İçindekiler

Kaspersky Endpoint Security for Windows Yardım

Sürüm 12.1'deki yenilikler

- Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olan Kaspersky Endpoint Detection and Response bileşenini yönetmek için yerleşik bir aracı eklendi. EDR (KATA)'yı kullanmak için artık Kaspersky Endpoint Agent'a ihtiyacınız yok. Kaspersky Endpoint Security, tüm Kaspersky Endpoint Agent işlevlerini gerçekleştirebilir.
- 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

Tehditleri ortadan kaldırma

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

KES'i diğer çözümlerin bir parçası olarak kullanma

- Kaspersky EDR
- Kaspersky Sandbox
- Kaspersky MDR

Veri sağlama

- Son Kullanıcı Lisans Sözleşmesi kapsamında
- KSN'yi kullanırken
- GDPR

Yenilikler

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, Azure sanal makinesinin durumunun Kaspersky Anti Targeted Attack Platform konsolunda doğru şekilde 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.

Güncelleme 12.0

Kaspersky Endpoint Security 12.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Kaspersky Endpoint Security'nin sunucular üzerinde çalışması iyileştirildi. Artık Kaspersky Security for Windows Server'dan Kaspersky Endpoint Security for Windows'a geçebilir ve iş istasyonlarını ve sunucuları korumak için tek bir çözüm kullanabilirsiniz. Uygulama ayarlarının geçişini gerçekleştirmek için İlkeler ve görevler toplu dönüştürme sihirbazını çalıştırın. KSWS lisans anahtarı, KES'i etkinleştirmek için kullanılabilir. KES'e geçiş yaptıktan sonra sunucuyu yeniden başlatmanıza gerek yoktur. KES'e geçiş hakkında daha fazla bilgi için bkz. Geçiş Rehberi .

2. Uygulamanın Amazon Machine Image'da (AMI) ücretli bir sanal makine görüntüsünün parçası olarak lisanslanması iyileştirildi. Uygulamayı ayrıca etkinleştirmeye gerek yoktur. Bu durumda, Kaspersky Security Center, uygulamaya zaten eklenmiş olan bulut ortamı için olan lisans anahtarını kullanır.

3. Aygıt Denetimi geliştirildi:

   - Taşınabilir aygıtlar (MTP) için erişim kurallarını (okuma/yazma) yapılandırabilir, aygıtlara erişimi olan kullanıcıları veya kullanıcı grubunu seçebilir veya bir aygıt erişim programı yapılandırabilirsiniz. Artık taşınabilir aygıtlar için de çıkarılabilir sürücülerle aynı şekilde erişim kuralları oluşturabilirsiniz.

   - Artık Android Debug Bridge (ADB) veya benzeri uygulamalarda mobil cihazlara kullanıcı erişimini yapılandırabilirsiniz. Yani, örneğin, mobil cihazın yalnızca ADB'de kullanılmasına izin verebilir ve mobil cihazın çıkarılabilir bir sürücü olarak kullanılmasını

engelleyebilirsiniz.

- Artık, mobil cihaza erişim engellenmiş olsa bile, bir mobil cihazı bilgisayarın USB bağlantı noktasına bağlayarak şarj edebilirsiniz.
- Yazıcılar için artık kullanıcılar için yazdırma izinlerini yapılandırabilirsiniz. Kaspersky Endpoint Security, yerel ve ağ yazıcılarına erişim üzerinde kontrolü destekler. Artık bireysel kullanıcılar için yerel veya ağ yazıcılarında yazdırmaya izin verebilir veya bunları engelleyebilirsiniz.
- Wi-Fi ağlarına bağlantıları kontrol etmek için WPA3 protokol desteği eklendi. Artık güvenilir Wi-Fi ağ ayarlarında WPA3 protokolünü kullanmayı seçebilir ve daha az güvenli bir protokol kullanarak ağa bağlantıyı reddedebilirsiniz.

Güncelleme 11.11.0

Kaspersky Endpoint Security 11.11.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Sunucular için Günlük Denetimi bileşeni eklendi. Günlük Denetimi, Windows olay günlüğü inceleme sonuçlarına göre korunan ortamın bütünlüğünü izler. Uygulama, sistemde tipik olmayan davranış belirtilerini tespit ettiğinde, bu davranış bir siber saldırı girişiminin göstergesi olabileceğinden yöneticiyi bilgilendirir.
2. Sunucular için Dosya Bütünlük İzleyicisi bileşeni eklendi. Dosya Bütünlük İzleyicisi, belirli bir izleme alanındaki nesnelerde (dosyalar ve klasörler) yapılan değişiklikleri algılar. Bu değişiklikler bir bilgisayar güvenlik ihlalini gösterebilir. Nesne değişiklikleri tespit edildiğinde uygulama yöneticiyi bilgilendirir.
3. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) için uyarı ayrıntıları arabirimi iyileştirildi. Tehdit geliştirme zincirinin unsurları düzenlendi, zincirdeki süreçler arasındaki bağlantılar artık çakışmıyor. Bu, tehdidin gelişimini analiz etmeyi kolaylaştırır.
4. Uygulama performansı iyileştirildi. Bu amaçla, Ağ Tehdidi Koruması bileşeni tarafından ağ trafiğinin işlenmesi optimize edilmiştir.
5. Kaspersky Endpoint Security'yi yeniden başlatmadan yükseltme seçeneği eklendi. Bu, uygulamayı yükseltirken sunucuların kesintisiz olarak çalışmaya devam etmesini sağlamanıza olanak tanır. 11.10.0 sürümünden itibaren, uygulamayı yeniden başlatma yapmadan yükseltebilirsiniz. Ayrıca 11.11.0 sürümünden itibaren yamaları yeniden başlatma yapmadan da yükleyebilirsiniz.
6. Kaspersky Security Center Konsolunda *Virüs Tarama* görevi yeniden adlandırıldı. Bu görevin adı artık *Kötü Amaçlı Yazılım Taraması*.

Güncelleme 11.10.0

Kaspersky Endpoint Security 11.10.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Kaspersky Tam Disk Şifreleme ile Çoklu Oturum Açma için üçüncü taraf kimlik bilgisi sağlayıcıları desteği eklendi. Kaspersky Endpoint Security, kullanıcının ADSelfService Plus parolasını izler ve örneğin kullanıcı parolasını değiştirdiğinde Kimlik Doğrulama Aracısı verilerini günceller.
2. Cloud Sandbox teknolojisi tarafından tespit edilen tehditlerin görüntülenmesini etkinleştirme seçeneği eklendi. Bu teknoloji, Endpoint Detection and Response çözümlerinin (EDR Optimum veya EDR Expert) kullanıcılarına sunulur. *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.
3. EDR Optimum kullanıcıları için dosyalar hakkında ek bilgiler uyarı ayrıntılarına eklendi. Uyarı ayrıntıları artık güven grubu, dosyanın dijital imzası ve dağıtımı hakkında bilgiler ve diğer bilgileri içeriyor. Ayrıca, doğrudan uyarı ayrıntılarından Kaspersky Threat Intelligence Portal'daki (KL TIP) ayrıntılı dosya açıklamasına geçiş yapılması mümkün olacak.
4. Uygulama performansı iyileştirildi. Bunu yapmak için arka plan taramasının çalışmasını optimize ettik ve tarama zaten çalışıyorsa tarama görevlerini kuyruğa alma özelliğini ekledik.

Güncelleme 11.9.0

Kaspersky Endpoint Security 11.9.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Artık Kaspersky Disk Encryption'u kullanırken bir Kimlik Doğrulama Aracısı hizmet hesabı oluşturabilirsiniz. Hizmet hesabı, örneğin kullanıcı parolasını unuttuğunda bilgisayara erişim sağlamak için gereklidir. Hizmet hesabını bir rezerve hesap olarak da kullanabilirsiniz.

2. Kaspersky Endpoint Agent dağıtım paketi artık uygulama dağıtım kitinin bir parçası değil. Detection and Response çözümleri için Kaspersky Endpoint Security yerleşik aracısını kullanabilirsiniz. Gerekirse Kaspersky Endpoint Agent dağıtım paketini Kaspersky Anti Targeted Attack Platform dağıtım kitinden indirebilirsiniz.

3. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) için uyarı ayrıntıları arabirimi iyileştirildi. Tehdit Yanıtı özellikleri artık araç ipuçlarına sahip. Ayrıca, güvenlik ihlali göstergeleri tespit edildiğinde kurumsal altyapının güvenliğini sağlamaya yönelik adım adım bir talimat görüntülenir.

4. Artık Kaspersky Endpoint Security for Windows'u bir Kaspersky Hybrid Cloud Security lisans anahtarı ile etkinleştirebilirsiniz.

5. Güvenilmez sertifikalara sahip alanlarla bağlantı kurma ve şifreli bağlantıları tarama hatalarıyla ilgili yeni olaylar eklendi.

Güncelleme 11.8.0

Kaspersky Endpoint Security 11.8.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Kaspersky Endpoint Detection and Response Expert çözümünün çalışmasını desteklemek için yerleşik aracı eklendi. *Kaspersky Endpoint Detection and Response Expert*, kurumsal 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. 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.

2. Ağ İzleyicisi arabirimi geliştirildi. Ağ İzleyicisi artık TCP'ye ek olarak UDP protokolünü de gösteriyor.

3. *Virüs Taraması* görevi iyileştirildi. Tarama sırasında bilgisayarı yeniden başlattıysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır.

4. Artık görev yürütme süresi için bir sınır belirleyebilirsiniz. *Virüs Taraması* ve *IOC Taraması* görevleri için yürütme süresini sınırlayabilirsiniz. Belirtilen süre sonunda Kaspersky Endpoint Security görevi durdurur. *Virüs Taraması* görevinin uygulama süresini kısaltmak için, örneğin tarama kapsamını yapılandırabilir ya da taramayı optimize edebilirsiniz.

5. Windows 10 Enterprise çoklu oturumunda yüklenmiş uygulama için sunucu platformlarının sınırlamaları kaldırılmıştır. Kaspersky Endpoint Security artık Windows 10 Enterprise çoklu oturumunu bir sunucu işletim sistemi olarak değil bir iş istasyonu işletim sistemi olarak kabul ediyor. Aynı şekilde, sunucu platformu kısıtlamaları artık Windows 10 Enterprise çoklu oturumundaki uygulama için geçerli değil. Uygulama ayrıca etkinleştirme için bir sunucu lisans anahtarı yerine bir iş istasyonu lisans anahtarı kullanıyor.

Güncelleme 11.7.0

Kaspersky Endpoint Security for Windows 11.7.0 aşağıdaki yeni özellikleri ve iyileştirmeleri sunar:

1. Kaspersky Endpoint Security for Windows arabirimi güncellendi.

2. Windows 11, Windows 10 21H2 ve Windows Server 2022 desteği.

3. Yeni bileşenler eklendi:

   - Kaspersky Sandbox ile Entegrasyon için yerleşik aracı eklendi. *Kaspersky Sandbox çözümü* bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Kaspersky Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Kaspersky Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Kaspersky Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözümle ilgili ayrıntılı bilgi almak için Kaspersky Sandbox Yardım içeriğine bakın.

Kaspersky Sandbox'u 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. Kaspersky Sandbox'un tüm işlevlerinin çalışabilmesi için Kaspersky Security Center 13.2 gereklidir. Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçiş hakkında ayrıntılı bilgi için uygulama yardımına bakabilirsiniz.

- Kaspersky Endpoint Detection and Response Optimum çözümünün çalışmasını desteklemek için yerleşik aracı eklendi. *Kaspersky Endpoint Detection and Response Optimum*, 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.

  Kaspersky Endpoint Detection and Response bileşenini kullanmak için artık Kaspersky Endpoint Agent'a ihtiyacınız yok. Tüm Kaspersky Endpoint Agent işlevleri Kaspersky Endpoint Security tarafından gerçekleştirilecektir. Kaspersky Endpoint Agent ilkelerinin ve görevlerinin taşınması için Geçiş Sihirbazı'nı kullanın. Kaspersky Endpoint Detection and Response Optimum, tüm işlevleri kullanmak için Kaspersky Security Center 13.2'ye ihtiyaç duyar. Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçiş hakkında ayrıntılı bilgi için uygulama yardımına bakabilirsiniz.

4. Kaspersky Endpoint Agent ilkeleri ve görevleri için Geçiş Sihirbazı eklendi. Geçiş Sihirbazı, Kaspersky Endpoint Security for Windows için yeni birleştirilmiş ilkeler ve görevler oluşturur. Sihirbaz, Detection and Response çözümlerinin Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçirilmesine izin verir. Detection and Response çözümlerinde Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) ve Kaspersky Managed Detection and Response (MDR) yer alır.

5. Dağıtım kitinde yer alan Kaspersky Endpoint Agent sürüm 3.11'e güncellendi.

   Kaspersky Endpoint Security yükseltilirken, uygulama Kaspersky Endpoint Agent'ın sürümünü ve ayarlanmış amacını tespit eder. Eğer Kaspersky Endpoint Agent, Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) ve Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) için ayarlanmışsa, Kaspersky Endpoint Security bu çözümlerin çalışmasını, uygulamanın yerleşik aracısına alır. Kaspersky Sandbox and EDR Optimum için, uygulama Kaspersky Endpoint Agent'ı otomatik olarak kaldırır. MDR için, Kaspersky Endpoint Agent'ı manuel olarak kaldırabilirsiniz. Uygulama Kaspersky Endpoint Detection and Response Expert (EDR Expert) çalışması için ayarlanmışsa, Kaspersky Endpoint Security, Kaspersky Endpoint Agent'ın sürümünü yükseltir. Uygulama hakkında daha fazla ayrıntı için lütfen Kaspersky Endpoint Agent'ı destekleyen Kaspersky çözümlerinin belgelerine bakın.

6. BitLocker şifrelemesi işlevi iyileştirildi:

   - Genişletilmiş PIN artık BitLocker Drive Encryption ile kullanılabilir. *Genişletilmiş PIN* sayısal karakterlere ek olarak büyük ve küçük Latin harfleri, özel karakterler ve boşluklar gibi diğer karakterlerin kullanılmasına da izin verir.

   - İşletim sistemini yükseltmek veya güncelleme paketlerini yüklemek için BitLocker kimlik doğrulamasını devre dışı bırakma özelliği eklendi. Güncellemeler yüklenirken bilgisayarın birden fazla kez yeniden başlatılması gerekebilir. Güncellemeleri doğru şekilde yüklemek için BitLocker kimlik doğrulamasını geçici olarak kapatabilir ve güncellemeleri yükledikten sonra kimlik doğrulamasını yeniden etkinleştirebilirsiniz.

   - Artık BitLocker şifreleme parolası veya PIN için bir sona erme tarihi ayarlayabilirsiniz. Parola veya PIN'in süresi dolduğunda Kaspersky Endpoint Security kullanıcıdan yeni bir parola ister.

7. Artık BadUSB Saldırısını Önleme için maksimum klavye yetkilendirme denemesi sayısını yapılandırabilirsiniz. Yetkilendirme kodu girilirken yapılandırılan başarısız deneme sayısına ulaşıldığında, USB cihazı geçici olarak kilitlenir.

8. Güvenlik duvarı işlevi geliştirildi:

   - Artık Güvenlik duvarı paket kuralları için bir IP adres aralığı yapılandırabilirsiniz. IPv4 veya IPv6 biçiminde bir adres aralığı girebilirsiniz. Örneğin, `192.168.1.1-192.168.1.100` veya `12:34::2-12:34::99`.

   - Artık Güvenlik duvarı paket kuralları için IP adresleri yerine DNS adlarını girebilirsiniz. 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.

9. İnternet Denetimi kuralı araması iyileştirildi. Bir internet kaynağı erişim kuralı aramak için kuralın adına ek olarak, internet sitesinin URL'sini, bir kullanıcı adını, bir içerik kategorisini veya bir veri türünü kullanabilirsiniz.

10. *Virüs Taraması* görevi iyileştirildi:

- Boştayken *Virüs Taraması* görevi iyileştirildi. Tarama sırasında bilgisayarı yeniden başlattıysanız, Kaspersky Endpoint Security, taramanın kesintiye uğradığı noktadan devam ederek görevi otomatik olarak çalıştırır.

- *Virüs Taraması* görevi optimize edildi. Varsayılan olarak Kaspersky Endpoint Security, taramayı sadece bilgisayar boştayken çalıştırır. Bilgisayar taramasının ne zaman çalıştırılacağını görev özelliklerinden yapılandırabilirsiniz.

11. Artık Uygulama Etkinlik İzleyicisi tarafından sağlanan verilere kullanıcı erişimini kısıtlayabilirsiniz. *Uygulama Etkinlik İzleyicisi*, bir kullanıcının bilgisayarındaki uygulamaların etkinlikleri hakkında gerçek zamanlı bilgi görüntülemek için tasarlanmış bir araçtır. Yönetici, uygulama ilkesi özelliklerinde Uygulama Etkinlik İzleyicisini kullanıcıdan gizleyebilir.

12. REST API aracılığıyla uygulamanın yönetilmesinde güvenlik iyileştirildi. Kaspersky Endpoint Security artık REST API aracılığıyla gönderilen isteklerin imzalarını doğruluyor. Programı yönetmek için bir istek tanımlama sertifikası yüklemeniz gerekir.

Kaspersky Endpoint Security 11.4.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Görev çubuğu bildirim alanındaki uygulama simgesi için yeni tasarım. Eski simgesinin yerine artık yeni simgesi görüntülenecek. Kullanıcının bir eylem gerçekleştirmesi gerekirse (örneğin uygulamayı güncelledikten sonra bilgisayarı yeniden başlatmak), simge olarak değişecektir. Uygulamanın koruma bileşenleri devre dışı bırakılır ya da çalışmaz hale gelirse, simge veya olarak değişir. Simgenin üzerine geldiğinizde, Kaspersky Endpoint Security bilgisayar korumasındaki sorun için bir açıklama görüntüleyecektir.

2. Dağıtım kitinde yer alan Kaspersky Endpoint Agent sürüm 3.9'a güncellendi. Kaspersky Endpoint Agent 3.9, yeni Kaspersky çözümleriyle entegrasyon desteği sunuyor. Uygulama hakkında daha fazla ayrıntı için lütfen Kaspersky Endpoint Agent'ı destekleyen Kaspersky çözümlerinin belgelerine bakın.

3. Kaspersky Endpoint Security bileşenleri için *Lisans tarafından desteklenmiyor* durumu eklendi. Ana uygulama penceresindeki bileşenler listesinden bileşenlerin durumunu görüntüleyebilirsiniz.

4. Raporlara Yeni Exploit Önleme etkinlikleri eklendi.

5. Kaspersky Disk Encryption teknolojisi sürücüleri artık sürücü şifreleme başlatıldığında Windows Kurtarma Ortamına (WinRE) otomatik olarak ekleniyor. Sürücüleri, uygulama yüklenirken önceki Kaspersky Endpoint Security sürümü eklemiştir. Sürücülerin WinRE'ye eklenmesi, Kaspersky Disk Encryption teknolojisi tarafından korunan bilgisayarlardaki işletim sistemini geri yüklerken işlemin kararlılığını iyileştirebilir.

Endpoint Sensor bileşeni Kaspersky Endpoint Security'den kaldırıldı. Bilgisayarda Kaspersky Endpoint Security 11.0.0 ila 11.3.0 sürümler yüklü ise bir ilkede Endpoint Sensor ayarlarını yine de yapılandırabilirsiniz.

Kaspersky Endpoint Security 11.5.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Windows 10 20H2 desteği. Microsoft Windows 10 işletim sistemi desteği hakkında ayrıntılar için lütfen Teknik Destek Bilgi Bankası 'na bakın.

2. Güncellenmiş uygulama arabirimi. Ayrıca bildirim alanındaki, uygulama bildirimlerindeki ve iletişim kutularındaki uygulama simgesi de güncellendi.

3. Uygulama Denetimi, Aygıt Denetimi ve Uyarlamalı Anomali Denetimi bileşenleri için Kaspersky Endpoint Security web eklentisinin geliştirilmiş arabirimi.

4. XML biçiminde kural ve istisna listelerini içe ve dışa aktarmak için eklenen işlevsellik. XML biçimi, listeleri dışa aktarıldıktan sonra düzenlemenizi sağlar. Listeleri yalnızca Kaspersky Security Center Console'da yönetebilirsiniz. Aşağıdaki listeler dışa/içe aktarma için mevcuttur:

   - Davranış Tespiti (istisnalar listesi).
   - Web Tehdidi Koruması (Güvenilir internet adreslerinin listesi).
   - Posta Tehdidi Koruması (ek filtresi uzantılarının listesi).

- Ağ Tehdidi Koruması (istisnalar listesi).
- Güvenlik duvarı (ağ paketi kuralları listesi).
- Uygulama Denetimi (kurallar listesi).
- İnternet Denetimi (kurallar listesi).
- Ağ bağlantı noktası izleme (Kaspersky Endpoint Security tarafından izlenen bağlantı noktalarının ve uygulamaların listeleri).
- Kaspersky Disk Encryption (istisnalar listesi).
- Çıkarılabilir sürücüleri şifreleme (kurallar listesi).

5. Tehdit algılama raporuna nesne MD5 bilgileri eklendi. Uygulamanın önceki sürümlerinde Kaspersky Endpoint Security, bir nesnenin yalnızca SHA256'sını gösteriyordu.

6. Aygıt Denetimi ayarlarında aygıt erişimi kuralları için öncelik atama özelliği eklendi. Öncelik ataması, cihazlara kullanıcı erişiminin daha esnek bir şekilde yapılandırılmasını sağlar. Bir kullanıcı birden çok gruba eklendiyse, Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre aygıt erişimini düzenler. Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 0 önceliği ve Herkes grubuna 1 önceliği atayın. Önceliği yalnızca bir dosya sistemine sahip cihazlar için yapılandırabilirsiniz. Buna sabit sürücüler, çıkarılabilir sürücüler, disketler, CD/DVD sürücüleri ve taşınabilir aygıtlar (MTP) dahildir.

7. Yeni işlevler eklendi:

   - Sesli bildirimleri yönetin.
   - Kaspersky Endpoint Security'nin Maliyet Bilinçli Ağ İletişimi özelliği, İnternet bağlantısı sınırlıysa (örneğin, bir mobil bağlantı aracılığıyla) kendi ağ trafiğini sınırlar.
   - Kaspersky Endpoint Security ayarlarını güvenilir uzaktan yönetim uygulamaları (TeamViewer, LogMeIn Pro ve Remotely Anywhere) aracılığıyla yönetin. Kaspersky Endpoint Security'yi başlatmak ve uygulama arabirimindeki ayarları yönetmek için uzaktan yönetim uygulamalarını kullanabilirsiniz.
   - Firefox ve Thunderbird'de güvenli trafiği taramak için ayarları yönetin. Mozilla tarafından kullanılacak sertifika deposunu seçebilirsiniz: Windows sertifika deposu veya Mozilla sertifika deposu. Bu işlevsellik, yalnızca uygulanan bir ilkeye sahip olmayan bilgisayarlar için kullanılabilir. Bir bilgisayara bir politika uygulanıyorsa, Kaspersky Endpoint Security, Firefox ve Thunderbird'de Windows sertifika deposunun kullanımını otomatik olarak etkinleştirir.

8. Güvenli trafik tarama modunu yapılandırma özelliği eklendi: koruma bileşenleri devre dışı bırakılsa bile her zaman trafiği tarayın veya koruma bileşenleri tarafından talep edildiğinde trafiği tarayın.

9. Raporlardan bilgi silmek için revize edilmiş prosedür. Bir kullanıcı yalnızca tüm raporları silebilir. Uygulamanın önceki sürümlerinde, bir kullanıcı bilgileri raporlardan silinecek belirli uygulama bileşenlerini seçebiliyordu.

10. Kaspersky Endpoint Security ayarlarını içeren bir yapılandırma dosyasını içe aktarmak için revize edilmiş prosedür ve uygulama ayarlarını geri yüklemek için revize edilmiş prosedür. Kaspersky Endpoint Security, içe aktarma veya geri yükleme öncesinde sadece bir uyarı gösterir. Uygulamanın önceki sürümlerinde, yeni ayarların değerlerini, bu ayarlar uygulanmadan önce görüntüleyebiliyordunuz.

11. BitLocker tarafından şifrelenmiş bir sürücüye erişimi geri yüklemek için basitleştirilmiş prosedür. Erişim kurtarma prosedürünü tamamladıktan sonra Kaspersky Endpoint Security, kullanıcıdan yeni bir parola veya PIN kodu belirlemesini ister. Yeni bir parola belirledikten sonra, BitLocker sürücüyü şifreleyecektir. Uygulamanın önceki sürümünde, kullanıcının BitLocker ayarlarında parolayı elle sıfırlaması gerekiyordu.

12. Kullanıcılar artık belirli bir bilgisayar için kendi yerel güvenilen bölgelerini oluşturma olanağına sahiptir. Bu şekilde, kullanıcılar bir ilkedeki genel güvenilen bölgeye ek olarak kendi yerel istisnalar ve güvenilir uygulamalar listelerini oluşturabilir. Bir yönetici, yerel istisnaların veya yerel güvenilir uygulamaların kullanımına izin verebilir veya bunları engelleyebilir. Bir yönetici, bilgisayar özelliklerindeki liste öğelerini görüntülemek, eklemek, düzenlemek veya silmek için Kaspersky Security Center'ı kullanabilir.

13. Güvenilir uygulamaların özelliklerine yorum girme özelliği eklendi. Yorumlar, güvenilir uygulamalar için aramayı ve sıralamayı basitleştirmeye yardımcı olur.

14. REST API aracılığıyla uygulamanın yönetilmesi:

    - Artık Outlook için Posta Tehdidi Koruması uzantısının ayarlarını yapılandırma özelliği var.
    - Virüslerin, solucanların ve Truva atlarının tespit edilmesini devre dışı bırakmak yasaktır.

Kaspersky Endpoint Security 11.6.0 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Windows 10 21H1 desteği. Microsoft Windows 10 işletim sistemi desteği hakkında ayrıntılar için lütfen Teknik Destek Bilgi Bankası 'na bakın.
2. Managed Detection and Response bileşeni eklendi. Bu bileşen, Kaspersky Managed Detection and Response adıyla bilinen çözümle etkileşimi kolaylaştırır. Kaspersky Managed Detection and Response (MDR), yüksek nitelikli uzmanlar bulmakta zorlanan veya sınırlı dahili kaynaklara sahip kuruluşlar için sayıları gitgide artan otomatik koruma mekanizmalarını atlayabilen tehditlere karşı yirmi dört saat koruma sağlar. Çözümün nasıl çalıştığı hakkında ayrıntılı bilgi için lütfen Kaspersky Managed Detection and Response Yardım içeriğine bakın.
3. Dağıtım kitinde yer alan Kaspersky Endpoint Agent sürüm 3.10'a güncellendi. Kaspersky Endpoint Agent 3.10 yeni özellikler sunar, önceki bazı sorunları çözer ve iyileştirilmiş bir kararlılığa sahiptir. Uygulama hakkında daha fazla ayrıntı için lütfen Kaspersky Endpoint Agent'ı destekleyen Kaspersky çözümlerinin belgelerine bakın.
4. Artık Ağ Tehdidi Koruması ayarları ile Ağ Taşma ve Bağlantı Noktası Tarama gibi saldırılara karşı korumayı yönetme imkanı sağlar.
5. Güvenlik Duvarı için yeni bir ağ kuralları oluşturma yöntemi eklendi. Ağ İzleyicisi penceresinde görüntülenen bağlantılar için paket kuralları ve uygulama kuralları ekleyebilirsiniz. Ancak ağ kuralı bağlantı ayarları otomatik olarak yapılandırılacaktır.
6. Ağ İzleyicisi arabirimi geliştirildi. Ağ etkinliği hakkında bilgiler eklendi: ağ etkinliğini başlatan işlem kimliği; ağ türü (yerel ağ veya İnternet); yerel bağlantı noktaları. Ağ türü hakkındaki bilgiler varsayılan olarak gizlidir.
7. Artık yeni Windows kullanıcıları için Kimlik Doğrulama Aracısı hesaplarını otomatik olarak oluşturma imkanı vardır. Aracı, bir kullanıcının Kaspersky Disk Encryption teknolojisi kullanılarak şifrelenmiş sürücülere erişim sağlamak ve işletim sistemini yüklemek için kimlik doğrulamayı tamamlamasına olanak tanır. Uygulama, 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. Bu, zaten şifrelenmiş sürücülere sahip bilgisayarlar için Kimlik Doğrulama Aracısı hesaplarını manuel olarak eklemeniz gerekmediği anlamına gelir.
8. Artık kullanıcıların bilgisayarlarındaki uygulama arabiriminde disk şifreleme sürecini (Kaspersky Disk Encryption ve BitLocker) izleme özelliği var. Şifreleme İzleyicisi aracını ana uygulama penceresinden çalıştırabilirsiniz.

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?

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?

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?

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).

Davranış analizi

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

Otomatik analiz

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.

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.

Kaspersky 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 Optimum'u 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.

Seçim ağacı

Bölüm	Bileşen
Temel Tehdit Koruması	**Dosya Tehdidi Koruması** Dosya Tehdidi Koruması bileşeni, bilgisayarın dosya sistemine virüs bulaşmasını önlemenizi sağlar. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni kalıcı olarak bilgisayarın RAM'inde bulunur. Bileşen bilgisayarın tüm sürücülerindeki ve bağlı sürücülerdeki 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, İnternet üzerinden zararlı dosyaların indirilmesini önler ve aynı zamanda zararlı ve kimlik avı amaçlı web sitelerini 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. Varsayılan olarak, Posta Tehdidi Koruması bileşeni kalıcı olarak bilgisayarın RAM'inde bulunur ve POP3, SMTP, IMAP veya NNTP protokolleri ya da Microsoft Office Outlook posta istemcisi (MAPI) kullanılarak alınan veya gönderilen tüm mesajları tarar. Bileşen, anti-virüs veritabanları, Kaspersky Security Network bulut hizmeti ve sezgisel analiz yardımıyla bilgisayar koruması sağlar. **Ağ Tehdidi Koruması** Ağ Tehdidi Koruması bileşeni (Ayrıca Saldırı Tespit Sistemi olarak da adlandırılır), ağ saldırılarının karakteristik aktiviteleri için gelen ağ trafiğini izler. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security veritabanlarında sunulmaktadır. Ağ Tehdidi Koruması bileşeninin tespit ettiği ağ saldırıları listesi, veritabanı ve uygulama modülü güncellemeleri sırasında güncellenir. **Güvenlik Duvarı** Güvenlik Duvarı, İnternet veya yerel ağ üzerinde çalışırken bilgisayara izinsiz bağlantılar kurulmasını 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.

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 dosyaların kategorisi ve tanınırlığı hakkındaki bilgilerle birlikte taranan web adreslerinin 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.

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.

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'nin 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, bilgisayarı bu tür aygıtlar bağlandığında virüslere karşı korur ve veri kaybını veya sızıntılarını önler.

İnternet Denetimi

İnternet Denetimi, kullanıcının internet kaynaklarına 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 inceleme sonuçlarına göre korunan ortamın bütünlüğünü izler. Uygulama, sistemde tipik olmayan davranış belirtilerini tespit ettiğinde, bu davranış bir siber saldırı girişiminin göstergesi olabileceğinden yöneticiyi bilgilendirir.

Dosya Bütünlük İzleyicisi

Dosya Bütünlük İzleyicisi, belirli bir izleme alanındaki nesnelerde (dosyalar ve klasörler) yapılan değişiklikleri algılar. Bu değişiklikler bir bilgisayar güvenlik ihlalini gösterebilir. Nesne değişiklikleri tespit edildiğinde uygulama yöneticiyi bilgilendirir.

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.

Güncelle

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 elle 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.

Bütünlük denetimi

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

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.

Kaspersky Sandbox

Kaspersky Sandbox çözümü için yerleşik aracı. *Kaspersky Sandbox çözümü* bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Kaspersky Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Kaspersky Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Kaspersky Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözümle ilgili ayrıntılı bilgi almak için Kaspersky Sandbox 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.

Dağıtım kiti

Dağıtım kiti aşağıdaki dağıtım paketlerini içerir:

- **Güçlü şifreleme (AES256)**

  Bu dağıtım paketi, 256 bit etkin anahtar uzunluğuna sahip AES (Gelişmiş Şifreleme Standardı) şifreleme algoritmasını kullanan şifreleme araçlarını içerir.

- **Hafif şifreleme (AES56)**

  Bu dağıtım paketi, 56 bit etkin anahtar uzunluğuna sahip AES şifreleme algoritmasını kullanan şifreleme araçlarını içerir.

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 için Kaspersky Endpoint Security Yönetim Eklentisi kurulum paketi.
`bases.cab`	Kurulum sırasında kullanılan güncelleme paketi dosyaları.
`cleaner.cab`	Uyumsuz yazılımları kaldırma dosyaları.
`incompatible.txt`	Uyumsuz yazılımların listesini içeren dosya.
`ksn_<dil kodu>.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.
`keswin_web_plugin.zip`	Kaspersky Endpoint Security web eklentisinin yüklenmesi için gereken dosyaları içeren arşiv.

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

Donanım ve yazılım gereksinimleri

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

Minimum genel gereksinimler:

- Sabit sürücüde 2 GB boş disk alanı;
- İŞLEMCİ:
  - İş İstasyonu: 1 GHz;
  - Sunucu: 1.4 GHz;
  - SSE2 komut seti desteği.

- RAM:
  - İş İstasyonu (x86): 1 GB;
  - İş İstasyonu (x64): 2 GB;
  - Sunucu: 2 GB.

İş istasyonları

İş istasyonları için desteklenen işletim sistemleri:

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

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 (Küme Modu). Uygulama ayrıca Çekirdek Modu desteği sunuyor (bilinen sorunlara bakın).

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 veya üstü;
- Windows Web Server 2008 R2 Service Pack 1 veya üzeri;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2016 Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2019 Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Çekirdek Modu dahil).

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 SP2 veya üstü;
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 veya üstü;
- Windows Server 2008 Standard / Enterprise / Datacenter SP2 veya üstü;
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP2 veya üstü;
- Microsoft Small Business Server 2008 Standard / Premium SP2 veya üstü.

Sanal platformlar

Desteklenen sanal platformlar:

- VMware Workstation 17.0 Pro;
- VMware ESXi 8.0a;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2212;
- Citrix Provisioning 2212;
- Citrix Hypervisor 8.2 (Kümülatif Güncelleme 1).

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.

Kaspersky Security Center desteği

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

- Kaspersky Security Center 12
- Kaspersky Security Center 13

- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2
- Kaspersky Security Center 13.2.2
- Kaspersky Security Center 14
- Kaspersky Security Center 14.1
- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2

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 özellikleri karşılaştırması

Özellik	İş istasyonu	Sunucu
Gelişmiş Tehdit Koruması		
Kaspersky Security Network	✓	✓
Davranış Tespiti	✓	✓
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 Denetleyici	–	✓
Uygulama Denetimi	✓	✓
Aygıt Denetimi	✓	✓
İnternet Denetimi	✓	✓
Uyarlamalı Anomali Denetimi	✓	–
Dosya Bütünlüğü İzleyici	–	✓
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	✓	✓
Endpoint Detection and Response (KATA)	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response (MDR)	✓	✓

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. Web Console üzerinde çalışmak için Yönetim Sunucusuna erişimi olan herhangi bir bilgisayardaki bir tarayıcıyı kullanabilirsiniz.

Uygulamayı, Kaspersky Security Center Cloud Console kullanarak da yönetebilirsiniz. *Kaspersky Security Center Cloud Console*, Kaspersky Security Center'ın bulut 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 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	✓	✓	✓
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 Denetleyici	✓	✓	✓
Uygulama Denetimi	✓	✓	✓
Aygıt Denetimi	✓	✓	✓
İnternet Denetimi	✓	✓	✓
Uyarlamalı Anomali Denetimi	✓	✓	✓
Dosya Bütünlüğü İzleyici	✓	✓	✓
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	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Kaspersky Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Görevler			
Anahtar ekle	✓	✓	✓
Uygulama bileşenlerini değiştirme	✓	✓	✓
Envanter	✓	✓	✓
Güncelle	✓	✓	✓
Güncellemeyi geri alma	✓	✓	✓
Kötü Amaçlı Yazılım Taraması	✓	✓	✓
Bütünlük denetimi	✓	✓	–
Veri Silme	✓	✓	✓
Kimlik Doğrulama Aracısı hesaplarını yönet (Kaspersky Disk Encryption)	✓	✓	–
IOC Taraması (EDR)	–	✓	✓
Dosyayı Karantinaya taşı (EDR)	–	✓	✓
Dosyayı al (EDR)	–	✓	✓
Dosyayı sil (EDR)	–	✓	✓
İşlem başlangıcı (EDR)	–	✓	✓
İşlemi sonlandır (EDR)	–	✓	✓

Diğer uygulamalarla uyumluluk

Kurulumdan önce Kaspersky Endpoint Security, bilgisayarda Kaspersky uygulamalarının var olup olmadığını denetler. Uygulama ayrıca bilgisayardaki uyumsuz yazılımları denetler.

Üçüncü taraf uygulamalarla uyumluluk

Uyumsuz yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında mevcuttur.

INCOMPATIBLE.TXT DOSYASINI İNDİRİN

Kaspersky uygulamaları ile uyumluluk

Kaspersky Endpoint Security, aşağıdaki Kaspersky uygulamaları ile uyumlu değildir:

- 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 (Endpoint Sensor bileşeni dahil).
- Kaspersky Sandbox (Kaspersky Endpoint Agent dahil).
- Kaspersky Endpoint Detection and Response (Endpoint Sensor bileşeni dahil).

  Endpoint Agent bileşeni bir bilgisayara başka Kaspersky uygulamalarının dağıtım araçları kullanılarak yüklenmişse, bu bileşenler Kaspersky Endpoint Security ürününün yüklenmesi sırasında otomatik olarak kaldırılır. Uygulama bileşenleri listesinden Endpoint Sensor/Kaspersky Endpoint Agent seçilirse, Kaspersky Endpoint Security, Endpoint Sensor bileşenini de içerebilir.

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

Uyumsuz yazılım kontrolünü atlama

Kaspersky Endpoint Security bilgisayarda uyumsuz yazılım tespit ederse uygulamanın kurulumu devam etmez. Kuruluma devam etmek için uyumsuz yazılımı kaldırmanız gerekir. Ancak, üçüncü taraf yazılım satıcısı belgelerinde yazılımlarının Endpoint Protection Platforms (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 uyumsuz bir yazılım kontrolü çalıştırmadan başlatmanız gerekir. Bunu yapmak için yükleyiciye aşağıdaki parametreleri aktarın:

- `SKIPPRODUCTCHECK=1`. Uyumsuz yazılım kontrolü devre dışı bırakın. Uyumsuz yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında mevcuttur. Bu parametre için hiçbir değer ayarlanmaz ve uyumsuz yazılım tespit edildiği takdirde Kaspersky Endpoint Security yüklemesi sonlandırılır.

- `SKIPPRODUCTUNINSTALL=1`. Tespit edilen uyumsuz yazılımın otomatik kaldırılmasını devre dışı bırakın. Bu parametre için hiçbir değer ayarlanmazsa, Kaspersky Endpoint Security uyumsuz yazılımı kaldırmayı dener.

- `CLEANERSIGNCHECK=0`. Tespit edilen uyumsuz yazılımın dijital imza doğrulamasını devre dışı bırakma. 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.

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.

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

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. 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.

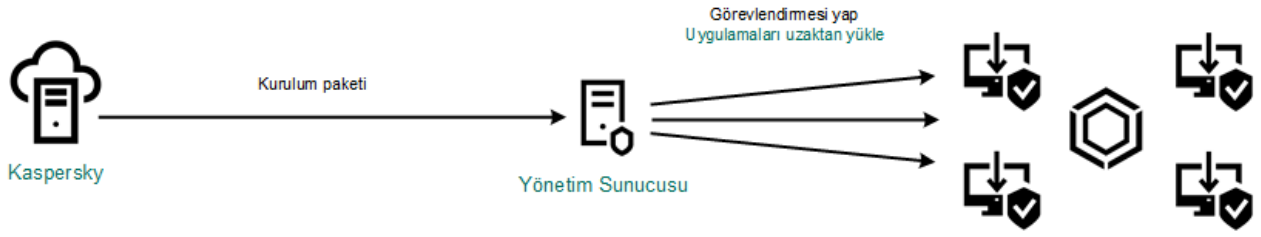
Uygulamanın standart kurulumu

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.

   Kurulum 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. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Gelişmiş** → **Uzaktan kurulum** klasörüne gidin.
2. **Kurulum paketini yönetilen cihazlara dağıt (iş istasyonları)** bağlantısına tıklayın.

Bu, Koruma Dağıtım Sihirbazını başlatır. Sihirbazın talimatlarını uygulayın.

İstemci bilgisayarda 139 ve 445 numaralı TCP bağlantı noktaları ile 137 ve 138 numaralı UDP bağlantı noktaları 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 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 elle belirtin veya adresleri listeden içe aktarın. Görevi atamak istediğiniz aygıtların NetBIOS adlarını, IP adreslerini ve IP alt ağlarını belirleyebilirsiniz.

3. Adım. Uzak kurulum görevi ayarlarını tanımlama

Şu ek uygulama ayarlarını yapılandırın:

- **Kurulum paketini indirmeye zorla**. Uygulama kurulum yöntemini seçin:
  - **Ağ Aracısını kullanarak**. Ağ Aracısı bilgisayara yüklü değilse öncelikle işletim sisteminin araçları kullanılarak Ağ Aracısı yüklenir. 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.

4. 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.

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. 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 (aşağıdaki resme bakın).

7. 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.

8. Adım. yüklemenin başlatılması

Sihirbazdan çıkın. 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 ana penceresinden **Keşif ve Dağıtım → Dağıtım ve Atama → Koruma Dağıtım Sihirbazı** seçimini yapın.

Bu, Koruma Dağıtım Sihirbazını başlatır. Sihirbazın talimatlarını uygulayın.

İstemci bilgisayarda 139 ve 445 numaralı TCP bağlantı noktaları ile 137 ve 138 numaralı UDP bağlantı noktaları 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 elle 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 seçme:
  - **Ağ Aracısını kullanarak**. Ağ Aracısı bilgisayara yüklü değilse öncelikle işletim sisteminin araçları kullanılarak Ağ Aracısı yüklenir. 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 elle 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 (aşağıdaki resme bakın).

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

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

Kurulum paketi oluşturma

Kurulum 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** düğmesine 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 12.1*.

3. Adım. Kurulum için dağıtım paketini seçme

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

Gerekirse, **Güncellemeleri veri havuzundan kurulum paketine kopyala** onay kutusunu kullanarak kurulum paketindeki antivirüs veritabanlarını güncelleyin.

4. Adım. Son Kullanıcı Lisans Sözleşmesi ve Gizlilik İlkesi

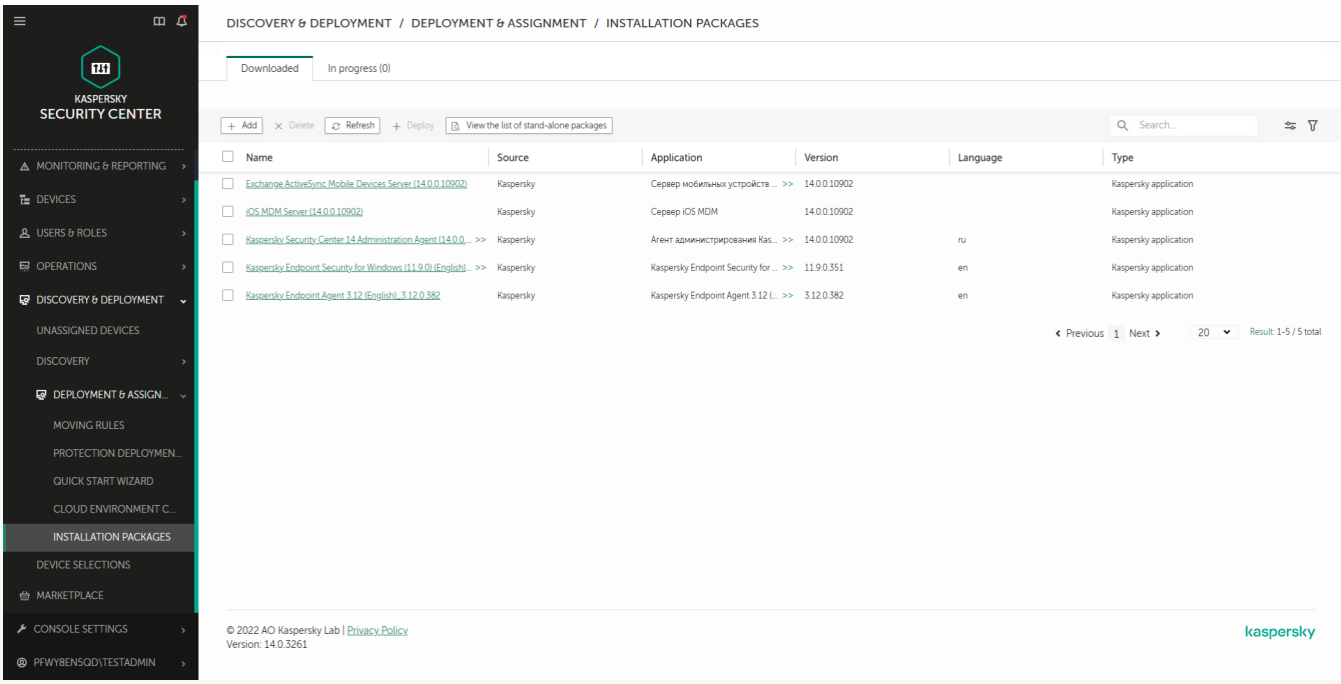
Son Kullanıcı Lisans Sözleşmesi ile Gizlilik İlkesi'nin şartlarını okuyun ve kabul edin.

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 ayarlarından ayrıca uygulama bileşenlerini seçebilir ve uygulama yükleme ayarlarını yapılandırabilirsiniz (aşağıdaki tabloya bakın). 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 ve Cloud Console'da nasıl bir kurulum paketi 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** düğmesine tıklayın.

Yeni Paketler Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.



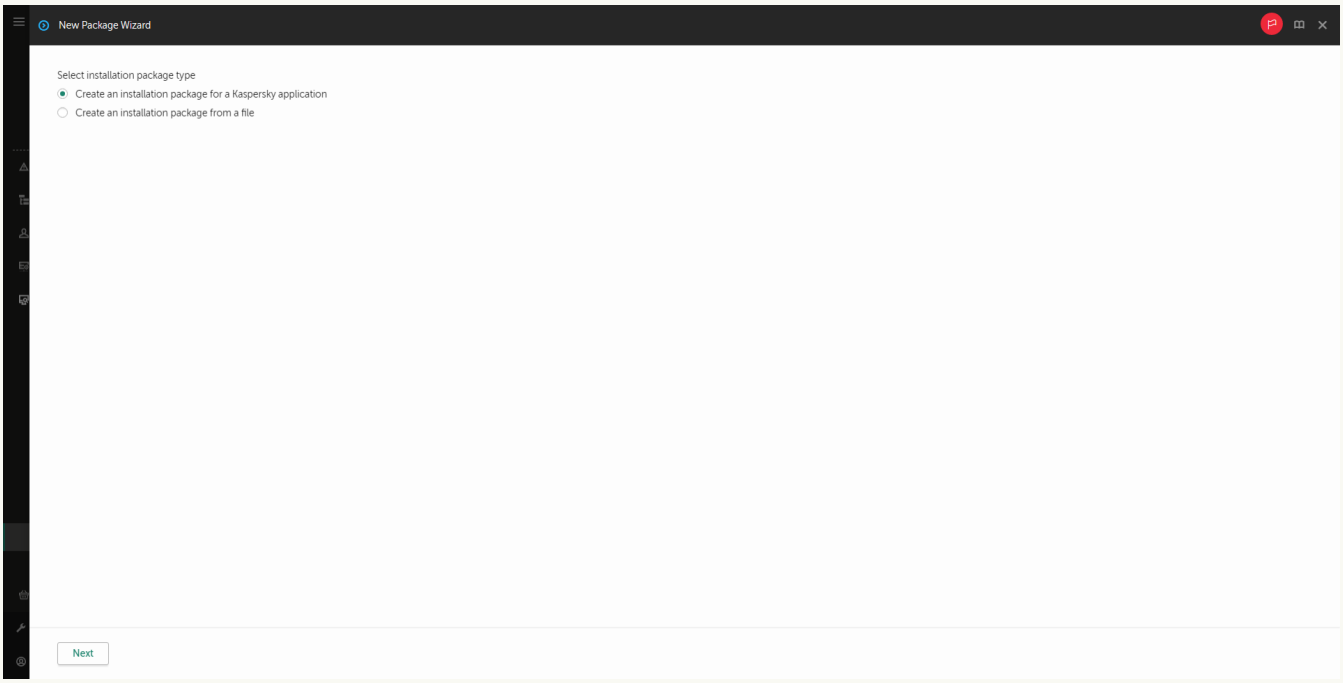
Kurulum paketlerinin listesi

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.

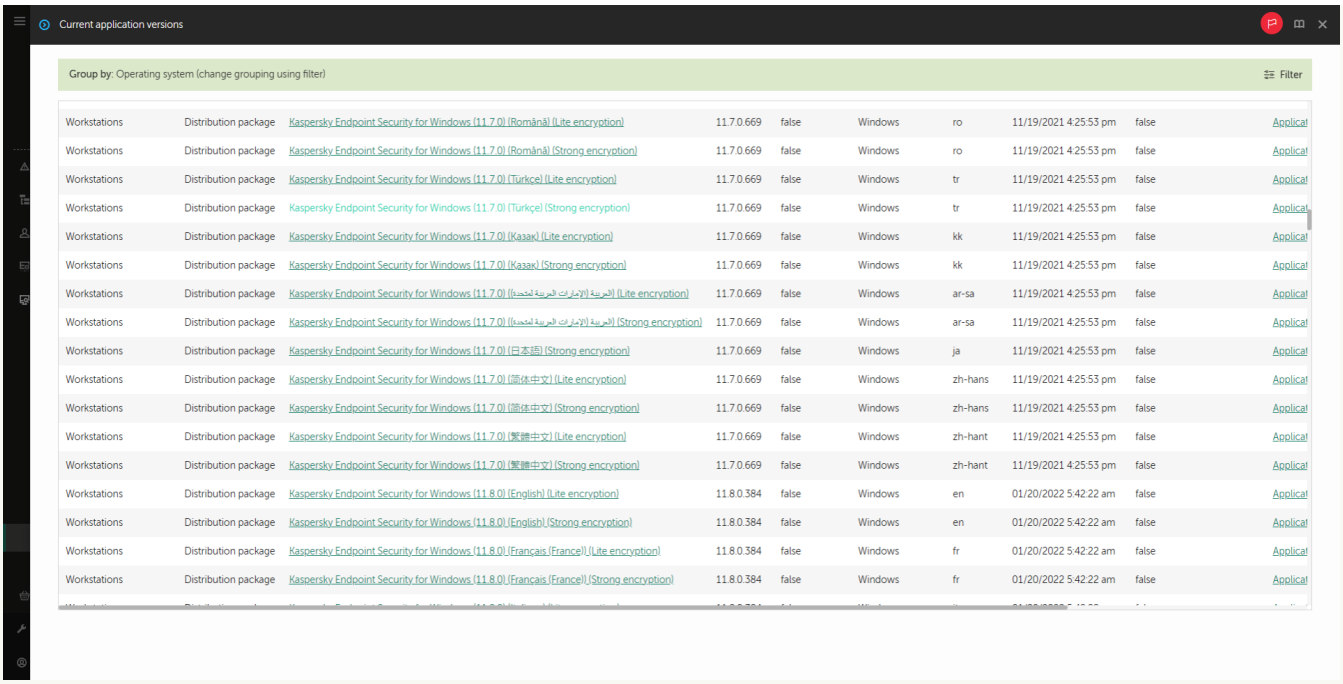
Ayrıca bir dosyadan da bir kurulum paketi oluşturabilirsiniz.



Kurulum paketi türleri

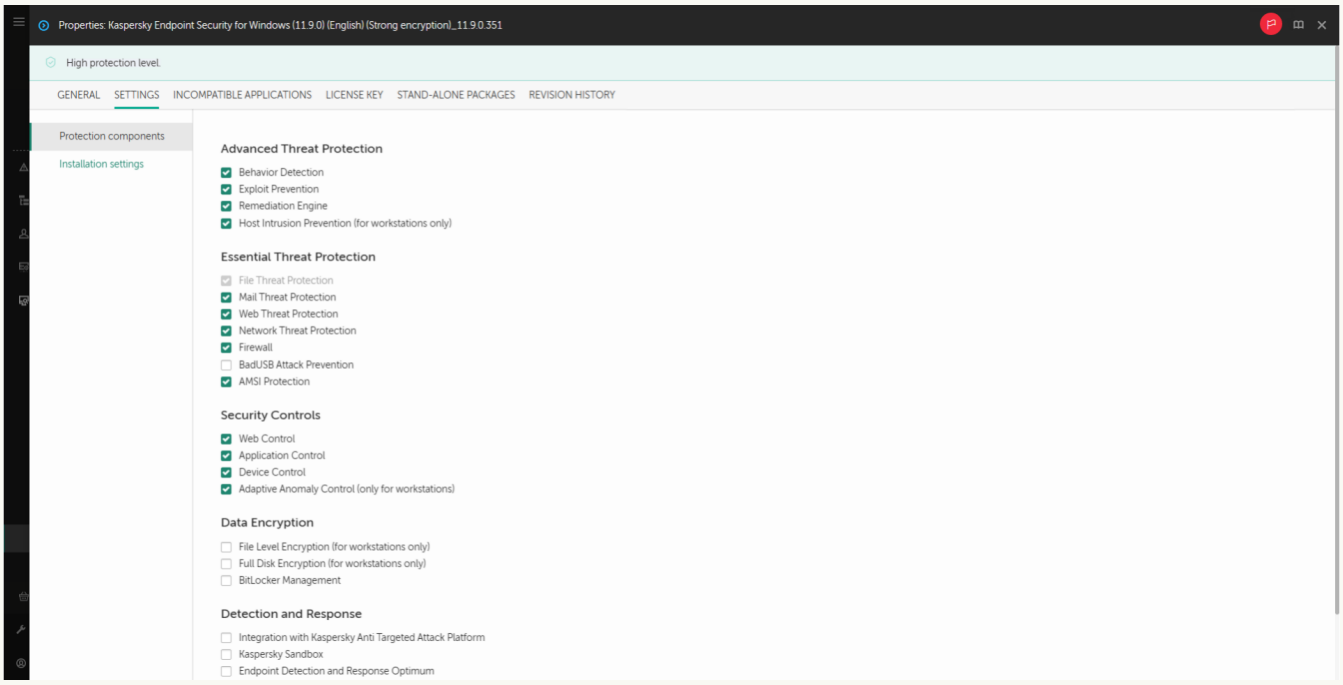
2. Adım. Kurulum paketleri

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.

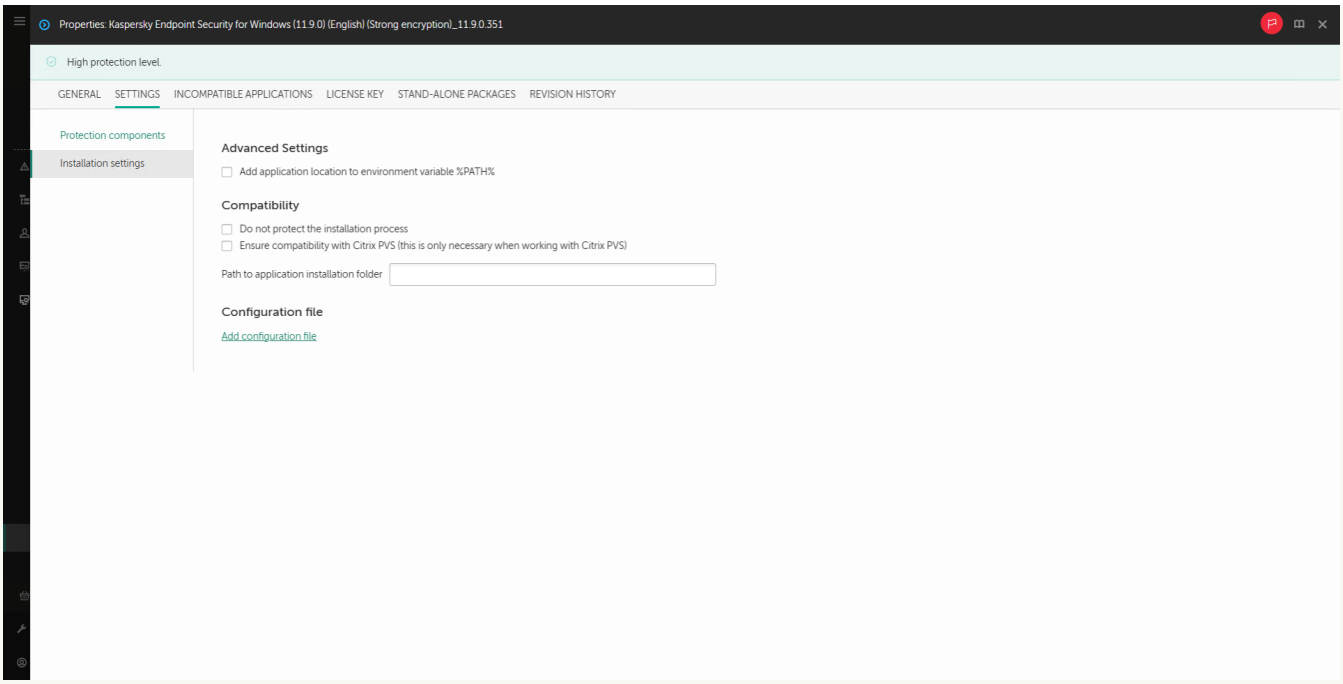


Kaspersky sunucularındaki kurulum paketlerinin listesi

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 ayarlarından ayrıca uygulama bileşenlerini seçebilir ve uygulama yükleme ayarlarını yapılandırabilirsiniz (aşağıdaki tabloya bakın). 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	Bu bölümde, kullanılabilir olacak uygulama bileşenlerini seçebilirsiniz. *Uygulama bileşenlerini değiştir* görevini kullanarak uygulama bileşenlerini daha sonra değiştirebilirsiniz. BadUSB Saldırısı Önleme bileşeni, Detection and Response bileşeni ve veri şifreleme bileşenleri varsayılan olarak yüklenmez. Bu bileşenler kurulum paketi ayarlarında eklenebilir. Detection and Response bileşenlerini yüklemeniz gerekiyorsa Kaspersky Endpoint Security aşağıdaki yapılandırmaları destekler: • Sadece Endpoint Detection and Response Optimum • Sadece Endpoint Detection and Response Expert • Sadece Endpoint Detection and Response (KATA) • Sadece Kaspersky Sandbox • Endpoint Detection and Response Optimum ve Kaspersky Sandbox • Endpoint Detection and Response Expert ve Kaspersky Sandbox • Endpoint Detection and Response (KATA) ve Kaspersky Sandbox Kaspersky Endpoint Security, uygulamayı yüklemeden önce bileşenlerin seçimini doğrular. Detection and Response bileşenlerinin seçilen yapılandırması desteklenmiyorsa Kaspersky Endpoint Security yüklenemez.
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.

Kurulum işlemini koruma. 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 yüklenemezse (örneğin Windows Uzak Masaüstü yardımıyla uzaktan kurulum gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız tavsiye edilir.

Citrix PVS ile uyumluluğu sağla (seçenek sadece Citrix PVS ile çalışırken gereklidir). Kaspersky Endpoint Security'yi sanal bir makineye yüklemek için Citrix Provisioning Services desteğini etkinleştirebilirsiniz.

Azure WVD uyumluluk modunu kullan. Bu özellik, Azure sanal makinesinin durumunun Kaspersky Anti Targeted Attack Platform konsolunda doğru şekilde görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensör Kimliği) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensör Kimliği atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensör Kimliği değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir.

Uygulama yükleme klasörüne giden yol. Bir istemci bilgisayarda Kaspersky Endpoint Security'nin kurulum yolunu değiştirebilirsiniz. Varsayılan olarak uygulama, `%ProgramFiles%\Kaspersky Lab\KES` klasörüne yüklenir.

Yapılandırma dosyası. Kaspersky Endpoint Security ayarlarını tanımlayan bir dosya yükleyebilirsiniz. Uygulamanın yerel arabiriminde bir yapılandırma dosyası oluşturabilirsiniz.

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. 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 paketinin özelliklerini açın.
3. **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. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.

   Görevler listesi açılır.

2. **Yeni görev** düğmesine 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 Aracısını kullanarak**. Ağ Aracısı bilgisayara yüklü değilse öncelikle işletim sisteminin araçları kullanılarak Ağ Aracısı yüklenir. 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 elle 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 12.1 yükle*.

10. Adım. Görev oluşturmayı bitirme

Sihirbazdan çıkın. 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 **Aygıtlar** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. **Ekle** düğmesine 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 cihazları seçin** 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 (12.1) 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 Aracısını kullanarak**. Ağ Aracısı bilgisayara yüklü değilse öncelikle işletim sisteminin araçları kullanılarak Ağ Aracısı yüklenir. 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 elle 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

Bitir 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 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.

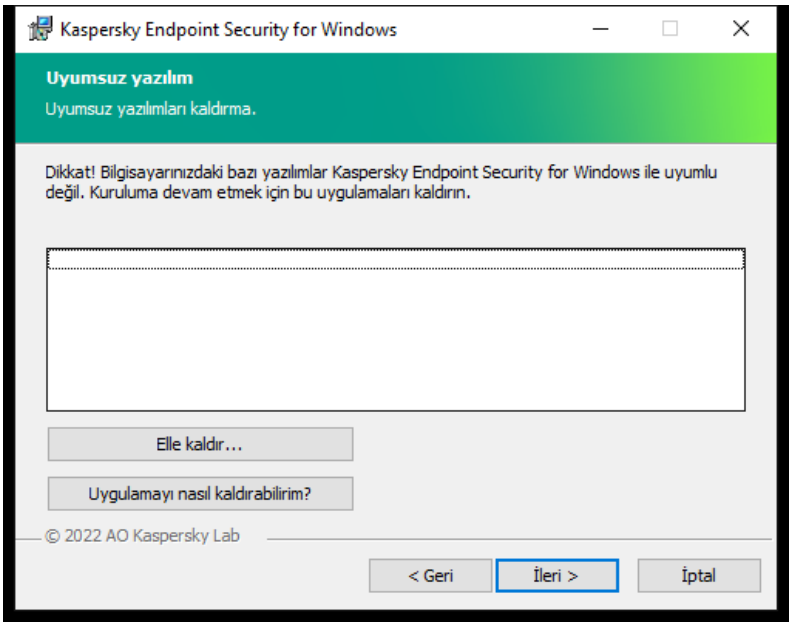
Kurulum Sihirbazı başlatılır.

Yükleme için hazırlık

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

- Yüklenmiş uyumsuz yazılımların varlığı (uyumsuz yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında mevcuttur).
- Donanım ve yazılım gereksinimlerinin karşılanıp karşılanmadığı.
- 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 yazılımı kaldırma

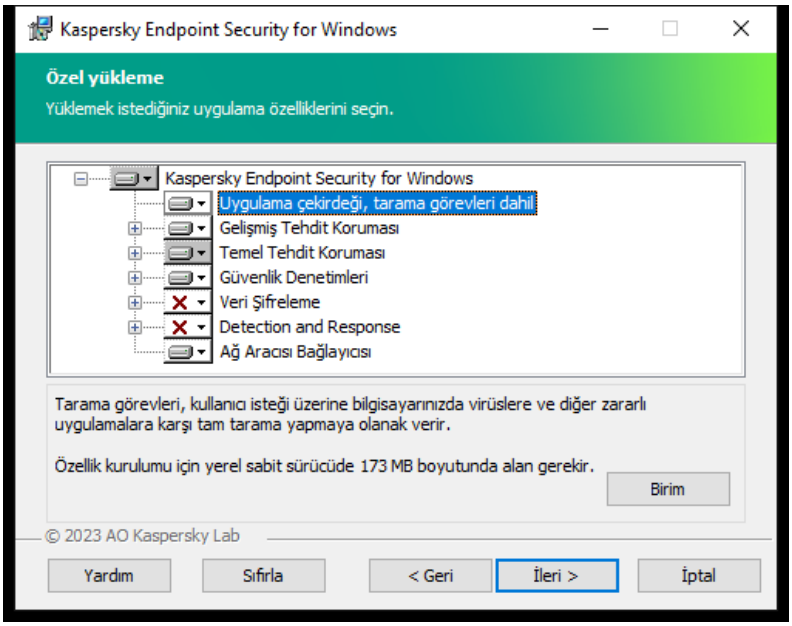
Bilgisayar belirtilen gereksinimleri karşılıyorsa Kurulum Sihirbazı, yüklenen uygulama ile birlikte aynı anda çalışırken çakışmaya neden olabilecek Kaspersky uygulamalarını arar. Bu uygulamalar bulunur bunları elle kaldırmanız istenir.

Algılanan uygulamalar Kaspersky Endpoint Security'nin önceki sürümlerini içeriyorsa geçiş yapabilen tüm veriler (etkinleştirme verileri ve uygulama ayarları gibi) korunur ve Kaspersky Endpoint Security 12.1 for Windows'un yüklenmesi sırasında kullanılır ve uygulamanın önceki sürümü otomatik olarak kaldırılır. Bu, aşağıdaki uygulama sürümleri için geçerlidir:

- Kaspersky Endpoint Security 11.6.0 for Windows (yapı 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (yapı 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 for Windows (yapı 11.8.0.384).
- Kaspersky Endpoint Security 11.9.0 for Windows (yapı 11.9.0.351).
- Kaspersky Endpoint Security 11.10.0 for Windows (yapı 11.10.0.399).
- Kaspersky Endpoint Security 11.11.0 for Windows (yapı 11.11.0.452).
- Kaspersky Endpoint Security 12.0 for Windows (yapı 12.0.0.465).

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 yükleme bileşenleri yüklenmek üzere seçilidir:

- BadUSB Saldırısı Önleme.
- Veri Şifreleme bileşenleri.
- Detection and Response bileşenleri.

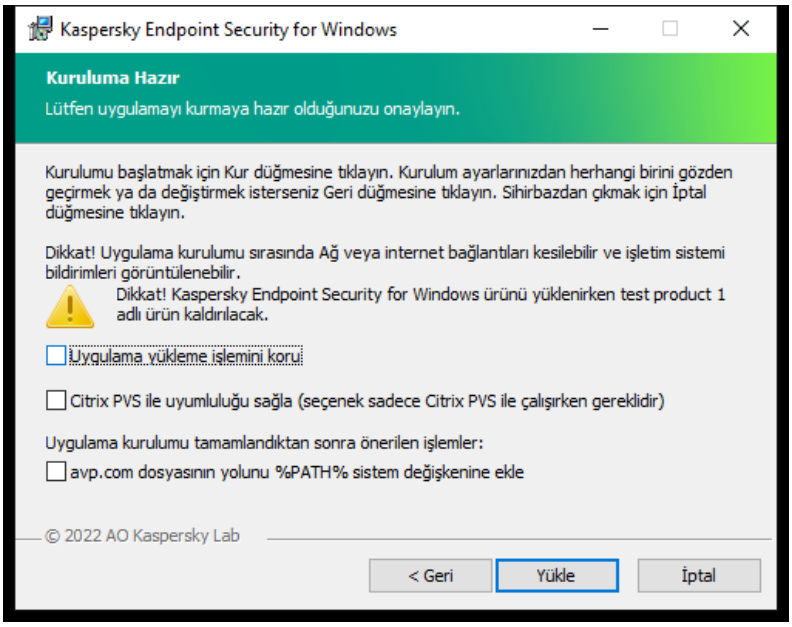
Uygulama yüklendikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz. Bunu yapmak için, Kurulum Sihirbazını tekrar çalıştırmanız ve kullanılabilir bileşenleri değiştirmeyi seçmeniz gerekir.

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

- Sadece Endpoint Detection and Response Optimum
- Sadece Endpoint Detection and Response Expert
- Sadece Endpoint Detection and Response (KATA)
- Sadece Kaspersky Sandbox
- Endpoint Detection and Response Optimum ve Kaspersky Sandbox
- Endpoint Detection and Response Expert ve Kaspersky Sandbox
- Endpoint Detection and Response (KATA) ve Kaspersky Sandbox

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

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 yüklenemezse (örneğin Windows Uzak Masaüstü yardımıyla uzaktan kurulum gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız tavsiye edilir.

Citrix PVS ile uyumluluğu sağla (seçenek sadece Citrix PVS ile çalışırken gereklidir). 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 file dosyasından ayarları uygulamak için bu dosyayı Kaspersky Endpoint Security dağıtım paketini içeren klasöre yerleştirin.

SETUP.INI DOSYASINI İNDİRİN

setup.ini dosyası aşağıdaki bölümleri içerir:

- `[Setup]` – uygulama yüklemesinin genel ayarları.
- `[Components]` – 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. Managed Detection and Response bileşeni de bu blokta yoktur. Bu bileşeni yüklemek için Kaspersky Security Center Konsolunda Managed Detection and Response özelliğini etkinleştirmeniz gerekir.
- `[Tasks]` – Kaspersky Endpoint Security görevlerinin listesine eklenecek görevlerin seçimi. Herhangi bir görev belirtilmezse tüm görevler Kaspersky Endpoint Security'nin görev listesine eklenir.

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

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

setup.ini dosyasının ayarları

Bölüm	Parametre	Açıklama
`[Setup]`	`InstallDir`	Uygulama yükleme klasörüne giden yol.
	`ActivationCode`	Kaspersky Endpoint Security etkinleştirme kodu.
	`EULA=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.
	`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.
	`Parola`	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.

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 yüklenemezse (örneğin Windows Uzak Masaüstü yardımıyla uzaktan kurulum gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız tavsiye edilir.

`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, Azure sanal makinesinin durumunun Kaspersky Anti Targeted Attack Platform konsolunda doğru şekilde görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensör Kimliği) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensör Kimliği atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensör Kimliği değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir.

`Reboot=1`

Uygulamanın yüklenmesinin veya yükseltilmesinin ardından gerekirse bilgisayarın otomatik olarak yeniden başlatılması. Bu parametre için bir değer ayarlanmadığı takdirde bilgisayarın otomatik olarak yeniden başlatılması engellenir.

Kaspersky Endpoint Security'yi yüklerken yeniden başlatma gerekli değildir. Yalnızca kurulumdan önce uyumsuz uygulamaları kaldırmanız gerekirse yeniden başlatma gereklidir. Uygulama sürümünü güncellerken de yeniden başlatma gerekebilir.

`AddEnvironment`

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 `Zorla` yükseltme modu belirtilmişse ve uygulama ayarlarında `Kesintisiz` modu belirtilmişse, yükseltme yeniden başlatılmadan yüklenecektir (`Zorla`). `UPGRADEMODE` parametresinin belirtilmediği setup.ini dosyasını kullanıyorsanız, yükleyici varsayılan değeri (`Kesintisiz`) 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.21.13\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.
	`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 `<ETKİ ALANI>\<KullanıcıAdı>` (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 bağlantı noktasıdır. Varsayılan olarak 6782 bağlantı noktası kullanılır. Bağlantı noktasının 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.
`[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 ve Response Optimum ile birlikte Kaspersky Sandbox bileşenleri de bilgisayara yüklenir. Endpoint Detection and Response Expert 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.
	`Güvenlik Duvarı`	Güvenlik Duvarı.
	`NetworkThreatProtection`	Ağ Tehdidi Koruması.
	`WebControl`	İnternet Denetimi.
	`DeviceControl`	Aygıt Denetimi.
	`ApplicationControl`	Uygulama Denetimi.
	`AdaptiveAnomaliesControl`	Uyarlamalı Anomali Denetimi.
	`LogInspector`	Günlük Denetleyici
	`FileIntegrityMonitor`	Dosya Bütünlüğü İzleyici
	`FileEncryption`	Dosya Düzeyinde Şifreleme kitaplıkları.
	`DiskEncryption`	Tam Disk Şifreleme kitaplıkları.
	`BadUSBAttackPrevention`	BadUSB Saldırısı Önleme.
	`EDR`	Endpoint Detection and Response Optimum (EDR Optimum). Bileşen, EDR Expert (`EDRCloud`) ve EDR KATA (`EDRKATA`) bileşenleri ile uyumlu değildir.
	`EDRCloud`	Endpoint Detection and Response Expert (EDR Expert). Bileşen, EDR Optimum (`EDR`) ve EDR KATA (`EDRKATA`) bileşenleri ile uyumlu değildir.
	`AntiAPTFeature`	Endpoint Detection and Response (KATA). Bileşen, EDR Expert (`EDRCloud`) ve EDR Optimum (`EDR`) bileşenleri ile uyumlu değildir.
	`SB`	Kaspersky Sandbox.
	`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.
`[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.

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.

- 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.

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

1. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.

   Görevler listesi açılır.

2. **Yeni görev** düğmesine tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (12.1) → **Yüklenecek bileşenleri seçin** seçimini yapın.

2. Adım. Uygulama bileşenlerini değiştirme için görev ayarları

Kullanıcının bilgisayarında kullanılabilecek uygulama bileşenlerini seçin.

Görev için gelişmiş ayarları 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 elle 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 *Uygulama Denetimi bileşenini ekle*.

6. Adım. Görev oluşturmayı tamamlama

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

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.

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

1. Web Console'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine 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 (12.1)** 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 cihazları seçin** 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 ve kullanılabilecek uygulama bileşenlerini seçin. Görev için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

Değişiklikleri kaydedin ve görevi çalıştırın.

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.

Görevin Gelişmiş Ayarları

Parametre	Açıklama
Uyumsuz üçüncü taraf uygulamalarını kaldır	Uyumsuz uygulamalar listesi, dağıtım kitinde bulunan `incompatible.txt` dosyasından görülebilir. Bilgisayarda uyumsuz uygulamalar yüklüyse Kaspersky Endpoint Security'nin kurulumu bir hata ile sonlanır.
Uygulama bileşenleri kümesini 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.
Azure WVD uyumluluk modunu kullan	Bu özellik, Azure sanal makinesinin durumunun Kaspersky Anti Targeted Attack Platform konsolunda doğru şekilde görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensör Kimliği) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensör Kimliği atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensör Kimliği değişebilir. Bu, konsolda sanal makinelerin kopyalarının görünmesine neden olabilir.
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 sürümünden yükseltme

Uygulamanın önceki sürümünü yeni sürüme güncellerken şunlara dikkat edin:

- Kaspersky Endpoint Security'nin yeni sürümünün yerelleştirmesi, uygulamanın yüklü sürümünün yerelleştirmesiyle aynı olmalıdır. Uygulamaların yerelleştirmeleri eşleşmediği takdirde, uygulama yükseltmesi bir hatayla sonlanabilir.
- 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.

Kaspersky Endpoint Security, uygulamanın şu sürümleri için güncellemeleri destekler:

- Kaspersky Endpoint Security 11.6.0 for Windows (yapı 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (yapı 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 for Windows (yapı 11.8.0.384).
- Kaspersky Endpoint Security 11.9.0 for Windows (yapı 11.9.0.351).
- Kaspersky Endpoint Security 11.10.0 for Windows (yapı 11.10.0.399).
- Kaspersky Endpoint Security 11.11.0 for Windows (yapı 11.11.0.452).
- Kaspersky Endpoint Security 12.0 for Windows (yapı 12.0.0.465).

Uygulama yükseltme yöntemleri

Kaspersky Endpoint Security bilgisayardan şu yollarla güncellenebilir:

- 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 dağıtımı yapılan uygulama, varsayılan setten farklı bir bileşenler seti içeriyorsa, uygulamanın Yönetim Konsolu (MMC) aracılığıyla güncellenmesi ile Web Console ve Cloud Console aracılığıyla güncellenmesi farklı olacaktır. Kaspersky Endpoint Security'yi güncelleyeceğiniz zaman şunları dikkate alın:

- Kaspersky Security Center Web Console veya Kaspersky Security Center Cloud 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 sahip olursa, o zaman örneğin BadUSB Saldırısı Önleme bilgisayardan kaldırılır, çünkü bu bileşen varsayılan sete dahil değildir. 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 bileşenlerini değiştirdikten veya uygulamayı onardıktan sonra, bilgisayarı yeniden başlatmanız gerekir.

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

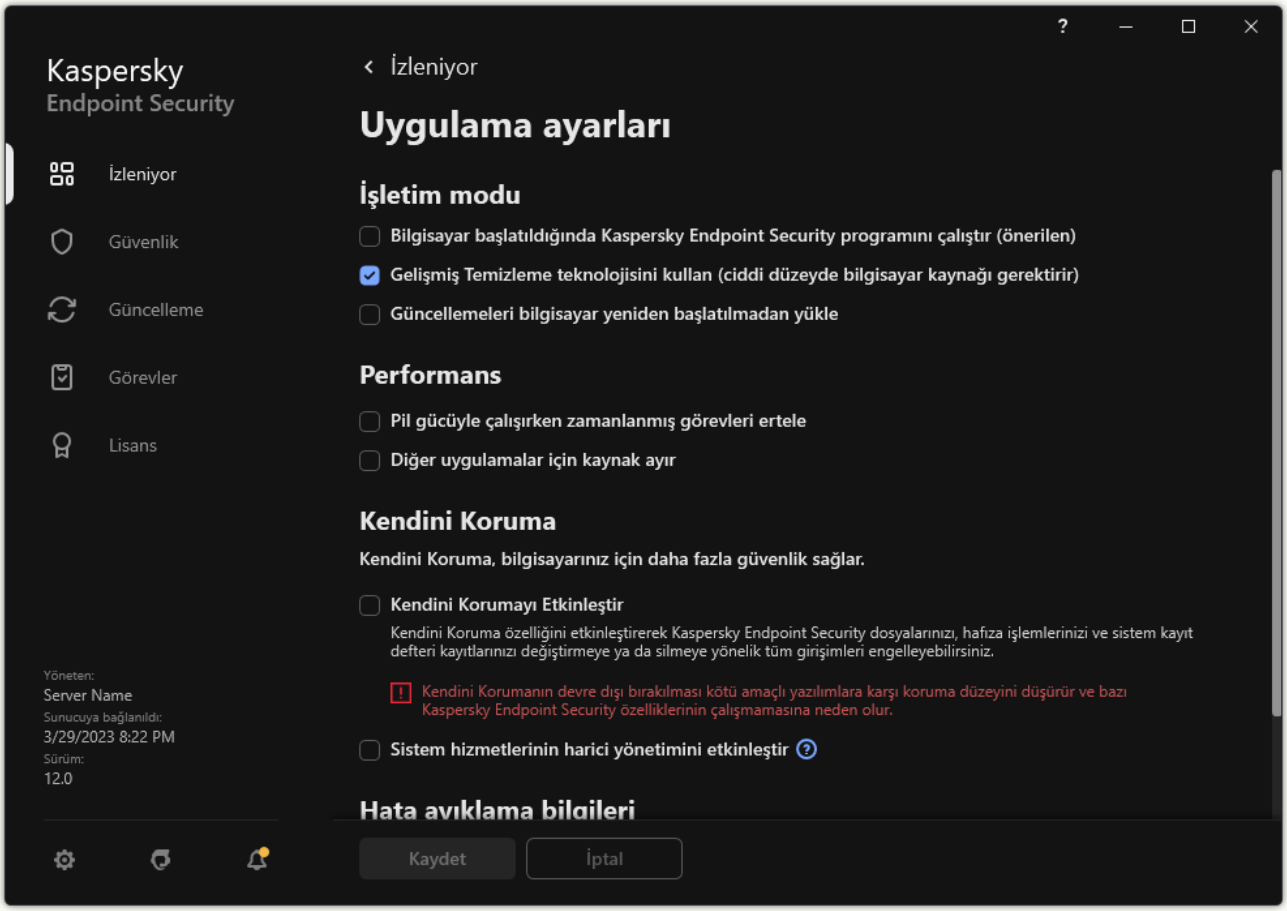
1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
5. Uygulama yükseltme modunu yapılandırmak için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

Web Console'da uygulama yükseltme modu nasıl seçilir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Uygulama Ayarları**'na gidin.
5. Uygulama yükseltme modunu yapılandırmak için **Gelişmiş ayarlar** bloğunda **Uygulama güncellemelerini yeniden başlatmadan yükle** onay kutusunu işaretleyin ya da işaretini kaldırın.
6. 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 **İşletim modu** bloğunda **Güncellemeleri bilgisayar yeniden başlatılmadan yükle** onay kutusunu işaretleyin ya da işaretini kaldırın.

4. Değişikliklerinizi kaydedin.

Sonuç olarak, uygulamayı yeniden başlatma yapmadan yükselttikten sonra, bilgisayara uygulamanın iki sürümü yüklenecektir. Yükleyici, uygulamanın yeni sürümünü Program Dosyaları ve Program Verileri klasörlerindeki ayrı alt klasörlere yükler. Yükleyici ayrıca uygulamanın yeni sürümü için ayrı bir kayıt defteri anahtarı oluşturur. Uygulamanın önceki sürümünü manuel olarak kaldırmanız gerekmez. Bilgisayar yeniden başlatıldığında önceki sürüm otomatik olarak kaldırılacaktır.

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

Uygulamayı kaldır

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

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. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.

   Görevler listesi açılır.

2. **Yeni görev** düğmesine 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 (12.1) seçimini yapın.

4. Adım. Kaldırma aracı ayarları

Şu ek uygulama ayarlarını yapılandırın:

- **Kaldırma yardımcı programını indirmeyi zorla**. Araç dağıtım yöntemini seçin:
  - **Ağ Aracısını 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 elle 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 12.1 sürümünü kaldır*.

10. Adım. Görev oluşturmayı bitirme

Sihirbazdan çıkın. 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine 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 cihazları seçin** 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** seçeneğini belirleyin.
2. **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.
3. **Kaldırma yardımcı programını indirmeyi zorla**. Araç dağıtım yöntemini seçin:
   - **Ağ Aracısını 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

Bitir 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 **Aygıtlar** → **Görevler**'i seçin.

   Görevler listesi açılır.
2. **Uygulamayı uzaktan kaldır** Kaspersky Security Center 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. Aşağıdaki içeriğe sahip bir BAT dosyası oluşturun:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<kullanıcı adı> KLPASSWD=<parola> /qn
   ```

   <GUID> uygulamanın benzersiz kimliğidir. Aşağıdaki komutu kullanarak uygulamanın GUID'ini bulabilirsiniz:

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

   Örnek:

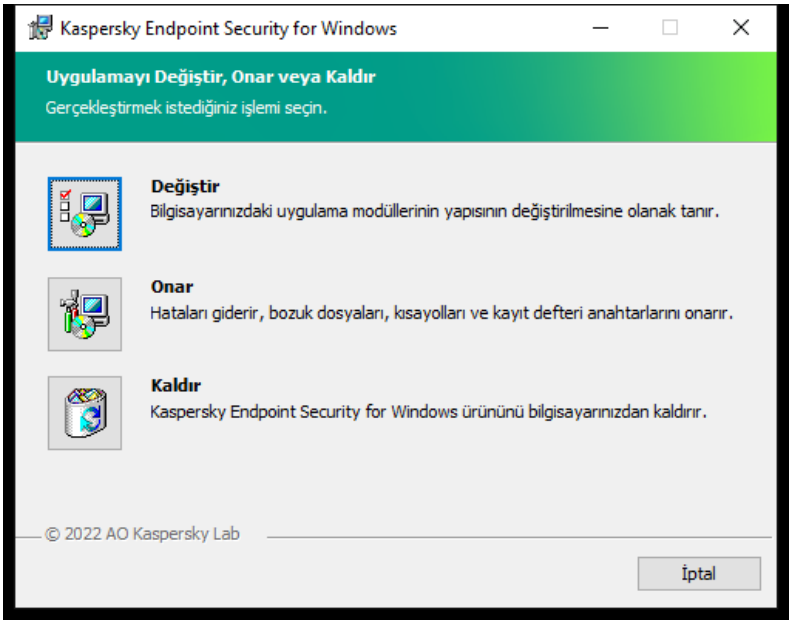
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=!Password1 /qn
   ```

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.

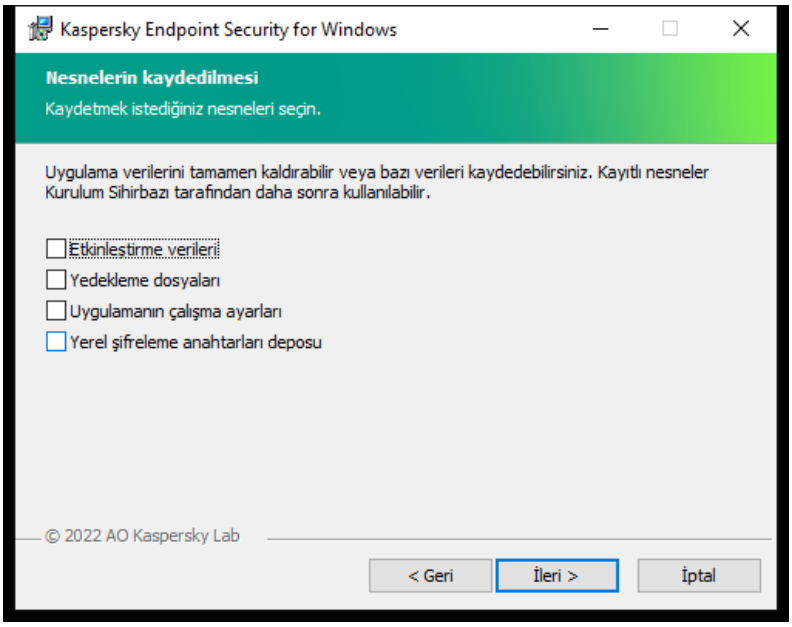
Uygulamayı yerel olarak kaldırma

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.

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.

- *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 anahtarı 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 aktif anahtar eklenir. Aktif 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.

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

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

Deneme lisansının anahtarı sadece aktif anahtar olarak eklenebilir. Rezerve anahtar olarak eklenemez. Deneme lisansı anahtarı, ticari lisansın aktif 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 aktif 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.

Uygulama bir anahtar dosyası kullanılarak etkinleştirildiğinde aktif 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 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	✓	✓	✓	✓	✓	✓	✓	✓
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 Denetleyici	–	–	–	–	–	–	–	–
Uygulama Denetimi	✓	✓	✓	✓	✓	✓	✓	✓
Aygıt Denetimi	✓	✓	✓	✓	✓	✓	✓	✓
İnternet Denetimi	✓	✓	✓	✓	✓	✓	✓	✓
Uyarlamalı Anomali Denetimi	–	✓	✓	✓	✓	✓	–	✓
Dosya Bütünlüğü İzleyici	–	–	–	–	–	–	–	–
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								
Kaspersky Sandbox *(Kaspersky Sandbox lisansı ayrıca satın alınmalıdır)*	✓	✓	✓	✓	✓	✓	✓	✓

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 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	✓	✓	✓	✓	✓	✓	✓	✓
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 Denetleyici	–	–	–	–	–	–	–	✓
Uygulama Denetimi	–	✓	✓	✓	✓	✓	–	✓
Aygıt Denetimi	–	✓	✓	✓	✓	✓	✓	✓
İnternet Denetimi	–	✓	✓	✓	✓	✓	✓	✓
Uyarlamalı Anomali Denetimi	–	–	–	–	–	–	–	–
Dosya Bütünlüğü İzleyici	–	–	–	–	–	–	–	✓
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	–	–	–	–	–	✓	–	–
Kaspersky Sandbox	✓	✓	✓	✓	✓	✓	✓	✓

(Kaspersky Sandbox lisansı ayrıca satın alınmalıdır)

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:

- Yerel olarak uygulama arabiriminden Etkinleştirme Sihirbazı'nı kullanarak. Hem aktif anahtarı hem de rezerve anahtarı bu şekilde ekleyebilirsiniz.
- Uzaktan Kaspersky Security Center yazılım paketiyle bir lisans anahtarı ekleme görevi oluşturarak ve ardından başlatarak. Hem aktif anahtarı hem de rezerve anahtarı bu şekilde ekleyebilirsiniz.
- Kaspersky Security Center Yönetim Sunucusu anahtar deposunda depolanan anahtar dosyalarını ve etkinleştirme kodlarını istemci bilgisayarlara dağıtarak uzaktan. Anahtar dağıtımı hakkında daha fazla ayrıntı için lütfen Kaspersky Security Center Yardımı 'na başvurun. Hem aktif anahtarı hem de rezerve anahtarı bu şekilde ekleyebilirsiniz.

  > Abonelikle satın alınan etkinleştirme kodu ilk seferde dağıtılır.

- Komut satırını kullanarak.

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

Uygulamayı Kaspersky Security Center üzerinden etkinleştirmek için

Uygulamayı, Kaspersky Security Center üzerinden şu yöntemleri kullanarak uzaktan etkinleştirebilirsiniz:

- *Anahtar ekle* görevini kullanarak.

  Bu yöntem belirli bir bilgisayara veya yönetim grubunun parçası olan bilgisayarlara bir anahtar eklemenize olanak tanır.

- 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.

- 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.

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.

Lisansların kullanımını aşağıdaki adımları uygulayarak izleyebilirsiniz:

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

Uygulama Yönetim Konsolu (MMC) ile nasıl uzaktan kaldırılır

1. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.
   Görevler listesi açılır.
2. **Yeni görev** düğmesine tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (12.1) → **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 elle 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

Sihirbazdan çıkın. 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine 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 (12.1)** 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 cihazları seçin** 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 elle 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

Bitir 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.

Anahtar ekle görevinin özelliklerinde bilgisayara bir rezerve anahtar ekleyebilirsiniz. Aktif anahtarın süresi dolduğunda veya anahtar silindiğinde *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 **Yönetim Sunucusu** → **Kaspersky Lisansları** klasörüne gidin.
   Bir lisans anahtarları listesi açılır.
2. Lisans anahtarı özelliklerini açın.
3. **Genel** bölümünden **Otomatik olarak dağıtılan lisans anahtarı** 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

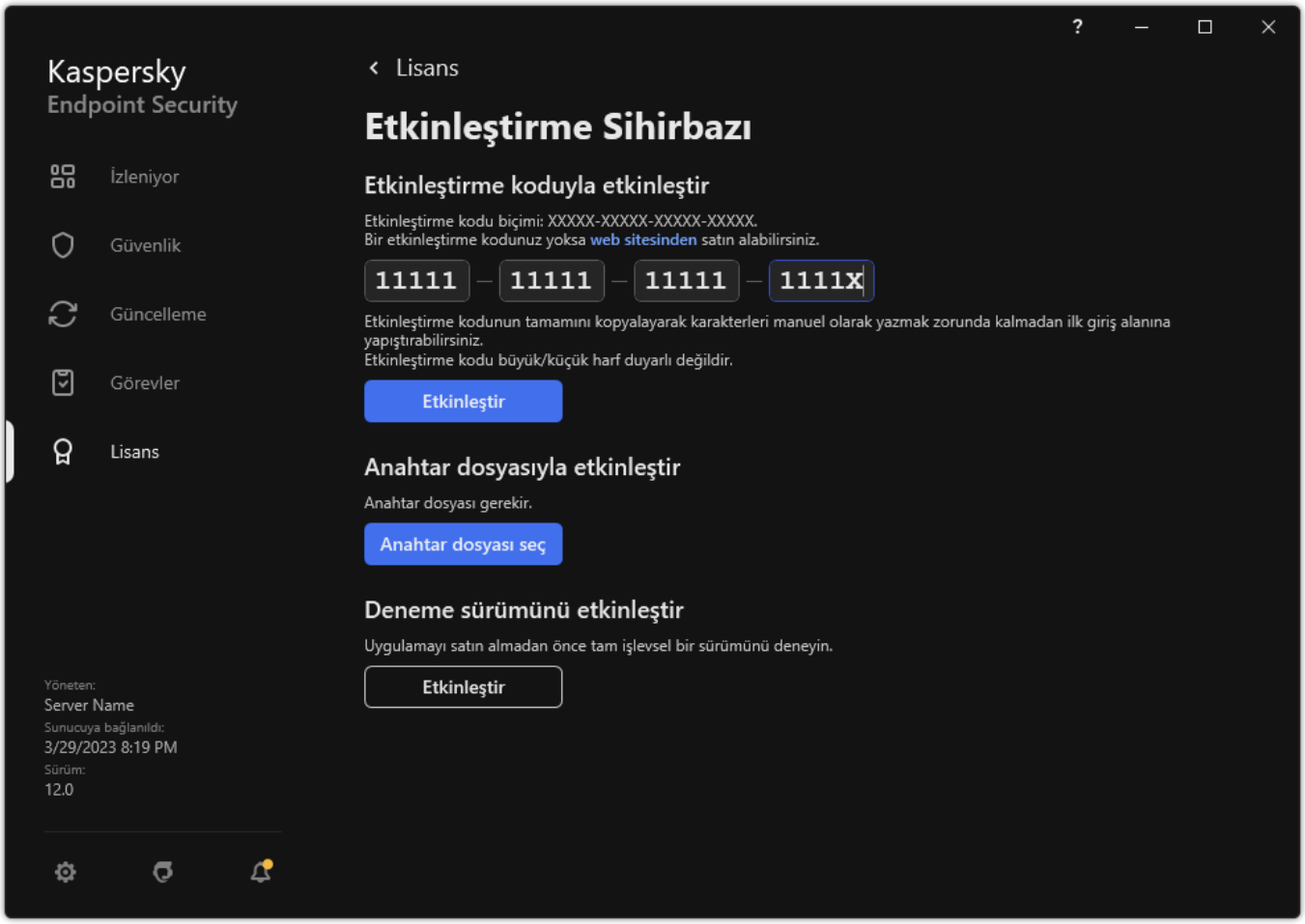
1. Web Console ana penceresinden **İşlemler** → **Lisanslama** → **Kaspersky Lisansları** seçimini yapın.
   Bir lisans anahtarları listesi açılır.
2. Lisans anahtarı özelliklerini açın.
3. **Genel** sekmesinden **Lisans anahtarını otomatik olarak dağıt** iki durumlu düğmesini açık duruma getirin.
4. 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 etkinleştirmek için Etkinleştirme Sihirbazını kullanma

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

1. Ana uygulama penceresinde **Lisans** bölümüne gidin.
2. **Uygulamayı yeni bir lisans kullanarak etkinleştirin**'e tıklayın.
   Uygulama Etkinleştirme Sihirbazı başlatılır. Etkinleştirme Sihirbazı talimatlarını uygulayın.

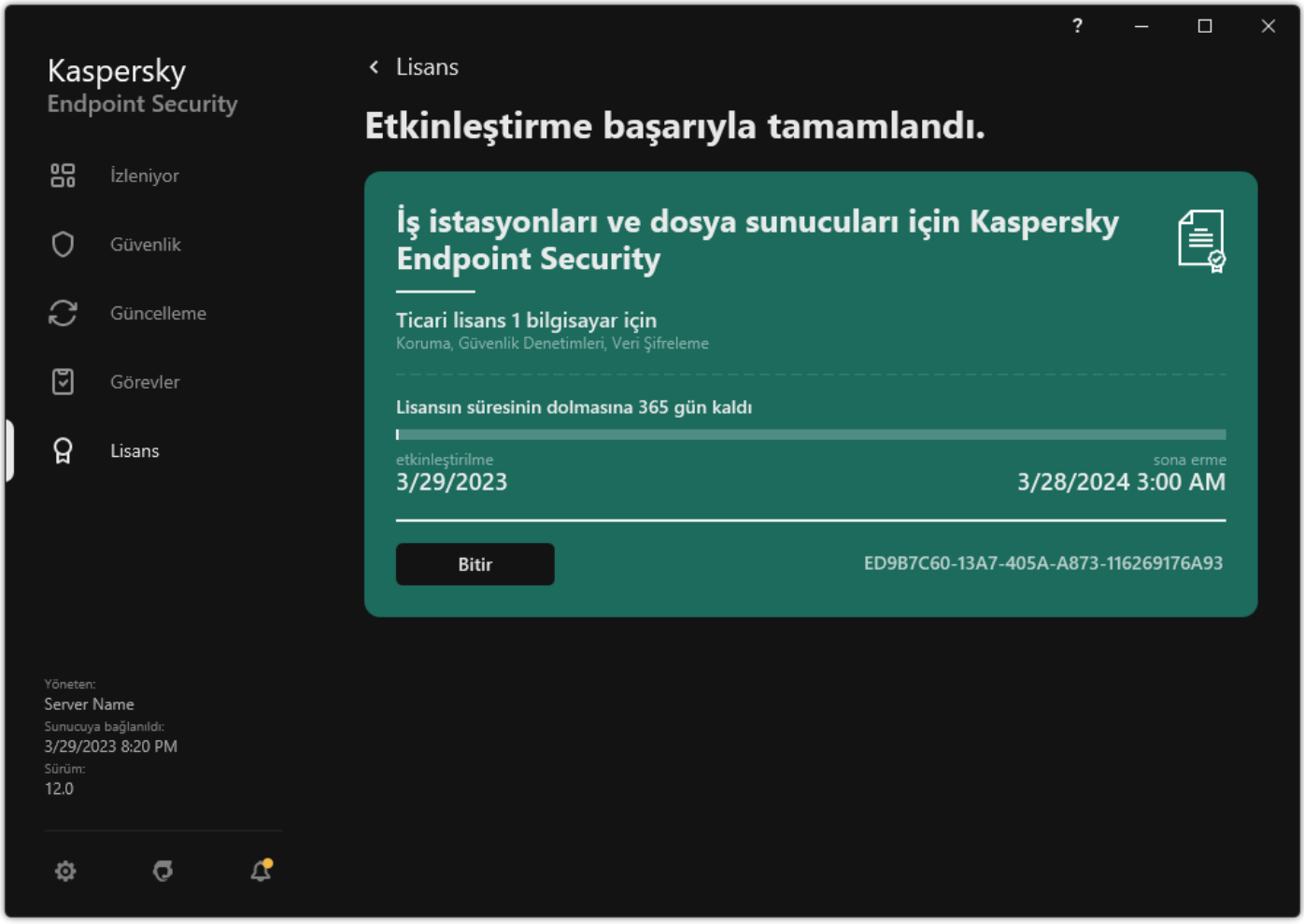


Uygulamayı etkinleştirme

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 aktif anahtarı olamaz. Rezerve anahtar sadece aktif 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 aktif 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.

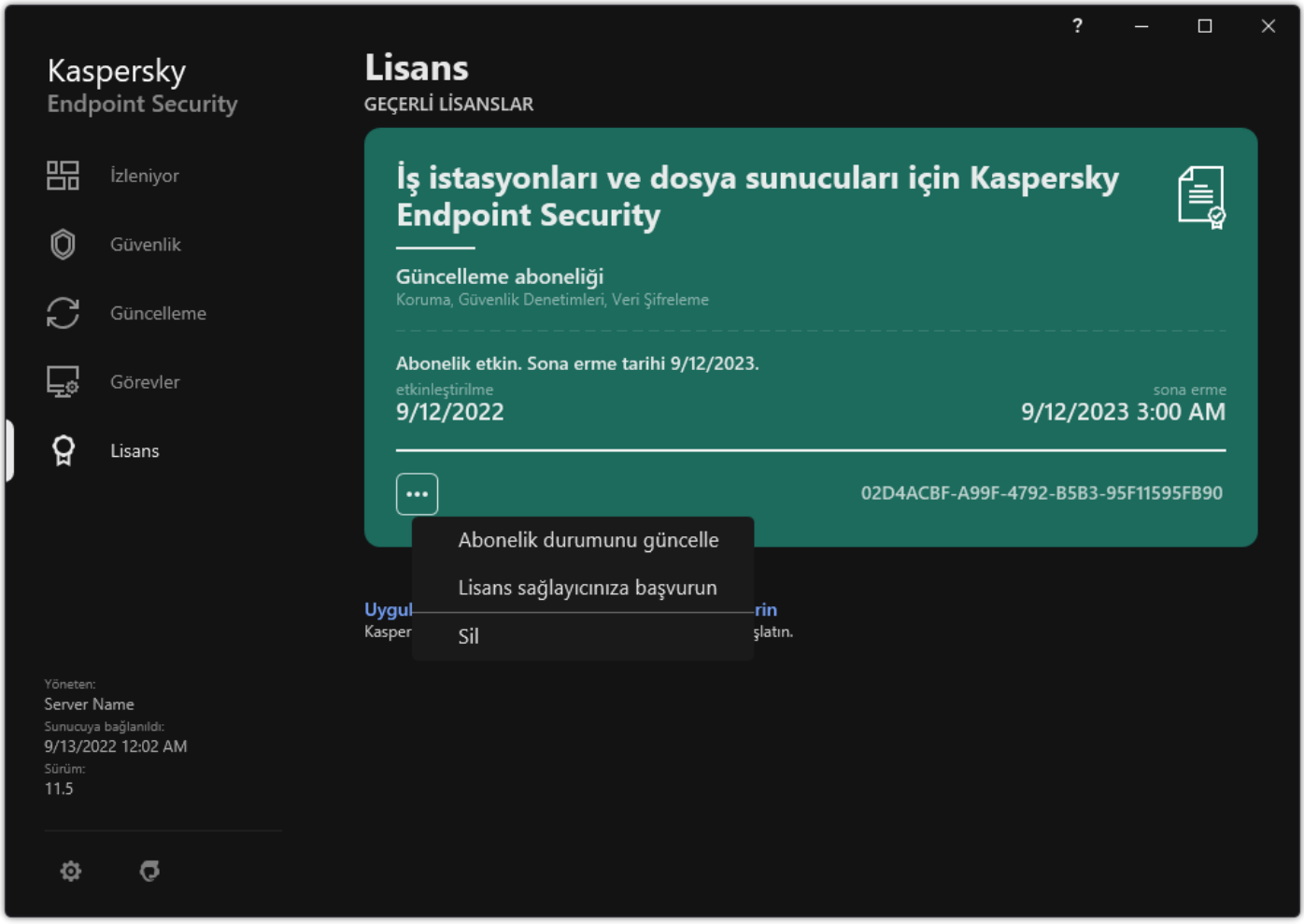
Uygulamayı sınırlı bir abonelikle kullanıyorsanız aboneliğin sona erme tarihinde (veya abonelik yenileme ödemesiz süresinin sona erme tarihinde) Kaspersky Endpoint Security sizi bu konuda bilgilendirir ve aboneliği otomatik olarak yenilemeye çalışmayı bırakır. Bu durumda Kaspersky Endpoint Security, 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

Veri sağlama

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 aktif anahtar tanımlayıcısı;
- İşletim sisteminin türü, sürümü ve bit hızı ile sanal ortamın adı (Kaspersky Endpoint Security sanal ortamda yüklüyse);
- Bilgiler iletildiğinde etkin olan Kaspersky Endpoint Security bileşenlerinin kimlikleri.

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

Etkinleştirme kodu kullanarak yukarıda listelenen verileri otomatik olarak iletmeyi kabul edersiniz. Bu 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;
- Aktif anahtar;
- Yükseltme görevinin başlatılmasının benzersiz kimliği;
- Kaspersky Endpoint Security yüklemesinin benzersiz kimliği.

- Kaspersky Endpoint Security arabiriminden bağlantıları takip ederken:
  - Kaspersky Endpoint Security sürümü;
  - İşletim sistemi sürümü;
  - Kaspersky Endpoint Security'nin etkinleştirilme tarihi;
  - lisans 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;
  - Aktif 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 Statement'ı onayladıktan sonra uygulama kullanımıyla ilgili bilgileri nasıl aldığımız, işlediğimiz, depoladığımız ve imha ettiğimizle ilgili daha fazla bilgi için Son Kullanıcı Lisans Sözleşmesi'ni okuyun ve Kaspersky İnternet sitesini ziyaret edin. License.txt ve ksn_<dil kodu>.txt dosyaları Son Kullanıcı Lisans Sözleşmesi ile Kaspersky Security Network Statement 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 Statement'ı 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 Statement'ı 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);

- tüm potansiyel olarak zararlı nesneler ve etkinlikler hakkında bilgiler: tespit edilen nesnenin adı ve nesnenin bilgisayardaki tam yolu, işlenen dosyaların sağlamaları (MD5, SHA2-256, SHA1), tespit etme tarihi ve saati, virüslü dosyaların adları ve boyutları ile bu dosyaların yolları, yol şablon kodu, yürütülebilirler dosya bayrağı, nesnenin konteyner olup olmadığına dair gösterge, paket oluşturucunun adı (dosya sıkıştırıldıysa), dosya türü kodu, dosya biçimi kimliği, zararlı yazılımlar tarafından gerçekleştirilen işlemlerin listesi ile yazılım ve bunlara yanıt veren kullanıcı tarafından alınan karar, antivirüs veritabanlarının ve karar vermek için kullanılan bu antivirüs veritabanlarındaki kayıtların kimlikleri, potansiyel olarak zararlı nesnenin göstergesi, Hak Sahibinin sınıflandırmasına göre tespit edilen tehdidin adı, tehlike düzeyi, tespit etme durumu ve tespit yöntemi, analiz edilen içeriğe dahil edilme nedeni ve dosyanın içerikteki sıra numarası, sağlamalar (MD5, SHA2-256, SHA1), virüslü mesajın veya bağlantının aktarıldığı uygulamanın yürütülebilir dosyasının adı ve öznitelikleri, engellenen nesnenin ana bilgisayarının kişisel olmayan IP adresleri (IPv4 ve IPv6), dosya entropisi, dosya otomatik çalıştırma göstergesi, dosyanın sistemde ilk tespit edildiği zaman, son istatistikler gönderildikten sonra dosyanın çalıştırılma sayısı, zararlı nesnenin alındığı posta istemcisinin adı, sağlamaları (MD5, SHA2-256, SHA1) ve boyutu hakkında bilgiler, taramayı gerçekleştiren yazılım görevinin kimliği, dosya tanınırlığının veya imzanın kontrol edilip edilmediğine ilişkin gösterge, dosya işleme sonucu, nesne için toplanan şablonun sağlaması (MD5), bayt cinsinden şablon boyutu ve uygulanan tespit etme 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: bağlantı noktasını 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 noktalarının numaraları, bağlantı durumu ve bağlantı noktası 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 bağlantı noktası
- Yerel bağdaştırıcı IP adresi
- Yerel bağdaştırıcıda açık bağlantı noktası
- 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 isteğini yapan 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 bağlantı noktası
- İşlenen web isteğinin uzak IP bağlantı noktası
- 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 bağlantı noktası
- Yerel bağdaştırıcı IP adresi
- Yerel bağdaştırıcıda açık bağlantı noktası
- 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 isteğini yapan işlemin benzersiz tanımlayıcısı

Kaspersky Anti Targeted Attack Platform (EDR)

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:

- Kaspersky Endpoint Security'nin yerleşik aracısının yapılandırılması sırasında kullanıcı tarafından girilen işlenmiş dosyalar ve veriler:
  - Karantinaya alınan dosyalar
  - Kaspersky Endpoint Security'nin yerleşik aracısının ayarları:
    - Merkezi Düğüm ile entegrasyon için kullanılan sertifikanın genel anahtarı
    - Lisans verileri

- Merkezi Düğüm ile entegrasyon için gerekli veriler:
  - Telemetri olay paketi kuyruğu
  - Merkezi Düğümden alınan IOC dosya tanımlayıcılarının önbelleği
  - *Dosya al* görevi içinde sunucuya iletilecek nesneler
  - *Adli bilgi al* görev sonuçları raporu

KATA'ya yapılan taleplerdeki veriler (EDR)

Kaspersky Anti Targeted Attack Platform ile entegre edilirken, şu veriler bilgisayarda yerel olarak depolanır:

Kaspersky Endpoint Security'nin yerleşik aracısından gelen veriler Merkezi Düğüm bileşenine talepte bulunur:

- 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
  - Merkezi Düğüm 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
- Telemetri paketleri
- 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

- Telemetri verileri:

- Ana bilgisayar IP adresi
- Gerçekleştirilen güncelleme işleminden önce kayıt defterindeki veri türü
- Gerçekleştirilen değişiklik işleminden önce kayıt defteri anahtarındaki veriler
- İşlenen komut dizisinin metni veya bir kısmı
- İşlenen nesnenin türü
- Komut yorumlayıcısına bir komut aktarma yolu

Merkezi Düğüm bileşeninin isteklerinden Kaspersky Endpoint Security'nin yerleşik aracısına gelen veriler:

- 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, bağlantı noktaları, 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

- 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, bağlantı noktaları, iletişim kuralları, tam yürütülebilir dosya yolları
  - Kullanıcı adları
  - Kullanıcı giriş türleri
  - Filtrelerin uygulandığı telemetri olaylarının türleri

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.

YARA taraması sonuçları şu verileri içerir:

- 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

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.
- Döküm yazımı.

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 Anlaşması ve Kaspersky Security Network Statement'ta 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 Statement'ı onayladıktan sonra uygulama kullanımıyla ilgili bilgileri nasıl aldığımız, işlediğimiz, depoladığımız ve imha ettiğimizle ilgili daha fazla bilgi için Son Kullanıcı Lisans Sözleşmesi'ni okuyun ve Kaspersky İnternet sitesini ziyaret edin. License.txt ve ksn_<dil kodu>.txt dosyaları Son Kullanıcı Lisans Sözleşmesi ile Kaspersky Security Network Statement 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 Statement'ta 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.

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 ifade edilecektir), bir kuruluşun ağının güvenlik sistemini yönetmek ve sistemin bakımını yapmak için ana görevlerin merkezi bir şekilde gerçekleştirilebilmesi amacıyla geliştirilmiş bir web uygulamasıdır. Web Console, kullanıcı arabirimi sağlayan bir Kaspersky Security Center bileşenidir. 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; bir yönetici iş istasyonuna yüklenen Kaspersky Security Center Yönetim Console'un yönelik Yönetim Eklentisinin aksine Kaspersky Security Center Web Console'un yüklü 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**. Web eklentileri sürümleri ile Web Console uyumluluğu hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine bakın.

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.

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 kuralları kullanırken özel hususlar

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, 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.

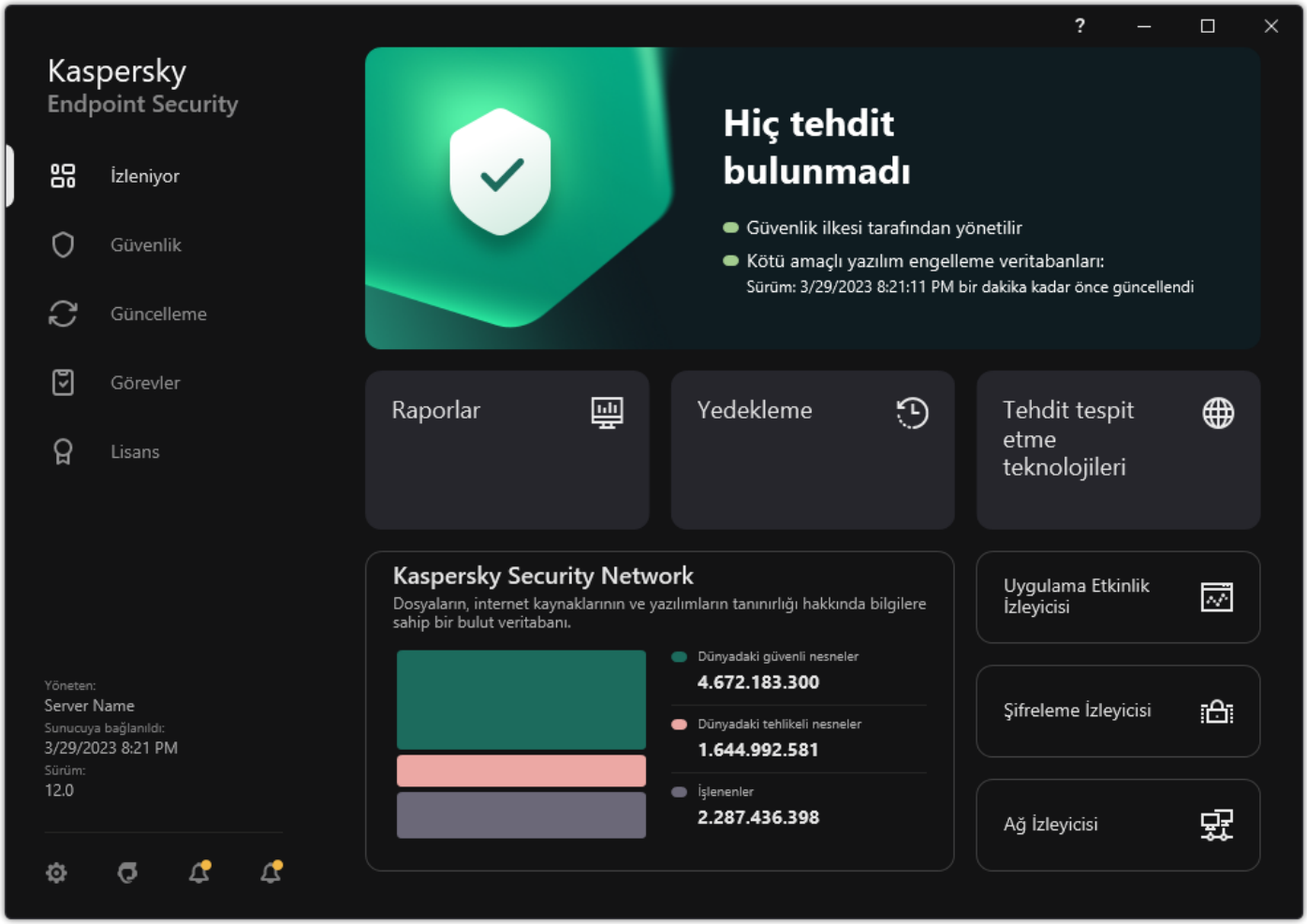
TLS kullanımı, aşağıdaki özelliklerin sunulmasıyla uygulamayı güvence altına alır:

- 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 bir ortak anahtar altyapısı (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 protokolünün ayrıştırılmasını destekleyen yazılım ve donanım araçları) sahip ortamlar, Kaspersky Endpoint Security tarafından güvensiz kabul edilir. Kaspersky hizmetleriyle çalışırken hatalarla karşılaşılabilir. Örneğin, kendinden imzalı sertifikaların kullanımıyla 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 dosyaların kategorisi ve tanınırlığı hakkındaki bilgilerle birlikte taranan web adreslerinin tanınırlığı hakkında bilgi sağlar.
- **Uygulama Etkinlik İzleyicisi**. Yüklü uygulamaların çalışmasıyla ilgili bilgileri görüntüleyin. Sistem İzleyici 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 denetimi 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.

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.

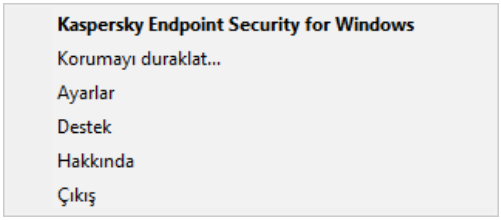
  Koruma ve denetim bileşenlerinin çalışması duraklatılmadan önce, uygulama Kaspersky Endpoint Security erişimi için parola ister (hesap parolası veya geçici parola). Süreyi duraklatmayı seçebilirsiniz: belirli bir süre için, bir yeniden başlatmaya kadar ya da kullanıcı isteği üzerine.

  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 bırakır. 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.

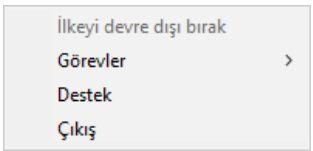


Uygulama simgesi bağlam menüsü

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 bırakır. 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:
  - **Bütünlük denetimi**.
  - **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 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 ayrıca uygulama simgesinin üzerinde bildirimler görüntüler.
- **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.

- **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'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** → **Arabirim** öğesini seçin.
5. **Kullanıcıyla etkileşim** bloğunda aşağıdakilerden birini yapın:
   - Aşağıdaki arabirim öğelerinin istemci bilgisayarda görüntülenmesini isterseniz **Kullanıcı arabirimini göster** onay kutusunu işaretleyin:
     - **Başlangıç** menüsünde uygulama adını içeren klasör
     - Microsoft Windows görev çubuğu bildirim alanındaki Kaspersky Endpoint Security simgesi
     - Açılır pencere bildirimleri

     Bu onay kutusu işaretlenirse kullanıcı, uygulama ayarlarını görüntüleyebilir ve kullanılabilir haklara bağlı olarak uygulama arabiriminden değiştirebilir.
   - İstemci bilgisayarda Kaspersky Endpoint Security'nin tüm işaretlerini gizlemek isterseniz **Kullanıcı arabirimini göster** onay kutusunun işaretini kaldırın.
6. Basitleştirilmiş uygulama arabirimi öğesinin Kaspersky Endpoint Security yüklü bir istemci bilgisayarda görüntülenmesini isterseniz **Kullanıcıyla etkileşim** bloğunda **Basitleştirilmiş arabirimi görüntüle** onay kutusunu işaretleyin.

Web Console'da ve Cloud Console'da uygulama arabirimi görüntüleme modu nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Arabirim** bölümüne gidin.
5. **Kullanıcıyla etkileşim** bloğunda uygulama arabiriminin nasıl görüntüleneceğini seçin:
   - **Basitleştirilmiş arabirim ile**. 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 ayrıca uygulama simgesinin üzerinde bildirimler görüntüler.
   - **Tam arabirim ile**. 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.
   - **Arabirim yok**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin çalıştığına dair hiçbir işaret görüntülenmez. Windows bildirim alanındaki simge ve bildirimler yoktur.

6. Değişikliklerinizi kaydedin.

Başlarken

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.

- *Güncelleme* ve *Kötü Amaçlı Yazılım Taraması* görevlerini oluşturun.

  Güncelleme görevi, bilgisayarın güvenliğini güncel tutmak için gereklidir. Görev gerçekleştirildiğinde Kaspersky Endpoint Security antivirüs veritabanları ve uygulama modüllerini günceller. *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.

  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. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.

   Görevler listesi açılır.

2. **Yeni görev** düğmesine tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (12.1) → **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 uygulanacak eylemi seçin:

- **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.
- **Temizle; temizleme başarısız olursa bildir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme mümkün değilse Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
- **Bildir**. 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'ı kullanarak görev çalışma modunu yapılandırın. Bu onay kutusu, bilgisayar kaynakları sınırlı olduğunda *Kötü Amaçlı Yazılım Taraması* görevini askıya alan işlevi etkinleştirir/devre dışı bırakır. Kaspersky Endpoint Security, ekran koruyucu kapalı olduğunda ve bilgisayar kilidi kaldırıldığında *Kötü Amaçlı Yazılım Taraması* görevini duraklatır.

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 elle 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

Sihirbazdan çıkın. 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. **Ekle** düğmesine tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** 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 cihazları seçin** bloğunda görev kapsamını seçin.

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.
5. Sihirbazdan çıkın.
   Görevler listesinde yeni bir görev görüntülenir.
6. Görev zamanlamasını yapılandırmak için görev özelliklerine gidin.
   Görevin, haftada en az bir kez çalıştırılmak üzere zamanlanması tavsiye edilir.
7. Görevin yanındaki onay kutusunu seçin.
8. **Çalıştır** düğmesine 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.

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.

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 bağlantı noktası 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.

Etkin ve etkin olmayan ilke

İlke, yönetilen bilgisayarların bir grubuna yöneliktir ve etkin veya etkin olmayan durumdadır. 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.

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.

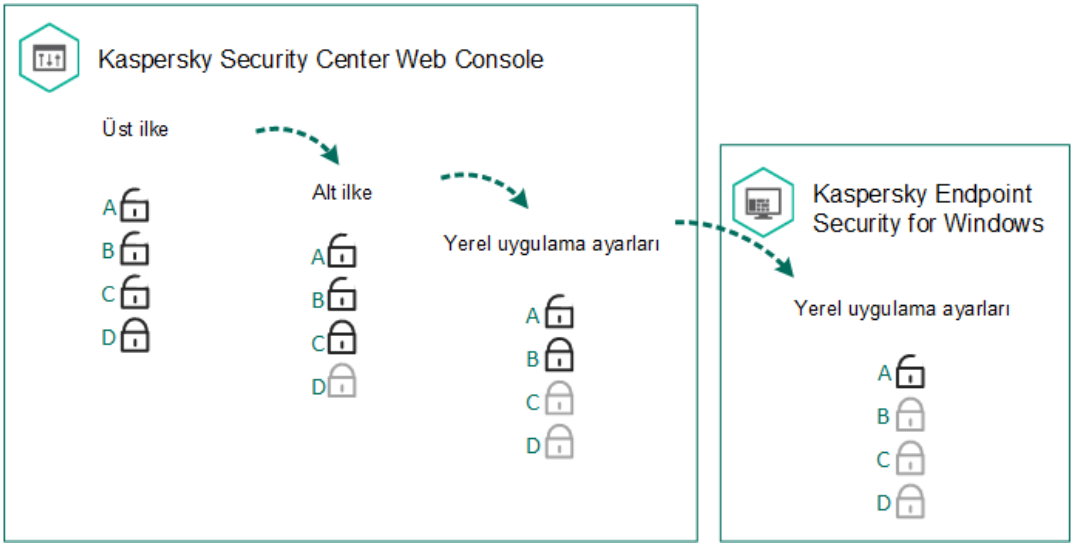
İşyeri dışında ilkesi

İşyeri dışında ilkesi, bir bilgisayar kuruluş ağından ayrıldığında etkinleştirilir.

Ayarların devralınması

Yönetim grupları gibi ilkeler bir hiyerarşi içinde düzenlenir. Varsayılan olarak, bir alt ilke ana ilkenin ayarlarını devralır. *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. Ayar devralmayı ana ilkeden devre dışı bırakabilirsiniz.

Her ilke ayarının, ayaların alt ilkelerde mi yoksa yerel uygulama ayarlarında mı değiştirilebileceğini gösteren bir özniteliği vardır. özelliği yalnızca alt ilkeye yönelik üst ilke ayarlarının devralınması etkinleştirilirse geçerlidir. 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.

İlke oluşturma

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** düğmesine tıklayın.
   İlke Sihirbazı başlatılır.
5. İlke Sihirbazı talimatlarını uygulayın.

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

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. **Ekle** düğmesine tıklayın.
   İlke Sihirbazı başlatılır.
3. Kaspersky Endpoint Security'yi seçin ve **İleri**'ye tıklayın.
4. Kaspersky Security Network (KSN) Beyanının hükümlerini okuyup kabul edin ve **İleri**'ye tıklayın.
5. **Genel** sekmesinde, aşağıdaki eylemleri gerçekleştirebilirsiniz:
   - İlke adını değiştirme.
   - İlke durumunu seçme:
     - **Etkin**. İlke bir sonraki senkronizasyondan sonra bilgisayarda etkin ilke olarak kullanılır.

- **Etkin değil**. Yedek ilke. Gerekli olduğunda etkin olmayan bir ilke etkin duruma geçebilir.
- **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 kilitli 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, kilitsiz ile işaretlenmiş ayarlar haricinde üst ilkeden devralınır. Üst ilke için kilitli ayarlandıysa alt ilke ayarları düzenlenemez.

6. **Uygulama ayarları** sekmesinde Kaspersky Endpoint Security ilke ayarlarını yapılandırabilirsiniz.
7. Değişikliklerinizi kaydedin.

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.

Güvenlik düzeyi göstergesi

Güvenlik düzeyi göstergesi Özellikler**: <İlke Adı>** 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.
  - **Önemli**. Bu kategori aşağıdaki bileşenleri içerir:
    - Kaspersky Security Network.
    - Web Tehdidi Koruması.
    - Posta Tehdidi Koruması.
    - Sunucu Yetkisiz Erişim Önleme.
- **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 **Gelişmiş ayarlar** penceresini açan bir bağlantı görüntülenir. Bu pencerede, önerilen koruma bileşenlerinden herhangi birini etkinleştirebilirsiniz.

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.
- **Güncelleme**. Kaspersky Endpoint Security, veritabanlarını ve uygulama modüllerini günceller. *Güncelleme* 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.
- **Bütünlük denetimi**. 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.

Görevler bir bilgisayarda yalnızca Kaspersky Endpoint Security çalışıyorsa gerçekleştirilir.

Yeni bir görev ekle

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** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.

4. Görev Sihirbazı talimatlarını uygulayın.

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

1. Web Console'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.
   b. **Görev türü** açılır listesinde, kullanıcıların bilgisayarlarında çalıştırmak istediğiniz görevi seçin.
   c. **Görev adı** alanına kısa bir açıklama girin.
   d. **Görevin atanacağı cihazları seçin** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. Bir sonraki adıma geçin.
5. Sihirbazdan çıkın.

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 ve raporlama** → **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 erişim denetimi

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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Yerel Görevler** → **Görev yönetimi** seçimini yapın.
5. Görev yönetimi modunu yapılandırın (aşağıdaki tabloya bakın).
6. Değişikliklerinizi kaydedin.

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

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerel Görevler** → **Görev yönetimi** bölümüne gidin.
5. Görev yönetimi modunu yapılandırın (aşağıdaki tabloya bakın).
6. Değişikliklerinizi kaydedin.

Görev yönetimi ayarları

Parametre	Açıklama
Yerel görevlerin kullanılmasına izin ver	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. Onay kutusu işaretlenmezse yerel görevlerin kullanımı durdurulur. 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 görevlerinin gösterilmesine izin ver	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 görevlerinin yönetimine izin ver	Onay kutusu işaretlenirse, kullanıcılar Kaspersky Security Center'da 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'da 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 bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Cihazlar** sekmesini seçin.
4. Kaspersky Endpoint Security ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
5. İstemci bilgisayarın bağlam menüsünden **Özellikler**'i seçin.
   İstemci bilgisayar özellikleri penceresi açılır.

6. İstemci bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.

   İstemci bilgisayarda yüklü Kaspersky uygulamalarının listesi, istemci bilgisayar özellikleri penceresinin sağında görülür.

7. Kaspersky Endpoint Security'yi seçin.

8. Kaspersky uygulamalarının listesinden **Özellikler** düğmesine tıklayın.

   Bu, **Kaspersky Endpoint Security for Windows uygulama ayarları** penceresini açar.

9. **Genel Ayarlar** bölümünde, Kaspersky Endpoint Security ile birlikte Raporlar ve Depolama Alanını da yapılandırın.

   Kaspersky Endpoint Security for Windows uygulama ayarları penceresinin diğer bölümleri, 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.

10. Değişikliklerinizi kaydedin.

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

1. Web Console'un ana penceresinde **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.

2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.

   Bu, bilgisayar özelliklerini açar.

3. **Uygulamalar** sekmesini seçin.

4. **Kaspersky Endpoint Security for Windows**'a 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'nu açın.

