ESET Server Security

Kullanıcı Kılavuzu

Bu belgenin yardım sürümünü görüntülemek için burayı tıklayın

Digital Security
Progress. Protected.

Telif hakkı ©2023: ESET, spol. s r.o.

ESET Server Security, ESET, spol. s r.o. tarafından geliştirildi

Daha fazla bilgi için https://www.eset.com adresini ziyaret edin.

Tüm hakları saklıdır. Bu dokümanda yer alan hiçbir bölüm yazarından yazılı izin alınmadan yeniden üretilemez, yeniden kullanılabilir bir sistemde saklanamaz ya da herhangi bir biçimde ya da herhangi bir araçla (elektronik, mekanik, fotokopi, kayıt, tarama veya diğer) ile iletilemez.

ESET, spol. s r.o. açıklanan uygulama yazılımlarından herhangi birini önceden bildirilmeksizin değiştirme hakkını saklı tutar.

Teknik Destek: https://support.eset.com

REVİZE. 19.03.2023

1 Başlangıç ... 1
2 Genel Bakış ... 2
2.1 Başlıca özellikler ... 2
2.2 Yenilikler ... 3
2.3 Koruma türleri ... 3
3 Yükleme için hazırlanma ... 4
3.1 Sistem gereksinimleri ... 5
3.2 SHA-2 gerekli uyumluluk ... 6
3.3 ESET Server Security yükleme adımları ... 7
3.3 Mevcut bir yüklemeyi değiştirme ... 10
3.4 Sessiz / Katılımsız yükleme ... 12
3.4 Komut satırı yüklemesi ... 13
3.5 Ürün etkinleştirme ... 15
3.5 ESET Business Account ... 17
3.5 Etkinleştirme başarılı ... 17
3.5 Etkinleştirme hatası ... 17
3.5 Lisans ... 17
3.6 Daha yeni sürüme yükseltme ... 18
3.6 ESET PROTECT üzerinden yükseltme ... 18
3.6 ESET Cluster üzerinden yükseltme ... 20
3.7 Küme ortamında yükleme ... 23
3.8 Terminal sunucu ... 23
4 Başlarken ... 23
4.1 ESET PROTECT Üzerinden yönetilir ... 24
4.2 Koruma durumu ... 24
4.2 Durum ... 26
4.2 Windows güncellemesi var ... 27
4.2 Ağ yalıtımı ... 27
5 Komut için argüman olarak ESET Server Security ... 28
5.1 Tara ... 29
5.1 Tarama penceresi ve tarama günlüğü ... 31
5.2 Günlük dosyaları ... 32
5.2 Günlük filtreleme ... 35
5.3 Güncelleme ... 37
5.4 Ayarlar ... 39
5.4 Sunucu ... 40
5.4 Bilgisayar ... 41
5.4 Ağ ... 42
5.4 Ağ sorunu giderme sihirbazı ... 43
5.4 Web ve e-posta ... 43
5.4 Araçlar - Tanı amaçlı günlüğe kaydetme ... 44
5.4 Ayarları içe ve dışa aktarma ... 45
5.5 Araçlar ... 46
5.5 Çalışan işlemler ... 47
5.5 Etkinlik izleme ... 49
5.5 Koruma istatistikleri ... 50
5.5 Küme ... 52
5.5 Küme sihirbazı - Düğümleri seç ... 54
5.5 Küme sihirbazı - Küme ayarları ... 55
5.5 Küme sihirbazı - Küme kurulum ayarları ... 55

5.5 Küme sihirbazı - Düğüm denetimi ... 56
5.5 Küme sihirbazı - Düğüm yükleme ... 57
5.5 ESET Shell ... 60
5.5 Kullanım ... 62
5.5 Komutlar ... 67
5.5 Toplu dosyalar / Komut dosyası ... 70
5.5 ESET SysInspector ... 71
5.5 ESET SysRescue Live ... 72
5.5 Zamanlayıcı ... 72
5.5 Zamanlayıcı - Görev ekle ... 73
5.5 Görev türü ... 76
5.5 Görev zamanlaması ... 77
5.5 Olay tetiklediğinde ... 77
5.5 Uygulamayı çalıştır ... 78
5.5 Atlanan görev ... 78
5.5 Zamanlanan göreve genel bakış ... 78
5.5 Örnekleri analiz için gönderin ... 78
5.5 Şüpheli dosya ... 79
5.5 Şüpheli site ... 80
5.5 Hatalı pozitif dosya ... 80
5.5 Hatalı pozitif site ... 81
5.5 Diğer ... 81
5.5 Karantina ... 81
5.6 OneDrive tarama ayarları ... 83
5.6 ESET OneDrive tarayıcısını kaydedin ... 86
5.6 ESET OneDrive tarayıcısının kaydını kaldırın ... 91
6 Genel ayarlar ... 95
6.1 Algılama Altyapısı ... 96
6.1 Makine Öğrenimini algılama ... 98
6.1 Tarama dışı öğeler ... 100
6.1 Performansla ilgili tarama dışı bırakma işlemleri ... 101
6.1 Algılama dışı bırakılan öğeler ... 102
6.1 Tarama dışı bırakma sihirbazı oluştur ... 104
6.1 Gelişmiş seçenekler ... 104
6.1 Otomatik dışlamalar ... 105
6.1 Paylaşılan yerel önbellek ... 105
6.1 Sızıntı algılandı ... 105
6.1 Gerçek zamanlı dosya sistemi koruması ... 106
6.1 ThreatSense parametreleri ... 108
6.1 Ek ThreatSense parametreleri ... 112
6.1 Tarama dışında bırakılan dosya uzantıları ... 112
6.1 Tarama dışı tutma işlemlerini yerine getirir ... 112
6.1 Bulut tabanlı koruma ... 114
6.1 Tarama dışı bırakma filtresi ... 116
6.1 Kötü amaçlı yazılım taramaları ... 116
6.1 Profil yöneticisi ... 117
6.1 Profil hedefleri ... 118
6.1 Tarama hedefleri ... 120
6.1 Boşta durumu taraması ... 121
6.1 Başlangıç taraması ... 122
6.1 Başlangıçta otomatik dosya denetimi ... 122

6.1 Çıkarılabilir medya ... 123
6.1 Belge koruması ... 123
6.1 Hyper-V taraması ... 124
6.1 OneDrive taraması ... 126
6.1 HIPS ... 127
6.1 HIPS kural ayarları ... 129
6.1 HIPS gelişmiş ayarları ... 132
6.2 Güncelleme yapılandırması ... 132
6.2 Güncelle geri dönüşü ... 136
6.2 Zamanlanan Görev - Güncelleme ... 136
6.2 Güncelle yansıtması ... 137
6.3 Ağ koruması ... 139
6.3 IDS özel durumları ... 140
6.3 Geçici IP adresi kara listesi ... 141
6.4 Web ve e-posta ... 141
6.4 Protokol filtrelemesi ... 142
6.4 Web ve e-posta istemcileri ... 143
6.4 SSL/TLS ... 143
6.4 Bilinen sertifikalar listesi ... 144
6.4 Şifrelenmiş SSL iletişimi ... 145
6.4 E-posta istemci koruması ... 146
6.4 E-posta protokolleri ... 147
6.4 Uyarılar ve bildirimler ... 147
6.4 MS Outlook araç çubuğu ... 148
6.4 Outlook Express ve Windows Mail araç çubuğu ... 148
6.4 Onay iletişim penceresi ... 149
6.4 İletileri yeniden tara ... 149
6.4 Web erişimi koruması ... 149
6.4 URL adresi yönetimi ... 150
6.4 Yeni liste oluştur ... 151
6.4 Kimlik Avı web koruması ... 153
6.5 Cihaz Kontrolü ... 154
6.5 Aygıt kuralları ... 154
6.5 Aygıt grupları ... 156
6.6 Araçların yapılandırılması ... 157
6.6 Zaman aralığı ... 158
6.6 Microsoft Windows® Update ... 158
6.6 Komut satırı tarayıcısı ... 158
6.6 ESET CMD ... 161
6.6 ESET RMM ... 162
6.6 Lisans ... 163
6.6 WMI Sağlayıcı ... 164
6.6 Sağlanan veriler ... 164
6.6 Sağlanan Verilere Erişme ... 171
6.6 ESET PROTECT tarama hedefleri ... 172
6.6 Geçersiz kılma modu ... 173
6.6 Günlük dosyaları ... 176
6.6 Proxy sunucu ... 177
6.6 Bildirimler ... 178
6.6 Uygulama bildirimleri ... 178
6.6 Masaüstü bildirimleri ... 179

6.6 E-posta bildirimleri 180
6.6 Özelleştirme 181
6.6 Sunum modu 182
6.6 Tanılamalar 182
6.6 Teknik destek 183
6.6 Küme 183
6.7 Kullanıcı arabirimi 185
6.7 Uyarılar ve mesaj kutuları 186
6.7 Erişim ayarları 187
6.7 ESET Shell 188
6.7 Terminal Sunucuda GUI'yi devre dışı bırakma 188
6.7 Devre dışı bırakılan iletiler ve durumlar 189
6.7 Uygulama durumları ayarları 189
6.7 Sistem tepsisi simgesi 190
6.8 Varsayılan ayarlara döndür 191
6.9 Yardım ve destek 192
6.9 Destek isteği gönderme 193
6.9 ESET Server Security Hakkında 193
6.10 Sözlük 193
7 Son Kullanıcı Lisans Sözleşmesi 194
8 Gizlilik Politikası 200

Başlangıç

Bu kılavuz, ESET Server Security ürününden en iyi şekilde yararlanmanız amacıyla tasarlanmıştır. Programdaki herhangi bir pencereyle ilgili daha fazla bilgi için, halihazırda açık olan pencerede, klavyenizdeki **F1** tuşuna basın. Görüntülemekte olduğunuz pencereyle ilgili yardım sayfası açılır.

Tutarlılık sağlamak ve karışıklığı önlemek için bu kılavuz kapsamında kullanılan terminoloji, ESET Server Security parametre adlarına dayanmaktadır. Ayrıca, belirli ilgi veya öneme sahip konuları vurgulamak için de tek tip bir semboller dizisi kullanılmıştır.

NOT
Not, kısa bir gözlem aktarır. Not kısımları atlanabilir ancak bazen bu bölümlerde belirli özellikler veya diğer ilgili başlıklara yönelik bir bağlantı gibi değerli bilgiler sunulur.

ÖNEMLİ
Bu kısımlara dikkat edilmelidir ve bu kısımların atlanması önerilmez. Önemli notlar, önemli olan ancak kritik olmayan bilgileri içerir.

UYARI
Daha fazla dikkat göstererek ele almanız gereken kritik bilgilerdir. Uyarılar, zarar getirebilecek olası hatalar yapmanızı engellemek için özellikle belirtilir. Lütfen son derece hassas sistem ayarları veya diğer riskli durumlardan bahseden uyarı parantezlerinin içindeki metni okuyun ve anlayın.

ÖRNEK
Bu, belirli bir işlev veya özelliğin nasıl kullanılacağını anlamanıza yardımcı olan kullanıma veya uygulamaya yönelik bir örnektir.

Yardım sayfasının sağ üst köşesinde aşağıdaki öğeyi görebilirsiniz. Bu, ESET Server Security aracının grafik kullanıcı arabiriminin (GUI) pencereleri içerisindeki gezinmeyi gösterir. Her bir yardım sayfasında açıklanan pencereye gitmek için şu talimatları uygulayın.

ESET Server Security Uygulamasını aç
Ayarlar > Sunucu > OneDrive Tarama ayarları > Kayıt

Biçimlendirme kuralları:

Kural	Anlam
Kalın yazı tipi	Bölüm başlıkları, özellik adları veya düğmeler gibi kullanıcı arabirimi öğeleri.
İtalik yazı tipi	Sağladığınız bilgilere yönelik yer tutucular. Örneğin, dosya adı veya yolu, bir dosyanın gerçek yolunu veya adını girdiğiniz anlamına gelir.

Kural	Anlam
`Courier New`	Kod örnekleri veya komutlar.
Köprü	Çapraz referanslı konulara veya harici web konumlarına hızlı ve kolay erişim sağlar. Köprüler mavi renkte vurgulanır ve altı çizili olabilir.
%ProgramFiles%	Yüklenen Windows programlarını ve diğerlerini depolayan Windows sistem dizini.

ESET Server Security online yardım sayfaları, çeşitli bölümlere ve alt bölümlere ayrılmıştır. Yardım sayfalarındaki İçerikler'e göz atarak istediğiniz bilgileri bulabilirsiniz. Alternatif olarak, kelime veya ifadeleri yazarak tam metin araması yapabilirsiniz.

Genel Bakış

ESET Server Security, Microsoft Windows Server ortamı için özel olarak tasarlanmış entegre bir çözümdür. ESET Server Security, çeşitli kötü amaçlı yazılım türlerine karşı etkili ve güvenilir koruma sağlar ve iki tür koruma sunar: Zararlı Yazılıma Karşı Koruma ve Antispyware.

Başlıca özellikler

Aşağıdaki tabloda ESET Server Security içinde bulunan özelliklerin listesi yer almaktadır. ESET Server Security aracı Microsoft Windows Server 2008 R2 SP1, 2012, 2016 ve 2019'un çoğu sürümünü bağımsız ve kümeli ortamlarda destekler. Daha büyük ağlarda, ESET Server Security ürününü ESET PROTECT yardımıyla uzaktan yönetebilirsiniz.

True 64 bit ürün çekirdeği	Ürün çekirdeği bileşenlerine daha yüksek performans ve istikrar kazandırır.
Zararlı yazılımlardan koruma	Zararlı yazılımlara karşı ödüllü ve yenilikçi bir savunma olan bu ileri düzey teknoloji, daha da iyi tespit oranları için bulut destekli tarama özelliğiyle saldırıları önler ve virüs, fidye yazılımı, rootkit, solucan, casus yazılım dahil olmak üzere her türden tehdidi yok eder. Küçük boyutuyla, çok az miktarda sistem kaynağı tükettiğinden sistem performansından ödün verilmesine neden olmaz. Katmanlı bir güvenlik modeli kullanır. Her katman veya aşama bir dizi çekirdek teknolojiden yararlanır. *Yürütme öncesi* aşamada, *UEFI Tarayıcı, Ağ Saldırısına Karşı Koruma, Tanınırlık ve Önbellek, Ürün İçi Sandbox (Korumalı alan), DNA Tespiti* gibi teknolojiler kullanılır. *Yürütme* aşamasında *Exploit Engelleyici, Fidye Yazılımı Koruması, Gelişmiş Bellek Tarayıcısı* ve *Script Scanner (AMSI)* gibi teknolojiler kullanılırken *Yürütme sonrası* aşamada *Botnet Koruması, Bulut Zararlı Yazılıma Karşı Koruma Sistemi* ile *Sandboxing* (Korumalı alan) kullanılır. Çekirdek teknolojilerden oluşan, çok çeşitli özellikler içeren bu set, benzersiz bir koruma düzeyi sağlar.
OneDrive taraması	OneDrive bulut depolamasında bulunan dosyaları taramak için daha fazla seçenek sunan yeni bir özelliktir. Örneğin Office 365 kurumsal hesabı.
Hyper-V taraması	Belirli VM'de herhangi bir "Agent"a gerek olmadan Microsoft Hyper-V Server'daki Sanal Makine (VM) taramasına olanak sağlayan yeni bir teknolojidir.
ESET Dynamic Threat Defense (EDTD)	ESET Bulut tabanlı hizmeti. ESET Server Security şüpheli bir kod veya davranış algıladığında, bunu geçici olarak ESET Dynamic Threat Defense karantinasına alarak daha fazla tehdit eylemini engeller. Şüpheli örnek, ileri teknolojili kötü amaçlı yazılım algılama altyapılarıyla analiz için otomatik olarak ESET Dynamic Threat Defense sunucusuna gönderilir. Daha sonra, ESET Server Security ürününüz analizin sonucunu alır ve şüpheli dosya bu sonuca göre yönetilir.

True 64 bit ürün çekirdeği	Ürün çekirdeği bileşenlerine daha yüksek performans ve istikrar kazandırır.
ESET Kümesi	ESET Kümesi, birden çok sunucunun tek bir konumdan yönetilmesine olanak tanır. İş istasyonlarının düğümlere katılması, bir yapılandırma ilkesini tüm küme üyelerine dağıtma becerisine bağlı olarak ek yönetim otomasyonu sağlar. Kümelerin kendilerinin oluşturulması, yüklenen düğüm kullanılarak mümkündür. Yüklenen bu düğüm, tüm düğümleri uzaktan yükleyip başlatabilir. ESET sunucu ürünleri birbirleriyle iletişim kurabilir ve yapılandırma ve bildirim gibi verileri gönderip alabilir, ayrıca yüklenmiş ürünler grubunun doğru işlemesi için gerekli olan verileri senkronize etmesinin yanı sıra gri listeye alınan veri tabanlarını senkronize edebilir. Bu, ürünün bir kümenin tüm üyelerinde aynı şekilde yapılandırılmasını sağlar. Windows Yük Devri Kümeleri ve Ağ Yükü Dengelemesi (NLB) Kümeleri, ESET Server Security tarafından desteklenir. Ayrıca, ESET Kümesi üyelerini, belirli Windows Kümesine ihtiyaç olmadan manuel olarak da ekleyebilirsiniz. ESET Kümeleri, hem etki alanı hem de çalışma grubu ortamlarında çalışır.
Otomatik dışlamalar	Düzgün çalışma ve performans için kritik uygulamaların ve sunucu dosyalarının otomatik olarak algılanması ve tarama dışı bırakılması.
Tarama dışı tutma işlemlerini yerine getirir	Belirli işlemleri Zararlı Yazılıma Karşı Koruma erişim taramasının dışında bırakır. Zararlı Yazılıma Karşı Koruma erişim temelli tarama, belirli durumlarda çakışmalara neden olabilir; örneğin, yedekleme veya sanal makineleri canlı taşıma işlemi sırasında. Tarama dışı bırakılan işlemler, potansiyel çakışma riskini en düşük düzeye indirir ve tarama dışı bırakılan uygulamaların performansını iyileştirerek işletim sisteminin genel performansı ve istikrarı üzerinde olumlu bir etki yaratır. Bir işlemin / uygulamanın tarama dışında bırakılması kendisine ait yürütülebilir dosyanın (*.exe*) tarama dışında bırakılmasıdır.
eShell ESET Shell	eShell 2.0 ileri düzey kullanıcılara ve yöneticilere ESET sunucu ürünlerini yönetmek için daha kapsamlı seçenekler sunan bir komut satırı arabirimidir.
ESET PROTECT	İsteğe bağlı tarama zamanlaması becerisine sahip ESET PROTECT ile daha iyi entegrasyon. Daha fazla bilgi için, bkz. ESET PROTECT Çevrimiçi yardım.
Bileşen tabanlı yükleme	Yükleme işlemi, ürünün yalnızca seçili bölümlerini içerecek şekilde özelleştirilebilir.

Yenilikler

ESET Server Security'deki yeni özellikler ve iyileştirmeler:

- True 64 bit ürün çekirdeği
- OneDrive taraması
- ESET Dynamic Threat Defense (EDTD)
- ESET Enterprise Inspector desteği
- ESET RMM
- Ağ yalıtımı
- Makine Öğrenimini algılama
- Denetim günlükleri
- Mikro Program Bileşeni Güncellemeleri

Koruma türleri

İki tür koruma vardır:

- Zararlı Yazılıma Karşı koruma
- Antispyware koruması

Zararlı Yazılıma Karşı Koruma ve Antispyware koruması, ESET Server Security ürününün temel işlevlerinden biridir. Bu koruma dosyayı, e-postayı ve İnternet iletişimini denetleyerek kötü amaçlı sistem saldırılarına karşı koruma sağlar. Bir tehdit bulunursa, tespit modülü tehdidi engelleyerek, ardından temizleyerek, silerek ve Karantinaya alarak ortadan kaldırabilir.

Yükleme için hazırlanma

Ürün yüklemesi için hazırlanırken izlemenizi önerdiğimiz birkaç adım vardır:

- ESET Server Security ürününü satın aldıktan sonra `.msi` yükleme paketini ESET web sitesinden indirin.
- ESET Server Security aracını yüklemeyi planladığınız sunucunun sistem gereksinimlerini karşıladığından emin olun.
- Bir Yönetici hesabını kullanarak sunucuda oturum açın.

> NOT
> Yükleyiciyi, Tümleşik Yönetici hesabı veya bir etki alanı Yönetici hesabı (yerel Yönetici hesabı devre dışı bırakılmışsa) kullanarak yürütmeniz gerektiğini lütfen unutmayın. Yöneticiler grubunun üyesi olmasına rağmen başka bir kullanıcının yeterli erişim hakkı yoktur. Bu nedenle, yerel veya etki alanı Yöneticisi'nden başka bir kullanıcı hesabı altında yüklemeyi başarılı bir şekilde tamamlayamayacağınız için, Tümleşik Yönetici hesabını kullanmanız gerekir.

- Mevcut bir ESET Server Security yüklemesinden yükseltme yapacaksanız, Ayarları dışa aktar özelliğini kullanarak mevcut yapılandırmasını yedeklemenizi öneririz.
- Sisteminizden, varsa tüm üçüncü taraf antivirus yazılımlarını kaldırın veya yüklemelerini kaldırın. ESET AV Remover aracını kullanmanızı öneririz. ESET AV Remover kullanılarak kaldırılabilecek olan üçüncü taraf antivirus yazılımlarının listesi için bu BB makalesine bakın.
- Windows Server 2016'ya ESET Server Security yüklüyorsanız Microsoft, bir makinede yüklü birden çok antivirus ürününün bulunmasından kaynaklanan sorunları önlemek için Windows Defender Özelliklerinin yüklemesini kaldırmanızı ve Windows Defender ATP kaydından geri çekilmenizi önerir.
- Windows Server 2019, Microsoft Windows Server 2022 a ESET Server Security yüklüyorsanız Microsoft, bir makinede yüklü birden çok antivirus ürününün bulunmasından kaynaklanan sorunları önlemek için Windows Defender'ı **pasif moda** almanızı önerir.

ESET Server Security yükleyicisini iki yükleme modunda çalıştırabilirsiniz:

- Grafik kullanıcı arabirimi (GUI)
  Bu, bir yükleme sihirbazıyla yapılan ve önerilen yükleme türüdür.
- Sessiz / Katılımsız yükleme
  Yükleme sihirbazına ek olarak, ESET Server Security ürününü komut satırı üzerinden sessizce yüklemeyi de seçebilirsiniz.

> ÖNEMLİ
> ESET Server Security ürününü mümkünse yeni yüklenmiş ve yapılandırılmış bir işletim sistemine yüklemenizi öneririz. Mevcut sisteme yüklemeniz gerekiyorsa, önceki ESET Server Security sürümünün yüklemesini kaldırıp sunucuyu yeniden başlatmanızı ve ardından yeni ESET Server Security ürününü yüklemenizi öneririz.

- Daha yeni sürüme yükseltme

Eski bir ESET Server Security sürümü kullanıyorsanız, uygun yükseltme yöntemini seçebilirsiniz.

ESET Server Security ürününüzü başarıyla yükledikten veya yükselttikten sonra şu işlemler söz konusu olur:

- Ürün etkinleştirme
  Etkinleştirme penceresindeki belirli bir etkinleştirme senaryosunun kullanılabilirliği, ülkeye ve dağıtım şekline bağlı olarak değişiklik gösterebilir.

- Genel ayarları yapılandırma
  ESET Server Security ürününüzü, ihtiyaçlarınıza göre özelliklerin her birinin gelişmiş ayarlarını değiştirerek hassaslaştırabilirsiniz.

Sistem gereksinimleri

Desteklenen İşletim Sistemleri:

- Microsoft Windows Server 2022 (Server Core ve Desktop Experience)
- Microsoft Windows Server 2019 (Server Core ve Desktop Experience)
- Microsoft Windows Server 2016 (Server Core ve Desktop Experience)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- KB4474419 ve KB4490628 yamasıyla birlikte yüklenen Microsoft Windows Server 2008 R2 SP1 (SHA-2 gerekli uyumluluk bölümünü okuyun)
- Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2)

> NOT
> Windows Server 2008 R2 SP1'de **Ağ koruma** bileşeni **Normal** yüklemede varsayılan olarak devre dışıdır. Bu bileşenin yüklenmesi için **Özel** yükleme seçeneğini kullanın.

Depolama, Küçük İşletme ve MultiPoint sunucuları:

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Temeli
- Microsoft Windows Small Business Server 2011 SP1 (x64) KB4474419 ve KB4490628 yamasıyla birlikte yüklendi

- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011

- Microsoft Windows MultiPoint Server 2010

Desteklenen Ana bilgisayar İşletim Sistemleri (Hyper-V rolüyle birlikte):

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 - Sanal Makineler yalnızca çevrimdışıyken taranabilir

Donanım gereksinimleri, kullanılan işletim sistemi sürümüne bağlıdır. Donanım gereksinimleriyle ilgili ayrıntılı bilgiler için Microsoft Windows Server ürün belgelerini okumanızı öneririz.

> NOT
> ESET güvenlik ürününüzü yüklemeden önce, Microsoft Server işletim sisteminiz için en son Hizmet Paketini ve sunucu uygulamasını yüklemenizi kesinlikle öneririz. Ayrıca kullanıma sunulduğunda en son Windows güncellemelerini ve düzeltmeleri de yüklemenizi öneririz.

Minimum donanım gereksinimleri:

Bileşen	Gereksinim
İşlemci	Intel veya AMD tek çekirdek x64
Bellek	256 MB boş bellek
Sabit Sürücü	700 MB boş disk alanı
Ekran çözünürlüğü	800 x 600 piksel veya üzeri

SHA-2 gerekli uyumluluk

Microsoft Secure Hash Algorithm 1'in (SHA-1) kullanımdan kaldırıldığını duyurdu ve 2019 yılının başında SHA-2'ye geçiş sürecini başlattı. Bu nedenle, SHA-1 algoritmasıyla imzalanan tüm sertifikaları artık tanınmayacak ve güvenlik uyarılarına neden olacak. Maalesef algoritmada bulunan zayıf noktalar, daha fazla işleyici performansı ve bulut işlemciliğinin ortaya çıkması nedeniyle SHA-1 hash algoritmasının güvenliği zaman içinde zayıfladı.

SHA-2 hash algoritması (SHA-1'in ardılı olarak) SSL güvenliğinin temin edilmesi için şu anda tercih edilen yöntemdir. Daha fazla bilgi için Hash ve İmza Algoritmaları başlıklı Microsoft Docs makalesini okuyun.

> NOT
> Bu değişiklik, SHA-2 desteği bulunmayan işletim sistemlerinde ESET güvenlik çözümünüzün algılama altyapısı da dahil olmak üzere modüllerini artık güncelleyemeyeceği anlamına geliyor. Bu durum zaman içinde ESET Server Security aracınızın tam işlev göstermemesine ve yeterli korumayı sağlayamamasına neden olacaktır.

