeyi: Yüksek

Solucanlar ve virüslerden farklı olarak Truva atları kendi kendine çoğalmamaktadır. Örneğin, kullanıcı virüslü bir İnternet sayfasını ziyaret ettiğinde, bir bilgisayara e-posta veya tarayıcı aracılığıyla girerler. Truva atları kullanıcının katılımıyla başlatılır. Kötü amaçlı eylemlerini başlatıldıktan hemen sonra yapmaya başlarlar.

Farklı Truva atları virüslü bilgisayarlarda farklı davranır. Truva atlarının başlıca işlevleri, bilgileri engellemek, değiştirmek veya yok etmek ve bilgisayarları veya ağları devre dışı bırakmaktır. Truva atları ayrıca dosyaları alabilir veya gönderebilir, çalıştırabilir, mesajları ekranda gösterebilir, İnternet sayfalarını isteyebilir, programları indirip yükleyebilir ve bilgisayarı yeniden başlatabilir.

Bilgisayar korsanları sıklıkla çeşitli Truva atlarının "setlerini" kullanırlar.

Truva atı davranışının türleri aşağıdaki tabloda açıklanmaktadır.

Virüslü bir bilgisayardaki Truva atı davranışı türleri

Tür	Ad	Açıklama
Trojan-ArcBomb	Truva atları - "arşiv bombaları"	Paket açıldığında, bu arşivler bilgisayarın çalışmasını etkileyecek büyüklükteki boyuta ulaşırlar. Kullanıcı bu tür bir arşivin paketini açmaya çalıştığında, bilgisayar yavaşlayabilir ya da donabilir: sabit sürücü "boş" veri ile doldurulabilir. "Arşiv bombaları" özellikle dosya ve e-posta sunucuları için tehlikelidir. Sunucu, gelen bilgiyi işlemek için otomatik bir sistem kullanıyorsa bir "arşiv bombası" sunucuyu durdurabilir.
Backdoor	Uzaktan yönetim için truva atları	Bunlar en tehlikeli Truva atı türü olarak kabul edilir. Bunlar işlevlerinde, bilgisayarlara yüklenen uzaktan yönetim uygulamalarına benzerdir. Bu programlar kullanıcının dikkatini çekmeden kendisini bilgisayara yükler ve saldırganın bilgisayarı uzaktan yönetmesini sağlar.
Trojan	Truva atları	Bunlar aşağıdaki zararlı uygulamaları içerir: • **Klasik Truva Atları**. Bu programlar, yalnızca Truva atlarının ana işlevlerini gerçekleştirir: bilgiyi engelleme, değiştirme ve yok etme ile bilgisayarları veya ağları devre dışı bırakma. Tabloda açıklanan Truva atı türlerinden farklı olarak hiçbir ileri düzey özelliğe sahip değillerdir. • **Çok yönlü Truva atları**. Bu programlar, çeşitli Truva atları türlerine özgü gelişmiş özelliklere sahiptir.
Trojan-Ransom	Fidye Truva atları	Kullanıcının bilgilerini "rehin" alır, değiştirir veya engeller ya da bilgisayarın çalışmasına etki eder; böylece kullanıcı bilgiyi kullanma kabiliyetini kaybeder. Saldırgan, bilgisayarın performansını ve üzerine depolanan verileri geri yüklemek için bir uygulama göndermeyi vaat ederek kullanıcıdan bir fidye ister.
Trojan-Clicker	Truva atı tıklayıcılar	Komutları kendi başına bir tarayıcıya göndererek veya işletim sistemi dosyalarında belirtilen İnternet adreslerini değiştirerek İnternet sayfalarına kullanıcının bilgisayarından erişirler. Bu programları kullanarak saldırganlar ağ saldırılarını gerçekleştirir ve İnternet sitesi ziyaretlerini arttırır, böylece reklam pencerelerinin gösterim sayısını artırır.
Trojan-Downloader	Truva atı indiriciler	Saldırganın İnternet sayfasına erişir, diğer zararlı uygulamaları buradan indirir ve kullanıcının bilgisayarına yükler. İndirilecek zararlı uygulamanın dosya adını içerebilir veya bunu erişilen İnternet sayfasından alabilir.
Trojan-Dropper	Truva atı bırakıcılar	Sabit sürücüye yükledikleri ve daha sonra kurdukları diğer Truva atlarını içerirler. Saldırganlar, aşağıdaki amaçlar için Truva atı-Bırakıcı türü programları kullanabilir: • Kullanıcı tarafından fark edilmeden bir zararlı uygulama yükleme: Truva atı-Bırakıcı türü programlar hiçbir mesaj görüntülemez veya örneğin bir arşivdeki veya işletim sisteminin uyumsuz bir sürümündeki bir hatayı bildiren sahte mesajlar görüntüler. • Bilinen diğer zararlı uygulamayı tespit edilmekten korur: tüm anti-virüs yazılımları Truva atı-Bırakıcı türü bir uygulama içindeki zararlı bir uygulamayı tespit edemez.
Trojan-Notifier	Truva atı uyarıcılar	Bir saldırgana virüslü bilgisayara erişilebilir olduğu bildirilir, saldırgana bilgisayar hakkında bilgiler gönderir: IP adresi, açık port numarası veya e-posta adresi. Saldırgan ile e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla bağlantı kurar. Truva atı-Uyarıcı türü programlar genellikle birkaç Truva atından oluşan setler halinde kullanılır. Saldırgana diğer Truva atlarının kullanıcının bilgisayarına başarılı bir şekilde yüklendiğini bildirir.
Trojan-Proxy	Truva atı proxy'leri	Saldırganın, kullanıcının bilgisayarını kullanarak isimsiz bir şekilde İnternet sayfalarına erişmesine izin verir; genellikle spam göndermek için kullanılır.
Trojan-PSW	Parola-çalma-yazılımı	Parola-çalma-yazılımı, yazılım kayıt verileri gibi kullanıcı hesaplarını çalan bir Truva atı türüdür. Bu Truva atları, sistem dosyalarında ve kayıt defterinde gizli verileri bulur ve e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla "saldırgana" gönderir. Bu Truva atlarından bazıları, bu tabloda açıklanan ayrı türlerde kategorilere ayrılmıştır. Bunlar; banka hesaplarını çalan (Truva atı-Banker), anlık ileti uygulamaları kullanıcılarından gelen verileri çalan (Truva atı-IM) ve çevrimiçi oyun kullanıcılarından gelen bilgileri çalan (Truva atı-OyunHırsızı) Truva atlarıdır.
Trojan-Spy	Truva atı casusları	Kullanıcı ile ilgili casusluk yapar, kullanıcının bilgisayarında çalışırken yaptığı işlemler hakkında bilgi toplar. Kullanıcının klavyede girdiklerini okuyabilir, ekran görüntülerini alabilir veya etkin uygulamaların listelerini toplayabilir. Bilgileri aldıktan sonra bunları saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla iletir.
Trojan-DDoS	Truva atı ağ saldırganları	Kullanıcı bilgisayarından uzaktaki bir sunucuya çok sayıda istek gönderirler. Sunucunun tüm istekleri işlemek için yeterli kaynağı bulunmamaktadır; bu nedenle çalışmayı durdurur (Hizmet Reddi veya yalnızca DoS). Bilgisayar korsanları, genellikle bu programlarla çok sayıda bilgisayara virüs bulaştırır; böylece bilgisayarları aynı anda tek bir sunucuya saldırmak için kullanabilirler. DoS programları, kullanıcının bilgisi dahilinde tek bir bilgisayardan bir saldırı gerçekleştirir. DDoS (Dağıtılan DoS) programları, virüslü bilgisayar kullanıcısı tarafından fark edilmeden çeşitli bilgisayarlardan dağıtılan saldırılar gerçekleştirir.
Trojan-IM	Truva atları anlık ileti uygulamaları kullanıcılarından bilgi çalar	Anlık ileti uygulamaları kullanıcılarının hesap numaralarını ve parolalarını çalar. Verileri saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla iletir.
Rootkit	Rootkit'ler	Diğer zararlı uygulamaları ve onların etkinliklerini maskeler, dahası programların işletim sistemindeki kalıcılığını uzatırlar. Ayrıca dosyaları, virüs bir bilgisayarın belleğindeki işlemleri veya zararlı uygulamaları çalıştıran kayıt defteri anahtarlarını gizleyebilirler. Rootkit'ler, kullanıcı bilgisayarındaki ve ağdaki diğer bilgisayarlardaki uygulamalar arasındaki veri alışverişini maskeleyebilir.
Trojan-SMS	SMS mesajları biçimindeki Truva atları	Cep telefonlarına virüs bulaştırır, özel tarifeli telefon numaralarına SMS mesajları gönderir.
Trojan-GameThief	Çevrimiçi oyun kullanıcılarından bilgi çalan Truva atları	Çevrimiçi oyunların kullanıcılarından hesap kimlik bilgilerini çalar ve daha sonra verileri saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla iletir.

Trojan-Banker	Banka hesaplarını çalan Truva atları	Banka hesap bilgilerini veya e-para sistem verilerini çalar, daha sonra verileri bilgisayar korsanına e-posta ile, FTP üzerinden, bilgisayar korsanının İnternet sayfasına erişerek ya da başka bir yöntem kullanarak iletir.
Trojan-Mailfinder	E-posta adreslerini toplayan Truva atları	Bir bilgisayarda saklanan e-posta adreslerini toplar ve bunları saldırgana e-posta, FTP, saldırganın İnternet sayfasına erişim veya başka bir yolla gönderir. Saldırganlar, toplanan adreslere spam gönderebilir.

- **Zararlı araçlar**;

  Alt kategori: Zararlı araçlar

  Tehlike düzeyi: Orta

  Zararlı yazılımların diğer türlerinden farklı olarak zararlı araçlar başlatıldıktan hemen sonra eylemlerini gerçekleştirmez. Güvenle saklanabilir ve kullanıcının bilgisayarında başlatılır. Saldırganlar genellikle virüs, solucan ve Truva atı oluşturmak, ağ saldırılarını uzak sunucularda gerçekleştirmek, bilgisayarları hacklemek veya diğer zararlı eylemleri gerçekleştirmek için bu programların özelliklerini kullanır.

  Zararlı araçların çeşitli özellikleri, aşağıdaki tabloda açıklanan türlere göre gruplandırılmıştır.

  Zararlı araçların özellikleri

Tür	Ad	Açıklama
Constructor	Oluşturucular	Yeni virüsler, solucanlar ve Truva atları oluşturmaya izin verir. Bazı oluşturucular, oluşturulacak zararlı uygulamanın türünün, hata ayıklayıcıları önleme biçiminin ve diğer özelliklerin kullanıcılar tarafından seçilebildiği standart bir pencere tabanlı arabirime sahiptir.
DoS	Ağ saldırıları	Kullanıcı bilgisayarından uzaktaki bir sunucuya çok sayıda istek gönderirler. Sunucunun tüm istekleri işlemek için yeterli kaynağı bulunmamaktadır; bu nedenle çalışmayı durdurur (Hizmet Reddi veya yalnızca DoS).
Exploit	Açık bırakıcılar	Bir *açık bırakıcı*, işlendiği uygulamanın zayıf noktalarını kullanan veri seti veya program kodudur ve bilgisayarda kötü amaçlı eylemler gerçekleştirir. Örneğin, bir açık bırakıcı dosyaları yazabilir veya okuyabilir ya da "virüslü" İnternet sayfalarını isteyebilir. Farklı açık bırakıcılar, farklı uygulamalar veya ağ hizmetlerinde zayıf noktaları kullanır. Ağ paketi olarak gizlenmiş bir açık bırakıcı ağ üzerinden çok sayıda bilgisayara iletilir, hassas ağ hizmetlerine sahip bilgisayarları arar. Bir DOC dosyasında bulunan açık bırakıcı bir metin düzenleyicinin zayıf noktalarını kullanır. Kullanıcı virüslü dosyayı açtığında hacker tarafından önceden programlanmış eylemleri gerçekleştirmeye başlayabilir. Bir e-posta mesajında gömülü olan bir açık bırakıcı herhangi bir e-posta istemcisindeki zayıf noktaları arar. Kullanıcı bu e-posta istemcisindeki virüslü mesajı açar açmaz kötü amaçlı bir eylemi gerçekleştirmeye başlayabilir. Net-Solucanları, açık bırakıcıları kullanarak ağlara yayılırlar. Nuke atıcı açık bırakıcıları, bilgisayarları devre dışı bırakan ağ paketleridir.
FileCryptor	Şifreleyiciler	Anti virüs uygulamasından gizlemek için diğer zararlı uygulamaları şifrelerler.
Flooder	"Kirleten" ağlar için programlar	Ağ kanalları üzerinden çok sayıda mesaj gönderir. Bu tür araçlar, İnternet Bağlantılı Sohbetleri kirleten programları içerir. Bombacı tipteki araçlar, e-postalar, Anlık ileti uygulamaları ve mobil iletişim sistemleri tarafından kullanılan kanalları "kirleten" programları içermez. Bu programlar, tabloda açıklanan farklı türler olarak ayrılırlar (Email-Flooder, IM-Flooder, ve SMS-Flooder).
HackTool	Saldırı araçları	Yüklendikleri bilgisayarlara veya başka bilgisayarlara saldırmayı mümkün kılar (örneğin, kullanıcının izni olmadan yeni sistem hesapları ekleyerek veya işletim sistemindeki varlıklarının izini gizlemek için sistem kayıtlarını silerek). Bu tür araçlar, parola ele geçirme gibi zararlı işlevlerin özelliğindeki bazı dinleyicileri içerir. Dinleyiciler, ağ trafiğinin görüntülenmesine olanak tanıyan programlardır.
Hoax	Asılsız uyarılar	Bunlar kullanıcıyı virüs benzeri mesajlarla uyarırlar: virüslü olmayan bir dosyada "bir virüs tespit edebilirler" veya kullanıcıya, gerçekte olmadığı halde, sürücünün biçimlendirildiği bildiriminde bulunurlar.
Spoofer	Aldatma araçları	Göndericinin sahte bir adresini içeren mesajlar ve ağ istekleri gönderir. Saldırganlar, Aldatıcı türü araçları örneğin kendilerini mesajların gerçek göndericisiymiş süsü vermek için kullanır.
VirTool	Zararlı uygulamaları değiştiren araçlar	Diğer kötü amaçlı programların değiştirilmesine olanak tanır ve kötü amaçlı programları anti-virüs uygulamalarından gizler.
Email-Flooder	E-posta adreslerini "kirleten" programlardır	Çeşitli e-posta adreslerine çok sayıda mesaj gönderirler, böylece söz konusu adresleri "kirletirler". Büyük miktardaki gelen mesaj, kullanıcının gelen kutusunda faydalı mesajları görmesine engel olur.
IM-Flooder	Anlık ileti uygulamalarının trafiğini "kirleten" programlar	Anlık ileti uygulamalarının kullanıcılarını mesajlarla bombalar. Büyük miktardaki mesajlar, kullanıcının faydalı gelen mesajları görmesine engel olur.
SMS-Flooder	SMS mesajlarıyla trafiği "kirleten" programlar	Cep telefonlarına çok sayıda SMS mesajları gönderir.

- **Reklam yazılımı**

  Alt kategori: Reklam yazılımı (Reklam Yazılımı);

  Tehlike düzeyi: Orta

  Reklam yazılımı, kullanıcıya reklam bilgilerini gösterir. Reklam yazılımı programları, diğer programların arabiriminde reklam penceresi görüntüler ve arama sorgularını reklam İnternet sayfalarına yönlendirir. Bunlardan bazıları, kullanıcı hakkında pazarlama bilgileri toplar ve geliştiriciye gönderir: bu bilgiler kullanıcının ziyaret ettiği İnternet sitelerinin adlarını ve kullanıcının arama sorgularının içeriğini kapsar. Truva atı-Casus türü programlardan farklı olarak, reklam yazılımları bu bilgileri geliştiriciye kullanıcının izni ile gönderir.

- **Otomatik çeviriciler**

  Alt kategori: İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım içeriyor.

Tehlike düzeyi: Orta

Bu uygulamaların çoğu faydalıdır, bu yüzden çoğu kullanıcı bunları çalıştırır. Bu uygulamalar IRC istemcilerini, otomatik çeviricileri, dosya indirme programlarını, bilgisayar sistem etkinliği ekranlarını, parola özelliklerini ve FTP, HTTP ve Telnet için İnternet sunucularını içerir.

Bununla birlikte, saldırganlar bu programlara erişim kazanırsa veya kullanıcının bilgisayarına yerleştirirse uygulamanın özelliklerinin bazıları güvenlik ihlali için kullanılabilir.

Bu uygulamalar işleve göre farklılık gösterebilir; türleri aşağıdaki tabloda açıklanmıştır.

Tür	Ad	Açıklama
Client-IRC	İnternet sohbeti istemcileri	Kullanıcılar bu programları İnternet Bağlantılı Sohbetlerde insanlarla konuşmak için yükler. Saldırganlar bunları zararlı yazılımları yaymak için kullanır.
Downloader	İndirilecek programlar	İnternet sayfalarından programları gizli modda indirir.
Monitor	İzleme programları	Bunlar, yüklendikleri bilgisayarla ilgili etkinlik izlemeye olanak tanır (hangi uygulamaların etkin olduğunu ve diğer bilgisayarlara yüklü uygulamalarla nasıl veri alışverişi yapıldığını görürler).
PSWTool	Parola geri yükleyiciler	Unutulan parolaların görüntülenmesine ve yeniden yüklenmesine olanak tanır. Saldırganlar, aynı amaçla bunları kullanıcının bilgisayarına gizlice yerleştirir.
RemoteAdmin	Uzaktan yönetim programları	Çoğunlukla sistem yöneticileri tarafından kullanılır. Bu programlar, izlemek ve yönetmek için uzak bilgisayarın arabirimine erişim elde etmeye olanak tanır. Saldırganlar, uzak bilgisayarları izlemek ve yönetmek amacıyla bunları kullanıcının bilgisayarına yerleştirir. Yasal uzaktan yönetim programları, uzaktan yönetim için arkak apı türü Truva atlarından farklıdır. Truva atları işletim sistemlerine bağımsız olarak girme ve kendilerini yükleme kabiliyetine sahiptirler: yasal programlar bunu gerçekleştiremez.
Server-FTP	FTP sunucuları	FTP sunucuları olarak işlev gösterir. Saldırganlar, FTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Server-Proxy	Proxy sunucular	Proxy sunucuları olarak işlev gösterir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
Server-Telnet	Telnet sunucuları	Telnet sunucuları olarak işlev gösterir. Saldırganlar, Telnet aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Server-Web	İnternet sunucuları	İnternet sunucuları olarak işlev gösterir. Saldırganlar, HTTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
RiskTool	Yerel bir bilgisayarda çalışmak için araçlar	Kullanıcının kendi bilgisayarında çalışırken kullanıcıya ek seçenekler sağlar. Araçlar kullanıcıya etkin uygulamaların dosyalarını veya pencerelerini gizleme olanağı tanır ve etkin işlemleri sonlandırır.
NetTool	Ağ araçları	Kullanıcıya ağdaki başka bilgisayarla çalışırken ek seçenekler sunar. Bu araçlar, yeniden başlatmaya, açık portları tespit etmeye ve bilgisayarda yüklü uygulamaları başlatmaya olanak tanır.
Client-P2P	P2P ağ istemcileri	Eşdüzey ağlarda çalışmaya olanak tanır. Saldırganlar tarafından zararlı yazılımların yayılması için kullanılır.
Client-SMTP	SMTP istemcileri	Kullanıcının bilgisi olmadan e-posta mesajları gönderir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
WebToolbar	İnternet Araç çubukları	Arama motorlarını kullanmak için araç çubuklarını diğer uygulamaların arabirimlerine ekler.
FraudTool	Sahte programlar	Kendilerine başka program süsü verir. Örneğin, zararlı yazılımların tespit edilmeleri hakkında mesajlar görüntüleyen sahte anti-virüs programları vardır. Bununla birlikte, gerçekte herhangi bir şey bulamazlar veya temizleyemezler.

- **İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım**

  Alt kategori: İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım içeriyor.

  Tehlike düzeyi: Orta

  Bu uygulamaların çoğu faydalıdır, bu yüzden çoğu kullanıcı bunları çalıştırır. Bu uygulamalar IRC istemcilerini, otomatik çeviricileri, dosya indirme programlarını, bilgisayar sistem etkinliği ekranlarını, parola özelliklerini ve FTP, HTTP ve Telnet için İnternet sunucularını içerir.

  Bununla birlikte, saldırganlar bu programlara erişim kazanırsa veya kullanıcının bilgisayarına yerleştirirse uygulamanın özelliklerinin bazıları güvenlik ihlali için kullanılabilir.

  Bu uygulamalar işleve göre farklılık gösterebilir; türleri aşağıdaki tabloda açıklanmıştır.

Tür	Ad	Açıklama
Client-IRC	İnternet sohbeti istemcileri	Kullanıcılar bu programları İnternet Bağlantılı Sohbetlerde insanlarla konuşmak için yükler. Saldırganlar bunları zararlı yazılımları yaymak için kullanır.
Downloader	İndirilecek programlar	İnternet sayfalarından programları gizli modda indirir.
Monitor	İzleme programları	Bunlar, yüklendikleri bilgisayarla ilgili etkinlik izlemeye olanak tanır (hangi uygulamaların etkin olduğunu ve diğer bilgisayarlara yüklü uygulamalarla nasıl veri alışverişi yapıldığını görürler).
PSWTool	Parola geri yükleyiciler	Unutulan parolaların görüntülenmesine ve yeniden yüklenmesine olanak tanır. Saldırganlar, aynı amaçla bunları kullanıcının bilgisayarına gizlice yerleştirir.

RemoteAdmin	Uzaktan yönetim programları	Çoğunlukla sistem yöneticileri tarafından kullanılır. Bu programlar, izlemek ve yönetmek için uzak bilgisayarın arabirimine erişim elde etmeye olanak tanır. Saldırganlar, uzak bilgisayarları izlemek ve yönetmek amacıyla bunları kullanıcının bilgisayarına yerleştirir. Yasal uzaktan yönetim programları, uzaktan yönetim için arkak apı türü Truva atlarından farklıdır. Truva atları işletim sistemlerine bağımsız olarak girme ve kendilerini yükleme kabiliyetine sahiptirler: yasal programlar bunu gerçekleştiremez.
Server-FTP	FTP sunucuları	FTP sunucuları olarak işlev gösterir. Saldırganlar, FTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Server-Proxy	Proxy sunucular	Proxy sunucuları olarak işlev gösterir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
Server-Telnet	Telnet sunucuları	Telnet sunucuları olarak işlev gösterir. Saldırganlar, Telnet aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Server-Web	İnternet sunucuları	İnternet sunucuları olarak işlev gösterir. Saldırganlar, HTTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
RiskTool	Yerel bir bilgisayarda çalışmak için araçlar	Kullanıcının kendi bilgisayarında çalışırken kullanıcıya ek seçenekler sağlar. Araçlar kullanıcıya etkin uygulamaların dosyalarını veya pencerelerini gizleme olanağı tanır ve etkin işlemleri sonlandırır.
NetTool	Ağ araçları	Kullanıcıya ağdaki başka bilgisayarla çalışırken ek seçenekler sunar. Bu araçlar, yeniden başlatmaya, açık portları tespit etmeye ve bilgisayarda yüklü uygulamaları başlatmaya olanak tanır.
Client-P2P	P2P ağ istemcileri	Eşdüzey ağlarda çalışmaya olanak tanır. Saldırganlar tarafından zararlı yazılımların yayılması için kullanılır.
Client-SMTP	SMTP istemcileri	Kullanıcının bilgisi olmadan e-posta mesajları gönderir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
WebToolbar	İnternet Araç çubukları	Arama motorlarını kullanmak için araç çubuklarını diğer uygulamaların arabirimlerine ekler.
FraudTool	Sahte programlar	Kendilerine başka program süsü verir. Örneğin, zararlı yazılımların tespit edilmeleri hakkında mesajlar görüntüleyen sahte anti-virüs programları vardır. Bununla birlikte, gerçekte herhangi bir şey bulamazlar veya temizleyemezler.

- **Paketlemesi, kötü amaçlı kodu korumak için kullanılabilecek paketlenmiş nesneler**;

  Alt kategori: Zarar verebilecek paketlenmiş dosyalar.

  Tehlike düzeyi: orta.

  Dosya, kötü amaçlı yazılımları paketlemek için kullanılan özel bir paketleyici kullanılarak paketlenir: virüsler, solucanlar, Truva atları. Kaspersky Endpoint Security, SFX (kendi başına açılan) arşivlerindeki paket açıcı modülünü tarar.

  Bilgisayar korsanları, kötü amaçlı yazılımları antivirüs tarafından tespit edilmekten gizlemek için özel paketleyiciler kullanarak paketlemektedir. Kaspersky uzmanları bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

- **Çoklu paketlenmiş nesneler**.

  Alt kategori: Zarar verebilecek paketlenmiş dosyalar.

  Tehlike düzeyi: orta.

  Dosya, kötü amaçlı yazılımları paketlemek için kullanılan özel bir paketleyici kullanılarak paketlenir: virüsler, solucanlar, Truva atları. Kaspersky Endpoint Security, SFX (kendi başına açılan) arşivlerindeki paket açıcı modülünü tarar.

  Bilgisayar korsanları, kötü amaçlı yazılımları antivirüs tarafından tespit edilmekten gizlemek için özel paketleyiciler kullanarak paketlemektedir. Kaspersky uzmanları bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

İstisnalar

Bu tablo, tarama istisnaları hakkında bilgi içerir.

> Mutlak yollar yerine göreceli yollar belirtmenizi öneririz. Bu, yalnızca dosya sistemi nesnelerini değil, dosyasız nesneleri de dışarıda tutmayı sağlar. Örneğin, `*\Program Files (x86)\Folder\Subfolder`.

Aşağıdaki yöntemleri kullanarak nesneleri taramaların dışında tutabilirsiniz:

- Dosyanın veya klasörün yolunu belirtmek.
- Nesne karmasını girmek.
- Maskeler kullanarak:
  - `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `*` (yıldız) karakteri. Örneğin, `C:\*\*.txt` maskesi, alt klasörler hariç C: sürücüsündeki klasörlerde bulunan TXT uzantılı tüm dosya yollarını içerir.
  - İki ardışık `*` karakteri, `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) dahil olmak üzere dosya veya klasör adındaki (boş küme dahil) herhangi bir karakter kümesinin yerine geçer. Örneğin `C:\Folder\**\*.txt` maskesi, `Folder` adlı klasörün kendisi hariç olmak üzere tüm `Folder` alt klasörlerinde bulunan TXT uzantılı tüm dosya yollarını içerir. Maske en az bir iç içe yerleştirme düzeyi içermelidir. `C:\**\*.txt` maskesi geçerli bir maske değildir.

- `\` ve `/` karakterleri (dosya ve klasör yollarında dosya ve klasörlerin ad sınırlayıcıları) hariç olmak üzere herhangi bir karakter kümesinin yerine geçen `?` (soru işareti) karakteri. Örneğin `C:\Folder\???.txt` maskesi, `Folder` isimli klasörde yer alan ve hem TXT uzantısına hem de üç karaktere sahip olan tüm dosya yollarını içerir.

  Maskeleri bir dosya veya klasör yolunda herhangi bir yerde kullanabilirsiniz. Örneğin, tarama kapsamının bilgisayardaki tüm kullanıcı hesapları için İndirilenler klasörünü içermesini istiyorsanız, `C:\Users\*\Downloads\` maskesini girin.

  Kaspersky Endpoint Security ortam değişkenlerini destekler

  > Kaspersky Endpoint Security, Kaspersky Security Center konsolunda bir istisnalar listesi listesi oluştururken `%userprofile%` ortam değişkenini desteklemez. Girişi tüm kullanıcı hesaplarına uygulamak için * karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

- Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Email-Worm`, `Rootkit` veya `RemoteAdmin`). Maskeleri `?` karakteri (herhangi bir tek karakteri değiştirir) ve `*` karakteri ile (herhangi bir sayıda karakteri değiştirir) kullanabilirsiniz. Örneğin, `Client*` maskesi belirtilirse, uygulama `Client-IRC`, `Client-P2P` ve `Client-SMTP` nesnelerini taramaların dışında tutar.

> Kaspersky Endpoint Security, tarama istisnalarının yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel tarama istisnaları yasaklanmışsa (**Yerel istisnaların kullanılmasına izin ver** onay kutusunun işareti kaldırılmışsa) uygulamanın kullanıcı arabirimindeki tarama istisnaları listesini gizler.

Güvenilir uygulamalar

Bu tabloda, çalışması sırasında Kaspersky Endpoint Security tarafından etkinlikleri izlenmeyen güvenilir uygulamalar listelenir.

Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

> Kaspersky Endpoint Security, Kaspersky Security Center konsolunda bir güvenilir uygulamalar listesi oluştururken `%userprofile%` ortam değişkenini desteklemez. Girişi tüm kullanıcı hesaplarına uygulamak için * karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

Uygulama Denetimi bileşeni, uygulamanın güvenilir uygulamalar tablosunda bulunup bulunmadığına bakılmaksızın her uygulamanın başlatılmasını düzenler.

> Kaspersky Endpoint Security, güvenilir uygulamaların yapılandırılması yönetici tarafından konsolda engellenmişse ("kapalı kilit" simgesi) ve yerel güvenilir uygulamalar yasaklanmışsa (**Yerel güvenilir uygulamaların kullanımına izin ver** onay kutusunun işareti kaldırılmışsa), uygulamanın kullanıcı arabirimindeki birleştirilmiş güvenilir uygulamalar listesini gizler.

Devralırken değerleri birleştir

(sadece Kaspersky Security Center Konsolunda mevcuttur)

Bu, Kaspersky Security Center'ın üst ve alt ilkelerindeki tarama istisnaları ve güvenilir uygulamalar listesini birleştirir. Listeleri birleştirmek için, alt ilke, Kaspersky Security Center'ın üst ilkesinin ayarlarını devralacak şekilde yapılandırılmalıdır.

Onay kutusu seçiliyse, Kaspersky Security Center üst ilkesindeki liste öğeleri alt ilkelerde görüntülenir. Bu şekilde, örneğin, tüm kuruluş için birleştirilmiş bir güvenilir uygulamalar listesi oluşturabilirsiniz.

Bir alt ilkedeki devralınan liste öğeleri silinemez veya düzenlenemez. Tarama istisnaları listesindeki öğeler ve devralma sırasında birleştirilen güvenilir uygulamalar listesi, yalnızca üst ilkede silinebilir ve düzenlenebilir. Daha düşük düzey alt ilkelerdeki liste öğelerini ekleyebilir, düzenleyebilir veya silebilirsiniz.

Alt ve üst ilke listelerindeki öğeler eşleşirse, bu öğeler üst ilkenin aynı öğesi olarak görüntülenir.

Onay kutusu seçilmezse, Kaspersky Security Center ilkelerinin ayarlarını devralırken liste öğeleri birleştirilmez.

Bu işlevsellik aynı zamanda ilke profillerindeki listelerin birleştirilmesine de olanak tanır. Listeleri birleştirmek için, en yüksek öncelikli profilde, ayarların daha düşük öncelikli bir profilden devralınmasını etkinleştirin. İlke profili öncelikleri hakkında daha fazla ayrıntı için lütfen Kaspersky Security Center Yardımı 'na başvurun.

Yerel istisnaların kullanılmasına izin ver/Yerel güvenilir uygulamaların kullanımına izin ver

(sadece Kaspersky Security Center Konsolunda mevcuttur)

Yerel istisnalar ve yerel güvenilir uygulamalar (yerel güvenilen bölge) - belirli bir bilgisayar için Kaspersky Endpoint Security'de bulunan nesnelerin ve uygulamaların kullanıcı tanımlı listesi. Kaspersky Endpoint Security, yerel güvenilir bölgedeki nesneleri ve uygulamaları izlemez. Bu şekilde, kullanıcılar bir ilkedeki genel güvenilen bölgeye ek olarak kendi yerel istisnalar ve güvenilir uygulamalar listelerini oluşturabilir.

Onay kutusu seçiliyse, bir kullanıcı yerel bir tarama istisnaları listesi ve yerel bir güvenilir uygulamalar listesi oluşturabilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan tarama istisnaları ve güvenilir uygulamaların genel listelerine erişebilir.

EDR (KATA) / NDR (KATA) telemetri *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu tablo, EDR telemetri istisnaları hakkında bilgi içerir.
KUMA telemetrisi *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Kaspersky Unified Monitoring and Analysis Platform (KUMA) platformuna gönderilecek olayların listesi. Kaspersky Endpoint Security şu modlarda çalışır: • **Tüm olayları gönder**. Bu modda, uygulama, istisna kurallarına eklenen olaylar hariç, Windows günlüğündeki tüm olayları gönderir. • **Yalnızca seçilen etkinlikleri gönder**. Bu modda, uygulama yalnızca dahil etme kurallarına eklenen olayları gönderir.
Güvenilir sistem sertifika deposu	Güvenilir sistem sertifika depolarından biri seçilirse, Kaspersky Endpoint Security, güvenilir bir dijital imza ile imzalanmış uygulamaları taramaların dışında bırakır. Kaspersky Endpoint Security, bu tür uygulamaları otomatik olarak **Güvenilir** gruba atar. **Kullanma** seçilirse, Kaspersky Endpoint Security uygulamaları dijital imzaları olup olmadığına bakılmaksızın tarar. Kaspersky Endpoint Security bir uygulamayı bir güven grubuna, bu uygulamanın bilgisayar için oluşturduğu tehdidin seviyesine göre yerleştirir.