2. Konsol ağacında **İlkeler**'i seçin.

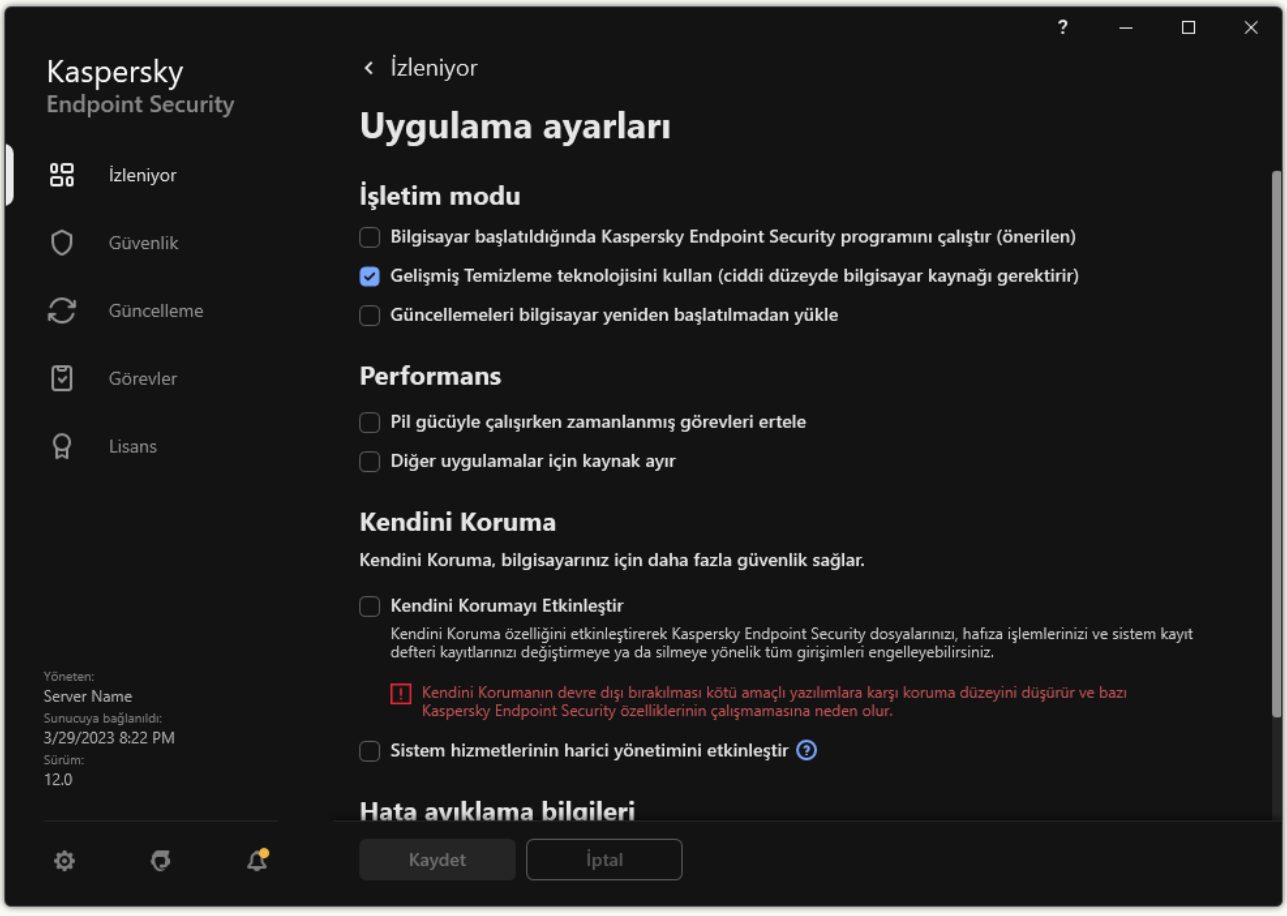
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Uygulama ayarları** öğesini seçin.
5. Uygulama başlatmasını yapılandırmak için **Bilgisayar başlatılırken Kaspersky Endpoint Security'yi başlat (önerilir)** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

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

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Uygulama Ayarları**'na gidin.
5. Uygulama başlatmasını yapılandırmak için **Bilgisayar başlatılırken Kaspersky Endpoint Security'yi başlat (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.



3. Uygulama başlatmasını yapılandırmak için **Bilgisayar başlatılırken Kaspersky Endpoint Security'yi başlat (önerilir)** onay kutusunu kullanın.
4. Değişikliklerinizi kaydedin.

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

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 bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Cihazlar** sekmesini seçin.
4. Uygulamayı başlatmak veya durdurmak istediğiniz bilgisayarı seçin.
5. İstemci bilgisayarın bağlam menüsünü görüntülemek için sağ tıklayın ve **Özellikler**'i seçin.
6. İstemci bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.
   İstemci bilgisayarda yüklü Kaspersky uygulamalarının listesi, istemci bilgisayar özellikleri penceresinin sağında görülür.
7. Kaspersky Endpoint Security'yi seçin.
8. Aşağıdakileri uygulayın:
   - Uygulamayı başlatmak için Kaspersky uygulamalarının listesinin sağındaki  düğmesine tıklayın.
   - 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
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. Kaspersky Endpoint Security yürütülebilir dosyasının 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).

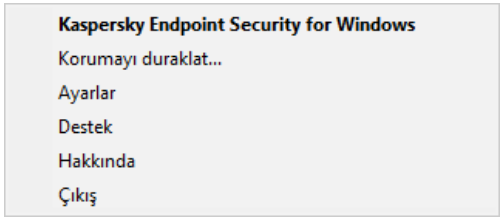
   Bu bağlam menüsü sadece Parolası Koruması etkinleştirilmişse kullanılabilir.

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.
  Bunu yapabilmek için yapılandırma dosyasını, dağıtım paketinin bulunduğu aynı klasöre kaydetmelisiniz.
- Önceden tanımlanmış ayarlarla Kaspersky Security Center aracılığıyla Kaspersky Endpoint Security'nin uzaktan kurulumunu yapabilirsiniz.
- Kaspersky Endpoint Security ayarlarını bir bilgisayardan diğerine taşıyabilirsiniz (aşağıdaki talimatlara bakın).

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. Açılan pencerede yapılandırma dosyasını kaydetmek istediğiniz yolu belirtin ve adını girin.

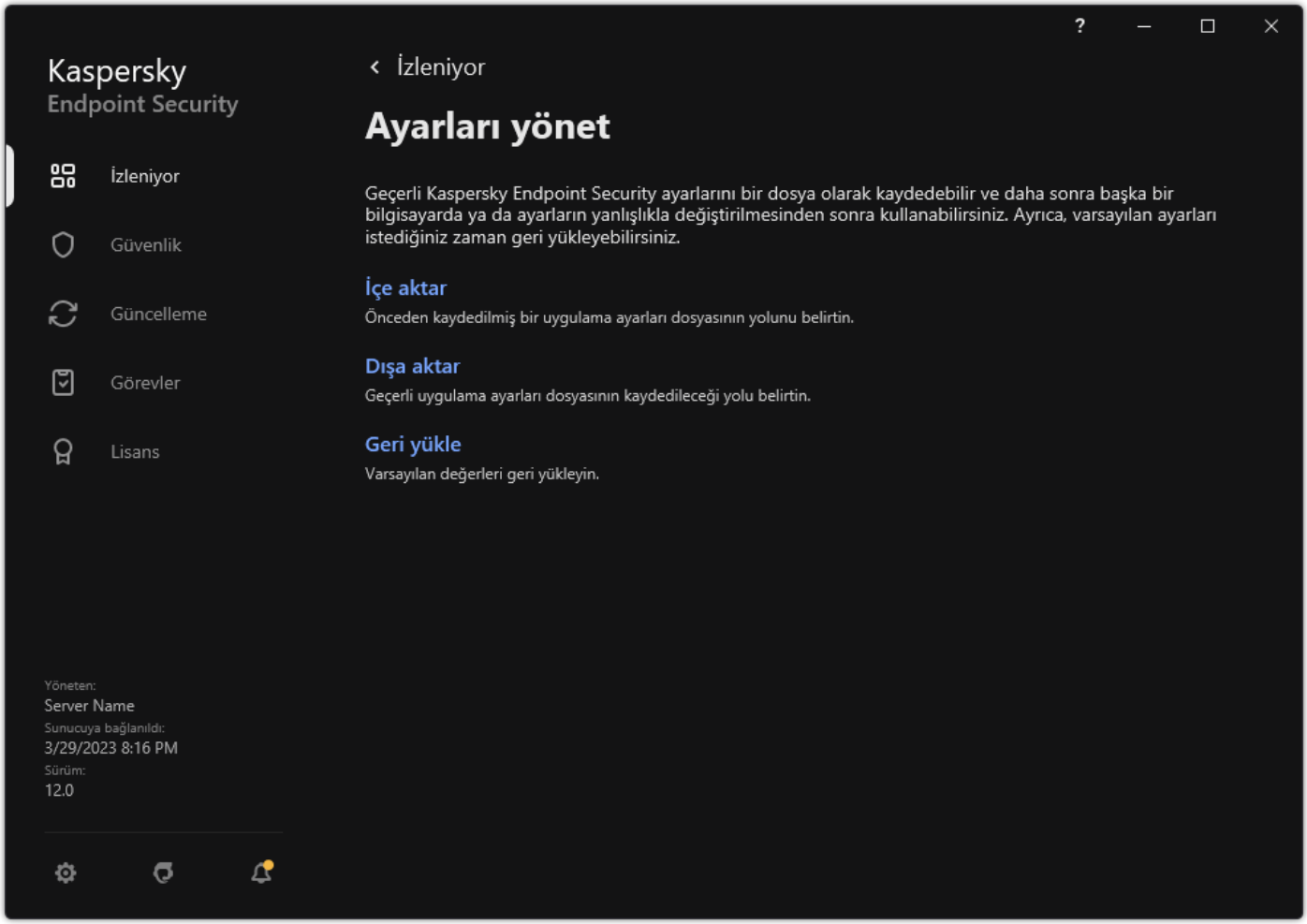
   Yapılandırma dosyasını Kaspersky Endpoint Security'nin yerel veya uzaktan kurulumunda kullanmak için install.cfg olarak adlandırmalısınız.

5. Dosyaya kaydet.

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. Dosyayı aç.

Kaspersky Endpoint Security ayarlarının bütün değerleri, seçilen yapılandırma dosyasına göre ayarlanacaktır.



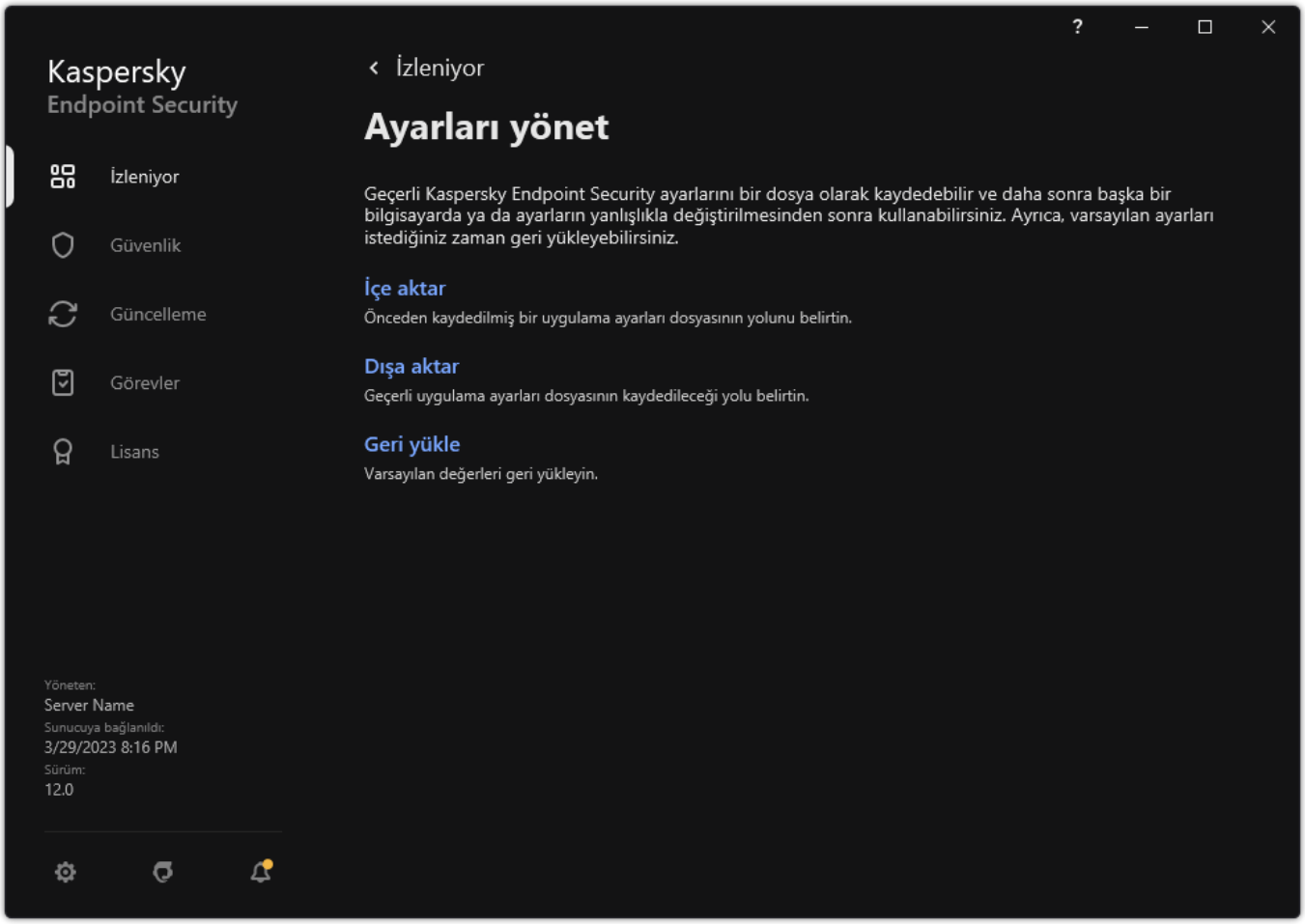
Uygulama ayarlarını yönetme

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

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
- Microsoft Outlook posta kutusu
- 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 türlerinden (örneğin tam tarama) daha az bilgisayar kaynağı gerektirir. Bu modda, Kaspersky Endpoint Security başlangıç nesnelerini, önyükleme kesimini, sistem belleğini ve sistem bölümünü tarar.

Bütünlük denetimi

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. Kaspersky Security Center'da *Arka plan taraması* görevi de mevcuttur. Arka plan taraması yapılandırılamaz.

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 ve Cloud Console'da nasıl bir tarama çalıştırılır

1. Web Console'un ana penceresinde **Aygıtlar** → **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.
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. Tarama görevi görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

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.
- **Günlüğe kaydedildi**. Etkilenen dosya temizlenemedi. Uygulama, algılanan virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
- **Yazma desteklenmiyor** veya **Yazım hatası**. Etkilenen dosya temizlenemedi. Uygulamanın yazma erişimi yok.
- **Zaten işlenmiş**. 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 dosyalar taranırken, uygulama e-posta biçimli dosyaları da tarar. • **Önerilen**. Kaspersky Endpoint Security, tüm sabit sürücülerde, ağ sürücülerinde ve bilgisayarın çıkarılabilir ortam depolama alanında ve ayrıca gömülü OLE nesnelerinde sadece belirtilen dosya biçimlerini tarar. Uygulama, arşivleri veya kurulum paketlerini taramaz. • **Düşük**. Kaspersky Endpoint Security bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde sadece belirtilen uzantılara sahip yeni veya değiştirilmiş dosyaları tarar. Uygulama, bileşik dosyaları taramaz. Ön tanımlı güvenlik düzeylerinden birini seçebilir veya güvenlik düzeyi ayarlarını elle yapılandırabilirsiniz. Güvenlik düzeyi ayarlarını değiştirirseniz önerilen güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.
Tehdit algılandığında uygulanacak eylem	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler. **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme mümkün değilse Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler. **Bildir**. 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, e-posta veritabanları, sabit sürücü, çıkarılabilir sürücü veya ağ sürücüsü, klasör veya dosya içerebilir.

Tarama zamanlaması

Elle. 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 elle de 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 tarama görevini gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış tarama görevinin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan tarama görevlerini çalıştırmaz. Bunun yerine, bir sonraki tarama görevini geçerli zamanlamaya uygun olarak yürütür.

Sadece bilgisayar boştayken çalıştır

Bilgisayar kaynakları meşgul olduğunda tarama görevinin başlatılması ertelenen başlangıcı. 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.

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.

Şundan uzun süre taranan

Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.

nesneleri atla: N saniye

Aynı anda birden fazla tarama görevi çalıştırmayın

Bir tarama zaten çalışıyorsa tarama görevlerinin başlatılması geciktirilir. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security yeni tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, uygulamanın zamanlamaya göre bir Tam Tarama görevi başlattığını varsayalım. Bir kullanıcı uygulama arabiriminden bir hızlı tarama başlatmayı denediğinde, Kaspersky Endpoint Security bu hızlı tarama görevini kuyruğa alır ve ardından Tam Tarama görevi tamamlandıktan sonra bu görevi otomatik olarak başlatır.

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

Bu onay kutusu, üçüncü taraf dağıtım paketlerinin taranmasını etkinleştirir/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. Kaspersky Endpoint Security, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.

E-posta biçimlerini 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, MS Outlook e-posta sitemcisinin 64 bit sürümünü desteklemez. Bu, bilgisayarda MS Outlook'un 64 bit sürümü yüklüyse, tarama kapsamına posta dahil edilse bile Kaspersky Endpoint Security'nin MS 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.

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 tarama 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Yerel Görevler** → **Çıkarılabilir sürücü taraması** seçimini yapın.
5. **Bir çıkarılabilir sürücü bağlandığında yapılacak eylem** açılır listesinde, **Ayrıntılı Tarama** veya **Hızlı Tarama** arasından seçim yapın.
6. Çıkarılabilir sürücü taraması için gelişmiş seçenekleri yapılandırın (aşağıdaki tabloya bakın).
7. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Çıkarılabilir sürücü taraması nasıl yapılandırılır

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerel Görevler** → **Çıkarılabilir sürücü taraması** bölümüne gidin.
5. **Bir çıkarılabilir sürücü bağlandığında yapılacak eylem** açılır listesinde, **Ayrıntılı Tarama** veya **Hızlı Tarama** arasından seçim yapın.
6. Çıkarılabilir sürücü taraması için gelişmiş seçenekleri yapılandırın (aşağıdaki tabloya bakın).
7. 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 kullanımını yasaklamış demektir.

Çıkarılabilir sürücü taraması görev ayarları

Parametre	Açıklama
Bir çıkarılabilir sürücü bağlandığında yapılacak eylem	**Ayrıntılı Tarama**. Bu öğe işaretlendiğinde, bir çıkarılabilir sürücü bağlandığında Kaspersky Endpoint Security, bileşik nesnelerde iç içe geçmiş dosyalar, arşivler, dağıtım paketleri ve ofis biçimlerindeki dosyalar dahil olmak üzere çıkarılabilir sürücüde bulunan 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.
En büyük çıkarılabilir sürücü boyutu	Bu onay kutusu işaretlenirse belirtilen maksimum sürücü boyutundan daha büyük olmayan bir boyuta sahip çıkarılabilir sürücülerde Kaspersky Endpoint Security tarafından **Bir çıkarılabilir sürücü bağlandığında yapılacak eylem** açılır listesinden seçilen eylem gerçekleştirilir. Bu onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security **Bir çıkarılabilir sürücü bağlandığında yapılacak eylem** açılır listesinde seçilen eylemi her boyutta çıkarılabilir sürücüde gerçekleştirir.
Tarama ilerlemesini göster	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.
Tarama görevinin durdurulmasını 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 türlerinden (örneğin tam tarama) 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Yerel Görevler** → **Arka plan taraması** seçimini yapın.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Arka plan taramasını çalıştır** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da arka plan taraması nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.

4. **Yerel Görevler** → **Arka plan taraması** bölümüne gidin.

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Arka plan taramasını çalıştır** onay kutusunu 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.

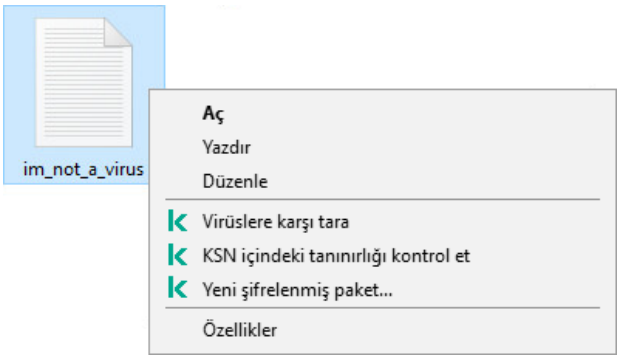
4. Değişikliklerinizi kaydedin.

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'nu açın.

2. Konsol ağacında **İlkeler**'i seçin.

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

4. İlke penceresinde, **Yerel Görevler** → **Bağlam Menüsünden Tarama** seçimini yapın.

5. Bağlam Menüsünden Taramayı yapılandırma (aşağıdaki tabloya bakın).

6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Bağlam Menüsünden Tarama nasıl yapılandırılır

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Yerel Görevler** → **Bağlam Menüsünden Tarama** seçeneklerini kullanın.
5. Bağlam Menüsünden Taramayı yapılandırma (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 kullanımını 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 dosyalar taranırken, uygulama e-posta biçimli dosyaları da tarar. • **Önerilen**. Kaspersky Endpoint Security, tüm sabit sürücülerde, ağ sürücülerinde ve bilgisayarın çıkarılabilir ortam depolama alanında ve ayrıca gömülü OLE nesnelerinde sadece belirtilen dosya biçimlerini tarar. Uygulama, arşivleri veya kurulum paketlerini taramaz. • **Düşük**. Kaspersky Endpoint Security bilgisayarın tüm sabit sürücülerinde, çıkarılabilir sürücülerinde ve ağ sürücülerinde sadece belirtilen uzantılara sahip yeni veya değiştirilmiş dosyaları tarar. Uygulama, bileşik dosyaları taramaz.
Tehdit algılandığında uygulanacak eylem	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler. **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme mümkün değilse Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler. **Bildir**. 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.

Şundan uzun süre taranan nesneleri atla: N saniye

Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.

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. Kaspersky Endpoint Security, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis biçimlerindeki dosyaları tarar.

E-posta biçimlerini 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, MS Outlook e-posta sitemcisinin 64 bit sürümünü desteklemez. Bu, bilgisayarda MS Outlook'un 64 bit sürümü yüklüyse, tarama kapsamına posta dahil edilse bile Kaspersky Endpoint Security'nin MS 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.

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 tarama 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. *Bütünlük denetimi* görevinin amacı uygulama dosyalarının denetlenmesidir. Kaspersky Endpoint Security bir zararlı nesne tespit ettiği halde onu etkisiz hale getirmezse *Bütünlük denetimi* görevini çalıştırın.

Bütünlük denetimi 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 bütünlük denetimi Yönetim Konsolu (MMC) aracılığıyla nasıl çalıştırılır

1. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.

   Görevler listesi açılır.

2. **Yeni görev** düğmesine tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (12.1) → **Bütünlük denetimi**'ni 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 elle 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

Sihirbazdan çıkın. 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 bütünlük denetimi zamanlaması yapılandırabilirsiniz (aşağıdaki tabloya bakın).

Bir uygulama bütünlük denetimi Web Console aracılığıyla nasıl çalıştırılır

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

   Görevler listesi açılır.

2. **Ekle** düğmesine tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Bütünlük denetimi**'ni seçin.

   c. **Görev adı** alanına kısa bir açıklama girin, örneğin, *Bilgisayara virüs bulaştıktan sonra uygulamanın bütünlüğünü kontrol et*.

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

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

5. Sihirbazdan çıkın.

   Görevler listesinde yeni bir görev görüntülenir.

6. Görevin yanındaki onay kutusunu seçin.

Sonuç olarak Kaspersky Endpoint Security uygulamanın bütünlüğünü denetleyecektir. İsterseniz görev özelliklerinden de bir uygulama bütünlük denetimi zamanlaması yapılandırabilirsiniz (aşağıdaki tabloya bakın).

Uygulama arabiriminde bütünlük denetimi nasıl yapılır

1. Ana uygulama penceresinde **Görevler** bölümüne gidin.

2. Görev listesi açılır; *Bütünlük denetimi* görevini seçin ve **Çalıştır**'a tıklayın.

Sonuç olarak Kaspersky Endpoint Security uygulamanın bütünlüğünü denetleyecektir. İsterseniz görev özelliklerinden de bir uygulama bütünlük denetimi zamanlaması yapılandırabilirsiniz (aşağıdaki tabloya bakın). *Bütünlük denetimi* görüntülenmiyorsa, yönetici ilkede yerel görevlerin kullanımını yasaklamış demektir.

Bütünlük denetimi görev ayarları

Parametre	Açıklama
Tarama zamanlaması	**Elle**. 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 elle de başlatabilirsiniz.
Atlanmış görevleri çalıştır	Onay kutusu işaretlenirse Kaspersky Endpoint Security, atlanan tarama görevini gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış tarama görevinin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan tarama görevlerini çalıştırmaz. Bunun yerine, bir sonraki tarama görevini geçerli zamanlamaya uygun olarak yürütür.
Sadece bilgisayar boştayken çalıştır	Bilgisayar kaynakları meşgul olduğunda tarama görevinin başlatılması ertelenen başlangıcı. 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.

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:

- **E-postam**.

  Outlook posta istemcisiyle ilgili dosyalar: veri dosyaları (PST), çevrimdışı veri dosyaları (OST).

- **Sistem belleği**.
- **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**.

  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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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 nesnenin yanındaki onay kutusunun işaretini kaldırın.
8. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir tarama kapsamı nasıl düzenlenir

1. Web Console'un ana penceresinde **Aygıtlar** → **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** düğmesine tıklayın.

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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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

Bilgisayarın tamamen taranması biraz zaman alır ve bilgisayarın kaynaklarını kullanır. Diğer yazılımların performansını olumsuz etkilemekten kaçınmak adına, bilgisayar taraması yapmak için en uygun zamanı seçmelisiniz. Kaspersky Endpoint Security, bilgisayarı taramak için normal bir zamanlama yapılandırmanıza olanak tanır. Bu, kuruluşunuzun bir çalışma zamanlaması varsa kullanışlıdır. Bir bilgisayar taramasını gece veya hafta sonları çalışacak şekilde yapılandırabilirsiniz. Tarama görevini herhangi bir nedenle çalıştırmak mümkün değilse (örneğin bilgisayar o sırada kapalıysa) atlanan görevi mümkün olur olmaz otomatik olarak çalışacak şekilde yapılandırabilirsiniz.

Optimum bir tarama zamanlaması yapılandırmanın imkansız olduğu durumlarda, Kaspersky Endpoint Security bir bilgisayar taraması çalıştırmanıza aşağıdaki özel koşullar karşılandığında izin verir:

- Bir veritabanı güncellemesinden sonra.

  Kaspersky Endpoint Security, bilgisayar taramasını güncellenmiş imza veritabanlarıyla çalıştırır.
- Uygulama başlatıldıktan sonra.

Kaspersky Endpoint Security, uygulama başlatıldıktan sonra belirli bir süre geçtiğinde bir bilgisayar taraması gerçekleştirir. İşletim sistemi başlangıcında birçok işlem çalışır, bu nedenle tarama görevini çalıştırmayı Kaspersky Endpoint Security'nin başlatılmasından hemen sonra çalıştırmak yerine ertelemek avantajlıdır.

- LAN'da Uyandırma.

  Kaspersky Endpoint Security, bilgisayar kapalı olsa bile zamanlamaya göre bir bilgisayar taraması gerçekleştirir. Bunu yapmak için uygulama, işletim sisteminin LAN'da Uyandırma özelliğini kullanır. LAN'da Uyandırma özelliği, yerel ağ üzerinden özel bir sinyal göndererek bilgisayarın uzaktan açılmasını sağlar. Bu özelliği kullanmak için BIOS ayarlarından LAN'da Uyandırmayı etkinleştirmeniz gerekir.

  Taramayı çalıştırmayı LAN'da Uyandırma özelliğini kullanarak sadece Kaspersky Security Center'daki *Kötü Amaçlı Yazılım Taraması* görevi için yapılandırabilirsiniz. Uygulama arabiriminde bilgisayarı taramak için LAN'da Uyandırmayı 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, uygulamanın tam bir bilgisayar taramasını tamamlaması için birkaç gün gerekebileceği anlamına gelir.

Yönetim Konsolu'nda (MMC) nasıl bir tarama zamanlaması yapılandırılır

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. Bilgisayar özellikleri penceresinde **Zamanlama** bölümünü seçin.
5. Tarama görevi zamanlamasını yapılandırın.
6. Seçilen sıklığa bağlı olarak görev çalışma zamanlamasını belirten gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).
7. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir tarama zamanlaması nasıl yapılandırılır

1. Web Console'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. Tarama görevine tıklayın.
   Görev özellikleri penceresi açılır.
3. **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	**Elle**. 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 elle de 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 tarama görevini gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, zamanlanmış tarama görevinin başlatılma saatinde bilgisayar kapalıysa, tarama görevi atlanabilir. Onay kutusunun işareti kaldırılırsa Kaspersky Endpoint Security atlanan tarama görevlerini çalıştırmaz. Bunun yerine, bir sonraki tarama görevini geçerli zamanlamaya uygun olarak yürütür.
Sadece bilgisayar boştayken çalıştır	Bilgisayar kaynakları meşgul olduğunda tarama görevinin başlatılması ertelenen başlangıcı. 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.
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.
Görev N dakikadan uzun bir zamandır çalışıyorsa durdur	Belirtilen süreden sonra görev yürütme süresi sınırlandığında, 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.

(sadece Kaspersky Security Center Konsolunda mevcuttur)

Görev Wake-on-LAN ile başlatılmadan önce cihazı etkinleştir (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.

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 **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. Tarama görevine tıklayın.

Görev özellikleri penceresi açılır.

3. **Ayarlar** sekmesini seçin.
4. **Hesap** bloğunda, **Ayarlar**'a 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

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. **Tarama optimizasyonu** 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**. Bu, tek bir nesnenin taranması için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.

- **Aynı anda birden fazla tarama görevi çalıştırmayın**. Bir tarama zaten çalışıyorsa tarama görevlerinin başlatılması geciktirilir. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security yeni tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, uygulamanın zamanlamaya göre bir Tam Tarama görevi başlattığını varsayalım. Bir kullanıcı uygulama arabiriminden bir hızlı tarama başlatmayı denediğinde, Kaspersky Endpoint Security bu hızlı tarama görevini kuyruğa alır ve ardından Tam Tarama görevi tamamlandıktan sonra bu görevi otomatik olarak başlatır.

7. **Diğer**'e tıklayın.

   Bu, birleşik dosyaları tarama ayarları penceresini açar.

8. **Boyut sınırı** bloğunda, **Büyük bileşik dosya paketlerini açma** onay kutusunu işaretleyin. Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.

   Kaspersky Endpoint Security, **Büyük bileşik dosya paketlerini açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük dosyaları tarar.

9. **Tamam**'a tıklayın.

10. **Diğer** sekmesini seçin.

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 tarama 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 Console'da ve Cloud Console'da tarama nasıl optimize edilir

1. Web Console'un ana penceresinde **Aygıtlar** → **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 uygulanacak 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. Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın

süresini kısaltır.

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. Bir tarama zaten çalışıyorsa tarama görevlerinin başlatılması geciktirilir. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security yeni tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, uygulamanın zamanlamaya göre bir Tam Tarama görevi başlattığını varsayalım. Bir kullanıcı uygulama arabiriminden bir hızlı tarama başlatmayı denediğinde, Kaspersky Endpoint Security bu hızlı tarama görevini kuyruğa alır ve ardından Tam Tarama görevi tamamlandıktan sonra bu görevi otomatik olarak başlatır.
7. **Gelişmiş ayarlar** bloğundan **Bu süreden daha uzun süreyle taranan dosyaları atla: N saniyeden** onay kutusunu işaretleyin. Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.
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. **Tarama optimizasyonu** 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.
   - **Şundan uzun süre taranan nesneleri atla: N saniye**. Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.
   - **Aynı anda birden fazla tarama görevi çalıştırmayın**. Bir tarama zaten çalışıyorsa tarama görevlerinin başlatılması geciktirilir. Mevcut tarama devam ediyorsa Kaspersky Endpoint Security yeni tarama görevlerini kuyruğa alır. Bu, bilgisayardaki yükün optimize edilmesine yardımcı olur. Örneğin, uygulamanın zamanlamaya göre bir Tam Tarama görevi başlattığını varsayalım. Bir kullanıcı uygulama arabiriminden bir hızlı tarama başlatmayı denediğinde, Kaspersky Endpoint Security bu hızlı tarama görevini kuyruğa alır ve ardından Tam Tarama görevi tamamlandıktan sonra bu görevi otomatik olarak başlatır.
5. **Boyut sınırı** bloğunda, **Büyük bileşik dosya paketlerini açma** onay kutusunu işaretleyin. Bu, tek bir nesneyi taramak için bir süre sınırı belirler. Belirtilen süre sonunda uygulama bir dosyayı taramayı durdurur. Bu yardım, bir taramanın süresini kısaltır.

   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 tarama 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.

Düzenli güncellemeler için geçerli bir lisans gerekir. Geçerli bir lisans yoksa, güncellemeyi günde sadece bir kez gerçekleştirebilirsiniz.

Kaspersky Endpoint Security'nin ana güncelleme kaynağı, Kaspersky güncelleme sunucularıdır.

Kaspersky güncelleme sunucularından güncelleme paketini başarılı bir şekilde indirmek için bilgisayarınız İnternet'e bağlı olmalıdır. Varsayılan olarak İnternet bağlantısı ayarları otomatik olarak tespit edilir. Proxy sunucusu kullanıyorsanız, 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.

İçerik yardım dosyaları, uygulama modülü güncellemeleri ile birlikte güncellenebilir.

Veritabanları eskiyse, güncelleme paketi çok büyük olabilir ve ek İnternet trafiğine (onlarca MB) neden olabilir.

Kaspersky Endpoint Security veritabanlarının geçerli 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.

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:

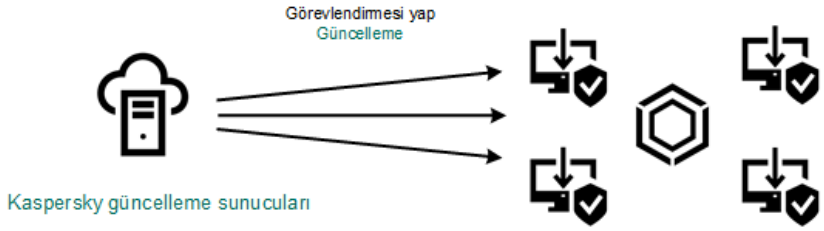
- Anti-virüs veritabanları. Anti-virüs veritabanları; zararlı yazılım imzalarının veritabanlarını, ağ saldırılarının açıklamasını, şüpheli ve kimlik avı yapan İnternet adreslerinin veritabanlarını, reklam pencerelerinin veritabanlarını, spam veritabanlarını ve diğer verileri içerir.

- 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).

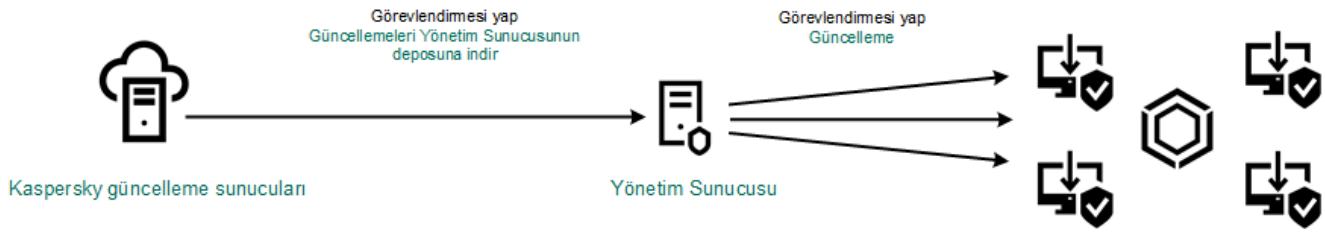
     Güncelleme paketini paylaşılan bir klasöre aşağıdaki yöntemleri kullanarak indirebilirsiniz:

     - Kaspersky Endpoint Security *Güncelleme* görevini kullanma. Görev, yerel şirket ağındaki bilgisayarlardan biri için tasarlanmıştır.

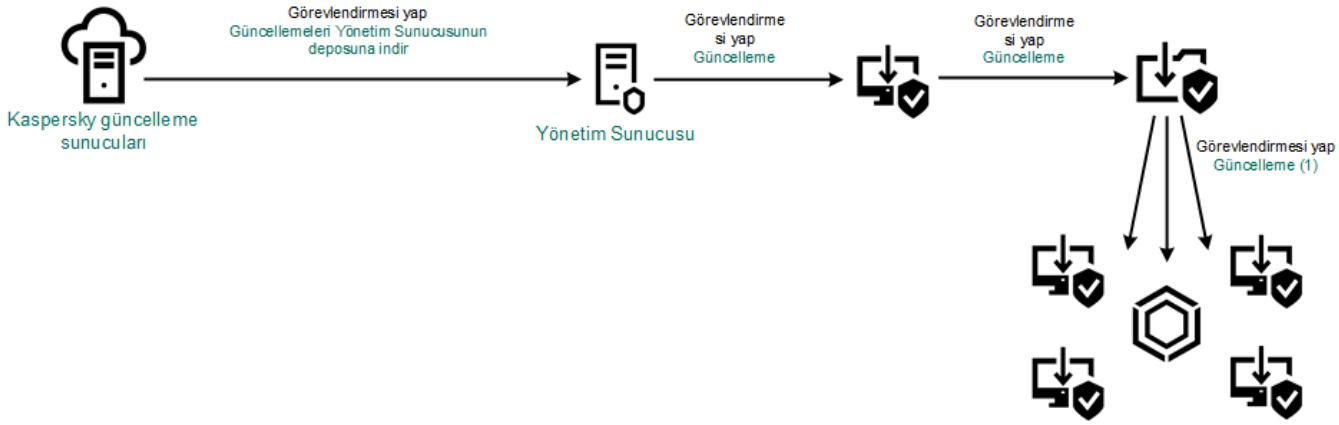
     - Kaspersky Update Utility'yi Kullanma. Kaspersky Update Utility'yi kullanma hakkında ayrıntılı bilgi için Kaspersky Bilgi Bankası 'na bakın.

  3. Güncelleme paketini istemci bilgisayarlara dağıtın.

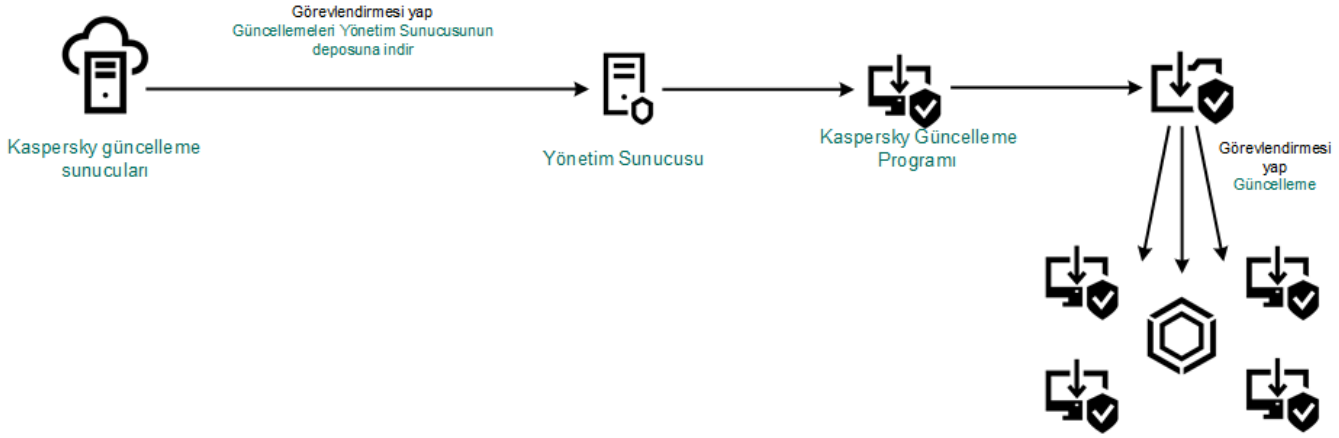
     Güncelleme paketi, Kaspersky Endpoint Security *Güncelleme* görevi ile istemci bilgisayarlara dağıtılır. Her bir yönetim grubu için sınırsız sayıda güncelleme görevi oluşturabilirsiniz.



Bir sunucu veri havuzu üzerinden güncelleme



Bir paylaşım klasörü üzerinden güncelleme



Kaspersky Update Utility aracıyla güncelleme

Web Konsolu 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 deposuna 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 (*Güncelleme* görevi).

Yönetim Konsolu'nda (MMC) belirtilen sunucu depolama alanından Kaspersky Endpoint Security güncellemesi nasıl yapılandırılır

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

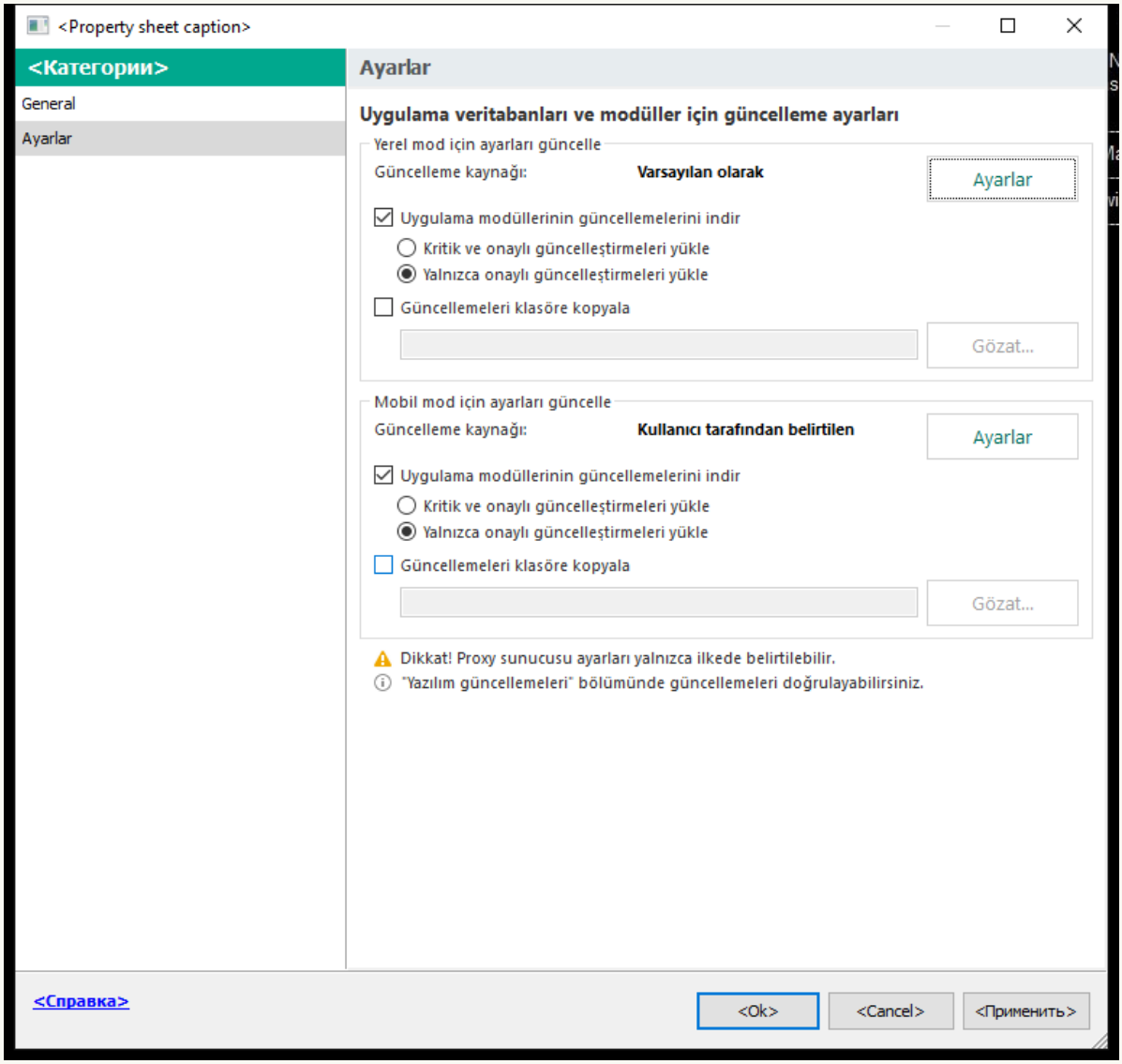
   Konsol ağacında **Görevler**'i seçin.

2. Kaspersky Endpoint Security'nin **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. Görev özellikleri penceresinde **Ayarlar** bölümünü seçin.



Güncelleme görevi 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:

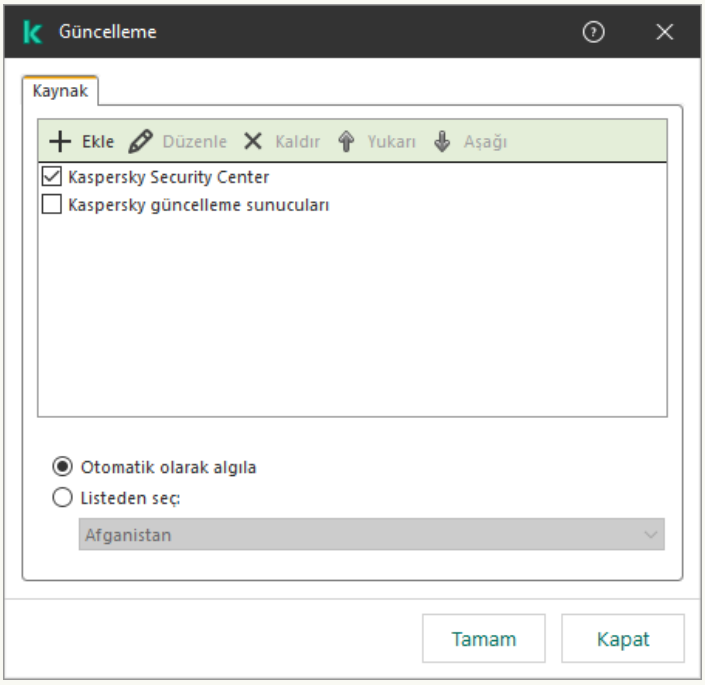
   a. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

   b. **Kaynak** 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 Sunucusuna indir* depo 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   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** sekmesinden **Yerel mod** seçimini yapın.

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:

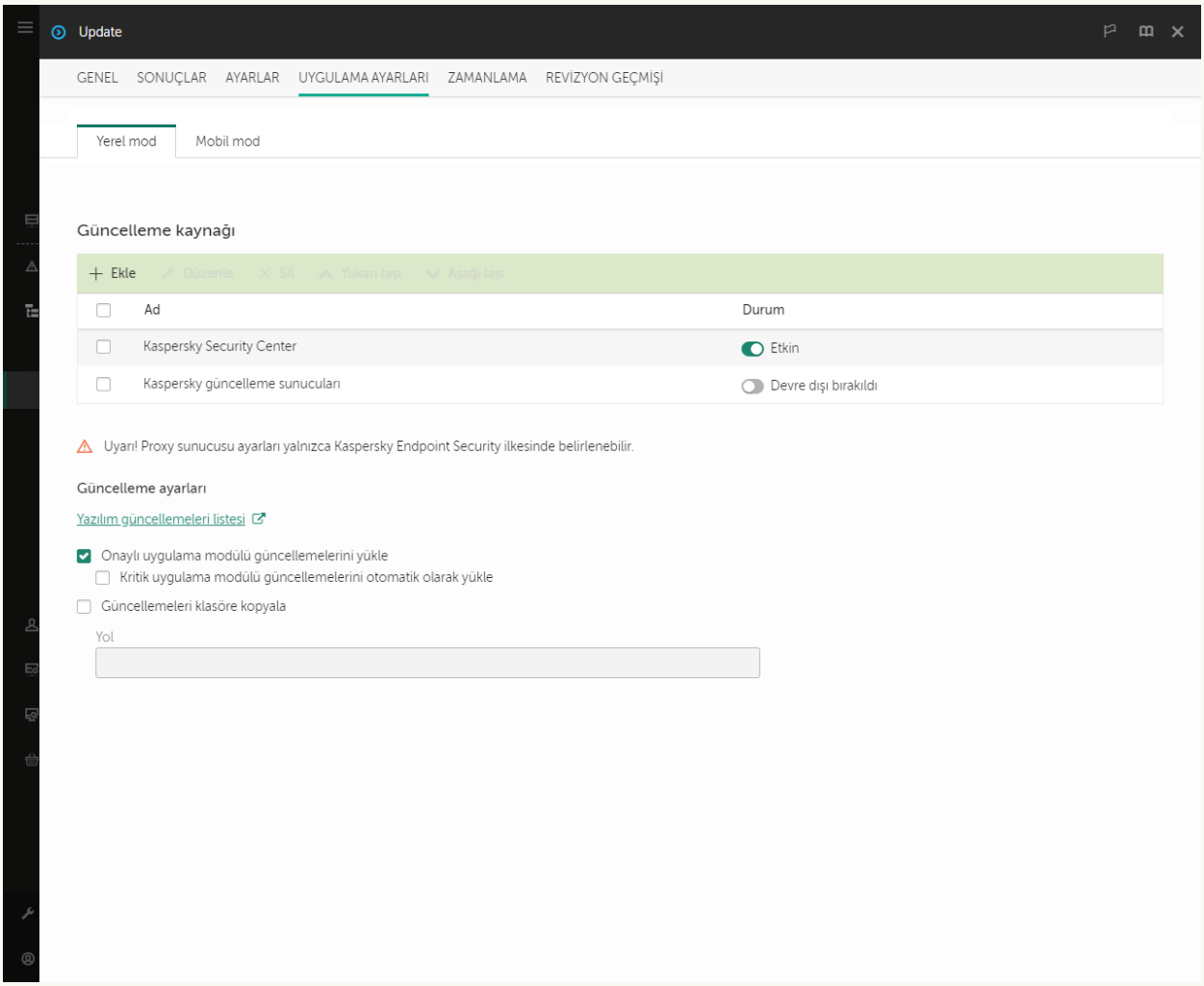
a. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.

b. **Kaynak** 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 Sunucusuna indir* depo görevi).

c. **Tamam**'a tıklayın.

Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.



Güncelleme kaynakları

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.

7. Görev özellikleri penceresinde, **Zamanlama** bölümünü seçin ve görev çalışma modunu yapılandırın.

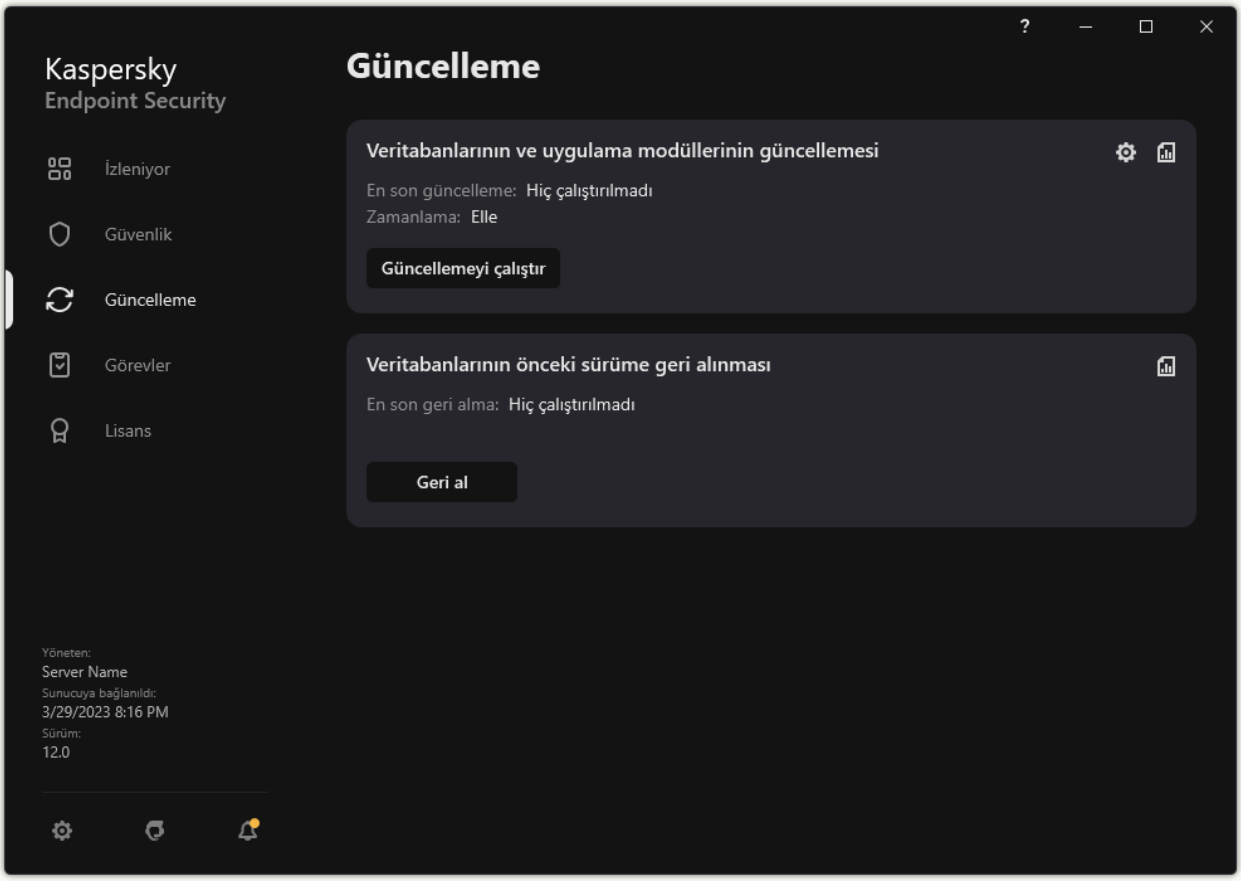
8. Varsayılan olarak, Kaspersky Endpoint Security görevi manuel modda çalıştırır.

9. Değişikliklerinizi kaydedin.

[Uygulama arabiriminde belirtilen sunucu depolama alanından Kaspersky Endpoint Security güncellemesi nasıl yapılandırılır](#)

Güncelleme grubu görevini uygulama arabiriminde yapılandıramazsınız. Yalnızca yerel bir güncelleme görevi olan *Veritabanlarının ve uygulama modüllerinin güncellenmesi* 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

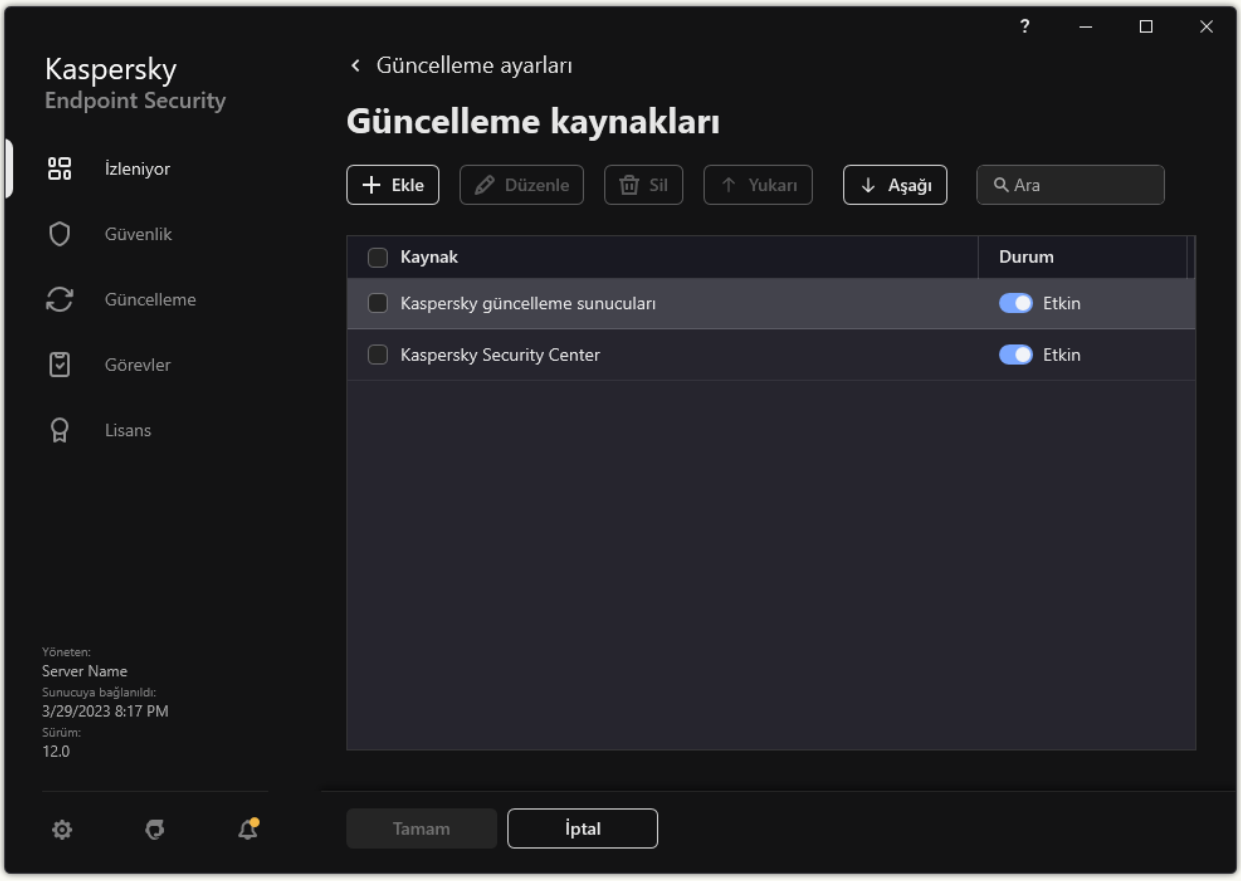
2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın. Görev özellikleri penceresi açılır.

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 Sunucusuna indir* depo görevi).

b. **Seç**'e tıklayın.

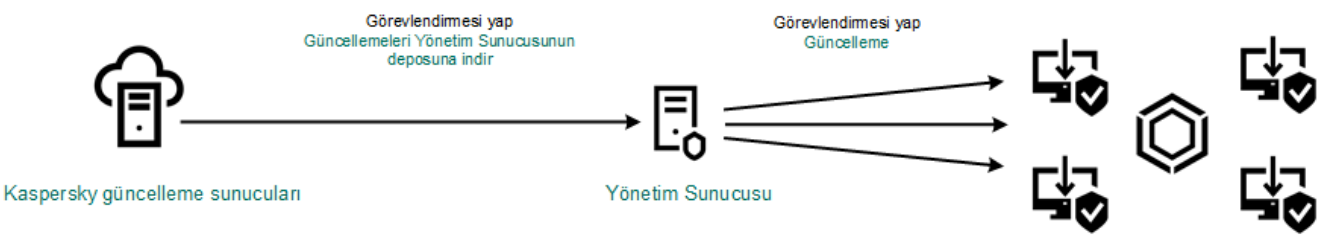
Güncelleme kaynağını, güncelleme kaynakları listesinden kaldırmanın dışında tutabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.

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 güncellenmesi* görevi için çalışma modunu yapılandırmak mümkün değildir. Görevi yalnızca manuel olarak çalıştırabilirsiniz.

7. Değişikliklerinizi kaydedin.



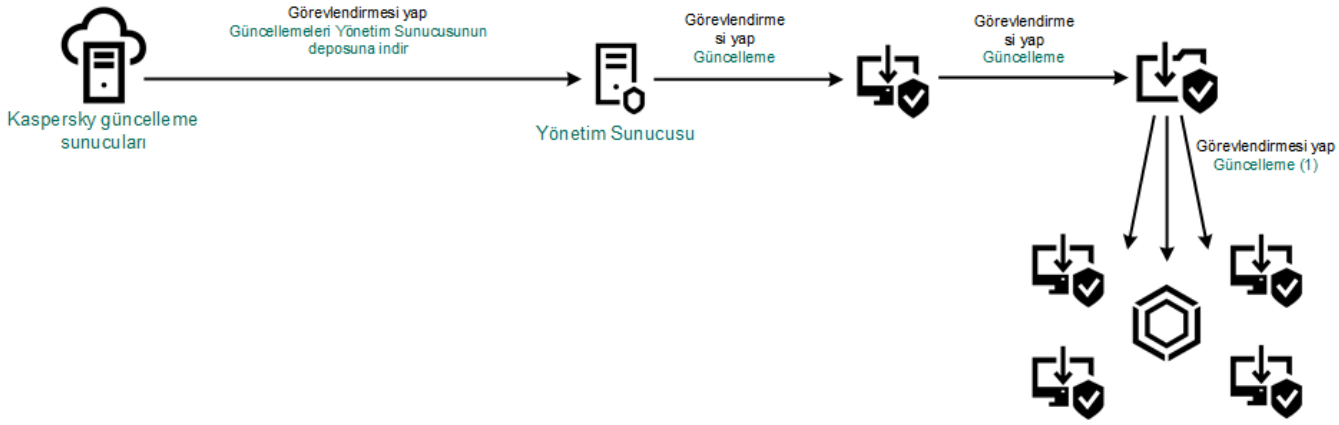
Bir paylaşım klasörü üzerinden güncelleme

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.

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. Kurumsal LAN üzerindeki bilgisayarlardan birindeki bir paylaşım klasörüne bir güncelleme paketinin kopyalanmasını etkinleştirme (aşağıdaki talimatlara bakın).
3. Kurumsal LAN ağındaki diğer bilgisayarları veritabanı ve uygulama modülü güncellemelerini belirli bir paylaşım klasörü üzerinden yapacak şekilde yapılandırma (aşağıdaki talimatlara bakın).

> 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.



Bir paylaşım klasörü üzerinden güncelleme

Güncelleme paketinin paylaşım klasörüne kopyalanmasını etkinleştirmek için:

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

   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** sekmesinden **Yerel mod** seçimini yapın.

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\Share\Update distribution`).

   Alan boş bırakılırsa Kaspersky Endpoint Security, güncelleme paketini `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\` klasörüne kopyalar.
7. Değişikliklerinizi kaydedin.

Güncellemeleri bir paylaşım klasörü üzerinden yapılandırmak için:

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

   Görevler listesi açılır.
2. **Ekle** düğmesine tıklayın.

   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** 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 cihazları seçin** 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. Sihirbazdan çıkın.

   Görevler tablosunda yeni bir görev görüntülenir.
6. Yeni oluşturulan *Güncelleme* görevine tıklayın.

   Görev özellikleri penceresi açılır.
7. **Uygulama ayarları** bölümüne gidin.
8. **Yerel mod** sekmesine gidin.
9. **Güncelleme kaynağı** bloğunda, **Ekle**'ye tıklayın.
10. **Kaynak** alanına paylaşım klasörünün yolunu girin.

    > Kaynak adresi, daha önce paylaşılan güncelleme paketinin kopyalanmasını yapılandırırken **Yol** alanında belirtmiş olduğunuz adresle aynı olmalıdır (yukarıdaki talimata bakın).
11. **Tamam**'a tıklayın.
12. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.
13. Değişikliklerinizi kaydedin.

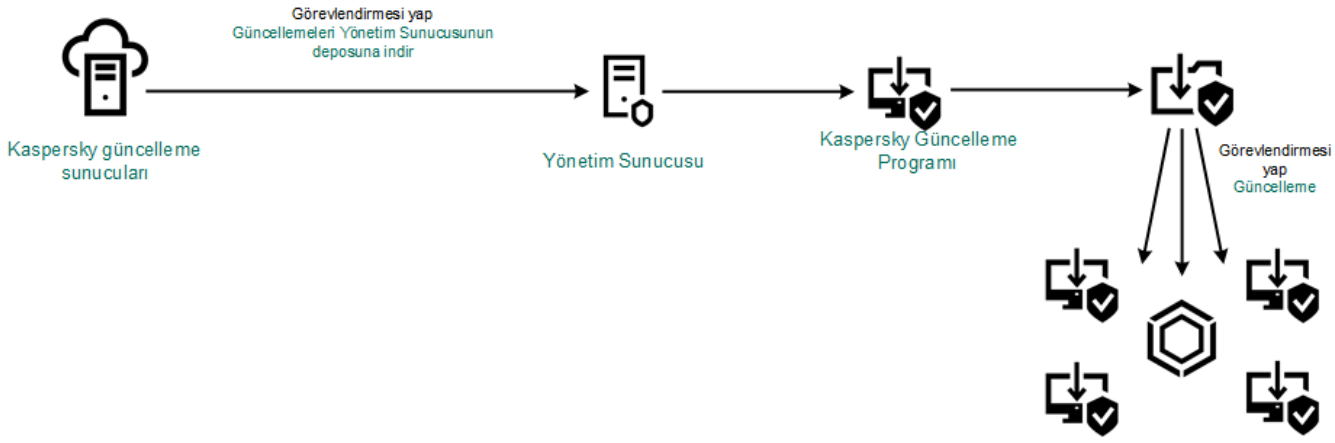
Kaspersky Update Utility aracıyla güncelleme

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.

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.
4. Kuruluşun LAN ağındaki diğer bilgisayarları veritabanı ve uygulama modülü güncellemelerini belirli bir paylaşım klasörü üzerinden yapacak şekilde yapılandırma.

> 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.



Kaspersky Update Utility aracıyla güncelleme

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.

Güncellemeleri bir paylaşım klasörü üzerinden yapılandırmak için:

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

   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** sekmesinden **Yerel mod** seçimini yapın.
4. Güncelleme kaynakları listesinde **Ekle** düğmesine tıklayın.
5. **Kaynak** alanına paylaşılan klasöre giden UNC yolunu girin (örneğin `\\Server\Share\Update distribution`).

> Kaynak adresi, Kaspersky Update Utility ayarlarında belirtilen adresle aynı olmalıdır.

6. **Tamam**'a tıklayın.

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

8. Değişikliklerinizi kaydedin.

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 işyeri dışında ilkesi ile belirlenir. İşyeri dışında ilkesi ayrıca oluşturulmalıdır. Kaspersky Endpoint Security, mobil moda geçtiğinde güncelleme görevi her iki saatte bir başlatılır.

Mobil mod için güncelleme ayarlarını yapılandırmak için:

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

   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** sekmesinden **Mobil mod** seçimini yapın.

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

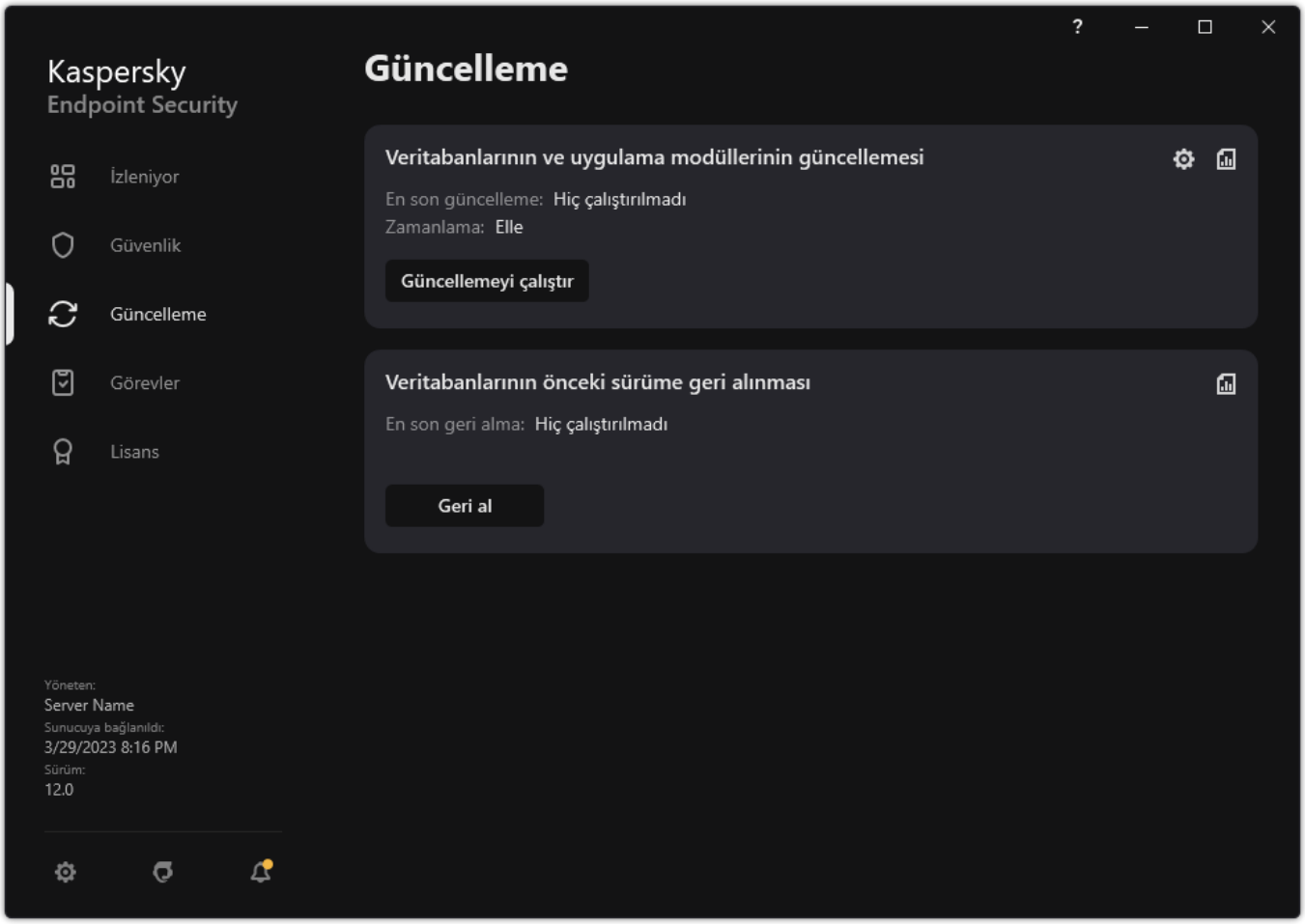
- duraklatılmış bir güncelleme görevini seçerek sürdürün veya yeniden başlatın

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:

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.

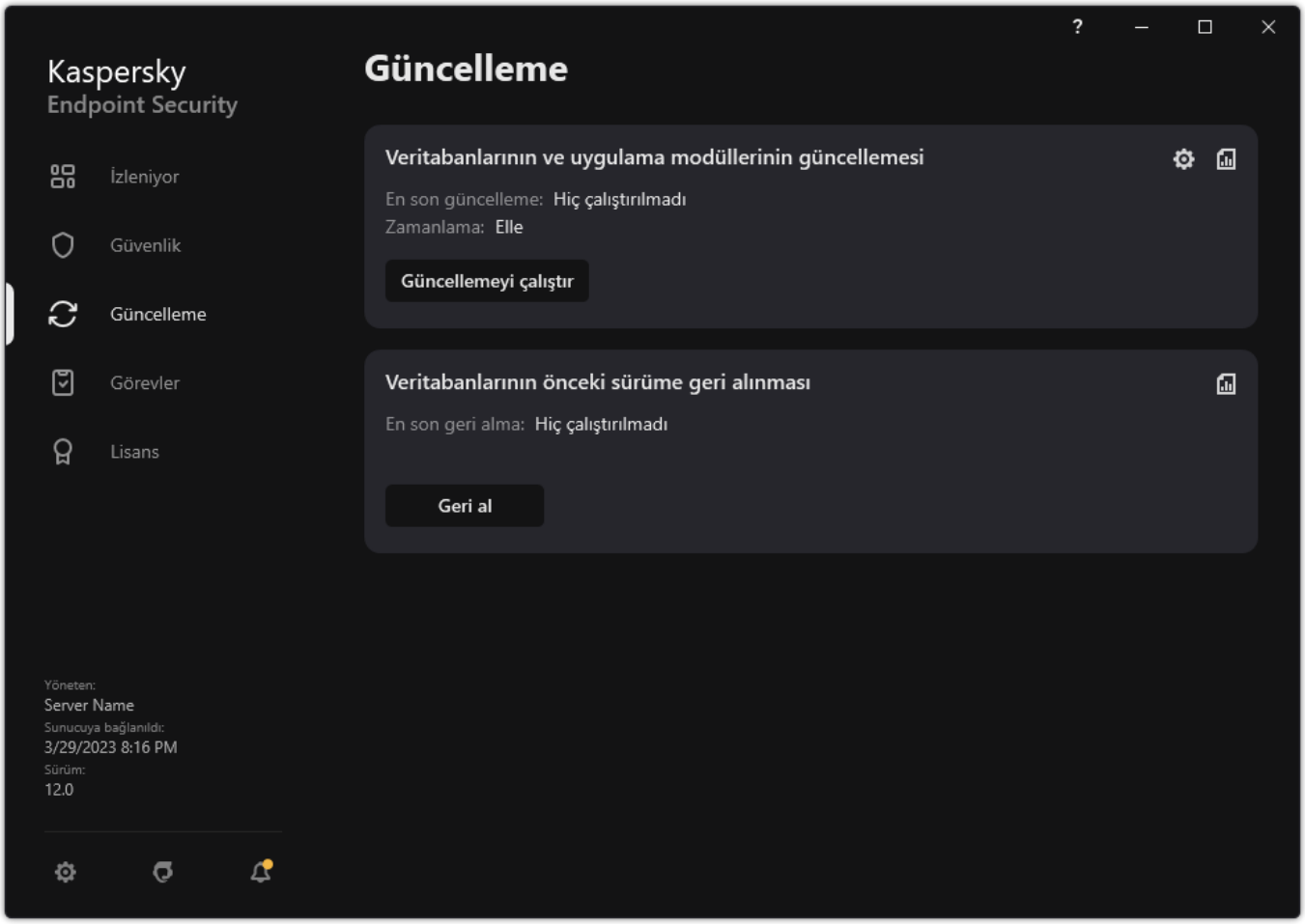
Güncelleme görevinin çalışma modunu seçme

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:

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 **Elle** 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.

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.

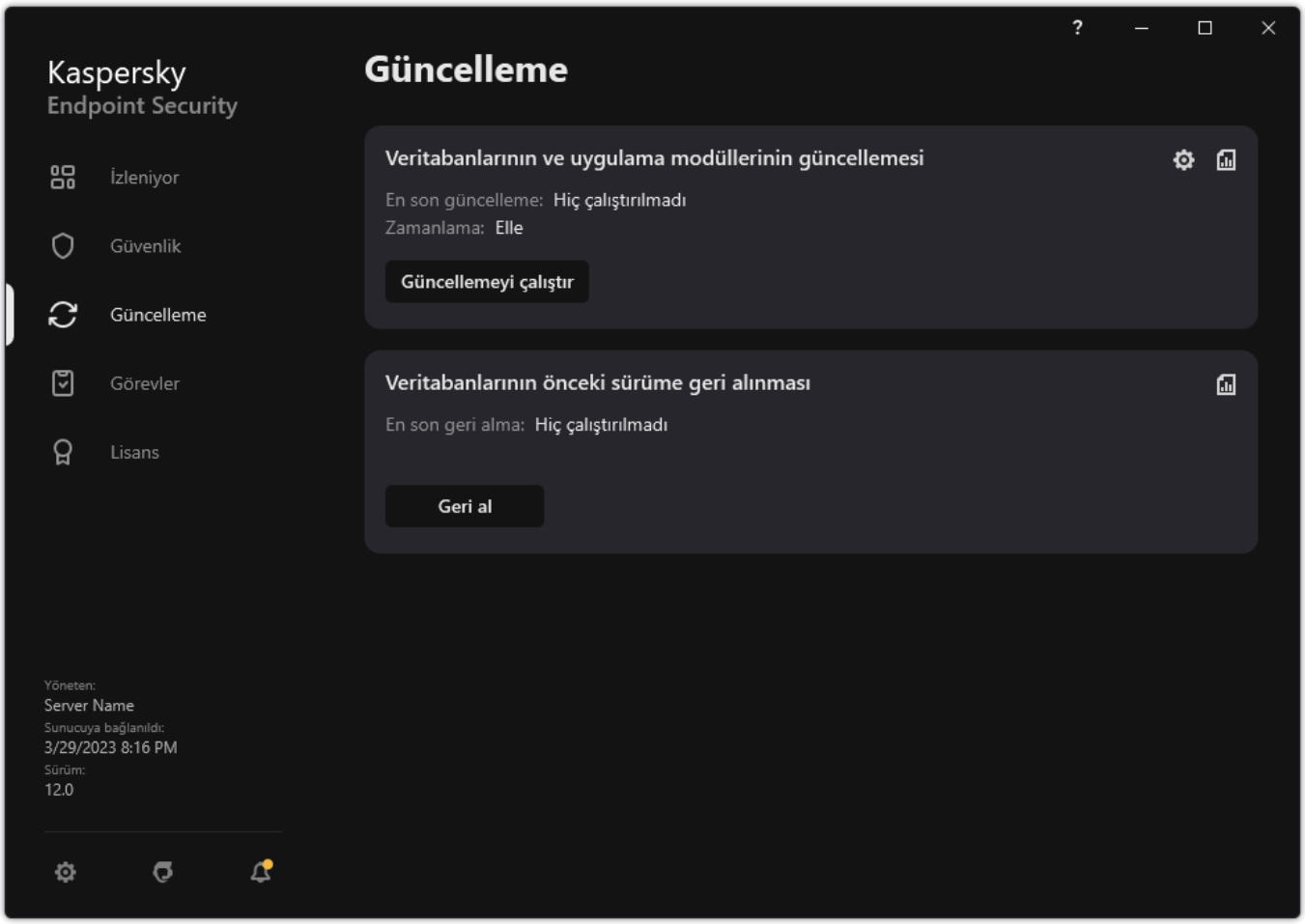
Varsayılan güncelleme kaynaklarının listesi, Kaspersky Security Center ve Kaspersky güncelleme sunucularını içerir. Listeye başka güncelleme kaynakları da ekleyebilirsiniz. HTTP/FTP sunucuları ve paylaşım klasörlerini güncelleme kaynakları olarak belirtebilirsiniz.

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.

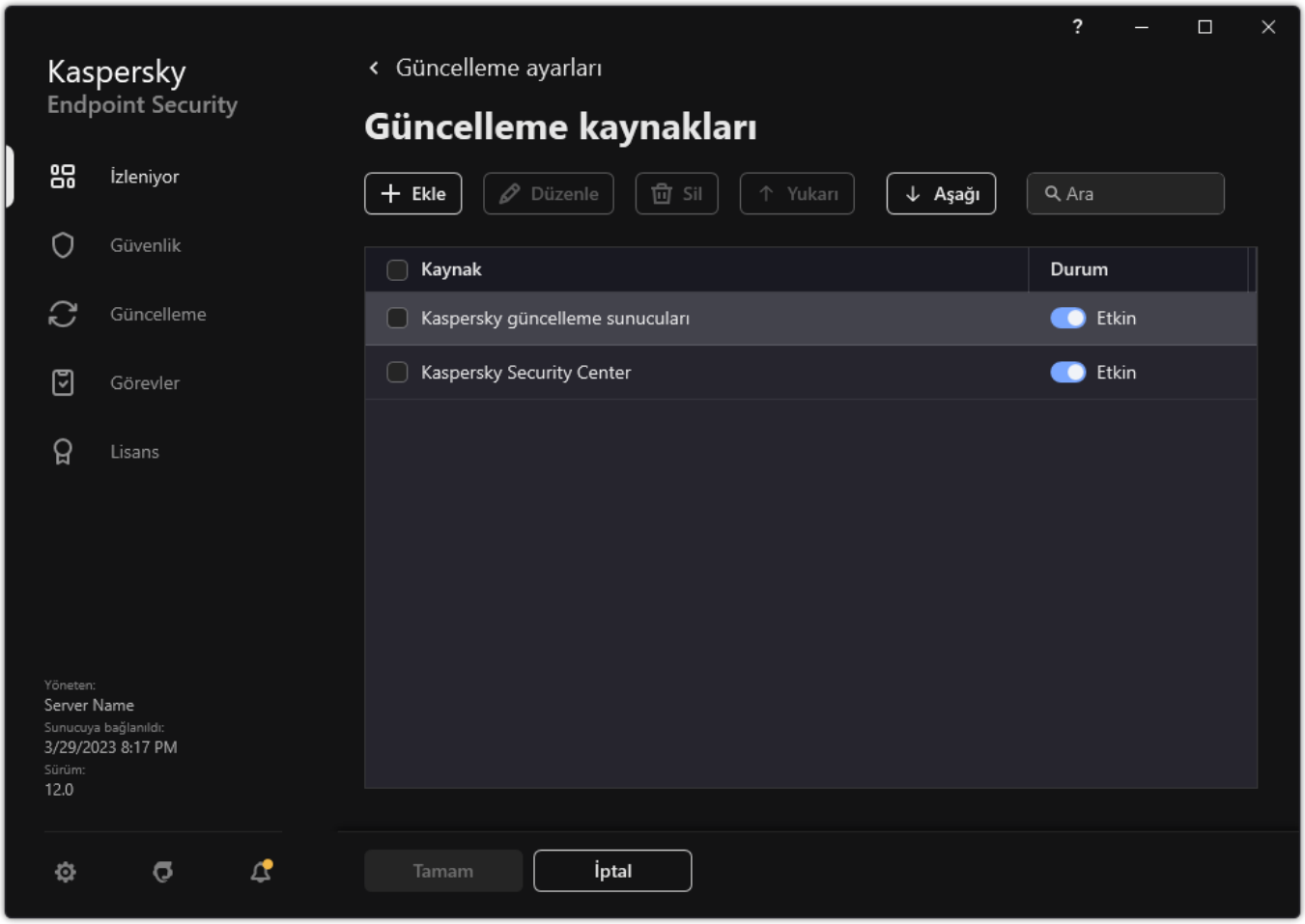
Bir güncelleme kaynağı eklemek için:

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** düğmesine 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://<kullanıcı adı>:<parola>@<host>:<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\AVP11\Update distribution\`.

6. **Seç** düğmesine tıklayın.

7. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.

8. Değişikliklerinizi kaydedin.

Paylaşım klasöründen güncellemeleri yapılandırma

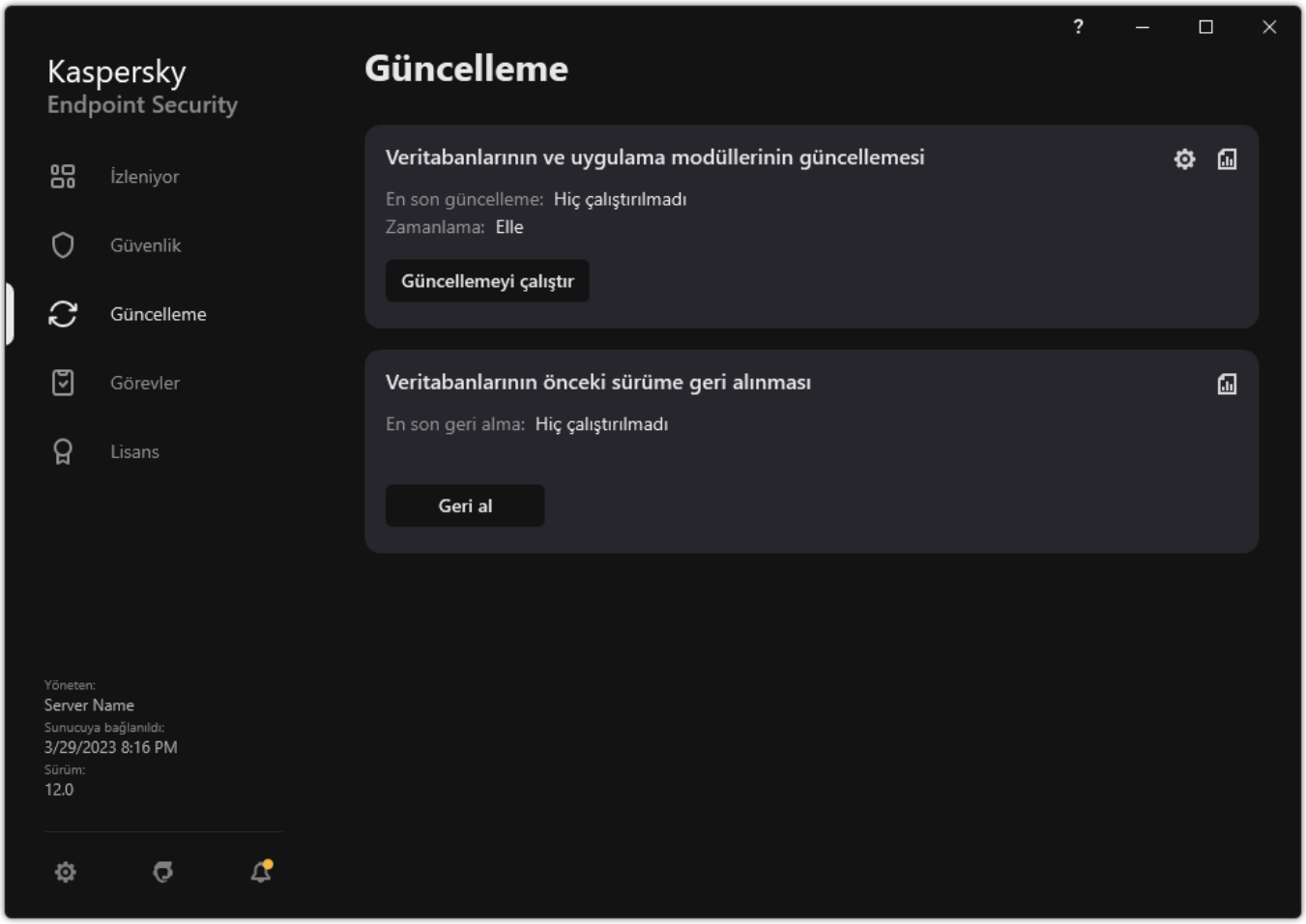
İnternet trafiğini düşük tutmak için kuruluşun LAN ağındaki bilgisayarların veritabanları ve uygulama modülleri güncellemelerini bir paylaşım klasörü üzerinden gerçekleştirilmek üzere yapılandırabilirsiniz. Bu amaçla, kuruluşun LAN ağındaki bilgisayarlardan biri Kaspersky Security Center Yönetim Sunucusu 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.

Aşağıdaki adımları uygulayarak veritabanı ve uygulama modüllerini bir paylaşım klasörü üzerinden güncellenecek şekilde yapılandırma:

1. Yerel ağ üzerindeki bilgisayarlardan birindeki bir paylaşım klasörüne bir güncelleme paketinin kopyalanmasını etkinleştirme.
2. Kuruluşun LAN ağındaki diğer bilgisayarları veritabanı ve uygulama modülü güncellemelerini belirli bir paylaşım klasörü üzerinden yapacak şekilde yapılandırma.

Güncelleme paketinin paylaşım klasörüne kopyalanmasını etkinleştirmek için:

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.

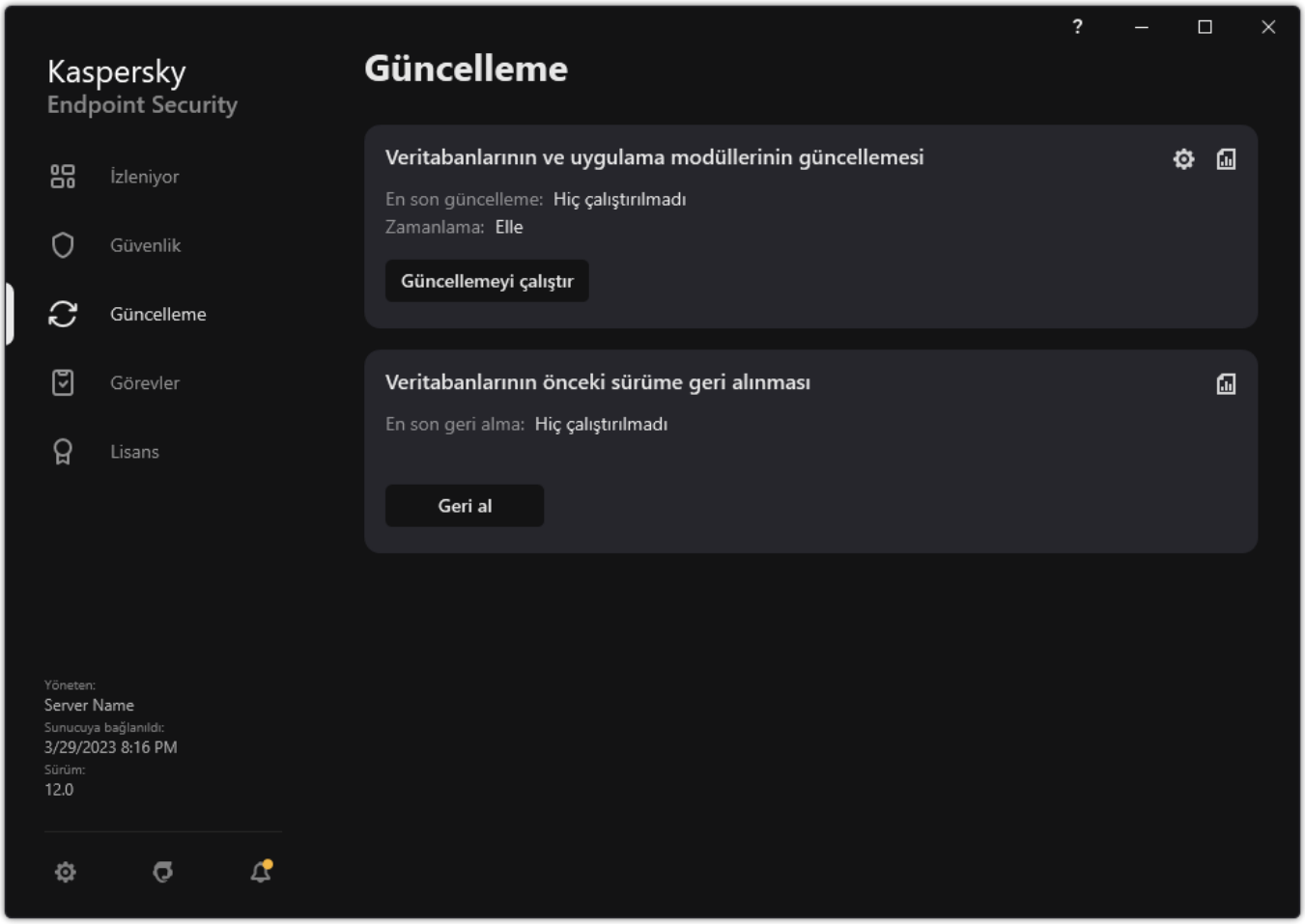


Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.
   Görev özellikleri penceresi açılır.
3. **Güncellemelerin dağıtımı** bloğunda, **Güncellemeleri klasöre kopyala** onay kutusunu seçin.
4. Paylaşılan klasöre giden UNC yolunu girin (örneğin `\\Server\Share\Update distribution`).
5. Değişikliklerinizi kaydedin.

Güncellemeleri bir paylaşım klasörü üzerinden yapılandırmak için:

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. Açılan görev listesinden *Veritabanlarının ve uygulama modüllerinin güncellemesi* görevini seçin ve ⚙ düğmesine tıklayın.
3. Görev özellikleri penceresi açılır.
4. **Güncelleme kaynaklarını seç**'e tıklayın.
5. Açılan pencerede **Ekle** düğmesine tıklayın.
6. Açılan pencereye paylaşım klasörünün yolunu girin.

   Kaynak adresi, daha önce paylaşılan güncelleme paketinin kopyalanmasını yapılandırırken belirtmiş olduğunuz adresle aynı olmalıdır (yukarıdaki talimata bakın).

7. **Seç**'e tıklayın.
8. **Yukarı** ve **Aşağı** düğmelerini kullanarak güncelleme kaynaklarının önceliklerini yapılandırın.
9. Değişikliklerinizi kaydedin.

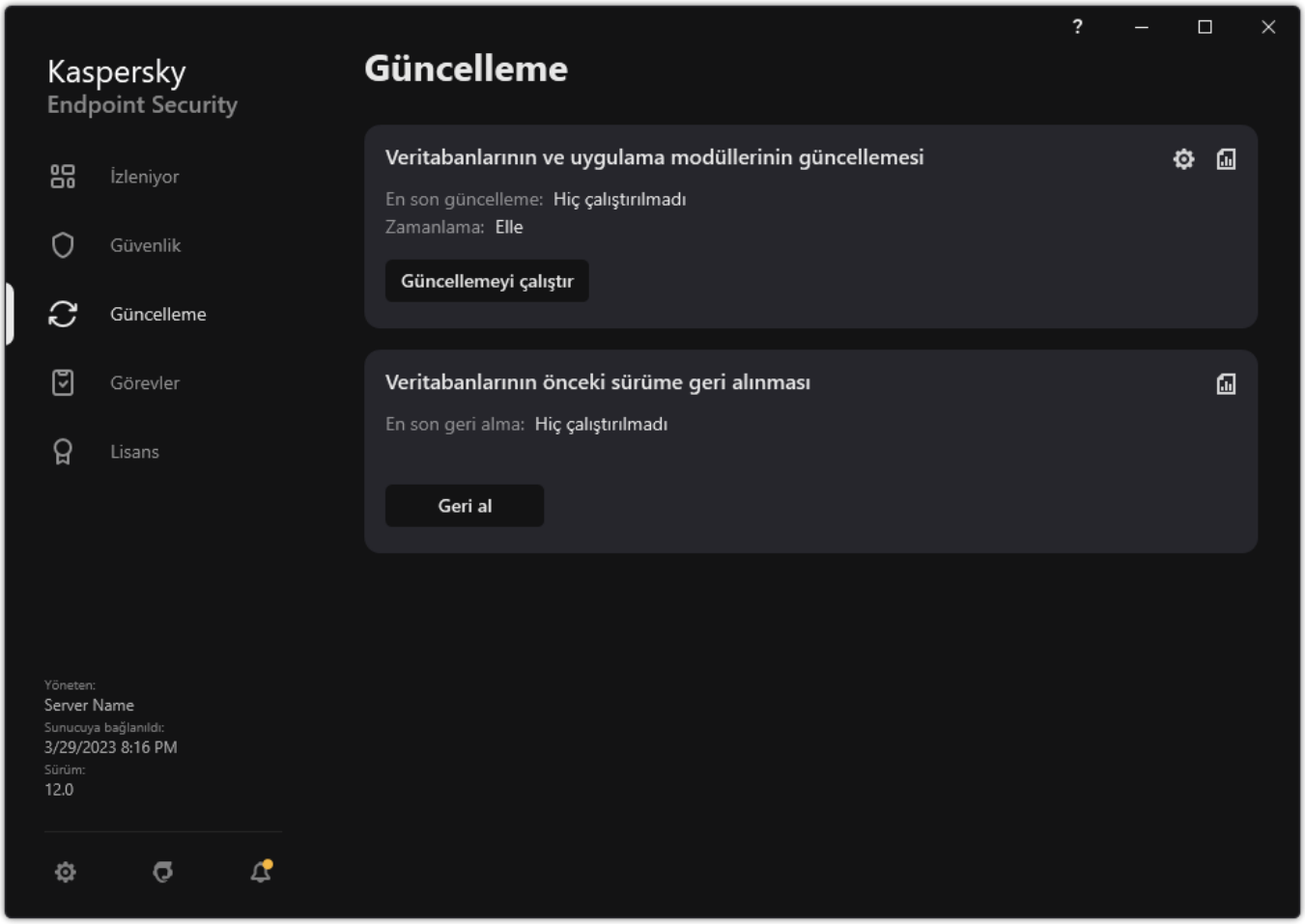
Uygulama modüllerini güncelleme

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. Kaspersky Security Center'da uygulama modülü güncellemelerini takip etme ve bir güncellemeyi onaylama hakkında ayrıntılar için lütfen Kaspersky Security Center Yardım içeriğine bakın.

Bir uygulama güncellemesini yükledikten sonra bilgisayarınızı yeniden başlatmanız gerekebilir.

Uygulama modülü güncellemelerini yapılandırmak için:

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 sunucusu 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:

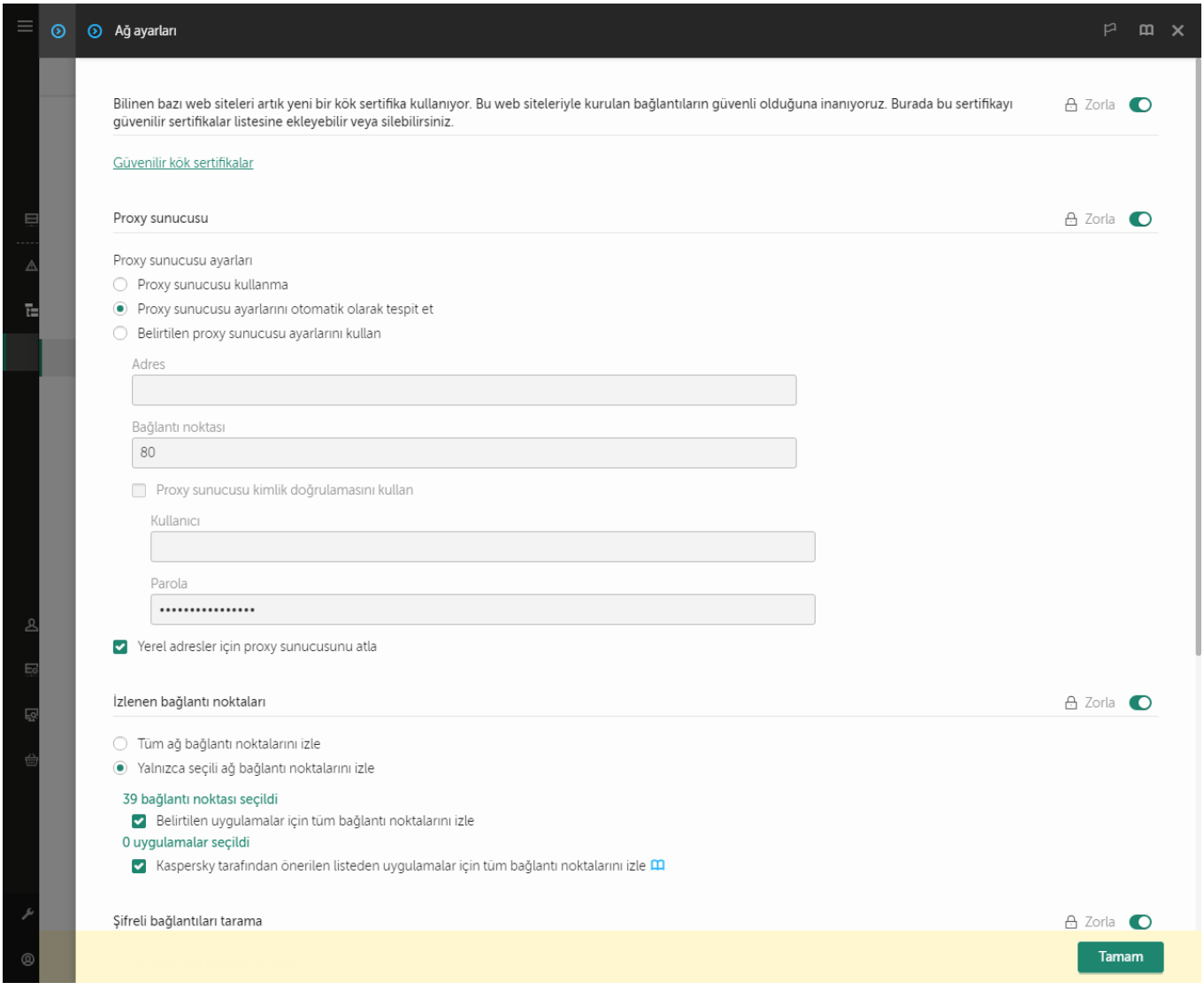
1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

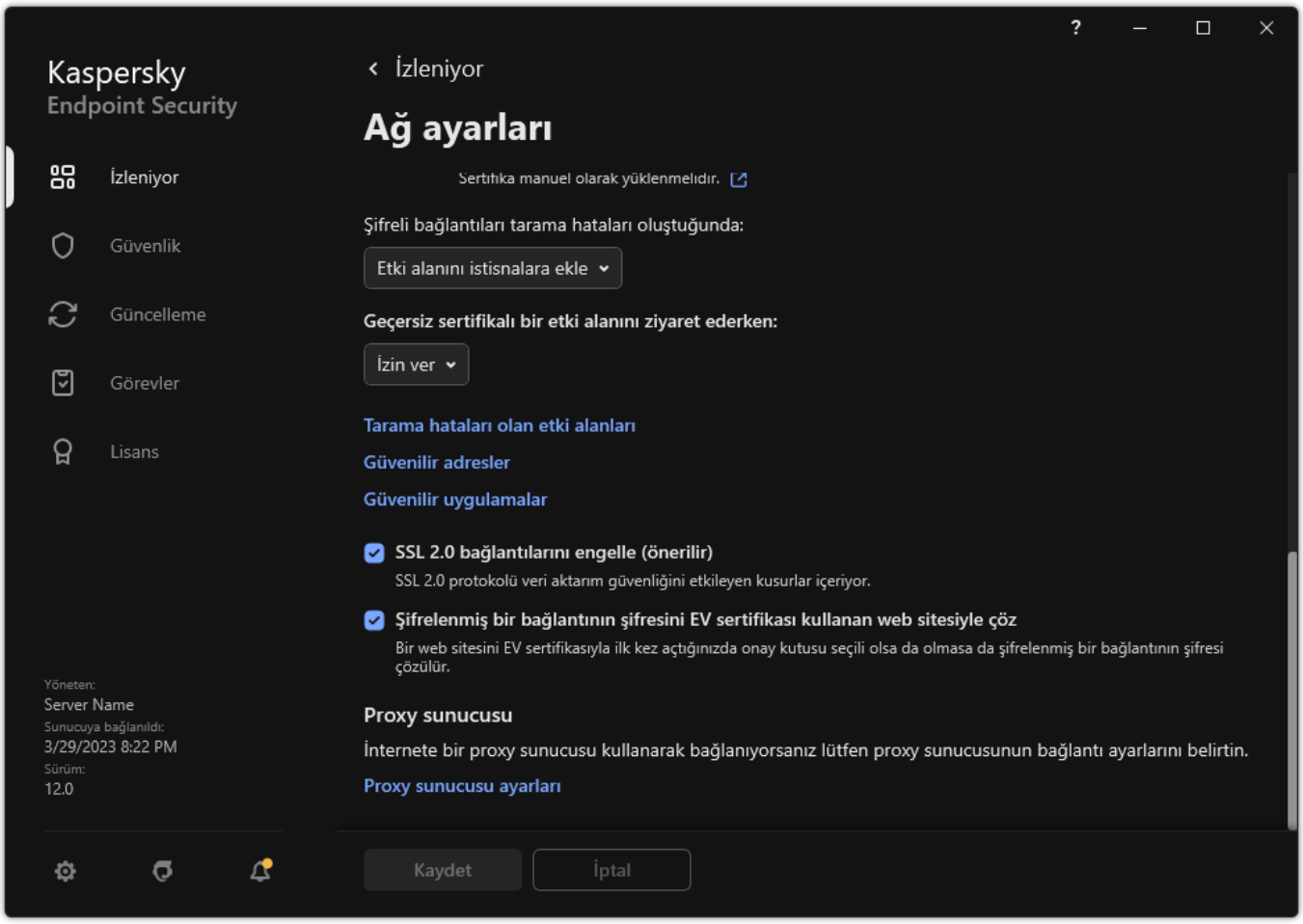
4. **Genel Ayarlar** → **Ağ ayarları** bölümüne gidin.



5. **Proxy sunucusu ayarları** bloğunda **Yerel adresler için proxy sunucusunu atla** seçimini yapın.
6. Değişikliklerinizi kaydedin.

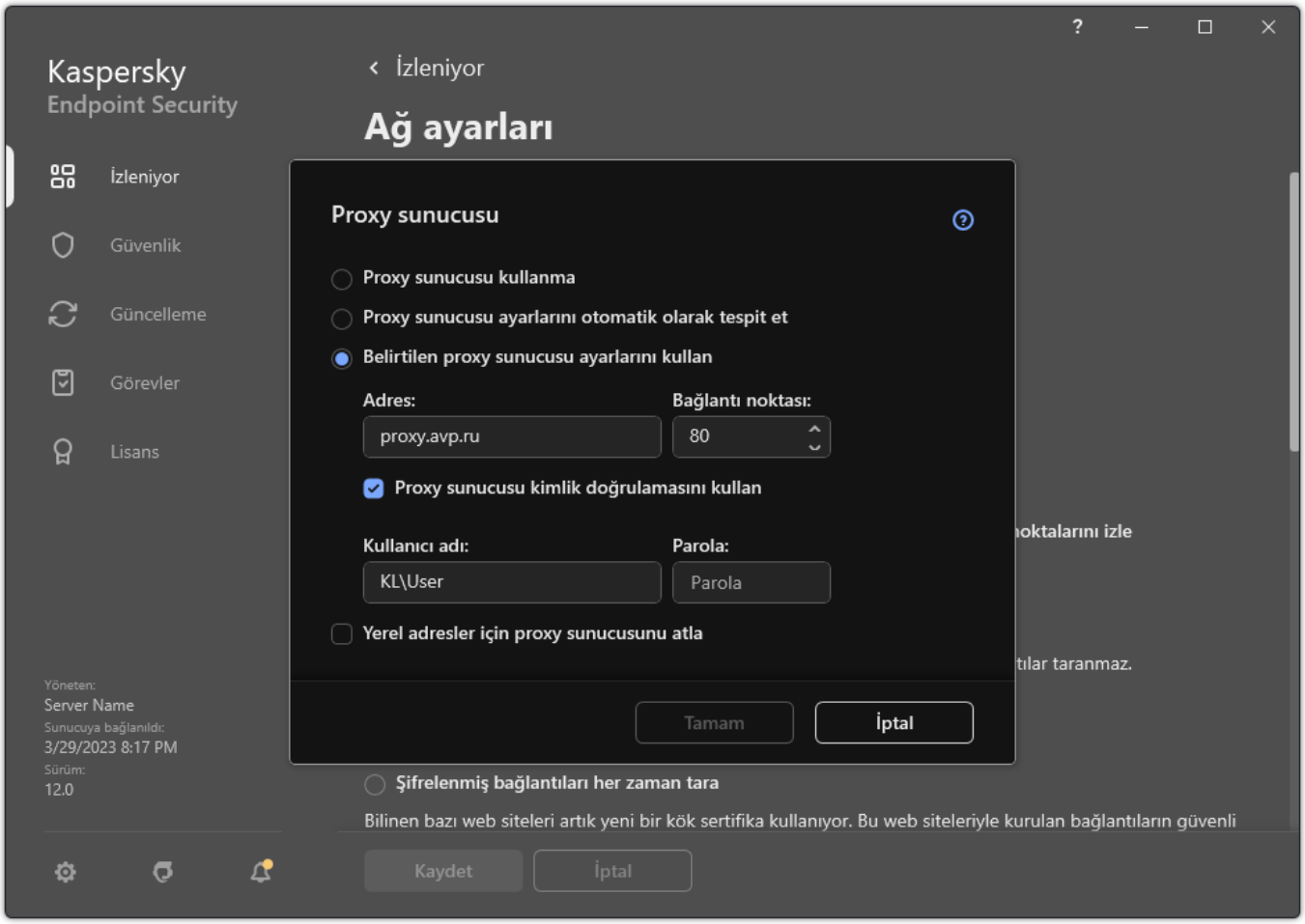
Proxy sunucusu ayarlarını uygulama arabiriminde yapılandırmak için:

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:

   - **Proxy sunucusu ayarlarını otomatik olarak tespit et**.

     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. Proxy sunucusuda kimlik doğrulamasını etkinleştirmek istiyorsanız, **Proxy sunucusu kimlik doğrulamasını kullan** onay kutusunu seçin ve kullanıcı hesabı kimlik bilgilerinizi girin.

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.

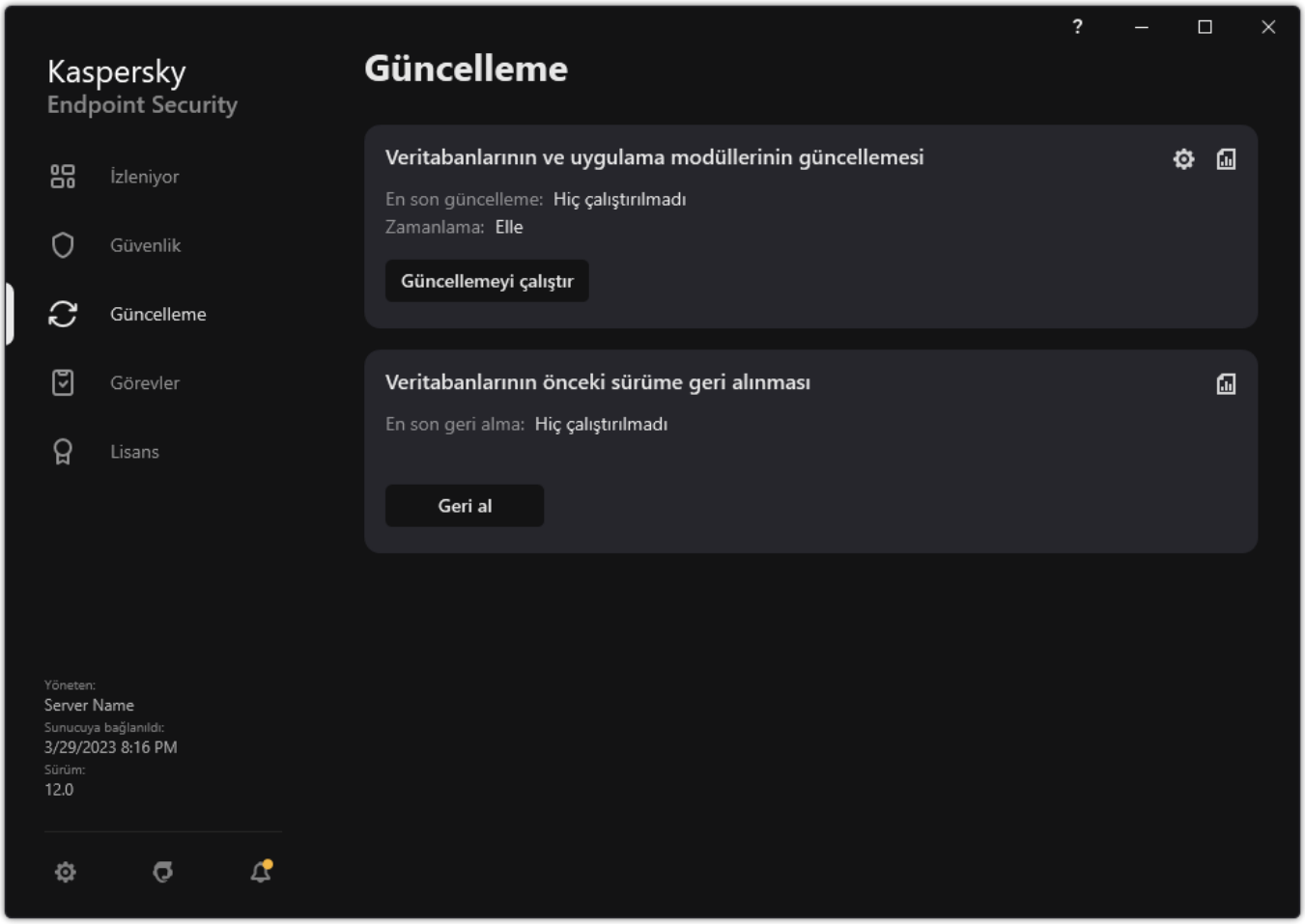
Son güncellemeyi geri alma

Veritabanları ve uygulama modülleri ilk kez güncellendikten sonra, veritabanları ve uygulama modüllerini önceki sürümlere geri alma işlevi mevcut olur.

Kullanıcı güncelleme işlemine her başladığında Kaspersky Endpoint Security, mevcut veritabanları ve uygulama modüllerinin bir yedekleme kopyasını oluşturur. Bu, gerektiğinde veritabanlarını ve uygulama modüllerini önceki sürümlerine geri almanıza olanak tanır. Son güncellemeyi geri almak, örneğin yeni veritabanı Kaspersky Endpoint Security'nin güvenli bir uygulamayı engellemesine neden olan geçersiz bir imza içerdiğinde faydalı olabilir.

Son güncellemeyi geri almak için:

1. Ana uygulama penceresinde, **Güncelleme** düğmesine tıklayın.



Yerel güncelleme görevleri

2. **Veritabanlarının önceki sürüme geri alınması** kutucuğunda, **Geri al** düğmesine tıklayın.

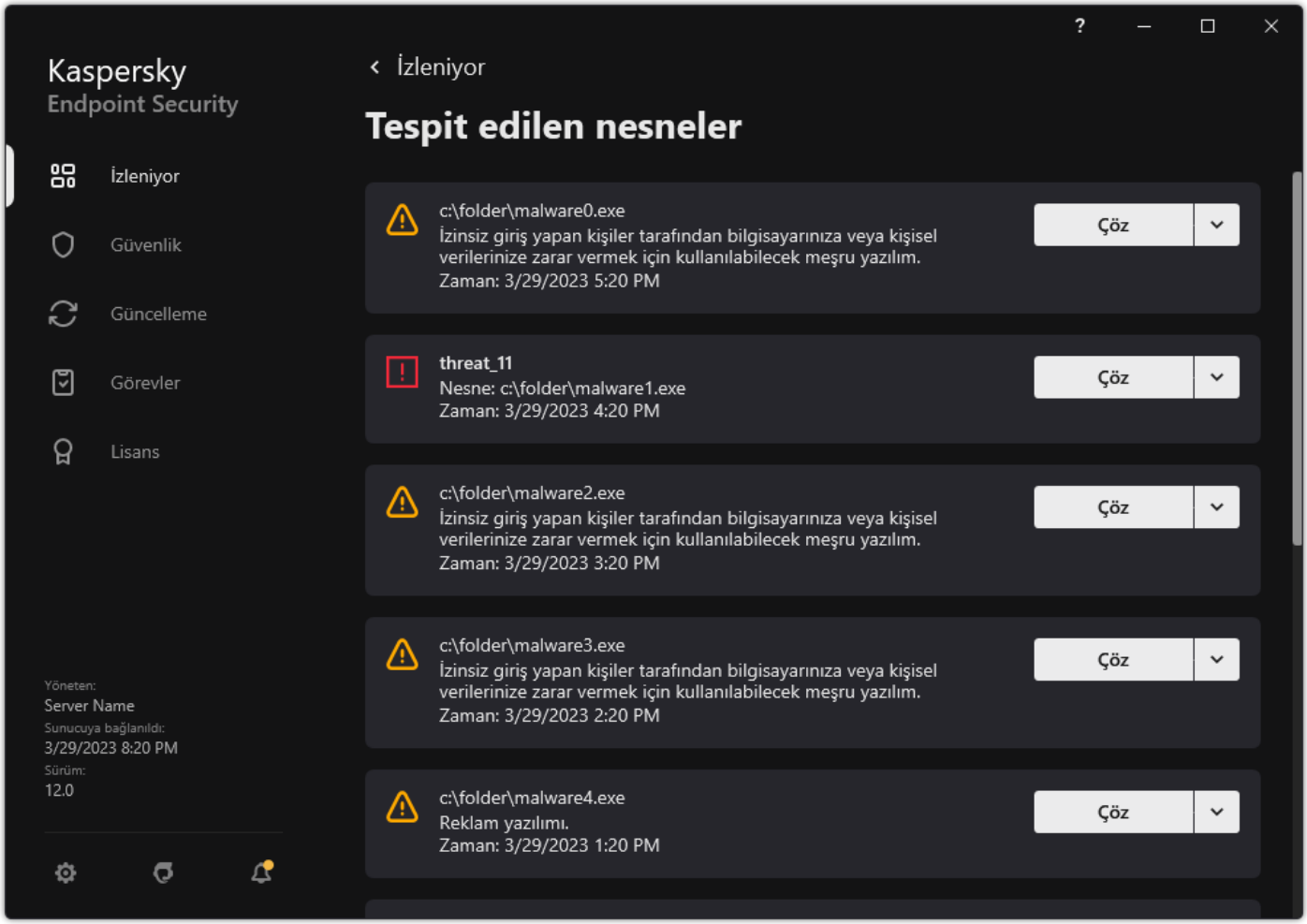
Kaspersky Endpoint Security, son veritabanı güncellemesini geri almaya başlayacak. Uygulama geri alma ilerlemesini, indirilen dosyaların boyutunu ve güncelleme kaynağını gösterecektir. **Güncellemeyi durdur** düğmesine tıklayarak görevi istediğiniz zaman durdurabilirsiniz.

Basitleştirilmiş uygulama arabirimi görüntülendiğinde geri alma 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 geri alma görevini seçerek başlatın.
   - Çalışan bir geri alma görevini seçerek durdurun.
   - Duraklatılmış bir geri alma görevini seçerek sürdürün veya yeniden başlatın.

Etkin tehditlerle çalışma

Kaspersky Endpoint Security bazı nedenlerle işlemediği dosyalar hakkında bilgi kaydeder. Bu bilgiler, etkin tehditler listesine olaylar biçiminde kaydedilir (aşağıdaki resme bakın). 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.

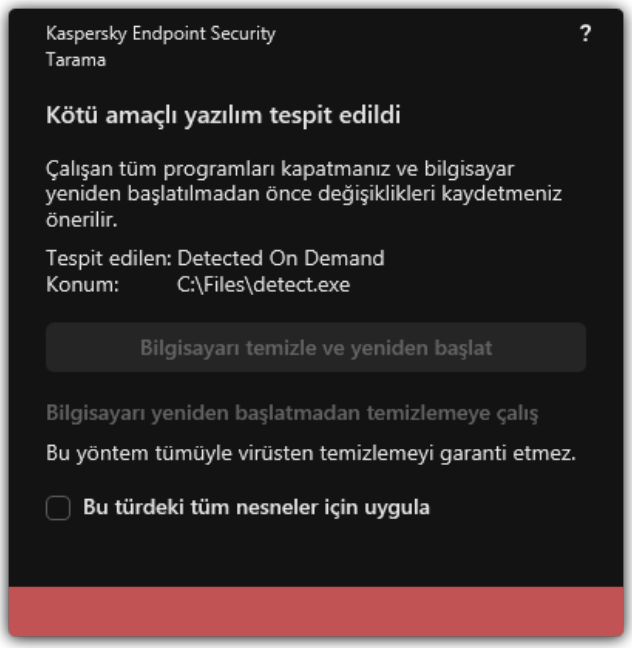


Etkin tehditlerin listesi

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 yüzden kullanıcı etkin bir tehdidi temizlemek için bir eylem seçemez. 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.

Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma

Kaspersky Endpoint Security bir kötü amaçlı yazılımın çalışmasını durduramadığında, Gelişmiş Temizleme teknolojisini kullanabilirsiniz. Gelişmiş Temizleme teknolojisi, çok fazla bilgisayar kaynağı kullandığından varsayılan olarak devre dışı durumdadır. Dolayısıyla, Gelişmiş Temizlemeyi sadece etkin tehditlerle çalışma sırasında etkinleştirebilirsiniz.

Gelişmiş Temizleme, iş istasyonları ve sunucular için farklı çalışır. Teknolojiyi sunucularda kullanmak için *Kötü Amaçlı Yazılım Taraması* görevinin özelliklerinden gelişmiş temizlemeyi derhal çalıştırmayı 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'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. **İşletim modu** bloğunda, Gelişmiş Temizleme teknolojisini etkinleştirmek veya devre dışı bırakmak için **Gelişmiş Temizleme teknolojisini etkinleştir** onay kutusunu işaretleyin ya da işaretini kaldırın.

6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Gelişmiş Temizleme teknolojisi etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

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

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel ayarlar** → **Uygulama Ayarları** seçimini yapın.

5. **İşletim modu** bloğunda, Gelişmiş Temizleme teknolojisini etkinleştirmek veya devre dışı bırakmak için **Gelişmiş Temizleme teknolojisini etkinleştir** onay kutusunu işaretleyin ya da işaretini kaldırın.

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. **İşletim modu** 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, Etkin Temizleme devam ederken çoğu işletim sistemi özelliğini kullanamaz. Temizleme tamamlandığında bilgisayar yeniden başlatılır.

Etkin tehditlerin işlenmesi

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 uygulanacak eylem olarak **Bildir** ayarlıdır. Ardından, ekranda virüslü dosya bildirimi görüntülendiğinde, kullanıcı **Atla** 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, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.
   - **Sil**.

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, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.
   - **Sil**.

Uygulama arabiriminde bir tehdit nasıl işlenir

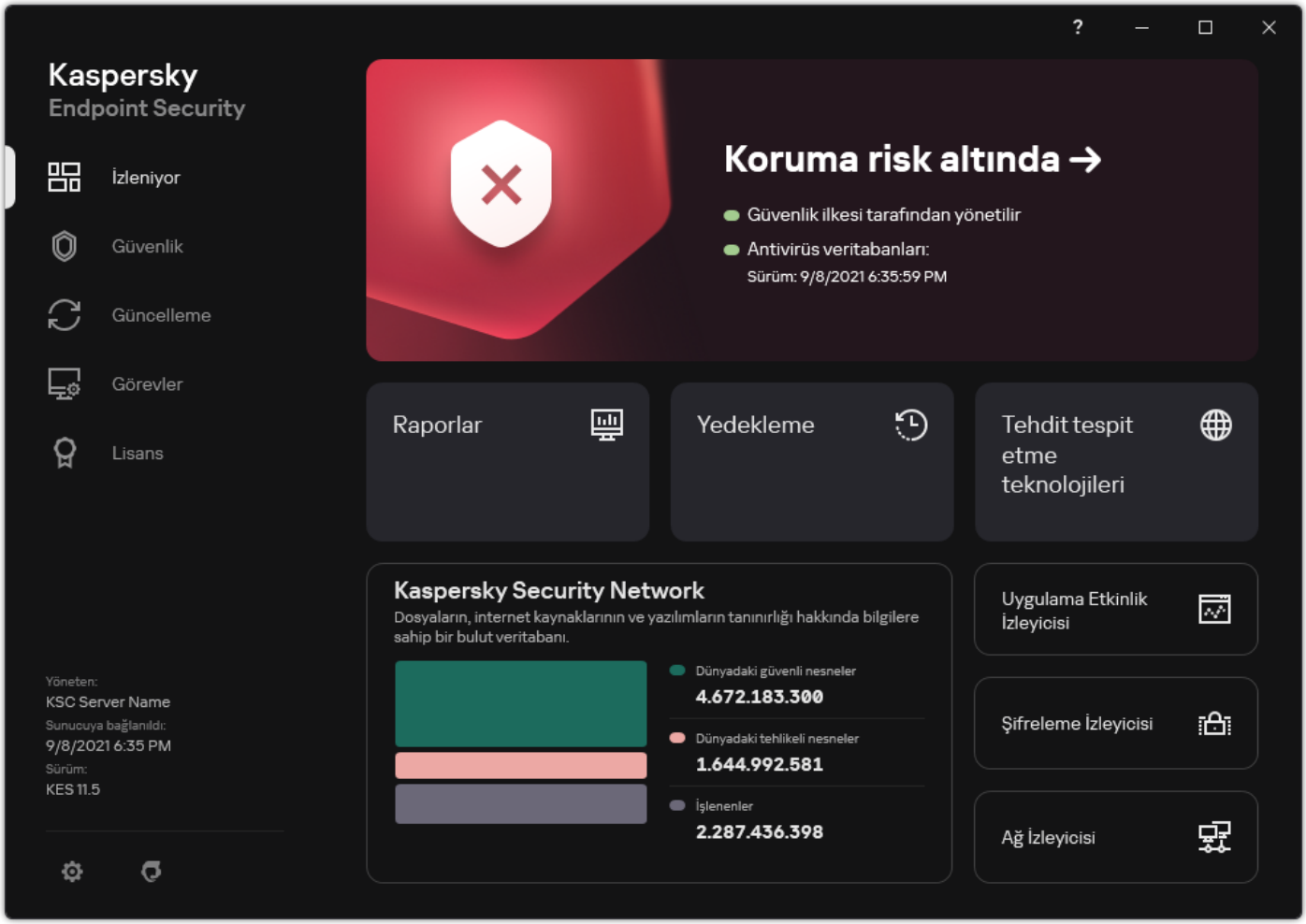
1. Ana uygulama penceresinde, **İzleniyor** bölümündeki **Koruma risk altında** kutucuğuna tıklayın.

   Etkin tehditler listesi açılır.

2. İşlemek istediğiniz nesneyi seçin.

3. Tehdit karşısında ne yapılmasını istediğinizi seçin:

   - **Çöz**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.
   - **İstisnalara ekle**. Bu eylem seçilirse, Kaspersky Endpoint 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 işaretlenirse, Kaspersky Endpoint Security Kaspersky Virüs Ansiklopedisi web sitesini açar.



Bir tehdit algılandığında ana uygulama penceresi

Bilgisayar koruması

Dosya Tehdidi Koruması

Dosya Tehdidi Koruması bileşeni, bilgisayarın dosya sistemine virüs bulaşmasını önlemenizi sağlar. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni kalıcı olarak bilgisayarın RAM'inde bulunur. Bileşen bilgisayarın tüm sürücülerindeki ve bağlı sürücülerdeki 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.

İçerikleri OneDrive bulut alanında yer alan bir dosyaya erişim sağlamayı denediğinizde, Kaspersky Endpoint Security dosya içeriklerini 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 elle yapılandırabilirsiniz. Güvenlik düzeyi ayarlarını değiştirirseniz önerilen güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

Dosya Tehdidi Koruması bileşenini etkinleştirmek veya devre dışı bırakmak için:

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. Önerilen güvenlik düzeyi için ayarların değerleri aşağıdaki tabloda verilmiştir.
     - **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.

     Önerilen güvenlik düzeyini geri yükle düğmesine tıklayarak önceden ayarlanmış güvenlik seviyelerinin değerlerini geri yükleyebilirsiniz.
5. 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 tarama 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. Kaspersky Endpoint Security, onay kutusunun seçili olup olmadığına bakılmaksızın, boyutu 1 MB altında olan küçük ofis 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 uygulanacak eylem	**Temizle; temizleme başarısız olursa sil**	Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları 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 uygulanacak eylem** bloğunda gereken seçeneği seçin:
   - **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.
   - **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme mümkün değilse Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.
   - **Engelle**. Bu seçenek işaretlenirse Dosya Tehdidi Koruması bileşeni, virüs bulaşmış tüm dosyaları temizlemeye 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. Koruma kapsamına eklemek için bir nesne seçin.

   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 tarama 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 dosya taraması** bloğunda, taramak istediğiniz bileşik dosyaların türünü belirtin: arşivler, dağıtım paketi veya Office biçimlerindeki dosyalar.

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.

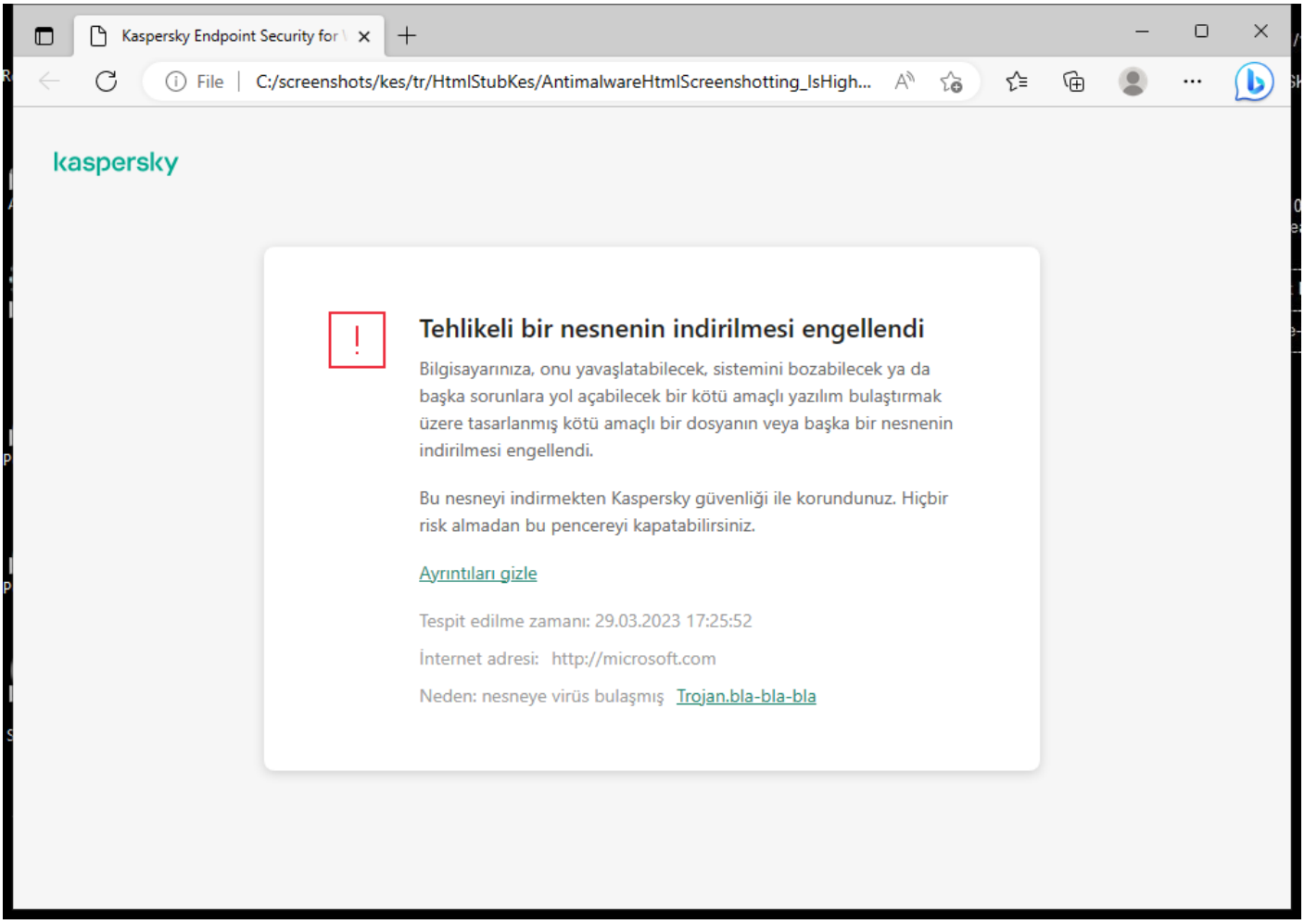
Web Tehdidi Koruması

Web Tehdidi Koruması bileşeni, İnternet üzerinden zararlı dosyaların indirilmesini önler ve aynı zamanda zararlı ve kimlik avı amaçlı web sitelerini 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. Kaspersky Endpoint Security'nin izleyeceği bağlantı noktalarını belirleyebilir ya da tüm bağlantı noktalarını seçebilirsiniz.