Microsoft Windows Server 2008 R2 SP1 veya **Microsoft Windows Small Business Server 2011 SP1** kullanıyorsanız sisteminizin SHA-2 ile uyumlu olduğundan emin olun. Belirli işletim sistemi sürümünüze uygun olan yamaları aşağıdaki gibi uygulayın:

- **Microsoft Windows Server 2008 R2 SP1** — KB4474419 ve KB4490628 yamasını uygulayın (sistemde ek bir yeniden başlatma işlemi gerekebilir)

- **Microsoft Windows Small Business Server 2011 SP1** (x64) — KB4474419 ve KB4490628 yamalarını uygulayın (sistemde ek bir yeniden başlatma işlemi gerekebilir)

> ÖNEMLİ
> Güncellemeleri yükledikten ve sisteminizi yeniden başlattıktan sonra ESET Server Security GUI'sini açarak durumunu kontrol edin. Durum turuncu renkteyse sistemde ek bir yeniden başlatma işlemi yapın. Bunun ardından durum maksimum koruma olduğunu göstererek yeşile dönecektir.

> NOT
> Microsoft Server işletim sisteminiz için en son Hizmet Paketini ve sunucu uygulamasını yüklemenizi kesinlikle öneririz. Ayrıca kullanıma sunulduğunda en son Windows güncellemelerini ve düzeltmeleri de yüklemenizi öneririz.

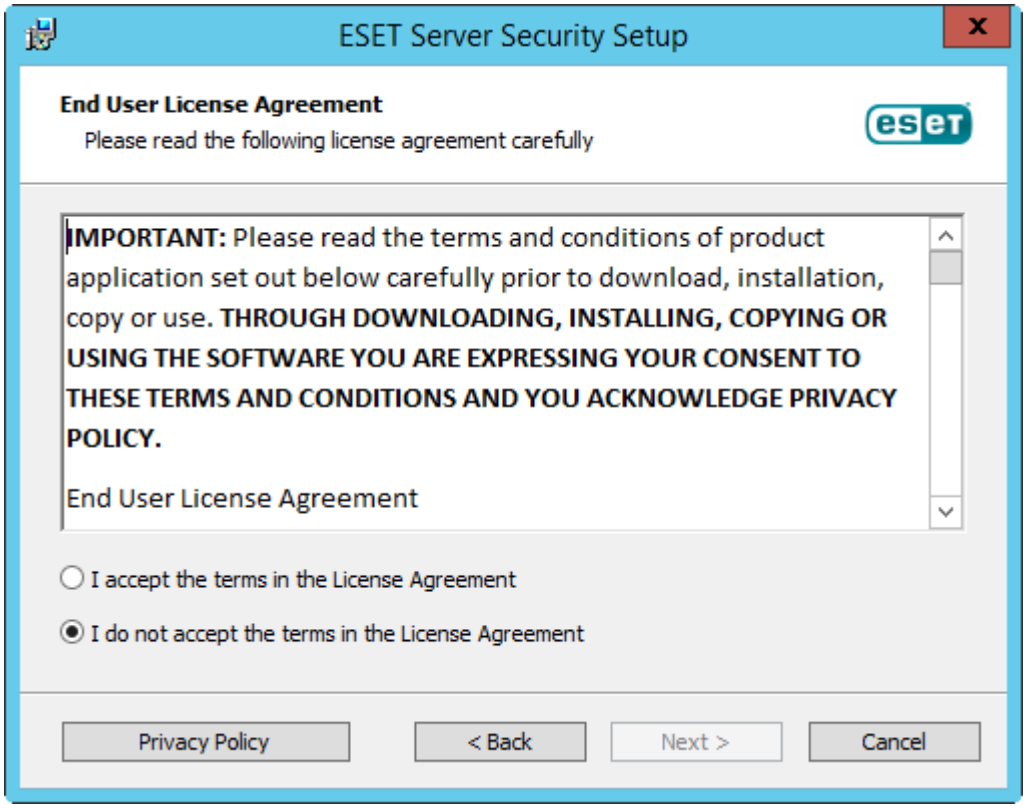
ESET Server Security yükleme adımları

Bu tipik bir GUI yükleme sihirbazıdır. `.msi` paketini çift tıklayın ve ESET Server Security yükleme adımlarını izleyin:

1. Devam etmek için **İleri**'yi tıklayın veya yüklemeden çıkmak istiyorsanız **İptal**'i tıklayın.

2. Yükleme sihirbazı, işletim sisteminizin **Bölge** > **Yer** ayarının **Ev konumu** (veya eski sistemlerde **Bölge ve Dil** > **konum** ayarının **Mevcut konum**) olarak belirtilen bir dilde çalışır. **Ürün dilini** seçmek için açılır menüyü kullanın. ESET Server Security aracınız bu dilde yüklenecektir. ESET Server Security için seçilen dil, yükleme sihirbazında gördüğünüz dilden bağımsızdır.

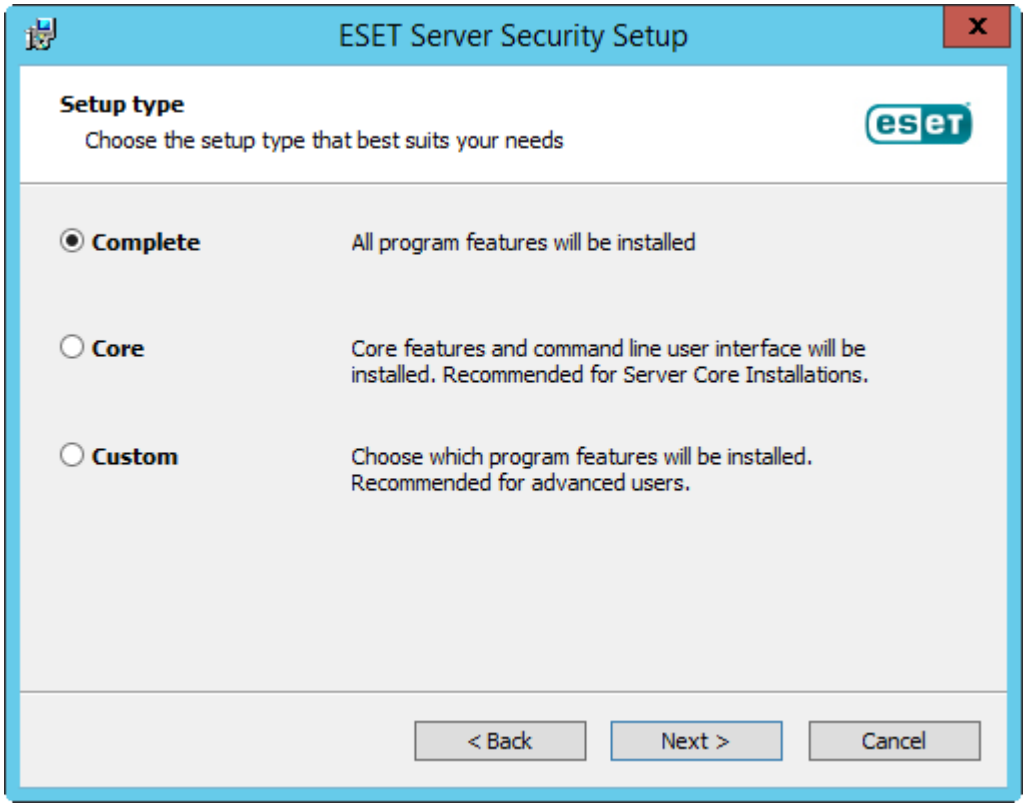
3. **İleri**'yi tıkladığınızda Son Kullanıcı Lisans Sözleşmesi görüntülenir. **Son Kullanıcı Lisans Sözleşmesi**'ni ve Gizlilik Politikası'nı kabul ettiğinizi belirttikten sonra **İleri**'yi tıklayın.



4.Mevcut yükleme türlerinden birini seçin (türlerin kullanılabilirliği, işletim sisteminize bağlıdır):

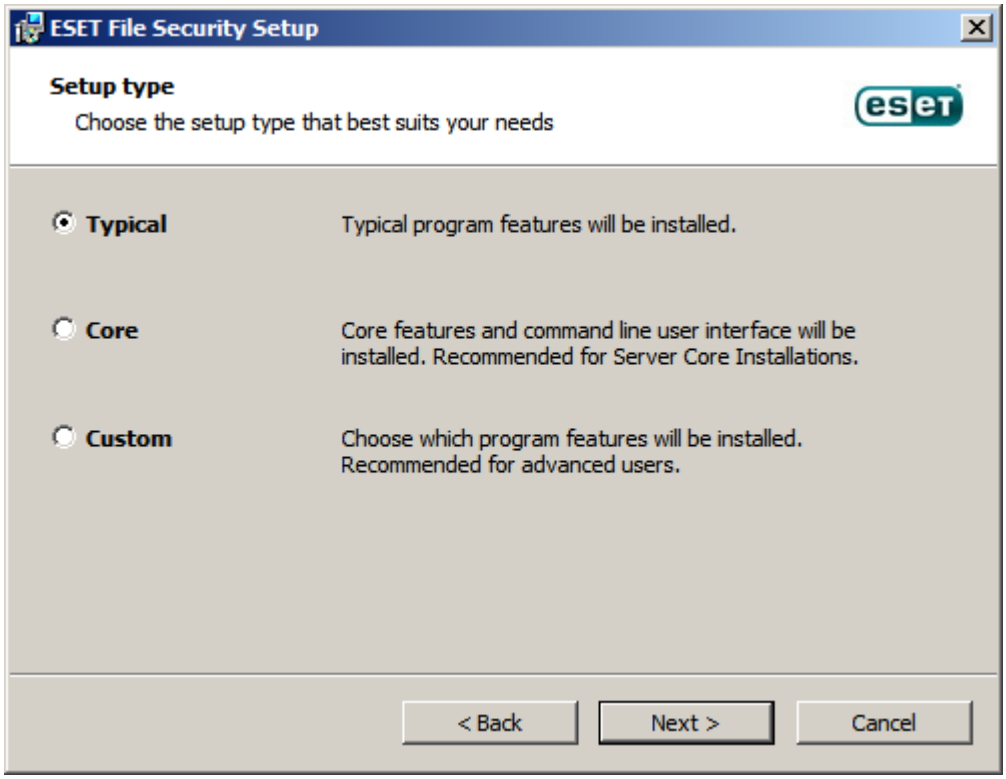
Tam

Tüm ESET Server Security özelliklerini yükler. Tam yükleme de denir. Bu, **Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials ve 2019 Essentials** için önerilen yükleme türüdür.



Standart

Önerilen ESET Server Security özelliklerini yükler. 2008 R2 SP1 ve 2011 için kullanılabilir.



Çekirdek

Bu yükleme türü, Windows Server Çekirdeği yayın sürümleri için tasarlanmıştır. Yükleme adımları tam yükleme adımlarıyla aynıdır, ancak yalnızca çekirdek özellikler ve komut satırı kullanıcı arabirimi yüklenir. Çekirdek yüklemesi temel olarak Windows Server Core'da kullanım için olsa da tercih etmeniz halinde normal Windows Server üzerine de yükleyebilirsiniz. Çekirdek yükleme kullanılarak yüklenen ESET güvenlik ürününde GUI olmaz. Bu, ESET Server Security ile çalışırken yalnızca komut satırı kullanıcı arabirimini kullanabileceğiniz anlamına gelir. Daha ayrıntılı bilgiler ve diğer özel parametrelerle ilgili detaylar için Komut satırı yüklemesi bölümüne bakın.

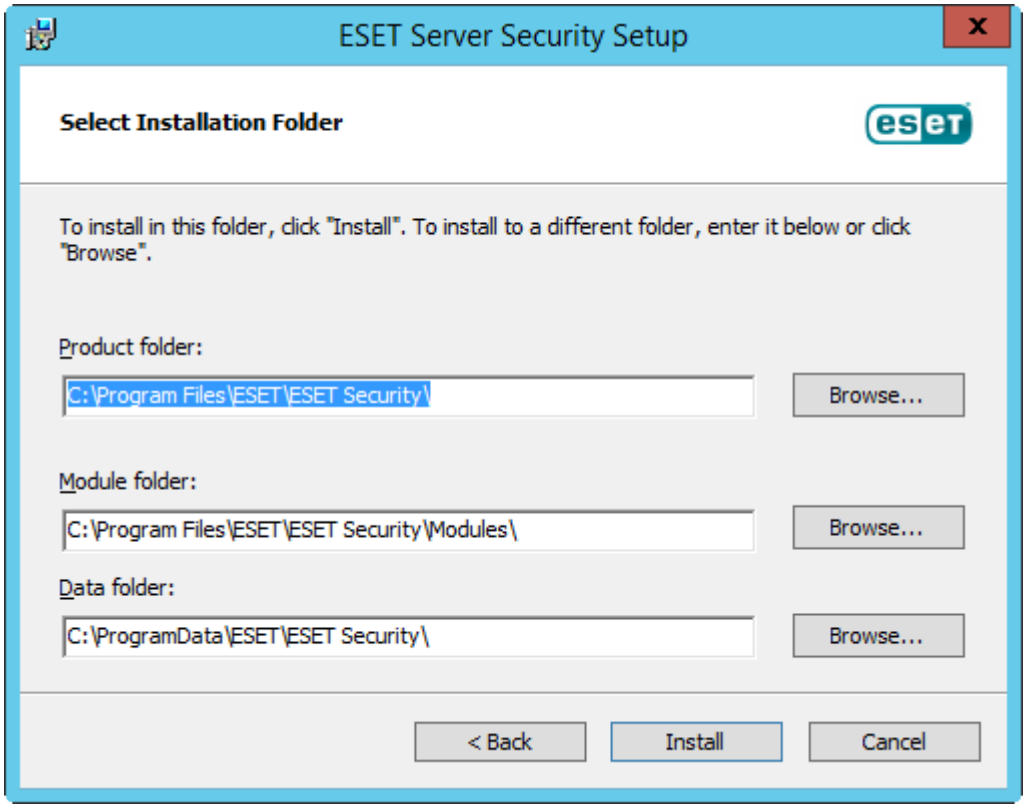
ÖRNEK
Çekirdek yüklemeyi komut satırı üzerinden yürütmek için aşağıdaki örnek komutu kullanın:
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base
```

Özel

Sisteminize yüklenecek olan ESET Server Security özelliklerini seçmenize olanak sağlar. Yükleme işlemine başlamadan önce ürün modülleri ve özelliklerinin listesi görüntülenir. ESET Server Security aracını ihtiyacınız olan bileşenlerle özelleştirmek istiyorsanız bu seçenek kullanılır.

NOT
Windows Server 2008 SP1 R2'de **Ağ koruması** bileşeninin yüklemesi varsayılan olarak devre dışı bırakılmıştır (**Standart** yükleme). Bu bileşenin yüklenmesini istiyorsanız, **Özel** yükleme türünü seçin.

5.ESET Server Security aracının yükleneceği konumu seçmeniz istenir. Varsayılan olarak program şu konuma yüklenir: *:\Program Files\ESET\ESET Server Security*. Bu konumu değiştirmek için **Gözat**'ı tıklayın (önerilmez).

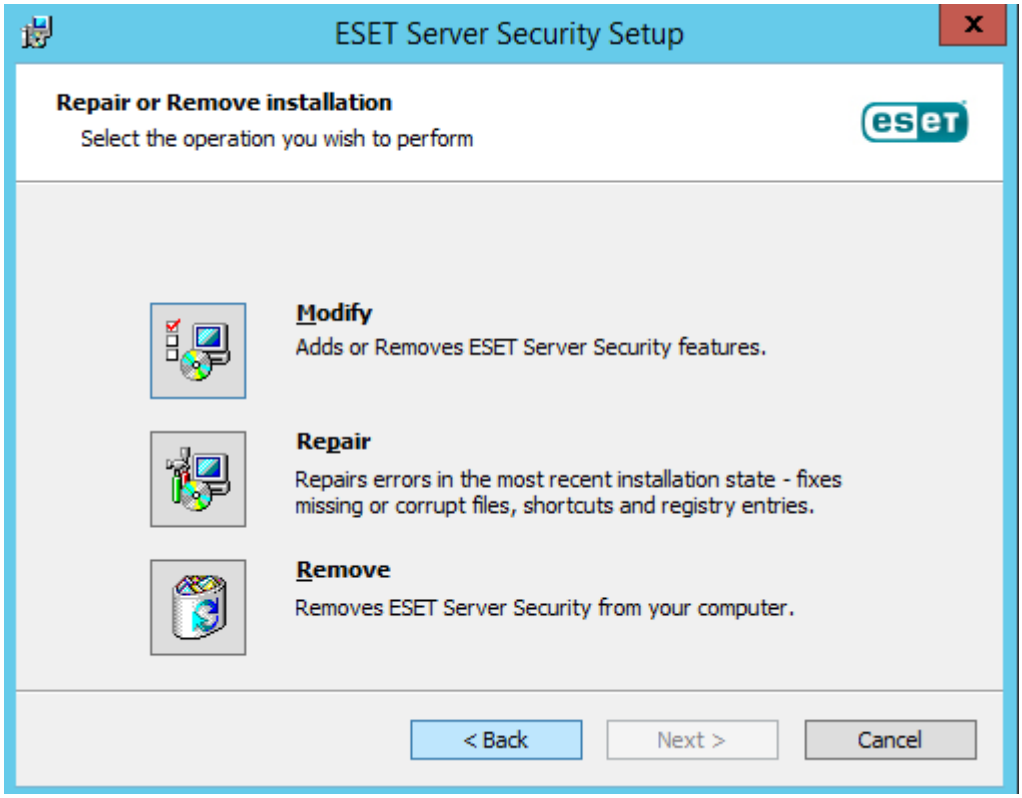


6. Yükleme işlemini başlatmak için **Yükle**'yi tıklayın. Yükleme işlemi tamamlandığında, ESET GUI'si başlatılır ve bildirim alanında tepsi simgesi gösterilir (sistem tepsisi).

Mevcut bir yüklemeyi değiştirme

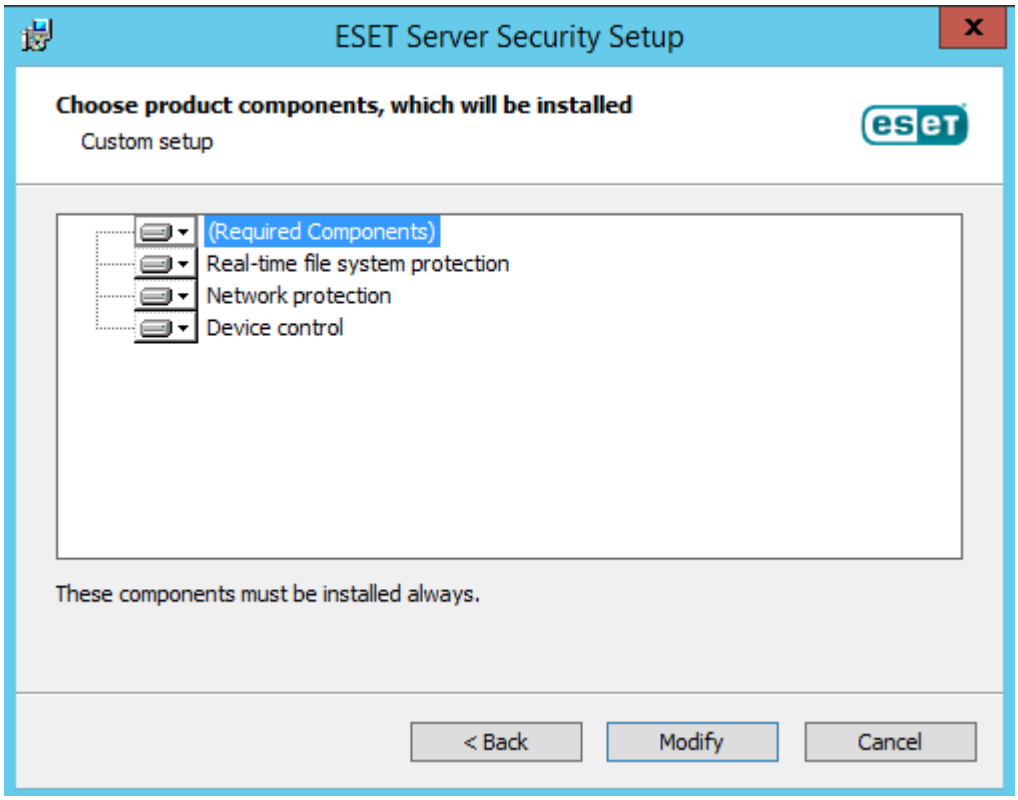
Yüklemenize bileşenler ekleyebilir veya kaldırabilirsiniz. Bunun için, ilk yükleme sırasında kullandığınız `.msi` yükleyici paketini çalıştırın veya **Programlar ve Özellikler**'e gidin (Windows Kontrol Paneli'nden erişilebilir). ESET Server Security ürününü sağ tıklayıp **Değiştir**'i seçin. Bileşenleri eklemek veya kaldırmak için aşağıdaki adımları uygulayın.

Kullanılabilir 3 seçenek vardır: Yüklenen bileşenleri **değiştirebilir**, ESET Server Security yüklemenizi **Onarabilir** veya tamamen **Kaldırabilirsiniz** (yüklemeyi kaldırma).



Değiştir'i seçerseniz, kullanılabilir program bileşenlerinin bir listesi gösterilir.

Eklemek veya kaldırmak istediğiniz bileşenleri seçin. Birden çok bileşeni aynı anda ekleyebilir/kaldırabilirsiniz. Bileşeni tıklayın ve açılır menüden bir seçenek belirleyin:



Seçeneği belirledikten sonra değişiklikleri yapmak için **Değiştir**'i tıklatın.

NOT
Yükleyiciyi çalıştırarak yüklediğiniz bileşenleri dilediğiniz zaman değiştirebilirsiniz. Çoğu bileşen için değişikliği yapmak amacıyla sunucunun yeniden başlatılması gerekmez. GUI yeniden başlatılır ve yalnızca yüklemek için seçtiğiniz bileşenleri görürsünüz. Sunucunun yeniden başlatılmasını gerektiren bileşenler için, Windows Yükleyicisi yeniden başlatmanızı ister. Bunun ardından yeni bileşenler sunucu yeniden online olduğunda kullanılabilir hale gelir.

Sessiz / Katılımsız yükleme

Yüklemeyi komut satırı üzerinden tamamlamak için şu komutu kullanın: `msiexec /i <packagename> /qn /l*xv msi.log`

NOT
Windows Server 2008 R2 SP1'de **Ağ koruması** özelliği yüklenmez.

Yüklemenin başarılı olduğundan emin olmak için veya yüklemede herhangi bir sorun olması halinde, **Uygulama Günlüğünü** kontrol etmek için Windows Olay Görüntüleyicisi'ni kullanın (Kaynak: MsiInstaller'dan gelen kayıtları arayın).

ÖRNEK
64 bit sistemde **tam yükleme**:

```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Yükleme işlemi tamamlandığında, ESET GUI'si başlatılır ve bildirim alanında (sistem tepsisi) tepsi simgesi gösterilir.