Uygulama Ayarları

Uygulamanın aşağıdaki genel ayarlarını yapılandırabilirsiniz:

- İşletim modu
- Kendini Koruma
- Performans
- Hata ayıklama bilgileri
- Ayarlar uygulandığında bilgisayarın durumu

Uygulama Ayarları

Parametre	Açıklama
Uygulamayı bilgisayar başlangıcında çalıştır (önerilir)	Bu seçenek belirlendiğinde, Kaspersky Endpoint Security işletim sistemi yüklendikten sonra başlatılır ve tüm oturum boyunca bilgisayarı korur. Bu seçenek devre dışı bırakıldığında, Kaspersky Endpoint Security işletim sistemi yüklendikten sonra kullanıcı manuel olarak başlatana kadar başlatılmaz. Bilgisayar koruması devre dışı olur ve kullanıcı verileri tehditlere maruz kalabilir.
Gelişmiş Temizleme teknolojisini kullan (ciddi düzeyde bilgisayar kaynağı gerektirir)	Genellikle Kaspersky Endpoint Security, bilgisayara virüs bulaşmadan önce tespit edilen kötü amaçlı yazılımları sonlandırır. Gelişmiş Temizleme Teknolojisi bilgisayarı halihazırda aktif olan kötü amaçlı yazılımlardan (aktif enfeksiyon) korur, böylece veri kaybı ve tehdidin yayılma riskini en aza indirir. Bu teknoloji etkinleştirilirse, kötü amaçlı etkinlik algılandığında Kaspersky Endpoint Security bir açılır bildirim görüntüler. Kaspersky Endpoint Security bildirimde kullanıcıya bilgisayarın Gelişmiş Virüs Temizleme işlemini gerçekleştirme seçeneği sunar. Kullanıcının bu işlemi onaylamasından sonra, Kaspersky Endpoint Security tehdidi etkisiz duruma getirir ve ardından bilgisayarı yeniden başlatır. Gelişmiş temizleme teknolojisi, oldukça fazla bilgisayar kaynağı kullanır, bu da diğer uygulamaları yavaşlatabilir. Uygulama etkin bir virüs bulaşması algılama sürecindeyken, işletim sisteminin bazı işlevleri kullanılamayabilir. Gelişmiş Temizleme tamamlandığında ve bilgisayar yeniden başlatıldığında işletim sistemi eski durumuna döner. Kaspersky Endpoint Security, Windows for Servers çalıştıran bir bilgisayarda yüklüyse Kaspersky Endpoint Security bildirimi görüntülemez. Bu nedenle, etkin bir tehdidi temizlemek için bir eylem seçemezsiniz. Bir tehdidi temizlemek için uygulama ayarlarından Gelişmiş Temizleme teknolojisini etkinleştir ve *Kötü Amaçlı Yazılım Taraması* görev ayarlarından Gelişmiş Temizlemeyi derhal çalıştır seçimini yapın. Ardından *Kötü Amaçlı Yazılım Taraması* görevini başlatmalısınız.

Parametre	Açıklama
Etkinleştirme için proxy sunucusu olarak Kaspersky Security Center'ı kullan *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu onay kutusu işaretlenirse, uygulama Kaspersky Security Center Yönetim Sunucusu'nu etkinleştirme sunucularına bağlanmak için bir proxy sunucusu olarak kullanır. Bu, uygulamayı internet erişimi olmayan yalıtılmış bir ağ segmentinde etkinleştirmek için bir etkinleştirme kodu kullandığınızda gereklidir. Uygulamayı bir anahtar dosyası ile etkinleştiriyorsanız, internet erişimi gerekli değildir.
Kendini Korumayı Etkinleştir	Bu işlev etkinleştirildiğinde, Kaspersky Endpoint Security, sabit sürücüdeki uygulama dosyalarının, bellek işlemlerinin ve sistem kayıt defterindeki girdilerin değiştirilmesini veya silinmesini önler.
Uygulama hizmetlerinin harici yönetimini engelle	Bu işlev etkinleştirildiğinde, Kaspersky Endpoint Security, üçüncü taraf uygulamaları (CMD gibi) kullanarak uygulama hizmetlerinin yönetilmesine izin vermez. Üçüncü taraf uygulamalar kullanılarak uygulama hizmetleri yönetilmeye çalışıldığında, Microsoft Windows görev çubuğunda uygulama simgesinin üzerinde bir bildirim görüntülenir (bildirim hizmeti kullanıcı tarafından devre dışı bırakılmamışsa). Uygulama hizmetlerinin dış yönetimine yalnızca AM-PPL teknolojisini desteklemeyen bilgisayarlarda veya teknolojinin devre dışı bırakıldığı bilgisayarlarda izin verebilirsiniz.
Pil gücüyle çalışırken zamanlanmış görevleri ertele	Onay kutusu işaretlendiğinde, bilgisayar pil gücüyle çalışırken güç tasarrufu modu etkinleştirilir. Kaspersky Endpoint Security, zamanlanmış görevleri erteler. Gerekirse bir taramayı ve güncelleme görevlerini manuel olarak başlatabilirsiniz. Güç tasarrufu modu etkinleştirildiğinde ve bilgisayar pil gücüyle çalışırken, aşağıdaki görevler zamanlanmış olsa bile çalıştırılmaz: • *Tam Tarama*. • *Kritik Alanları Tarama*. • *Özel Tarama*. • *Uygulama Bütünlüğü Kontrolü*. • *IOC Taraması* • *Veritabanlarının ve uygulama modüllerinin güncellemesi* (sadece yamalar) Uygulama, yalnızca dizüstü bilgisayar pil ile çalışırken ve pil seviyesi %30'un (varsayılan değer) altında olduğunda planlanmış veritabanı güncellemelerini atlar. Kayıt defterini düzenleyerek uygulamanın planlanmış antivirüs veritabanı güncellemelerini atlamaya başladığı minimum pil şarj seviyesini değiştirebilirsiniz. Diğer tüm durumlarda, Kaspersky Endpoint Security, dizüstü bilgisayarın şarja bağlı ya da pil ile çalışıyor olmasına veya uygulamanın güç tasarrufu modunda olup olmamasına bakılmaksızın, veritabanlarını zamanlamaya göre günceller.
Kaynakları diğer uygulamalara bırak	Bir bilgisayarı tararken Kaspersky Endpoint Security tarafından bilgisayar kaynaklarının tüketilmesi, CPU ve sabit sürücü alt sistemleri üzerindeki yükü artırabilir. Bu diğer uygulamaları yavaşlatabilir. Kaspersky Endpoint Security, performansı optimize etmek için bir *kaynakları diğer uygulamalara aktarma modu* sunar. Bu modda, işletim sistemi CPU yükü yüksek olduğunda Kaspersky Endpoint Security tarama görevi iş parçacıklarının önceliğini düşürebilir. Bu, işletim sistemi kaynaklarının diğer uygulamalara yeniden dağıtılmasını sağlar. Böylece tarama görevleri daha az CPU süresi almış olur. Sonuç olarak, Kaspersky Endpoint Security'nin bilgisayarı taraması daha uzun sürer. Varsayılan olarak uygulama, kaynakları diğer uygulamalara bırakacak şekilde yapılandırılmıştır.
Tarama görevleri için işlemci kullanımını sınırla	Kaspersky Endpoint Security performansını optimize etmek için *Kötü Amaçlı Yazılım Taraması* görevi aracılığıyla işlemci kullanımını sınırlayabilirsiniz. Onay kutusu seçilirse, *Kötü Amaçlı Yazılım Taraması* görevinin tüm işlemci çekirdekleri üzerindeki ortalama yük belirtilen değere yaklaşır. Varsayılan olarak, onay kutusu temizlenmiştir.
Döküm yazımını etkinleştir	Onay kutusu işaretlenirse Kaspersky Endpoint Security çöktüğünde dökümler yazılır. Onay kutusu işaretlenmezse Kaspersky Endpoint Security dökümleri yazmaz. Uygulama ayrıca mevcut döküm dosyalarını bilgisayarın sabit sürücüsünden siler.
Bellek dökümü ve iz dosyaları korumasını etkinleştir	Bu onay kutusu işaretlenirse döküm dosyalarına erişim izni, sistem yöneticisi ve yerel yöneticiyle birlikte döküm dosyası yazmayı etkinleştiren kullanıcıya da verilir. İz dosyalarına yalnızca sistem ve yerel yöneticiler tarafından erişilebilir. Onay kutusu işaretlenmezse herhangi bir kullanıcı döküm dosyalarına ve iz dosyalarına erişebilir.
Ayarlar uygulandığında bilgisayarın durumu *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bir ilkeyi uygularken veya görevi gerçekleştirirken hatalar oluştuğunda, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların durumlarını Web Console'da görüntüleme ayarları. Şu durumlar mevcuttur *Tamam*, *Uyarı* ve *Kritik*.

Parametre	Açıklama
Güncellemeleri bilgisayar yeniden başlatılmadan yükle	Uygulamayı bilgisayarı yeniden başlatmadan yükseltmek sunucuların kesintisiz çalışmasını garanti altına almanızı sağlar. 11.10.0 sürümünden itibaren, uygulamayı yeniden başlatma yapmadan yükseltebilirsiniz. Uygulamanın önceki bir sürümünü yükseltmek için bilgisayarı yeniden başlatmanız gerekir. 11.11.0 sürümünden başlayarak, bilgisayarı yeniden başlatmadan şu eylemleri gerçekleştirebilirsiniz: • Yamaları yükleme • Uygulama bileşenlerini değiştirme • Kaspersky Endpoint Security'yi Kaspersky Security for Windows Server üzerinden yükleme Parametrenin varsayılan değeri, işletim sisteminin türüne göre değişir. Uygulama bir iş istasyonuna kuruluysa uygulamayı yeniden başlatmadan yükseltme seçeneği devre dışı bırakılır. Uygulama bir sunucuda kuruluysa uygulamayı yeniden başlatmadan yükseltme seçeneği etkinleştirilir.
Uzaktan yönetim yazılımlarıyla uyumluluk *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Kaspersky Endpoint Security'yi Uzaktan Yönetim Araçları (RAT) ile birlikte kullanmak sorunlara neden oluyorsa uyumluluk modunu etkinleştirebilirsiniz. Sorunlar, RAT'lerin uygulamanın Secure Desktop işlevselliği ile uyumsuzluğu ile ilgili olabilir. Bu işlevin amacı, bilgisayarın güvenlik düzeyi potansiyel olarak düşürebilecek eylemleri onaylamaktır. Bu işlevsellik, bir uygulamanın diğer işlemlerden yalıtılmış bir onay iletişim kutusu görüntülemesini sağlar. Bu işlevsellik, isteği güvence altına almak için yükseltilmiş haklar kullanır. Bu şekilde, kötü amaçlı yazılım değil, yalnızca kullanıcı eylemi onaylayabilir. Bu seçenek seçilirse, RAT uyumluluk modu etkinleştirilir. Uygulama, bu işlevsellik olmadan bir onay iletişim kutusu görüntüler. Bu, bilgisayarın güvenlik düzeyini düşürebilir. Kaspersky Endpoint Security, RAT'ınızla ilgili sorunlara neden olmuyorsa uyumluluk modunu etkinleştirmenizi önermeyiz. Bu seçenek temizlenirse, RAT uyumluluk modu devre dışı bırakılır. Varsayılan olarak, onay kutusu temizlenmiştir. Örnek: Tarayıcıyı RemoteApp modunda kullanırken, Kaspersky Endpoint Security güvenilmez sertifikaya sahip bir web sitesini ziyaret ederken bir onay penceresi görüntülemeyebilir çünkü RemoteApp, uygulamanın Güvenli Masaüstü işlevini desteklemez. Bu, tarayıcının yanıt vermemesine neden olabilir. Tarayıcının RemoteApp modunda düzgün çalışması için uyumluluk modunu etkinleştirmeniz gerekir. Diğer üçüncü taraf yazılımları kullanırken Güvenli Masaüstü işlevselliği ile ilgili sorunlarla karşılaşırsanız uyumluluk modunu etkinleştirmeyi de deneyebilirsiniz.

Raporlar ve depolama

Raporlar

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, `C:\ProgramData\Kaspersky Lab\KES.14.2\Report` klasöründe saklanır.

Yedekle

Yedekleme depoları, temizleme esnasında silinen veya değiştirilen dosyaların yedek kopyalarını saklar. *Yedek kopya*, dosya temizlenmeden veya silinmeden önce oluşturulan bir dosya kopyasıdır. Dosyaların yedekleme kopyaları, özel bir biçimde saklanır ve bir tehdit oluşturmaz.

Dosyaların yedek kopyaları, `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` klasöründe saklanır.

Yönetici grubundaki kullanıcılara, bu klasör için tam erişim izni verilir. Hesabını Kaspersky Endpoint Security'yi yüklemek için kullanılan kullanıcıya, bu klasör için sınırlı erişim hakkı verilir.

Kaspersky Endpoint Security, dosyaların kopyalarının yedeklenmesine ilişkin kullanıcı erişim izinlerini yapılandırma özelliği sağlamaz.

Karantina

Karantina bilgisayardaki özel bir yerel depolama alanıdır. Kullanıcı, bilgisayar için tehlikeli olduğunu düşündüğü dosyaları karantinaya alabilir. Karantinaya alınan dosyalar şifrelenmiş bir durumda saklanır ve cihazın güvenliğini tehdit etmez. Kaspersky Endpoint Security, Karantinayı yalnızca Kaspersky Detection and Response çözümleriyle entegre edildiğinde kullanır. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantina'nın yönetimi hakkında ayrıntılar için lütfen Kaspersky Sandbox Yardım, Kaspersky Endpoint Detection and Response Optimum Yardım, Kaspersky Endpoint Detection and Response Expert Yardım, Kaspersky Anti Targeted Attack Platform Yardım ve Kaspersky Endpoint Detection and Response Expert (on-premises) Yardım belgelerine bakın.

Karantina yalnızca Web Console kullanılarak yapılandırılabilir. Karantinaya alınan nesneleri yönetmek (geri yükleme, silme, ekleme vb.) için Web Console'u da kullanabilirsiniz. Komut satırını kullanarak bilgisayarda yerel olarak nesneleri geri yükleyebilirsiniz.

Kaspersky Endpoint Security, dosyaları karantinaya almak için sistem hesabını (SYSTEM) kullanır.

Raporlar ve depolama alanı ayarları

Parametre	Açıklama
Raporları belirli bir zaman geçtikten sonra sil (gün)	Bu onay kutusu seçildiğinde maksimum raporlama depolama süresi tanımlanan zaman aralığı ile sınırlanır. Raporlar için varsayılan maksimum depolama süresi 30 gündür. Bu süre dolduktan sonra Kaspersky Endpoint Security, en eski kayıtları rapor dosyasından otomatik olarak siler.
Rapor dosyasının boyutunu şununla sınırla (MB)	Bu onay kutusu seçildiğinde maksimum rapor dosyası boyutu tanımlanan değerle sınırlanır. En büyük dosya boyutu varsayılan olarak 1024 MB'tır. Maksimum rapor dosyası boyutunu aşmamak için Kaspersky Endpoint Security, maksimum rapor dosyası boyutuna ulaşıldığında en eski kayıtları rapor dosyasından otomatik olarak siler.
Nesneleri belirli bir süre sonra sil (gün)	Bu onay kutusu seçildiğinde maksimum dosya depolama süresi tanımlanan zaman aralığı ile sınırlanır. Dosyalar için varsayılan maksimum depolama süresi 30 gündür. Maksimum depolama süresinin sona ermesinin ardından Kaspersky Endpoint Security, en eski dosyaları Yedekleme'den siler.
Yedekleme boyutunu şununla sınırla (MB)	Bu onay kutusu seçildiğinde maksimum depolama boyutu tanımlanan değerle sınırlanır. Varsayılan olarak, maksimum boyut 1024 MB'tır. Maksimum depolama boyutunu aşmamak için Kaspersky Endpoint Security, maksimum depolama dosyası boyutuna ulaşıldığında en eski dosyaları depolama alanından otomatik olarak siler.
Karantina boyutunu şununla sınırla	Bu onay kutusu seçildiğinde maksimum Karantina boyutu tanımlanan değerle sınırlanır. Varsayılan olarak, maksimum boyut 1024 MB'tır. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security *Karantina depolamasında yeterli alan yok* olayını Kaspersky Security Center'a gönderir ve olayı Windows Olay Günlüğünde yayınlar. Bu arada uygulama yeni nesneleri karantinaya almayı durdurur. Karantiyanı manuel olarak boşaltmanız gerekir.
Karantina depolamasının boyutu şu seviyeye ulaştığında bildirim yap (%)	Karantinanın eşik değeri. Örneğin, Karantina eşiğini %50 olarak ayarlayabilirsiniz. Karantina eşiğe ulaştığında, Kaspersky Endpoint Security ilgili olayı Kaspersky Security Center'a gönderir ve olayı Windows Olay Günlüğünde yayınlar. Bu arada uygulama yeni nesneleri karantinaya almaya devam eder.

Parametre	Açıklama
Yönetim Sunucusu'na veri aktarımı *(yalnızca Kaspersky Security Center'da mevcuttur)*	Yönetim Sunucusuna bilgilerinin aktarılması gereken istemci bilgisayarlardaki olayların kategorileri. Yönetim Sunucusu'ndaki disk alanını optimize etmek için bazı verilerin aktarımını devre dışı bırakabilirsiniz. Uygulama şu kategorilerdeki olayları gönderir: • **Karantina dosyaları hakkında**. Karantinaya alınan dosyaların listesini Kaspersky Security Center konsolunda **Gelişmiş** → **Veri havuzları** → **Karantina** klasöründe görüntüleyebilirsiniz. Kaspersky Endpoint Security, Karantinayı yalnızca Kaspersky Detection and Response çözümleriyle entegre edildiğinde kullanır. • **Yedekleme'deki dosyalar hakkında**. Yedeklemedeki dosyaların listesini Kaspersky Security Center konsolunda **Gelişmiş** → **Veri havuzları** → **Yedekleme** klasöründe görüntüleyebilirsiniz. • **İşlenmemiş dosyalar hakkında**. İşlenmemiş dosyaların listesini Kaspersky Security Center konsolunda **Gelişmiş** → **Veri havuzları** → **Etkin tehditler** klasöründe görüntüleyebilirsiniz. • **Yüklenmiş aygıtlar hakkında**. Bağlı cihazların listesini Kaspersky Security Center konsolunda **Gelişmiş** → **Veri havuzları** → **Donanım** klasöründe görüntüleyebilirsiniz. Cihazların listesi bilgisayar özelliklerinde ve Kaspersky Endpoint Security for Windows ilkesinde (**Aygıt Denetimi** bölümü) de mevcuttur. • **Başlatılmış uygulamalar hakkında**. Yürütülebilir dosyaların listesini Kaspersky Security Center konsolunda **Gelişmiş** → **Uygulama yönetimi** → **Yürütülebilir dosyalar** klasöründe görüntüleyebilirsiniz. Yürütülebilir dosyaların listesi bilgisayar özelliklerinde de mevcuttur. • **Dosya şifreleme hataları hakkında**. Dosya şifreleme hatalarının listesini Kaspersky Security Center konsolunda **Gelişmiş** → **Veri şifreleme ve koruma** → **Şifreleme olayları** klasöründe görüntüleyebilirsiniz. Hataların listesi bilgisayar özelliklerinde de bulunabilir. • **Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor**. Raporu Kaspersky Security Center konsolunda, **Raporlar** sekmesindeki **Yönetim Sunucusu** düğümünde görüntüleyebilirsiniz. Bu rapor, Kaspersky Endpoint Security for Windows ilke özelliklerinde de mevcuttur (**Uyarlamalı Anomali Denetimi** bölümü). • **Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor**. Raporu Kaspersky Security Center konsolunda, **Raporlar** sekmesindeki **Yönetim Sunucusu** düğümünde görüntüleyebilirsiniz. Bu rapor, Kaspersky Endpoint Security for Windows ilke özelliklerinde de mevcuttur (**Uyarlamalı Anomali Denetimi** bölümü). • **Bir tehdit geliştirme zinciri hakkında**. Algılama ayrıntılarını Kaspersky Security Center Web Console'da **İzleme** → **Uyarılar** bölümünde görüntüleyebilirsiniz. Tehdit geliştirme zinciri hakkındaki bilgiler Kaspersky Endpoint Detection and Response çözümleri tarafından kullanılır.

Ağ ayarları

İnternete bağlanmak ve antivirüs veritabanlarını güncellemek için kullanılan proxy sunucuyu yapılandırabilir, ağ portu izleme modunu seçebilir ve şifrelenmiş bağlantıları tarayacak şekilde ayarlayabilirsiniz.

Ağ seçenekleri

Parametre	Açıklama
Tarifeli bağlantılarda trafiği sınırlandır	Bu onay kutusu işaretlenirse uygulama, İnternet bağlantısının sınırlı olduğu durumlarda kendi ağ trafiğini azaltır. Kaspersky Endpoint Security, yüksek hızlı mobil İnternet bağlantılarını sınırlı bağlantı olarak, Wi-Fi bağlantılarını ise sınırsız bağlantı olarak tanımlar. Maliyete Duyarlı Ağ, Windows 8 veya üzerini çalıştıran bilgisayarlarda çalışır.
Web sayfalarıyla etkileşim için internet trafiğine komut yerleştir	Onay kutusu seçilirse, Kaspersky Endpoint Security web trafiğine web sayfası etkileşim betiği ekler. Bu komut dosyası, İnternet Denetimi bileşeninin düzgün çalışabilmesini sağlar. Komut dosyası, İnternet Denetimi olaylarının kaydını sağlar. Bu komut dosyası olmadan, kullanıcının İnternet etkinliği izlemeyi etkinleştiremezsiniz. Kaspersky uzmanları, İnternet Denetiminin doğru çalışmasını sağlamak için bu web sayfası etkileşim komut dosyasının trafiğe eklenmesini önermektedir.
Proxy sunucusu ayarları	İstemci bilgisayarların kullanıcılarının İnternet erişiminde kullanılan proxy sunucusunun ayarları. Kaspersky Endpoint Security, veritabanlarının ve uygulama modüllerinin güncellenmesi de dahil olmak üzere belirli koruma bileşenleri için bu ayarları kullanır. Kaspersky Endpoint Security, bir proxy sunucusunun otomatik olarak yapılandırılması için WPAD (İnternet Proxy Otomatik Bulma) iletişim kuralını kullanır. Proxy sunucusunun IP adresi bu iletişim kuralı kullanılarak belirlenemiyorsa uygulama, Microsoft Internet Explorer tarayıcı ayarlarında belirtilen proxy sunucusu adresini kullanır.
Yerel adresler için proxy sunucuyu devre dışı tut	Onay kutusu işaretlenirse Kaspersky Endpoint Security, paylaşılan klasörden güncelleme yaparken proxy sunucusu kullanmaz.

Parametre	Açıklama
Proxy sunucusu kimlik doğrulama ayarları	İnternet erişimi için proxy sunucusundaki uygulamanın kimliğini doğrulamak istiyorsanız, kullanıcının kimlik bilgilerini girmeniz gerekir. Kaspersky Endpoint Security, proxy sunucusunda otomatik kimlik doğrulamayı destekler. Otomatik kimlik doğrulama başarısız olursa, uygulama sizden kimlik bilgilerini girmenizi ister. **Kimlik doğrulama kullanma**. **NTLM kimlik doğrulaması**. Geçerli kullanıcı hesabıyla NTLM kimlik doğrulaması (varsayılan). **Kullanıcı adı ve parola ile NTLM kimlik doğrulaması**. Manuel olarak belirtilen kimlik bilgileriyle NTLM kimlik doğrulaması. **Kullanıcı adı ve parolası**. Manuel olarak belirtilen kimlik bilgileriyle kimlik doğrulama. **Otomatik kimlik doğrulama**. **Kerberos kimlik doğrulaması**. Geçerli kullanıcı hesabıyla Kerberos kimlik doğrulaması. Proxy sunucusu adresi için CNAME kayıtları kullanılırken Kerberos kimlik doğrulamasının düzgün çalışmasını sağlamak için, her bir CNAME kaydı için bir Hizmet İlkesi Adı (SPN) kaydetmeniz gerekir. **Kullanıcı adı ve parola ile Kerberos kimlik doğrulaması**. Manuel olarak belirtilen kimlik bilgileriyle Kerberos kimlik doğrulaması. Kerberos kimlik doğrulaması seçilirse, Kaspersky Endpoint Security, proxy sunucusu ayarlarına bağlı olarak Kerberos veya NTLM iletişim kuralını kullanarak kimlik doğrulaması gerçekleştirebilir.
İzlenen portlar	**Tüm ağ portlarını izle**. Bu ağ portu izleme modunda, koruma bileşenleri (Dosya Tehdidi Koruması, Web Tehdidi Koruması ve Posta Tehdidi Koruması), bilgisayarın tüm açık ağ portu aracılığıyla aktarılan veri akışlarını izler. **Yalnızca seçili ağ portlarını izle**. Bu ağ portu izleme modunda, koruma bileşenleri bilgisayarın seçilen portlarını ve seçilen uygulamaların ağ etkinliğini izler. E-posta ve ağ trafiğinin aktarımı için normalde kullanılan ağ portlarının listesi, Kaspersky uzmanlarının önerilerine göre yapılandırılmıştır. **Kaspersky tarafından önerilen listeden uygulamalar için tüm portları izle**. Bu, ağ portları Kaspersky Endpoint Security tarafından izlenen uygulamaların önceden tanımlanmış bir listesini kullanır. Örneğin, bu listede Google Chrome, Adobe Reader, Java ve diğer uygulamalar yer alır. **Belirtilen uygulamalar için tüm portları izle**. Bu, ağ portları Kaspersky Endpoint Security tarafından izlenen uygulamaların bir listesini kullanır.
Şifreli bağlantıları tarama	Kaspersky Endpoint Security, aşağıdaki protokoller üzerinden iletilen şifrelenmiş ağ trafiğini tarar: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security şu şifrelenmiş bağlantı tarama modlarını destekler: • **Şifrelenmiş bağlantıları tarama**. Kaspersky Endpoint Security, adresleri `https://` ile başlayan web sitelerinin içeriklerine erişmeyecektir. • **Koruma bileşenlerinden gelen talep üzerine şifrelenmiş bağlantıları tara**. Kaspersky Endpoint Security, şifrelenmiş trafiği sadece Web Tehdidi Koruması, Posta Tehdidi Koruması ve İnternet Denetimi bileşenleri tarafından istendiğinde tarayacaktır. • **Şifrelenmiş bağlantıları her zaman tara**. Kaspersky Endpoint Security şifrelenmiş ağ trafiğini, koruma bileşenleri devre dışı bırakılsa bile tarayacaktır. Kaspersky Endpoint Security, trafik taramanın devre dışı bırakıldığı güvenilir uygulamalar tarafından kurulan şifreli bağlantıları taramaz. Kaspersky Endpoint Security, önceden tanımlanmış güvenilir web siteleri listesinden şifrelenmiş bağlantıları taramaz. Önceden tanımlanmış güvenilir web siteleri listesi Kaspersky uzmanları tarafından oluşturulur. Bu liste, uygulamanın anti-virüs veritabanları ile güncellenir. Önceden tanımlanmış güvenilir web siteleri listesini yalnızca Kaspersky Endpoint Security arabiriminde görüntüleyebilirsiniz. Listeyi Kaspersky Security Center Konsolunda görüntüleyemezsiniz.

Parametre	Açıklama
Güvenilir kök sertifikaları	Güvenilir kök sertifikalarının listesi. Kaspersky Endpoint Security, örneğin yeni bir sertifikalandırma merkezi kullanılma almanız gerektiğinde, güvenilir kök sertifikalarını yüklemenize izin verir. Uygulama Kaspersky Endpoint Security sertifika deposuna bir sertifika eklemenize izin verir. Bu durumda, sertifika sadece Kaspersky Endpoint Security uygulaması için güvenilir kabul edilir. Başka bir deyişle, kullanıcı tarayıcıdaki yeni bir sertifika ile bir web sitesine erişim kazanabilir. Başka bir uygulamanın web sitesine erişim kazanmaya çalışması durumunda, bir sertifika sorunu nedeniyle bir bağlantı hatası alabilirsiniz. Sistem sertifika deposuna eklemek için Active Directory grubu ilkelerini kullanabilirsiniz.
Güvenilmeyen sertifikalı bir etki alanını ziyaret etme	• **İzin ver**. Kaspersky Endpoint Security güvenilir olmayan bir sertifikaya sahip bir etki alanını ziyaret ederken ağ bağlantısı kurulmasına izin verir. Kaspersky Endpoint Security, güvenilmeyen bir sertifikaya sahip bir etki alanını tarayıcıda açarken bir uyarı ve bu etki alanının ziyaret edilmesinin neden önerilmediğini gösteren bir HTML sayfası gösterir. Kullanıcı, talep edilen internet kaynağına erişim elde etmek için HTML uyarı sayfasındaki bağlantıya tıklayabilir. Eğer bir üçüncü taraf uygulaması veya hizmeti güvenilmez bir sertifikaya sahip bir etki alanıyla bağlantı kurarsa, Kaspersky Endpoint Security trafiği taramak için kendi sertifikasını oluşturur. Yeni ilke *Güvenilmez* durumuna sahiptir. Bu, üçüncü taraf uygulamasını güvenilmez bağlantı hakkında uyarmak için gereklidir, çünkü bu durumda HTML sayfası görüntülenemez ve bağlantı arka plan modunda kurulabilir. • **Engelle**. Kaspersky Endpoint Security güvenilir olmayan bir sertifikaya sahip bir etki alanını ziyaret ederken ağ bağlantısı kurulmasını engeller. Kaspersky Endpoint Security, güvenilmeyen bir sertifikaya sahip bir etki alanını tarayıcıda açarken bu etki alanının neden engellendiğini gösteren bir HTML sayfası gösterir.
Şifrelenmiş bağlantı tarama hatası olan bir etki alanını ziyaret etme	• **Engelle**. Bir şifreli bağlantıları tarama hatası meydana geldiğinde, Kaspersky Endpoint Security, ağ bağlantısını engeller. • **İzin ver ve etki alanını istisnalara ekle**. Şifreli bağlantıları tarama hatası oluştuğunda Kaspersky Endpoint Security, hatayla sonuçlanan etki alanını tarama hatası olan etki alanları listesine ekler ve bu etki alanı ziyaret edildiğinde şifrelenmiş ağ trafiğini izlemez. Şifreli bağlantılar tarama hatalarına sahip etki alanlarının bir listesini sadece uygulamanın yerel arabiriminde görüntüleyebilirsiniz. Listenin içeriğini temizlemek için **Engelle**'i seçin. Kaspersky Endpoint Security ayrıca şifrelenmiş bağlantıları tarama hatası için bir olay oluşturur.
SSL 2.0 bağlantılarını engelle	Onay kutusu işaretlendiğinde, uygulama SSL 2.0 iletişim kuralı üzerinden kurulmuş ağ bağlantılarını izler ve engeller. Onay kutusunun işareti kaldırıldığında, uygulama SSL 2.0 iletişim kuralı üzerinden kurulan ağ bağlantılarını engellemez. Ancak, uygulama bu iletişim kuralı üzerinden ağ trafiğini izlemez.
SSL 3.0 bağlantılarını engelle	Onay kutusu işaretlendiğinde, uygulama SSL 3.0 protokolü üzerinden kurulmuş ağ bağlantılarını engeller. Onay kutusunun işareti kaldırıldığında, uygulama SSL 3.0 iletişim kuralı üzerinden kurulan ağ bağlantılarını engellemez. Uygulama bu iletişim kuralı üzerinden ağ trafiğini izler. Uygulamanın tüm bileşenleri kısıtlama olmaksızın çalışır.
TLS 1.0 bağlantılarını engelle	Onay kutusu işaretlendiğinde, uygulama TLS 1.0 protokolü üzerinden kurulmuş ağ bağlantılarını engeller. Onay kutusunun işareti kaldırıldığında, uygulama TLS 1.0 iletişim kuralı üzerinden kurulan ağ bağlantılarını engellemez. Uygulama bu iletişim kuralı üzerinden ağ trafiğini izler. Uygulamanın tüm bileşenleri kısıtlama olmaksızın çalışır.
Şifrelenmiş bir bağlantının şifresini EV sertifikası kullanan web sitesiyle çöz	EV sertifikaları (Extended Validation Certificate), web sitelerinin gerçekliğini onaylar ve bağlantının güvenliğini artırır. Tarayıcılar, bir web sitesinin bir EV sertifikasına sahip olduğunu belirtmek için adres çubuğunda bir kilit simgesi görüntüler. Tarayıcılar ayrıca adres çubuğunu yeşil renkte de görüntüleyebilir. Bu kutucuk seçildiğinde, uygulama bir EV sertifikası kullanan web siteleriyle şifreli bağlantıların şifresini çözer ve izler. Bu kutucuğun işareti kaldırıldığında, uygulama HTTPS trafiğinin içeriğine erişemez. Bu nedenle, uygulama HTTPS trafiğini sadece web sitesi adresine göre izler, örneğin `https://bing.com`. EV sertifikasına sahip bir web sitesini ilk kez açıyorsanız, şifreli bağlantı bu kutucuğun işareti olup olmadığından bağımsız olarak çözülür.
Güvenilir adresleri yapılandır	Bu, Kaspersky Endpoint Security'nin ağ bağlantılarını taramadığı web adreslerinin bir listesini kullanır. Bu durumda, Kaspersky Endpoint Security, Web Tehdidi Koruması, Posta Tehdidi Koruması, İnternet Denetimi bileşenleri işlerini yaparken güvenilir internet adreslerinin HTTPS trafiğini taramaz. Bir etki alanı adı veya IP adresi girebilirsiniz. Kaspersky Endpoint Security alan adına maske girilmesi için `*` karakterini destekler. Kaspersky Endpoint Security, IP adresleri için `*` sembolünü desteklemez. Bir alt ağ maskesi kullanarak bir IP adresi aralığı seçebilirsiniz (örneğin, 198.51.100.0/24). Örnekler: • `domain.com` - kayıt şu adresleri içerir: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Kayıt, alt etki adlarını içermez (örneğin, `subdomain.domain.com`). • `subdomain.domain.com` – kayıt şu adresleri içerir: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Kayıt `domain.com` etki alanını içermez. • `*.domain.com` – kayıt şu adresleri içerir: `https://movies.domain.com`, `https://images.domain.com/page123`. Kayıt `domain.com` etki alanını içermez.
Güvenilir uygulamaları yapılandır	Çalışması sırasında Kaspersky Endpoint Security tarafından etkinlikleri izlenmeyen uygulamalar listesi. Kaspersky Endpoint Security'nin izlemeyeceği uygulama etkinliği türlerini seçebilirsiniz (örneğin ağ trafiğini tarama). Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

Parametre	Açıklama
Kendi sertifika deposuna sahip uygulamalarda şifrelenmiş bağlantıları taramak için şunu kullanın *(yalnızca Kaspersky Endpoint Security arabiriminde mevcuttur)*	Bu onay kutusu seçilirse uygulama, Mozilla Firefox tarayıcısında ve Thunderbird posta istemcisindeki şifrelenmiş trafiği tarar. Bazı sitelere HTTPS protokolü aracılığıyla erişim engellenebilir. Mozilla Firefox tarayıcısında ve Thunderbird posta istemcisinde trafiği taramak için Şifreli Bağlantıları Taramayı etkinleştirmelisiniz. Şifreli Bağlantıları Tarama devre dışı bırakıldığı takdirde, uygulama Mozilla Firefox tarayıcısında ve Thunderbird posta istemcisindeki şifrelenmiş trafiği taramaz. Uygulama, şifrelenmiş trafiğin şifresini çözmek ve analiz etmek için Kaspersky kök sertifikasını kullanır. Kaspersky kök sertifikasını içerecek sertifika deposunu seçebilirsiniz. • **Windows sertifika deposu (önerilir)**. Kaspersky kök sertifikası, Kaspersky Endpoint Security kurulumu sırasında bu depoya eklenir. • **Kendi sertifika deposu**. Mozilla Firefox ve Thunderbird kendi sertifika depolarını kullanır. Mozilla sertifika deposu seçilirse, Kaspersky kök sertifikasını tarayıcı özelliklerinden bu depoya manuel olarak eklemeniz gerekir.