HTTPS trafiğini izleme için şifrelenmiş bağlantı taramasını etkinleştirin.

Bir kullanıcı kötü amaçlı veya kimlik avı yapan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller ve bir uyarı gösterir (aşağıdaki şekle bakın).



Web sitesine erişim engellendi mesajı

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'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. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Web Tehdidi Koruması** kutucuğunu işaretleyin.
6. Bileşeni etkinleştirdiyseniz, **Güvenlik düzeyi** bloğunda aşağıdakilerden birini yapın:
   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz, kaydırma çubuğuyla seçin.
     - **Yüksek**. Web Tehdidi Koruması bileşeninin bilgisayarın HTTP ve FTP iletişim kuralları aracılığıyla aldığı web trafiğinde maksimum tarama yaptığı güvenlik düzeyidir. Web Tehdidi Koruması, uygulama veritabanlarının tam setini kullanarak tüm İnternet trafiği nesnelerini ayrıntılı olarak tarar ve mümkün olan en ayrıntılı sezgisel analizi gerçekleştirir.
     - **Önerilen**. Kaspersky Endpoint Security'nin 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.

     Varsayılan olarak düğmesine tıklayarak önceden ayarlanmış güvenlik düzeylerinin değerlerini geri yükleyebilirsiniz.
7. **Tehdit algılandığında uygulanacak 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.
   - **Bildir**. 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.
8. Değişikliklerinizi kaydedin.

[Web Console'da ve Cloud Console'da Web Tehdidi Koruması bileşenini etkinleştirme veya devre dışı bırakma]

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması → Web Tehdidi Koruması** bölümüne gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Web Tehdidi Koruması** geçiş düğmesini kullanın.
6. **Tehdit algılandığında uygulanacak 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.
   - **Bildir**. 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 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 bilgisayarın HTTP ve FTP iletişim kuralları aracılığıyla aldığı web trafiğinde maksimum tarama yaptığı güvenlik düzeyidir. Web Tehdidi Koruması, uygulama veritabanlarının tam setini kullanarak tüm İnternet trafiği nesnelerini ayrıntılı olarak tarar ve mümkün olan en ayrıntılı sezgisel analizi gerçekleştirir.
     - **Önerilen**. Kaspersky Endpoint Security'nin 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.

     Önerilen güvenlik düzeyini geri yükle düğmesine tıklayarak önceden ayarlanmış güvenlik seviyelerinin değerlerini geri yükleyebilirsiniz.
5. **Tehdit algılandığında uygulanacak 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.
   - **Bildir**. 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
İnternet 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.
İnternet 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	**Normal**	Bu teknoloji, Kaspersky uygulama veritabanlarının güncel sürümünü kullanarak tespit

kullan (Web Tehdidi Koruması)	**tarama**	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 uygulanacak 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, 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'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, adreslerin kötü amaçlı internet adresleri veritabanına göre kontrol edilmesini etkinleştirmek veya devre dışı bırakmak için bu penceredeki **Tarama yöntemleri** bloğundan **İnternet adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et** onay kutusunu işaretleyin ya da işaretini kaldırın.
7. 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 **İnternet 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'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. **Tarama yöntemleri** bloğunda, uygulamanın web trafiğini virüslere ve diğer zararlı yazılımlara karşı tararken sezgisel analiz kullanmasını istiyorsanız **Sezgisel Analiz kullan** onay kutusunu seçin.
7. 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.
8. 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'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, Kimlik Avı Korumasını etkinleştirmek veya devre dışı bırakmak için bu penceredeki **Kimlik Avı Koruması ayarları** bloğundan **İnternet 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.

7. 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.

8. 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 **İnternet 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 internet trafiğini tarama** onay kutusunu seçin.

   Onay kutusu işaretlenirse 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. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir güvenilir internet adresi nasıl eklenir

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması** → **Web Tehdidi Koruması** bölümüne gidin.
5. **Güvenilir internet adresleri** bloğunda, **Güvenilir adreslerin internet trafiğini tarama** onay kutusunu işaretleyin.

   Onay kutusu işaretlenirse 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.
6. 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.
7. 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.

   Onay kutusu işaretlenirse 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 bağlantı noktaları 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'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 internet adreslerinin listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz güvenilir web adreslerini seçin. Birden fazla bağlantı noktası 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.
8. 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.
9. Değişikliklerinizi kaydedin.

Güvenilir web adreslerinin bir listesini Web Console ve Cloud Console'da dışa akarma ve içe aktarma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması** → **Web Tehdidi Koruması** bölümüne gidin.
5. **Güvenilir adresler** bloğundaki istisnalar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz güvenilir web adreslerini seçin.
   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.

6. **Güvenilir adresler** bloğundaki istisnalar 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.

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

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 Tehdit Koruması uzantısı Outlook 2010, 2013, 2016 ve 2019 ile çalışmayı 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. Posta Tehdidi Koruması için Kaspersky Endpoint Security, farklı ayar grupları uygular. 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.

Posta Tehdidi Koruması bileşenini etkinleştirmek veya devre dışı bırakmak için:

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**. Kaspersky Endpoint Security 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.

  Önerilen güvenlik düzeyini geri yükle düğmesine tıklayarak önceden ayarlanmış güvenlik seviyelerinin değerlerini geri yükleyebilirsiniz.

5. 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. E-postalar, Microsoft Outlook için uzantı kullanılarak taranıyorsa Önbellekli Exchange Modu'nun 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. Kaspersky Endpoint Security, 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	**Temizle; temizleme**	Alınan veya gönderilen bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse Kaspersky Endpoint Security virüslü

uygulanacak eylem	**başarısız olursa sil**	nesneyi siler. Kaspersky Endpoint Security, 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 uygulanacak eylem** bloğunda Kaspersky Endpoint Security'nin virüslü bir mesajı tespit ettiğinde gerçekleştireceği eylemi seçin:
   - **Temizle; temizleme başarısız olursa sil**. Alınan veya gönderilen bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse Kaspersky Endpoint Security virüslü nesneyi siler. Kaspersky Endpoint Security, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*.
   - **Temizle; temizleme başarısız olursa engelle**. Alınan bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, Kaspersky Endpoint Security mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Gönderilen bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, Kaspersky Endpoint Security mesajın iletimini engeller ve posta istemcisi bir hata görüntüler.
   - **Engelle**. Gelen bir mesajdaki virüslü bir nesne temizlenemezse, Kaspersky Endpoint Security mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Gönderilen bir mesajdaki virüslü bir nesne temizlenemezse, Kaspersky Endpoint Security 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. Kaspersky Endpoint Security, 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 Kaspersky Endpoint Security 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**. 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.

5. Değişikliklerinizi kaydedin.

E-posta mesajları ek filtrelemesi

Ek filtresi işlevselliği, 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. 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 pencerede, **Ek filtresi** sekmesini seçin.

7. Uzantılar listesini dışa aktarmak için:

   a. Dışa aktarmak istediğiniz uzantıları seçin. Birden fazla bağlantı noktası 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.

8. 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.

9. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bir ek filtre uzantıları listesi nasıl dışa ve içe aktarılır

1. Web Console'un ana penceresinde **Aygıtlar → İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Temel Tehdit 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.

Microsoft Office Outlook'ta e-postaları tarama

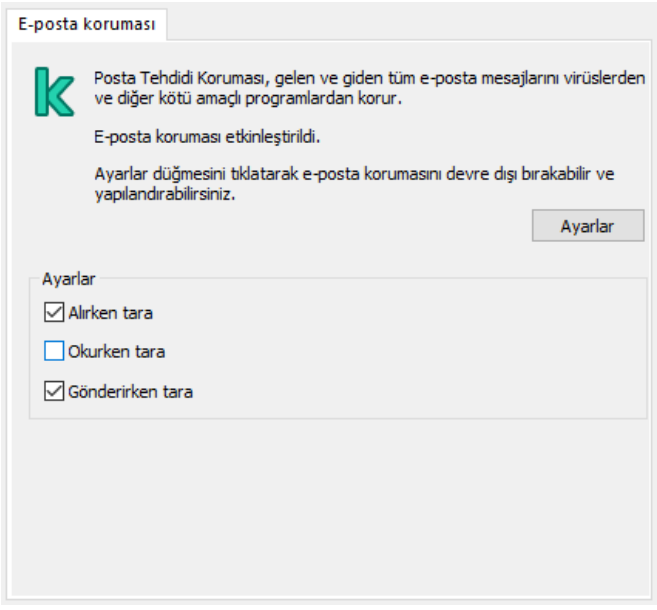
Kaspersky Endpoint Security'nin yüklenmesi sırasında Posta Tehdidi Koruması eklentisi, Microsoft Office Outlook'a eklenir (bundan sonra Outlook olarak ifade edilecektir). Posta Tehdidi Koruması bileşeninin ayarlarını Outlook'tan açmanıza ve e-posta mesajlarında virüs ve diğer tehditlerin ne zaman taranacağını belirtmenize olanak tanır. Outlook'un Posta Tehdidi Koruması eklentisi, POP3, SMTP, NNTP, IMAP ve MAPI iletişim kuralları üzerinden aktarılan gelen ve giden mesajları tarayabilir. Kaspersky Endpoint Security ayrıca diğer e-posta istemcileri ile çalışmayı da destekler (Microsoft Outlook Express®, Windows Mail ve Mozilla™ Thunderbird™ dahil).

Posta Tehdit Koruması uzantısı Outlook 2010, 2013, 2016 ve 2019 ile çalışmayı destekler.

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.

Outlook'ta gelen mesajlar öncelikle Posta Tehdidi Koruması bileşeni tarafından (Kaspersky Endpoint Security'nin arabiriminde POP3, SMTP, NNTP ve IMAP trafiği 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.

E-postalar, Microsoft Outlook için Posta Tehdidi Koruması uzantısı kullanılarak taranıyorsa Önbellekli Exchange Modu'nun kullanılması önerilir. Önbelleklenmiş Exchange modu ve nasıl kullanıldığıyla ilgili öneriler hakkında daha ayrıntılı bilgi için Microsoft Bilgi Bankası 'na bakın.

Outlook için Posta Tehdidi Koruması uzantısının çalışma modunu yapılandırmak için:

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. **Bağlanabilirlik** bloğunda, **Ayarlar** düğmesine tıklayın.
7. **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.
8. Değişikliklerinizi kaydedin.

Ağ Tehdidi Koruması

Ağ Tehdidi Koruması bileşeni, gelen ağ trafiğinde ağ saldırılarında tipik olarak görülen etkinliği tarar. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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. Gerekirse Ağ Tehdidi Koruması'nı devre dışı bırakabilirsiniz.

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

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Ağ Tehdidi Koruması** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak, Ağ Tehdidi Koruması etkinleştirilirse, Kaspersky Endpoint Security, ağ saldırılarına özgü aktiviteler için gelen ağ trafiğini tarar. Kaspersky Endpoint Security kullanıcının bilgisayarına gerçekleştirilen bir ağ saldırısı tespit ederse, saldıran bilgisayarla ağ bağlantısını engeller.

Saldırıda bulunan bir bilgisayarı engellemek

Saldırıda bulunan bir bilgisayarı engellemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması**'nı seçin.
3. **Saldırıda bulunan cihazları N dakikaboyunca engelle** onay kutusunu seçin.

Onay kutusu işaretlenirse Ağ Tehdidi Koruması bileşeni saldıran bilgisayarı engellenen 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.

4. **Saldırıda bulunan cihazları N dakika boyunca engelle** onay kutusunun sağındaki 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.

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.

Engelleme istisnalarının adreslerini yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Ağ Tehdidi Koruması**'nı seçin.
3. **İstisnaları yönet** bağlantısını tıklayın.
4. Açılan pencerede **Ekle** düğmesine tıklayın.
5. Ağ saldırılarının engellenmemesi gereken bilgisayarın IP adresini girin.
6. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security, istisnalar listesindeki cihazlardan gelen etkinliği izlemez.

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'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. Kurallar listesini dışa aktarmak için:
   a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla bağlantı noktası seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
   Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.

b. **Dışa aktar** bağlantısına 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.

7. 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.

8. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bir istisnalar listesinş dışa aktarma ve içe aktarma

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

İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması** → **Ağ Tehdidi Koruması** bölümüne gidin.
5. **Ağ Tehdidi Koruması ayarları** bloğunda **İstisnalar ve tespit edilen nesneler** bağlantısına tıklayın.

İstisnalar listesi açılır.

6. Kurallar listesini dışa aktarmak için:

a. Dışa aktarmak istediğiniz istisnaları seçin.

b. **Dışa aktar**'a tıklayın.

c. Yalnızca seçili istisnaları veya tüm istisnalar listesini dışa aktarmak istediğinizi onaylayın.

d. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

e. Dosyaya kaydet.

Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.

7. 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.

8. Değişikliklerinizi kaydedin.

Ağ saldırılarına karşı korumayı 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.

- *Bağlantı Noktası Tarama* saldırısı, bilgisayardaki UDP bağlantı noktalarını, TCP bağlantı noktalarını ve ağ hizmetlerini taramaktan oluşur. Bu saldırı, saldırganın daha tehlikeli ağ saldırıları gerçekleştirmeden önce bilgisayarın güvenlik açığı düzeyini belirlemesine olanak tanır. Bağlantı Noktası Tarama sayesinde saldırgan aynı zamanda bilgisayardaki işletim sistemini tanımlayabilir ve bu işletim sistemi için uygun ağ saldırılarını seçebilir.

- *MAC aldatma 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, Bağlantı Noktası Tarama ve MAC aldatma saldırılarını izlemez.

Türe göre ağ saldırılarına karşı korumayı yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → Ağ Tehdidi Koruması**'nı seçin.
3. Bu saldırıların algılanmasını etkinleştirmek veya devre dışı bırakmak için **Bağlantı noktası tarama ve ağ taşma olaylarına saldırı olarak davran** geçiş düğmesini kullanın.

   Bu işlev etkinleştirilirse Kaspersky Endpoint Security, bağlantı noktası 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. **MAC Kafesleme Koruması** geçiş düğmesini kullanın.
5. **Bir MAC kimlik sahtekarlığı saldırısı tespit edildiğinde** bloğunda, aşağıdaki seçeneklerden birini seçin:
   - **Bildir**.
   - **Engelle**.
6. Değişikliklerinizi kaydedin.

Güvenlik Duvarı

Güvenlik Duvarı, İnternet veya yerel ağ üzerinde çalışırken bilgisayara izinsiz bağlantılar kurulmasını 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 bağlantı noktası açar. Hangi bağlantı noktalarının açılacağı bilgisayarın rolüne bağlıdır (örneğin, dağıtım noktası). Bilgisayarda açılacak bağlantı noktaları 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 bağlantı noktaları 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 durumları

Güvenlik Duvarı, ağ bağlantısının durumuna bağlı olarak ağ etkinliklerini kontrol etmenize olanak tanır. Kaspersky Endpoint Security ağ bağlantısı durumunu bilgisayarın işletim sisteminden alır. İşletim sistemindeki ağ bağlantısının durumu, bağlantının ayarlanması sırasında kullanıcı tarafından ayarlanır. Kaspersky Endpoint Security ayarlarından ağ bağlantısı durumunu değiştirebilirsiniz. Güvenlik Duvarı ağ etkinliklerini işletim sistemindeki ağ durumuna göre değil Kaspersky Endpoint Security ayarlarındaki ağ durumuna göre izleyecektir.

Ağ bağlantısı, aşağıdaki durum türlerinden birine sahip olabilir:

- **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 İnternet'e *Ortak ağ* durumunu atar. İnternet'in durumunu 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'nın etkinleştirilmesi veya devre dışı bırakılması

Varsayılan olarak Güvenlik Duvarı etkinleştirilmiştir ve optimum modda çalışır.

Güvenlik Duvarı'nı etkinleştirmek veya devre dışı bırakmak için:

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, gelen ağ trafiğinde ağ saldırılarında tipik olarak görülen etkinliği tarar.

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 durumunu değiştirme

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

Ağ bağlantısı durumunu 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. Durumunu değiştirmek istediğiniz ağ bağlantısını seçin.
5. **Ağ türü** sütununda ağ bağlantısının durumunu 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 bırakıldı* durumundaki ağ paketi kuralları listesinde görülmesini önlemek için bir ağ paketi kuralını kaldırabilirsiniz.

Bir ağ paketi kuralını kaldırma

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.

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

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** sekmesini seçin.

   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 elle 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**'ye tıklayın.

   Paket kuralı özellikleri açılır.
5. Paket kuralı için **Etkin** durumu ayarlayın.
6. Ağ hizmetinin adını **Ad** alanına elle 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'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** → **Güvenlik Duvarı**'nı seçin.
5. **Güvenlik duvarı ayarları** bloğunda **Ayarlar** düğmesine tıklayın.

   Ağ paketi kuralları listesi ve uygulama ağ kuralları listesi açılır.

6. **Ağ paketi kuralları** sekmesini seçin.

   Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

7. **Ekle**'ye tıklayın.

   Bu, paket kuralı özelliklerini açar.

8. Ağ hizmetinin adını **Ad** alanına elle girin.
9. 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.

10. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.
11. Yeni ağ kuralını kaydet.
12. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.
13. 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 ve Cloud Console'da bir ağ paketi kuralı nasıl oluşturulur

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

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
5. **Güvenlik Duvarı Ayarları** bloğunda, **Ağ paketi kuralları** bağlantısına tıklayın.

Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.

6. **Ekle**'ye tıklayın.

   Bu, paket kuralı özelliklerini açar.

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

8. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

   Şablon seç 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 **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. Paket kuralını etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş düğmesini kullanın.

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.
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 virgülle ayrılmış bağlantı noktası numaralarını belirtebilirsiniz.
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 bağlantısının kullanıcı bilgisayarı tarafından mı uzak bilgisayar tarafından mı başlatıldığına bakmaksızın, ağ kuralını 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 denetimini yaşam sürelerine (TTL) göre kısıtlayın.
Uzak adres	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.

Kaspersky Endpoint Security, 11.7.0 sürümünden itibaren DNS adlarını destekler. 11.6.0 veya daha eski sürümler için bir DNS adı belirlediğinizde, Kaspersky Endpoint Security ilgili kuralı tüm adreslere uygulayabilir.

Yerel adres

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.

Kaspersky Endpoint Security, 11.7.0 sürümünden itibaren DNS adlarını destekler. 11.6.0 veya daha eski sürümler için bir DNS adı belirlediğinizde, Kaspersky Endpoint Security ilgili kuralı tüm adreslere uygulayabilir.

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'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** → **Güvenlik Duvarı**'nı seçin.
5. **Güvenlik duvarı ayarları** bloğunda **Ayarlar** düğmesine tıklayın.
   Ağ paketi kuralları listesi ve uygulama ağ kuralları listesi açılır.
6. **Ağ paketi kuralları** sekmesini seçin.
7. Ağ paketi kuralları listesini dışa aktarmak için:
   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla bağlantı noktası 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.

8. 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.

9. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da ağ paketi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
5. **Güvenlik Duvarı Ayarları** bloğunda, **Ağ paketi kuralları** bağlantısına tıklayın.
6. Ağ paketi 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. 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.

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` – **Requests to DNS server over TCP**. `101` – **Requests to DNS server over UDP**. `102` – **Sending email messages**. `110` – **Any network activity** (Trusted networks). `125` – **Any network activity** (Local networks). `130` – **Remote Desktop network activity**. `131` – **TCP connections through local ports**. `132` – **UDP connections through local ports**. `133` – **Incoming TCP stream**. `134` – **Incoming UDP stream**. `137` – **ICMP Destination Unreachable incoming responses**. `138` – **ICMP Echo Reply incoming packets**. `140` – **ICMP Time Exceeded incoming responses**. `142` – **Incoming ICMP stream**. `266` – **ICMPv6 Echo Request incoming packets**.
`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` – **Any address**. `50` – **Trusted networks**. `51` – **Local networks**. `52` – **Public networks**. `<Network Identifier>` – **Addresses from the list** (adresler manuel olarak tanımlanır).
`AccessFlag`	**Action** parametresinin değeri.	`0` – **Allow**. `2` – **By application rules**. `3` – **Block**. `4` – **Allow** ve **Log events**. `6` – **By application rules** ve **Log events**. `7` – **Block** ve **Log events**.

`</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`	**Remote ports** parametresinin değeri.	Uzak bağlantı noktası aralıklarının listesi.
`LocalPorts`	**Local ports** parametresinin değeri.	Yerel bağlantı noktası aralıklarının listesi.
`AdapterBindings`	**Network adapters** parametresinin değeri.	`IpAddresses` – **IP addresses** parametresinin değeri. `MacAddresses` – **MAC addresses** parametresinin değeri. `AdapterName` – ağ bağdaştırıcısının adı.

		`InterfaceType` – **Interface type** parametresinin değeri: • `0` – **Other**. • `1` – **LoopBack**. • `2` – **Wired network (Ethernet)**. • `3` – **Wireless network (Wi-Fi)**. • `4` – **Tunnel**. • `5` – **PPP connection**. • `6` – **PPPoE connection**. • `7` – **VPN connection**. • `8` – **Modem connection**.
`unique`	Yapının dahili kimliği.	Tamsayı Bu parametrenin değiştirilmeden bırakılması önerilir.
`Proto`	**Protocol** parametresinin değeri.	`0` – devre dışı. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
Yön	**Direction** parametresinin değeri.	`1` – **Inbound (packet)**. `2` – **Outbound (packet)**. `3` – **Inbound / Outbound**. `4` – **Inbound**. `5` – **Outbound**.
`IcmpType`	**ICMP type** parametresinin değeri.	ICMP protokolü `0` – **Echo Reply** (ICMP) veya devre dışı. `3` – **Destination Unreachable** (ICMP). `4` – **Source Quench**. `5` – **Redirect**. `6` – **Alternate Host Address**. `8` – **Echo Request**. `9` – **Router Advertisement**. `10` – **Router Solicitation**. `11` – **Time Exceeded**. `12` – **Parameter Problem**. `13` – **Timestamp**. `14` – **Timestamp Reply**.

15 – Information Request.

16 – Information Reply.

17 – Address Mask Request.

18 – Address Mask Reply.

30 – Traceroute.

31 – Datagram Conversion Error.

32 – Mobile Host Redirect.

33 – IPv6 Where-Are-You.

34 – IPv6 I-Am-Here.

35 – Mobile Registration Request.

36 – Mobile Registration Reply.

37 – Domain Name Request.

38 – Domain Name Reply.

40 – Photuris.

ICMPv6 protokolü

1 – Destination Unreachable.

2 – Packet Too Big.

3 – Time Exceeded.

4 – Parameter Problem.

128 – Echo Request.

129 – Echo Reply.

130 – Multicast Listener Query.

131 – Multicast Listener Report.

132 – Multicast Listener Done.

133 – Router Solicitation.

134 – Router Advertisement.

135 – Neighbor Solicitation.

136 – Neighbor Advertisement.

137 – Redirect Message.

138 – Router Renumbering.

139 – ICMP Node Information Query.

141 – Inverse Neighbor Discovery Solicitation Message.

142 – Inverse Neighbor Discovery Advertisement Message.

143 – Version 2 Multicast Listener Report.

144 – **Home Agent Address Discovery Request Message**.

145 – **Home Agent Address Discovery Reply Message**.

146 – **Mobile Prefix Solicitation**.

147 – **Mobile Prefix Advertisement**.

148 – **Certification Path Solicitation Message**.

149 – **Certification Path Advertisement Message**.

151 – **Multicast Router Advertisement**.

152 – **Multicast Router Solicitation**.

153 – **Multicast Router Termination**.

`IcmpCode`	**ICMP code** parametresinin değeri.	`0` – **Code 0** veya devre dışı. `1` – **Code 1**. `2` – **Code 2**.
`Flags`	Yapı özniteliği işaretçisi.	Tamsayı Bu parametrenin değiştirilmeden bırakılması önerilir.
`TTL`	**Time to live (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 bağlantı noktaları** sekmesini seçin.

   Ağ etkinliği sekmesinde, bilgisayardaki etkin tüm ağ bağlantıları görüntülenir. Hem giden hem de gelen ağ bağlantıları görüntülenir.

   Açık bağlantı noktaları sekmesinde, bilgisayarın açık bağlantı noktalarının tamamı listelenir.

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 elle 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 elle 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'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** → **Güvenlik Duvarı**'nı seçin.
5. **Güvenlik duvarı ayarları** bloğunda **Ayarlar** düğmesine tıklayın.
   Ağ paketi kuralları listesi ve uygulama ağ kuralları listesi açılır.
6. **Uygulama ağ kuralları** sekmesini seçin.
7. **Ekle**'ye tıklayın.
8. 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.
9. **Yenile** düğmesine tıklayın.
   Kaspersky Endpoint Security uygulamayı, yönetilen bilgisayarlardaki yüklü uygulamalar birleştirilmiş listesinde arar. Kaspersky Endpoint Security, arama kriterlerinizi karşılayan uygulamaların bir listesini görüntüler.
10. Gereken uygulamayı seçin.
11. **Seçilen uygulamayı güvenilirlik grubuna ekle** açılır listesinden **Varsayılan gruplar** seçimini yapın ve **Tamam**'a tıklayın.
    Uygulama varsayılan gruba eklenecektir.
12. İlgili uygulamayı seçin ve ardından uygulamanın bağlam menüsünden **Uygulama hakları**'nı seçin.
    Uygulama kuralları ve özellikler penceresi açılır.
13. **Ağ kuralları** sekmesini seçin.
    Bu, Güvenlik Duvarı tarafından belirlenen varsayılan ağ kurallarının listesini açar.
14. **Ekle**'ye tıklayın.
    Paket kuralı özellikleri açılır.
15. Ağ hizmetinin adını **Ad** alanına elle girin.
16. 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.
17. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayları günlüğe kaydet** onay kutusunu işaretleyin.
18. Yeni ağ kuralını kaydet.
19. Ağ kuralının önceliğini ayarlamak için **Yukarı**/**Aşağı** düğmelerini kullanın.
20. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir uygulama ağ kuralı oluşturma

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Temel Tehdit Koruması** → **Güvenlik Duvarı**'nı seçin.
5. **Güvenlik Duvarı Ayarları** bloğunda, **Uygulama ağ kuralları** 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 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. Sihirbazdan çıkın.

    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 **Ad** alanına elle girin.
16. Ağ kuralı ayarlarını yapılandırın (aşağıdaki tabloya bakın).

    Şablon seç 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 **Yukarı**/**Aşağı** düğmelerini 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 virgülle ayrılmış bağlantı noktası numaralarını belirtebilirsiniz.
Yön	**Gelen**. **Gelen/Giden**. **Giden**.
Uzak adres	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. Kaspersky Endpoint Security, 11.7.0 sürümünden itibaren DNS adlarını destekler. 11.6.0 veya daha eski sürümler için bir DNS adı belirlediğinizde, Kaspersky Endpoint Security ilgili kuralı tüm adreslere uygulayabilir.
Yerel adres	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.

Kaspersky Endpoint Security, 11.7.0 sürümünden itibaren DNS adlarını destekler. 11.6.0 veya daha eski sürümler için bir DNS adı belirlediğinizde, Kaspersky Endpoint Security ilgili kuralı tüm adreslere uygulayabilir.

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 bağlantı noktaları** sekmesinde, bilgisayarın açık bağlantı noktalarının 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 Tehdidi Koruması bileşeni tarafından ağ etkinliği engellenen uzak bilgisayarların IP adresleri listelenir.

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 aygıt 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.

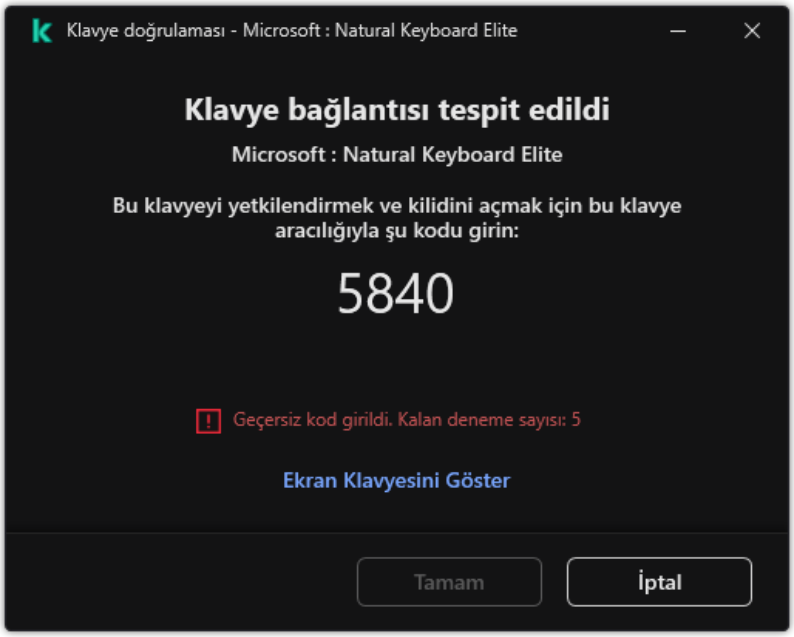
Kod doğru girildiyse uygulama klavyenin VID/PID'si ve bağlandığı bağlantı noktasının numarası gibi tanımlama parametrelerini yetkilendirilen klavyeler listesine kaydeder. Klavye yeniden bağlandığında ya da işletim sistemi yeniden başlatıldıktan sonra klavye yetkilendirmenin tekrarlanması gerekmez.

Yetkilendirilen klavye bilgisayarın farklı bir USB bağlantı noktasına bağlandığında, uygulama bu klavyenin yetkilendirilmesi için tekrar 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.

BadUSB Saldırısı Önleme bileşeni varsayılan olarak yüklenmez. BadUSB Saldırısı Önleme bileşenine ihtiyacınız varsa, bu bileşeni uygulamayı yüklemeden önce yükleme paketinin özelliklerinden ekleyebilir ya da uygulamayı yükledikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz.



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.

BadUSB Saldırısı Önleme'yi etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **BadUSB Saldırısı Önleme**'yi seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **BadUSB Saldırısı Önleme** geçiş düğmesini kullanın.
4. **Bağlandığında USB klavye yetkilendirme** bloğunda, yetkilendirme kodunu girmek için güvenlik ayarlarını yapın:
   - **Maksimum sayıda USBB 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 5 denemeye

izin verirseniz, USB cihazı beşinci başarısız denemeden sonra bloke olur. Kaspersky Endpoint Security, USB cihazı için engelleme süresini görüntüler. Bu süre geçtikten sonra, yetkilendirme kodunu girmek için 5 deneme hakkınız vardır.

- **Maksimum girişim sayısına ulaşılırken zaman aşımı**. Belirtilen sayıda başarısız denemeden sonra yetkilendirme kodunun girilmesi için USB cihazının 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 karakterlerin girişin desteklemeyen USB aygıtların (ör. barkod tarayıcılar) yetkilendirilmesi için kullanılmalıdır. Bilinmeyen USB aygıtların yetkilendirilmesi için Ekran Klavyesi'nin kullanılması önerilmez.

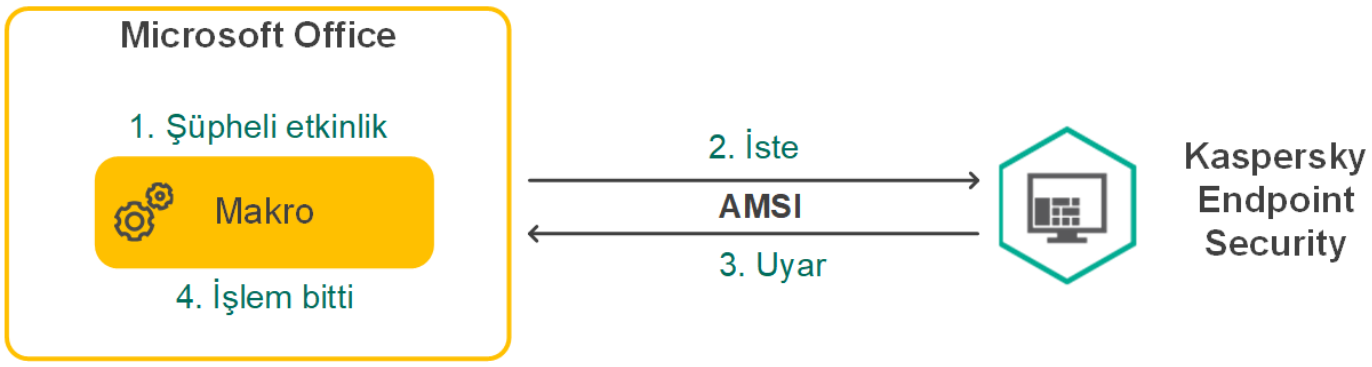
Yetkilendirme için Ekran Klavyesi'nin kullanımına izin vermek veya yasaklamak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması → BadUSB Saldırısı Önleme**'yi seçin.
3. Yetkilendirme için Ekran Klavyesinin kullanımına izin vermek için **USB cihazlarının kimlik doğrulaması için Ekran Klavyesinin kullanımını yasakla** onay kutusunun işaretini kaldırın.
4. Değişikliklerinizi kaydedin.

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. Üçüncü taraf uygulama, bir tehdit bildirimi aldıktan sonra zararlı işlemlerin gerçekleştirilmesine izin vermez (örneğin sonlandırılır).



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;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise;

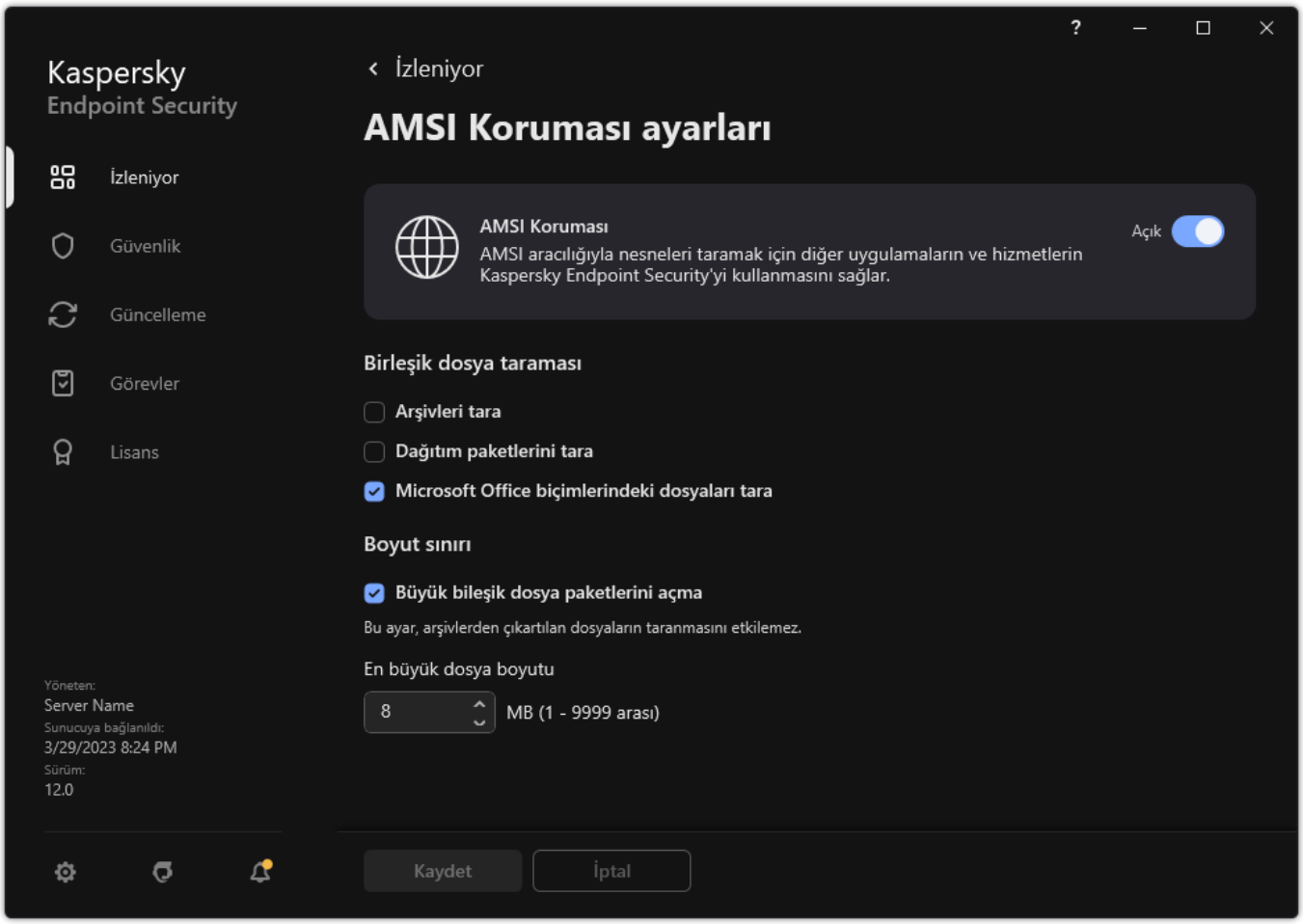
- Windows Server 2016 Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2019 Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Çekirdek Modu dahil).

AMSI Korumasını etkinleştirme ve devre dışı bırakma

Varsayılan olarak AMSI Koruması etkin durumdadır.

AMSI Korumasıyı etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **AMSI Koruması** seçimini yapın.



AMSI Koruma ayarları

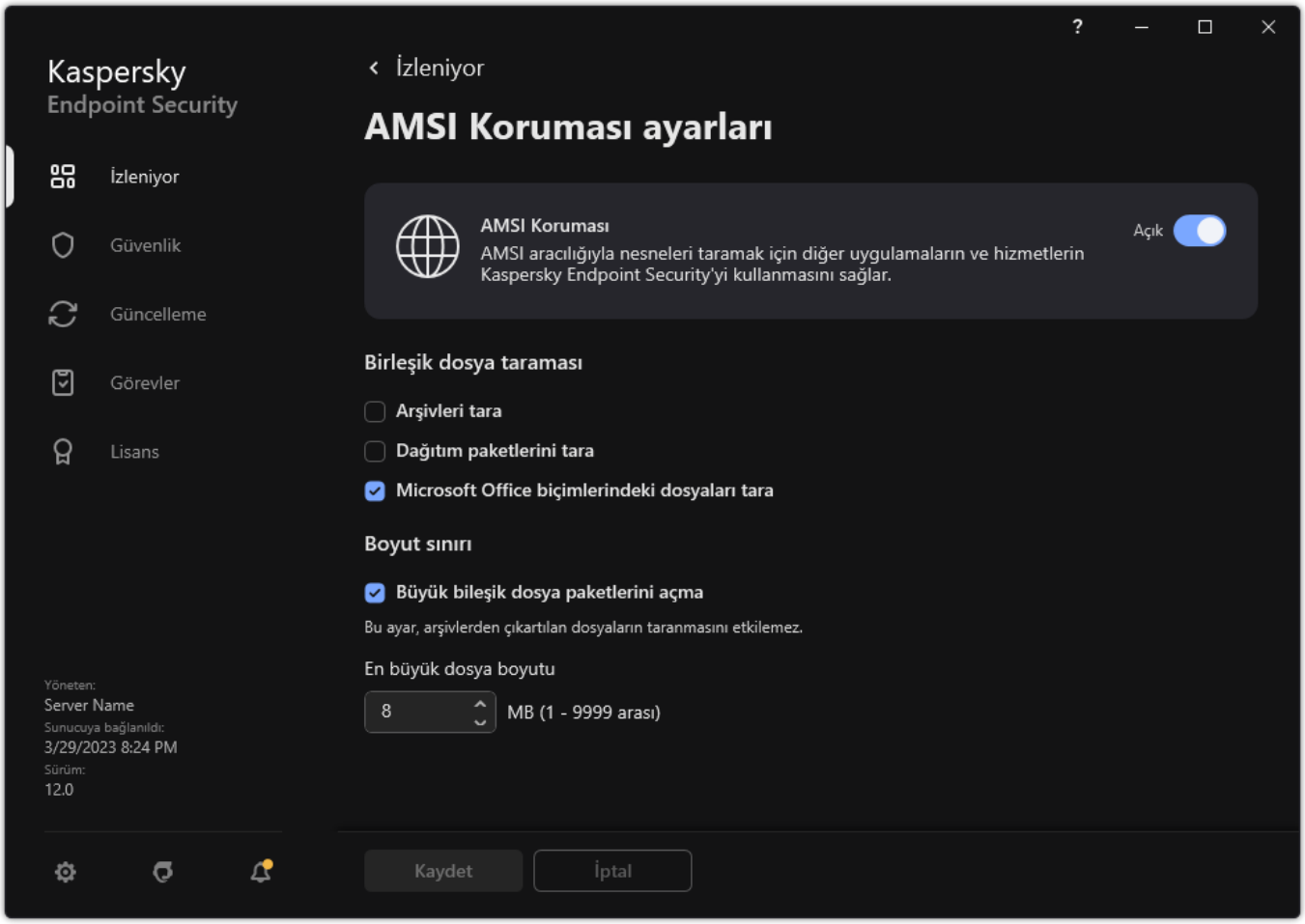
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **AMSI Koruması** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Birleşik dosyaları taramak için AMSI Korumasını kullanma

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 dosyaların türlerini sınırlayarak taramayı hızlandırabilirsiniz.

Bileşik dosyaların AMSI Koruması taramalarını yapılandırmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Temel Tehdit Koruması** → **AMSI Koruması** seçimini yapın.



AMSI Koruma ayarları

3. **Birleşik dosya taraması** 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 dosya paketlerini açmasını engellemek için **Büyük bileşik dosya paketlerini açma** onay kutusunu işaretleyin ve **En büyük dosya boyutu** alanında gereken 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.

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'yi etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Exploit Önleme etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Gerekirse Exploit Önleme'yi devre dışı bırakabilirsiniz.

Exploit Önleme'yi etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Exploit Önleme**'yi seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Exploit Önleme** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak, Exploit Önleme etkinleştirilirse, Kaspersky Endpoint Security, savunmasız uygulamalar tarafından çalıştırılan yürütülebilir dosyaları izleyecektir. Kaspersky Endpoint Security, hassas bir uygulamadan başlatılan yürütülebilir bir dosyanın kullanıcı dışında çalıştırıldığını tespit ederse Kaspersky Endpoint Security, seçilen eylemi gerçekleştirecektir (örneğin, işlemi engelleyecektir).

Exploit tespit edildiğinde uygulanacak eylemi seçme

Varsayılan olarak, exploit tespit edildiğinde Kaspersky Endpoint Security, exploit tarafından girişimde bulunulan işlemleri engeller.

Exploit tespit edildiğinde uygulanacak eylemi seçmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Exploit Önleme**'yi seçin.
3. **Exploit algılandığında** bloğunda gereken eylemi seçin:
   - **İşlemi 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.
   - **Bildir**. 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.
4. Değişikliklerinizi kaydedin.

Sistem işlemleri bellek koruması

Varsayılan olarak sistem işlemi bellek koruması etkindir.

Sistem işlemi bellek korumasını etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Exploit Önleme**'yi seçin.
3. Bu özelliği etkinleştirmek veya devre dışı bırakmak için **Sistem işlemleri bellek korumasını etkinleştir** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak Kaspersky Endpoint Security, sistem süreçlerine erişmeye çalışan harici işlemleri engelleyecektir.

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.

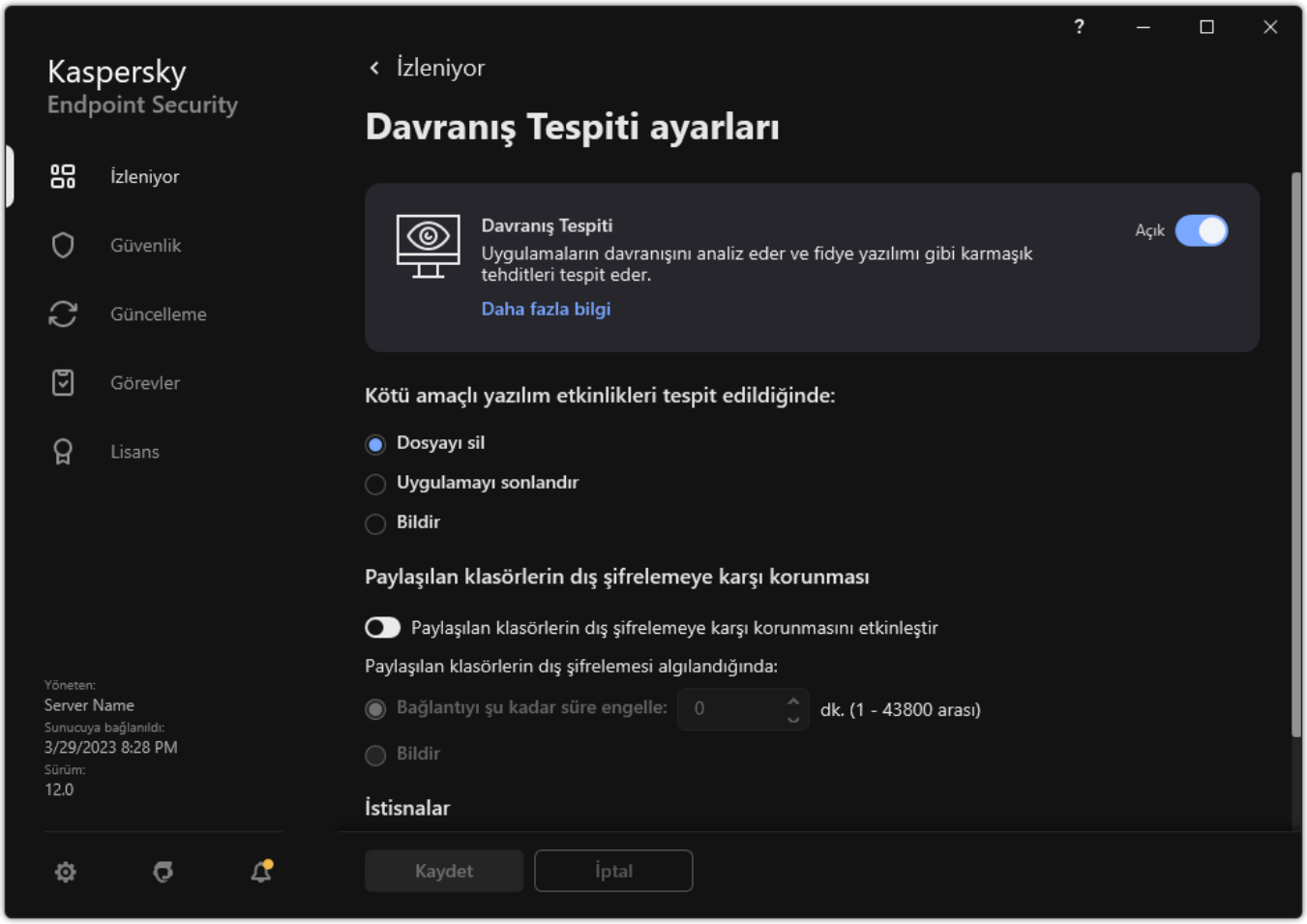
Davranış Tespiti'ni etkinleştirme ve devre dışı bırakma

Varsayılan olarak Davranış Tespiti etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Gerekirse Davranış Tespiti'ni devre dışı bırakabilirsiniz.

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.

Davranış Tespiti'ni etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Davranış Tespiti**'ni seçin.



Davranış Tespiti ayarları

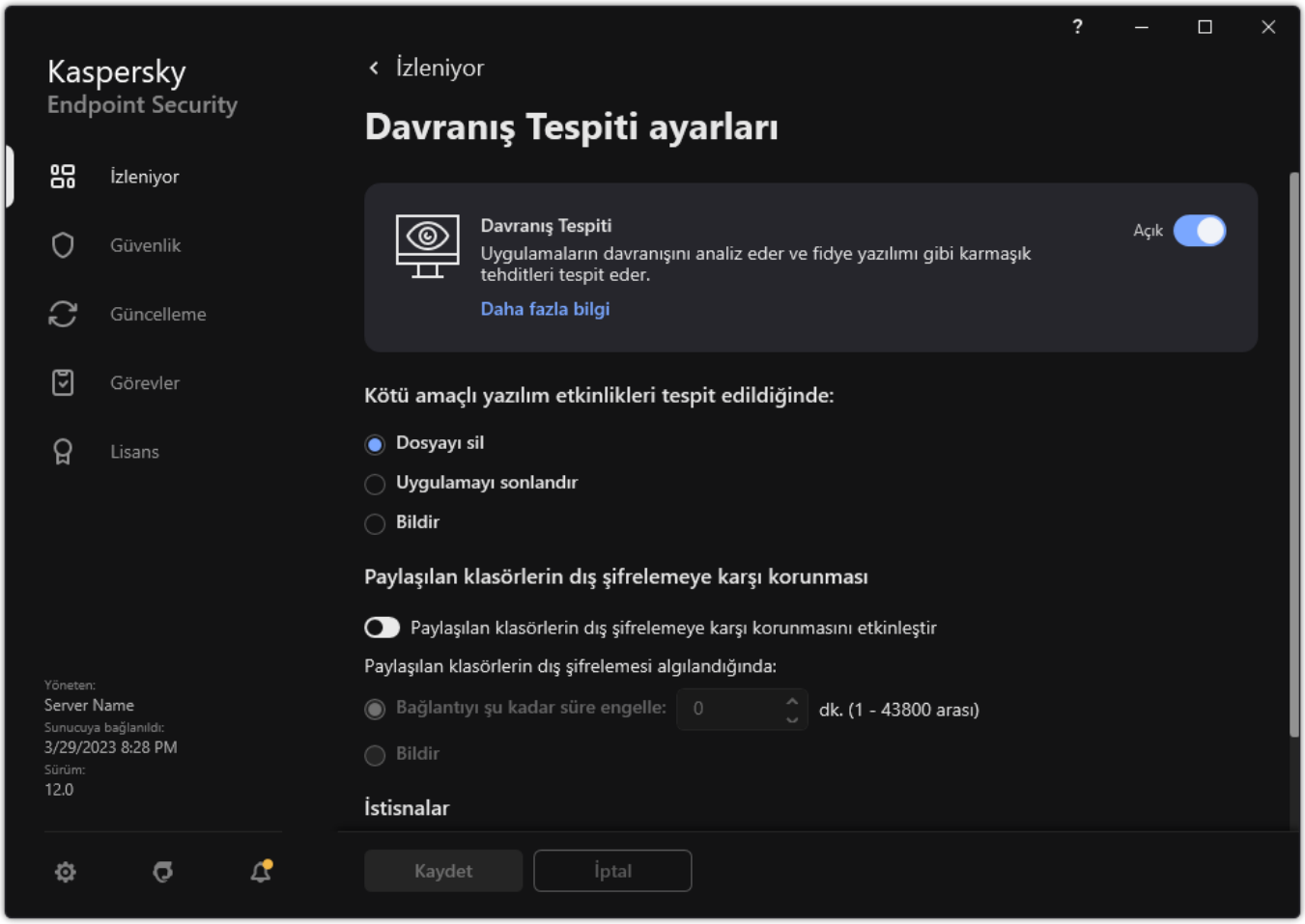
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Davranış Tespiti** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak, Davranış Tespiti etkinleştirilirse, Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz etmek için davranış akışı imzalarını kullanır.

Kötü amaçlı yazılım etkinlikleri tespit edildiğinde gerçekleştirilecek eylemin seçilmesi

Bir uygulamanın zararlı bir faaliyette bulunması durumunda ne yapılacağını seçmek için aşağıdaki adımları uygulayın:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması** → **Davranış Tespiti**'ni seçin.



Davranış Tespiti ayarları

3. **Kötü amaçlı yazılım etkinlikleri tespit edildiğinde** bloğunda gereken eylemi seçin:

   - **Dosyayı 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.
   - **Uygulamayı sonlandır**. Bu öğe seçilirse zararlı yazılımların etkinlikleri tespit edildiğinde Kaspersky Endpoint Security, bu uygulamayı sonlandırır.
   - **Bildir**. Bu öğe seçilirse ve uygulamanın zararlı yazılım etkinliği tespit edilirse Kaspersky Endpoint Security, uygulamanın zararlı yazılım etkinliği hakkındaki bilgileri etkin tehditler listesine ekler.

4. Değişikliklerinizi kaydedin.

Paylaşılan klasörlerin dış şifrelemeye karşı korunması

Bileşen yalnızca NTFS dosya sistemli ve EFS ile şifrelenmemiş yığın depolama aygıtlarında saklanan dosyalarda gerçekleştirilen işlemleri görüntüler.

Paylaşılan klasörlerin dış şifrelemeye karşı korunması, paylaşılan klasörlerde etkinliğin analizini sağlar. Bu etkinlik, dış şifreleme için tipik olan bir davranış akışı imzasıyla eşleşirse Kaspersky Endpoint Security seçili eylemi gerçekleştirir.

Varsayılan olarak paylaşılan klasörlerin dış şifrelemeye karşı korunması devre dışıdır.

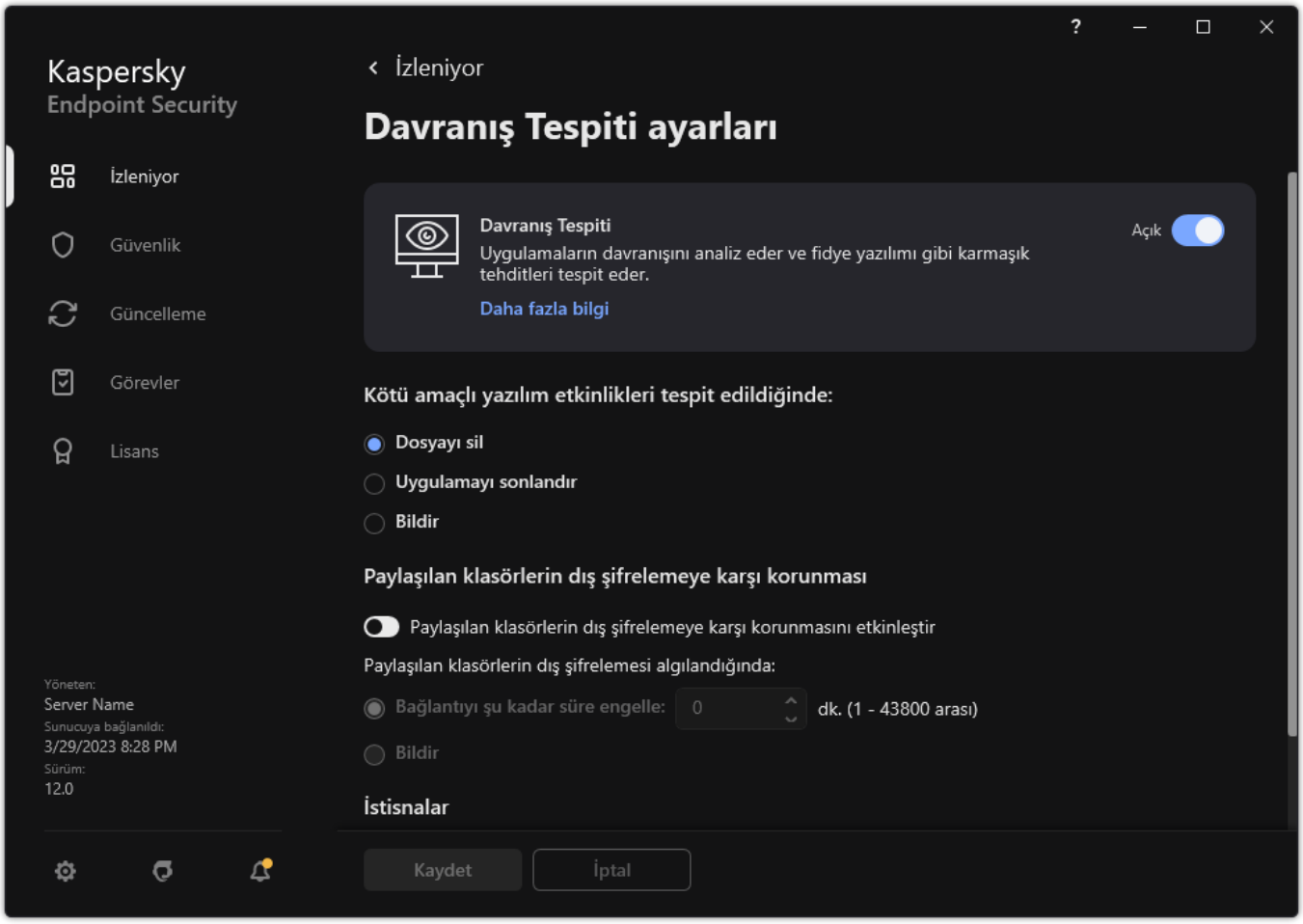
Kaspersky Endpoint Security yüklendikten sonra paylaşılan klasörlerin dış şifrelemeye karşı korunması bilgisayar yeniden başlatılıncaya kadar sınırlıdır.

Paylaşılan klasörlerin dış şifrelemeye karşı korunmasını etkinleştirme ve devre dışı bırakma

Kaspersky Endpoint Security yüklendikten sonra paylaşılan klasörlerin dış şifrelemeye karşı korunması bilgisayar yeniden başlatılıncaya kadar sınırlıdır.

Paylaşılan klasörlerin dış şifrelemeye karşı korunmasını etkinleştirme veya devre dışı bırakma:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Davranış Tespiti**'ni seçin.



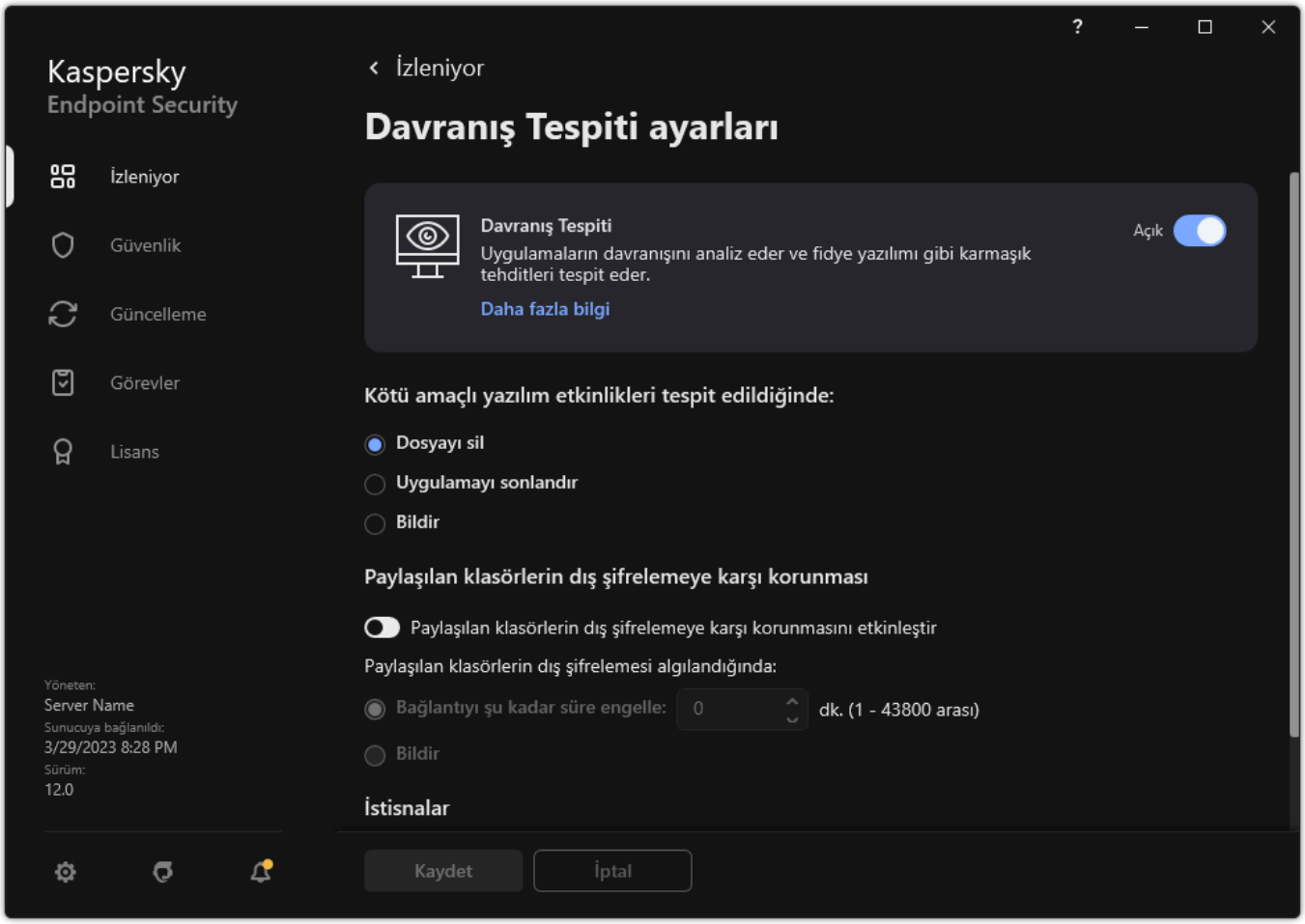
Davranış Tespiti ayarları

3. Dış şifrelemede tipik olan etkinlik algılamasını etkinleştirmek veya devre dışı bırakmak için **Paylaşılan klasörlerin dış şifrelemeye karşı korunmasını etkinleştir** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Paylaşılan klasörlerin dış şifrelemesi algılandığında uygulanacak eylemi seçme

Paylaşılan klasörlerin dış şifrelemesi algılandığında uygulanacak eylemi seçmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Davranış Tespiti**'ni seçin.



Davranış Tespiti ayarları

3. **Paylaşılan klasörlerin dış şifrelemeye karşı korunması** bloğunda ilgili eylemi seçin:

   - **Bağlantıyı şu kadar süre engelle: N dk. (1 - 43800 arası)**. Bu seçenek tercih edilir ve 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.
     - Kaspersky Security Center'a tespit edilen zararlı etkinlik hakkında bilgiler gönderir.

     Ayrıca Düzeltme Altyapısı bileşeni etkinse değiştirilen dosyalar yedek kopyalarından geri yüklenir.

   - **Bildir**. Bu seçenek tercih edilir ve Kaspersky Endpoint Security paylaşılan klasörlerde bir dosya değiştirme girişimi algılarsa şu eylemleri yapar:

     - Yerel uygulama arabirimi raporlarına bir giriş ekler.
     - Etkin tehditler listesine bir girdi ekler.
     - Kaspersky Security Center'a tespit edilen zararlı etkinlik hakkında bilgiler gönderir.

4. Değişikliklerinizi kaydedin.

Paylaşılan klasörlerin dış şifrelemeye karşı korunması için bir istisna oluşturma

Kuruluşunuz paylaşılan klasörleri kullanarak dosya alışverişi yaparken veri şifreleme kullanıyorsa bir klasörü hariç tutmak hatalı pozitif sonuçların sayısını 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.

[Yönetim Konsolu (MMC) kullanılarak paylaşılan klasörlerin korunması için bir istisna 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** öğesini seçin.
5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, **Tarama istisnaları** sekmesini seçin.

   Bu, istisnaların listesini içeren bir pencere açar.
7. 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.
8. 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.
9. **Ekle**'ye tıklayın.
10. **Özellikler** bloğunda **Dosya veya klasör** onay kutusunu işaretleyin.
11. **Dosya veya klasör seç** penceresinde **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğunda **dosya veya klasör seçin** bağlantısına tıklayın.
12. **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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.
13. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.
14. **Bileşenleri seçin** bağlantısını etkinleştirmek için **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğunda **herhangi** bağlantısına tıklayın.

15. **Bileşenleri seçin** bağlantısına tıklayarak **Koruma bileşenleri** penceresini açın.
16. **Davranış Tespiti** bileşeninin yanındaki onay kutusunu seçin.
17. Değişikliklerinizi kaydedin.

[Web Console ve Cloud Console kullanılarak paylaşılan klasörlerin korunması için bir istisna oluşturma](#)

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel ayarlar** → **İstisnalar ve tespit edilen nesne türleri** bölümüne gidin.
5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Tarama istisnaları** düğmesine 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.
8. **Ekle**'ye tıklayın.
9. **Dosya veya klasör** istisnasını nasıl eklemek istediğinizi seçin.
10. **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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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. **Koruma bileşenleri** bloğundan **Davranış Tespiti** bileşenini seçin.
12. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.
13. İstisna için **Etkin** durumu seçin.
    İstediğiniz zaman bir istisnayı durdurmak için geçiş düğmesini kullanabilirsiniz.

14. Değişikliklerinizi kaydedin.

[Uygulama arabirimindeki paylaşılan klasörlerin korunması için bir istisna oluşturma](#)

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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.
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.

Paylaşılan klasörlerin dış şifrelemeye karşı korunması istisnalarının adreslerini yapılandırma

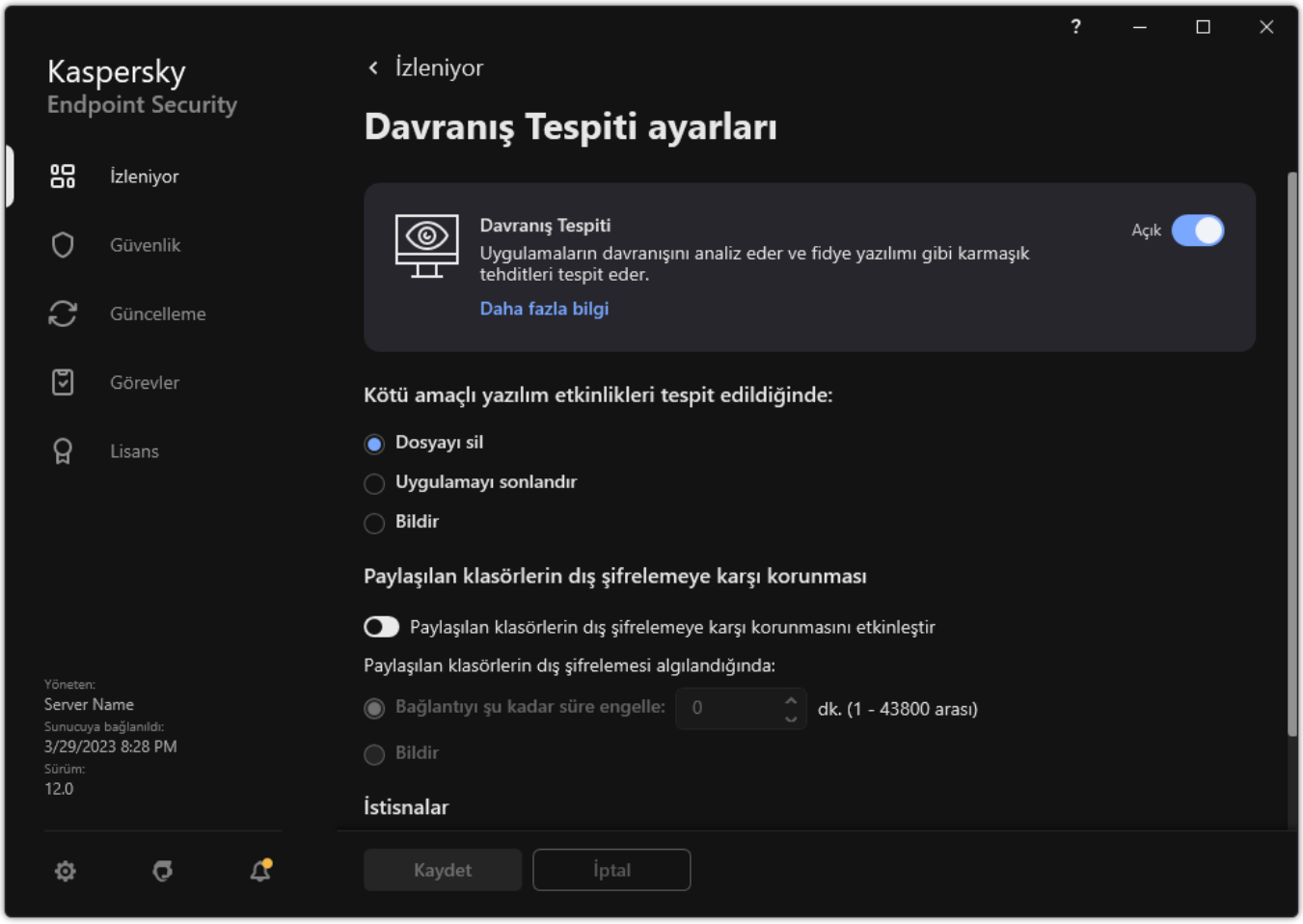
Oturum Açı Denetle hizmetinin, paylaşılan klasörlerin dış şifrelemeye karşı korunmasına karşı istisnaları etkinleştirmek amacıyla etkinleştirilmesi gerekir. Varsayılan olarak Oturum Açı Denetle hizmeti devre dışıdır (Oturum Açı Denetle hizmetini etkinleştirme hakkında daha ayrıntılı bilgi için lütfen 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.

Paylaşılan klasörlerin dış şifreleme işlemini gerçekleştiren uzak bilgisayarları hariç tutmak için:

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde, **Gelişmiş Tehdit Koruması → Davranış Tespiti**'ni seçin.



Davranış Tespiti ayarları

3. **İstisnalar** bloğunda, **İstisnaların adreslerini yapılandır** bağlantısını tıklayın.

4. İstisnalar listesine bir IP adresi veya bilgisayar adı eklemek isterseniz **Ekle** düğmesine tıklayın.

5. Dış şifreleme girişimlerinin işlenmemesi gereken IP adresini veya bilgisayar adını girin.

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'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. **Paylaşılan klasörlerin dış şifrelemeye karşı korunması** bloğunda **İstisnalar** düğmesine tıklayın.

6. Kurallar listesini dışa aktarmak için:

a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla bağlantı noktası seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.

b. **Dışa aktar** bağlantısına 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.

7. 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.

8. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bir istisnalar listesinş dışa aktarma ve içe aktarma

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

İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Davranış Tespiti** bölümüne gidin.
5. **İstisnalar** bloğundaki istisnaların listesini dışa aktarmak için:

a. Dışa aktarmak istediğiniz istisnaları seçin.

b. **Dışa aktar**'a tıklayın.

c. Yalnızca seçili istisnaları veya tüm istisnalar listesini dışa aktarmak istediğinizi onaylayın.

d. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

e. Dosyaya kaydet.

Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.

6. **İstisnalar** bloğundaki istisnalar 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.

7. 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 (dosyalar ve uygulamalar gibi)

Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

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.

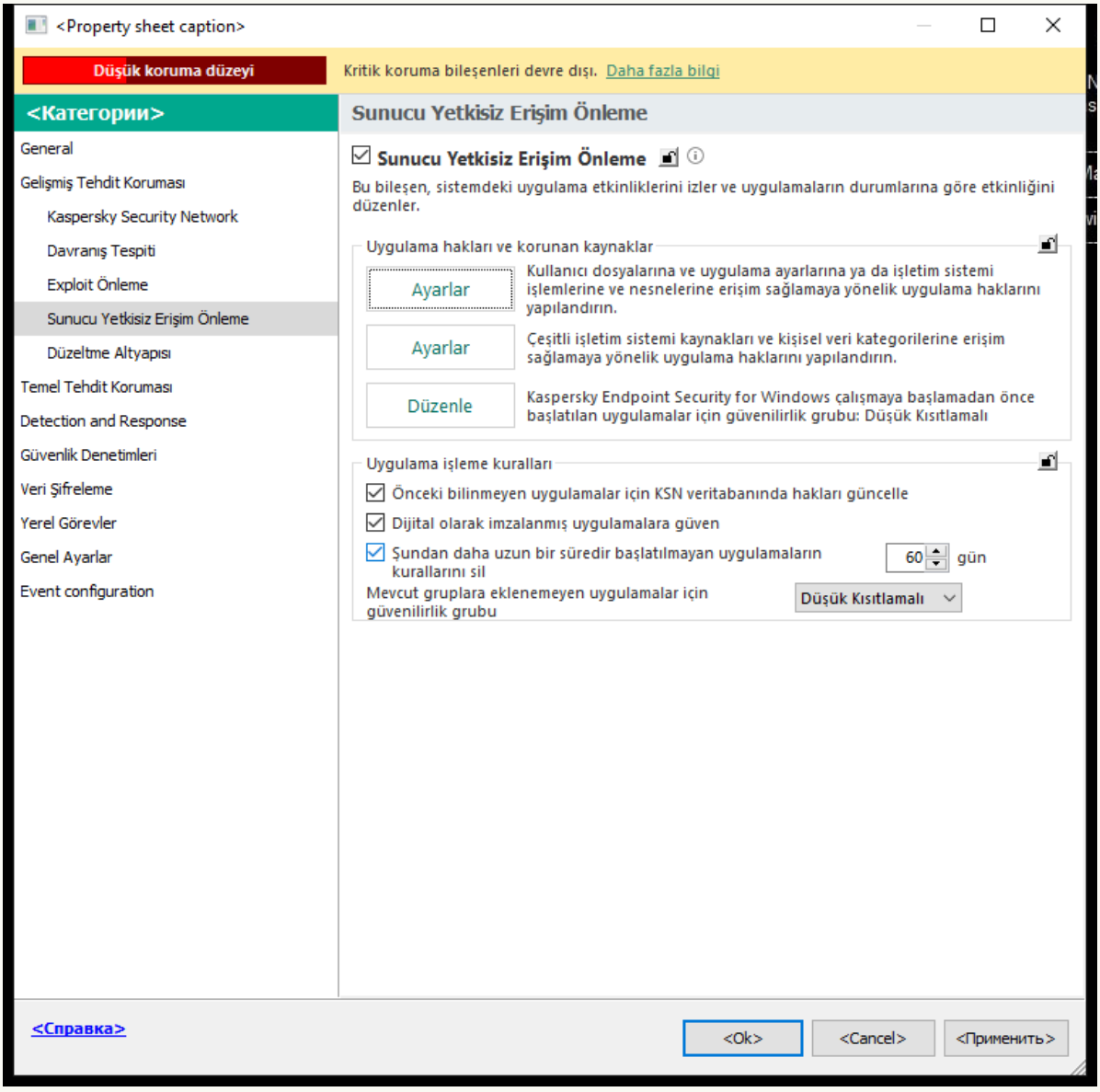
Uygulamanın bir sonraki başlatılmasında, Kaspersky Endpoint Security uygulamanın bütünlüğünü kontrol eder. Uygulama değişmediyse bileşen, geçerli uygulama haklarını kullanır. Uygulama değiştirildiyse Kaspersky Endpoint Security ilk kez başlatılıyormuş gibi uygulamayı analiz eder.

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'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



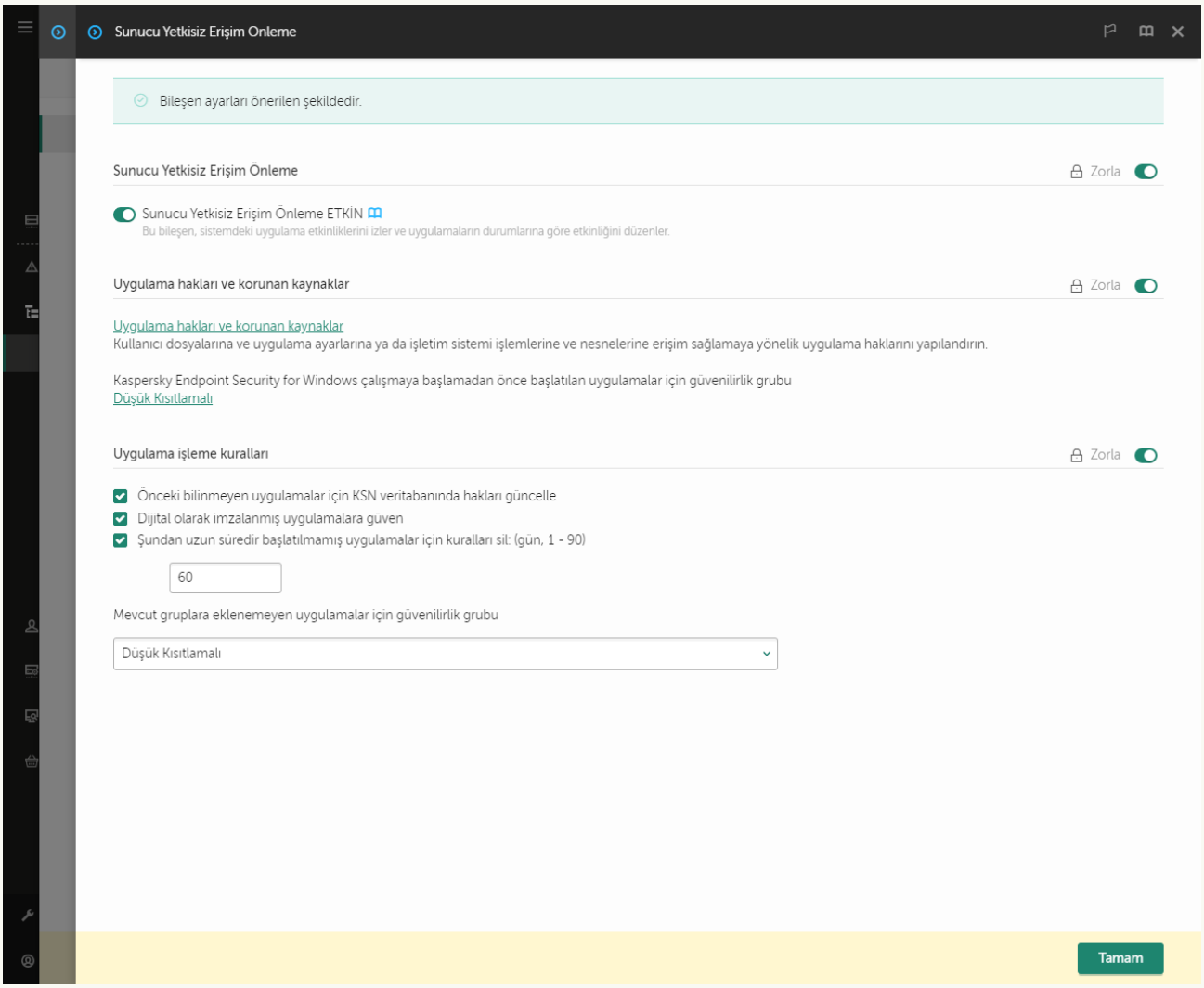
Yetkisiz Erişim Önleme ayarları

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sunucu Yetkisiz Erişim Önleme** onay kutusunu kullanın.
6. 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 **Aygıtlar → İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.

4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Sunucu Yetkisiz Erişim Önleme** 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 ataması için bir güvenilirlik grubu seçebilirsiniz. Kaspersky Endpoint Security'den önce başlayan uygulamalar otomatik olarak Sunucu Yetkisiz Erişim Önleme bileşeni ayarlarında tanımlanan güvenilirlik grubuna taşınır.

Kaspersky Endpoint Security'den önce başlatılan uygulamalar için yalnızca ağ etkinliği denetlenir. Denetim, Güvenlik Duvarı ayarlarında tanımlanan ağ kurallarına göre gerçekleştirilir.

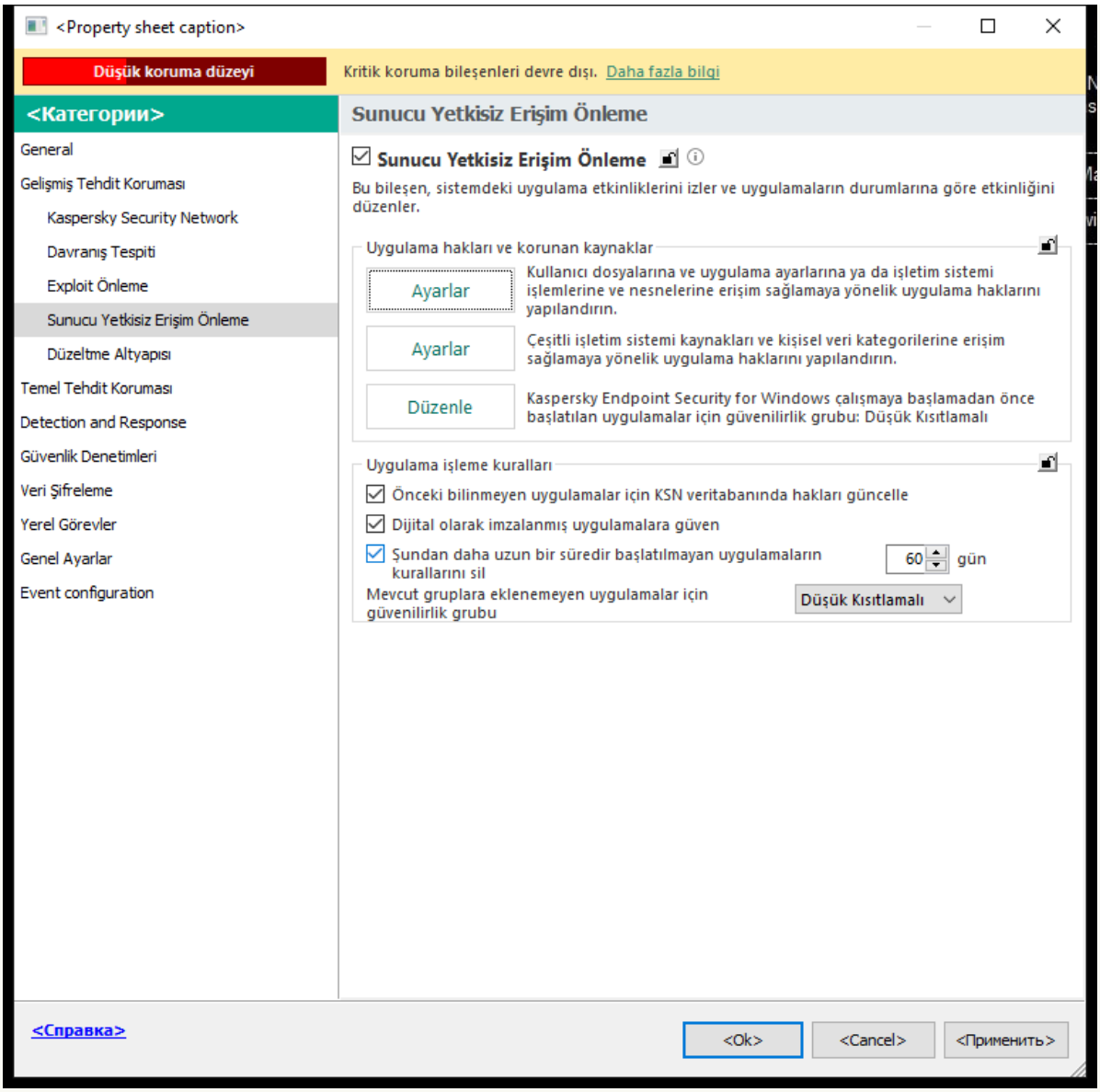
Bir uygulamanın güvenilirlik grubunu değiştirme

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'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** → **Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

6. **Uygulama hakları** sekmesini seçin.

7. **Ekle**'ye tıklayın.

8. 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.

9. **Yenile**'ye tıklayın.

   Kaspersky Endpoint Security uygulamayı, yönetilen bilgisayarlardaki yüklü uygulamalar birleştirilmiş listesinde arar. Kaspersky Endpoint Security, arama kriterlerinizi karşılayan uygulamaların bir listesini görüntüler.

10. Gereken uygulamayı seçin.

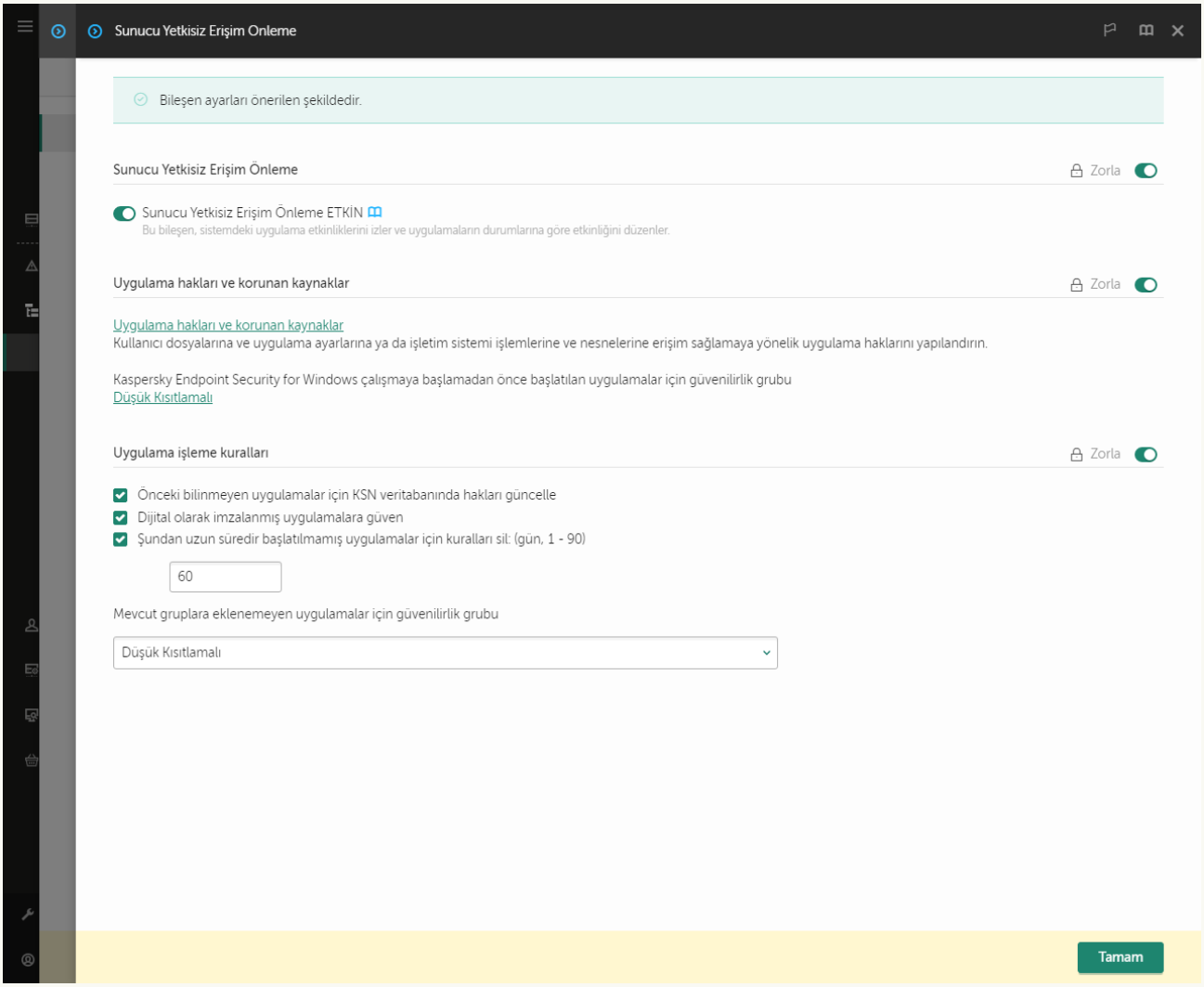
11. **Seçilen uygulamayı güvenilirlik grubuna ekle** açılır listesinden uygulama için gerekli güvenilirlik grubunu seçin.

12. Değişikliklerinizi kaydedin.

[Bir uygulamanın güvenilirlik grubu Web Console'da ve Cloud Console'da nasıl değiştirilir](#)

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

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. Sihirbazdan çıkın.

    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.

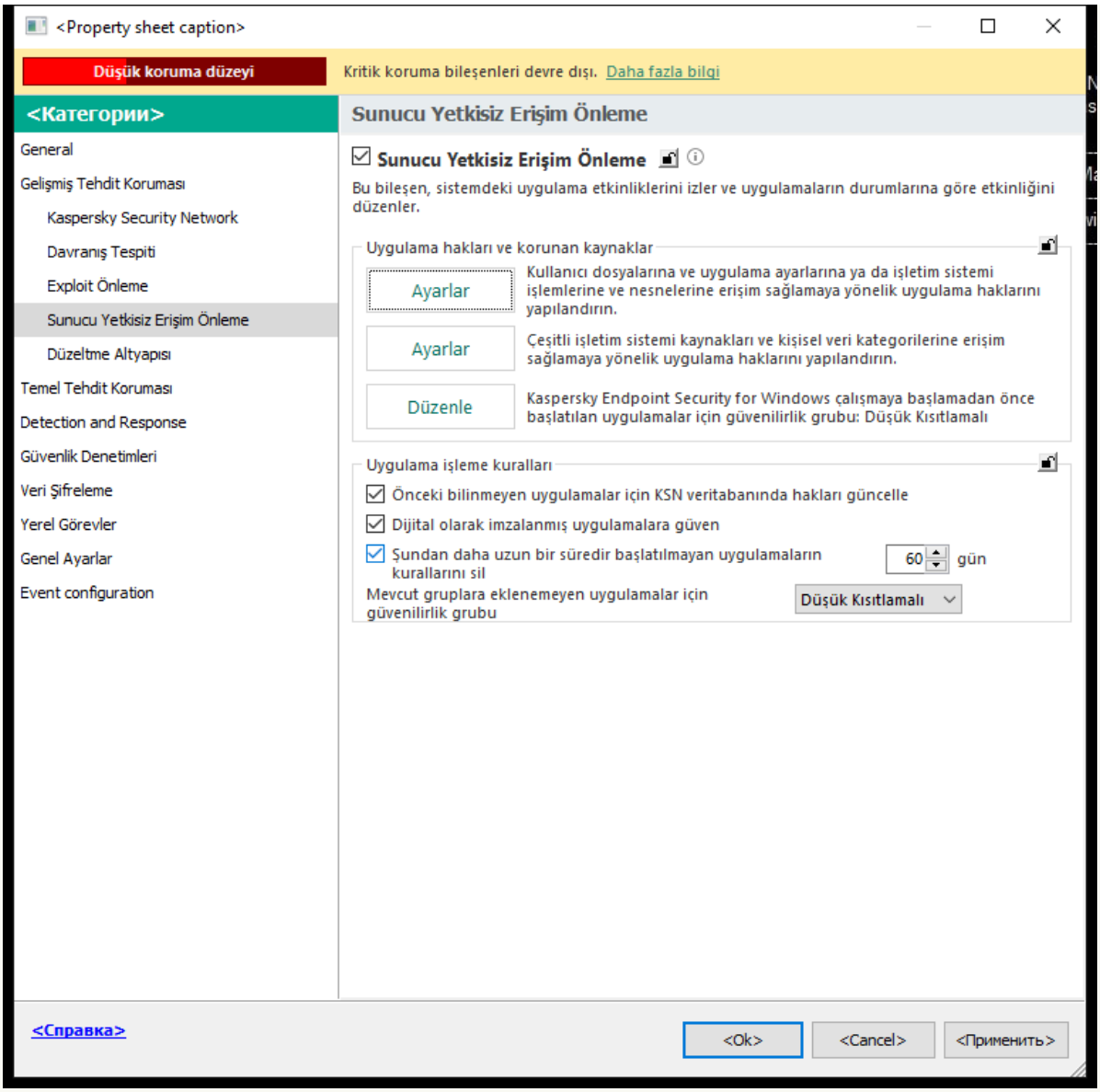
Sonuç olarak, uygulama diğer güvenilirlik grubuna konulacaktır. Kaspersky Endpoint Security, daha sonra güvenilirlik grubuna bağlı olarak uygulamanın eylemlerini engeller. Uygulamaya *(kullanıcı tanımlı)* durumu atanır. Kaspersky Security Network'te uygulamanın tanınırlığı değişirse, Sunucu Yetkisiz 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'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** → **Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

6. **Uygulama hakları** sekmesini seçin.

7. Gerekli güvenilirlik grubunu seçin.

8. Güvenilirlik grubunun bağlam menüsünde **Grup hakları**'nı seçin.

   Güvenilirlik grubu özellikleri açılır.

9. Aşağıdakilerden birini yapın:

   - Uygulamanın işletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarları ile çalışmayı düzenleyen güvenilirlik gruplarını düzenlemek için **Dosya ve sistem kayıt defteri** sekmesini seçin.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** sekmesini seçin.

   Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

10. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** (✓) veya **Engelle** (⊘).

11. Bilgisayar kaynaklarının kullanımını izlemek için **Olayları günlüğe kaydet**'i seçin (/).

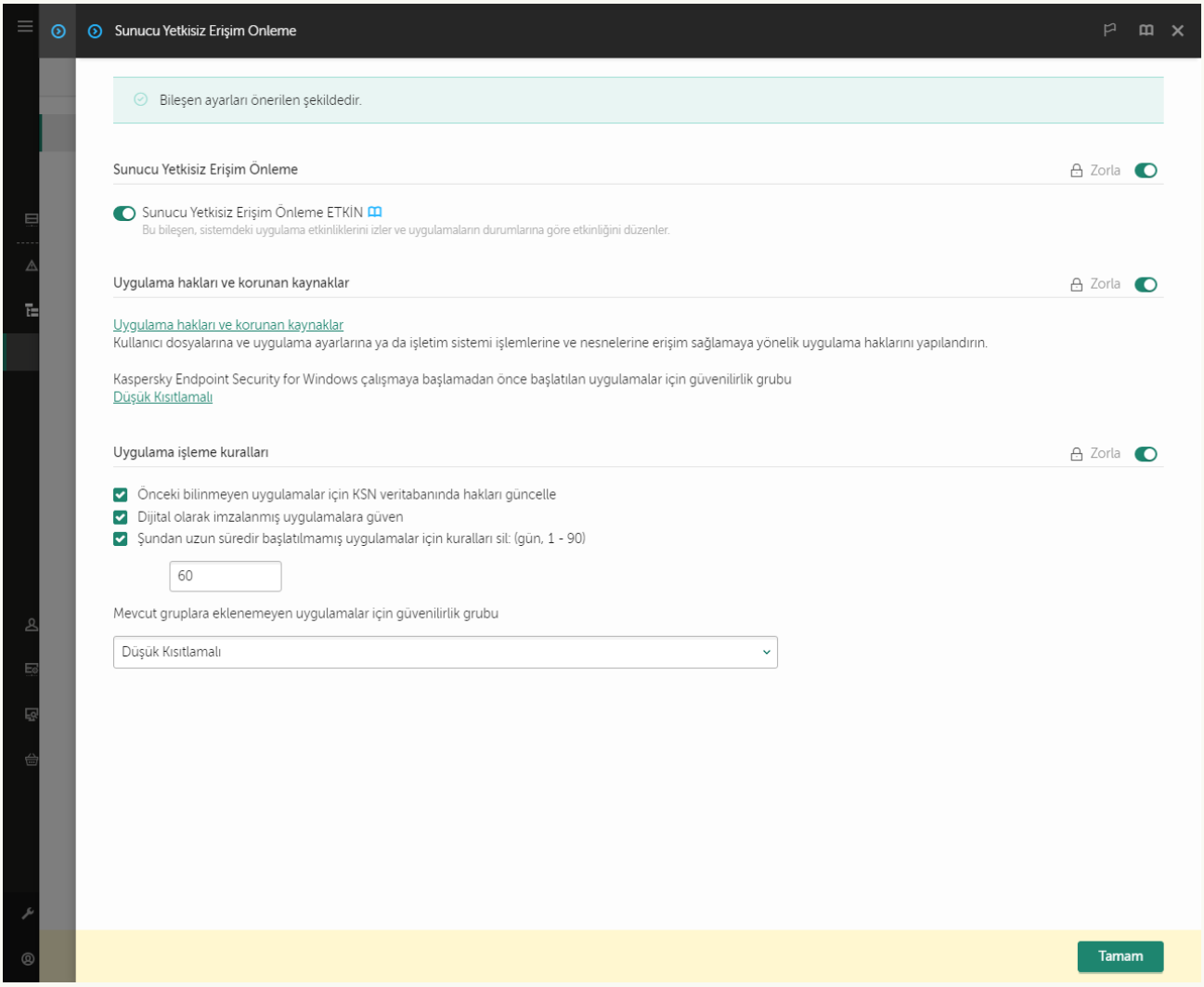
    Kaspersky Endpoint Security, Sunucu Yetkisiz Erişim Önleme bileşeninin çalışmasıyla ilgili bilgileri kaydedecektir. Raporlar, uygulama tarafından gerçekleştirilen bilgisayar kaynaklarıyla yapılan işlemler hakkında bilgi içerir (izin verildi veya yasaklandı). Raporlarda kaynakları kullanan uygulamalar hakkında bilgiler de yer alır.

12. Değişikliklerinizi kaydedin.

[Web Console'da ve Cloud Console'da güvenilirlik grubu hakları nasıl değiştirilir](#)

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

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. 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.

   Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

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:

   - Uygulamanın işletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarları ile çalışmayı düzenleyen güvenilirlik gruplarını düzenlemek için **Dosya ve sistem kayıt defteri** sekmesini seçin.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** sekmesini seçin.

   Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

7. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** ( ), **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.

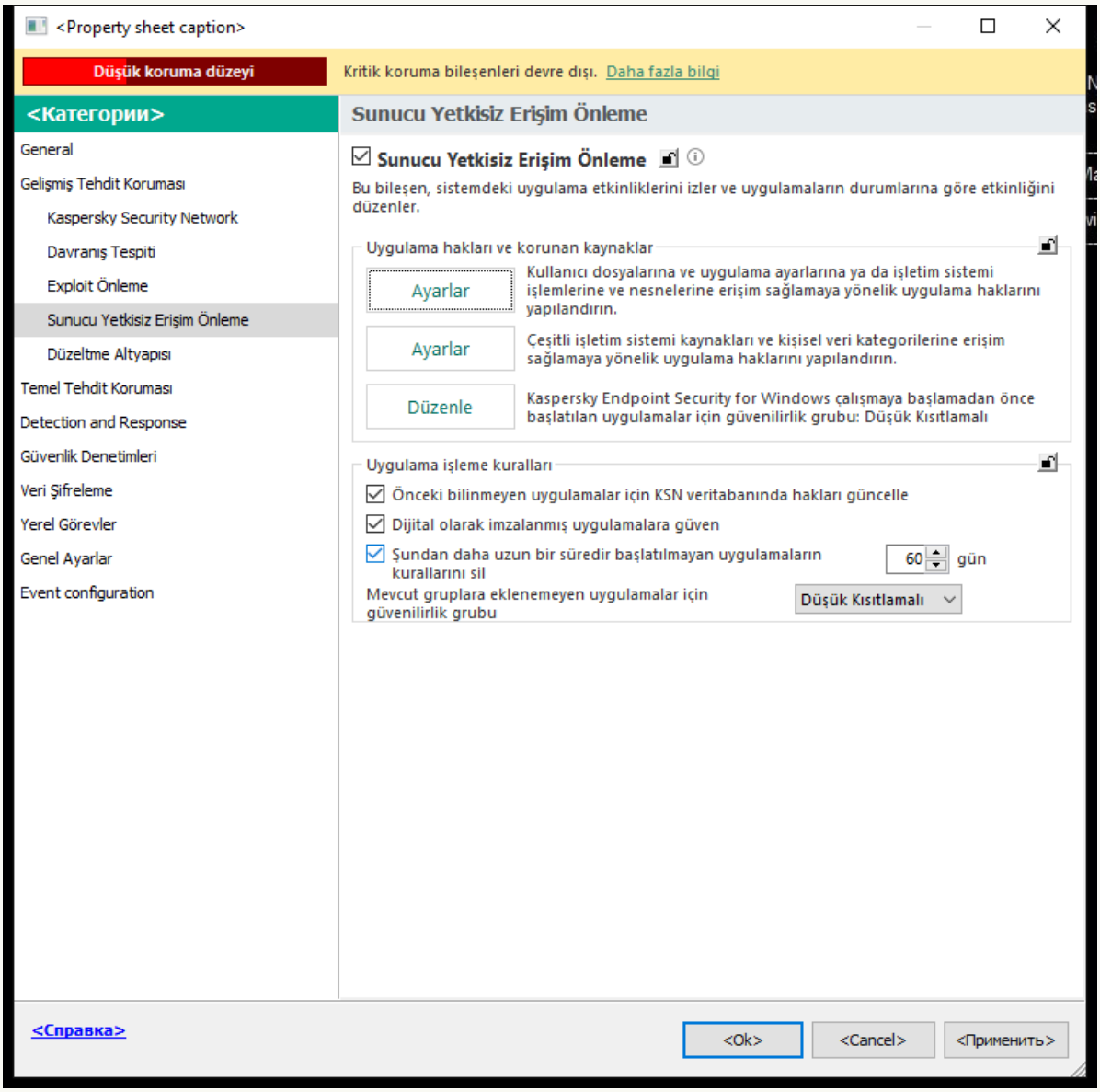
Güvenilirlik grubu hakları değiştirilecek. Kaspersky Endpoint Security, daha sonra güvenilirlik grubuna bağlı olarak uygulamanın eylemlerini engeller. Durum (*Özel ayarlar*) güvenilirlik grubuna atanacaktır.

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'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.

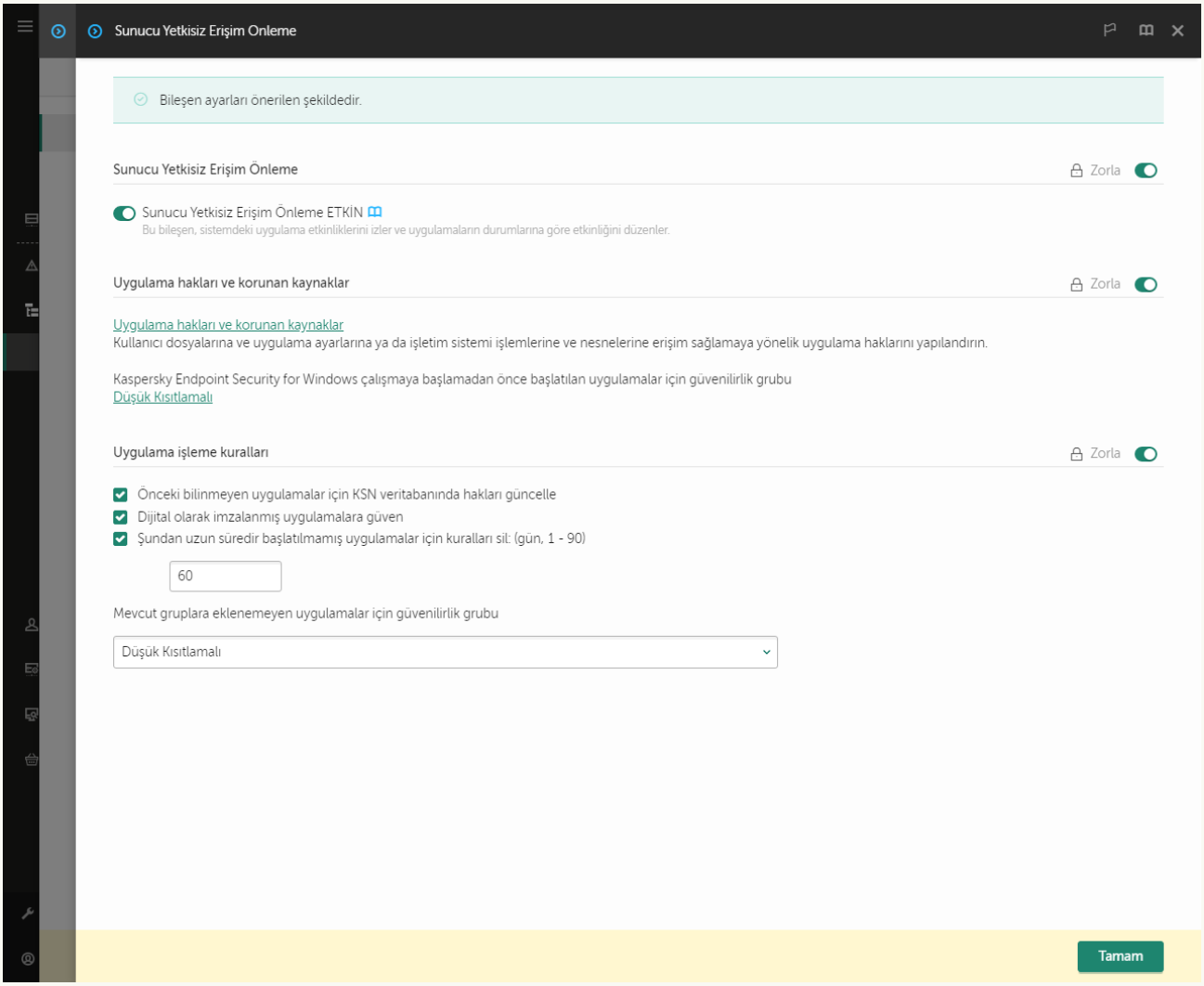


Yetkisiz Erişim Önleme ayarları

5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Düzenle** düğmesine tıklayın.
6. **Kaspersky Endpoint Security for Windows çalışmaya başlamadan önce başlatılan uygulamalar için güvenilirlik grubu** ayarı için uygun güvenilirlik grubu seçimini yapın.
7. 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 **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

5. **Kaspersky Endpoint Security for Windows çalışmaya başlamadan önce 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 for Windows çalışmaya başlamadan önce başlatılan uygulamalar için güvenilirlik grubu** bloğunda, 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.

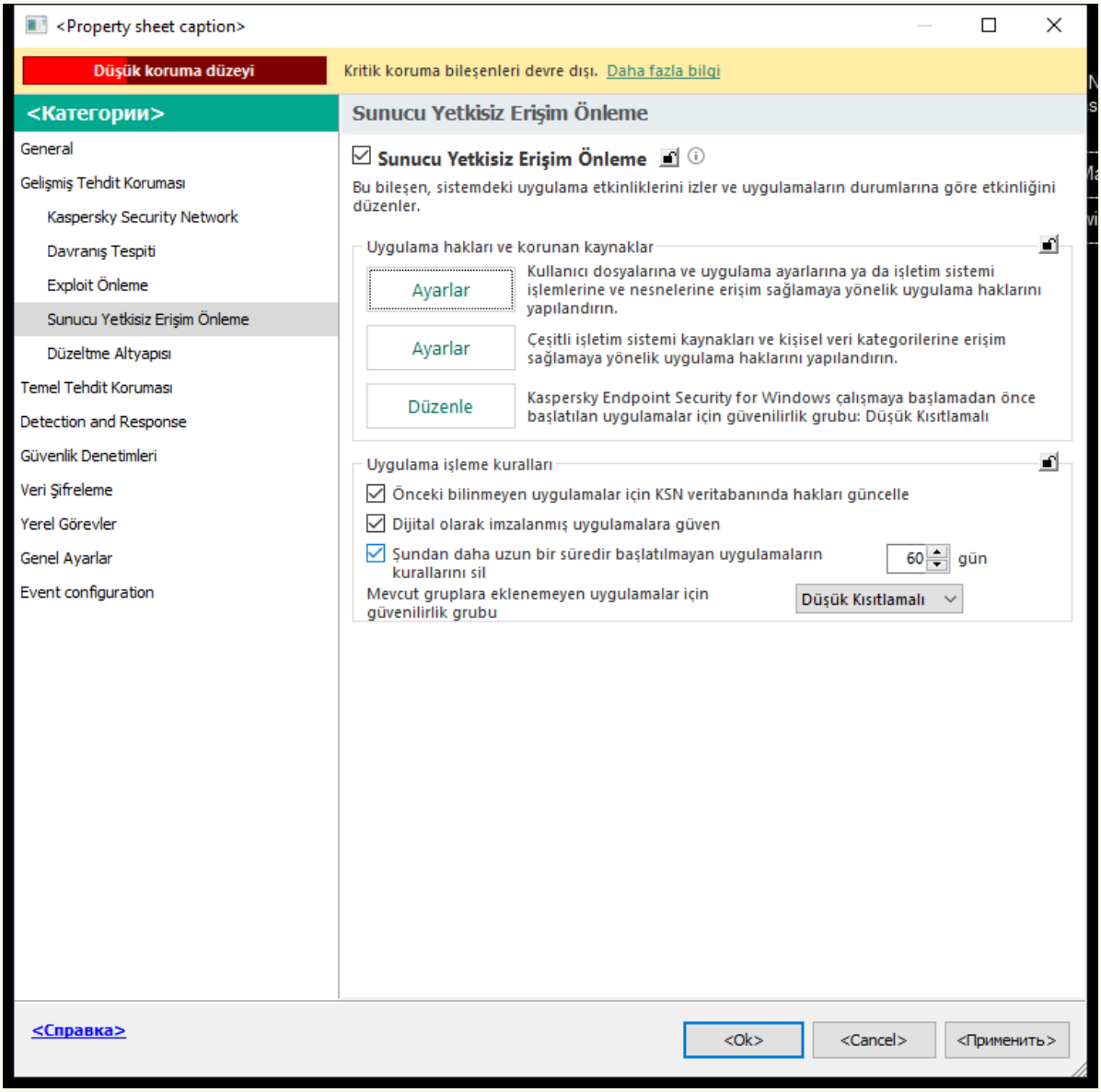
Yönetim Konsolu'nda (MMC) bilinmeyen uygulamalar için bir güvenilirlik grubu nasıl seçilir

1. Kaspersky Security Center Yönetim Konsolu'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama işleme kuralları** bloğunda, gerekli güvenilirlik grubunu seçmek için **Mevcut gruplara eklenemeyen 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.

Web Console ve Cloud Console'da bilinmeyen uygulamalar için bir güvenilirlik grubu nasıl seçilir

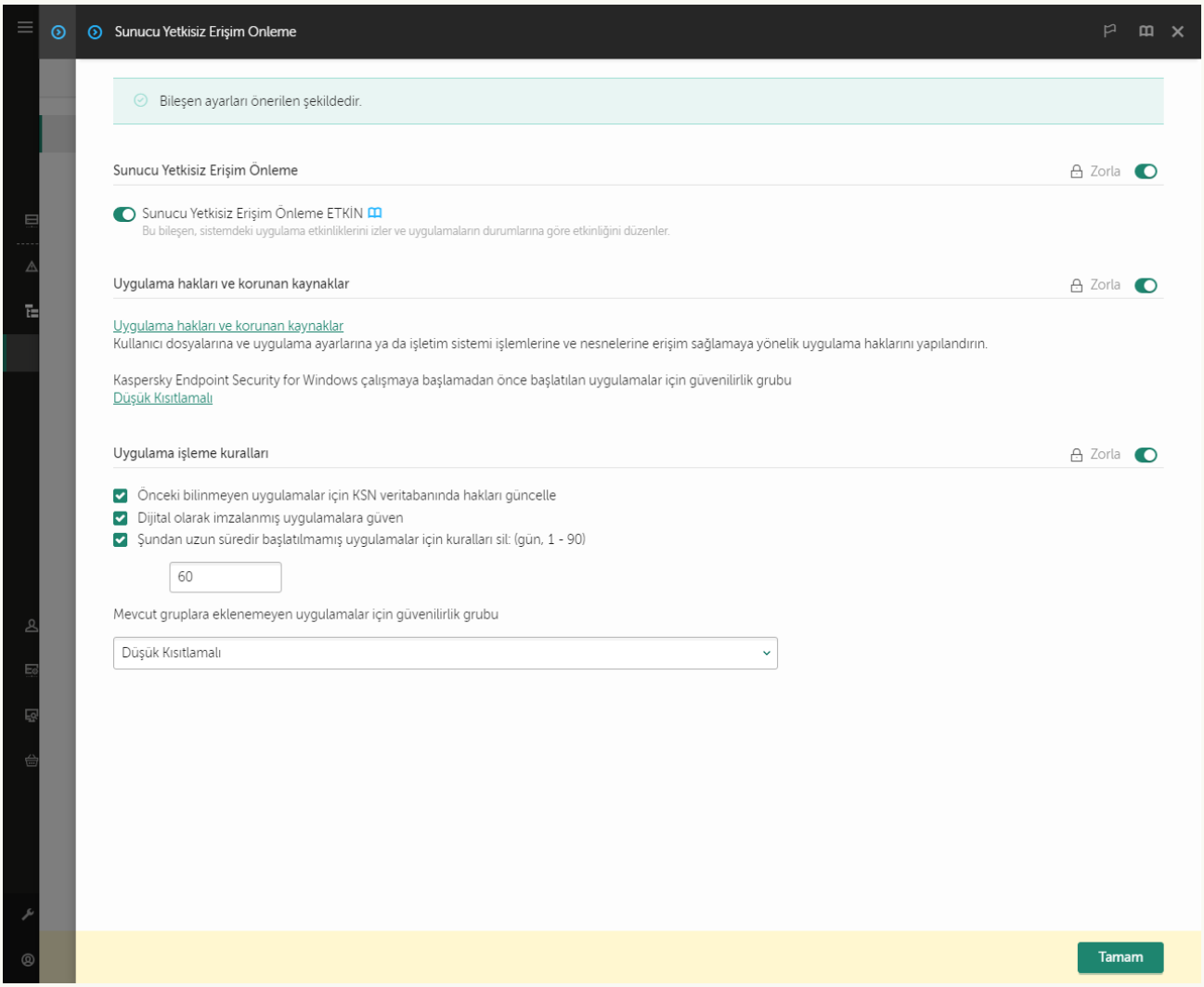
1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama işleme kuralları** bloğunda, gerekli güvenilirlik grubunu seçmek için **Mevcut gruplara eklenemeyen 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.

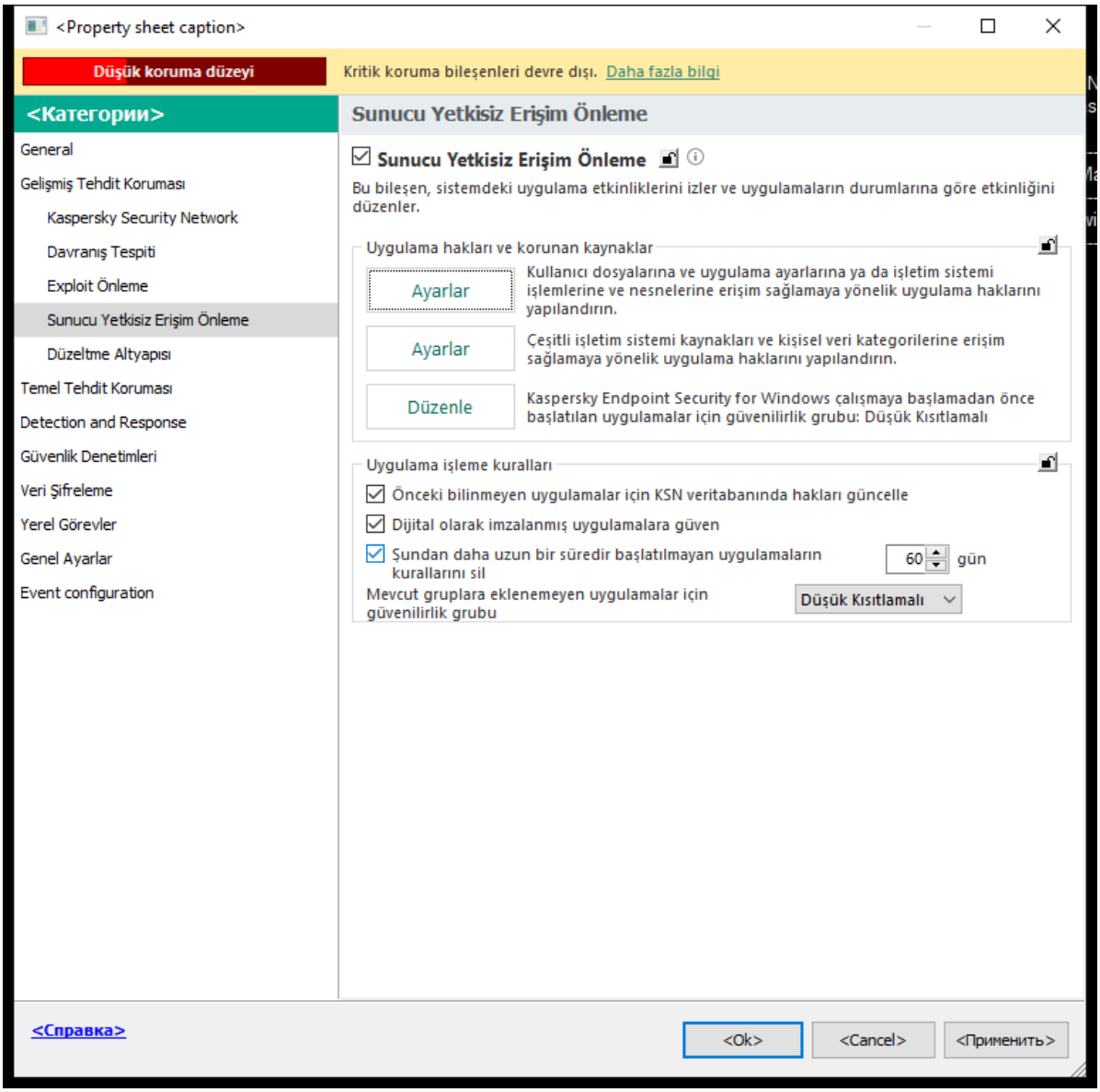
Dijital imzalı uygulamalar için bir güvenilirlik grubu Yönetim Konsolu (MMC) ile nasıl seçilir

1. Kaspersky Security Center Yönetim Konsolu'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama işleme kuralları** bloğunda, güvenilir satıcıların dijital imzalarını içeren uygulamalar için Güvenilirlik 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.

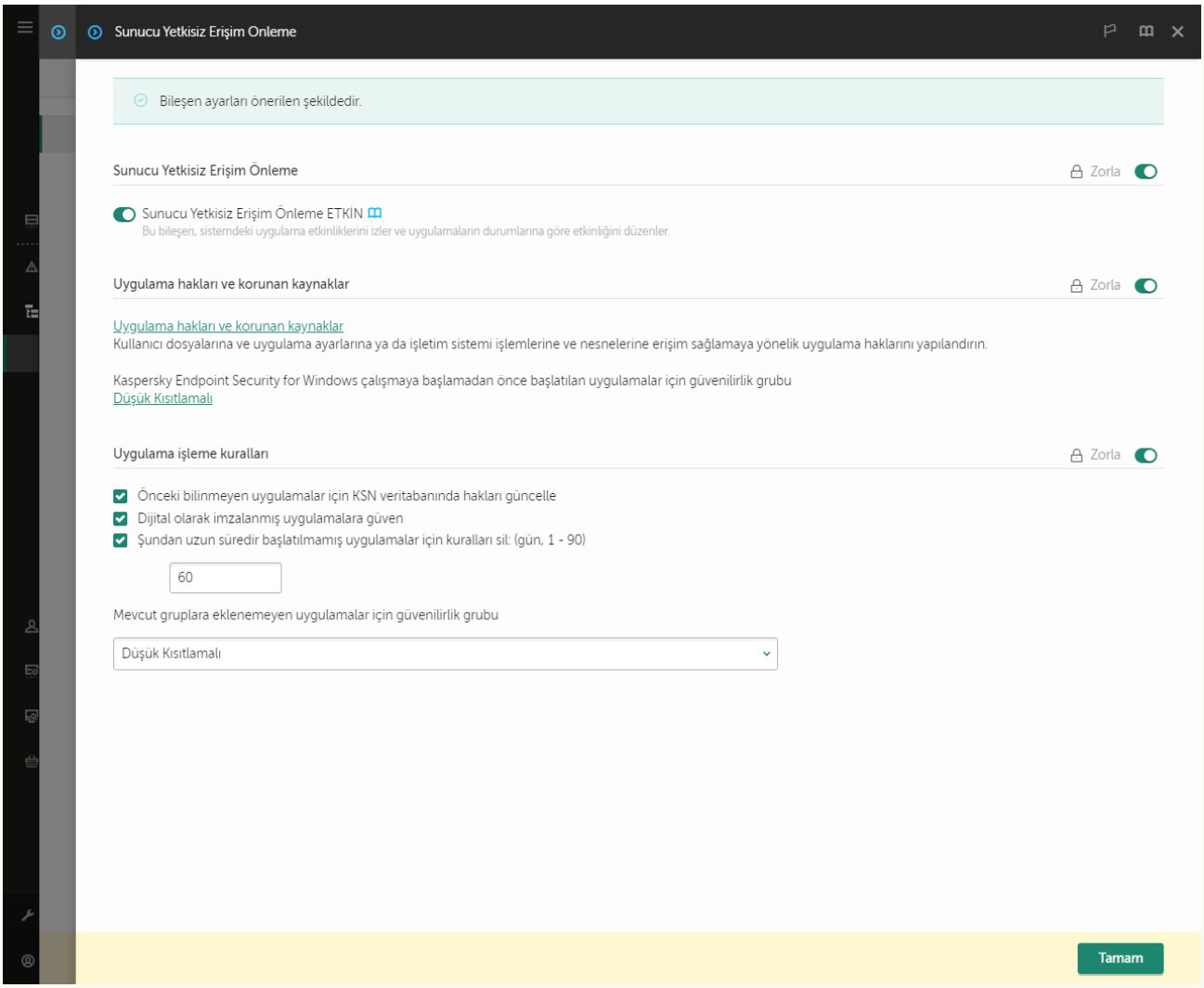
   Onay kutusunun işareti kaldırılırsa Sunucu Yetkisiz Erişim Önleme bileşeni, dijital olarak imzalanan uygulamaları güvenilir kabul etmez ve onların güvenilirlik gruplarını belirlemek için başka parametreler kullanır.

6. Değişikliklerinizi kaydedin.

Dijital imzalı uygulamalar için bir güvenilirlik grubu Web Console ve Cloud Console ile nasıl seçilir

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama işleme kuralları** bloğunda, güvenilir satıcıların dijital imzalarını içeren uygulamalar için Güvenilirlik 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, güvenilir satıcıların dijital imzalarını içeren uygulamalar için Güvenilirlik 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

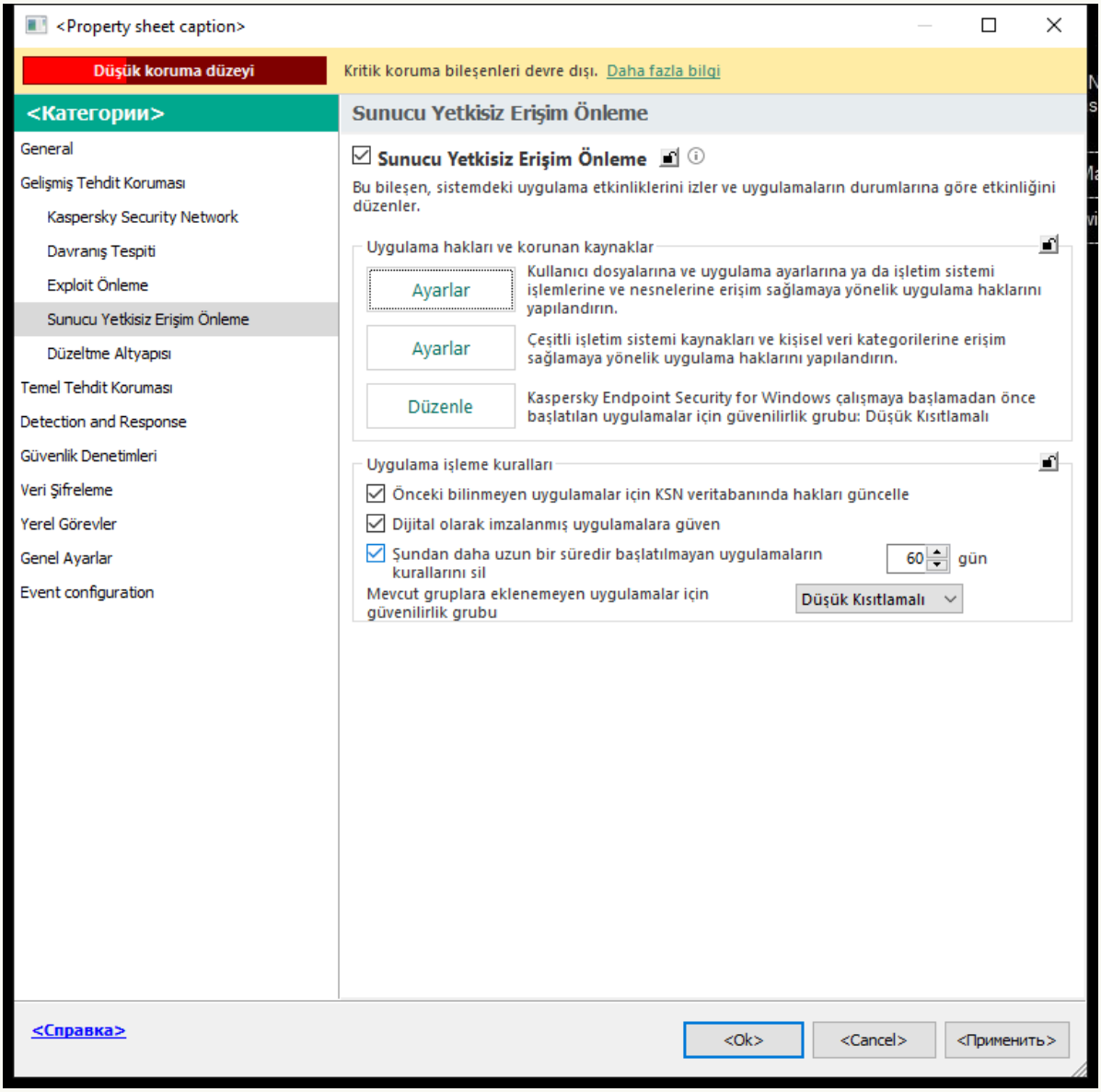
Varsayılan olarak uygulama etkinliği, Kaspersky Endpoint Security'nin uygulamaya ilk kez başladığında atadığı belirli güvenilirlik grubu için tanımlanmış uygulama haklarına göre denetlenir. Gerekirse bütün bir güvenilirlik grubu, tek bir uygulama veya bir güvenilirlik grubu içindeki bir grup uygulamanın, 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'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

6. **Uygulama hakları** sekmesini seçin.

7. **Ekle**'ye tıklayın.

8. 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.

9. **Yenile** düğmesine tıklayın.

   Kaspersky Endpoint Security uygulamayı, yönetilen bilgisayarlardaki yüklü uygulamalar birleştirilmiş listesinde arar. Kaspersky Endpoint Security, arama kriterlerinizi karşılayan uygulamaların bir listesini görüntüler.

10. Gereken uygulamayı seçin.

11. **Seçilen uygulamayı güvenilirlik grubuna ekle** açılır listesinden **Varsayılan gruplar** seçimini yapın ve **Tamam**'a tıklayın.

    Uygulama varsayılan gruba eklenecektir.

12. İlgili uygulamayı seçin ve ardından uygulamanın bağlam menüsünden **Uygulama hakları**'nı seçin.

    Bu, uygulama özelliklerini açar.

13. Aşağıdakilerden birini yapın:

    - Uygulamanın işletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarları ile çalışmayı düzenleyen güvenilirlik gruplarını düzenlemek için **Dosya ve sistem kayıt defteri** sekmesini seçin.
    - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** sekmesini seçin.

Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

14. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** ( ) veya **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.