ÖRNEK
Ürünü **belirtilen dilde** (Almanca) yükleme:

```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```

Daha fazla ayrıntı ve dil kodu listesi için Komut satırı yüklemesindeki **Dil parametrelerine** bakın.

ÖNEMLİ
`REINSTALL` parametresi için değer belirtirken, `ADDLOCAL` veya `REMOVE` parametresi için değer olarak kullanılmayan diğer özellikleri listelemelisiniz. Komut satırı yüklemesinin düzgün çalışması için `REINSTALL`, `ADDLOCAL` ve `REMOVE` parametreleri için değer olarak tüm özellikleri listelemeniz gerekir. `REINSTALL` parametresini kullanıyorsanız ekleme veya çıkarma işlemleri başarılı olmayabilir.
Özelliklerin tam listesi için Komut satırı yüklemesi bölümüne bakın.

ÖRNEK
64 bit sistemde **tam kaldırma** (yüklemeyi kaldırma):

```
msiexec /x efsw_nt64.msi /qn /l*xv msi.log
```

NOT
Sunucunuz başarılı kaldırma işleminin ardından otomatik olarak yeniden başlatılır.

Komut satırı yüklemesi

Aşağıdaki ayarlar, kullanıcı arayüzünün **sadece indirgenmiş**, **temel** ve **hiçbiri** düzeyinde kullanımı içindir. İlgili komut satırı geçişleri için kullanılan **msiexec** sürümü hakkındaki belgelere bakın.

Desteklenen parametreler:

APPDIR=<path>

- yol - Geçerli dizin yolu
- Uygulama yükleme dizini
- Örneğin: `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- yol - Geçerli dizin yolu
- Uygulama Verileri yükleme dizini

MODULEDIR=<path>

- yol - Geçerli dizin yolu
- Modül yüklemesi dizini

ADDLOCAL=<list>

- Bileşen yüklemesi - yerel olarak yüklenecek zorunlu olmayan özelliklerin listesi.
- ESET `.msi` paketleriyle birlikte kullanım: `efsw_nt64.msi /qn ADDLOCAL=<list>`
- `ADDLOCAL` Özelliği hakkında daha fazla bilgi için bkz. https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- `ADDLOCAL` listesi yüklenecek tüm özellik adlarının virgülle ayrılmış olarak yer aldığı bir listedir.
- Yüklemek üzere bir özellik seçerken tam yol (tüm üst özellikler) listeye açıkça eklenmelidir.

REMOVE=<list>

- Bileşen yüklemesi - yerel olarak yüklenmesini istemediğiniz üst özellik.
- ESET `.msi` paketleriyle birlikte kullanım: `efsw_nt64.msi /qn REMOVE=<list>`
- `REMOVE` Özelliği hakkında daha fazla bilgi için bkz. https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove
- `REMOVE` listesi yüklenmeyecek olan (veya mevcut yüklemeleri varsa kaldırılacak olan) tüm üst özellik adlarının virgülle ayrılmış olarak yer aldığı bir listedir.
- Üst özelliği belirtmek yeterlidir. Her alt özelliğin listeye açıkça eklenmesine gerek yoktur.

ADDEXCLUDE=<list>

- `ADDEXCLUDE` listesi, yüklenmeyecek tüm özellik adlarının virgülle ayrılmış bir listedir.
- Yüklenmeyecek bir özelliği seçerken, yolun tamamı (tüm alt özellikleriyle birlikte) ve ilgili görünmez özellikleri listeye açıkça eklenmelidir.
- ESET `.msi` paketleriyle birlikte kullanım: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

> NOT
> `ADDEXCLUDE`, `ADDLOCAL` ile birlikte kullanılamaz.

Özellik Yapısı

- **Zorunlu** - Özellik her zaman yüklenir.
- **İsteğe Bağlı** - Özellik yükleme için devre dışı bırakılabilir.
- **Görünmez** - Diğer özelliklerin düzgün çalışması için zorunlu olan mantıksal özellik.

ESET Server Security özelliklerinin listesi:

> ÖNEMLİ
> Tüm özelliklerin adları büyük/küçük harf duyarlıdır, örneğin `RealtimeProtection`, `REALTIMEPROTECTION` ile aynı değildir.

Özellik Adı	Özellik Yapısı
`SERVER`	Zorunlu
`RealtimeProtection`	Zorunlu
`WMIProvider`	Zorunlu
`HIPS`	Zorunlu
`Updater`	Zorunlu
`eShell`	Zorunlu
`UpdateMirror`	Zorunlu
`DeviceControl`	İsteğe Bağlı
`DocumentProtection`	İsteğe Bağlı
`WebAndEmail`	İsteğe Bağlı
`ProtocolFiltering`	Görünmez
`NetworkProtection`	İsteğe bağlı
`IdsAndBotnetProtection`	İsteğe bağlı
`Rmm`	İsteğe bağlı
`WebAccessProtection`	İsteğe Bağlı
`EmailClientProtection`	İsteğe Bağlı
`MailPlugins`	Görünmez
`Cluster`	İsteğe bağlı
`_Base`	Zorunlu
`eula`	Zorunlu
`ShellExt`	İsteğe Bağlı
`_FeaturesCore`	Zorunlu
`GraphicUserInterface`	İsteğe Bağlı
`SysInspector`	İsteğe Bağlı
`SysRescue`	İsteğe bağlı
`EnterpriseInspector`	İsteğe bağlı

Aşağıdaki özelliklerden herhangi birini kaldırmak istiyorsanız, gruba ait olan her özelliği belirterek grubun tamamını kaldırmanız gerekir. Aksi halde, özellik kaldırılamaz. Burada iki grup yer almaktadır (her satır bir grubu temsil eder):

`GraphicUserInterface,ShellExt`

`NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection`

ÖRNEK
Ağ Koruması bölümünü (alt özellikler dahil olmak üzere) `REMOVE` parametresini kullanarak ve yalnızca üst özelliği belirterek hariç tutun:
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```
Alternatif olarak, `ADDEXCLUDE` parametresini kullanabilirsiniz, ancak tüm alt özellikleri de belirtmeniz gerekir:
```
msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