Arabirim

Uygulama arabiriminin ayarlarını yapılandırabilirsiniz.

Arabirim ayarları

Parametre	Açıklama
Kullanıcıyla etkileşim *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	**Basitleştirilmiş arabirimi görüntüle**. Bir istemci bilgisayarında, ana uygulama penceresine erişilemez, sadece Windows bildirim alanındaki simge kullanılabilir. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile kısıtlı sayıda işlem gerçekleştirebilir. Kaspersky Endpoint Security, uygulama simgesinin üzerinde yalnızca kullanıcı müdahalesi gerektiren bildirimleri gösterir. **Kullanıcı arabirimini göster**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin ana penceresi ve Windows bildirim alanındaki simge vardır. Simgenin bağlam menüsünden, kullanıcı Kaspersky Endpoint Security ile işlemler gerçekleştirebilir. Kaspersky Endpoint Security ayrıca uygulama simgesinin üzerinde bildirimler görüntüler. **Uygulama Etkinlik İzleyicisi bölümünü gizle**. İstemci bilgisayarda, Kaspersky Endpoint Security'nin ana penceresinde, **Uygulama Etkinlik İzleyicisi** düğmesi yoktur. *Uygulama Etkinlik İzleyicisi*, bir kullanıcının bilgisayarındaki uygulamaların etkinlikleri hakkında gerçek zamanlı bilgi görüntülemek için tasarlanmış bir araçtır. **Kullanıcı arabirimini gösterme**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin çalıştığına dair hiçbir işaret görüntülenmez. Windows bildirim alanındaki simge ve bildirimler yoktur.
Yerel görevlere erişim	Onay kutusu işaretlenirse yerel görevler Kaspersky Endpoint Security yerel arabiriminde görüntülenir. Ek ilke kısıtlamaları olmadığında kullanıcı görevleri yapılandırabilir ve çalıştırabilir. Ancak kullanıcı yine de görev çalışma zamanlamasının yapılandıramaz. Kullanıcı, görevleri yalnızca manuel olarak çalıştırabilir. Bu onay kutusunun işareti kaldırılırsa yerel görevler uygulama arabiriminde gizlenir. Bu modda, yerel görevler zamanlamaya göre çalışmaz. Görevler, Kaspersky Endpoint Security'nin yerel arabiriminde veya komut satırı ile çalışırken başlatılamaz veya yapılandırılamaz. Kullanıcı, dosya veya klasörün içerik menüsünde **Virüslere karşı tara** seçeneği işaretleyerek bir dosyanın veya klasörün virüs taramasını hala başlatabilir. Tarama görevi, özel tarama görevi için varsayılan ayar değerleri ile başlatılır.
Grup görevlerini görüntüle	Onay kutusu işaretlenirse grup görevler. Kaspersky Endpoint Security yerel arabiriminde görüntülenir. Kullanıcı, tüm görevlerin listesini uygulama arabiriminde görebilir. Onay kutusu işaretlenmezse Kaspersky Endpoint Security boş bir görev listesi görüntüler.
Grup görevlerini yönet	Onay kutusu işaretlenirse, kullanıcılar Kaspersky Security Center konsolunda belirtilen grup görevlerini başlatabilir ve durdurabilir. Kullanıcılar, uygulama arabiriminde ya da basitleştirilmiş uygulama arabiriminde görevleri başlatabilir ve durdurabilir. Onay kutusunun işaretlenmezse, Kaspersky Security Center zamanlanmış görevleri otomatik olarak başlatır ya da yönetici yönetim görevlerini Kaspersky Security Center konsolunda manuel olarak başlatır.
Bildirimleri yapılandır	Bir bileşen, görev veya tüm uygulamanın çalışması sırasında oluşabilecek farklı önem düzeylerindeki olaylar hakkında bildirimlerin ayarlarını içeren bir tablodur. Kaspersky Endpoint Security, bu olaylarla ilgili bildirimleri ekranda gösterir, e-postayla gönderir veya bunları günlüğe kaydeder.

Parametre	Açıklama
E-posta bildirimlerini yapılandır	Uygulamanın çalışması sırasında kaydedilen olaylar hakkındaki bildirimlerin teslime dilmesi için kullanılacak SMTP sunucusu ayarları. Varsayılan olarak Kaspersky Endpoint Security, Kaspersky Security Center'dan e-posta bildirim ayarlarını kullanır. E-posta bildirim ayarları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun. Bireysel e-posta bildirimini yapılandırmanız gerekirse şu ayarları düzenleyebilirsiniz: • **Gönderenin adresi**. Gönderenin e-posta adresi. Var olmayan bir adresin kullanılması önerilmez. • **SMTP sunucusu**. Kuruluşunuzun e-posta sunucularının bir veya birden fazla adresi (örneğin, `mail.company.com`). Bir IP adresi (IPv4 veya IPv6) girebilirsiniz. Kullanıcının SMTP sunucusunda kimliğini doğrulamak için gönderenin kimlik bilgilerini ilgili alanlara girin. E-posta bildirimlerini test etmek için bir test mesajı gönderebilirsiniz. • **Alıcının adresi**. Uygulamanın bildirim göndereceği alıcıların e-posta adresleri. • **Gönderim modu**. E-posta bildirimleri gönderme modu. Kaspersky Endpoint Security, bir olay meydana geldiğinde hemen mesaj gönderebilir; alternatif olarak önceden yapılandırılmış bir zamanlamayı takip edebilir.
Uygulamanın durumunu bildirim alanında göster	Kaspersky Endpoint Security simgesinin Microsoft Windows görev çubuğu bildirim alanında (veya) değişerek bir açılır pencere bildirimiyle sonuçlanmasına neden olan uygulama olayı kategorileri.
Yerel kötü amaçlı yazılım engelleme veritabanı durum bildirimleri	Uygulama tarafından kullanılan eski antivirüs veritabanları hakkındaki bildirim ayarları.
Parola koruması	Bu iki durumlu düğme açılırsa, bir kullanıcı Parola koruması kapsamındaki bir işlem gerçekleştirmeye çalıştığında Kaspersky Endpoint Security kullanıcıdan bir parola ister. Yasaklı işlemler (koruma bileşenlerinin devre dışı bırakılması gibi) ve Parola koruması kapsamının hangi kullanıcı hesaplarına uygulanacağı Parola Koruması kapsamındadır. Parola koruması etkinleştirildiğinde, Kaspersky Endpoint Security sizden KLAdmin hesabı için bir parola belirlemenizi ister.
Kullanıcı desteği / İnternet kaynaklarına bağlantılar *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Kaspersky Endpoint Security için teknik destek hakkında bilgi içeren İnternet kaynaklarına bağlantılarının listesi. Eklenen bağlantılar, standart bağlantılar yerine Kaspersky Endpoint Security'nin yerel arabirimindeki **Destek** penceresinde görüntülenir.
Kullanıcı desteği / Açıklama *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Kaspersky Endpoint Security'nin yerel arabiriminin **Destek** penceresinde görüntülenen mesajdır.

Ayarları Yönet

Mevcut Kaspersky Endpoint Security ayarlarını bir dosyaya kaydedebilir ve uygulamayı farklı bir bilgisayarda hızlı bir şekilde yapılandırmak için kullanabilirsiniz. Uygulamayı, bir kurulum paketi ile Kaspersky Security Center aracılığıyla dağıtırken bir yapılandırma dosyası da kullanabilirsiniz. Varsayılan ayarları istediğiniz zaman geri yükleyebilirsiniz.

Uygulama yapılandırma yönetimi ayarları yalnızca Kaspersky Endpoint Security arabiriminde mevcuttur.

Uygulama yapılandırma yönetimi ayarları

Ayarlar	Açıklama
İçe aktar	Uygulama ayarlarını CFG biçimli bir dosyadan alın ve uygulayın.
Dışa aktar	Geçerli uygulama ayarlarını CFG biçimli bir dosyaya kaydedin.
Geri yükle	Kaspersky tarafından önerilen uygulama ayarlarını dilediğiniz zaman geri yükleyebilirsiniz. Ayarlar geri yüklendiğinde tüm koruma bileşenleri için **Önerilen** güvenlik düzeyi ayarlanır.

Veritabanlarını ve uygulama yazılım modüllerini güncelleme

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.

Güncellemeler işlevselliği (anti-virüs imza güncellemeleri ve kod temeli güncellemeleri sağlama dahil olmak üzere) ABD'de yazılımda kullanılabilir olmayabilir.

Düzenli güncellemeler için geçerli bir lisans gerekir. Geçerli bir lisans yoksa, güncellemeyi günde sadece bir kez gerçekleştirebilirsiniz.

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, proxy sunucusu ayarlarını yapılandırmanız gerekir.

Güncellemeler, HTTPS protokolü üzerinden indirilir. HTTPS protokolü üzerinden güncellemeleri indirmek mümkün olmadığında HTTP protokolü de kullanılabilir.

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.

Veritabanları eskiyse, güncelleme paketi çok büyük olabilir ve ek internet trafiğine (onlarca MB) neden olabilir.

Kaspersky Endpoint Security veritabanlarının geçerli durumuyla ilgili bilgiler, ana uygulama penceresinde veya imleci bildirim alanındaki uygulamanın simgesinin üzerine getirdiğinizde gördüğünüz araç ipucunda görüntülenir.

Güncelleme sonuçları ve güncelleme görevinin gerçekleştirilmesi sırasında gerçekleşen tüm olaylarla ilgili bilgiler Kaspersky Endpoint Security raporuna kaydedilir.

Uygulama Light Agent modunda çalışıyorsa, uygulama veritabanlarının ve modüllerinin güncellenmesinde özel hususlar söz konusudur.

Uygulama modülü ve veritabanı güncellemesi ayarları

Parametre	Açıklama
Veritabanlarının güncelleme takvimi	**Otomatik**. Bu modda, uygulama belirli bir sıklıkta güncelleme kaynağında yeni güncelleme paketlerinin bulunup bulunmadığını denetler. Güncelleme paketinin kontrol edilme sıklığı, virüs salgınlarında artmakta ve virüs salgını olmadığında azalmaktadır. Yeni bir güncelleme paketi tespit ettikten sonra Kaspersky Endpoint Security, bunu indirir ve güncellemeleri bilgisayarınıza yükler. **Manuel**. Bu güncelleme görevinin çalışma modu, güncelleme görevini elle başlatmanızı sağlar. **Zamanlamaya göre**. Bu güncelleme görevinin çalışma modunda Kaspersky Endpoint Security, güncelleme görevini belirttiğiniz zamanlamaya uygun olarak çalıştırır. Bu güncelleme görevinin çalışma modu seçilirse Kaspersky Endpoint Security güncelleme görevini elle de başlatabilirsiniz.
Eksik görevleri çalıştır	Onay kutusu işaretlenirse Kaspersky Endpoint Security, atlanan görevi gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış görevin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Uygulama kaçırılan görevleri yürütme fırsatı bulduğunda, bilgisayar üzerindeki yükü dağıtmak için görevleri belirli bir zaman aralığında rastgele çalıştırır. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan görevleri çalıştırmaz. Bunun yerine, bir sonraki görevi geçerli zamanlamaya uygun olarak yürütür.
Güncelleme kaynakları	*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. Kaspersky güncelleme sunucuları erişilemez durumdaysa, Kaspersky Endpoint Security veritabanlarını ve uygulama yazılımı modüllerini güncellemek için alternatif etki alanlarını kullanabilir. Ayrıntılı bilgi için Teknik Destek Bilgi Tabanına bakın. 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. Kaspersky Endpoint Security, Kaspersky'nin güncelleme sunucuları olmadığı sürece, HTTPS sunucularından gelen güncellemeleri desteklemez. 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. Kaspersky Endpoint Security ilk güncelleme kaynağı olarak varsayılan olarak Kaspersky Security Center sunucusunu kullanır. Bu, güncelleme sırasında trafiğin korunmasına yardımcı olur. Bilgisayara bir ilke uygulanmazsa, uygulamanın Kaspersky Security Center sunucusuna erişimi olmayabileceğinden, Yerel *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevinin ayarlarında ilk güncelleme kaynağı olarak Kaspersky sunucuları seçilir. Uygulama Light Agent modunda çalışıyorsa, SVM üzerindeki bir klasör güncelleme kaynağı olarak seçilir.
Veritabanı güncellemelerini şu kullanıcı olarak çalıştır	Varsayılan olarak Kaspersky Endpoint Security güncelleme görevi, işletim sisteminde oturum açmak için hesabını kullandığınız kullanıcı adına başlatılır. Ancak Kaspersky Endpoint Security, gerekli hakların olmaması nedeniyle kullanıcının erişemediği bir güncelleme kaynağından (örneğin bir güncelleme paketi içeren bir paylaşım klasöründen) veya proxy sunucusu kimlik doğrulamasının yapılandırılmadığı bir güncelleme kaynağından güncellenebilir. Uygulama ayarlarında, bu haklara sahip bir kullanıcı belirtebilir ve Kaspersky Endpoint Security güncelleme görevini o kullanıcı hesabı altında başlatabilirsiniz.

Parametre	Açıklama
Uygulama modüllerinin güncellemelerini indir	Uygulama modülü güncellemelerini, uygulama veritabanı güncellemeleri ile indirmedir. Onay kutusu işaretlenirse Kaspersky Endpoint Security kullanıcıya kullanılabilir uygulama modülü güncellemeleri hakkında bildirimde bulunur ve bu bildirimler güncelleme görevi çalışırken güncelleme paketindeki uygulama modülü güncellemelerini içerir. Uygulama modülü güncellemelerinin uygulanma biçimi aşağıdaki ayarlarla belirlenir: • **Kritik ve onaylı güncelleştirmeleri yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, kritik güncellemeleri otomatik olarak ve tüm diğer uygulama modülü güncellemelerini ise uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler. • **Yalnızca onaylı güncelleştirmeleri yükle**. Bu seçenek işaretlenirse uygulama modülü güncellemeleri kullanılabilir olduğunda Kaspersky Endpoint Security, güncellemeleri uygulama arabirimi aracılığıyla yüklemelerin yerel olarak veya Kaspersky Security Center tarafından onaylanmasının ardından yükler. Bu seçenek varsayılan olarak seçilidir. Onay kutusu işaretlenmezse Kaspersky Endpoint Security, kullanıcıya kullanılabilir uygulama modülü güncellemeleri hakkında bildirimde bulunmaz ve bu bildirimler güncelleme görevi çalışırken güncelleme paketindeki uygulama modülü güncellemelerini içermez. Uygulama modülü güncellemeleri, Son Kullanıcı Lisans Sözleşmesi koşullarının gözden geçirilmesini ve kabul edilmesini gerektirirse uygulama, Son Kullanıcı Lisans Sözleşmesi koşullarının kabul edilmesinden sonra güncellemeleri yükler. Onay kutusu varsayılan olarak işaretlidir.
Güncellemeleri klasöre kopyala	Bu onay kutusu işaretlenirse Kaspersky Endpoint Security onay kutusunun altında belirtilen paylaşım klasörüne güncelleme paketini kopyalar. Ardından yerel ağdaki diğer bilgisayarlar bu paylaşım klasöründen güncelleme paketini alabilir. Böylece İnternet trafiği azaltılır çünkü güncelleme paketi sadece bir kez indirilir. Yandaki klasör varsayılan olarak belirlenmiştir: `C:\ProgramData\Kaspersky Lab\KES.14.2\Update distribution\`.
Güncellemeler için proxy sunucusu *(yalnızca Kaspersky Endpoint Security arabiriminde mevcuttur)*	Uygulama modüllerini ve veritabanlarını güncellemek için istemci bilgisayar kullanıcılarının İnternet erişimi için proxy sunucusu ayarları. Kaspersky Endpoint Security, bir proxy sunucusunun otomatik olarak yapılandırılması için WPAD (Web Proxy Auto-Discovery Protocol) iletişim kuralını kullanır. Proxy sunucusunun IP adresi bu iletişim kuralı kullanılarak belirlenemiyorsa Kaspersky Endpoint Security, Microsoft Internet Explorer tarayıcı ayarlarında belirtilen proxy sunucusu adresini kullanır.
Yerel adresler için proxy sunucuyu devre dışı tut *(yalnızca Kaspersky Endpoint Security arabiriminde mevcuttur)*	Onay kutusu işaretlenirse Kaspersky Endpoint Security, paylaşılan klasörden güncelleme yaparken proxy sunucusu kullanmaz.

Ek 2. Uygulama güven grupları

Kaspersky Endpoint Security bilgisayarda başlatılan uygulamaların tümünü güvenilirlik grubu kategorilerine ayırır. Uygulamaların işletim sistemleri için oluşturduğu tehdidin seviyesine göre uygulamalar güvenilirlik grubu kategorilerine ayrılır.

Güven grupları aşağıdaki gibidir:

- **Güvenilir**. Bu grup aşağıdaki koşulların biri veya daha fazlasını karşılayan uygulamaları içerir:
  - Güvenilir satıcılar tarafından dijital olarak imzalanan uygulamalar.
  - Kaspersky Security Network'ün güvenilir uygulamalar veritabanına kaydedilmiş uygulamalar.
  - Kullanıcı uygulamayı *Güvenilir* gruba yerleştirmiştir.

  Bu uygulamalar için hiç bir işlem yasaklanmamıştır.

- **Düşük Kısıtlamalı**. Bu grup aşağıdaki koşulları karşılayan uygulamaları içerir:
  - Güvenilir satıcılar tarafından dijital olarak imzalanmamış uygulamalar.
  - Kaspersky Security Network'ün güvenilir uygulamalar veritabanına kaydedilmemiş uygulamalar.
  - Kullanıcı uygulamayı *Düşük Kısıtlamalı* grubuna yerleştirmiştir.

  Bu uygulamalar, işletim sistemi kaynaklarına erişimle ilgili en düşük sınırlamalara tabidir.
- **Yüksek Kısıtlamalı**. Bu grup aşağıdaki koşulları karşılayan uygulamaları içerir:
  - Güvenilir satıcılar tarafından dijital olarak imzalanmamış uygulamalar.
  - Kaspersky Security Network'ün güvenilir uygulamalar veritabanına kaydedilmemiş uygulamalar.
  - Kullanıcı uygulamayı *Yüksek Kısıtlamalı* grubuna yerleştirmiştir.

  Bu uygulamalar, işletim sistemi kaynaklarına erişimle ilgili en yüksek sınırlamalara tabidir.
- **Güvenilmez**. Bu grup aşağıdaki koşulları karşılayan uygulamaları içerir:
  - Güvenilir satıcılar tarafından dijital olarak imzalanmamış uygulamalar.
  - Kaspersky Security Network'ün güvenilir uygulamalar veritabanına kaydedilmemiş uygulamalar.
  - Kullanıcı uygulamayı *Güvenilmez* grubuna yerleştirmiştir.

  Bu tür uygulamalar için tüm işlemler engellenir.

Ek 3. Hızlı çıkarılabilir sürücü taraması için dosya uzantıları

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

msg – Microsoft Mail e-posta iletisi

plg – e-posta mesajı

mbx – kayıtlı Microsoft Office Outlook e-posta mesajı

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

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 slaydı

sldm – makro destekli bir Microsoft PowerPoint 2007 slaytı

thmx – bir Microsoft Office 2007 teması

Ek 4. Posta Tehdidi Koruması ek filtresi için dosya türleri

Bir dosyanın gerçek biçiminin dosya adı uzantısı ile uyuşmayabileceğini unutmayın.

E-posta eklerinin filtrelenmesini etkinleştirirseniz Posta Tehdidi Koruması bileşeni, 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

msg – Microsoft Mail e-posta iletisi

plg – e-posta mesajı

mbx – kayıtlı Microsoft Office Outlook e-posta mesajı

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

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 slaydı

sldm – makro destekli bir Microsoft PowerPoint 2007 slaytı

thmx – bir Microsoft Office 2007 teması

Ek 5. Dış hizmetlerle etkileşim için ağ ayarları

Kaspersky Endpoint Security ve Kaspersky Security Center, Kaspersky'nin dış hizmetleriyle çalışmak için TLS (Aktarım Katmanı Güvenliği) ile şifreli bir iletişim kanalı kullanır.

Kaspersky Endpoint Security, dış hizmetlerle etkileşim için aşağıdaki ağ ayarlarını kullanır.

Ağ ayarları

Adres	Açıklama
`activation-v2.kaspersky.com/activationservice/activationservice.svc` İletişim kuralı: `HTTPS` Port: `443`	Uygulamayı etkinleştirme.

Adres	Açıklama

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
İletişim kuralı: `HTTPS`
Port: `443`
	Veritabanlarını ve uygulama yazılım modüllerini güncelleme.

`downloads.upd.kaspersky.com` İletişim kuralı: `HTTPS` Port: `443`	• Veritabanlarını ve uygulama yazılım modüllerini güncelleme. • Kaspersky sunucularına erişimi doğrulama. Sunuculara sistem DNS'si kullanılarak erişim mümkün olmazsa, uygulama genel DNS'yi kullanır. Bu, antivirüs veritabanlarının güncellendiğinden ve bilgisayar için güvenlik düzeyinin korunduğundan emin olmak için gereklidir. Kaspersky Endpoint Security, buradaki genel DNS sunucuları listesini aşağıdaki sırayla kullanır: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Uygulama tarafından gönderilen istekler, uygulama DNS sunucusuyla bir TCP/UDP bağlantısı kurduğundan, etki alanlarının adreslerini ve kullanıcının genel IP adresini içerebilir. Bu bilgi, örneğin HTTPS kullanıldığında bir web kaynağının sertifikasını doğrulamak için gereklidir. Kaspersky Endpoint Security genel bir DNS sunucusu kullanıyorsa veri işleme ilgili hizmetin gizlilik politikasına tabidir. Kaspersky Endpoint Security'nin genel bir DNS sunucusu kullanmasını önlemek istiyorsanız, özel bir yama için Teknik Destek ile iletişime geçin.
`touch.kaspersky.com` İletişim kuralı: `HTTP`	• Sertifikanın geçerlilik süresinin kontrol edilmesi için güvenilen sürenin alınması (TLS bağlantısı). • Web Tehdidi Koruması çalışırken tarayıcıda bir web kaynağına erişimin engellenmesiyle ilgili uyarı.

Adres	Açıklama

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
İletişim kuralı: `HTTP`
Port: `80`
	Veritabanlarını ve uygulama yazılım modüllerini güncelleme.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
İletişim kuralı: `HTTPS`
Port: `443`
	Kaspersky Security Network'ü kullanma.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
İletişim kuralı: `KSN`
Port: `443`, `1443`
	Kaspersky Security Network'ü kullanma.

`click.kaspersky.com`
`redirect.kaspersky.com`
İletişim kuralı: `HTTPS`
Port: `443`
	Arabirimden bağlantıları takip edin.

Şifreleme için kullanılan ayarlar

Adres	Açıklama

`crl.kaspersky.com`
`ocsp.kaspersky.com`
İletişim kuralı: `HTTP`
Port: `80`
	Genel Anahtar Altyapısı (PKI).

Ek 6. Uygulama olayları

Her bir Kaspersky Endpoint Security bileşeninin çalışmasına dair bilgiler, veri şifreleme olayları, her bir kötü amaçlı yazılım taraması görevi, güncelleme görevi ve bütünlük denetimi görevinin tamamlanma sonuçları ve uygulamanın genel çalışma bilgileri Kaspersky Security Center olay günlüğüne ve Windows olay günlüğüne kaydedilir.

Kaspersky Endpoint Security, aşağıdaki türlerde olaylar oluşturur: genel olaylar ve belirli olaylar. Belirli olaylar sadece Kaspersky Endpoint Security for Windows için oluşturulur. Belirli olayların `000000cb` gibi basit kimlikleri vardır. Belirli olaylar aşağıdaki gerekli parametreleri içerir:

- `GNRL_EA_DESCRIPTION` olayın içeriğidir.
- `GNRL_EA_ID` olayın hizmet kimliğidir.
- `GNRL_EA_SEVERITY` olayın durumudur. `1` – *Bilgi*, `2` – *Uyarı*, `3` – *İşlev hatası*, `4` – *Kritik*.
- `EVENT_TYPE_DISPLAY_NAME` olayın başlığıdır.
- `TASK_DISPLAY_NAME` olayı başlatan uygulama bileşeninin adıdır.

Genel olaylar, Kaspersky Endpoint Security for Windows ve diğer Kaspersky uygulamaları (örneğin Kaspersky Security for Windows Server) tarafından oluşturulabilir. Genel olayların `GNRL_EV_VIRUS_FOUND` gibi daha karmaşık kimlikleri olur. Genel olaylar, gerekli ayarlara ek olarak gelişmiş ayarlar da içerir.

Olaylar sunucuda ne kadar süreyle saklanır?

Kritik

Lisansın süresi doldu

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	`201`
Kaspersky Security Center olay kimliği	`GNRL_EV_LICENSE_EXPIRATION`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Lisans süresi sona ermek üzere

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	`203`
Kaspersky Security Center olay kimliği	`000000cb`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Veritabanları eksik veya bozuk

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	206
Kaspersky Security Center olay kimliği	000000ce
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Veritabanları son derece eski

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	207
Kaspersky Security Center olay kimliği	000000cf
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulamaların otomatik çalıştırılması devre dışı

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	209
Kaspersky Security Center olay kimliği	000000d1
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Etkinleştirme hatası

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	229
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Etkin tehdit tespit edildi. Gelişmiş Temizleme başlatılmalıdır

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	231
Kaspersky Security Center olay kimliği	000000e7
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KSN sunucuları kullanılabilir değil

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	2023
Kaspersky Security Center olay kimliği	000007e7
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Karantina depolamasında yeterli alan yok

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	343
Kaspersky Security Center olay kimliği	00000157
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Karantinadan geri yüklenmedi

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	346
Kaspersky Security Center olay kimliği	0000015a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Karantinadan silinmedi

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	348
Kaspersky Security Center olay kimliği	0000015c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama güvenilmeyen sertifikaya sahip bir web sitesine bağlantı kurdu

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	57
Kaspersky Security Center olay kimliği	00000039
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Şifrelenmiş bir bağlantı doğrulanamadı. Etki alanı istisnalar listesine eklendi

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	`60`
Kaspersky Security Center olay kimliği	`0000003c`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kötü amaçlı nesne tespit edildi (yerel veritabanları)

Durum	!
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Sunucu Yetkisiz Erişim Önleme Davranış Tespiti Şifreleyici Önleyici Exploit Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`302`
Kaspersky Security Center olay kimliği	`GNRL_EV_VIRUS_FOUND`
Olay parametreleri	• `GNRL_EA_PARAM_1`, nesnenin karma değeridir (SHA256). • `GNRL_EA_PARAM_2`, nesnenin adıdır. Paylaşılan klasörlerde harici şifreleme tespit edildiğinde, uygulama hedef dosyanın yolunu gösterir. • `GNRL_EA_PARAM_5` Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin `EICAR-Test-File`. • `GNRL_EA_PARAM_7` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_8` tehdidin türüdür (`type`). • `GNRL_EA_PARAM_9`, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (`engine`). Tehdit tespit etme teknolojisi (`method`). Tehdit Kaspersky Private Security Network tarafından tespit edildi (`blacklist`): `true` veya `false`. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kötü amaçlı nesne tespit edildi (KSN)

Durum	!
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Sunucu Yetkisiz Erişim Önleme Davranış Tespiti Şifreleyici Önleyici Exploit Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`302`

Kaspersky Security Center olay kimliği	GNRL_EV_VIRUS_FOUND_BY_KSN
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type). • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Kaspersky Private Security Network tarafından tespit edildi (blacklist): true veya false. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Temizleme mümkün değil

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Davranış Tespiti Şifreleyici Önleyici Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	312
Kaspersky Security Center olay kimliği	GNRL_EV_OBJECT_NOTCURED
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type). • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Kaspersky Private Security Network tarafından tespit edildi (blacklist): true veya false. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Silinemez

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Davranış Tespiti Şifreleyici Önleyici Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	313
Kaspersky Security Center olay kimliği	00000139
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem hatası

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme AMSI Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`317`
Kaspersky Security Center olay kimliği	`0000013d`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem sonlandırıldı

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Davranış Tespiti Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`452`
Kaspersky Security Center olay kimliği	`000001c4`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem sonlandırılamıyor

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Davranış Tespiti Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`453`
Kaspersky Security Center olay kimliği	`000001c5`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Tehlikeli bağlantı engellendi

Durum	ⓘ
Bileşen	Web Tehdidi Koruması
Windows olay kimliği	`362`
Kaspersky Security Center olay kimliği	`GNRL_EV_VIRUS_FOUND_AND_BLOCKED`
Olay parametreleri	• `GNRL_EA_PARAM_2` nesnenin yoludur. • `GNRL_EA_PARAM_5`, Kaspersky sınıflandırmasına göre nesnenin adıdır. • `GNRL_EA_PARAM_7` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_8` tehdidin türüdür (`type`). • `GNRL_EA_PARAM_9`, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (`engine`). Tehdit tespit etme teknolojisi (`method`). Tehdit Özel KSN tarafından tespit edildi (`blacklist`): `true` veya `false`.

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tehlikeli bağlantı açıldı

Durum	ⓘ
Bileşen	Web Tehdidi Koruması
Windows olay kimliği	`363`
Kaspersky Security Center olay kimliği	`GNRL_EV_VIRUS_FOUND_AND_REPORTED`
Olay parametreleri	• `GNRL_EA_PARAM_2` nesnenin yoludur. • `GNRL_EA_PARAM_5`, Kaspersky sınıflandırmasına göre nesnenin adıdır. • `GNRL_EA_PARAM_7` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_8` tehdidin türüdür (`type`). • `GNRL_EA_PARAM_9`, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (`engine`). Tehdit tespit etme teknolojisi (`method`). Tehdit Özel KSN tarafından tespit edildi (`blacklist`): `true` veya `false`.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Daha önce açılmış tehlikeli bağlantı tespit edildi

Durum	ⓘ
Bileşen	Web Tehdidi Koruması
Windows olay kimliği	`1201`
Kaspersky Security Center olay kimliği	`GNRL_EV_VIRUS_FOUND_AND_PASSED`
Olay parametreleri	• `GNRL_EA_PARAM_2` nesnenin yoludur. • `GNRL_EA_PARAM_5`, Kaspersky sınıflandırmasına göre nesnenin adıdır. • `GNRL_EA_PARAM_7` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_8` tehdidin türüdür (`type`). • `GNRL_EA_PARAM_9`, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (`engine`). Tehdit tespit etme teknolojisi (`method`). Tehdit Özel KSN tarafından tespit edildi (`blacklist`): `true` veya `false`.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşleme eylemi engellendi

Durum	ⓘ
Bileşen	Uyarlamalı Anomali Denetimi
Windows olay kimliği	`2200`
Kaspersky Security Center olay kimliği	`GNRL_EV_ADSEC_DETECT`
Olay parametreleri	• `GNRL_EA_PARAM_1` Uyarlamalı Anomali Denetimi kuralının adıdır. • `GNRL_EA_PARAM_2` sezgisel kuralın kimliğidir. • `GNRL_EA_PARAM_3` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_4` kaynak işlemdir. • `GNRL_EA_PARAM_5` kaynak nesnedir. • `GNRL_EA_PARAM_6` hedef işlemdir. • `GNRL_EA_PARAM_7` hedef nesnedir. • `GNRL_EA_PARAM_8`, algılanan nesne hakkındaki ek bilgilerdir: Kaynak sürecin/nesnenin ve hedef sürecin/nesnenin sağlama toplamları. İşlem engellendi (`verdict_type`): `true` veya `false`. Kullanıcı güvenlik kimliği (SID).