Web Console'da ve Cloud Console'da uygulama hakları nasıl değiştirilir

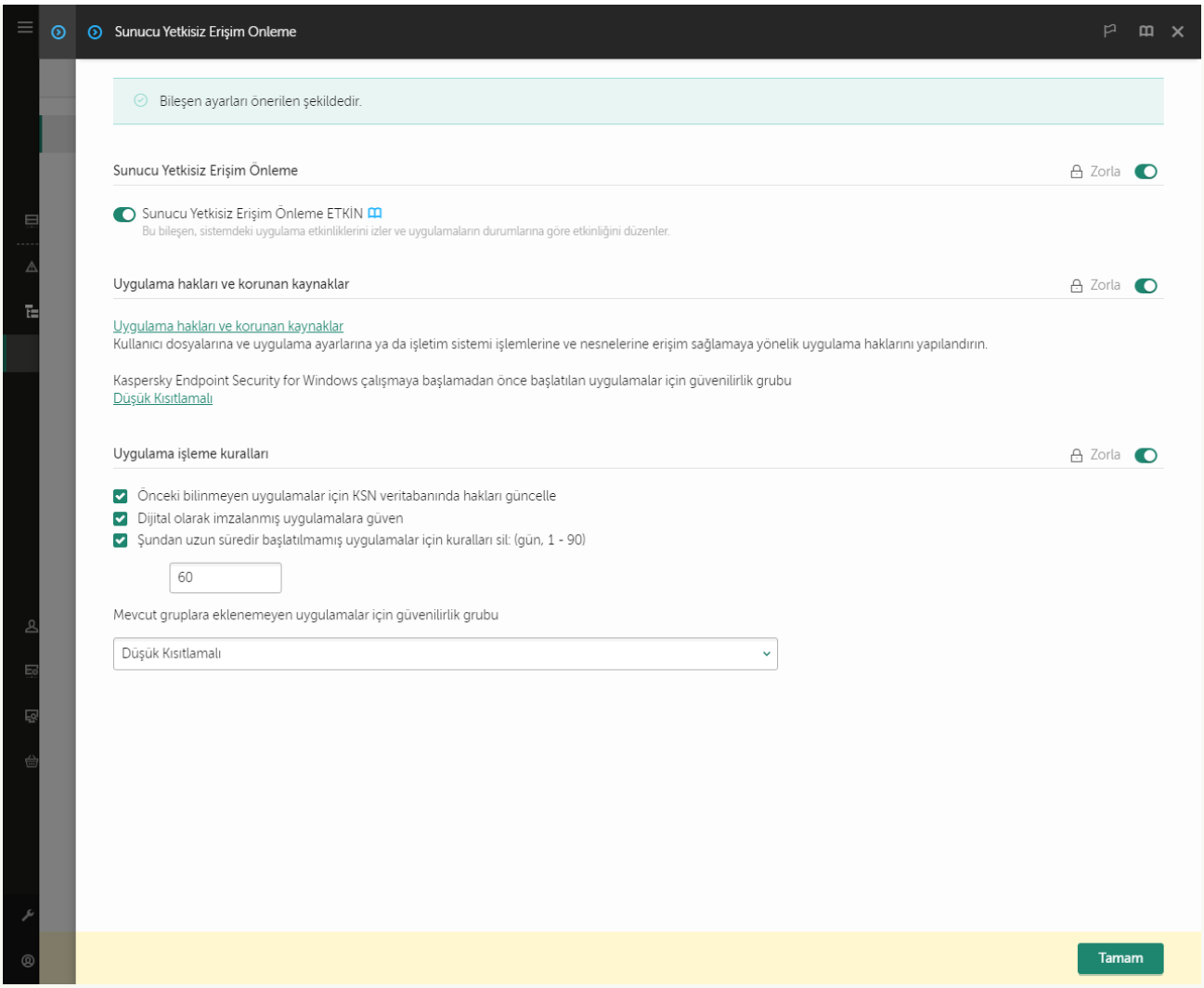
1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

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, 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. Sihirbazdan çıkın.

    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.

Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

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:
   - Uygulamanın işletim sistemi kayıt defteri, kullanıcı dosyaları ve uygulama ayarları ile çalışmayı düzenleyen güvenilirlik gruplarını düzenlemek için **Dosya ve sistem kayıt defteri** sekmesini seçin.
   - İşletim sistemi işlemlerine ve nesnelerine erişimi düzenleyen güvenilirlik grubu haklarını düzenlemek için **Haklar** sekmesini seçin.
7. İlgili kaynak için, ilgili eylemin sütununda, bağlam menüsünü açmak için sağ tıklayın ve gerekli seçeneği seçin: **Devral**, **İzin ver** ( ), **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
Açmadan önce 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.

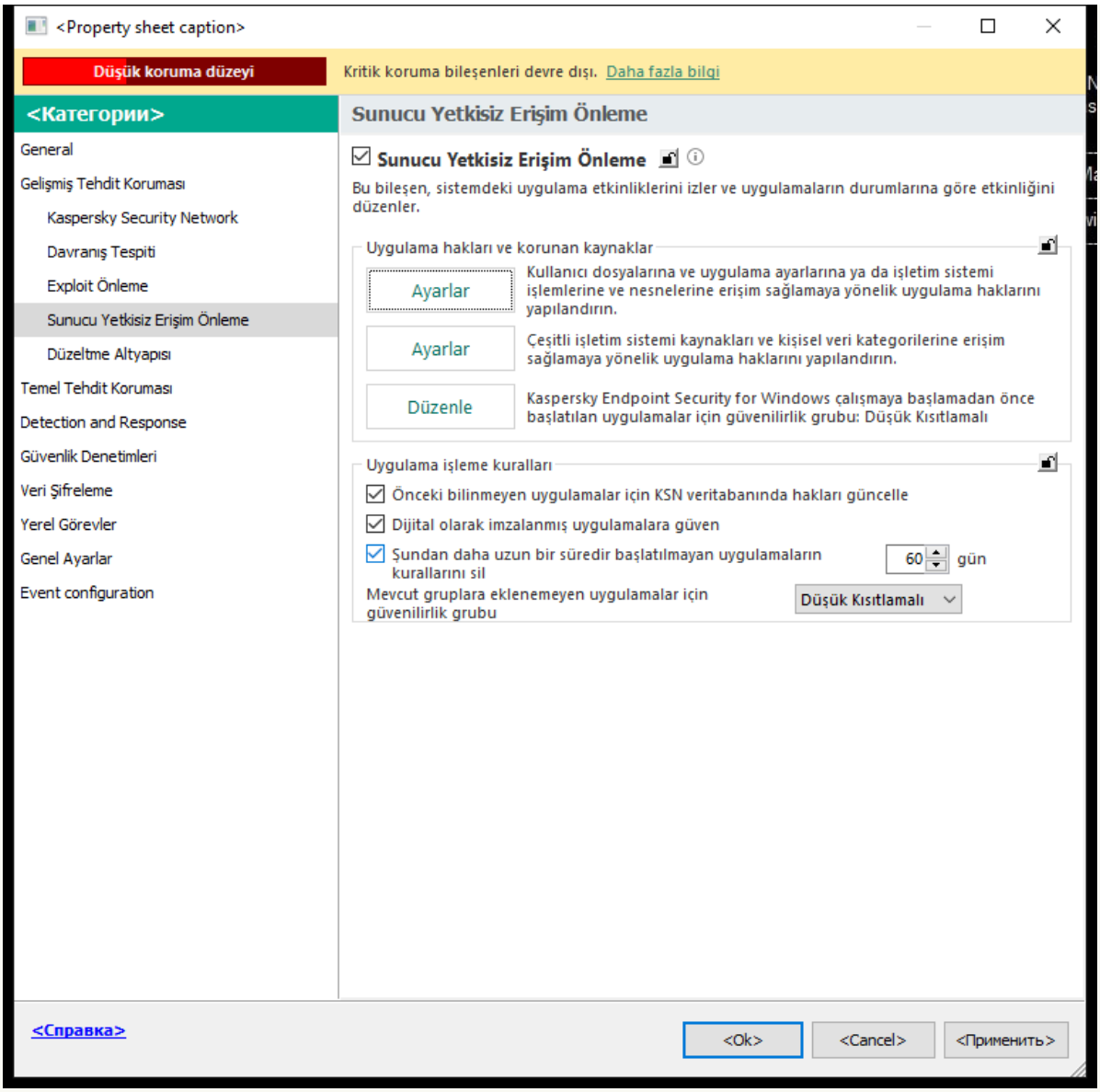
Uygulama etkinliğini izleme	Kaspersky Endpoint Security, uygulamanın işletim sistemindeki dosya ve ağ etkinliğini izlemez. Uygulama etkinliği aşağıdaki bileşenler tarafından izlenir: Davranış Tespiti, Exploit Önleme, Sucnucu Yetksiz Erişim Önleme, Düzeltme Altyapısı ve Güvenlik Duvarı.
Üst işlemin (uygulama) 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.
Kaspersky Endpoint Security for Windows 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 bağlantı noktası numaralarını da taramalardan hariç tutabilirsiniz.

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'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **Uygulama hakları ve korunan kaynaklar** bloğunda, **Ayarlar** düğmesine tıklayın.

   Bu, uygulama hakları yapılandırma penceresini ve korunan kaynaklar listesini açar.

6. **Korunan kaynaklar** sekmesini seçin.

   Pencerenin sol tarafında korunan kaynakların bir listesini ve belirli bir güvenilirlik grubuna bağlı olarak bu kaynaklara erişim için karşılık gelen hakları göreceksiniz.

7. Yeni bir korumalı kaynak eklemek istediğiniz korumalı kaynaklar kategorisini seçin.

   Bir alt kategori eklemek istiyorsanız, **Ekle** → **Kategori**'ye tıklayın.

8. **Ekle** düğmesine tıklayın. Açılır listeden eklemek istediğiniz kaynak türünü seçin: **Dosya veya klasör** veya **Kayıt defteri anahtarı**.

9. Açılan pencerede bir dosya, klasör veya kayıt defteri anahtarı seçin.

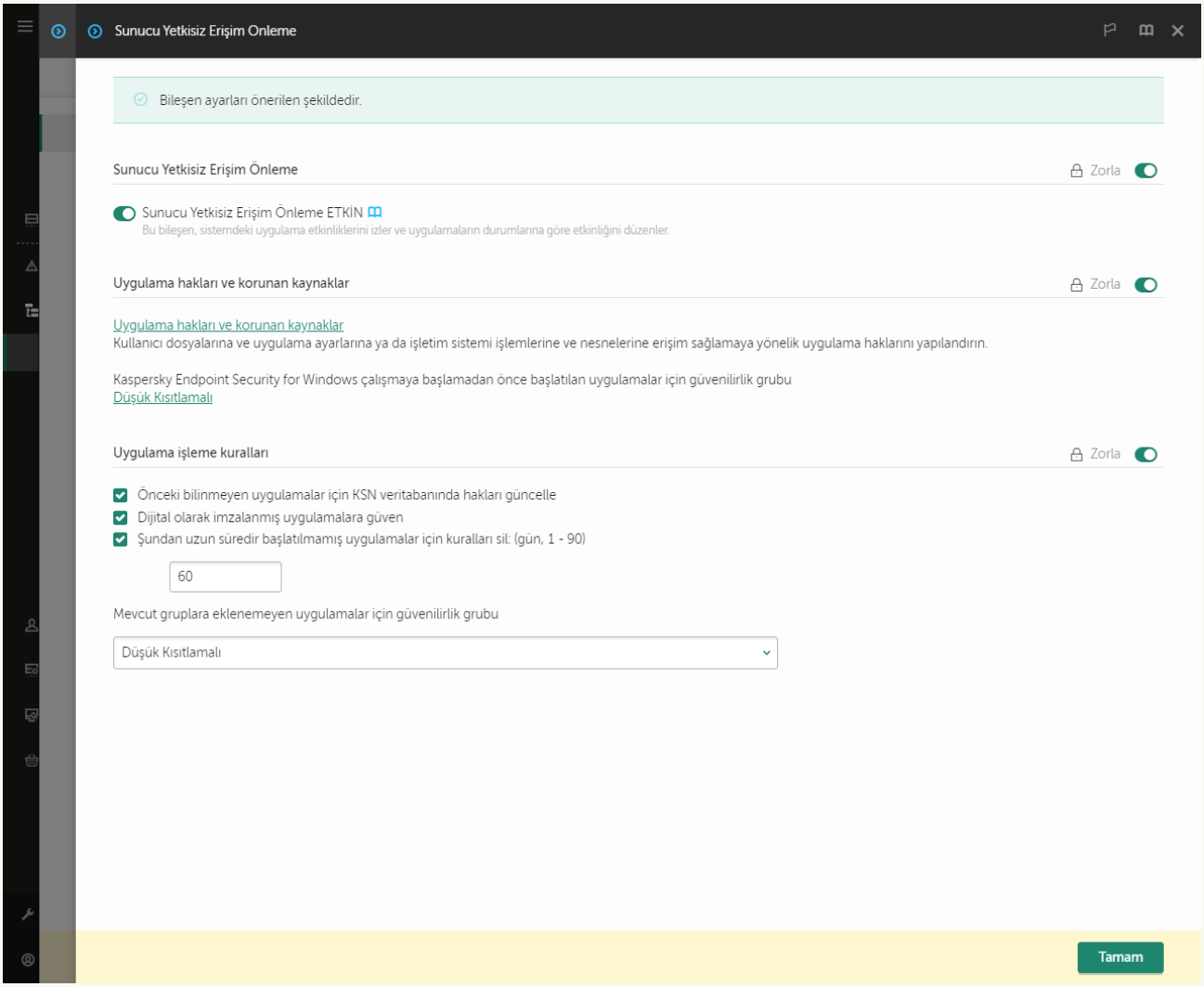
   Eklenen kaynaklara erişmek için uygulamaların haklarını görüntüleyebilirsiniz. Bunu yapmak için, pencerenin sol kısmında ek bir kaynak seçin; Kaspersky Endpoint Security her güvenilirlik grubu için erişim haklarını gösterecektir. Ayrıca, yeni bir kaynağın yanındaki onay kutusunu kullanarak kaynaklarla uygulama etkinliğinin denetimini devre dışı bırakabilirsiniz.

10. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir korumalı kaynak nasıl oluşturulur

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

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** sekmesini seçin.

   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. Yeni bir korumalı kaynak eklemek istediğiniz korumalı kaynaklar kategorisini seçmek için **Grup adı** bağlantısına tıklayın.

   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. Sihirbazdan çıkın.

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).

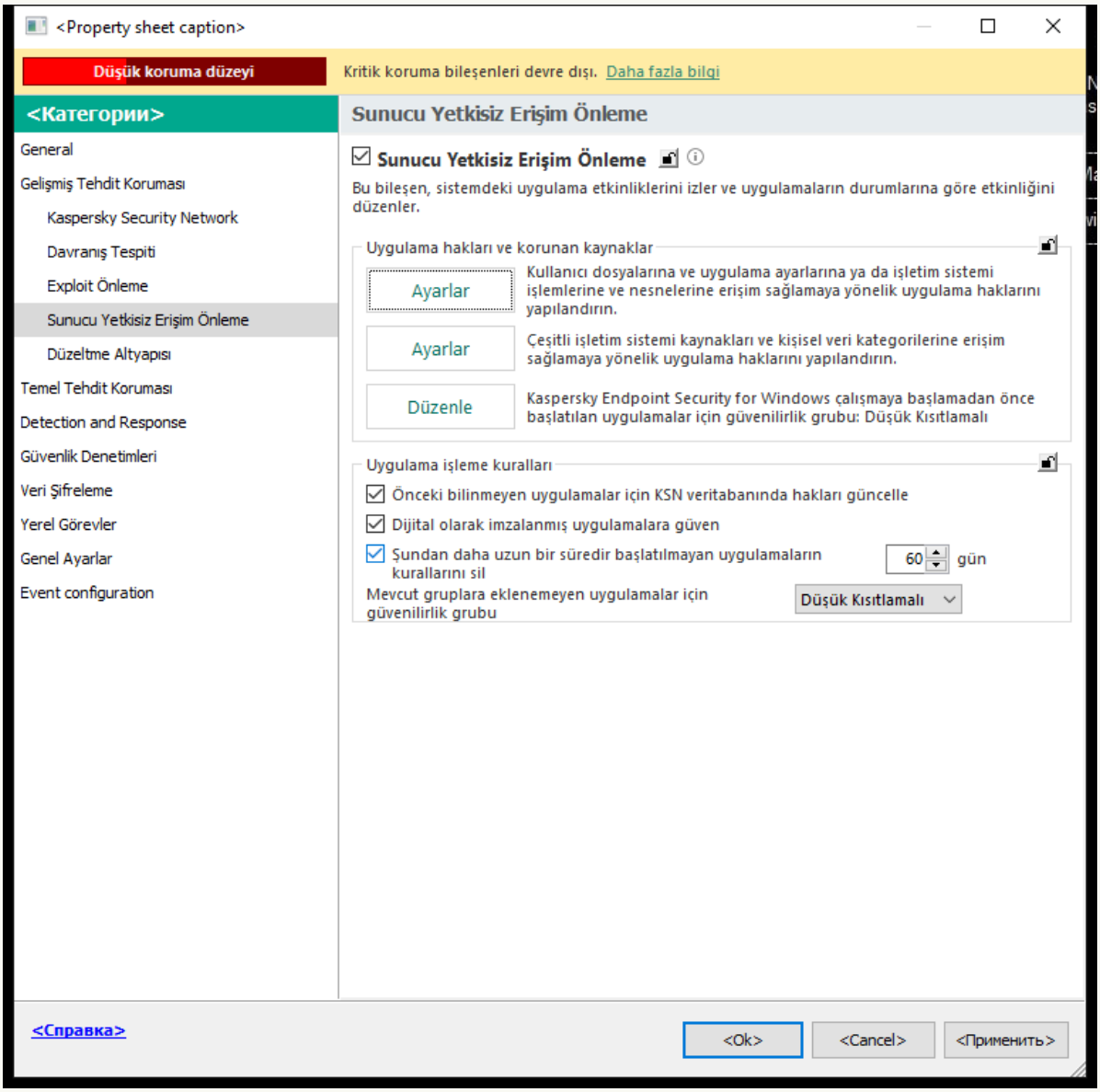
Bilgileri silinmiş bir uygulamayı başlattığınızda, Kaspersky Endpoint Security uygulamayı ilk kez başlatılıyormuş gibi analiz eder.

Yönetim Konsolu'nda (MMC) kullanılmayan uygulamalar hakkındaki bilgilerin otomatik olarak silinmesini yapılandırma

1. Kaspersky Security Center Yönetim Konsolu'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 → Sunucu Yetkisiz Erişim Önleme**'yi seçin.



Yetkisiz Erişim Önleme ayarları

5. **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.

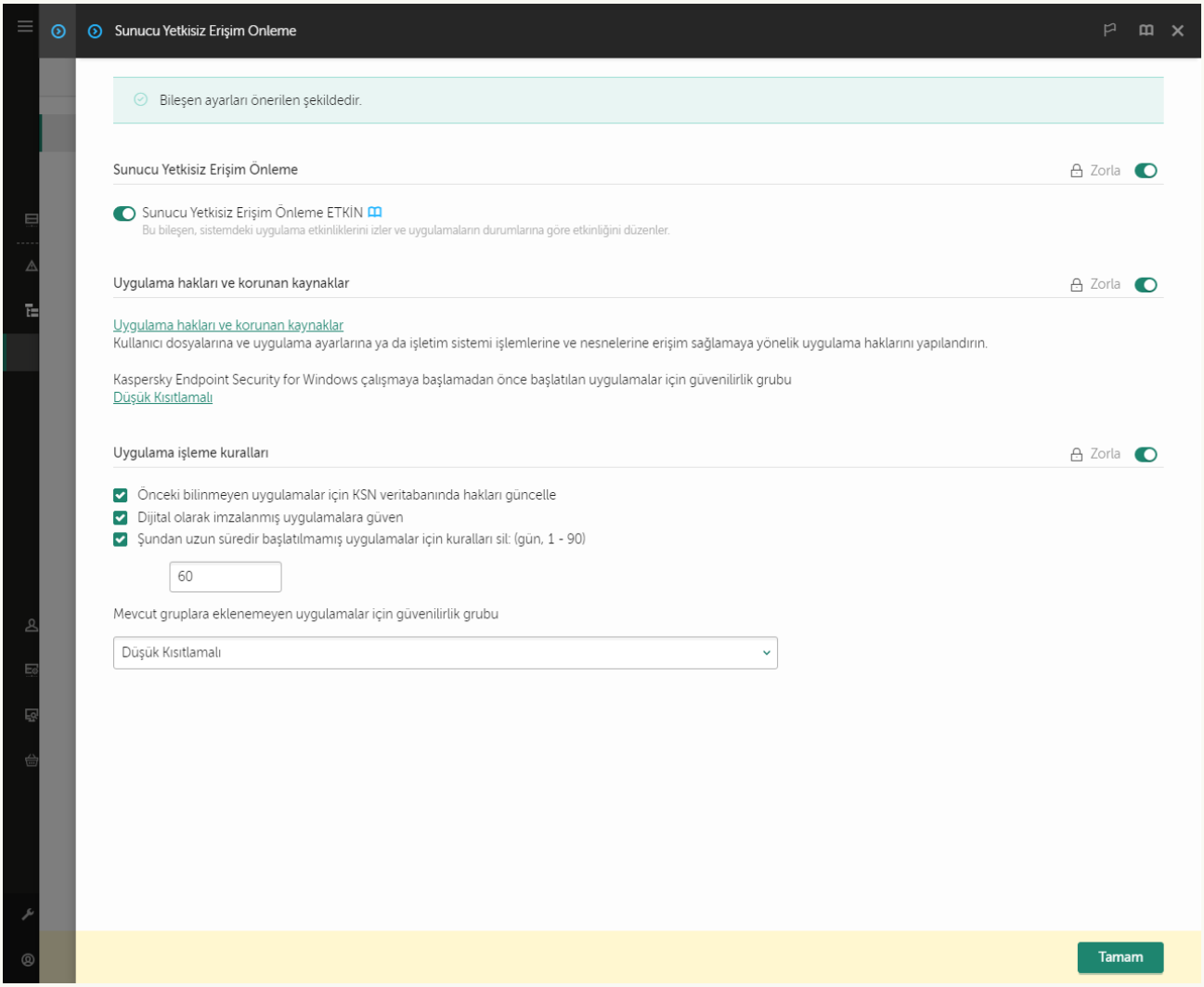
  Bir güven grubuna manuel olarak koyduğunuz veya erişim haklarını manuel olarak yapılandırdığınız uygulamalarla ilgili bilgiler, Kaspersky Endpoint Security tarafından herhangi bir depolama süresi sınırı olmadan süresiz olarak saklanır. Kaspersky Endpoint Security, yalnızca güven grubu ve uygulama hakları otomatik olarak belirlenmiş uygulamalar hakkındaki bilgileri 30 gün geçtikten sonra siler.

6. Değişikliklerinizi kaydedin.

[Web Console ve Cloud Console kullanılmayan uygulamalar hakkındaki bilgilerin otomatik olarak silinmesini yapılandırma](#)

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması** → **Sunucu Yetkisiz Erişim Önleme**'ye gidin.



Yetkisiz Erişim Önleme ayarları

5. **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.
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** 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.
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

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.

Kaspersky Endpoint Security, uygulamaların ses akışına ve video akışına erişimini varsayılan olarak aşağıdaki şekilde kontrol eder:

- *Güvenilir* ve *Düşük Kısıtlamalı* uygulamaların cihazlardan ses akışı ve video akışı almasına varsayılan olarak izin verilir.
- *Yüksek Kısıtlamalı* ve *Güvenilmez* uygulamaların cihazlardan ses akışı ve video akışı almasına varsayılan olarak 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.

Düzeltme Altyapısı

Düzeltme Altyapısı, Kaspersky Endpoint Security'nin 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'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** → **Düzeltme Altyapısı** seçimini yapın.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Düzeltme Altyapısı** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da Düzeltme Altyapısı bileşenini etkinleştirme veya devre dışı bırakma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Gelişmiş Tehdit Koruması → Düzeltme Altyapısı** bölümüne gidin.

5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Düzeltme Altyapısı** geçiş düğmesini 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.

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 dosyaların kategorisi ve tanınırlığı hakkındaki bilgilerle birlikte taranan web adreslerinin tanınırlığı hakkında bilgi sağlar.

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 Statement'a ve Kaspersky web sitesi 'ne başvurun. Kaspersky Security Network Statement 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 Center varsayılan olarak KSN kullanır. Yönetim Konsolu'nda (MMC), Kaspersky Security Center Web Console'da ve komut satırında KPSN kullanımını yapılandırabilirsiniz. Kaspersky Security Center Cloud Console üzerinden KPSN kullanımını yapılandırmak mümkün değildir.

KPSN hakkında daha fazla bilgi için lütfen Kaspersky Private Security Network belgelerine bakın.

Kaspersky Security Network'ün kullanımını etkinleştirme ve devre dışı bırakma

Kaspersky Security Network'ün kullanımını etkinleştirmek ve devre dışı bırakmak için:

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 Beyanı'nı görüntüler. Kabul ediyorsanız lütfen Kaspersky Security Network (KSN) Beyanı kullanım şartlarını okuyun ve kabul edin.

   Kaspersky Endpoint Security varsayılan olarak Genişletilmiş KSN modunu kullanır. *Genişletilmiş KSN modu*, Kaspersky Endpoint Security'nin Kaspersky'ye daha fazla veri gönderdiği bir moddur.
4. Gerekirse **Genişletilmiş KSN modunu etkinleştir** geçiş düğmesini kapalı konuma getirin.
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.

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.

Koruma bileşenleri için bulut modunu etkinleştirmek veya devre dışı bırakmak için:

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 KSN Proxy hizmeti aracılığıyla etkileşimde bulunabilir.

KSN Proxy hizmeti, aşağıdaki özellikleri sağlar:

- Kullanıcının bilgisayarı, doğrudan İnternet erişimi olmadan bile KSN'ye soru sorabilir ve KSN'ye bilgi gönderebilir.
- KSN Proxy 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 bağlantı noktasına sahip Kaspersky Security Center Yönetim Sunucusu'dur. Bu nedenle, KSN Proxy kullanılabilir olmadığında aşağıdakileri doğrulamanız gerekir:

- Yönetim Sunucusu'nda *ksnproxy* hizmetinin çalıştığı.
- Bilgisayardaki Güvenlik Duvarının 13111 numaralı bağlantı noktasını engellemediği.

KSN Proxy kullanımını şu şekilde yapılandırabilirsiniz: KSN Proxy'yi etkinleştirin veya devre dışı bırakın ve bağlantı için bağlantı noktasını yapılandırın. Bunu yapmak için Yönetim Sunucusu özelliklerini açmanız gerekir. KSN Proxy yapılandırması hakkında ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım içeriğine bakın. 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'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 → Kaspersky Security Network**'yi seçin.
5. KSN Proxy'yi etkinleştirmek veya devre dışı bırakmak için **KSN Proxy Ayarları** bloğundaki **KSN Proxy kullan** onay kutusunu kullanın.
6. Gerekirse **KSN Proxy kullanılabilir olmadığında KSN 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).
7. Değişikliklerinizi kaydedin.

Web Console'da KSN Proxy'yi etkinleştirme veya devre dışı bırakma

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Gelişmiş Tehdit Koruması → Kaspersky Security Network**'e gidin.
5. KSN Proxy'yi etkinleştirmek veya devre dışı bırakmak için **KSN Proxy kullan** onay kutusu.
6. Gerekirse **KSN Proxy kullanılabilir olmadığında KSN 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).
7. Değişikliklerinizi kaydedin.

KSN Proxy adresi, Yönetim Sunucusu adresiyle eşleşir. Yönetim Sunucusu etki alanı adı değiştirildiğinde, KSN Proxy adresini elle güncellemeniz gerekir.

KSN Proxy adresini yapılandırmak için:

1. Yönetim Konsolu'ndan **Yönetim Sunucusu → Gelişmiş → Uzaktan kurulum → Kurulum paketleri** klasörüne gidin.
2. **Kurulum paketleri** klasörünün bağlam menüsünden **Özellikler**'i seçin.
3. Açılan penceredeki **Genel** sekmesinde, KSN proxy sunucusunun yeni adresini belirtin.
4. Değişikliklerinizi kaydedin.

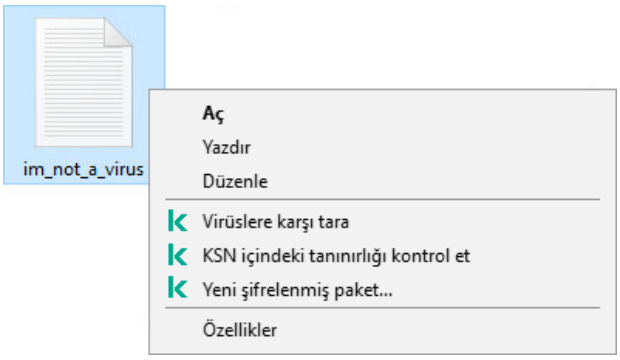
Kaspersky Security Network'den bir dosyanın saygınlığını kontrol etme

Bir dosyanın güvenliği konusunda şüpheleriniz olması durumunda, Kaspersky Security Network'te bu dosyanın tanınırlığını kontrol edebilirsiniz.

Kaspersky Security Network Statement 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). Çok sayıda Kaspersky Security Network kullanıcısı bu dosyanın güvenilir olduğunu onaylamıştır.

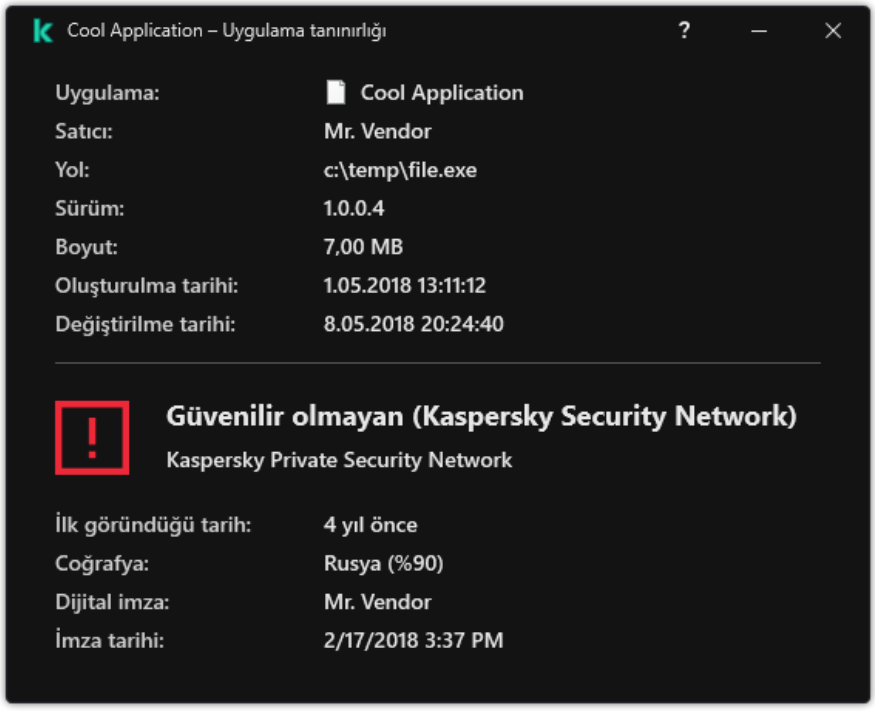
İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek meşru yazılım. Kötü amaçlı işlevler içermese bile bu uygulamalar saldırganlar tarafından kullanılabilir. Suçlular tarafından bir kullanıcının bilgisayarına veya kişisel verilerine zarar 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.

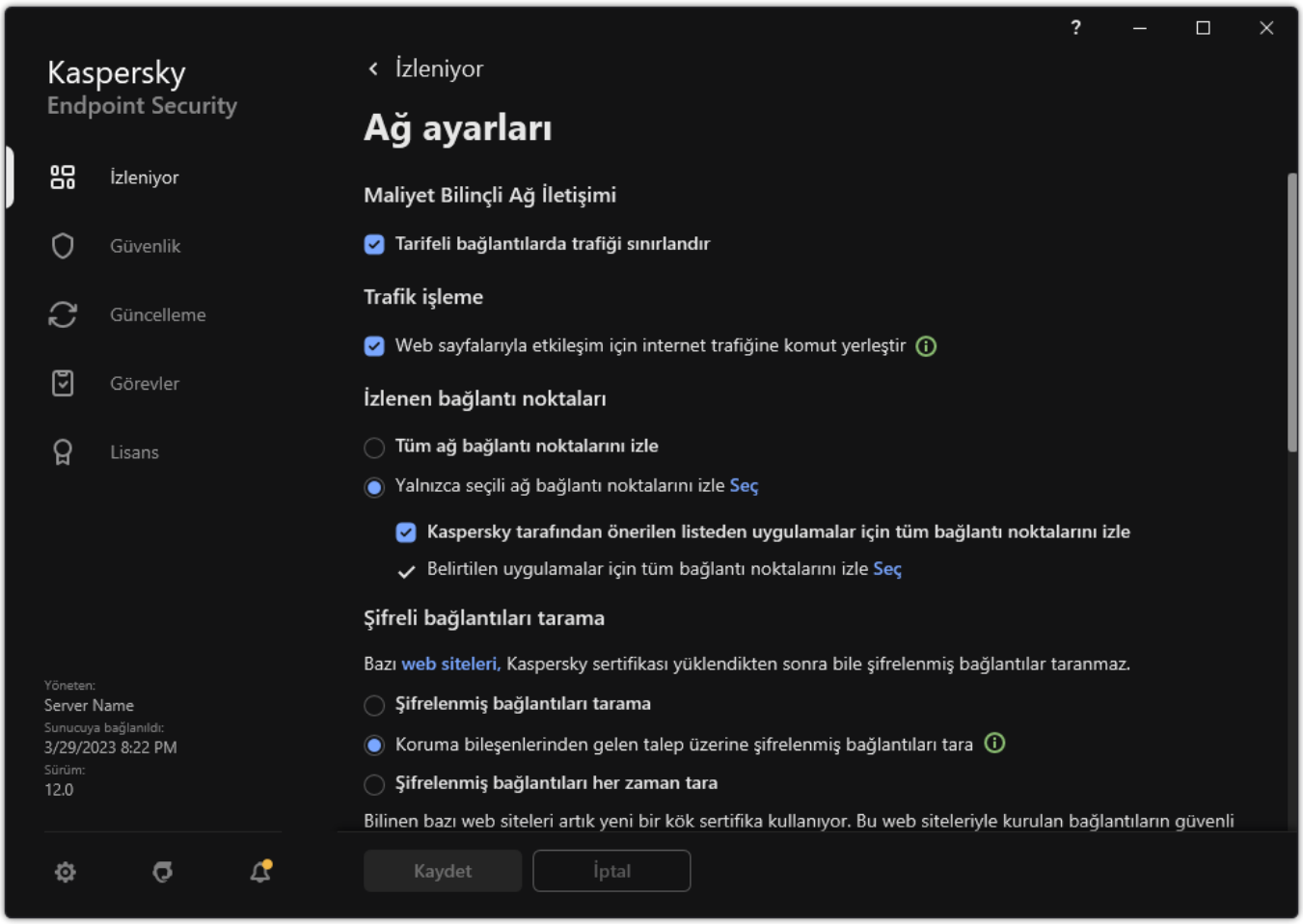
İnternet Denetimi, Posta Tehdidi Koruması, Web Tehdidi Koruması bileşenleri, aşağıdaki iletişim kurallarını kullanarak şifrelenmiş bağlantılar üzerinden aktarılan ağ trafiğinin şifresini çözebilir ve bu ağ trafiğini tarayabilir:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Şifreli bağlantıları taramayı etkinleştirme

Şifreli bağlantıları taramayı etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



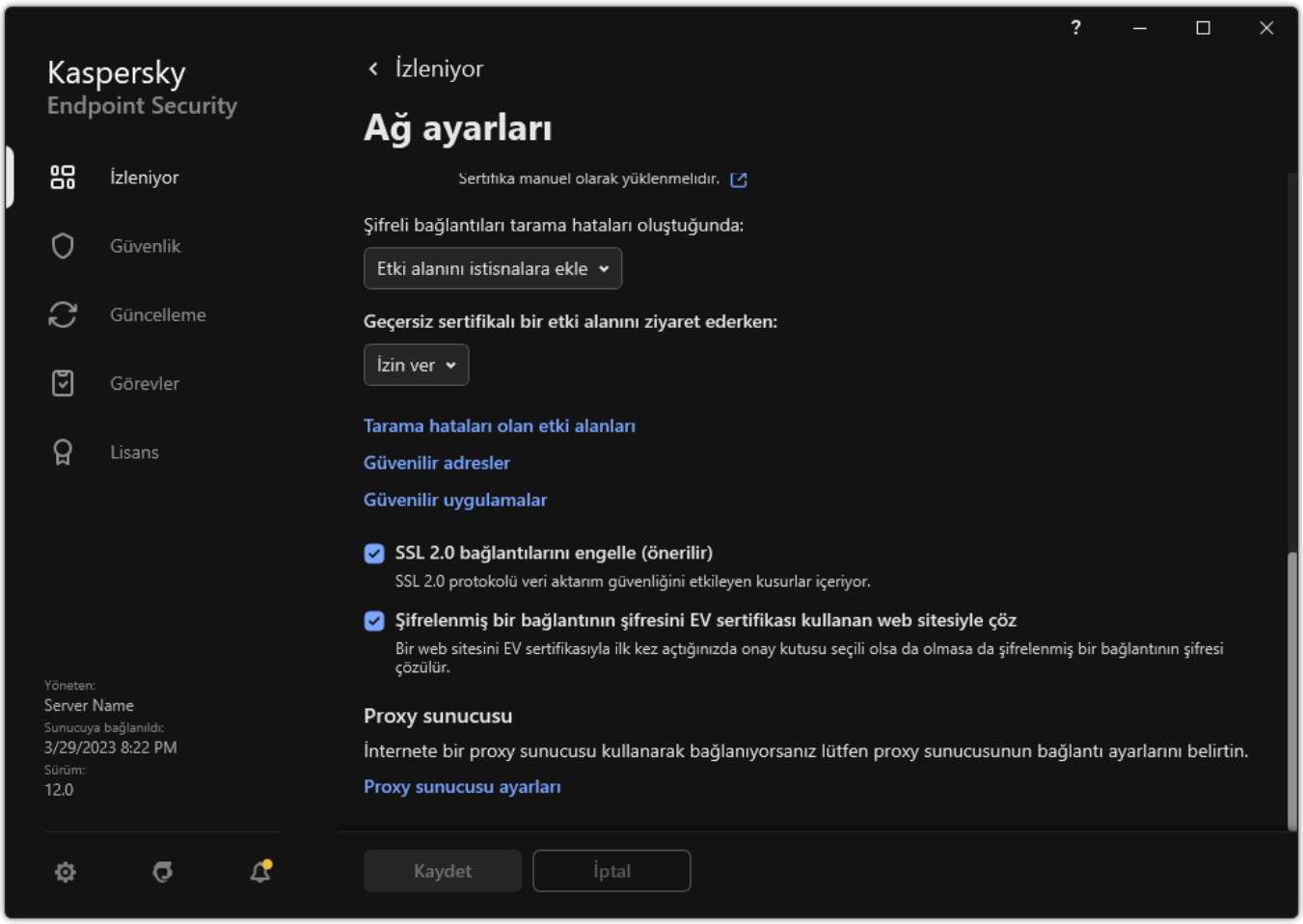
Şifreli bağlantıları tarama ayarları

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.
Geçersiz sertifikalı bir etki alanını ziyaret ederken	• **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.

- **Bağlantıyı 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.

Şifreli bağlantıları tarama hataları oluştuğunda

- **Bağlantıyı engelle**. Bu öğe seçildiğinde, bir şifreli bağlantıları tarama hatası meydana geldiğinde, Kaspersky Endpoint Security, ağ bağlantısını engeller.
- **Etki alanını istisnalara ekle**. Bu öğe seçilirse 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 **Bağlantıyı engelle**'i seçin. Kaspersky Endpoint Security ayrıca şifrelenmiş bağlantıları tarama hatası için bir olay oluşturur.

SSL 2.0 bağlantılarını engelle (önerilir)

Onay kutusu işaretlendiğinde, uygulama SSL 2.0 protokolü üzerinden kurulmuş ağ bağlantılarını engeller.

Onay kutusunun işareti kaldırıldığında, uygulama SSL 2.0 protokolü üzerinden kurulan ağ bağlantılarını engellemez ve bu bağlantılar üzerinden iletilen ağ trafiğini izlemez.

Şifrelenmiş bir bağlantının şifresini EV sertifikası kullanan web sitesiyle çöz

EV sertifikaları (Gelişmiş Doğrulama Sertifikaları), 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'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. **Güvenilir kök sertifikaları** bloğundan **Ekle**'ye tıklayın.
6. Bu bir pencere açar; bu pencerede bir güvenilir kök sertifika seçin.
   Kaspersky Endpoint Security, PEM, DER ve CRT uzantılı sertifikaları destekler.
7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da güvenilir kök sertifikalarını yükleme

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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.

- 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

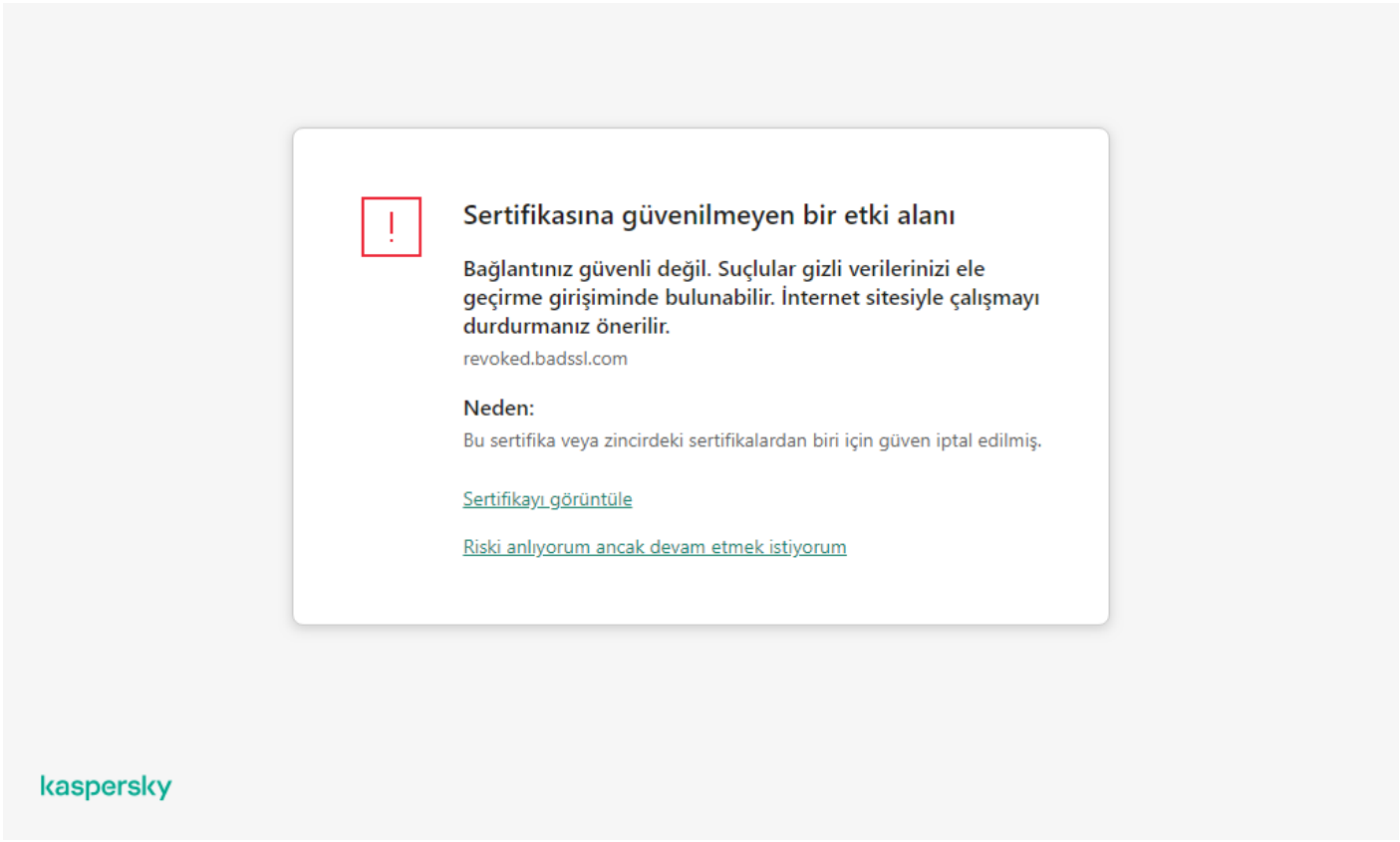
1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **Ağ ayarları** öğesini seçin.
5. **Şifreli bağlantıları tarama** bloğunda **Gelişmiş ayarlar** düğmesine tıklayın.
6. Açılan pencerede, güvenilmez bir sertifikaya sahip bir etki alanını ziyaret ederken kullanılacak uygulama işletim modunu seçin: **İzin ver** veya **Bağlantıyı engelle**.
7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da güvenilmez bir sertifika ile şifrelenmiş bağlantıların taranmasını yapılandırma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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** bölümünde, güvenilmez bir sertifikaya sahip bir etki alanını ziyaret ederken kullanılacak uygulama işletim modunu seçin: **İzin ver** veya **Bağlantıyı engelle**.
6. 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 **Bağlantıyı engelle**.
4. Değişikliklerinizi kaydedin.



Sertifikasına güvenilmeyen bir etki alanını ziyaret etme hakkında uyarı

Firefox ve Thunderbird'de şifreli bağlantıları tarama

Yükleme sonrasında, Kaspersky Endpoint Security, Kaspersky sertifikasını güvenilir sertifikaların sistem depolamasına ekler (Windows sertifika deposu). Varsayılan olarak, Firefox ve Thunderbird, Windows sertifika deposu yerine kendi tescilli Mozilla sertifika deposunu kullanır. Kuruluşunuzda Kaspersky Security Center kuruluysa ve bir bilgisayara bir ilke uygulanıyorsa, Kaspersky Endpoint Security, bu uygulamaların trafiğini taramak için Firefox ve Thunderbird'deki Windows sertifika deposunun kullanımını otomatik olarak etkinleştirir. Bilgisayara bir ilke uygulanmıyorsa, Mozilla uygulamaları tarafından kullanılacak sertifika deposunu seçebilirsiniz. Mozilla sertifika deposunu seçtiyseniz, ona elle bir Kaspersky sertifikası 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.

Mozilla deposuna bir sertifika eklemeden önce, Kaspersky sertifikasını Windows Denetim Masası'ndan (tarayıcı özellikleri) dışa aktarın. Kaspersky sertifikasını dışa aktarma hakkında ayrıntılı bilgi için lütfen Teknik Destek Bilgi Bankası 'na başvurun. Depoya sertifika eklemeyle ilgili ayrıntılar için Mozilla teknik destek web sitesini ziyaret edin.

Sertifika deposunu yalnızca uygulamanın yerel arabiriminde seçebilirsiniz.

Firefox ve Thunderbird'de 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. **Mozilla Firefox ve Thunderbird** bloğunda, **Mozilla uygulamalarında şifreli bağlantıları taramak için seçilen sertifika deposunu kullan** onay kutusunu işaretleyin.
4. Bir sertifika deposu seçin:

- **Windows sertifika deposunu kullan (önerilir)**. Kaspersky kök sertifikası, Kaspersky Endpoint Security kurulumu sırasında bu depoya eklenir.
- **Mozilla sertifika deposunu kullan**. Mozilla Firefox ve Thunderbird kendi sertifika depolarını kullanır. Mozilla sertifika deposu seçilirse, Kaspersky kök sertifikasını tarayıcı özelliklerinden bu depoya elle eklemeniz gerekir.

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 adresler** 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. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da bir web adresini şifreli bağlantı taramalarından hariç tutma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 **Güvenilir adresler** 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:

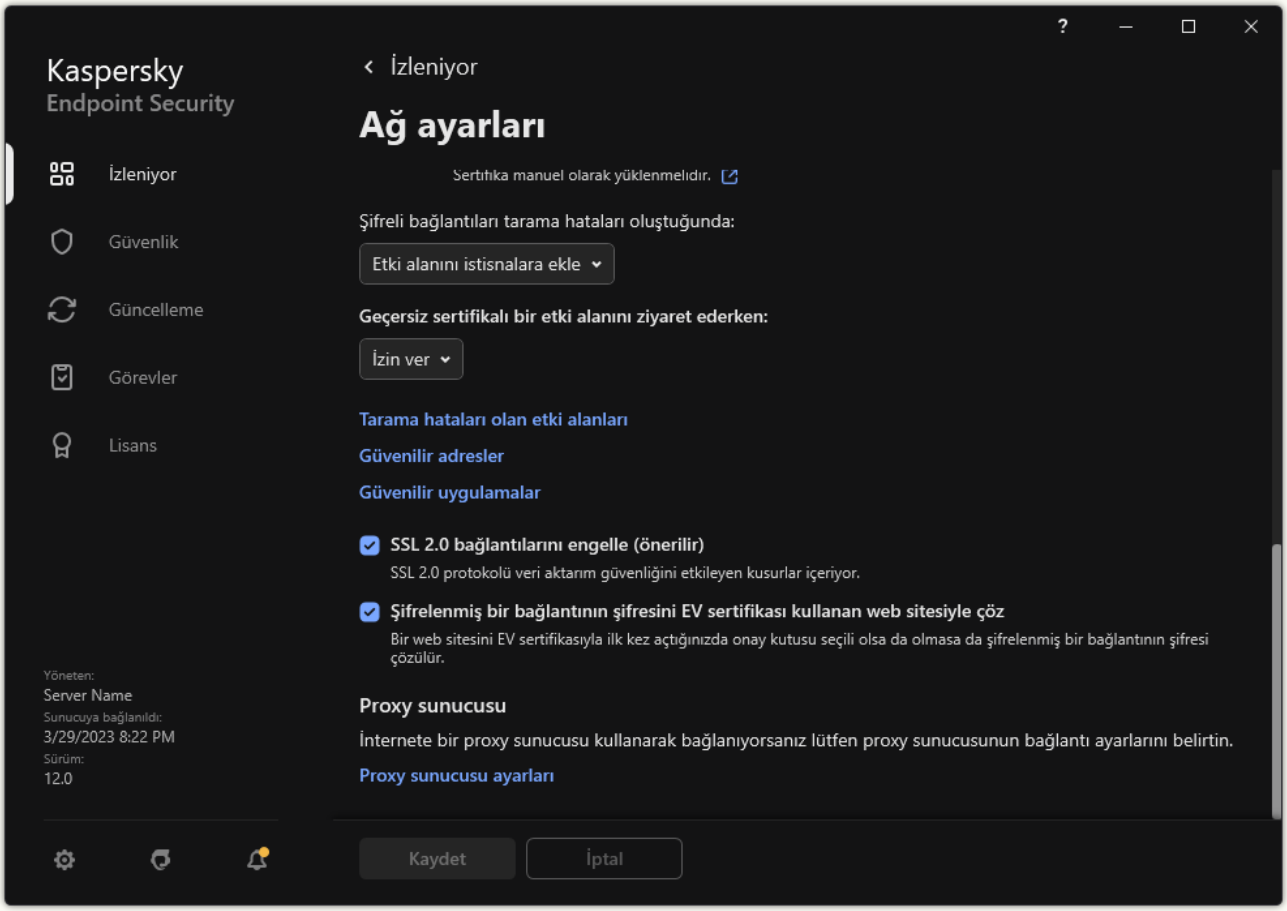
   - `domain.com` - kayıt şu adresleri içerir: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Kayıt, alt etki adlarını içermez (örneğin, `subdomain.domain.com`).
   - `subdomain.domain.com` – kayıt şu adresleri içerir: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. 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. 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 adresler** 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 hatası 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.

Veri Silme

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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** 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 cihazları seçin** 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. Sihirbazdan çıkın.
   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.

Ertelenen veri silme işlemini yapılandırırken, çalışanların tatile çıkmadan önce bilgisayarlarını kapatabileceklerini unutmayın. Böyle bir durumda bağlantısız süre aşılabilir ve veriler silinebilir. 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.

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. **Çalıştır** düğmesine 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, kullanıcının internet kaynaklarına 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).

Kaspersky Endpoint Security sadece HTTP ve HTTPS trafiğini izler.

HTTPS trafiğini izleme için şifrelenmiş bağlantı taramasını etkinleştirin.

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**. Kullanıcıların bir web sitesindeki verilere erişimini kısıtlayabilir ve örneğin web sitelerindeki resimleri 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 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.

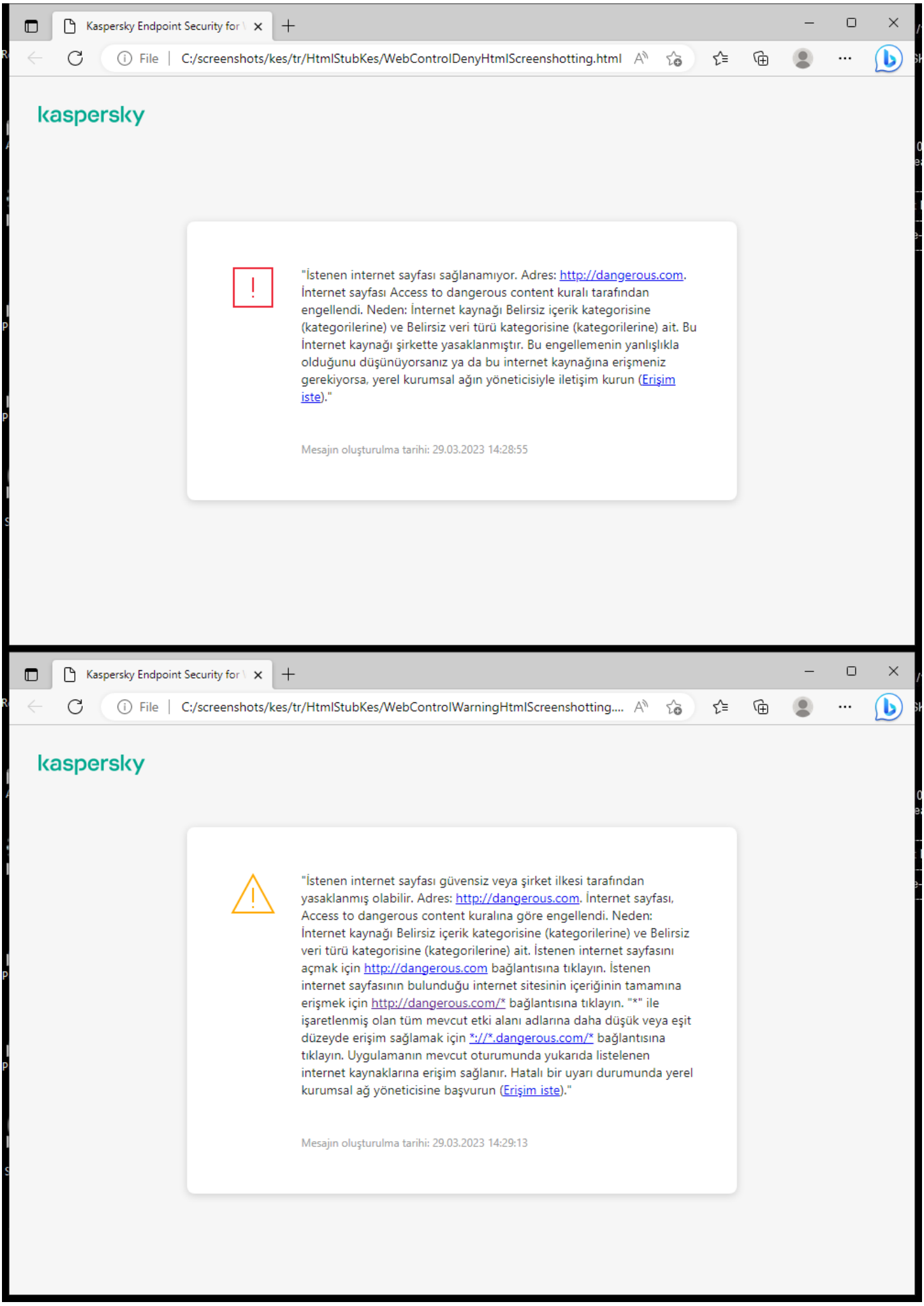
  Örneğin BT departmanı hariç olmak üzere şirketin tüm çalışanlarının bir tarayıcı üzerinden İnternete erişmesini kısıtlayabilirsiniz.

- 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'ni etkinleştirme ve devre dışı bırakma

Varsayılan olarak İnternet Denetimi etkindir.

İnternet Denetimini etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **İnternet Denetimi** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

İnternet kaynağı erişim kurallarıyla ilgili eylemler

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.

İnternet kaynağı erişim kuralı ekleme

Bir İnternet kaynağı erişim kuralı eklemek veya düzenlemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
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**. Bu değer seçilirse Kaspersky Endpoint Security, kural parametreleriyle eşleşen İnternet kaynaklarına erişime izin verir.
   - **Engelle**. Bu değer seçiliyse Kaspersky Endpoint Security, kural parametreleriyle eşleşen İnternet kaynaklarına erişimi engeller.
   - **Uyar**. Bu değer seçilirse Kaspersky Endpoint Security, kullanıcının kuralla eşleşen İnternet kaynaklarına erişim girişimi sırasında bir İnternet kaynağının istenmediği şeklinde bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

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. **Adresler** bloğundan ilgili web kaynağı adres filtresini seçin:

   - **Tüm adreslere**. İnternet Denetimi, internet kaynaklarını adrese göre filtrelemeyecektir.
   - **Tek tek adreslere**. İnternet Denetimi, listeden yalnızca web kaynağı adreslerini filtreleyecektir. Web kaynağı adresleri listesi oluşturmak için:

     a. **Adres ekle** veya **Bir adres grubu ekle** düğmesine tıklayın.

     b. Açılan pencerede, 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.

     c. Web kaynağı erişim kuralını yapılandırmak için pencereye geri dönün.

   Şifreli Bağlantıları Tarama devre dışı bırakılırsa HTTPS iletişim kuralı için yalnızca sunucu adıyla filtreleme yapabilirsiniz.

10. **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, internet kaynaklarını yalnızca belirli kullanıcılar için filtreleyecektir. Kuralı uygulamak istediğiniz kullanıcıların bir listesini oluşturmak için:

      a. **Ekle**'ye tıklayın.

      b. Açılan pencerede, web kaynağı erişim kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı grubunu seçin.

      c. Web kaynağı erişim kuralını yapılandırmak için pencereye geri dönün.

11. **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.

12. Değişikliklerinizi kaydedin.

İnternet kaynağı erişim kurallarına öncelikler atama

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.

Kuralları belirli bir sırayla düzenleyerek kurallar listesinden her bir kurala öncelik atayabilirsiniz.

Bir İnternet kaynağı erişim kuralına öncelik atamak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
3. **Ayarlar** bloğunda, **İnternet kaynaklarına erişim kuralları** düğmesine tıklayın.
4. Açılan pencerede, önceliğini değiştirmek istediğiniz kuralı seçin.
5. Kuralı, web kaynağı erişim kuralları listesinde ilgili konuma taşımak için **Yukarı** ve **Aşağı** düğmelerini kullanın.
6. Değişikliklerinizi kaydedin.

İnternet kaynağı erişim kuralını etkinleştirme ve devre dışı bırakma

Bir İnternet kaynağı erişim kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
3. **Ayarlar** bloğunda, **İnternet kaynaklarına erişim kuralları** düğmesine tıklayın.
4. Açılan pencerede, etkinleştirmek veya devre dışı bırakmak istediğiniz kuralı seçin.
5. **Durum** sütununda aşağıdakileri yapın:
   - Kuralın kullanımını etkinleştirmek istiyorsanız **Açık** değerini seçin.
   - Kuralın kullanımını devre dışı bırakmak istiyorsanız **Kapalı** değerini seçin.
6. Değişikliklerinizi kaydedin.

İnternet Denetimi kurallarını dışa ve içe aktarma

İnternet Denetimi kuralları listesini bir XML 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'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 kuralları listesini dışa aktarmak için:
   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla bağlantı noktası 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.
6. 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.
7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da İnternet Denetimi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 **Kural Listesi** bloğunda:
   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.
6. Kural listesini içeri aktarmak için **Kural Listesi** bloğunda:

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.

7. Değişikliklerinizi kaydedin.

İnternet kaynağı erişim kurallarını test etme

İnternet Denetimi kurallarının tutarlılığını denetlemek amacıyla bunları test edebilirsiniz. Bu amaçla İnternet Denetimi bileşeni, Kuralları tanılama işlevini içerir.

İnternet kaynağı erişim kurallarını test etmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
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.

İnternet kaynağı adreslerinin listesini dışa aktarma ve içe aktarma

Bir İnternet kaynağı erişim kuralında İnternet kaynağı adreslerinin listesini oluşturduysanız .txt dosyasına dışa aktarabilirsiniz. Ardından bir erişim kuralını yapılandırırken İnternet kaynağı adreslerinin yeni listesini elle oluşturmaktan kaçınmak için dosyadan bu listeyi içe aktarabilirsiniz. Örneğin benzer parametrelerle erişim kuralları oluştururursanız İnternet kaynağı adreslerinin listesini dışa aktarma ve içe aktarma seçeneği faydalı olabilir.

İnternet kaynağı adreslerinin listesini bir dosyaya içe/dışa aktarmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
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 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.

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 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.

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:

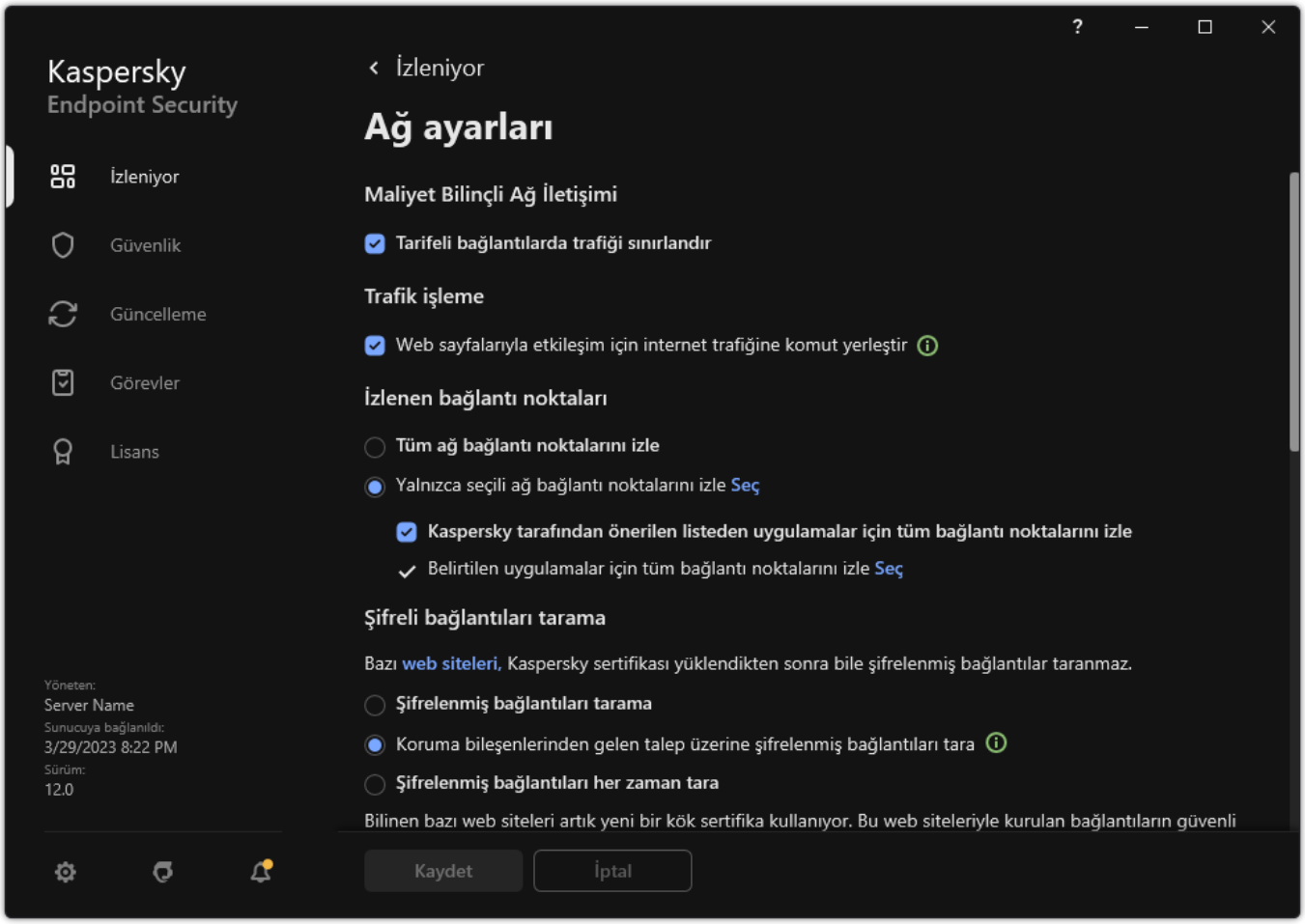
- Web sitesini engelleme (*Önemli olaylar* durumu).
- Önerilmeyen bir web sitesini ziyaret etme (*Uyarılar* durumu).
- İzin verilen bir web sitesine ziyaret (*Bilgilendirici mesajlar* durumu).

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 dosyasını internet trafiğine eklemek için:

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 kullanıcının bilgisayarına günlük kaydını yapılandırmak için:

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.

3. **Bildirim ayarları** bloğunda **Bildirimler** 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 ve 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 için olay günlük kaydını etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
3. **Diğer** bloğunda **Gelişmiş Ayarlar** düğmesine tıklayın.
4. Açılan pencerede, **İzin verilen sayfaların açılması için günlük kaydı tut** kutucuğunu işaretleyin.
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.

  Kullanıcı İnternet kaynağının yanlışlıkla engellendiğini düşünüyorsa yerel kurumsal ağ yöneticisine önceden oluşturulmuş bir mesaj göndermek için İnternet kaynağı engelleme bildirimi mesajındaki bağlantıya tıklayabilir.

Uyarı mesajı, bir İnternet kaynağının engellendiğini bildiren mesaj ve LAN yöneticisine gönderilen mesaj için özel şablonlar sağlanmaktadır. Bunların içeriğini değiştirebilirsiniz.

İnternet Denetimi mesajlarının şablonunu değiştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **İnternet Denetimi**'ni seçin.
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.

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 `*.` `resimleri` temsil eder.
   - `http://user.pictures.example.com`. `*.` etki alanı maskesi `resimleri` ve `kullanıcıyı` 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: `example.com` maskesi `http://example.com` ve `https://example.com` adreslerini kapsar.

   - Adres maskesi bir ağ iletişim kuralını içeriyorsa bu adres maskesi sadece adres maskesi ile aynı ağ iletişim kuralına sahip adresleri kapsar.

     Örneğin: `http://*.example.com` adres maskesi `http://www.example.com` adresini kapsar ancak `https://www.example.com` adresini kapsamaz.

9. Çift tırnak içindeki bir adres maskesi ek değiştirmeleri göz önünde bulundurmadan işlenir ancak başlangıçta adres maskesine dahil edildiyse `*` karakteri istisnadır. Çift tırnak işareti ile çevrelenen adres maskeleri için kural 5 ve 7 geçerli değildir (aşağıdaki tabloda örnek 14 – 18'e bakınız).

10. Bir İnternet kaynağının adres maskesiyle karşılaştırma yaparken kullanıcı adı ve parolası, bağlantı noktası ve karakterin büyük/küçük harf durumu göz önünde bulundurulur.

Adres maskeleri oluştururken kuralların nasıl kullanılacağının örnekleri

No.	Adres maskesi	Doğrulanacak İnternet kaynağının adresi	Adres maskesi	Yorum

			adresi kapsıyor mu?	
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.

Aygıt Denetimi

Aygıt Denetimi, bilgisayara yüklenen veya bağlanan aygıtlara (örneğin sabit sürücüler, kameralar veya Wi-Fi modülleri) kullanıcı erişimini yönetir. Bu, bilgisayarı bu tür aygıtlar bağlandığında virüslere karşı korur ve veri kaybını veya sızıntılarını önler.

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. Bu nedenle tüm aygıtların bağlantısını, örneğin USB üzerinden kısıtlayabilirsiniz.

  Aygıt erişimini aşağıdaki şekilde yapılandırabilirsiniz:

  - İzin ver – ✓.
  - Engelle – ⊘.

- **Güvenilir aygıtlar**. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

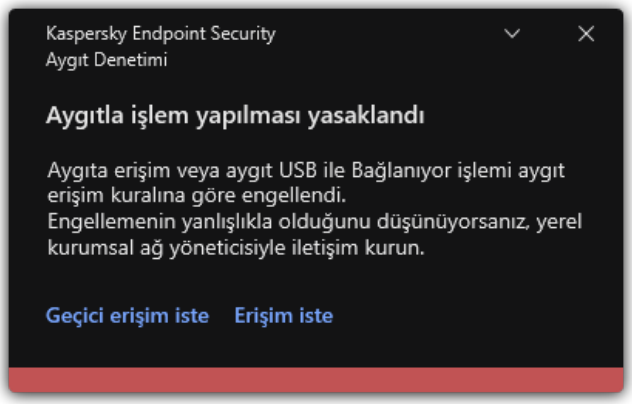
  Güvenilir aygıtları aşağıdaki verilere göre ekleyebilirsiniz:

  - **Kimliğe göre aygıtlar**. Her cihazın benzersiz bir tanımlayıcısı vardır (Donanım Kimliği veya HWID). Bu kimliği, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. Örnek aygıt kimliği: `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 satıcı kimliği (VID) ve bir ürün kimliği (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.

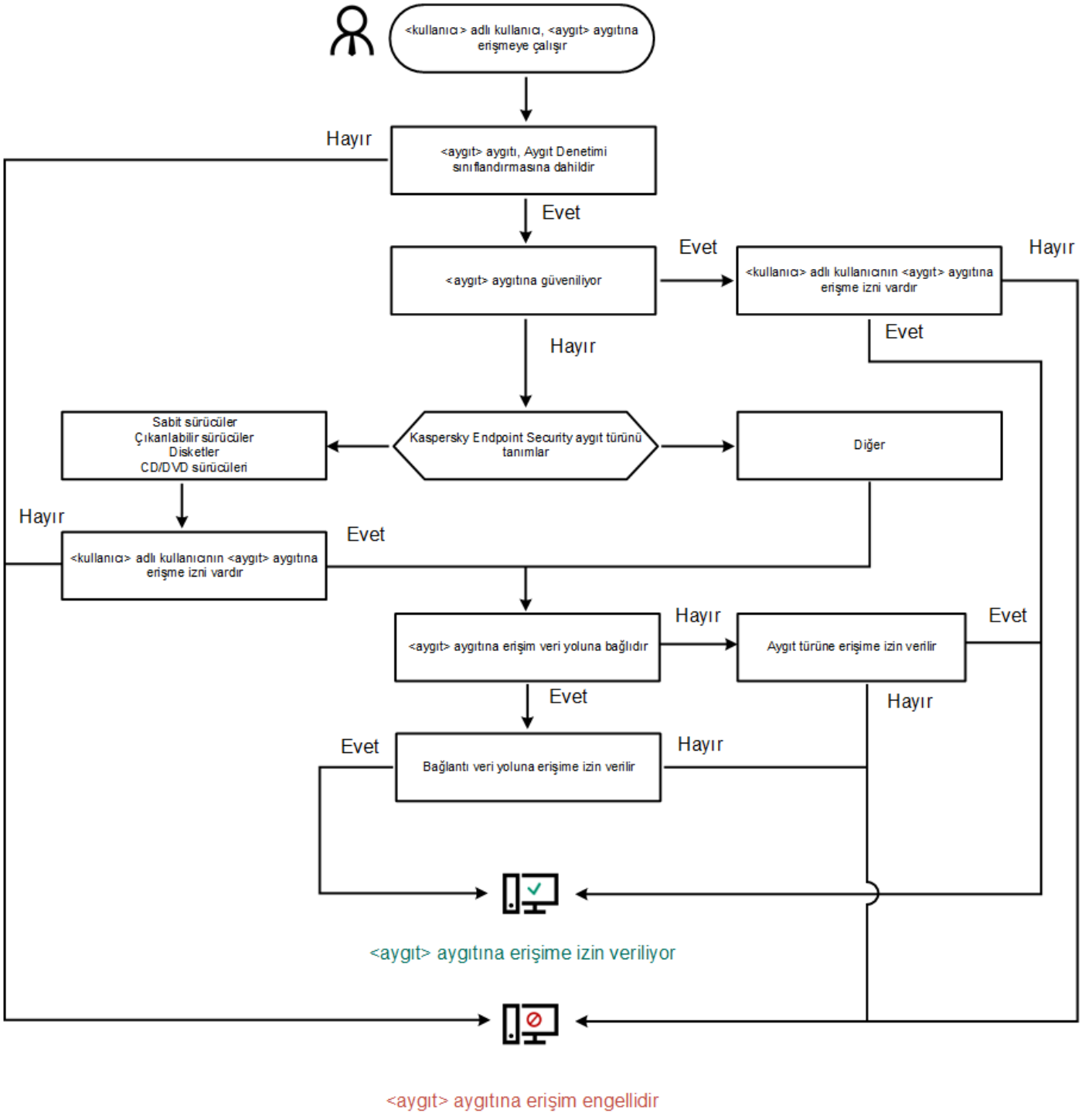
Aygıt Denetimi tarafından engellenen bir aygıt bilgisayara bağlandığında, Kaspersky Endpoint Security erişimi engeller ve bir bildirim gösterir (aşağıdaki şekle bakın).



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 Denetimini etkinleştirme ve devre dışı bırakma

Varsayılan olarak Aygıt Denetimi etkindir.

Aygıt Denetimini etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.

3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Aygıt Denetimi** geçiş düğmesini kullanın.

4. Değişikliklerinizi kaydedin.

Sonuç olarak, Aygıt Denetimi etkinleştirilirse, uygulama bağlı cihazlar hakkındaki bilgileri Kaspersky Security Center'a aktarır. Bağlı cihazların listesini Kaspersky Security Center'daki **Gelişmiş** → **Depolama Alanı** → **Donanım** klasöründe görüntüleyebilirsiniz.

Erişim kuralları hakkında

Erişim kuralları, bilgisayarda yüklü veya bağlı olan aygıtlara erişebilecek kullanıcıları belirleyen ayarlardan oluşur. 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

Bağlantı veri yolu erişim kuralları, aygıtlara bağlantıya izin verildiğini (✓ durumu) veya bu erişimin yasaklandığını (⊘ durumu) belirtir. Veri yollarına erişime izin veren kurallar, varsayılan olarak Aygıt Denetimi bileşeni sınıflandırmasında bulunan bütün bağlantı veri yolları için oluşturulur.

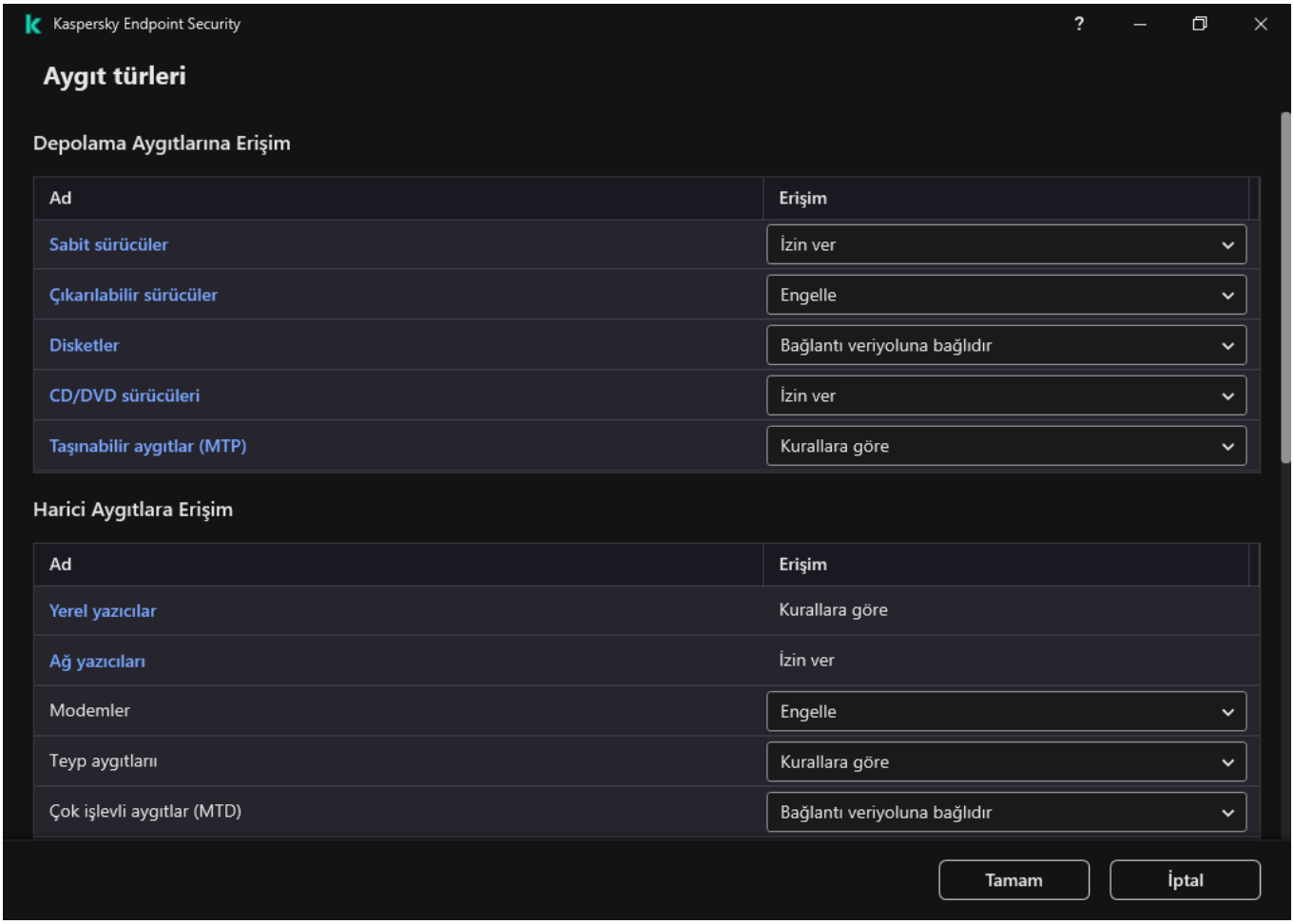
Klavye ve fare Aygıt Denetimi kullanılarak kilitlenemez. USB bağlantı veri yoluna erişimi yasaklarsanız, kullanıcı USB üzerinden bağlı bir klavye ve fare ile çalışmaya devam edecektir. BadUSB Saldırısı Önleme bileşeni, klavyeleri taklit eden virüslü USB cihazlarının bilgisayara bağlanmasını önlemek için tasarlanmıştır.

Aygıt erişim kuralını düzenleme

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.

Bir aygıt erişim kuralını düzenlemek 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** bloğunda, düzenlemek istediğiniz erişim kuralını seçin. Blok, ek erişim ayarlarını yapılandırabileceğiniz bir dosya sistemine sahip aygıtları içerir. Varsayılan olarak aygıt erişim kuralı, tüm kullanıcılara herhangi bir zamanda belirtilen türden cihazlara tam erişim sağlar.

   a. **Erişim** sütununda, uygun aygıt erişim seçeneğini seçin:

   - **İzin ver**.
   - **Engelle**.
   - **Bağlantı veriyoluna bağlıdır**.

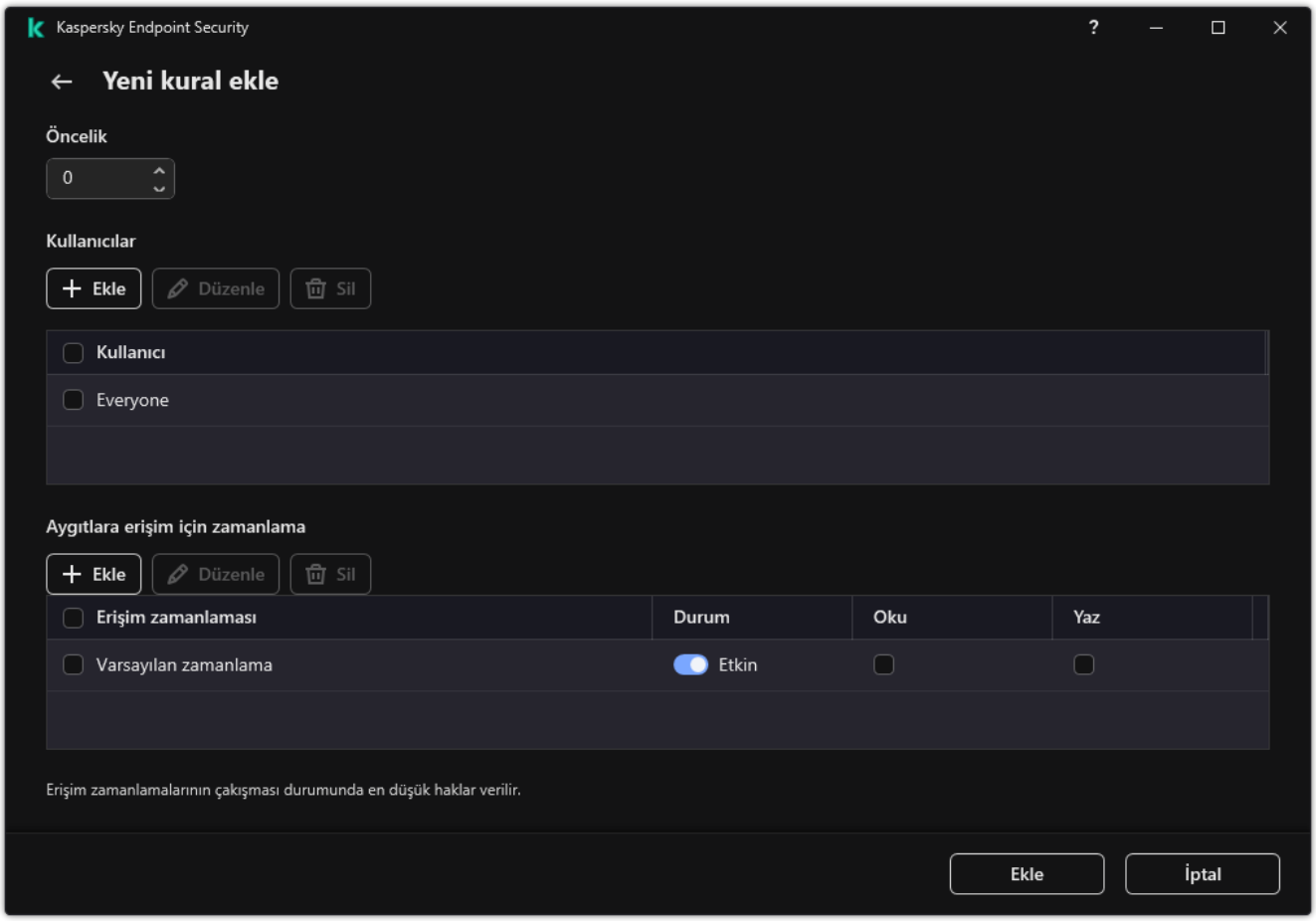
Bir aygıta erişimi engellemek veya izin vermek için, bağlantı veri yoluna erişimi yapılandırın.

- **Kurallara göre**.

  Bu seçenek, kullanıcı haklarını, izinlerini ve aygıt erişimi için bir zamanlama yapılandırmanıza olanak tanır.

b. **Kullanıcıların hakları** bloğunda, **Ekle** düğmesine tıklayın.

Bu, yeni bir aygıt erişim kuralı eklemek için bir pencere açar.



Aygıt Denetimi kural ayarları

a. Yeni *kurala* bir öncelik atayın. 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 arası bir öncelik ataması yapmanıza izin verir. 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. Aygıt erişim kuralı için **Etkin** durumu ayarlayın.

c. Kullanıcıların aygıt erişim izinlerini yapılandırın: okuma ve/veya yazma.

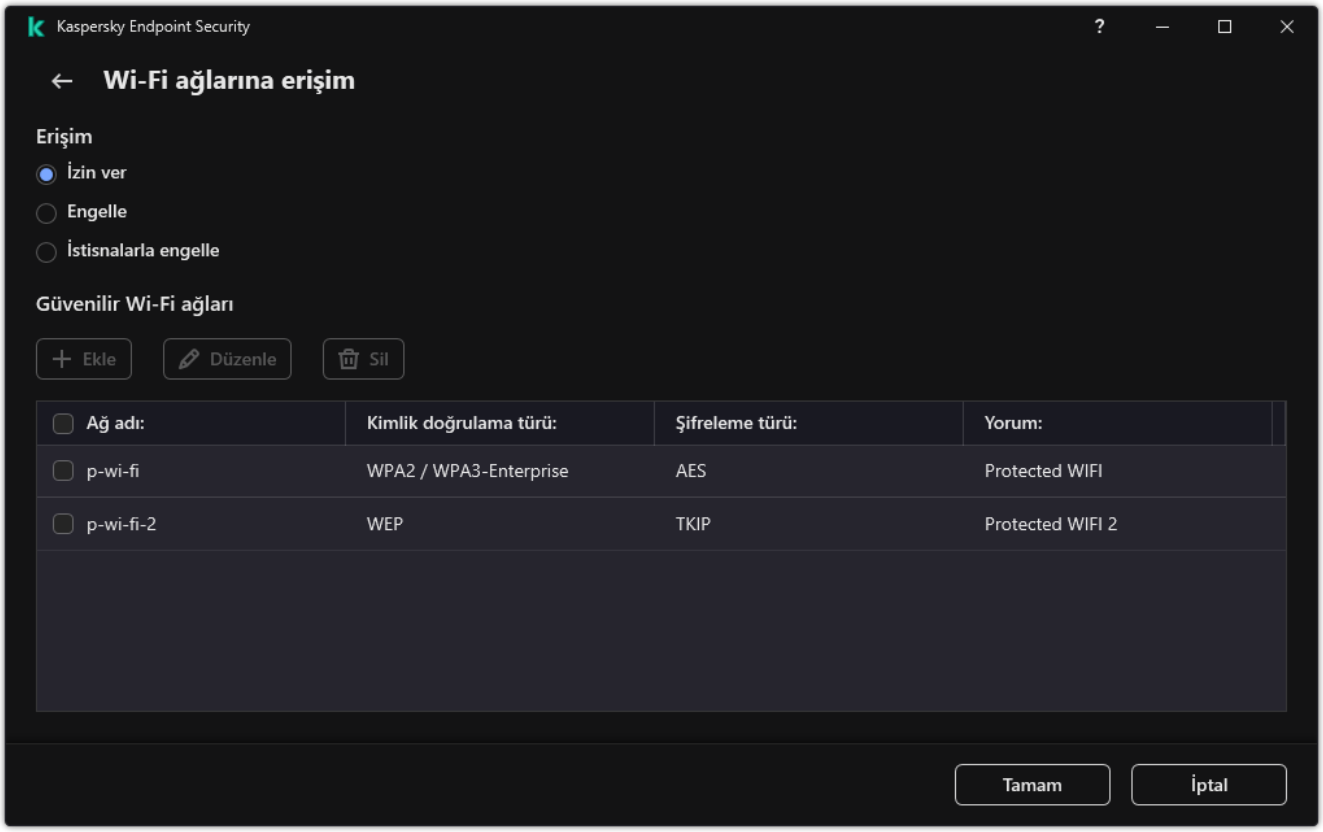
d. Aygıt erişim kuralını uygulamak istediğiniz kullanıcıları veya kullanıcı grubunu seçin.

e. Kullanıcılar için bir aygıt erişim zamanlaması yapılandırın.

f. **Ekle**'ye tıklayın.

5. **Harici Aygıtlara Erişim** bloğunda, kuralı seçin ve erişimi yapılandırın: **İzin ver**, **Engelle** veya **Bağlantı veriyoluna bağlıdır**. Gerekirse bağlantı veri yoluna erişimi yapılandırın.

6. **Wi-Fi ağlarına erişim** bloğunda, **Wi-Fi** bağlantısını tıklayın ve erişimi yapılandırın: **İzin ver**, **Engelle** veya **İstisnalarla engelle**. Gerekirse, Güvenilir listeye bir Wi-Fi ağı ekleyin.



Wi-Fi erişim ayarları

7. Değişikliklerinizi kaydedin.

Bir bağlantı veri yolu erişim kuralını düzenleme

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 Bağlantı Noktası** (COM) veya **Paralel Bağlantı Noktası** (LPT), erişim kuralını etkinleştirmek için bilgisayarı yeniden başlatmanız gerekir.

6. Değişikliklerinizi kaydedin.

Mobil cihazlara erişimi yönetme

Kaspersky Endpoint Security, Android ve iOS çalıştıran mobil cihazlardaki verilere erişimi kontrol etmenizi sağlar. Mobil cihazlar, taşınabilir cihazlar (MTP) kategorisine aittir. Bu nedenle, mobil cihazlara erişimi yapılandırmak için taşınabilir cihazlara (MTP) yönelik veri erişim ayarlarını düzenlemeniz gerekir.

Bilgisayara bir mobil cihaz bağlandığında işletim sistemi cihaz türünü belirler. Bilgisayarda Android Hata Ayıklama Köprüsü (ABD), iTunes veya bunların dengi uygulamalar yüklü ise işletim sistemi mobil cihazları ABD veya iTunes cihazları olarak tanımlar. Diğer tüm durumlarda işletim sistemi mobil cihaz türünü dosya aktarımı için taşınabilir cihaz (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, mobil cihazlara (MTP) erişim kurallarına uygun olarak mobil cihazlara erişime izin verir.

Mobil cihazlara erişimi yönetme

Mobil cihazlar, taşınabilir cihazlar (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 bağlantı noktasına 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 bağlantı noktasına 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 cihazlar (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'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 **Cihaz türleri** sekmesini seçin.
   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **Taşınabilir cihazlar (MTP)** cihaz türü için bağlam menüsünde, mobil cihaz erişim modunu yapılandırın: **İzin ver**, **Engelle**, veya **Bağlantı veriyoluna bağlıdır**.
7. Mobil cihaz erişim kurallarını yapılandırmak için çift tıklayarak kural listesini açın.
8. 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 arası bir öncelik ataması yapmanıza izin verir. 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.

d. **Tamam**'a tıklayın.

9. **Seçilen erişim kuralı için zamanlama** böllümünde, kullanıcılar için bir mobil cihaz erişim programı yapılandırın.

> ADB cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir. ADB cihazları ve taşınabilir cihazlar (MTP) için ortak bir erişim planı yapılandırabilirsiniz.

10. Dosya yöneticisinde kullanıcıların mobil cihazlara erişim izinlerini yapılandırın **(Okuma**/**Yazma**).

11. **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.

12. **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.

13. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da mobil cihaz erişim kurallarını yapılandırma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 Denetimi Ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları için erişim kuralları** bağlantına tıklayın.

Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.

6. **Taşınabilir cihazlar (MTP)** cihaz ürünü seçin.

Taşınabilir cihazlar (MTP) erişim hakları açılır.

7. **Cihaz erişim kuralları yapılandırma** bölümünde, mobil cihazlar erişim modunu yapılandırın: **İzin ver**, **Reddet**, **Bağlantı veriyoluna bağlıdır** veya **Kurallara göre**.
8. **Kurallara göre** modunu seçtiğinizde, yazıcılar için yazdırma kuralları eklemelisiniz. Bunu yapmak için, **Kullanıcılar** altında **Ekle** düğmesine tıklayın ve mobil cihaz erişim kuralını yapılandırın:

a. **Cihazlara erişim kuralı** 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 arası bir öncelik ataması yapmanıza izin verir. 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. **Kullanıcılar** bölümünde, mobil cihazlara erişim için kullanıcıları veya kullanıcı gruplarını seçin.

c. **Aygıtlara erişim için zamanlama** altında, kullanıcılar için bir mobil cihaz erişim zamanlaması yapılandırın.

   > ADB cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir. ADB cihazları ve taşınabilir cihazlar (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.

f. **iTunes üzerinden erişim** altında, iTunes uygulaması aracılığıyla mobil aygıttaki verilere erişimi yapılandırın.

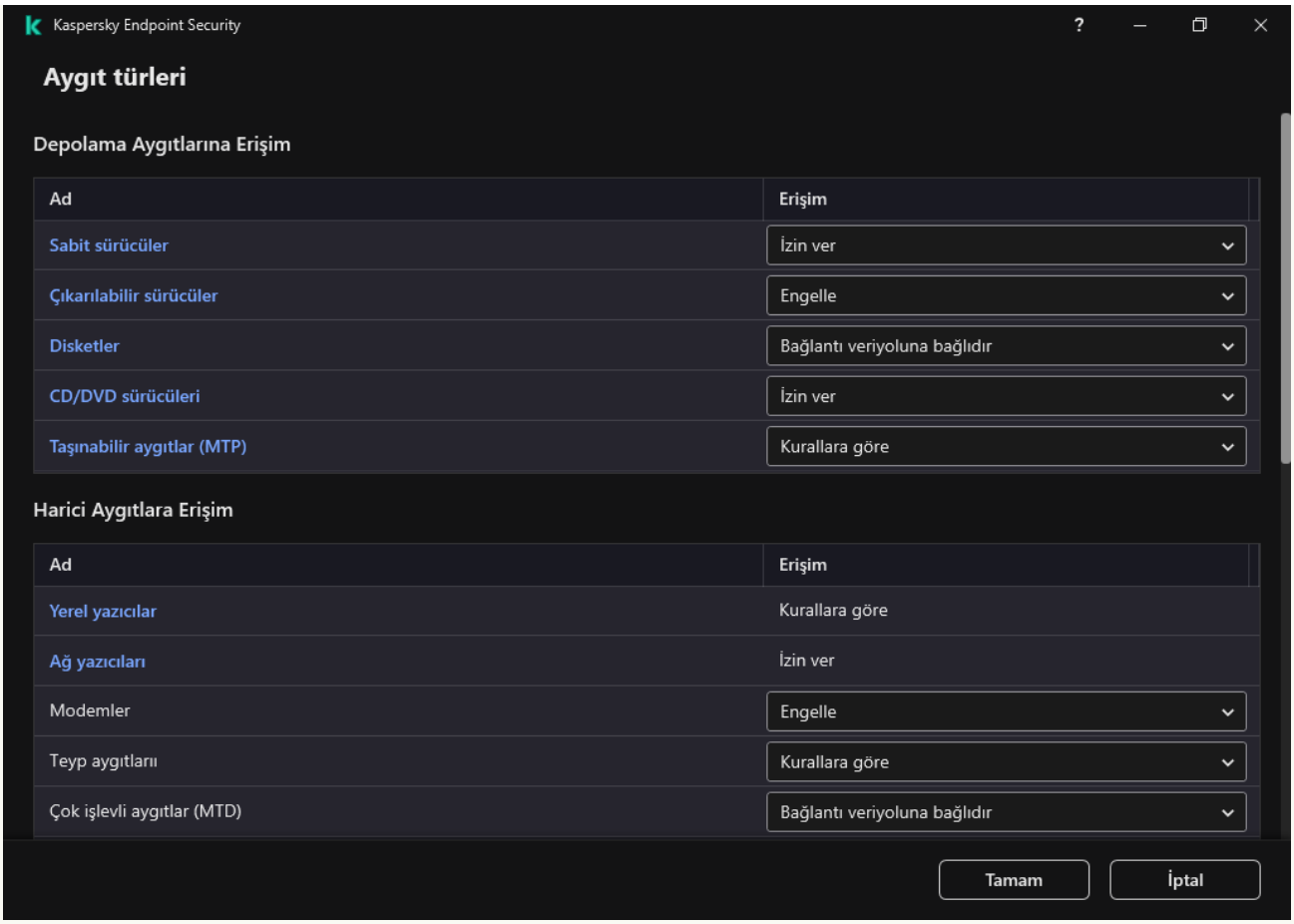
   > Kaspersky Endpoint Security, tüm kullanıcılar için iTunes uygulaması aracılığıyla mobil cihaz erişimi ayarlarını uygular. iTunes cihazları için ayrı bir erişim planı yapılandırmak mümkün değildir.

9. Değişikliklerinizi kaydedin.

Uygulamanın arayüzünde 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 cihazlar (MTP)** bağlantısına tıklayın.

   Taşınabilir cihazlar (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 arası bir öncelik ataması yapmanıza izin verir. 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.

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 cihazlar (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

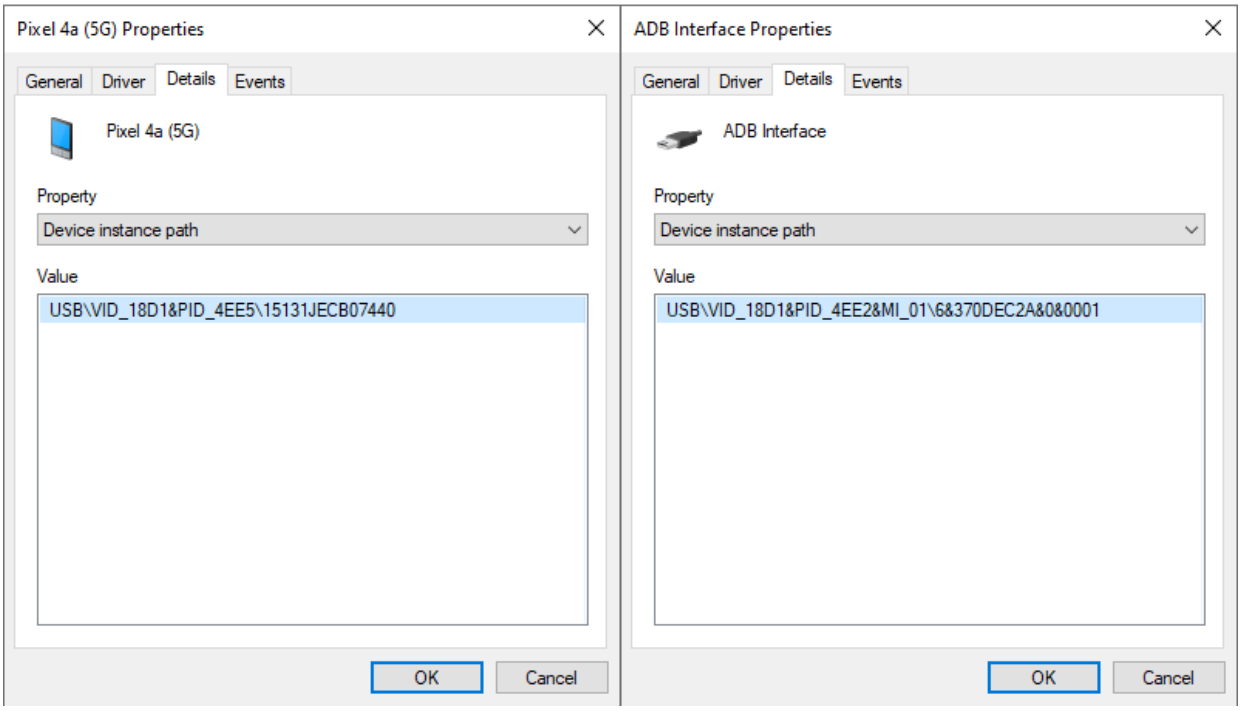
Güvenilir aygıtlar, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

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 (Donanım Kimliği – HWID) ihtiyacınız olacaktır. Kimliği, işletim sistemi araçlarını kullanarak cihaz özelliklerinde bulabilirsiniz (aşağıdaki şekle bakın). Aygıt Yöneticisi aracı bunu yapmanızı sağlar. Taşınabilir cihazların (MTP) ve ADB, iTunes cihazlarının kimlikleri, aynı mobil cihaz için bile farklıdır. Bir taşınabilir cihazın (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 Satıcı Kimliğine (VID) ve Ürün Kimliğine (PID) 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

Yazdırma denetimi

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 bağlantı noktalarına bağlantısını yalnızca veri yolu düzeyinde kontrol eder. Yani, yazıcıların COM ve LPT bağlantı noktalarına bağlanmasını engellemek için tüm cihaz türlerinin COM ve LPT veri yollarına bağlanmasını yasaklamalısınız. USB'ye bağlı yazıcılar için uygulama iki seviyede kontrol uygular: cihaz türü (yerel yazıcılar) ve bağlantı veriyolu (USB). Bu nedenle, yerel yazıcılar dışındaki tüm cihaz türlerinin USB'ye bağlanmasına izin verebilirsiniz.

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 kullanıcıların ağ yazıcılarından yazdırma erişimine izin verir ve yazdırma bilgilerini 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'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 **Cihaz türleri** sekmesini seçin.

   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **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).
7. Yerel ve ağ yazıcılarında yazdırma kurallarını yapılandırmak için, kural listelerini çift tıklayarak açın.
8. Yazıcı erişim modu olarak **Kurallara göre** seçimini yapın.
9. 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 arası bir öncelik ataması yapmanıza izin verir. 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.

   e. **Tamam**'a tıklayın.
10. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da yazdırma kuralları ekleme

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 Denetimi Ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları için erişim kuralları** bağlantına 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), **Bağlantı veriyoluna bağlıdır** (yalnızca yerel yazıcılar için) veya **Kurallara göre**.
8. **Kurallara göre** 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 arası bir öncelik ataması yapmanıza izin verir. Değer ne kadar büyük olursa öncelik de o kadar yüksektir. Başka bir deyişle, 0 değeri ön düşük önceliğe sahiptir.

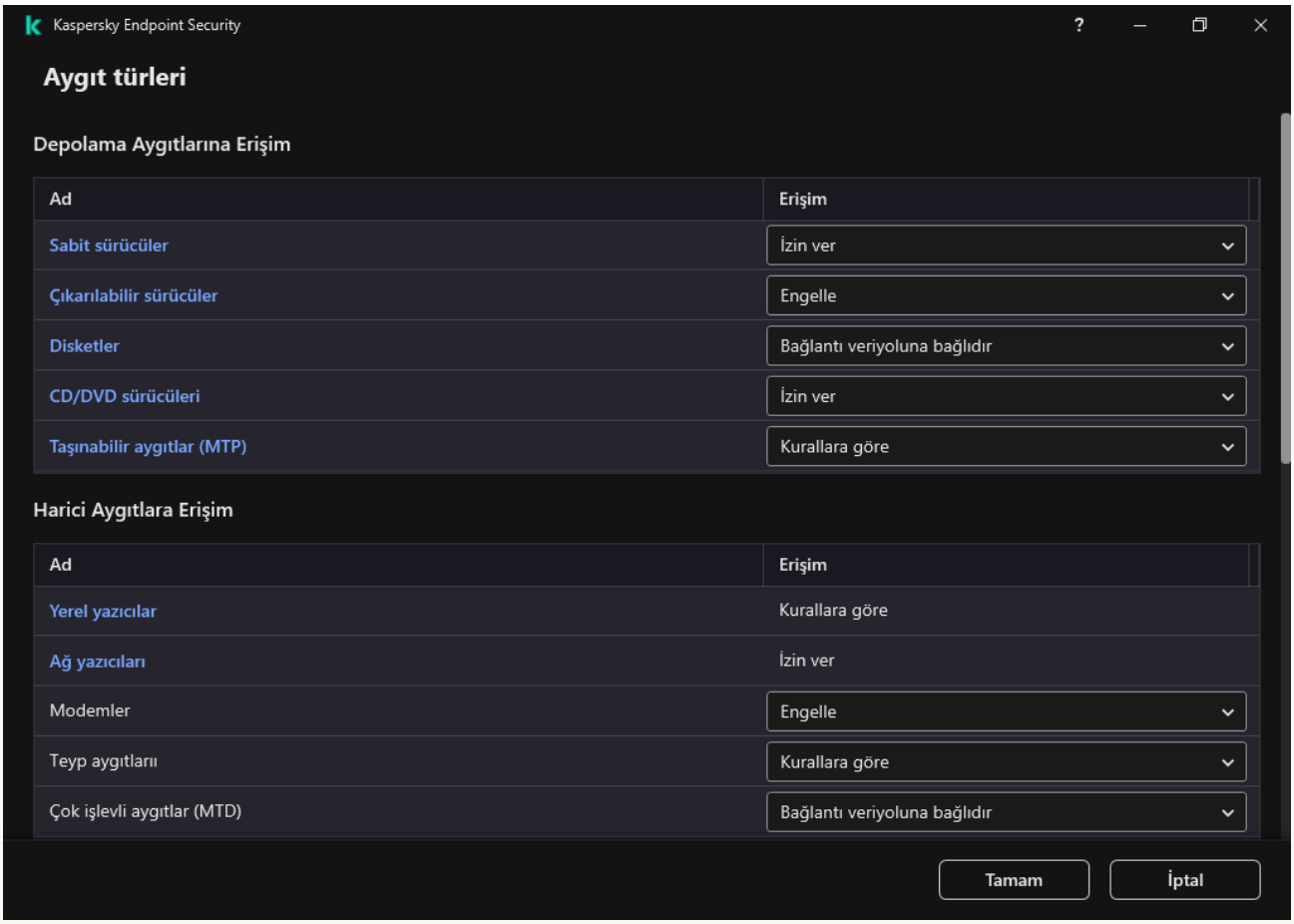
   Örneğin, Herkes grubuna salt okunur izinler verebilir ve yöneticiler grubuna okuma/yazma izinleri verebilirsiniz. Bunu yapmak için, yöneticiler grubuna 1 önceliği ve Herkes grubuna 0 önceliği atayın.

   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. **Kullanıcılar ve gruplar** bölümünde, yazdırmaya erişim için kullanıcıları veya kullanıcı gruplarını seçin.
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 Cihazlara 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 arası bir öncelik ataması yapmanıza izin verir. 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.

7. Değişikliklerinizi kaydedin.

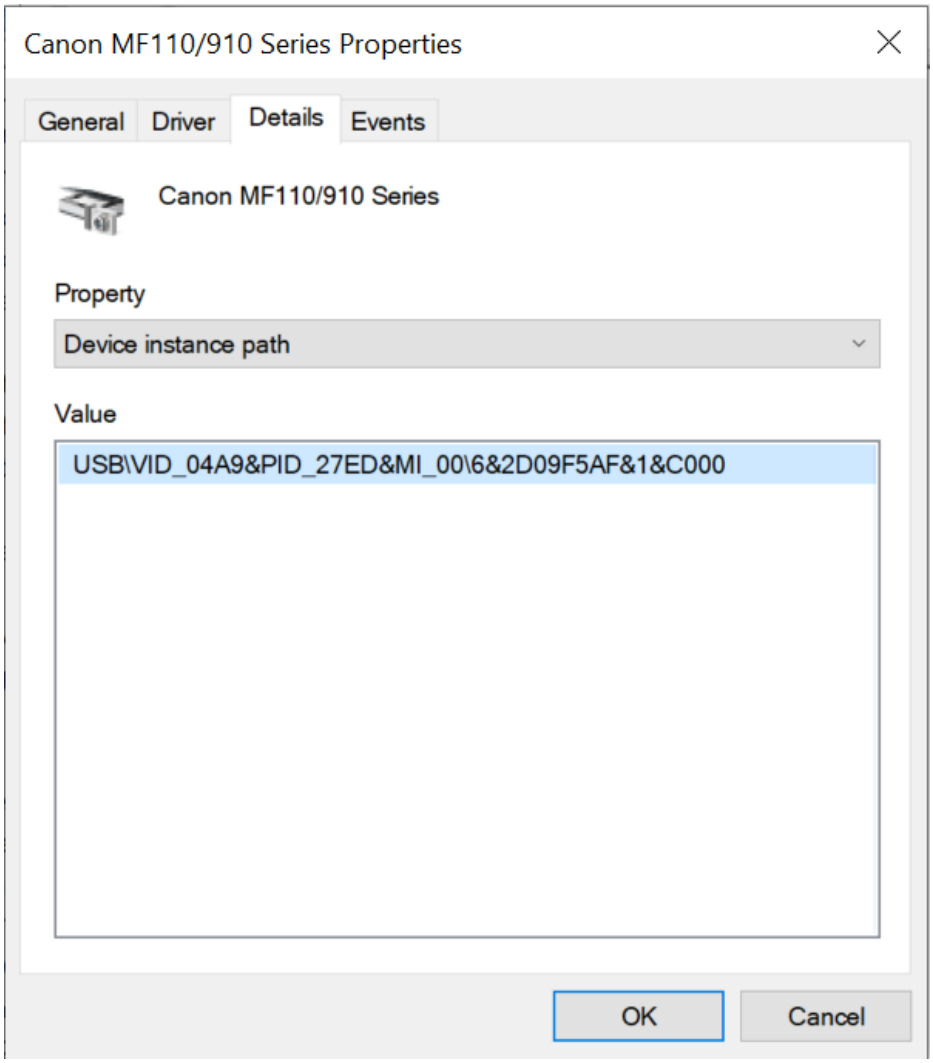
Güvenilir yazıcılar

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 (Donanım Kimliği – HWID) ihtiyacınız olacaktır. Kimliği, işletim sistemi araçlarını kullanarak cihaz özelliklerinde bulabilirsiniz (aşağıdaki şekle bakın). Aygıt Yöneticisi 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 Satıcı Kimliğine (VID) ve Ürün Kimliğine (PID) 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.

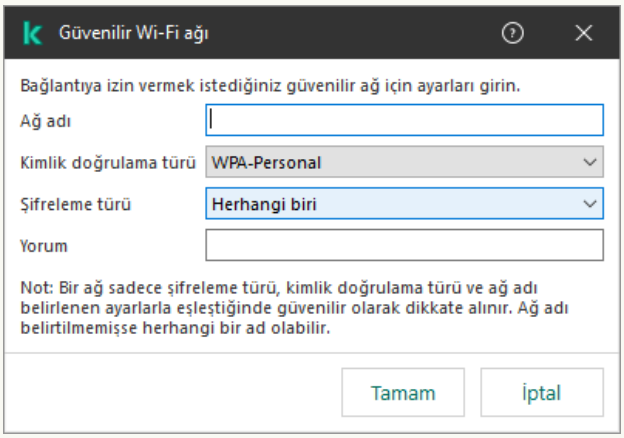
Yönetim Konsolu'nda (MMC) Wi-Fi bağlantılarını kısıtlama

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 **Cihaz türleri** sekmesini seçin.
   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.
6. **Wi-Fi** cihaz türünün bağlam menüsünde, Wi-Fi'ye bağlanırken gerçekleştirilen Aygıt Denetimi işlemini seçin: **İzin ver** (✓), **Engelle** (⊘) veya **İstisnalarla engelle** (▦).
7. **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 (Hizmet Kümesi Tanımlayıcısı).
      - **Kimlik doğrulama türü**. Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türü.
      - **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.

8. Değişikliklerinizi kaydedin.



Güvenilir Wi-Fi ağ ayarları

[Web Console ve Cloud Console'da Wi-Fi bağlantılarını kısıtlama](#)

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 Denetimi Ayarları** bloğunda, **Aygıtlar ve Wi-Fi ağları için erişim kuralları** bağlantına tıklayın.
   Tablo, Aygıt Denetimi bileşeninin sınıflandırmasında bulunan tüm cihazlar için erişim kurallarını listeler.

6. **Wi-Fi ağlarına erişim** bloğunda, **Wi-Fi** bağlantısına tıklayın.

7. **Wi-Fi ağlarına erişim** bölümünde Wi-Fi'ye bağlanırken gerçekleştirilen Aygıt Denetimi eylemini seçin: **İzin ver**, **Engelle** veya **İstisnalarla engelle**.

8. **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.

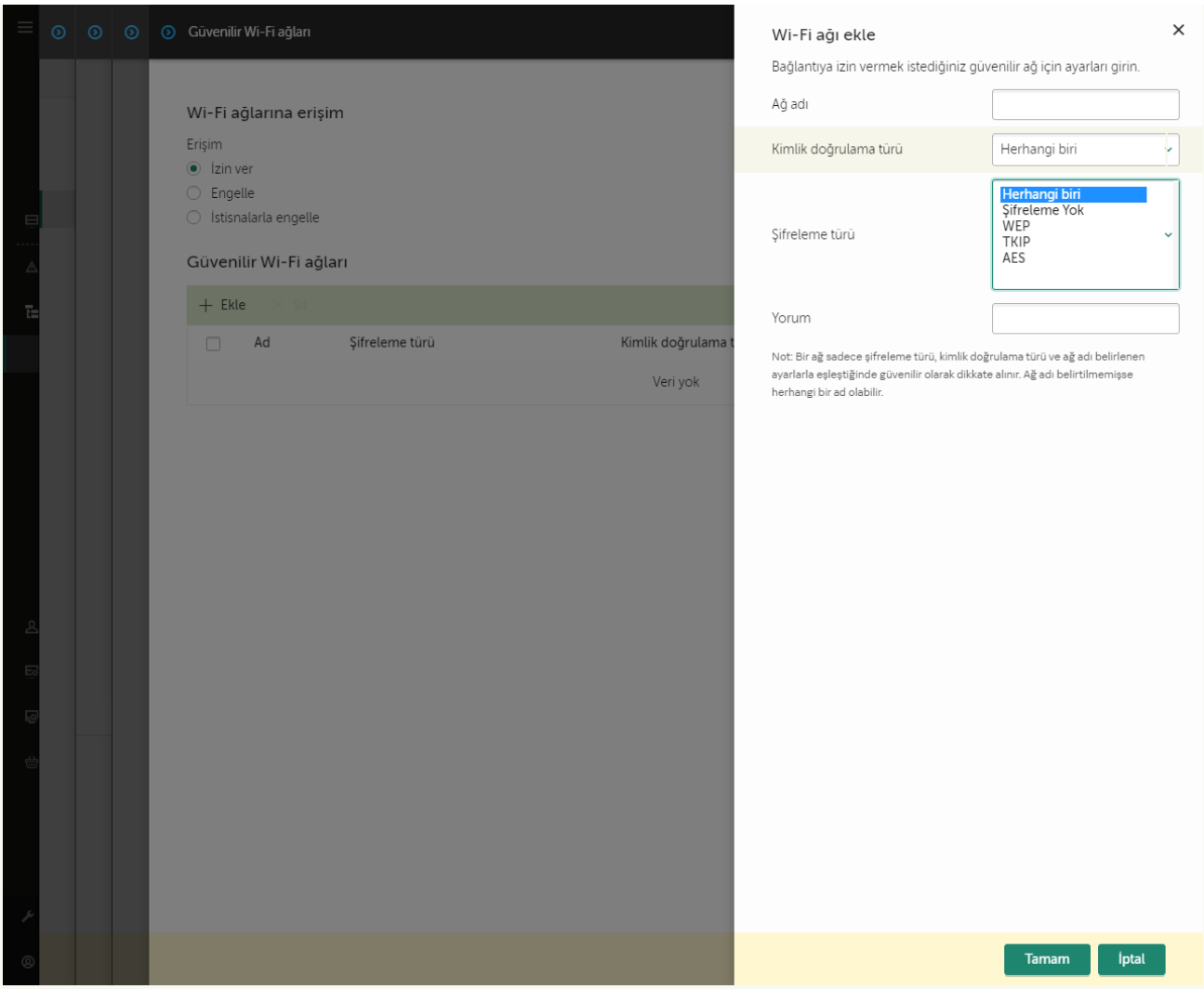
   c. Böylece açılan pencerede, güvenilir Wi-Fi ağını yapılandırın (aşağıdaki şekle bakın):

   - **Ağ adı**. Wi-Fi ağının adı veya SSID'si (Hizmet Kümesi Tanımlayıcısı).
   - **Kimlik doğrulama türü**. Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türü.
   - **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.

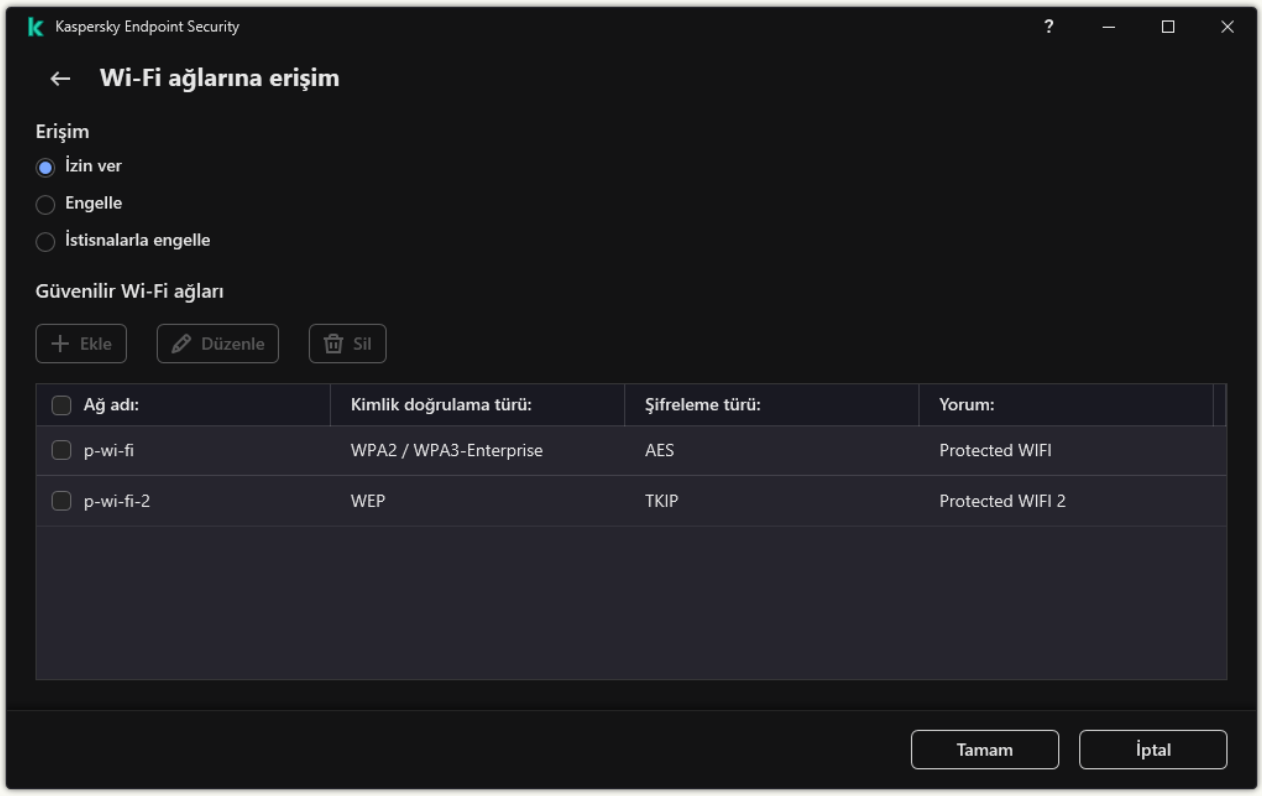
9. Değişikliklerinizi kaydedin.



Güvenilir Wi-Fi ağ ayarları

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.

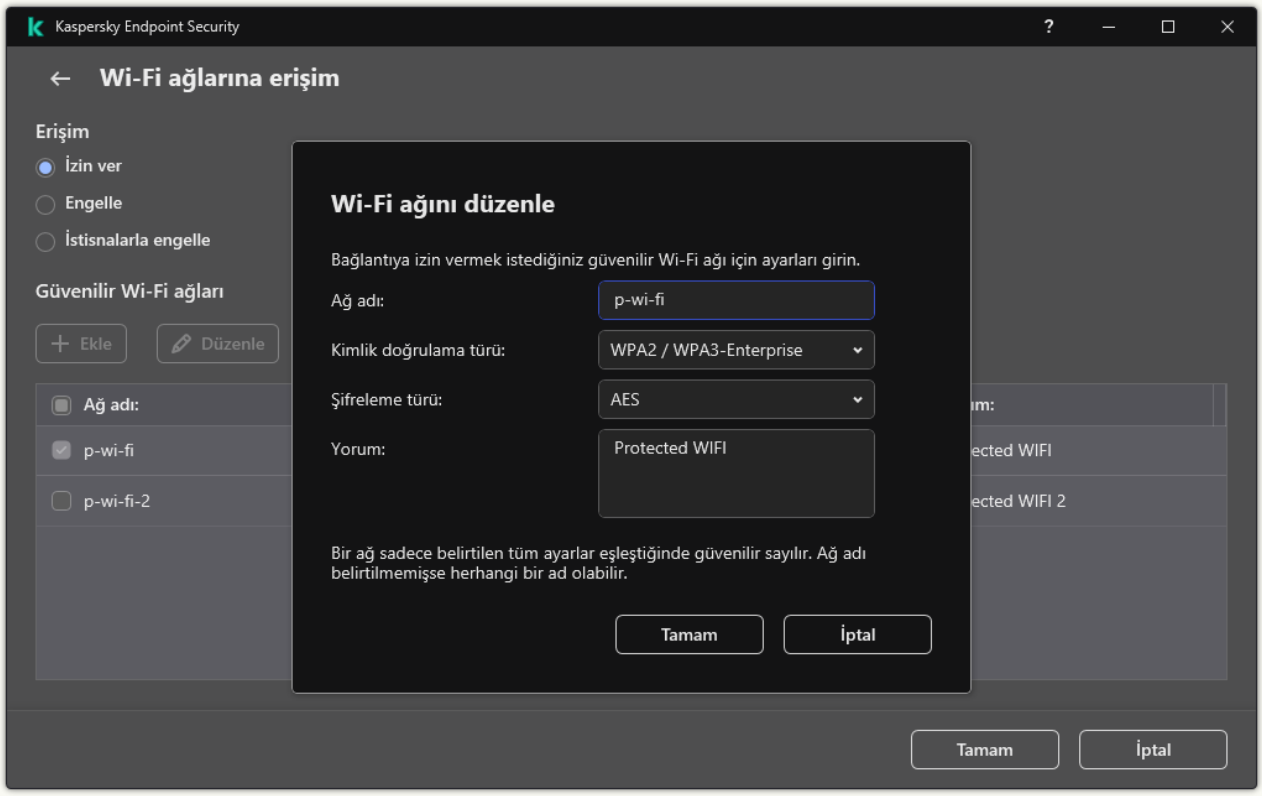
   b. Böylece açılan pencerede, güvenilir Wi-Fi ağını yapılandırın (aşağıdaki şekle bakın):

   - **Ağ adı**. Wi-Fi ağının adı veya SSID'si (Hizmet Kümesi Tanımlayıcısı).
   - **Kimlik doğrulama türü**. Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türü.
   - **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.

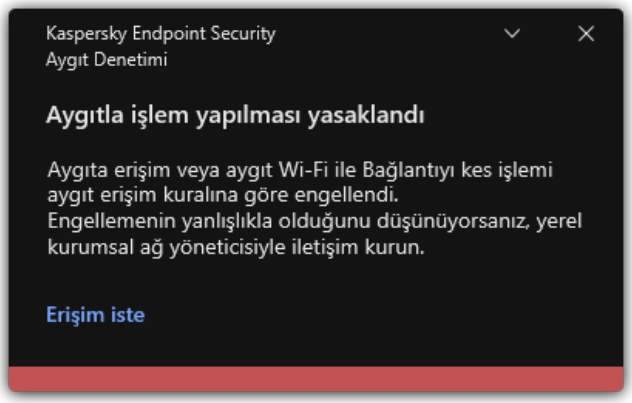
   > Bir Wi-Fi ağı, ayarları kuralda belirtilen tüm ayarlarla eşleşiyorsa güvenilir kabul edilir.

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* önem seviyesine sahiptir.

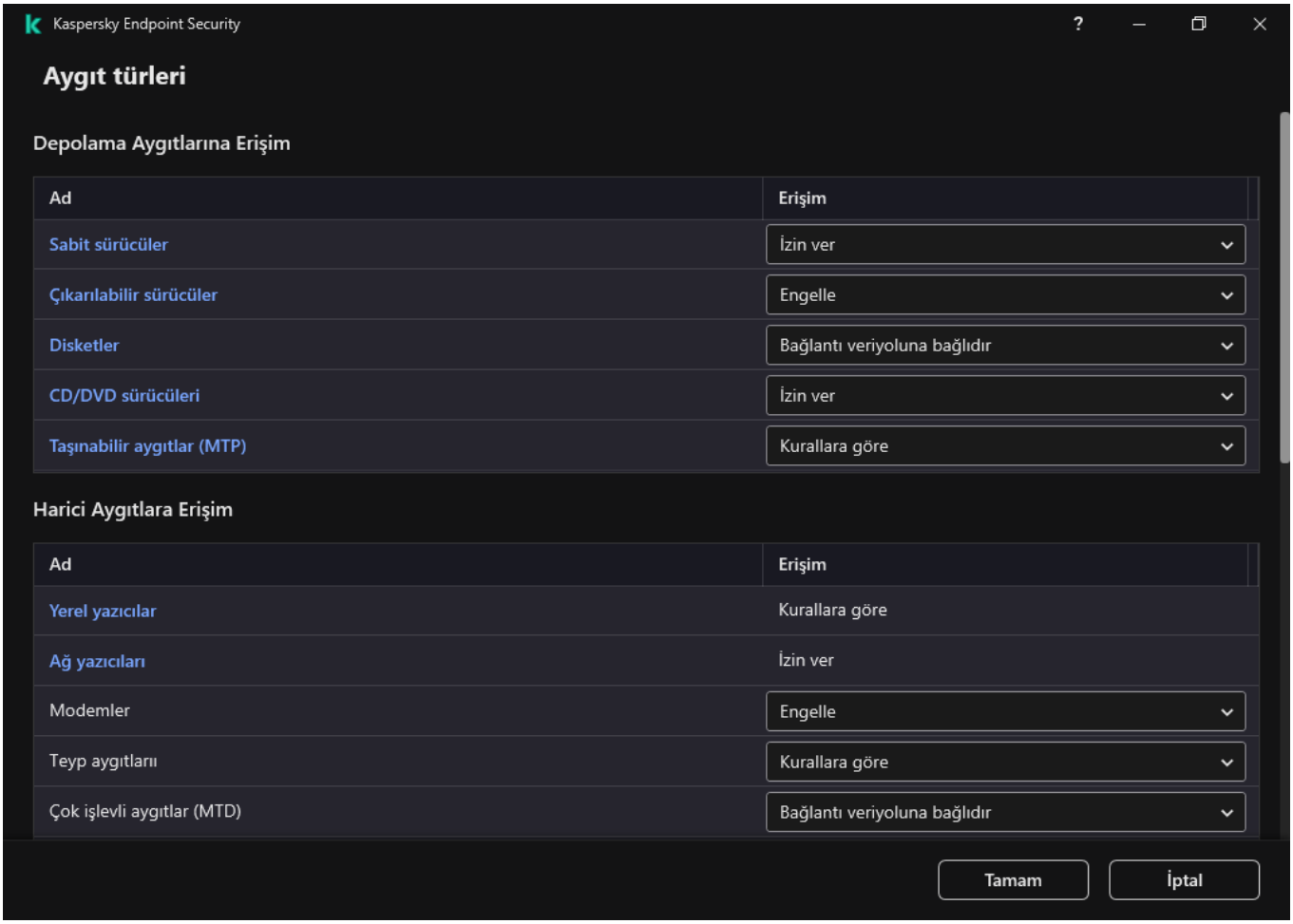
Çıkarılabilir sürücü kullanımını izlemeyi etkinleştirmek için:

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.