ÖRNEK
Core yükleme örneği:
```
msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

ESET Server Security ürününün yüklemeden sonra otomatik olarak yapılandırılmasını istiyorsanız, yükleme komutu içerisinde temel yapılandırma parametrelerini belirtebilirsiniz.

ÖRNEK
ESET Server Security aracını yükleyip ESET LiveGrid® aracını devre dışı bırakın:
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

Tüm yapılandırma özelliklerinin listesi:

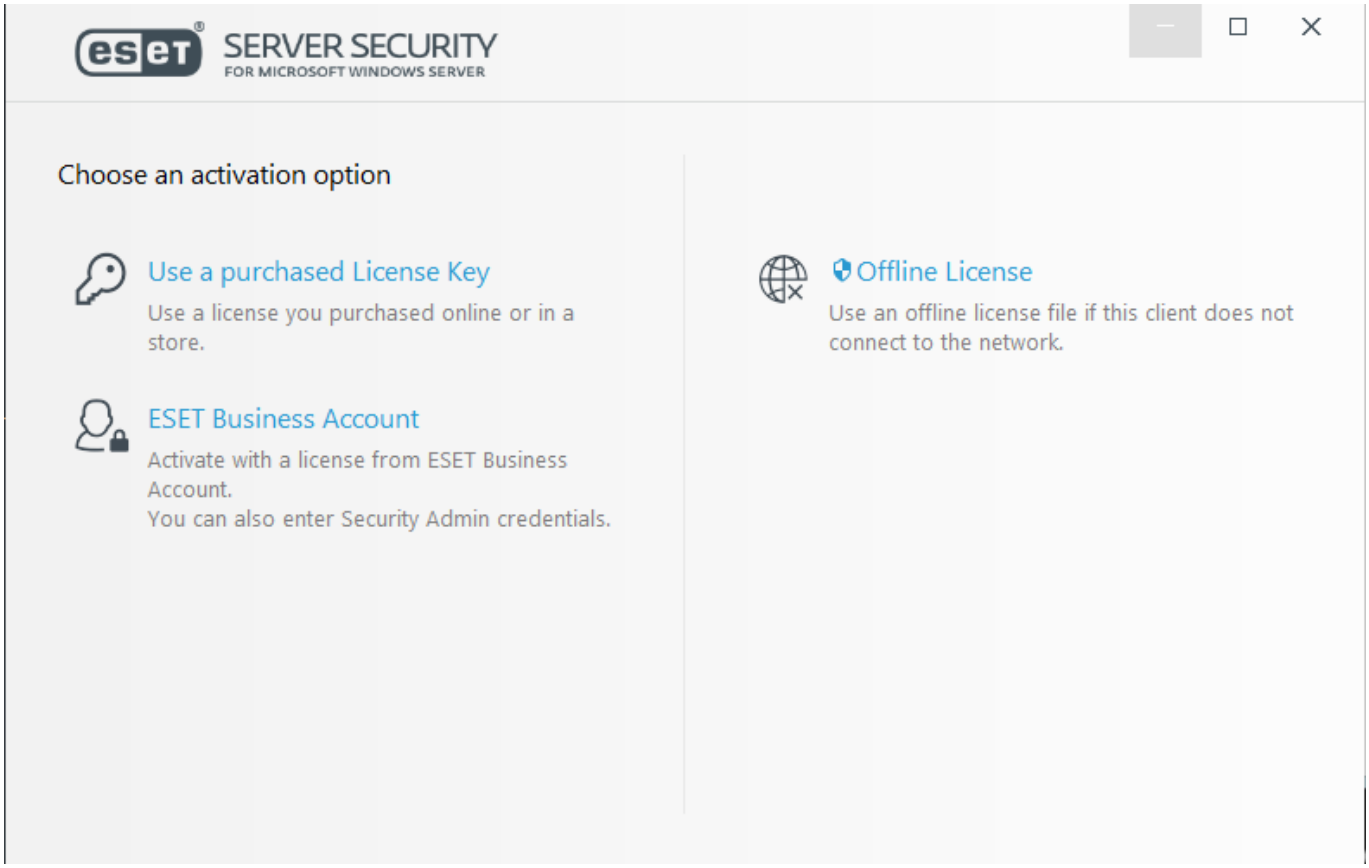
Değiştir	Değer
`CFG_POTENTIALLYUNWANTED_ENABLED=1/0`	0 - Devre dışı, 1 - Etkin
`CFG_LIVEGRID_ENABLED=1/0`	0 - Devre dışı, 1 - Etkin
`FIRSTSCAN_ENABLE=1/0`	0 - Devre dışı, 1 - Etkin
`CFG_PROXY_ENABLED=0/1`	0 - Devre dışı, 1 - Etkin
`CFG_PROXY_ADDRESS=<ip>`	Proxy IP adresi
`CFG_PROXY_PORT=<port>`	Proxy bağlantı noktası numarası
`CFG_PROXY_USERNAME=<user>`	Kimlik doğrulama için kullanıcı adı
`CFG_PROXY_PASSWORD=<pass>`	Kimlik doğrulama için parola

Dil parametreleri: Ürün dili (her iki parametreyi de belirtmelisiniz)

Değiştir	Değer
`PRODUCT_LANG=`	LCID Ondalığı (Yerel Kimlik), örneğin `1033` (*English - United States* için), bkz. dil kodu listesi.
`PRODUCT_LANG_CODE=`	LCID Dizesi (Dil Kültürü Adı) küçük harfli, örneğin `en-us` (*English - United States* için), bkz. dil kodu listesi.

Ürün etkinleştirme

Yükleme tamamlandıktan sonra ürününüzü etkinleştirmeniz istenir.



ESET Server Security ürününü etkinleştirmek için aşağıdaki yöntemlerden herhangi birini kullanabilirsiniz:

Lisans Anahtarını Girin

Lisans sahibinin tanımlanması ve lisans etkinleştirmesi için kullanılan XXXX-XXXX-XXXX-XXXX-XXXX biçiminde benzersiz bir dizidir.

ESET Business Account

Kayıt işlemini yapmışsanız ve ESET Business Account (EBA) (ESET Server Security lisansının içe aktarıldığı) hesabınız varsa bu seçeneği kullanın. Ayrıca ESET License Administrator portalında kullandığınız **Güvenlik Yöneticisi** kimlik bilgilerinizi de girebilirsiniz.

Çevrimdışı Lisans dosyası

Lisans bilgilerini sağlamak için ESET ürününe aktarılacak olan, otomatik olarak oluşturulmuş bir dosya. Çevrimdışı Lisans dosyanız lisans portalında oluşturulur ve uygulamanın lisans yetkilisine bağlanamadığı ortamlarda kullanılır.

Bilgisayarınız yönetilen bir ağın üyesiyse ESET PROTECT ile **Daha sonra etkinleştir** seçeneğini tıklayın. Yöneticiniz ESET PROTECT üzerinden uzaktan etkinleştirme işlemini gerçekleştirir. Ayrıca bu seçeneği, bu istemciyi daha sonra etkinleştirmek istediğiniz durumlarda da kullanabilirsiniz.

Dilediğiniz zaman lisans bilgilerinizi yönetmek için ana program penceresinde **Yardım ve destek** > **Lisansı yönet**'i seçin. ESET ürününüzü tanıtmak ve lisans tanıtımı için kullanılan genel lisans kimliğinizi görürsünüz. Bilgisayarınızın kayıtlı olduğu Kullanıcı Adınız Hakkında bölümünde saklanır; bu bölümü sistem tepsisi simgesini sağ tıklatarak görüntüleyebilirsiniz.

ESET Server Security ürününü başarılı bir şekilde etkinleştirmenizin ardından ana program penceresi açılır ve

İzleme sayfasında geçerli durumunuz gösterilir. İlk başta biraz ilgi göstermeniz gerekebilir, örneğin, ESET LiveGrid® ürününün parçası olmak isteyip istemediğiniz sorulur.

Ayrıca ana program penceresinde sistem güncellemeleri (Windows Update) veya tespit altyapısı güncellemeleri gibi diğer öğelerle ilgili bildirimler de gösterilir. İlgi göstermeniz gereken tüm hususlar çözümlendikten sonra izleme penceresi yeşil renge döner ve **Korunuyorsunuz** durumu görüntülenir.

Ayrıca ürününüzü ana menüden **Yardım ve destek** > **Ürünü etkinleştir** veya **İzleme** durumu > **Ürün etkinleştirilmedi** alanından da etkinleştirebilirsiniz.

> NOT
> ESET PROTECT yönetici tarafından kullanılabilir duruma getirilen lisansları kullanan istemci bilgisayarları gizlice etkinleştirebilir.

ESET Business Account

ESET Business Account birden çok lisansı yönetmenize olanak tanır. ESET Business Account uygulamanız yoksa **Hesap oluştur** seçeneğini tıklayın. Kaydolabileceğiniz ESET Business Account portalına yönlendirilirsiniz.

> NOT
> Daha fazla bilgi için ESET Business Account (EBA) Kullanıcı Kılavuzu'na bakın.

Güvenlik Yöneticisi kimlik bilgilerinizi kullanıyorsanız ve parolanızı unuttuysanız **Parolamı unuttum** seçeneğini tıkladığınızda, ESET License Administrator portalına yönlendirilirsiniz. E-posta adresinizi girin ve onaylamak için **Gönder** seçeneğine tıklayın. Bunu yaptığınızda, parolanızı sıfırlamaya yönelik talimatlar içeren bir ileti alırsınız.

Etkinleştirme başarılı

Etkinleştirme başarılı oldu ve ESET Server Security artık etkin. Bundan sonra ESET Server Security, son tehditleri tespit etmek üzere güncellemeleri düzenli olarak alacak ve bilgisayarınızın güvende olmasını sağlayacak. Ürün etkinleştirmesini sonlandırmak için **Bitti** seçeneğini tıklatın.

Etkinleştirme hatası

ESET Server Security ürünü etkinleştirilemedi. Doğru **Lisans Anahtarını** girdiğinizden veya **Çevrimdışı Lisans** eklediğinizden emin olun. Farklı bir **Çevrimdışı Lisans**'a sahipseniz lütfen bunu tekrar girin. Girdiğiniz lisans anahtarını kontrol etmek için, **Lisans Anahtarını tekrar denetle** öğesini tıklatın veya **farklı bir lisans girin**.

Etkinleştiremiyorsanız etkinleştirme sorun giderme sihirbazına bakın.

Lisans

ESET Server Security için kullanacağınız hesapla ilişkilendirilen bir lisansı seçmeniz istenir. Devam etmek için **Etkinleştir** seçeneğine tıklayın.

Daha yeni sürüme yükseltme

ESET Server Security ürününün yeni sürümleri, iyileştirmeler sağlamak veya program modüllerinin otomatik güncellemeleriyle çözülemeyen sorunları düzeltmek için yayımlanır.

Yükseltme yöntemleri:

- **Yüklemeyi kaldır / Yükle** - Yenisini yüklemeden önce eski sürümü kaldırın. En son ESET Server Security sürümünü indirin. Yapılandırmayı muhafaza etmek istiyorsanız mevcut ESET Server Security ürününüzden ayarları dışa aktarın. ESET Server Security ürününün yüklemesini kaldırın ve sunucuyu yeniden başlatın. İndirdiğiniz yükleyici ile yeni bir yükleme işlemi yapın. Yapılandırmanızı yüklemek için ayarları içe aktarın. ESET Server Security çalıştıran tek bir sunucunuz varsa bu işlemi öneririz.

- **Yerinde** - Mevcut sürümü kaldırmadan yeni sürümün eski ESET Server Security üzerine yüklendiği bir yükseltme yöntemi.

ÖNEMLİ
Sunucunuzda **beklemede Windows Update'leri olmaması** gerekir. Ayrıca Windows Update'lerinden veya başka bir nedenden kaynaklanan **beklemede herhangi bir yeniden başlatma işlemi de olmamalıdır**. Beklemede Windows Updates veya yeniden başlatma işlemi olduğu halde yerinde yükseltme işlemi yapmayı deniyorsanız, mevcut ESET Server Security sürümü düzgün bir şekilde kaldırılamayabilir. Ayrıca sonrasında ESET Server Security sürümünü manuel olarak kaldırmaya karar vermeniz durumunda da sorunlarla karşılaşabilirsiniz.

NOT
ESET Server Security yükseltmesi sırasında sunucunun yeniden başlatılması gerekecektir.

- Uzaktan - ESET PROTECT tarafından yönetilen büyük ağ ortamlarında kullanım için. Bu temelde, basit bir yükseltme yöntemidir, ancak uzaktan gerçekleştirilir. ESET Server Security çalıştıran birden çok sunucunuz varsa faydalı olur.

- ESET Küme sihirbazı - Bir yükseltme yöntemi olarak da kullanılabilir. ESET Server Security aracına sahip en az 2 sunucu için bu yöntemi kullanmanızı öneririz. Bu temelde, yerinde bir yükseltme yöntemidir ancak ESET Kümesi üzerinden gerçekleştirilir. Ayrıca yükseltme işlemi tamamlandığında, ESET Kümesi kullanmaya ve özelliklerinden yararlanmaya devam edebilirsiniz.

NOT
ESET Server Security yazılımınızı yükselttikten sonra, doğru bir şekilde ve gereksinimlerinize uygun olarak yapılandırıldığından emin olmak için tüm ayarları gözden geçirmenizi öneririz.

ESET PROTECT üzerinden yükseltme

ESET PROTECT eski bir ESET Server Security sürümü çalıştıran birden çok sunucuyu yükseltmenize olanak sağlar. Bu yöntem, aynı anda çok sayıda sunucuyu yükseltme avantajı sunar ve her bir ESET Server Security aracının aynı şekilde yapılandırılmasını sağlar (istenirse).

İşlem şu aşamalardan oluşmaktadır:

- **Birinci sunucuyu yükseltin** - Bu işlemi en son ESET Server Security sürümünü mevcut sürümünüz üzerine yükleyerek manuel olarak yapın, böylece kurallar, çeşitli beyaz ve kara listeler dahil yapılandırmanın tamamı

korunur. Bu aşama ESET Server Security çalıştıran sunucuda yerel olarak gerçekleştirilir.

- **7.x sürümüne yeni yükseltilen ESET Server Security aracının yapılandırmasını** isteyin ve ESET PROTECT aracında **İlkeye dönüştürün**. İlke daha sonra yükseltilen tüm sunuculara uygulanır. Bu aşama aşağıdaki aşamalarla birlikte ESET PROTECT kullanılarak uzaktan gerçekleştirilir.

- Eski ESET Server Security sürümünü çalıştıran tüm sunucularda **Yazılım Kaldırma görevini çalıştırın**.

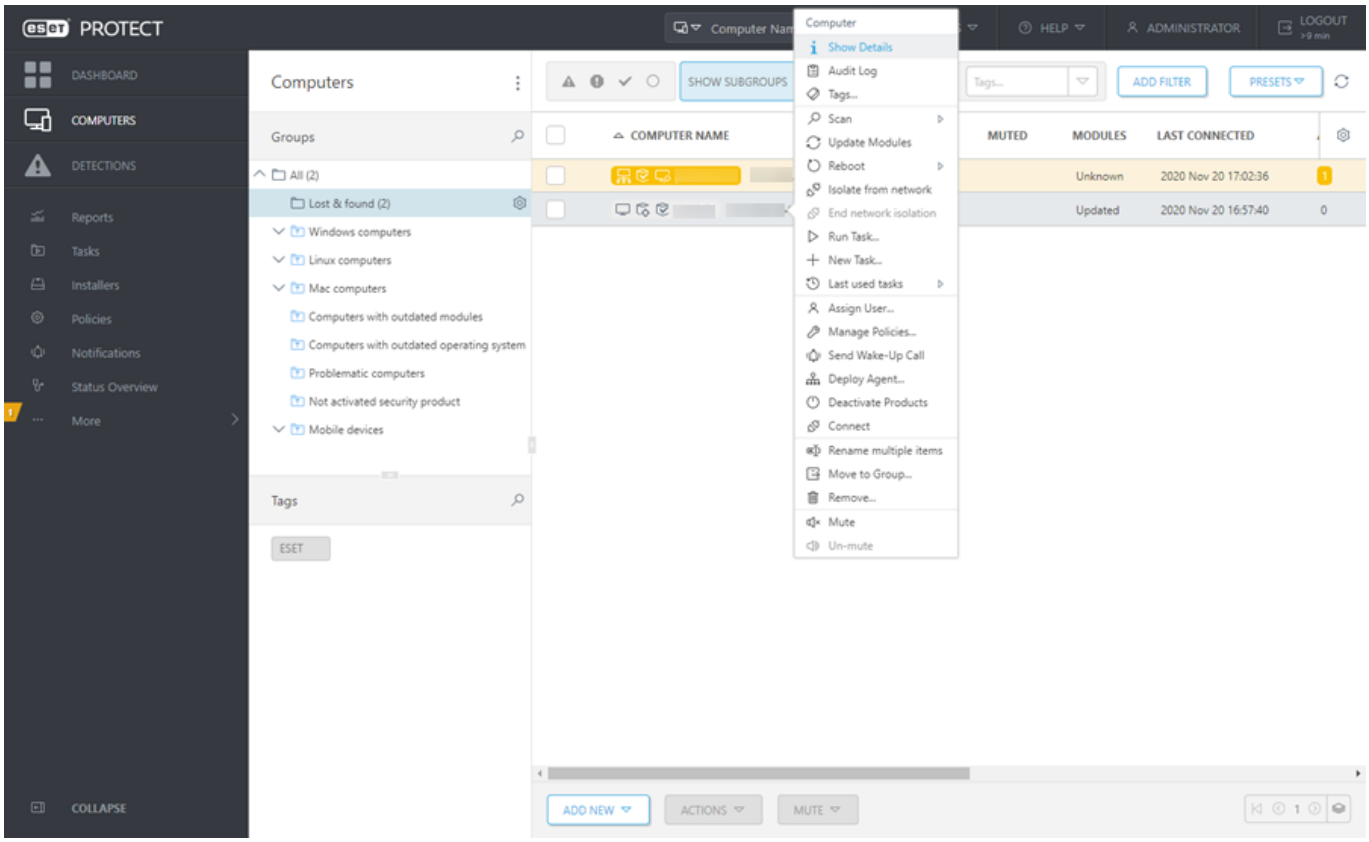
- En son ESET Server Security sürümünün çalışmasını istediğiniz tüm sunucularda **Yazılım Yükleme görevini çalıştırın**.

- En son ESET Server Security sürümünü çalıştıran tüm sunuculara **Yapılandırma ilkesini atayın**.

Adım adım işlem:

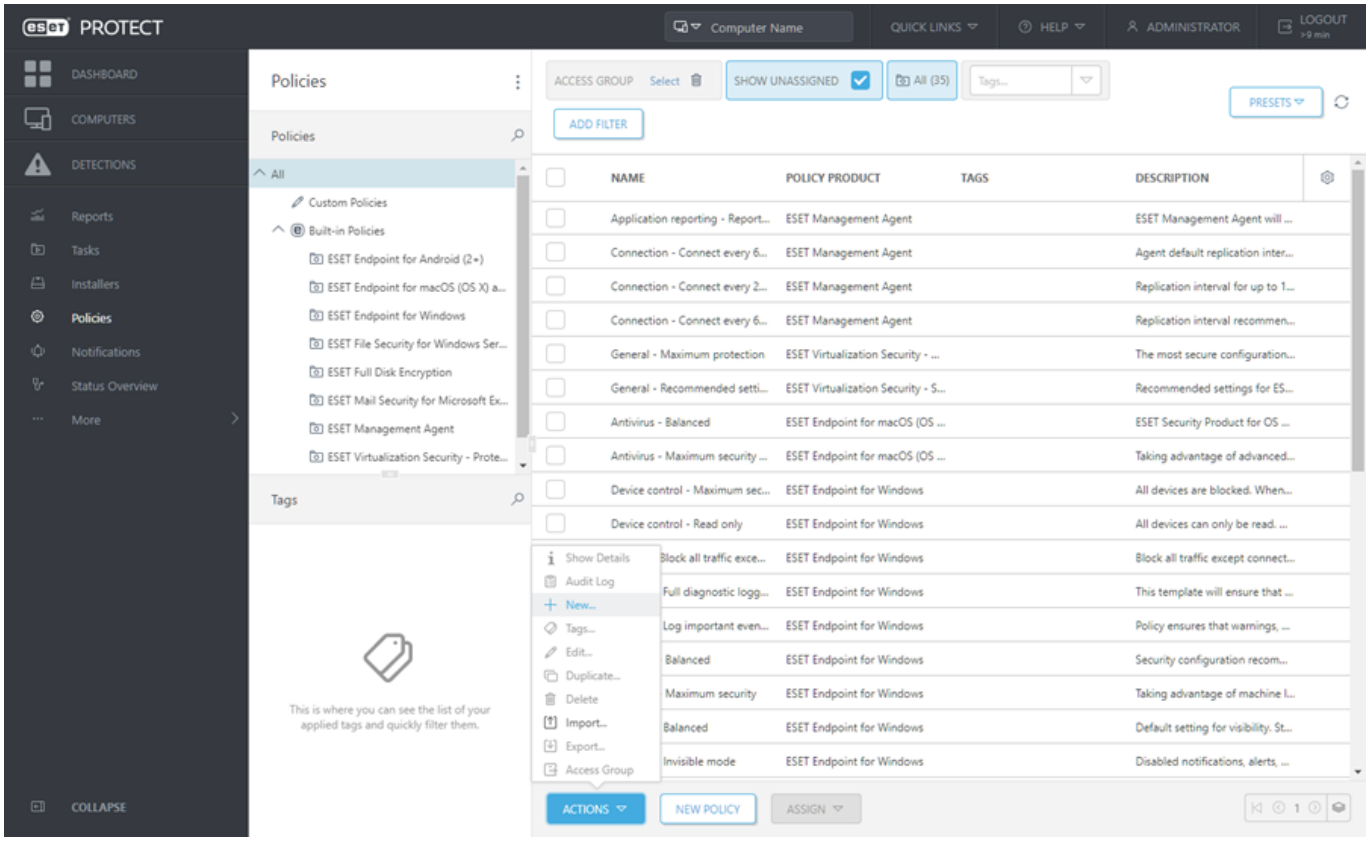
1. ESET Server Security çalıştıran sunuculardan birine giriş yapın ve en son sürümü indirdikten sonra mevcut sürümünüz üzerine yükleyerek yükseltin. Normal yükleme için adımları uygulayın. Eski ESET Server Security sürümünüzün ilk yapılandırmasının tamamı yükleme işlemi esnasında korunur.

2. **ESET PROTECTWeb Console**'nu açın, Statik veya Dinamik gruptan bir istemci bilgisayar seçin ve **Detayları Göster**'i tıklatın.



3. Yapılandırma sekmesine gidin ve yönetilen ürünün tüm yapılandırmasını toplamak için **Yapılandırmayı iste** düğmesini tıklatın. Yapılandırmayı almak için biraz bekleyin. En son yapılandırma listede göründüğünde, **Güvenlik ürününü** tıklatıp **Yapılandırmayı aç**'ı seçin.

4. **İlkeye dönüştür** düğmesini tıklatarak yapılandırma ilkesini oluşturun. Yeni ilke için **Ad** girin ve **Bitir**'i tıklatın.



5. **İstemci Görevleri** öğesine gidip Yazılım Kaldırma görevini seçin. Yükleme kaldırma görevini oluştururken, **Gerektiğinde otomatik olarak yeniden başlat** seçeneğinin onay kutusunu işaretleyerek kaldırma işleminin ardından sunucuyu yeniden başlatmanızı öneririz. Görev oluşturulduktan sonra, yükleme kaldırma işlemi için istenen tüm hedef bilgisayarları seçin.

6. ESET Server Security aracının tüm hedeflerden kaldırıldığından emin olun.

7. En son ESET Server Security sürümünün istenen tüm hedeflere yüklenmesi için Yazılım Yükleme görevi oluşturun.

8. ESET Server Security çalıştıran tüm sunuculara (ideal olarak bir gruba) **Yapılandırma ilkesini atayın**.

ESET Cluster üzerinden yükseltme

ESET Cluster oluşturmak, ESET Server Security eski sürümüne sahip birden çok sunucuyu yükseltmenize olanak sağlar. ESET PROTECT yükseltme işleminin alternatifidir. Ortamınızda ESET Server Security aracına sahip en az iki sunucunuz varsa ESET Cluster yöntemini kullanmanızı öneririz. Bu yükseltme işleminin başka bir faydası, ESET Cluster kullanmaya devam edebilmenizdir. ESET Server Security yapılandırması tüm üye düğümlerde senkronize edilir.

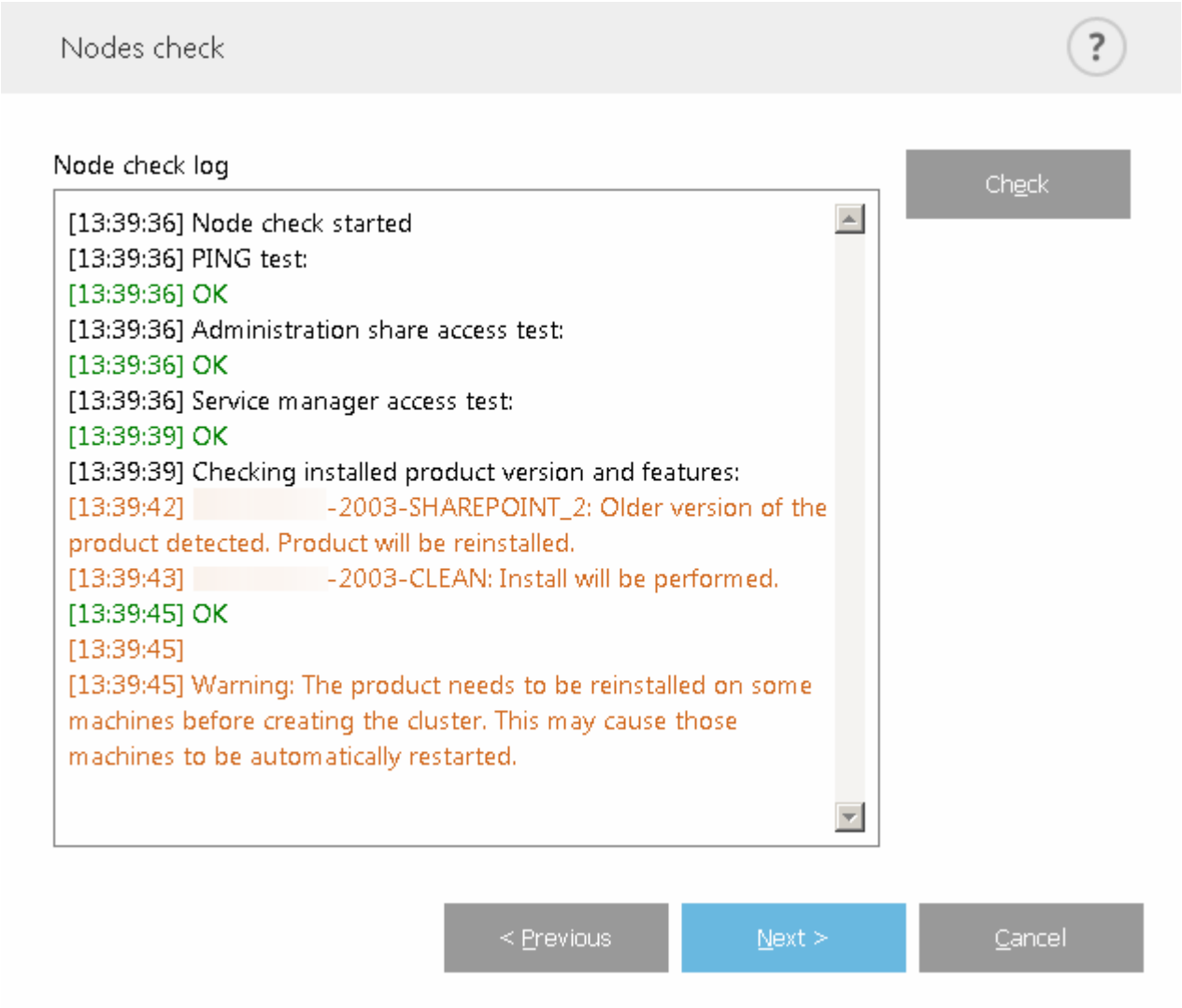
Bu yöntemi kullanarak yükseltmek için aşağıdaki adımları uygulayın:

1. ESET Server Security çalıştıran sunuculardan birine giriş yapın ve en son sürümü indirdikten sonra mevcut sürümünüz üzerine yükleyerek yükseltin. Normal yükleme için adımları uygulayın. Eski ESET Server Security sürümünüzün ilk yapılandırmasının tamamı yükleme işlemi esnasında korunur.

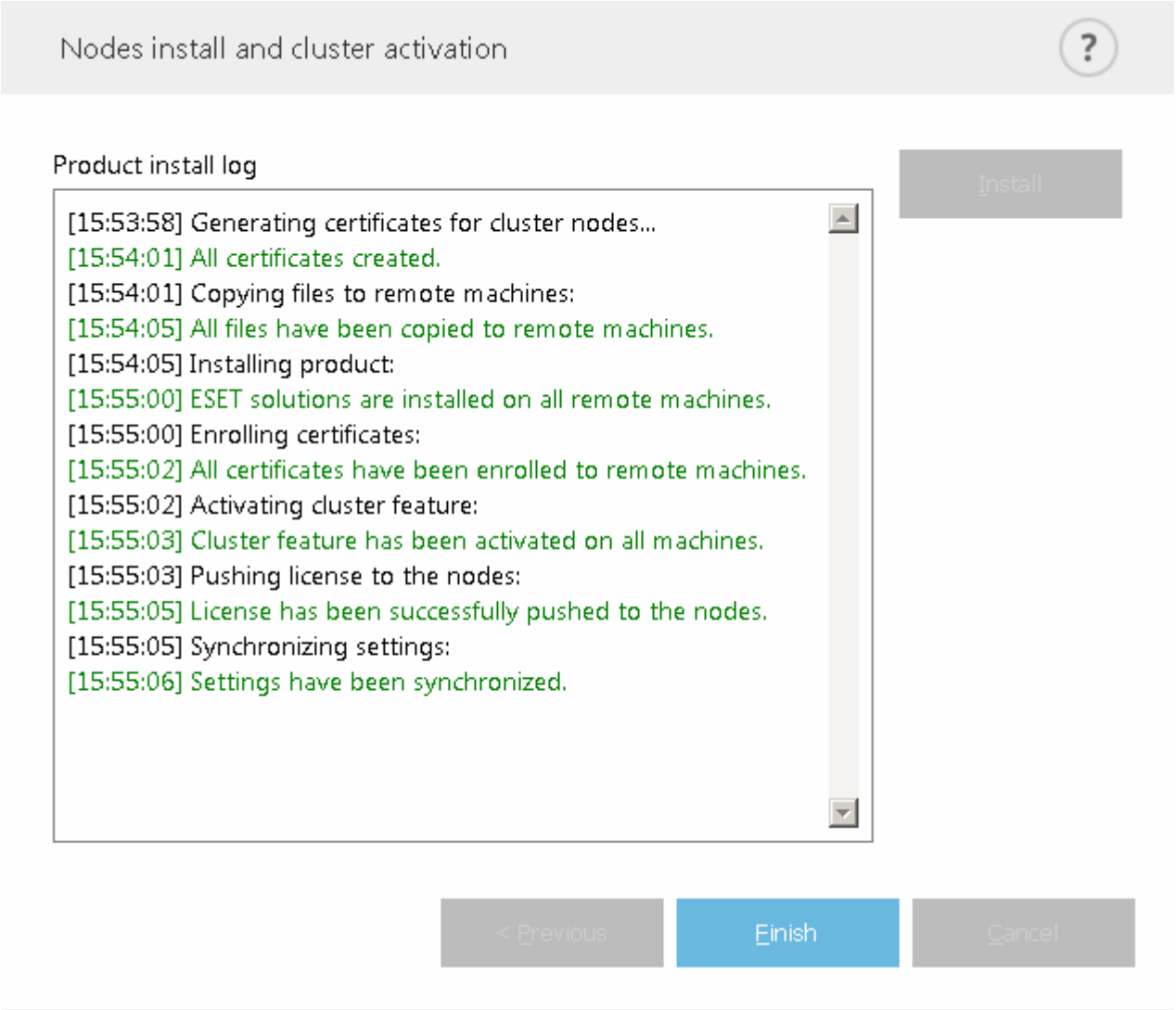
2. ESET Cluster sihirbazını çalıştırın ve küme düğümlerini (ESET Server Security yazılımını yükseltmek istediğiniz sunucuları) ekleyin. Gerekirse, henüz ESET Server Security çalıştırmayan diğer sunucuları ekleyebilirsiniz (bu sunucular üzerinde bir yükleme işlemi gerçekleştirilir). Küme adı ve yükleme türünü

belirtirken varsayılan ayarları olduğu gibi bırakmanızı öneririz (**Etkinleştirilen ürünü olmayan düğümlere lisansı gönder** seçeneği mutlaka işaretli olmalıdır).

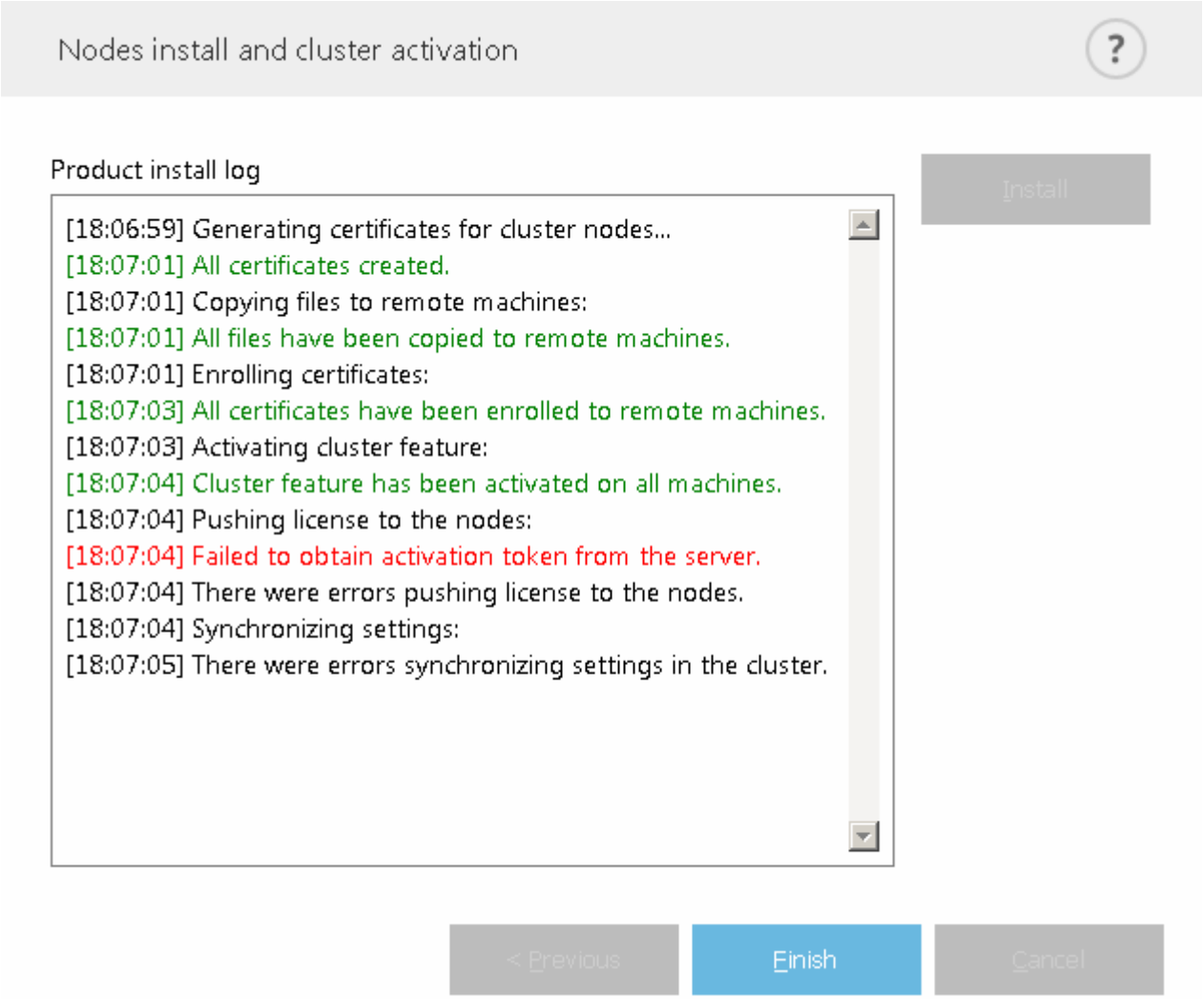
3.**Düğüm denetim günlüğü** ekranını inceleyin. Eski ürün sürümlerine sahip sunucuları listeler ve ürünün yeniden yükleneceğini gösterir. ESET Server Security halihazırda yüklenmediği diğer tüm sunuculara da yüklenecektir.



4.**Düğümlerin yüklenmesi ve küme etkinleştirmesi** ekranında, yükleme ilerlemesi gösterilir. Yükleme başarıyla tamamlandığında, şunlara benzer sonuçlarla sona erer:



Ağınız veya DNS doğru bir şekilde yapılandırılmamışsa, **Sunucudan etkinleştirme belirteci alınamadı** şeklinde bir hata mesajı alabilirsiniz. ESET Cluster sihirbazını yeniden çalıştırmayı deneyin. Kümeyi yok eder ve yeni bir küme oluşturur (ürünü yeniden yüklemeden); etkinleştirme işlemi bu kez başarıyla tamamlanmalıdır. Sorun devam ederse, ağınızı ve DNS ayarlarınızı kontrol edin.



Küme ortamında yükleme

ESET Server Security Aracını bir küme ortamına dağıtabilirsiniz (örneğin yük devri kümesi). ESET Server Security aracını etkin bir düğüme yüklemenizi, ardından ESET Server Security aracının ESET Cluster özelliğini kullanarak yüklemeyi pasif düğümlere yeniden dağıtmanızı öneririz. Yüklemeden ayrı olarak ESET Cluster, doğru bir çalışma için gereken küme düğümleri arasında tutarlılığı sağlamak için ESET Server Security yapılandırmasının bir çoğaltması olarak işlev görür.

Terminal sunucu

ESET Server Security ürününü Terminal Sunucu olarak işlev gören bir Windows Server'a yüklüyorsanız, bir kullanıcının her oturum açışında başlatılmasını önlemek için ESET Server Security GUI'sini devre dışı bırakmayı düşünebilirsiniz. GUI'yi devre dışı bırakmak için spesifik adımları görmek üzere Terminal Sunucuda GUI'yi devre dışı bırakma bölümüne bakın.

Başlarken

Aşağıdaki bölüm ESET Server Security kullanmaya başlamanıza yardımcı olacaktır.

İzleme

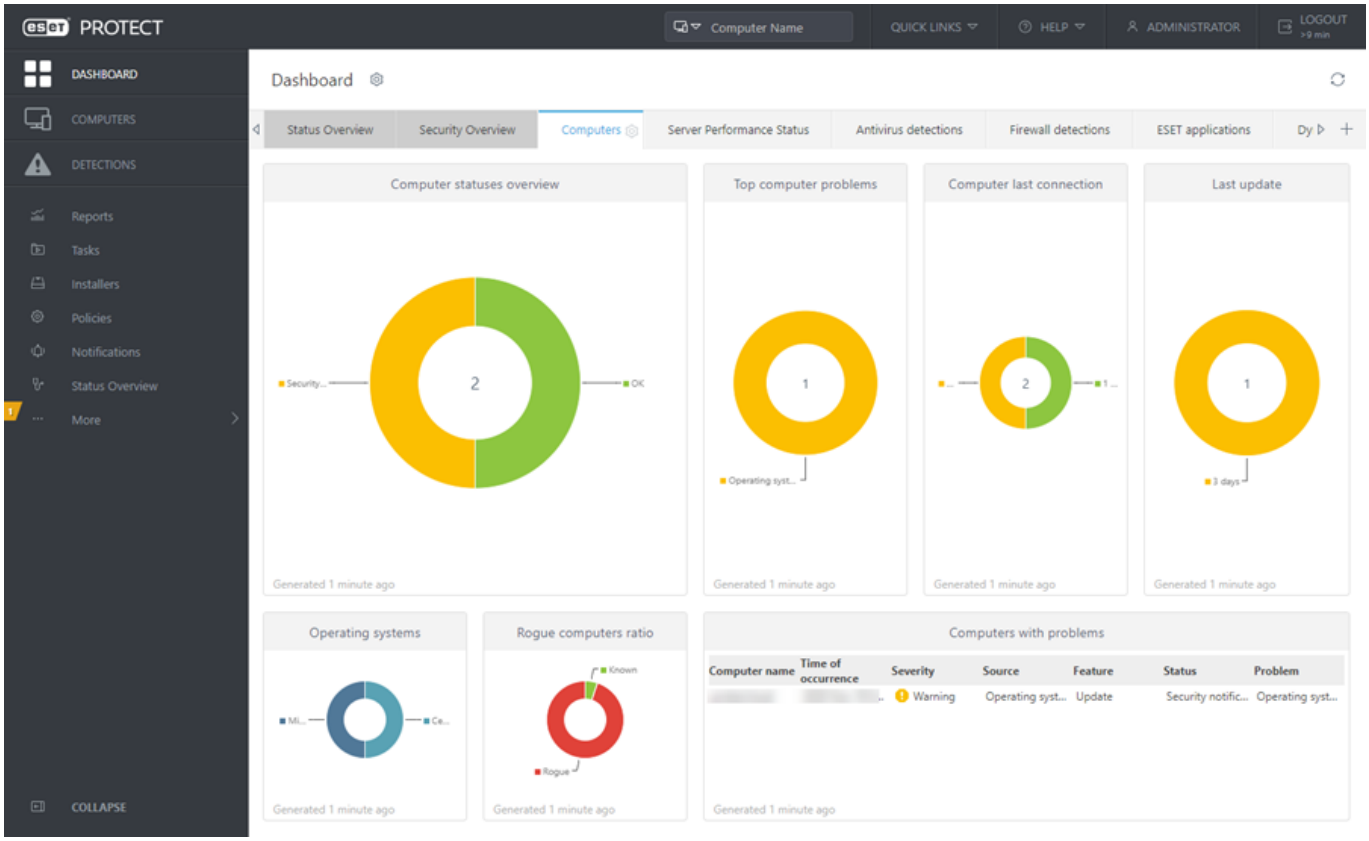
ESET Server Security ürününün mevcut durumuna hızlı bir genel bakış sunar. Dikkat etmenizi gerektiren herhangi bir sorun olup olmadığını hemen görebilirsiniz.

ESET PROTECT Üzerinden yönetilir

ESET PROTECT kullanarak ESET Server Security ürününü uzaktan yönetebilirsiniz.

ESET PROTECT Üzerinden yönetilir

ESET PROTECT ağa bağlı ortamdaki ESET ürünlerini tek bir merkezi konumdan yönetmenize olanak tanıyan bir uygulamadır. ESET PROTECT görev yönetimi sistemi, ESET güvenlik çözümlerini uzak bilgisayarlara yüklemenize, yeni sorunlara ve tehditlere hızlı bir şekilde yanıt verebilmenize olanak tanır. ESET PROTECT, kötü amaçlı kodlara karşı tek başına koruma sağlamaz, her bir istemcideki ESET güvenlik çözümünün varlığına güvenir. ESET güvenlik çözümleri birden fazla platform türü içeren ağları destekler. Ağınız mevcut Microsoft, Linux tabanlı, Mac işletim sistemi ve mobil işletim sistemlerinin bir birleşimini içerebilir.



ESET PROTECT hakkında daha fazla bilgi için ESET PROTECT Online yardım bölümüne bakın.

Koruma durumu

İzleme bölümünde gösterilen koruma durumu, bilgisayarınızın mevcut koruma düzeyi ile ilgili size bilgi verir. Birincil pencerede, ESET Server Security ürününün çalışması hakkında bir durum özeti görüntülenir.

Yeşil **Korunuyorsunuz** durumu, maksimum koruma sağlandığını belirtir.

Kırmızı simge ciddi sorunlar olduğunu belirtir; bilgisayarınız için maksimum koruma sağlanamaz. Olası koruma durumlarının bir listesi için Durum bölümüne bakın.

Turuncu simge, ESET ürününüzle ilgili ciddi olmayan bir sorunla ilgilenmeniz gerektiğini ifade eder.

Düzgün çalışan modüller, yeşil onay işaretiyle belirtilir. Tam işlevsel olmayan modüller, kırmızı ünlem işaretiyle veya turuncu bir bildirim simgesiyle gösterilir. Modülle ilgili ek bilgiler pencerenin üst kısmında gösterilir. Ayrıca modülün düzeltilmesi için bir çözüm önerisi de görüntülenir. Tek tek modüllerin durumunu değiştirmek için ana menüden Ayarlar'ı ve ardından istenen modülü tıklatın.

İzleme sayfası sisteminizle ilgili aşağıdaki bilgileri de içerir:

- **Ürün sürümü** - ESET Server Security ürününün sürüm numarası.
- **Sunucu Adı** - Makine ana bilgisayar adı veya FQDN.
- **Sistem** - işletim sistemi ayrıntıları.
- **Bilgisayar** - donanım ayrıntıları.
- **Sunucunun çalışır durumda kalma süresi** - Sistemin ne kadar süre çalıştığını gösterir; esas olarak çalışmama süresinin tam tersidir.

Önerilen çözümleri kullanarak sorunu çözemiyorsanız, yardım dosyalarına erişmek için **Yardım ve destek** öğesini tıklayın veya ESET Bilgi Bankası'nda arama yapın. Daha fazla yardıma ihtiyacınız olursa Destek isteği gönderebilirsiniz. ESET Teknik Desteği sorularınızı hızla yanıtlar ve çözüm yolu bulunmasına yardımcı olur.

Durum

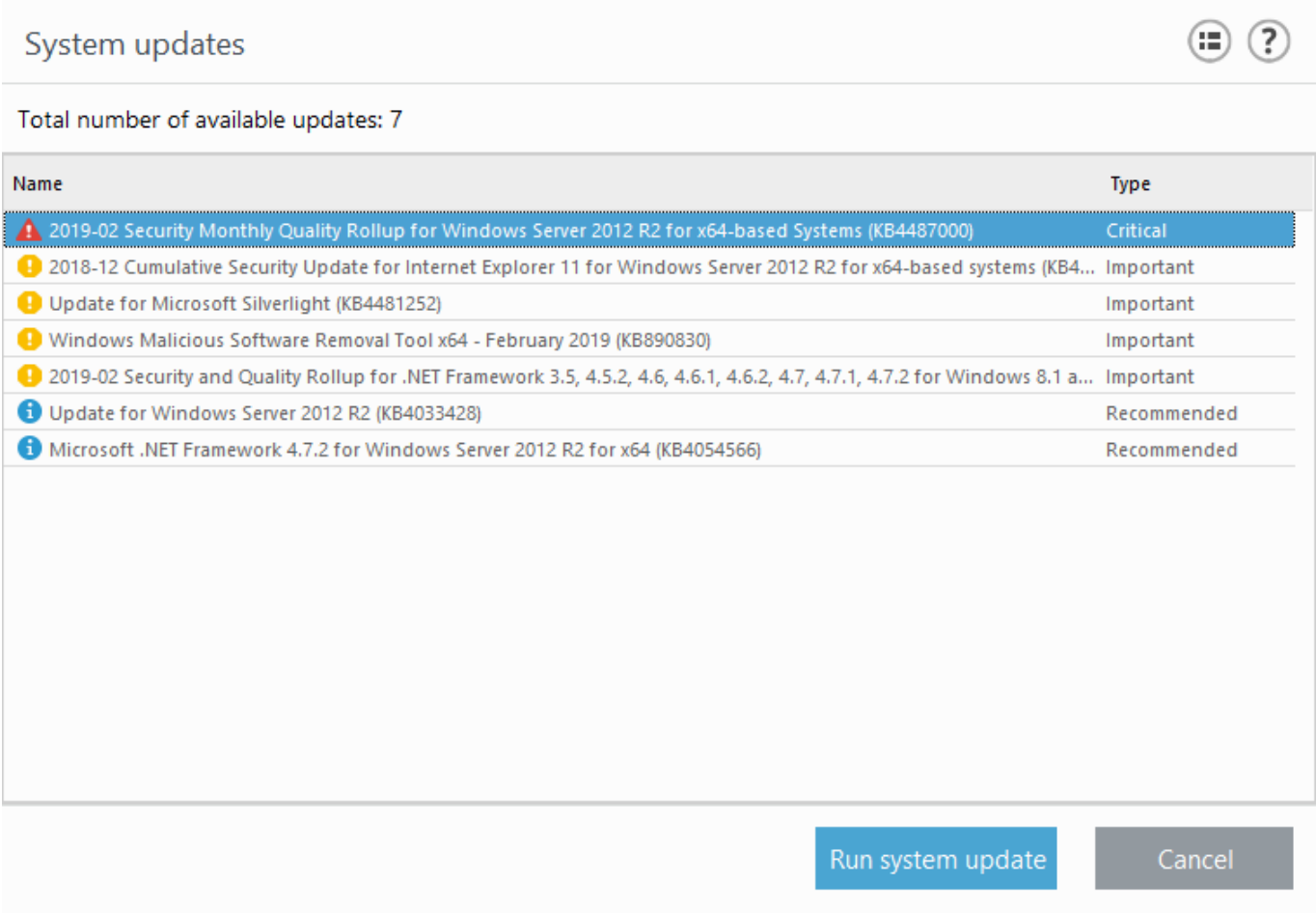
ESET Server Security için bir durum özeti, sisteminizde ilgili ayrıntılı bilgilerle ana pencerede gösterilir. Normalde, her şey sorunsuz bir şekilde çalışırken koruma durumu yeşil renktedir. Ancak belirli durumlarda koruma durumu değişebilir. Aşağıdakilerden biri oluşursa koruma durumu turuncu veya kırmızı uyarı iletisine dönüşür:

Uyarı iletisi	Uyarı iletisi ayrıntıları
İstenmeyen türden olabilecek uygulamanın algılanması yapılandırılmadı	İstenmeyen türden olabilecek uygulama (PUA); reklam yazılımı içeren, araç çubukları yükleyen veya diğer belirsiz nesnelere sahip olan bir programdır. Kullanıcının, tehlikeli türden olabilecek uygulamanın avantajlarının risklerinden daha fazla olduğunu düşündüğü bazı durumlar vardır.
Gerçek zamanlı dosya sistemi koruması duraklatıldı	İzleme sekmesinde **Gerçek zamanlı korumayı etkinleştir** öğesini tıklayın veya ana program penceresinin Ayarlar sekmesinde **Gerçek zamanlı dosya sistemi koruması**'nı yeniden etkinleştirin.
Kimlik avı koruması çalışmıyor	Gerekli olan diğer program modülleri etkin olmadığı için bu özellik çalışmıyor.
ESET LiveGrid® devre dışı	ESET LiveGrid®, **Gelişmiş ayarlar**'da devre dışı bırakıldığında bu sorun ortaya çıkar.
Protokol filtrelemesi devre dışı	Bu özelliği yeniden etkinleştirmek için Protokol filtrelemesini etkinleştir'i tıklayın.
İşletim sistemi güncel değil	Sistem penceresinde, indirilip kurulmaya hazır güncellemelerin listesi gösterilir.
Cihazınız kısa bir süre içinde bağlantıyı kaybedecek	Microsoft Windows sürümünüzü nasıl güncelleyeceğinizle ilgili bilgiler için Seçeneklerinize bakın bağlantısına tıklayın. **Microsoft Windows Server 2008 R2 SP1** veya **Microsoft Windows Small Business Server 2011 SP1** kullanıyorsanız sisteminizin SHA-2 ile uyumlu olduğundan emin olun. Belirli işletim sistemi sürümünüze uygun olan yamaları uygulayın.
Sunum modu etkinleştirildi	Tüm açılır pencereler bastırılır ve zamanlanan görevler duraklatılır.
Ağ saldırısına karşı koruma (IDS) duraklatıldı	Bu özelliği yeniden etkinleştirmek için Ağ saldırısına karşı korumayı etkinleştir (IDS) seçeneğini tıklayın.
Botnet koruması duraklatıldı	Bu özelliği yeniden etkinleştirmek için Botnet korumasını etkinleştir'i tıklayın.
Web erişimi koruması duraklatıldı	İzleme sekmesinde **Web erişimi korumasını etkinleştir** öğesini tıklayın veya ana program penceresinin Ayarlar bölmesinde Web erişimi korumasını yeniden etkinleştirin.
Cihaz Kontrolü duraklatıldı	Bu özelliği yeniden etkinleştirmek için Cihaz Kontrolünü etkinleştir'i tıklayın.
Ürün etkinleştirilmedi veya Lisansın süresi doldu	Bu durum Koruma durumu simgesinin kırmızı renge dönmesiyle belirtilir. Lisans süresi dolduktan sonra program güncellenemez. Lisansınızı yenilemek için uyarı penceresindeki talimatları uygulayın.
Policy ayarlarının geçersiz kılınması aktif	İlke tarafından ayarlanan yapılandırma geçici olarak, muhtemelen sorun giderme işleme tamamlanana dek kullanım dışı kalır. ESET Server Security aracını ESET PROTECT'yi kullanarak yönetiyorsanız ve atanmış bir ilkeniz varsa, hangi özelliklerin ilkeye ait olduğuna bağlı olarak durum bağlantısı kilitlenir (griye döner).
Bilgisayarın yeniden başlatılması gerekiyor	Bu ileti, Program Bileşeni Güncellemeleri (PCU) ve mikro Program Bileşeni Güncellemeleri (µPCU) uygulandıktan sonra görünebilir. PCU ve uPCU ile ilgili ayrıntılar için Güncelleme yapılandırmasına bakın.

Sorunu çözemiyorsanız, ESET Bilgi Bankası'nda arama yapın. Daha fazla yardıma ihtiyacınız olursa Destek isteği gönderebilirsiniz. ESET Teknik Desteği sorularınızı hızla yanıtlar ve çözüm yolu bulunmasına yardımcı olur.

Windows güncellemesi var

Sistem güncellemeleri penceresinde, indirilip yüklenmeye hazır güncellemelerin listesi gösterilir. Güncelle öncelik düzeyi, güncelleme adının yanında gösterilir. Ek bilgi içeren bir açılır pencere görüntülemek için bir güncelleme satırını sağ tıklayıp **Daha fazla bilgi** seçeneğine tıklayın:



Windows Güncellemesi penceresini açmak için **Sistem güncellemesini çalıştır**'ı tıklayın ve sistem güncellemelerine devam edin.

Ağ yalıtımı

ESET Server Security, ağ yalıtımı adı verilen ve sunucunuzun ağ bağlantısını engelleme olanağı tanıyan bir seçenek sunar. Bazı olağandışı senaryolarda, önleyici tedbir amacıyla ağı bir sunucudan yalıtmak isteyebilirsiniz. Örneğin, sunucunun zararlı yazılımdan etkilendiğini veya makinenin başka bir şekilde tehlikeye düştüğünü fark ederseniz.

Ağ yalıtımı etkinleştirildiğinde aşağıdakiler dışında tüm ağ trafiği engellenir:

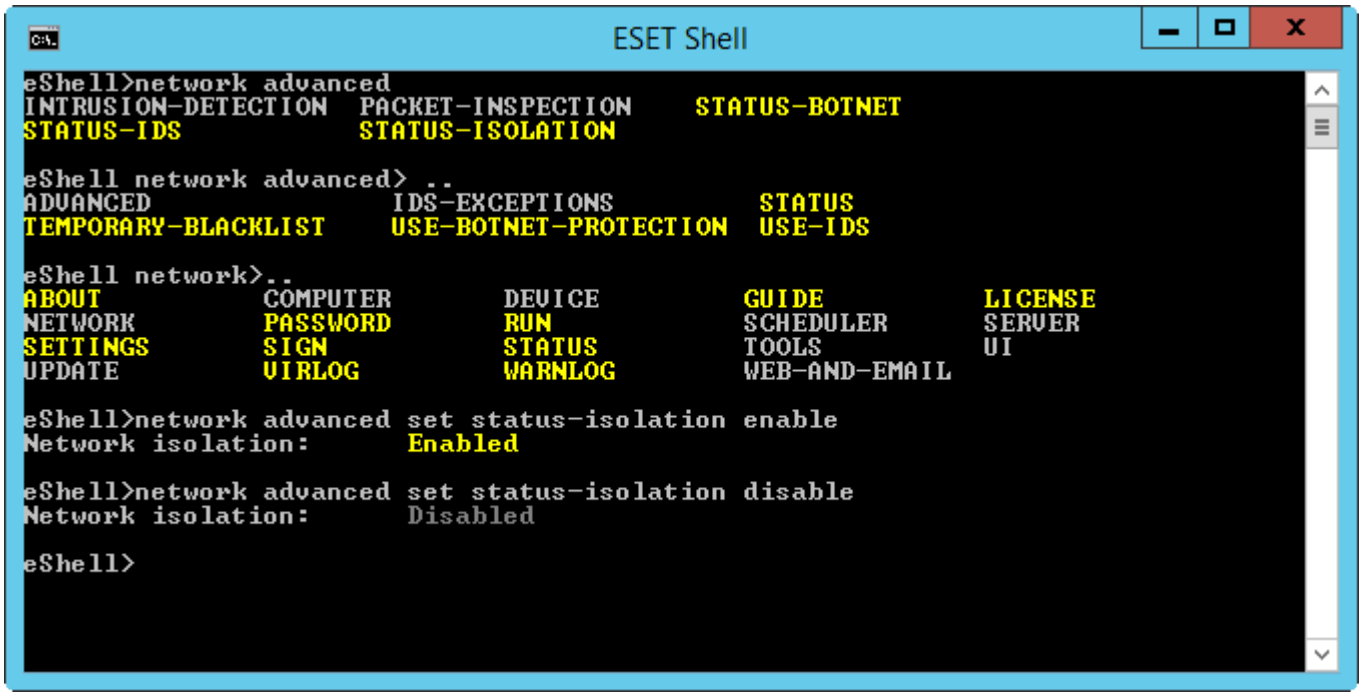
- Etki Alanı Yöneticisi bağlanabilirliği devam eder
- ESET Server Security iletişim kurmaya devam eder
- Varsa ESET Management Agent ve ESET Enterprise Inspector Agent ağ üzerinden iletişim kurabilir

eShell komutu veya ESET PROTECT istemci görevi kullanarak ağ yalıtımını etkinleştirin veya devre dışı bırakın.

eShell

Etkileşimli modda:

- Ağ yalıtımını etkinleştirin: `network advanced set status-isolation enable`
- Ağ yalıtımını devre dışı bırakın: `network advanced set status-isolation disable`



Alternatif olarak Toplu / Komut dosyası modunu kullanarak bir toplu dosya oluşturup çalıştırabilirsiniz.

ESET PROTECT

- Ağ yalıtımını istemci görevi üzerinden etkinleştirin.
- Ağ yalıtımını istemci görevi üzerinden devre dışı bırakın.

Ağ yalıtımı etkinleştirildiğinde ESET Server Security durumu kırmızıya dönüşür ve **Ağ erişimi engellendi** mesajı gösterilir.

Komut için argüman olarak ESET Server Security

Bu bölüm, programın kullanıcı arabiriminin ayrıntılı açıklamasını içerir ve ESET Server Security ürününün nasıl kullanılacağını açıklamak için tasarlanmıştır.

Kullanıcı arabirimi sık kullanılan özelliklere hızlıca erişmenize olanak tanır:

- İzleme
- Günlük dosyaları
- Tarama
- Güncelle
- Ayarlar
- Araçlar

Tara

İsteğe bağlı tarayıcı, ESET Server Security ürününün önemli bir parçasıdır. Bilgisayarınızdaki dosyalarda ve klasörlerde tarama işlemi gerçekleştirmek için kullanılır. Ağınızın güvenliğini sağlamak için, bilgisayar taramalarının yalnızca etkilenmeden şüphelenildiğinde değil, rutin güvenlik önlemlerinin bir parçası olarak düzenli aralıklarla çalıştırılması önemlidir. Gerçek zamanlı dosya sistemi koruması tarafından algılanmayan virüsleri algılamak için düzenli olarak (örneğin ayda bir kez) sisteminizde kapsamlı bir tarama gerçekleştirmenizi öneririz. Bu, Gerçek zamanlı dosya koruması devre dışı bırakıldığında bir tehdit algılanırsa, algılama altyapısı güncellenmediğinde veya bir dosya diske ilk kaydedildiğinde algılanmazsa gerçekleşebilir.

ESET Server Security ürününde mevcut isteğe bağlı taramaları seçin:

Depolama taraması

Yerel sunucuda tüm paylaşılan klasörleri tarar. Depolama taraması kullanılamıyorsa sunucunuzda paylaşılan klasör yoktur.

Bilgisayarınızı tarayın

Hızlı bir şekilde bilgisayar taraması başlatmanıza ve etkilenen dosyaları kullanıcı müdahalesine gerek kalmadan temizlemenize olanak verir. Bilgisayarınızı tarayın seçeneğinin avantajı, kullanımının kolay olması ve ayrıntılı tarama yapılandırması gerektirmemesidir. Tarama, yerel sürücülerdeki tüm dosyaları denetler ve algılanan sızıntıları otomatik olarak temizler veya siler. Temizleme düzeyi otomatik olarak varsayılan değere ayarlanır. Temizleme türleri hakkında ayrıntılı bilgi için Temizleme bölümüne bakın.

> NOT
> Ayda en az bir defa bilgisayar taraması çalıştırmanızı öneririz. Tarama, zamanlanan görev olarak yapılandırılabilir.

Özel tarama

Tarama hedefleri ve tarama yöntemleri gibi tarama parametreleri belirtmek isterseniz Özel tarama buna en uygun çözümdür. Özel taramanın avantajı, tarama parametrelerini ayrıntılı biçimde yapılandırabilme özelliğidir. Yapılandırmalar kullanıcı tanımlı tarama profillerine kaydedilebilir. Tarama aynı parametreler kullanılarak yineleniyorsa bu yararlıdır.

Çıkarılabilir medya taraması

Smart taramaya benzer. Bilgisayara bağlı olan çıkarılabilir medyanın (CD/DVD/USB) hızlı bir taramasını başlatır. Bu, bir bilgisayara USB flash sürücü bağladığınızda ve bunun içeriğini kötü amaçlı yazılım ve diğer olası tehditlere karşı taramak istediğinizde faydalı olabilir. Ayrıca bu tür tarama **Özel tarama** tıklandıktan sonra **Tarama hedefleri** açılır menüsünden **Çıkarılabilir medya** seçilerek ve **Tara** seçeneği belirlenerek de başlatılabilir.

Hyper-V taraması