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Klavye yetkilendirilmemiş

Durum	ⓘ
Bileşen	BadUSB Saldırısı Önleme
Windows olay kimliği	`2051`
Kaspersky Security Center olay kimliği	`00000803`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

AMSI isteği engellendi

Durum	ⓘ
Bileşen	AMSI Koruması
Windows olay kimliği	`2200`
Kaspersky Security Center olay kimliği	`00000898`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ etkinliği engellendi

Durum	ⓘ
Bileşen	Güvenlik Duvarı
Windows olay kimliği	`602`
Kaspersky Security Center olay kimliği	`00000329`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ saldırısı tespit edildi

Durum	ⓘ
Bileşen	Ağ Tehdidi Koruması
Windows olay kimliği	`651`
Kaspersky Security Center olay kimliği	`GNRL_EV_ATTACK_DETECTED`
Olay parametreleri	• `GNRL_EA_PARAM_1` saldırının adıdır. • `GNRL_EA_PARAM_2` protokoldür. • `GNRL_EA_PARAM_3` ağ saldırısının kaynağı olarak davranan bilgisayarın IP adresidir. IP adresi, ana bilgisayarın bayt sırasına göre belirtilir. Örneğin, `2886729929` için `172.16.0.201`. • `GNRL_EA_PARAM_4` port numarasıdır. • `GNRL_EA_PARAM_5` bir IPv6 adresidir, örneğin `12B012B012B012B012B012B012B012B0`. • `GNRL_EA_PARAM_6` ağ saldırısının hedef aldığı bilgisayarın IP adresidir. IP adresi, ana bilgisayarın bayt sırasına göre belirtilir. Örneğin, `2886729929` için `172.16.0.201`.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama başlatma yasaklandı

Durum	ⓘ
Bileşen	Uygulama Denetimi
Windows olay kimliği	702
Kaspersky Security Center olay kimliği	GNRL_EV_APPLICATION_LAUNCH_DENIED
Olay parametreleri	• GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3, manuel olarak oluşturulan kategori tanımlayıcısıdır. • GNRL_EA_PARAM_4 uygulama kategorisi kimliğidir. • GNRL_EA_PARAM_5, uygulamanın dijital imzası hakkındaki bilgilerdir. • GNRL_EA_PARAM_6, uygulamanın yürütülebilir dosyasının adıdır (örneğin chrome.exe). • GNRL_EA_PARAM_7, yürütülebilir dosyanın yoludur. • GNRL_EA_PARAM_8, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_9, kullanıcının çalıştırmayı denediği uygulamanın sürümüdür.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yasak işlem, Kaspersky Endpoint Security'nin başlatılmasından önce başlatılmış

Durum	ⓘ
Bileşen	Uygulama Denetimi
Windows olay kimliği	710
Kaspersky Security Center olay kimliği	000002c6
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Erişim reddedildi (yerel veritabanları)

Durum	ⓘ
Bileşen	İnternet Denetimi
Windows olay kimliği	752
Kaspersky Security Center olay kimliği	GNRL_EV_WEB_URL_BLOCKED
Olay parametreleri	• GNRL_EA_PARAM_1 URL'dir. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3 İnternet Denetimi kuralının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Erişim reddedildi (KSN)

Durum	ⓘ
Bileşen	İnternet Denetimi
Windows olay kimliği	752
Kaspersky Security Center olay kimliği	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Olay parametreleri	• GNRL_EA_PARAM_1 URL'dir. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3 İnternet Denetimi kuralının adıdır.

Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aygıtla işlem yapılması yasaklandı

Durum	!
Bileşen	Aygıt Denetimi
Windows olay kimliği	802
Kaspersky Security Center olay kimliği	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Olay parametreleri	• GNRL_EA_PARAM_1 Donanım kimliğidir (HWID). • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ bağlantısı engellendi

Durum	!
Bileşen	Aygıt Denetimi
Windows olay kimliği	809
Kaspersky Security Center olay kimliği	00000329
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Endpoint Security başlatılana kadar cihazla işlem yapılması yasaktır

Durum	!
Bileşen	Aygıt Denetimi
Windows olay kimliği	816
Kaspersky Security Center olay kimliği	00000330
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Endpoint Security başlatılana kadar cihaz bağlantısı yasaktır

Durum	!
Bileşen	Aygıt Denetimi
Windows olay kimliği	817
Kaspersky Security Center olay kimliği	00000331
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bileşen güncelleme hatası

Durum	!
Bileşen	Güncelle
Windows olay kimliği	1011

Kaspersky Security Center olay kimliği	000003f3
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bileşen güncellemelerini dağıtma hatası

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1012
Kaspersky Security Center olay kimliği	000003f4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yerel güncelleme hatası

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1014
Kaspersky Security Center olay kimliği	000003f6
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Ağ güncelleme hatası

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1015
Kaspersky Security Center olay kimliği	000003f7
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aynı anda iki görev başlatılamıyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1017
Kaspersky Security Center olay kimliği	000003f9
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama veritabanları ve modüllerini doğrulama hatası

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1018

Kaspersky Security Center olay kimliği	000003fa
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Security Center ile etkileşim hatası

Durum	!
Bileşen	Güncelle
Windows olay kimliği	1019
Kaspersky Security Center olay kimliği	000003fb
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bileşenlerin tümü güncellenmemiş

Durum	!
Bileşen	Güncelle
Windows olay kimliği	1021
Kaspersky Security Center olay kimliği	000003fd
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Güncelleme başarıyla tamamlandı, güncelleme dağıtımı başarısız oldu

Durum	!
Bileşen	Güncelle
Windows olay kimliği	1023
Kaspersky Security Center olay kimliği	000003ff
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dahili görev hatası

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	101
Kaspersky Security Center olay kimliği	00000065
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama yüklemesi başarısız oldu

Durum	!
Bileşen	Güncelle
Windows olay kimliği	2153

Kaspersky Security Center olay kimliği	00000869
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yama geri alma başarısız oldu

Durum	⚠
Bileşen	Güncelle
Windows olay kimliği	2156
Kaspersky Security Center olay kimliği	0000086c
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya şifreleme/şifre çözme kurallarının uygulamasında hata

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	904
Kaspersky Security Center olay kimliği	00000388
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya şifreleme/şifre çözme hatası

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	912
Kaspersky Security Center olay kimliği	GNRL_EV_ENCRYPTION_ERROR
Olay parametreleri	• GNRL_EA_PARAM_1 dosyanın yoludur. • GNRL_EA_PARAM_2 hatanın nedenidir. • GNRL_EA_PARAM_3 cihazın türüdür.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya erişimi engellendi

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	940
Kaspersky Security Center olay kimliği	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Olay parametreleri	• GNRL_EA_PARAM_1 hedef nesnedir. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3 dosyaya erişmeye çalışan uygulamanın yürütülebilir dosyasının adıdır(örneğin chrome.exe).
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Taşınabilir modu etkinleştirme hatası

Durum	!
Bileşen	Veri Şifreleme
Windows olay kimliği	951
Kaspersky Security Center olay kimliği	000003b7
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Taşınabilir modu devre dışı bırakma hatası

Durum	!
Bileşen	Veri Şifreleme
Windows olay kimliği	953
Kaspersky Security Center olay kimliği	000003b9
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Şifrelenmiş paketin oluşturulmasında hata

Durum	!
Bileşen	Veri Şifreleme
Windows olay kimliği	931
Kaspersky Security Center olay kimliği	000003a3
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aygıt şifreleme/şifre çözmede hata

Durum	!
Bileşen	Veri Şifreleme
Windows olay kimliği	1305
Kaspersky Security Center olay kimliği	00000519
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Şifreleme modülü yüklenemedi

Durum	!
Bileşen	Veri Şifreleme
Windows olay kimliği	1311
Kaspersky Security Center olay kimliği	0000051f
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kimlik Doğrulama Aracısı hesaplarını yönetme görevi hata vererek sonlandı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1340
Kaspersky Security Center olay kimliği	0000053c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İlke uygulanamadı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	1312
Kaspersky Security Center olay kimliği	00000520
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

FDE yükseltmesi başarısız

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1342
Kaspersky Security Center olay kimliği	0000053e
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

FDE yükseltmesini geri alma işlemi başarısız (daha fazla bilgi için lütfen Kaspersky Endpoint Security for Windows Çevrimiçi Yardım bölümüne bakın)

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1344
Kaspersky Security Center olay kimliği	00000540
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Anti Targeted Attack Platform sunucusu kullanılamıyor

Durum	ⓘ
Bileşen	Endpoint Sensor
Windows olay kimliği	2100
Kaspersky Security Center olay kimliği	00000834
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne silinemedi

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2252
Kaspersky Security Center olay kimliği	000008cc
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne karantinaya alınmadı (Sandbox)

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2603
Kaspersky Security Center olay kimliği	00000a2b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bir dahili hata meydana geldi

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2607
Kaspersky Security Center olay kimliği	00000a2f
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Geçersiz Sandbox sunucusu sertifikası

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2613
Kaspersky Security Center olay kimliği	00000a35
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sandbox düğümü kullanılamıyor

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2614
Kaspersky Security Center olay kimliği	00000a36
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sandbox'taki nesne işlenemedi

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2617
Kaspersky Security Center olay kimliği	00000a39
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sandbox içim maksimum yük aşıldı

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2618
Kaspersky Security Center olay kimliği	00000a3a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

IOC bulundu

Durum	!
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2651
Kaspersky Security Center olay kimliği	00000a5b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sandbox lisans doğrulaması başarısız oldu

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2620
Kaspersky Security Center olay kimliği	00000a3c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tarama görevi bir kullanıcı tarafından Sandbox'a gönderilemedi

Durum	!
Bileşen	Sandbox
Windows olay kimliği	2623
Kaspersky Security Center olay kimliği	00000a3e
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sandbox görevi oluşturulurken hata oluştu

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2621
Kaspersky Security Center olay kimliği	00000a3d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne başlatma engellendi

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2553
Kaspersky Security Center olay kimliği	000009f9
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem başlatma engellendi

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2551
Kaspersky Security Center olay kimliği	000009f7
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Komut dizisi yürütmesi engellendi

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2559
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne karantinaya alınmadı (Endpoint Detection and Response)

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2556
Kaspersky Security Center olay kimliği	000009fc
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem başlatma engellenmedi

Durum	!
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2561
Kaspersky Security Center olay kimliği	00000a01
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne engellenmedi

Durum	!
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2562
Kaspersky Security Center olay kimliği	00000a02
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Komut dizisi yürütmesi engellenmedi

Durum	!
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2563
Kaspersky Security Center olay kimliği	00000a03
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama bileşenleri değiştirilirken hata

Durum	!
Bileşen	Sistem Denetimi
Windows olay kimliği	1401
Kaspersky Security Center olay kimliği	00000579
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sistemde olası bir deneme yanılma saldırısının izleri var

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2800
Kaspersky Security Center olay kimliği	00000af0
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Olası bir Windows Olay Günlüğü kötüye kullanımının izleri var

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2801
Kaspersky Security Center olay kimliği	00000af1
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yüklenen yeni bir hizmet adına alışılmadık eylemler tespit edildi

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2802
Kaspersky Security Center olay kimliği	00000af2
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Açık kimlik bilgileri kullanan alışılmadık oturum açma algılandı

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2803
Kaspersky Security Center olay kimliği	00000af3
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sistemde olası bir Kerberos sahte PAC (MS14-068) saldırısının izleri var

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2804
Kaspersky Security Center olay kimliği	00000af4
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ayrıcalıklı yerleşik Yöneticiler grubunda şüpheli değişiklikler tespit edildi

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2805
Kaspersky Security Center olay kimliği	00000af5
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bir ağ oturum açma oturumu sırasında tespit edilen alışılmadık bir etkinlik var

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2806
Kaspersky Security Center olay kimliği	00000af6
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Günlük Denetimi kuralı tetiklendi

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2807
Kaspersky Security Center olay kimliği	00000af7
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Olağandışı olay çok sık meydana geliyor. Olay toplama başladı

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2808
Kaspersky Security Center olay kimliği	00000af8
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Toplama dönemi için alışılmadık bir olay hakkında rapor

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2809
Kaspersky Security Center olay kimliği	00000af9
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert sunucusuna bağlanırken hata oluştu

Durum	!
Bileşen	Endpoint Detection and Response Expert (on-premises)
Windows olay kimliği	2850
Kaspersky Security Center olay kimliği	00000b22
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert sunucusunun sertifikası geçersiz

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises)
Windows olay kimliği	2851
Kaspersky Security Center olay kimliği	00000b23
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert sunucusundaki aracının sertifikası geçersiz

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises)
Windows olay kimliği	2852
Kaspersky Security Center olay kimliği	00000b24
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert yanıt sunucusuna bağlanırken hata oluştu

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	2858
Kaspersky Security Center olay kimliği	00000b22
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert yanıt sunucusunun sertifikası geçersiz

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	2859
Kaspersky Security Center olay kimliği	00000b23
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert yanıt sunucusunda aracının sertifikası geçersiz

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	2860
Kaspersky Security Center olay kimliği	00000b24

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert telemetri toplama sunucusu bağlantı hatası

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	`2854`
Kaspersky Security Center olay kimliği	`00000b22`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert telemetri toplama sunucusunun sertifikası geçersiz

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	`2855`
Kaspersky Security Center olay kimliği	`00000b23`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert telemetri toplama sunucusundaki aracının sertifikası geçersiz

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	`2856`
Kaspersky Security Center olay kimliği	`00000b24`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

NDR sunucusuna bağlanırken hata oluştu

Durum	ⓘ
Bileşen	Network Detection and Response (KATA)
Windows olay kimliği	`3080`
Kaspersky Security Center olay kimliği	`00000c08`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

NDR sunucusunun sertifikası geçersiz

Durum	ⓘ
Bileşen	Network Detection and Response (KATA)
Windows olay kimliği	`3081`

Kaspersky Security Center olay kimliği	00000c09
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

NDR sunucusundaki aracının sertifikası geçersiz

Durum	ⓘ
Bileşen	Network Detection and Response (KATA)
Windows olay kimliği	3082
Kaspersky Security Center olay kimliği	00000c0a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Cihazınız güvenilmeyen bir Yönetim Sunucusuna bağlı. Lütfen yönetici ile iletişime geçin

Durum	ⓘ
Bileşen	Yönetim Sunucusu bağlantı koruması
Windows olay kimliği	3301
Kaspersky Security Center olay kimliği	00000ce5
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya veya klasör değişikliği tespit edildi

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2950
Kaspersky Security Center olay kimliği	00000b86
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Nesne çok sık değişiyor. Olay toplama başladı

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2955
Kaspersky Security Center olay kimliği	00000b8b
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Toplama dönemi için nesne değişikliği raporu

Durum	!
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2953
Kaspersky Security Center olay kimliği	00000b89
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Durum	i / ⚠ / !
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2956
Kaspersky Security Center olay kimliği	00000b8c
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Kayıt defteri değişikliği tespit edildi

Durum	i / ⚠ / !
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2951
Kaspersky Security Center olay kimliği	00000b87
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Cihaz bağlantısı / bağlantı kesilmesi tespit edildi

Durum	i / ⚠ / !
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2952
Kaspersky Security Center olay kimliği	00000b88
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

İzleme kapsamı yanlış nesneler içeriyor

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2903
Kaspersky Security Center olay kimliği	00000b89
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Nesne ile kısıtlanmış işlemleri gerçekleştirme girişimleri çok fazla. Olay toplama başladı

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2963
Kaspersky Security Center olay kimliği	00000b93
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İzleme kapsamındaki dosyalarla yapılan bir işlem engellendi

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2959
Kaspersky Security Center olay kimliği	00000b8f
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Kayıt defteri değişikliği engellendi

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2960
Kaspersky Security Center olay kimliği	00000b90
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

İşlem hatası

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2954
Kaspersky Security Center olay kimliği	00000b8a
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sistem Bütünlüğü İzleme: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2964
Kaspersky Security Center olay kimliği	00000b94
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama Denetimi: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı

Durum	ⓘ
Bileşen	Uygulama Denetimi
Windows olay kimliği	711
Kaspersky Security Center olay kimliği	000002c7
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aygıt Denetimi: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı

Durum	ⓘ
Bileşen	Aygıt Denetimi
Windows olay kimliği	810
Kaspersky Security Center olay kimliği	0000032a
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İnternet Denetimi: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı

Durum	ⓘ
Bileşen	İnternet Denetimi
Windows olay kimliği	757
Kaspersky Security Center olay kimliği	000002f5
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uyarlamalı Anomali Denetimi: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı

Durum	!
Bileşen	Uyarlamalı Anomali Denetimi
Windows olay kimliği	504
Kaspersky Security Center olay kimliği	000001f8
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Günlük Denetimi: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı

Durum	!
Bileşen	Günlük Denetimi
Windows olay kimliği	2810
Kaspersky Security Center olay kimliği	00000afa
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

SVM kullanılabilir değil

Durum	!
Bileşen	Light Agent
Windows olay kimliği	3151
Kaspersky Security Center olay kimliği	00000c4f
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kötü amaçlı nesne tespit edildi. Gelişmiş Temizleme sanal makine şablonunda başlatılmalıdır

Durum	!
Bileşen	Light Agent
Windows olay kimliği	3182
Kaspersky Security Center olay kimliği	00000c6e
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kullanımdan kaldırılan iletişim üzerinden kurulan ağ bağlantısı engellendi

Durum	!
Bileşen	Koruma
Windows olay kimliği	75
Kaspersky Security Center olay kimliği	0000004b
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KUMA sunucusu bağlantı hatası

Durum	!
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	2854
Kaspersky Security Center olay kimliği	00000b26
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KUMA sunucusunun sertifikası geçersiz

Durum	!
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	2855
Kaspersky Security Center olay kimliği	00000b27
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KUMA sunucusundaki aracının sertifikası geçersiz

Durum	!
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	2856
Kaspersky Security Center olay kimliği	00000b28
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

SIEM sunucusu bağlantı hatası

Durum	!
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	3250
Kaspersky Security Center olay kimliği	00000cb2
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

SIEM sunucusunun sertifikası geçersiz

Durum	!
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	3251
Kaspersky Security Center olay kimliği	00000cb3
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

SIEM sunucusundaki aracının sertifikası geçersiz

Durum	⊗
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	3252
Kaspersky Security Center olay kimliği	00000cb4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlev hatası

Görev gerçekleştirilemedi

Durum	⊗
Bileşen	Sistem Denetimi
Windows olay kimliği	212
Kaspersky Security Center olay kimliği	000000d4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Geçersiz görev ayarları. Ayarlar uygulanmadı

Durum	⊗
Bileşen	Sistem Denetimi
Windows olay kimliği	707
Kaspersky Security Center olay kimliği	000002c3
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uyarı

Uygulama, önceki oturum sırasında çöktü

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	237
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Lisans yakında sona erecek

Durum	⚠
Bileşen	Sistem Denetimi

Windows olay kimliği	204
Kaspersky Security Center olay kimliği	000000cc
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Veritabanları güncel değil

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	208
Kaspersky Security Center olay kimliği	000000d0
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Otomatik güncellemeler devre dışı bırakıldı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	210
Kaspersky Security Center olay kimliği	000000d2
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kendini Koruma devre dışı bırakıldı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	211
Kaspersky Security Center olay kimliği	000000d3
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Koruma bileşenleri devre dışı bırakıldı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	214
Kaspersky Security Center olay kimliği	000000d6
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bilgisayar güvenli modda çalışıyor

Durum	⚠
Bileşen	Sistem Denetimi

Windows olay kimliği	215
Kaspersky Security Center olay kimliği	000000d7
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

İşlenmemiş dosyalar var

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	216
Kaspersky Security Center olay kimliği	000000d8
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Grup ilkesi uygulandı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	219
Kaspersky Security Center olay kimliği	000000db
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Görev durduruldu

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	222
Kaspersky Security Center olay kimliği	000000de
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Güncellemenin tamamlanması için uygulamayı kapatıp yeniden açın

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	224
Kaspersky Security Center olay kimliği	0000057b
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bilgisayarın yeniden başlatılması gerek

Durum	⚠
Bileşen	Sistem Denetimi

Windows olay kimliği	225
Kaspersky Security Center olay kimliği	000000e1
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Lisans, yüklü olmayan bileşenlerin kullanılabilmesine olanak sağlıyor

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	226
Kaspersky Security Center olay kimliği	000000e2
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Gelişmiş Temizleme işlemi başladı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	232
Kaspersky Security Center olay kimliği	000000e8
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Gelişmiş Temizleme işlemi tamamlandı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	233
Kaspersky Security Center olay kimliği	000000e9
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Geçersiz rezerve anahtar

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	230
Kaspersky Security Center olay kimliği	000000e6
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aboneliğin süresi yakında sona eriyor

Durum	⚠
Bileşen	Sistem Denetimi

Windows olay kimliği	240
Kaspersky Security Center olay kimliği	000000f0
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Engellendi

Durum	⚠
Bileşen	Davranış Tespiti Şifreleyici Önleyici Exploit Önleme Web Tehdidi Koruması
Windows olay kimliği	331
Kaspersky Security Center olay kimliği	GNRL_EV_OBJECT_BLOCKED
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. Paylaşılan klasörlerde harici şifreleme tespit edildiğinde, uygulama hedef dosyanın yolunu gösterir. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type). • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Kaspersky Private Security Network tarafından tespit edildi (blacklist): true veya false. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

İşletim sistemi ayarları Wi-Fi ağlarına erişimin kontrol edilmesine izin vermiyor

Durum	⚠
Bileşen	Aygıt Denetimi
Windows olay kimliği	249
Kaspersky Security Center olay kimliği	000000f9
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Nesne Yedekten geri yüklenmedi

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	336
Kaspersky Security Center olay kimliği	00000150

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Şüpheli ağ etkinliği tespit edildi

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	2001
Kaspersky Security Center olay kimliği	000007d1
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Şifreli bağlantı sonlandırıldı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	250
Kaspersky Security Center olay kimliği	000007d3
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KSN'ye katılım devre dışı bırakıldı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	2021
Kaspersky Security Center olay kimliği	000007e5
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bazı İşletim Sistemi fonksiyonlarının işlenmesi devre dışı bırakıldı

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	245
Kaspersky Security Center olay kimliği	000000f5
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Karantina depolama alanı neredeyse doldu

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	344
Kaspersky Security Center olay kimliği	00000158

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ bağlantısı engellendi

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	809
Kaspersky Security Center olay kimliği	00000abe
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yedek kopya oluşturulamadı

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Davranış Tespiti Şifreleyici Önleyici Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	310
Kaspersky Security Center olay kimliği	00000136
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne işlenmedi

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme AMSI Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	314
Kaspersky Security Center olay kimliği	0000013a
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne şifrelendi

Durum	⚠
Bileşen	Sunucu Yetkisiz Erişim Önleme
Windows olay kimliği	320
Kaspersky Security Center olay kimliği	00000140
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Nesne bozuk

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`321`
Kaspersky Security Center olay kimliği	`00000141`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım algılandı (yerel veritabanları)

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme AMSI Koruması Davranış Tespiti Şifreleyici Önleyici Şifreleyici Önleyici Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`303`
Kaspersky Security Center olay kimliği	`GNRL_EV_VIRUS_FOUND`
Olay parametreleri	• `GNRL_EA_PARAM_1`, nesnenin karma değeridir (SHA256). • `GNRL_EA_PARAM_2`, nesnenin adıdır. • `GNRL_EA_PARAM_5` Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin `EICAR-Test-File`. • `GNRL_EA_PARAM_7` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_8` tehdidin türüdür (`type`).
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım algılandı (KSN)

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme AMSI Koruması Davranış Tespiti Şifreleyici Önleyici Şifreleyici Önleyici Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`303`

Kaspersky Security Center olay kimliği	GNRL_EV_VIRUS_FOUND_BY_KSN
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type).
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne silindi

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Exploit Önleme Davranış Tespiti Şifreleyici Önleyici Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	307
Kaspersky Security Center olay kimliği	GNRL_EV_OBJECT_DELETED
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type). • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Kaspersky Private Security Network tarafından tespit edildi (blacklist): true veya false. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne temizlendi

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	306

Kaspersky Security Center olay kimliği	`GNRL_EV_OBJECT_CURED`
Olay parametreleri	• `GNRL_EA_PARAM_1`, nesnenin karma değeridir (SHA256). • `GNRL_EA_PARAM_2`, nesnenin adıdır. • `GNRL_EA_PARAM_5` Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin `EICAR-Test-File`. • `GNRL_EA_PARAM_7` oturum açan kullanıcının adıdır. • `GNRL_EA_PARAM_8` tehdidin türüdür (`type`). • `GNRL_EA_PARAM_9`, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (`engine`). Tehdit tespit etme teknolojisi (`method`). Tehdit Kaspersky Private Security Network tarafından tespit edildi (`blacklist`): `true` veya `false`. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne yeniden başlatmada temizlenecek

Durum	⚠
Bileşen	Sunucu Yetkisiz Erişim Önleme Dosya Tehdidi Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	324
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Nesne yeniden başlatmada silinecek

Durum	⚠
Bileşen	Davranış Tespiti Şifreleyici Önleyici Exploit Önleme Sunucu Yetkisiz Erişim Önleme Dosya Tehdidi Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	323
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Nesne ayarlara göre silindi

Durum	⚠
Bileşen	Posta Tehdidi Koruması
Windows olay kimliği	342
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Geri alma tamamlandı

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Davranış Tespiti Şifreleyici Önleyici Exploit Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	455
Kaspersky Security Center olay kimliği	000001c7
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulamanın önceki bir sürümü kaldırılırken hata oluştu

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	246
Kaspersky Security Center olay kimliği	000000f6
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne indirme işlemi engellendi

Durum	⚠
Bileşen	Web Tehdidi Koruması
Windows olay kimliği	341
Kaspersky Security Center olay kimliği	GNRL_EV_OBJECT_BLOCKED
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type). • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Kaspersky Private Security Network tarafından tespit edildi (blacklist): true veya false. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Klavye yetkilendirme hatası

Durum	⚠
Bileşen	BadUSB Saldırısı Önleme
Windows olay kimliği	2052
Kaspersky Security Center olay kimliği	00000804
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne tarama sonucu üçüncü taraf uygulamaya gönderildi

Durum	⚠
Bileşen	AMSI Koruması
Windows olay kimliği	1512
Kaspersky Security Center olay kimliği	GNRL_EV_OBJECT_REPORTED
Olay parametreleri	• GNRL_EA_PARAM_1, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_5 Kaspersky sınıflandırmasına göre tehdidin adıdır, örneğin EICAR-Test-File. • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_8 tehdidin türüdür (type). • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Kaspersky Private Security Network tarafından tespit edildi (blacklist): true veya false. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Görev ayarları başarıyla uygulandı

Durum	⚠
Bileşen	Uygulama Denetimi
Windows olay kimliği	708
Kaspersky Security Center olay kimliği	000002c4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İstenmeyen içerik hakkında uyarı (yerel veritabanları)

Durum	⚠
Bileşen	İnternet Denetimi
Windows olay kimliği	708
Kaspersky Security Center olay kimliği	GNRL_EV_WEB_URL_WARNING
Olay parametreleri	• GNRL_EA_PARAM_1 URL'dir. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3 İnternet Denetimi kuralının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İstenmeyen içerik hakkında uyarı (KSN)

Durum	⚠
Bileşen	İnternet Denetimi
Windows olay kimliği	708

Kaspersky Security Center olay kimliği	GNRL_EV_WEB_URL_WARNING
Olay parametreleri	• GNRL_EA_PARAM_1 URL'dir. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3 İnternet Denetimi kuralının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bir uyarıdan sonra istenmeyen içeriğe erişildi

Durum	⚠
Bileşen	İnternet Denetimi
Windows olay kimliği	754
Kaspersky Security Center olay kimliği	000002f2
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıta geçici erişim etkinleştirildi

Durum	⚠
Bileşen	Aygıt Denetimi
Windows olay kimliği	803
Kaspersky Security Center olay kimliği	000002f2
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

İşlem kullanıcı tarafından iptal edildi

Durum	⚠
Bileşen	Güncelle
Windows olay kimliği	1016
Kaspersky Security Center olay kimliği	000003f8
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kullanıcı şifreleme ilkesine katılmamayı seçti

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	1306
Kaspersky Security Center olay kimliği	0000051a
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya şifreleme/şifre çözme kurallarının uygulanması kesintiye uğradı

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	903
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya şifreleme/şifre çözme kesintiye uğradı

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	914
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifreleme/şifre çözme kesintiye uğradı

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	1303
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

WinRE görüntüsündeki Kaspersky Disk Encryption sürücülerinin yüklenmesi veya güncellenmesi başarısız oldu

Durum	⚠
Bileşen	Veri Şifreleme
Windows olay kimliği	1345
Kaspersky Security Center olay kimliği	00000541
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Modül imza denetimi başarısız oldu

Durum	⚠
Bileşen	Sistem Bütünlük Denetimi
Windows olay kimliği	2002
Kaspersky Security Center olay kimliği	000007d2
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama başlatma engellendi

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2105
Kaspersky Security Center olay kimliği	00000839
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Belge açma engellendi

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2106
Kaspersky Security Center olay kimliği	0000083a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem Kaspersky Anti Targeted Attack Platform sunucusu yöneticisi tarafından sonlandırıldı

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2112
Kaspersky Security Center olay kimliği	00000840
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama Kaspersky Anti Targeted Attack Platform sunucusu yöneticisi tarafından sonlandırıldı

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2113
Kaspersky Security Center olay kimliği	00000841
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya veya akış Kaspersky Anti Targeted Attack Platform sunucusu yöneticisi tarafından silindi

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2111
Kaspersky Security Center olay kimliği	0000083f
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya Kaspersky Anti Targeted Attack Platform sunucusunda yönetici tarafından karantinadan geri yüklendi

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2110
Kaspersky Security Center olay kimliği	0000083e
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya Kaspersky Anti Targeted Attack Platform sunucusunda yönetici tarafından karantinaya alındı.