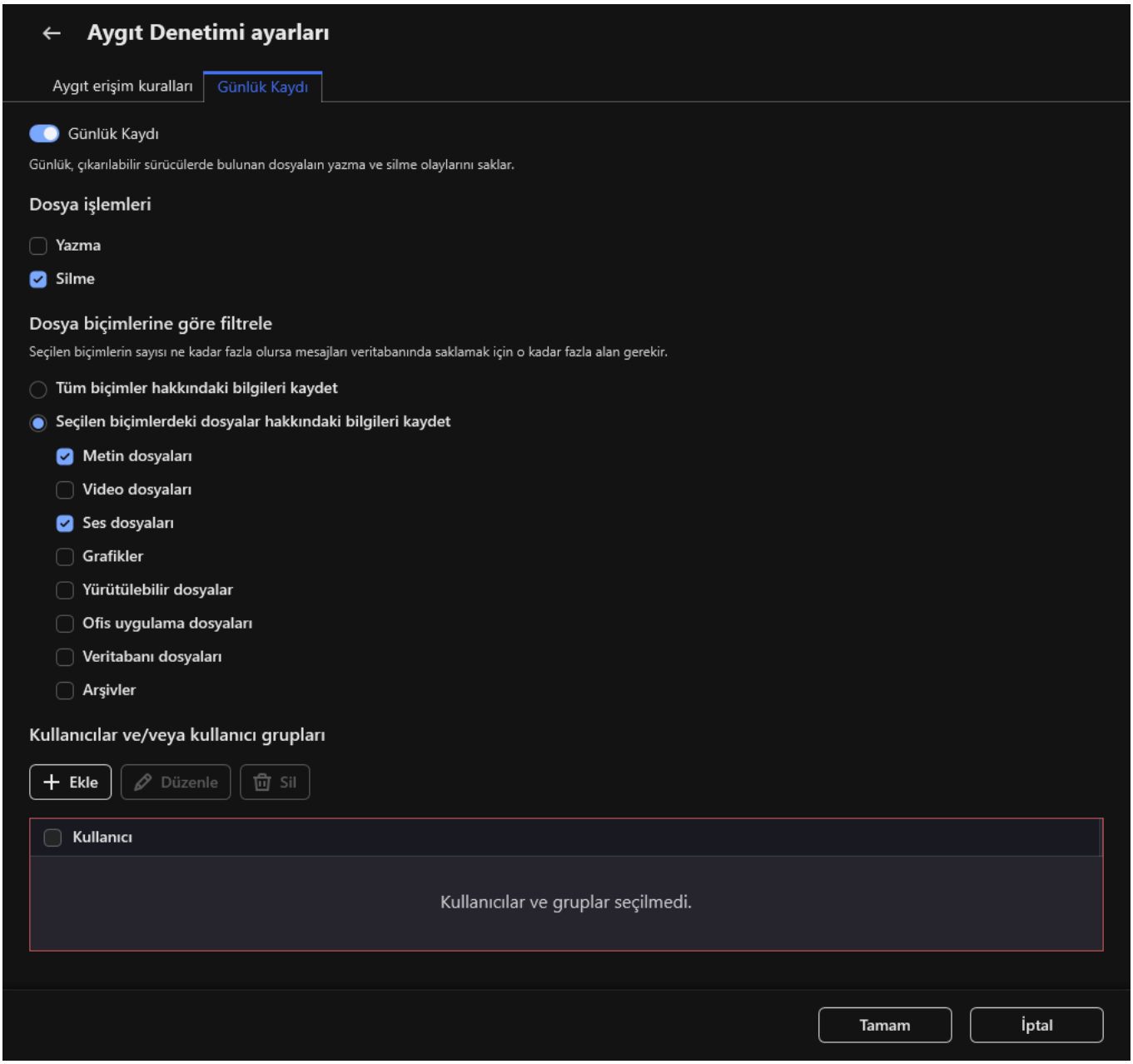
   Açılan pencere, Aygıt Denetimi bileşen sınıflandırmasına dahil olan tüm aygıtlar için erişim kurallarını gösterir.



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\environment]`
   - 32-bit işletim sistemleri için: `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\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 1000'den fazla güvenilir cihaz eklenmesi önerilmez.

Kaspersky Endpoint Security, bir aygıtı güvenilir listeye şu şekillerde eklemenize izin verir:

- Kaspersky Security Center kuruluşunuzda dağıtılmış değilse, aygıtı 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* önem seviyesine sahiptir.

Uygulama arabiriminden Güvenilir listeye aygıt ekleme

Varsayılan olarak güvenilir aygıtlar listesine bir aygıt eklendiğinde tüm kullanıcılara aygıtlara erişim izni verilir (Herkes kullanıcı grubu).

Uygulama arabiriminden Güvenilir listesine bir aygıt eklemek için:

1. 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.
6. **Yorum** alanında, güvenilir aygıtla ilgili her türlü bilgiyi sağlayabilirsiniz.
7. Güvenilir aygıtlara erişmesine izin vermek istediğiniz kullanıcıları veya kullanıcı grubunu seçin.
8. Değişikliklerinizi kaydedin.

Kaspersky Security Center'dan Güvenilir listeye bir aygıt ekleme

Kaspersky Security Center, Kaspersky Endpoint Security bilgisayarlarda yüklü ve Aygıt Denetimi etkinleştirilmiş ise aygıtlar hakkında bilgi alır. Kaspersky Security Center'da bu aygıt hakkındaki bilgiler kullanılabilir olmadığında, bu aygıtı güvenilir listeye eklemek mümkün olmaz.

Bir aygıtı güvenilir listeye şu verilere göre ekleyebilirsiniz:

- **Kimliğe göre aygıtlar**. Her cihazın benzersiz bir tanımlayıcısı vardır (Donanım Kimliği veya HWID). Bu kimliği, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. Örnek aygıt kimliği: `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 satıcı kimliği (VID) ve bir ürün kimliği (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_ *`.

Aygıtları güvenilir aygıtlar listesine eklemek için:

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**).

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. Bu esnada, **Yenile** düğmesine tıklandığında 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 adı** 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. **Yenile** düğmesine 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.

15. Active Directory'de bir kullanıcı veya grup seçin ve seçiminizi onaylayın.

    Varsayılan olarak, Herkes grubu için güvenilir aygıtlara erişime izin verilir.

16. 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 ayarlarından 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.

      Bilgisayar zaten bir güvenilir aygıtlar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.
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:

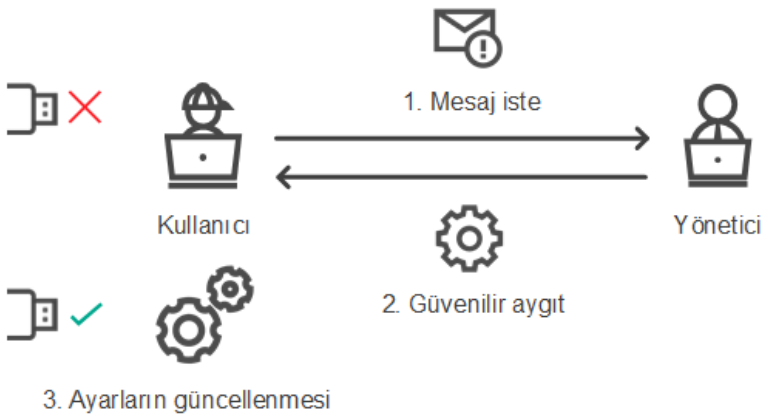
1. Kullanıcı yöneticiye bir erişim isteği mesajı gönderir.
2. Yönetici, Kaspersky Security Center konsolunda isteği içeren bir mesaj alır.

   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

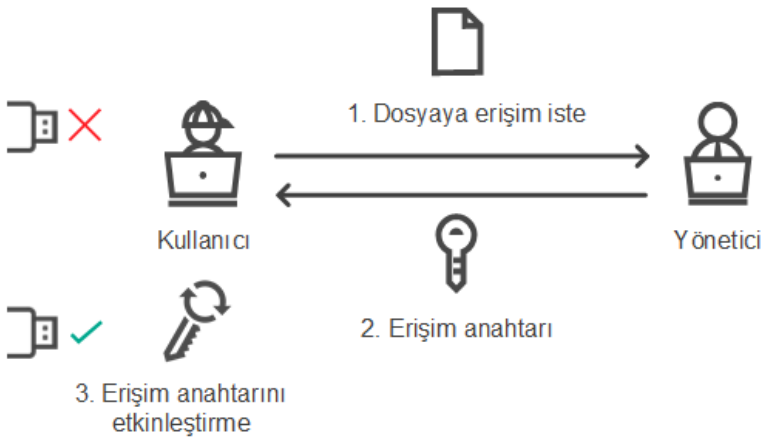
Erişim vermek için çevrimdışı mod

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:

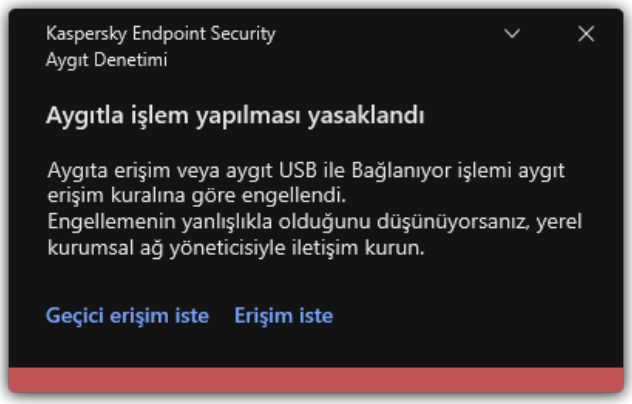
1. Aygıtı bilgisayara bağlayın.

   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

Bundan sonra yönetici, Kaspersky Security Center konsolunda *Yöneticiye aygıta erişimin engellenmesine yönelik mesaj* şeklinde bir olay alacaktır. Olay, kullanıcı adı, bilgisayar adı, kullanıcının erişmeye çalıştığı cihaz hakkında bilgi ve diğer verileri içerir. Yöneticiyi bu tür olaylar hakkında bilgilendirmek için bir yöntem yapılandırabilir ve örneğin bir e-posta bildirimi seçebilirsiniz. Kaspersky Security Center konsolunda, kullanıcılardan gelen mesajların kolay takibi için önceden ayarlanmış bir olay seçimi *Kullanıcı istekleri* yer alır.

Erişim izni vermek için bir cihazı güvenilenler listesine eklemeniz gerekir. Bilgisayarda Kaspersky Endpoint Security ayarlarını güncelledikten sonra kullanıcı cihaza erişim sağlayacaktır.

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.

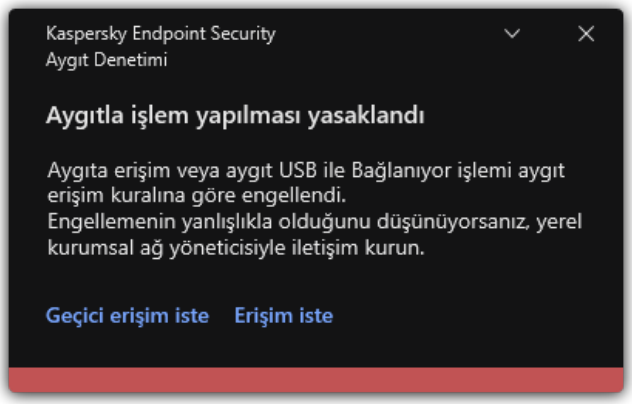
3. Bağlanan aygıtlar listesinden erişim elde etmek istediğiniz aygıtı seçin.

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. Açılan pencerede, **Aygıt 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
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. **Gözat** düğmesine tıklayın ve kullanıcıdan alınan istek erişim 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. Kullanıcı, aygıta erişimin yanlışlıkla engellendiğini veya aygıt içeriğiyle işlem yapmanın yanlışlıkla yasaklandığını düşünüyorsa engellenen işlemle ilgili mesajda görüntülenen bağlantıya tıklayarak yerel kurumsal ağ yöneticisine bir mesaj gönderebilir.

Engellenen aygıt erişimi veya yasaklanan aygıt içeriği işlemleriyle ilgili mesajlar ve yöneticiye gönderilen mesajlar için şablonlar mevcuttur. Mesaj şablonlarını değiştirebilirsiniz.

Aygıt Denetimi mesajlarının şablonlarını düzenlemek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Aygıt Denetimi**'ni seçin.
3. **Mesaj şablonları** bloğunda, Aygıt 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. 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.

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 durumunda kuralları tetikleme** veri havuzunda günlüğe kaydeder.

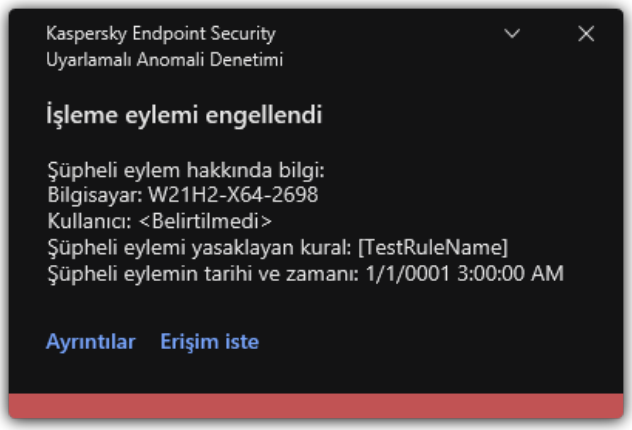
2. Kural tetikleme raporunu analiz etme.

   Yönetici, kural tetikleme raporunu veya **Akıllı Eğitim durumunda kuralları tetikleme** 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 gerçek zamanlı olarak yapılandırılır. Uyarlamalı Anomali Denetimi şu kanallar üzerinden 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 durumunda kuralları tetikleme** veri havuzunun içeriğini gözden geçirdikten sonra Uyarlamalı Anomali Denetiminin çalışmasını yapılandırır. Kural tetikleme raporunun ve **Akıllı Eğitim durumunda kuralları tetikleme** veri havuzunun içeriğinin kontrol edilmesi önerilir.

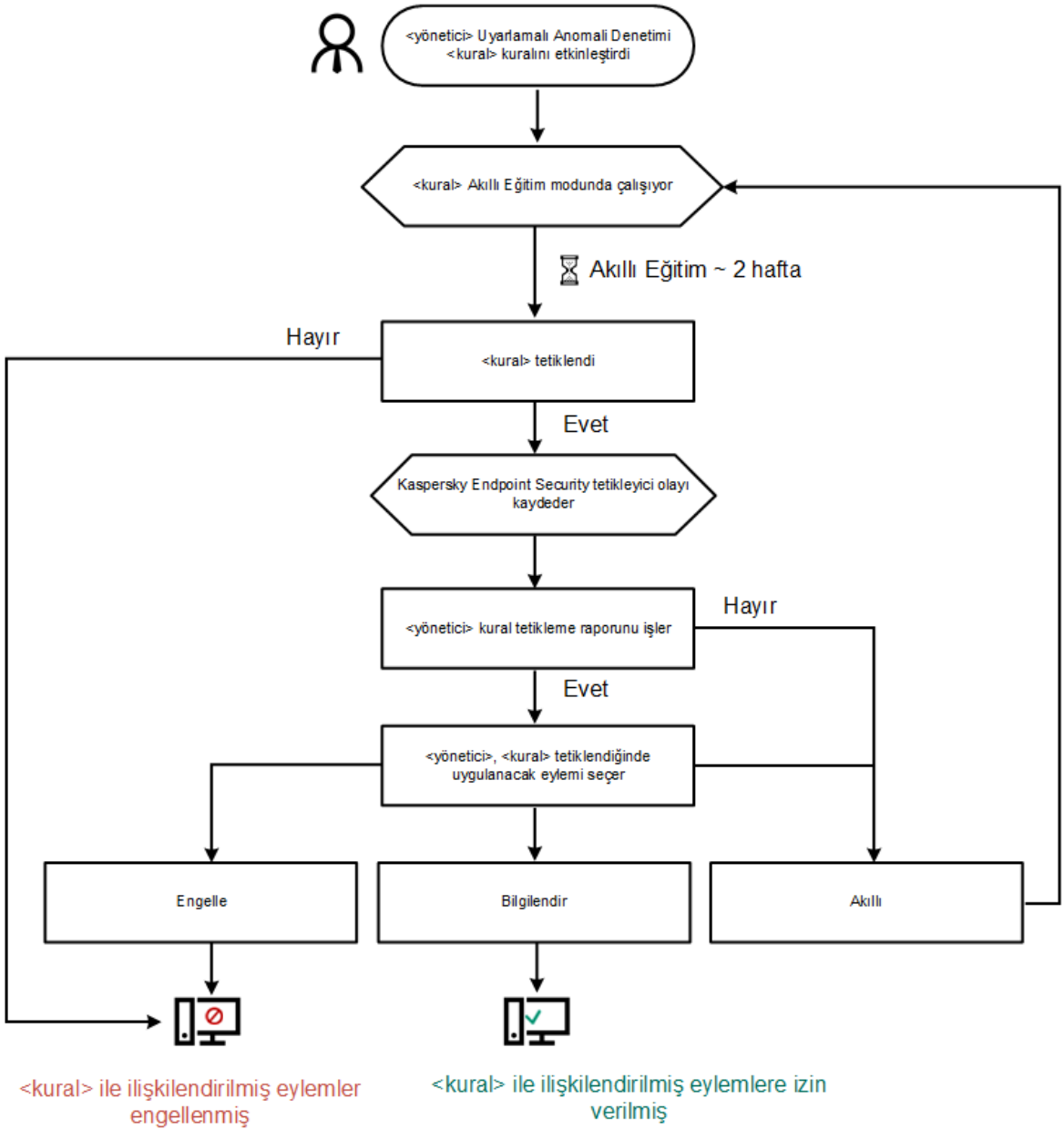
Zararlı bir uygulama eylemde bulunmaya çalıştığında Kaspersky Endpoint Security, eylemi engeller ve bir bildirim gösterir (aşağıdaki resme bakın).



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 Denetimini etkinleştirme ve devre dışı bırakma

Uyarlamalı Anomali Denetimi varsayılan olarak etkin durumdadır.

Uyarlamalı Anomali Denetimini etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uyarlamalı Anomali Denetimi**'ni seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Uyarlamalı Anomali Denetimi** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak Uyarlanabilir Anomali Denetimi eğitim moduna geçecektir. Eğitim sırasında, Uyarlanabilir Anomali Denetimi kural tetiklemesini izler. Eğitim tamamlandığında, Uyarlanabilir Anomali Denetimi bir şirketin ağındaki bilgisayarlar için tipik olmayan eylemleri engellemeye başlar.

Kuruluşunuz bazı yeni araçları kullanmaya başladıysa ve Uyarlanabilir Anomali Denetimi bu araçların eylemlerini engelliyorsa, eğitim modunun sonuçlarını sıfırlayabilir ve eğitimi tekrarlayabilirsiniz. Bunu yapmak için, kural tetiklendiğinde gerçekleştirilen eylemi değiştirmeniz gerekir (örneğin, **Bildir** olarak ayarlayın). Ardından eğitim modunu yeniden etkinleştirmelisiniz (**Akıllı** değerini ayarlayın).

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 durumunda kuralları tetikleme** 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.

- **Bildir**. 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, `dosya.xlsx` adlı bir dosya açtığınızı varsayalım. Bunun sonucunda bilgisayar belleğine DLL uzantılı bir kitaplık dosyası yüklenir. Bu kitaplık bir tarayıcı tarafından kullanılır (`tarayıcı.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.

   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**. Dosya karma kodu.

   - **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://<nesne>`; burada `<nesne>`, 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**. Dosya karma kodu.

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**. Dosya karma kodu.
    - **Hedef nesne**. Hedef işlemi başlatma komutu. `object://<komut>` 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**. Dosya karma kodu.

    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. Kurallar 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.

Potansiyel olarak zararlı eylemleri engelleme hakkında mesaj ve yöneticiye gönderilecek mesaj için özel şablonlar mevcuttur. Mesaj şablonlarını değiştirebilirsiniz.

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: **Yöneticiye 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.
4. Değişikliklerinizi kaydedin.

Uyarlamalı Anomali Denetimi raporlarını görüntüleme

Uyarlamalı Anomali Denetimi raporlarını görüntülemek için:

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.

   Uyarlamalı Anomali Denetimi bileşeninin ayarları pencerenin sağ kısmında görüntülenir.

5. Aşağıdakilerden birini yapın:

   - Uyarlamalı Anomali Denetimi kurallarının ayarları hakkındaki bir raporu görüntülemek istiyorsanız **Uyarlamalı Anomali Denetimi kurallarının durumu hakkında rapor** düğmesine tıklayın.
   - Uyarlamalı Anomali Denetimi kurallarının tetiklenmesi hakkındaki bir raporu görüntülemek istiyorsanız **Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor** düğmesine tıklayın.

6. Rapor üretme işlemi başlar.

Rapor yeni bir pencerede görüntülenir.

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*), 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.

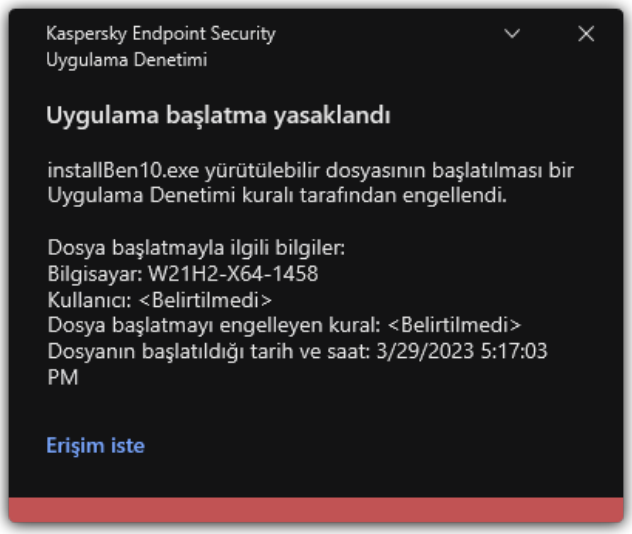
3. Uygulama Denetimi modunu seçme.

   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.

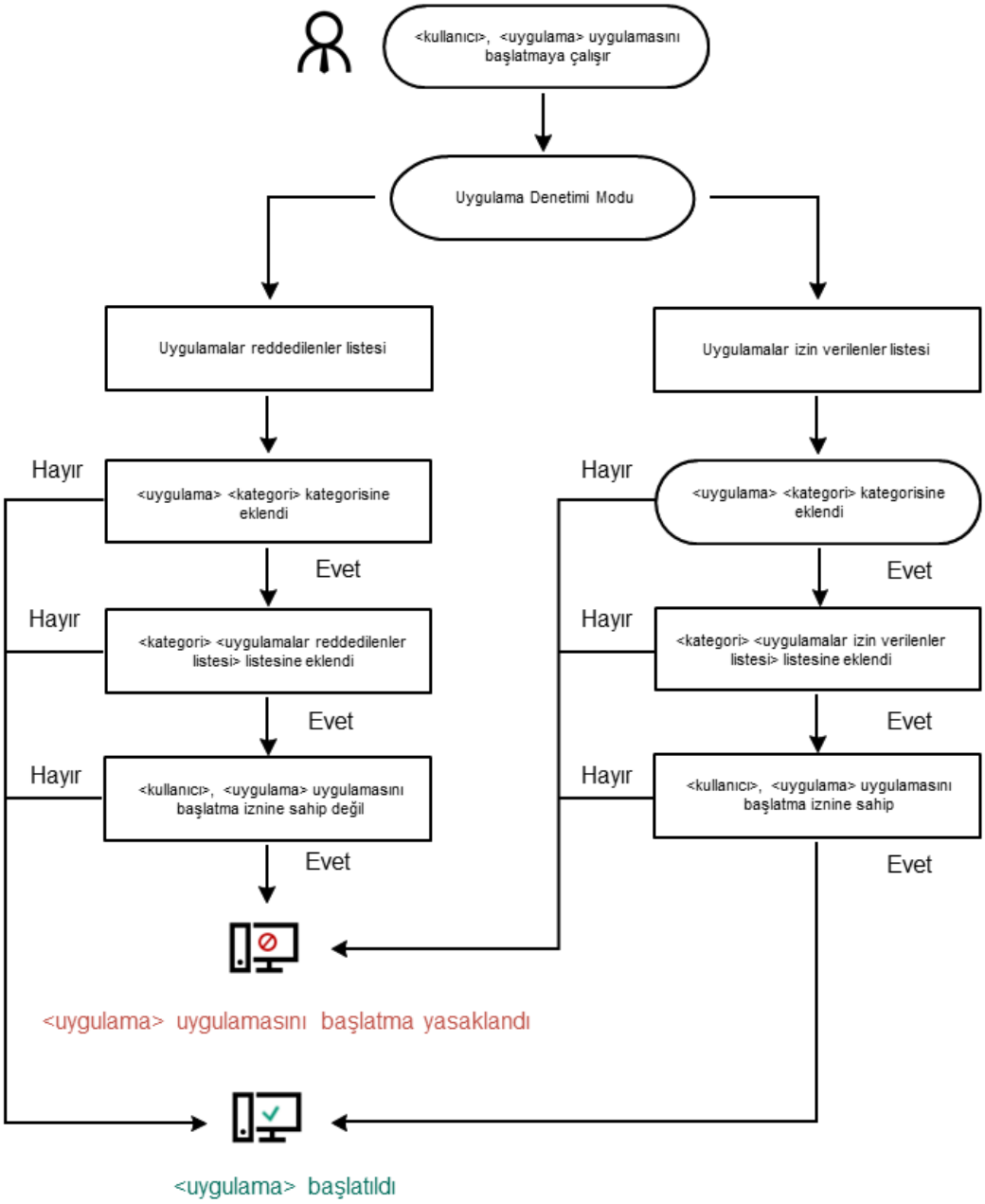
  Kaspersky Security Center Yönetim Konsolunda oluşturulan Uygulama Denetimi kuralları, Kaspersky Endpoint Security yerel arabiriminde olduğu gibi dahil etme ve hariç tutma koşullarına değil, özel uygulama kategorilerine dayanır.

- 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 tanınırlığına göre güvenilen **Diğer uygulamalar\KSN'deki tanınırlığına göre güvenilir uygulamalar**, KSN sunucularına bir bağlantının mevcut 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.

Kullanıcı bilgisayarlarına yüklenen uygulamalar hakkında bilgi toplama

Optimum Uygulama Denetimi kurallarını oluşturmak için öncelikle kurumsal LAN'daki bilgisayarlarda kullanılan uygulamaların bir resmini edinmeniz önerilir. Bunu yapmak için aşağıdaki bilgileri edinebilirsiniz:

- Satıcılar, sürümler ve kurumsal LAN'da kullanılan uygulamaların yerelleştirmeleri.
- Uygulama güncellemelerinin sıklığı.
- Şirket tarafından benimsenen uygulama kullanım ilkesi (bu güvenlik ilkeleri veya yönetimsel ilkeler olabilir).
- Uygulama dağıtım paketlerinin depolama alanı konumu.

Kurumsal LAN ağı bilgisayarlarında kullanılan uygulamalar hakkındaki bilgiler, **Yürütülebilir dosyalar** klasöründe **Uygulama kayıt defteri** klasöründe yer almaktadır. **Uygulama kayıt defteri** klasörü ve **Yürütülebilir dosyalar** klasörü, Kaspersky Security Center Yönetim Konsolu ağacında **Uygulama yönetimi** klasöründe yer almaktadır.

Uygulama kayıt defteri klasörü, istemci bilgisayarında yüklü Ağ Aracısı tarafından tespit edilen uygulamaların listesini içerir.

Yürütülebilir dosyalar klasörü, istemci bilgisayarlarda şimdiye kadar başlatılmış veya Kaspersky Endpoint Security'nin envanter görevi sırasında tespit edilen tüm yürütülebilir dosyaların bir listesini içerir.

Uygulama ve yürütülebilir dosyaları ile bir uygulamanın yüklendiği bilgisayarların listesi hakkında genel bilgiler görüntülemek için **Uygulama kayıt defteri** klasöründe veya **Yürütülebilir dosyalar** klasöründe seçilen bir uygulamanın özellikler penceresini açın.

Uygulama kayıt defteri klasöründe bulunan uygulama özellikleri penceresini açmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Uygulama kayıt defteri**'ni seçin.
3. Bir uygulama seçin.
4. Uygulamanın bağlam menüsünde **Özellikler**'i seçin.

Yürütülebilir dosyalar klasöründe bulunan yürütülebilir bir dosyanın özellikler penceresini açmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Gelişmiş** → **Uygulama yönetimi** → **Yürütülebilir dosyalar** klasörünü seçin.
3. Yürütülebilir bir dosya seçin.
4. Yürütülebilir dosyanın bağlam menüsünden **Özellikler**'i seçin.

Uygulama Denetimi'ni etkinleştirme ve devre dışı bırakma

Varsayılan olarak Uygulama Denetimi devre dışıdır.

Uygulama Denetimi'ni etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Uygulama Denetimi** geçiş düğmesini kullanın.
4. Değişikliklerinizi kaydedin.

Sonuç olarak, Uygulama Denetimi etkinleştirilirse, uygulama yürütülebilir dosyaların çalıştırılmasına ilişkin bilgileri Kaspersky Security Center'a iletir. **Yürütülebilir dosyalar** klasöründeki Kaspersky Security Center'da çalışan yürütülebilir dosyaların listesini görüntüleyebilirsiniz. Yalnızca çalışan çalıştırılabilir dosyalar yerine tüm yürütülebilir dosyalar hakkında bilgi almak için *Envanter* görevini çalıştırın.

Uygulama Denetimi modunu seçme

Uygulama Denetimi modunu seçmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Uygulama Denetimi**'ni seçin.
3. **Uygulama Başlatma Denetimi modu** bloğunda, aşağıdaki seçeneklerden birini seçin:
   - **Engellenen uygulamalar**. Bu seçenek belirlenirse Uygulama Denetimi engelleme kurallarının koşullarının yerine getirildiği durumlar haricinde, Uygulama Denetimi tüm kullanıcıların herhangi bir uygulamayı başlatmasına izin verir.
   - **İzin verilen uygulamalar**. Bu seçenek belirlenirse Uygulama Denetimi izin verme kuralları koşullarının yerine getirildiği durumlar haricinde, Uygulama Denetimi tüm kullanıcıların herhangi bir uygulamayı başlatmasını engeller.

     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.

   Seçilen mod sırasında oluşturulan tüm kurallar mod değiştirildikten sonra kaydedilerek kuralların tekrar kullanılabilmesi sağlanır. Bu kuralları kullanmaya geri dönmek için tek yapmanız gereken gerekli modu seçmektir.
4. **Engellenen uygulamaların başlangıcındaki işlem** bloğunda, kullanıcı Uygulama Denetimi kuralları tarafından engellenen bir uygulamayı başlatmaya çalıştığı zaman bileşen tarafından gerçekleştirilecek eylemi seçin.
5. Uygulamalar, kullanıcılar tarafından başlatıldığında Kaspersky Endpoint Security'nin DLL modüllerinin yüklenmesini izlemesini istiyorsanız **DLL modülleri yüklenmesini denetle** onay kutusunu işaretleyin.

   Modül ve modüle yüklenen uygulamayla ilgili bilgiler bir rapora kaydedilir.

   Kaspersky Endpoint Security, yalnızca onay kutusu seçildikten sonra yüklenen DLL modüllerini ve sürücüleri izler. Kaspersky Endpoint Security başlatılmadan önce yüklenenler de dahil olmak üzere Kaspersky Endpoint Security'nin tüm DLL modüllerini ve sürücüleri izlemesini isterseniz, onay kutusunu seçtikten sonra bilgisayarı yeniden başlatın.

   DLL modüllerinin ve sürücülerin yüklenmesine ilişkin denetimi etkinleştirirken, Uygulama Denetimi ayarlarındaki kurallardan varsayılan **Altın İmaj** kuralının ya da "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.

   Uygulama ayarlarını yapılandırmak için parola korumasını açmanızı öneririz; böylece Kaspersky Security Center ilke ayarlarını değiştirmeden kritik DLL modüllerinin ve sürücülerin başlatılmasını engelleyen kuralları kapatmak mümkündür.
6. Değişikliklerinizi kaydedin.

Uygulama Denetimi kurallarını yönetme

Kaspersky Endpoint Security, kullanıcıların uygulamaları başlatmasını kurallarla denetler. Uygulama Denetimi kuralı, tetikleme koşullarını ve kural tetiklendiğinde (kullanıcılar tarafından uygulamanın başlatılmasına izin verir veya engeller) Uygulama Denetimi bileşeni 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 ediliyor**. 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** klasörünü seçin.
3. Çalışma alanında **Yeni kategori** düğmesine tıklayın.

   Kullanıcı kategorisi oluşturma sihirbazı başlar.
4. Kullanıcı kategorisi oluşturma sihirbazının talimatlarını uygulayın.

1. Adım. Kategori türünü seçme

Bu adımda, aşağıdaki uygulama kategorileri türlerinden birini seçin:

- **İçeriğin yer aldığı kategori elle eklendi**. Bu kategori türünü seçtiyseniz "Kategorideki uygulamaları dahil etme koşullarını yapılandırma" adımında ve "Kategoriden uygulamaları hariç tutma koşullarını yapılandırma" adımında, yürütülebilir dosyaları bir kategoriye dahil ederek kriterleri tanımlayabilirsiniz.
- **Seçilen cihazlardaki yürütülebilir dosyaları içeren kategori**. Bu kategori türünü seçtiyseniz "Ayarlar" adımında, yürütülebilir dosyaları kategoriye otomatik olarak dahil edileceği bir bilgisayar belirtebilirsiniz.
- **Belirli bir klasördeki yürütülebilir dosyaları içeren kategori**. Bu kategori türünü seçtiyseniz "Veri havuzu klasörü" adımında, yürütülebilir dosyaların kategoriye otomatik olarak dahil edileceği bir klasör belirtebilirsiniz.

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

İçeriğin yer aldığı kategori elle 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**. 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.
- **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 elle 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**. 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 SHA-256'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.
- **Tarama aralığı (s)** alanı. Bu alanda, Kaspersky Security Center uygulama kategorisini temizledikten ve **Yürütülebilir dosyalar** klasöründe bulunan bilgisayarlardan tüm yürütülebilir dosyaları buna ekledikten sonra bu süreyi (saat olarak) belirtebilirsiniz.

  Verileri Yönetim Sunucusu veri havuzuyla senkronize et onay kutusu işaretlenirse bu alan kullanılabilir.

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 SHA-256'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 (s)** alanı. 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

Sihirbazdan çıkın.

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, 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 **Konu** 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** klasörünü seçin.
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 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)**.
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'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.

   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.

5. **Ekle**'ye tıklayın.

   Uygulama Denetimi kuralı penceresi açılır.

6. Aşağıdakilerden birini yapın:

   - Yeni bir kategori oluşturmak istiyorsanız:

     a. **Kategori oluştur**'a tıklayın.

Kullanıcı kategorisi oluşturma sihirbazı başlar.

b. Kullanıcı kategorisi 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.

7. **Kişiler ve hakları** tablosunda **Ekle** düğmesine tıklayın.
8. Açılan pencerede, seçilen kategoriden uygulamaları başlatmak için izinlerini yapılandırmak istediğiniz kullanıcıların ve/veya kullanıcı gruplarının listesini belirtin.
9. **Kişiler 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.
10. **Konu** sütununda görülmeyen ve **Konu** sütununda belirtilen kullanıcı grubunun parçası olmayan tüm kullanıcıların seçilen kategorilere ait uygulamaları başlatmasını engellemek isterseniz **Diğer kullanıcılar için reddet** onay kutusunu işaretleyin.
11. 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.

12. 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. Kural tetikleme koşullarını karşılayan uygulamaları başlatmasına izin verilen veya izin verilmeyen kullanıcılar ve/veya kullanıcı gruplarının bir listesini derleyin veya düzenleyin. Bunun için **Kişiler ve hakları** tablosunda **Ekle** düğmesine tıklayın.

Kural varsayılan olarak tüm kullanıcılar için geçerlidir.

> Tabloda belirtilen kullanıcı yoksa kural kaydedilemez.

d. **Kişiler ve hakları** tablosunda, geçiş düğmesini kullanıcıların uygulamaları başlatma hakkını tanımlamak için kullanın.

e. Uygulamanın, **Kişiler ve hakları** tablosunda listelenmeyen ve **Kişiler ve hakları** tablosunda listelenen kullanıcı gruplarının üyesi olmayan tüm kullanıcılar için kural tetikleme koşullarını karşılayan uygulamaların çalışmasının engellemesini istiyorsanız **Diğer kullanıcılar için reddet** onay kutusunu işaretleyin.

> **Diğer kullanıcılar için reddet** onay kutusu işaretlenmezse Kaspersky Endpoint Security, **Kişiler ve hakları** tablosunda belirtilmeyen ve **Kişiler 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 üzerinde değiştirmek için:

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.

Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.

5. 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.

6. Değişikliklerinizi kaydedin.

Uygulama Denetimi kuralının durumunu Yönetim Konsolu üzerinden 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 ediliyor**. 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'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 kuralları listesini dışa aktarmak için:
   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla bağlantı noktası 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.
6. 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.

7. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da Uygulama Denetimi kuralları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Güvenlik Denetimleri** → **Uygulama Denetimi**'ne gidin.
5. **Kurallar Listeleri Ayarları** bağlantısına tıklayın.
6. Bir kural listesi seçin: uygulama reddedilenler listesi veya izin verilenler listesi.
7. Uygulama Denetimi 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.
8. 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.
9. 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'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.
   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.
5. **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.

6. 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.

7. 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.

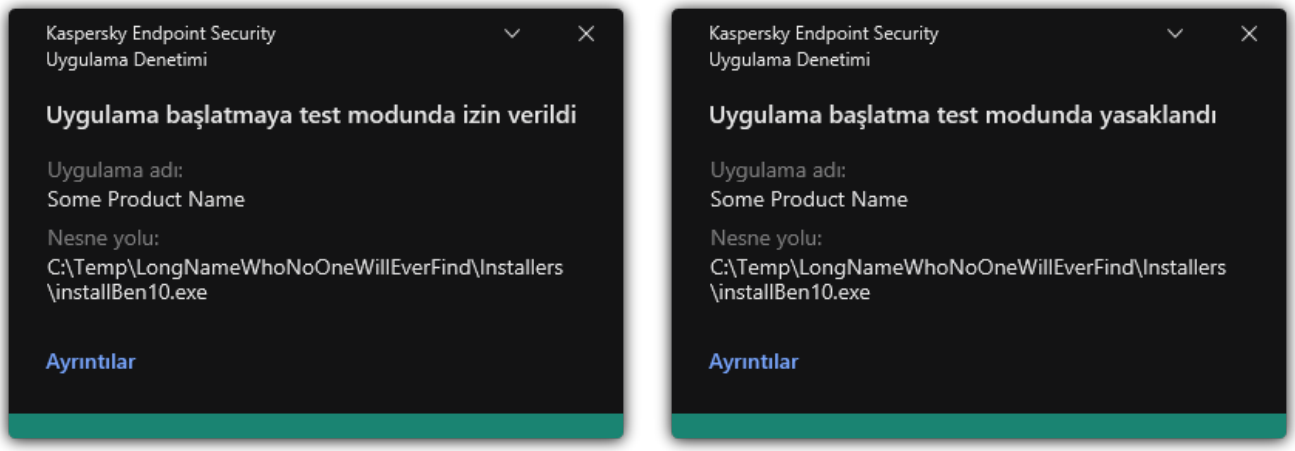
   Bu, Uygulama Denetimi kurallarının listesini açar.

4. **Durum** bölümünde **Test ediliyor** 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

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'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** → **Arabirim** öğesini seçin.
5. Araca erişim vermek ya da erişimi iptal etmek için **Uygulama Etkinlik İzleyicisi bölümünü gizle** onay kutusunu kullanın.
6. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console kullanılarak uygulama arabiriminde Uygulama Etkinlik İzleyicisi nasıl gizlenir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel Ayarlar** → **Arabirim** 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. Kullanıcı, uygulamanın başlatılmasının yanlışlıkla engellendiğini düşünüyorsa mesaj metnindeki bağlantıyı kullanarak yerel kurumsal ağ yöneticisine bir mesaj gönderebilir.

Uygulamanın başlatılması engellendiğinde görüntülenen mesaj ve yöneticiye gönderilen mesaj için özel şablonlar mevcuttur. Mesaj şablonlarını değiştirebilirsiniz.

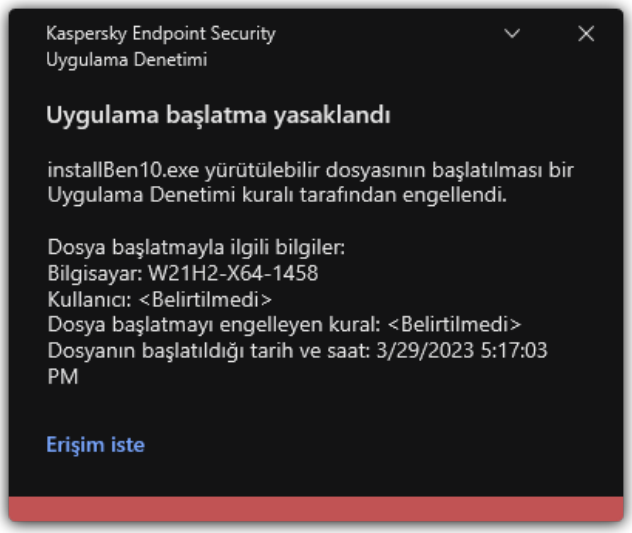
Bir mesaj şablonunu düzenlemek için:

1. 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. Engellenen bir uygulama ile ilgili bildirim aşağıdaki gibi gösterilir.

     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. 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.

4. Değişikliklerinizi kaydedin.



Uygulama Denetimi bildirimi

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 elle 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.
- **Seçilen 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 bağlantı noktalarını izleme

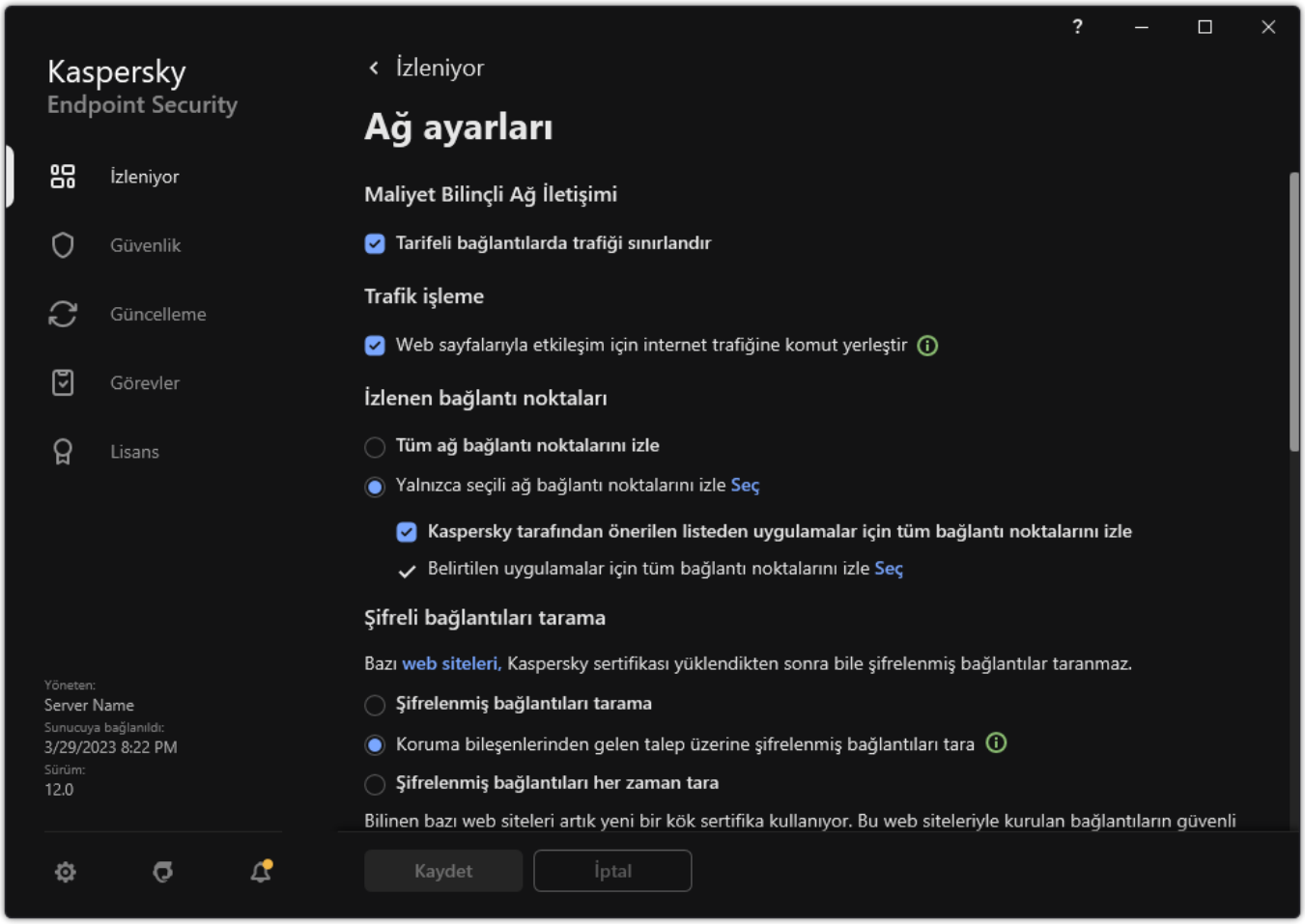
Kaspersky Endpoint Security'nin çalışması sırasında İnternet Denetimi, Posta Tehdidi Koruması ve Web Tehdidi Koruması bileşenleri, belirli iletişim kurallarından aktarılan ve kullanıcı bilgisayarında TCP ve UDP gibi belirli açık bağlantı noktalarından geçen veri akışlarını izler. Örneğin Posta Tehdidi 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 bağlantı noktalarını riskten etkilenme olasılığına bağlı olarak birkaç gruba ayırır. Bazı ağ bağlantı noktaları hassas hizmetler için ayrılmıştır. Bu bağlantı noktalarını daha iyi izlemeniz önerilir çünkü bunların bir ağ saldırısı tarafından hedef alınma ihtimali daha fazladır. Standart olmayan ağ bağlantı noktalarından yararlanan standart olmayan hizmetler kullanıyorsanız, bu ağ bağlantı noktaları da saldıran bilgisayar tarafından hedeflenebilir. Ağa erişim isteyen ağ bağlantı noktalarının listesini ve uygulamaların listesini de belirtebilirsiniz. Ağ trafiğini izleme sırasında Posta Tehdidi Koruması ve Web Tehdidi Koruması bileşenleri bu bağlantı noktalarına ve uygulamalara özellikle dikkat eder.

Tüm ağ bağlantı noktalarını izlemeyi etkinleştirme

Tüm ağ bağlantı noktalarını izlemeyi etkinleştirmek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.



Ağ bağlantı noktaları izleme ayarları

3. **İzlenen bağlantı noktaları** bloğunda, **Tüm ağ bağlantı noktalarını izle**'yi seçin.
4. Değişikliklerinizi kaydedin.

İzlenen ağ bağlantı noktalarının listesini oluşturma

İzlenen ağ bağlantı noktalarının listesini oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **İzlenen bağlantı noktaları** bloğunda, **Yalnızca seçili ağ bağlantı noktalarını izle**'yi seçin.
4. **Seç**'e tıklayın.

   Bu, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ bağlantı noktalarının listesini açar. Ağ bağlantı noktalarının listesi, Kaspersky Endpoint Security paketinde yer alır.
5. Ağ bağlantı noktası izlemeyi etkinleştirmek veya devre dışı bırakmak için **Durum** sütunundaki geçiş düğmesini kullanın.
6. Ağ bağlantı noktalarının listesinde bir ağ bağlantı noktası görülmüyorsa aşağıdaki işlemleri yaparak ekleyin:

   a. **Ekle**'ye tıklayın.

   b. Açılan pencerede, ağ bağlantı noktası numarası ve kısa açıklama girin.

c. Ağ bağlantı noktası izleme için **Etkin** veya **Etkin değil** durumunu ayarlayın.

7. Değişikliklerinizi kaydedin.

FTP iletişim kuralı pasif modda çalıştığında, izlenen ağ bağlantı noktalarının listesine eklenmeyen rastgele bir ağ bağlantı noktası üzerinden bağlantı kurulur. Bu tür bağlantıları korumak için, tüm ağ bağlantı noktalarının izlenmesini etkinleştirin veya FTP bağlantıları kuran uygulamalar için ağ bağlantı noktalarının denetimini yapılandırın.

Tüm ağ bağlantı noktalarının izlendiği uygulamaların listesini oluşturma

Kaspersky Endpoint Security'nin tüm ağ bağlantı noktalarını izlediği uygulamaların bir listesini oluşturabilirsiniz.

FTP iletişim kuralı üzerinden veri alan veya ileten uygulamaların, Kaspersky Endpoint Security'nin tüm ağ bağlantı noktalarını izlediği uygulamalar listesine eklenmesini öneririz.

Tüm ağ bağlantı noktalarının izlendiği uygulamaların listesini oluşturmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Ağ ayarları** seçimini yapın.
3. **İzlenen bağlantı noktaları** bloğunda, **Yalnızca seçili ağ bağlantı noktalarını izle**'yi seçin.
4. **Kaspersky tarafından önerilen listeden uygulamalar için tüm bağlantı noktalarını izle** onay kutusunu işaretleyin.
   Bu onay kutusu işaretlenirse Kaspersky Endpoint Security aşağıdaki uygulamalar için tüm bağlantı noktalarını 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 bağlantı noktalarını izle** onay kutusunu işaretleyin.
6. **Seç**'e tıklayın.
   Bu, Kaspersky Endpoint Security'nin ağ bağlantı noktalarını izlediği uygulamaların bir listesini açar.
7. Ağ bağlantı noktası 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 bağlantı noktalarını izleme için **Etkin** veya **Etkin değil** durumunu ayarlayın.

9. Değişikliklerinizi kaydedin.

İzlenen bağlantı noktalarının listelerini dışa ve içe aktarma

Kaspersky Endpoint Security, ağ bağlantı noktalarını izlemek için aşağıdaki listeleri kullanır: ağ bağlantı noktalarının listesi ve bağlantı noktaları Kaspersky Endpoint Security tarafından izlenen uygulamaların listesi. İzlenen bağlantı noktalarının listelerini bir XML dosyasına aktarabilirsiniz. Daha sonra, örneğin aynı açıklamaya sahip çok sayıda bağlantı noktası eklemek için dosyayı değiştirebilirsiniz. İzlenen bağlantı noktaları listelerini yedeklemek veya listeyi farklı bir sunucuya taşımak için dışa/içe aktarma işlevini de kullanabilirsiniz.

[Yönetim Konsolu'nda (MMC) izlenen bağlantı noktalarının listelerini 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** → **Ağ ayarları** öğesini seçin.
5. **İzlenen bağlantı noktaları** bloğunda, **Yalnızca seçili ağ bağlantı noktalarını izle**'yi seçin.
6. **Ayarlar**'a tıklayın.

   Ağ bağlantı noktaları penceresi açılır. **Ağ bağlantı noktaları** penceresinde, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ bağlantı noktalarının listesi görüntülenir. Ağ bağlantı noktalarının listesi, Kaspersky Endpoint Security paketinde yer alır.

7. Ağ bağlantı noktaları listesini dışa aktarmak için:

   a. Ağ bağlantı noktaları listesinden dışa aktarmak istediğiniz bağlantı noktalarını seçin. Birden fazla bağlantı noktası seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

   Herhangi bir bağlantı noktası seçmediyseniz, Kaspersky Endpoint Security tüm bağlantı noktalarını dışa aktarır.

   b. **Dışa aktar**'a tıklayın.

   c. Açılan pencerede, güvenilir aygıtlar listesini dışa aktarmak istediğiniz XML dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   d. Dosyaya kaydet.

   Kaspersky Endpoint Security, ağ bağlantı noktaları listesinin tamamını XML dosyasına aktarır.

8. Kaspersky Endpoint Security tarafından bağlantı noktaları izlenen uygulamaların listesini dışa aktarmak için:

   a. **Belirtilen uygulamalar için tüm bağlantı noktalarını izle** onay kutusunu işaretleyin.

   b. Uygulamalar listesinden, dışa aktarmak istediğiniz uygulamaları seçin. Birden fazla bağlantı noktası 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.

9. Ağ bağlantı noktaları listesini içe aktarmak için:

a. Ağ bağlantı noktaları listesinde **İçe aktar** düğmesine tıklayın.

Açılan pencerede, ağ bağlantı noktaları listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir ağ bağlantı noktaları listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

10. Kaspersky Endpoint Security tarafından bağlantı noktaları 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.

11. Değişikliklerinizi kaydedin.

Web Console ve Cloud Console'da izlenen bağlantı noktalarının listelerini dışa/içe aktarma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 bağlantı noktaları listesini dışa aktarmak için:

a. **İzlenen bağlantı noktaları** bloğunda, **Yalnızca seçili ağ bağlantı noktalarını izle**'yi seçin.

b. **N bağlantı noktası selçildi** bağlantısına tıklayın.

Ağ bağlantı noktaları penceresi açılır. **Ağ bağlantı noktaları** penceresinde, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ bağlantı noktalarının listesi görüntülenir. Ağ bağlantı noktalarının listesi, Kaspersky Endpoint Security paketinde yer alır.

c. Ağ bağlantı noktaları listesinden dışa aktarmak istediğiniz bağlantı noktalarını seçin.

d. **Dışa aktar**'a tıklayın.

e. Açılan pencerede, güvenilir aygıtlar listesini dışa aktarmak istediğiniz XML dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

f. Dosyaya kaydet.

Kaspersky Endpoint Security, ağ bağlantı noktaları listesinin tamamını XML dosyasına aktarır.

6. Kaspersky Endpoint Security tarafından bağlantı noktaları izlenen uygulamaların listesini dışa aktarmak için:

a. **İzlenen bağlantı noktaları** bloğunda, **Belirtilen uygulamalar için tüm bağlantı noktalarını izle** onay kutusunu seçin.

b. **N uygulama selçildi** 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 bağlantı noktaları listesini içe aktarmak için:

a. Ağ bağlantı noktaları listesinde **İçe aktar** düğmesine tıklayın.

Açılan pencerede, ağ bağlantı noktaları listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

b. Dosyayı aç.

Bilgisayar zaten bir ağ bağlantı noktaları 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 bağlantı noktaları 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.

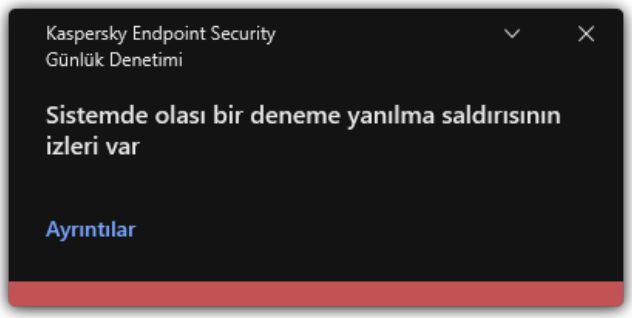
Günlük Denetleyici

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, 11.11.0 sürümünden itibaren Günlük Denetimi bileşenini içerir. 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, güvenlik denetimi ilkesinin yapılandırıldığından ve sistemin ilgili olayları günlüğe kaydettiğinden emin olun (ayrıntılar için bkz. Microsoft teknik destek web sitesi.).



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'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** → **Günlük Denetimi** seçimini yapın.
5. **Günlük Denetimi** onay kutusunun seçili olduğundan emin olun.
6. **Önceden tanımlanmış kurallar** bloğunda **Ayarlar** düğmesine tıklayın.
7. 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 kullanımına ilişkin izler var**.
   - **Yüklenen yeni bir hizmet adına tespit edilen alışılmadık eylemler**.
   - **Açık kimlik bilgileri kullanan olağandışı oturum açma algılandı**.
   - **Sistemde olası bir Kerberos sahte PAC (MS14-068) saldırısının izleri var**.
   - **Ayrıcalıklı yerleşik Yöneticiler grubunda şüpheli değişiklikler tespit edildi**.
8. 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.
9. **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 12:00 - 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.

Kaspersky Endpoint Security, bu kullanıcılar ve bilgisayarlar için oturum açma girişimlerini izlemez.

d. **Tamam**'a tıklayın.

10. Değişikliklerinizi kaydedin.

[Web Console'da ve Cloud Console'da önceden tanımlanmış kuralları yapılandırma](#)

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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** onay kutusunun 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 kullanımına ilişkin izler var**.
   - **Yüklenen yeni bir hizmet adına tespit edilen alışılmadık eylemler**.
   - **Açık kimlik bilgileri kullanan olağandışı 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 12:00 - 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.

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 kullanımına ilişkin izler var**.
   - **Yüklenen yeni bir hizmet adına tespit edilen alışılmadık eylemler**.
   - **Açık kimlik bilgileri kullanan olağandışı 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 12:00 - 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.

   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: *Application*, *Security* or *System*. 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'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** → **Günlük Denetimi** seçimini yapın.
5. **Günlük Denetimi** onay kutusunun seçili olduğundan emin olun.
6. **Özel kurallar** bloğunda **Ayarlar** düğmesine tıklayın.
7. Açılan pencerede, etkinleştirmek istediğiniz özel kuralların yanındaki onay kutularını seçin.
8. Gerekirse, kendi özel kurallarınızı oluşturmak için **Ekle**'ye tıklayın.
9. Bir pencere açılır; bu pencerede özel kuralı yapılandırın:
   - **Kural adı**.
   - **Günlük adı**. Windows Olay Günlükleri. Şu günlükler mevcuttur: *Application*, *Security*, *System*.
   - **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.
10. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da bir özel kaynak nasıl oluşturulur

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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** onay kutusunun 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**.
   - **Windows Olay Günlüğü adı**. Windows Olay Günlükleri. Şu günlükler mevcuttur: *Application*, *Security*, *System*.
   - **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).
   - **Windows Olay Günlüğü tanımlayıcısı**. 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: *Application*, *Security*, *System*.
   - **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.

Dosya Bütünlüğü İzleyici

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.

Dosya Bütünlük İzleyicisi yalnızca NTFS veya ReFS dosya sistemine sahip sunucularda çalışır.

Kaspersky Endpoint Security for Windows, 11.11.0 sürümünden itibaren Dosya Bütünlük İzleyicisi bileşenini içerir. Dosya Bütünlük İzleyicisi, belirli bir izleme alanındaki nesnelerde (dosyalar ve klasörler) yapılan değişiklikleri algılar. Bu değişiklikler bir bilgisayar güvenlik ihlalini gösterebilir. Nesne değişiklikleri tespit edildiğinde uygulama yöneticiyi bilgilendirir.

Dosya Bütünlük İzleyicisini kullanmak için bileşenin kapsamını yapılandırmalısınız, yani durumu bileşen tarafından izlenmesi gereken nesneleri seçmelisiniz.

Kaspersky Security Center'da ve Kaspersky Endpoint Security for Windows arabiriminde Dosya Bütünlük İzleyicisi işleminin sonuçları hakkındaki bilgileri görüntüleyebilirsiniz.

Tarama kapsamının düzenlenmesi

Dosya Bütünlük İzleyicisi, belirli bir izleme kapsamı olmadan çalışamaz. Bu, Dosya Bütünlük İzleyicisi'nin kontrol edeceği değişikliklerin dosya ve klasörlerin yollarını belirtmeniz gerektiği anlamına gelir. Nadiren değiştirilen nesneleri veya yalnızca yöneticinin erişebildiği nesneleri eklemenizi öneririz. Bu, Dosya Bütünlük İzleyicisi olaylarının sayısını azaltacaktır.

Olay sayısını azaltmak için izleme kurallarına istisnalar da ekleyebilirsiniz. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir. Örneğin, kuruluş, dosyalarını bütünlük açısından izlemek istediğiniz bir uygulama kullanıyordur. Bunu yapmak için, uygulamanın bulunduğu klasörün yolunu eklemeniz gerekir (örneğin, `C:\Users\Testadmin\Desktop\Utilities`). Bu tür dosyalar sistem güvenliğini etkilemediğinden, günlük dosyalarını izleme kuralının dışında tutabilirsiniz. Ayrıca, uygulama günlük dosyalarını sürekli olarak değiştirir ve bu da çok sayıda benzer olayla sonuçlanır. Bunu önlemek için istisnalara günlük dosyaları ekleyin (örneğin, `C:\Users\Testadmin\Desktop\Utilities\*.log`).

Yönetim Konsolu'nda (MMC) bir izleme kapsamı nasıl düzenlenir

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** → **Dosya Bütünlük İzleyicisi**'ni seçin.
5. **Dosya Bütünlük İzleyicisi** onay kutusunun seçili olduğundan emin olun.
6. **İzleme kuralları** bloğunda, **Ekle** düğmesine tıklayın.
7. Bir pencere açılır; bu pencerede izleme kuralını yapılandırın:
   - **Kural adı**. Kuralın adını girin, örneğin, *A uygulamasını izleme*.
   - **Olay önem düzeyi**. Dosya Bütünlüğü İzleyicisinin günlüğe kaydedeceği olay önem seviyesini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.
   - **İzleme kapsamı**. Klasör veya dosyanın yolunu girin.

     İzleme kapsamını yapılandırırken, klasör veya dosya yolunun bir sürücü harfi ya da bir sistem ortam değişkeni ile başladığından emin olun. Uygulama, kullanıcı ortam değişkenlerini desteklemez. Klasörün veya dosyanın yolu yanlış belirtildiği takdirde, Kaspersky Endpoint Security belirtilen izleme kapsamını eklemeyecektir.

     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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

- **İstisnalar**. Klasör veya dosyanın yolunu girin. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.

8. **Tamam**'a tıklayın.

   İzleme kuralları listesine yeni bir kural eklenir. İzleme kuralını, kurallar listesinden kaldırmadan devre dışı bırakabilirsiniz. Bunu yapmak için nesnenin yanındaki onay kutusunun işaretini kaldırın.

9. Değişikliklerinizi kaydedin.

[Web Console'da bir tarama kapsamı nasıl düzenlenir]

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Güvenlik Denetimleri** → **Dosya Bütünlük İzleyicisi**'ne gidin.

5. **Dosya Bütünlük İzleyicisi** geçiş anahtarının açık durumda olduğundan emin olun.

6. **İzleme kuralları** bloğunda, **Ekle** düğmesine tıklayın.

7. Bir pencere açılır; bu pencerede izleme kuralını yapılandırın:

   - **Kural adı**. Kuralın adını girin, örneğin, *A uygulamasını izleme*.

   - **Olay önem düzeyi**. Dosya Bütünlüğü İzleyicisinin günlüğe kaydedeceği olay önem seviyesini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   - **İzleme kapsamı**. Klasör veya dosyanın yolunu girin.

     > İzleme kapsamını yapılandırırken, klasör veya dosya yolunun bir sürücü harfi ya da bir sistem ortam değişkeni ile başladığından emin olun. Uygulama, kullanıcı ortam değişkenlerini desteklemez. Klasörün veya dosyanın yolu yanlış belirtildiği takdirde, Kaspersky Endpoint Security belirtilen izleme kapsamını eklemeyecektir.

     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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

- **İstisnalar**. Klasör veya dosyanın yolunu girin. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.

8. **Tamam**'a tıklayın.

   İzleme kuralları listesine yeni bir kural eklenir. İzleme kuralını, kurallar listesinden kaldırmadan devre dışı bırakabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.

9. Değişikliklerinizi kaydedin.

[Uygulama arabiriminde bir izleme kapsamı nasıl düzenlenir](#)

1. Ana uygulama penceresinde düğmesine tıklayın.

2. Uygulama ayarları penceresinden **Güvenlik Denetimleri** → **Dosya Bütünlük İzleyicisi**'ni seçin.

3. **Dosya Bütünlük İzleyicisi** geçiş anahtarının açık durumda olduğundan emin olun.

4. **İzleme kuralları** bloğunda, **Kuralları yapılandır**'a tıklayın.

5. **İzleme kuralları** bloğunda, **Ekle** düğmesine tıklayın.

6. Bir pencere açılır; bu pencerede izleme kuralını yapılandırın:

   - **Kural adı**. Kuralın adını girin, örneğin, *A uygulamasını izleme*.

   - **Olay önem düzeyi**. Dosya Bütünlüğü İzleyicisinin günlüğe kaydedeceği olay önem seviyesini seçin: *Bilgilendirici*, *Uyarı*, *Kritik*.

   - **İzleme kapsamı**. Klasör veya dosyanın yolunu girin.

     > İzleme kapsamını yapılandırırken, klasör veya dosya yolunun bir sürücü harfi ya da bir sistem ortam değişkeni ile başladığından emin olun. Uygulama, kullanıcı ortam değişkenlerini desteklemez. Klasörün veya dosyanın yolu yanlış belirtildiği takdirde, Kaspersky Endpoint Security belirtilen izleme kapsamını eklemeyecektir.

     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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

   - **İstisnalar**. Klasör veya dosyanın yolunu girin. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. İstisna girişleri, kapsam girişlerini izlemekten daha yüksek önceliğe sahiptir.

7. **Tamam**'a tıklayın.

İzleme kuralları listesine yeni bir kural eklenir. İzleme kuralını, kurallar listesinden kaldırmadan devre dışı bırakabilirsiniz. Bunu yapmak için yanındaki anahtarı kapalı konuma getirin.

8. Değişikliklerinizi kaydedin.

Sistem bütünlüğü bilgilerini görüntüleme

Dosya Bütünlük İzleyicisi işleminin sonuçlarıyla ilgili bilgiler aşağıdaki şekillerde görüntülenir:

Kaspersky Security Center Konsolu ve Kaspersky Endpoint Security arabirimindeki olaylar

Kaspersky Endpoint Security, dosyalarda bir değişiklik algıladığında Kaspersky Security Center'a bir olay gönderir. Olay seçimini, Dosya Bütünlük İzleyicisi bileşeninden olayları görüntülemek üzere yapılandırabilirsiniz. Olay seçimi ayarları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun.

Kaspersky Endpoint Security arabirimi, Dosya Bütünlük İzleyicisi bileşeni için ayrı bir rapor sağlar.

Kaspersky Endpoint Security, Dosya Bütünlük İzleyici olaylarının sayısını azaltmak için olay toplama araçlarına sahiptir. Kaspersky Endpoint Security, şu durumlarda olay toplamayı etkinleştirir:

- tek bir nesnede çok sık değişiklik olması (dakikada beşten fazla)
- tek bir izleme kuralının çok sık tetiklenmesi (dakikada 10 defadan fazla)

Sonuç olarak Kaspersky Endpoint Security, toplama araçları tetiklenene kadar nesne değişikliklerinde ayrı olaylar oluşturur. Bu noktada, Kaspersky Endpoint Security olay toplamayı etkinleştirir ve buna karşılık gelen bir olay oluşturur. Kaspersky Endpoint Security, 24 saat boyunca (toplama dönemi) veya Kaspersky Endpoint Security durdurulana kadar olay toplama gerçekleştirir. Kaspersky Endpoint Security'yi yeniden başlattıktan veya toplama süresi sona erdikten sonra uygulama özel olaylar oluşturur: *Toplama dönemi için alışılmadık bir olay hakkında rapor* ve *Toplama dönemi için nesne değişikliği raporu*. Bu raporlar, toplama döneminin başlangıcı ve bitişi ile toplanmış olayların sayısı hakkında bilgiler içerir.

Kaspersky Security Center Konsolundan bilgisayarın durumu

Dosya Bütünlük İzleyicisi bileşeninden önem seviyesi *Kritik* veya *Uyarı* olan olaylar alındığında, Kaspersky Security Center bilgisayarın durumunu *Kritik* veya *Uyarı* olarak değiştirir.

Yönetilen bir uygulamadan bilgisayar durumu alma (**Uygulama koşuluna göre tanımlanan cihaz durumu**), Kaspersky Security Center'da bir cihaza *Kritik* veya *Uyarı* durumu atamak için karşılanması gereken koşullar listesinde etkinleştirilmelidir. Bir cihaza durum atama koşulları yönetim grubunun özellikler penceresinde yapılandırılır.

Bilgisayar durumu ve durum değişikliklerinin tüm nedenleri, yönetim grubunun aygıt listesinde görüntülenir. Bilgisayar durumları hakkında daha ayrıntılı bilgi için Kaspersky Security Center Yardım içeriğine başvurun.

Kaspersky Security Center Konsolundaki raporlar

Kaspersky Security Center iki tür rapor sunar:

- Dosya Bütünlüğü İzleme / Sistem Bütünlüğü İzleme kurallarının en sık tetiklendiği ilk 10 cihaz.
- Cihazlarda en sık tetiklenen Dosya Bütünlüğü İzleme / Sistem Bütünlüğü İzleme'nin ilk 10 kuralı.

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.

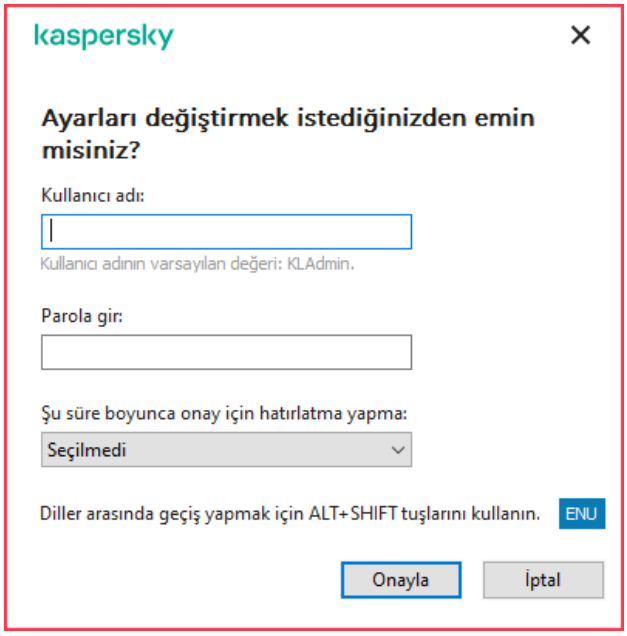
  Bu yöntem, günlük işlemler için uygundur. Parola korumalı bir eylemi gerçekleştirmek için gerekli izne sahip etki alanı hesabınızın bilgilerini girmeniz gerekir. Bu durumda bilgisayar o etki alanında olmalıdır. Bilgisayar etki alanında değilse, KLAdmin hesabını kullanabilirsiniz.

- 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.

Kullanıcı, parola korumalı bir eylem gerçekleştirmeye çalıştığında Kaspersky Endpoint Security, kullanıcıdan kullanıcı adı ve parolasını veya geçici parolayı girmesini ister (aşağıdaki resme 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 parola

Kaspersky Endpoint Security'ye erişmek için etki alanı hesabınızın 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.

- **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.

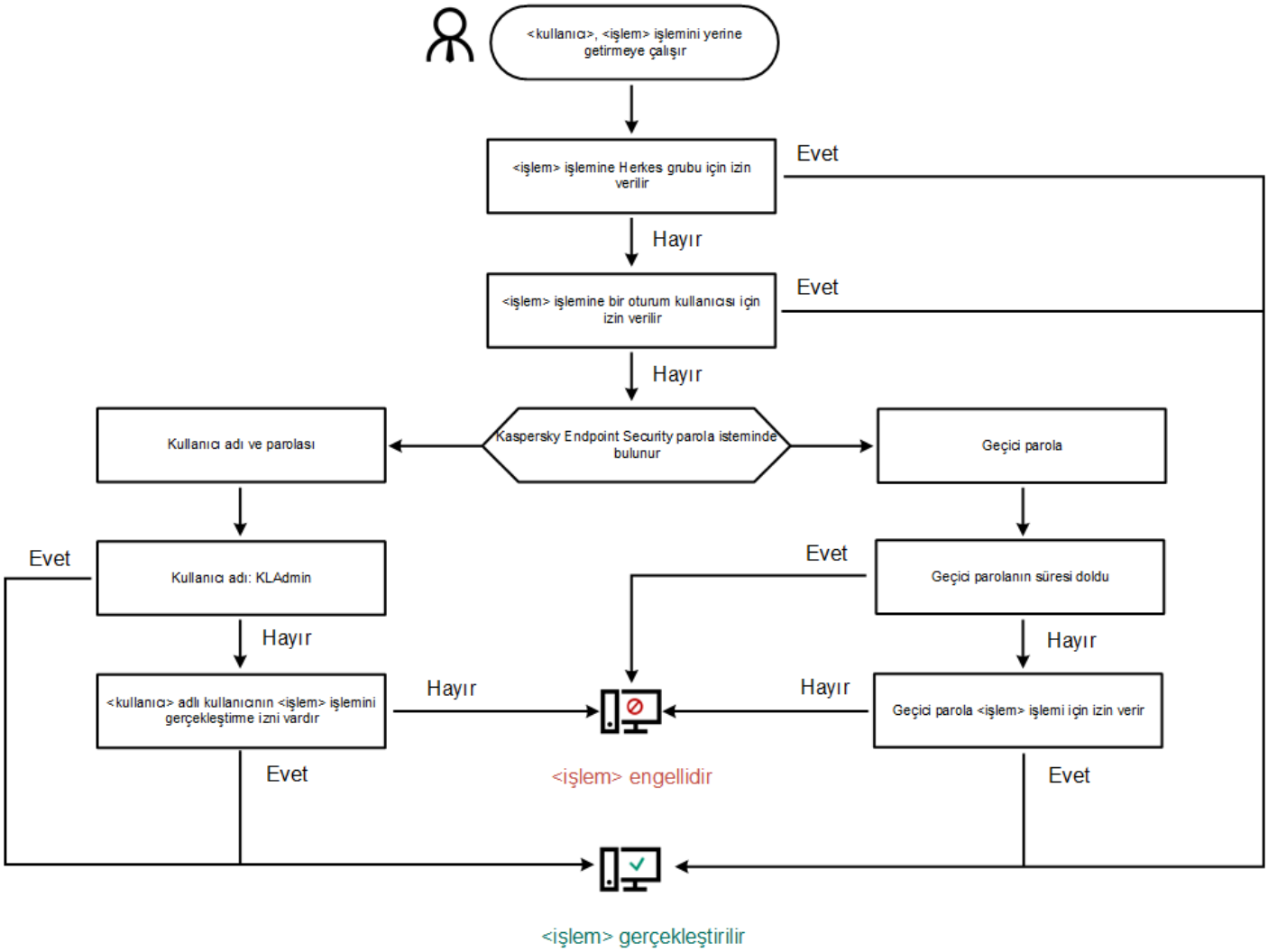
- **Oturum kullanıcısı**. Windows oturumunu başlatan kullanıcının hesabı. Bir parola istendiğinde (**Parolayı bu oturum için kaydet** onay kutusu) başka bir oturum kullanıcısına geçiş yapabilirsiniz. Bu durumda Kaspersky Endpoint Security Windows oturumunu başlatan kullanıcının yerine hesap bilgileri 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.

Parola korumasının çalışma algoritması

Kaspersky Endpoint Security, parola korumalı bir eyleme izin verilip verilmeyeceğini aşağıdaki algoritmaya (aşağıdaki şekle bakın) göre belirler.



Parola korumasının çalışma algoritması

Parola korumasını etkinleştir

Parola koruması, kullanıcıların Kaspersky Endpoint Security'ye erişimlerini kendilerine verilen izinler kapsamında (uygulamadan çıkma izni gibi) kısıtlamanızı sağlar.

Parola korumasını etkinleştirmek için:

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

Ayrı ayrı kullanıcılara veya gruplara Kaspersky Endpoint Security erişimi 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.

Ayrı ayrı kullanıcılara veya gruplara izinler vermek için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.
2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Arabirim** öğesini seçin.
3. Hesap tablosunda **Ekle**'ye tıklayın.
4. Açılan pencerede **Kullanıcı veya grup seçin** düğmesine tıklayın.

   Standart Kullanıcıları veya Grupları Seçin iletişim kutusu açılır.

5. Active Directory'de bir kullanıcı veya grup seçin ve seçiminizi onaylayın.
6. **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.

7. 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** 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. **Geçici parola** bloğunda **Ayarlar** düğmesine tıklayın.
10. **Geçici parola oluştur** penceresi açılır.
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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
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. **Parola koruması** bloğunda **Geçici parola** düğmesine tıklayın.

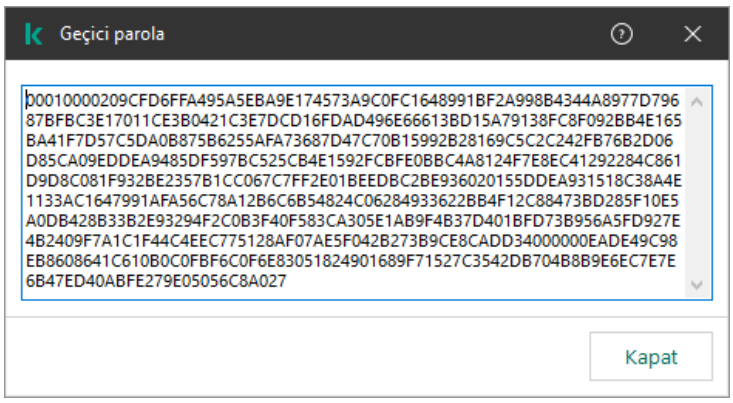
8. **Sona erme tarihi** alanında geçici parolanın süresinin dolacağı sona erme tarihini belirtin.

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

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.

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'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** → **Arabirim** öğesini seçin.
5. **Parola koruması** bloğunda **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, **Parola korumasını etkinleştir** kutucuğunu işaretleyin.
7. Değişikliklerinizi kaydedin.
8. **Parola korumasını etkinleştir** onay kutusunu tekrar işaretleyin.
9. **Tamam**'a tıklayın.
   Yönetici parolası penceresi açılır.
10. KLAdmin hesabının yeni parolasını belirtin ve onaylayın.
11. Değişikliklerinizi kaydedin.

KLAdmin hesabı parolasını Web Console ve Cloud Console'da sıfırlama

1. Web Console'un ana penceresinde **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows**'a tıklayın.
   Bu, yerel uygulama ayarlarını açar.
5. **Uygulama ayarları** sekmesini seçin.
6. **Genel Ayarlar** → **Arabirim** 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.

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.

Tarama istisnası oluşturma

Tarama istisnası, Kaspersky Endpoint Security'nin belirli bir nesnede virüsleri ve diğer tehditleri taramaması için karşılanması gereken koşullar kümesidir.

Tarama istisnaları, saldırganlar tarafından bilgisayar veya kullanıcı verilerine zarar vermek amacıyla kullanılabilecek meşru yazılımın güvenli bir şekilde kullanılabilmesine imkan tanır. Kötü amaçlı işlevler içermese bile bu uygulamalar 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 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* görevleri.

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** öğesini seçin.
5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, **Tarama istisnaları** sekmesini seçin.
   Bu, istisnaların listesini içeren bir pencere açar.

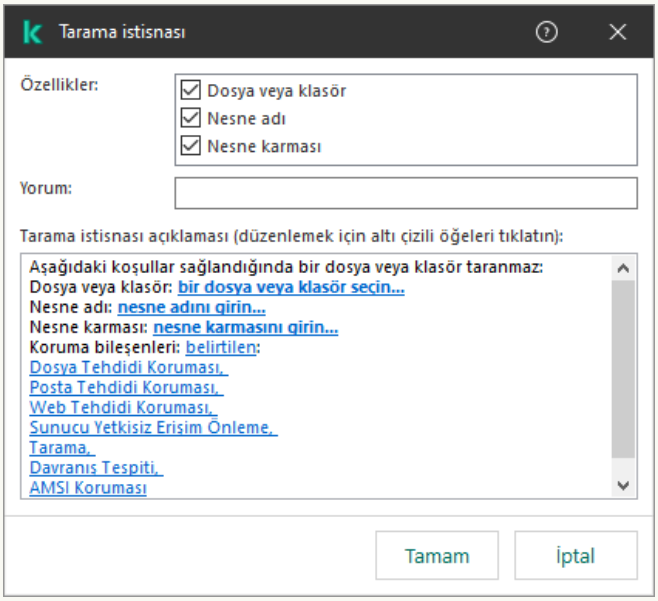
7. Şirketteki tüm bilgisayarlar için birleştirilmiş bir istisnalar listesi oluşturmak isterseniz **Devralırken değerleri birleştir** onay kutusunu işaretleyin. Ana ve alt ilkelerdeki istisnaların listesi birleştirilecektir. Devralırken değerleri birleştirme etkinleştirilmişse listeler birleştirilecektir. Ana ilkedeki istisnalar, alt ilkelerde salt okunur olarak görüntülenir. Ana ilkenin istisnalarının değiştirilmesi veya silinmesi mümkün değildir.

8. 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.

9. **Ekle**'ye tıklayın.

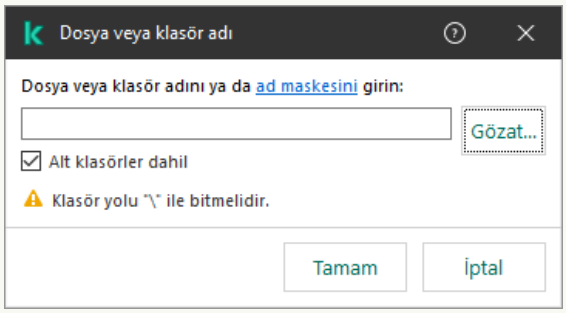
10. Bir dosya veya klasörü tarama dışında tutmak için:



İstisna ayarları

a. **Özellikler** bloğunda **Dosya veya klasör** onay kutusunu işaretleyin.

b. **Dosya veya klasör adı** penceresinde **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğunda **dosya veya klasör seçin** bağlantısına 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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

Kaspersky Endpoint Security ortam değişkenlerini destekler

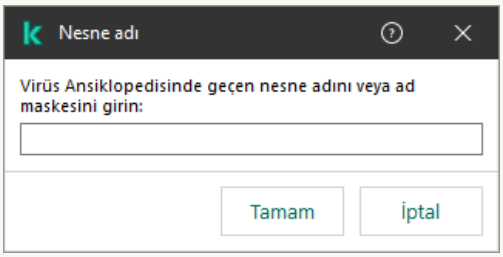
> Kaspersky Endpoint Security, Kaspersky Security Center konsolunda bir istisnalar listesi listesi oluştururken `%userprofile%` ortam değişkenini desteklemez. Girişi tüm kullanıcı hesaplarına uygulamak için `*` karakterini kullanabilirsiniz (örneğin, `C:\Users\*\Documents\File.exe`). Yeni bir ortam değişkeni eklediğinizde, uygulamayı yeniden başlatmanız gerekir.

b. Değişikliklerinizi kaydedin.

11. Belirli bir ada sahip nesneleri tarama dışında tutmak için:

a. **Özellikler** bloğunda **Nesne adı** onay kutusunu işaretleyin.

b. **Nesne adı** penceresinde **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğunda **nesne adını girin** bağlantısına tıklayın.



Nesne seç

a. Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Eposta-Solucan`, `Rootkit` veya `UzakYönetici`).

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.

12. Tek bir dosyayı taramaların dışında tutmak istiyorsanız:

a. **Özellikler** bloğunda **Nesne karması** onay kutusunu işaretleyin.

b. **Nesne karması** penceresini açmak için **nesne karması gir** bağlantısına 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.

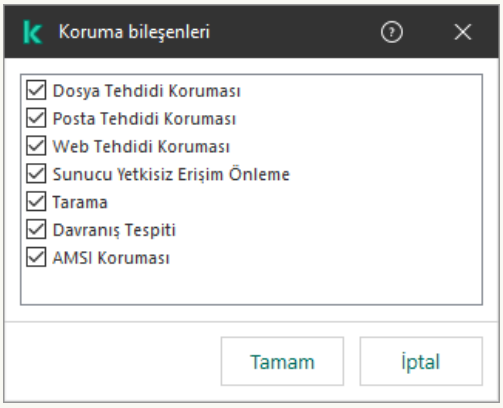
b. Değişikliklerinizi kaydedin.

13. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

14. Tarama istisnasını kullanması gereken Kaspersky Endpoint Security bileşenlerini belirtin:

a. **Bileşenleri seçin** bağlantısını etkinleştirmek için **Tarama istisnası açıklaması (düzenlemek için altı çizili öğeleri tıklatın)** bloğunda **herhangi** bağlantısına tıklayın.

b. **Bileşenleri seçin** bağlantısına tıklayarak **Koruma bileşenleri** penceresini açın.



Koruma bileşenlerini devre seçme

a. Tarama istisnasının uygulanması gereken bileşenlerin karşısındaki onay kutularını işaretleyin.

b. Değişikliklerinizi kaydedin.

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.

15. Onay kutusunu kullanarak istisnayı istediğiniz zaman durdurabilirsiniz.

16. Değişikliklerinizi kaydedin.

[Web Console'da ve Cloud Console'da bir tarama istisnası nasıl oluşturulur](#)

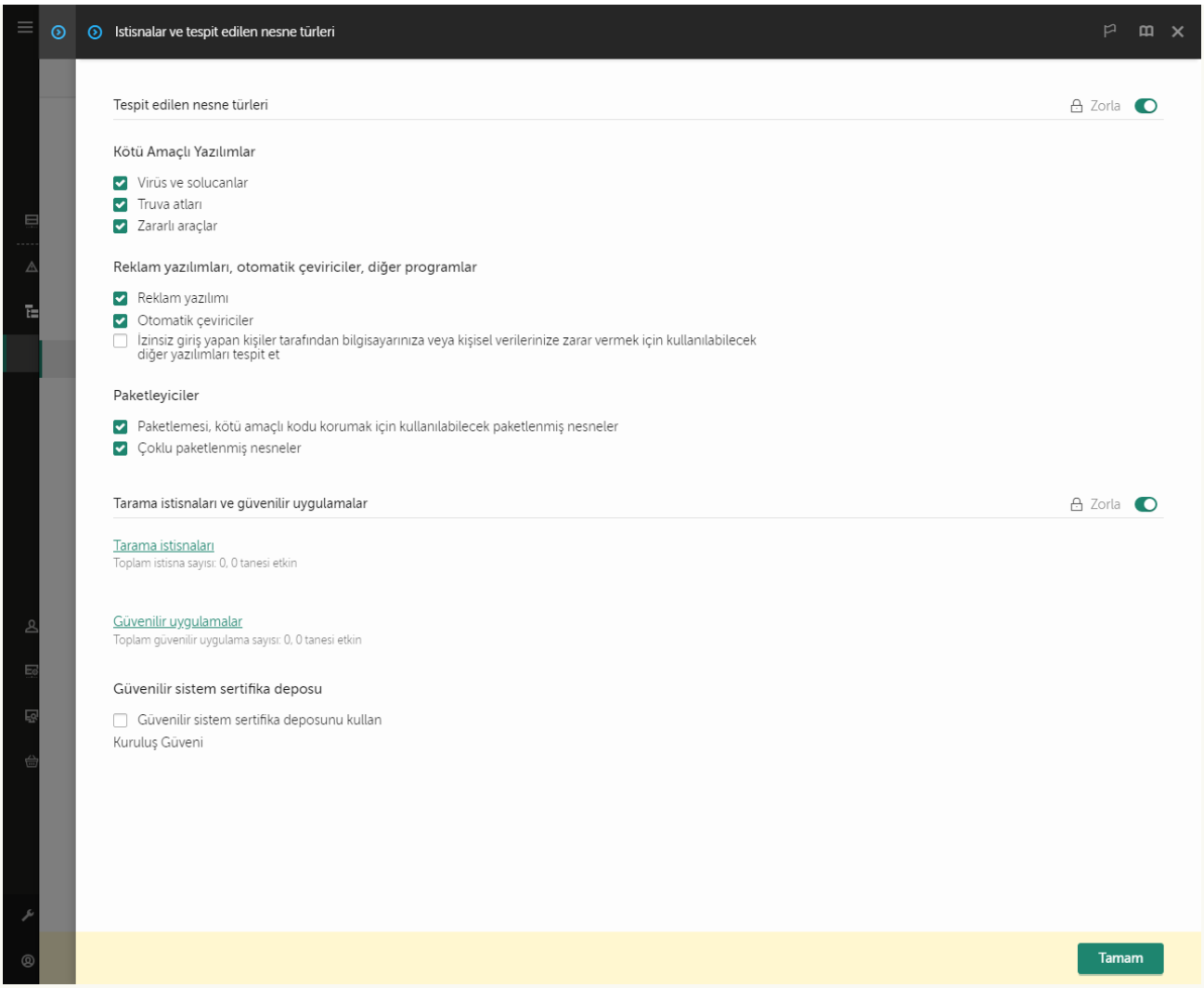
1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel ayarlar** → **İstisnalar ve tespit edilen nesne türleri** bölümüne gidin.



İstisna ayarları

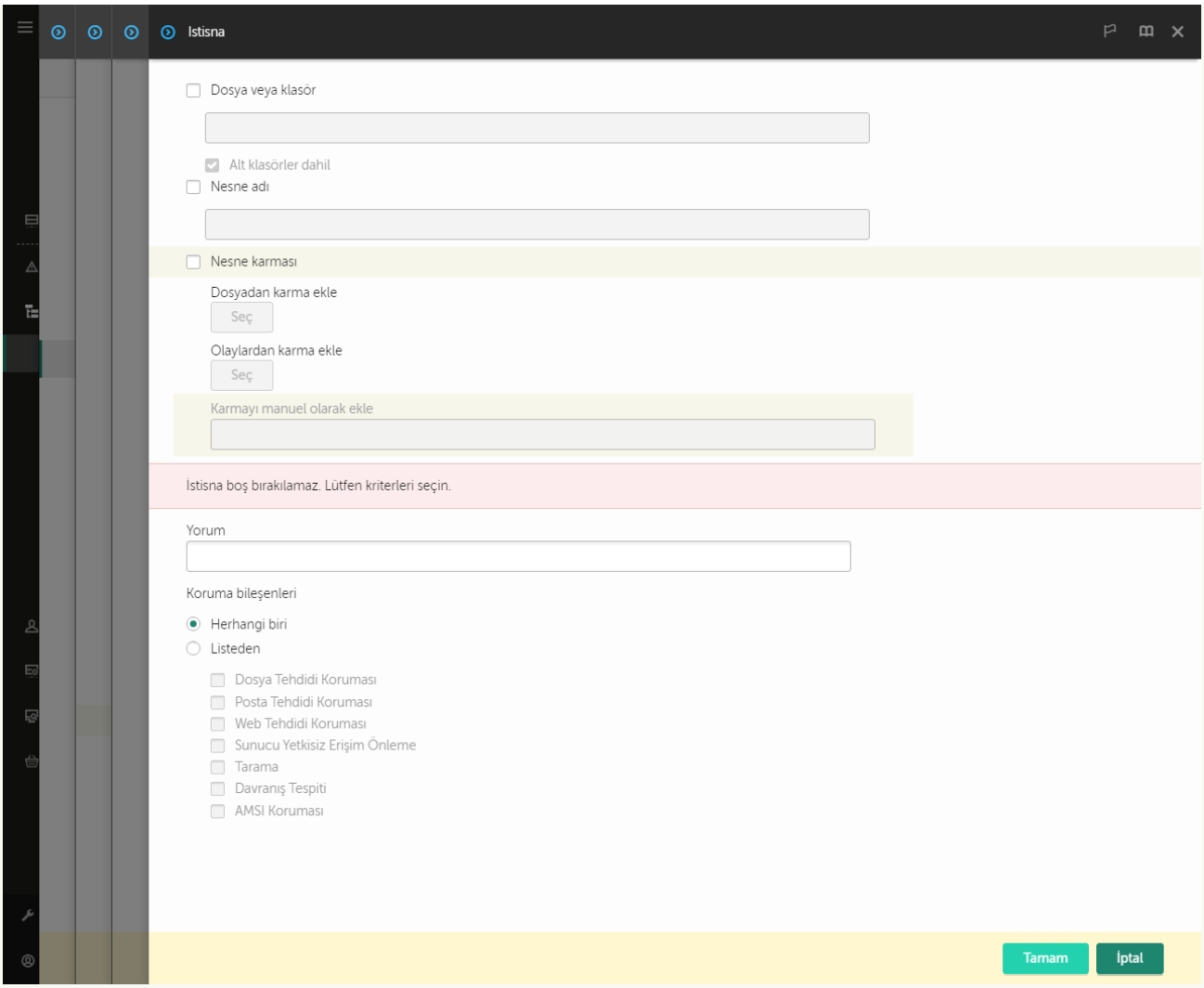
5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Tarama istisnaları** düğmesine tıklayın.

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.

8. **Ekle** düğmesine tıklayın.



İstisna ayarları

9. İstisnayı nasıl eklemek istediğinizi seçin: **Dosya veya klasör**, **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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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. Eğer taramalardan nesnenin belirli türünü dışlamak istiyorsanız, **Nesne adı** alanında Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Eposta-Solucan`, `Rootkit` veya `UzakYönetici`).

    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.

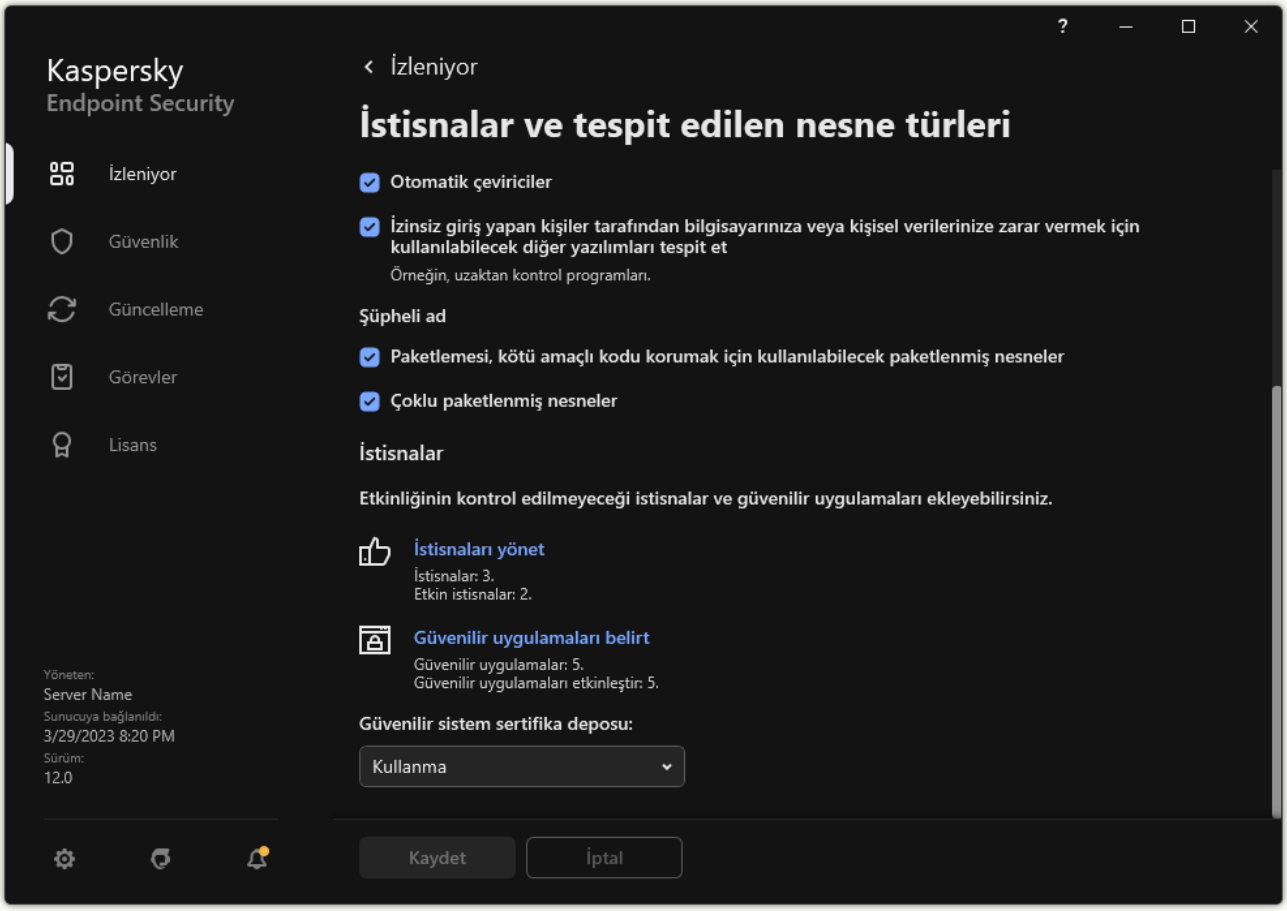
12. Tek bir dosyayı taramaların dışında tutmak istiyorsanız, **Nesne karması** alanına dosya karma değerini girin.

Dosya değiştirilirse, dosya karması da değiştirilecektir. Böyle bir durumda, değiştirilen dosya istisnalara eklenmeyecektir.

13. **Koruma bileşenleri** bloğunda, tarama istisnasının uygulanmasını istediğiniz bileşenleri seçin.
14. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.
15. İstediğiniz zaman bir istisnayı durdurmak için geçiş düğmesini kullanabilirsiniz.
16. 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.



İstisna ayarları

4. **Ekle**'ye tıklayın.
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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

6. Eğer taramalardan nesnenin belirli türünü dışlamak istiyorsanız, **Nesne** alanında Kaspersky Ansiklopedisinin sınıflandırmasına göre nesnenin adını girin (örneğin `Eposta-Solucan`, `Rootkit` veya `UzakYönetici`).

   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, **Dosya karması** alanına dosya karma değerini girin.

   Dosya değiştirilirse, dosya karması da değiştirilecektir. Böyle bir durumda, değiştirilen dosya istisnalara eklenmeyecektir.

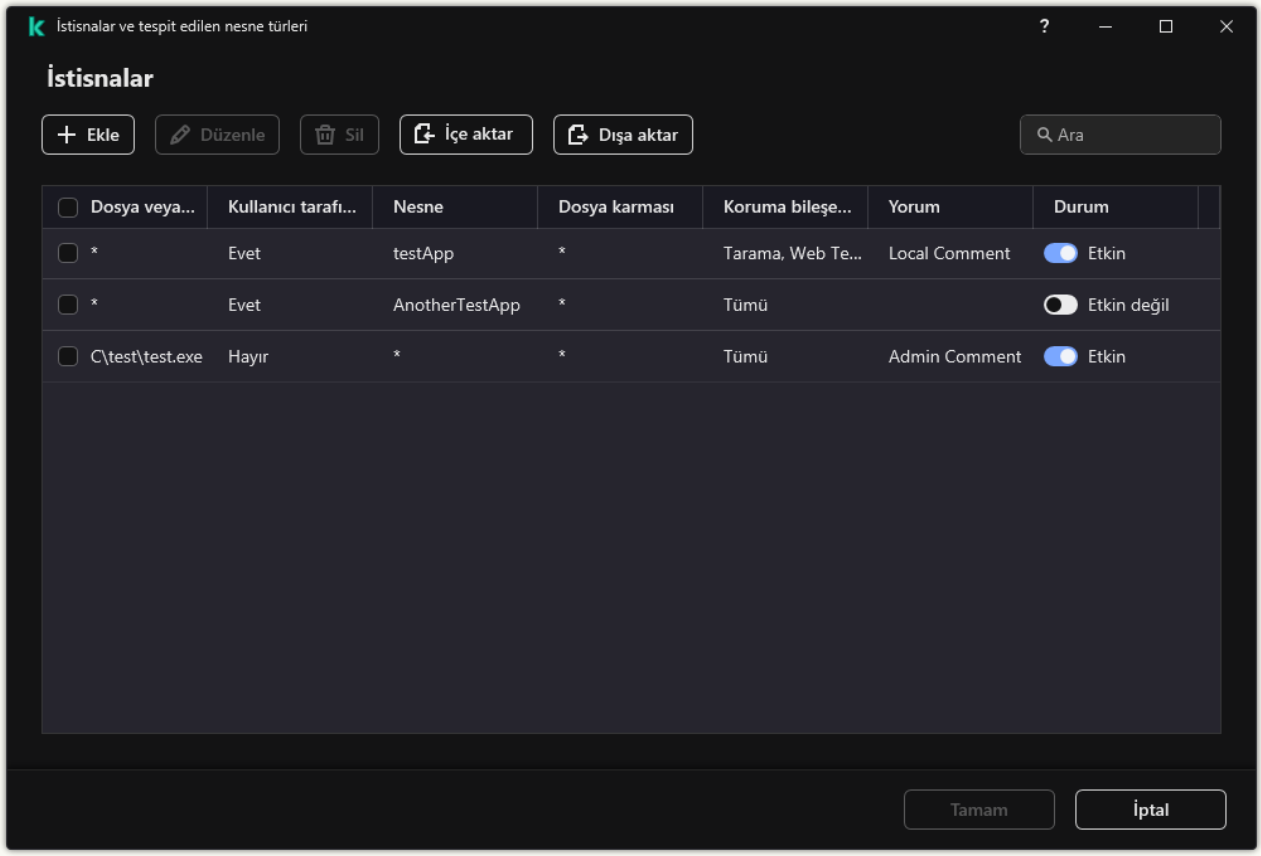
8. **Koruma bileşenleri** bloğunda, tarama istisnasının uygulanmasını istediğiniz bileşenleri seçin.

9. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

10. İstisna için **Etkin** durumu seçin.

    Geçişi kullanarak istisnayı istediğiniz zaman durdurabilirsiniz.

11. Değişikliklerinizi kaydedin.



İstisnalar listesi

Yol maskesi örnekleri:

Herhangi bir klasörde bulunan dosya yolları:

- "`*.exe`" maskesi, exe uzantısı olan tüm dosya yollarını içerir.

- `Örnek*` maskesi, ÖRNEK adlı tüm dosya yollarını içerir.

Belirtilen bir klasörde bulunan dosya yolları:

- `C:\dir\*.*` maskesi, C:\dir\ klasöründe bulunan tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
- `C:\dir\` maskesi, C:\dir\ klasöründe bulunan tüm dosya yollarını, 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 edilebilir nesne türlerini seçme

Tespit edilebilir nesne türlerini seçmek için:

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:
   - **Virüs ve solucanlar**;

     Alt kategori: virüs ve solucanlar (Viruses_and_Worms)

     Tehdit 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. *Üzerine yazan* virüsler, kodlarını virüslü dosyanın kodu üzerine yazar, böylece dosyanın içeriği silinir. Virüslü dosya çalışmaz ve geri yüklenemez. *Asalak* virüsler dosyaları tamamen veya kısmen işlevsel bırakarak değiştirir. *Eşlik eden* virüsler dosyaları değiştirmez, bunun yerine kopyalarını oluşturur. Virüslü bir dosya açıldığında, dosyanın (aslında bir virüs olan) kopyası başlatılır. Şu virüs türlerine de rastlanmaktadır: *bağlantı virüsleri*, *OBJ virüsleri*, *LIB virüsleri*, *kaynak kod* virüsleri ve diğerleri.

Solucan

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	Name	Açıklama
E-posta-Solucanı	E-posta-Solucanı	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 Solucanı	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 Solucanı	İnternet sohbeti solucanları	Gerçek zamanlı olarak İnternet üzerinden diğer insanlarla iletişim kurmaya izin veren hizmet sistemlerinden İnternet Bağlantılı Sohbetler 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-Solucanı	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.
Solucan	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

Tehdit 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	Name	Açıklama
Truva atı-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.
Arka kapı	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.
Truva atı	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.
Truva atı-Fidye	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.
Truva atı-Tıklayıcı	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.

Truva atı-İndirici	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.
Truva atı-Bırakıcı	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.
Truva atı-Uyarıcı	Truva atı uyarıcılar	Bir saldırgana virüslü bilgisayara erişilebilir olduğu bildirilir, saldırgana bilgisayar hakkında bilgiler gönderir: IP adresi, açık bağlantı noktası 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.
Truva atı-Proxy	Truva atı proxy'leri	Saldırganın, kullanıcının bilgisayarını kullanarak isimsiz bir şekilde İnternet sayfalarına erişmesine izin verir; genellikle spam göndermek için kullanılır.
Truva atı-Şifre aracısı	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.
Truva atı-Casus	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.
Truva atı-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.
Truva atı-Anında Mesajlaşma	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.

Truva atı-SMS	SMS mesajları biçimindeki Truva atları	Cep telefonlarına virüs bulaştırır, özel tarifeli telefon numaralarına SMS mesajları gönderir.
Truva atı-OyunHırsızı	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.
Truva atı-Bankacı	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.
Truva atı-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	Name	Açıklama
Oluşturucu	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).
Açık bırakıcı	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.
Dosya şifreleyicisi	Şifreleyiciler	Anti virüs uygulamasından gizlemek için diğer zararlı uygulamaları şifrelerler.
Bombacı	"Kirleten" ağlar	Ağ kanalları üzerinden çok sayıda mesaj gönderir. Bu tür araçlar, İnternet

	için programlar	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 (E-posta-Bombacısı, IM-Bombacısı ve SMS-Bombacısı).
Saldırı aracı	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.
Asılsız uyarı	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.
Aldatıcı	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.
E-posta bombacısı	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-Bombacısı	Anlık ileti uygulamalarının trafiğini "kirleten" programlar	Anlık ileti uygulamalarının kullanıcılarını mesajlarla bombalar. Büyük miktardaki mesajlar, kullanıcının faydalı gelen mesajları görmesine engel olur.
SMS-Bombacısı	SMS mesajlarıyla trafiği "kirleten" programlar	Cep telefonlarına çok sayıda SMS mesajları gönderir.

- Reklam yazılımı;

  Alt kategori: reklam yazılımı (Reklam Yazılımı);

  Tehdit 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: suçlular tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım.

  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	Name	Açıklama
Client-IRC	İnternet sohbeti istemcileri	Kullanıcılar bu programları İnternet Bağlantılı Sohbetlerde insanlarla konuşmak için yükler. Saldırganlar bunları zararlı yazılımları yaymak için kullanır.
Çeviriciler	Otomatik çeviriciler	Gizli modda bir modem üzerinden telefon bağlantıları kurabilir.
İndirici	İndirilecek programlar	İnternet sayfalarından programları gizli modda indirir.
Monitör	İzleme programları	Bunlar, yüklendikleri bilgisayarla ilgili etkinlik izlemeye olanak tanır (hangi uygulamaların etkin olduğunu ve diğer bilgisayarlara yüklü uygulamalarla nasıl veri alışverişi yapıldığını görürler).
PSWAracı	Parola geri yükleyiciler	Unutulan parolaların görüntülenmesine ve yeniden yüklenmesine olanak tanır. Saldırganlar, aynı amaçla bunları kullanıcının bilgisayarına gizlice yerleştirir.
UzakYönetici	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 Arkakapı türü Truva atlarından farklıdır. Truva atları işletim sistemlerine bağımsız olarak girme ve kendilerini yükleme kabiliyetine sahiptirler: yasal programlar bunu gerçekleştiremez.
Sunucu FTP	FTP sunucuları	FTP sunucuları olarak işlev gösterir. Saldırganlar, FTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Sunucu Proxy	Proxy sunucular	Proxy sunucuları olarak işlev gösterir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
Sunucu Telnet	Telnet sunucuları	Telnet sunucuları olarak işlev gösterir. Saldırganlar, Telnet aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Sunucu İnternet	İnternet sunucuları	İnternet sunucuları olarak işlev gösterir. Saldırganlar, HTTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
RiskAracı	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.
NetAracı	Ağ araçları	Kullanıcıya ağdaki başka bilgisayarla çalışırken ek seçenekler sunar. Bu araçlar, yeniden başlatmaya, açık bağlantı noktalarını 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.
İnternet Araç çubuğu	İnternet Araç çubukları	Arama motorlarını kullanmak için araç çubuklarını diğer uygulamaların arabirimlerine ekler.
Dolandırıcı Aracı	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 diğer yazılımları tespit et;

Alt kategori: suçlular tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım.

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	Name	Açıklama
Client-IRC	İnternet sohbeti istemcileri	Kullanıcılar bu programları İnternet Bağlantılı Sohbetlerde insanlarla konuşmak için yükler. Saldırganlar bunları zararlı yazılımları yaymak için kullanır.
Çeviriciler	Otomatik çeviriciler	Gizli modda bir modem üzerinden telefon bağlantıları kurabilir.
İndirici	İndirilecek programlar	İnternet sayfalarından programları gizli modda indirir.
Monitör	İzleme programları	Bunlar, yüklendikleri bilgisayarla ilgili etkinlik izlemeye olanak tanır (hangi uygulamaların etkin olduğunu ve diğer bilgisayarlara yüklü uygulamalarla nasıl veri alışverişi yapıldığını görürler).
PSWAracı	Parola geri yükleyiciler	Unutulan parolaların görüntülenmesine ve yeniden yüklenmesine olanak tanır. Saldırganlar, aynı amaçla bunları kullanıcının bilgisayarına gizlice yerleştirir.
UzakYönetici	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 Arkakapı türü Truva atlarından farklıdır. Truva atları işletim sistemlerine bağımsız olarak girme ve kendilerini yükleme kabiliyetine sahiptirler: yasal programlar bunu gerçekleştiremez.
Sunucu FTP	FTP sunucuları	FTP sunucuları olarak işlev gösterir. Saldırganlar, FTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Sunucu Proxy	Proxy sunucular	Proxy sunucuları olarak işlev gösterir. Saldırganlar, kullanıcının adı altında spam göndermek için kullanıcının bilgisayarına yerleştirir.
Sunucu Telnet	Telnet sunucuları	Telnet sunucuları olarak işlev gösterir. Saldırganlar, Telnet aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
Sunucu İnternet	İnternet sunucuları	İnternet sunucuları olarak işlev gösterir. Saldırganlar, HTTP aracılığıyla uzak erişimi açmak için kullanıcının bilgisayarına yerleştirir.
RiskAracı	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.
NetAracı	Ağ araçları	Kullanıcıya ağdaki başka bilgisayarla çalışırken ek seçenekler sunar. Bu araçlar, yeniden başlatmaya, açık bağlantı noktalarını 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.
İnternet Araç çubuğu	İnternet Araç çubukları	Arama motorlarını kullanmak için araç çubuklarını diğer uygulamaların arabirimlerine ekler.
Dolandırıcı Aracı	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;

  Kaspersky Endpoint Security, sıkıştırılmış nesneleri ve SFX (kendi başına açılan) arşivlerdeki paket açıcı modülünü tarar.

  Tehlikeli programları anti-virüs uygulamalarından gizlemek için saldırganlar özel paketleyicileri kullanarak bunları arşivler veya çoklu sıkıştırılmış dosyalar oluşturur.

  Kaspersky virüs analistleri bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

  Kaspersky Endpoint Security bir dosyada böyle bir paketleyici tespit ederse dosya büyük olasılıkla bir zararlı uygulama veya bilgisayarınıza ya da kişisel verilerinize zarar vermek için suçlular tarafından kullanılan bir uygulama içeriyordur.

  Kaspersky Endpoint Security aşağıdaki program türlerini eler:

  - *Zarar verebilecek paketlenmiş dosyalar* – virüsler, solucanlar ve Trojanlar gibi zararlı yazılımların paketlenmesi için kullanılır.
  - *Çoklu paketlenmiş dosyalar* (orta tehdit düzeyi) – nesne, bir veya daha fazla paketleyici tarafından üç kez paketlenmiştir.

- Çoklu paketlenmiş nesneler.

  Kaspersky Endpoint Security, sıkıştırılmış nesneleri ve SFX (kendi başına açılan) arşivlerdeki paket açıcı modülünü tarar.

  Tehlikeli programları anti-virüs uygulamalarından gizlemek için saldırganlar özel paketleyicileri kullanarak bunları arşivler veya çoklu sıkıştırılmış dosyalar oluşturur.

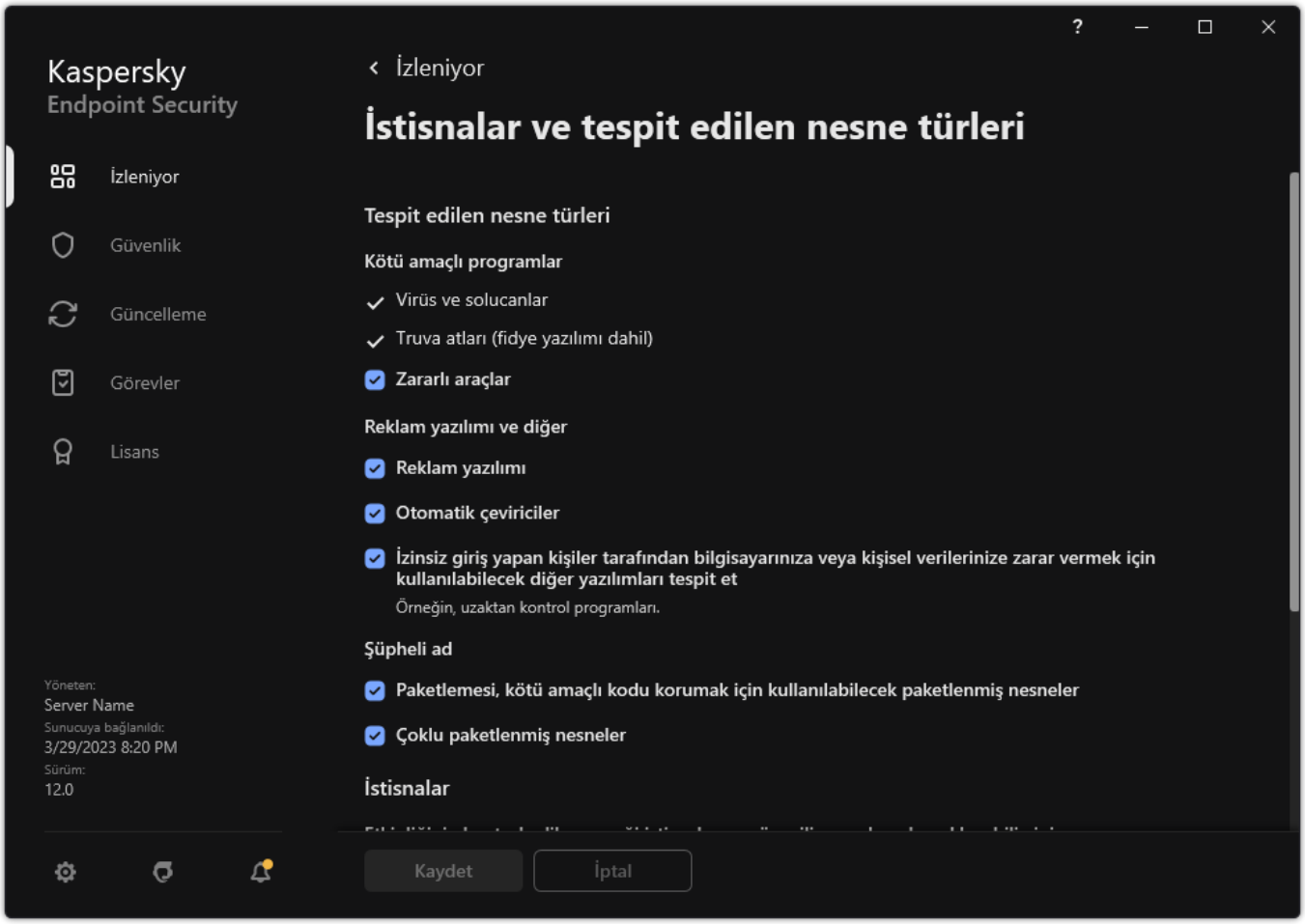
  Kaspersky virüs analistleri bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

  Kaspersky Endpoint Security bir dosyada böyle bir paketleyici tespit ederse dosya büyük olasılıkla bir zararlı uygulama veya bilgisayarınıza ya da kişisel verilerinize zarar vermek için suçlular tarafından kullanılan bir uygulama içeriyordur.

  Kaspersky Endpoint Security aşağıdaki program türlerini eler:

  - *Zarar verebilecek paketlenmiş dosyalar* – virüsler, solucanlar ve Trojanlar gibi zararlı yazılımların paketlenmesi için kullanılır.
  - *Çoklu paketlenmiş dosyalar* (orta tehdit düzeyi) – nesne, bir veya daha fazla paketleyici tarafından üç kez paketlenmiştir.

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

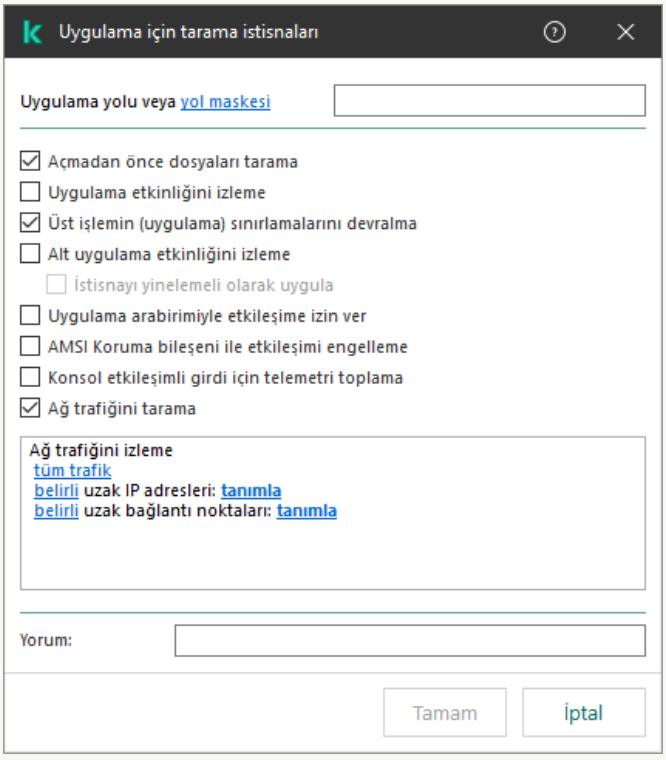
1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde **Genel Ayarlar** → **İstisnalar** öğesini seçin.
5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, **Güvenilir uygulamalar** sekmesini seçin.

   Bu, güvenilir uygulamaların listesini içeren bir pencere açar.
7. 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.
8. 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.
9. **Ekle**'ye tıklayın.
10. Açılan pencerede, güvenilir uygulamanın yürütülebilir dosyasının yolunu girin (aşağıdaki resme bakın).

    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.

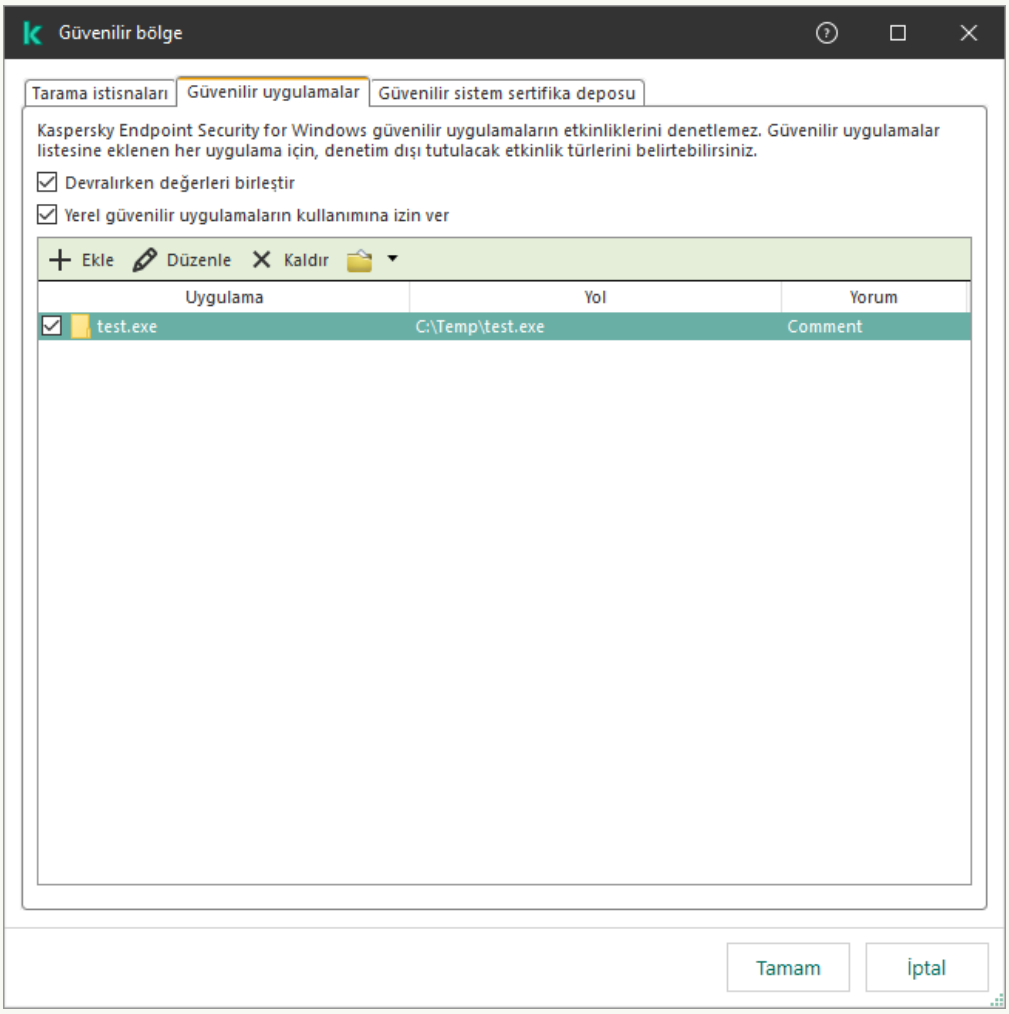


Güvenilir uygulama ayarları

11. Güvenilir uygulama için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).

12. Herhangi bir zamanda bir uygulamayı güvenilen bölgeden çıkarmak için onay kutusunu kullanabilirsiniz (aşağıdaki resme bakın).

13. Değişikliklerinizi kaydedin.



Güvenilir uygulamaların listesi

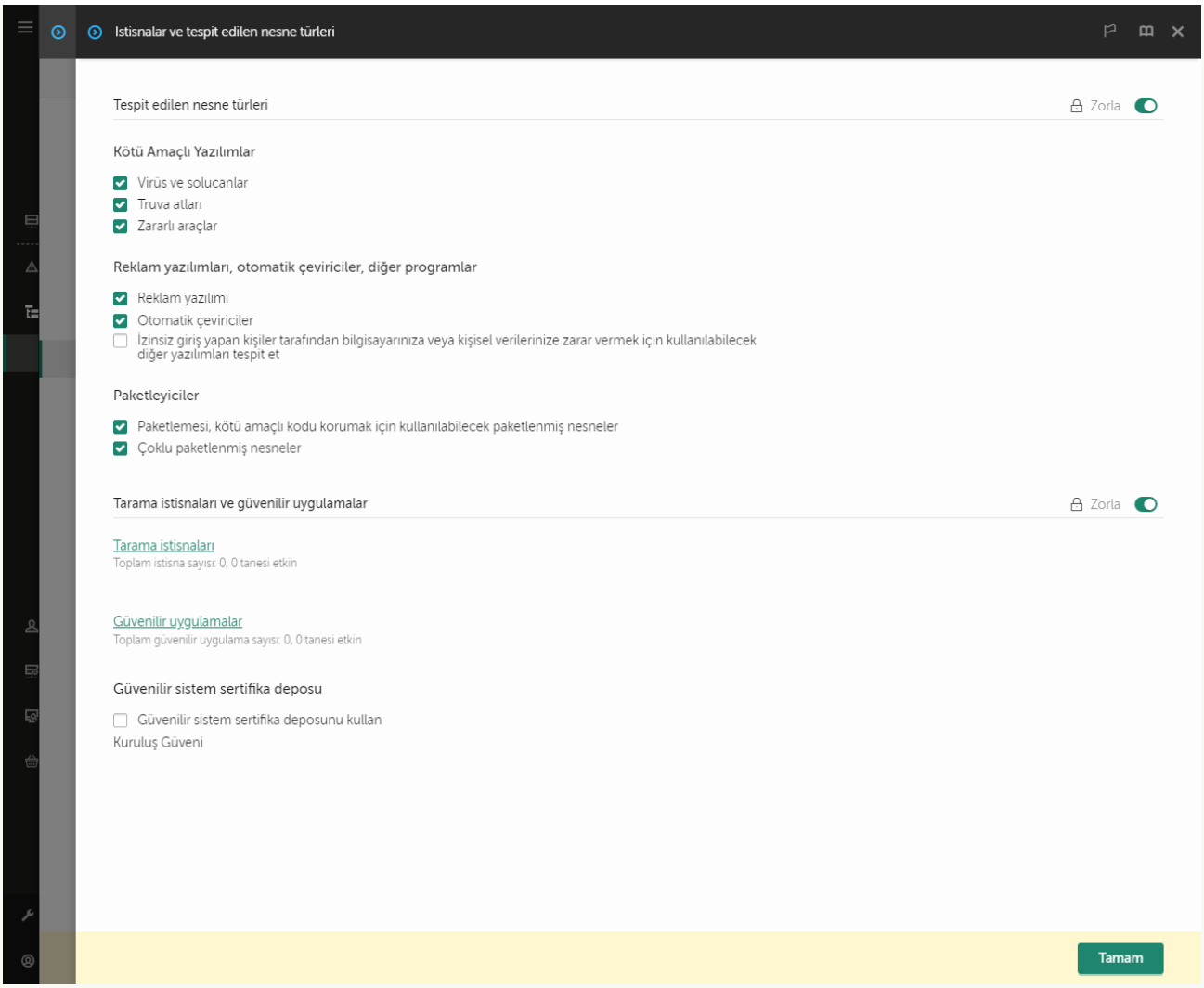
Web Console'da ve Cloud Console'da bir uygulama güvenilir listeye nasıl eklenir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.

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

3. **Uygulama ayarları** sekmesini seçin.

4. **Genel ayarlar** → **İstisnalar ve tespit edilen nesne türleri** bölümüne gidin.



İstisna ayarları

5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Güvenilir uygulamalar** 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.

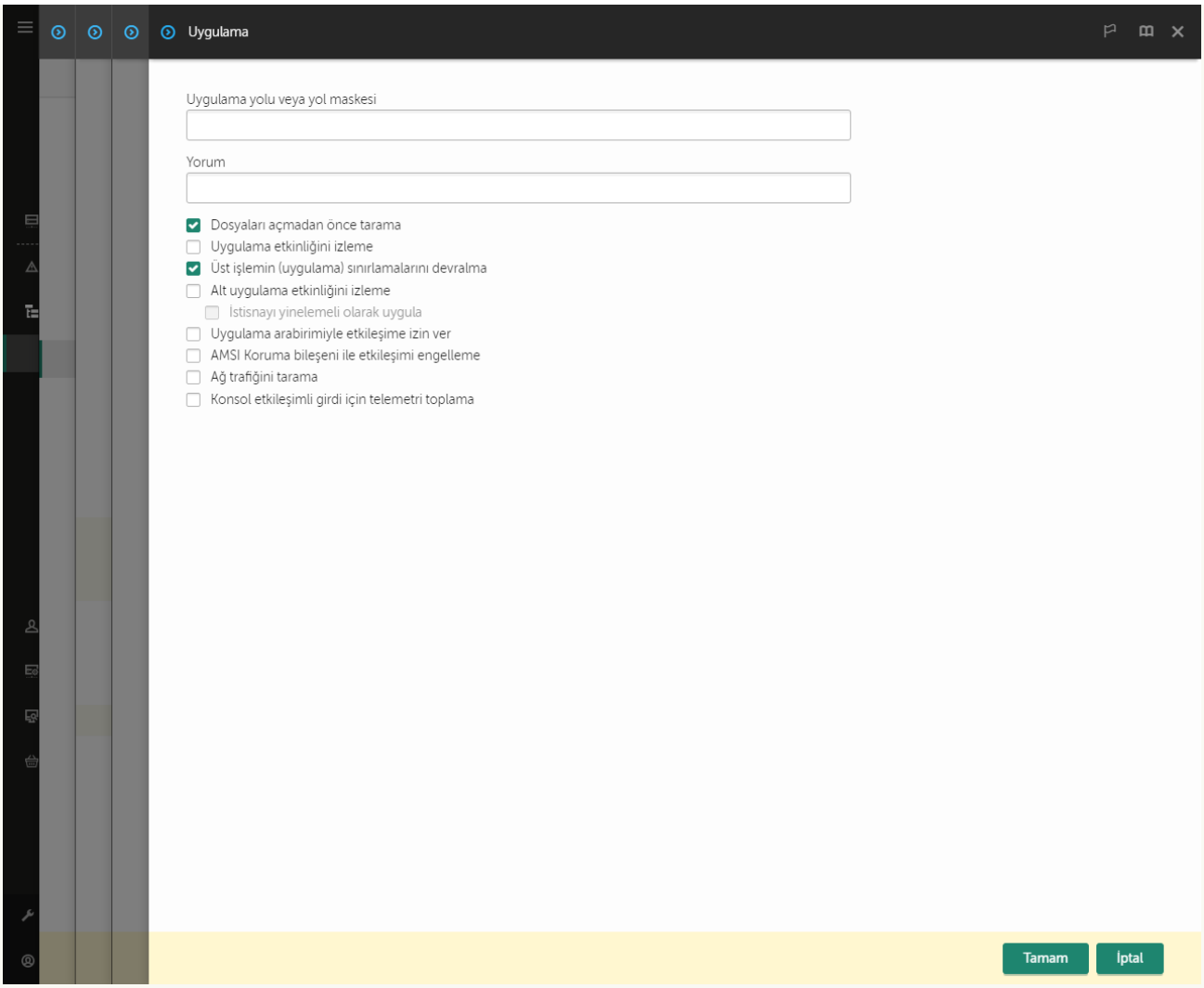
   Onay kutusu işaretli değilse, kullanıcı yalnızca ilkede oluşturulan güvenilir uygulamaların genel listesine erişebilir.

8. **Ekle** düğmesine tıklayın.

9. Açılan pencerede, güvenilir uygulamanın yürütülebilir dosyasının yolunu girin (aşağıdaki resme bakın).

   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.