Bu seçenek, yalnızca ESET Server Security ürününün çalıştığı sunucuda bir Hyper-V Yöneticisi yüklenmişse görüntülenir. Hyper-V taraması, belirli VM'de herhangi bir "Agent"a gerek olmadan Microsoft Hyper-V Server'daki Sanal Makine (VM) disklerinin taranmasına olanak tanır.

OneDrive taraması

OneDrive bulut depolamasında yer alan kullanıcı dosyalarını taramanıza olanak tanır.

Son taramayı tekrar edin

Son tarama işleminizi, son taramadaki ayarların aynısını kullanarak tekrarlar.

> NOT
> İsteğe bağlı veri tabanı taraması mevcutsa son taramayı yineleme işlevi kullanılamaz.

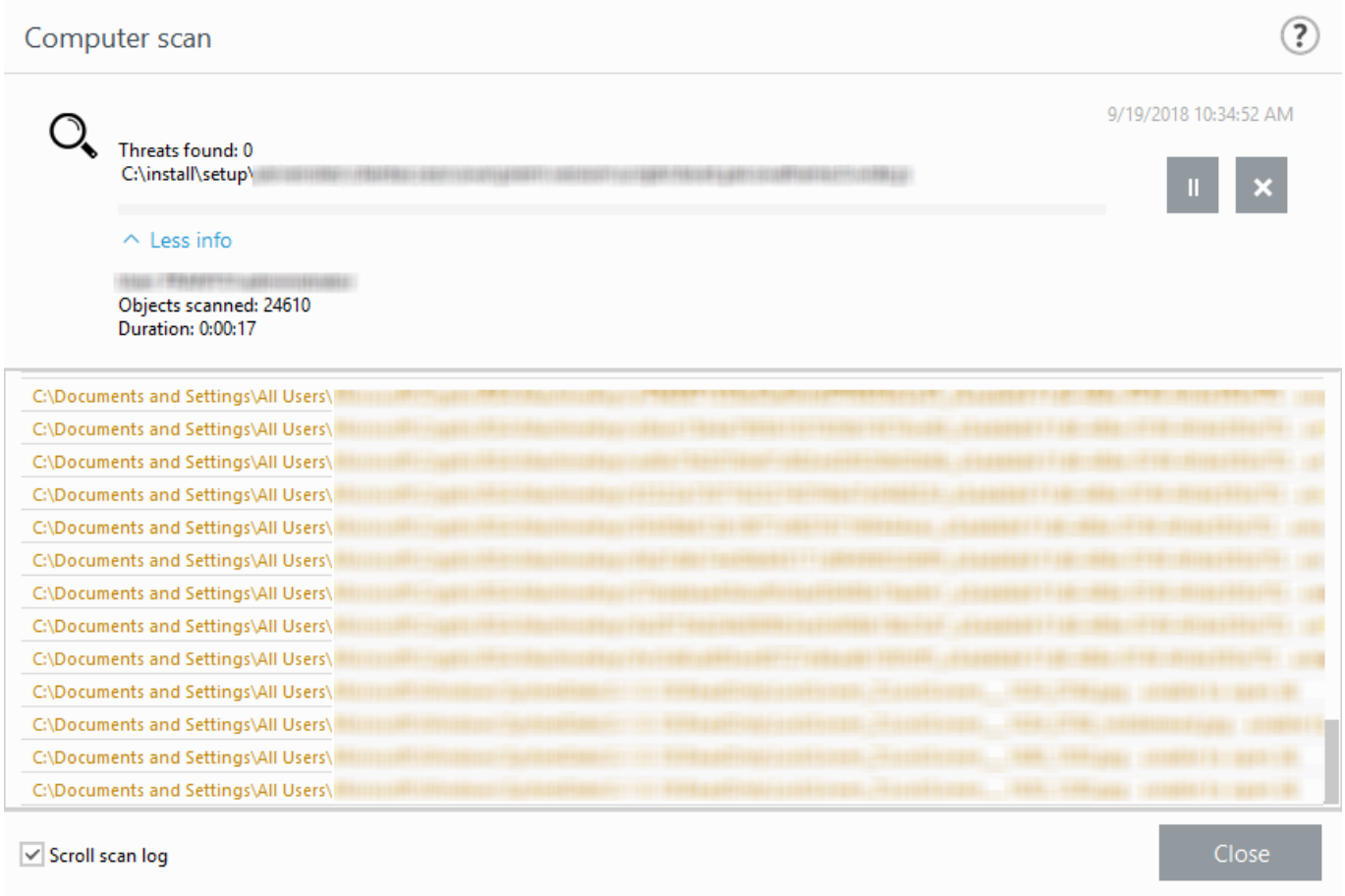
Tarama durumları hakkında daha fazla bilgi gösteren seçenekleri kullanabilirsiniz:

Dosyaları sürükle ve bırak	**Dosyaları ayrıca ESET Server Security tarama penceresine sürükleyip bırakabilirsiniz. Bu dosyalarda hemen virüs taraması yapılır**
Kapat / Tümünü kapat	Verilen iletileri kapatır.
Tarama durumları	İlk taramanın durumunu gösterir. Bu tarama tamamlanmış veya kullanıcı tarafından kesilmiştir.
Günlüğü göster	Daha ayrıntılı bilgiler gösterir.
Daha fazla bilgi	Taramayı yürüten **Kullanıcı**, **Taranan nesne** sayısı ve tarama **Süresi** gibi ayrıntıların tarama sırasında görülmesini sağlar.
Tarama pencerelerini aç	Tarama ilerleme durumu penceresi taramanın geçerli durumunu ve kötü amaçlı kod içerdiği belirlenen dosya sayısı hakkında bilgileri gösterir.

Tarama penceresi ve tarama günlüğü

Tarama penceresinde taranmakta olan nesneler ile bunların konumları, bulunan tehdit sayısı (varsa), taranan nesne sayısı ve tarama süresi gösterilir. Pencerenin alt bölümünde algılama altyapısı sürümü numarasını, taramanın başlatıldığı tarihi ve saati ve hedef seçimini gösteren bir tarama günlüğü bulunur.

Tarama devam ederken taramayı geçici olarak kesmek isterseniz **Duraklat**'ı tıklayabilirsiniz. Taram işlemi duraklatıldığında **Devam ettir** seçeneği kullanılabilir hale gelir.

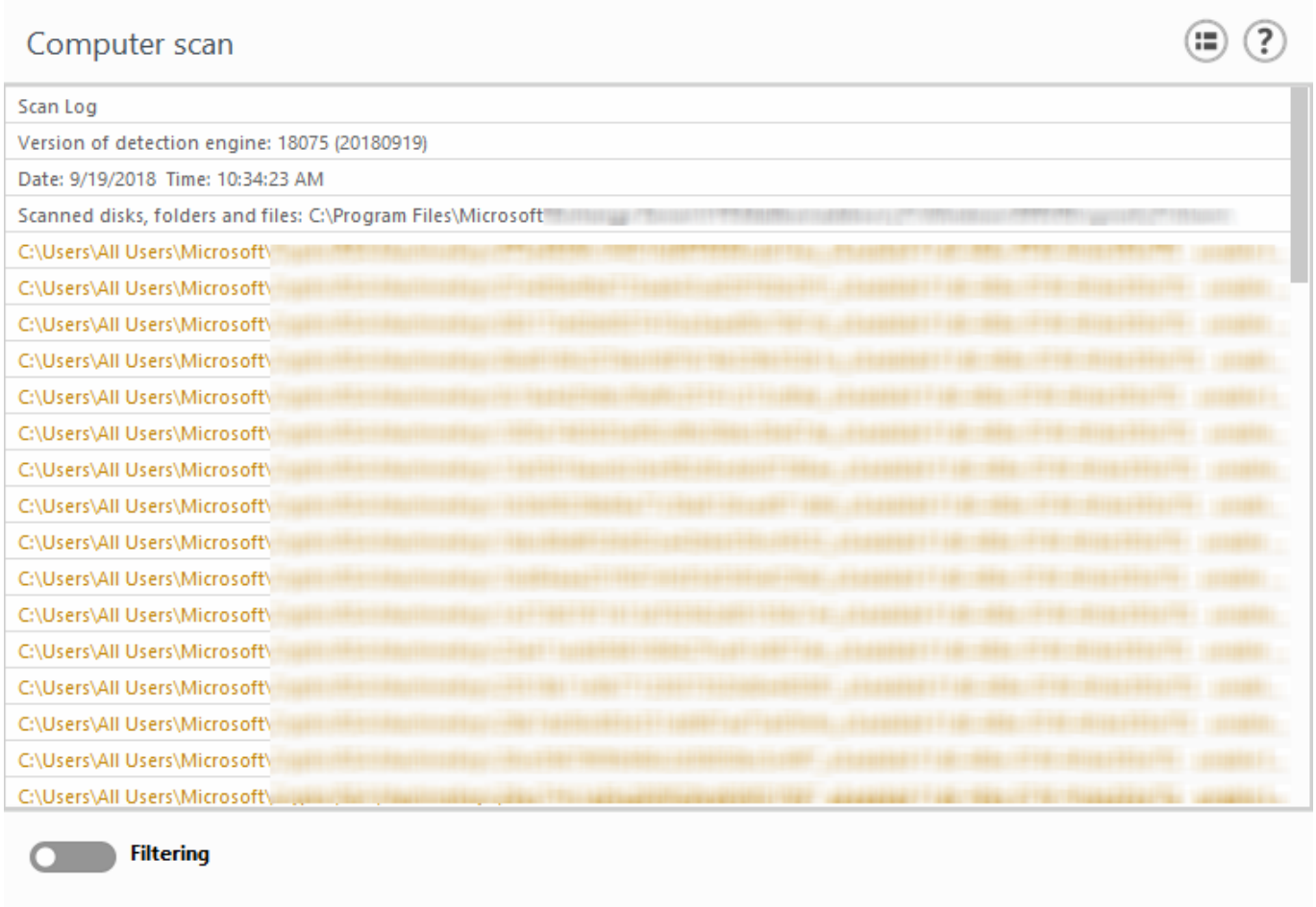


Tarama günlüğünü kaydır

Günlük dosyaları penceresinde eski günlükleri otomatik kaydırmak ve etkin günlükleri görüntülemek için bu seçeneği etkin bırakın.

> NOT
> Parolayla korunan dosyalar ve özel olarak sistem tarafından kullanılan dosyalar (tipik olarak *pagefile.sys* ve belirli günlük dosyaları) gibi bazı dosyaların taranamaması normaldir.

Tarama tamamlandıktan sonra, söz konusu taramayla ilgili tüm bilgileri içeren tarama günlüğünü görürsünüz.



Filtreleme veya arama ölçütlerini tanımlayabileceğiniz Günlük filtreleme penceresini açmak için **Filtreleme** anahtar simgesini tıklayın. İçerik menüsünü görüntülemek için belirli bir günlük girişini sağ tıklayın:

Eylem	Kullanım	Kısayol	Ayrıca bkz.
Aynı kayıtları filtrele	Günlük filtrelemeyi etkinleştirerek yalnızca seçilen kayıtla aynı türdeki kayıtları gösterir.	Ctrl + Shift + F	
Filtrele...	Bu seçeneği tıkladıktan sonra, Günlük filtreleme penceresi belirli günlük girişleri için filtreleme ölçütlerini tanımlamanıza olanak sağlar.		Günlük filtreleme
Filtreyi etkinleştir	Filtre ayarlarını etkinleştirir. Filtrelemeyi etkinleştirdiğiniz ilk seferde ayarları tanımlamalısınız.		
Filtreyi devre dışı bırak	Filtrelemeyi kapatır (alt kısımdaki anahtarı tıklamakla aynıdır).		
Kopyala	Seçilen/vurgulanan kayıtlardaki bilgileri panoya kopyalar.	Ctrl + C	
Tümünü kopyala	Pencerede bulunan tüm kayıtlardaki bilgileri kopyalar.		
Dışa aktar...	Seçilen/vurgulanan kayıtlardaki bilgileri bir XML dosyasına aktarır.		
Tümünü ver...	Penceredeki tüm bilgileri bir XML dosyasına aktarır.		

Günlük dosyaları

Günlük dosyaları, gerçekleşen önemli program olayları hakkında bilgi içerir ve tarama sonuçlarına, algılanan tehditlere vs. genel bir bakış sağlar. Günlükler sistem çözümlemesi, tehdit algılama ve sorun giderme açısından önemli bir araçtır. Günlüğe kaydetme işlemi herhangi bir kullanıcı müdahalesi olmadan arka planda etkin biçimde gerçekleşir. Bilgiler, geçerli günlük ayrıntı düzeyi ayarlarına göre kaydedilir. Metin iletilerini ve günlükleri,

doğrudan ESET Server Security ortamından görüntülemek veya başka bir yerde görüntülemek üzere dışa aktarmak da mümkündür.

Açılır menüden uygun günlük türünü seçin. Şu günlükler kullanılabilir:

Algılamalar

Algılamalar günlüğü, ESET Server Security modülleri tarafından algılanan sızıntılar hakkında ayrıntılı bilgiler sunar. Bilgiler, algılama zamanı, sızıntının adı, konum, gerçekleştirilen işlem ve sızıntı algılandığında oturum açmış olan kullanıcının adını içerir. Ayrıntıları ayrı bir pencerede görüntülemek için bir günlük girişini çift tıklayın. Gerekirse, algılama dışı bırakma işlemi oluşturabilirsiniz. Bunun için bir günlük kaydını (algılamayı) sağ tıklayıp **Tarama dışı bırakma işlemi oluştur**'u tıklayın. Bu, önceden tanımlanmış ölçütlerle tarama dışı bırakma sihirbazını açar. Tarama dışı bırakılmış bir dosyanın yanında bir algılama adı varsa bu, dosyanın yalnızca söz konusu algılama için tarama dışı bırakılmış olduğu anlamına gelir. Bu dosya daha sonra başka bir zararlı yazılım ile enfekte olursa algılanır.

Olaylar

ESET Server Security tarafından gerçekleştirilen tüm önemli eylemler olay günlüğüne kaydedilir. Olay günlüğünde olaylarla ilgili bilgiler ve programda oluşan hatalar bulunur. Bu, sistem yöneticilerinin ve kullanıcıların sorunları çözmesine yardımcı olmak üzere tasarlanmıştır. Burada bulunan bilgiler genellikle programda oluşan bir soruna çözüm bulmanıza yardımcı olabilir.

Bilgisayar taraması

Tüm tarama sonuçları bu pencerede görüntülenir. Her satır tek bir bilgisayar denetimine karşılık gelir. İlgili taramanın ayrıntılarını görmek için herhangi bir girişi çift tıklayın.

Engellenen dosyalar

Engellenen ve erişilemeyen dosyaların kayıtlarını içerir. Engellemenin nedeni ve dosyayı engelleyen kaynak modülü, aynı zamanda dosyayı yürüten uygulama ve kullanıcı protokolde gösterilir.

Gönderilen dosyalar

Bulut tabanlı koruma, ESET Dynamic Threat Defense ve ESET LiveGrid® dosyalarının kayıtlarını içerir.

Denetim günlükleri

Yapılandırma ve koruma durumundaki değişiklik kayıtlarını içerir ve daha sonra başvurmak üzere anlık görüntüler oluşturur. Gerçekleştirilen değişiklikle ilgili ayrıntılı bilgileri görmek için Ayar değişiklikleri türünde herhangi bir kaydı sağ tıklayıp içerik menüsünden **Değişiklikleri göster**'i seçin. Önceki ayara geri dönmek isterseniz **Geri yükle**'yi seçin. Ayrıca günlük kayıtlarını silmek için **Tümünü sil**'i de seçebilirsiniz. Denetleme günlüğünü etkinleştirmek isterseniz **Gelişmiş ayarlar** > **Araçlar** > **Günlük dosyaları** > Denetleme günlüğü'ne gidin.

HIPS

Kayıt için işaretlenen belirli kuralların kaydını içerir. Protokol, işlem olarak adlandırılan uygulamayı, sonucu (kuralın izin verilme veya yasaklanma durumu) ve oluşturulan kuralın adını gösterir.

Ağ koruması

Botnet koruması ve IDS (Ağ saldırısına karşı koruma) tarafından engellenen dosyaların kayıtlarını içerir.

Filtrelenen web siteleri

Web erişimi koruması ve Bu günlükler söz konusu web sitesine bir bağlantının açıldığı zamanı, bağlantı URL'sini, bağlantıyı açan kullanıcıyı ve uygulamayı gösterir.

Cihaz Kontrolü

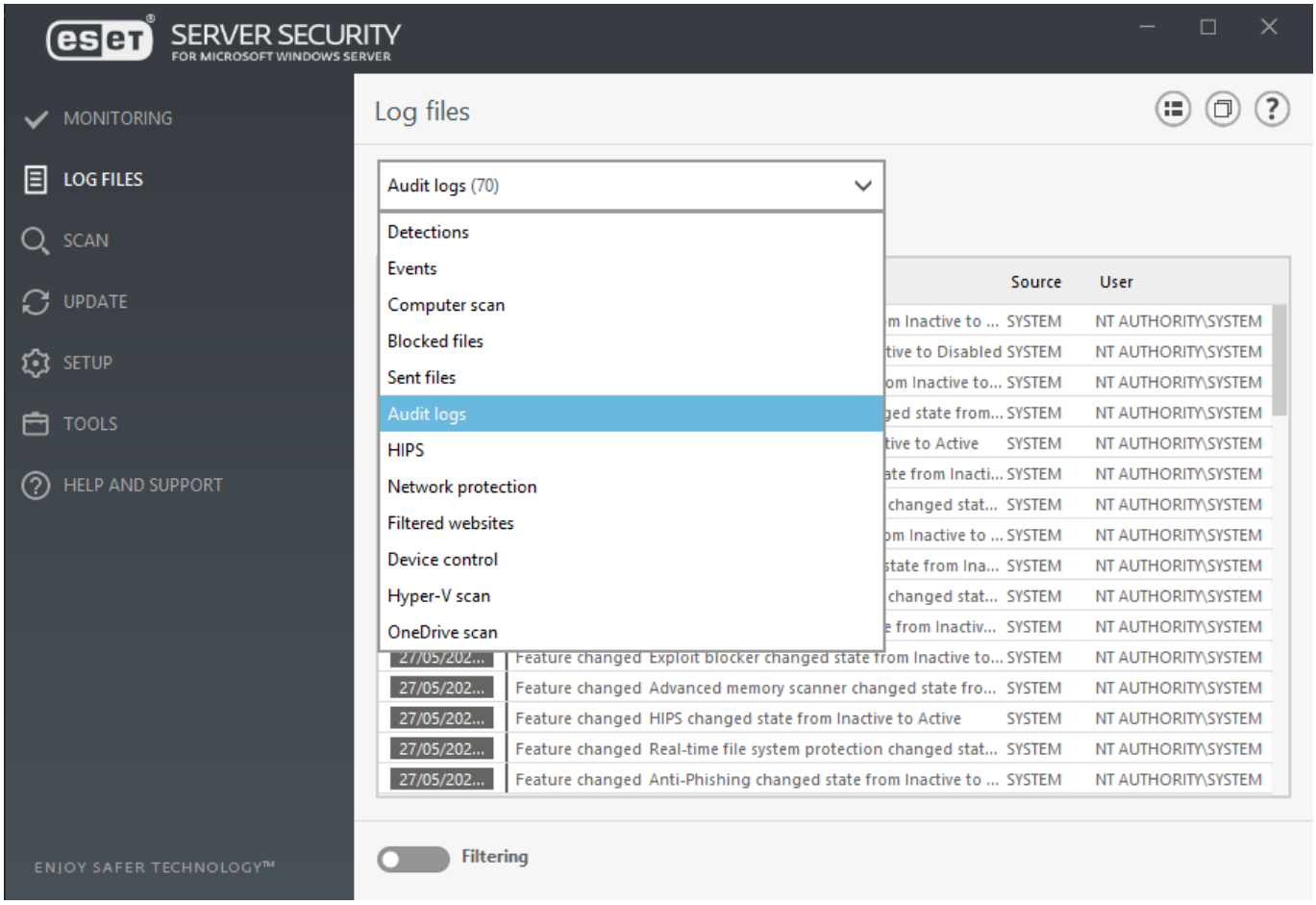
Bilgisayara bağlanan çıkarılabilir medya veya aygıtların kayıtlarını içerir. Yalnızca Aygıt denetimi kuralına sahip aygıtlar günlük dosyasına kaydedilir. Kural, bağlı bir aygıtla eşleşmiyorsa, bağlı aygıta yönelik bir günlük girişi oluşturulmaz. Burada aygıt türü, seri numarası, satıcı adı ve medya boyutu gibi (varsa) ayrıntılara da bakabilirsiniz.

Hyper-V taraması

Hyper-V tarama sonuçlarının listesini içerir. İlgili taramanın ayrıntılarını görmek için herhangi bir girişi çift tıklayın.

OneDrive taraması

OneDrive taraması sonuçlarının bir listesini içerir.



İçerik menüsü (sağ tıklama) seçilen günlük kaydında bir işlem seçmenize olanak tanır:

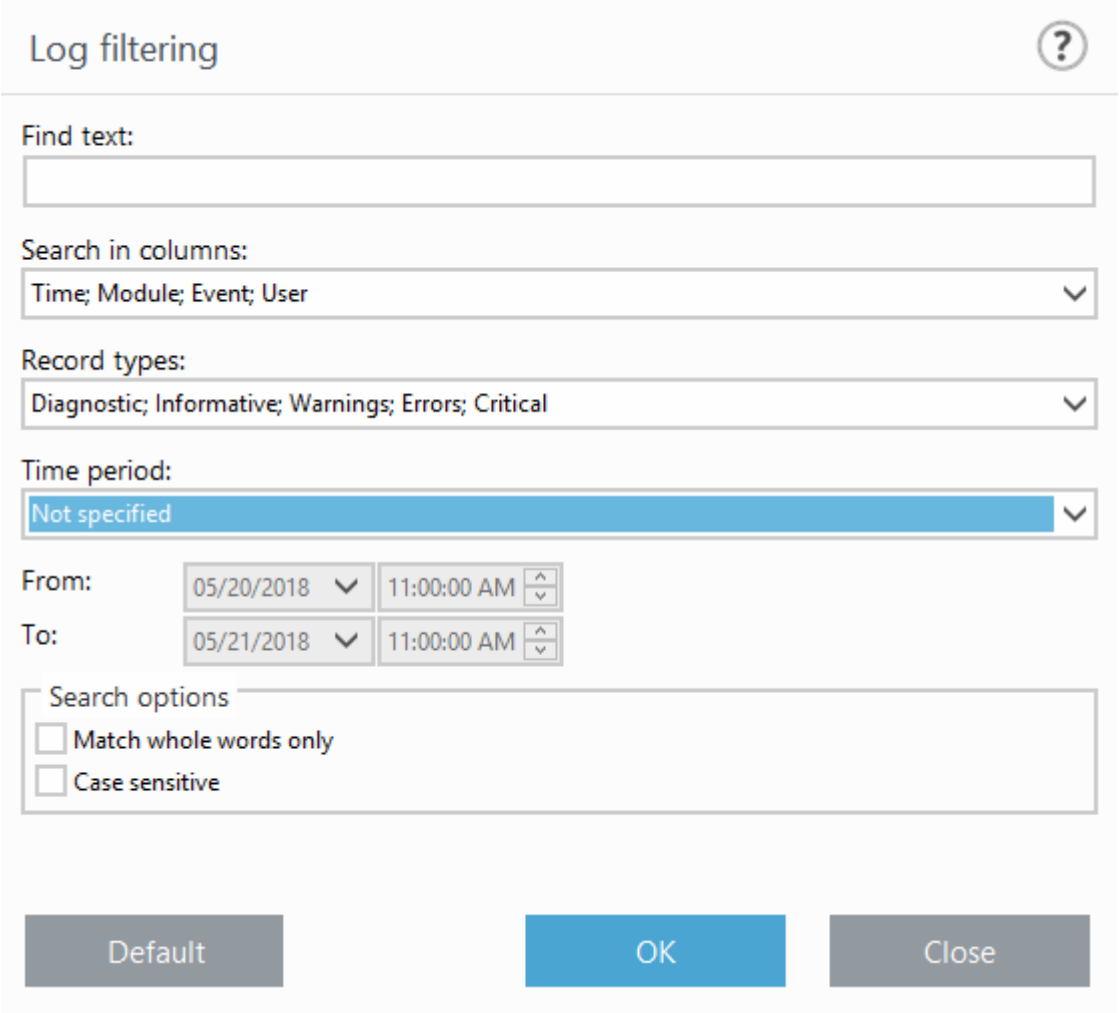
Eylem	Kullanım	Kısayol	Ayrıca bkz.

Eylem	Kullanım	Kısayol	Ayrıca bkz.
Göster	Yeni bir pencerede, seçilen günlük hakkında daha ayrıntılı bilgiler görüntüler (çift tıklama ile aynıdır).		
Aynı kayıtları filtrele	Günlük filtrelemeyi etkinleştirerek yalnızca seçilen kayıtla aynı türdeki kayıtları gösterir.	Ctrl + Shift + F	
Filtrele...	Bu seçeneği tıkladıktan sonra, Günlük filtreleme penceresi belirli günlük girişleri için filtreleme ölçütlerini tanımlamanıza olanak sağlar.		Günlük filtreleme
Filtreyi etkinleştir	Filtre ayarlarını etkinleştirir. Filtrelemeyi etkinleştirdiğiniz ilk seferde ayarları tanımlamalısınız.		
Filtreyi devre dışı bırak	Filtrelemeyi kapatır (alt kısımdaki anahtarı tıklamakla aynıdır).		
Kopyala	Seçilen/vurgulanan kayıtlardaki bilgileri panoya kopyalar.	Ctrl + C	
Tümünü kopyala	Pencerede bulunan tüm kayıtlardaki bilgileri kopyalar.		
Sil	Seçilen/vurgulanan kayıtları siler - bu eylem yönetici ayrıcalıkları gerektirir.	Del	
Tümünü sil	Penceredeki tüm kayıtları siler - bu eylem yönetici ayrıcalıkları gerektirir.		
Dışa aktar...	Seçilen/vurgulanan kayıtlardaki bilgileri bir XML dosyasına aktarır.		
Tümünü ver...	Penceredeki tüm bilgileri bir XML dosyasına aktarır.		
Bul...	Günlükte bul penceresini açar ve arama kriterlerini tanımlamanıza olanak sağlar. Filtreleme özelliği açık olduğunda bile, belirli bir kaydı bulmak için bul özelliğini kullanabilirsiniz.	Ctrl + F	Günlükte bulma
Sonrakini bul	Tanımlanan arama ölçütlerinizin sonraki örneğini bulur.	F3	
Öncekini bul	Önceki örneği bulur.	Shift + F3	
Tarama dışı bırakma işlemi oluştur	Algılama adını, yolunu veya hash'ini kullanarak nesneleri temizleme dışı bırakmak için.		Tarama dışı bırakma işlemi oluştur

Günlük filtreleme

Günlük filtreleme özelliği, özellikle çok sayıda kayıt olduğunda aradığınız bilgileri bulmanıza yardımcı olur. Örneğin belirli tür bir olayı, durumu veya zaman dilimini arıyorsanız günlük kayıtlarını daraltmanıza olanak tanır. Belirli arama seçeneklerini belirleyerek günlük kayıtlarını filtreleyebilirsiniz. Günlük dosyaları penceresinde yalnızca alakalı kayıtlar (söz konusu arama seçeneklerine göre) görüntülenir.

Metin bul alanına aradığınız anahtar kelimeyi yazın. Aramanızı hassaslaştırmak için **Sütunlarda ara** açılır menüsünü kullanın. **Kayıt günlüğü türleri** açılır menüsünden bir veya daha fazla kayıt seçin. Sonuçların gösterilmesini istediğiniz **zaman aralığını** tanımlayın. **Yalnızca tam sözcükleri eşleştir** veya **Büyük küçük harf duyarlı** gibi diğer arama seçeneklerini de kullanabilirsiniz.



Sonrakini bul

Bir dize yazın (kelime veya kelimenin bir bölümü). Yalnızca bu dizeyi içeren kayıtlar gösterilir. Diğer kayıtlar atlanır.

Sütunlarda ara

Arama yaparken hangi sütunların dikkate alınacağını seçin. Arama için kullanılmak üzere bir veya daha fazla sütun seçebilirsiniz.

Kayıt türleri

Açılır menüden bir veya daha fazla günlük kaydı türü seçin:

- **Tanılama** - Programı ve yukarıdaki tüm kayıtları hassas bir şekilde ayarlamak için gereken bilgileri günlüğe kaydeder.
- **Bilgilendirici** - Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarılar** - Kritik hataları ve uyarı iletilerini kaydeder.
- **Hatalar** - "Dosya indirme hatası" gibi hatalar ve kritik hatalar kaydedilir.
- **Kritik** - Yalnızca kritik hataları günlüğe kaydeder.

Zaman dilimi

Görüntülenmesini istediğiniz sonuçların ait olduğu zaman dilimini tanımlayın:

- **Belirtilmedi** (varsayılan) - Arama, zaman diliminde değil, tüm günlükte yapılır.
- **Son gün**
- **Geçen hafta**
- **Geçen ay**
- **Zaman dilimi** - Tam zaman dilimini (Başlangıç: ve Bitiş:) belirterek yalnızca belirtilen zaman dilimine ait kayıtları filtreleyebilirsiniz.

Yalnızca tam sözcükleri eşleştir

Daha kesin sonuçlar için tam sözcükleri aramak isterseniz bu onay kutusunu kullanın.

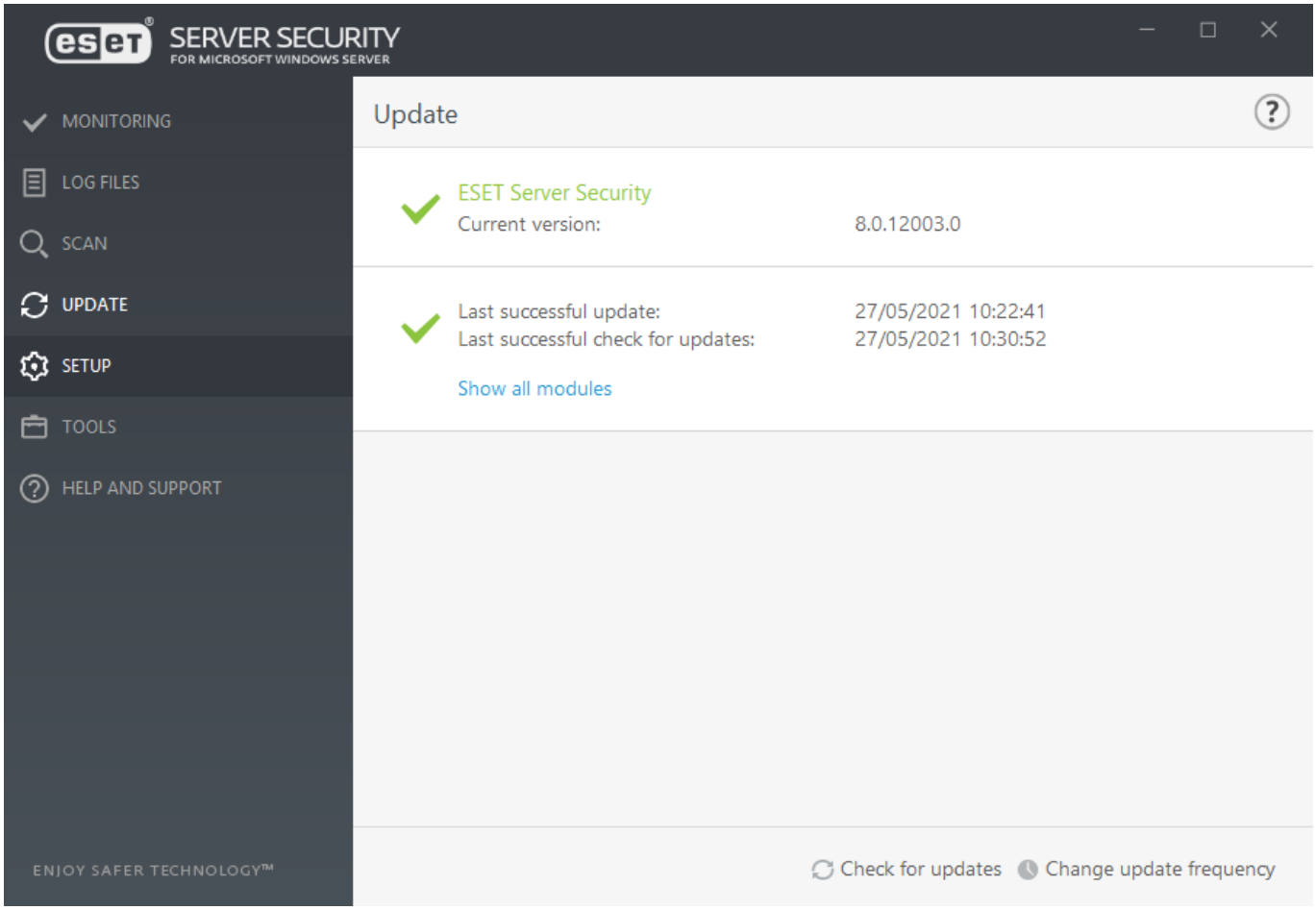
Büyük küçük harf duyarlı

Filtreleme sırasında büyük veya küçük harf kullanmak sizin için önemliyse bu seçeneği etkinleştirin. Filtreleme/arama seçeneklerinizi yapılandırdıktan sonra, filtrelenen günlük kayıtlarını göstermek için **Tamam**'ı veya aramaya başlamak için **Bul**'u tıklayın. Günlük dosyaları, bulunduğunuz konumdan (vurgulanan kayıt) başlayarak yukarıdan aşağıya doğru aranır. Arama, ilk eşleşen kaydı bulduğunda durur. Bir sonraki kaydı aramak için **F3**'e basın veya arama seçeneklerinizi hassaslaştırmak için sağ tıklayıp **Bul**'u seçin.

Güncelleme

Güncelleme bölümünde, son başarılı güncelleme tarihi ve saati dahil olmak üzere ESET Server Security ürününüzün geçerli güncelleme durumunu görebilirsiniz. ESET Server Security ürününün düzenli olarak güncellenmesi, sunucunuzda maksimum güvenlik düzeyini sağlamak için en iyi yöntemdir. Güncelleme modülü, şu iki yöntemle programın her zaman güncel olmasını sağlar: algılama altyapısını ve program bileşenlerini güncelleyerek. Algılama altyapısının ve program bileşenlerinin güncellenmesi, kötü amaçlı koda karşı tam koruma sağlamanın önemli bir parçasıdır.