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2109
Kaspersky Security Center olay kimliği	0000083d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tüm üçüncü taraf uygulamaların ağ etkinliği engellendi

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2107
Kaspersky Security Center olay kimliği	0000083b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tüm üçüncü taraf uygulamaların ağ etkinliğinin engellemesi kaldırıldı

Durum	⚠
Bileşen	Endpoint Sensor
Windows olay kimliği	2108
Kaspersky Security Center olay kimliği	0000083c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne yeniden başlatmadan sonra silinecek (Sandbox)

Durum	⚠
Bileşen	Sandbox
Windows olay kimliği	2605
Kaspersky Security Center olay kimliği	00000a2d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tarama görevlerinin toplam boyutu sınırı aştı

Durum	⚠
Bileşen	Sandbox
Windows olay kimliği	2612
Kaspersky Security Center olay kimliği	00000a34
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne başlatmaya izin verildi, olay günlüğe alındı

Durum	⚠
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2553
Kaspersky Security Center olay kimliği	000009fa
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlem başlatmaya izin verildi, olay günlüğe alındı

Durum	⚠
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2554
Kaspersky Security Center olay kimliği	000009f8
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne yeniden başlatmadan sonra silinecek (Endpoint Detection and Response)

Durum	⚠
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2558
Kaspersky Security Center olay kimliği	000009fe
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ izolasyonu

Durum	⚠
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2700
Kaspersky Security Center olay kimliği	00000a8c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ izolasyonunun sonlandırılması

Durum	⚠
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2701
Kaspersky Security Center olay kimliği	00000a8d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Görev tamamlamak için yeniden başlatma gerekiyor

Durum	⚠
Bileşen	Sistem Denetimi
Windows olay kimliği	225
Kaspersky Security Center olay kimliği	0000057b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Güvenilmez sertifikaya sahip bir web sitesiyle bağlantı kullanıcı kararıyla kurulur

Durum	⚠
Bileşen	Network Detection and Response (KATA)
Windows olay kimliği	70
Kaspersky Security Center olay kimliği	00000046
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yönetici için uygulama başlatmasını engelleme mesajı

Durum	⚠
Bileşen	Uygulama Denetimi
Windows olay kimliği	503
Kaspersky Security Center olay kimliği	GNRL_EV_AC_USER_REQUEST
Olay parametreleri	• GNRL_EA_DESCRIPTION kullanıcıya mesajdır. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_6, uygulamanın yürütülebilir dosyasının adıdır (örneğin chrome.exe). • GNRL_EA_PARAM_7, yürütülebilir dosyanın yoludur. • GNRL_EA_PARAM_8, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_9, kullanıcının çalıştırmayı denediği uygulamanın sürümüdür.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yöneticiye aygıta erişimin engellenmesine yönelik mesaj

Durum	⚠
Bileşen	Aygıt Denetimi
Windows olay kimliği	804

Kaspersky Security Center olay kimliği	GNRL_EV_DC_USER_REQUEST
Olay parametreleri	• c_er_descr kullanıcıya mesajdır. • GNRL_EA_PARAM_1 Donanım kimliğidir (HWID). • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yönetici için web sayfası erişimini engelleme mesajı

Durum	⚠
Bileşen	İnternet Denetimi
Windows olay kimliği	755
Kaspersky Security Center olay kimliği	GNRL_EV_WC_USER_REQUEST
Olay parametreleri	• GNRL_EA_DESCRIPTION kullanıcıya mesajdır. • GNRL_EA_PARAM_1 URL'dir. • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aygıtla bağlantı engellendi

Durum	⚠
Bileşen	Aygıt Denetimi
Windows olay kimliği	807
Kaspersky Security Center olay kimliği	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Olay parametreleri	• GNRL_EA_PARAM_1 Donanım kimliğidir (HWID). • GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yönetici için uygulama etkinliği engelleme mesajı

Durum	⚠
Bileşen	Uyarlamalı Anomali Denetimi
Windows olay kimliği	503
Kaspersky Security Center olay kimliği	GNRL_EV_ADSEC_USER_REQUEST
Olay parametreleri	• GNRL_EA_DESCRIPTION kullanıcıya mesajdır. • GNRL_EA_PARAM_1 Uyarlamalı Anomali Denetimi kuralının adıdır. • GNRL_EA_PARAM_2 sezgisel kuralın kimliğidir. • GNRL_EA_PARAM_3 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_4 kaynak işlemdir. • GNRL_EA_PARAM_5 kaynak nesnedir. • GNRL_EA_PARAM_6 hedef işlemdir. • GNRL_EA_PARAM_7 hedef nesnedir. • GNRL_EA_PARAM_8, algılanan nesne hakkındaki ek bilgilerdir: Kaynak işlemin/nesnenin karmaları ve hedef işlem/nesne. İşlem engellendi (verdict_type): true veya false. Kullanıcı güvenlik kimliği (SID).
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bulut hizmeti istemci uygulamasının başlatılması engellendi

Durum	⚠
Bileşen	Cloud Discovery
Windows olay kimliği	2212
Kaspersky Security Center olay kimliği	000008a4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bulut hizmetine erişim engellendi

Durum	⚠
Bileşen	Cloud Discovery
Windows olay kimliği	2213
Kaspersky Security Center olay kimliği	000008a5
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya veya klasör değişikliği tespit edildi

Durum	ⓘ / ⚠ / ⓔ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2950
Kaspersky Security Center olay kimliği	00000b86
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Nesne çok sık değişiyor. Olay toplama başladı

Durum	ⓘ / ⚠ / ⓔ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2955
Kaspersky Security Center olay kimliği	00000b8b
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Toplama dönemi için nesne değişikliği raporu

Durum	ⓘ / ⚠ / ⓔ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2956
Kaspersky Security Center olay kimliği	00000b8c
Windows olay günlüğü (varsayılan)	–

Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Kayıt defteri değişikliği tespit edildi

Durum	ⓘ / ⚠ / ⓔ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2951
Kaspersky Security Center olay kimliği	00000b87
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Cihaz bağlantısı / bağlantı kesilmesi tespit edildi

Durum	ⓘ / ⚠ / ⓔ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2952
Kaspersky Security Center olay kimliği	00000b88
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

İzleme kapsamı yanlış nesneler içeriyor

Durum	ⓘ / ⚠ / ⓔ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2903
Kaspersky Security Center olay kimliği	00000b89
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Yasaklanan işlemin test modunda çalışmasına izin verildi

Durum	⚠
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2961
Kaspersky Security Center olay kimliği	00000b91
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Entegrasyon Sunucusuna 30 dakikadan fazla bir süredir bağlanılamıyor. Entegrasyon Sunucusu durumunu ve ağ ayarlarını kontrol edin

Durum	⚠
Bileşen	Light Agent
Windows olay kimliği	3102
Kaspersky Security Center olay kimliği	00000c1e
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Entegrasyon Sunucusuna 6 saatten fazla bir süredir bağlanılamıyor. Entegrasyon Sunucusu durumunu ve ağ ayarlarını kontrol edin

Durum	⚠
Bileşen	Light Agent
Windows olay kimliği	3103
Kaspersky Security Center olay kimliği	00000c1f
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Entegrasyon Sunucusuna bağlanılamıyor. Entegrasyon Sunucusu durumunu ve ağ ayarlarını kontrol edin

Durum	⚠
Bileşen	Light Agent
Windows olay kimliği	3101
Kaspersky Security Center olay kimliği	00000c1d
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sanal makine şablonunun güncellenmesi gerekiyor

Durum	⚠
Bileşen	Light Agent
Windows olay kimliği	3181
Kaspersky Security Center olay kimliği	00000c6d
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Standard lisansı sonlandırıldı. Uygulama Enterprise lisansı ile çalışıyor

Durum	⚠
Bileşen	Light Agent
Windows olay kimliği	3171
Kaspersky Security Center olay kimliği	00000c64
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Durum	⚠
Bileşen	Dosya Bütünlük İzleyicisi
Windows olay kimliği	2901
Kaspersky Security Center olay kimliği	00000b55
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Durum	⚠
Bileşen	Dosya Bütünlük İzleyicisi
Windows olay kimliği	2900
Kaspersky Security Center olay kimliği	00000b54
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bilgilendirici mesaj

Uygulama başlatıldı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	235
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Uygulama durduruldu

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	236
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Kendini Koruma, korunan kaynağa erişimi kısıtladı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	213
Kaspersky Security Center olay kimliği	000000d5
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Rapor temizlendi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	217
Kaspersky Security Center olay kimliği	000000d9
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Grup ilkesi devre dışı bırakıldı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	220
Kaspersky Security Center olay kimliği	000000dc
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Uygulama ayarları değiştirildi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	218
Kaspersky Security Center olay kimliği	000000da
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Görev başlatıldı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	221
Kaspersky Security Center olay kimliği	000000dd
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Görev tamamlandı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	223
Kaspersky Security Center olay kimliği	000000df
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Lisans tarafından tanımlanmış tüm uygulama bileşenleri yüklendi ve normal modda çalıştırıldı

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	227
Kaspersky Security Center olay kimliği	000000e3
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Abonelik ayarları değişti

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	238
Kaspersky Security Center olay kimliği	000000ee
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Abonelik yenilendi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	239
Kaspersky Security Center olay kimliği	000000ef
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Yedekten geri yüklendi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	335
Kaspersky Security Center olay kimliği	0000014f
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kullanıcı adı ve parola girişi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	2000
Kaspersky Security Center olay kimliği	000007d0
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

KSN'ye katılım etkinleştirildi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	2020
Kaspersky Security Center olay kimliği	000007e4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KSN sunucuları kullanılabilir

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	2022
Kaspersky Security Center olay kimliği	000007e6
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulamanın çalışması ve veri işleme, ilgili yasalara göre gerçekleştirilir ve uygun altyapı kullanılır

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	2024
Kaspersky Security Center olay kimliği	000007e8
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Karantinadan geri yüklendi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	345
Kaspersky Security Center olay kimliği	00000159
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Karantinadan silindi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	347
Kaspersky Security Center olay kimliği	0000015b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesnenin bir yedek kopyası oluşturuldu

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Posta Tehdidi Koruması Davranış Tespiti Şifreleyici Önleyici Sunucu Yetkisiz Erişim Önleme Sandbox Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	308
Kaspersky Security Center olay kimliği	00000134
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Daha önce temizlenmiş bir kopya tarafından üzerine yazıldı

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	327
Kaspersky Security Center olay kimliği	00000147
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Parola korumalı arşiv tespit edildi

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	322
Kaspersky Security Center olay kimliği	GNRL_EV_PASSWD_ARCHIVE_FOUND
Olay parametreleri	• GNRL_EA_PARAM_2, nesnenin adıdır. • GNRL_EA_PARAM_3, nesnenin oluşturulma tarihidir (isteğe bağlı). • GNRL_EA_PARAM_7 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_9, algılanan nesne hakkındaki ek bilgilerdir: Uygulama bileşeni (engine). Tehdit tespit etme teknolojisi (method). Tehdit Özel KSN tarafından tespit edildi (denylist): true veya false.

Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tespit edilen nesne hakkında bilgi

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	332
Kaspersky Security Center olay kimliği	0000014c
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Kaspersky Private Security Network izin verilenler listesinde

Durum	ⓘ
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Sunucu Yetkisiz Erişim Önleme Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	340
Kaspersky Security Center olay kimliği	00000154
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne yeniden adlandırıldı

Durum	ⓘ
Bileşen	Posta Tehdidi Koruması Exploit Önleme Davranış Tespiti Şifreleyici Önleyici Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	329
Kaspersky Security Center olay kimliği	00000149
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne işlendi

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	301

Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Nesne atlandı

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme Dosya Tehdidi Koruması AMSI Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	315
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Arşiv tespit edildi

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	318
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Paketlenmiş nesne tespit edildi

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması AMSI Koruması Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	319
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Bağlantı işlendi

Durum	ⓘ
Bileşen	Web Tehdidi Koruması
Windows olay kimliği	361
Kaspersky Security Center olay kimliği	–

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Uygulama başlatmaya izin verildi

Durum	ⓘ
Bileşen	Uygulama Denetimi
Windows olay kimliği	701
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Güncelleme kaynağı seçildi

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1001
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Proxy sunucusu seçildi

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1002
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Bağlantı, Kaspersky Private Security Network izin verilenler listesinde

Durum	ⓘ
Bileşen	Web Tehdidi Koruması
Windows olay kimliği	370
Kaspersky Security Center olay kimliği	00000172
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama güvenilir gruba yerleştirildi

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme
Windows olay kimliği	401
Kaspersky Security Center olay kimliği	00000191

Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama kısıtlamalı gruba yerleştirildi

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme
Windows olay kimliği	402
Kaspersky Security Center olay kimliği	00000192
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Sunucu Yetkisiz Erişim Önleme tetiklendi

Durum	ⓘ
Bileşen	Sunucu Yetkisiz Erişim Önleme
Windows olay kimliği	403
Kaspersky Security Center olay kimliği	00000193
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya geri yüklendi

Durum	ⓘ
Bileşen	Davranış Tespiti Şifreleyici Önleyici Exploit Önleme Sunucu Yetkisiz Erişim Önleme
Windows olay kimliği	457
Kaspersky Security Center olay kimliği	000001c9
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kayıt defteri değeri geri yüklendi

Durum	ⓘ
Bileşen	Davranış Tespiti Exploit Önleme
Windows olay kimliği	458
Kaspersky Security Center olay kimliği	000001ca
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Kayıt defteri değeri silindi

Durum	ⓘ
Bileşen	Davranış Tespiti Exploit Önleme

Windows olay kimliği	459
Kaspersky Security Center olay kimliği	000001cb
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

İşleme eylemi atlandı

Durum	ⓘ
Bileşen	Uyarlamalı Anomali Denetimi
Windows olay kimliği	2201
Kaspersky Security Center olay kimliği	GNRL_EV_ADSEC_DETECT
Olay parametreleri	• GNRL_EA_PARAM_1 Uyarlamalı Anomali Denetimi kuralının adıdır. • GNRL_EA_PARAM_2 sezgisel kuralın kimliğidir. • GNRL_EA_PARAM_3 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_4 kaynak işlemdir. • GNRL_EA_PARAM_5 kaynak nesnedir. • GNRL_EA_PARAM_6 hedef işlemdir. • GNRL_EA_PARAM_7 hedef nesnedir. • GNRL_EA_PARAM_8, algılanan nesne hakkındaki ek bilgilerdir: Kaynak işlemin/nesnenin karmaları ve hedef işlem/nesne. İşlem engellendi (verdict_type): true veya false. Kullanıcı güvenlik kimliği (SID).
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Klavye yetkilendirilmiş

Durum	ⓘ
Bileşen	BadUSB Saldırısı Önleme
Windows olay kimliği	2050
Kaspersky Security Center olay kimliği	00000802
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ağ etkinliğine izin verildi

Durum	ⓘ
Bileşen	Güvenlik Duvarı
Windows olay kimliği	601
Kaspersky Security Center olay kimliği	00000259
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Uygulama başlatma test modunda yasaklandı

Durum	ⓘ
Bileşen	Uygulama Denetimi
Windows olay kimliği	703

Kaspersky Security Center olay kimliği	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Olay parametreleri	• GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3, manuel olarak oluşturulan kategori tanımlayıcısıdır. • GNRL_EA_PARAM_4, hesap güvenlik tanımlayıcısıdır (SID). • GNRL_EA_PARAM_5, uygulamanın dijital imzası hakkındaki bilgilerdir. • GNRL_EA_PARAM_6, uygulamanın yürütülebilir dosyasının adıdır (örneğin chrome.exe). • GNRL_EA_PARAM_7, yürütülebilir dosyanın yoludur. • GNRL_EA_PARAM_8, nesnenin karma değeridir (SHA256). • GNRL_EA_PARAM_9, kullanıcının çalıştırmayı denediği uygulamanın sürümüdür.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama başlatmaya test modunda izin verildi

Durum	ⓘ
Bileşen	Uygulama Denetimi
Windows olay kimliği	704
Kaspersky Security Center olay kimliği	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Olay parametreleri	• GNRL_EA_PARAM_2 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_3, manuel olarak oluşturulan kategori tanımlayıcısıdır. • GNRL_EA_PARAM_4, hesap güvenlik tanımlayıcısıdır (SID). • GNRL_EA_PARAM_5, uygulamanın dijital imzası hakkındaki bilgilerdir.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

İzin verilen bir sayfa açıldı

Durum	ⓘ
Bileşen	İnternet Denetimi
Windows olay kimliği	751
Kaspersky Security Center olay kimliği	000002f4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıtla işleme izin verildi

Durum	ⓘ
Bileşen	Aygıt Denetimi
Windows olay kimliği	801
Kaspersky Security Center olay kimliği	00000321
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya işlemi gerçekleştirildi

Durum	ⓘ
Bileşen	Aygıt Denetimi
Windows olay kimliği	808

Kaspersky Security Center olay kimliği	GNRL_EV_USB_FILE_OPERATION
Olay parametreleri	• GNRL_EA_PARAM_1 dosya işlemidir (yazma veya silme). • GNRL_EA_PARAM_2 dosyanın yoludur. • GNRL_EA_PARAM_3 cihazın adıdır. • GNRL_EA_PARAM_4 oturum açan kullanıcının adıdır. • GNRL_EA_PARAM_5 Donanım kimliğidir (HWID).
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Kullanılabilir güncelleme yok

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1020
Kaspersky Security Center olay kimliği	000003fc
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Güncelleme dağıtımı başarıyla tamamlandı

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1022
Kaspersky Security Center olay kimliği	000003fe
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosyalar indiriliyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1003
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya indirildi

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1004
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya yüklendi

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1005
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya güncellendi

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1006
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya, güncelleme hatası nedeniyle geri alındı

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1007
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosyalar güncelleniyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1008
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Güncellemeler dağıtılıyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1009
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosyalar geri alınıyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1010
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

İndirilecek dosyaların listesi oluşturuluyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	1013
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yamalar indiriliyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	2150
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama yükleniyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	2151
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama yüklendi

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	2152
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama geri alınıyor

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	2154
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama geri alındı

Durum	ⓘ
Bileşen	Güncelle
Windows olay kimliği	2155
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya şifreleme/şifre çözme kuralları uygulanmaya başlandı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	901
Kaspersky Security Center olay kimliği	00000385
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya şifreleme/şifre çözme kuralları uygulanması bitirildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	902
Kaspersky Security Center olay kimliği	00000386
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya şifreleme/şifre çözme kurallarının uygulanmasına devam edildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	905
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya şifreleme/şifre çözme başlatıldı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	910
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya şifreleme/şifre çözme tamamlandı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	911
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya bir istisna olduğu için şifrelenemedi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	913
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Taşınabilir mod etkinleştirildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	950
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Taşınabilir mod devre dışı bırakıldı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	952
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifreleme/şifre çözme başlatıldı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1301
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifreleme/şifre çözme tamamlandı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1302
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifreleme/şifre çözme işlemine devam edildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1304
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifrelenmedi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1307
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifreleme/şifre çözme işlemi etkin moda geçti

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1308
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Aygıt şifreleme/şifre çözme işlemi pasif moda geçti

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1309
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Şifreleme modülü yüklendi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1310
Kaspersky Security Center olay kimliği	0000051e
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yeni Kimlik Doğrulama Aracısı hesabı oluşturuldu

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1330
Kaspersky Security Center olay kimliği	00000532
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Kimlik Doğrulama Aracısı hesabı silindi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1331
Kaspersky Security Center olay kimliği	00000533
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Kimlik Doğrulama Aracısı hesabı parolası değiştirildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1332
Kaspersky Security Center olay kimliği	00000534
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Başarılı Kimlik Doğrulama Aracısı oturum açılışı

Durum	
Bileşen	Veri Şifreleme
Windows olay kimliği	1333
Kaspersky Security Center olay kimliği	00000535
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Başarısız Kimlik Doğrulama Aracısı oturum açma girişimi

Durum	
Bileşen	Veri Şifreleme
Windows olay kimliği	1334
Kaspersky Security Center olay kimliği	00000536
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Şifrelenmiş aygıtlara erişim talep etme prosedürü kullanılarak sabit sürücüye erişildi

Durum	
Bileşen	Veri Şifreleme
Windows olay kimliği	1335
Kaspersky Security Center olay kimliği	00000537
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Şifrelenmiş aygıtlara erişim talep etme prosedürünü kullanarak sabit sürücüye erişim girişimi başarısız

Durum	
Bileşen	Veri Şifreleme
Windows olay kimliği	1336
Kaspersky Security Center olay kimliği	00000538
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Hesap eklenmedi. Bu hesap zaten mevcut

Durum	
Bileşen	Veri Şifreleme
Windows olay kimliği	1337
Kaspersky Security Center olay kimliği	00000539
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Hesap değiştirilmedi. Bu hesap mevcut değil

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1338
Kaspersky Security Center olay kimliği	0000053a
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Hesap silinmedi. Bu hesap mevcut değil

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1339
Kaspersky Security Center olay kimliği	0000053b
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

FDE yükseltmesi başarılı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1341
Kaspersky Security Center olay kimliği	0000053d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

FDE yükseltmesini geri alma başarılı

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1343
Kaspersky Security Center olay kimliği	0000053f
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

WinRE görüntüsünden Kaspersky Disk Encryption sürücülerinin kaldırılması başarısız oldu

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1346
Kaspersky Security Center olay kimliği	00000542
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

BitLocker kurtarma anahtarı değiştirildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1370
Kaspersky Security Center olay kimliği	0000055a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

BitLocker parolası/PIN değiştirildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1371
Kaspersky Security Center olay kimliği	0000055b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

BitLocker kurtarma anahtarı bir çıkarılabilir sürücüye kaydedildi

Durum	ⓘ
Bileşen	Veri Şifreleme
Windows olay kimliği	1372
Kaspersky Security Center olay kimliği	0000055c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Anti Targeted Attack Platform sunucusundan gelen görevleri işleme etkin değil

Durum	ⓘ
Bileşen	Endpoint Sensor
Windows olay kimliği	2103
Kaspersky Security Center olay kimliği	00000837
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Endpoint Sensor sunucuya bağlandı

Durum	ⓘ
Bileşen	Endpoint Sensor
Windows olay kimliği	2101
Kaspersky Security Center olay kimliği	00000835
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Anti Targeted Attack Platform sunucusu ile yeniden bağlantı kuruldu

Durum	ⓘ
Bileşen	Endpoint Sensor
Windows olay kimliği	2102
Kaspersky Security Center olay kimliği	00000836
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Anti Targeted Attack Platform sunucusundan gelen görevler işleniyor

Durum	ⓘ
Bileşen	Endpoint Sensor
Windows olay kimliği	2104
Kaspersky Security Center olay kimliği	00000838
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne silindi

Durum	ⓘ
Bileşen	Verileri sil
Windows olay kimliği	2251
Kaspersky Security Center olay kimliği	000008cb
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Silme görevi istatistikleri

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises)
Windows olay kimliği	2853
Kaspersky Security Center olay kimliği	00000b25
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Durum	ⓘ
Bileşen	Verileri sil
Windows olay kimliği	2253
Kaspersky Security Center olay kimliği	000008cd
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne karantinaya alındı (Sandbox)

Durum	ⓘ
Bileşen	Sandbox

Windows olay kimliği	2602
Kaspersky Security Center olay kimliği	00000a2a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne silindi (Sandbox)

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2604
Kaspersky Security Center olay kimliği	00000a2c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

IOC Taraması başlatıldı

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2652
Kaspersky Security Center olay kimliği	00000a5c
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

IOC Taraması tamamlandı

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2653
Kaspersky Security Center olay kimliği	00000a5d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne karantinaya alındı (Endpoint Detection and Response)

Durum	ⓘ
Bileşen	Endpoint Detection and Response
Windows olay kimliği	2555
Kaspersky Security Center olay kimliği	000009fb
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne silindi (Endpoint Detection and Response)

Durum	ⓘ
Bileşen	Endpoint Detection and Response

Windows olay kimliği	2557
Kaspersky Security Center olay kimliği	000009fd
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Uygulama bileşenleri başarıyla değiştirildi

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	1402
Kaspersky Security Center olay kimliği	0000057a
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2606
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2609
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2610
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2616
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Cihazınızın bağlı olduğu Yönetim Sunucusu güvenilir olarak ayarlanmıştır

Durum	ⓘ
Bileşen	Yönetim Sunucusu bağlantı koruması
Windows olay kimliği	3300
Kaspersky Security Center olay kimliği	00000ce4
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Cihazınız yeni bir güvenilir Yönetim Sunucusuna bağlandı

Durum	ⓘ
Bileşen	Yönetim Sunucusu bağlantı koruması
Windows olay kimliği	3302
Kaspersky Security Center olay kimliği	00000ce6
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Cihazınızın bağlı olduğu Yönetim Sunucusu artık güvenilir olarak ayarlı değil

Durum	ⓘ
Bileşen	Yönetim Sunucusu bağlantı koruması
Windows olay kimliği	3303
Kaspersky Security Center olay kimliği	00000ce7
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Eşzamanlı olmayan Sandbox algılaması

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2619
Kaspersky Security Center olay kimliği	GNRL_EV_APP_INCIDENT_OCCURED
Olay parametreleri	• GNRL_EA_PARAM_1, Sandbox bileşenlerinin parametreleridir. • GNRL_EA_PARAM_2 nesnenin yoludur. • GNRL_EA_PARAM_3 olayın kimliğidir. • GNRL_EA_PARAM_4, nesnenin karma değeridir (SHA256).
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Tarama görevi bir kullanıcı tarafından Sandbox'a başarıyla gönderildi

Durum	ⓘ
Bileşen	Sandbox
Windows olay kimliği	2622
Kaspersky Security Center olay kimliği	00000a3e
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aygıt bağlandı

Durum	ⓘ
Bileşen	Aygıt Denetimi
Windows olay kimliği	`805`
Kaspersky Security Center olay kimliği	`GNRL_EV_DEVCTRL_DEV_PLUGGED`
Olay parametreleri	• `GNRL_EA_PARAM_1` Donanım kimliğidir (HWID). • `GNRL_EA_PARAM_2` oturum açan kullanıcının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Aygıt bağlantısı kesildi

Durum	ⓘ
Bileşen	Aygıt Denetimi
Windows olay kimliği	`806`
Kaspersky Security Center olay kimliği	`GNRL_EV_DEVCTRL_DEV_UNPLUGGED`
Olay parametreleri	• `GNRL_EA_PARAM_1` Donanım kimliğidir (HWID). • `GNRL_EA_PARAM_2` oturum açan kullanıcının adıdır.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert sunucusuna bağlantı başarılı

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises)
Windows olay kimliği	`2853`
Kaspersky Security Center olay kimliği	`00000b25`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert yanıt sunucusuna başarılı bağlantı

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows olay kimliği	`2853`
Kaspersky Security Center olay kimliği	`00000b25`
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

EDR Expert telemetri toplama sunucusuna başarılı bağlantı

Durum	ⓘ
Bileşen	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)

Windows olay kimliği	2857
Kaspersky Security Center olay kimliği	00000b26
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

NDR sunucusuna bağlantı başarılı

Durum	ⓘ
Bileşen	Network Detection and Response (KATA)
Windows olay kimliği	3083
Kaspersky Security Center olay kimliği	00000c0b
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bulut hizmeti istemci uygulamasının başlatılmasına izin veriliyor

Durum	ⓘ
Bileşen	Cloud Discovery
Windows olay kimliği	2210
Kaspersky Security Center olay kimliği	000008a2
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bulut hizmetine erişime izin veriliyor

Durum	ⓘ
Bileşen	Cloud Discovery
Windows olay kimliği	2211
Kaspersky Security Center olay kimliği	000008a3
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Korunan alana erişim

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	2004
Kaspersky Security Center olay kimliği	000007d4
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Dosya veya klasör değişikliği tespit edildi

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme

Windows olay kimliği	2950
Kaspersky Security Center olay kimliği	00000b86
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Nesne çok sık değişiyor. Olay toplama başladı

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2955
Kaspersky Security Center olay kimliği	00000b8b
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Toplama dönemi için nesne değişikliği raporu

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2956
Kaspersky Security Center olay kimliği	00000b8c
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Kayıt defteri değişikliği tespit edildi

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2951
Kaspersky Security Center olay kimliği	00000b87
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Cihaz bağlantısı / bağlantı kesilmesi tespit edildi

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2952
Kaspersky Security Center olay kimliği	00000b88
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

İzleme kapsamı yanlış nesneler içeriyor

Durum	ⓘ / ⚠ / ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2903
Kaspersky Security Center olay kimliği	00000b89
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

Temel oluşturuldu

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2957
Kaspersky Security Center olay kimliği	00000b8d
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Temel güncellendi

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme
Windows olay kimliği	2958
Kaspersky Security Center olay kimliği	00000b8e
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Güvenilir kullanıcı tarafından bir işlem gerçekleştirildi

Durum	ⓘ
Bileşen	Sistem Bütünlüğü İzleme

Windows olay kimliği	2962
Kaspersky Security Center olay kimliği	00000b92
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bu olayın saklama süresini yapılandırmak için ilkenin **Olay yapılandırması** bölümüne gidin ve genel Sistem Bütünlüğü İzleme olayı - *Dosya veya klasör değişikliği tespit edildi* için saklama süresini ayarlayın.

SVM'ye bağlandı

Durum	ⓘ
Bileşen	Light Agent
Windows olay kimliği	3152
Kaspersky Security Center olay kimliği	00000c50
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yeni bir geçici parola oluşturuldu

Durum	ⓘ
Bileşen	Sistem Denetimi
Windows olay kimliği	265
Kaspersky Security Center olay kimliği	00000109
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Entegrasyon Sunucusuna bağlantı sağlandı

Durum	ⓘ
Bileşen	Light Agent
Windows olay kimliği	3105
Kaspersky Security Center olay kimliği	00000c21
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Entegrasyon Sunucusuna bağlantı tekrar kuruluyor

Durum	ⓘ
Bileşen	Light Agent
Windows olay kimliği	3104
Kaspersky Security Center olay kimliği	00000c20
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

KUMA sunucusuna bağlantı başarılı

Durum	ⓘ
Bileşen	KUMA Entegrasyonu
Windows olay kimliği	2857
Kaspersky Security Center olay kimliği	00000b29
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Ek 7. Yürütme önleme için desteklenen dosya uzantıları

Kaspersky Endpoint Security, belirli uygulamalarda ofis biçimindeki dosyaların açılmasının engellenmesini destekler. Desteklenen dosya uzantıları ve uygulamalar hakkındaki bilgiler aşağıdaki tabloda listelenmiştir.

Yürütme önleme için desteklenen dosya uzantıları

Uygulama adı	Yürütülebilir dosya	Dosya uzantısı
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Uygulama adı	Yürütülebilir dosya	Dosya uzantısı
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

Ek 8. Yürütme önleme için desteklenen komut dizisi yorumlayıcıları

Yürütme önleme, şu komut dosyası yorumlayıcılarını destekler:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Yürütme önleme, Java çalışma zamanı ortamında (java.exe ve javaw.exe processes) Java uygulamaları ile çalışmayı destekler.

Ek 9. Kayıt defterindeki IOC tarama kapsamı (RegistryItem)

Windows kayıt defteri - RegistryItem veri türünü IOC Taraması kapsamına eklediğinizde, Kaspersky Endpoint Security varsayılan olarak aşağıdaki kayıt defteri anahtarlarını tarar:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Ek 10. IOC dosya gereksinimleri

IOC Taraması görevleri oluştururken aşağıdaki IOC dosyası gereksinimlerini ve sınırlamalarını göz önünde bulundurun:

- Uygulama, güvenlik ihlali göstergelerini tanımlamak için açık standart OpenIOC 1.0 ve 1.1 sürümlerinde IOC ve XML uzantılarına sahip IOC dosyalarını destekler.
- IOC dosyalarını yükledikten sonra, dosyaları yerleşik düzenleyicide doğrudan görev özelliklerinde manuel olarak düzenleyebilirsiniz. Kaspersky Endpoint Security, OpenIOC 1.1 standardıyla uyumlu IOC dosyalarının düzenlenmesini destekler. OpenIOC sürüm 1.0 ile uyumlu IOC dosyalarının içeriğini değiştirmek mümkün değildir.
- Komut satırında bir *IOC Taraması* görevi oluşturulurken, bazıları desteklenmeyen IOC dosyalarını yüklemeniz durumunda, görev çalıştırıldığında uygulama sadece desteklenen IOC dosyalarını kullanır. Komut satırında bir *IOC Taraması* görevi oluşturulurken yüklediğiniz tüm IOC dosyalarının desteklenmediği ortaya çıkması durumunda, görev yine de çalıştırılabilir ancak herhangi bir güvenlik ihlali göstergeleri tespit edilmeyecektir. Web Console veya Cloud Console kullanılarak desteklenmeyen IOC dosyalarının yüklenmesi mümkün değildir.

- IOC dosyalarındaki anlamsal hatalar ve desteklenmeyen IOC terimleri ve etiketleri, görevin yürütülmesinde başarısızlığa neden olmaz. IOC dosyalarının bu tür bölümlerinde uygulama hiçbir eşleşme algılamaz.
- Tek bir IOC Taraması görevinde kullanılan tüm IOC dosyalarının tanımlayıcıları benzersiz olmalıdır. Aynı tanımlayıcıya sahip IOC dosyaları olduğunda, bu görev yürütme sonuçlarını etkileyebilir.
- Tek bir IOC dosyasının en fazla 2 MB olabilir. Daha büyük dosyaların kullanılması, IOC Taraması görevlerinin bir hatayla sonlandırılmasına neden olur. IOC koleksiyonuna eklenen tüm dosyaların toplam boyutu en fazla 10 MB olabilir. Tüm dosyaların toplam boyutu 10 MB üzerinde olduğu takdirde, IOC koleksiyonunu bölmeniz ve birkaç *IOC Taraması* görevi oluşturmanız gerekir.
- Her tehdit başına bir IOC dosyası oluşturmanız önerilir. Böylece *IOC Taraması* görevinin sonuçlarını analiz etmek kolaylaşır.

Aşağıdaki bağlantıya tıklayarak indirebileceğiniz dosyada, OpenIOC standardının IOC terimlerinin tam listesini içeren bir tablo bulunur.

IOC_TERMS.XLSX DOSYASINI İNDİRİN

Uygulamanın OpenIOC standardını desteklemesine ilişkin özellikler ve sınırlamalar aşağıdaki tabloda gösterilmiştir.

OpenIOC sürüm 1.0 ve 1.1 desteğinin özellikleri ve sınırlamaları.

Desteklenen koşullar	OpenIOC 1.0:
	
	`is`
	`isnot` (setten bir istisna olarak)
	`contains`
	`containsnot` (setten bir istisna olarak)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	E-posta/* terimleri için, sadece `contains` ve `is` koşulları desteklenir. Geriye Dönük IOC Taraması'nın doğru çalışması için, `is` koşulu kullanılırken, IOC dosyalarındaki e-posta adresleri şu biçim kullanılarak belirtilmelidir: `"name@example.org" <SMTP:name@example.org>`. *IOC Taraması* görevini normal şekilde çalıştırırken, e-posta adresini aşağıdaki biçimde belirtmek yeterlidir: `name@example.org`.

Desteklenen koşulların özellikleri	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Desteklenen operatörler	`AND` `OR`
Desteklenen veri türleri	`"date"`: tarih (geçerli koşullar: `is`, `greater-than`, `less-than`) `"int"`: tamsayı (geçerli koşullar: `is`, `greater-than`, `less-than`) `"string"`: dize (geçerli koşullar: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: saniye olarak süre (geçerli koşullar: `is`, `greater-than`, `less-than`)

Veri türü yorumlama özellikleri	`"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` ve `"base64Binary"` veri türleri, dize olarak yorumlanır.
	
	Uygulama, aralıklar biçiminde ayarlandığında `int` ve `date` veri türleri için `Content` ayarının yorumlanmasını destekliyor:
	
	OpenIOC 1.0:
	`Content` alanında `TO` operatörünü kullanarak:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	`greater-than` ve `less-than` koşullarını kullanarak
	`Content` alanında `TO` operatörünü kullanarak
	Uygulama, `ISO 8601, Zulu time zone, UTC` biçiminde olduğu sürece `date` ve `duration` veri türlerinin yorumlanmasını destekler.

Ek 11. EDR Tehdit Yanıtı için API

Kaspersky Endpoint Security 12.9 for Windows, Kaspersky Security Center OpenAPI kullanan EDR Tehdit Yanıt eylemleri (EDR responses) için destek sunuyor. Yani, Python kullanarak EDR tehdit yanıtını otomatikleştirmek için OpenAPI yöntemlerini çağırabilirsiniz. SIEM çözümleri ile entegre edildiğinde bu yöntemleri çağırabilirsiniz. Kaspersky SIEM çözümü olan *Kaspersky Unified Monitoring and Analysis Platform*, 3.4.1 sürümünden itibaren EDR Tehdit Yanıtı OpenAPI'yi destekliyor. Örnek komut dizileri için lütfen KUMA belgelerine bakın.

EDR Tehdit Yanıtı eylemlerini gerçekleştirmek için bir istek oluşturmanız ve bunu KSC Open API (`AddIncident`) kullanarak göndermeniz gerekir. Talep işlendikten sonra Kaspersky Security Center konsolunda özel bir görev oluşturulur.

EDR tehditlerine yanıt verirken görevler oluşturmak için Yönetim Sunucusu ile Kaspersky Security Center Web Console arasında bir arka plan bağlantısı kurmanız gerekir. Arka plan bağlantısı hizmeti Kaspersky Security Center Windows 14.2 veya sonraki sürümlerinde ve Kaspersky Security Center Linux 15.2 veya üzerinde bulunur. Kaspersky Detection and Response çözümlerinin konsolları da dahil olmak üzere diğer konsollar desteklenmez.

EDR Tehdit Yanıtı için, örneğin JSON biçiminde temel istek parametrelerini belirtmeniz gerekir:

- `task` görevin türüdür (aşağıya bakın).
- `targetHost` komut dizisinin çalıştırılacağı bilgisayarın kimliğidir. Gerekli argüman. Komut dizisi bu argümanı olaydan alır.
- `responseEventIncidentArea`, komut dizisini çalıştıran uygulamanın adıdır (örneğin `KUMA`). Bu parametre oluşturulan görevin adına eklenir.

EDR Tehdit Yanıtını yapılandırmak için, görev ayarlarını `"KLINCDT_BODY": json.dumps(data)` parametresinde JSON biçiminde belirtmeniz gerekir. Sonuç olarak uygulama Kaspersky Security Center Konsolunda `[Response] [KUMA] <task type> - <Date> <Time> - <ID>` görevini oluşturur.

Kaspersky Security Center OpenAPI'ye bağlanma

EDR Threat Response'un bir parçası olarak uygulama, Kaspersky Security Center konsolunda özel görevler oluşturur. Bu görevlerin oluşturulması için bilgisayar ile Kaspersky Security Center arasında bir bağlantı kurulması gerekir. Bunu başarmak için istekte Kaspersky Security Center bağlantı parametrelerinin belirtilmesi gerekir.