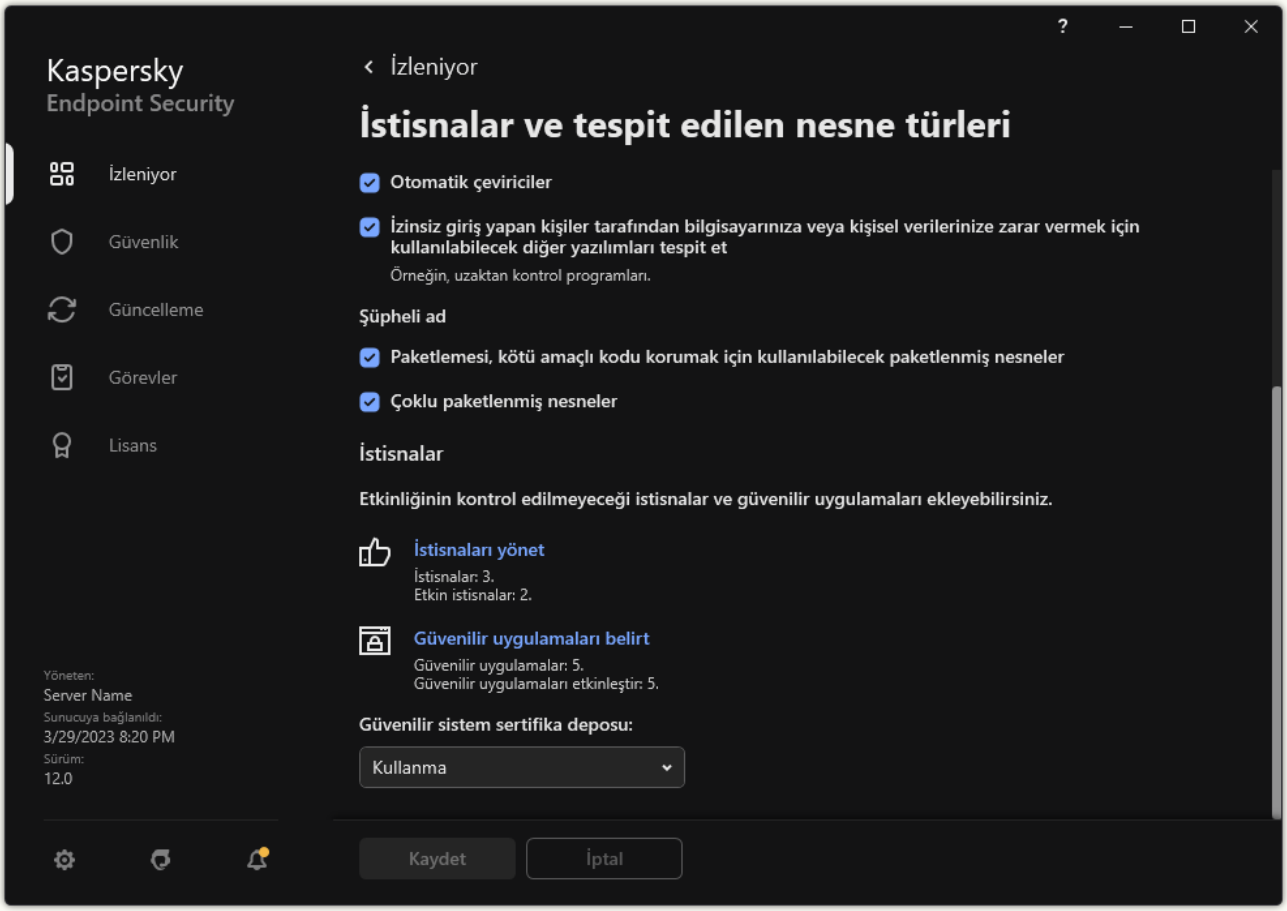


Güvenilir uygulama ayarları

10. Güvenilir uygulama için gelişmiş ayarları yapılandırın (aşağıdaki tabloya bakın).
11. Herhangi bir zamanda bir uygulamayı güvenilen bölgeden çıkarmak için onay kutusunu kullanabilirsiniz (aşağıdaki resme bakın).
12. 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.



İstisna ayarları

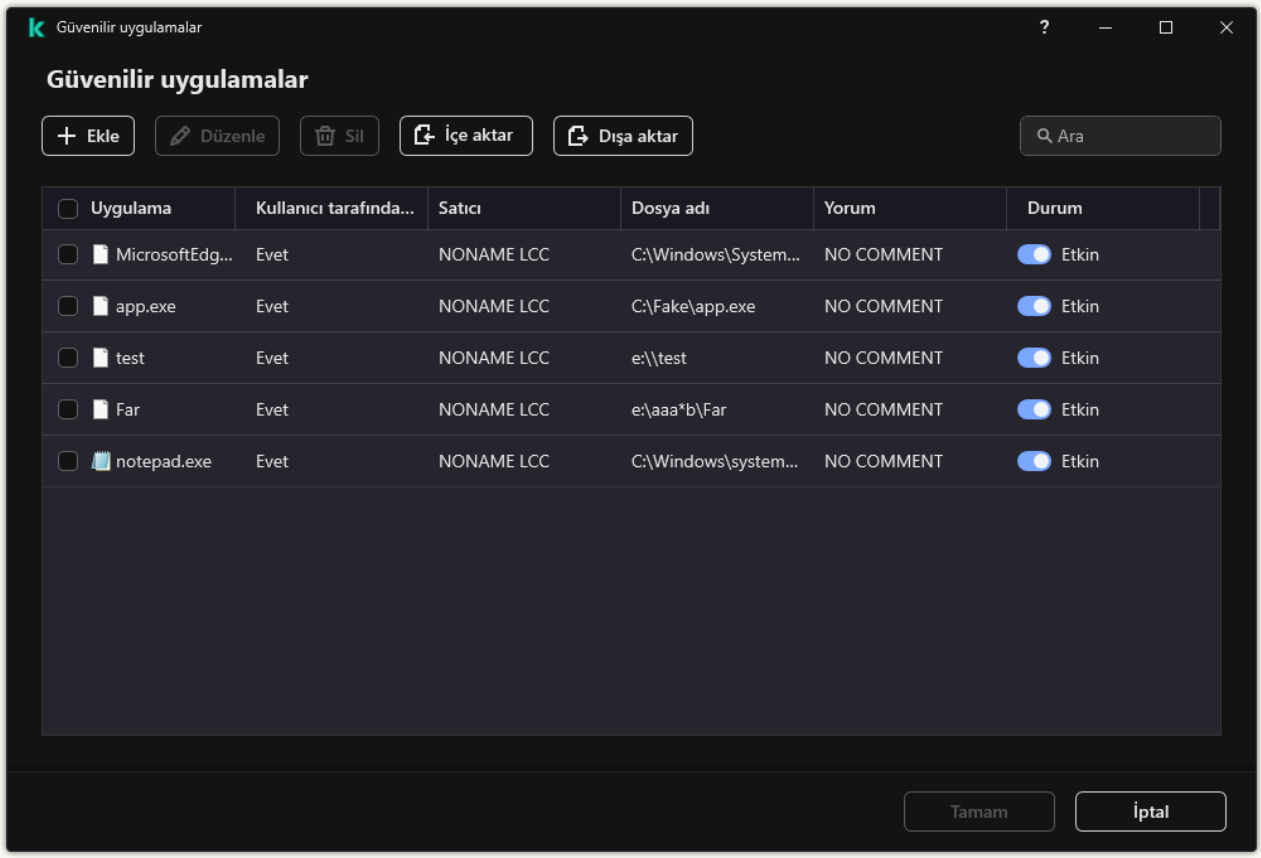
4. Açılan pencerede **Ekle** düğmesine tıklayın.
5. Güvenilir uygulamanın yürütülebilir dosyasını seçin.

   Yolu manuel olarak da silebilirsiniz. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler.

   > 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 (aşağıdaki tabloya bakın).
7. Herhangi bir zamanda bir uygulamayı güvenilen bölgeden çıkarmak için geçiş düğmesini kullanabilirsiniz (aşağıdaki resme bakın).
8. Değişikliklerinizi kaydedin.



Güvenilir uygulamaların listesi

Güvenilir uygulama ayarları

Parametre	Açıklama
Açmadan önce 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. Uygulama etkinliği aşağıdaki bileşenler tarafından izlenir: Davranış Tespiti, Exploit Önleme, Sucnucu Yetksiz Erişim Önleme, Düzeltme Altyapısı ve Güvenlik Duvarı.
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.
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.
Konsol etkileşimli girdi için telemetri toplama	Kaspersky Endpoint Security, konsolda uygulamanın yönetilmesiyle ilgili telemetri verileri göndermez. Telemetri verileri Kaspersky Anti Targeted Attack Platform (EDR) tarafından kullanılır.

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 bağlantı noktası numaralarını da taramalardan hariç tutabilirsiniz.
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.

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'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** öğesini seçin.
5. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Ayarlar** düğmesine tıklayın.
6. Kurallar listesini dışa aktarmak için:
   a. **Tarama istisnaları** sekmesini seçin.
      Bu, istisnaların listesini içeren bir pencere açar.
   b. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla bağlantı noktası seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.
      Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.
   c. **Dışa aktar** bağlantısına tıklayın.
   d. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.
   e. Dosyaya kaydet.
      Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır. Kaspersky Endpoint Security, istisnalar listesinin bir DAT dosyasına aktarılmasını da destekler.

7. Güvenilir uygulamalar listesini dışa aktarmak için:

   a. **Güvenilir uygulamalar** sekmesini seçin.

      Bu, güvenilir uygulamaların listesini içeren bir pencere açar.

   b. Dışa aktarmak istediğiniz güvenilir uygulamaları seçin. Birden fazla bağlantı noktası seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

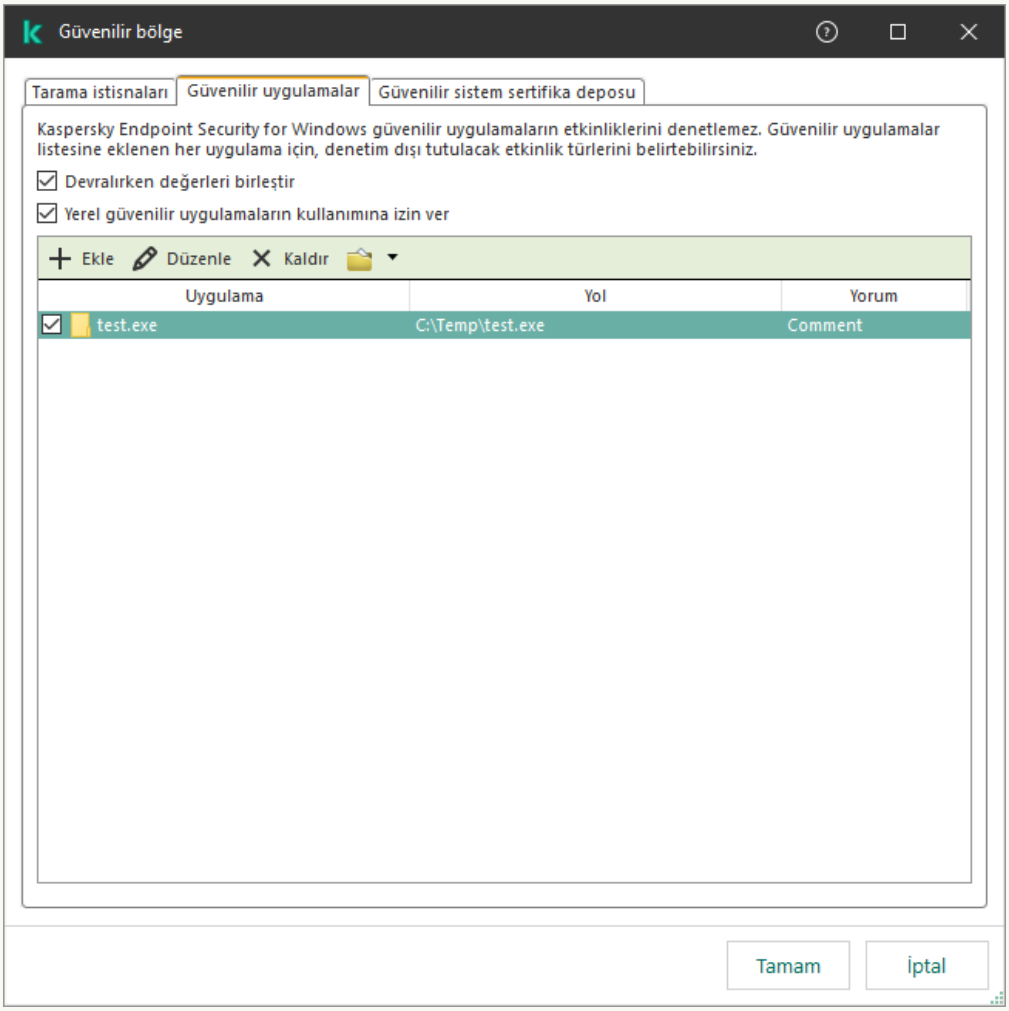
      Herhangi bir güvenilir uygulama seçmezseniz Kaspersky Endpoint Security tüm güvenilir uygulamaları dışa aktarır.

   c. **Dışa aktar** bağlantısına tıklayın.

   d. Böylece açılan pencerede, güvenilir uygulamalar listesini dışa aktarmak istediğiniz XML dosyasının adını girin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   e. Dosyaya kaydet.

      Kaspersky Endpoint Security, güvenilen uygulamaların listesini XML dosyasına aktarır.



Güvenilir uygulamaların listesi

8. İstisnalar listesini içe aktarmak için:

   a. **Tarama istisnaları** sekmesini seçin.

      Bu, istisnaların listesini içeren bir pencere açar.

   b. **İçe aktar**'a tıklayın.

   c. Açılan pencerede, istisnalar listesini içe aktarmak için kullanmak istediğiniz XML dosyasını seçin.

   d. 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.

9. Güvenilir uygulamaların bir listesini içe aktarmak için:

   a. **Güvenilir uygulamalar** sekmesini seçin.

      Bu, güvenilir uygulamaların listesini içeren bir pencere açar.

   b. **İçe aktar**'a tıklayın.

   c. Açılan pencerede, güvenilir uygulamalar listesini almak istediğiniz XML dosyasını seçin.

   d. Dosyayı aç.

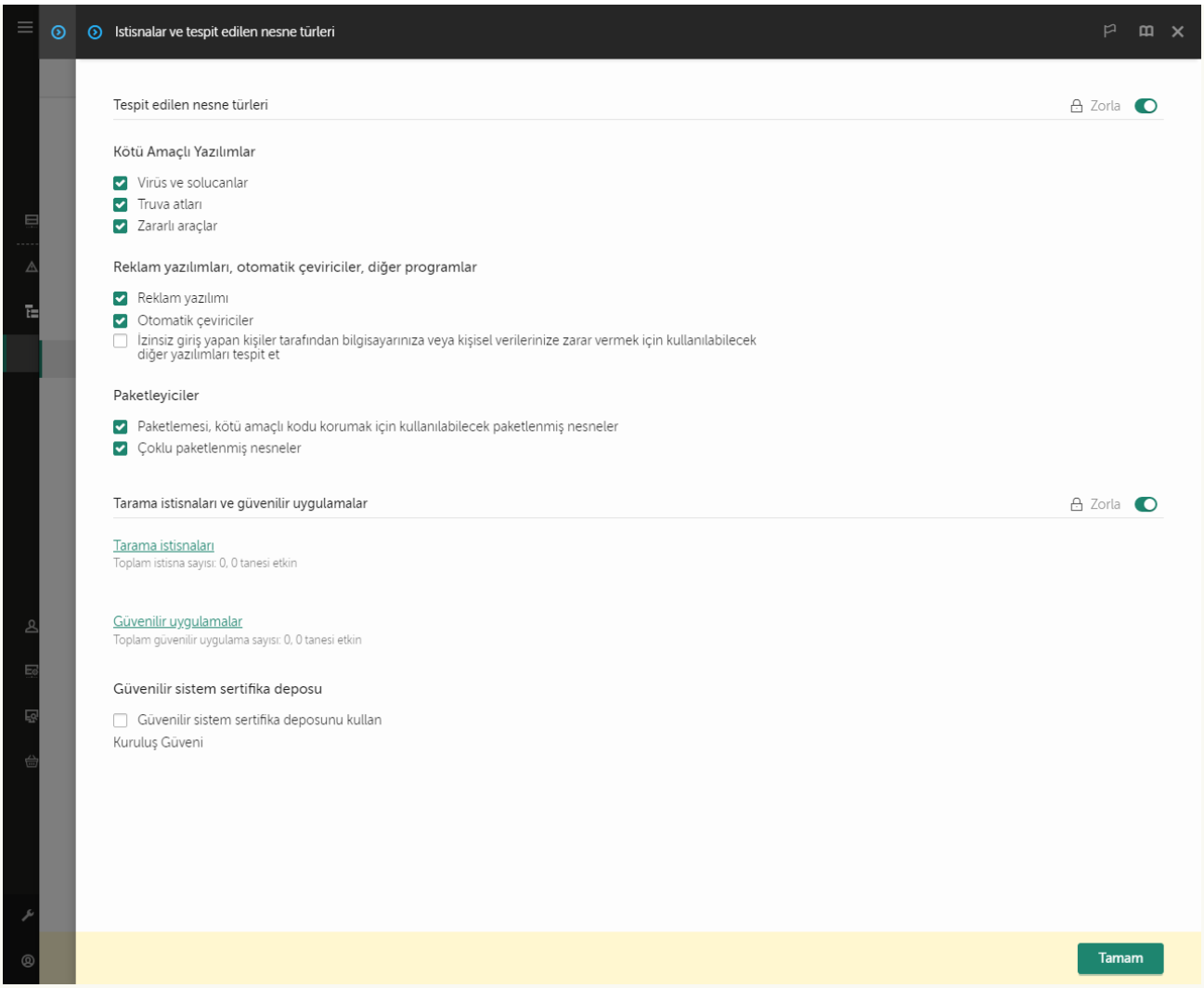
      Bilgisayar zaten bir güvenilir uygulamalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

10. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da güvenilir bölge nasıl dışa veya içe aktarılır

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Genel ayarlar** → **İstisnalar ve tespit edilen nesne türleri** bölümüne gidin.



İstisna ayarları

5. Kurallar listesini dışa aktarmak için:

   a. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Tarama istisnaları** düğmesine 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 XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   f. Dosyaya kaydet.

   g. Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.

6. Güvenilir uygulamalar listesini dışa aktarmak için:

   a. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Güvenilir uygulamalar** düğmesine 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 XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

f. Dosyaya kaydet.

Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.

7. 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.

8. Güvenilir uygulamaların bir listesini içe aktarmak için:

a. **Tarama istisnaları ve güvenilir uygulamalar** bloğunda, **Güvenilir uygulamalar** düğmesine tıklayın.

b. **İçe aktar**'a tıklayın.

c. Açılan pencerede, güvenilir uygulamalar listesini almak istediğiniz XML dosyasını seçin.

d. Dosyayı aç.

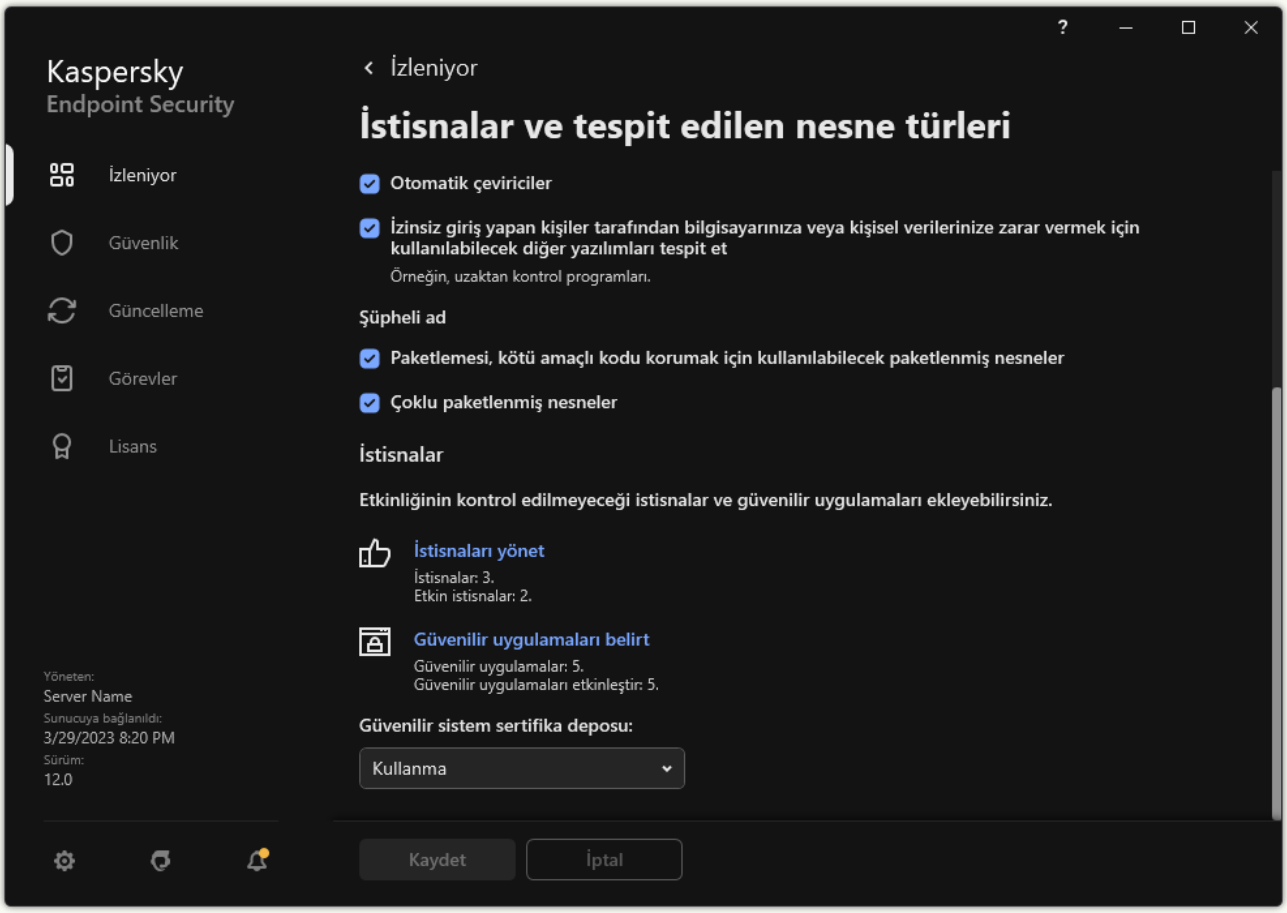
Bilgisayar zaten bir güvenilir uygulamalar listesine sahipse, Kaspersky Endpoint Security var olan bu listeyi silmenizi ister ya da bu listeye XML dosyasından yeni girişler ekler.

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.



3. Kurallar listesini dışa aktarmak için:

   a. **İstisnalar** bloğunda, **İstisnaları yönet** bağlantısını tıklayın.

   b. Dışa aktarmak istediğiniz istisnaları seçin.

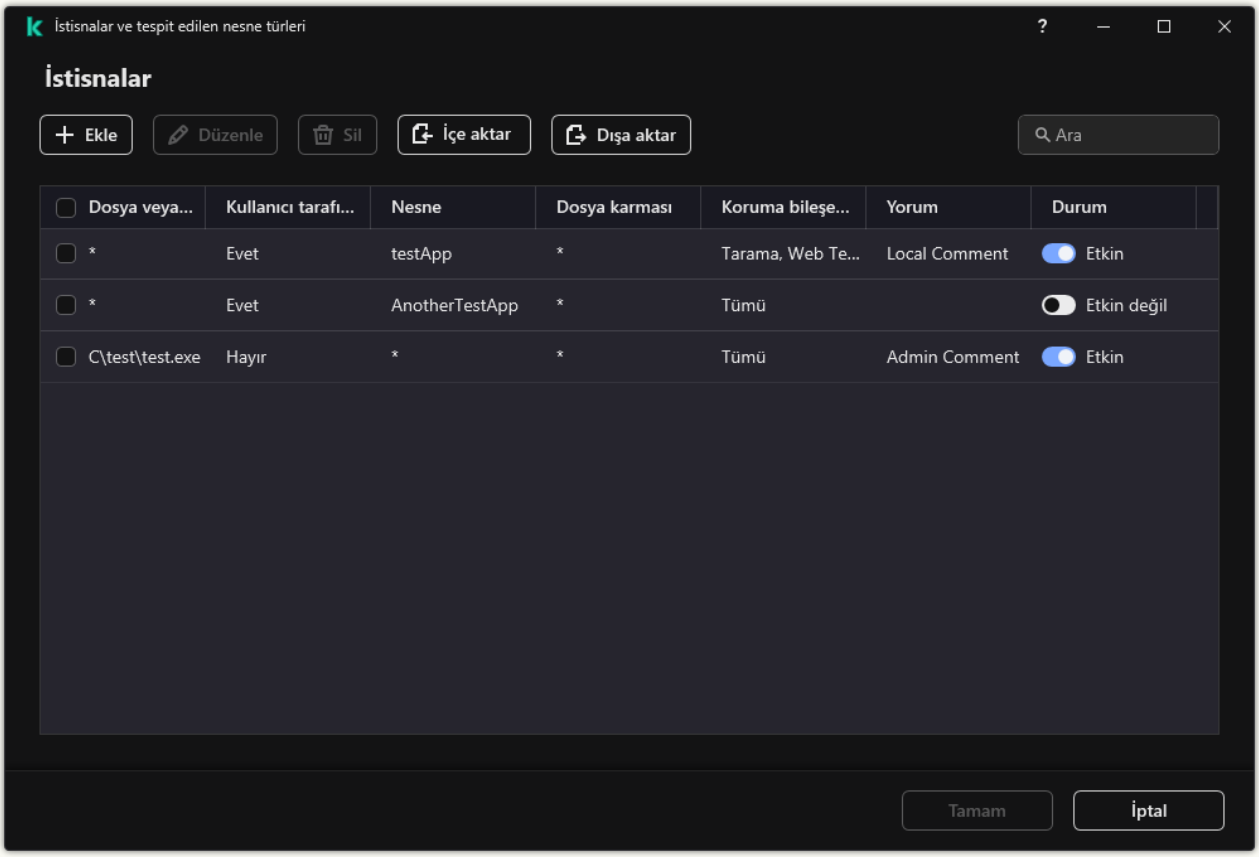
   c. **Dışa aktar**'a tıklayın.

   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.

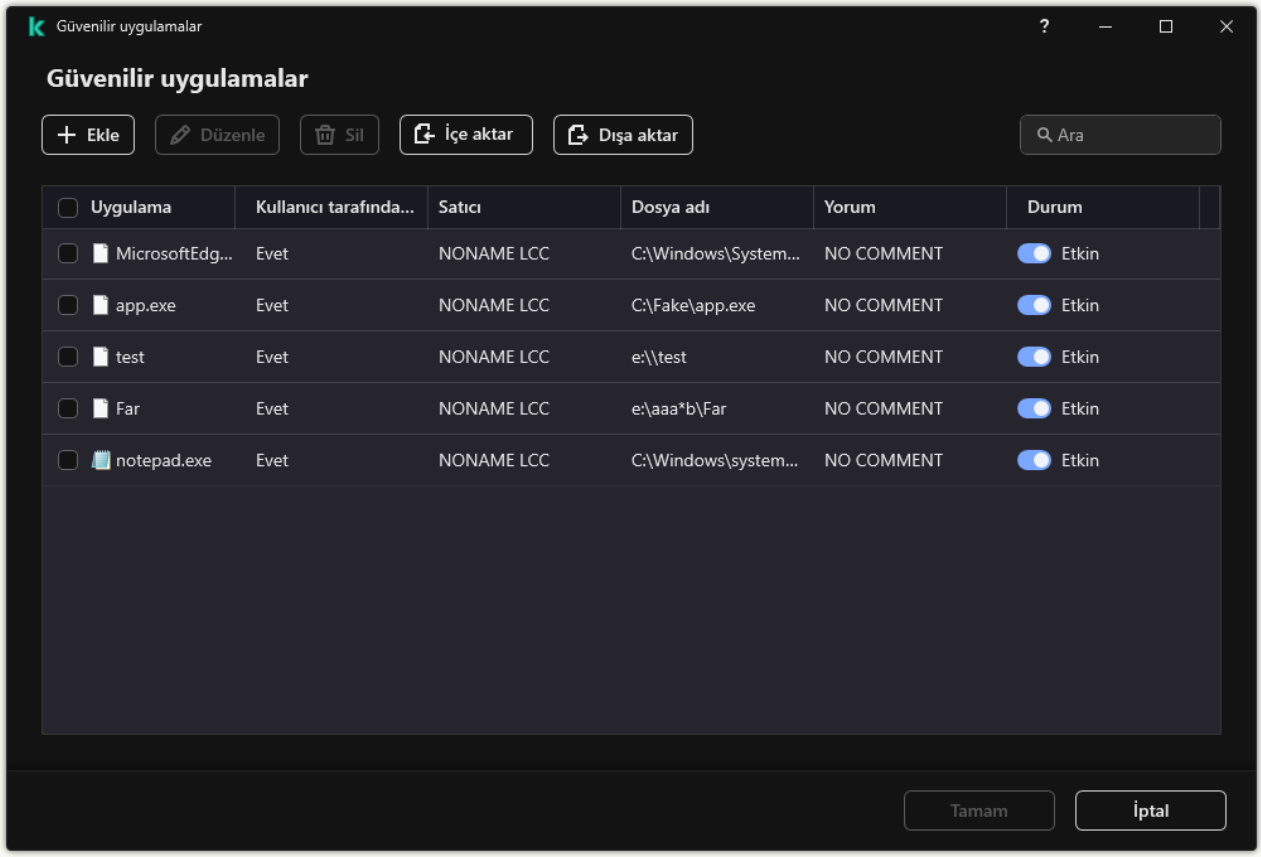
   c. **Dışa aktar**'a tıklayın.

   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.

Güvenilir sistem sertifikası depolama alanını kullanma

Sistem sertifikası depolama alanının kullanılması, güvenilir bir dijital imza ile imzalanan uygulamaları virüs taramasından istisna tutmanıza olanak tanır. Kaspersky Endpoint Security, bu tür uygulamaları otomatik olarak *Güvenilir* gruba atar.

Güvenilir sistem sertifikası depolama alanını kullanmaya başlamak için:

1. 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.

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.21.13\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.

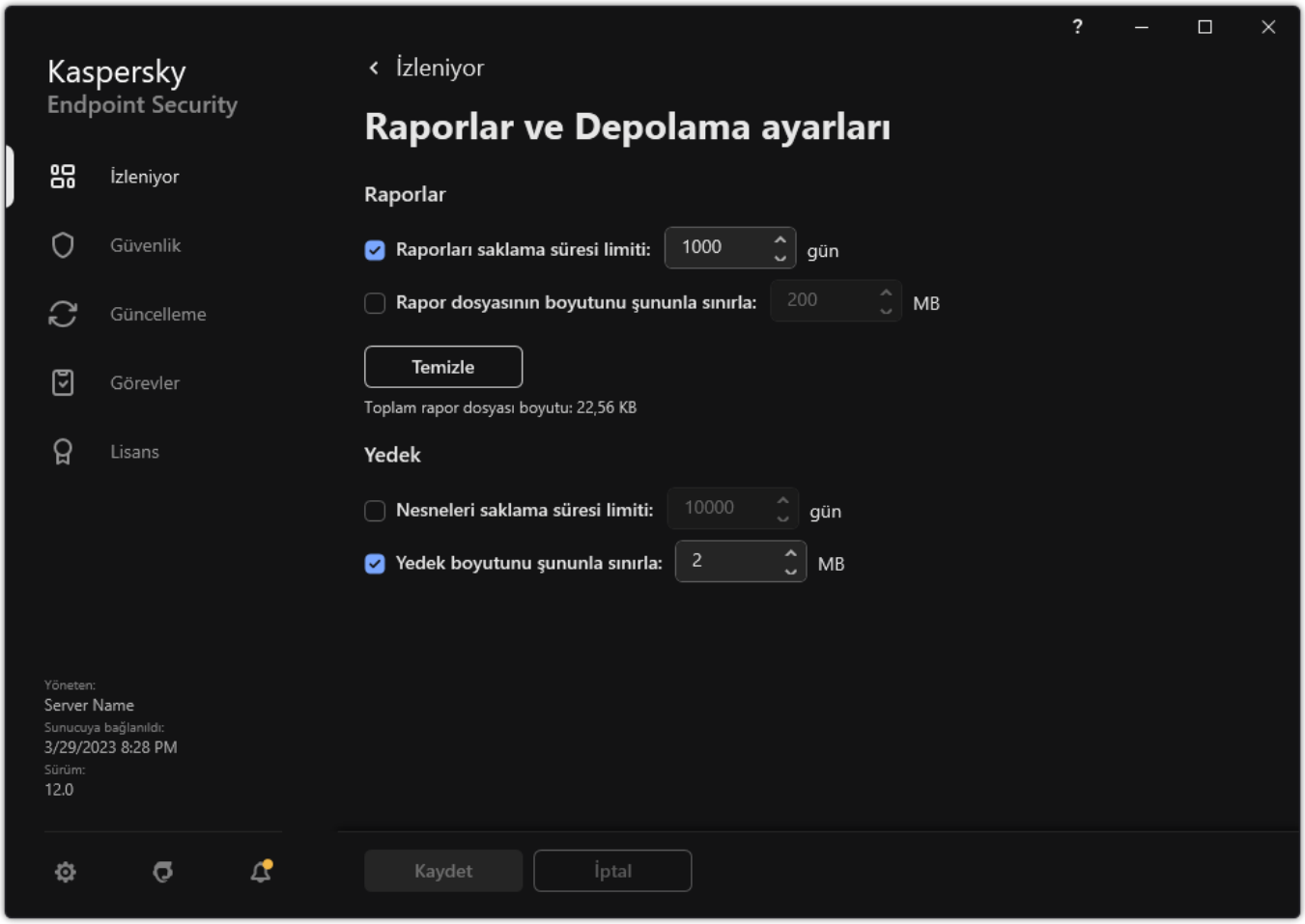
Kaspersky Endpoint Security, Kaspersky Security Center yönetimi kapsamında çalışıyorsa dosyaların yedek kopyaları Kaspersky Security Center Yönetim Sunucusuna iletilebilir. Kaspersky Security Center'da dosyaların yedek kopyalarını yönetme hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center 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** → **Raporlar ve Depolama Alanı** öğesini seçin.



Yedekleme ayarları

3. Yedekleme'deki dosyaların kopyalarının depolama dönemini sınırlamak istiyorsanız, **Yedek** bloğundaki **Nesneleri saklama süresi limiti: N gün** onay kutusunu seçin. Yedekleme'deki dosyalar için maksimum depolama süresini girin.

4. Değişikliklerinizi kaydedin.

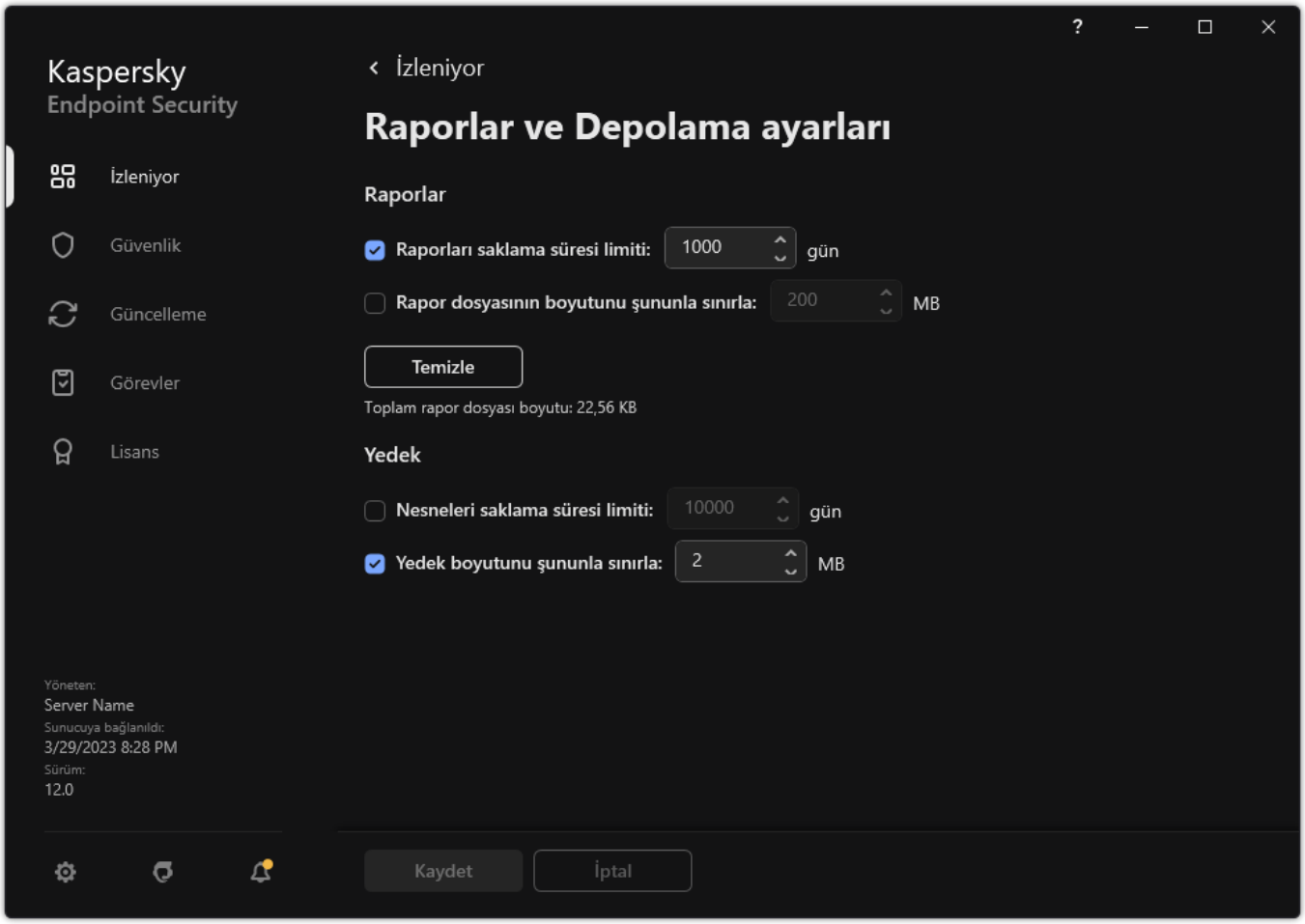
Yedekleme için maksimum boyutu yapılandırma

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** → **Raporlar ve Depolama Alanı** öğesini seçin.



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* 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. Microsoft Windows 8 işletim sisteminin araçlarını kullanarak Windows Store uygulamasının bütünlüğünü geri yükleyebilirsiniz (Windows Store uygulamalarının geri yüklenmesiyle ilgili ayrıntılar için Microsoft Windows 8 yardım dosyaları bölümüne bakınız).

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.

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.

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. **Bildirim ayarları** bloğunda **Bildirimler** 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. **Bildirim ayarları** bloğunda **Bildirimler** düğmesine tıklayın.

   Kaspersky Endpoint Security bileşenleri ve görevleri pencerenin sol kısmında yer alır. Pencerenin sağ kısmında seçilen bileşen veya seçilen 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 bildirim ayarları**'na 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.21.13\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.

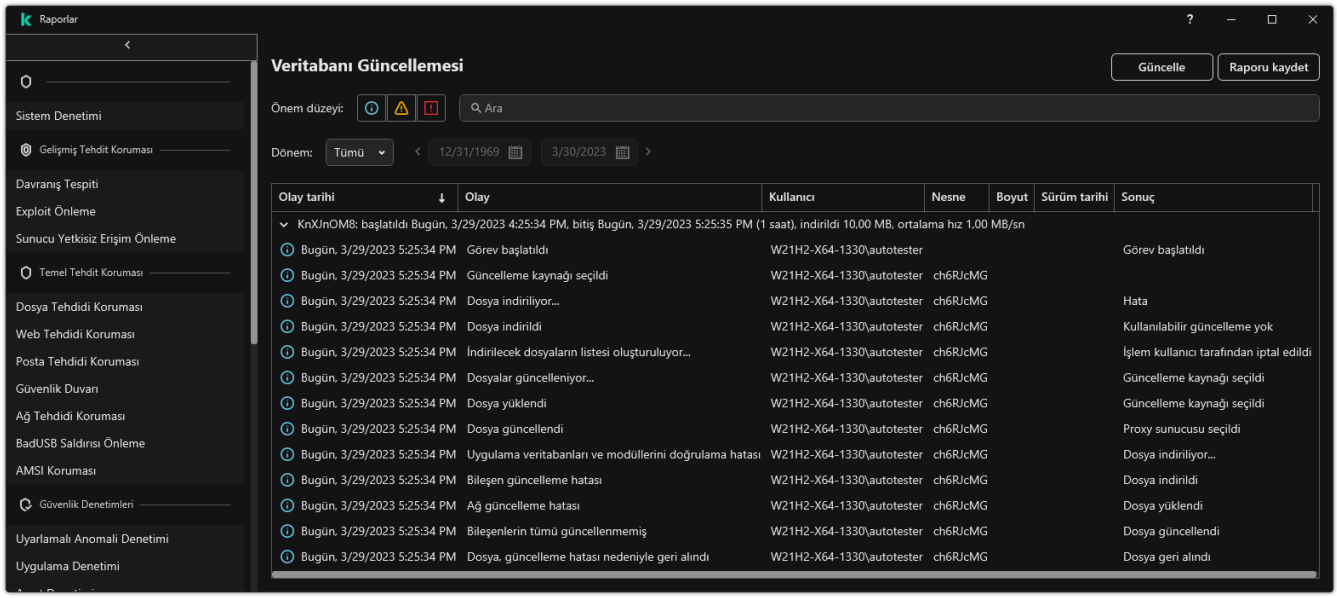
Kaspersky Endpoint Security, Kaspersky Security Center yönetimi altında çalışıyorsa, olaylar hakkındaki bilgiler Kaspersky Security Center Yönetim Sunucusu'na aktarılabilir (daha fazla bilgi için Kaspersky Security Center Yardımı 'na başvurun).

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.

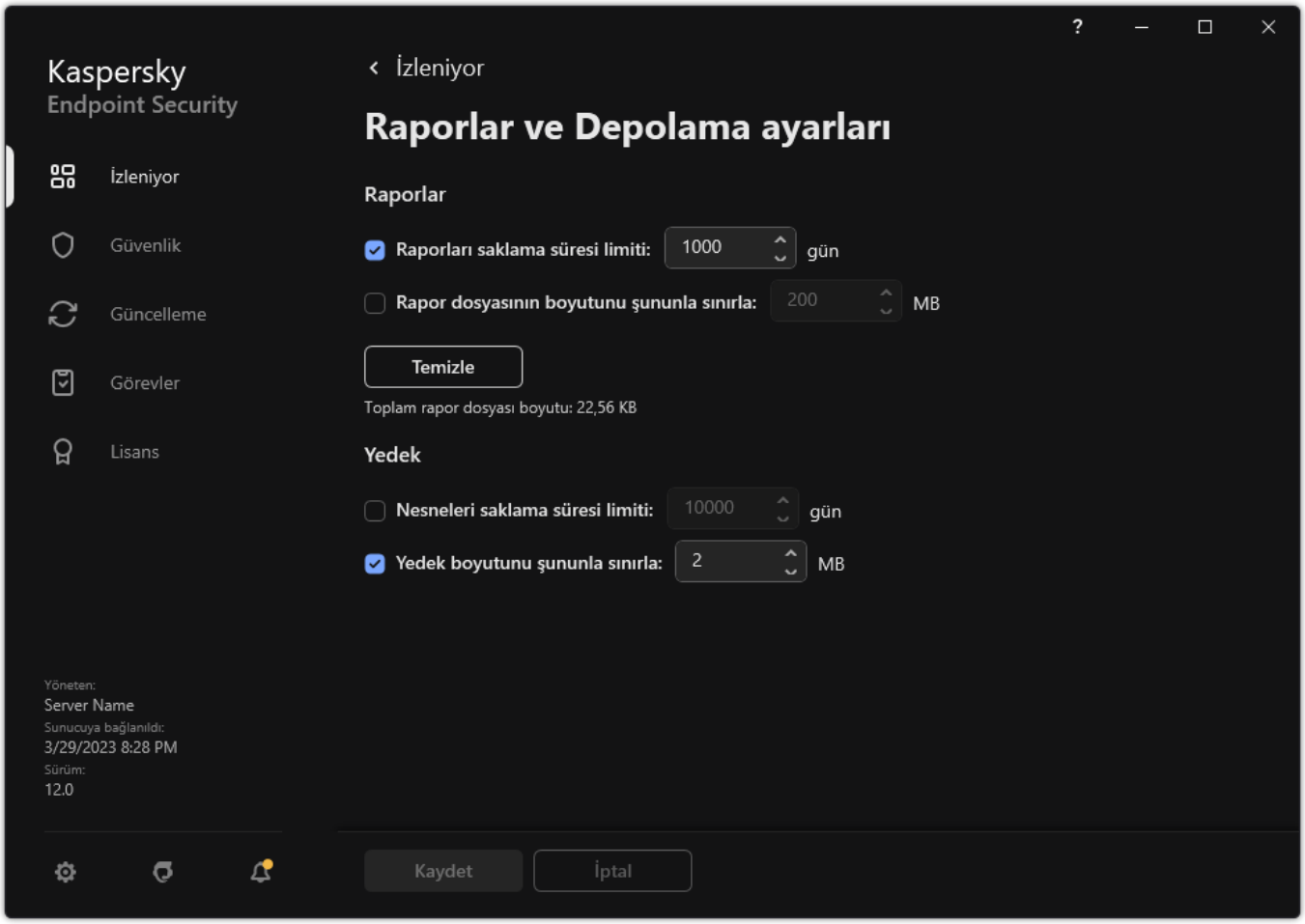
Maksimum rapor depolama süresini yapılandırma

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** → **Raporlar ve Depolama Alanı** öğesini seçin.



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.

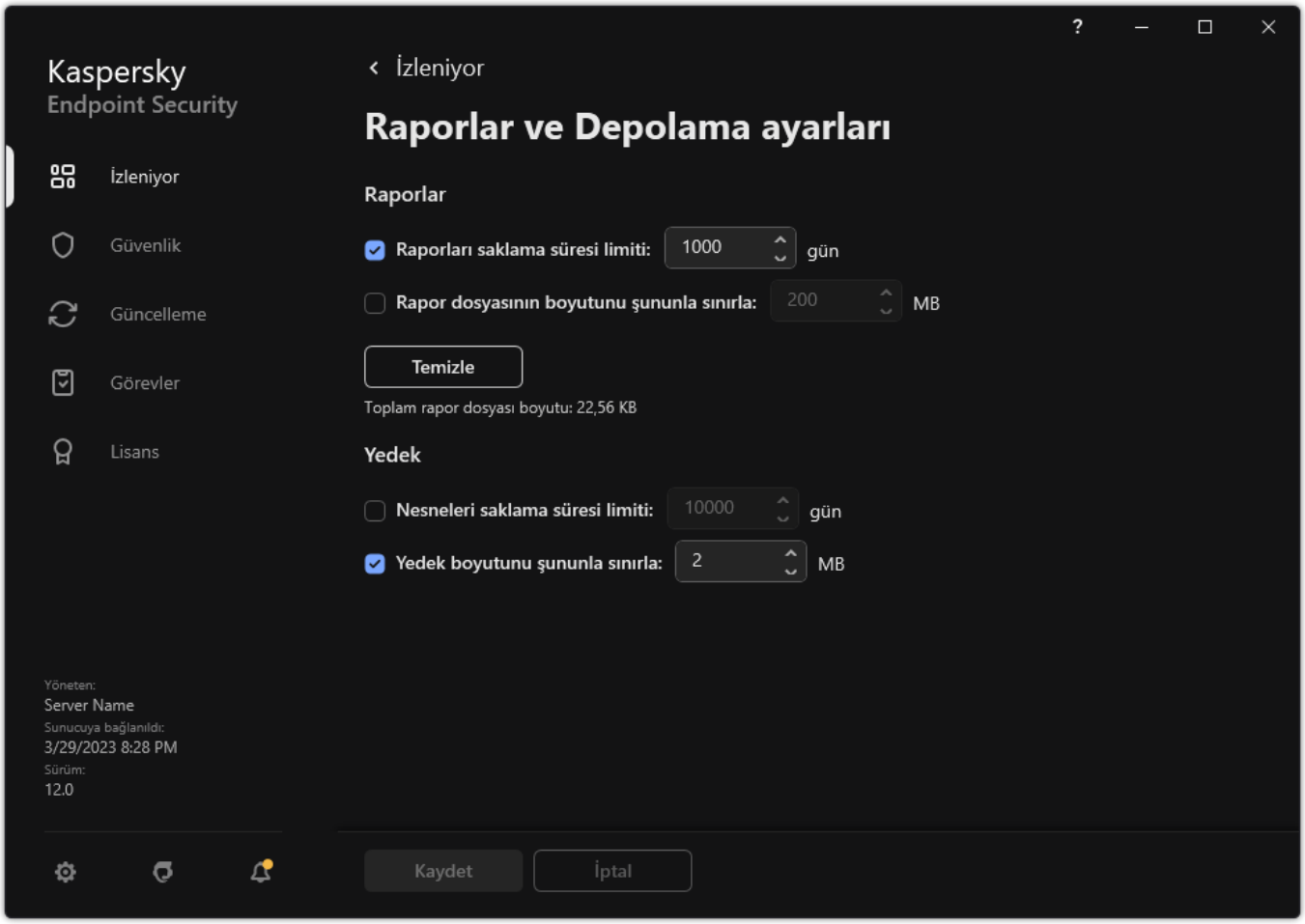
Rapor dosyasının maksimum boyutunu yapılandırma

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** → **Raporlar ve Depolama Alanı** öğesini seçin.



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

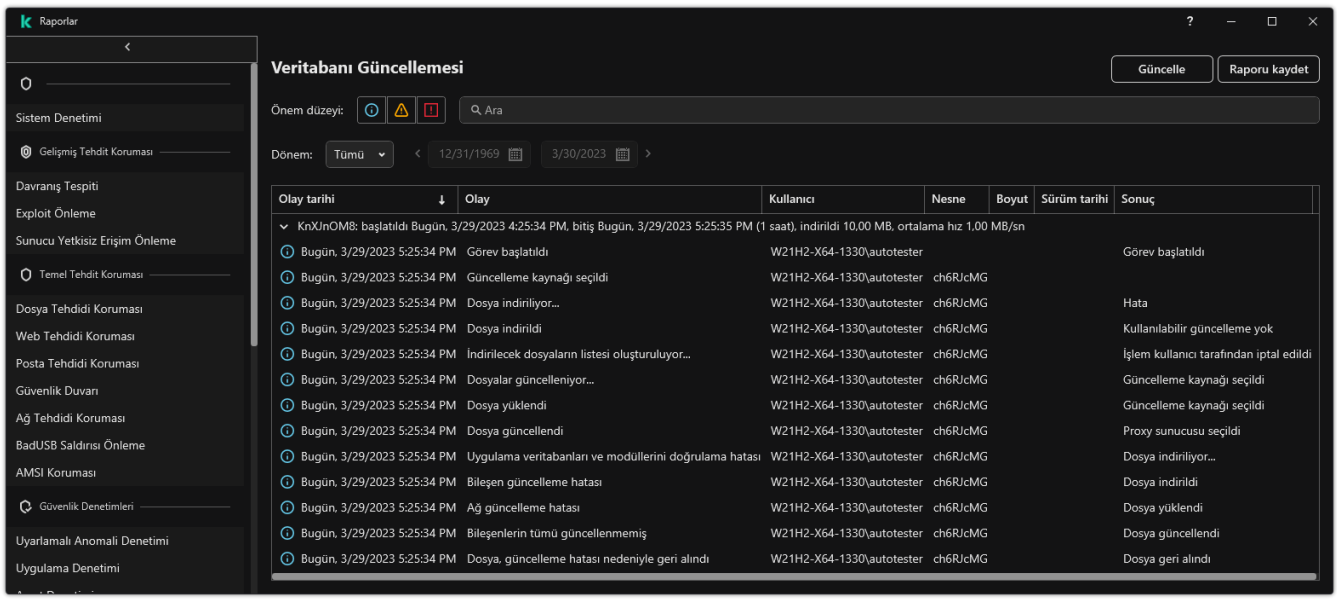
Kullanıcı, dosyaya kaydedilen bir rapordaki bilgilerin güvenliğini sağlamaktan ve özellikle de bu bilgilere erişimi denetlemekten ve kısıtlamaktan sorumludur.

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.

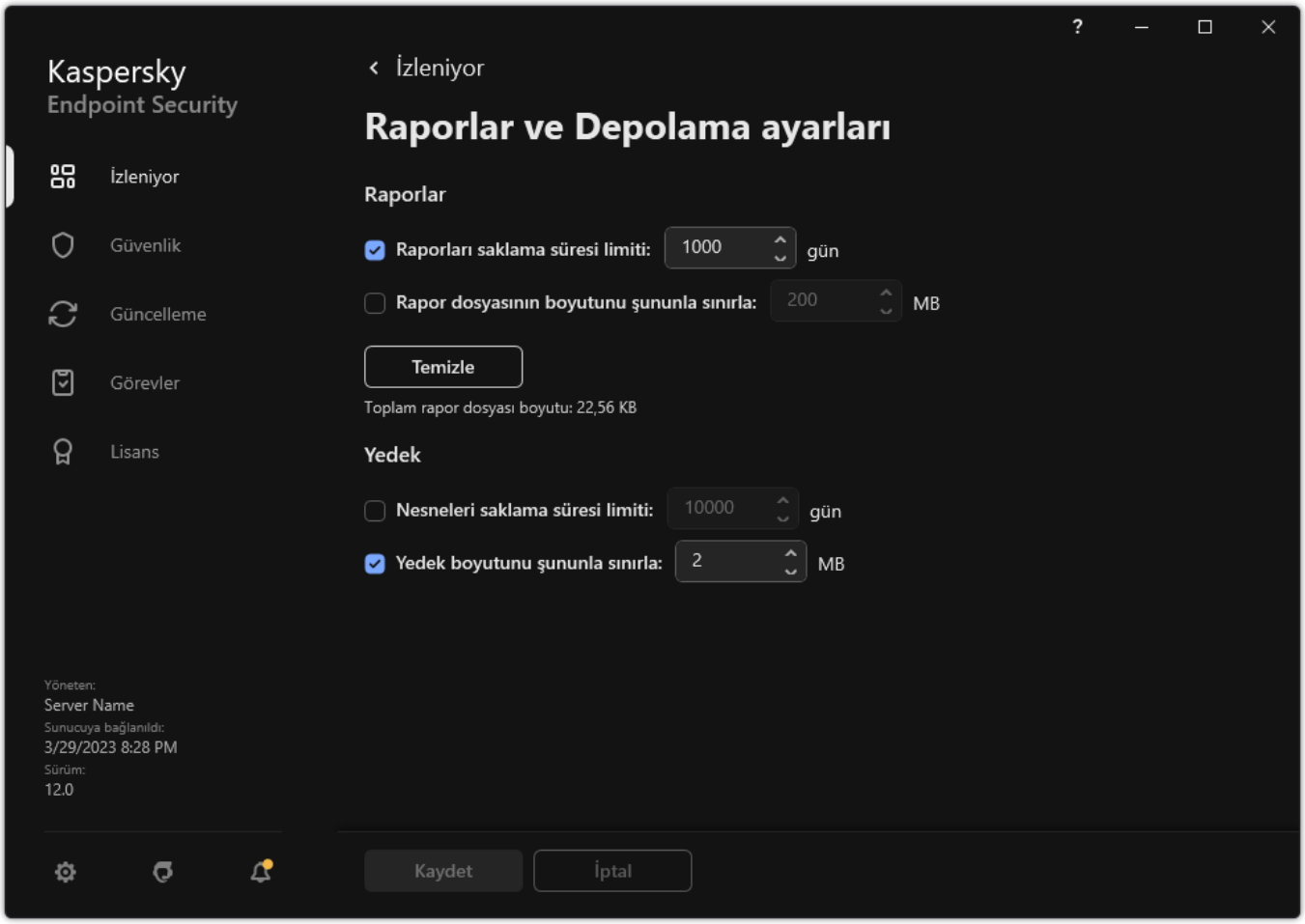
8. Değişikliklerinizi kaydedin.

Raporları temizleme

Raporlardan bilgi çıkarmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar** → **Raporlar ve Depolama Alanı** öğesini seçin.



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).

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.

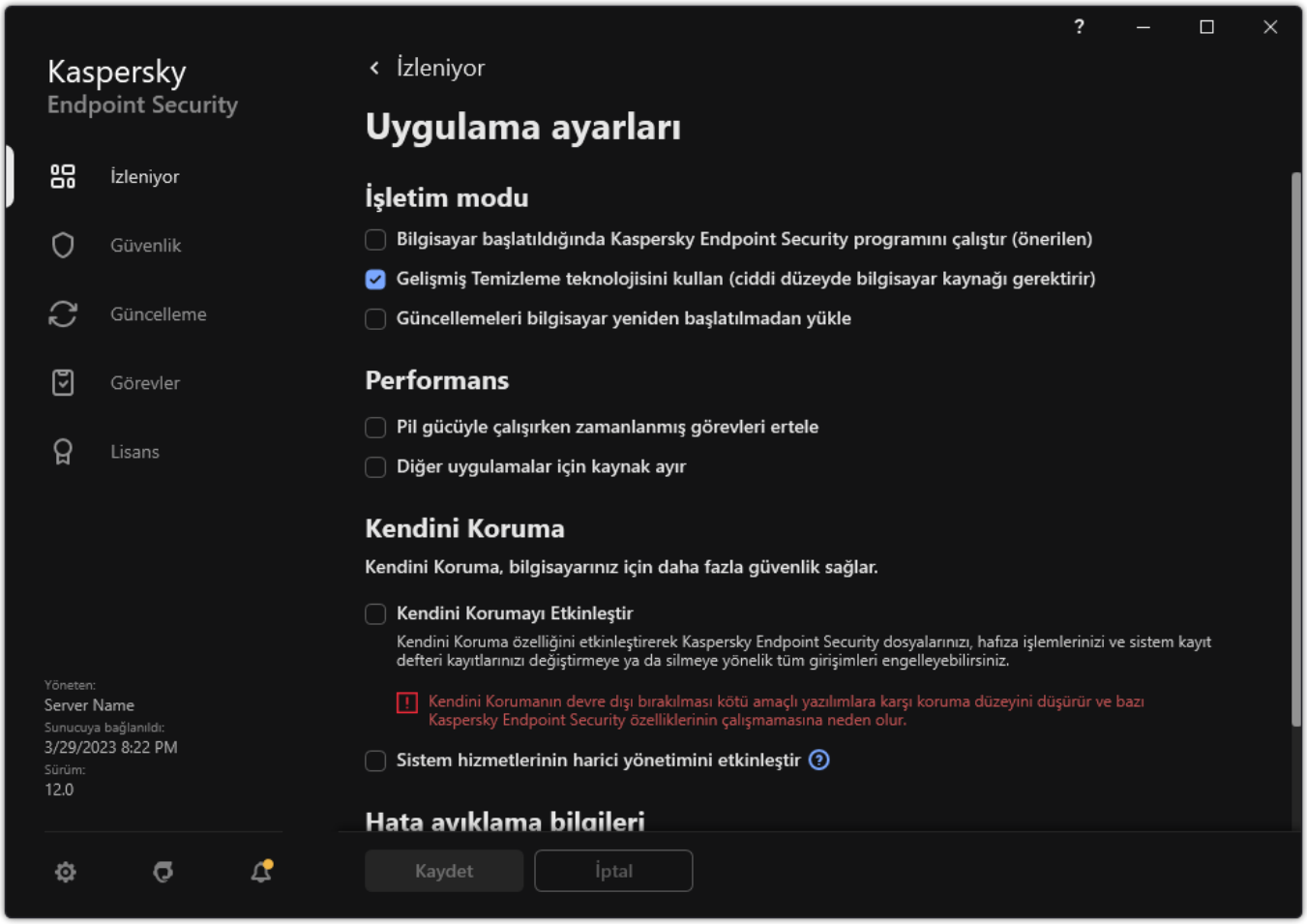
Harici yönetim koruma mekanizması	Bu teknoloji, uzaktan yönetim uygulamalarının (örneğin TeamViewer veya RemotelyAnywhere) Kaspersky Endpoint Security'ye erişmesini engeller.	✓	– (Windows 7 hariç)

Kendini Koruma'yı etkinleştirme ve devre dışı bırakma

Kaspersky Endpoint Security'nin Kendini Koruma mekanizması varsayılan olarak etkindir.

Kendini Korumayı etkinleştirmek veya devre dışı bırakmak için:

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 teknolojisi Windows Server 2019 ve Windows 10 sürüm 1703 (RS2) veya üstü işletim sistemlerinde bulunur.

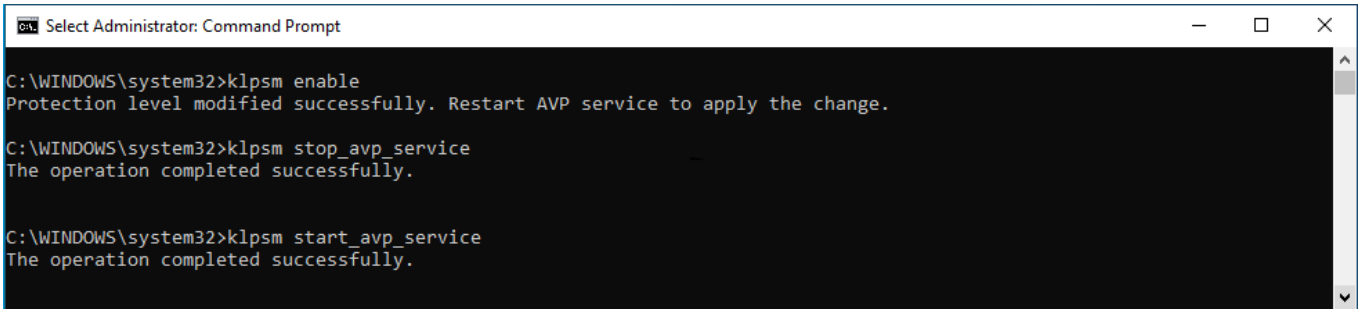
AM-PPL teknolojisi, sadece 32 bit işletim sistemleri çalıştıran bilgisayarlarda kullanılabilir. Bu teknoloji, 64 bit işletim sistemleri çalıştıran bilgisayarlarda kullanılamaz.

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.
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

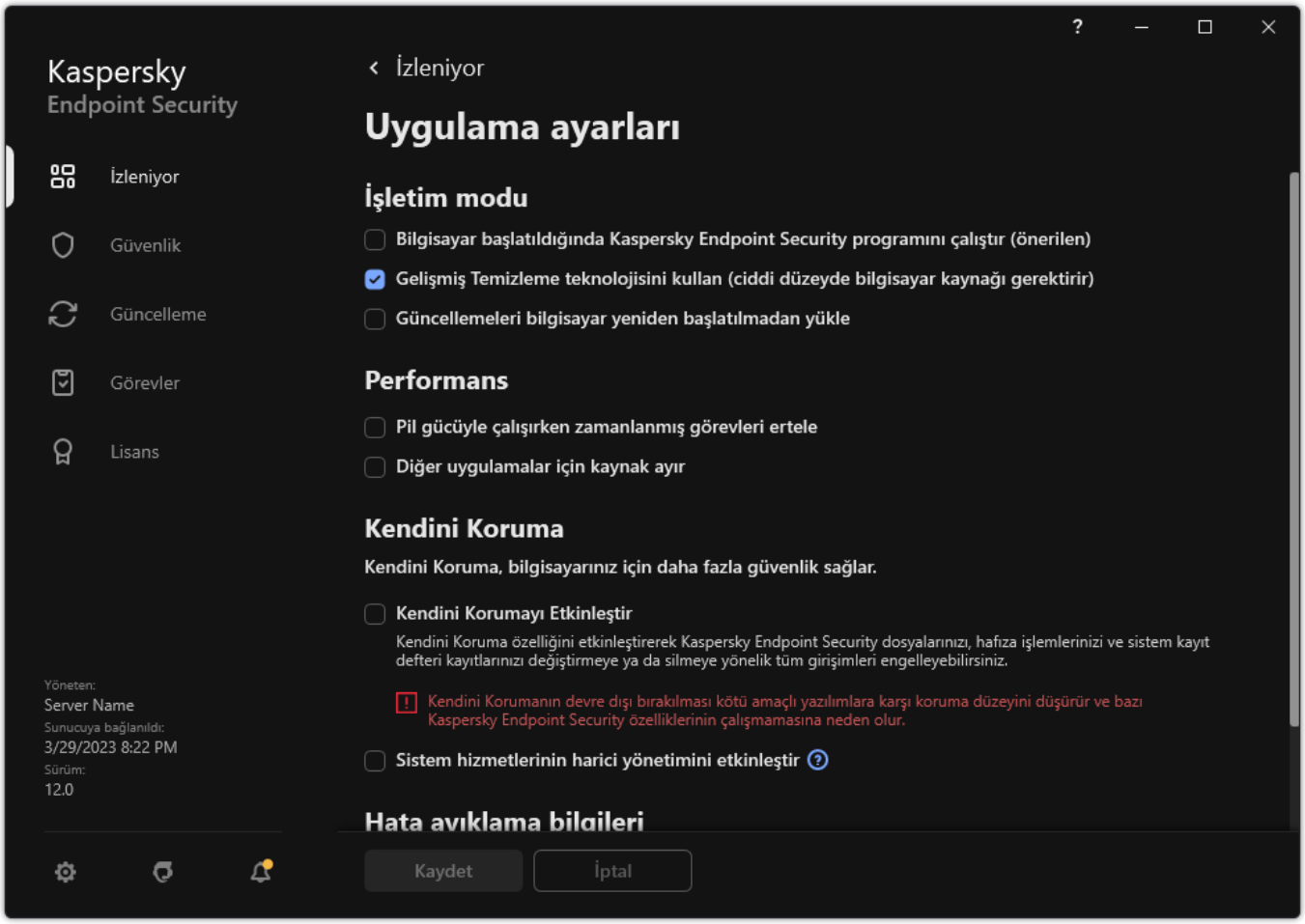
Uygulama hizmetlerinin harici yönetime karşı korunması, kullanıcıların ve diğer uygulamaların Kaspersky Endpoint Security hizmetlerini durdurma girişimlerini engeller. Koruma, şu hizmetlerin çalışmasını sağlar:

- Kaspersky Endpoint Security Service (avp)
- Kaspersky Seamless Update Service (avpsus)

Komut satırını kullanarak uygulamadan çıkmak için Kaspersky Endpoint Security hizmetlerinin harici yönetime karşı korumasını devre dışı bırakın.

Uygulama hizmetlerinin harici yönetime karşı korunmasını etkinleştirmek veya devre dışı bırakmak için:

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 **Sistem hizmetlerinin harici yönetimini etkinleştir** 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.

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.

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.

- Güncelleme görevi;
- 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 Kaspersky Endpoint Security tarafından bilgisayar kaynaklarının tüketilmesi, CPU ve sabit sürücü alt sistemleri üzerindeki yükü artırabilir ve diğer uygulamaların performansını etkileyebilir. 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.

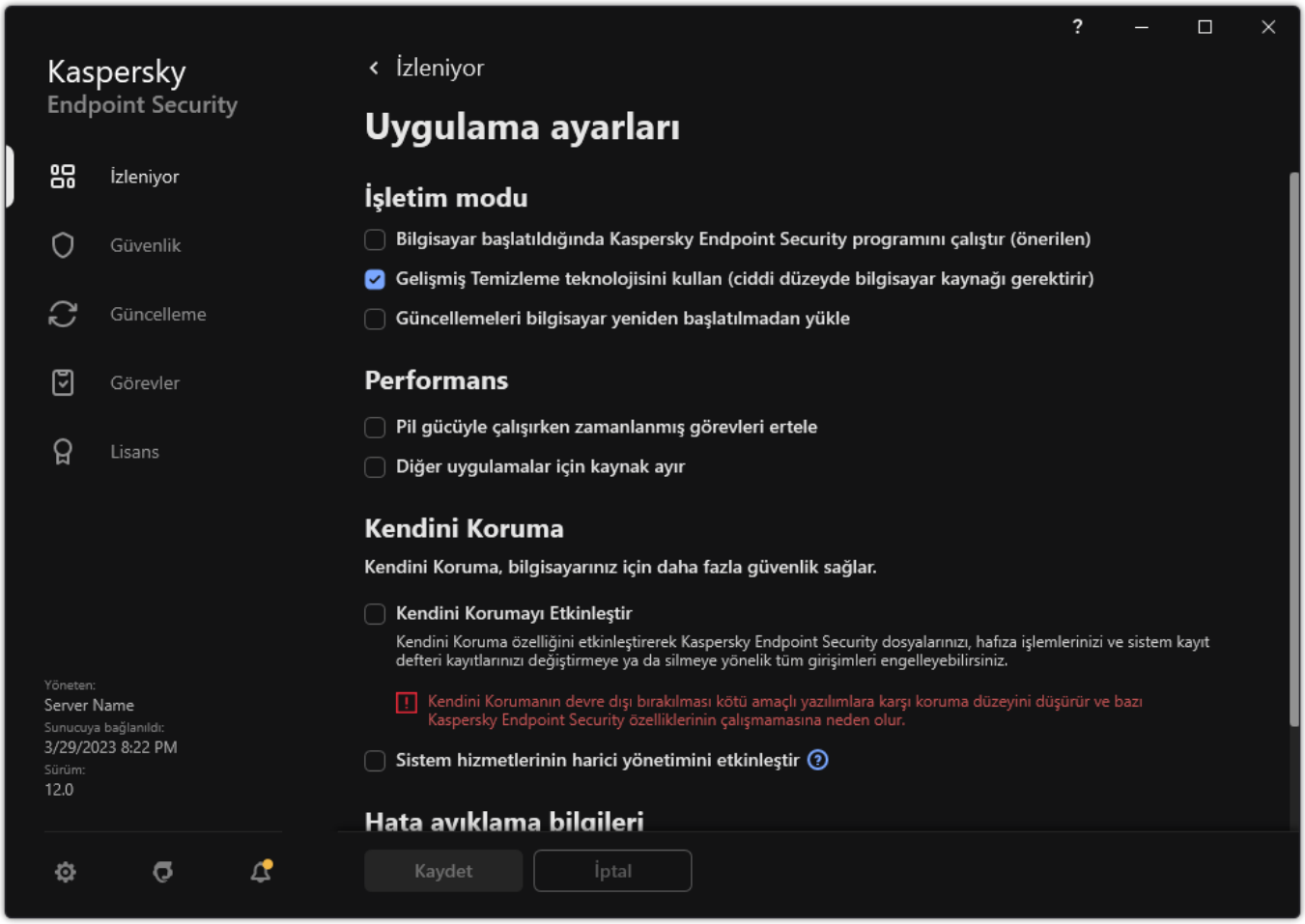
Sunucularla ilgili Kaspersky Endpoint Security özelliklerinden dolayı Microsoft Windows'un kurulu olduğu bir bilgisayarda yeniden yükleme istemi mümkün değildir. Dosya sunucusunun plansız bir şekilde yeniden başlatılması, sunucu verilerinin geçici olarak kullanılamaması veya kaydedilmemiş verilerin kaybedilmesi 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 Etkin Temizleme gerektiğini belirten bilgilerle olay, Kaspersky Security Center'a aktarılır. Bir sunucudaki etkin virüsü temizlemek için sunucular için Etkin 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

Enerji tasarruf modunu etkinleştirmek veya devre dışı bırakmak için:

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.

   Enerji tasarruf modu etkinleştirildiğinde ve bilgisayar pil gücüyle çalışırken aşağıdaki görevler zamanlanmış olsa bile çalıştırılmaz:

   - *Güncelle*
   - *Tam Tarama*
   - *Kritik Alanları Tarama*
   - *Özel Tarama*
   - *Bütünlük denetimi*
   - *IOC Taraması.*

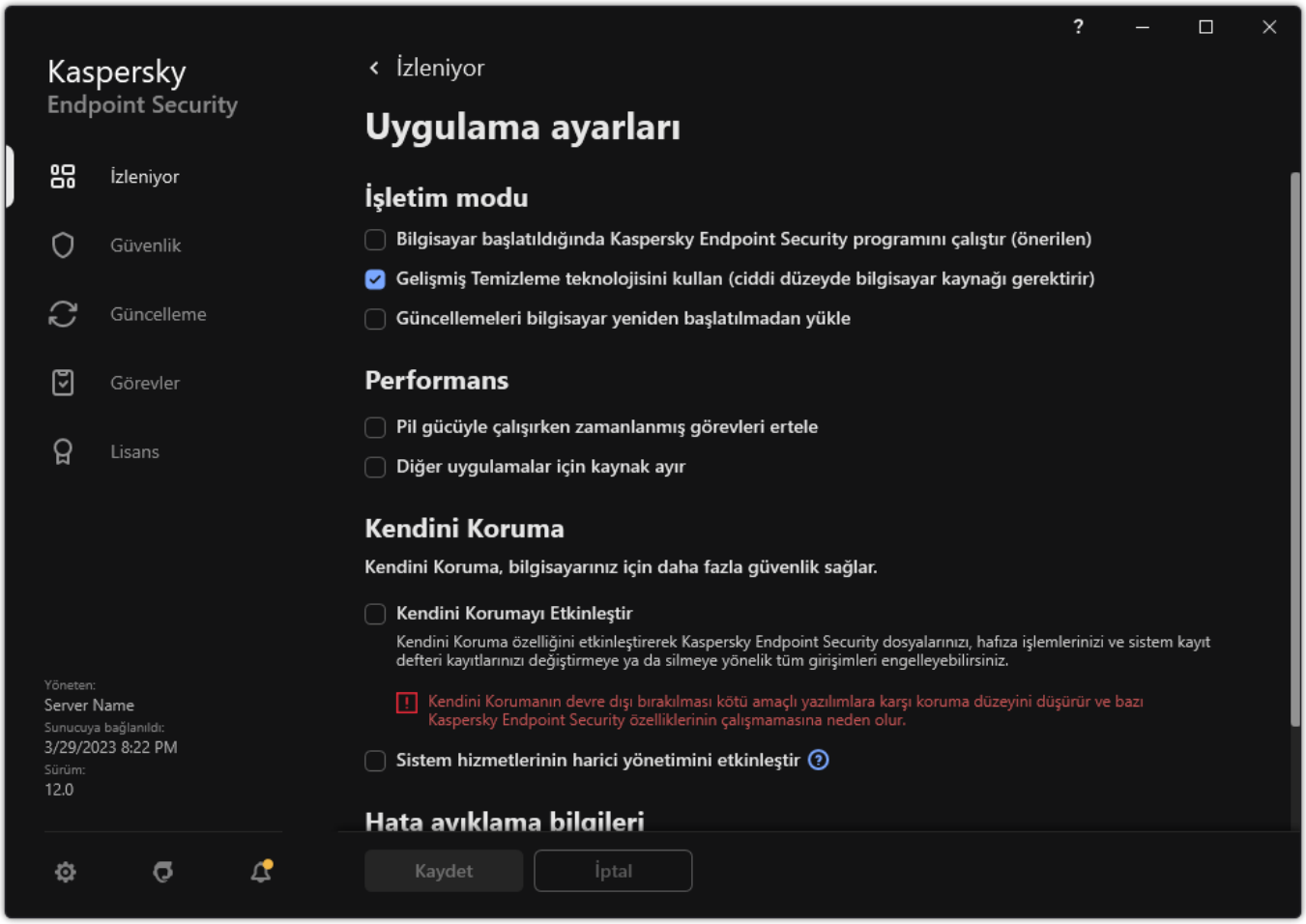
4. Değişikliklerinizi kaydedin.

Diğer uygulamalar için kaynak yaratmayı etkinleştirme veya devre dışı bırakma

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, diğer uygulamalar için kaynak yaratacak şekilde yapılandırılmıştır.

Diğer uygulamalar için kaynak yaratmayı etkinleştirmek veya devre dışı bırakmak için:

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.

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 türlerinden (örneğin tam tarama) 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. Optimum bilgisayar taraması zamanlamasını yapılandırın.

   Görevi, bilgisayar minimum yük altında çalışırken çalışacak şekilde yapılandırabilirsiniz. Örneğin, görevi gece veya hafta sonları çalışacak şekilde yapılandırabilirsiniz.

   Kullanıcılar günün sonunda bilgisayarlarını kapatırsa, tarama görevini aşağıdaki gibi yapılandırabilirsiniz:

   - LAN'da Uyandırmayı etkinleştirin. LAN'da Uyandırma özelliği, yerel ağ üzerinden özel bir sinyal göndererek bilgisayarın uzaktan açılmasını sağlar. Bu özelliği kullanmak için BIOS ayarlarından LAN'da Uyandırmayı etkinleştirmeniz gerekir. Tarama bittikten sonra bilgisayarın otomatik olarak kapanmasını da sağlayabilirsiniz.
   - "Eksik görevleri çalıştır" özelliğini devre dışı bırakın. Kaspersky Endpoint Security, kullanıcı bilgisayarı açtığında eksik olan görevleri atlar. Bilgisayar açıldıktan sonra görevleri çalıştırmak, tarama büyük bir kaynak ayrılmasını gerektirdiğinden kullanıcıyı rahatsız edebilir.

   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.

2. Bir tarama kapsamı tanımlayın.

   Aşağıdaki nesnelerin taranmasını seçin:

   - Çekirdek belleği;
   - Çalışan işlemler ve Başlangıç Nesneleri;
   - Önyükleme kesimleri;
   - Sistem sürücüsü (%systemdrive%).

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 tarama 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.

Sunucularda Kötü Amaçlı Yazılım Taraması

Kötü Amaçlı Yazılım Taraması görevini aşağıdaki önerilere göre yapılandırın:

1. Optimum bilgisayar taraması zamanlamasını yapılandırın.

   Görevi, bilgisayar minimum yük altında çalışırken çalışacak şekilde yapılandırabilirsiniz. Örneğin, görevi gece veya hafta sonları çalışacak şekilde yapılandırabilirsiniz.

2. 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 tarama 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.

3. 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.

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 dosyaların kategorisi ve tanınırlığı hakkındaki bilgilerle birlikte taranan web adreslerinin 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 etkinleştirin.

   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.

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, Gelişmiş Şifreleme Standardı (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.

> 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 Güvenilir Platform Modülü (TPM) bulunuyorsa BitLocker, şifrelenmiş sabit sürücüye erişim sağlayan kurtarma anahtarlarını bu modülü kullanarak depolar. Bilgisayar başlatıldığında BitLocker, Güvenilir Platform Modülü'nden sabit sürücü 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. Ayrıca, Kimlik Doğrulama Aracısı hesabının kullanıcı adını ve parolasını kullanarak işletim sistemine otomatik olarak giriş yapan Çoklu Oturum Açma (SSO) teknolojisi 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 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
  - MoBo 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 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Tam Disk Şifreleme** seçimini yapın.
5. **Şifreleme teknolojisi** açılır listesinde **Kaspersky Disk Encryption** öğesini seçin.

   Kaspersky Disk Encryption teknolojisi, bilgisayarda BitLocker ile şifrelenen sabit sürücüler varsa kullanılamaz.

6. **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.

7. Gelişmiş Kaspersky Disk Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
8. Değişikliklerinizi kaydedin.

Kaspersky Disk Encryption bileşeni Web Console ve Cloud Console üzerinden nasıl çalıştırılır

1. Web Console'un ana penceresinde **Aygıtlar → İlkeler ve Profiller**'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. **Şifrelemeyi yönet** bloğunda, **Kaspersky Disk Encryption** seçeneğini belirleyin.
6. **Kaspersky Disk Encryption** bağlantısına tıklayın.
   Kaspersky Disk Encryption ayarları penceresi açılır.

   Kaspersky Disk Encryption teknolojisi, bilgisayarda BitLocker ile şifrelenen sabit sürücüler varsa kullanılamaz.

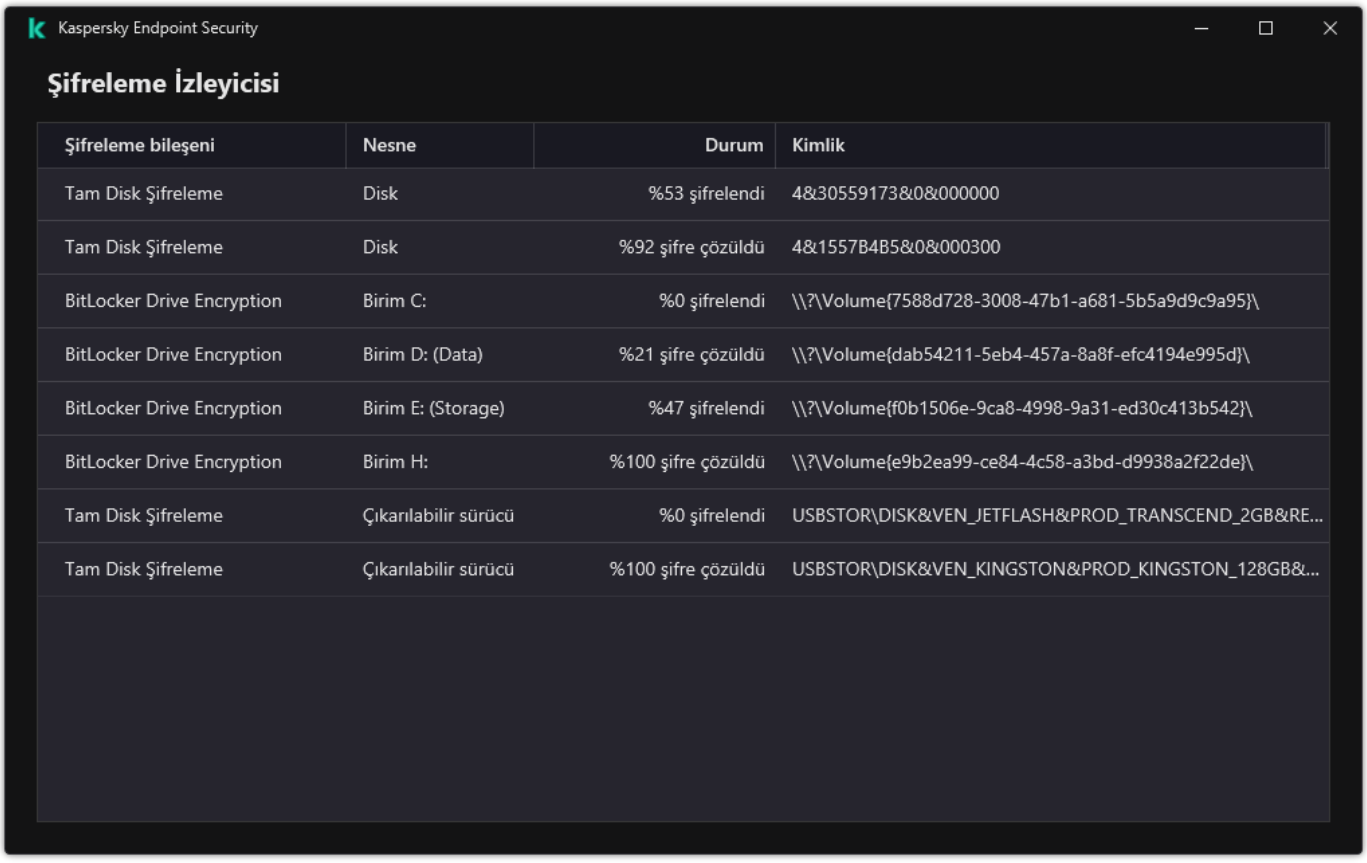
7. **Şifreleme modu** açılır listesinden **Tüm sabit sürücüleri şifrele** seçeneğini seçin.

   Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca şifreleme işleminin gerçekleştirildiği işletim sistemini yükleyebilirsiniz.

   Sabit sürücülerin bir kısmını şifreleme dışında tutmak isterseniz bu sabit sürücülerin bir listesini oluşturun.

8. Gelişmiş Kaspersky Disk Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
9. 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.
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, bu onay kutusu işaretlenmemiştir.
Legacy USB Support'u kullan (önerilmez)	Bu kutucuk, Legacy USB Support işlevini etkinleştirir/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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
5. **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.
6. Şifreleme dışında tutulan sabit sürücülerin listesine sabit sürücüleri eklemek için:
   a. **Ekle**'ye tıklayın.
   b. Açılan pencerede **Aygıt adı**, **Bilgisayar adı**, **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.
7. 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
5. **Şifreleme teknolojisi** açılır listesinde **Kaspersky Disk Encryption** öğesini seçin.

Şifreleme dışında tutulan sabit sürücülerin girişleri, **Aşağıdaki sabit sürücüleri şifreleme** tablosunda görülür.

6. İstisnalar listesini dışa aktarmak için:

   a. Dışa aktarmak istediğiniz istisnaları seçin. Birden fazla bağlantı noktası seçmek için **CTRL** veya **SHIFT** tuşlarını kullanın.

   Herhangi bir istisna seçmediyseniz, Kaspersky Endpoint Security tüm adresleri dışa aktaracaktır.

   b. **Dışa aktar** bağlantısına 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.

7. Kurallar 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.

8. Değişikliklerinizi kaydedin.

Web Console'da bir sabit sürücü şifreleme istisnaları listesi nasıl dışa aktarılır ve içe aktarılır

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 ve ayarları yapılandırmak için bağlantıyı takip edin.

   Şifreleme ayarları açılır.
6. **İstisnalar** düğmesine tıklayın.
7. Kurallar listesini dışa aktarmak için:

   a. Dışa aktarmak istediğiniz istisnaları seçin.

   b. **Dışa aktar**'a tıklayın.

   c. Yalnızca seçili istisnaları veya tüm istisnalar listesini dışa aktarmak istediğinizi onaylayın.

   d. Açılan pencerede, istisnalar listesini dışa aktarmak istediğiniz XML dosyasının adını belirtin ve bu dosyayı kaydetmek istediğiniz klasörü seçin.

   e. Dosyaya kaydet.

   Kaspersky Endpoint Security, istisnalar listesinin tamamını XML dosyasına aktarır.
8. Kurallar 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.

9. Değişikliklerinizi kaydedin.

Çoklu Oturum Açma (SSO) teknolojisini kullanma

Çoklu Oturum Açma (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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Ortak şifreleme ayarları** seçimini yapın.
5. **Parola ayarları** bloğunda **Ayarlar** düğmesine tıklayın.
6. Açılan pencerenin **Kimlik Doğrulama Aracısı** sekmesinden **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.

Web Console'da Çoklu Oturum Açma kullanımı nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 ve ayarları yapılandırmak için bağlantıyı takip edin.

   Şifreleme ayarları açılır.

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 11.10.0, üçüncü taraf kimlik bilgisi sağlayıcıları için destek sunuyor.

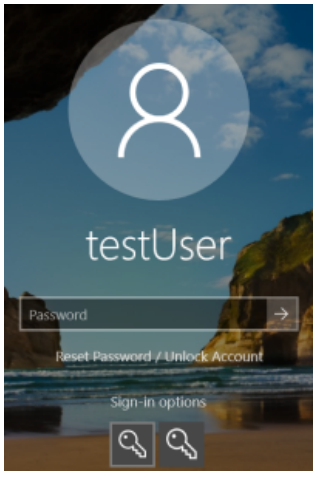
Kaspersky Endpoint Security, üçüncü taraf kimlik bilgisi sağlayıcı ADSelfService Plus'ı destekler.

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.



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. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.
   Görevler listesi açılır.
2. **Yeni görev** düğmesine tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (12.1) → **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 elle 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

Sihirbazdan çıkın. 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine 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 (12.1)** 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 cihazları seçin** 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

Sihirbazdan çıkın. 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   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.

   Bu, Kimlik Doğrulama Aracısı Hesap Yönetimi Sihirbazını başlatır.

5. **Ekle** komut türünü seçin.

6. 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 hesap güvenlik tanımlayıcısını (SID) belirler. Bu, hesabı doğrulamak için gereklidir. Kullanıcı adını yanlış girdiyseniz, Kaspersky Endpoint Security görevi bir hata ile sonlandırır.

7. Kimlik Doğrulama Aracısı hesabı ayarlarını yapılandırın.

   - **Var olan hesabın yerine yeni bir Kimlik Doğrulama Aracısı 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.

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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   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.

   Bu, Kimlik Doğrulama Aracısı Hesap Yönetimi Sihirbazını başlatır.

5. **Değiştir** komut türünü seçin.

6. 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 hesap güvenlik tanımlayıcısını (SID) belirler. Bu, hesabı doğrulamak için gereklidir. Kullanıcı adını yanlış girdiyseniz, Kaspersky Endpoint Security görevi bir hata ile sonlandırır.

7. Düzenlemek istediğiniz ayarların yanındaki onay kutularını işaretleyin.

8. Kimlik Doğrulama Aracısı hesabı ayarlarını yapılandırın.

   - **Var olan hesabın yerine yeni bir Kimlik Doğrulama Aracısı 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.

9. Değişikliklerinizi kaydedin.
10. 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   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.

   Bu, Kimlik Doğrulama Aracısı Hesap Yönetimi Sihirbazını başlatır.
5. **Sil** komut türünü seçin.

6. Bir kullanıcı hesabı seçin. Etki alanı hesapları listesinden bir hesap seçebilir ya da hesap adını manuel olarak girebilirsiniz.

7. Değişikliklerinizi kaydedin.

8. 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.

Kimlik Doğrulama Aracısı hesaplarının bir listesi Web Console aracılığıyla nasıl görüntülenir

1. Web Console'un ana penceresinde **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.

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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.

5. **Şifreleme teknolojisi** açılır listesinde, sabit sürücülerin şifrelendiği teknolojiyi seçin.

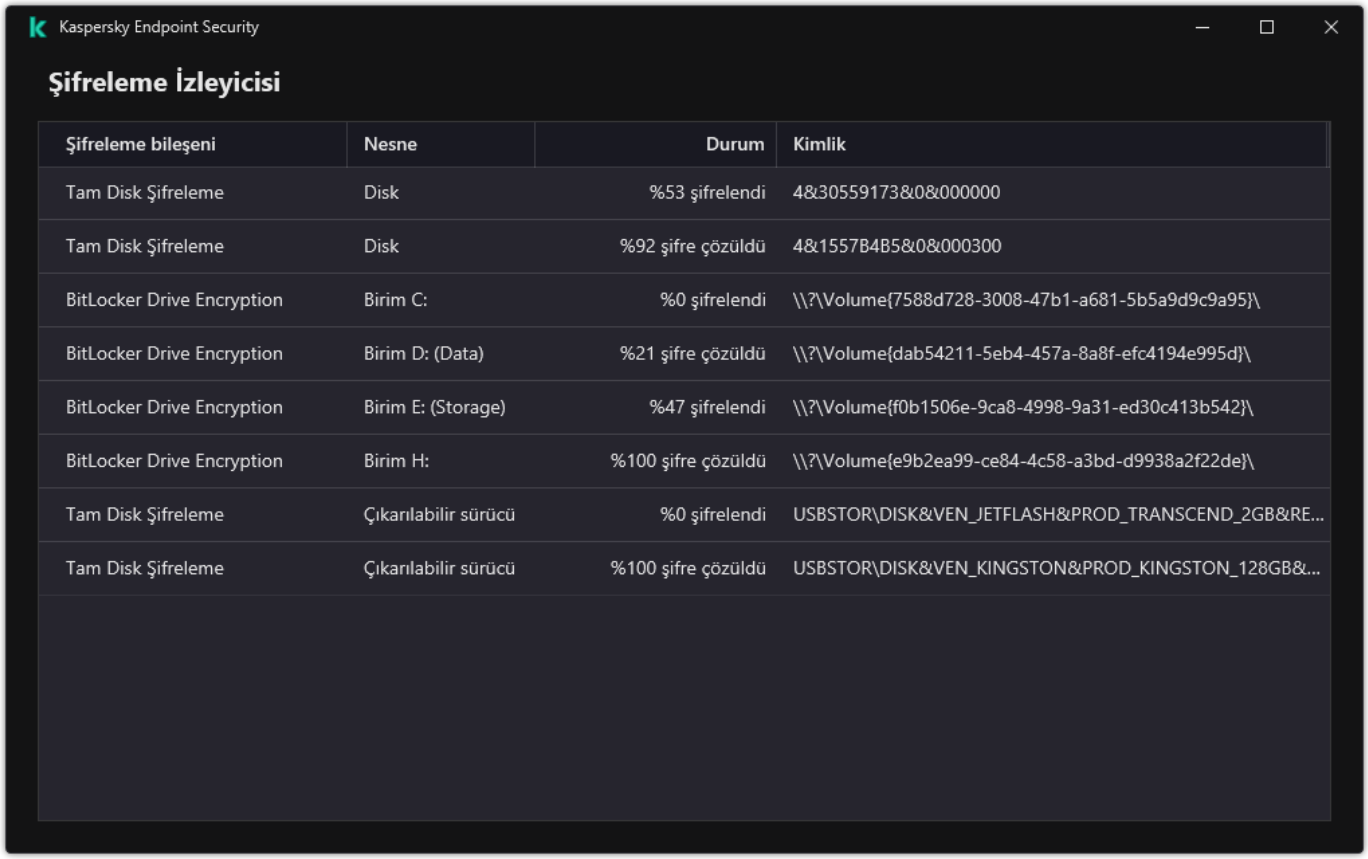
6. Aşağıdakilerden birini yapın:

   - **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.

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

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.

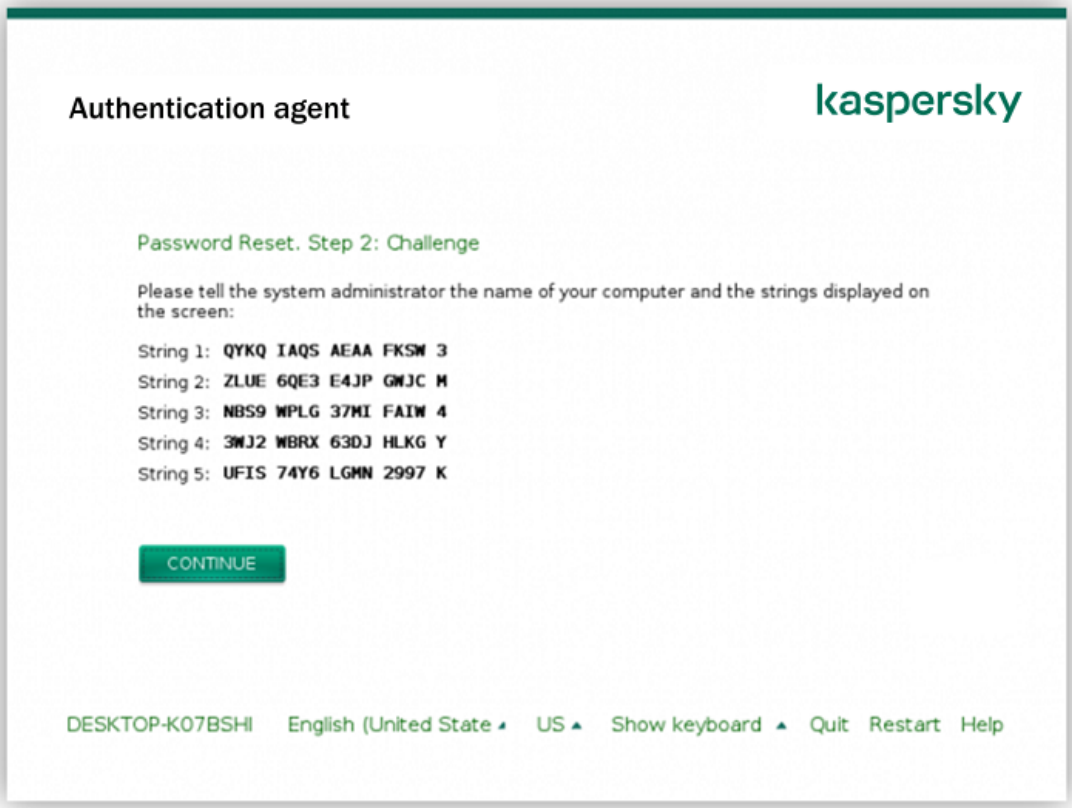
Kaspersky Disk Encryption teknolojisi tarafından korunan bir sürücüye yeniden erişim sağlamak

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 **Forgot your password** 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. Açılan pencerede, **Kimlik Doğrulama Aracısı** sekmesini seçin.

6. **Kullanılmakta olan şifreleme algoritması** bloğundan bir şifreleme algoritması seçin: **AES56** veya **AES256**.

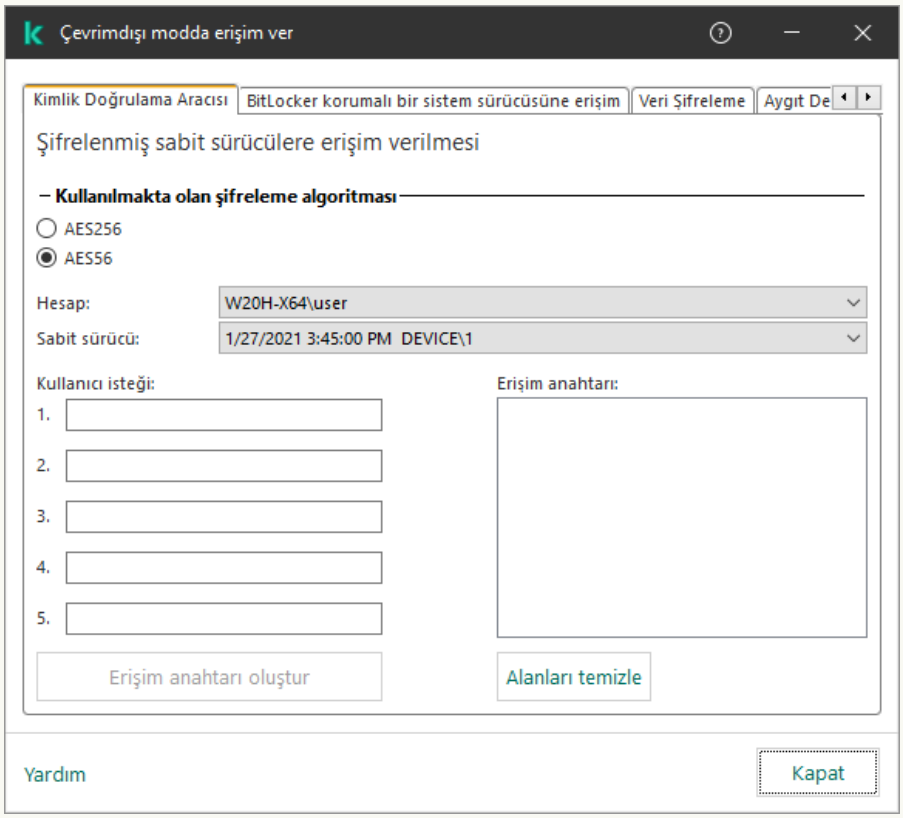
   Veri şifreleme algoritması, dağıtım paketine dahil olan AES şifreleme kitaplığına bağlıdır: *Güçlü şifreleme (AES256)* veya *Hafif şifreleme (AES56)*. AES şifreleme kitaplığı uygulama ile birlikte yüklenir.

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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.

2. Sürücüsüne tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.

3. **Cihaza çevrimdışı modda erişim izni ver** düğmesine 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:

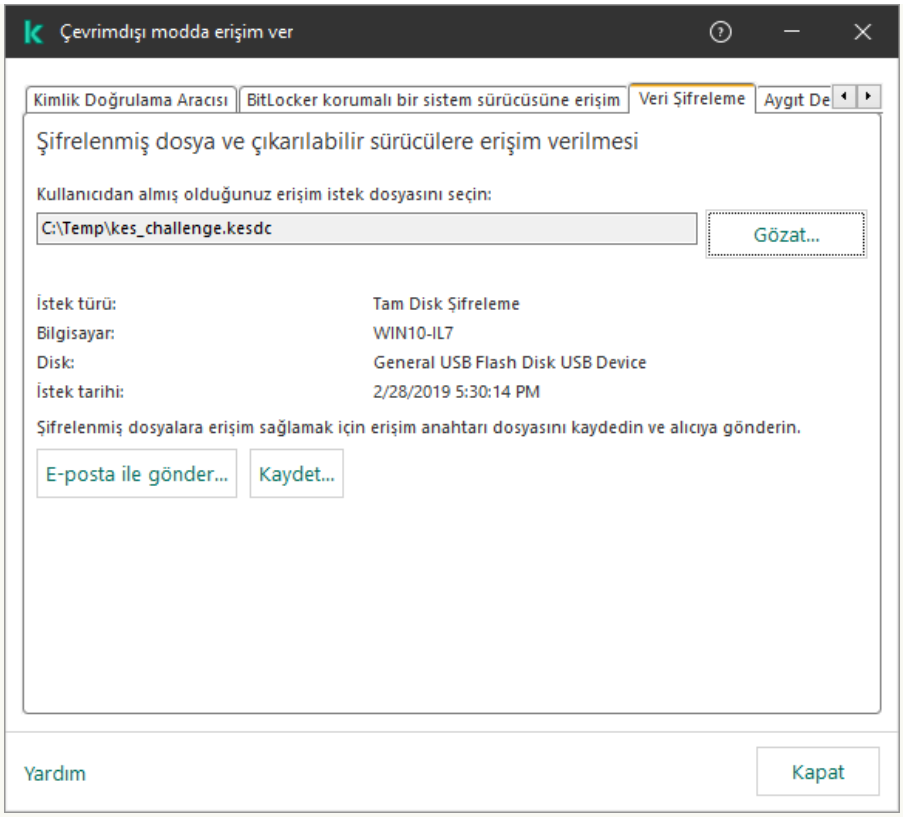
1. Kullanıcı yöneticiye bir istek erişim dosyası gönderir.
2. Yönetici istek erişim dosyasını Kaspersky Security Center'a ekler, bir istek erişim dosyası oluşturur ve bu dosyayı kullanıcıya gönderir.
3. Kullanıcı erişim anahtarını Kaspersky Endpoint Security'ye ekler ve sabit sürücüye erişim elde eder.

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. Açılan 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
2. Verilerine tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.
3. **Cihaza çevrimdışı modda erişim izni ver** düğmesine 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 (KESDC 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
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 sistemini güvenli bir şekilde güncelleme hakkında ayrıntılar için lütfen Teknik Destek Bilgi Bankası 'na başvurun.

İşletim sisteminin otomatik güncellenmesi aşağıdaki koşullarda kullanılabilir:

1. İşletim sistemi WSUS (Windows Server Update Services) ile güncellenmiştir.

2. Bilgisayarda Windows 10 sürüm 1607 (RS1) veya üzeri yüklüdür.

3. Bilgisayarda Kaspersky Endpoint Security sürüm 11.2.0 veya üzeri yüklü ise.

Tüm koşullar yerine getirilirse işletim sistemini her zamanki gibi güncelleyebilirsiniz.

Kaspersky Disk Encryption (FDE) teknolojisini kullanıyorsanız ve bilgisayarda Kaspersky Endpoint Security for Windows 11.1.0 veya 11.1.1 sürümü yüklüyse, Windows 10'u güncellemek için sabit sürücülerin şifresini çözmenize gerek yoktur.

İşletim sistemini güncellemek için şunları yapmanız gerekir:

1. Sistemi güncellemeden önce cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf ve klfdefsf.sys adlı sürücüleri yerel bir klasöre kopyalayın. Örneğin, C:\fde_drivers.

2. Sistem güncelleme kurulumunu `/ReflectDrivers` anahtarıyla çalıştırın ve kaydedilen sürücüleri içeren klasörü belirtin:

   ```
   setup.exe /ReflectDrivers C:\fde_drivers
   ```

BitLocker Drive Encryption teknolojisini kullanıyorsanız Windows 10'u güncellemek için sabit sürücülerin şifresini çözmenize gerek yoktur. BitLocker hakkında daha ayrıntılı bilgi için lütfen *Microsoft İnternet sitesini* ziyaret edin.

Şifreleme işlevselliğini güncelleme hatalarını ortadan kaldırma

Tam Disk Şifreleme, uygulamanın önceki bir sürümü Kaspersky Endpoint Security for Windows 12.1 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 Aracısı izleme düzeyini seçme

Uygulama, Kimlik Doğrulama Aracısı'nın işlemleri hakkında hizmet bilgisini ve Kimlik Doğrulama Aracısı ile kullanıcının yaptığı işlemler hakkındaki bilgiyi izleme dosyasına kaydeder.

Kimlik Doğrulama Aracısı izleme düzeyini seçmek için:

1. Şifrelenmiş sabit sürücüye sahip bir bilgisayar açılır açılmaz Kimlik Doğrulama Aracısı ayarlarını yapılandırmak amacıyla pencere açmak için **F3** tuşuna basın.

2. Kimlik Doğrulama Aracısı ayarları penceresinden izleme düzeyini seçin:

   - **Disable debug logging (default)**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı olayları hakkında izleme dosyasına bilgi kaydetmez.

- **Enable debug logging**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgileri izleme dosyasına kaydeder.
- **Enable verbose logging**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki ayrıntılı bilgilerin günlüğünü izleme dosyasında tutar.

  Enable debug logging seçeneğinin düzeyi ile karşılaştırıldığında bu seçenek altındaki giriş ayrıntılarının düzeyi daha yüksektir. Yüksek düzeyde giriş ayrıntıları Kimlik Doğrulama Aracısı ve işletim sisteminin açılışını yavaşlatabilir.

- **Enable debug logging and select serial port**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgilerin günlüğünü izleme dosyasında tutar ve bunu COM bağlantı noktası üzerinden aktarır.

  Şifrelenmiş sabit sürücülü bir bilgisayar COM bağlantı noktası üzerinden başka bir bilgisayara bağlanırsa Kimlik Doğrulama Aracısı olayları söz konusu diğer bilgisayardan incelenebilir.

- **Enable verbose debug logging and select serial port**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgilerin ayrıntılı günlüğünü izleme dosyasında tutar ve bunu COM bağlantı noktası üzerinden aktarır.

  Enable debug logging and select serial port seçeneğinin düzeyi ile karşılaştırıldığında bu seçenek altındaki giriş ayrıntılarının düzeyi daha yüksektir. Yüksek düzeyde giriş ayrıntıları Kimlik Doğrulama Aracısı ve işletim sisteminin açılışını yavaşlatabilir.

Bilgisayarda şifrelenmiş sabit sürücüler varsa veya tam disk şifreleme sırasında, veriler Kimlik Doğrulama Aracısı izleme dosyasına kaydedilir.

Uygulamanın diğer iz dosyalarından farklı olarak Kimlik Doğrulama Aracısı iz dosyası Kaspersky'ye gönderilmez. Gerekirse Kimlik Doğrulama Aracısı iz dosyasını analiz için Kaspersky'ye elle gönderebilirsiniz.

Kimlik Doğrulama Aracısı 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Ortak şifreleme ayarları** seçimini yapın.
5. **Şablonlar** bloğunda, **Yardım** düğmesine tıklayın.
6. 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.
7. 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.

8. 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.

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 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 Security Center'ı kullanarak BitLocker'ı kontrol etmenize ve yönetmenize izin verir. BitLocker mantıksal birimleri şifreler. BitLocker, çıkarılabilir sürücülerin şifrelenmesi için kullanılamaz. BitLocker hakkında daha ayrıntılı bilgi için Microsoft belgelerine bakın.

BitLocker, bir güvenilir platform modülü kullanarak erişim anahtarlarının güvenli bir şekilde depolanmasını sağlar. *Güvenilir Platform Modülü (TPM)* güvenlikle ilgili temel işlevleri sunmak (örneğin şifreleme anahtarını saklamak) için 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.

Bir sürücüyü şifreledikten sonra, BitLocker bir ana anahtar oluşturur. Kaspersky Endpoint Security, ana anahtarı Kaspersky Security Center'a gönderir, böylece mesela bir kullanıcı parolasını unuttuysa diske erişimi geri yükleyebilirsiniz.

Bir kullanıcı diski BitLocker kullanarak şifrelediğinde, Kaspersky Endpoint Security disk şifrelemeyle ilgili bilgileri Kaspersky Security Center'a gönderir. Ancak Kaspersky Endpoint Security, ana anahtarı Kaspersky Security Center'a göndermez. Bu nedenle Kaspersky Security Center kullanılarak diske erişimin geri yüklenmesi mümkün değildir. BitLocker'ın Kaspersky Security Center ile düzgün bir şekilde çalışabilmesi için bir ilke kullanarak sürücünün şifresini çözün ve sonra tekrar şifreleyin. Bir sürücünün şifresini yerel olarak ya da bir ilke kullanarak çözebilirsiniz.

Sistem sabit sürücüsünü şifreledikten sonra, işlem sistemini önyüklemek için kullanıcının BitLocker kimlik doğrulamasını gerçekleştirmesi gerekir. Kimlik doğrulama prosedüründen sonra, BitLocker kullanıcıların giriş yapmasına izin verecektir. BitLocker çoklu oturum açma (SSO) desteği sunmaz.

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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Tam Disk Şifreleme** seçimini yapın.
5. **Şifreleme teknolojisi** açılır listesinde **BitLocker Drive Encryption** öğesini seçin.
6. **Şifreleme modu** açılır listesinden **Tüm sabit sürücüleri şifrele** seçeneğini seçin.

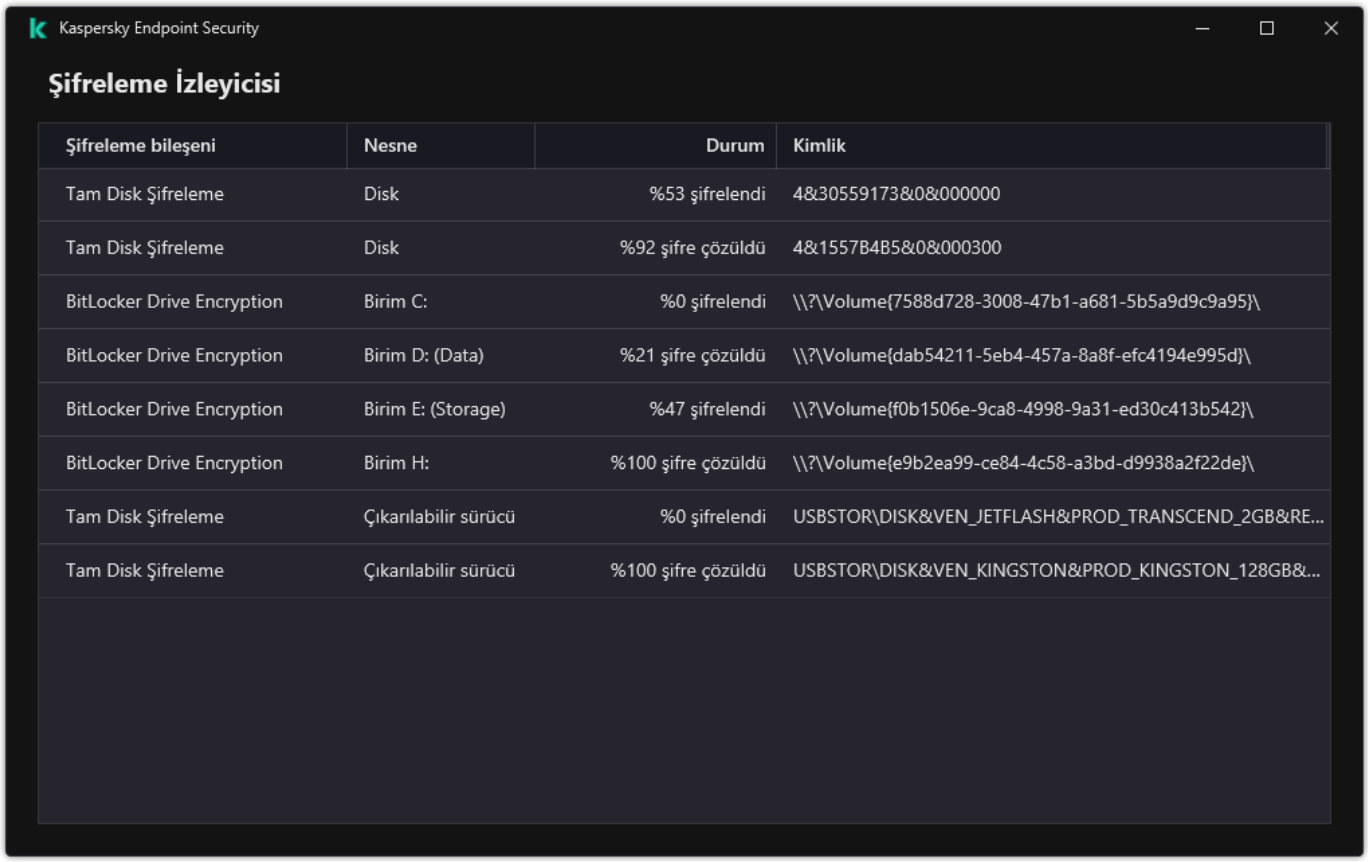
   Bilgisayarda birkaç işletim sistemi yüklüyse şifreleme işleminden sonra yalnızca şifreleme işleminin gerçekleştirildiği işletim sistemini yükleyebilirsiniz.
7. Gelişmiş BitLocker Drive Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
8. Değişikliklerinizi kaydedin.

BitLocker Drive Encryption bileşeni Web Console ve Cloud Console üzerinden nasıl çalıştırılır

1. Web Console'un ana penceresinde **Aygıtlar → İlkeler ve Profiller**'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. **Şifrelemeyi yönet** bloğunda, **BitLocker Drive Encryption** seçeneğini belirleyin.
6. **BitLocker Drive Encryption** bağlantısına tıklayın.
   BitLocker Drive Encryption ayarları penceresi açılır.
7. **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.
8. Gelişmiş BitLocker Drive Encryption seçeneklerini yapılandırın (aşağıdaki tabloya bakın).
9. 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	Bu onay kutusu, platform önyükleme girişi özelliğine sahip değilse bile (örneğin tabletlerdeki dokunmatik ekran klavyeleri ile), bir önyükleme ortamında veri girişini gerektiren kimlik doğrulama kullanımını etkinleştirir/devre dışı bırakır. 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 klavyesi gibi bir önyükleme ortamında alternatif veri girişi araçlarına sahip aygıtlar 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 artırmanıza ve daha az bilgisayar kaynağı kullanmanıza olanak tanır.

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, bu onay kutusu işaretlenmemiştir.

Kimlik doğrulama yöntemi

Parola kullan (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.

Güvenilir Platform Modülü (TPM) güvenlikle ilgili temel işlevleri sunmak (örneğin şifreleme anahtarını saklamak) için 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.

Kullanıcının genişletilmiş PIN'i kullanmasına izin verebilirsiniz. *Genişletilmiş PIN* sayısal karakterlere ek olarak büyük ve küçük Latin harfleri, özel karakterler ve boşluklar gibi diğer karakterlerin kullanılmasına da izin verir.

- **Güvenilir platform modülü (TPM) veya TPM kullanılamıyorsa parola**. Onay kutusu seçilirse, bir Güvenilir Platform Modülü (TPM) kullanılamadığında, kullanıcı şifreleme anahtarlarına erişmek için bir parola kullanabilir.

  Bu onay kutusu işaretlenmemişse ve TPM kullanılabilir değilse, tam disk şifreleme başlamaz.

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.

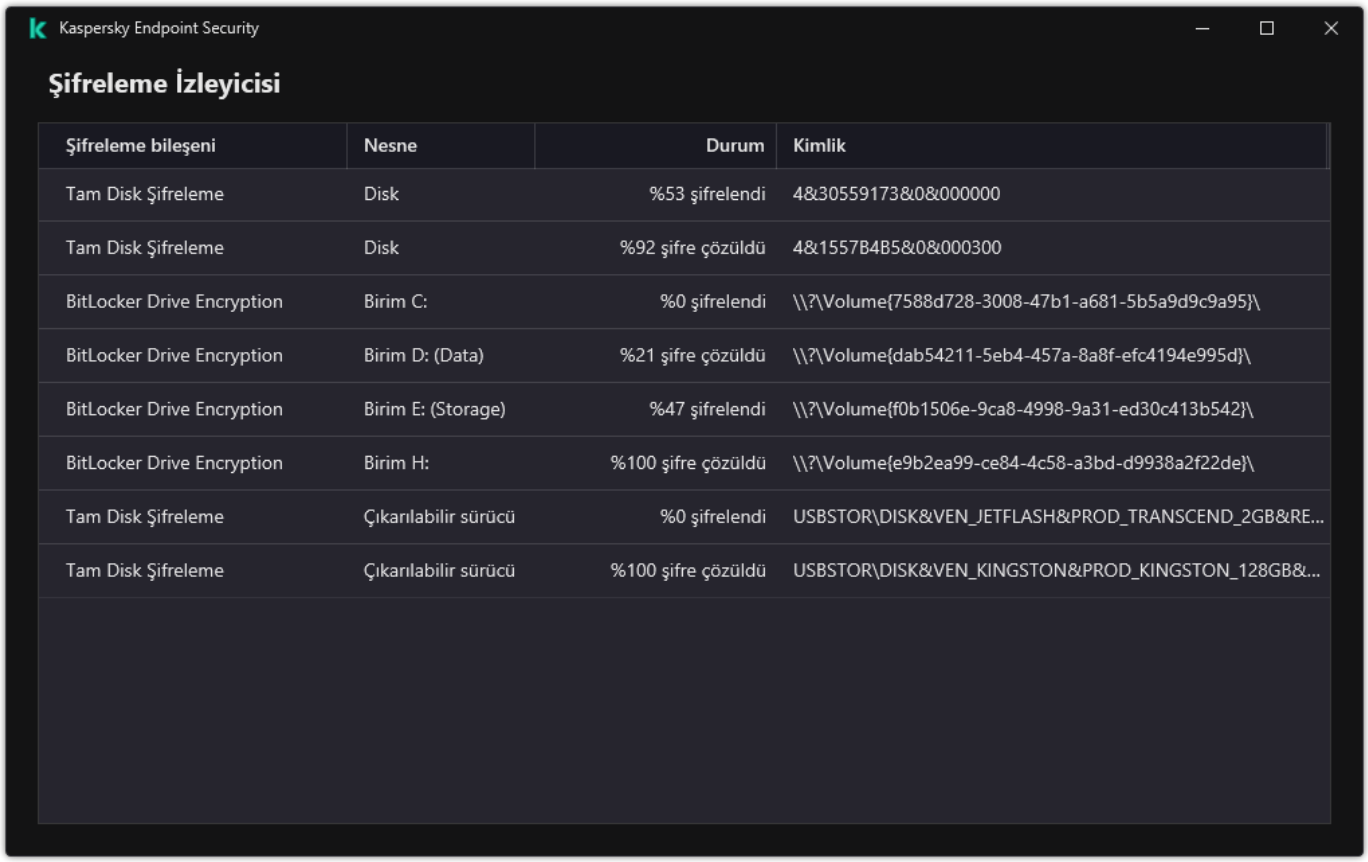
BitLocker tarafından korunan bir sürücünün şifresi Yönetim Konsolu (MMC) kullanılarak nasıl çözülür

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Tam Disk Şifreleme** seçimini yapın.
5. **Şifreleme teknolojisi** açılır listesinde **BitLocker Drive Encryption** öğesini seçin.
6. **Şifreleme modu** açılır listesinden **Tüm sabit sürücülerin şifresini çöz** seçeneğini seçin.
7. Değişikliklerinizi kaydedin.

BitLocker ile şifrelenmiş bir sabit sürücünün şifresini Web Console ve Cloud Console aracılığıyla çözme

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 Drive Encryption** teknolojisini seçin ve ayarları yapılandırmak için bağlantıyı takip edin.
   Şifreleme ayarları açılır.
6. **Şifreleme modu** açılır listesinden **Tüm sabit sürücülerin şifresini çöz** seçeneğini 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:

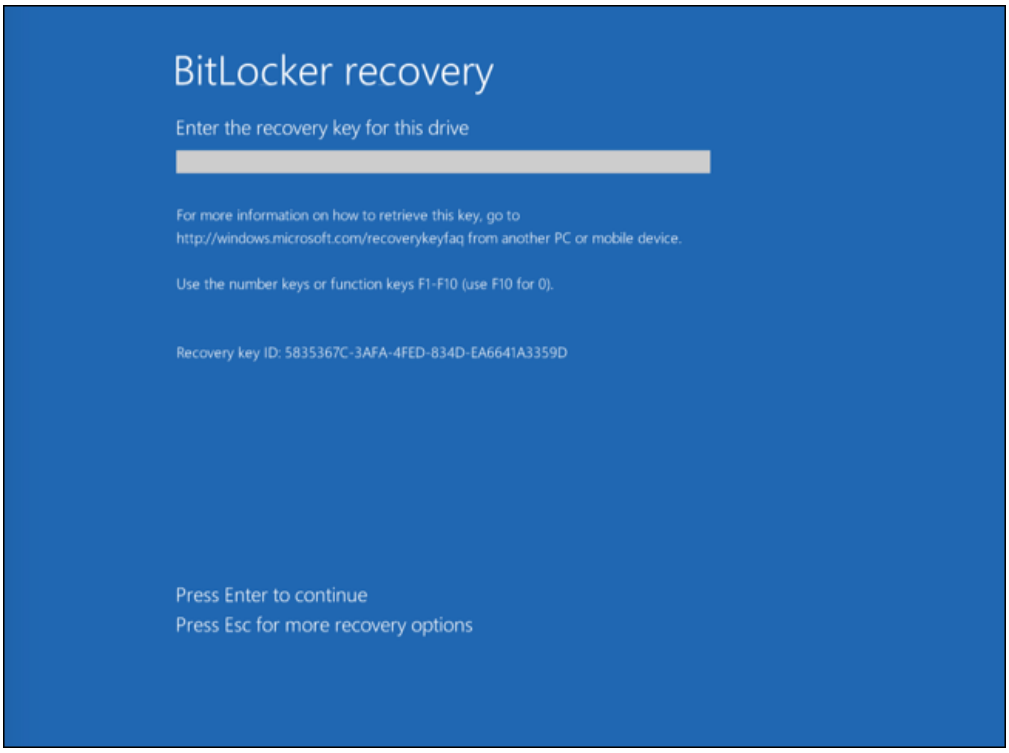
1. Kullanıcı, yöneticiye kurtarma anahtarı kimliğini söyler (aşağıdaki şekle bakın).
2. Yönetici, kurtarma anahtarının kimliğini, Kaspersky Security Center'ın bilgisayar özelliklerinde doğrular. Kullanıcının sunduğu kimlik ile bilgisayar özelliklerinde görüntülenen kimlik eşleşmelidir.
3. Kurtarma anahtarı 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.

4. Kullanıcılar kurtarma anahtarını girerek sabit sürücüye erişim kazanır.



BitLocker tarafından şifrelenen bir sabit sürücüye erişimi geri yükleme

Bir sistem sürücüsüne yeniden erişim

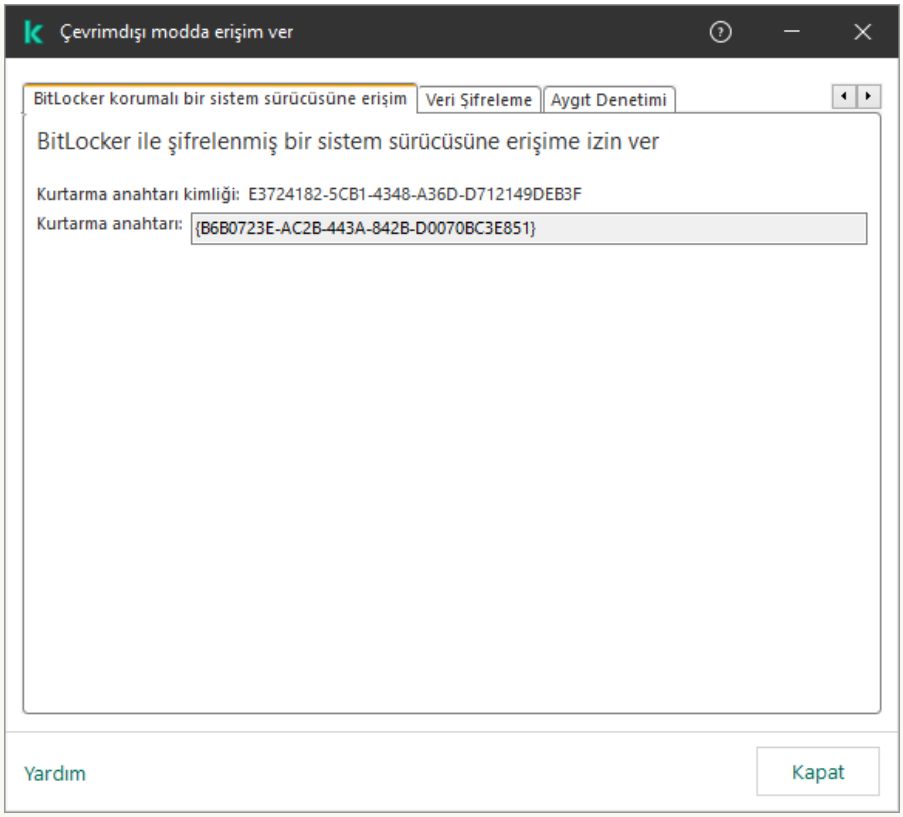
Kurtarma prosedürünü başlatmak için kullanıcının önyükleme kimlik doğrulaması aşamasında **Esc** tuşuna basması gerekir.

[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: **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. Açılan pencerede **BitLocker korumalı bir 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
2. Sürücüsüne tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.
3. **Cihaza çevrimdışı modda erişim izni ver** düğmesine 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 ana anahtar 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

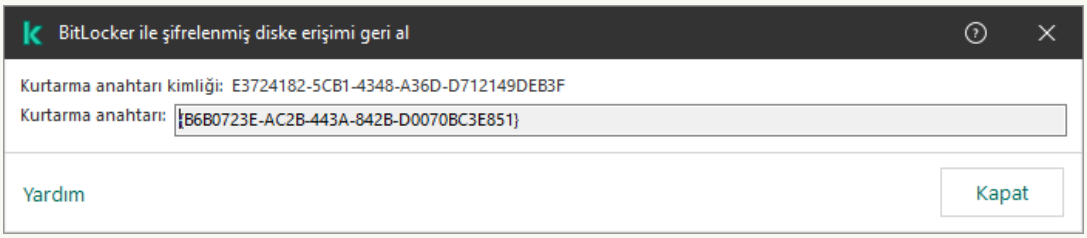
Kurtarma prosedürünü başlatmak için kullanıcının, sürücüye erişim sağlayan penceredeki **Forgot your password** düğmesine tıklaması gerekir. Şifrelenmiş sürücüye erişim kazandıktan sonra kullanıcı, BitLocker ayarlarından, Windows kimliklik doğrulaması sırasında sürücünün kilidinin otomatik olarak kaldırılmasını 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 for Windows'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** düğmesine 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. Yönetim Konsolu'ndan **Yönetim Sunucusu** → **Görevler** klasörüne gidin.

   Görevler listesi açılır.

2. **Yeni görev** düğmesine tıklayın.

Görev Sihirbazı başlatılır. Sihirbazın talimatlarını uygulayın.

1. Adım. Görev türünü seçme

Kaspersky Endpoint Security for Windows (12.1) → **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 elle 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

Sihirbazdan çıkın. 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 **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine 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 (12.1)** 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 cihazları seçin** 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

Sihirbazdan çıkın. 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 konsolundaki bilgisayar özelliklerinde de öğrenebilirsiniz.

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

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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme** seçimini yapın.
5. **Şifreleme modu** açılır listesinden **Kurallara göre** seçimini yapın.
6. **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 elle 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.

7. 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

Uygulamalar için şifrelenmiş dosyaya erişim kuralları oluşturmak amacıyla:

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 **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme** seçimini yapın.
5. **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.

6. Pencerenin sağ kısmında, **Uygulamalar için kurallar** sekmesini seçin.
7. 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.
8. Uygulamaları elle 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.
9. 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Dosya Düzeyinde Şifreleme** seçimini yapın.
5. **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.

6. Pencerenin sağ kısmında, **Uygulamalar için kurallar** sekmesini seçin.
7. 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.
8. Uygulamaları elle 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.
9. Değişikliklerinizi kaydedin.

Şifre çözme kuralı oluşturma

Bir şifre çözme kuralı oluşturmak için:

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 **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme** seçimini yapın.
5. **Şifreleme modu** açılır listesinden **Kurallara göre** seçimini yapın.
6. **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 elle 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.

7. 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Dosya Düzeyinde Şifreleme** seçimini yapın.
5. Pencerenin sağ kısmında, **Şifreleme** sekmesini seçin.
6. Şifresini çözmek istediğiniz dosya ve klasörleri şifreleme listesinden kaldırın. Bunun için dosyaları seçin ve **Kaldır** düğmesinin bağlam menüsündeki **Kuralı silin ve dosyaların şifresini çözün** öğesini seçin.