> NOT
> Lisans anahtarını henüz girmediyseniz, güncellemeleri alamazsınız ve sizden ürününüzü etkinleştirmeniz istenir. Bunu yapmak için **Yardım ve destek** > **Ürünü Etkinleştir** bölümüne gidin.



Geçerli sürüm

ESET Server Security yapı sürümüdür.

Son başarılı güncelleme

Son güncelleme tarihidir. Modüllerin güncel olduğunu gösteren yakın bir tarih olduğundan emin olun.

Güncellemeler için son başarılı denetleme

Modüllerin güncellenmesinin denendiği en son tarihtir.

Tüm modülleri göster

Yüklenen modülleri açmak için kullanılır.

Güncellemeleri denetle

Modüllerin güncellenmesi, kötü amaçlı kodlara karşı tam koruma sağlamanın önemli bir parçasıdır.

Güncelleme sıklığını değiştir

Düzenli otomatik güncelleme zamanlayıcı görevi için görev zamanlamasını düzenleyebilirsiniz.

Mümkün olan en kısa zamanda Güncellemeleri denetlemezseniz, aşağıdaki iletilerden biri görüntülenir:

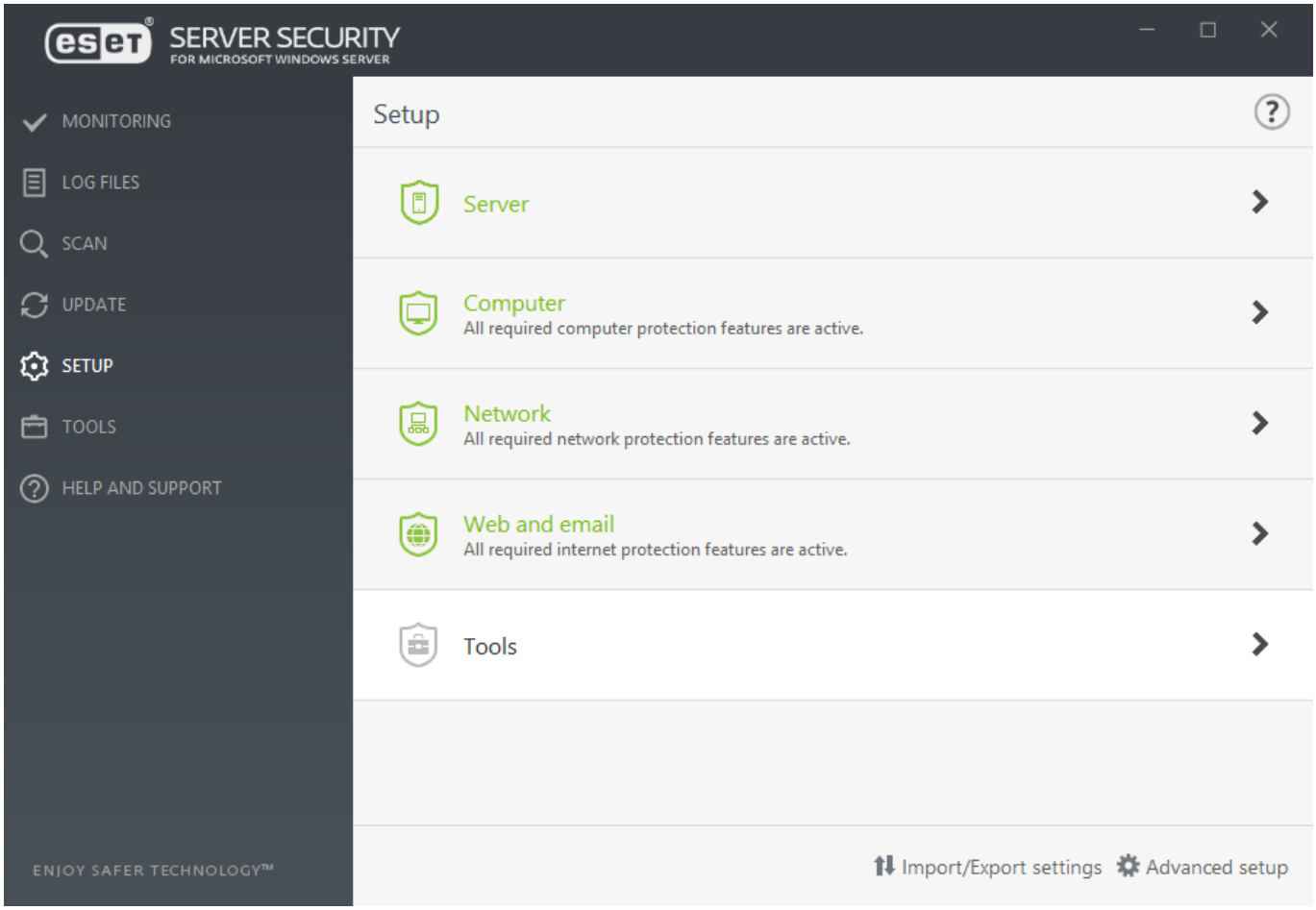
Hata iletisi	Açıklamalar
Modül güncellemesi güncel değil	Bu hata, modül güncellemesine yönelik birkaç başarısız girişimden sonra görüntülenir. Güncelleme ayarlarını denetlemenizi öneririz. Bu hatanın en yaygın nedeni, yanlış girilmiş kimlik doğrulama verileri veya yanlış yapılandırılmış bağlantı ayarlarıdır.
Modül güncellemesi başarısız oldu - Ürün etkinleştirilmedi	Lisans anahtarı, güncelleme ayarlarına yanlış girilmiş. Kimlik doğrulama verilerinizi kontrol etmenizi öneririz. **Gelişmiş ayarlar** (**F5**) penceresi ek güncelleme seçenekleri içerir. Yeni bir lisans anahtarı girmek için ana menüden **Yardım ve Destek** > Lisansı yönet seçeneğini tıklayın.
Güncelleme dosyaları karşıdan yüklenirken hata oluştu	Hatanın nedeni yanlış İnternet bağlantısı ayarları olabilir. İnternet bağlantınızı, web tarayıcınızda herhangi bir web sitesi açarak denetlemenizi öneririz. Web sitesi açılmazsa İnternet bağlantısının kurulmamış olması veya bilgisayarınızda bağlantı sorunları bulunması mümkündür. Etkin bir İnternet bağlantınız yoksa lütfen İnternet Hizmet Sağlayıcınız (ISP) ile iletişim kurun.
Modül güncellemesi başarısız oldu Hata 0073	**Güncelle** > **Güncellemeleri Denetle**'yi tıklayın, daha fazla bilgi için şu Bilgi Bankası makalesini ziyaret edin.

NOT
Çeşitli güncelleme profilleri için proxy sunucu seçenekleri farklı olabilir. Bu durumda, **Gelişmiş ayarlar** (**F5**) bölümünde **Güncelle** > Profil'i tıklayın.

Ayarlar

Ayar menüsü penceresi aşağıdaki bölümleri içerir:

- Sunucu
- Bilgisayar
- Ağ
- Web ve e-posta
- Araçlar - Tanı amaçlı günlüğe kaydetme



Tek tek modülleri geçici olarak devre dışı bırakmak için, ilgili modülün yanındaki yeşil kaydırıcı çubuğu tıklayın. Bu işlem sunucunuzun koruma düzeyini düşürebilir.

Devre dışı bırakılan bir güvenlik bileşeninin korumasını yeniden etkinleştirmek için, uygun modülün yanındaki kırmızı kayırıcı çubuğu tıklayın. Bileşen etkin duruma geri döner.

Belirli bir güvenlik bileşeninin ayrıntılı ayarlarına erişmek için, dişli simgesini tıklayın.

Ayarları Al/Ver

Bir *.xml* yapılandırma dosyasını kullanarak ayar parametrelerini yükleyin veya geçerli ayar parametrelerini bir yapılandırma dosyasına kaydedin.

Gelişmiş ayarlar'da farklı güncelleme profillerini

İhtiyaçlarınıza göre gelişmiş ayarları ve seçenekleri yapılandırın. Programdaki herhangi bir konumdan **Gelişmiş ayarlar** ekranına erişmek için **F5** tuşuna basın.

Sunucu

Kaydırıcı çubuğu kullanarak etkinleştirebileceğiniz/devre dışı bırakabileceğiniz bileşenlerin bir listesini görürsünüz. Belirli bir öğenin ayarlarını yapılandırmak için dişli simgesini tıklayın.

Otomatik dışlamalar

Önemli sunucu uygulamalarını ve sunucu işletim sistemi dosyalarını tespit eder ve bunları otomatik olarak tarama dışı bırakmalar listesine ekler. Bu işlev, potansiyel çakışma riskinin en düşük düzeye indirilmesine ve tehdit tespiti yazılımı çalışırken sunucunun genel performansının artırılmasına yardımcı olur.

Küme

ESET Kümesi'ni yapılandırmak ve etkinleştirmek içindir.

OneDrive tarama ayarları

ESET OneDrive tarayıcı uygulamasını Microsoft OneDrive'a kaydedebilir veya OneDrive'dan uygulamanın kaydını silebilirsiniz.

Tek tek modülleri geçici olarak devre dışı bırakmak için, ilgili modülün yanındaki yeşil kaydırıcı çubuğu tıklayın. Bu işlem sunucunuzun koruma düzeyini düşürebilir.

Devre dışı bırakılan bir güvenlik bileşeninin korumasını yeniden etkinleştirmek için, uygun modülün yanındaki kırmızı kayırıcı çubuğu tıklayın. Bileşen etkin duruma geri döner.

Belirli bir güvenlik bileşeninin ayrıntılı ayarlarına erişmek için, dişli simgesini tıklayın.

Ayarları Al/Ver

Bir *.xml* yapılandırma dosyasını kullanarak ayar parametrelerini yükleyin veya geçerli ayar parametrelerini bir yapılandırma dosyasına kaydedin.

Gelişmiş ayarlar'da farklı güncelleme profillerini

İhtiyaçlarınıza göre gelişmiş ayarları ve seçenekleri yapılandırın. Programdaki herhangi bir konumdan **Gelişmiş ayarlar** ekranına erişmek için **F5** tuşuna basın.

Bilgisayar

ESET Server Security, sunucunun bir bilgisayar olarak ciddi bir şekilde korunmasını sağlamak için gerekli bileşenlerin tamamına sahiptir. Bu modül, aşağıdaki bileşenleri etkinleştirmenize/devre dışı bırakmanıza ve yapılandırmanıza olanak sağlar:

Gerçek zamanlı dosya sistemi koruması

Tüm dosyalar bilgisayarınızda açıldığında, oluşturulduğunda veya çalıştırıldığında kötü amaçlı kodlara karşı taranır. Gerçek zamanlı dosya sistemi koruması için ayrıca **Yapılandırma** veya **Tarama dışı öğeleri düzenleme** seçenekleri mevcuttur, ardından dosyaları ve klasörleri tarama dışı bırakabileceğiniz tarama dışı öğeler ayar penceresi açılır.

Cihaz Kontrolü

Bu modül; genişletilmiş filtreleri/izinleri taramanıza, engellemenize veya ayarlamanıza ve bir kullanıcının belirli bir aygıta erişme ve aygıtta çalışma yetkisini tanımlamanıza olanak tanır.

Host Tabanlı Saldırı Önleme Sistemi (HIPS)

Sistem işletim sisteminde meydana gelen olayları izler ve bunlara özelleştirilmiş bir kurallar kümesine göre yanıt verir.

- Gelişmiş bellek tarayıcı
- Exploit Engelleyici
- Fidye Yazılımı Koruması

Sunum modu

Yazılımlarını kesintisiz olarak kullanabilmeyi talep eden, açılır pencerelerle rahatsız edilmek istemeyen ve CPU kullanımının en aza inmesini isteyen kullanıcılara yönelik bir özelliktir. Sunum modu etkinleştirildikten sonra bir uyarı iletisi (olası güvenlik riski) alırsınız ve ana program penceresi turuncu renge döner.

Antivirus ve antispyware korumasını duraklat

Antivirus ve antispyware korumasını geçici olarak devre dışı bıraktığınızda, açılır menüden seçili bileşenin devre dışı kalmasını istediğiniz süreyi belirtin ve ardından güvenlik bileşenini devre dışı bırakmak için **Uygula** seçeneğini tıklayın. Korumayı yeniden etkinleştirmek için **Antivirus ve antispyware korumasını etkinleştir** seçeneğini tıklayın veya kaydırma çubuğuyla etkinleştirin.

Tek tek modülleri geçici olarak devre dışı bırakmak için, ilgili modülün yanındaki yeşil kaydırıcı çubuğu tıklayın. Bu işlem sunucunuzun koruma düzeyini düşürebilir.

Devre dışı bırakılan bir güvenlik bileşeninin korumasını yeniden etkinleştirmek için, uygun modülün yanındaki kırmızı kayırıcı çubuğu tıklayın. Bileşen etkin duruma geri döner.

Belirli bir güvenlik bileşeninin ayrıntılı ayarlarına erişmek için, dişli simgesini tıklayın.

Ayarları Al/Ver

Bir *.xml* yapılandırma dosyasını kullanarak ayar parametrelerini yükleyin veya geçerli ayar parametrelerini bir yapılandırma dosyasına kaydedin.

Gelişmiş ayarlar'da farklı güncelleme profillerini

İhtiyaçlarınıza göre gelişmiş ayarları ve seçenekleri yapılandırın. Programdaki herhangi bir konumdan **Gelişmiş ayarlar** ekranına erişmek için **F5** tuşuna basın.

Ağ

Filtreleme kurallarınıza göre bireysel ağ bağlantılarına izin verilerek veya ağ bağlantıları reddedilerek gerçekleştirilir. Uzak bilgisayarlardan gelen saldırılara karşı koruma sağlar ve tehlike potansiyeli taşıyan bazı hizmetleri engeller.

Ağ modülü, aşağıdaki bileşenleri etkinleştirmenize/devre dışı bırakmanıza ve yapılandırmanıza olanak sağlar:

Ağ saldırısına karşı koruma (IDS)

Ağ trafiğinin içeriğini analiz eder ve ağ saldırılarına karşı koruma sağlar. Zararlı olduğu düşünülen tüm trafikler engellenir.

Botnet koruması

Botnet iletişimini algılama ve engelleme. Sistemdeki kötü amaçlı yazılımları hızla ve doğru bir şekilde tanımlar.

Geçici IP adresi kara listesi (engellenen adresler)

Saldırı kaynakları olduğu algılanan ve bağlantının belirli bir süreliğine engellenmesi için kara listeye eklenen IP adreslerinin bir listesini görüntüler

Sorun giderme sihirbazı (yakın zamanda engellenen uygulamalar veya aygıtlar)

Ağ saldırısı korumasının neden olduğu bağlantı sorunlarını çözmenize yardımcı olur.

Tek tek modülleri geçici olarak devre dışı bırakmak için, ilgili modülün yanındaki yeşil kaydırıcı çubuğu tıklayın. Bu işlem sunucunuzun koruma düzeyini düşürebilir.

Devre dışı bırakılan bir güvenlik bileşeninin korumasını yeniden etkinleştirmek için, uygun modülün yanındaki kırmızı kayırıcı çubuğu tıklayın. Bileşen etkin duruma geri döner.

Belirli bir güvenlik bileşeninin ayrıntılı ayarlarına erişmek için, dişli simgesini tıklayın.

Ayarları Al/Ver

Bir *.xml* yapılandırma dosyasını kullanarak ayar parametrelerini yükleyin veya geçerli ayar parametrelerini bir yapılandırma dosyasına kaydedin.

Gelişmiş ayarlar'da farklı güncelleme profillerini

İhtiyaçlarınıza göre gelişmiş ayarları ve seçenekleri yapılandırın. Programdaki herhangi bir konumdan **Gelişmiş ayarlar** ekranına erişmek için **F5** tuşuna basın.

Ağ sorunu giderme sihirbazı

Sorun giderme sihirbazı; tüm engellenen bağlantıları izler ve belirli uygulamalar veya aygıtlar ile ilgili ağ saldırısına karşı koruma sorunlarını düzeltmek üzere sorun giderme işlemi sırasında sizi yönlendirir. Ardından sihirbaz, onaylamanız durumunda uygulanacak yeni bir kural kümesi önerir.

Web ve e-posta

Web ve e-posta, aşağıdaki bileşenleri etkinleştirmenize/devre dışı bırakmanıza ve yapılandırmanıza olanak sağlar:

Web erişimi koruması

Etkinleştirilirse, tüm HTTP veya HTTPS trafiği kötü amaçlı yazılımlara karşı taranır.

E-posta istemci koruması

POP3 ve IMAP protokolleri yoluyla alınan iletişimleri izler.

Kimlik Avı Koruması

Yasa dışı olan ancak yasal görünen web sitelerinin parola, banka verileri ve başka hassas bilgileri elde etme girişimlerine karşı sizi korur.

Tek tek modülleri geçici olarak devre dışı bırakmak için, ilgili modülün yanındaki yeşil kaydırıcı çubuğu tıklayın. Bu işlem sunucunuzun koruma düzeyini düşürebilir.

Devre dışı bırakılan bir güvenlik bileşeninin korumasını yeniden etkinleştirmek için, uygun modülün yanındaki kırmızı kayırıcı çubuğu tıklayın. Bileşen etkin duruma geri döner.

Belirli bir güvenlik bileşeninin ayrıntılı ayarlarına erişmek için, dişli simgesini tıklayın.

Ayarları Al/Ver

Bir *.xml* yapılandırma dosyasını kullanarak ayar parametrelerini yükleyin veya geçerli ayar parametrelerini bir yapılandırma dosyasına kaydedin.

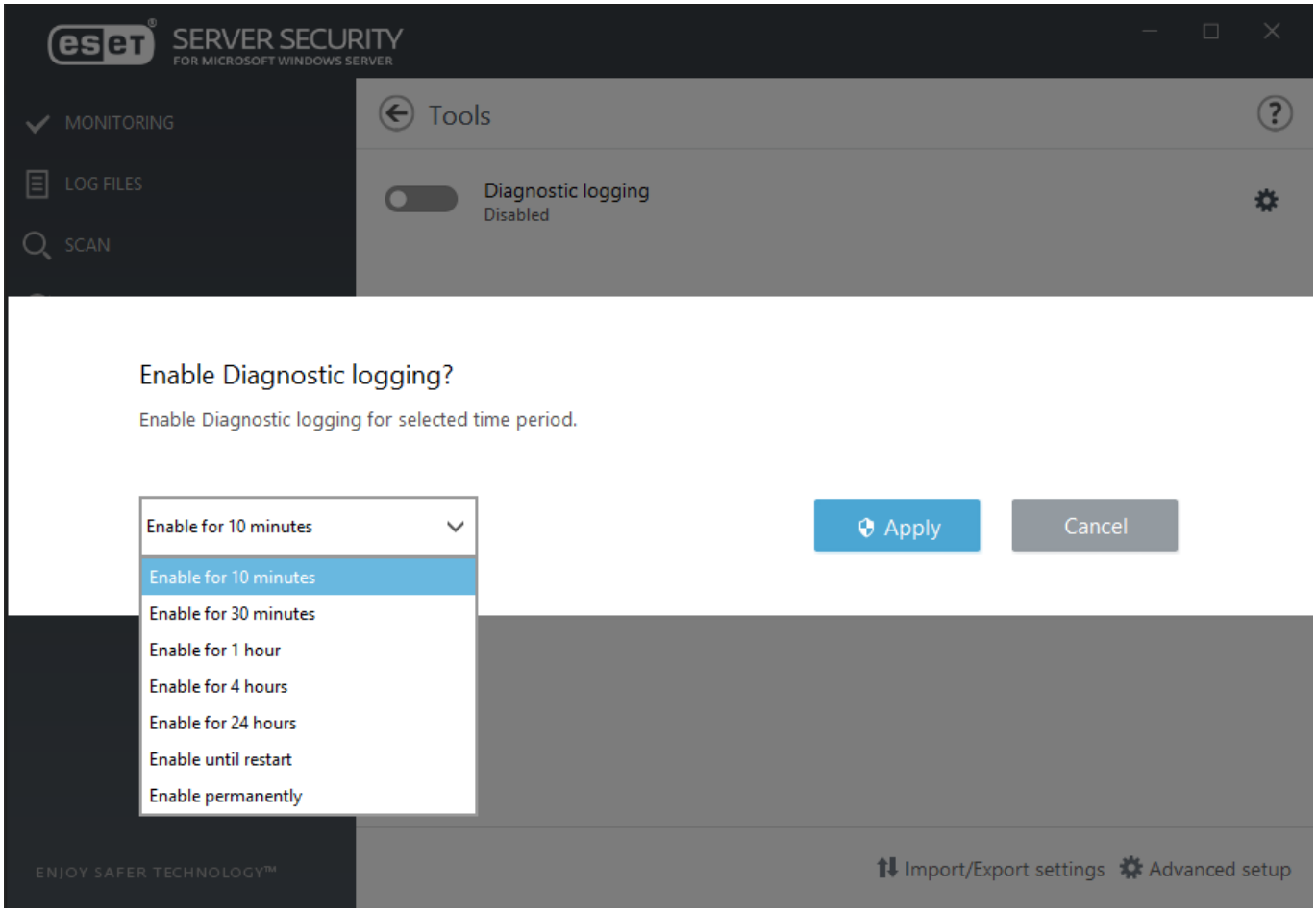
Gelişmiş ayarlar'da farklı güncelleme profillerini

İhtiyaçlarınıza göre gelişmiş ayarları ve seçenekleri yapılandırın. Programdaki herhangi bir konumdan **Gelişmiş ayarlar** ekranına erişmek için **F5** tuşuna basın.

Araçlar - Tanı amaçlı günlüğe kaydetme

Belirli bir ESET Server Security özelliğinin (örneğin sorun giderme) davranışı hakkında ayrıntılı bilgilere ihtiyacınız olduğunda Tanı amaçlı günlüğe kaydetme seçeneğini etkinleştirebilirsiniz. Dişli simgesini tıkladığınızda, hangi özellikler için tanı amaçlı günlüklerin toplanacağını yapılandırabilirsiniz.

Hangi süreyle etkin olacağını seçin (10 dakika, 30 dakika, 1 saat, 4 saat, 24 saat, sunucunun bir sonraki yeniden başlatılmasına kadar veya kalıcı olarak). Tanı amaçlı günlüğe kaydetme açıldığında, etkinleştirilen özelliklere bağlı olarak ESET Server Security ayrıntılı günlükleri toplar.



Tek tek modülleri geçici olarak devre dışı bırakmak için, ilgili modülün yanındaki yeşil kaydırıcı çubuğu tıklayın. Bu işlem sunucunuzun koruma düzeyini düşürebilir.

Devre dışı bırakılan bir güvenlik bileşeninin korumasını yeniden etkinleştirmek için, uygun modülün yanındaki kırmızı kayırıcı çubuğu tıklayın. Bileşen etkin duruma geri döner.