Kaspersky XDR 2.1 sürümünde, taleplerin yetkilendirilme yöntemi değiştirilmiştir. Kaspersky XDR, kullanıcı adı ve parola ile kimlik doğrulama yerine PAT belirteçlerini kullanır. Bu nedenle, Kaspersky XDR'da komut dosyalarını çalıştırmak mümkün değildir. İzin talebi hakkında daha fazla bilgi için lütfen Kaspersky XDR Yardım bölümüne bakın.

Kaspersky Security Center bağlantı parametreleri

Parametre	Tür	Açıklama
`kscHost`	`string`	Kaspersky Security Center Yönetim Sunucusu Adresi. Gerekli parametre.
`kscPort`	`int`	Yönetim Sunucusu bağlantı portu. Gerekli parametre.
`kscCert`	`string`	Kaspersky Security Center Yönetim Sunucusu'na bağlanmak için bir sertifika dosyasının yolu. Parametre varsayılan olarak `False` ayarlanmıştır.
`kscUser`	`string`	Kullanıcı hesabı adı. Gerekli parametre.
`kscPassword`	`string`	Kullanıcı hesabı parolası. Gerekli parametre.

Örnek

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Kullanıcı hesabı verileri korunmaz, bu nedenle yalnızca bu eylemleri gerçekleştirmek için kullanılacak ayrı bir kullanıcı tahsis etmeniz gerekir.

Dosyayı al – getFile

Dosyayı al görev ayarları

Parametre	Tür	Açıklama
`md5hash`	`string`	Almak istediğiniz dosyanın MD5 karması.
`sha256hash`	`string`	Almak istediğiniz dosyanın SHA256 karması.
`path`	`string`	Almak istediğiniz dosyanın yolu.

Örnek

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Dosyayı sil – deleteFile

Dosyayı sil görev ayarları

Parametre	Tür	Açıklama
`md5hash`	`string`	Silmek istediğiniz dosyanın MD5 karması.
`sha256hash`	`string`	Silmek istediğiniz dosyanın SHA256 karması.
`path`	`string`	Silmek istediğiniz dosyanın yolu.
`searchInSubfolders?`	`boolean`	Silmek istediğiniz dosyayı alt klasörlerde arayın.

Örnek

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Dosyayı Karantinaya taşı – quarantineFile

Dosyayı Karantinaya taşı görev ayarları

Parametre	Tür	Açıklama
`md5hash`	`string`	Karantinaya almak istediğiniz dosyanın MD5 karması.
`sha256hash`	`string`	Karantinaya almak istediğiniz dosyanın SHA256 karması.
`path`	`string`	Karantinaya almak istediğiniz dosyanın yolu.

Örnek

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

IOC Taraması – iocScan

IOC Taraması görev ayarları

Parametre	Tür	Açıklama
`ioc`	`string`	Tarama için kullanmak istediğiniz IOC dosyasını içeren ZIP arşivinin yolu.
`isolateHost`	`boolean`	Tehdidin yayılmasını önlemek için bir tehlike göstergesi tespit edildiğinde bilgisayarı ağdan izole edin.
`scanCriticalAreas`	`boolean`	Bir tehlikeye girme göstergesi tespit edildiğinde *Kritik Alanları Tarama* görevini çalıştırın.
`quarantineObject`	`boolean`	Bir güvenlik ihlali algılandığında kötü amaçlı nesneyi silin. Kaspersky Endpoint Security, nesneyi silmeden önce nesnenin daha sonra geri yüklenmesi gerekebileceği ihtimaline karşı bir yedek kopya oluşturur. Kaspersky Endpoint Security, yedek kopyayı Karantinaya taşır.

Örnek

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

İşlemi başlat – startProcess

İşlemi başlat görev ayarları

Parametre	Tür	Açıklama
`executablePath`	`string`	İşlemi başlatmak için kullanılan yürütülebilir dosyanın yolu.
`arguments?`	`string`	Süreci başlatmak için ek komut satırı argümanları.
`workingFolder?`	`string`	Sürecin çalışma klasörünün yolu.

Örnek

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

İşlemi sonlandır – terminateProcess

İşlemi sonlandır görev ayarları

Parametre	Tür	Açıklama
`md5hash`	`string`	İşlemini sonlandırmak istediğiniz dosyanın MD5 karması.
`sha256hash`	`string`	İşlemini sonlandırmak istediğiniz dosyanın SHA256 karması.
`path`	`string`	Silmek istediğiniz dosyanın yolu.
`caseSensitive`	`boolean`	Dosya aranırken büyük/küçük harf duyarlılığı.

Örnek

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Bilgisayar ağ izolasyonu – isolateHost

Bilgisayar ağ izolasyonu ayarları

Parametre	Tür	Açıklama
`action`	`string`	Ağ izolasyonunun çalışma modu.

Örnek

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Yürütme önleme – preventExecution

Yürütme önleme ayarları

Parametre	Tür	Açıklama
`hash`	`string`	Çalışmasını engellemek istediğiniz dosyanın MD5 karması.
`path`	`string`	Çalışmasını engellemek istediğiniz dosyanın yolu.
`caseSensitive`	`boolean`	Dosya aranırken büyük/küçük harf duyarlılığı.

Örnek

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Kötü Amaçlı Yazılım Taraması – onDemandScan

Kötü Amaçlı Yazılım Taraması görev ayarları

Parametre	Tür	Açıklama
`path`	`string`	Özel Tarama için dosya ve klasörlerin alanla sınırlandırılmış listesi.
`recursive`	`boolean`	Tekrarlayan tarama modu.

Parametre	Tür	Açıklama
type	number	Tarama kapsamı.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Örnek

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Ek 12. Uygulama bileşeni kurallarında kullanıcı hesapları

Bazı uygulama bileşenlerini yapılandırmak için özel kurallar eklemeniz gerekir. Örneğin, İnternet Denetimi için, uygulamanın engellemesini istediğiniz web adreslerinin listesini içeren bir kural eklemelisiniz. Uygulama bileşeni kurallarında, bileşen için bir zamanlama da yapılandırabilir veya uygulamanın kuralı uygulaması gereken kullanıcıları seçebilirsiniz.

Aşağıdaki uygulama bileşenlerini yapılandırmak için kurallar eklenmelidir:

- Uygulama Denetimi.
- İnternet Denetimi.
- Aygıt Denetimi.
- Günlük Denetimi.
- Uyarlamalı Anomali Denetimi.
- Sistem Bütünlüğü İzleme.

Kaspersky Endpoint Security for Windows 12.5 sürümünden itibaren, yalnızca Active Directory'den değil, Kaspersky Security Center'daki kullanıcı listesinden de kullanıcıları seçebilirsiniz. Yerel kullanıcı hesabı verilerini manuel olarak da girebilirsiniz. Bu, aşağıdaki şekillerde kullanıcı ekleyebileceğiniz anlamına gelir:

- Active Directory (önerilir)
- Kaspersky Security Center'daki kullanıcıların listesi
- Yerel kullanıcı hesabı

Tüm kullanıcı seçim yöntemlerini doğru şekilde kullanmak için Kaspersky Endpoint Security uygulamasını ve yönetim eklentisini 12.5 veya daha yüksek bir sürüme güncellemeniz gerekir.

Kaspersky, yerel kullanıcı hesaplarının yalnızca etki alanı kullanıcı hesaplarının kullanılmasının mümkün olmadığı özel durumlarda kullanılmasını önerir. Yerel hesapları kullanmanın güvenlik riskleri hakkında ayrıntılı bilgi için Microsoft Bilgi Bankası 'na bakın. Yerel kullanıcı hesapları kullanılıyorsa bilgisayarın güvenliğiyle ilgili tüm sorumluluk size aittir; özellikle Kaspersky Endpoint Security ayarlarına erişimi kontrol etme ve kısıtlama sorumluluğu da buna dahildir.

Uygulama, kullanıcıları tanımlamak için kullanıcının SID'sini (Güvenlik Tanımlayıcısı) kullanır. Active Directory'den veya Kaspersky Security Center kullanıcı listesinden kullanıcı hesapları kullanılırken, uygulama Yönetim Sunucusundaki SID'yi belirler. Bu, uygulamanın bir kullanıcıyı tanımlamak için bilgisayara fazladan yük bindirmediği anlamına gelir. Bir uygulama kuralına 1000'den fazla yerel kullanıcı hesabı eklediyseniz, uygulamalar kullanıcıyı tanımlamak için etki alanı denetleyicisine başvurur. Bu da bilgisayar üzerindeki yükün artması anlamına gelir. Bilgisayardaki performans etkisini optimize etmek için Active Directory'deki veya Kaspersky Security Center kullanıcı listesindeki kullanıcı hesaplarını kullanmanızı öneririz.

Uygulama, `<username>` ve `<hostname>\<username>` biçimlerinde manuel olarak eklenen kullanıcı hesaplarının tanımlanması için NetBIOS adlarını kullanır. Bir NetBIOS adı en fazla 16 bayt (15 karakter) uzunluğunda olabilir. Bilgisayar adı 15 karakterden uzunsa, uygulama kullanıcıyı tanımlayamaz. Ardından uygulama kuralı devre dışı bırakır ve bir hata oluşturur, örneğin, *İnternet Denetimi: güvenlik tanımlayıcısıyla (SID) eşleşmeyen kullanıcı hesapları için kural tetikleme devre dışı*. Kuralın çalışması için bilgisayar adını manuel olarak kısaltmanız gerekir. Active Directory veya Kaspersky Security Center'dan kullanıcı hesapları ekleyebilirsiniz. Bu durumda, uygulama bilgisayar adını otomatik olarak kısaltır.

Kaspersky Endpoint Security, kurallarda yerleşik kullanıcıları ve grupları ("Tümü" grubu gibi) da destekler. Bir kullanıcının SID'sinin nasıl belirlendiğine bağlı olarak, uygulama yalnızca Active Directory'den eklenen yerleşik kullanıcı hesaplarının veya Kaspersky Security Center'daki kullanıcı listesinin kullanılmasına izin verir. Yerleşik bir kullanıcı hesabının yerel olarak eklendiği kurallar çalışmaz.

Yasal Bilgiler

Veri sağlama

Bu bölüm, Kaspersky Endpoint Security uygulamasının cihazda depolayabileceği ve çalışması sırasında Kaspersky'ye otomatik olarak iletebileceği veriler hakkında bilgiler içermektedir.

Alınan bilgiler Kaspersky tarafından Kaspersky'nin ilgili yönetmeliklerine ve yasalara uygun olarak korunmaktadır. Veriler, şifrelenmiş iletişim kanalları üzerinden aktarılır.

Son Kullanıcı Lisans Sözleşmesi kapsamında veri sağlama

Kaspersky Endpoint Security'yi etkinleştirmek için etkinleştirme kodu uygulanırsa uygulamanın doğru kullanıldığını doğrulamak amacıyla aşağıdaki bilgileri düzenli bir şekilde otomatik olarak göndermeyi 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 etkin anahtar tanımlayıcısı;
- İşletim sisteminin türü, sürümü ve bit hızı ile sanal ortamın adı (Kaspersky Endpoint Security sanal ortamda yüklüyse);
- Hak Sahibi hizmetlerine yönelik benzersiz istek kimliği;
- 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 bilgileri 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;
  - Etkin 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 sona erme 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 kalan gün sayısı;
  - Anahtarın eklenmesinden bu yana geçen gün sayısı;
  - Lisansın sona ermesinden bu yana geçen gün sayısı;
  - Geçerli lisansın uygulandığı bilgisayar sayısı;
  - Etkin anahtar;
  - Kaspersky Endpoint Security lisans süresi;
  - Lisansın geçerli durumu;
  - Geçerli lisans türü;
  - Uygulama türü;
  - Yükseltme görevinin başlatılmasının benzersiz kimliği;
  - Bilgisayardaki Kaspersky Endpoint Security yüklemesinin benzersiz kimliği;
  - Kaspersky Endpoint Security arabirimi dili.

Alınan bilgiler Kaspersky tarafından Kaspersky'nin ilgili yönetmeliklerine ve yasalara uygun olarak korunmaktadır. Veriler, şifrelenmiş iletişim kanalları üzerinden aktarılır.

Son Kullanıcı Lisans Sözleşmesi'ni kabul ettikten ve Kaspersky Security Network Bildirimini 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 web sitesini ziyaret edin. License.txt ve ksn_<dil kodu>.txt dosyaları Son Kullanıcı Lisans Sözleşmesi ile Kaspersky Security Network Bildirimi metnini içerir ve uygulama dağıtım kitinde yer almaktadır.

Kaspersky Security Network kullanırken veri sağlama

Kaspersky Endpoint Security'nin Kaspersky'ye gönderdiği veri kümesi, lisans türüne ve Kaspersky Security Network kullanım ayarlarına bağlıdır.

KSN'nin lisans altında en fazla 4 bilgisayarda kullanılması

Kaspersky Security Network Bildirimi'ni kabul ederek şu bilgileri otomatik olarak iletmeyi kabul etmiş olursunuz:

- KSN yapılandırma güncellemeleri hakkında bilgiler: etkin yapılandırmanın tanımlayıcısı, alınan yapılandırmanın tanımlayıcısı, yapılandırma güncellemesinin hata kodu;
- Taranan dosyalar ve URL adresleri hakkında bilgiler: taranan dosyanın sağlamaları (MD5, SHA2-256, SHA1) ve dosya şablonları (MD5), şablon boyutu, tespit edilen tehdidin türü ve Hak Sahibinin sınıflandırmasına göre adı, anti-virüs veritabanlarının tanımlayıcısı, tanınırlığın talep edildiği URL adresi ve yönlendirici URL adresi, bağlantının iletişim kuralı tanımlayıcısı ve kullanılan bağlantı noktası sayısı;
- Tehdidi algılayan tarama görevinin kimliği;
- Orijinalliğini doğrulamak için kullanılan dijital sertifikalar hakkında bilgiler: taranan nesneyi ve sertifikanın ortak anahtarını imzalamak için kullanılan sertifikanın sağlamaları (SHA256);
- Taramayı gerçekleştiren Yazılım bileşeninin tanımlayıcısı;
- Anti-virüs veritabanlarının ve bu anti-virüs veritabanlarındaki kayıtların kimlikleri;
- Yazılımın Bilgisayarda etkinleştirilmesi hakkında bilgiler: etkinleştirme hizmetinden gelen biletin imzalı başlığı (bölgesel etkinleştirme merkezinin tanımlayıcısı, etkinleştirme kodunun sağlaması, biletin sağlaması, biletin oluşturulma tarihi, biletin benzersiz tanımlayıcısı, bilet sürümü, lisans durumu, bilet geçerliliğinin başlangıç/bitiş tarihi ve saati, lisansın benzersiz tanımlayıcısı, lisans sürümü), bilet başlığını imzalamak için kullanılan sertifikanın tanımlayıcısı, anahtar dosyasının sağlaması (MD5);
- Hak Sahibinin Yazılımı hakkında bilgiler: tam sürüm, tür, Kaspersky hizmetlerine bağlanmak için kullanılan iletişim kuralının sürümü.

KSN'nin lisans altında en fazla 5 bilgisayarda kullanılması

Kaspersky Security Network Bildirimi'ni kabul ederek şu bilgileri otomatik olarak iletmeyi kabul etmiş olursunuz:

Kaspersky Security Network onay kutusu işaretlenirse ve **Genişletilmiş KSN modunu etkinleştir** onay kutusunun işareti kaldırılırsa, uygulama aşağıdaki bilgileri gönderir:

- KSN yapılandırma güncellemeleri hakkında bilgiler: etkin yapılandırmanın tanımlayıcısı, alınan yapılandırmanın tanımlayıcısı, yapılandırma güncellemesinin hata kodu;
- Taranan dosyalar ve URL adresleri hakkında bilgiler: taranan dosyanın sağlamaları (MD5, SHA2-256, SHA1) ve dosya şablonları (MD5), şablon boyutu, tespit edilen tehdidin türü ve Hak Sahibinin sınıflandırmasına göre adı, anti-virüs veritabanlarının tanımlayıcısı, tanınırlığın talep edildiği URL adresi ve yönlendirici URL adresi, bağlantının iletişim kuralı tanımlayıcısı ve kullanılan bağlantı noktası sayısı;
- Tehdidi algılayan tarama görevinin kimliği;
- Orijinalliğini doğrulamak için kullanılan dijital sertifikalar hakkında bilgiler: taranan nesneyi ve sertifikanın ortak anahtarını imzalamak için kullanılan sertifikanın sağlamaları (SHA256);
- Taramayı gerçekleştiren Yazılım bileşeninin tanımlayıcısı;
- Anti-virüs veritabanlarının ve bu anti-virüs veritabanlarındaki kayıtların kimlikleri;
- Yazılımın Bilgisayarda etkinleştirilmesi hakkında bilgiler: etkinleştirme hizmetinden gelen biletin imzalı başlığı (bölgesel etkinleştirme merkezinin tanımlayıcısı, etkinleştirme kodunun sağlaması, biletin sağlaması, biletin oluşturulma tarihi, biletin benzersiz tanımlayıcısı, bilet sürümü, lisans durumu, bilet geçerliliğinin başlangıç/bitiş tarihi ve saati, lisansın benzersiz tanımlayıcısı, lisans sürümü), bilet başlığını imzalamak için kullanılan sertifikanın tanımlayıcısı, anahtar dosyasının sağlaması (MD5);
- Hak Sahibinin Yazılımı hakkında bilgiler: tam sürüm, tür, Kaspersky hizmetlerine bağlanmak için kullanılan iletişim kuralının sürümü.

Kaspersky Security Network onay kutusu ve **Genişletilmiş KSN modunu etkinleştir** onay kutusu işaretlenirse, uygulama yukarıda listelenen bilgilere ek olarak şu bilgiler de gönderir:

- Ana bilgisayarın işlenmiş URL ve IP adresini içeren istenen İnternet kaynaklarının kategorilere ayırma sonuçları, kategorilere ayırma işlemini gerçekleştiren Yazılım bileşeninin sürümü, kategorilere ayırma yöntemi ve İnternet kaynağı için tanımlanan kategori seti hakkında bilgiler;
- Bilgisayarda yüklü olan yazılım hakkında bilgiler: yazılım uygulamalarının ve yazılım satıcılarının adları, kayıt defteri anahtarları ve değerleri, yüklü yazılım bileşenlerinin dosyaları hakkında bilgiler (sağlamalar (MD5, SHA2-256, SHA1), ad, dosyanın Bilgisayardaki yolu, boyut, sürüm ve dijital imza);
- Bilgisayarın virüse karşı koruma durumu hakkında bilgiler: kullanılan antivirüs veritabanlarının sürümleri ve sürüm zaman damgaları, taramayı gerçekleştiren görevin ve Yazılımın tanımlayıcısı;
- Son Kullanıcı tarafından indirilen dosyalar hakkında bilgiler: indirilen dosyaların ve indirme sayfalarının URL'leri ve IP adresleri, indirme iletişim kuralın kimliği ve bağlantı noktasının numarası, URL'lerin zararlı veya değil olarak durumu, dosyanın öznitelikleri, boyutu ve sağlamaları (MD5, SHA2-256, SHA1), dosyayı indiren işlem hakkında bilgiler (sağlamalar (MD5, SHA2-256, SHA1), oluşturulma/yapı tarihi ve saati, otomatik oynatma durumu, öznitelikler, paketleyicilerin adları, imzalar hakkında bilgiler, yürütülebilir dosya bayrağı, biçim kimliği ve entropi), dosya adı ve dosyanın Bilgisayardaki yolu, dijital imzası ve oluşturulduğu zaman damgası, tehdidin tespit edildiği URL adresi, sayfada şüpheli veya zararlı görünen komut dizisi sayısı, oluşturulan HTTP istekleri ve bunlara verilen yanıtlara ilişkin bilgiler;

- Çalışan uygulamalar ve modülleri hakkında bilgiler: sistemde çalışan işlemler hakkında veriler (işlem kimliği (PID), işlem adı, işlemin başlatıldığı hesapla ilgili bilgiler, işlemi başlatan uygulama ve komut, güvenilir programın veya işlemin imzası, işlemin dosyalarının ve bunların sağlamalarının tam yolu (MD5, SHA2-256, SHA1), başlangıç komut satırı, işlemin bütünlük düzeyi, işlemin ait olduğu ürünün açıklaması (ürünün adı ve yayıncı hakkında bilgiler), ayrıca kullanılmakta olan dijital sertifikalar ve bunların orijinalliğini doğrulamak için gereken bilgiler veya bir dosyanın dijital imzasının olmadığıyla ilgili bilgiler) ve işlemlere yüklenen modüller hakkında bilgiler (adları, boyutları, türleri, oluşturulma tarihleri, öznitelikleri, sağlamaları (MD5, SHA2-256, SHA1), Bilgisayardaki yolları), PE dosyası başlık bilgisi, paketleyicilerin adları (dosya paketlenmişse);

- potansiyel olarak zararlı tüm nesneler ve etkinlikler hakkında bilgiler: tespit edilen nesnenin adı ve bilgisayardaki tam yolu, işlenen dosyaların sağlama toplamları (MD5, SHA2-256, SHA1), tespit tarihi ve saati, virüs bulaşmış dosyaların adları ve boyutları ile bunlara giden yollar, yol şablonu kodu, yürütülebilir dosya bayrağı, nesnenin bir Kapsayıcı olup olmadığına dair gösterge, paketleyicinin adları (dosya paketlenmişse), dosya türü kodu, dosya biçimi kimliği, kötü amaçlı yazılım tarafından gerçekleştirilen eylemlerin listesi ve bunlara yanıt olarak yazılım ve kullanıcı tarafından verilen karar, kararın alınmasında kullanılan antivirüs veritabanlarının ve bu veritabanlarındaki kayıtların kimlikleri, potansiyel olarak zararlı nesne göstergesi, Hak Sahibinin sınıflandırmasına göre tespit edilen tehdidin adı, tehlike seviyesi, tespit durumu ve tespit yöntemi, analiz edilen bağlama dahil edilme nedeni ve bağlamdaki dosyanın sıra numarası, sağlama toplamları (MD5, SHA2-256, SHA1), virüslü mesajın veya bağlantının iletildiği uygulamanın yürütülebilir dosyasının adı ve öznitelikleri, engellenen nesnenin ana bilgisayarının kimlik bilgileri gizlenmiş IP adresleri (IPv4 ve IPv6), dosya entropisi, dosya otomatik çalıştırma göstergesi, dosyanın sistemde ilk kez tespit edildiği zaman, son istatistiklerin gönderilmesinden bu yana dosyanın kaç kez çalıştırıldığı, kötü amaçlı nesnenin alındığı posta istemcisinin adı, sağlama toplamları (MD5, SHA2-256, SHA1) ve boyutu hakkında bilgiler, taramayı gerçekleştiren yazılım görevinin kimliği, dosya itibarının veya imzasının kontrol edilip edilmediğine dair gösterge, dosya işleme sonucu, nesne için toplanan kalıbın sağlama toplamı (MD5), kalıbın bayt cinsinden boyutu ve uygulanan algılama teknolojilerinin teknik özellikleri;

- Taranan nesneler hakkında bilgiler: dosyanın yerleştirildiği ve/veya alındığı atanan güvenilirlik grubu, dosyanın bu kategoriye yerleştirilme nedeni, kategori tanımlayıcısı, kategorilerin kaynağı hakkında bilgiler ve kategori veritabanının sürümü, dosyanın güvenilir sertifika bayrağı, dosyanın satıcısının adı, dosya sürümü, dosyayı içeren yazılım uygulamasının adı ve sürümü;

- Tespit edilen zayıf noktalarla ilgili bilgiler: zayıf noktaların veritabanındaki zayıf nokta kimliği, zayıf nokta tehlike sınıfı;

- Yürütülebilir dosyanın öykünmesi hakkında bilgiler: dosya boyutu ve sağlamaları (MD5, SHA2-256, SHA1), öykünme bileşeninin sürümü, öykünme derinliği, öykünme sırasında elde edilen mantıksal blokların ve mantıksal bloklar içindeki işlevlerin özelliklerinin bir dizisi, yürütülebilir dosyanın PE başlıklarından veriler;

- saldıran bilgisayarın IP adresleri (IPv4 ve IPv6), ağ saldırısının yönlendirildiği Bilgisayardaki bağlantı noktası sayısı, saldırının bulunduğu IP paketinin iletişim kuralının tanımlayıcısı, saldırının hedefi (kuruluş adı, İnternet sitesi), saldırıya verilen tepkinin bayrağı, saldırının ağırlığı, güven düzeyi;

- Ziyaret edilen web sitelerinin DNS ve IP adreslerinin (IPv4 veya IPv6) veya ağ kaynaklarının aldatıcı olmasıyla ilişkili saldırılar hakkında bilgiler;

- İstenen İnternet kaynağının DNS ve IP adresleri (IPv4 veya IPv6), İnternet kaynağına erişen dosya ve İnternet istemcisi hakkında bilgiler, dosyanın adı, boyutu ve sağlamaları (MD5, SHA2-256, SHA1), dosyanın tam yolu ve yol şablon kodu, dijital imza denetiminin sonucu ve KSN'deki durumu;

- Zararlı yazılım eylemlerini geri alma işlemi hakkında bilgiler: eylemi geri alınan dosyadaki veriler (dosyanın adı, dosyanın tam yolu, boyutu ve sağlamaları (MD5, SHA2-256, SHA1)), başarılı ve başarısız dosya silme, yeniden adlandırma ve kopyalama ile kayıt defterindeki değerleri geri yükleme (kayıt defteri anahtarlarının adları ve değerleri) eylemlerine ilişkin veriler ve geri alma işleminden önce ve sonra zararlı yazılım tarafından değiştirilen sistem dosyaları hakkında bilgiler;

- Uyarlamalı Anomali Denetimi bileşeni için ayarlanan istisnalar hakkında bilgiler: tetiklenen kuralın kimliği ve durumu, kural tetiklendiğinde Yazılım tarafından gerçekleştirilen eylem, işlemin veya tehdidin şüpheli etkinliği gerçekleştirdiği kullanıcı hesabının türü, şüpheli etkinliğe maruz kalan işlem hakkında bilgiler (komut dizisi kimliği veya işlem dosyası adı, işlem dosyasının tam yolu, yol şablon kodu, işlem dosyasının sağlamaları (MD5, SHA2-256, SHA1)); şüpheli eylemleri gerçekleştiren nesne ve şüpheli eylemlere maruz kalan nesne hakkında bilgiler (kayıt defteri anahtarı adı veya dosya adı, dosyanın tam yolu, yol şablon kodu ve dosyanın sağlamaları (MD5, SHA2-256, SHA1)).

- Yüklü yazılım modülleri hakkında bilgiler: modül dosyasının adı, boyutu ve sağlamaları (MD5, SHA2-256, SHA1), dosyanın tam yolu ve yol şablon kodu, modül dosyasının dijital imza ayarları, imza oluşturma tarihi ve saati, modül dosyasını imzalayan kişi ve kuruluşun adı, modülün yüklendiği işlemin kimliği, modül tedarikçisinin adı ve yükleme kuyruğundaki modülün sıra numarası;

- Yazılımın KSN hizmetleriyle etkileşim kalitesi hakkında bilgiler: istatistiklerin oluşturulduğu dönemin başlangıç ve bitiş tarihi ve saati, isteklerin kalitesi ve kullanılan her bir KSN hizmeti bağlantısı hakkında bilgiler (KSN hizmeti kimliği, başarılı istek sayısı, önbellekten yanıtları olan istek sayısı, başarısız istek sayısı (ağ sorunları, Yazılım ayarlarında KSN'nin devre dışı bırakılması, hatalı yönlendirme), başarılı isteklerin zaman yayılımı, iptal edilen isteklerin zaman yayılımı, süre sınırını aşan isteklerin zaman yayılımı, önbellekten alınan KSN bağlantısı sayısı, başarılı KSN bağlantısı sayısı, başarısız KSN bağlantısı sayısı, başarılı işlem sayısı, başarısız işlem sayısı, başarılı KSN bağlantılarının zaman yayılımı, başarısız KSN bağlantılarının zaman yayılımı, başarılı işlemlerin zaman yayılımı, başarısız işlemlerin zaman yayılımı);

- Potansiyel olarak zararlı bir nesne algılanırsa işlemlerin belleğindeki veriler hakkında bilgiler sağlanır: sistem nesnesi hiyerarşisinin öğeleri (ObjectManager), UEFI BIOS belleğindeki veriler, kayıt defteri anahtarlarının adları ve değerleri;

- Sistem günlüklerindeki olaylar hakkında bilgiler: olayın zaman damgası, olayın tespit edildiği günlüğün adı, olay türü ve kategorisi, olay kaynağının adı ve olayın açıklaması;

- Ağ bağlantıları hakkında bilgiler: portu açan ve işlemin başlatıldığı dosyanın sürümü ve sağlamaları (MD5, SHA2-256, SHA1), işlem dosyasının yolu ve dijital imzası, yerel ve uzak IP adresleri, yerel ve uzak bağlantı portlarının numaraları, bağlantı durumu ve portun açılışının zaman damgası;

- Yazılım kurulumu ve Bilgisayadaki etkineştirme tarihi hakkında bilgiler: lisansı satan ortağın kimliği, lisansın seri numarası, etkinleştirme hizmetinden gelen biletin imzalı başlığı (bölgesel etkinleştirme merkezinin kimliği, Etkinleştirme kodunun sağlama toplamı, biletin sağlama toplamı, bilet oluşturma tarihi, biletin benzersiz kimliği, bilet sürümü, lisans durumu, bilet başlangıç/bitiş tarihi ve saati, lisansın benzersiz kimliği, lisans sürümü), bilet başlığını imzalamak için kullanılan sertifikanın kimliği, anahtar dosyasının sağlama toplamı (MD5), Bilgisayardaki Yazılım kurulumunun benzersiz kimliği, güncellenen uygulamanın türü ve kimliği, güncelleme görevi;

- Yüklenen tüm güncellemeler kümesi, en son yüklenen/kaldırılan güncellemeler kümesi, güncellenen bilgilerin gönderilmesine neden olan olay türü, en son güncellemenin yüklenmesinden bu yana geçen süre ve şu anda yüklü olan tüm antivirüs veritabanları hakkında bilgiler;

- Bilgisayarda yazılımın çalışması hakkında bilgiler: CPU kullanımına ilişkin veriler, bellek kullanımına ilişkin veriler (Özel Bayt Sayısı, Disk Belleği Olmayan Havuz, Disk Belleği Havuzu), yazılım işlemindeki etkin tehditlerin ve bekleyen tehditlerin sayısı ve hatadan önce yazılımın işlem süresi;

- Yazılımın yüklenmesinden ve son güncellemeden bu yana yazılım dökümlerinin ve sistem dökümlerinin (BSOD) sayısı, çöken Yazılım modülünün kimliği ve sürümü, Yazılım işlemindeki bellek yığını ve çözme zamanındaki antivirüs veritabanları hakkında bilgiler;

- Sistem dökümü (BSOD) hakkındaki veriler: Bilgisayardaki BSOD oluşumunu gösteren bir bayrak, BSOD'ye neden olan sürücünün adı, sürücüdeki adres ve bellek yığını, BSOD meydana gelmeden önce işletim sistemi oturumunun süresini gösteren bir bayrak, çöken sürücünün bellek yığını, saklanan bellek dökümünün türü, BSOD'den önceki işletim sistemi oturumunun 10 dakikadan uzun sürdüğünü gösteren bayrak, dökümün benzersiz tanımlayıcısı, BSOD'nin zaman damgası;

- Yazılım bileşenlerinin çalışması sırasında oluşan hatalar veya performans sorunları hakkında bilgiler: Yazılımın durum kimliği, hata türü, kodu ve nedeni ile hatanın oluşma zamanı, hatanın oluştuğu ürünün bileşen, modül ve işlem kimlikleri, hatanın oluşma zamanındaki görevin veya güncelleme kategorisinin kimliği, Yazılım tarafından kullanılan sürücülerin günlükleri (hata kodu, modül adı, kaynak dosyanın adı ve hatanın oluştuğu satır);

- antivirüs veritabanlarının ve Yazılım bileşenlerinin güncellemeleri hakkında bilgiler: son güncellemede indirilen ve mevcut güncellemede indirilmekte olan dizin dosyalarının adı, tarihi ve saati;

- Yazılım işleminin anormal sonlandırması hakkında bilgiler: dökümün oluşturulma zaman damgası, türü, Yazılım işleminin anormal sonlandırılmasına neden olan olay türü (beklenmeyen kapanma, üçüncü taraf uygulamanın çökmesi), beklenmedik kapanmanın tarihi ve saati;

- Yazılım sürücülerinin donanım ve Yazılım ile uyumluluğu hakkında bilgiler: Yazılım bileşenlerinin işlevselliğini kısıtlayan işletim sistemi özellikleri (Secure Boot, KPTI, WHQL Enforce, BitLocker, Büyük/Küçük Harf Duyarlılığı) hakkında bilgiler, yüklenen indirme Yazılımının türü (UEFI, BIOS), Güvenilir Platform Modülü (TPM) tanımlayıcısı, TPM teknik bilgi sürümü, Bilgisayara yüklü CPU hakkında bilgiler, Kod Bütünlüğü ve Aygıt Korumasının işletim modu ve parametreleri, sürücülerin işletim modu ve geçerli modun kullanım nedeni, Yazılım sürücülerinin sürümü, Bilgisayarın yazılım ve donanım sanallaştırma desteği durumu;

- Hataya neden olan üçüncü taraf uygulamalar hakkında bilgiler: adları, sürümleri ve yerelleştirmeleri, hata kodu ve uygulamaların sistem günlüğünden gelen hata hakkında bilgiler, hatanın adresi ve üçüncü taraf uygulamanın bellek yığını, Yazılım bileşeninde hatanın oluştuğunu gösteren bayrak, üçüncü taraf uygulamanın hata oluşmadan önce çalıştığı süre, hatanın oluştuğu uygulama işlem görüntüsünün sağlamaları (MD5, SHA2-256, SHA1), uygulama işlem görüntüsünün yolu ve yolun şablon kodu, uygulama ile ilişkili hatanın bir açıklaması bulunan ve sistem günlüğünden gelen bilgiler, hatanın oluştuğu uygulama modülü hakkında bilgiler (istisna tanımlayıcısı, uygulama modülünde ofset olarak kaza belleği adresi, modülün adı ve sürümü, Hak Sahibinin eklentisinde uygulama çökme kimliği ve çökmenin bellek yığını, uygulamanın çökmeden önceki oturumun süresi);