   Şifreleme listesinden kaldırılan dosya ve klasörler otomatik olarak şifre çözme listesine eklenir.
7. Dosya şifre çözme listesi oluşturma.
8. 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.

4. İlke penceresinden **Veri Şifreleme** → **Ortak şifreleme ayarları** seçimini yapın.
5. **Parola ayarları** bloğunda **Ayarlar** düğmesine tıklayın.
6. Açılan pencerede, **Şifrelenmiş paketler** sekmesini seçin.
7. Şifrelenmiş paketleri oluştururken parola karmaşıklığı ayarlarını yapılandırın.

Web Console'da yeni bir şifrelenmiş paket oluştururken parola güvenliği denetimi nasıl etkinleştirilir

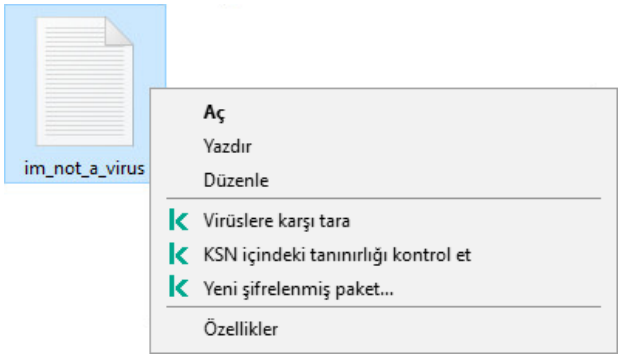
1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Dosya Düzeyinde Şifreleme**'ye gidin.
5. **Şifrelenmiş paket parola ayarları** bloğunda, şifrelenmiş paketler oluştururken gerekli olan parola gücü ölçütlerini yapılandırın.

Dosya 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.

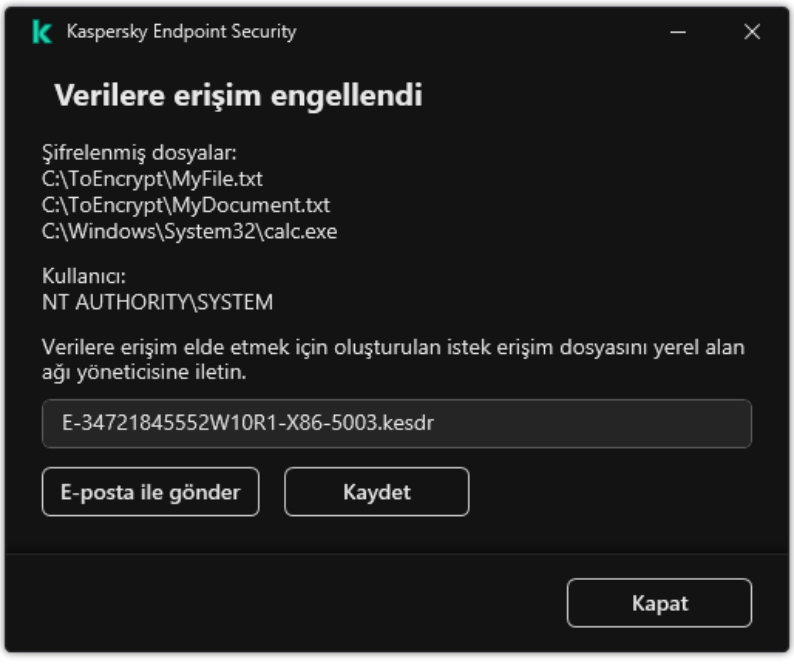
  Kullanıcı, şifrelenmiş dosyalarla aşağıdaki durumlarda çalışabilir:

  - 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

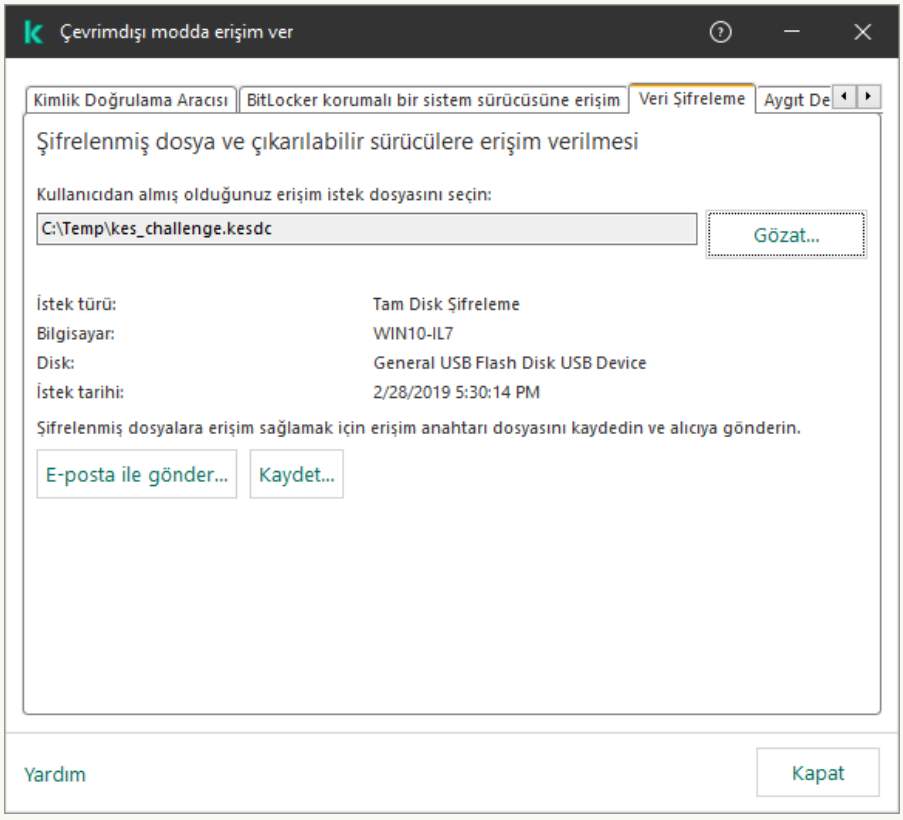
Kurtarma prosedürünü başlatmak için kullanıcının bir dosyaya erişim girişiminde bulunması gerekir. Sonuç olarak, Kaspersky Endpoint Security bir istek erişim dosyası oluşturur (KESDC uzantılı bir dosya) ve kullanıcının bu dosyayı yöneticiye göndermesi gerekir, örneğin e-posta ile.

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. Açılan 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
2. Verilerine tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.
3. **Cihaza çevrimdışı modda erişim izni ver** düğmesine 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 (KESDC 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.

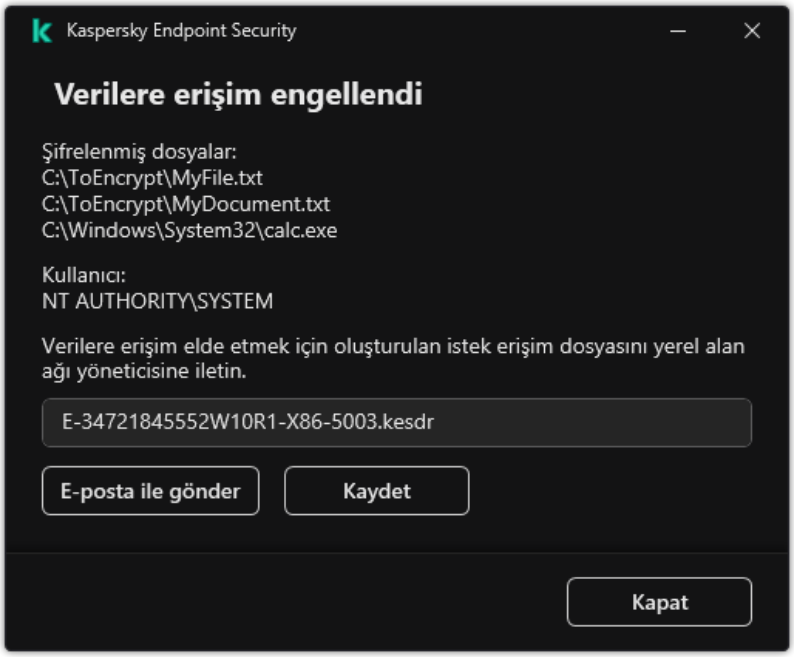
Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenleme

Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenlemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Ortak şifreleme ayarları** seçimini yapın.
5. **Şablonlar** bloğunda, **Şablonlar** düğmesine tıklayın.
6. 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.

7. Mesaj şablonlarını düzenleyin.

8. Değişikliklerinizi kaydedin.



Şifrelenmiş dosyalara yeniden erişim sağlama

Çıkarılabilir sürücüleri şifreleme

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:

- Tam Disk Şifreleme (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.

- Dosya Düzeyinde Şifreleme (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, FAT32 ve NTFS dosya sistemlerinde şifrelemeyi destekler. Bilgisayara, desteklenmeyen bir dosya sistemine sahip çıkarılabilir sürücü bağlandıysa, çıkarılabilir sürücü şifrelemesi bir hata ile sonlanır ve Kaspersky Endpoint Security çıkartılabilir sürücüye salt okunur erişimi 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
5. **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.
6. 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.
7. 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.
8. Çıkarılabilir sürücüler için şifrelemeyi teker teker yapılandırmak isterseniz şifreleme kuralları tanımayın.
9. 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.
10. 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).

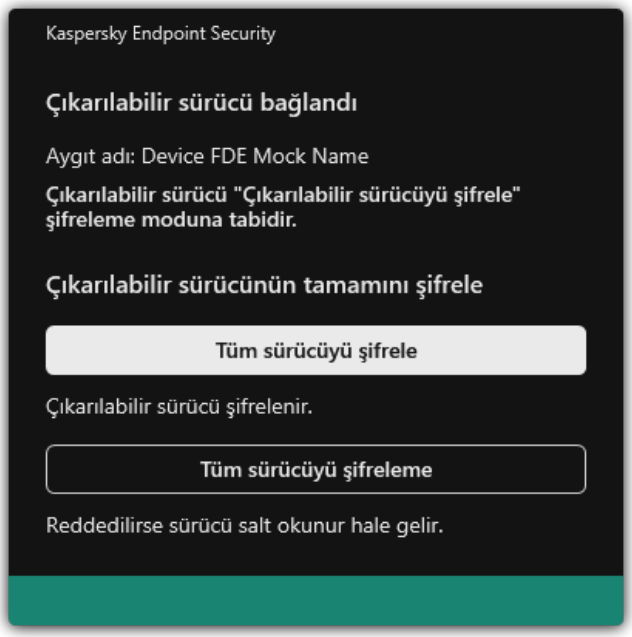
Uygulama şu işlemleri gerçekleştirmenize izin verir:

- 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
5. **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.
6. **Seçili aygıtlar için şifreleme modu** açılır listesinde, Kaspersky Endpoint Security tarafından seçilen çıkarılabilir sürücülerde kayıtlı dosyalara uygulanacak eylemi seçin.
7. 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.

8. Kaspersky Endpoint Security'nin sadece dosyalar tarafından kullanılan disk sektörlerini şifrelemesini istiyorsanız **Sadece kullanılan disk alanını şifrele** onay kutusunu seçin.

   Şifrelemeyi zaten kullanımda olan bir sürücüye uyguluyorsanız, tüm sürücünün şifrelenmesi önerilir. Böylece, hala kurtarılabilir bilgi içeren silinmiş veriler dahil tüm veriler korunur. **Sadece kullanılan disk alanını şifrele** işlevi, daha önce kullanılmamış yeni sürücüler için önerilir.

   > Bir aygıt daha önce **Sadece kullanılan disk alanını şifrele** işlevini kullanarak şifrelendiyse **Çıkarılabilir sürücünün tamamını şifrele** modunda bir ilke uygulandıktan sonra, dosyalar tarafından kullanılmayan sektörler yine de şifrelenmez.

9. **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.

10. 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. 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 **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
5. Çıkarılabilir sürücüler için şifreleme kuralları listesini dışa aktarmak için:
   a. Düzenlemek istediğiniz kuralları seçin. Birden fazla bağlantı noktası 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.
6. 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.

7. Değişikliklerinizi kaydedin.

Çıkarılabilir sürücü şifreleme kurallarının bir listesini Web Console'da dışa ve içe aktarma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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 aygıtlar için şifreleme kuralları** bloğunda, **Şifreleme 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.

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:

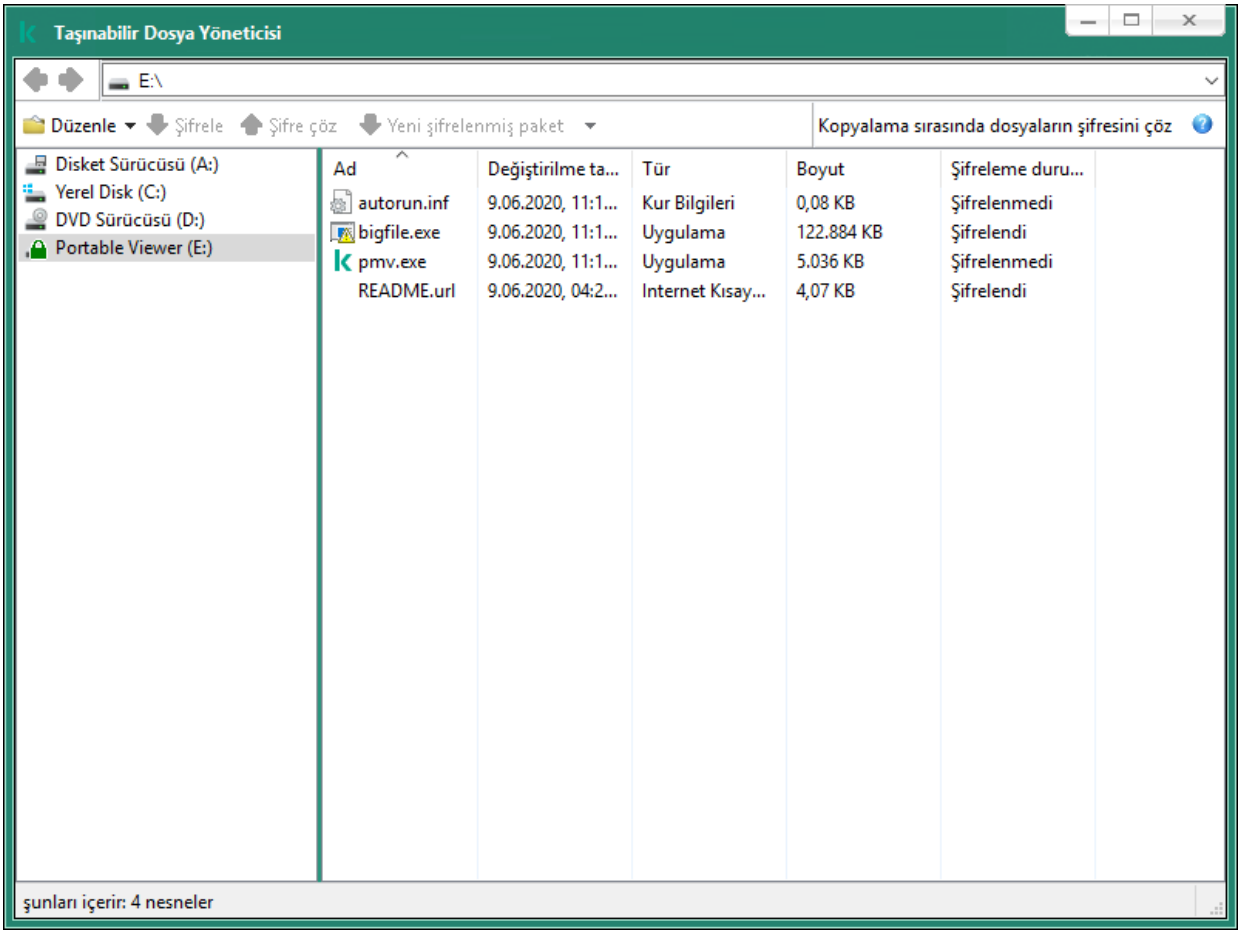
- Bilgisayar ile Kaspersky Security Center Yönetim Sunucusu arasında bağlantı olmadığında.
- Kaspersky Security Center Yönetim Sunucusunun değişimi ile altyapı değiştiğinde.
- Kaspersky Endpoint Security bilgisayarda yüklü olmadığında.

Taşınabilir Dosya Yöneticisi

Taşınabilir modda çalışmak için Kaspersky Endpoint 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

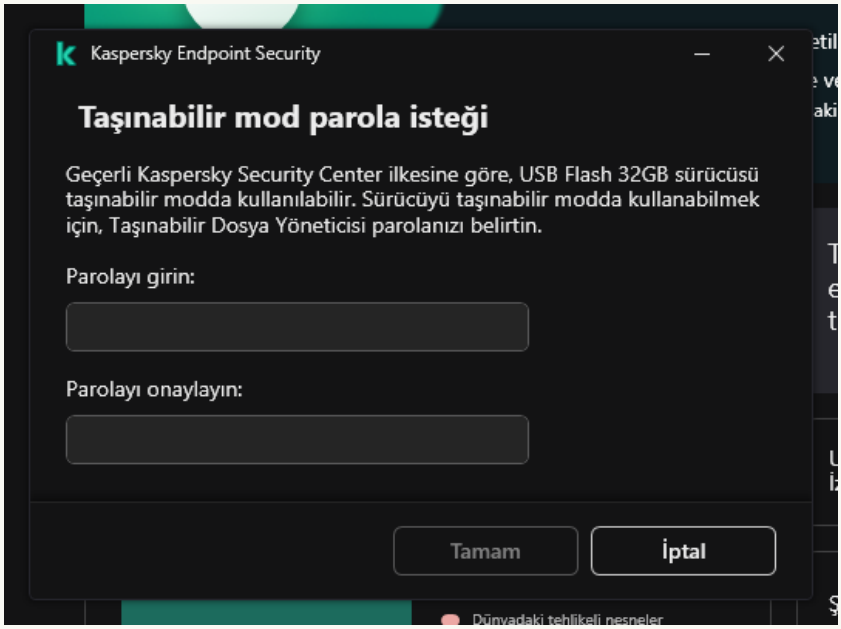
[Yönetim Konsolu'nda (MMC) çıkarılabilir sürücüler üzerindeki şifrelenmiş dosyalarla çalışmak için taşınabilir mod desteği nasıl etkinleştirilir](#)

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
5. **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.

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 talebi

11. Güç gereksinimlerini karşılayan bir şifre belirleyin ve onaylayın.
12. Değişikliklerinizi kaydedin.

Web Console'da çıkarılabilir sürücüler üzerindeki şifrelenmiş dosyalarla çalışırken taşınabilir mod desteği nasıl etkinleştirilir

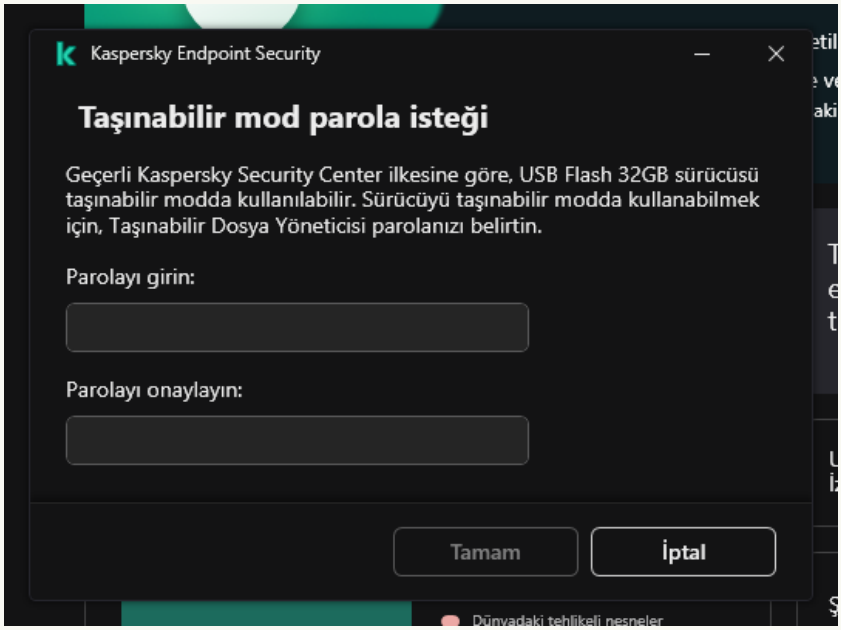
1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Veri Şifreleme** → **Çıkarılabilir sürücüleri şifreleme** seçimini yapın.
5. **Şifrelemeyi yönet** 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 talebi

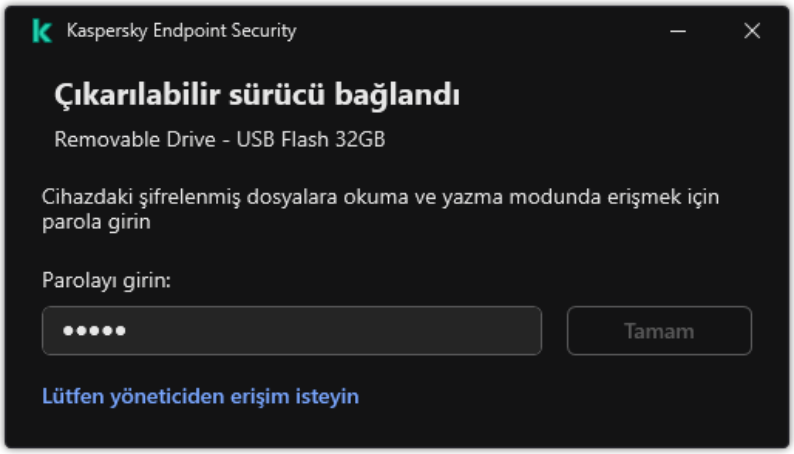
11. Güç gereksinimlerini karşılayan bir şifre belirleyin ve onaylayın.
12. Değişikliklerinizi kaydedin.

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.

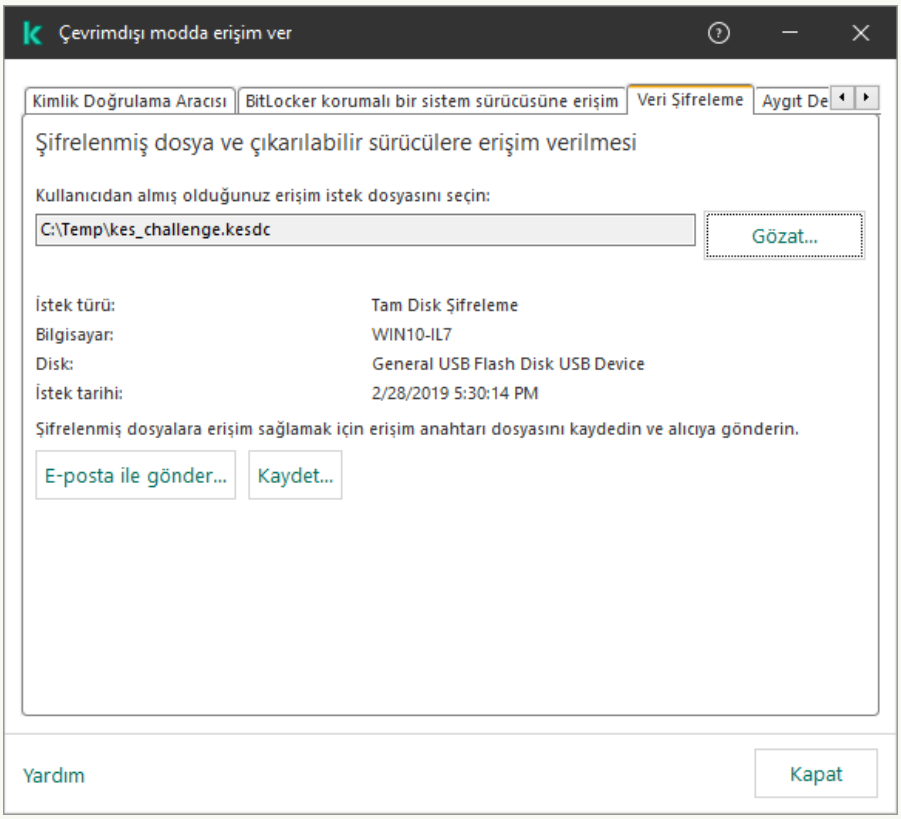
4. İçerik menüsünde **Çevrimdışı modda erişim ver** seçeneğini belirleyin.

5. Açılan 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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.

2. Verilerine tekrar erişim sağlamak istediğiniz bilgisayarın adının yanındaki onay kutusunu işaretleyin.

3. **Cihaza çevrimdışı modda erişim izni ver** düğmesine 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 (KESDC 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinden **Veri Şifreleme → Çıkarılabilir sürücüleri şifreleme** seçimlerini yapın.
5. Çıkarılabilir sürücülerde kayıtlı tüm şifrelenmiş dosyaların şifresini çözmek isterseniz, **Şifreleme modu** açılır listesinde **Çıkarılabilir sürücünün tamamının şifresini çöz** seçeneğini seçin.
6. 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**'e tıklayın.
7. 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.
- **Toplu depolama cihazlarının şifreleme durumu hakkındaki raporu görüntüle**. 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

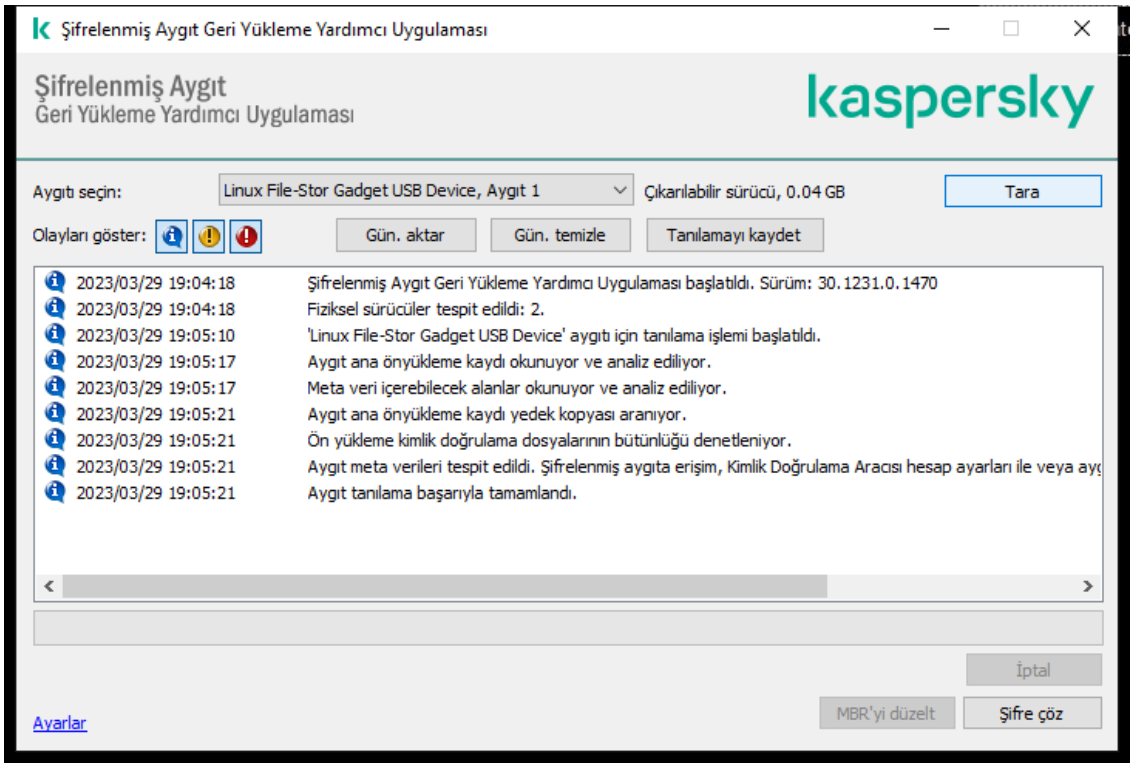
Sabit sürücüde arıza olursa sistem çökebilir. Böyle bir durumda, Kaspersky Disk Encryption teknolojisi tarafından korunan veriler kullanılamaz. Verilerin şifresini çözüp onları yeni bir sürücüye kopyalayabilirsiniz.

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 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 elle 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 for Windows'da aygıta erişim al**'a tıklayın.

   Erişim isteği dosyasının hangi bilgisayar için oluşturulduğundan emin değilseniz Yönetim Konsolu ağacında, **Diğer → Veri şifreleme ve koruma** klasörünü seçin ve çalışma alanında **Kaspersky Endpoint Security for Windows'da aygıt şifreleme anahtarı 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. **Aç** düğmesine 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** düğmesine 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. **Dosya seç**in düğmesine tıklayın ve kullanıcıdan gelen istek erişim dosyasını (FDERTC uzantılı bir dosya) seçin.

   d. **Anahtarı kaydet** düğmesine tıklayın ve şifrelenmiş verilere erişim için anahtar dosyasının (FDERTR uzantılı bir dosya) kaydedileceği 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 Endpoint Security, Detection and Response çözümlerini yerleşik bir aracı kullanarak destekler. Detection and Response bileşenini kullanmak için uygulamayı yüklerken bu çözümlerle entegrasyonu etkinleştirmeniz gerekir. 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 bileşeni;
- Kaspersky Sandbox 2.0.

Kaspersky Endpoint Security'yi, Detection and Response çözümü ile birlikte farklı yapılandırmalarda kullanabilirsiniz, örneğin [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

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 Endpoint Detection and Response Expert 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.

Detection and Response çözümlerini yönetmek için bütünleşik aracıyı dağıtma

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)
11.5.0	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
11.7.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent
11.9.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent
11.10.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent
11.11.0	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent
12	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	Kaspersky Endpoint Agent
12.1	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**	**Bütünleşik aracı**

Kaspersky Endpoint Agent için İlke ve Görev Geçişi

Kaspersky Endpoint Security for Windows, 11.7.0 sürümünden itibaren 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 (EDR)

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 İlke 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'yi seçmek için bir 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

Sihirbazdan çıkın. 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 Merkezi Düğüm sunucularına bağlana sırasında hatalarla karşılaşabilirsiniz. Bunun nedeni, Web Console geçiş sihirbazının şu ilke ayarlarını atlaması ve bunları geçirmemesidir:

  - Ayarlar değişiklik yasağı **KATA sunucularına bağlanmak için ayarlar** ("kilit").

    Varsayılan olarak ayarlar değiştirilebilir ("kilit" açıktır). Bu nedenle ayarlar bilgisayarda uygulanmaz. Ayarların değiştirilmesi yasaklanmalı ve "kilit" kapatılmalıdır.

  - Kripto konteyneri.

    Merkezi Düğüm 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.

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 Bildirimini 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

Sihirbazdan çıkın. Sihirbazın sonucunda yeni bir Kaspersky Endpoint Security ilkesi oluşturulacaktır.

[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 kaldırılır.

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 Yönetim 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 (KATA EDR)'yi kullanmak için Kaspersky Endpoint Security sürüm 12.1 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 Beyanını 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 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 Optimum 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).

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 Yönetim Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
   - *Uygulama bileşenleri durum raporunu* görüntüleyerek yerleşik aracının çalışma durumunu kontrol edin. Bir bileşenin durumu *Yüklenmedi* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin.
   - Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Beyanını kabul ettiğinizden emin olun.
   - *Uygulama bileşenleri durum raporunu* kullanarak EDR Optimum işlevinin etkinleştirildiğinden emin olun. Bir bileşen *Lisans kapsamında değil* durumuna sahipse, EDR Optimum'un otomatik lisans anahtarı dağıtım işlevinin açık olduğundan emin olun.

Managed Detection and Response

11.6.0 sürümünden itibaren, Kaspersky Endpoint Security for Windows artık Managed Detection and Response çözümü için yerleşik bir aracıya sahip. *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

Kaspersky Managed Detection and Response ile entegrasyonu ayarlamak için Managed Detection and Response bileşenini etkinleştirmeniz ve Kaspersky Endpoint Security'yi yapılandırmanız gerekir.

Managed Detection and Response bileşeninin çalışması için şu bileşenleri etkinleştirmeniz gerekir:

- Kaspersky Security Network (genişletilmiş mod).
- Davranış Tespiti.

Bu bileşenlerin etkinleştirilmesi isteğe bağlı değildir. Aksi takdirde Kaspersky Managed Detection and Response gerekli telemetri verilerini alamayacağından çalışamaz.

Kaspersky Managed Detection and Response diğer uygulama bileşenlerinden aldığı verileri de kullanır. Bu bileşenlerin etkinleştirilmesi isteğe bağlıdır. Ek veriler sunan bileşenler şunlardır:

- Web Tehdidi Koruması.
- Posta Tehdidi Koruması.
- Güvenlik Duvarı.

Kaspersky Managed Detection and Response bileşeninin Kaspersky Security Center Web Console aracılığıyla Yönetim Sunucusu ile çalışabilmesi için ayrıca yeni bir güvenli bir bağlantı, yani bir *arka plan bağlantısı* kurmanız da şarttır. Kaspersky Managed Detection and Response, çözümün dağıtımını yaparken, sizden bir arka plan bağlantısı kurmanızı ister. Arka plan bağlantısının kurulduğundan emin olun. Kaspersky Security Center'ın diğer Kaspersky çözümleriyle entegre edilmesi hakkında ayrıntılı bilgi almak için Kaspersky Security Center Yardım içeriğine bakın.

Kaspersky Managed Detection and Response ile entegrasyon aşağıdaki adımlardan oluşur:

1. **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 <dosya adı>
   ```

   burada `<dosya adı>` 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: *KSN sağlayıcısı: Kaspersky Private Security Network*.

Managed Detection and Response bileşeninin çalışması için genişletilmiş KSN modunu etkinleştirmeniz gerekir.

2 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.

Managed Detection and Response, Yönetim Konsolu (MMC) ile 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 penceresinden **Detection and Response** → **Managed Detection and Response** seçimini yapın.
5. **Managed Detection and Response** onay kutusunu seçin.
6. **Ayarlar** bloğunda, **İçe aktar**'a tıklayın ve Kaspersky Managed Detection and Response Konsolu'nda alınan BLOB dosyasını seçin. Dosya P7 uzantısına sahiptir.
7. Değişikliklerinizi kaydedin.

[Web Console ve Cloud Console'da Managed Detection and Response bileşeni nasıl etkinleştirilir]

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Managed Detection and Response** bölümüne gidin.
5. **Managed Detection and Response** geçiş düğmesini açık duruma getirin.
6. **İçe aktar**'a tıklayın ve Kaspersky Managed Detection and Response Konsolu'nda elde edilen BLOB dosyasını seçin. Dosya P7 uzantısına sahiptir.
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 <dosya adı> /login=<kullanıcı adı> /password=<parola>
   ```

   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 yükler ve Kaspersky Security Center ile bir sonraki senkronizasyon sırasında dosyayı bilgisayara gönderir. *Uygulama bileşenleri durum raporunu* 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.

Kaspersky Endpoint Agent'tan Geçiş

Kaspersky Endpoint Security sürüm 11 ve üstü, MDR çözümünü destekler. Kaspersky Endpoint Security'nin 11 – 11.5.0 arası sürümleri, tehdit tespitini mümkün kılmak için Kaspersky Managed Detection and Response bileşenine telemetri verileri gönderir. Kaspersky Endpoint Security sürüm 11.6.0, yerleşik aracının işlevselliğine sahiptir (Kaspersky Endpoint Agent).

Kaspersky Endpoint Security 11 - 11.5.0 kullanıyorsanız, MDR çözümü ile çalışmak için veritabanlarını en son sürüme güncellemelisiniz. Ayrıca Kaspersky Endpoint Agent'ı da yüklemeniz gerekir.

Kaspersky Endpoint Security 11.6.0 veya sonraki bir sürümünü kullanıyorsanız, MDR çözümünü kullanmak için Kaspersky Endpoint Agent'ı yüklemeniz gerekmez.

Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security'ye geçiş için:

1. Kaspersky Endpoint Security ilkesinde, Kaspersky Managed Detection and Response ile entegrasyonu yapılandırın.
2. Kaspersky Endpoint Agent ilkesinde Managed Detection and Response bileşenini devre dışı bırakın.

Kaspersky Endpoint Security ilkesi, Kaspersky Endpoint Security 11 – 11.5.0 sürümleri yüklü olmayan bilgisayarlarda da geçerli ise bu bilgisayarlar için ayrı bir Kaspersky Endpoint Agent ilkesi oluşturmalısınız. Yeni ilkede Kaspersky Managed Detection and Response ile entegrasyonu yapılandırın.

Endpoint Detection and Response

11.7.0 sürümünden itibaren, Kaspersky Endpoint Security for Windows, artık Kaspersky Endpoint Detection and Response Optimum çözümü (bundan böyle "EDR Optimum" olarak anılacaktır) için yerleşik bir aracıya sahip. 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 algılama ayrıntılarını ayrı bir pencerede görüntüler. *Algılama ayrıntıları*, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Algılama ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Algılama 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 Detection and Response, aşağıdaki Tehdit İstihbarat araçlarını kullanır:

- Kaspersky bilgi tabanından 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. EDR Expert, verileri, cihazlardan alınan verileri KSN'ye göndermeden bölgesel sunuculara gönderen Kaspersky Private Security Network (KPSN) çözümünü kullanır.
- Dosyaların ve internet adreslerinin tanınırlığı hakkında bilgi içeren ve görüntüleyen Kaspersky Threat Intelligence Portal portalı ile entegrasyon.
- Kaspersky Tehditler veritabanı.
- Tespit edilwn dosyaları yalıtılmış bir ortamda çalıştırmanıza ve tanınırlıklarını kontrol etmenize olanak tanıyan Cloud Sandbox teknolojisi.

Kaspersky Endpoint Detection and Response ile entegrasyon

Kaspersky Endpoint Detection and Response ile entegrasyon için Endpoint Detection and Response Optimum (EDR Optimum) bileşenini ya da Endpoint Detection and Response Expert (EDR Expert) bileşenini eklemeli ve Kaspersky Endpoint Security'yi yapılandırmalısınız.

EDR Optimum, EDR Expert ve EDR (KATA) 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.
- 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 ve 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 ve ayrıca *Uygulama bileşenlerini değiştir* görevini kullanırken EDR Optimum veya EDR Expert 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 özellik, 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.

     Bu özellik, Kaspersky Endpoint Detection and Response için ayrı bir anahtar ekledikten sonra kullanılabilir. Sonuç olarak bilgisayara iki anahtar yüklenir: 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.

3. **Endpoint Detection and Response bileşenlerini etkinleştirme**

   Kaspersky Endpoint Security for Windows ilke ayarlarından bileşeni etkinleştirebilir veya devre dışı bırakabilirsiniz.

   Web Console ve Cloud Console'da Endpoint Detection and Response bileşenini etkinleştirme veya devre dışı bırakma

   1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
   2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
      İlke özellikleri penceresi açılır.
   3. **Uygulama ayarları** sekmesini seçin.
   4. **Detection and Response** → **Endpoint Detection and Response** bölümüne gidin.

5. **Endpoint Detection and Response** geçiş düğmesini açık duruma getirin.

6. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Detection and Response bileşeni etkinleştirilir. *Uygulama bileşenleri durum raporunu* 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** 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 ve Cloud Console aracılığıyla bilgi almak için gereklidir. Örneğin, Web Console ve Cloud Console'da analiz için karantinadan bir dosya indirebilirsiniz.

- Tehdit gelişim zinciri verileri.

  Veriler, bir bilgisayarda tespit edilen tehditler hakkında Web Console ve Cloud Console üzerinden bilgi almak için gereklidir. Web Console ve Cloud Console'da algılama ayrıntılarını görüntüleyebilir ve müdahale eylemleri gerçekleştirebilirsiniz.

Web Console ve Cloud Console'da Yönetim Sunucusu'na veri aktarımını etkinleştirme

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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. Lütfen **Yönetim Sunucusu'na veri aktarımı** bloğundaki şu kutucukları işaretleyin:

   - **Karantina dosyaları hakkında**.
   - **Bir tehdit geliştirme zinciri hakkında**.

6. Değişikliklerinizi kaydedin.

Kaspersky Endpoint Agent'tan Geçiş

EDR Optimum bileşenini (bütünleşik aracı) yüklü halde Kaspersky Endpoint Security 11.7.0 veya daha yüksek bir sürümü kullanıyorsanız, Kaspersky Endpoint Detection and Response Optimum çözümü ile bütünleşme desteği yükleme sonrasında hemen kullanılabilir. EDR Optimum bileşeni, Kaspersky Endpoint Agent ile uyumlu değildir. Bilgisayarda Kaspersky Endpoint Agent yüklüyse, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Security 11.7.0 sürümüne güncellendiğinde Kaspersky Endpoint Security ile çalışmaya devam eder ([KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi). Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır. Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçişi tamamlamak için ilke ve görev ayarlarını Geçiş Sihirbazı ile aktarmanız gerekir.

Kaspersky Endpoint Detection and Response Optimum ile birlikte çalışabilirlik için Kaspersky Endpoint Security 11.4.0–11.6.0 kullanıyorsanız, uygulama Kaspersky Endpoint Agent'ı içerir. Kaspersky Endpoint Security'yi Kaspersky Endpoint Agent ile birlikte yükleyebilirsiniz.

Kaspersky Endpoint Security 11.2.0 - 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.

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.

Kaspersky Endpoint Security'nin bir parçası olan EDR Optimum bileşeni, Kaspersky Endpoint Detection and Response Optimum 2.0 çözümüyle etkileşimi destekler. Kaspersky Endpoint Detection ve Response Optimum sürüm 1.0 ile etkileşim desteklenmez.

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.

Bir IOC Taraması görevi oluşturma

IOC Taraması görevlerini manuel olarak oluşturabilirsiniz:

- Uyarı ayrıntılarında (sadece EDR Optimum için).

  Algılama ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Algılama ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Algılama 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.

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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   Görevler listesi açılır.

2. **Ekle** düğmesine tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.

   b. **Görev türü** açılır listesinde, **IOC Taraması**'nı seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

   d. **Görevin atanacağı cihazları seçin** 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. Sihirbazdan çıkın.

   Görevler listesinde yeni bir görev görüntülenir.

7. Yeni göreve tıklayın.

   Görev özellikleri penceresi açılır.

8. **Uygulama ayarları** sekmesini seçin.

9. **IOC taraması ayarları** bölümüne gidin.

10. Güvenlik ihlali göstergelerini aramak için IOC dosyalarını yükleyin.

    IOC dosyalarını yükledikten sonra, IOC dosyalarından göstergelerin listesini görüntüleyebilirsiniz.

    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. IOC tespit edildiğinde uygulanacak eylem:

    - **Bilgisayarı 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.
    - **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 alanların taranmasını çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Kritik Alanları Tarama* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.

12. **Gelişmiş** bölümüne gidin.

13. Görevin bir parçası olarak analiz edilmesi gereken veri türlerini (IOC belgeleri) seçin.

Kaspersky Endpoint Security, *IOC Scan* 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 günlükleri - 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.

Windows kayıt defteri - RegistryItem veri türü için Kaspersky Endpoint Security bir kayıt defteri anahtarları grubunu tarar.

14. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.
15. Görev zamanlamasını yapılandırın.

    LAN'da Uyandırma bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

16. Değişikliklerinizi kaydedin.
17. Görevin yanındaki onay kutusunu seçin.
18. **Çalıştır** düğmesine 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 sonuçları 30 gün boyunca saklanır. Bu süre sonrasında Kaspersky Endpoint Security en eski kayıtları otomatik olarak siler.

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 Detection and Response çözümleriyle çalışırken kullanır: EDR Optimum, EDR Expert, KATA (EDR), Kaspersky Sandbox. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantinayı yönetmeyle ilgili ayrıntılar için lütfen Kaspersky Sandbox Yardımı, Kaspersky Endpoint Detection and Response Optimum Yardımı, Kaspersky Endpoint Detection and Response Expert Yardımı ve Kaspersky Anti Targeted Attack Platform Yardımı 'na başvurun.

Karantinaya taşı görevlerini şu yöntemlerle oluşturabilirsiniz:

- Uyarı ayrıntılarında (sadece EDR Optimum için).

  Algılama ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Algılama ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Algılama 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.

Dosyayı Karantinaya taşı görevi şu sınırlamalara sahiptir:

1. Dosya boyutu 100 MB'ı geçemez.
2. Kritik Sistem Nesneleri (SCO) karantinaya alınamaz. Kritik Sistem Nesneleri, işletim sisteminin ve Kaspersky Endpoint Security for Windows uygulamasının çalışmak için ihtiyaç duyduğu dosyalardır.
3. EDR Optimum için Web Console ve Cloud Console'da görev yapılandırabilirsiniz. EDR Expert için görev ayarları sadece Cloud Console'da kullanılabilir.

Bir Dosyayı Karantinaya taşı görevi oluşturmak için:

1. Web Console'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.
   b. **Görev türü** açılır listesinde, **Dosyayı Karantinaya taşı** seçimini yapın.
   c. **Görev adı** alanına kısa bir açıklama girin.
   d. **Görevin atanacağı cihazları seçin** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri** düğmesine tıklayın.
5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri** düğmesine tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Bitir** 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.

    LAN'da Uyandırma bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. **Kaydet** düğmesine tıklayın.

14. Görevin yanındaki onay kutusunu seçin.

15. **Çalıştır** düğmesine tıklayın.

    Sonuç olarak Kaspersky Endpoint Security, dosyayı Karantinaya alır. Dosya farklı bir işlem tarafından kilitlenirse göre: *Tamamlanmış* 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 alanında 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. Dosyayı almak için özel bir görev oluşturmanız gerekir. Görevin yürütülmesiyle dosya Karantinaya kaydedilir. Bu dosyayı, Web Console kullanarak Karantinadan bilgisayarınıza indirebilirsiniz. Kullanıcının bilgisayarında, dosya orijinal klasöründe kalır.

Dosya boyutu 100 MB'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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.

2. **Ekle** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Dosyayı al**'ı seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

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

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri** düğmesine tıklayın.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri** düğmesine tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Bitir** 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.

    > LAN'da Uyandırma bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.
13. **Kaydet** düğmesine tıklayın.
14. Görevin yanındaki onay kutusunu seçin.
15. **Çalıştır** düğmesine 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.

Dosyayı sil görevi şu sınırlamalara sahiptir:

- Kritik Sistem Nesneleri (SCO) silinemez. Kritik Sistem Nesneleri, işletim sisteminin ve Kaspersky Endpoint Security for Windows uygulamasının çalışmak için ihtiyaç duyduğu dosyalardır.
- 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.

   Görevler listesi açılır.
2. **Ekle** düğmesine tıklayın.

   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.

   b. **Görev türü** açılır listesinde, **Dosyayı sil**'i seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

   d. **Görevin atanacağı cihazları seçin** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri** düğmesine tıklayın.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri** düğmesine tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Bitir** 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.

    LAN'da Uyandırma bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. **Kaydet** düğmesine tıklayın.

14. Görevin yanındaki onay kutusunu seçin.

15. **Çalıştır** düğmesine tıklayın.

    Böylece Kaspersky Endpoint Security dosyayı bilgisayardan siler. Dosya farklı bir işlem tarafından kilitlenirse göre: *Tamamlanmış* 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* hatasını verebilir. Dosya için bir işlemi sonlandır görevi oluşturun ve tekrar deneyin.

İşlem başlangıcı

İşlemi başlat görevini kullanarak dosyaları uzaktan çalıştırabilirsiniz. Örneğin, bilgisayar yapılandırma dosyasını oluşturan bir yardımcı programı uzaktan çalıştırabilirsiniz. Bundan sonra, Kaspersky Security Center Web Console'da oluşturulan dosyayı 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 İşlemi başlat görevi oluşturmak için:

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

   Görevler listesi açılır.

2. **Ekle** düğmesine tıklayın.

   Görev Sihirbazı başlatılır.

3. Görev ayarlarını yapılandırın:

   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.

   b. **Görev türü** açılır listesinde, **İşlemi başlat**'ı seçin.

   c. **Görev adı** alanına kısa bir açıklama girin.

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

4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri** düğmesine tıklayın.

5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri** düğmesine tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Bitir** 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.

    Örneğin, `conf.txt` adlı bir dosyaya bilgisayarın yapılandırması hakkındaki bilgileri kaydeden bir yardımcı programı (`utility.exe`) çalıştırmak istiyorsanız aşağıdaki değerleri girmelisiniz:

    - **Yürütülebilir komut** - `utility.exe`
    - **Komut satırı bağımsız değişkenleri (isteğe bağlı)** - `/R conf.txt`
    - **Çalışma klasörü yolu (isteğe bağlı)** - `C:\Users\admin\Diagnostic\`

    Alternatif olarak, **Yürütülebilir komut** alanında `C:\Users\admin\Diagnostic\utility.exe /R conf.txt` girişi yapabilirsiniz. Bu durumda diğer ayarları girmenize gerek yoktur.

11. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

12. Görev zamanlamasını yapılandırın.

    LAN'da Uyandırma bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

13. **Kaydet** düğmesine tıklayın.

14. Görevin yanındaki onay kutusunu seçin.

15. **Çalıştır** düğmesine 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:

- Kritik Sistem Nesneleri (SCO) sonlandırılamaz. Kritik Sistem Nesneleri, işletim sisteminin ve Kaspersky Endpoint Security for Windows uygulamasının çalışmak için ihtiyaç duyduğu dosyalardır.
- 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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   Görevler listesi açılır.
2. **Ekle** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.
3. Görev ayarlarını yapılandırın:
   a. **Uygulama** açılır listesinden **Kaspersky Endpoint Security for Windows (12.1)** seçimini yapın.
   b. **Görev türü** açılır listesinde, **İşlemi sonlandır**'ı seçin.
   c. **Görev adı** alanına kısa bir açıklama girin.
   d. **Görevin atanacağı cihazları seçin** bloğunda görev kapsamını seçin.
4. Seçilen görev kapsamı seçeneğine göre aygıtları belirleyin. **İleri** düğmesine tıklayın.
5. Bir görevi çalıştırmak için haklarını kullanmak istediğiniz kullanıcının hesap kimlik bilgilerini girin. **İleri** düğmesine tıklayın.

   Kaspersky Endpoint Security, görevi varsayılan olarak sistem kullanıcı hesabı (SYSTEM) olarak başlatır.

6. **Bitir** düğmesine tıklayarak sihirbazı sonlandırın.
   Görevler listesinde yeni bir görev görüntülenir.
7. Yeni göreve tıklayın.
   Görev özellikleri penceresi açılır.
8. **Uygulama ayarları** sekmesini seçin.
9. 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.
10. Bilgisayar özellikleri penceresinde **Zamanlama** sekmesini seçin.

11. Görev zamanlamasını yapılandırın.

    LAN'da Uyandırma bu görev için mevcut değildir. Bilgisayarın görevi çalıştırmak için açık olduğundan emin olun.

12. **Kaydet** düğmesine tıklayın.

13. Görevin yanındaki onay kutusunu seçin.

14. **Çalıştır** düğmesine tıklayın.

    Böylece Kaspersky Endpoint Security bilgisayardaki işlemi sonlandırır. Örneğin bir "OYUN" 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).

  Algılama ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Algılama ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Algılama 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 veya MD5) ya da hem dosya yolunu hem de 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. Kritik sistem nesnelerinin (SCO) başlatılmasını engellemek mümkün değildir. Kritik Sistem Nesneleri, işletim sisteminin ve Kaspersky Endpoint Security for Windows uygulamasının çalışmak için ihtiyaç duyduğu dosyalardır.

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 **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Endpoint Detection and Response** bölümüne gidin.
5. **Yürütme Önleme ETKİNLEŞTİRİLDİ** iki durumlu düğmesini açık duruma getirin.
6. **Yasak nesnenin yürütülmesi veya açılması ile ilgili eylem** bloğundan bileşen çalışma modunu seçin:
   - **Engelle ve rapora yaz**. 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.
   - **Sadece olayları günlüğe kaydet**. 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.
7. 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 veya MD5), dosyanın tam yolunu veya hem karmayı 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 Kaspersky Endpoint Security dosyayı veya komut dosyasını engellemez.

      Yürütme önleme bir ofis dosyası uzantıları grubunu ve bir komut dizisi yorumlayıcısı grubunu destekler.
   e. **Tamam**'a tıklayın.
8. 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.

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 **Aygıtlar** → **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. **IOC tespit edildiğinde uygulanacak eylem** bloğundan, **Bir IOC bulunduktan sonra yanıt eylemleri gerçekleştir** ve **Bilgisayarı ağdan izole et** kutularını işaretleyin.
5. Değişikliklerinizi kaydedin.

Sonuç olarak, bir IOC tespit edildiğinde uygulama, tehdidin yayılmasını önlemek için bilgisayarı ağdan izole eder.

Ağ izolasyonunu belirli bir süre geçtikten sonra otomatik olarak kapatılacak 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 **Cihazlar** → **İlkeler ve profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Endpoint Detection and Response** bölümüne gidin.
5. **Ağ izolasyonu** bloğundan **Bilgisayar kilidi kaldırma ayarlarını yapılandırın**'a tıklayın.
6. Böylece bir pencere açılır; bu pencereden **İzole edilen bilgisayarın kilidini şu süre içinde kaldır: N saat** kutucuğunu işaretleyin ve Ağ izolasyonunun otomatik olarak kapanacağı gecikme süresini girin.
7. Değişikliklerinizi kaydedin.

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).
  Algılama ayrıntıları, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Algılama ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Algılama 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.

Bir bilgisayarın ağ izolasyonunu manuel olarak açma

1. Web Console'un ana penceresinde **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows**'a 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.

Ağ izolasyonunu belirli bir süre geçtikten sonra otomatik olarak kapatılacak 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 **Cihazlar** → **Yönetilen cihazlar**'ı seçin.
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 **Aygıtlar** → **Yönetilen cihazlar**'ı seçin.
2. Yerel uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
   Bu, bilgisayar özelliklerini açar.
3. **Uygulamalar** sekmesini seçin.
4. **Kaspersky Endpoint Security for Windows**'a 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 **Ağdan izole edilmiş bilgisayarın kilidini kaldır** seçeneğine tıklayın.

Ağ izolasyonunu, komut satırı ile yerel olarak da kaldırabilirsiniz.

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 **Cihazlar** → **İlkeler ve profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Endpoint Detection and Response** bölümüne gidin.
5. **Ağ izolasyonu istisnaları** bloğundan, **İstisnalar**'a tıklayın.
6. 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.
7. 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.
8. Değişikliklerinizi kaydedin.

Manuel modda ağ izolasyonu istisnası ekleme

1. Web Console'un ana penceresinde **Cihazlar** → **Yönetilen cihazlar**'ı seçin.
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.

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'u zaten dağıttıysanız Cloud Sandbox tarafından algılanan tehditler için ayrı bir sayaç etkinleştirebilirsiniz. Algılanan tehditlerin analizi sırasında istatistik oluşturmak için bu sayacı kullanabilirsiniz.

Cloud Sandbox sayacını etkinleştirmek için:

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Endpoint Detection and Response** bölümüne gidin.
5. **Cloud Sandbox** düğmesini açık konumuna getirin.
6. 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.

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows, 11.7.0 sürümünden itibaren Kaspersky Sandbox çözümü ile entegrasyon için yerleşik bir aracı içerir. *Kaspersky Sandbox çözümü* bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Kaspersky Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Kaspersky Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Kaspersky Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözümle ilgili ayrıntılı bilgi almak için Kaspersky Sandbox Yardım içeriğine bakın.

Kaspersky Sandbox çözümü için şu yapılandırmalar mümkündür:

Kaspersky Sandbox 2.0

Kaspersky Sandbox 2.0, [KES+bütünleşik aracı] yapılandırmasını destekler.

Minimum gereksinimler:

- Kaspersky Endpoint Security 11.7.0 for Windows veya üzeri.
- Kaspersky Endpoint Agent gerekli değildir.
- Kaspersky Security Center 13.2.

Kaspersky Sandbox 1.0

Kaspersky Sandbox 1.0, [KES + KEA] yapılandırmasını destekler.

Minimum gereksinimler:

- Kaspersky Endpoint Security 11.2.0 – 11.6.0 for Windows.
- Kaspersky Endpoint Agent 3.8.

  Kaspersky Endpoint Agent'ı, Kaspersky Endpoint Security for Windows dağıtım paketinden yükleyebilirsiniz.
- Kaspersky Security Center 11.

Kaspersky Sandbox ile Entegrasyon

Kaspersky Sandbox bileşeniyle entegrasyon için Kaspersky Sandbox bileşeninin eklenmesi gerekir. Kaspersky 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 aktarımını etkinleştirme

  1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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. **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 **Konsol ayarları** → **Entegrasyon** seçimini yapın.
  2. **Tümleştirme** bölümüne gidin.
  3. **Tümleştirme için bir arka plan bağlantısı kur** 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.

- Kaspersky Sandbox bileşeni etkinleştirilmelidir.

  Kaspersky Sandbox ile entegrasyonu Web Konsolu'nda veya Komut satırını kullanarak yerel olarak etkinleştirebilir veya devre dışı bırakabilirsiniz.

Kaspersky Sandbox ile entegrasyonu etkinleştirmek veya devre dışı bırakmak için:

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Kaspersky Sandbox**'a gidin.
5. Bileşeni etkinleştirmek veya devre dışı bırakmak için **Kaspersky Sandbox ile Entegrasyon ETKİNLEŞTİRİLDİ** iki durumlu düğmesini kullanın.
6. Değişikliklerinizi kaydedin.

Sonuç olarak, Kaspersky Sandbox bileşeni etkinleştirilir. *Uygulama bileşenleri durum raporunu* görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Kaspersky Sandbox** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecek.

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.

Kaspersky Endpoint Agent'tan Geçiş

Kaspersky Sandbox bileşeni (bütünleşik aracı) yüklü olarak Kaspersky Endpoint Security 11.7.0 veya daha yeni bir sürümünü kullanıyorsanız, Kaspersky Sandbox çözümü ile birlikte çalışabilirlik yüklemeden hemen sonra sunulur. Kaspersky Sandbox bileşeni, Kaspersky Endpoint Agent ile uyumlu değildir. Bilgisayarda Kaspersky Endpoint Agent yüklüyse, Kaspersky Sandbox, Kaspersky Endpoint Security 11.7.0 sürümüne güncellendiğinde Kaspersky Endpoint Security ile çalışmaya devam eder ([KES+KEA] yapılandırmasının [KES+bütünleşik aracı]'ya geçişi). Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılacaktır. Kaspersky Endpoint Agent'tan Kaspersky Endpoint Security for Windows'a geçişi tamamlamak için ilke ve görev ayarlarını Geçiş Sihirbazı ile aktarmanız gerekir.

Kaspersky Sandbox ile birlikte çalışabilirlik için Kaspersky Endpoint Security 11.4.0–11.6.0 kullanıyorsanız, uygulama Kaspersky Endpoint Agent'ı içerir. Kaspersky Endpoint Security'yi Kaspersky Endpoint Agent ile birlikte yükleyebilirsiniz.

Kaspersky Endpoint Security 11.2.0 - 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.

Kaspersky Endpoint Security'nin parçası olan Kaspersky Sandbox bileşeni, Kaspersky Sandbox çözümü 2.0 ile birlikte çalışabilirliği destekler. Kaspersky Sandbox çözümü 1.0 desteklenmez.

TLS sertifikası ekleme

Kaspersky Sandbox sunucularıyla güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Ardından, sertifikayı Kaspersky Sandbox sunucularına ve Kaspersky Endpoint Security ilkesine eklemelisiniz. Sertifikayı hazırlama ve sertifikayı sunuculara eklemeyle ilgili ayrıntılar için Kaspersky Sandbox Yardım içeriğine bakın.

Komut satırı üzerinden Web Console'a yerel olarak bir TLS sertifikası ekleyebilirsiniz.

Web Console kullanılarak bir TLS sertifikası eklemek için:

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response → Kaspersky Sandbox**'a gidin.
5. **Sunucu bağlantı ayarları** bağlantısına tıklayın.

   Kaspersky Sandbox sunucusu bağlantı ayarları penceresi açılır.
6. **Sunucu TLS sertifikası** bloğundan **Ekle**'ye tıklayın ve TLS sertifika dosyasını seçin.

   Kaspersky Endpoint Security, bir Kaspersky Sandbox sunucusu için yalnızca bir TLS sertifikasına sahip olabilir. Daha önce bir TLS sertifikası eklediyseniz, o sertifika iptal edilir. Yalnızca son eklenen sertifika kullanılır.
7. Kaspersky Sandbox sunucuları için gelişmiş bağlantı ayarlarını yapılandırın:

   - **Zaman Aşımı**. Kaspersky 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 stabil değilse Kaspersky Sandbox için bağlantı zaman aşımı süresini artırabilirsiniz. Önerilen istek zaman aşımı 0,5 saniye veya daha kısadır.
   - **Kaspersky Sandbox istek kuyruğu**. İstek kuyruğu klasörünün boyutu. Bilgisayarda bir nesneye erişildiğinde (yürütülebilir dosya başlatıldığında veya örneğin DOCX veya PDF biçiminde bir belge açıldığında), Kaspersky Endpoint Security, Kaspersky Sandbox tarafından taranacak nesneyi de gönderebilir. Birden çok istek olduğunda, Kaspersky Endpoint Security bir istek kuyruğu oluşturur. İstek kuyruğu klasörünün boyutu varsayılan olarak 100 MB ile sınırlandırılmıştır. Maksimum boyuta ulaşıldıktan sonra, Kaspersky Sandbox kuyruğa yeni isteklerin eklenmesini durdurur ve ilgili olayı Kaspersky Security Center'a gönderir. İstek kuyruğu klasörünün boyutunu sunucu yapılandırmanıza göre yapılandırabilirsiniz.
8. 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.

Kaspersky Sandbox sunucuları ekleyin

Bilgisayarları, işletim sistemlerinin sanal görüntüleri ile Kaspersky Sandbox sunucularına bağlamak için bir sunucu adresi ve bir bağlantı noktası girmelisiniz. Sanal görüntüleri dağıtma ve Kaspersky Sandbox sunucularını yapılandırma hakkında ayrıntılar için Kaspersky Sandbox Yardım içeriğine bakın.

Kaspersky Sandbox sunucularını Web Console'a eklemek için:

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

   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response → Kaspersky Sandbox**'a gidin.
5. **Kaspersky Sandbox sunucusu** bloğından **Ekle**'ye tıklayın.
6. Açılan pencerede, Kaspersky Sandbox sunucusunun adresini (IPv4, IPv6, DNS) ve bağlantı noktasını girin.

7. Değişikliklerinizi kaydedin.

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'un ana penceresinde **Aygıtlar** → **Görevler**'i seçin.
   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 alanların taranmasını çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Kritik Alanları Tarama* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.
6. **Sadece bilgisayar boştayken çalıştır** onay kutusunu kullanarak IOC Taraması görevi çalışma modunu yapılandırın. Bu onay kutusu, bilgisayar kaynakları sınırlı olduğunda *IOC Taraması* görevini askıya alan işlevi etkinleştirir/devre dışı bırakır. Kaspersky Endpoint Security, ekran koruyucu kapalı olduğunda ve bilgisayar kilidi kaldırıldığında *IOC Taraması* görevini duraklatır.
   Bu zamanlama seçeneği, bilgisayar kullanılırken bilgisayar kaynaklarını korumanıza olanak tanır.
7. 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 Anti Targeted Attack Platform (EDR)

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. *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 iki işlevsel blok içerir: Kaspersky Anti Targeted Attack (bundan sonra kısaca "*KATA*" olarak anılacaktır) ve Kaspersky Endpoint Detection and Response (bundan sonra kısaca "*EDR (KATA)*" olarak alınacaktır). EDR (KATA)'yı ayrıca satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için lütfen Kaspersky Anti Targeted Attack Platform Yardım içeriğine bakın.

Kaspersky Endpoint Detection and Response, aşağıdaki Tehdit İstihbarat araçlarını kullanır:

- Kaspersky bilgi tabanından 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.
- Dosyaların ve internet adreslerinin tanınırlığı hakkında bilgi içeren ve görüntüleyen Kaspersky Threat Intelligence Portal portalı ile entegrasyon.
- Kaspersky Tehditler veritabanı.

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) 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 (KATA) ile entegrasyon

EDR (KATA) ile entegrasyon için Endpoint Detection and Response (KATA) bileşenini eklemeniz gerekir. EDR KATA bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştirme* görevini kullanırken seçebilirsiniz.

EDR Optimum, EDR Expert ve EDR (KATA) bileşenleri birbirleriyle uyumlu değildir.

Endpoint Detection and Response (KATA) bileşeninin çalışması için şu şartlar sağlanmalıdır:

- Kaspersky Anti Targeted Attack Platform sürüm 4.1 veya üzeri.
- Kaspersky Security Center sürüm 13.2 veya üstü. Kaspersky Security Center'ın önceki sürümlerinde Endpoint Detection and Response (KATA) özelliğini etkinleştirmek mümkün değildir.
- Uygulama etkinleştirilmiş ve işlevsellik lisans kapsamında olmalıdır.
- Endpoint Detection and Response (KATA) bileşeni açık olmalıdır.
- Endpoint Detection ve Response (KATA) bileşeninin bağlı olduğu uygulama bileşenleri etkin ve çalışır durumda olmalıdır. Aşağıdaki bileşenler EDR (KATA)'nın çalışmasını sağlar:

- 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 (KATA) bileşenini yükleme**

   EDR KATA bileşenini, yükleme veya yükseltme sırasında ve ayrıca *Uygulama bileşenlerini değiştirme* görevini kullanırken seçebilirsiniz.

   > Uygulamayı yeni bileşenlerle yükseltmeyi tamamlamak için bilgisayarınızı yeniden başlatmanız gerekir.

2. **Endpoint Detection and Response (KATA)'yı etkinleştirme**

   Kaspersky Endpoint Detection and Response (KATA)'yı kullanmak için aşağıdaki yöntemlerle bir lisans alabilirsiniz:

   - Endpoint Detection and Response (KATA) işlevselliği, Kaspersky Endpoint Security for Windows lisansına dahildir.

     Bu özellik, Kaspersky Endpoint Security for Windows etkinleştirildikten hemen sonra kullanılabilir.

   - EDR (KATA) (Kaspersky Endpoint Detection and Response (KATA) Eklentisi) için ayrı bir lisans satın almak.

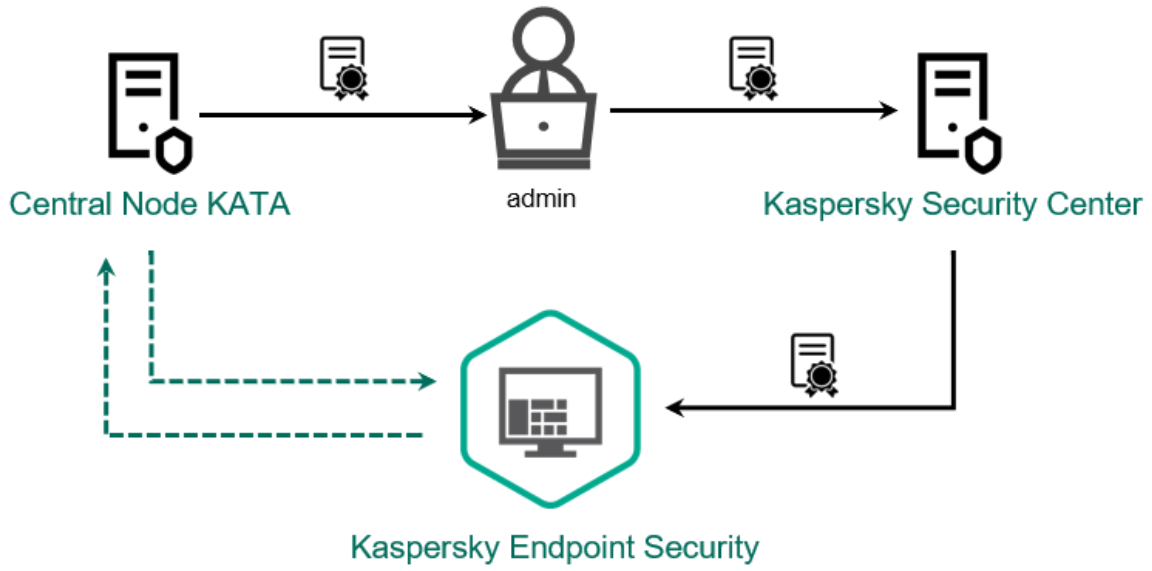
     Bu özellik, Kaspersky Endpoint Detection and Response (KATA) için ayrı bir anahtar ekledikten sonra kullanılabilir. Sonuç olarak bilgisayara iki anahtar yüklenir: Kaspersky Endpoint Security için bir anahtar ve Kaspersky Endpoint Detection and Response (KATA) için bir anahtar.

     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.

3. **Merkezi Düğüme bağlanma**

   Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security ile Merkezi Düğüm 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 Merkezi Düğümün TLS sertifikasını kontrol eder. Bağlantıyı daha güvenli hale getirmek için, bilgisayarın Merkezi Düğüm üzerinde doğrulanmasını da etkinleştirebilirsiniz (iki yönlü kimlik doğrulama). Bu doğrulamayı etkinleştirmek için Merkezi Düğüm 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 Merkezi Düğüme 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 penceresinden **Detection and Response → Endpoint Detection and Response (KATA)** seçimini yapın.
5. **Endpoint Detection and Response (KATA)** onay kutusunu seçin.
6. **KATA sunucularına bağlantı için ayarlar**'a tıklayın.
7. Sunucu bağlantısını yapılandırın:
   - **Zaman Aşımı**. Maksimum Merkezi Düğüm sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Merkezi Düğüm sunucusuna bağlanmayı dener.
   - **Sunucu TLS sertifikası**. Merkezi Düğüm 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 kullanın**. İki yönlü kimlik doğrulama, Merkezi Düğümdeki bilgisayarın ek bir doğrulamasının yapılmasına olanak tanır. Bu doğrulamayı etkinleştirmek için Merkezi Düğüm 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).

     Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
8. **Tamam**'a tıklayın.

9. Merkezi Düğüm sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için bağlantı noktasını belirtin.
10. Değişikliklerinizi kaydedin.

Web Console kullanılarak bir Kaspersky Endpoint Security bilgisayarı Merkezi Düğüme nasıl bağlanır

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'i seçin.
2. Kaspersky Endpoint Security ilkesinin adına tıklayın.
   İlke özellikleri penceresi açılır.
3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response** → **Endpoint Detection and Response (KATA)** bölümüne gidin.
5. **Endpoint Detection and Response (KATA) ETKİN** iki durumlu düğmesini açık duruma getirin.
6. **KATA sunucularına bağlantı için ayarlar**'a tıklayın.
7. Sunucu bağlantısını yapılandırın:
   - **Zaman Aşımı**. Maksimum Merkezi Düğüm sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Merkezi Düğüm sunucusuna bağlanmayı dener.
   - **Sunucu TLS sertifikası**. Merkezi Düğüm 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 kullanın**. İki yönlü kimlik doğrulama, Merkezi Düğümdeki bilgisayarın ek bir doğrulamasının yapılmasına olanak tanır. Bu doğrulamayı etkinleştirmek için Merkezi Düğüm 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).

     Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
8. **Tamam**'a tıklayın.
9. Merkezi Düğüm sunucuları ekleyin. Bunu yapmak için, sunucu adresini (IPv4, IPv6) ve sunucuya bağlanmak için bağlantı noktasını belirtin.
10. Değişikliklerinizi kaydedin.

Sonuç olarak, bilgisayar Kaspersky Anti Targeted Attack Platform konsoluna eklenir. *Uygulama bileşenleri durum raporunu* görüntüleyerek bileşenin çalışma durumunu denetleyin. Kaspersky Endpoint Security'nin yerel arabirimindeki raporlarda bir bileşenin çalışma durumunu da görüntüleyebilirsiniz. **Endpoint Detection and Response (KATA)** bileşeni, Kaspersky Endpoint Security bileşenleri listesine eklenecektir.

Telemetriyi 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 (yukarıdaki 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) EDR telemetri yapılandırması

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 **Detection and Response → Endpoint Detection and Response (KATA)** seçimini yapın.
5. **KATA sunucusuna her (dakika) senkronizasyon isteği gönder** ayarını yapılandırın. Merkezi Düğüm 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** bloğunda **Maksimum olay iletim gecikmesi (sn)** ayarını yapılandırın. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
8. Gerekirse, **Talep daraltma** bloğunda **Talep daraltmayı etkinleştir** onay kutusunu seçin.

   Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Onay kutusu işaretlendiğinde uygulama iletilen olayları 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.
   - **Olay sınırı aşımının 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. Değişikliklerinizi kaydedin.

Web Console'da (MMC) EDR telemetri yapılandırması

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

   İlke özellikleri penceresi açılır.

3. **Uygulama ayarları** sekmesini seçin.
4. **Detection and Response → Endpoint Detection and Response (KATA)** bölümüne gidin.
5. **KATA sunucusuna her (dakika) senkronizasyon isteği gönder** ayarını yapılandırın. Merkezi Düğüm 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** bloğunda **Maksimum olay iletim gecikmesi (sn)** ayarını yapılandırın. Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur. Varsayılan değer ayarı 30 saniyedir.
8. Gerekirse, **Talep daraltma** bloğunda **Talep daraltmayı etkinleştir** onay kutusunu seçin.

   Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Onay kutusu işaretlendiğinde uygulama iletilen olayları 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.
   - **Olay sınırı aşımının 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. Değişikliklerinizi kaydedin.

Telemetri istisnaları

İletilen verileri optimize etmek için, güvenilir uygulamalar listesine bir yürütülebilir dosya ekleyebilirsiniz. Bu durumda, Kaspersky Endpoint Security bu uygulama için telemetri olayları göndermez. Bu, ağ trafiğini azaltmanıza ve güvenilir nesnelerden gelen olay miktarını en aza indirmenize olanak tanır.

1. Web Console'un ana penceresinde **Aygıtlar → İlkeler ve Profiller**'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 *VE* 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'nu açın.
2. Konsol ağacında **İlkeler**'i seçin.
3. Gereken ilkeyi seçin ve ilke özellikleri penceresini açmak için çift tıklayın.
4. İlke penceresinde KATA **entegrasyonu** → **Telemetri istisnaları** seçeneğini belirleyin.
5. **Veri iletim ayarları** bölümünde, **İstisnaları kullan** onay kutusunu seçin.
6. **Ekle**'ye tıklayın ve istisnaları yapılandırın:

   Kriterler mantıksal *VE* 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.

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 4.1 veya üzeri.
- Kaspersky Security Center sürüm 13.2 veya üstü (Ağ Aracısı 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

     Sihirbazdan çıkın. 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:

     - Ayarlar değişiklik yasağı **KATA sunucularına bağlanmak için ayarlar** ("kilit").

       Varsayılan olarak ayarlar değiştirilebilir ("kilit" açıktır). Bu nedenle ayarlar bilgisayarda uygulanmaz. Ayarların değiştirilmesi yasaklanmalı ve "kilit" kapatılmalıdır.

     - Kripto konteyneri.

Merkezi Düğüm sunucularına bağlanmak için iki yönlü kimlik doğrulama kullanıyorsanız, kripto konteynerini yeniden eklemeniz gerekir.

Geçiş Sihirbazı bu ayarları taşımadığından, bilgisayarı Merkezi Düğüm 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`.

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) Eklenti lisansının etkinleştirilmesi şu özel hususları içerir:

- Kaspersky Endpoint Security'yi EDR Optimum veya EDR Expert özellikleriyle lisanslamak için bir *anahtar dosyası* kullanıyorsanız, bağımsız bir Kaspersky Endpoint Detection and Response (KATA) Eklenti lisansını etkinleştiremezsiniz. 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, bağımsız bir Kaspersky Endpoint Detection and Response (KATA) Eklenti lisansını anahtar dosyaları tekrar yayınlanmadan etkinleştirebilirsiniz.

- 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 bileşenleri durum raporunu* görüntüleyerek yerleşik aracının çalışma durumunu kontrol edin. Bir bileşenin durumu *Yüklenmedi* 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 Beyanını 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 *Kaspersky Anti Targeted Attack Platform sunucusuna bağlantı başarılı oldu* 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.

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 Detection and Response çözümleriyle çalışırken kullanır: EDR Optimum, EDR Expert, KATA (EDR), Kaspersky Sandbox. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantinayı yönetmeyle ilgili ayrıntılar için lütfen Kaspersky Sandbox Yardımı , Kaspersky Endpoint Detection and Response Optimum Yardımı , Kaspersky Endpoint Detection and Response Expert Yardımı ve Kaspersky Anti Targeted Attack Platform Yardımı 'na başvurun.

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 200 MB ile sınırlandırılmıştır. Kaspersky Endpoint Security, maksimum boyuta ulaşıldıktan sonra Karantina konumundan en eski dosyaları otomatik olarak siler.

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 bilgisayardaki toplam RAM boyutuna (örneğin, 8 GB) eşit olacak şekilde ayarlamanızı öneririz.

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. **Karantina** bloğundan Karantina boyutunu yapılandırın:
   - **Karantina boyutunu şununla sınırla: N MB**. MB cinsinden maksimum Karantina boyutu. Örneğin, maksimum Karantina boyutunu 200 MB olarak ayarlayabilirsiniz. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security ilgili olayı 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 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.
6. Değişikliklerinizi kaydedin.

Web Console'da ve Cloud Console'da maksimum karantina boyutunu yapılandırma

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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: N MB**. MB cinsinden maksimum Karantina boyutu. Örneğin, maksimum Karantina boyutunu 200 MB olarak ayarlayabilirsiniz. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security ilgili olayı 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 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.

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 Sunucusuna 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.

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. Açılan pencerede, **Karantina dosyaları hakkında** kutucuğunu işaretleyin.

7. Değişikliklerinizi kaydedin.

Karantinaya alınan dosya verilerinin Web Console'a aktarılması nasıl etkinleştirilir

1. Web Console'un ana penceresinde **Aygıtlar** → **İlkeler ve Profiller**'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. **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. EDR Optimum ve EDR Expert çözümlerinde, uygulama dosyayı geri yükledikten sonra siler. Diğer çözümler için, uygulamalar dosyanın bir kopyasını Karantinada tutar.

KSWS'den KES'e Geçiş Kılavuzu

Kaspersky Endpoint Security, 11.8.0 sürümünden itibaren Kaspersky Security for Windows Server (KSWS) çözümünün temel işlevlerini destekler. *Windows Server için Kaspersky Security* 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).
   - 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, tarama görevleri dahil
Log Inspection	Günlük Denetleyici
Device Control	Aygıt Denetimi
Firewall	*(desteklenmiyor)*

Management	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	Dosya Bütünlüğü İzleyici
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, tarama görevleri dahil
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

Tümünü genişlet | Tümünü daralt

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.
Do not start scheduled	**Pil gücüyle çalışırken zamanlanmış görevleri ertele** (**Uygulama ayarları** alt bölümü)

scan tasks	
Stop current scan tasks	*(geçiş gerçekeşmez)* 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) Kaspersky Endpoint Security, NTLM kimlik doğrulamasını desteklemez. KSWS ayarlarında NTLM kimlik doğrulaması etkinleştirilmişse, geçişten sonra proxy sunucusu kimlik doğrulamasını yapılandırmanız ve bir kullanıcı adı ile parola belirlemeniz gerekir. Proxy sunucusu kimlik doğrulama parolası taşınmaz. Bir ilke taşındıktan sonra parolanın elle 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 *Güncelle* 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	**Tarama istisnaları** (Tarama istisnaları)

(Exclusions)	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 eklemeniz gerekir.
Apply also to subfolders (Exclusions)	**Alt klasörler dahil** (Tarama istisnaları)
Objects to detect (Exclusions)	**Nesne adı** (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, bir dosyada olduğu gibi yapılandırılmış güvenilir süreçlere sahipse, 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 Görevi ayarları

Kaspersky Security for Windows Server ayarları	Kaspersky Endpoint Security for Windows ayarları
Scan removable drives on connection via USB	**Bir çıkarılabilir sürücü bağlandığında 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**	**Bir çıkarılabilir sürücü bağladığında yapılacak eylem**: • **Ayrıntılı Tarama** • **Hızlı Tarama**. KSWS güvenlik düzeyleri, şu KES tarama modlarına karşılık gelir: • Maximum protection – Ayrıntılı Tarama.

- Recommended – Hızlı Tarama.
- Maximum performance – Hızlı Tarama.

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 Security ayarları	Kaspersky Endpoint Security for Windows ayarları
Backup folder	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, dosyaların yedek kopyalarını `C:\ProgramData\Kaspersky Lab\KES.21.13\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 gerçekleşmez)* Eşiğin %50'si dolduğunda, Kaspersky Endpoint Security *Karantina depolama alanı neredeyse doldu* olayını günlüğe kaydeder.
Target folder for restoring objects	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, dosyaları orijinal klasörlerine geri yükler.
Quarantine folder	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, dosyaların yedek kopyalarını `C:\ProgramData\Kaspersky Lab\KES.21.13\QB` klasörüne kaydeder.
Maximum Quarantine size (MB)	*(geçiş gerçekleşmez)* 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 gerçekleşmez)* 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 gerçekleşmez)* Kaspersky Endpoint Security, dosyaları orijinal klasörlerine geri yükler.
Unblock automatically in N	**Saldıran cihazları N dakika boyunca engelle** (**Temel Tehdit Koruması** → **Ağ Tehdit Koruması** bölümü)

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** • **Yürütüldüğünde** • **Erişildiğinde** • **Erişim ve değiştirme durumunda**.
Deeper analysis of launching processes	*(geçiş gerçekleşmez)* 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 gerçekleşmez)* Kaspersky Endpoint Security, güvenilir bölgeyi tüm bileşenlere uygular. İstisnaları güvenilir bölge ayarlarında yapılandırabilirsiniz.
Use KSN for protection	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, tüm uygulama bileşenleri için KSN kullanır.
Block access to network shared resources for the hosts that show malicious activity	*(geçiş gerçekleşmez)* 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 gerçekleşmez)* Kaspersky Endpoint Security, etkin bir virüs tespit edildiğinde kritik alanları tarama görevini başlatmaz.
Use Kaspersky Sandbox for protection	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security nesneleri tarama için varsayılan olarak Kaspersky Sandbox'a gönderir.
Protection scope	**Koruma kapsamı**
Schedule settings	*(geçiş gerçekleşmez)* 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 Beyanı** Kaspersky Endpoint Security, uygulama yüklendiğinde, yeni bir ilke oluşturulduğunda veya Kaspersky Security Network kullanımı etkinleştirildiğinde Kaspersky Security Network Beyanı 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 uygulanacak 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	**KSN Proxy kullan**
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.

Trafik Güvenliği ayarları

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 gerçekleşmez)* Kaspersky Endpoint Security, korunan cihaza zarar vermek için kullanılabilecek meşru web kaynaklarına erişime izin verir.
Allow access to legitimate advertisement	*(geçiş gerçekleşmez)* İnternet Denetimi ayarlarında *Reklam pencereleri* web kaynağı kategorisini kullanarak meşru reklamlara erişimi yönetebilirsiniz.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security yalnızca Driver Interceptor modunu destekler.
ICAP-service connection settings	*(geçiş gerçekleşmez)* 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 gerçekleşmez)* 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	**Geçersiz sertifikalı bir etki alanını ziyaret ederken** (**Ağ ayarları** alt bölümü)
Intercept ports (Interception area)	**İzlenen bağlantı noktaları** (**Ağ ayarları** alt bölümü) Geçiş sırasında KES, **Kaspersky tarafından önerilen listeden uygulamalar için tüm bağlantı noktalarını izle** ve **Belirtilen uygulamalar için tüm bağlantı noktalarını izle** onay kutularını temizler.
Exclude ports (Interception area)	*(geçiş gerçekleşmez)*
Exclude IP addresses (Interception area)	**Güvenilir adresler** (**Ağ ayarları** alt bölümü)
Exclude processes (Interception area)	**Güvenilir uygulamalar** (**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 bağlantı noktası için ağ trafiğini taramaz. • Güvenilir uygulama ayarlarındaki diğer onay kutuları temizlenir.
Security port	*(geçiş gerçekleşmez)*
Use malicious URL database to scan web links	**İnternet adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et** (**Web Tehdidi Koruması** alt bölümü)
Use anti-phishing database to scan web pages	**İnternet adresini kimlik avı internet adresleri veritabanıyla karşılaştırarak kontrol et** (**Web Tehdidi Koruması** alt bölümü)
Use KSN for protection	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, tüm uygulama bileşenleri için KSN kullanır.
Use Trusted Zone	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security, güvenilir bölgeyi tüm bileşenlere uygular. İstisnaları güvenilir bölge ayarlarında yapılandırabilirsiniz.

Use heuristic analyzer	**Sezgisel Analiz Kullan** (**Web Tehdidi Koruması** ve **Posta Tehdidi Koruması** alt bölümleri)
Security level	*(geçiş gerçekleşmez)* 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 gerçekleşmez)* 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**: • **İşlemi engelle** • **Bildir**.
Notify about abused processes via Terminal Service	*(geçiş gerçekleşmez)* Kaspersky Endpoint Security terminal hizmetlerini desteklemez.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(geçiş gerçekleşmez)* 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 gerçekleşmez)* 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	Bilgisayar 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, piroteknik
For children	*(geçiş gerçekeşmez)*
Discrimination	Şiddet
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 yasalarınca yasaklandı
Restricted by Federal Law 436 (RF)	Rusya Federasyonu yasalarınca yasaklandı
Restricted by RF legislation	Rusya Federasyonu yasalarınca yasaklandı
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	Bilgisayar oyunları
Health and beauty	*(geçiş gerçekeşmez)*
Culture and society	*(geçiş gerçekeşmez)*
LGBT	Yetişkinlere yönelik içerik
Lotteries	Kumar, piyango, çekiliş
Medicine	*(geçiş gerçekeşmez)*
Fashion	*(geçiş gerçekeşmez)*
Music	*(geçiş gerçekeşmez)*
Drugs	Alkol, tütün, uyuşturucu
Violence	Şiddet
Discontent	*(geçiş gerçekeşmez)*
Illegal drugs	Alkol, tütün, uyuşturucu
Hate and discrimination	Şiddet
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, piroteknik
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
Tobacco	Alkol, tütün, uyuşturucu
Torrents	Torrentler
Mentioned in Federal list of extremists (RF)	Rusya Federasyonu yasalarınca yasaklandı
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
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 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 modülleri yüklenmesini denetle (sistemin 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	*(geçiş gerçekeşmez)*

untrusted by KSN	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 uygulamalar → KSN'deki tanınırlığına göre güvenilir uygulamalar** KL kategorisini içeren bir Uygulama Denetimi izin verme kuralındaki **Kişiler 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	**Güvenilir sistem sertifika deposunu kullan** (**İstisnalar** alt bölümü) **Güvenilir sistem sertifika deposu** ayarı **Güvenilen kök sertifikaları** değerine sahiptir.
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.
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.

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 gerçekeşmez)* 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 gerçekeşmez)* 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 gerçekeşmez)* 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, Anti-Cryptor for NetApp'ı desteklemez. Anti-Cryptor'ın 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. Geçişten tamamlandıktan sonra, Kaspersky Endpoint Security Güvenlik Duvarını yapılandırabilirsiniz.

Anti-Cryptor

Ağ Anti-Cryptor ayarları, **Gelişmiş Tehdit Koruması** bölümünün Davranış Tespiti alt bölümüne taşındı.

Anti-Cryptor ayarları

KSWS ayarları	KES ayarları
Operation mode: • **Statistics only** • **Active**	**Paylaşılan klasörlerin dış şifrelemesi algılandığında**: • **Bildir** • **Bağlantıyı engelle**.
Heuristic analyzer	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Davranış Tespiti için Sezgisel Analiz kullanmaz.
Configuration of protection scope:	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, korunan bilgisayarın tüm paylaşılan ağ klasörlerinin şifrelenmesini engeller.

• All shared network folders on the protected device • Only specified shared folders	
Exclusions	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, Davranış Tespiti bileşeni için kendi istisnalarına sahiptir. Geçiş işleminden sonra istisnaları elle 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 **Dosya Bütünlüğü İzleyicisi** 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** *(sınırlamalarla desteklenir)* Devre dışı bırakılan izleme kapsamı kayıtları KES'e taşınmaz. Kaspersky Endpoint Security, izleme kapsamına yalnızca etkinleştirilmiş kayıtları ekler.
Trusted users	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, izleme kapsamındaki tüm kullanıcıların eylemlerini bir güvenlik ihlali olarak kabul eder.
File operation markers	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, mevcut tüm dosya işlemi işaretleyicilerini dikkate alır.
Calculate checksum for the file if possible	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, değiştirilen dosya için bir sağlama toplamı hesaplamaz.
Exclusions	**İstisnalar**

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	*(geçiş gerçekeşmez)*

inspection	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 algılama**
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 gerçekeşmez)* Kaspersky Endpoint Security, raporları `C:\ProgramData\Kaspersky Lab\KES.21.13\Report` klasörüne kaydeder.
Remove task logs older than N day(s)	*(geçiş gerçekeşmez)* KES raporları için saklama süresini **Genel Ayarlar**, **Raporlar ve Depolama Alanı** bölümünden yapılandırabilirsiniz.
Remove from the audit log events N day(s)	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, sistem denetim raporları dahil olmak üzere tüm raporlara raporları depolama sınırlamaları uygular.
Integration with SIEM	*(geçiş gerçekeşmez)* 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 gerçekeşmez)* 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 gerçekeşmez)* 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 hakkında**
Backed up files	**Yedekleme'deki dosyalar hakkında**
Blocked hosts	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, engellenen ana bilgisayarlarla ilgili verileri otomatik olarak gönderir.

Tasks

Activation of the application

Kaspersky Endpoint Security *Application activation* görevini desteklemez (KSWS). Bir *Anahtar ekle* görevi (KES) oluşturabilir, Kurulum paketine bir lisans anahtarı ekleyebilir veya otomatik lisans anahtarı dağıtımını etkinleştirebilirsiniz.

Copying Updates

Copying Updates görev ayarları (KSWS) Güncelleme görevine (KES) taşındı.

Güncellemeleri Kopyalama görev ayarları

Kaspersky Security	Kaspersky Endpoint Security for Windows ayarları

for Windows Server 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

Kaspersky Endpoint Security *Baseline File Integrity Monitor* görevini desteklemez. Bütünlük izleme işlevi, Davranış Tespiti gibi diğer uygulama bileşenleri tarafından sağlanır.

Database Update

Database Update görev ayarları (KSWS) Güncelleme 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) Güncelleme 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	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, tüm bileşenler için proxy sunucusunu kullanır. Uygulamanın ağ seçeneklerinde proxy sunucusu bağlantısını yapılandırabilirsiniz.

to Kaspersky update servers	
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.
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) görev başlatma zamanlayıcısı için *Manuel* seçeneğine sahip.

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 klasörler dahil**
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 biçimlerini 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 uygulanacak eylem: • Temizle; temizleme başarısız olursa sil • Temizle; temizleme başarısız olursa bildir • Bildir.
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	*(geçiş gerçekeşmez)* Kaspersky Endpoint Security, çevrimdışı dosyaları bütünüyle tarar.

- **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**

Application Integrity Control

Application Integrity Control görev ayarları (KSWS) Bütünlük denetimi 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

Sihirbazdan çıkın. 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** düğmesine tıklayın.

   İlke Sihirbazı başlatılır.
5. İlke Sihirbazı talimatlarını uygulayın.
6. Bir ilke oluşturmak için Kaspersky Endpoint Security'yi seçin. Bir sonraki adıma geçin.
7. Grup ilkesi için yeni bir ad girme adımında, **Uygulamanın daha önceki bir sürümüne ilişkin ilke ayarlarını kullan** onay kutusunu seçin.
8. **Göz at**'a tıklayın ve KSWS ilkesini seçin. Bir sonraki adıma geçin.
9. Yeni İlke Sihirbazı talimatlarını sonuna kadar uygulayın.

Sihirbaz tamamlandığında, KSWS ilkesinden gelen ayarları içeren yeni bir Kaspersky Endpoint Security for Windows ilkesi oluşturulur.

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`.

- 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 Beyanının 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** 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.

- *Güncelleme* görevleri. *Güncelleme* görevinin ayarlarının doğru şekilde taşındığından emin olun. KES, KSWS'nin üç görevi yerine tek bir KES görevi kullanır. *Güncelleme* 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 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 kaldırıldıktan sonra, mevcut ytöntemlerden herhangi birini kullanarak Kaspersky Endpoint Security for Windows'u yükleyin.

Kaspersky Endpoint Security'yi yükleme

Yöneticiler genellikle KSWS'ye erişimi kısıtlamak için Parola korumasını etkinleştirir. Bu, KSWS'yi kaldırmak için parola girmeniz gerekeceği anlamına gelir. Kaspersky Endpoint Security, KSWS üzerine KES yüklerken Kaspersky Security for Windows Server'ı kaldırmak için parola aktarımını desteklemez. Parolayı yalnızca KES'i komut satırına yüklüyorsanız aktarabilirsiniz. Bu nedenle, KSWS'yi kaldırmadan önce uygulama ayarlarından Parola korumasını kapatmalı ve KSWS'den KES'e geçişi tamamladıktan sonra uygulama ayarlarından Parola korumasını tekrar açmalısınız.

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 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 ve MDR çözümleri Kaspersky Endpoint Security ile çalışmaya devam eder. Ayrıca, Kaspersky Endpoint Agent bilgisayardan kaldırılır.

[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.

   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 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 Optimum 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 Yönetim Aracısı 13.2 veya daha yüksek bir sürümün kurulu olduğundan emin olun.
- *Uygulama bileşenleri durum raporunu* görüntüleyerek yerleşik aracının çalışma durumunu kontrol edin. Bir bileşenin durumu *Yüklenmedi* ise, *Uygulama bileşenlerini değiştirme* görevini kullanarak bileşeni yükleyin.
- Kaspersky Endpoint Security for Windows'un yeni ilkesindeki Kaspersky Security Network Beyanını kabul ettiğinizden emin olun.

Uygulama bileşenleri durum raporunu kullanarak EDR Optimum işlevinin 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

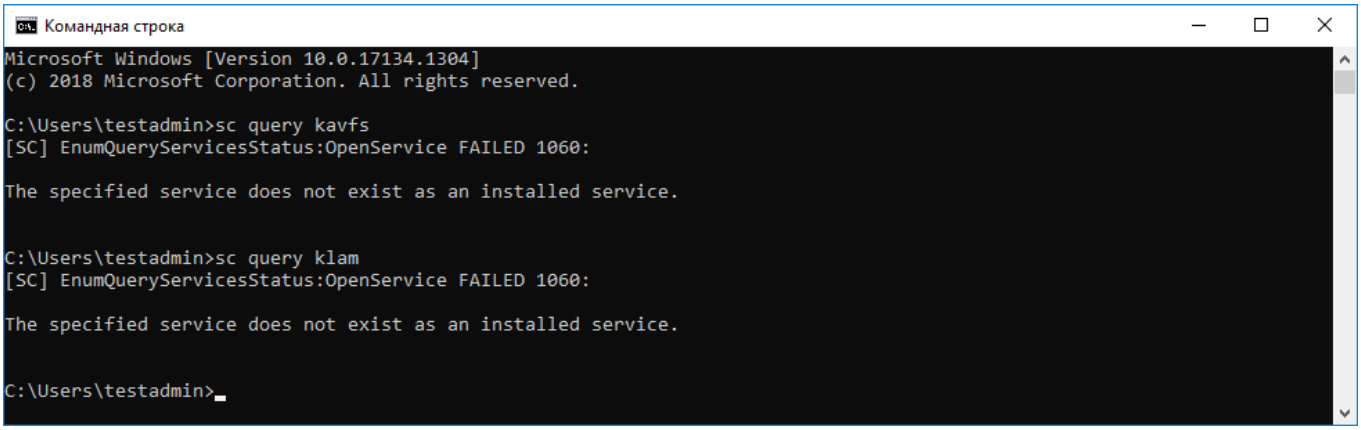
Kaspersky Security for Windows Server'ın tamamen kaldırıldığından emin olun:

- `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` klasörü mevcut değil.
- Şu hizmetler mevcut değil:
  - Kaspersky Güvenlik Hizmeti (KAVFS)
  - Kaspersky Güvenlik Yönetimi (KAVFSGT)
  - Kaspersky Security Exploit Önleme (KAVFSSLP)
  - Kaspersky Security Komut Dosyası Denetleyicisi (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	KSWS lisans anahtarı özelliklerinde otomatik anahtar dağıtımı etkinleştirildiğinde, KES, KSWS

bilgisayarlara otomatik dağıtımı.	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.
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 Tehdit 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.

[KSWS+KEA]'dan KES'e geçiş örneği

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 raporu* 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.

Uygulamayı bir Çekirdek Mod sunucusu üzerinde yönetme

Çekirdek Modundaki bir sunucunun grafik kullanıcı arabirimi yoktur. 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.

> Çekirdek Modu sunucusunda 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 Çekirdek Modu sunucusunda yönetmek, bir bilgisayarı yönetmekten farklı değildir. Uygulamayı yapılandırmak için ilkeleri ve görevleri kullanabilirsiniz.

Uygulamayı Çekirdek Modu sunucularında yönetmek, aşağıdaki özel hususları içerir:

- Çekirdek Modu sunucusunun 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 Çekirdek Modu sunucusuna 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
```

Uygulamanın komut satırından yönetimi

Kaspersky Endpoint Security'yi komut satırından yönetebilirsiniz. `HELP` komutunu yürüterek uygulama yönetimi için kullanılabilecek komutların listesini görebilirsiniz. Belirli bir komutun söz dizimi hakkında bilgi almak için `HELP <komut>` komutunu girin.

> Komutta özel karakterler atlatılmalıdır. `&`, `|`, `(`, `)`, `<`, `>`, `^` karakterlerini atlamak için `^` kaçış karakterini kullanın (örneğin `&` karakterini kullanmak için `^&` girin). `%` karakterini atlatmak için `%%` girin.

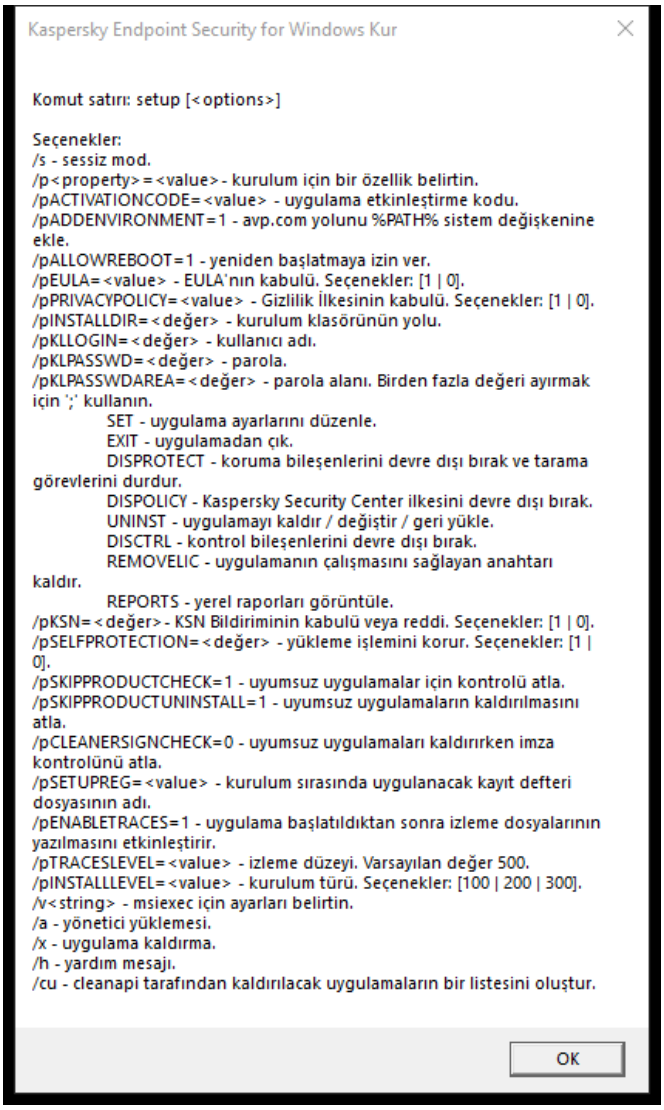
Uygulamayı yükleme

Kaspersky Endpoint Security, komut satırından aşağıdaki modlardan birinde yüklenebilir:

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

  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 yürüterek uygulama kurulumu 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] [/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1]
[/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<kullanıcı adı> /pKLPASSWD=<parola> /pKLPASSWDAREA=<parola
kapsamı>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<izleme düzeyi>] [/s]
```

veya

```
msiexec /i <dağıtım kiti adı> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1]
[KLLOGIN=<kullanıcı adı> KLPASSWD=<parola> KLPASSWDAREA=<parola kapsamı>] [ENABLETRACES=1|0
TRACESLEVEL=<izleme düzeyi>] [/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 katılmayı kabul etme veya reddetme. Bu parametre için değer belirtilmezse Kaspersky Endpoint Security ilk başlatıldığında KSN'ye katılım izni veya reddinizi onaylamanızı ister. Kullanılabilir değerler:

- `1` – KSN'ye katılmayı kabul etme.
- `0` – KSN'ye katılmayı reddetme (varsayılan değer).

Kaspersky Endpoint Security dağıtım paketi, Kaspersky Security Network ile kullanılmak üzere optimize edilmiştir. Kaspersky Security Network'e katılmamayı seçtiyseniz yükleme tamamlandıktan sonra Kaspersky Endpoint Security'yi güncellemeniz gerekir.

`ALLOWREBOOT=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`

Uyumsuz yazılım kontrolü devre dışı bırakın. Uyumsuz yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında mevcuttur. Bu parametre için hiçbir değer ayarlanmaz ve uyumsuz yazılım tespit edildiği takdirde Kaspersky Endpoint Security yüklemesi sonlandırılır.

`SKIPPRODUCTUNINSTALL=1`

Tespit edilen uyumsuz yazılımın otomatik kaldırılmasını devre dışı bırakın. Bu parametre için hiçbir değer ayarlanmazsa, Kaspersky Endpoint Security uyumsuz yazılımı kaldırmayı dener.

> Kaspersky Endpoint Security, msiexec yükleyicisi kullanılarak yüklendiğinde, uyumsuz yazılımların otomatik olarak kaldırılması etkinleştirilemez. Uyumsuz yazılımların otomatik olarak kaldırılmasını etkinleştirmek için setup_kes.exe dosyasını kullanın.

`CLEANERSIGNCHECK=0|1`

Tespit edilen uyumsuz yazılım dosyalarının dijital imzalarının doğrulanması. Uyumsuz yazılımı kaldırmak için Kaspersky Endpoint Security, yazılımın yükleyici dosyasını çalıştırır. Yükleyici dosyasının dijital imzası yoksa Kaspersky Endpoint Security, dosyayı güvenilmez olarak kabul eder ve potansiyel olarak kötü amaçlı kod çalıştırmayı önlemek için uyumsuz yazılımların kaldırılmasını durdurur. Uygulama, tespit edilen uyumsuz yazılım dosyasının dijital imzasını doğrulayamadığı takdirde, Kaspersky Endpoint Security yüklemesi bir hata vererek 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).

`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.
- Örneğin, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`.

`ENABLETRACES`

Uygulama izlemeyi etkinleştirme veya devre dışı bırakma. Kaspersky Endpoint Security başladıktan sonra, iz dosyalarını `%ProgramData%\Kaspersky Lab\KES.21.13\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, Azure sanal makinesinin durumunun Kaspersky Anti Targeted Attack Platform konsolunda doğru şekilde görüntülenmesini sağlar. Bilgisayarın performansını izlemek için Kaspersky Endpoint Security, KATA sunucularına telemetri gönderir. Telemetri, bilgisayarın bir kimliğini (Sensör Kimliği) içerir. Azure WVD uyumluluk modu, bu sanal makinelere kalıcı benzersiz bir Sensör Kimliği atanmasına olanak tanır. Uyumluluk modu kapatılırsa, Azure sanal makinelerinin çalışma şekli nedeniyle bilgisayar yeniden başlatıldıktan sonra Sensör Kimliği 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 `Zorla` güncelleme modu ve uygulama ayarlarında `Kesintisiz` modu belirtilmişse, yükseltme bilgisayarın yeniden başlatılmasıyla birlikte yüklenir (`Kesintisiz`).

`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 `<ETKİ ALANI>\<KullanıcıAdı>` (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 bağlantı noktasıdır. Varsayılan olarak 6782 bağlantı noktası kullanılır. Bağlantı noktasının 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.

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 yükleme için genel ayarlar
- install.cfg – Kaspersky Endpoint Security işleminin ayarları
- setup.reg – kayıt defteri anahtarları

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

setup.ini, install.cfg ve setup.reg dosyalarından ayarları uygulamak için bu dosyaları, Kaspersky Endpoint Security dağıtım paketini içeren klasöre yerleştirin. Setup.reg dosyasını farklı bir klasöre de koyabilirsiniz. Bunu yaparsanız, aşağıdaki uygulama yükleme komutunda dosyanın yolunu belirtmeniz gerekir: `SETUPREG=<setup.reg dosyasının yolu>`.

Uygulamayı etkinleştirme

Komut satırından uygulamayı etkinleştirmek için

komut satırına şu dizeyi yazın:

```
avp.com license /add <etkinleştirme kodu ya da anahtar dosyası> [/login=<kullanıcı adı> /password=
<parola>]
```

Parola Koruması etkinleştirildiyse kullanıcı hesabı kimlik bilgilerini (`/login=<kullanıcı adı> /password=<parola>`) girmelisiniz.

Uygulamayı kaldır

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. 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 parolayla korunmuyorsa:

     `setup_kes.exe /s /x`

     veya

     `msiexec.exe /x <GUID> /qn`

     `<GUID>` uygulamanın benzersiz kimliğidir. Aşağıdaki komutu kullanarak uygulamanın GUID'ini bulabilirsiniz:

     `wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber`
   - Kaldırma işlemi parolayla korunuyorsa:

     `setup_kes.exe /pKLLOGIN=<kullanıcı adı> /pKLPASSWD=<parola> /s /x`

     veya

     `msiexec.exe /x <GUID> KLLOGIN=<kullanıcı adı> KLPASSWD=<parola> /qn`

Örnek:

`msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=!Password1 /qn`

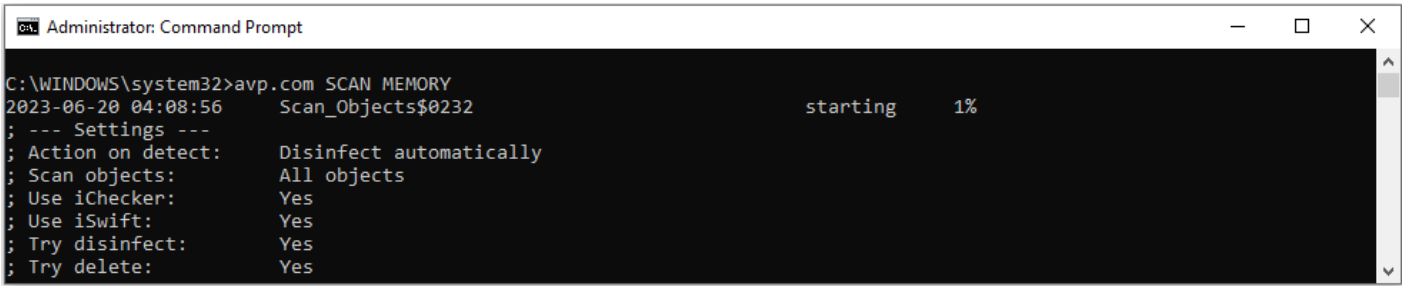
AVP komutları

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.
3. Komut yürütmek için aşağıdakini girin:

   avp.com <komut> [seçenekler]

Böylece Kaspersky Endpoint Security, komutu yürütecektir (aşağıdaki şekle bakın).



Uygulamanın komut satırından yönetimi

SCAN. Kötü Amaçlı Yazılım Taraması

Kötü Amaçlı Yazılım Taraması görevini çalıştır.

Komut söz dizimi

```
avp.com SCAN [<tarama kapsamı>] [<tehdit algılandığında yapılacak işlem>] [<dosya türleri>] [<tarama istisnaları>] [/R[A]:<rapor dosyası>] [<tarama teknolojileri>] [/C:<kötü amaçlı yazılım tarama ayarlarını içeren dosya>]
```

Tarama kapsamı

`<taranacak dosyalar>` — 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

`/MEMORY` — Çekirdek belleği tara

`/STARTUP` — İşletim sistemi başlatılırken yüklenen Nesneleri tara

`/MAIL` — Outlook posta kutusunu tara

`/REMDRIVES` — Çıkarılabilir sürücüleri tara.

`/FIXDRIVES` — Sabit sürücüleri tara.

`/NETDRIVES` — Ağ sürücülerini tara.

`/QUARANTINE` — Kaspersky Endpoint Security Yedeklemesindeki dosyaları tara.

`/@:<list.lst dosyası>` — 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 uygulanacak eylem

`/i0` **Bildir**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilmeleri halinde virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.

`/i1` **Temizle; temizleme başarısız olursa engelle**. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme mümkün değilse Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.

`/i2` **Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.

Bu eylem varsayılan olarak seçilmiştir.

`/i3` Virüslü olduğu algılanan dosyaları temizle. Temizleme başarısız olursa virüslü dosyaları sil. Ayrıca virüslü dosya temizlenemez veya silinemezse birleşik dosyaları da (örneğin, arşivler) sil.

`/i4` Virüslü dosyaları 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:b` Posta veritabanları, gelen ve giden e-postalar tarama kapsamında değildir.

`-e:<dosya maskesi>` Dosya maskesiyle eşleşen dosyalar tarama kapsamında değildir. Örneğin:

- "`*.exe`" maskesi, exe uzantısı olan tüm dosya yollarını içerir.
- `Örnek*` maskesi, ÖRNEK adlı tüm dosya yollarını içerir.

`-e:<saniye>` Tarama işlemi belirtilen süre sınırını (saniye cinsinden) aşan dosyalar tarama kapsamında değildir.

`-es:<megabayt>` 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:<rapor dosyası>` Yalnızca önemli olayları rapor dosyasına kaydet.

`/RA:<rapor dosyası>` 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 tarama dışında tutulur. iSwift teknolojisi, NTFS dosya sistemi için iChecker teknolojisinin geliştirilmiş bir halidir.

Gelişmiş ayarlar

`/C:<kötü amaçlı yazılım tarama ayarlarını içeren dosya>` — *Kötü Amaçlı Yazılım Taraması* görevi ayarları içeren dosya. Dosya manuel olarak oluşturulmalı ve TXT biçiminde kaydedilmelidir. Dosyada şu içerikler olabilir: `[<tarama kapsamı>] [<tehdit algılandığında yapılacak işlem>] [<dosya türleri>] [<tarama istisnaları>] [/R[A]:<rapor dosyası>] [<tarama teknolojileri>]`.

Örnek:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Veritabanlarını ve uygulama yazılım modüllerini güncelleme

Güncelleme görevini çalıştırın.

Komut söz dizimi

```
avp.com UPDATE [local]["<güncelleme kaynağı>"] [/R[A]:<rapor dosyası>] [/C:<güncelleme ayarlarını içeren dosya>]
```

Güncelleme görevi ayarları

`local` — Uygulama yüklendikten sonra otomatik olarak oluşturulan *Güncelleme* görevinin başlatılması. *Güncelleme* görevinin ayarlarını, yerel uygulama arabiminde veya Kaspersky Security Center konsolunda değiştirebilirsiniz. Bu ayar yapılandırılmazsa Kaspersky Endpoint Security, varsayılan ayarlarla veya komutta belirtilen ayarlarla *Güncelleme* görevini başlatır. *Güncelleme* görevi ayarlarını aşağıdaki şekilde yapılandırabilirsiniz:

- `UPDATE` varsayılan ayarlarla *Güncelleme* görevini başlatır: güncelleme kaynağı Kaspersky güncelleme sunucularıdır, hesap Sistemdir ve diğer varsayılan ayarlar kullanılır.
- `UPDATE local` kurulum sonrasında otomatik olarak oluşturulan *Güncelleme* görevini (önceden tanımlanmış görev) başlatır.
- `UPDATE <günceleme ayarları>` *Güncelleme* görevini manuel olarak tanımlanmış ayarlarla başlatır (aşağıya bakınız).

Güncelleme kaynağı

`"<güncelleme kaynağı>”` — 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:<rapor dosyası>` — Yalnızca önemli olayları rapor dosyasına kaydet.

`/RA:<rapor dosyası>`	Tüm olayları bir rapor dosyasına kaydet.

Gelişmiş ayarlar

`/C:<güncelleme ayarlarını içeren dosya>`	*Güncelleme* görevi ayarları içeren dosya. Dosya manuel olarak oluşturulmalı ve TXT biçiminde kaydedilmelidir. Dosyada şu içerikler olabilir: `["<güncelleme kaynağı>"] [/R[A]:<rapor dosyası>]`.

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 al. 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.

Komut söz dizimi

```
avp.com ROLLBACK [/R[A]:<rapor dosyası>]
```

Olayları bir rapor dosyası moduna kaydetme (yalnızca Tarama, Güncelleme ve Geri alma profilleri için)

`/R:<rapor dosyası>`	Yalnızca önemli olayları rapor dosyasına kaydet.
`/RA:<rapor dosyası>`	Tüm olayları bir rapor dosyasına kaydet.

Örnek:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. İzleme

İzlemeyi etkinleştir/devre dışı bırak. 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.21.13\Traces` klasöründe saklanır. Varsayılan olarak izleme devre dışı bırakılmıştır.

Komut söz dizimi

```
avp.com TRACES on|off [<izleme düzeyi>] [<gelişmiş ayarlar>]
```

İzleme düzeyi

`<izleme düzeyi>`	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`	`dbg`, `file` ve `mem` parametreleriyle bir komut çalıştırın.
`dbg`	OutputDebugString işlevini kullanıp izleme dosyasını kaydedin. OutputDebugString işlevi, bir karakter dizesini ekranda göstermesi için uygulama hata ayıklayıcısına gönderir. Ayrıntılar için MSDN web sitesini ziyaret edin.
`file`	Bir izleme dosyasını kaydedin (boyut sınırı yoktur).
`rot`	Boyutları ve sayıları sınırlı dosyalara izleri kaydedin ve maksimum boyuta ulaşıldığında eski dosyaların üzerine yazın.
`mem`	İzleri döküm dosyalarına kaydedin.

Örnekler:

```
avp.com TRACES on 500
avp.com TRACES on 500 dbg
avp.com TRACES off
avp.com TRACES on 500 dbg mem
avp.com TRACES off file
```

START. Profili başlatma

Profili başlatın (örneğin, veritabanlarını güncellemek veya bir koruma bileşenini etkinleştirmek için).

```
Komut söz dizimi
avp.com START <profil> [/R[A]:<rapor dosyası>]
```

Profil

`<profil>`	Profil adı. *Profil* bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Kullanılabilir profillerin listesini `HELP START` komutunu yürüterek görebilirsiniz.

Olayları bir rapor dosyası moduna kaydetme (yalnızca Tarama, Güncelleme ve Geri alma profilleri için)

`/R:<rapor dosyası>`	Yalnızca önemli olayları rapor dosyasına kaydet.
`/RA:<rapor dosyası>`	Tüm olayları bir rapor dosyasına kaydet.

Örnek:

```
avp.com START Scan_Objects
```

STOP. Profili durdurma

Çalışan profili durdurun (örneğin, taramayı durdur, çıkarılabilir sürücü taramasını durdur veya bir koruma bileşenini devre dışı bırak).

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcı **Koruma bileşenlerini devre dışı bırak** ve **Denetim bileşenlerini devre dışı bırak** izinlerine sahip olmalıdır.

```
Komut söz dizimi
avp.com STOP <profil> /login=<kullanıcı adı> /password=<parola>
```

Profil

`<profil>`	Profil adı. *Profil* bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Kullanılabilir profillerin listesini `HELP STOP` komutunu yürüterek görebilirsiniz.

Kimlik Doğrulama

`/login=<kullanıcı adı> /password=<parola>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

STATUS. Profil durumu

Uygulama profilleri için durum bilgilerini görüntüleyin (örneğin, `çalışıyor` veya `tamamlandı`). Kullanılabilir profillerin listesini `HELP STATUS` komutunu yürüterek görebilirsiniz.

Kaspersky Endpoint Security, servis profillerinin durumu hakkındaki bilgileri de görüntüler. Kaspersky Teknik Destek ile iletişim kurarken servis profillerinin durumu hakkındaki bilgiler gerekebilir.

```
Komut söz dizimi
avp.com STATUS [<profil>]
```

Komutu bir profil olmadan girerseniz Kaspersky Endpoint Security, uygulamanın tüm profillerinin durumunu görüntüler.

STATISTICS. Profil işlem istatistikleri

Bir uygulama profili hakkındaki istatistiksel bilgileri görüntüleyin (örneğin, tarama süresi veya algılanan tehdit sayısı.) Kullanılabilir profillerin listesini `HELP STATISTICS` komutunu çalıştırarak görebilirsiniz.

```
Komut söz dizimi
avp.com STATISTICS <profil>
```

RESTORE. Yedekleme konumundan dosyaları geri yükleme

Bir dosyayı Yedekleme'den orijinal klasörüne geri yükleyebilirsiniz. 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.21.13\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.

Komut söz dizimi

```
avp.com RESTORE [/REPLACE] <dosya adı> /login=<kullanıcı adı> /password=<parola>
```

Gelişmiş ayarlar

`/REPLACE`	Var olan bir dosyanın üzerine yaz.
`<dosya adı>`	Geri yüklenecek dosyanın adı.

Kimlik Doğrulama

`/login=<kullanıcı adı> /password=<parola>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Uygulama ayarlarını dışa aktarma

Kaspersky Endpoint Security ayarlarını bir dosyaya dışa aktar. Dosya, `C:\Windows\SysWOW64` klasöründe yer alır.

Komut söz dizimi

```
avp.com EXPORT <profil> <dosya adı>
```

Profil

`<profil>`	Profil adı. *Profil* bir Kaspersky Endpoint Security bileşeni, görevi veya özelliğidir. Kullanılabilir profillerin listesini `HELP EXPORT` komutunu yürüterek görebilirsiniz `.`

Dışa aktarılacak dosya

`<dosya adı>`	Uygulama ayarlarının dışa aktarılacağı dosyanın adı. Kaspersky Endpoint Security ayarlarını DAT veya CFG yapılandırma dosyası, TXT metin dosyası veya XML belgesine dışa aktarabilirsiniz.

Örnekler:

```
avp.com EXPORT ids ids_config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Uygulama ayarlarını içe aktarma

Kaspersky Endpoint Security ayarlarını `EXPORT` komutuyla oluşturulmuş bir dosyadan içe aktarır.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Uygulama ayarlarını yapılandır** izninin olması gerekir.

Komut söz dizimi

```
avp.com IMPORT <dosya adı> /login=<kullanıcı adı> /password=<parola>
```

İçe aktarılacak dosya

`<dosya adı>`	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=<kullanıcı adı> /password=<parola>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Anahtar dosyasını uygulama

Kaspersky Endpoint Security'yi etkinleştirmek için anahtar dosyasını uygulayın. Uygulama zaten etkinleştirilmişse anahtar rezerve anahtar olarak eklenir.

Komut söz dizimi

```
avp.com ADDKEY <dosya adı> [/login=<kullanıcı adı> /password=<parola>]
```

Anahtar dosyası

`<dosya adı>`	Anahtar dosyası adı.

Kimlik Doğrulama

`/login=<kullanıcı adı> /password=<parola>`	Kullanıcı hesabı kimlik bilgileri. Bu kimlik bilgilerinin yalnızca Parola koruması etkinleştirildiğinde girilmesi gerekir.

Örnek:

```
avp.com ADDKEY file.key
```

LICENSE. Lisanslama

İşlemleri Kaspersky Endpoint Security lisans anahtarlarıyla veya EDR Optimum veya EDR Expert (Kaspersky Endpoint Detection and Response Eklentisi) anahtarlarıyla gerçekleştirin.

Bu komutu yürütmek ve bir lisans anahtarını kaldırmak için Parola koruması etkinleştirilmelidir. Kullanıcının **Anahtarı kaldır** izninin olması gerekir.

Komut söz dizimi

```
avp.com LICENSE <işlem> [/login=<kullanıcı adı> /password=<parola>]
```

İşlem

`/ADD <dosya adı>`	Kaspersky Endpoint Security'yi etkinleştirmek için anahtar dosyasını uygulayın. Uygulama zaten etkinleştirilmişse anahtar rezerve anahtar olarak eklenir.
`/ADD <etkinleştirme kodu>`	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 EDR`	Kaspersky Endpoint Detection and Response Eklentisi lisansının durumunu güncelleyin. Uygulama, Kaspersky etkinleştirme sunucularından güncel lisans durumu bilgilerini alır.
`/DEL /login=<kullanıcı adı> /password=<parola>`	Uygulamanın lisans anahtarını kaldırın. Rezerve anahtar da kaldırılacaktır.
`/DEL EDR /login=<kullanıcı adı> /password=<parola>`	Kaspersky Endpoint Detection and Response Eklentisi lisans anahtarını kaldırın. Rezerve anahtar da kaldırılacaktır.

Kimlik Doğrulama

`/login=<kullanıcı adı> /password=<parola>`	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 EDR /login=KLAdmin /password=!Password1
```

RENEW. Lisans satın alma

Lisansınızı satın almak veya yenilemek için Kaspersky web sitesini açın.

PBATESTRESET. Diski şifrelemeden önce disk denetimi sonuçlarını sıfırla

Hem Kaspersky Disk Encryption hem de BitLocker Drive Encryption teknolojileri dahil olmak üzere Tam Disk Şifreleme (FDE) için uyumluluk denetimi sonuçlarını sıfırla.

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.

EXIT. Uygulamadan çık

Kaspersky Endpoint Security'den çıkar. Uygulama, bilgisayarın RAM'inden kaldırılacaktır.

Bu komutu yürütmek için Parola koruması etkinleştirilmelidir. Kullanıcının **Uygulamadan çık** izninin olması gerekir.

```
Komut söz dizimi
avp.com EXIT /login=<kullanıcı adı> /password=<parola>
```

EXITPOLICY. İlkeyi devre dışı bırakma

Bilgisayardaki Kaspersky Security Center ilkesini devre dışı bırakır. 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.

```
Komut söz dizimi
avp.com EXITPOLICY /login=<kullanıcı adı> /password=<parola>
```

STARTPOLICY. İlkeyi etkinleştirme

Bilgisayardaki Kaspersky Security Center ilkesini etkinleştirir. Uygulama ayarları ilkeye göre yapılandırılır.

DISABLE. Korumayı devre dışı bırakma

Kaspersky Endpoint Security lisansı sona eren bir bilgisayardaki Dosya Tehdidi Korumasını devre dışı bırakır. Uygulamanın etkinleştirilmediği ya da geçerli bir lisansa sahip olmayan bir bilgisayarda bu komut çalıştırılamaz.

SPYWARE. Casus yazılım algılama

Casus yazılım algılamayı etkinleştir / devre dışı bırak. Varsayılan olarak casus yazılım algılama etkindir.

```
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.

```
Komut söz dizimi
avp.com KSN /global | /private <dosya adı>
```

Kaspersky Security Network yapılandırma dosyası	
`<dosya adı>`	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
```

KESCLI komutları

KESCLI komutları, OPSWAT bileşeni kullanılarak bilgisayar korumasının durumu hakkında bilgi almanızı ve *Kötü Amaçlı Yazılım Taraması* ve *Güncelleme* görevleri gibi standart görevleri gerçekleştirmenizi sağlar.

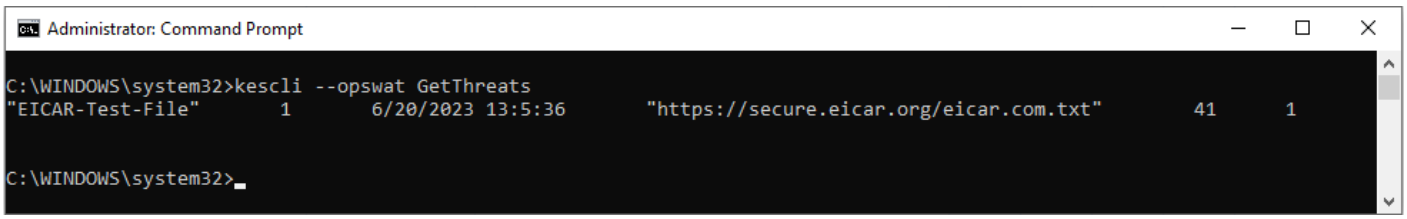
KESCLI komutlarının listesini `--help` komutunu ya da `-h` kısaltılmış komutunu kullanarak görüntüleyebilirsiniz.

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.
3. Komut yürütmek için aşağıdakini girin:

   kescli <command> [seçenekler]

   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 çalıştırın.

Görevi çalıştırmak için yönetici Yerel görevlerin kullanılmasına izin vermelidir.

```
Komut söz dizimi
kescli --opswat Scan "<tarama kapsamı>" <tehdit tespit edildiğinde yapılacak işlem>
```

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

`<taranacak dosyalar>`	`;`-dosyaların ve klasörlerin boşlukla ayrılmış bir listesi. Örneğin `"C:\Program Files (x86)\Example Folder"`.

Tehdit algılandığında uygulanacak eylem

`0`	**Bildir**. 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, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları 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 hakkında bilgi alın:

- `1` – tarama devam ediyor.
- `0` – tarama çalışmıyor.

```
Komut söz dizimi
kescli --opswat GetScanState
```

GetLastScanTime. Taramanın tamamlanma süresinin belirlenmesi

Son *Kötü Amaçlı Yazılım Taraması* (Tam Tarama) görevinin tamamlanmasının tarihi ve saati hakkında bilgiler alın.

```
Komut söz dizimi
kescli --opswat GetLastScanTime
```

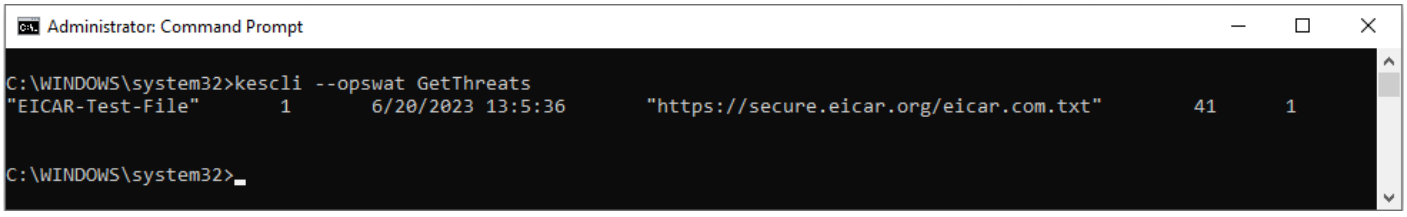
GetThreats. Tespit edilen tehditler hakkında veriler alma

Algılanan tehditlerin bir listesini alın (*Tehdit raporu*). Bu rapor, rapor oluşturmadan önceki son 30 gün boyunca gerçekleşen tehditler ve virüs aktivitesi hakkında bilgi içerir.

```
Komut söz dizimi
kescli --opswat GetThreats
```

Bu komut çalıştırıldığında, Kaspersky Endpoint Security şu biçimde bir yanıt gönderir:

```
<tespit edilen nesnenin adı> <nesnenin türü> <tespit edilme tarihi ve saati> <dosyanın yolu> <tehdit algılandığında uygulanacak eylem> <tehdit tehlike düzeyi>
```



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	`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 uygulanacak 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

Güncelleme görevini çalıştırın. Kaspersky Endpoint Security varsayılan kaynağı kullanır: Kaspersky güncelleme sunucuları.

Görevi çalıştırmak için yönetici Yerel görevlerin kullanılmasına izin vermelidir.

```
Komut söz dizimi
kescli --opswat UpdateDefinitions
```

`GetDefinitionsetState` komutunu kullanarak geçerli antivirüs veritabanlarının yayınlanma tarihini ve saatini görüntüleyebilirsiniz.

GetDefinitionState. Güncellemenin tamamlanma süresinin belirlenmesi

Kullanılan antivirüs veritabanlarının yayınlanma tarihi ve saati hakkında bilgi alın.

```
Komut söz dizimi
kescli --opswat GetDefinitionState
```

EnableRTP. Korumanın etkinleştirilmesi

Bilgisayarda şu Kaspersky Endpoint güvenlik koruma bileşenlerini etkinleştirin: 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).