- Yazılım güncelleyici bileşeninin sürümü, bileşen ömrü boyunca güncelleme görevlerini çalıştırırken güncelleyici bileşeninin çökme sayısı, güncelleme görevi türünün kimliği, güncelleme görevini tamamlamak için güncelleme bileşeninin başarısız olan deneme sayısı;

- Yazılım sistemi izleme bileşenlerinin çalışması hakkında bilgiler: bileşenlerin tam sürümleri, bileşenlerin başlatıldığı tarih ve saat, olay sırasını aşan olayın kodu ve bu tür olayların sayısı, sırayı aşan olaylarının toplam sayısı, olayı başlatan işlemin dosyası hakkında bilgiler (dosya adı ve dosyanın Bilgisayardaki yolu, dosya yolunun şablon kodu, dosyayla ilişkili işlemin sağlamaları (MD5, SHA2-256, SHA1), dosya sürümü), gerçekleşen olay durdurmanın kimliği, durdurma filtresinin tam sürümü, durdurulan olay türünün tanıtıcısı, olay sırasının boyutu ve sıradaki ilk olay ile geçerli olay arasındaki olay sayısı, sıradaki gecikmiş olayların sayısı, geçerli olayı başlatan işlemin dosyası hakkında bilgiler (dosya adı ve dosyanın Bilgisayardaki yolu, dosya yolunun şablon kodu, dosyayla ilişkili işlemin sağlamaları (MD5, SHA2-256, SHA1)), olay işleme süresi, olay işlemenin maksimum süresi, istatistik gönderme olasılığı, işlem süresi sınırının aşıldığı işletim sistemi olayları hakkında bilgiler (olayın tarihi ve saati, antivirüs veritabanlarının tekrarlanan başlatma sayısı, güncellendikten sonra antivirüs veritabanlarının son tekrarlanan başlatma işleminin tarihi ve saati, her bir sistem izleme bileşeni için olay işleme gecikme süresi, sıraya alınmış olay sayısı, işlenmiş olay sayısı, geçerli türde gecikmiş olay sayısı, geçerli türdeki olayların toplam gecikme süresi, tüm olayların toplam gecikme süresi);

- Yazılım performans sorunlarında Windows olay izleme aracından (Windows için Olay İzleme, ETW) ve Microsoft'un SysConfig / SysConfigEx / WinSATAssessment olaylarının tedarikçilerinden gelen bilgiler: Bilgisayar hakkında bilgiler (model, üretici, kasa form faktörü, sürüm), Windows performans ölçümleri hakkında bilgiler (WinSAT değerlendirmeleri, Windows performans endeksi), etki alanı adı, fiziksel ve mantıksal işlemciler hakkında bilgiler (fiziksel ve mantıksal işlemci sayısı, üretici, model, adımlama düzeyi, çekirdek sayısı, saat frekansı, CPUID, önbellek özellikleri, mantıksal işlemci özellikleri, desteklenen modların göstergeleri ve talimatlar), RAM modülleri hakkında bilgiler (tür, form faktörü, üretici, model, kapasite, bellek ayırmanın taneciklilği), ağ arabirimleri hakkında bilgiler (IP ve MAC adresleri, ad, açıklama, ağ arabirimleri yapılandırması, ağ paketlerinin sayının ve boyutunun türe göre dağılımı, ağ değişim hızı, ağ hatası sayısının türe göre dağılımı), IDE denetleyicisi yapılandırması, DNS sunucularının IP adresleri, ekran kartı hakkında bilgiler (model, açıklama, üretici, uyumluluk, video belleği kapasitesi, ekran izni, piksel başına bit sayısı, BIOS sürümü), tak ve kullan aygıtlar hakkında bilgiler (ad, açıklama, aygıt tanımlayıcısı [PnP, ACPI], diskler ve depolama aygıtları hakkında bilgiler (disk veya flash sürücü sayısı, üretici, model, disk kapasitesi, silindir sayısı, silindir başına parça sayısı, parça başına sektör sayısı, sektör kapasitesi, önbellek özellikleri, sıralı numara, bölüm sayısı, SCSI denetleyicisi yapılandırması), mantıksal diskler hakkında bilgiler (sıralı numara, bölüm kapasitesi, birim kapasitesi, birim harfi, bölüm türü, dosya sistemi türü, küme sayısı, küme boyutu, küme başına sektör sayısı, boş ve dolu küme sayısı, önyüklenebilir birimin harfi, diskin başlangıcı ile ilgili bölümün ofset adresi), BIOS anakartı hakkında bilgiler (üretici, sürüm tarihi, sürüm), anakart hakkında bilgiler (üretici, model, tür), fiziksel bellek hakkında bilgiler (paylaşılan ve boş kapasite), işletim sistemi hizmetleri hakkında bilgiler (ad, açıklama, durum, etiket, işlemler hakkında bilgiler [ad ve PID]), Bilgisayarın enerji tüketimi parametreleri, kesme denetleyicisi yapılandırılması, Windows sistem klasörlerinin yolu (Windows ve System32), işletim sistemi hakkında bilgiler (sürüm, yapı, sürüm tarihi, ad, tür, kurulum tarihi), disk bellek dosyasının boyutu, monitörler hakkında bilgiler (sayı, üretici, ekran izni, çözünürlük kapasitesi, tür), ekran kartı sürücüsü hakkında bilgiler (üretici, sürüm tarihi, sürüm);

- Microsoft'un EventTrace / EventMetadata olaylarının tedarikçileri olan ETW'den gelen bilgiler: sistem olaylarının sırası hakkında bilgiler (tür, zaman, tarih, saat dilimi), izleme sonuçlarının bulunduğu dosya hakkında meta veriler (ad, yapı, izleme parametreleri, izleme işlemi sayısının türe göre dağılımı), işletim sistemi hakkında bilgiler (ad, tür, sürüm, yapı, sürüm tarihi, başlangıç zamanı);

- Microsoft'un İşlem / Microsoft Windows Çekirdek İşlemi / Microsoft Windows Çekirdek İşlemcisi Güç olaylarının tedarikçileri olan ETW'den gelen bilgiler: başlatılan ve tamamlanan işlemler hakkında bilgiler (ad, PID, başlangıç parametreleri, komut satırı, dönüş kodu, güç yönetimi parametreleri, başlangıç ve tamamlanma zamanı, erişim belirteci türü, SID, Oturum Kimliği, yüklü tanımlayıcı sayısı), tehdit önceliklerindeki değişiklikler hakkında bilgiler (TID, öncelik, zaman), işlemin disk işlemleri hakkında bilgiler (tür, zaman, kapasite, sayı), kullanılabilir bellek işlemlerinin yapısı ve kapasitesinde yapılan değişikliklerin geçmişi hakkında bilgiler;

- Microsoft'un StackWalk / Perfinfo olaylarının tedarikçileri olan ETW'den gelen bilgiler: performans sayaçları hakkında bilgiler (kod bölümlerinin ayrı ayrı performansı, ISR'lerin ve DPC'lerin işlev çağrıları, PID, TID, adresleri ve özniteliklerinin sırası);

- Microsoft'un KernelTraceControl-ImageID olaylarının tedarikçisi olan ETW'den gelen bilgiler: yürütülebilir dosyalar ve dinamik kitaplıklar (ad, görüntü boyutu, tam yol) hakkında bilgiler, PDB dosyaları hakkında bilgiler (ad, tanımlayıcı), yürütülebilir dosyalar için VERSIONINFO kaynak verileri (ad, açıklama, oluşturan, yerelleştirme, uygulama sürümü ve kimliği, dosya sürümü ve kimliği);

- Microsoft'un FileIo / DiskIo / Image / Windows Çekirdek Diski olaylarının tedarikçileri olan ETW'den gelen bilgiler: dosya ve disk işlemleri hakkında bilgiler (tür, kapasite, başlangıç zamanı, tamamlanma zamanı, süre, tamamlanma durumu, PID, TID, sürücü işlev çağrısı adresleri, G/Ç İstek Paketi (IRP), Windows dosya nesnesi öznitelikleri), dosya ve disk işlemlerinde yer alan dosyalar hakkında bilgiler (ad, sürüm, boyut, tam yol, öznitelikler, ofset, görüntü sağlaması, açık seçenekler ve erişim seçenekleri);

- Microsoft'un PageFault olaylarının tedarikçisi olan ETW'den gelen bilgiler: bellek sayfası erişim hataları hakkında bilgiler (adres, zaman, kapasite, PID, TID, Windows dosya nesnesinin öznitelikleri, bellek ayırma parametreleri);

- Microsoft'un Thread olaylarının tedarikçisi olan ETW'den gelen bilgiler: tehdit oluşturulması/tamamlanması hakkında bilgiler, başlatılan tehditler hakkında bilgiler (PID, TID, yığın boyutu, CPU kaynaklarının öncelikleri ve ayrılması, G/Ç kaynakları, tehditler arasında bellek sayfaları, yığın adresi, init işlevinin adresi, Thread Environment Block adresi (TEB), Windows hizmet etiketi);

- Microsoft'un Microsoft Windows Çekirdek Belleği olaylarının tedarikçisi olan ETW'den gelen bilgiler: bellek yönetimi işlemleri (tamamlanma durumu, zaman, miktar, PID), bellek ayırma yapısı (tür, kapasite, Oturum Kimliği, PID);

- Performans sorunlarında Yazılımın çalışması hakkında bilgiler: Yazılım kurulum tanımlayıcısı, performans düşüşünün türü ve değeri, Yazılım içindeki olayların sırası hakkında bilgiler (zaman, saat dilimi, tür, tamamlanma durumu, Yazılım bileşeni tanımlayıcısı, Yazılım işletim senaryosu tanımlayıcısı, TID, PID, işlev çağrı adresleri), denetlenecek ağ bağlantıları hakkında bilgiler (URL, bağlantının yönü, ağ paketinin boyutu), PDB dosyaları hakkında bilgiler (ad, tanımlayıcı, yürütülebilir dosyanın görüntü boyutu), denetlenecek dosyalar hakkında bilgiler (ad, tam yol, sağlama), Yazılım performansı izleme parametreleri;

- İşletim sisteminin son başarısız yeniden başlatma işlemi hakkında bilgiler: işletim sistemi kurulumundan itibaren başarısız yeniden başlatma sayısı, sistem dökümü hakkında veriler (işletim sistemi çalışmasında hataya neden olan modülün hata kodu ve parametreleri, adı, sürümü ve sağlaması (CRC32), modülde ofset olarak hata adresi, sistem dökümünün sağlamaları (MD5, SHA2-256, SHA1));

- Dosyaları imzalamak için kullanılan dijital sertifikaların doğruluğunu onaylamaya ilişkin bilgiler: sertifikanın parmak izi, sağlama algoritması, sertifikanın genel anahtarı ve seri numarası, sertifikayı veren kuruluşun adı, sertifika doğrulama sonucu ve sertifikanın veritabanı tanımlayıcısı;

- Yazılımın kendini koruma bölümünde saldırıyı yürüten işlem hakkında bilgiler: işlem dosyasının adı ve boyutu, sağlamaları (MD5, SHA2-256, SHA1), işlem dosyasının tam yolu ve dosya yolunun şablon kodu, oluşturulma/yapı zaman damgaları, yürütülebilir dosya bayrağı, işlem dosyasının öznitelikleri, işlem dosyasını imzalamak için kullanılan sertifika hakkında bilgiler, işlemi başlatmak için kullanılan hesabın kodu, işleme erişmek için gerçekleştirilen işlemlerin kimliği, işlemin gerçekleştirildiği kaynağın türü (işlem, dosya, kayıt defteri nesnesi, FindWindow arama işlevi), işlemin gerçekleştirildiği kaynağın adı, işlem başarısını gösteren bayrak, işlem dosyasının durumu ve KSN'ye göre imzası;

- Hak Sahibinin Yazılımı hakkında bilgi: kullanılan Yazılımın tam sürümü, türü, yerelleştirilmesi ve çalışma durumu, yüklü Yazılım bileşenlerinin sürümleri ve çalışma durumu, yüklü Yazılım güncellemeleri hakkında bilgiler, HEDEF filtresinin değeri, Hak Sahibinin hizmetlerine bağlanmak için kullanılan iletişim kuralı sürümü;

- Bilgisayarda yüklü olan donanım hakkında bilgiler: tür, ad, model adı, ürün üretici yazılımı sürümü, yerleşik ve bağlı aygıtların parametreleri, yüklenen Yazılıma sahip Bilgisayarın benzersiz tanıtıcısı;

- İşletim sistemi sürümleri ve yüklenen güncellemeler, işletim sistemi çalışma modunun kelime boyutu, sürümü ve parametreleri, işletim sistemi çekirdek dosyasının sürümü ve sağlamaları (MD5, SHA2-256, SHA1) ile işletim sistemi başlangıç tarihi ve saati hakkında bilgiler;

- tamamen veya kısmen yürütülebilir ve yürütülebilir olmayan dosyalar;

- Bilgisayar RAM'inin kısımları;

- İşletim sisteminin önyükleme işlemine dahil olan kesimler;

- Ağ trafiği veri paketleri;

- Şüpheli ve zararlı nesneler içeren web sayfaları ve e-postalar;

- WMI veri havuzunun sınıflarının ve sınıf örneklerinin açıklaması;

- uygulama etkinlik raporları:
  - gönderilen dosyanın adı, boyutu ve sürümü, açıklaması ve sağlama toplamları (MD5, SHA2-256, SHA1), dosya türü tanımlayıcısı, dosyanın satıcısının adı, dosyanın ait olduğu ürünün adı, Bilgisayardaki dosyanın tam yolu, yolun şablon kodu, dosyanın oluşturuldığı ve değiştirildiği zaman damgaları;
  - sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihi/saati (dosyanın dijital imzası varsa), imzanın tarihi ve saati, sertifikayı veren kuruluşun adı, sertifika sahibi hakkında bilgiler, parmak izi, sertifikanın genel anahtarı ve uygun algoritmaları ve sertifikanın seri numarası;
  - işlemin çalıştığı hesabın adı;
  - işlemin üzerinde çalıştığı Bilgisayarın adının sağlama toplamları (MD5, SHA2-256, SHA1);
  - işlem pencerelerinin başlıkları;
  - antivirüs veritabanları için Tanımlayıcı, Hak Sahibinin sınıflandırmasına göre tespit edilen tehdidin adı;
  - yüklü Yazılım lisansı, tanımlayıcısı, türü ve bitiş tarihi hakkındaki veriler;
  - bilgi sağlama anında Bilgisayarın yerel saati;
  - işlem tarafından erişilen dosyaların adları ve yolları;
  - işlem tarafından erişilen kayıt defteri anahtarlarının adları ve değerleri;
  - işlem tarafından erişilen URL ve IP adresleri;
  - çalışan dosyanın indirildiği URL ve IP adresleri.

Detection and Response çözümlerini kullanırken veri sağlama

Kaspersky Endpoint Security yüklü bilgisayarlarda, Kaspersky Endpoint Detection and Response, Kaspersky Sandbox ve Kaspersky Anti Targeted Attack Platform sunucularına otomatik olarak gönderilmek üzere hazırlanan veriler depolanır. Dosyalar bilgisayarlarda düz, şifrelenmemiş biçimde depolanır.

Spesifik veri seti, Kaspersky Endpoint Security'nin kullanıldığı çözüme bağlıdır.

Kaspersky Endpoint Detection and Response

Uygulamanın bilgisayarda yerel olarak depoladığı tüm veriler, Kaspersky Endpoint Security kaldırıldığında bilgisayardan silinir.

IOC Taraması görevinin yürütülmesi (standart görev) sonucunda alınan veriler

Kaspersky Endpoint Security, *IOC Taraması* görevi yürütme sonuçlarına ilişkin verileri otomatik olarak Kaspersky Security Center'a gönderir.

IOC Taraması görevi yürütme sonuçlarındaki veriler şu bilgileri içerebilir:

- ARP tablosundan IP adresi
- ARP tablosundan fiziksel adres
- DNS kayıt türü ve adı
- Korunan bilgisayarın IP adresi
- Korunan bilgisayarın fiziksel adresi (MAC adresi)
- Olay günlüğü girişindeki tanımlayıcı
- Günlükteki veri kaynağı adı
- Günlük adı
- Olay zamanı
- Dosyanın MD5 ve SHA256 karmaları
- Dosyanın tam adı (yol dahil olmak üzere)
- Dosya boyutu
- Tarama sırasında bağlantı kurulan uzak IP adresi ve port
- Yerel bağdaştırıcı IP adresi
- Yerel bağdaştırıcıda açık port
- Sayı olarak protokol (IANA standardına uygun olarak)
- İşlem adı
- İşlem argümanları
- İşlem dosyasının yolu
- İşlemin Windows tanımlayıcısı (PID)
- Ana işlemin Windows tanımlayıcısı (PID)
- İşlemi başlatan kullanıcı hesabı
- İsteğin başladığı tarih ve saat
- Hizmet adı
- Hizmet açıklaması
- DLL hizmetinin yolu ve adı (svchost için)
- Hizmet yürütülebilir dosyasının yolu ve adı

- Hizmetin Windows tanımlayıcısı (PID)
- Hizmet türü (örneğin, bir çekirdek sürücüsü veya bağdaştırıcı)
- Hizmet durumu
- Hizmet başlatma modu
- Kullanıcı hesabı adı.
- Birim adı
- Birim harfi
- Birim tipi
- Windows kayıt defteri değeri
- Kayıt defteri kovanı değeri
- Kayıt anahtarı yolu (kovan ve değer adı olmadan)
- Kayıt defteri ayarı
- Sistem (ortam)
- Bilgisayarda yüklü olan işletim sisteminin adı ve sürümü
- Korunan bilgisayarın ağ adı
- Korunan bilgisayarın ait olduğu etki alanı veya grup
- Tarayıcı adı
- Tarayıcı sürümü
- Web kaynağına en son erişim zamanı
- HTTP isteğinden URL
- HTTP isteği için kullanılan hesabın adı
- HTTP isteğini yapan işlemin dosya adı
- HTTP isteğini yapan işlemin dosyasının tam yolu
- HTTP isteğini yapan işlemin Windows tanımlayıcısı (PID)
- HTTP yönelten (HTTP istek kaynağı URL'si)
- HTTP üzerinden istenen kaynağın URI'si
- HTTP kullanıcı aracısı (HTTP isteğini yapan uygulama) hakkında bilgi

- HTTP isteği yürütme süresi
- HTTP sorgusunu gerçekleştiren işlemin benzersiz tanımlayıcısı

Tehdit geliştirme zinciri oluşturmak için veriler

Bir tehdit geliştirme zinciri oluşturmak için kullanılan veriler varsayılan olarak yedi gün boyunca saklanır. Veriler otomatik olarak Kaspersky Security Center'a gönderilir.

Bir tehdit geliştirme zinciri oluşturmaya yönelik veriler şu bilgileri içerebilir:

- Olay tarihi ve saati
- Tespit adı
- Tarama modu
- Tespitle ilgili son eylemin durumu
- Tespit işleminin başarısız olmasının nedeni
- Tespit edilen nesne türü
- Tespit edilen nesne adı
- Nesne işlendikten sonra tehdit durumu
- Nesne üzerindeki eylemlerin yürütülmesinin başarısız olmasının nedeni
- Kötü amaçlı eylemleri geri almak için gerçekleştirilen eylemler
- İşlenen nesne hakkında bilgiler:
  - İşlemin benzersiz tanımlayıcısı
  - Ana işlemin benzersiz tanımlayıcısı
  - İşlem dosyasının benzersiz tanımlayıcısı
  - Windows işlem tanımlayıcısı (PID)
  - İşlem komut satırı
  - İşlemi başlatan kullanıcı hesabı
  - İşlemin çalıştığı giriş oturumunun kodu
  - İşlemin çalıştığı oturumun türü
  - İşlemnlemkte İşlenmekte olan işlemin bütünlük düzeyi
  - İşlemi başlatan kullanıcı hesabının ayrıcalıklı yerel ve etki alanı gruplarındaki üyeliği

- İşlenen nesnenin tanımlayıcısı
- İşlenen nesnenin tam adı
- Korunan aygıtın tanımlayıcısı
- Nesnenin tam adı (yerel dosya adı veya indirilen dosya web adresi)
- İşlenen nesnenin MD5 veya SHA256 karması
- İşlenen nesnenin türü
- İşlenen nşlenen nesnenin oluşturulma tarihi
- İşlenen nesnenin en son değiştirildiği tarih
- İşlenen nesnenin boyutu
- İşlenen nesnenin öznitelikleri
- İşlenen nesneyi imzalayan kuruluş
- İşlenen nesne dijital sertifika doğrulamasının sonucu
- İşlenen nesnenin güvenlik tanımlayıcısı (SID)
- İşlenen nesnenin saat dilimi tanımlayıcısı
- İşlenen nesnenin indirileceği web adresi (yalnızca diskteki dosyalar için)
- Dosyayı indiren uygulamanın adı
- Dosyayı indiren uygulamanın MD5 ve SHA256 karmaları
- Dosyayı en son değiştiren uygulamanın adı
- Dosyayı en son değiştiren uygulamanın MD5 ve SHA256 karmaları
- İşlenen nesne başlangıçlarının sayısı
- İşlenen nesnenin ilk başlatıldığı tarih ve saat
- Dosyanın benzersiz tanımlayıcıları
- Dosyanın tam adı (yerel dosya adı veya indirilen dosya web adresi)
- İşlenen Windows kayıt defteri değişkeninin yolu
- İşlenen Windows kayıt defteri değişkeninin adı
- İşlenen Windows kayıt defteri değişkeninin değeri
- İşlenen Windows kayıt defteri değişkeninin türü
- Otomatik çalıştırma noktasında işlenen kayıt defteri anahtarı üyeliğinin göstergesi

- İşlenen web isteğinin web adresi
- İşlenen web isteğinin bağlantı kaynağı
- İşlenen web isteğinin kullanıcı aracısı
- İşlenen web isteğinin türü (`GET` veya `POST`)
- İşlenen web isteğinin yerel IP portu
- İşlenen web isteğinin uzak IP portu
- İşlenen web isteğinin bağlantı yönü (gelen veya giden)
- Kötü amaçlı kodun gömülü olduğu işlemin tanımlayıcısı

Kaspersky Sandbox

Uygulamanın bilgisayarda yerel olarak depoladığı tüm veriler, Kaspersky Endpoint Security kaldırıldığında bilgisayardan silinir.

Hizmet verileri

Kaspersky Endpoint Security, otomatik yanıt sırasında işlenen aşağıdaki verileri depolar:

- Kaspersky Endpoint Security'nin yerleşik aracısının yapılandırılması sırasında kullanıcı tarafından girilen işlenmiş dosyalar ve veriler:
  - Karantinaya alınan dosyalar
  - Kaspersky Sandbox ile entegrasyon için kullanılan sertifikanın genel anahtarı
- Kaspersky Endpoint Security'nin yerleşik aracısının önbelleği:
  - Tarama sonuçlarının önbelleğe yazıldığı zaman
  - Tarama görevinin MD5 karması
  - Tarama görevi tanımlayıcısı
  - Nesne için tarama sonucu
- Nesne tarama istekleri kuyruğu:
  - Kuyruktaki nesnenin kimliği
  - Nesnenin kuyruğa yerleştirildiği zaman
  - Kuyruktaki nesnenin işlenme durumu

- Nesne tarama görevinin oluşturulduğu işletim sistemindeki kullanıcı oturumunun kimliği
- Görevi oluşturmak için hesabı kullanılan işletim sistemi kullanıcısının sistem tanımlayıcısı (SID)
- Nesne tarama görevinin MD5 karması

- Kaspersky Endpoint Security'nin yerleşik aracısının Kaspersky Sandbox'tan tarama sonuçlarını beklediği görevler hakkında bilgiler:
  - Nesne tarama görevinin alındığı zaman
  - Nesne işleme durumu
  - Nesne tarama görevinin oluşturulduğu işletim sistemindeki kullanıcı oturumunun kimliği
  - Nesne tarama görevinin tanımlayıcısı
  - Nesne tarama görevinin MD5 karması
  - Görevi oluşturmak için hesabı kullanılan işletim sistemi kullanıcısının sistem tanımlayıcısı (SID)
  - Otomatik olarak oluşturulan IOC'nin XML şeması
  - Taranan nesnenin MD5 veya SHA256 karması
  - İşleme hataları
  - Görevin oluşturulduğu nesnelerin adları
  - Nesne için tarama sonucu

Kaspersky Sandbox'a gelen taleplerdeki veriler

Kaspersky Endpoint Security'nin yerleşik aracısından Kaspersky Sandbox'a gelen isteklerden gelen şu veriler bilgisayarda yerel olarak depolanır:

- Tarama görevinin MD5 karması
- Tarama görevi tanımlayıcısı
- Taranan nesne ve ilgili tüm dosyalar

IOC Taraması görevinin yürütülmesi sonucunda alınan veriler (tek başına görev)

Kaspersky Endpoint Security, *IOC Taraması* görevi yürütme sonuçlarına ilişkin verileri otomatik olarak Kaspersky Security Center'a gönderir.

IOC Taraması görevi yürütme sonuçlarındaki veriler şu bilgileri içerebilir:

- ARP tablosundan IP adresi
- ARP tablosundan fiziksel adres
- DNS kayıt türü ve adı
- Korunan bilgisayarın IP adresi
- Korunan bilgisayarın fiziksel adresi (MAC adresi)
- Olay günlüğü girişindeki tanımlayıcı
- Günlükteki veri kaynağı adı
- Günlük adı
- Olay zamanı
- Dosyanın MD5 ve SHA256 karmaları
- Dosyanın tam adı (yol dahil olmak üzere)
- Dosya boyutu
- Tarama sırasında bağlantı kurulan uzak IP adresi ve port
- Yerel bağdaştırıcı IP adresi
- Yerel bağdaştırıcıda açık port
- Sayı olarak protokol (IANA standardına uygun olarak)
- İşlem adı
- İşlem argümanları
- İşlem dosyasının yolu
- İşlemin Windows tanımlayıcısı (PID)
- Ana işlemin Windows tanımlayıcısı (PID)
- İşlemi başlatan kullanıcı hesabı
- İsteğin başladığı tarih ve saat
- Hizmet adı
- Hizmet açıklaması
- DLL hizmetinin yolu ve adı (svchost için)
- Hizmet yürütülebilir dosyasının yolu ve adı

- Hizmetin Windows tanımlayıcısı (PID)
- Hizmet türü (örneğin, bir çekirdek sürücüsü veya bağdaştırıcı)
- Hizmet durumu
- Hizmet başlatma modu
- Kullanıcı hesabı adı.
- Birim adı
- Birim harfi
- Birim tipi
- Windows kayıt defteri değeri
- Kayıt defteri kovanı değeri
- Kayıt anahtarı yolu (kovan ve değer adı olmadan)
- Kayıt defteri ayarı
- Sistem (ortam)
- Bilgisayarda yüklü olan işletim sisteminin adı ve sürümü
- Korunan bilgisayarın ağ adı
- Korunan bilgisayarın ait olduğu etki alanı veya grup
- Tarayıcı adı
- Tarayıcı sürümü
- Web kaynağına en son erişim zamanı
- HTTP isteğinden URL
- HTTP isteği için kullanılan hesabın adı
- HTTP isteğini yapan işlemin dosya adı
- HTTP isteğini yapan işlemin dosyasının tam yolu
- HTTP isteğini yapan işlemin Windows tanımlayıcısı (PID)
- HTTP yönelten (HTTP istek kaynağı URL'si)
- HTTP üzerinden istenen kaynağın URI'si
- HTTP kullanıcı aracısı (HTTP isteğini yapan uygulama) hakkında bilgi

- HTTP isteği yürütme süresi
- HTTP sorgusunu gerçekleştiren işlemin benzersiz tanımlayıcısı

Kaspersky Endpoint Detection and Response Expert (on-premises)

Uygulamanın bilgisayarda yerel olarak depoladığı tüm veriler, Kaspersky Endpoint Security kaldırıldığında bilgisayardan silinir.

Hizmet verileri

Kaspersky Endpoint Security'nin yerleşik aracısı şu verileri yerel olarak depolar:

- EDR Expert (on-premises) bileşeniyle entegrasyon için gerekli veriler:
  - KATA Merkezi Düğüm sunucusuna bağlanmak için adres ve port
  - Telemetri aktarım sunucusuna bağlanmak için adres ve port
  - Yanıt sunucusuna bağlanmak için adres ve port
  - KATA Central Node ile entegrasyon için kullanılan sertifikalar hakkında bilgiler
  - Telemetri iletim sunucusu ile entegrasyon için kullanılan sertifikalar hakkında bilgiler
  - Yanıt sunucusu ile entegrasyon için kullanılan sertifikalar hakkında bilgiler
- Karantinaya alınan dosyalar

İletilen telemetri olaylarından gelen veriler

- **Telemetri verileri**
  - Dosyalardaki veriler:
    - Dosyanın benzersiz tanımlayıcıları
    - Dosya türü
    - Tam dosya yolu
    - Dosya boyutu
    - Dosya öznitelikleri
    - Bölge tanımlayıcısı

    - Dosyanın oluşturulduğu tarih ve saat
    - Dosyanın en son değiştirildiği tarih ve saat
    - Orijinal dosya adı
    - Uygulama adı
    - Uygulama sürümü.
    - Uygulama sağlayıcısı
    - Dosya açıklaması
    - Dosya sürümü.
    - Nesnenin MD5 ve SHA256 karmaları
    - Dosya imza doğrulamasının sonucu
    - Sertifika veren kuruluşun adı
    - Sertifika sahibinin adı
    - Sertifika seri numarası
- AMSI taramasıyla ilgili veriler:
    - Etkinliği başlatan işlemin benzersiz tanımlayıcısı
    - AMSI'ye iletilen nesnenin içerik türü
    - AMSI'ye iletilen nesnenin içeriği
    - Nesne adı
    - Nesnenin MD5 ve SHA256 karmaları
- Uygulama engellemeyle ilgili veriler:
    - Uygulamanın kilitlenmesine neden olan işlemin benzersiz tanımlayıcısı
    - Ana işlemin benzersiz tanımlayıcısı
    - İşlemin benzersiz sistem tanımlayıcısı
    - Bir işlemi başlatmak için kullanılan komut
    - Giriş oturumu kimliği
    - İşlem bütünlüğü seviyesi
    - İşlem durumu
    - İşlem dosyasının benzersiz tanımlayıcısı

- İşlem komut satırı
- Yorumlanmış dosyaların benzersiz tanımlayıcılarının listesi

- Engellenen dosya açılışlarına ilişkin veriler:
  - Dosyanın açılmasını başlatan işlemin benzersiz tanımlayıcısı
  - Dosyanın benzersiz tanımlayıcıları
- Sürücü yüklemeyle ilgili veriler:
  - Yüklenen sürücünün benzersiz tanımlayıcısı
- Etkinlikler hakkındaki veriler:
  - Olayın benzersiz tanımlayıcısı
  - Etkinlik tarihi ve saati
- Dosya değişikliğiyle ilgili veriler:
  - Dosya değişikliğini başlatan işlemin benzersiz tanımlayıcısı
  - Dosyanın benzersiz tanımlayıcıları
  - Değişiklik işleminin türü
  - Bilgisayar yeniden başlatıldıktan sonra dosyanın silineceğini belirten bayrak
  - Değiştirilen dosyanın benzersiz tanımlayıcısı
  - Değişiklikten önceki dosyanın benzersiz tanımlayıcısı
  - Dosyanın nasıl açıldığını belirleyen bit bayrakları kümesi
  - Erişim kontrol listesindeki işlemlerle ilgili veriler
  - Dosyanın sahipliğinde veya ana grubunda yapılan değişikliklere ilişkin veriler
- Giriş oturumuna ilişkin veriler:
  - Giriş oturumu kimliği
  - Giriş yapan kullanıcının adı
  - Kullanıcı hesabı türü
  - Oturum türü
- Ağ bağlantıları hakkındaki veriler:
  - Bağlantıyı başlatan işlemin benzersiz tanımlayıcısı
  - Bağlantıyı başlatmak için kullanılan yerel IP adresi

    - Bağlantı uç noktasının uzak IP adresi
    - Bağlantı yönü
    - Veri aktarım iletişim kuralı
    - HTTP yöntemi
    - Ana bilgisayar adı içermeyen yol
    - Ana bilgisayar adı
    - Bağlantı anındaki dinamik işlem durumu
    - Bağlantının ham soket düzeyinde açık olduğunu belirten bayrak
    - Bağlantı oturumunda kullanılan TLS sürümü
    - TLS sunucusunun adı
    - TLS sunucu sertifikasının MD5 ve SHA1 karma değerleri
    - Sertifikanın Konu Alternatif Adları (SAN) listesi
    - TLS sertifika düzenleyicisinin adı
    - Sertifika seri numarası
    - Kullanılan şifreleme algoritması
    - Sertifikanın başlangıç ve bitiş tarihleri
    - TLS istemcisinin JA3 parmak izi
    - Sunucunun JA3S parmak izi
- Bir ağ portunda dinleme sırasında toplanan veriler:
    - Bağlantıyı başlatan işlemin benzersiz tanımlayıcısı
- Komut satırı giriş verileri:
    - Konsol girişini başlatan işlemin benzersiz tanımlayıcısı
    - Konsol giriş türü
    - Bir kullanıcı veya işlem tarafından girilen metin
- İşlem oluşturma ile ilgili veriler:
    - İşlemin benzersiz tanımlayıcısı
    - Ana işlemin benzersiz tanımlayıcısı
    - İşlemin benzersiz sistem tanımlayıcısı

    - Bir işlemi başlatmak için kullanılan komut
    - Giriş oturumu kimliği
    - İşlem bütünlüğü seviyesi
    - İşlem dosyasının benzersiz tanımlayıcısı
    - Yorumlanmış dosyaların benzersiz tanımlayıcılarının listesi
    - İşlem türü
- İşlem tarafından yüklenen modül hakkındaki veriler:
    - İndirmeyi başlatan işlemin benzersiz tanımlayıcısı
    - İşleme yüklenen dosyanın tam yolu
    - Modül dosyasının benzersiz tanımlayıcısı
    - Yüklenen dosya bir .NET modülü ise, .NET derlemesinin tam nitelikli adı
    - Bildiriminde tanımlanan .NET derlemesinin bayrakları
- İşlem sonlandırma ile ilgili veriler:
    - Sonlandırılan işlemin benzersiz tanımlayıcısı
- Kayıt defteri değişikliklerine ilişkin veriler:
    - Kayıt defteri değişikliğini başlatan işlemin benzersiz tanımlayıcısı
    - Kayıt defteri işlemi türü
    - Kayıt defteri anahtarının tam yolu
    - Kayıt defteri anahtarındaki değerin adı
    - Kayıt defteri anahtarının değerinde depolanan veri türü
    - Kayıt defteri anahtarı değerinde belirtilen veriler
    - Yeniden adlandırılmadan önceki anahtarın adı
    - Anahtar veya birincil anahtar grubunun sahipliğinde meydana gelen değişiklikle ilgili bilgiler
    - Anahtarın erişim kontrol listesindeki (ACL) değişikliklerin listesi
- Tespit edilen tehdit ve bu tehditle ilgili işlemler hakkında bilgiler:
    - Arka planda tehdit algılama işleminin yürütüldüğünü gösteren bayrak
    - Tehdit kararı
    - Karar adı

- Veritabanı kaydının benzersiz tanımlayıcısı
- Tehdit kaydının veritabanına kaydedildiği zaman
- Tehdit işleme modu
- Virüs bulaşmış nesnenin türü
- Virüs bulaşmış nesnenin adı
- Nesnenin MD5 ve SHA256 karmaları
- Virüs bulaşmış nesnenin benzersiz tanımlayıcısı
- İnternetten virüs bulaşmış nesneyi indiren işlemin benzersiz tanımlayıcısı
- Virüs bulaşmış dosyanın indirildiği URL
- Virüs bulaşmış dosyayı gönderen e-posta adresi
- Virüs bulaşmış nesnenin alındığı ağ protokolü
- Virüs bulaşmış nesnenin alındığı yerel adres
- Virüs bulaşmış alındığı harici adres
- Nesne içerik türü
- Nesne içeriği

- İşlemlere erişimle ilgili veriler:
  - Erişmeye çalışan işlemin benzersiz tanımlayıcısı
  - Erişilen hedef işlemin benzersiz tanımlayıcısı
  - Hedef işlemden talep edilen haklar kümesi
  - İşlem türü
  - Bir işleme erişim anında gerçekleştirilen çağrılar dizisi
  - Kaynak işlem tanımlayıcısı
  - Hedef işlem tanımlayıcısı
- DNS hakkındaki veriler:
  - DNS sorgusunu başlatan işlemin benzersiz tanımlayıcısı
  - DNS sunucusu IP adresi
  - DNS sorgusunun davranışını yöneten bayraklar
  - Talep tamamlanma durumu

    - DNS sorgusunda belirtilen tam etki alanı adı
    - DNS sorgusundaki veri türü
    - DNS sunucusu yanıtları
- Kod enjeksiyonu ile ilgili veriler:
    - Kod enjekte etmeye çalışan işlemin benzersiz tanımlayıcısı
    - Kullanılan erişim yöntemi
    - Enjekte edilen kodun tespit edildiği anda yapılan çağrılar
    - Kodun yüklendiği hedef işlemin benzersiz tanımlayıcısı
    - Hedef işlemin komut dizisindeki değişikliklere ilişkin veriler
    - Hedef işlem adresi
    - Hedef işleme yüklenen DLL kitaplığının adı
    - DDL dosyasının tam yolu
- Adlandırılmış kanallarla yapılan işlemler hakkındaki veriler:
    - Kanalı oluşturan veya kanala bağlanan işlemin benzersiz tanımlayıcısı
    - Adı belirtilen kanalın tam adı
    - İşlem türü (oluşturma veya bağlanma)
- WMI sorguları hakkındaki veriler:
    - WMI işlemini başlatan işlemin benzersiz tanımlayıcısı
    - WMI işlem türü
    - WMI sorgusu için hedef cihazın adı
    - WMI sorgusunu başlatan kullanıcı hesabı
    - WMI sorgusunun metni
    - WMI sorgusunun gerçekleştirildiği ad alanı
    - WMI filtre adı
    - Tüketici nesnesinin adı
    - Tüketici nesnesinin işlevini açıklayan metin

- LDAP sorguları hakkındaki veriler:
  - LDAP sorgusunu gerçekleştiren işlemin benzersiz tanımlayıcısı
  - LDAP sorgularının arama kapsamı
  - LDAP filtresi
  - Sorgunun yönlendirildiği Active Directory bölümünü belirten parametre
  - LDAP arama öznitelikleri
- Bağlı USB cihazlarına ilişkin veriler:
  - USB cihazının çalışma türü
  - USB cihaz türü
  - USB cihazının tanımlayıcısı
  - USB cihazının adı
  - USB cihazının yolu
  - USB cihazının bir sistem sürücüsü olduğunu belirten bayrak
- Zamanlanmış bir görevin oluşturulması, silinmesi ve değiştirilmesine ilişkin veriler
- Hizmetlerin oluşturulması, silinmesi ve değiştirilmesine ilişkin veriler
- Dosya sisteminin bağlanması/bağlantısının kesilmesi ile ilgili veriler
- EDR Expert on-premise bileşeninin çalışmasına ilişkin veriler:
  - Aracıyı başlatma/durdurma hakkında bilgiler
  - Ajanın yüklenmesi/kaldırılması hakkında bilgiler
  - Aracının başlatılması için benzersiz tanımlayıcı
  - Aracı işlemin sistem tanımlayıcısı
  - Aracı işlemin benzersiz tanımlayıcısı
  - Temsilcinin işine son verilme nedeni
  - Ajan işleminin sonlandırma kodu
- Olay filtreleme ayarları:
  - Modül adları
  - Nesnelerin tam yolları
  - Nesnelerin MD5 ve SHA256 karmaları

- Windows olay günlüğündeki girdilerin tanımlayıcıları
- Dijital sertifika ayarları
- Trafik yönü, IP adresleri, portlar, iletişim kuralları, tam yürütülebilir dosya yolları
- Kullanıcı adları
- Kullanıcı oturum açma türleri
- Filtrelerin uygulandığı telemetri olaylarının türleri

EDR Expert bileşeninin Kaspersky Endpoint Security'nin yerleşik ajanıya gönderdiği taleplerden elde edilen veriler

- Genel görev ayarları:
  - Görev türü
  - Görev zamanlama ayarları
  - Görevlerin çalıştırılabileceği hesapların adları ve parolaları
  - Ayarların sürümleri
  - Karantinaya alınan nesnelerin tanımlayıcıları
  - Nesnelere giden yollar
  - Nesnelerin MD5 ve SHA256 karmaları
  - İşlemi bağımsız değişkenlerle başlatmak için komut satırı
  - Görevlerin tamamlanmasının ardından gerçekleştirilen ek eylemlerin bayrakları
  - Sunucudan alınacak IOC dosya tanımlayıcıları
  - IOC dosyaları
  - Hizmet adı
  - Hizmet başlatma türü
  - *Adli bilgi al* görevinin sonuçlarının alınması gereken klasörler
  - *Adli bilgi al* görevi için nesne adlarının ve uzantılarının maskeleri
- Ağ izolasyonu ayarları:
  - Ayar türleri
  - Ayarların sürümleri

- Ağ izolasyon istisnaları ve istisna ayarları listeleri: trafik yönü, IP adresleri, portlar, iletişim kuralları ve yürütülebilir dosyaların tam yolları
- Ek eylemlerin bayrakları
- Otomatik izolasyonun devre dışı bırakılma zamanı

- Yürütme önleme ayarları:
  - Ayar türleri
  - Ayarların sürümleri
  - Yürütme önleme kuralları ve kural ayarları listeleri: nesnelere giden yollar, nesne türleri, nesnelerin MD5 ve SHA256 karmaları
  - Ek eylemlerin bayrakları

Kaspersky Endpoint Security tarafından EDR Expert bileşenine gönderilen taleplerden elde edilen veriler

EDR Expert (on-premises) çözümüyle entegrasyon sırasında aşağıdaki veriler bilgisayarlarda yerel olarak depolanır.

- Senkronizasyon isteklerinde:
  - Benzersiz kimlik
  - Sunucu web adresinin temel kısmı
  - Bilgisayar adı
  - Bilgisayar IP adresi
  - Bilgisayar MAC adresi
  - Bilgisayardaki yerel saat
  - Kaspersky Endpoint Security'nin kendini savunma durumu
  - Bilgisayarda yüklü olan işletim sisteminin adı ve sürümü
  - Kaspersky Endpoint Security sürümü
  - Uygulama ayarlarının ve görev ayarlarının sürümleri
  - Görev durumları: görevlerin tanımlayıcıları, yürütme durumları, hata kodları
- Sunucudan dosya almak için yapılan isteklerde:
  - Dosyaların benzersiz tanımlayıcıları
  - Benzersiz Kaspersky Endpoint Security tanımlayıcısı
  - Sertifikaların benzersiz tanımlayıcıları

- Central Node bileşeninin kurulu olduğu sunucunun web adresinin temel kısmı
- Ana bilgisayar IP adresi

- Görev yürütme sonuçlarına ilişkin raporlarda:
  - Ana bilgisayar IP adresi
  - Bir IOC taraması veya YARA taraması sırasında tespit edilen nesneler hakkında bilgiler
  - Görevlerin tamamlanmasının ardından gerçekleştirilen ek eylemlerin bayrakları
  - Görev yürütme hataları ve dönüş kodları
  - Görev tamamlama durumları
  - Görev tamamlama süresi
  - Görevlerin yürütülmesi için kullanılan ayarların sürümleri
  - Sunucuya gönderilen nesneler, karantinaya alınan nesneler ve karantinadan geri yüklenen nesneler hakkında bilgiler: nesnelere giden yollar, MD5 ve SHA256 karmaları, karantinaya alınan nesnelerin tanımlayıcıları
  - Sunucunun isteği üzerine bir bilgisayarda başlatılan veya durdurulan işlemler hakkında bilgiler: PID ve UniquePID, hata kodu, nesnelerin MD5 ve SHA256 karmaları
  - Sunucunun isteği üzerine bilgisayarda başlatılan veya durdurulan hizmetler hakkında bilgiler: hizmet adı, başlatma türü, hata kodu, hizmetlerin dosya görüntülerinin MD5 ve SHA256 karmaları
  - Bir YARA taraması için bellek dökümü yapılan nesneler hakkında bilgiler (yollar, döküm dosyası tanımlayıcısı)
  - Sunucu tarafından istenen dosyalar
- Çalışan işlemlere ilişkin veriler:
  - Tam yol ve uzantı dahil olmak üzere yürütülebilir dosya adı
  - İşlem otomatik çalıştırma parametreleri
  - İşlem kimliği
  - Giriş oturumu kimliği
  - Oturum açma adı
  - İsteğin başladığı tarih ve saat
  - Nesnenin MD5 ve SHA256 karmaları
- Dosyalardaki veriler:
  - Dosya yolu
  - Dosya adı.

- Dosya boyutu
- Dosya öznitelikleri
- Dosyanın oluşturulduğu tarih ve saat
- Dosyanın en son değiştirildiği tarih ve saat
- Dosya açıklaması
- Şirket adı
- Nesnenin MD5 ve SHA256 karmaları
- Kayıt defteri anahtarı (otomatik çalıştırma noktaları için)

- Nesneler hakkında bilgi alınırken oluşan hatalardaki veriler:
  - Bir hata oluştuğunda işlenen nesnenin tam adı
  - Hata kodu
- YARA taraması sonuçlarındaki veriler:

  Kaspersky Endpoint Security'nin yerleşik aracısı, tehdit geliştirme zinciri oluşturmak için YARA taraması sonuçlarını otomatik olarak Kaspersky Anti Targeted Attack Platform'a aktarır.

  Veriler, görev yürütme sonuçlarının Kaspersky Anti Targeted Attack Platform sunucusuna gönderilmesi için yerel olarak kuyrukta geçici olarak depolanır. Veriler gönderildikten sonra geçici depolama alanından silinir.
  - Dosyanın MD5 ve SHA256 karmaları
  - Dosyanın tam adı
  - Dosya yolu
  - Dosya boyutu
  - İşlem adı
  - İşlem argümanları
  - İşlem dosyasının yolu
  - İşlemin Windows tanımlayıcısı (PID)
  - Ana işlemin Windows tanımlayıcısı (PID)
  - İşlemi başlatan kullanıcı hesabı
  - İsteğin başladığı tarih ve saat
- IOC taraması sonuçlarındaki veriler:
  - ARP tablosundan IP adresi
  - ARP tablosundan fiziksel adres

- DNS kayıt adı
- DNS kayıt türü
- Ana bilgisayar adı
- IP adresi
- Günlükteki olay kimliği
- Günlükteki veri kaynağı adı
- Günlük adı
- Kullanıcı adı
- Etkinliğin oluşturulduğu tarih ve saat (ISO biçiminde)
- Dosyanın MD5 ve SHA256 karmaları
- Dosyanın tam adı
- Dosya boyutu
- Tarama sırasında bağlantı kurulan uzak IP adresi ve port
- Yerel bağdaştırıcının IP adresi ve portu
- İletişim kuralı
- İşlem adı
- İşlem argümanları
- İşlem dosyasının yolu
- İşlemin Windows tanımlayıcısı (PID)
- Ana işlemin Windows tanımlayıcısı (PID)
- İşlemi başlatan kullanıcı hesabı
- İsteğin başladığı tarih ve saat
- Kayıt defteri anahtarının yolu
- Kayıt defteri anahtar adı
- Kayıt defteri anahtarının metin değeri
- Hizmet adı
- Hizmet açıklaması
- DLL hizmetinin yolu ve adı

- Hizmet yürütülebilir dosyasının yolu ve adı
- Hizmetin Windows tanımlayıcısı (PID)
- Hizmet türü
- Hizmet durumu
- Hizmet başlatma modu
- İşletim sistemi adı
- İşletim sistemi sürümü
- Etki alanı içermeyen bilgisayar ağı adı
- Etki alanı veya çalışma grubu
- Kullanıcı adı
- Birim adı
- Birim harfi
- Birim tipi

Kaspersky Network Detection and Response (KATA)

Uygulamanın bilgisayarda yerel olarak depoladığı tüm veriler, Kaspersky Endpoint Security kaldırıldığında bilgisayardan silinir.

Telemetri verileri

- **Dosyalar hakkındaki veriler**
  - Dosyanın benzersiz tanımlayıcıları
  - Dosya türü
  - Tam dosya yolu
  - Dosya boyutu
  - Dosya öznitelikleri
  - Bölge tanımlayıcısı
  - Dosyanın oluşturulduğu tarih ve saat

- Dosyanın en son değiştirildiği tarih ve saat
- Orijinal dosya adı
- Uygulama adı
- Uygulama sürümü.
- Uygulama sağlayıcısı
- Dosya açıklaması
- Dosya sürümü.
- Nesnenin MD5 ve SHA256 karmaları
- Dosya imza doğrulamasının sonucu
- Dosya imzasının oluşturulduğu tarih ve saat
- İmza dosyasında kullanılan sertifika zincirleri
- Sertifika zinciri türü
- Zincirdeki sertifikalar
- Sertifika veren kuruluşun adı
- Sertifika sahibinin adı
- Sertifika seri numarası
- Sertifika parmak izi algoritması
- Sertifika parmak izi
- Sertifikanın geçerlilik süresi

- **Giriş oturumuna ilişkin veriler**
  - Giriş oturumu kimliği
  - Giriş yapan kullanıcının hesap adı
  - Kullanıcı hesabı türü
  - Oturum türü
  - Giriş girişiminin yapıldığı bilgisayarın IP adresi
  - Giriş denemesinin yapıldığı yerel bilgisayarın IP adresi
  - Bu olayın temsil ettiği oturumun yükseltilmiş ayrıcalıklara ve yönetici haklarına sahip olduğunu belirten bayrak
  - Bu oturumla başka oturumların bağlantılı olup olmadığını gösteren parametre

- Terminal oturumu için kullanılan iletişim kuralı
- Terminal oturumu için kullanılan IPv4 iletişim kuralı

- **Ağ iletişimi ile ilgili veriler**
  - Verilerin toplandığı zaman aralığının başlangıcı ve bitişi
  - Bağlantı listesi
  - Bilgisayarın yerel IP adresi
  - Bilgisayarın yerel MAC adresi
  - Bilgisayarın uzak IP adresi
  - Bilgisayarın uzak MAC adresi
  - Ağ geçidi IP adresi
  - İletilen veri paketlerinin sayısı
  - Alınan veri paketlerinin sayısı
  - Aktarılan toplam bayt sayısı
  - Veri aktarım iletişim kuralı
  - Ethernet çerçevesi EtherType alanı
  - Aralıktaki ilk paketin yük ön eki
  - İletişimin yakalandığı ağ arabiriminin IPv4 adresi
- **Ağ bağlantısıyla ilgili veriler**
  - Bağlantıyı başlatan işlemin benzersiz tanımlayıcısı
  - Veri aktarım iletişim kuralı
  - Bağlantıyı başlatmak için kullanılan yerel IP adresi
  - Bağlantı uç noktasının uzak IP adresi
  - HTTP yöntemi
  - Ana bilgisayar adı içermeyen yol
  - Ana bilgisayar adı
  - Bağlantı anındaki dinamik işlem durumu
  - Bağlantı yönü

- Dinamik işlem durumu
- Ethernet çerçevesi EtherType alanı

- **Bir ağ portunda dinleme sırasında toplanan veriler**
  - Bağlantıyı başlatan işlemin benzersiz tanımlayıcısı
  - Veri aktarım iletişim kuralı
  - Yerel adres
  - Bağlantı anındaki dinamik işlem durumu
- **Bağlantı doğrulama sonucu**
  - Ana bilgisayar ağ ayarları
  - Ağ arabirim açıklaması
  - DNS alan adı
  - Bilgisayarın yerel MAC adresi
  - IP bağlantı metrik numarası
  - IP adreslerinin listesi
  - IP adresi
  - Ağ maskesi
  - Ağ geçidi IP adresi
  - Ağ geçidi MAC adresi
  - Yüklü yamaların listesi
  - Yama numarası
  - Yama yükleme tarihi
  - Cihaz modeli
  - Cihaz üreticisi
  - Kaspersky Security Center'daki ana bilgisayar kimliği
  - Yüklü Kaspersky antivirüsünün açıklaması
  - Yüklü Kaspersky antivirüsünün bileşen adı
  - Yüklü Kaspersky antivirüsünün bileşen sürümü
  - Yüklü Kaspersky antivirüs bileşeninin veritabanı sürümü

- Yüklü Kaspersky antivirüs bileşeninin veritabanının en son güncellenme tarihi
- Yüklü Kaspersky antivirüsünün bileşen durumu
- Lisans anahtarlarının listesi
- Anahtar seri numarası
- Anahtar türü
- Anahtar geçerlilik tarihi
- Anahtar durumu

- **Ana bilgisayarda işlem oluşturma ile ilgili veriler**
  - İşlemin benzersiz tanımlayıcısı
  - Ana işlemin benzersiz tanımlayıcısı
  - İşlemin benzersiz sistem tanımlayıcısı
  - Bir işlemi başlatmak için kullanılan komut
  - Giriş oturumu kimliği
  - Terminal oturum kimliği
  - İşlem dosyasının benzersiz tanımlayıcısı
  - İşlem bütünlüğü seviyesi
  - İşlem hakları belirteçlerinin listesi
  - Nitelik hakları
  - Yorumlanmış dosyaların benzersiz tanımlayıcılarının listesi
  - İşlem durumu
  - Bir işlemi başlatmak için kullanılan komut
- **İşlem sonlandırma ile ilgili veriler**
  - İşlemin benzersiz tanımlayıcısı
- **Tespit edilen tehditle ilgili veriler**
  - Tehdit bilgileri
  - Tehdit kararı
  - AMR kayıt numarası
  - Antivirüs veritabanı sürümü

- Tehdit algılama modu
- Tehdidin benzersiz tanımlayıcısı
- Koruma teknolojisi
- Virüs bulaşmış nesne hakkında bilgiler
- Virüs bulaşmış nesnenin türü
- Virüs bulaşmış nesnenin adı
- Nesnenin MD5 ve SHA256 karmaları
- Virüs bulaşmış işlemin benzersiz tanımlayıcısı
- Virüs bulaşmış nesnenin benzersiz tanımlayıcısı
- İnternetten virüs bulaşmış nesneyi indiren işlemin benzersiz tanımlayıcısı
- Virüs bulaşmış dosyanın indirildiği URL
- Virüs bulaşmış dosyayı gönderen e-posta adresi
- Virüs bulaşmış nesnenin alındığı ağ protokolü
- Virüs bulaşmış nesnenin alındığı yerel adres
- Virüs bulaşmış alındığı harici adres
- Nesne içerik türü
- Tespit edilen tehdidin bağlamı
- Nesne içeriği
- Arka planda tehdit algılama işleminin yürütüldüğünü gösteren bayrak

- **Tehdit işlemeyle ilgili veriler**
  - Tehdit bilgileri
  - Tehdit kararı
  - AMR kayıt numarası
  - Antivirüs veritabanı sürümü
  - Tehdit algılama modu
  - Virüs bulaşmış nesnenin adı
  - Nesnenin MD5 ve SHA256 karmaları
  - Virüs bulaşmış işlemin benzersiz tanımlayıcısı

- Virüs bulaşmış nesnenin benzersiz tanımlayıcısı
- Virüs bulaşmış nesnenin alındığı ağ protokolü
- Virüs bulaşmış nesnenin alındığı yerel adres
- Virüs bulaşmış alındığı harici adres
- Tehdit işleme durumu
- Tehdidin ortadan kaldırılamamasının nedeni
- Yerel fiziksel adres

- **Kullanıcılar hakkında veriler**
  - Kullanıcı güvenlik tanımlayıcısı
  - Kullanıcı kimliği
  - Kullanıcı adı
  - Kullanıcının tam adı
  - Kullanıcı açıklaması
  - Hesabın etkin durumda mı yoksa engellenmiş mi olduğu
  - Parolanın süresinin dolup dolmadığı
  - Parola değişikliğinin gerekli olup olmadığı
  - Parola değiştirmenin mümkün olup olmadığı
  - Kullanıcı hesabı türü
  - Bu hesap için otomatik oturum açmanın etkin olup olmadığı
  - Kullanıcının üyesi olduğu grupların listesi

Kaspersky Unified Monitoring and Analysis Platform (KUMA) ile entegrasyon

Uygulamanın bilgisayarda yerel olarak depoladığı tüm veriler, Kaspersky Endpoint Security kaldırıldığında bilgisayardan silinir.

Kaspersky Unified Monitoring and Analysis Platform (KUMA) ile entegrasyon sırasında, bağlantı ayarları verilerinin yanı sıra Windows Günlüklerinde kaydedilen tüm olaylar da aktarılır.

Ana Windows Olay Günlükleri; Sistem, Güvenlik, Uygulama, İletilen Olaylar ve Donanım Olayları günlükleridir. Kullanıcılar ayrıca özel ihtiyaçlarını karşılamak üzere özel günlükler oluşturabilir ve bunları kullanabilir.

Avrupa Birliği mevzuatına (GDPR) uygunluk

Kaspersky Endpoint Security, aşağıdaki senaryolar kapsamında Kaspersky'ye veri iletebilir:

- Kaspersky Security Network'ü kullanma.
- Uygulamayı bir etkinleştirme koduyla etkinleştirme.
- Uygulama modüllerini ve anti-virüs veritabanlarını güncelleme.
- Uygulama arabirimdeki bağlantıları izleme.

Veri sınıflandırması ve verilerin alındığı bölgeden bağımsız olarak Kaspersky, veri güvenliği için yüksek standartlara bağlı kalır ve yürürlükteki mevzuatla garanti edilen kullanıcı haklarının yerine getirilmesi için kullanıcıların verilerini korumak, veri güvenliğini ve gizliliğini garanti etmek ve ayrıca verilerin güvenliğini sağlamak için çeşitli yasal, organizasyonel ve teknik önlemler kullanır. Gizlilik İlkesi metni, uygulama dağıtım kitine dahildir ve Kaspersky web sitesinde mevcuttur.

Kaspersky Endpoint Security'yi kullanmadan önce, lütfen Son Kullanıcı Lisans Sözleşmesi ve Kaspersky Security Network Bildirimi'nde iletilen verilerin açıklamasını dikkatlice okuyun. Kaspersky Endpoint Security'den açıklanan senaryolardan herhangi biri kapsamında aktarılan belirli veriler, yerel yasalarınıza veya standartlarınıza göre kişisel veri olarak sınıflandırılabiliyorsa, bu tür verilerin yasal olarak işlendiğinden emin olmalı ve verilerin toplanması ve iletilmesi için son kullanıcıların onayını almalısınız.

Son Kullanıcı Lisans Sözleşmesi'ni kabul ettikten ve Kaspersky Security Network Bildirimini 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 web sitesini ziyaret edin. License.txt ve ksn_<dil kodu>.txt dosyaları Son Kullanıcı Lisans Sözleşmesi ile Kaspersky Security Network Bildirimi metnini içerir ve uygulama dağıtım kitinde yer almaktadır.

Kaspersky'ye veri iletmek istemiyorsanız, veri sağlamayı devre dışı bırakabilirsiniz.

Kaspersky Security Network'ü kullanma

Kaspersky Security Network'ü kullanarak, Kaspersky Security Network Bildirimi'nde listelenen verileri otomatik olarak sağlamayı kabul edersiniz. Bu verileri Kaspersky'ye vermeyi kabul etmiyorsanız, Kaspersky Private Security Network (KPSN)'yi kullanın veya KSN kullanımını devre dışı bırakın. KPSN hakkında daha fazla bilgi için lütfen Kaspersky Private Security Network belgelerine bakın.

Uygulamayı bir etkinleştirme koduyla etkinleştirme

Bir etkinleştirme kodu kullanarak, Son Kullanıcı Lisans Sözleşmesinde listelenen verileri otomatik olarak sağlamayı kabul edersiniz. Bu bilgileri Kaspersky'ye sağlamayı kabul etmiyorsanız Kaspersky Endpoint Security ürününü etkinleştirmek için bir anahtar dosyası kullanabilirsiniz.

Uygulama modüllerini ve anti-virüs veritabanlarını güncelleme

Kaspersky sunucularını kullanarak, Son Kullanıcı Lisans Sözleşmesinde listelenen verileri otomatik olarak sağlamayı kabul edersiniz. Kaspersky, Kaspersky Endpoint Security'nin yasal olarak kullanıldığını doğrulamak için bu bilgilere ihtiyaç duyar. Bu bilgileri Kaspersky'ye vermeyi kabul etmiyorsanız, veritabanı güncellemeleri için Kaspersky Security Center'ı veya Kaspersky Update Utility'yi kullanın.

Uygulama arabirimindeki bağlantıları izleme

Uygulama arabirindeki bağlantıları kullanarak, Son Kullanıcı Lisans Sözleşmesinde listelenen verileri otomatik olarak sağlamayı kabul edersiniz. Her bir özel bağlantıda iletilen verilerin kesin listesi, bağlantının uygulama arabiriminde nerede bulunduğuna ve hangi sorunu çözmeyi amaçladığına bağlıdır. Bu verileri Kaspersky'ye vermeyi kabul etmiyorsanız, basitleştirilmiş uygulama arayüzünü kullanın veya uygulama arayüzünü gizleyin.

Döküm yazımı

Döküm yazımını etkinleştirdiyseniz Kaspersky Endpoint Security, bu döküm dosyasının oluşturulduğu anda uygulama işlemlerinden gelen tüm bellek verilerini içeren bir döküm dosyası oluşturur.

Ticari marka bildirimleri

Tescilli ticari markalar ve hizmet markaları, bunların ilgili sahiplerinin mülkiyetindedir.

Adobe, Acrobat, Flash, Reader ve Shockwave, Amerika Birleşik Devletleri ve/veya diğer ülkelerde Adobe'nin kayıtlı ticari markaları ya da ticari markalarıdır.

Amazon, Amazon Web Services, AWS Amazon.com, Inc. veya bağlı kuruluşlarının ticari markalarıdır.

Apple, FireWire, iTunes, Mac ve Safari, Apple Inc. şirketinin ticari markalarıdır.

Arm, ABD'de ve/veya diğer ülkelerde Arm Limited'in (veya bağlı şirketlerinin) tescilli ticari markasıdır.

AutoCAD, Amerika Birleşik Devletleri ve/veya başka ülkelerde Autodesk, Inc.in ve/veya yan kuruluşlarının ve/veya bağlı kuruluşlarının bir ticari markası ya da tescilli ticari markasıdır.

Bluetooth kelimesinin, işaretinin ve logolarının Bluetooth SIG, Inc. şirketidir.

Borland, Borland Software Corporation'ın ticari markası veya tescilli ticari markasıdır.

Cisco, Cisco AnyConnect; IOS; Cisco Systems, Inc. ve/veya bağlı kuruluşlarının Amerika Birleşik Devletleri ve diğer bazı ülkelerdeki tescilli ticari markaları veya ticari markalarıdır.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop ve XenServer, Cloud Software Group, Inc. ve/veya iştiraklerinin Amerika Birleşik Devletleri ve/veya diğer ülkelerdeki tescilli ticari markaları veya ticari markalarıdır.

Cloudflare, Cloudflare Workers ve Cloudflare logosu, Amerika Birleşik Devletleri ve diğer yargı bölgelerinde Cloudflare, Inc.in ticari markaları ve/veya tescilli ticari markalarıdır.

Core, Intel Corporation veya bağlı şirketlerinin ticari markasıdır.

dBase, dataBased Intelligence, Inc.in ticari markasıdır.

Dell Technologies, Dell, EMC ve diğer ticari markalar, Dell Inc. veya yan kuruluşlarının ticari markalarıdır.

Docker ve Docker logosu, Docker, Inc. şirketinin Amerika Birleşik Devletleri ve/veya diğer ülkelerdeki ticari markaları veya tescilli ticari markalarıdır. Docker, Inc. ve diğer taraflar, burada kullanılan diğer terimlerle ilgili ticari marka haklarına da sahip olabilir.

ESET, ESET spol. s r.o. veya ilgili ESET kuruluşunun ticari markası veya tescilli ticari markasıdır.

Foxit, Foxit Corporation'ın tescilli ticari markasıdır.

Radmin, Famatech'in tescilli ticari markasıdır.

Google, Android, Google Public DNS, Google Chrome, Chrome, Google LLC şirketinin ticari markalarıdır.

HUAWEI, FusionCompute ve FusionSphere, Huawei Technologies Co., Ltd. şirketinin ticari markalarıdır.

ICQ, ICQ LLC kuruluşunun Ticari Markası ve/veya Hizmet markasıdır.

Intel, Intel Corporation veya bağlı şirketlerinin ticari markasıdır.

IBM, Business Machines Corporation şirketinin tüm dünyada birçok yasal bölgede kayıtlı olan bir ticari markasıdır.

Lenovo ve Lenovo ThinkPad, Birleşik Devletler ve/veya diğer yerlerde Lenovo'nun ticari markalarıdır.

Linux, Amerika Birleşik Devletleri ve diğer ülkelerde Linus Torvalds şirketinin tescilli ticari markasıdır.

Logitech, Amerika Birleşik Devletleri ve diğer ülkelerde Logitech'in bir ticari markası ya da tescilli ticari markasıdır.

LogMeIn Pro ve Remotely Anywhere, LogMeIn, Inc.in ticari markalarıdır.

Mail.ru, Mail.ru LLC'nin ticari markasıdır.

McAfee, McAfee LLC veya yan kuruluşlarının ABD ve/veya diğer ülkelerdeki ticari markası veya tescilli ticari markasıdır.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server, Windows Store, Microsoft şirketler grubunun tescilli ticari markalarıdır.

Mozilla, Firefox ve Thunderbird, Mozilla Foundation'ın ABD ve diğer ülkelerdeki ticari markalarıdır.

NetApp, Amerika Birleşik Devletleri ve/veya diğer ülkelerde NetApp, Inc.in ticari markası veya tescilli ticari markasıdır.

OpenSSL, OpenSSL Software Foundation'a ait bir ticari markadır.

OpenStack, OpenStack Foundation'ın Amerika Birleşik Devletleri ve diğer ülkelerdeki tescilli ticari markasıdır.

Oracle, Java ve JavaScript, Oracle Corporation ve/veya yan kuruluşlarının tescilli ticari markalarıdır.

Python, Python Software Foundation'ın ticari markası veya tescilli ticari markasıdır.

Realtek, Realtek Semiconductor Corporation'ın ticari markasıdır.

SAMSUNG, Amerika Birleşik Devletleri veya diğer ülkelerde SAMSUNG'un ticari markasıdır.

Thawte, Amerika Birleşik Devletleri ve diğer ülkelerde Symantec Corporation ve/veya bağlı kuruluşlarının ticari markası veya tescilli ticari markasıdır.

Trend Micro, Trend Micro Incorporated kuruluşunun ticari markası veya tescilli ticari markasıdır.

VERISIGN, Amerika Birleşik Devletleri ve diğer ülkelerde tescilli bir ticari marka veya VeriSign, Inc. ve yan kuruluşlarının tescilsiz bir ticari markasıdır.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere, Amerika Birleşik Devletleri ve/veya diğer ülkelerde, VMware, Inc. şirketinin ticari markaları ya da tescilli ticari markalarıdır.

Üçüncü taraf kod hakkında bilgi

Üçüncü taraf koduyla ilgili bilgiler, uygulama kurulum klasöründe bulunan legal_notices.txt dosyasında yer alır.