```
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 Tehdidi Koruması bileşeninin çalışma durumu hakkında bilgiler alın:

- `1` – bileşen etkinleştirilmiş.
- `0` – bileşen devre dışı.

```
Komut söz dizimi
kescli --opswat GetRealTimeProtectionState
```

Version. Uygulama sürümünün tanımlanması

Kaspersky Endpoint Security for Windows sürümünün tanımlanması.

```
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 yürüterek uygulama yönetimi için kullanılabilecek komutların listesini görebilirsiniz. Belirli bir komutun söz dizimi hakkında bilgi almak için `HELP <komut>` 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. Komut yürütmek için aşağıdakini girin:

   ```
   avp.com <komut> [seçenekler]
   ```

   Böylece Kaspersky Endpoint Security, komutu yürütecektir.

SANDBOX. Kaspersky Sandbox Yönetimi

Kaspersky Sandbox bileşenini yönetme komutları:

- Kaspersky Sandbox bileşenini etkinleştirin veya devre dışı bırakın.

  Kaspersky Sandbox bileşeni, Kaspersky Sandbox çözümü ile birlikte çalışabilirlik sunar.

- Kaspersky Sandbox bileşenini yapılandırın:

  - Bilgisayarı Kaspersky Sandbox sunucularına bağlayın.

    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 Kaspersky Sandbox sunucularını yapılandırma hakkında ayrıntılar için Kaspersky Sandbox Yardım içeriğine bakın.

  - Kaspersky Sandbox sunucusu için bağlantı zaman aşımını yapılandırın.

    Kaspersky Sandbox sunucusundan bir nesne tarama isteğine yanıt almak için belirlenen zaman aşımı süresi. Zaman aşımı süresi geçtikten sonra Kaspersky Sandbox, isteği bir sonraki sunucuya yönlendirir. Zaman aşımının değeri bağlantının hızına ve stasbilitesine bağlıdır. Varsayılan değer 5 saniyedir.

  - Bilgisayar ve Kaspersky Sandbox sunucuları arasında güvenilir bir bağlantı yapılandırın.

    Kaspersky Sandbox sunucularıyla güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Ardından, sertifikayı Kaspersky Sandbox sunucularına ve Kaspersky Endpoint Security ilkesine eklemelisiniz. Sertifikayı hazırlama ve sertifikayı sunuculara eklemeyle ilgili ayrıntılar için Kaspersky Sandbox Yardım içeriğine bakın.

- Bileşenin geçerli ayarlarını görüntüleyin.

```
Komut söz dizimi
avp.com stop sandbox [/login=<kullanıcı adı> /password=<parola>]

avp.com start sandbox
```

```
avp.com sandbox /set [--tls=yes|no] [--servers=<sunucu adresi>:<bağlantı noktası>] [--timeout=<Kaspersky Sandbox sunucusu zaman aşımı (ms)>] [--pinned-certificate=<TLS sertifikasının yolu>][/login=<kullanıcı adı> /password=<parola>]

avp.com sandbox /show
```

İşlem

`stop`	Kaspersky Sandbox bileşenini devre dışı bırak.
`start`	Kaspersky Sandbox bileşenini etkinleştir.
`set`	Kaspersky Sandbox bileşenini yapılandırın. Şu ayarları değiştirebilirsiniz: • Güvenilir bir bağlantı kullan (`--tls`); • Bir TLS sertifikası ekle (`--pinned-certificate`); • Kaspersky Sandbox sunucusu bağlantı zaman aşımını ayarla (`--timeout`); • Kaspersky Sandbox sunucuları ekle (`--servers`).

`show`	Bileşenin geçerli ayarlarını görüntüleyin. Aşağıdaki yanıtı alırsınız:
	`sandbox.timeout=<Kaspersky Sandbox sunucusu zaman aşımı (ms)>`
	`sandbox.tls=<güvenilir bağlantı durumu>`
	`sandbox.servers=<Kaspersky Sandbox sunucularının listesi>`

Kimlik Doğrulama

`/login=<kullanıcı adı> /password=<parola>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek:

```
avp.com start sandbox

avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"

avp.com sandbox /set --servers=10.10.111.0:147
```

ÖNLEME. Yürütme önleme yönetimi

Yürütme Engellemeyi devre dışı bırakın veya yürütme engelleme kuralları listesi de dahil olmak üzere geçerli bileşen ayarlarını gösterin.

```
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: <kural kimliği>
target: script|process|document
md5: <dosyanın MD5 karması>
```

```
sha256: <dosyanın SHA256 karması>
pattern: <nesnenin yolu>
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 argümanın 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).

İZOLASYON. Ağ izolasyonunu yönetme

Bilgisayarın ağ izolasyonunu kapatın veya bileşenin mevcut ayarlarını görüntüleyin. Bileşen ayarlarında istisnalara eklenen ağ bağlantılarının bir listesi de yer alır.

Komut söz dizimi:

```
avp.com isolation /OFF /login=<kullanıcı adı> /password=<parola>

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 yükleyebilirsiniz. *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 Detection and Response çözümleriyle çalışırken kullanır: EDR Optimum, EDR Expert, KATA (EDR), Kaspersky Sandbox. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantinayı yönetmeyle ilgili ayrıntılar için lütfen Kaspersky Sandbox Yardımı, Kaspersky Endpoint Detection and Response Optimum Yardımı, Kaspersky Endpoint Detection and Response Expert Yardımı ve Kaspersky Anti Targeted Attack Platform Yardımı'na başvurun.

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.

Komut söz dizimi

```
avp.com RESTORE [/REPLACE] <dosya adı> /login=<kullanıcı adı> /password=<parola>
```

Gelişmiş ayarlar

`/REPLACE`	Var olan bir dosyanın üzerine yaz.
`<dosya adı>`	Geri yüklenecek dosyanın adı.

Kimlik Doğrulama

`/login=<kullanıcı adı> /password=<parola>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

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

Güvenlik İhlali Göstergelerini tara (IOC) görevini çalıştırın. *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.

```
Komut söz dizimi
```

avp.com IOCSCAN <IOC dosyasının tam yolu>|/path=<IOC dosyaları klasörünün yolu> [/process=on|off] [/hint=<bir işlemin yürütülebilir dosyasının tam yolu|tam dosya yolu>] [/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=<olay yayınlanma tarihi>] [/channels=<kanalların listesi>] [/files=on|off] [/drives=< tümü|sistem|kritik|özel>] [/excludes= <istisnalar listesi>][/scope=<taranacak klasörler listesi>]

IOC dosyaları

`<IOC dosyasının tam yolu>`	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=<IOC dosyalarını içeren klasörün yolu>`	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=<işlemin yürütülebilir dosyasının tam yolu|dosyanın tam yolu>`

IOC taraması gerçekleştirirken dosya verilerini analiz et (ProcessItem ve FileItem terimleri).

Aşağıdaki yöntemlerden biriyle bir dosya seçebilirsiniz:

- `<işlemin yürütülebilir dosyasının tam yolu>` – ProcessItem terimi;
- `<dosyanın tam yolu>` – 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, ProcessItem 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 bağlantı noktaları 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.
`/datetime=<olay yayınlanma tarihi>`	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=<kanalların listesi>`	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 (Tam Adı 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 `<tümü>`. • İşletim sisteminin kurulu olduğu klasörlerdeki dosyalar için `<sistem>`. • Kullanıcı ve sistem klasörlerindeki geçici dosyalar için `<kritik>`. • Kullanıcı tanımlı kapsamlardaki dosyalar için `<özel>` (`/scope=<taranacak klasörler listesi>`). Argüman belirtilmezse tarama kritik alanlar için yapılır.
`/excludes=<istisnalar listesi>`	Fileltem IOC belgesi için verileri analiz ederken istisna kapsamını ayarlayın. Boşluklarla ayrılmış birden çok yol belirtebilirsiniz.
`/scope=<taranacak klasörler listesi>`	Fileltem IOC belgesi için verileri analiz ederken kullanıcı tanımlı IOC tarama kapsamı (`/drives=custom`). Boşluklarla ayrılmış birden çok yol belirtebilirsiniz.

Komut dönüş değerleri:

- `-1`, bilgisayarda yüklü olan Kaspersky sürümü tarafından komutun desteklenmediği anlamına gelir.
- `0`, komutun başarıyla yürütüldüğü anlamına gelir.
- `1`, komuta zorunlu bir argümanın 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 bileşenini etkinleştirmek için BLOB yapılandırma dosyasıyla işlemler gerçekleştirin. 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 ( ).

Komut söz dizimi

```
avp.com MDRLICENSE <işlem> [/login=<kullanıcı adı> /password=<parola>]
```

İşlem

`/ADD <dosya adı>`	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=<kullanıcı adı> /password=<parola>`	Gerekli Parola koruma izinlerine sahip kullanıcı hesabının kimlik bilgileri.

Örnek:

```
avp.com MDRLICENSE /ADD file.key

avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1
```

EDRKATA. EDR (KATA) ile entegrasyon

Endpoint Detection and Response bileşenini (KATA) yönetmek için komutlar:

- EDR bileşenini (KATA) etkinleştirin veya devre dışı bırakın.
  EDR bileşeni (KATA), Kaspersky Anti Targeted Attack Platform çözümü ile birlikte çalışabilirlik sağlar.
- Kaspersky Anti Targeted Attack Platform sunucularına bağlantıyı yapılandırın.
- Bileşenin geçerli ayarlarını görüntüleyin.

Komut söz dizimi

```
avp.com START EDRKATA

avp.com STOP EDRKATA

avp.com edrkata /set /servers=<sunucu adresi>:<bağlantı yolu> /server-certificate=<TLS sertifikasının yolu> [/timeout=<Merkezi Düğüm sunucu bağlantısı zaman aşımı(s)>] [/sync-period=<Merkezi Düğüm sunucusu senkronizasyon süresi (min)>]

avp.com edrkata /show
```

İşlem

`stop`	EDR bileşenini (KATA) devre dışı bırakın.
`start`	EDR bileşenini (KATA) etkinleştirin.
`set`	EDR bileşenini (KATA) yapılandırın. Şu ayarları değiştirebilirsiniz: • Merkezi Düğüm sunucuları (`servers=<sunucu adresi>:<bağlantı noktası>`) ekleyin. • Bir TLS sertifikası (`server-certificate=<TLS sertifikasına giden yol>`) ekleyin. • Merkezi Düğüm sunucusu bağlantı zaman aşımını ayarlayın (`/timeout=<Merkezi Düğüm sunucusu bağlantısı zaman aşımı (saniye)>`).

- Merkezi Düğüm sunucusu ile senkronizasyon süresini ayarlayın (`/sync-period=<Merkezi Düğüm sunucusu senkronizasyon süresi (dakika)>`).

`show` Bileşenin geçerli ayarlarını görüntüleyin.

Hata kodları

Uygulama ile komut satırından çalışılırken hatalar meydana gelebilir. Hatalar meydana geldiğinde, Kaspersky Endpoint Security bir hata mesajı görüntüler, örneğin `Hata: 'EntAppControl' görevi başlatılamıyor`. Kaspersky Endpoint Security ayrıca bir kod biçiminde ek bilgiler de gösterebilir, örneğin, `hata=8947906D` (aşağıdaki tabloya bakın).

Hata kodları

Hata kodu	Açıklama
09479001	Bu anahtar zaten kullanımda
0947901D	Lisansın süresi sona erdi. Veritabanı güncellemeleri kullanılamıyor
89479002	Anahtar bulunamadı
89479003	Dijital imza eksik veya bozuk
89479004	Veri 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	Lisans kitaplığı yüklenmedi
8947900F	Veritabanları bozuk ya da manuel olarak güncellenmiş
89479010	Veritabanları bozuk
89479011	Bir rezerve anahtar eklemek için geçersiz anahtar dosyası kullanılamaz
89479012	Sistem hatası
89479013	Bozuk anahtarların red listesi
89479014	Dosya imzası, Kaspersky'nin dijital imzası ile eşleşmiyor
89479015	Bir deneme lisansı anahtarını ticari lisans anahtarı olarak kullanamazsınız
89479016	Uygulamanın beta sürümünü kullanmak için beta testler için lisans 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 eksik, bozuk veya Kaspersky dijital imzasıyla eşleşmiyor

8947901C	Karşılık gelen ticari olmayan lisansın süresi dolduysa bir 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 başka bir anahtar zaten etkin durumda
89479020	Bozuk veya kayıp anahtarların red listesi
89479021	Güncelleme açıklaması eksik veya bozuk
89479022	Dahili veriler bu uygulamayla uyumlu değil
89479023	Bir rezerve anahtar eklemek için geçersiz 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 yanlış etkinleştirme kodu içeriyor
89479027	Yanıt durumu alınamadı
89479028	Geçici dosya kaydedilirken hata meydana geldi
89479029	Hatalı etkinleştirme kodu girilmiş veya bilgisayarda geçersiz sistem tarihi ayarlanmış. Bilgisayarınızdaki sistem tarihini kontrol edin
8947902A	Anahtar bu uygulama ile uyumlu değil veya lisansın süresi dolmuş
8947902B	Anahtar dosyası alınamadı Yanlış etkinleştirme kodu girildi
8947902C	Etkinleştirme kodu 400 hatası verdi
8947902D	Etkinleştirme kodu 401 hatası verdi
8947902E	Etkinleştirme kodu 403 hatası verdi
8947902F	Etkinleştirme sunucusunda gerekli kaynak yok. Etkinleştirme kodu 404 hatası verdi. Lütfen internet bağlantısı ayarlarınızı kontrol edin
89479030	Etkinleştirme kodu 405 hatası verdi
89479031	Etkinleştirme kodu 406 hatası verdi
89479032	Proxy kimlik doğrulaması gerekiyor. Lütfen ağ ayarlarınızı kontrol edin
89479033	İstek zaman aşımına uğradı
89479034	Etkinleştirme kodu 409 hatası verdi
89479035	Etkinleştirme sunucusunda gerekli kaynak yok. Etkinleştirme kodu 410 hatası verdi. Lütfen internet bağlantısı ayarlarınızı kontrol edin
89479036	Etkinleştirme kodu 411 hatası verdi
89479037	Etkinleştirme kodu 412 hatası verdi
89479038	Etkinleştirme kodu 413 hatası verdi
89479039	Etkinleştirme kodu 414 hatası verdi
8947903A	Etkinleştirme kodu 415 hatası verdi
8947903C	İç 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 tahsis hatası
89479049	Parametreler ANSI dizesine (URL, klasör, aracı) dönüştürülürken hata
8947904A	Çalışan iş parçacığı oluşturulurken hata oluştu
8947904B	Çalışan iş parçacığı zaten çalışıyor
8947904C	Çalışan iş parçacığı çalışmıyor
8947904D	Etkinleştirme sunucusuna anahtar dosyası bulunamadı
8947904E	Anahtar engellenmiş
8947904F	Etkinleştirme sunucusu dahili hatası
89479050	Etkinleştirme talebinde yeterli veri yok
89479053	Eklenen anahtara karşılık gelen lisansın süresi 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 aşılmış
89479058	Etkinleştirme prosedürü bir sistem hatası ile tamamlandı
89479059	Bir deneme lisansı anahtarını ticari lisans anahtarı olarak kullanamazsınız
8947905C	Etkinleştirme kodu gerekiyor
89479062	Etkinleştirme sunucusuna bağlanılamıyor
89479064	Etkinleştirme sunucusu kullanılamıyor. Lütfen İnternet bağlantı ayarlarınızı kontrol edin ve etkinleştirmeyi tekrar deneyin
89479065	Lisans süresi doldu
89479066	Aktif anahtar süresi dolmuş bir anahtarla değiştirilemez
89479067	İlgili lisansın süresi geçerli lisanstan önce doluyorsa rezerve eklenemez
89479068	Güncellenmiş abonelik anahtarı eksik
8947906A	Geçersiz etkinleştirme kodu
8947906B	Anahtar zaten aktif durumda
8947906C	Aktif ve rezerve anahtarlara karşılık gelen lisans türleri eşleşmiyor
8947906D	Bileşen lisans tarafından desteklenmiyor
8947906E	Abonelik anahtarı bir rezerve anahtar olarak eklenemiyor
89479213	Aktarım katmanı genel hatası
89479214	Etkinleştirme sunucusuna bağlanılamadı
89479215	Geçersiz web adresi biçimi

89479216	Proxy sunucusu adresi dönüştürülemedi
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 talebi gönderiminde hata
8947921C	SSL bağlantı hatası
8947921D	İşlem geri arama tarafından kesintiye uğradı
8947921E	Çok sayıda yönlendirme
8947921F	Alıcı denetimi başarısız
89479220	Etkinleştirme sunucusundan boş yanıt
89479221	Veri gönderilirken hata oluştu
89479222	Veri alınırken hata oluştu
89479223	SSL sertifikasıyla ilgili sorun
89479224	SSL şifrelemesiyle ilgili sorun
89479225	SSL sertifika merkeziyle ilgili sorun
89479226	Ağ paketinin içeriği geçersiz
89479227	Kullanıcı erişimi reddedildi
89479228	Geçersiz SSL sertifika dosyası
89479229	SSL bağlantısı kapatılamıyor
8947922A	Yinelenen hata
8947922B	İptal edilen sertifikalara sahip geçersiz dosya
8947922C	SSL sertifikası istek hatası
89479401	Bilinmeyen sunucu hatası
89479402	İç sunucu hatası
89479403	Girilen etkinleştirme kodu için anahtar yok
89479404	Aktif anahtar engellenmiş
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 gerekiyor
8947940B	Etkinleştirme süresi doldu
8947940C	Bu kodla gerçekleştirilebilecek etkinleştirmelerin sayısı aşıldı
8947940D	Geçersiz talep kimliği biçimi
8947940E	Etkinleştirme kodu zaten kullanımda

8947940F	Etkinleştirme kodu yenilenemedi
89479410	Etkinleştirme kodu bu bölge için geçerli değil
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	Hatalı etkinleştirme kodu biçimi
89479419	Bilgisayar saati, etkinleştirme sunucu saati ile senkronize değil
8947941A	Yanlış uygulama sürümü
8947941B	Abonelik sona erdi
8947941C	Etkinleştirme sayısı geçildi
8947941D	Geçersiz bilet imzası
8947941E	Daha fazla veri gerekiyor
8947941F	Veri doğrulama başarısız
89479420	Abonelik etkin değil
89479421	Etkinleştirme sunucusu bakımda
89479501	Beklenmeyen hata
89479502	Geçersiz parametre aktarıldı. Örneğin boş bir etkinleştirme sunucusu adresleri listesi
89479503	Geçersiz etkinleştirme kodu (geçersiz karma)
89479504	Geçersiz kullanıcı kimliği
89479505	Geçersiz kullanıcı parolası
89479506	Etkinleştirme sunucusundan geçersiz yanıt
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`, `EXPORT` ve `IMPORT` komutlarını yürütmek 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.
- `BehaviorDetection` – Davranış Algılama.

- `DeviceControl` – Cihaz kontrolü.
- `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` – Güncellemeyi geri al.
- `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` – Güncelleme.
- `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=<Kullanıcı adı>`

     Uygulamanın REST API aracılığıyla yönetilmesi için kullanıcı adı. Kullanıcı adını şu biçime göre girin `<ETKİ ALANI>\<KullanıcıAdı>` (örneğin, `RESTAPI_User=COMPANY\Administrator`). Uygulamayı REST API aracılığıyla sadece bu hesaptan yönetebilirsiniz. REST API ile çalışmak üzere sadece bir kullanıcı seçebilirsiniz.
   - `RESTAPI_Port=<Bağlantı noktası>`

     Uygulamanın REST API aracılığıyla yönetilmesi için kullanılan bağlantı noktasıdır. Varsayılan olarak 6782 bağlantı noktası kullanılır. Bağlantı noktasının boş olduğundan emin olun. İsteğe bağlı parametre.
   - `RESTAPI_Certificate=<Sertifikanın yolu>`

     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\RestApi`.
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 bölüm, uygulama hakkında bilgi kaynaklarının açıklamasını içerir.

Konunun önemine ve aciliyetine bağlı olarak en uygun bilgi kaynağını seçebilirsiniz.

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.21.13\Traces` klasöründe saklanır.

İz dosyaları şu şekilde adlandırılır: `KES<21.13_tarihXX.XX_saatXX.XX_pidXXX.><iz dosyası türü>.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.

Kaspersky Endpoint Security, kullanıcı parolalarını yalnızca şifrelenmiş biçimde bir iz dosyasına kaydeder.

SRV.log, GUI.log ve ALL.log iz dosyalarının içeriği

`SRV.log`, `GUI.log` ve `ALL.log` iz dosyaları genel bilgilere ek olarak aşağıdaki bilgileri depolayabilir:

- Yerel bilgisayardaki dosyaların yolunda bu bilgiler bulunuyorsa soyadı, ad ve ikinci ad dahil kişisel veriler.
- 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, bağlantı noktası, IP adresi ve kullanıcı adı. Uygulama bir proxy sunucusu kullanıyorsa bu bilgiler iz dosyalarına yazılır.
- Bilgisayarınızın bağlantı kurduğu uzak IP adresleri.
- Mesaj konusu, ID, gönderenin adı ve mesaj gönderenin sosyal ağdaki İnternet sayfasının adresi. İnternet Denetimi bileşeni etkinse bu bilgiler iz dosyalarına yazılır.
- 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<21.13_tarih.XX_saat.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-<iz dosyasının türü>.DESKTOP-<dosyanın güncellendiği tarih>.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, Sistem Birim Bilgisi klasörüne kaydedilir 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.

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:
   - **Dönüşlü**. Boyutları ve sayıları sınırlı dosyalara izleri kaydedin ve maksimum boyuta ulaşıldığında eski dosyaların üzerine yazın. Bu mod seçildiğinde, dönüş için maksimum dosya sayısını ve her dosya için maksimum boyutu tanımlayabilirsiniz.
   - **Tek bir dosyaya yaz**. Bir izleme dosyasını kaydedin (boyut sınırı yoktur).
5. **Düzey** açılır listesinde izleme düzeyini seçin.

   Gerekli izleme düzeyini bir Teknik Destek uzmanına danışmanız önerilir. Teknik Destek'e danışamazsanız izleme düzeyini **Normal (500)**'e ayarlayın.
6. Kaspersky Endpoint Security'yi yeniden başlatın.
7. 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.21.13\Traces` klasöründe bir uygulama çalışma izleri dosyası oluşturulur. İz dosyası oluşturulduktan sonra bu dosyayı 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 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:
   - **Dönüşlü**. Boyutları ve sayıları sınırlı dosyalara izleri kaydedin ve maksimum boyuta ulaşıldığında eski dosyaların üzerine yazın. Bu mod seçilirse, her dosya için maksimum boyutu belirleyebilirsiniz.

- **Tek bir dosyaya yaz**. 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.21.13\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.21.13\Traces` klasöründe saklanır.

Döküm yazımını etkinleştirmek veya devre dışı bırakmak için:

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

Döküm dosyalarının ve iz dosyalarının korumasını etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde ⚙ düğmesine tıklayın.

2. Uygulama ayarları penceresinde **Genel Ayarlar → Uygulama ayarları** öğesini seçin.

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.

Sınırlamalar ve uyarılar

Tümünü genişlet | Tümünü daralt

Kaspersky Endpoint Security'de, uygulamanın çalışması için kritik olmayan bazı sınırlamalar vardır.

Uygulamayı yükleme

- 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.
- 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.
- Uygulamanın kaldırılmasını iptal ettiyseniz, bilgisayar yeniden başlatıldıktan sonra kurtarmaya başlayın.
- 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 Windows için Kaspersky Endpoint Security 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.

Uygulamayı yükseltme

- 11.0.0 uygulama sürümünden itibaren, Kaspersky Endpoint Security for Windows MMC eklentisini önceki eklenti sürümünün üzerine yükleyebilirsiniz. Önceki bir eklenti sürümüne dönmek için geçerli eklentiyi silin ve eklentinin önceki bir sürümünü yükleyin.
- Kaspersky Endpoint Security 11.0.0 veya 11.0.1 for Windows'u yükseltirken, Güncelleme, *Kritik Alan Taraması*, *Özel Tarama* ve *Bütünlük 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 Windows için Kaspersky Endpoint Security'nin 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.
- Uygulamanın önceki bir sürümünü 12.1 sürümüne yükseltiyorsanız, Kaspersky Endpoint Agent'ı yüklemek için bilgisayarı yeniden başlatın ve sistemde, yerel yönetici haklarına sahip bir hesap kullanarak oturum açın. Aksi takdirde, yükseltme prosedürü sırasında Kaspersky Endpoint Agent yüklenmeyecektir.
- Kaspersky Endpoint Security'yi yükseltirken uygulama, Kaspersky Security Network Beyanı kabul edilene kadar KSN'nin kullanımını devre dışı bırakır. Ayrıca, bilgisayar durumu Kaspersky Security Center'da *Kritik* olarak değiştirilebilir; *KSN sunucuları kullanılamıyor* 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 Beyanı 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.
- Uygulama Kaspersky Endpoint Security 11 for Windows'tan önceki sürümlerden yükseltildikten sonra bilgisayarın yeniden başlatılması gerekir.

Sunucu platformları için destek

- 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.
- Çekirdek 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 Beyanı 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 oturumu 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` `komut satırı parametresi` 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 Security Center ile uyumluluk

- Uyarlamalı Anomali Denetimi bileşenini yalnızca Kaspersky Security Center sürüm 11 veya sonraki sürümlerde yönetebilirsiniz.
- Kaspersky Security Center 11 tehdit raporu, AMSI bileşeni tarafından tespit edilen tehditler üzerinde gerçekleştirilen eylemler hakkında bilgi göstermeyebilir.
- Kaspersky Security Center Web Console sürüm 14.1 ve önceki sürümlerinde, Günlük Denetimi ve Dosya Bütünlüğü İzleyici bileşenlerinin işlevsel alanlarının adları, Yönetim Sunucusu özelliklerinin kullanıcı erişim izinleri ayarları bölümünde doğru şekilde görüntülenmez.
- Kaspersky Security Center Linux, Kaspersky Endpoint Security için sınırlı destek sağlar. Destek sınırlamaları hakkında daha fazla bilgi için Kaspersky Security Center Linux 14.2 Yardım veya Kaspersky Security Center Linux 15 Yardım içeriğine bakın.

Lisanslama

- *Veri alırken hata* sistem mesajı görüntülenirse, etkinleştirmeyi gerçekleştirdiğiniz bilgisayarın ağ erişimine sahip olduğunu doğrulayın veya Kaspersky Security Center Etkinleştirme Proxy'si aracılığıyla etkinleştirme ayarlarını yapılandırın.

- Lisansın süresi dolduysa veya bilgisayarda bir deneme lisansı etkinse, uygulama Kaspersky Security Center aboneliği ile etkinleştirilemez. Bir deneme lisansını veya yakında süresi dolacak bir lisansı bir abonelik lisansıyla değiştirmek için lisans dağıtım görevini kullanın.
- 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. Bunun nedeni, uygulamanın ilk olarak, yükleme prosedürü sırasında etkinleştirme için İnternet erişimi gerektiren yerleşik deneme lisansını yükleyip etkinleştirmeye çalışmasıdır.
- 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. Bunun nedeni, uygulamanın bir kez daha, yükleme prosedürü sırasında etkinleştirme için İnternet erişimi gerektiren yerleşik deneme lisansını yükleyip etkinleştirmeye çalışmasıdır.
- 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 12.1 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

- Microsoft Outlook için Posta Tehdidi Koruması uzantısı ile posta tararken, Önbelleğe Alınmış Exchange Modunu (Önbelleğe Alınmış Exchange Modunu Kullan seçeneği) kullanmanız önerilir.
- Kaspersky Endpoint Security, MS Outlook e-posta sitemcisinin 64 bit sürümünü desteklemez. Bu, bilgisayarda MS Outlook'un 64 bit sürümü yüklüyse, tarama kapsamına posta dahil edilse bile Kaspersky Endpoint Security'nin MS Outlook dosyalarını (PST ve OST dosyaları) taramayacağı anlamına gelir.

Düzeltme Altyapısı

- Uygulama yalnızca NTFS veya FAT32 dosya sistemi olan aygıtlardaki dosyaları geri yükler.
- 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.
- Uygulama, dosyalarda bir ağ arabirimi üzerinden yapılan değişiklikleri izlemez (örneğin, bir dosya paylaşılan bir klasörde depolanıyorsa ve bir işlem başka bir bilgisayardan uzaktan başlatıldıysa).

Güvenlik Duvarı

- 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.

- 11.0.0 ve 11.0.1 uygulama sürümlerinde, tanımlanan MAC adresleri yanlış uygulanır. 11.0.0, 11.0.1 ve 11.1.0 veya sonraki sürümler için MAC adresi ayarları uyumlu değildir. Uygulamayı veya eklentiyi bu sürümlerden 11.1.0 veya sonraki bir sürüme yükselttikten sonra, Güvenlik Duvarı kurallarında tanımlanan MAC adreslerini doğrulamanız ve yeniden yapılandırmanız gerekir.
- Uygulamayı 11.1.1 ve 11.2.0 sürümlerinden 12.1 sürümüne yükseltirken, aşağıdaki Güvenlik duvarı kurallarının izin durumları taşınmaz:
  - TCP üzerinden DNS sunucusuna yapılan istekler.
  - UDP üzerinden DNS sunucusuna yapılan istekler.
  - Herhangi bir ağ etkinliği.
  - ICMP Hedefine Ulaşılamıyor gelen yanıtları.
  - Gelen ICMP akışı.
- 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 bağlantı noktaları, 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. Firewall 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.

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.

Uygulama Denetimi

- Kaspersky Security Center Web Console'da Uygulama Denetimi kuralları yönetilirken yalnızca boyutu 104 MB altında olan ZIP arşivleri desteklenir. RAR veya 7z gibi diğer biçimlerdeki arşivler desteklenmez. 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.
- 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.

Aygıt Denetimi

- 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 cihazlarıyla 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.
- 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 olarak** 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.

- 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.

İnternet Denetimi

- OGV ve WEBM formatları desteklenmemektedir.
- RTMP protokolü desteklenmemektedir.

Uyarlamalı Anomali Denetimi

- Etkinliğe göre otomatik olarak istisnaların oluşturulması önerilir. Elle bir dışlama eklerken, hedef nesneyi belirtirken yolun başlangıcına `*` karakterini ekleyin.
- Bir Uyarlamalı Anomali Denetimi Kuralları raporu, örnek adı 260'tan fazla karakter içeren bir olay içeriyorsa 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 kurallarında Raporla bölümüne de bir istisna ekleyebilirsiniz.

Sürücü Şifreleme (FDE)

- Uygulamayı yükledikten sonra, sabit sürücü şifrelemesinin düzgün çalışması için işletim sistemini yeniden başlatmanız gerekir.
- Kimlik Doğrulama Aracısı hiyeroglifleri veya `|` ve `\` özel karakterleri desteklemiyor.
- Şifreleme sonrası optimum bilgisayar performansına ulaşmak için işlemcinin AES-NI komut setini (Intel Gelişmiş Şifreleme Yeni Standardı) 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 politikası 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.
- Bir işletim sistemini yedekleme kopyasından şifrelenmiş bir GPT cihazına geri yüklemeye ilişkin ayrıntılar için Teknik Destek Bilgi Bankası'nı ziyaret edin.
- Şifrelenmiş bir bilgisayarda birden çok indirme aracısı bir arada bulunamaz.
- 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 `<etki alanı>/<Windows hesap adı>` 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. metnini içeren bir mesaj.Tamam'a tıklayın* belirir ve kullanıcı bilgisayarı yeniden başlatır, yeni şifre kaydedilmez. Eski parola, önyükleme ortamında sonraki kimlik doğrulama için kullanılmalıdır.
- Disk şifreleme, Intel Rapid Start teknolojisi ile uyumlu değildir.
- Disk şifreleme, ExpressCache teknolojisi ile 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)

- Dosya ve klasör şifreleme, Microsoft Windows Embedded ailesinin işletim sistemlerinde desteklenmez.
- Uygulamayı yükledikten sonra, dosya ve klasör şifrelemenin düzgün çalışması için işletim sistemini yeniden başlatmanız gerekir.
- 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 Şifreleme Dosya Sistemi ile şifrelenmiş dosyaların şifresini çözmeniz önerilir.
- Bir dosya şifrelendikten sonra boyutu 4 kB artar.
- Bir dosya şifrelendikten sonra, dosya özelliklerinde *Arşiv* özniteliği ayarlanır.
- 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.
- İstemci Tarafı Önbelleğe Alma (CSC) kullanılarak çevrimdışı dosyaların senkronizasyonu desteklenmez. Grup ilkesi düzeyinde paylaşılan kaynakların çevrimdışı yönetiminin yasaklanması önerilir. Çevrimdışı modda olan dosyalar düzenlenebilir. Senkronizasyondan sonra, çevrimdışı bir dosyada yapılan değişiklikler kaybolabilir. Şifreleme kullanırken İstemci Tarafı Önbelleğe Alma (CSC) desteğiyle ilgili ayrıntılar için lütfen Teknik Destek Bilgi Tabanına bakın.
- 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 (Linux için Windows Alt Sistemi) modunda çalışmaz.
- Dosya düzeyinde şifreleme bileşeni yüklendiğinde, dosyaları yeniden adlandırmak ve silmek için POSIX (Taşınabilir İşletim Sistemi Arabirimi) 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.
- Kaspersky Endpoint Security for Windows 11.0.1 veya önceki bir sürümünü güncelledikten sonra, bilgisayarı yeniden başlattıktan sonra şifrelenmiş dosyalara erişmek için Ağ Aracısının çalıştığından emin olun. Network Agent gecikmeli bir başlatmaya sahiptir, bu nedenle şifrelenmiş dosyalara işletim sistemi yüklendikten hemen sonra erişemezsiniz. Bir sonraki bilgisayar başlangıcından sonra Ağ Aracısının başlamasını beklemeye gerek yoktur.

Detection and Response (EDR, MDR, Kaspersky Sandbox)

- *Dosyayı karantinaya al* görevinin bir sonucu olarak karantinaya alınan bir nesneyi tarayamazsınız.
- 4 MB üzeri bir Alternatif Veri Akışını (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`.
- 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.
- *IOC Taraması* görevi çalıştırılırken bir güvenlik ihlali göstergesi algılandığında, uygulama sadece Fileltem 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 değiştir* görevinin bir sonucu olarak tek bir bilgisayara da yüklenebilir. Davranış, Kaspersky Endpoint Security ve Kaspersky Endpoint Agent sürümlerine bağlıdır.
- EDR Optimum ve Kaspersky Sandbox bileşenlerini yönetmek için Kaspersky Endpoint Security for Windows web eklentisi 11.7.0 veya üzeri gereklidir. EDR Expert bileşenini yönetmek için Kaspersky Endpoint Security for Windows web eklentisi 11.8.0 veya üzeri gereklidir. *Uygulama bileşenlerini değiştirme* görevini bu bileşenlerle çalışmayı desteklemeyen bir web eklentisi kullanarak oluşturduysanız yükleyici, EDR Optimum, EDR Expert veya Kaspersky Sandbox yüklü bilgisayarlarda bu bileşenleri silecektir.
- 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.

- Kaspersky Endpoint Agent'tan Kaspersky Anti Targeted Attack Platform (EDR) çözümü için Kaspersky Endpoint Security'ye geçiş yaparken, bilgisayarı Merkezi Düğüm sunucularına bağlana sırasında hatalarla karşılaşabilirsiniz. Bunun nedeni, Web Console geçiş sihirbazının şu ilke ayarlarını atlaması ve bunları geçirmemesidir:

  - Ayarlar değişiklik yasağı **KATA sunucularına bağlanmak için ayarlar** ("kilit").

    Varsayılan olarak ayarlar değiştirilebilir ("kilit" açıktır). Bu nedenle ayarlar bilgisayarda uygulanmaz. Ayarların değiştirilmesi yasaklanmalı ve "kilit" kapatılmalıdır.

  - Kripto konteyneri.

    Merkezi Düğüm 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.

Diğer sınırlamalar

- 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.

- Sistem İzleyici. İşlemlerle ilgili tüm bilgiler görüntülenmez.
- 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.
- Kaspersky Security Center'da, küresel Kaspersky Security Network'ü kullanmaktan özel Kaspersky Security Network'ü 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 politikasını düzenlerken okuyabilirsiniz.
- 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.
- Endpoint Sensor bileşeni Microsoft Windows Server 2008'e yüklenemez.
- 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 Hazır Önyükleme seçeneğini kullanın veya hizmetleri başlatmak için işletim sistemi zaman aşımını artırın.
- Uygulama Güvenli Modda çalışamaz.
- Kaspersky Endpoint Security for Windows'un 11.5.0 ve 11.6.0 sürümlerinin Cisco AnyConnect yazılımı ile düzgün bir şekilde çalışabilmesini sağlamak için Compliance Module sürüm 4.3.183.2048 veya üstünü yüklemeniz gerekir. Cisco Identity Services Engine ile uyumluluk hakkında daha fazla bilgi almak için Cisco belgelerine bakabilirsiniz.
- 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.
- KSN kullanılabilirlik kontrolü görevi artık desteklenmemektedir.
- "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.
- Uygulamayı 11.1.0 sürümünden 12.1 sürümüne yükseltirken, AMSI ayarları varsayılan değerlerine sıfırlanır.
- Yazılım kısıtlama ilkeleri (SRP) kullanıyorsanız, bilgisayar yüklenemeyebilir (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.<version>\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 (GPO) altındaki bir etki alanına aitse (Yalnızca İyi), Kaspersky Endpoint Security yüklü bilgisayarın yeniden başlatılması BSOD'ye neden olur. Bir hatayı önlemek için, Grup İlkesindeki Erken Başlatma Kötü Amaçlı Yazılımdan Koruma (ELAM) parametresi 1 (İyi ve bilinmeyen) 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 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 Tam Disk Şifreleme bileşeniyle uyumlu değildir.

Uygulama, Secret Net Studio'nun Tam Disk Şifreleme bileşeniyle birlikte dağıtıldığı bir bilgisayara yüklenemez. Birlikte çalışabilirliği mümkün kılmak için Tam Disk 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.

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.

Aktif anahtar

Uygulama tarafından kullanılmakta olan bir anahtar.

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.

Doğrulama Aracısı

Şifrelenen sabit sürücülere erişim sağlamak ve önyüklenebilir sabit sürücü şifrelendikten sonra işletim sistemini yüklemek için kimlik doğrulama işlemini tamamlamanızı sağlayan arabirimdir.

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.

Ek anahtar

Uygulamayı kullanma hakkını onaylayan ancak kullanımda olmayan bir anahtar.

Görev

Kaspersky uygulaması tarafından görev olarak gerçekleştirilen işlevler, örneğin: Gerçek Zamanlı Dosya Koruma, Tam Aygıt Tarama, Veritabanı Güncellemesi.

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.

Koruma kapsamı

Çalışıyorken Temel Tehdit Koruması tarafından sürekli olarak taranan nesneler. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir.

Lisans Sertifikası

Kaspersky'nin anahtar dosyası veya etkinleştirme kodu ile birlikte kullanıcıya aktardığı bir belge. Kullanıcıya verilen lisans hakkında bilgi içerir.

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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

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, bilgisayarın dosya sistemine virüs bulaşmasını önlemenizi sağlar. Varsayılan olarak, Dosya Tehdidi Koruması bileşeni kalıcı olarak bilgisayarın RAM'inde bulunur. Bileşen bilgisayarın tüm sürücülerindeki ve bağlı sürücülerdeki 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.

İçerikleri OneDrive bulut alanında yer alan bir dosyaya erişim sağlamayı denediğinizde, Kaspersky Endpoint Security dosya içeriklerini indirir ve tarar.

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. Bir nesneyi (çıkarılabilir sürücüler gibi) tarama dışında tutabilirsiniz.
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 uygulanacak eylem	**Temizle; temizleme başarısız olursa sil**. Bu seçenek işaretlenirse uygulama, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizlik başarısız olursa uygulama dosyaları siler.

Temizle; temizleme başarısız olursa engelle. Bu seçenek işaretlenirse Kaspersky Endpoint Security, tespit edilen tüm virüslü dosyaları otomatik olarak temizleme girişiminde bulunur. Temizleme mümkün değilse Kaspersky Endpoint Security, tespit edilen virüslü dosyalarla ilgili bilgileri etkin tehditler listesine ekler.

Engelle. Bu seçenek işaretlenirse Dosya Tehdidi Koruması bileşeni, virüs bulaşmış tüm dosyaları temizlemeye 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

Bu onay kutusu, üçüncü taraf dağıtım paketlerinin taranmasını etkinleştirir/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. Kaspersky Endpoint Security, 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.

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 tarama 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.

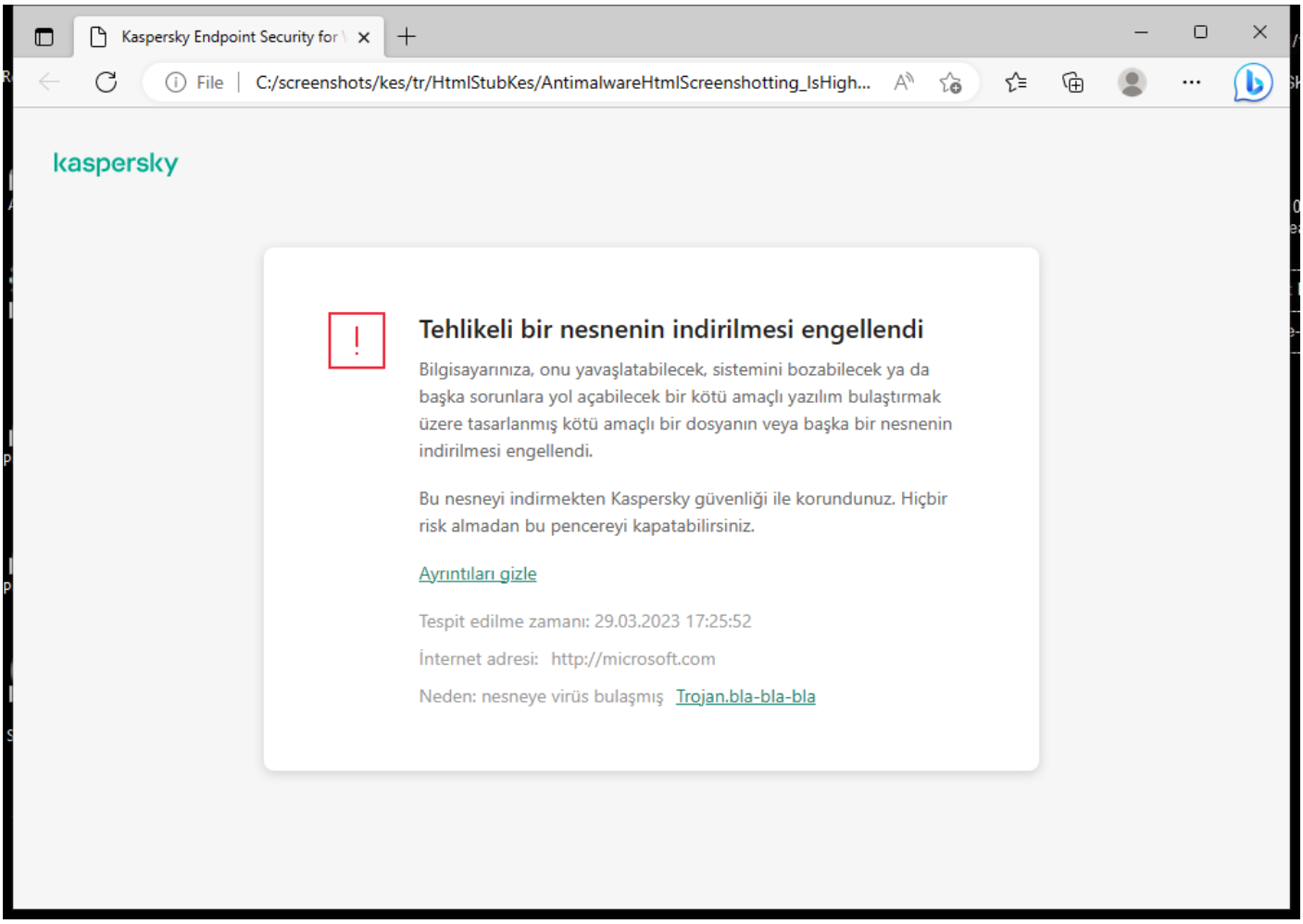
Web Tehdidi Koruması

Web Tehdidi Koruması bileşeni, İnternet üzerinden zararlı dosyaların indirilmesini önler ve aynı zamanda zararlı ve kimlik avı amaçlı web sitelerini 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. Kaspersky Endpoint Security'nin izleyeceği bağlantı noktalarını belirleyebilir ya da tüm bağlantı noktalarını seçebilirsiniz.

HTTPS trafiğini izleme için şifrelenmiş bağlantı taramasını etkinleştirin.

Bir kullanıcı kötü amaçlı veya kimlik avı yapan bir web sitesini açmaya çalıştığında, Kaspersky Endpoint Security erişimi engeller ve bir uyarı gösterir (aşağıdaki şekle bakın).



Web sitesine erişim engellendi mesajı

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 bilgisayarın HTTP ve FTP iletişim kuralları aracılığıyla aldığı web trafiğinde maksimum tarama yaptığı güvenlik düzeyidir. Web Tehdidi Koruması, uygulama veritabanlarının tam setini kullanarak tüm İnternet trafiği nesnelerini ayrıntılı olarak tarar ve mümkün olan en ayrıntılı sezgisel analizi gerçekleştirir. • **Önerilen**. Kaspersky Endpoint Security'nin 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 uygulanacak 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. **Bildir**. 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.
İnternet adresini kötü amaçlı internet adresleri veritabanıyla karşılaştırarak kontrol et	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.

(yalnızca Yönetim Konsolunda (MMC) ve Kaspersky Endpoint Security arabiriminde mevcuttur)

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.

İnternet 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 internet trafiğini tarama

Onay kutusu işaretlenirse 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

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 Tehdit Koruması uzantısı Outlook 2010, 2013, 2016 ve 2019 ile çalışmayı 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)*	Posta Tehdidi Koruması için Kaspersky Endpoint Security, farklı ayar grupları uygular. 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**. Kaspersky Endpoint Security 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.
Tehdit algılandığında uygulanacak eylem	**Temizle; temizleme başarısız olursa sil**. Alınan veya gönderilen bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse Kaspersky Endpoint Security virüslü nesneyi siler. Kaspersky Endpoint Security, mesajın konusuna gerçekleştirilen eylemin bilgilerini ekler, örneğin *[Mesaj işlendi] <mesajın konusu>*. **Temizle; temizleme başarısız olursa engelle**. Alınan bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Kullanıcı mesafe güvenli bir ekle erişim sağlayabilir. Nesne temizlenemezse, Kaspersky Endpoint Security mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Gönderilen bir mesajda virüs bulaşmış bir nesne tespit edilirse, Kaspersky Endpoint Security tespit edilen nesneyi temizlemeyi dener. Nesne temizlenemezse, Kaspersky Endpoint Security mesajın iletimini engeller ve posta istemcisi bir hata görüntüler. **Engelle**. Gelen bir mesajdaki virüslü bir nesne temizlenemezse, Kaspersky Endpoint Security mesajın konusuna bir uyarı ekler. Kullanıcı mesaja orijinal ek ile erişim sağlayabilir. Gönderilen bir mesajdaki virüslü bir nesne temizlenemezse, Kaspersky Endpoint Security 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	Onay kutusu POP3, SMTP, NNTP ve IMAP iletişim kuralları yoluyla aktarılan trafiğin, Posta Tehdidi Koruması bileşeni tarafından taranmasını etkinleştirir/devre dışı bırakır.
Microsoft Outlook	Bu onay kutusu işaretlenirse POP3, SMTP, NNTP, IMAP iletişim kuralları yoluyla iletilen e-posta mesajlarının taranması, Microsoft Outlook'a entegre uzantıda etkinleştirilir.

uzantısını bağla

E-postalar, Microsoft Outlook için uzantı kullanılarak taranıyorsa Önbellekli Exchange Modu'nun 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 Kaspersky Endpoint Security 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. Kaspersky Endpoint Security, 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 Saldırı Tespit Sistemi olarak da adlandırılır), ağ saldırılarının karakteristik aktiviteleri için gelen ağ trafiğini izler. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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
Bağlantı noktası 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. *Bağlantı Noktası Tarama* saldırısı, bilgisayardaki UDP bağlantı noktalarını, TCP bağlantı noktalarını ve ağ hizmetlerini taramaktan oluşur. Bu saldırı, saldırganın daha tehlikeli ağ saldırıları gerçekleştirmeden önce bilgisayarın güvenlik açığı düzeyini belirlemesine olanak tanır. Bağlantı Noktası 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 N dakika için engelle	Onay kutusu işaretlenirse Ağ Tehdidi Koruması bileşeni saldıran bilgisayarı engellenen 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. Uygulama, istisnalar listesinde bulunan IP adreslerinden gelen ağ saldırılarına ilişkin bilgileri günlüğe kaydetmez.
MAC Kafesleme Koruması	*MAC aldatma 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, İnternet veya yerel ağ üzerinde çalışırken bilgisayara izinsiz bağlantılar kurulmasını 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 bağlantı noktası açar. Hangi bağlantı noktalarının açılacağı bilgisayarın rolüne bağlıdır (örneğin, dağıtım noktası). Bilgisayarda açılacak bağlantı noktaları 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 bağlantı noktaları 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 durumları

Güvenlik Duvarı, ağ bağlantısının durumuna bağlı olarak ağ etkinliklerini kontrol etmenize olanak tanır. Kaspersky Endpoint Security ağ bağlantısı durumunu bilgisayarın işletim sisteminden alır. İşletim sistemindeki ağ bağlantısının durumu, bağlantının ayarlanması sırasında kullanıcı tarafından ayarlanır. Kaspersky Endpoint Security ayarlarından ağ bağlantısı durumunu değiştirebilirsiniz. Güvenlik Duvarı ağ etkinliklerini işletim sistemindeki ağ durumuna göre değil Kaspersky Endpoint Security ayarlarındaki ağ durumuna göre izleyecektir.

Ağ bağlantısı, aşağıdaki durum türlerinden birine sahip olabilir:

- **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 İnternet'e *Ortak ağ* durumunu atar. İnternet'in durumunu 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 bağlantı noktaları 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 önceliğe sahiptir.
Kullanılabilir ağlar	Bu tablo, Güvenlik Duvarı'nın bilgisayarda tespit ettiği ağ bağlantıları hakkında bilgi içerir. *Ortak ağ* durumu, varsayılan olarak İnternet'e 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 aygıt 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.

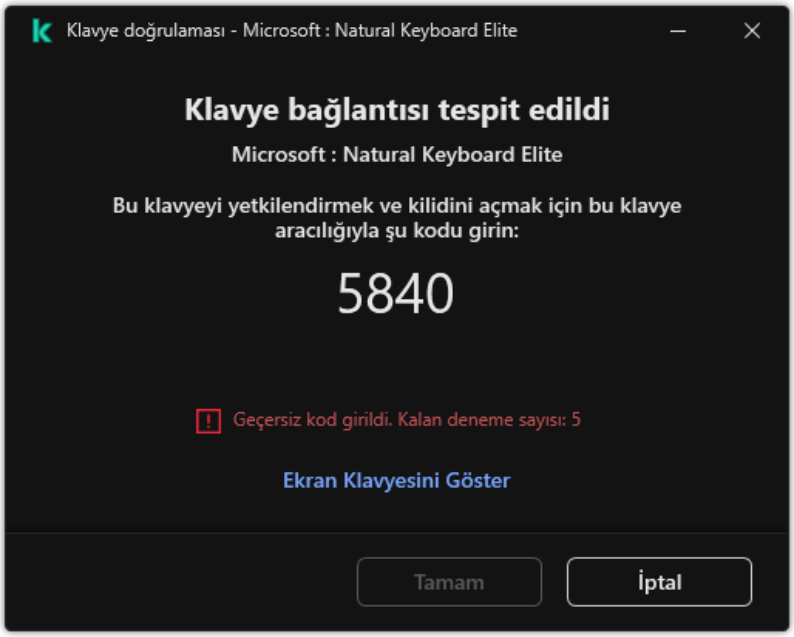
Kod doğru girildiyse uygulama klavyenin VID/PID'si ve bağlandığı bağlantı noktasının numarası gibi tanımlama parametrelerini yetkilendirilen klavyeler listesine kaydeder. Klavye yeniden bağlandığında ya da işletim sistemi yeniden başlatıldıktan sonra klavye yetkilendirmenin tekrarlanması gerekmez.

Yetkilendirilen klavye bilgisayarın farklı bir USB bağlantı noktasına bağlandığında, uygulama bu klavyenin yetkilendirilmesi için tekrar 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.

BadUSB Saldırısı Önleme bileşeni varsayılan olarak yüklenmez. BadUSB Saldırısı Önleme bileşenine ihtiyacınız varsa, bu bileşeni uygulamayı yüklemeden önce yükleme paketinin özelliklerinden ekleyebilir ya da uygulamayı yükledikten sonra kullanılabilir uygulama bileşenlerini değiştirebilirsiniz.



Klavye yetkilendirme

BadUSB Saldırısı Önleme bileşeni ayarları

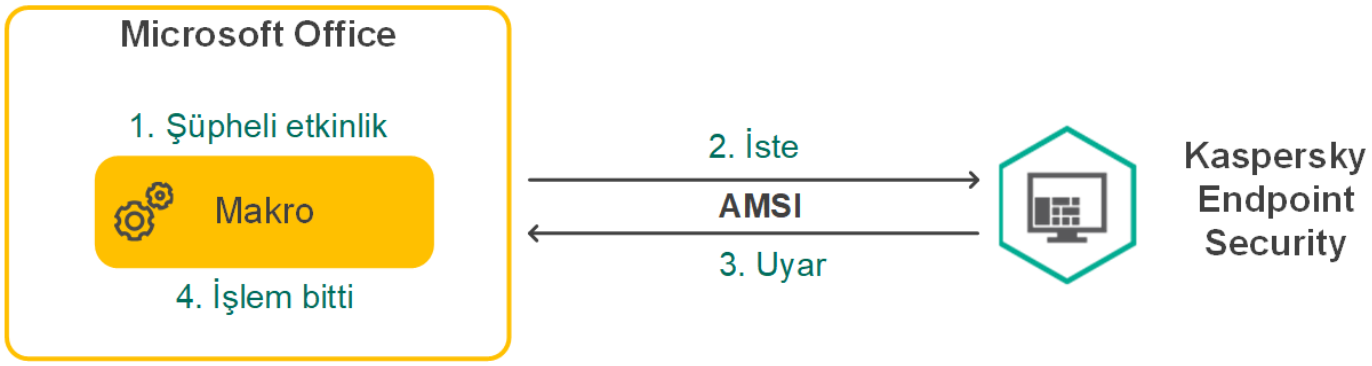
Parametre	Açıklama
USB cihazlarının kimlik doğrulaması için Ekran Klavyesinin kullanımını yasakla	Onay kutusu işaretlenirse uygulama, yetkilendirme kodunun girilemeyeceği bir USB aygıtının yetkilendirilmesi için Ekran Klavyesi kullanımını engeller.
Maksimum sayıda USBB	Yetkilendirme kodunun belirtilen sayıda yanlış girilmesi durumunda USB cihazı otomatik olarak bloke edilir. Geçerli değerler 1 ila 10 arasındadır. Örneğin, yetkilendirme kodunu girmek için 5 denemeye izin verirseniz,

cihazı doğrulama girişimi	USB cihazı beşinci başarısız denemeden sonra bloke olur. Kaspersky Endpoint Security, USB cihazı için engelleme süresini görüntüler. Bu süre geçtikten sonra, yetkilendirme kodunu girmek için 5 deneme hakkınız vardır.
Maksimum girişim sayısına ulaşılırken zaman aşımı	Belirtilen sayıda başarısız denemeden sonra yetkilendirme kodunun girilmesi için USB cihazının 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. Üçüncü taraf uygulama, bir tehdit bildirimi aldıktan sonra zararlı işlemlerin gerçekleştirilmesine izin vermez (örneğin sonlandırılır).



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;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2019 Essentials / Standard / Datacenter (Çekirdek Modu dahil);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Çekirdek Modu dahil).

AMSI Koruma 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	Bu onay kutusu, üçüncü taraf dağıtım paketlerinin taranmasını etkinleştirir/devre dışı bırakır.
Microsoft	Microsoft Office dosyalarını (DOC, DOCX, XLS, PPT ve diğer Microsoft uzantıları) tarar. Office

Office biçimlerindeki dosyaları tara	biçimindeki dosyalar da OLE nesnelerini içerir. Kaspersky Endpoint Security, 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 ayarları

Parametre	Açıklama
Exploit algılandığında	**İşlemi 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. **Bildir**. 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 ayarları

Parametre	Açıklama
Kötü amaçlı yazılım etkinlikleri tespit edildiğinde	**Dosyayı 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. **Uygulamayı sonlandır**. Bu seçenek seçilirse Kaspersky Endpoint Security, zararlı yazılımların etkinlikleri tespit edildiğinde bu uygulamayı sonlandırır. **Bildir**. 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.
Paylaşılan klasörlerin dış şifrelemeye karşı korunmasını etkinleştir	İki durumlu düğme açılırsa Kaspersky Endpoint Security, paylaşım klasöründeki 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. • **Bildir**. Bu seçenek işaretliyse Kaspersky Endpoint Security, paylaşım klasörlerindeki dosyaları değiştirme girişimi tespit ettiğinde paylaşım klasörlerinde dosyaları değiştirme girişimi ile ilgili bilgileri etkin tehditler listesine ekler.

- **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 (salt okunur) 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.

İstisnalar Paylaşılan klasörleri şifreleme girişimlerinin izlenmediği bilgisayarların listesidir.

Paylaşılan klasörlerin dış şifrelenmesine 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.

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 (dosyalar ve uygulamalar gibi)

Ağ kuralları kullanılarak Güvenlik Duvarı tarafından denetlenen uygulamaların ağ etkinliği.

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 bileşeni ayarları

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**. Bu tabloda, bir güvenilirlik grubundaki uygulamaların işletim sistemi kaynaklarına ve kişisel verilere erişim hakları yer alır. • **Haklar**. Bu tabloda, bir güvenilirlik grubundaki uygulamaların işletim sisteminin işlemlerine ve kaynaklarına erişim hakkı görüntülenir. • **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 for Windows çalışmaya başlamadan önce başlatılan uygulamalar için güvenilirlik 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.
Mevcut gruplara eklenemeyen 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'nin 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.

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 dosyaların kategorisi ve tanınırlığı hakkındaki bilgilerle birlikte taranan web adreslerinin tanınırlığı hakkında bilgi sağlar.

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 Statement'a ve Kaspersky web sitesi 'ne başvurun. Kaspersky Security Network Statement 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 Center varsayılan olarak KSN kullanır. Yönetim Konsolu'nda (MMC), Kaspersky Security Center Web Console'da ve komut satırında KPSN kullanımını yapılandırabilirsiniz. Kaspersky Security Center Cloud Console üzerinden KPSN kullanımını yapılandırmak mümkün değildir.

KPSN hakkında daha fazla bilgi için lütfen Kaspersky Private Security Network belgelerine bakın.

Kaspersky Security Network ayarları

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.

KSN Proxy kullan

(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 kullanılabilir olmadığında KSN 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).

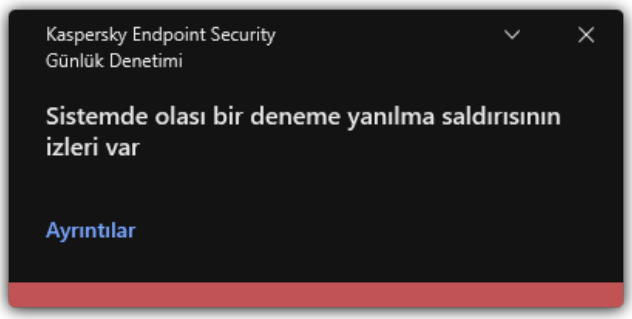
Günlük Denetleyici

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, 11.11.0 sürümünden itibaren Günlük Denetimi bileşenini içerir. 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, güvenlik denetimi ilkesinin yapılandırıldığından ve sistemin ilgili olayları günlüğe kaydettiğinden emin olun (ayrıntılar için bkz. Microsoft teknik destek web sitesi.).



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: *Application*, *Security* or *System*. Ayrıca bir üçüncü taraf uygulamasının günlüğünü de belirtebilirsiniz.

İnternet Denetimi

İnternet Denetimi, kullanıcının internet kaynaklarına 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).

Kaspersky Endpoint Security sadece HTTP ve HTTPS trafiğini izler.

HTTPS trafiğini izleme için şifrelenmiş bağlantı taramasını etkinleştirin.

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**. Kullanıcıların bir web sitesindeki verilere erişimini kısıtlayabilir ve örneğin web sitelerindeki resimleri 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 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.

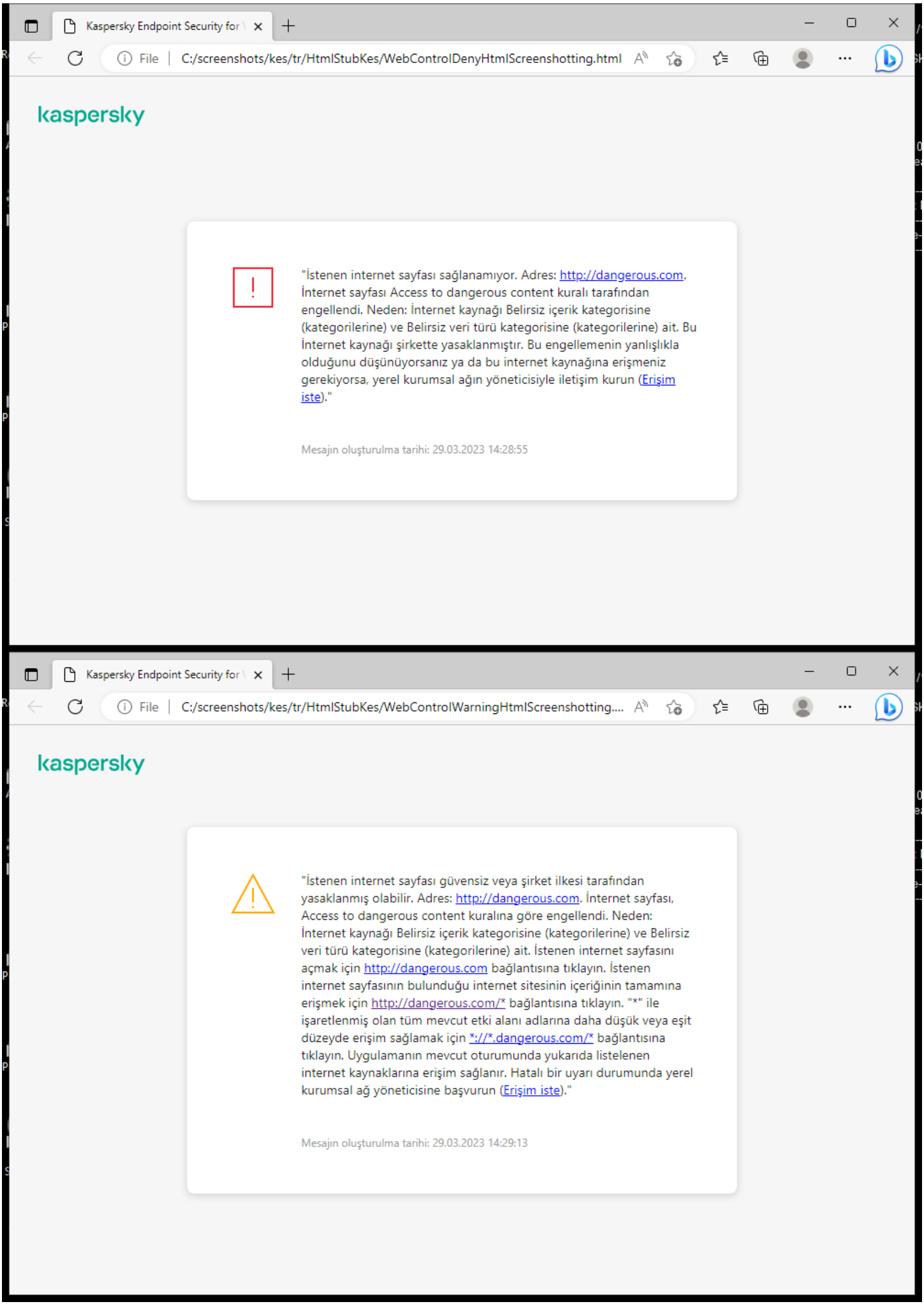
  Örneğin BT departmanı hariç olmak üzere şirketin tüm çalışanlarının bir tarayıcı üzerinden İnternete erişmesini kısıtlayabilirsiniz.

- 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

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**.
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.
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, bilgisayarı bu tür aygıtlar bağlandığında virüslere karşı korur ve veri kaybını veya sızıntılarını önler.

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. Bu nedenle tüm aygıtların bağlantısını, örneğin USB üzerinden kısıtlayabilirsiniz.

  Aygıt erişimini aşağıdaki şekilde yapılandırabilirsiniz:

  - İzin ver – .
  - Engelle – .

- **Güvenilir aygıtlar**. *Güvenilir aygıtlar*, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

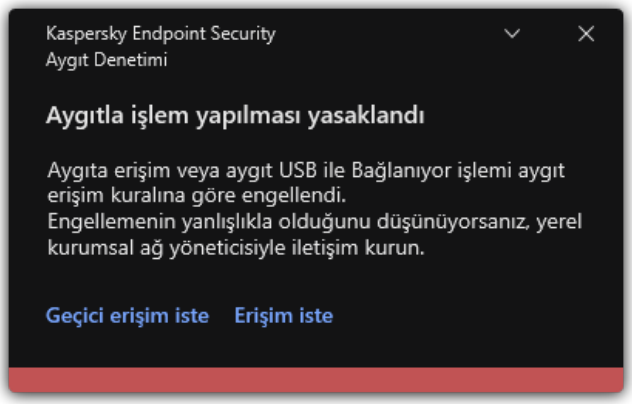
  Güvenilir aygıtları aşağıdaki verilere göre ekleyebilirsiniz:

  - **Kimliğe göre aygıtlar**. Her cihazın benzersiz bir tanımlayıcısı vardır (Donanım Kimliği veya HWID). Bu kimliği, işletim sistemi araçlarını kullanarak aygıt özelliklerinden görüntüleyebilirsiniz. Örnek aygıt kimliği: `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 satıcı kimliği (VID) ve bir ürün kimliği (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.

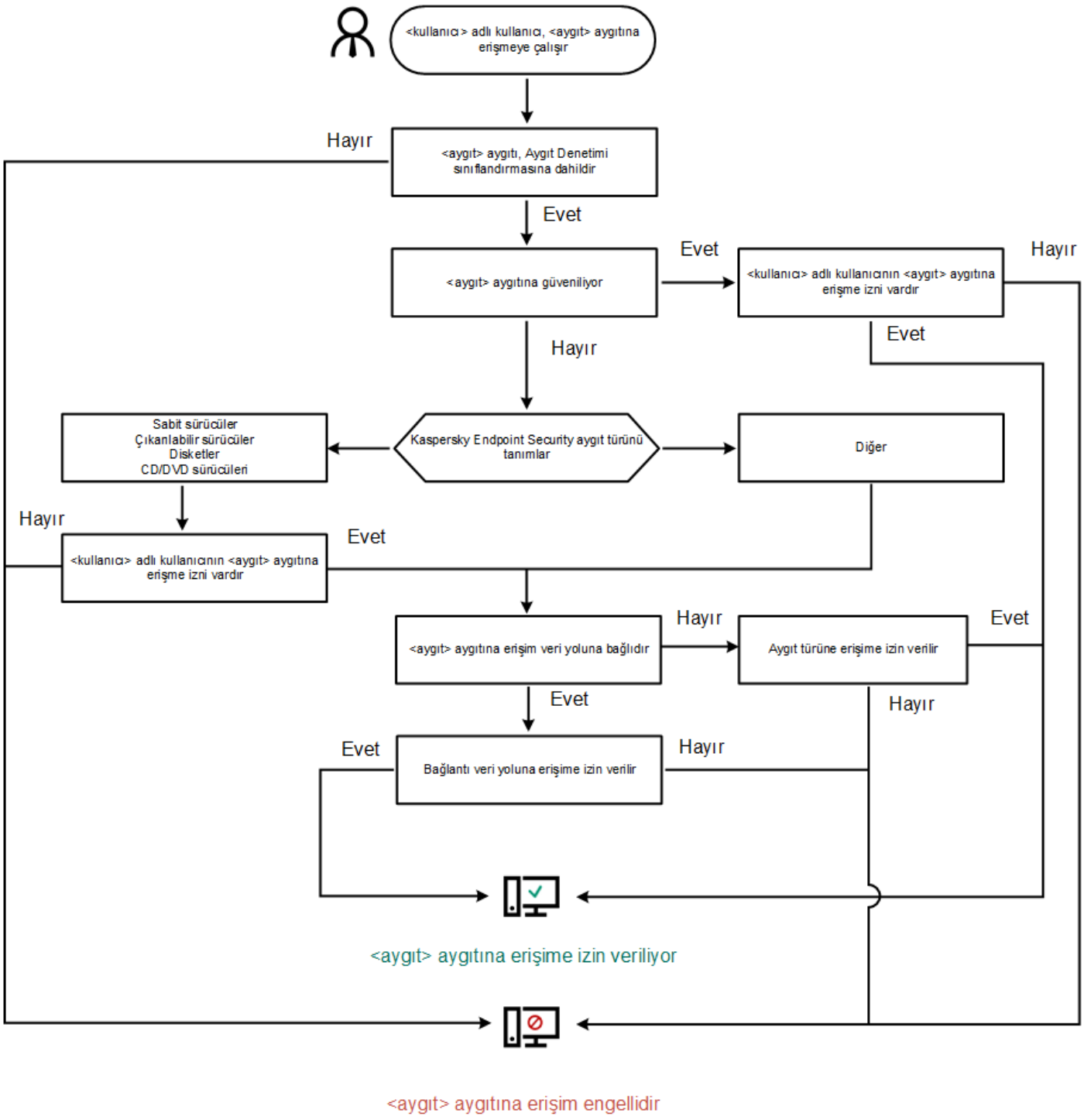
Aygıt Denetimi tarafından engellenen bir aygıt bilgisayara bağlandığında, Kaspersky Endpoint Security erişimi engeller ve bir bildirim gösterir (aşağıdaki şekle bakın).



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	Onay kutusu işaretlenirse **Erişim iste** düğmesi Kaspersky Endpoint Security'nin yerel arabirim aracılığıyla etkinleşir. Bu düğmeyi kullanarak, kullanıcı engellenen bir aygıta geçici erişim isteyebilir.

(sadece Kaspersky Security Center Konsolunda mevcuttur)

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.

Güvenilir aygıtlar

Bu aygıtlara erişim verilmiş güvenilir aygıtlar ve kullanıcılar listesi.

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*), 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.

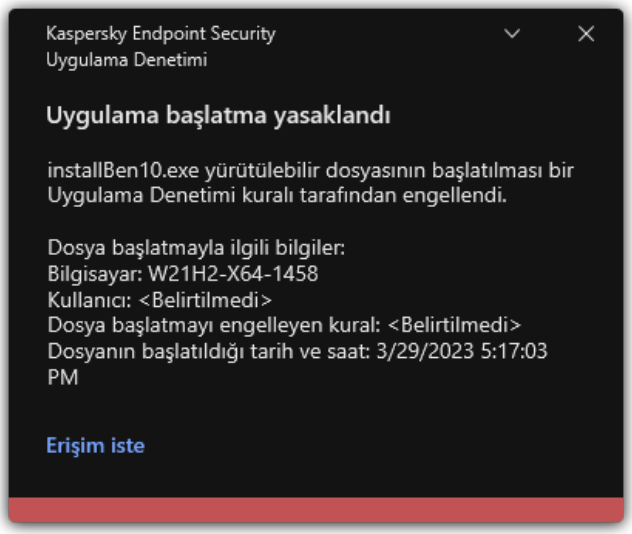
3. Uygulama Denetimi modunu seçme.

   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.

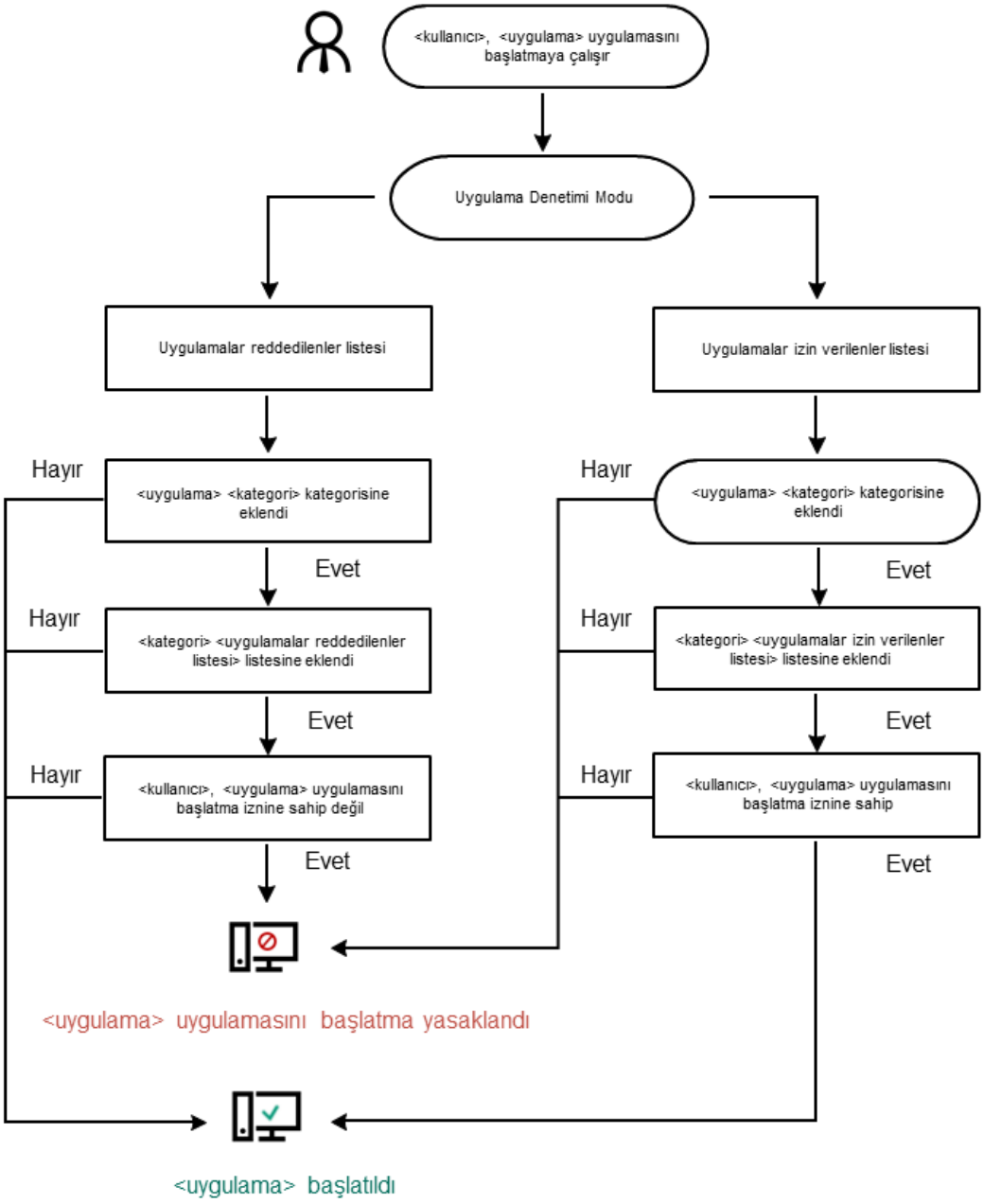
  Kaspersky Security Center Yönetim Konsolunda oluşturulan Uygulama Denetimi kuralları, Kaspersky Endpoint Security yerel arabiriminde olduğu gibi dahil etme ve hariç tutma koşullarına değil, özel uygulama kategorilerine dayanır.

- 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 bileşeni ayarları

Parametre	Açıklama
Engellenen uygulamaların başlangıcındaki işlem	**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 modülleri yüklenmesini denetle

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 "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.

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 durumunda kuralları tetikleme** veri havuzunda günlüğe kaydeder.

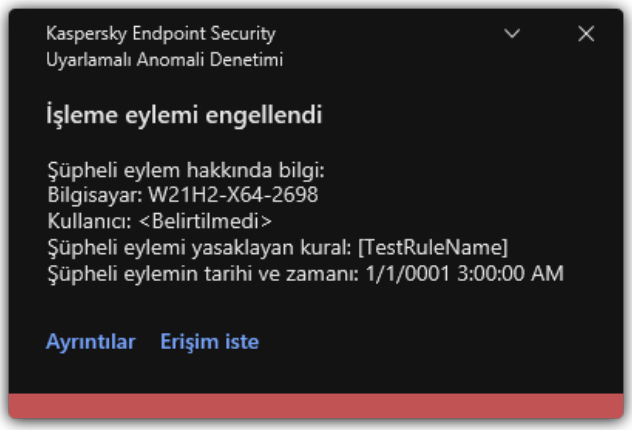
2. Kural tetikleme raporunu analiz etme.

   Yönetici, kural tetikleme raporunu veya **Akıllı Eğitim durumunda kuralları tetikleme** 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 gerçek zamanlı olarak yapılandırılır. Uyarlamalı Anomali Denetimi şu kanallar üzerinden 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 durumunda kuralları tetikleme** veri havuzunun içeriğini gözden geçirdikten sonra Uyarlamalı Anomali Denetiminin çalışmasını yapılandırır. Kural tetikleme raporunun ve **Akıllı Eğitim durumunda kuralları tetikleme** veri havuzunun içeriğinin kontrol edilmesi önerilir.

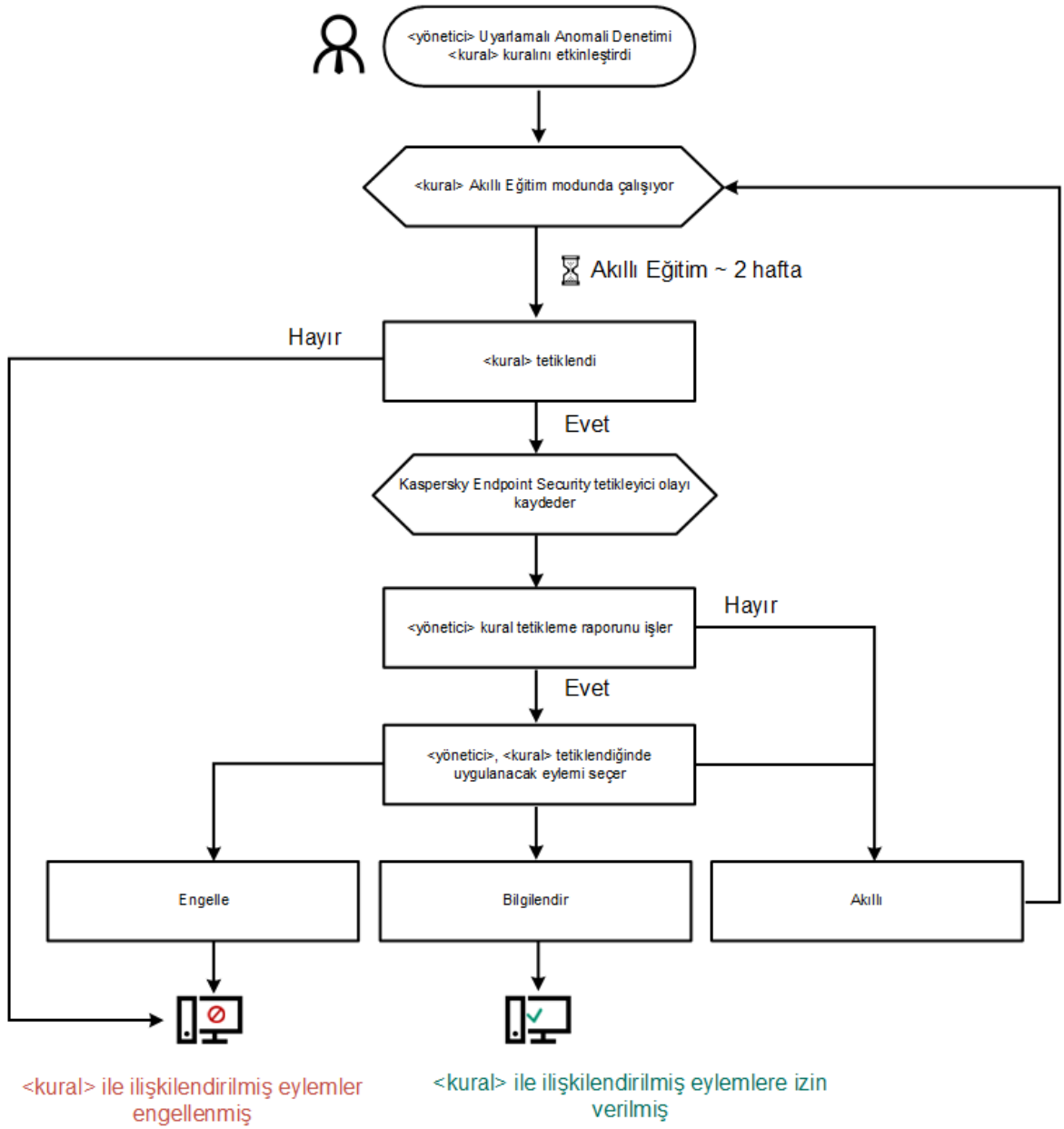
Zararlı bir uygulama eylemde bulunmaya çalıştığında Kaspersky Endpoint Security, eylemi engeller ve bir bildirim gösterir (aşağıdaki resme bakın).



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 bileşeni ayarları

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 bırakıldı* veya *Engelle*). Rapor, tüm yönetim grupları için oluşturulur.
Tetiklenen Uyarlamalı Anomali Denetimi kuralları hakkında rapor	Bu rapor, Uyarlamalı Anomali Denetimi kullanılarak tespit edilen tipik olmayan eylemler hakkında bilgiler içerir. Rapor, tüm yönetim grupları için oluşturulur.

(sadece Kaspersky Security Center Konsolunda mevcuttur)

Kurallar	Uyarlamalı Anomali Denetimi kuralları tablosu. Kurallar, potansiyel olarak zararlı etkinliğin tipik senaryolarına dayanarak Kaspersky uzmanları tarafından 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: **Yöneticiye 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.

Dosya Bütünlüğü İzleyici

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.

Dosya Bütünlük İzleyicisi yalnızca NTFS veya ReFS dosya sistemine sahip sunucularda çalışır.

Kaspersky Endpoint Security for Windows, 11.11.0 sürümünden itibaren Dosya Bütünlük İzleyicisi bileşenini içerir. Dosya Bütünlük İzleyicisi, belirli bir izleme alanındaki nesnelerde (dosyalar ve klasörler) yapılan değişiklikleri algılar. Bu değişiklikler bir bilgisayar güvenlik ihlalini gösterebilir. Nesne değişiklikleri tespit edildiğinde uygulama yöneticiyi bilgilendirir.

Dosya Bütünlük İzleyicisini kullanmak için bileşenin kapsamını yapılandırmalısınız, yani durumu bileşen tarafından izlenmesi gereken nesneleri seçmelisiniz.

Kaspersky Security Center'da ve Kaspersky Endpoint Security for Windows arabiriminde Dosya Bütünlük İzleyicisi işleminin sonuçları hakkındaki bilgileri görüntüleyebilirsiniz.

Dosya Bütünlük İzleyicisi bileşeni ayarları

Parametre	Açıklama
Olay önem seviyesi	Kaspersky Endpoint Security, izleme kapsamındaki bir dosya değiştirildiğinde dosya değiştirme olaylarını günlüğe kaydeder. Olay önem seviyeleri şunlardır: *Bilgilendirici*, *Uyarı*, *Kritik*.
İzleme kapsamı	Dosya Bütünlük İzleyicisi'nin izlediği dosya ve klasörlerin listesi. Kaspersky Endpoint Security, bir maske girerken ortam değişkenlerini ve `*` ve `?` karakterlerini destekler. Örneğin, `C:\Folder\Application\`.
İstisnalar	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.

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 (ATP), sıfır gün saldırıları ve diğer karmaşık tehditleri zamanında tespit etmek üzere tasarlanmış bir çözümdür. Kaspersky Anti Targeted Attack iki işlevsel blok içerir: Kaspersky Anti Targeted Attack (bundan sonra kısaca "*KATA*" olarak anılacaktır) ve Kaspersky Endpoint Detection and Response (bundan sonra kısaca "*EDR (KATA)*" olarak alınacaktır). EDR (KATA)'yı ayrıca satın alabilirsiniz. Çözüm hakkında ayrıntılı bilgi için 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.

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows, 11.7.0 sürümünden itibaren Kaspersky Sandbox çözümü ile entegrasyon için yerleşik bir aracı içerir. *Kaspersky Sandbox çözümü* bilgisayarlardaki gelişmiş tehditleri algılar ve otomatik olarak engeller. Kaspersky Sandbox, kuruluşun BT altyapısına yönelik hedeflenen saldırıların karakteristik özelliklerini ve kötü amaçlı etkinlikleri tespit etmek için nesne davranışını analiz eder. Kaspersky Sandbox, Microsoft Windows işletim sistemlerinin dağıtılmış sanal görüntülerini içeren özel sunuculardaki (Kaspersky Sandbox sunucuları) nesneleri analiz eder ve tarar. Çözümle ilgili ayrıntılı bilgi almak için Kaspersky Sandbox Yardım içeriğine bakın.

Bileşen yalnızca Kaspersky Security Center Web Console kullanılarak yönetilebilir. Bu bileşeni Yönetim Konsolu'nu (MMC) kullanarak yönetemezsiniz.

Kaspersky Sandbox bileşen ayarları

Parametre	Açıklama
Sunucu TLS sertifikası	Kaspersky Sandbox sunucularıyla güvenilir bir bağlantı yapılandırmak için bir TLS sertifikası hazırlamanız gerekir. Ardından, sertifikayı Kaspersky Sandbox sunucularına ve Kaspersky Endpoint Security ilkesine

	eklemelisiniz. Sertifikayı hazırlama ve sertifikayı sunuculara eklemeyle ilgili ayrıntılar için Kaspersky Sandbox Yardım içeriğine bakın.
Zaman Aşımı	Kaspersky 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 stabil değilse Kaspersky Sandbox için bağlantı zaman aşımı süresini artırabilirsiniz. Önerilen istek zaman aşımı 0,5 saniye veya daha kısadır.
Kaspersky Sandbox istek kuyruğu	İstek kuyruğu klasörünün boyutu. Bilgisayarda bir nesneye erişildiğinde (yürütülebilir dosya başlatıldığında veya örneğin DOCX veya PDF biçiminde bir belge açıldığında), Kaspersky Endpoint Security, Kaspersky Sandbox tarafından taranacak nesneyi de gönderebilir. Birden çok istek olduğunda, Kaspersky Endpoint Security bir istek kuyruğu oluşturur. İstek kuyruğu klasörünün boyutu varsayılan olarak 100 MB ile sınırlandırılmıştır. Maksimum boyuta ulaşıldıktan sonra, Kaspersky Sandbox kuyruğa yeni isteklerin eklenmesini durdurur ve ilgili olayı Kaspersky Security Center'a gönderir. İstek kuyruğu klasörünün boyutunu sunucu yapılandırmanıza göre yapılandırabilirsiniz.
Kaspersky Sandbox sunucusu	Kaspersky 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.
Tehdit algılandığında 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 alanların taranmasını çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security *Kritik Alanları Tarama* görevini çalıştırır. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar. **IOC taraması görevi çalıştır**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security otomatik olarak *IOC Taraması görevi (otonom IOC tarama görevi) oluşturur*. Bu görev için çalıştırma modunu, tarama kapsamını ve IOC tespit edildiğinde uygulanacak eylemi yapılandırabilirsiniz: nesneyi sil, *Kritik Alanları Tarama* görevi 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 sürücülerindeki dosya alanları**. Bu seçenek tercih edildiğinde, Kaspersky Endpoint Security bilgisayarın sistem sürücüsünde bir IOC taraması gerçekleştirir.
IOC taraması görevini çalıştır	**Elle**. *IOC taraması* görevinin seçtiğiniz bir zamanda manuel olarak çalıştırılabileceği bir çalışma modudur. **Tehdit tespit edildikten sonra**. Kaspersky Endpoint Security'nin *IOC Taraması* görevini bir tehdit algılandığında 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.

Endpoint Detection and Response

11.7.0 sürümünden itibaren, Kaspersky Endpoint Security for Windows, artık Kaspersky Endpoint Detection and Response Optimum çözümü (bundan böyle "EDR Optimum" olarak anılacaktır) için yerleşik bir aracıya sahip. 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 algılama ayrıntılarını ayrı bir pencerede görüntüler. *Algılama ayrıntıları*, tespit edilen bir tehdit hakkında toplanan bilgilerin tamamını görüntülemek için sunulan bir araçtır. Algılama ayrıntılarına örnek olarak bilgisayarda görünen dosyaların geçmişi verilebilir. Algılama ayrıntılarının yönetimi hakkında daha fazla bilgi için Kaspersky Endpoint Detection and Response Optimum Yardım ve Kaspersky Endpoint Detection and Response Expert Yardım içeriklerine bakabilirsiniz.

EDR Optimum bileşenini Web Console ve Cloud Console'dan yapılandırabilirsiniz. EDR Expert için bileşen ayarları sadece Cloud Console'da kullanılabilir.

Endpoint Detection and Response ayarları

Parametre	Açıklama
Ağ izolasyonu	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 edilen bilgisayarın kilidini şu süre içinde kaldır: N 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 rapora yaz**. 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. **Sadece olayları günlüğe kaydet**. 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.
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 (KATA)

Kaspersky Endpoint Security sürüm 12.1 artık Kaspersky Anti Targeted Attack Platform çözümünün bir parçası olarak Kaspersky Endpoint Detection and Response bileşenini yönetmek için yerleşik bir aracı içeriyor. *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 iki işlevsel blok içerir: Kaspersky Anti Targeted Attack (bundan sonra kısaca "*KATA*" olarak anılacaktır) ve Kaspersky Endpoint Detection and Response (bundan sonra kısaca "*EDR (KATA)*" olarak alınacaktır). EDR (KATA)'yı ayrıca 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) 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.

Endpoint Detection and Response (KATA) ayarları

Parametre	Açıklama
KATA sunucularına bağlantı için ayarlar	**Zaman Aşımı**. Maksimum Merkezi Düğüm sunucusu yanıt zaman aşımı. Zaman aşımı bittiğinde Kaspersky Endpoint Security, farklı bir Merkezi Düğüm sunucusuna bağlanmayı dener. **Sunucu TLS sertifikası**. Merkezi Düğüm 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 kullanın**. İki yönlü kimlik doğrulama, Merkezi Düğümdeki bilgisayarın ek bir doğrulamasının yapılmasına olanak tanır. Bu doğrulamayı etkinleştirmek için Merkezi Düğüm 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). Kripto konteyneri parola korumalı olmalıdır. Boş bir parola ile bir kripto konteyneri eklemek mümkün değildir.
KATA sunucuları	Merkezi düğüm sunucusu bağlantı ayarları. Bir IP adresi (IPv4 veya IPv6) girebilirsiniz.
KATA sunucusuna her (dakika) senkronizasyon isteği gönder	Merkezi Düğüm sunucusuna gönderilen senkronizasyon isteklerinin sıklığı. Senkronizasyon sırasında, Kaspersky Endpoint Security değiştirilen uygulama ayarları ve görevleri hakkında bilgi gönderir.
KATA'ya telemetri gönder	Bu işlev sunucuya telemetri gönderimini tamamen kapatmanızı sağlar. Kaspersky Anti Targeted Attack Platform'u telemetri de kullanan başka bir çözümle birlikte kullanıyorsanız, KATA (EDR) için telemetriyi kapatabilirsiniz. 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.
Maksimum olay	Uygulama, senkronizasyon aralığı sona erdikten sonra olayları göndermek için sunucu ile senkronize olur.

iletim gecikmesi (sn)	Varsayılan değer ayarı 30 saniyedir.
Talep daraltmayı etkinleştir	Bu özellik sunucu üzerindeki yükü optimize etmeye yardımcı olur. Onay kutusu işaretlendiğinde uygulama iletilen olayları 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.
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.

Tam Disk Şifreleme

Bir şifreleme teknolojisi seçebilirsiniz: Kaspersky Disk Encryption veya BitLocker Drive Encryption (bundan sonra "BitLocker" olarak ifade edilecektir).

Kaspersky Disk Encryption

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. Ayrıca, Kimlik Doğrulama Aracısı hesabının kullanıcı adını ve parolasını kullanarak işletim sistemine otomatik olarak giriş yapan Çoklu Oturum Açma (SSO) teknolojisi 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 Security Center'ı kullanarak BitLocker'ı kontrol etmenize ve yönetmenize izin verir. BitLocker mantıksal birimleri şifreler. BitLocker, çıkarılabilir sürücülerin şifrelenmesi için kullanılamaz. BitLocker hakkında daha ayrıntılı bilgi için Microsoft belgelerine bakın.

BitLocker, bir güvenilir platform modülü kullanarak erişim anahtarlarının güvenli bir şekilde depolanmasını sağlar. *Güvenilir Platform Modülü (TPM)* güvenlikle ilgili temel işlevleri sunmak (örneğin şifreleme anahtarını saklamak) için 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.

Bir sürücüyü şifreledikten sonra, BitLocker bir ana anahtar oluşturur. Kaspersky Endpoint Security, ana anahtarı Kaspersky Security Center'a gönderir, böylece mesela bir kullanıcı parolasını unuttuysa diske erişimi geri yükleyebilirsiniz.

Bir kullanıcı diski BitLocker kullanarak şifrelediğinde, Kaspersky Endpoint Security disk şifrelemeyle ilgili bilgileri Kaspersky Security Center'a gönderir. Ancak Kaspersky Endpoint Security, ana anahtarı Kaspersky Security Center'a göndermez. Bu nedenle Kaspersky Security Center kullanılarak diske erişimin geri yüklenmesi mümkün değildir. BitLocker'ın Kaspersky Security Center ile düzgün bir şekilde çalışabilmesi için bir ilke kullanarak sürücünün şifresini çözün ve sonra tekrar şifreleyin. Bir sürücünün şifresini yerel olarak ya da bir ilke kullanarak çözebilirsiniz.

Sistem sabit sürücüsünü şifreledikten sonra, işlem sistemini önyüklemek için kullanıcının BitLocker kimlik doğrulamasını gerçekleştirmesi gerekir. Kimlik doğrulama prosedüründen sonra, BitLocker kullanıcıların giriş yapmasına izin verecektir. BitLocker çoklu oturum açma (SSO) desteği sunmaz.

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 öğe 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 öğe seçilirse ilke uygulandığında uygulama daha önce şifrelenen 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.
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	Bu onay kutusu seçildiğinde, uygulama, Kimlik Doğrulama Aracısı'nı başlatmadan önce bilgisayardaki Windows kullanıcı hesapları hakkındaki bilgileri kontrol eder. Kaspersky Endpoint Security, Kimlik Doğrulama

tüm kullanıcılar için giriş yapıldığında Kimlik Doğrulama Aracısı hesapları oluştur

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, bu onay kutusu işaretlenmemiştir.

Legacy USB Support'u kullan (önerilmez)

Bu kutucuk, Legacy USB Support işlevini etkinleştirir/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.

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 öğe 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 öğe seçilirse ilke uygulandığında uygulama daha önce şifrelenen 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	Bu onay kutusu, platform önyükleme girişi özelliğine sahip değilse bile (örneğin tabletlerdeki dokunmatik ekran klavyeleri ile), bir önyükleme ortamında veri girişini gerektiren kimlik doğrulama kullanımını etkinleştirir/devre dışı bırakır. 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 klavyesi gibi bir önyükleme ortamında alternatif veri girişi araçlarına sahip aygıtlar 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 artırmanıza ve daha az bilgisayar kaynağı kullanmanıza olanak tanır.
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, bu onay kutusu işaretlenmemiştir.

Kimlik doğrulama yöntemi

Parola kullan (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.

Güvenilir Platform Modülü (TPM) güvenlikle ilgili temel işlevleri sunmak (örneğin şifreleme anahtarını saklamak) için 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.

  Kullanıcının genişletilmiş PIN'i kullanmasına izin verebilirsiniz. *Genişletilmiş PIN* sayısal karakterlere ek olarak büyük ve küçük Latin harfleri, özel karakterler ve boşluklar gibi diğer karakterlerin kullanılmasına da izin verir.

- **Güvenilir platform modülü (TPM) veya TPM kullanılamıyorsa parola**. Onay kutusu seçilirse, bir Güvenilir Platform Modülü (TPM) kullanılamadığında, kullanıcı şifreleme anahtarlarına erişmek için bir parola kullanabilir.

  Bu onay kutusu işaretlenmemişse ve TPM kullanılabilir değilse, tam disk şifreleme başlamaz.

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.

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.

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.
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

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:

- Tam Disk Şifreleme (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.

- Dosya Düzeyinde Şifreleme (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:
  - Aygıt Kimliğine göre (Donanım Kimliği veya HWID)
  - Aygıt modeline göre: satıcı Kimliği (VID) ve ürün kimliği (PID)

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.

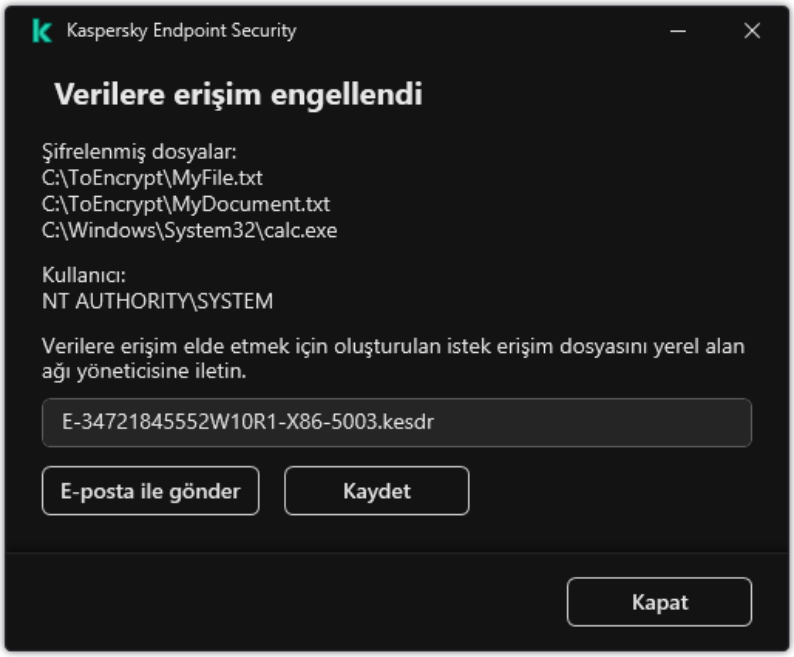
Onay kutusu işaretlenmezse Kaspersky Endpoint Security, Kaspersky Security Center ile bağlantı olmadığında çıkarılabilir sürücüleri şifrelemez.

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.

Tarama istisnaları

Tarama istisnası, Kaspersky Endpoint Security'nin belirli bir nesnede virüsleri ve diğer tehditleri taramaması için karşılanması gereken koşullar kümesidir.

Tarama istisnaları, saldırganlar tarafından bilgisayar veya kullanıcı verilerine zarar vermek amacıyla kullanılabilecek meşru yazılımın güvenli bir şekilde kullanılabilmesine imkan tanır. Kötü amaçlı işlevler içermese bile bu uygulamalar 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 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* görevleri.

Güvenilir uygulamaların listesi

Güvenilir uygulamaların listesi, dosya ve ağ etkinliği (kötü amaçlı etkinlik dahil) ve sistem kayıt defterine erişimi Kaspersky Endpoint Security tarafından izlenmeyen uygulamaların listesidir. Varsayılan olarak Kaspersky Endpoint Security, herhangi bir 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.

İstisna ayarları

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) **Tehdit 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. *Üzerine yazan* virüsler, kodlarını virüslü dosyanın kodu üzerine yazar, böylece dosyanın içeriği silinir. Virüslü dosya çalışmaz ve geri yüklenemez. *Asalak* virüsler dosyaları tamamen veya kısmen işlevsel bırakarak değiştirir. *Eşlik eden* virüsler dosyaları değiştirmez, bunun yerine kopyalarını oluşturur. Virüslü bir dosya açıldığında, dosyanın (aslında bir virüs olan) kopyası başlatılır. Şu virüs türlerine de rastlanmaktadır: *bağlantı virüsleri*, *OBJ virüsleri*, *LIB virüsleri*, *kaynak kod* virüsleri ve diğerleri.

Solucan

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	E-posta-Solucanı	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 İnternet Bağlantılı Sohbetler 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

Tehdit 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 bağlantı noktası 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.
Truva atı-Anında Mesajlaşma	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	Çevrimiçi oyunların kullanıcılarından hesap kimlik bilgilerini çalar ve daha sonra verileri saldırgana e-

	bilgi çalan Truva atları	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 (E-posta-Bombacısı, IM-Bombacısı ve SMS-Bombacısı).
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);

Tehdit 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: suçlular tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım.

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.
Dialer	Otomatik çeviriciler	Gizli modda bir modem üzerinden telefon bağlantıları kurabilir.
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 Arkakapı 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 bağlantı noktalarını 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 diğer yazılımları tespit et;

  Alt kategori: suçlular tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılım.

  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.
Dialer	Otomatik çeviriciler	Gizli modda bir modem üzerinden telefon bağlantıları kurabilir.
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 Arkakapı 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 bağlantı noktalarını 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

  Kaspersky Endpoint Security, sıkıştırılmış nesneleri ve SFX (kendi başına açılan) arşivlerdeki paket açıcı modülünü tarar.

  Tehlikeli programları anti-virüs uygulamalarından gizlemek için saldırganlar özel paketleyicileri kullanarak bunları arşivler veya çoklu sıkıştırılmış dosyalar oluşturur.

Kaspersky virüs analistleri bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

Kaspersky Endpoint Security bir dosyada böyle bir paketleyici tespit ederse dosya büyük olasılıkla bir zararlı uygulama veya bilgisayarınıza ya da kişisel verilerinize zarar vermek için suçlular tarafından kullanılan bir uygulama içeriyordur.

Kaspersky Endpoint Security aşağıdaki program türlerini eler:

- *Zarar verebilecek paketlenmiş dosyalar* – virüsler, solucanlar ve Trojanlar gibi zararlı yazılımların paketlenmesi için kullanılır.
- *Çoklu paketlenmiş dosyalar* (orta tehdit düzeyi) – nesne, bir veya daha fazla paketleyici tarafından üç kez paketlenmiştir.

- Çoklu paketlenmiş nesneler.

Kaspersky Endpoint Security, sıkıştırılmış nesneleri ve SFX (kendi başına açılan) arşivlerdeki paket açıcı modülünü tarar.

Tehlikeli programları anti-virüs uygulamalarından gizlemek için saldırganlar özel paketleyicileri kullanarak bunları arşivler veya çoklu sıkıştırılmış dosyalar oluşturur.

Kaspersky virüs analistleri bilgisayar korsanları arasındaki en popüler paketleyicileri tanımlamışlardır.

Kaspersky Endpoint Security bir dosyada böyle bir paketleyici tespit ederse dosya büyük olasılıkla bir zararlı uygulama veya bilgisayarınıza ya da kişisel verilerinize zarar vermek için suçlular tarafından kullanılan bir uygulama içeriyordur.

Kaspersky Endpoint Security aşağıdaki program türlerini eler:

- *Zarar verebilecek paketlenmiş dosyalar* – virüsler, solucanlar ve Trojanlar gibi zararlı yazılımların paketlenmesi için kullanılır.
- *Çoklu paketlenmiş dosyalar* (orta tehdit düzeyi) – nesne, bir veya daha fazla paketleyici tarafından üç kez paketlenmiştir.

İstisnalar

Bu tablo, tarama istisnaları hakkında bilgi içerir.

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:\Klasör\**\*.txt` maskesi, `Klasör` adlı klasörün kendisi hariç olmak üzere tüm `Klasör` 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.

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.

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.

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.

Güvenilir

Güvenilir sistem sertifika depolarından biri seçilirse, Kaspersky Endpoint Security, güvenilir bir dijital imza ile

sistem sertifika deposu	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
Bilgisayar başlatılırken Kaspersky Endpoint Security'yi başlat (önerilir)	Onay kutusu işaretlendiğinde işletim sistemi yüklendikten sonra Kaspersky Endpoint Security başlatılır ve bilgisayarı tüm oturum boyunca korur. Onay kutusu işaretlenmezse işletim sistemi yüklendikten sonra kullanıcı elle başlatana kadar Kaspersky Endpoint Security başlatılmaz. Bilgisayar koruması devre dışı olur ve kullanıcı verileri tehditlere maruz kalabilir.
Gelişmiş Temizleme teknolojisini kullan (ciddi düzeyde bilgisayar kaynağı gerektirir)	Onay kutusu işaretlenirse işletim sisteminde zararlı etkinlik tespit edildiğinde ekranda bir açılır pencere bildirimi görüntülenir. Kaspersky Endpoint Security bildirimde kullanıcıya bilgisayarın Gelişmiş Virüs Temizleme işlemini gerçekleştirmesini önerir. Kullanıcının bu işlemi onaylamasından sonra, Kaspersky Endpoint Security tehdidi etkisiz duruma getirir. Gelişmiş virüs temizleme işleminin tamamlanmasının ardından, Kaspersky Endpoint Security 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 yüzden kullanıcı etkin bir tehdidi temizlemek için bir eylem seçemez. 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.
Etkinleştirme için proxy sunucusu olarak Kaspersky Security Center'ı kullan *(sadece Kaspersky Security Center Konsolunda mevcuttur)*	Bu onay kutusu işaretlenirse uygulama etkinleştirilirken Kaspersky Security Center Yönetim Sunucusu, proxy sunucusu olarak kullanılır.

Kendini Korumayı Etkinleştir

Bu onay kutusu işaretlendiğinde Kaspersky Endpoint Security, sabit sürücüdeki uygulama dosyalarının, bellek işlemlerinin ve sistem kayıt defterindeki girdilerin değiştirilmesini veya silinmesini önler.

Sistem hizmetlerinin harici yönetimini etkinleştir

Onay kutusu seçilmişse, Kaspersky Endpoint Security, bir uzak bilgisayardan uygulama hizmetlerinin yönetimine izin verir. Uygulama hizmetlerini uzaktan yönetmek için bir girişim olduğunda Microsoft Windows görev çubuğunda uygulama simgesinin üstünde (kullanıcı tarafından bildirim hizmeti devre dışı bırakılmadığı sürece) bir bildirim görüntülenir.

Pil gücüyle çalışırken zamanlanmış görevleri ertele

Onay kutusu işaretlenirse enerji tasarrufu modu etkinleştirilir. Kaspersky Endpoint Security, zamanlanmış görevleri erteler. Gerekirse tarama ve güncelleme görevlerini elle başlatabilirsiniz.

Enerji tasarruf modu etkinleştirildiğinde ve bilgisayar pil gücüyle çalışırken aşağıdaki görevler zamanlanmış olsa bile çalıştırılmaz:

- *Güncelle*
- *Tam Tarama*
- *Kritik Alanları Tarama*
- *Özel Tarama*
- *Bütünlük denetimi*
- *IOC Taraması*.

Diğer uygulamalar için kaynak ayır

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, diğer uygulamalar için kaynak yaratacak şekilde yapılandırılmıştır.

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*.

Güncellemeleri bilgisayarı yeniden başlatmadan 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.

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.21.13\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.21.13\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 Detection and Response çözümleriyle çalışırken kullanır: EDR Optimum, EDR Expert, KATA (EDR), Kaspersky Sandbox. Diğer durumlarda, Kaspersky Endpoint Security ilgili dosyayı Yedeklemeye yerleştirir. Çözümlerin bir parçası olarak Karantinayı yönetmeyle ilgili ayrıntılar için lütfen Kaspersky Sandbox Yardımı , Kaspersky Endpoint Detection and Response Optimum Yardımı , Kaspersky Endpoint Detection and Response Expert Yardımı ve Kaspersky Anti Targeted Attack Platform Yardımı 'na başvurun.

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 saklama süresi limiti: N 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: N 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	Bu onay kutusu seçildiğinde maksimum dosya depolama süresi tanımlanan zaman aralığı ile sınırlanır.

saklama süresi limiti: N gün	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: N 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: N MB *(yalnızca Web Console'da bulunur)*	MB cinsinden maksimum Karantina boyutu. Örneğin, maksimum Karantina boyutunu 200 MB olarak ayarlayabilirsiniz. Karantina maksimum boyuta ulaştığında, Kaspersky Endpoint Security ilgili olayı 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 yüzdeye ulaştığında bildirim yap: yüzde N *(yalnızca Web Console'da bulunur)*	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.
Yönetim Sunucusu'na veri aktarımı *(yalnızca Kaspersky Security Center'da mevcuttur)*	Yönetim Sunucusuna bilgilerinin aktarılması gereken istemci bilgisayarlardaki olayların kategorileri.

Ağ ayarları

İnternete bağlanmak ve antivirüs veritabanları güncellemek için kullanılan proxy sunucuyu yapılandırabilir, ağ bağlantı noktası izleme modunu seçebilir ve şifrelenmiş bağlantı taramasını yapılandırabilirsiniz.

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	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 sunucusunu atla

Onay kutusu işaretlenirse Kaspersky Endpoint Security, paylaşılan klasörden güncelleme yaparken proxy sunucusu kullanmaz.

İzlenen bağlantı noktaları

Tüm ağ bağlantı noktalarını izle. Bu ağ bağlantı noktası izleme modunda, koruma bileşenleri (Dosya Tehdidi Koruması, Web Tehdidi Koruması, Posta Tehdidi Koruması), bilgisayarın tüm açık ağ bağlantı noktaları aracılığıyla aktarılan veri akışlarını izler.

Yalnızca seçili ağ bağlantı noktalarını izle. Bu ağ bağlantı noktası izleme modunda, koruma bileşenleri bilgisayarın seçilen bağlantı noktalarını ve seçilen uygulamaların ağ etkinliğini izler. E-posta ve ağ trafiğinin aktarımı için normalde kullanılan ağ bağlantı noktalarının listesi, Kaspersky uzmanlarının önerilerine göre yapılandırılmıştır.

Kaspersky tarafından önerilen listeden uygulamalar için tüm bağlantı noktalarını izle. Bu, ağ bağlantı noktaları 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 bağlantı noktalarını izle. Bu, ağ bağlantı noktaları 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.

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.

Geçersiz sertifikalı bir etki alanını ziyaret ederken

- **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.

- **Bağlantıyı 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.

Şifreli bağlantıları tarama hataları oluştuğunda

- **Bağlantıyı engelle**. Bu öğe seçildiğinde, bir şifreli bağlantıları tarama hatası meydana geldiğinde, Kaspersky Endpoint Security, ağ bağlantısını engeller.
- **Etki alanını istisnalara ekle**. Bu öğe seçilirse 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 **Bağlantıyı engelle**'i seçin. Kaspersky Endpoint Security ayrıca şifrelenmiş bağlantıları tarama hatası için bir olay oluşturur.

SSL 2.0 bağlantılarını engelle (önerilir)

Onay kutusu işaretlendiğinde, uygulama SSL 2.0 protokolü üzerinden kurulmuş ağ bağlantılarını engeller.

Onay kutusunun işareti kaldırıldığında, uygulama SSL 2.0 protokolü üzerinden kurulan ağ bağlantılarını engellemez ve bu bağlantılar üzerinden iletilen ağ trafiğini izlemez.

Şifrelenmiş bir bağlantının şifresini EV sertifikası kullanan web sitesiyle çöz

EV sertifikaları (Gelişmiş Doğrulama Sertifikaları), 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 adresler

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 uygulamalar

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.

Mozilla uygulamalarında şifreli bağlantıları taramak için seçilen sertifika deposunu kullan *(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 deposunu kullan (önerilir)**. Kaspersky kök sertifikası, Kaspersky Endpoint Security kurulumu sırasında bu depoya eklenir. • **Mozilla sertifika deposunu kullan**. Mozilla Firefox ve Thunderbird kendi sertifika depolarını kullanır. Mozilla sertifika deposu seçilirse, Kaspersky kök sertifikasını tarayıcı özelliklerinden bu depoya elle 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 ayrıca uygulama simgesinin üzerinde bildirimler görüntüler. **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. **Gösterme**. Bir istemci bilgisayarında, Kaspersky Endpoint Security'nin çalıştığına dair hiçbir işaret görüntülenmez. Windows bildirim alanındaki simge ve bildirimler yoktur.
Bildirim ayarları	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.
E-posta bildirim ayarları	Uygulamanın çalışması sırasında kaydedilen olaylar hakkındaki bildirimlerin teslime dilmesi için kullanılacak SMTP sunucusu ayarları.
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 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 işlemlerin gerçekleştirilmesi 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 / Tanım *(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.

> Düzenli güncellemeler için geçerli bir lisans gerekir. Geçerli bir lisans yoksa, güncellemeyi günde sadece bir kez gerçekleştirebilirsiniz.

Kaspersky Endpoint Security'nin ana güncelleme kaynağı, Kaspersky güncelleme sunucularıdır.

Kaspersky güncelleme sunucularından güncelleme paketini başarılı bir şekilde indirmek için bilgisayarınız İnternet'e bağlı olmalıdır. Varsayılan olarak İnternet bağlantısı ayarları otomatik olarak tespit edilir. Proxy sunucusu kullanıyorsanız, 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.

İçerik yardım dosyaları, uygulama modülü güncellemeleri ile birlikte güncellenebilir.

Veritabanları eskiyse, güncelleme paketi çok büyük olabilir ve ek İnternet trafiğine (onlarca MB) neden olabilir.

Kaspersky Endpoint Security veritabanlarının geçerli 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 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. **Elle**. 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 güncelleme görevini gerçekleştirilmesi mümkün olur olmaz başlatır. Örneğin, güncelleme görevinin başlatılma saatinde bilgisayar kapalıysa, güncelleme görevi atlanabilir. Onay kutusu işaretlenmezse Kaspersky Endpoint Security, kaçırılan güncelleme görevlerini başlatmaz. Bunun yerine, bir sonraki güncelleme görevini 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. 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.

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.

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.

Varsayılan olarak, bu onay kutusu 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.21.13\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 (İnternet Proxy Otomatik Bulma) 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 sunucusunu atla

Onay kutusu işaretlenirse Kaspersky Endpoint Security, paylaşılan klasörden güncelleme yaparken proxy sunucusu kullanmaz.

(yalnızca Kaspersky Endpoint Security arabiriminde mevcuttur)

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, dış hizmetlerle etkileşim için aşağıdaki ağ ayarlarını kullanır.

Ağ ayarları

Adres	Açıklama
`activation-v2.kaspersky.com/activationservice/activationservice.svc` İletişim kuralı: `HTTPS` Bağlantı noktası: `443`	Uygulamayı etkinleştirme.

`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`
Bağlantı noktası: `443`
	Veritabanlarını ve uygulama yazılım modüllerini güncelleme.

`downloads.upd.kaspersky.com` İletişim kuralı: `HTTPS` Bağlantı noktası: `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.

`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`

Veritabanlarını ve uygulama yazılım modüllerini güncelleme.

İletişim kuralı: `HTTP`

Bağlantı noktası: `80`

`ds.kaspersky.com` İletişim kuralı: `HTTPS` Bağlantı noktası: `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: `Any`
Bağlantı noktası: `443`, `1443`
	Kaspersky Security Network'ü kullanma.

`click.kaspersky.com`	Arabirimden bağlantıları takip edin.
`redirect.kaspersky.com` İletişim kuralı: `HTTPS`	

Şifreleme için kullanılan ayarlar

Adres	Açıklama

`crl.kaspersky.com`
`ocsp.kaspersky.com`
İletişim kuralı: `HTTP`
Bağlantı noktası: `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` – Bilgilendirici mesaj(ⓘ), `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.

Kritik

Son Kullanıcı Lisans Sözleşmesi ihlal edildi

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)	✓

Lisansın süresi dolmak 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 çok 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)	✓

Uygulamayı otomatik çalıştırma devre dışı bırakıldı

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 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, örneğin `Truva atları`. • `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 (`denylist`): `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 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, örneğin `Truva atları`. • `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 (`denylist`): `true` veya `false`. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Temizlenmesi olanaksız

Durum	❗
Bileşen	Dosya Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme 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, örneğin `Truva atları`. • `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 (`denylist`): `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 Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`313`
Kaspersky Security Center olay kimliği	`00000139`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşleme 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, örneğin `Truva atları`. • `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)	✓

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, örneğin `Truva atları`. • `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)	✓

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, örneğin `Truva atları`. • `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)	✓

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 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 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, `172.16.0.201` için `2886729929`. • `GNRL_EA_PARAM_4` bağlantı noktası 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, `172.16.0.201` için `2886729929`.
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)	✓

Bileşen güncelleme hatası

Durum	!
Bileşen	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
Windows olay kimliği	2153
Kaspersky Security Center olay kimliği	00000869
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Yama geri alma işlemi başarısız oldu

Durum	!
Bileşen	Veritabanı güncellemesi
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 mod etkinleştirmede hata

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 bırakmada hata

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	Kaspersky Sandbox
Windows olay kimliği	2252
Kaspersky Security Center olay kimliği	000008cc
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne karantinaya alınmadı (Kaspersky Sandbox)

Durum	!
Bileşen	Kaspersky 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	Kaspersky Sandbox
Windows olay kimliği	2607
Kaspersky Security Center olay kimliği	00000a2f
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Geçersiz Kaspersky Sandbox sunucusu sertifikası

Durum	!
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2613
Kaspersky Security Center olay kimliği	00000a35
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Sandbox düğümü kullanılamıyor

Durum	!
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2614
Kaspersky Security Center olay kimliği	00000a36
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne Kaspersky Sandbox'ta işlenirken bir hata meydana geldi

Durum	!

Bileşen	Kaspersky Sandbox
Windows olay kimliği	2617
Kaspersky Security Center olay kimliği	00000a39
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Sandbox içim maksimum yük aşıldı

Durum	!
Bileşen	Kaspersky 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)	✓

Kaspersky Sandbox lisans doğrulaması başarısız oldu

Durum	!
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2620
Kaspersky Security Center olay kimliği	00000a3c
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 kullanımına ilişkin izler 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 tespit edilen alışılmadık eylemler

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 olağandışı 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)	✓

Birleştirme 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)	✓

Kaspersky Anti Targeted Attack Platform sunucusuna bağlanırken hata oluştu

Durum	!
Bileşen	EDR (KATA)
Windows olay kimliği	2850
Kaspersky Security Center olay kimliği	00000b22
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Geçersiz Kaspersky Anti Targeted Attack Platform sunucu sertifikası

Durum	!
Bileşen	EDR (KATA)
Windows olay kimliği	2851
Kaspersky Security Center olay kimliği	00000b23
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Kaspersky Anti Targeted Attack Platform sunucusundaki aracının sertifikası geçersiz

Durum	!
Bileşen	EDR (KATA)
Windows olay kimliği	2852
Kaspersky Security Center olay kimliği	00000b24

Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İşlev hatası

Tümünü genişlet | Tümünü daralt

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

Tümünü genişlet | Tümünü daralt

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 eski

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

	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, örneğin `Truva atları`. • `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 (`denylist`): `true` veya `false`. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Nesne Yedekten geri yüklenemedi

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 kopyası oluşturulamadı

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Davranış Tespiti 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	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, örneğin `Truva atları`. • `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 (`denylist`): `true` veya `false`. EDR sürümü. EDR'deki tehdit tanımlayıcı. Nesnenin MD5 karması.
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 meşru yazılım algılandı (yerel veritabanları)

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme AMSI Koruması Davranış Tespiti Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`303`
Kaspersky Security Center olay kimliği	`GNRL_EV_SUSPICIOUS_OBJECT_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, örneğin `Truva atları`.
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İzinsiz giriş yapan kişiler tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek meşru yazılım algılandı (KSN)

Durum	⚠
Bileşen	Dosya Tehdidi Koruması Web Tehdidi Koruması Posta Tehdidi Koruması Sunucu Yetkisiz Erişim Önleme AMSI Koruması Davranış Tespiti Kötü Amaçlı Yazılım Taraması
Windows olay kimliği	`303`
Kaspersky Security Center olay kimliği	`GNRL_EV_SUSPICIOUS_OBJECT_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, örneğin `Truva atları`.
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 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, örneğin `Truva atları`. • `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 (`denylist`): `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	`GNRL_EV_OBJECT_CURED`

kimliği	
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, örneğin `Truva atları`. • `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 (`denylist`): `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 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 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)	✓

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, örneğin `Truva atları`.

	• `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 (`denylist`): `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, örneğin `Truva atları`. • `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 (`denylist`): `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	Veritabanı güncellemesi
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 imzası denetimi başarısız oldu

Durum	⚠
Bileşen	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 (Kaspersky Sandbox)

Durum	⚠
Bileşen	Kaspersky Sandbox
Windows olay kimliği	`2605`

Kaspersky Security Center olay kimliği	00000a2d
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Toplam tarama görevlerinin boyutu sınırı aştı

Durum	⚠
Bileşen	Kaspersky 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)	✓

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)	✓

Dosya değiştirildi

Durum	⚠
Bileşen	Dosya Bütünlüğü İzleyici
Windows olay kimliği	2900
Kaspersky Security Center olay kimliği	00000b54
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne çok sık değişiyor. Olay toplama başladı

Durum	⚠
Bileşen	Dosya Bütünlüğü İzleyici
Windows olay kimliği	2901
Kaspersky Security Center olay kimliği	00000b55
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Toplama dönemi için nesne değişikliği raporu

Durum	⚠
Bileşen	Dosya Bütünlüğü İzleyici
Windows olay kimliği	2902
Kaspersky Security Center olay kimliği	00000b56
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

İzleme kapsamı yanlış nesneler içeriyor

Durum	⚠
Bileşen	Dosya Bütünlüğü İzleyici
Windows olay kimliği	2903

Kaspersky Security Center olay kimliği	00000b57
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Bilgilendirici mesaj

Tümünü genişlet | Tümünü daralt

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 Sunucu Yetkisiz Erişim Önleme Kaspersky 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 kopyayla 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 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	Veritabanı güncellemesi
Windows olay kimliği	1001
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Proxy sunucusu seçildi

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
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 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	Veritabanı güncellemesi
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	Veritabanı güncellemesi
Windows olay kimliği	`1022`
Kaspersky Security Center olay kimliği	`000003fe`
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosyalar indiriliyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	1003
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya indirildi

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	1004
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya yüklendi

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	1005
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosya güncellendi

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
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	Veritabanı güncellemesi
Windows olay kimliği	1007
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosyalar güncelleniyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	1008
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Güncellemeler dağıtılıyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	1009
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Dosyalar geri alınıyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
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	Veritabanı güncellemesi
Windows olay kimliği	1013
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yamalar indiriliyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	2150
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama yükleniyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	2151
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama yüklendi

Durum	ⓘ

Bileşen	Veritabanı güncellemesi
Windows olay kimliği	2152
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama geri alınıyor

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
Windows olay kimliği	2154
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Yama geri alındı

Durum	ⓘ
Bileşen	Veritabanı güncellemesi
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)	–

Kimlik Doğrulama Aracısı oturum açma girişimi başarısız

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 var

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 işlemi 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 görevleri işleme etkin

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	Veri Silme
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	EDR (KATA)
Windows olay kimliği	2853
Kaspersky Security Center olay kimliği	00000b25
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Durum	ⓘ
Bileşen	Veri Silme
Windows olay kimliği	2253
Kaspersky Security Center olay kimliği	000008cd
Windows olay günlüğü (varsayılan)	–
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne karantinaya alındı (Kaspersky Sandbox)

Durum	ⓘ
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2602
Kaspersky Security Center olay kimliği	00000a2a
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	✓

Nesne silindi (Kaspersky Sandbox)

Durum	ⓘ

Bileşen	Kaspersky 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	Kaspersky Sandbox
Windows olay kimliği	2606
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Durum	ⓘ
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2609
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Durum	ⓘ

Bileşen	Kaspersky Sandbox
Windows olay kimliği	2610
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Durum	ⓘ
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2616
Kaspersky Security Center olay kimliği	–
Windows olay günlüğü (varsayılan)	✓
Kaspersky Security Center olay günlüğü (varsayılan)	–

Zaman uyumsuz Kaspersky Sandbox algılaması

Durum	ⓘ
Bileşen	Kaspersky Sandbox
Windows olay kimliği	2619
Kaspersky Security Center olay kimliği	GNRL_EV_APP_INCIDENT_OCCURED
Olay parametreleri	• GNRL_EA_PARAM_1 Kaspersky Sandbox bileşen ayarlarıdır • 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)	✓

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)	✓

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)	✓

Kaspersky Anti Targeted Attack Platform sunucusuna bağlantı başarılı oldu

Durum	ⓘ
Bileşen	EDR (KATA)
Windows olay kimliği	`2853`
Kaspersky Security Center olay kimliği	`00000b25`
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
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)

RegistryItem veri türünü IOC tarama kapsamına eklediğinizde, Kaspersky Endpoint Security şu 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.
- 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 standardı desteğinin özellikleri ve sınırlamaları 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`

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.

Üçüncü taraf kod hakkında bilgi

Üçüncü taraf kod hakkındaki bilgiler, uygulamanın yükleme klasöründe legal_notices.txt dosyasında bulunur.

Ticari marka bildirimleri

Tescilli ticari markalar ve hizmet markaları, 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 ve Safari, Apple Inc. şirketinin ticari markalarıdır.

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.

Android, Google Public DNS, Google Chrome, Chrome, Google LLC şirketinin ticari markalarıdır.

Citrix ve Citrix Provisioning Services, ve XenDesktop, Citrix Systems, Inc. ve/veya bir veya birden fazla yan kuruluşunun ticari markalarıdır ve Amerika Birleşik Devletleri Patent ve Marka Ofisi'nde ve diğer ülkelerde kayıtlı olabilir.

Cloudflare, Cloudflare Workers ve Cloudflare logosu, Amerika Birleşik Devletleri ve diğer yargı bölgelerinde Cloudflare, Inc.in ticari markaları ve/veya tescilli ticari markalarıdır.

Dell ve diğer ticari markalar, Dell Inc. veya yan kuruluşlarının ticari markalarıdır.

dBase, dataBased Intelligence, Inc.in ticari markasıdır.

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.

EMC, Amerika Birleşik Devletleri veya diğer ülkelerde EMC Corporation'un bir ticari markası veya tescilli ticari markasıdır.

Foxit, Foxit Corporation'ın tescilli ticari markasıdır.

Radmin, Famatech'in tescilli ticari markasıdır.

IBM, Business Machines Corporation şirketinin tüm dünyada birçok yasal bölgede kayıtlı olan bir ticari markasıdır.

Intel Amerika Birleşik Devletleri ve/veya diğer ülkelerde Intel Corporation'ın bir ticari markasıdır.

Cisco, Cisco AnyConnect; Cisco Systems, Inc. ve/veya bağlı kuruluşlarının ABD ve diğer bazı ülkelerdeki tescilli ticari markaları veya ticari markalarıdır.

Lenovo, 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 tescilli ticari markasıdır.

McAfee, McAfee LLC veya yan kuruluşlarının ABD ve/veya diğer ülkelerdeki ticari markası veya tescilli ticari markasıdır.

Microsoft, Microsoft Edge, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Skype, Surface, Hyper-V, SQL Server, 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.

Python, Python Software Foundation'ın ticari markası veya tescilli ticari markasıdır.

Java ve JavaScript, Oracle Corporation ve/veya yan kuruluşlarının tescilli ticari markalarıdır.

VERISIGN, Amerika Birleşik Devletleri ve diğer ülkelerde tescilli bir ticari marka veya VeriSign, Inc. ve yan kuruluşlarının tescilsiz bir ticari markasıdır.

VMware, VMware ESXi ve VMware Workstation, Amerika Birleşik Devletleri ve diğer yasal bölgelerde, VMware, Inc. şirketinin ticari markaları ya da tescilli ticari markalarıdır.

Tor, The Tor Project'in tescilli ticari markasıdır (ABD Tescil No. 3.465.432).

Thawte, Amerika Birleşik Devletleri ve diğer ülkelerde Symantec Corporation ve/veya bağlı kuruluşlarının ticari markası veya tescilli ticari markasıdır.

SAMSUNG, Amerika Birleşik Devletleri ve diğer ülkelerde SAMSUNG'un ticari markasıdır.