Belirli bir güvenlik bileşeninin ayrıntılı ayarlarına erişmek için, dişli simgesini tıklayın.

Ayarları Al/Ver

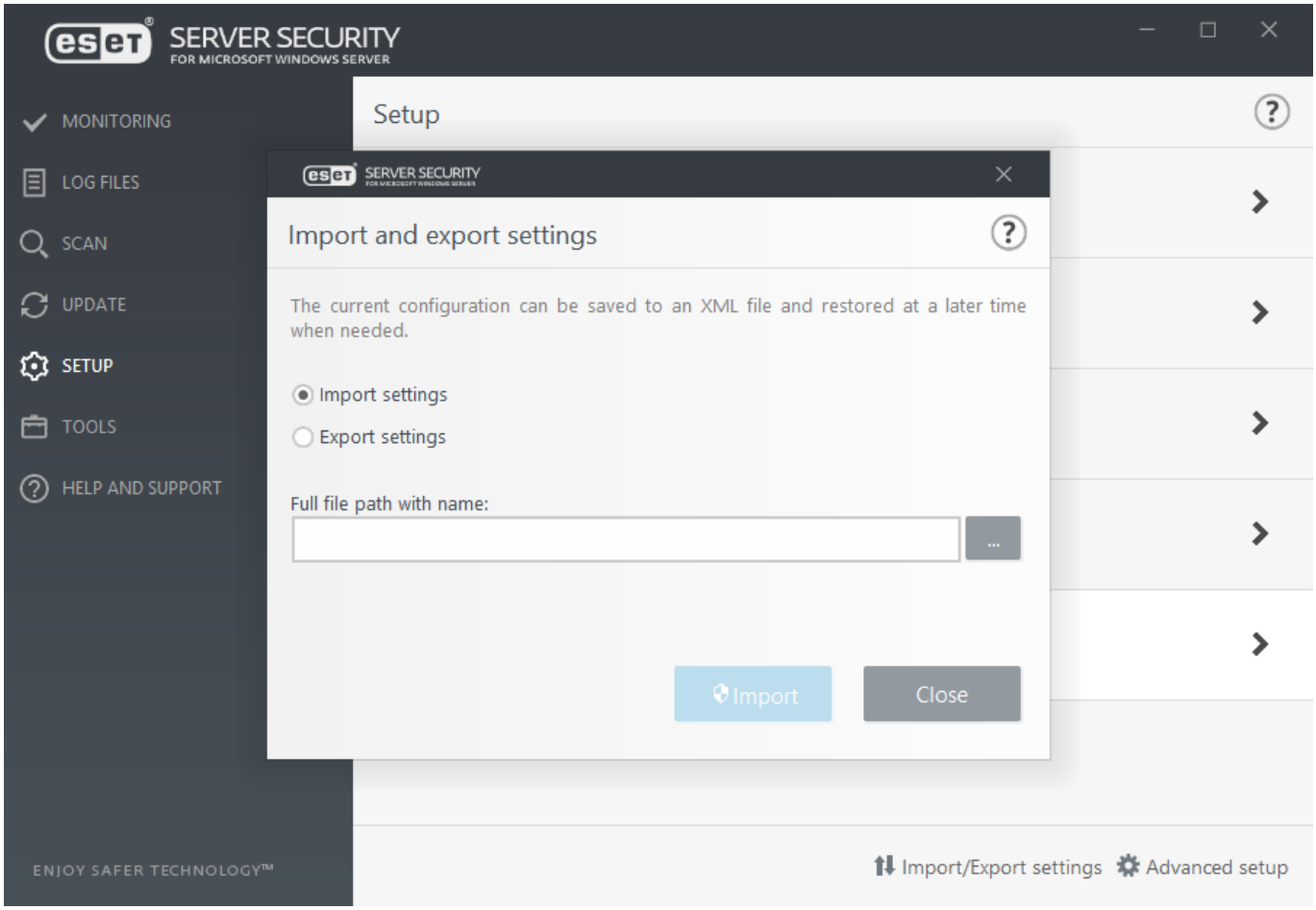
Bir *.xml* yapılandırma dosyasını kullanarak ayar parametrelerini yükleyin veya geçerli ayar parametrelerini bir yapılandırma dosyasına kaydedin.

Gelişmiş ayarlar'da farklı güncelleme profillerini

İhtiyaçlarınıza göre gelişmiş ayarları ve seçenekleri yapılandırın. Programdaki herhangi bir konumdan **Gelişmiş ayarlar** ekranına erişmek için **F5** tuşuna basın.

Ayarları içe ve dışa aktarma

Ayarları içe/dışa aktarma özelliği, ESET Server Security ürününüzün geçerli yapılandırmasını yedeklemeniz gerektiğinde kullanışlıdır. İçe aktarma özelliğini, aynı ayarları ESET Server Security bulunan başka sunuculara dağıtmak/uygulamak için de kullanabilirsiniz. Ayarlar bir *.xml* dosyasına aktarılır.



NOT
Dışa aktarılan dosyayı belirtilen dizine yazmak için izinleriniz yoksa, ayarları dışa aktarırken hata mesajı alabilirsiniz.

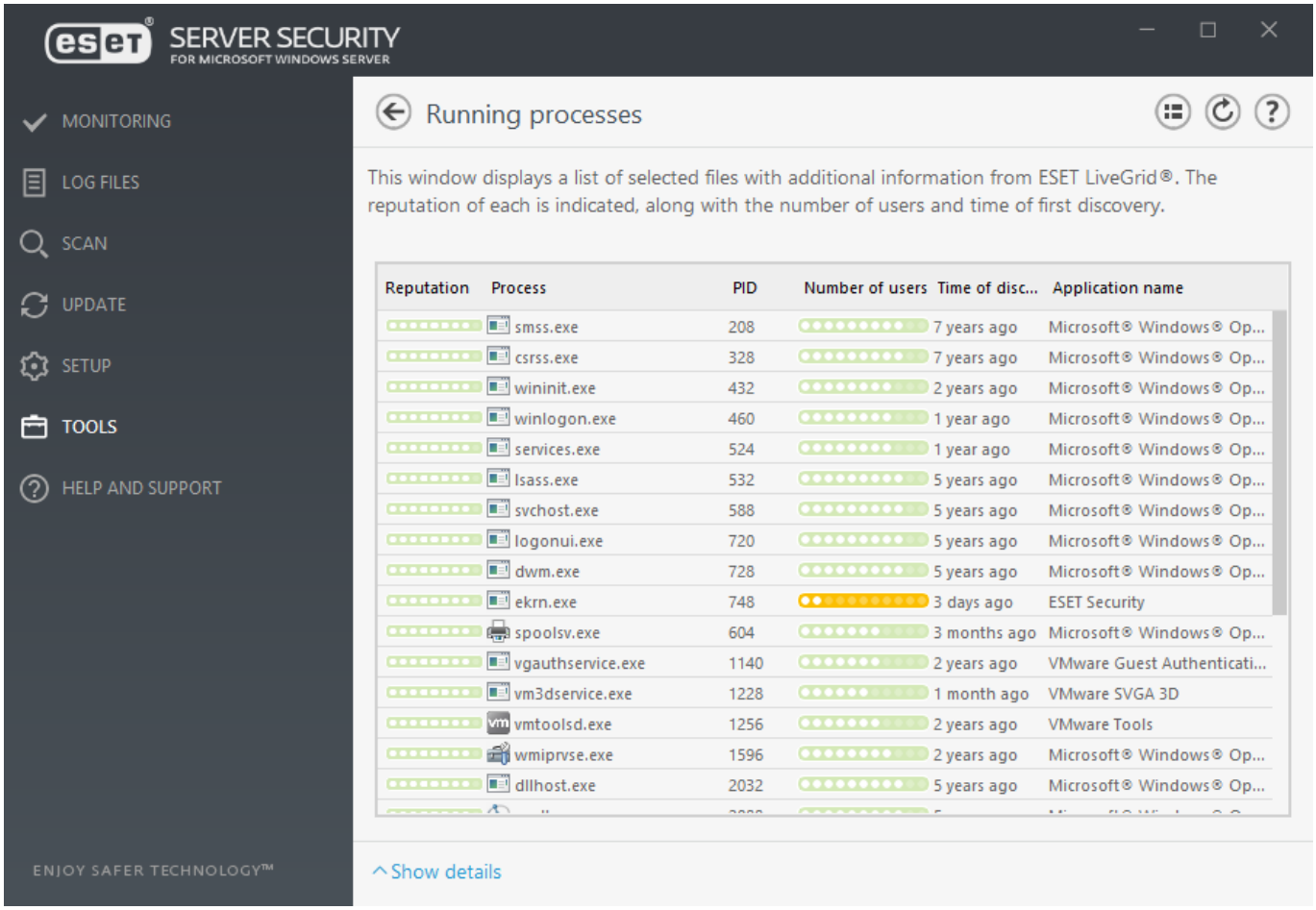
Araçlar

ESET Server Security yönetimi için aşağıdaki özellikler mevcuttur:

- Çalışan işlemler
- Etkinlik izleme
- Koruma istatistikleri
- Küme
- ESET Shell
- ESET Dynamic Threat Defense
- ESET SysInspector
- ESET SysRescue Live
- Zamanlayıcı
- Örneği analiz için gönder
- Karantina

Çalışan işlemler

Çalışan işlemler, bilgisayarınızda çalışan programları veya işlemleri görüntüler ve ESET'i hemen ve sürekli olarak yeni sızıntılarla ilgili bilgilendirir. ESET Server Security, kullanıcıları ESET LiveGrid® teknolojisiyle korumak için çalışan işlemlerle ilgili ayrıntılı bilgi sağlar.



NOT
En iyi bilinirlik (yeşil) olarak işaretlenmiş bilinen uygulamalar temizdir (beyaz listeye alınmıştır) ve isteğe bağlı bilgisayar taramasının veya bilgisayarınızdaki Gerçek zamanlı dosya sistemi korumasının tarama hızını iyileştireceği için tarama dışında bırakılırlar.

Bilinirlik	**Çoğu durumda, ESET Server Security ve ESET LiveGrid® teknolojisi, her nesnenin (dosyalar, işlemler, kayıt defteri anahtarları vb.) özelliklerini inceleyen ve ardından nesnenin kötü amaçlı etkinlik olasılığını ölçen bir dizi sezgisel tarama kuralı kullanarak nesnelere bilinirlik düzeyi atar. Bu sezgisel taramalar esas alınarak nesnelere 9 - En iyi bilinirlik (yeşil) ile 0 - En kötü bilinirlik (kırmızı) arasında bir bilinirlik düzeyi atanır.**
İşlem	Halihazırda bilgisayarınızda çalışan programın veya işlemin görüntü adı. Ayrıca, bilgisayarınızda çalışmakta olan tüm işlemleri görmek için Windows Görev Yöneticisini de kullanabilirsiniz. Görev Yöneticisi'ni görev çubuğunda boş bir alanı sağ tıklayıp ardından Görev Yöneticisi'ni tıklayarak veya klavyenizde Ctrl+Shift+Esc tuşlarına basarak açabilirsiniz.
PID	Windows işletim sistemlerinde çalışan işlemlerin kimliğidir.
Kullanıcı Sayısı	Belirli bir uygulamayı kullanan kullanıcıların sayısı. Bu bilgiler ESET LiveGrid® teknolojisiyle toplanır.
Bulunma Zamanı	Uygulamanın ESET LiveGrid® teknolojisi tarafından bulunmasından sonra geçen süre.
Uygulama adı	Bu işlemin ait olduğu programa verilen addır.

NOT
Bir uygulama Bilinmeyen (turuncu) olarak işaretlendiğinde, kötü amaçlı yazılım olmak zorunda değildir. Bu genellikle yeni bir uygulamadır. Dosyadan emin değilseniz, dosyayı ESET Virüs Laboratuvarı'na göndermek üzere Örneği analiz için gönder seçeneğini kullanın. Dosyanın kötü amaçlı bir uygulama olduğu anlaşılırsa, bu dosyanın algılanması yakında çıkarılacak olan algılama altyapısı güncellemelerinden birine eklenir.

Ayrıntıları göster

Aşağıdaki bilgiler pencerenin alt kısmında görünür:

- **Yol -** Bilgisayarınızdaki bir uygulamanın konumu.
- **Boyut** - kB (kilobayt) veya MB (megabayt) cinsinden dosya boyutu.
- **Açıklama** - İşletim sistemindeki açıklamaya dayalı dosya özellikleri.
- **Şirket** - Satıcının veya uygulama işleminin adı.
- **Sürüm** - Uygulama yayımcısından gelen bilgiler.
- **Ürün** - Uygulama adı ve/veya ticari ad.
- **Oluşturulma tarihi** - Uygulamanın oluşturulduğu tarih ve saat.
- **Değiştirilme tarihi** - Uygulamanın en son değiştirildiği tarih ve saat.

İşlem özel durumlarına ekle

Bir işlemi tarama dışında bırakmak için çalışan işlemler penceresinde söz konusu işlemi sağ tıklayın. İşlemin yolu Tarama dışı bırakılan işlemler listesine eklenir.

Etkinlik izleme

Etkinliği grafik biçiminde izlemek için, etkinlikten sonra gelen açılır menüden seçim yapın:

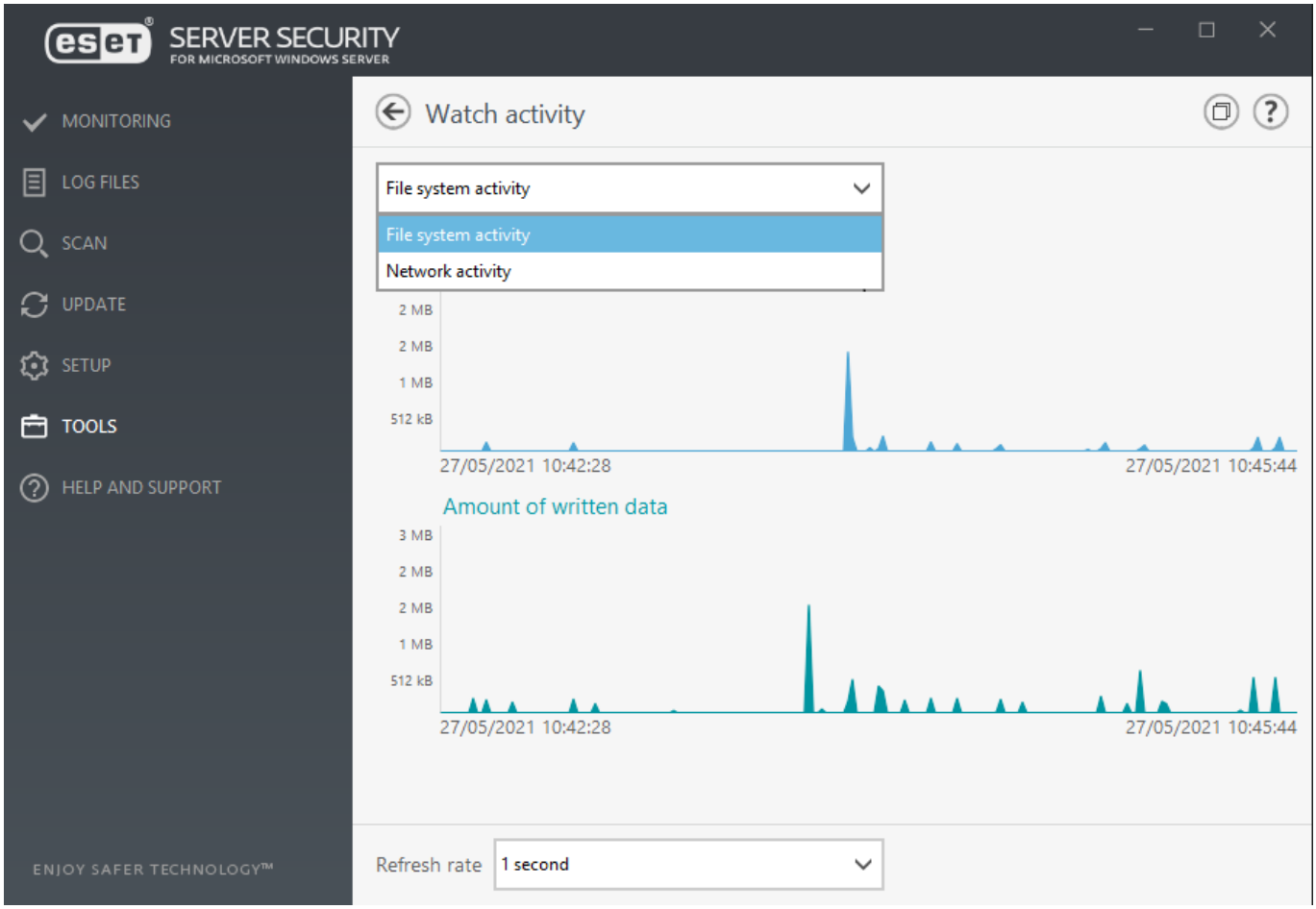
Dosya sistemi etkinliği

Okunan veya yazılan veri miktarıdır. Dikey grafik ekseni, okunan verileri (mavi) ve yazılan verileri (yeşil) temsil eder.

Ağ aktivitesi

Alınan veya gönderilen veri miktarıdır. Dikey grafik ekseni, alınan verileri (mavi) ve gönderilen verileri (yeşil) temsil eder.

Grafiğin en alt kısmında, dosya sistemi etkinliğini seçili zaman aralığına gerçek zamanlı olarak kaydeden bir zaman çizelgesi yer alır. Güncellemelerin sıklığını değiştirmek için **Yenileme hızı** açılır menüsünü kullanın.

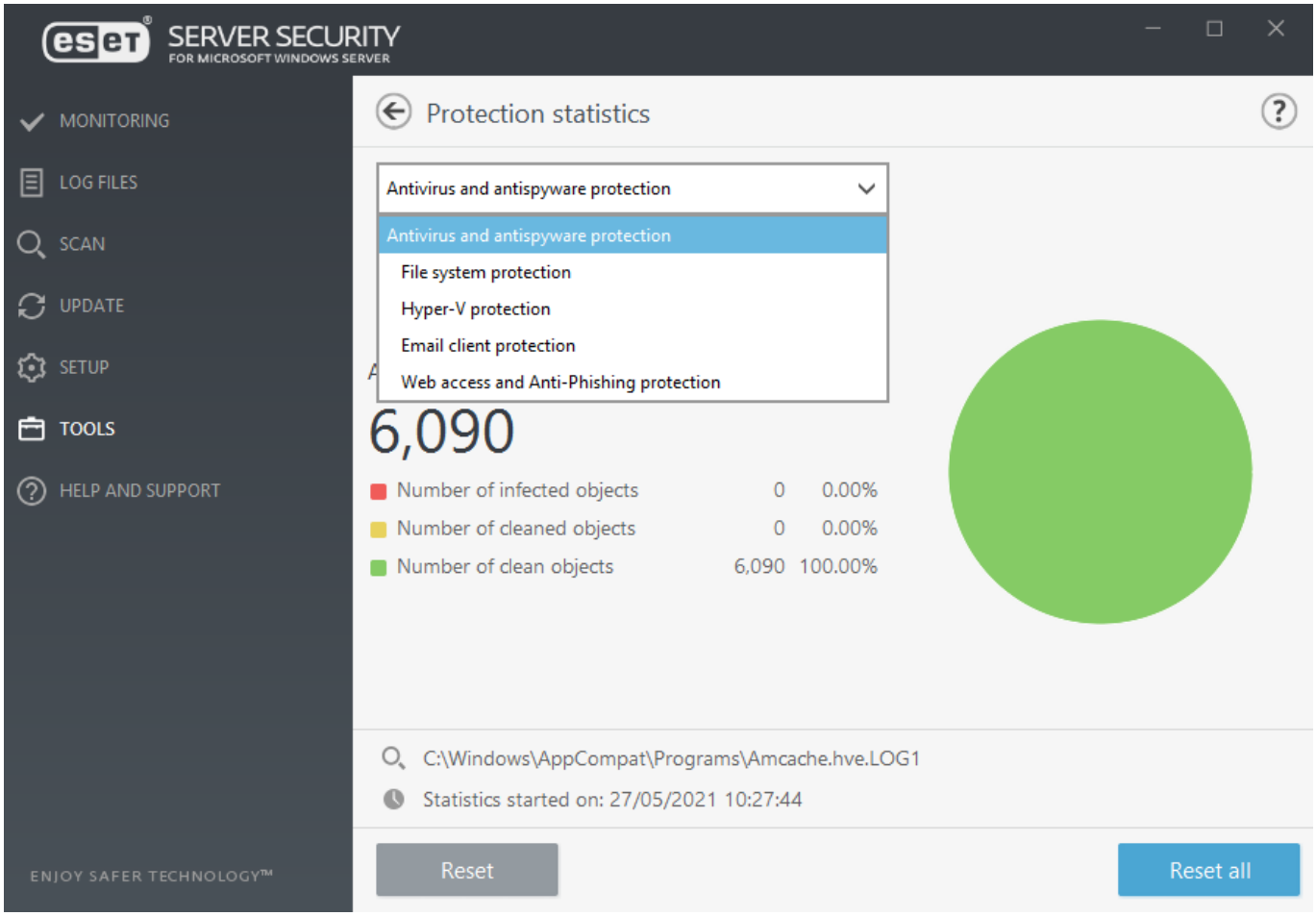


Kullanılabilir seçenekler şunlardır:

1 saniye	**Grafik her saniye yenilenir ve zaman çizelgesi son 10 dakikayı kapsar.**
1 dakika (son 24 saat)	Grafik her dakika yenilenir ve zaman çizelgesi son 24 saati kapsar.
1 saat (geçen ay)	Grafik her saat yenilenir ve zaman çizelgesi son ayı kapsar.
1 saat (seçili ay)	Grafik her saat yenilenir ve zaman çizelgesi seçilen ayı kapsar. Etkinliği görmek için açılır menüden bir ay (ve bir yıl) seçin. **Değiştir**'i tıklayın.

Koruma istatistikleri

ESET Server Security ürününün koruma modülleriyle ilgili istatistik verilerini görüntülemek için açılır menüden uygun koruma modülünü seçin. İstatistik grafiklerinin yanında tüm taranan nesnelerin, etkilenen nesnelerin, temizlenen nesnelerin ve temiz olan nesnelerin sayılarını görebilirsiniz. Farenizi grafiğin yanındaki bir nesnenin üzerine getirdiğinizde yalnızca o nesne için veriler grafikte gösterilir. Mevcut koruma modülü için istatistik bilgilerini temizlemek amacıyla **Sıfırla**'yı tıklayın. Tüm modüllere ait verileri temizlemek için **Tümünü sıfırla**'yı tıklayın.



ESET Server Security ürününde aşağıdaki istatistik grafikleri kullanılabilir:

Antivirus ve antispyware koruması

Etkilenen ve temizlenen nesnelerin toplam sayısını görüntüler.

Dosya sistemi koruması

Yalnızca dosya sisteminden okunan veya dosya sistemine yazılan nesneleri görüntüler.

Hyper-V koruması

Etkilenen, temizlenen ve temiz olan nesnelerin toplam sayısını görüntüler (yalnızca Hyper-V bulunan sistemlerde).

E-posta istemci koruması

Yalnızca e-posta istemcileri tarafından gönderilen veya alınan nesneleri görüntüler.

Web erişimi ve Kimlik avı koruması

Yalnızca web tarayıcıları tarafından indirilen nesneleri görüntüler.

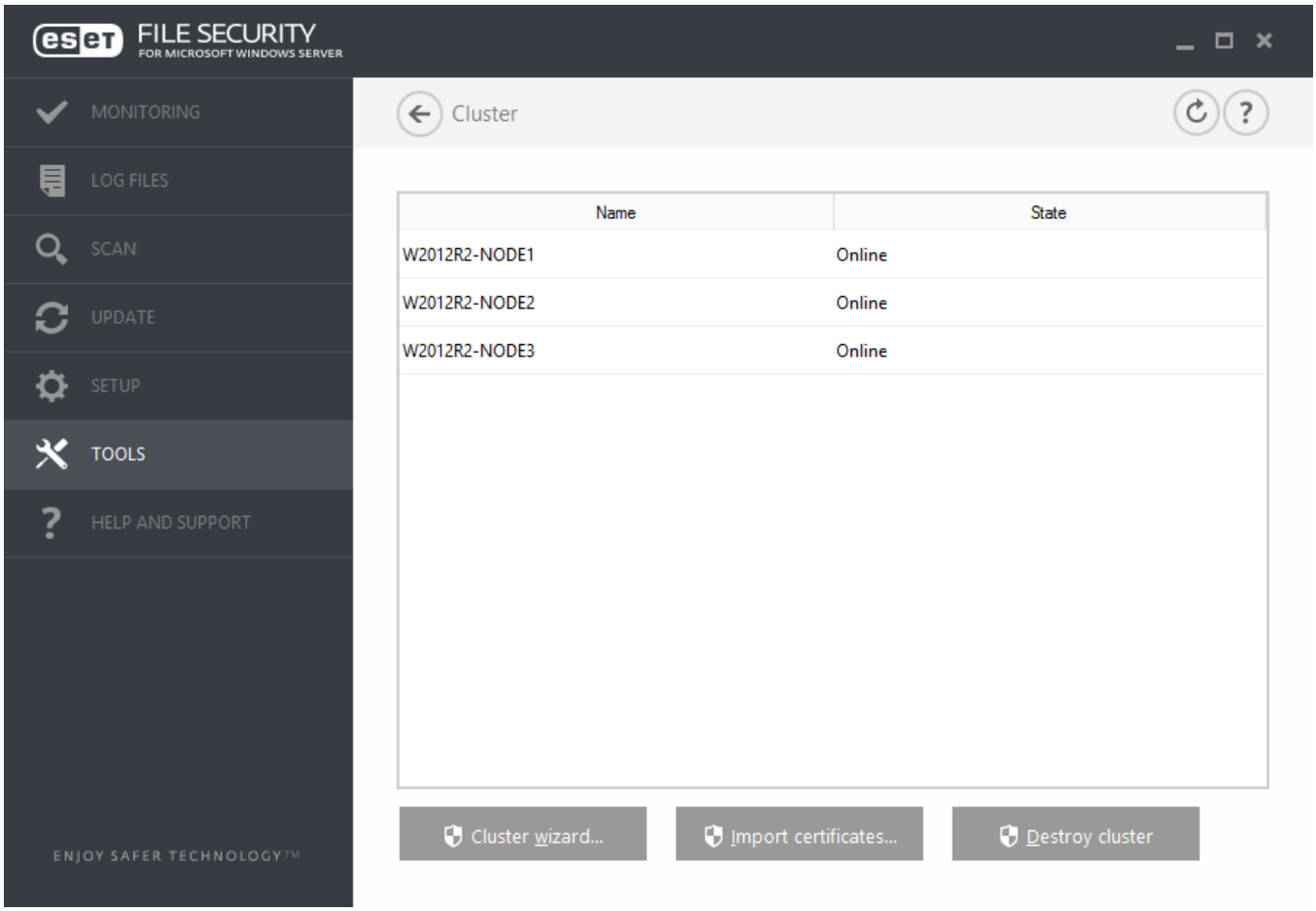
Küme

ESET Kümesi, Microsoft Windows Server için ESET ürün serisinin P2P iletişim altyapısıdır.

Bu altyapı, ESET sunucu ürünlerinin birbirleriyle iletişim kurmasını ve yapılandırma ve bildirimler gibi verileri gönderip almasının sağlar. Ayrıca bir grup ürün örneğinin doğru işlemesi için gerekli olan verileri de senkronize eder. Bu tür gruba örnek, ESET ürünlerinin yüklenmiş olduğu Windows Yük Devri Kümesi veya Ağ Yükü Dengelemesi (NLB) Kümesi içinde bulunan bir grup düğümdür ve kümenin tamamında ürünün aynı yapılandırmaya sahip olması gerekir. ESET Kümesi, yüklenmiş ürünler arasındaki tutarlılığı garantiler.

NOT
Kullanıcı arabirimi ve Zamanlanan görevler ayarları ESET Kümesi düğümleri arasında senkronize edilmez. Bu bilerek yapılmıştır.

ESET Kümesi durum sayfasında **Araçlar** > **Küme** bölümündeki anan menüden erişilebilir ve doğru şekilde yapılandırıldığında durum sayfası şöyle görünmelidir:



NOT
ESET Server Security ve Linux için ESET File Security arasında ESET Kümelerinin oluşturulması desteklenmez.

ESET kümesini ayarlarken düğüm eklemenin iki yolu vardır:

Otomatik olarak algıla

Bir Windows Yük Devri Kümesi'ne / NLB Kümesi'ne zaten sahipseniz, Otomatik olarak algıla özelliği üye

düğümlerini otomatik olarak ESET Kümesi'ne ekler.

Gözat

Sunucu adlarını yazarak (aynı Çalışma grubunun üyeleri veya aynı Etki alanının üyeleri) düğümleri manuel olarak ekleyebilirsiniz.

> NOT
> **Sunucuların** ESET Kümesi özelliğini kullanmak için bir Windows Yük Devri Kümesi'ne / NLB Kümesi'ne üye olmaları zorunlu değildir. ESET Kümelerini kullanmanız için Windows Yük Devri Kümesi veya NLB Kümesinin ortamınızda bulunması gerekmez.

ESET Kümenize düğümleri eklemenin ardından gelen adım, ESET Server Security ürününün her düğüme yüklenmesidir. Bu, ESET Kümesi'nin kurulumu sırasında otomatik olarak yapılır. ESET Server Security ürününün diğer küme düğümlerine uzaktan yüklenmesi için gerekli olan kimlik bilgileri:

Etki alanı senaryosu

Etki alanı yöneticisi kimlik bilgileridir.

Çalışma grubu senaryosu

Tüm düğümlerin, aynı yerel yönetici hesabı kimlik bilgilerini kullandığından emin olmanız gerekir

Bir ESET Kümesi'nde mevcut bir Windows Yük Devri Kümesi / NLB Kümesi'nin üyeleri şeklinde otomatik olarak eklenen düğümlerin bir kombinasyonunu da kullanabilirsiniz (aynı Etki Alanında yer almaları şartıyla).

> ÖNEMLİ
> Etki Alanı düğümlerini çalışma grubu düğümleriyle birleştirmek mümkün değildir.

ESET Kümesi'nin kullanılması için başka bir gereklilik de ESET Server Security ürününün ESET Kümesi düğümlerine gönderilmesinden önce Windows Güvenlik Duvarı'nda **Dosya ve Yazıcı Paylaşımı**'nın etkinleştirilmesidir.

Dilediğiniz zaman Küme sihirbazını çalıştırarak mevcut bir ESET Kümesi'ne yeni düğümler ekleyebilirsiniz.

Sertifikaları içe aktar

Sertifikalar, HTTPS kullanımında makineler arası güçlü kimlik doğrulama sağlamak için kullanılır. Her ESET Kümesi için bağımsız bir sertifika hiyerarşisi vardır. Hiyerarşide bir kök sertifika ve kök sertifika tarafından imzalanan bir düğüm sertifikaları kümesi bulunur. Kök sertifikanın özel anahtarı tüm düğüm sertifikaları oluşturulduktan sonra yıkılır. Kümeye yeni bir düğüm eklediğiniz zaman, yeni bir sertifika hiyerarşisi oluşturulur. Sertifikaları (Küme sihirbazı işlemi sırasında oluşturulan) içeren klasöre gidin. Sertifika dosyasını seçip **Aç**'ı tıklayın.

Kümeyi yok et

ESET Kümeleri dağıtılabilir. Her düğüm, yok edilmekte olan ESET Kümesi hakkında olay günlüklerinde bir kayıt oluşturur. Bunun ardından, tüm ESET güvenlik duvarı kuralları Windows Güvenlik Duvarı'ndan kaldırılır. Eski düğümler, önceki durumlarına geri döndürülür ve gerekirse başka bir ESET Kümesi'nde yeniden kullanılabilir.

Küme sihirbazı - Düğümleri seç

ESET Kümesi ayarlanırken yapılacak ilk işlem, düğümleri eklemektir. Düğüm eklemek için **Otomatik olarak algıla** seçeneğini veya **Gözat**'ı kullanabilirsiniz. Alternatif olarak, sunucu adını metin kutusuna yazıp **Ekle** öğesini tıklatabilirsiniz.

Otomatik olarak algıla

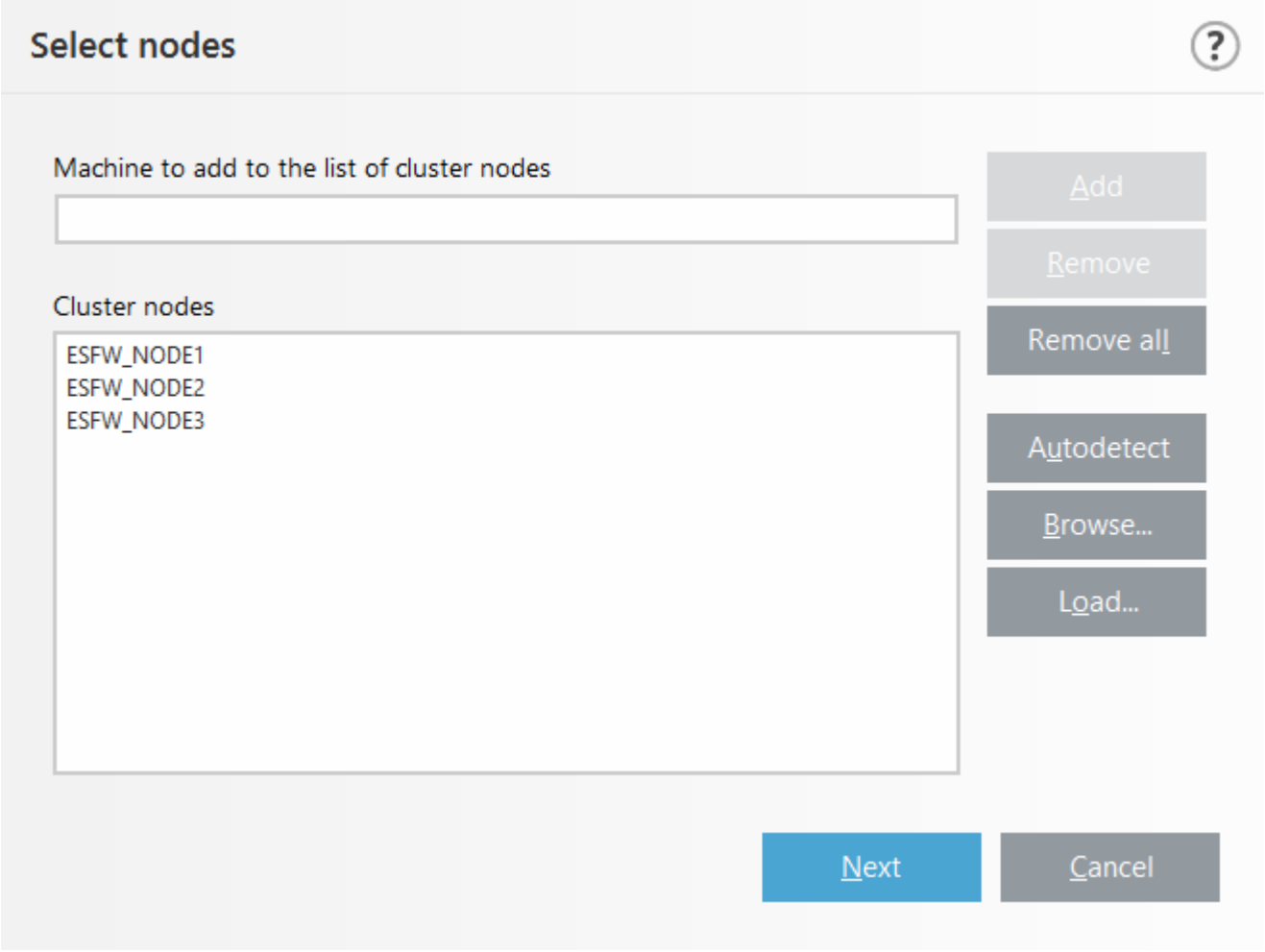
Mevcut bir Windows Failover Cluster / Network Load Balancing (NLB) Cluster Kümesi'nden düğümleri otomatik olarak ekler. Düğümlerin otomatik olarak eklenmesi için, ESET Kümesi oluşturmak üzere kullanmakta olduğunuz sunucunun, bu Windows Failover Cluster / NLB Cluster'nin üyesi olması gerekir. ESET Cluster'nin düğümleri doğru bir şekilde algılaması için NLB Kümesi'nin küme özelliklerinde **Uzaktan denetime izin ver** özelliğinin etkinleştirilmiş olması gerekir. Yeni eklenen düğümlerin listesine sahip olduktan sonra istenmeyenleri kaldırabilirsiniz.

Gözat

Bir Domain veya Workgroup bilgisayarları bulmak ve seçmek için. Bu yöntem, düğümlerin ESET Kümesi'ne manuel olarak eklenmesine olanak tanır. Düğümleri eklemenin bir başka yolu da eklemek istediğiniz sunucunun ana bilgisayar adını yazıp **Ekle**'yi tıklamaktır.

Yükle

Dosyadaki düğümlerin listesini içe aktarmak için.



Listedeki **Küme düğümlerini** değiştirmek için, kaldırmak istediğiniz düğümü seçin ve **Kaldır**'ı tıklatın ya da listeyi tamamen temizlemek için **Tümünü kaldır**'ı tıklatın.

Zaten bir ESET Kümeniz varsa dilediğiniz zaman bu kümeye yeni düğümler ekleyebilirsiniz. Adımlar, tıpkı yukarıda açıklandığı gibidir.

> NOT
> Listede kalan tüm düğümler çevrimiçi ve erişilebilir olmalıdır. Yerel ana bilgisayar, küme düğümlerine varsayılan olarak eklenir.

Küme sihirbazı - Küme ayarları

Küme adını ve ağ özelliklerini tanımlayın (gerekirse).

Küme adı

Kümeniz için bir ad yazın ve **İleri**'yi tıklayın.

Dinleme bağlantı noktası - (varsayılan bağlantı noktası 9777'dir)

Ağ ortamınızda zaten 9777 bağlantı noktasını kullanıyorsanız, kullanılmayan diğer bağlantı noktasını belirtin.

Bağlantı noktasını Windows güvenlik duvarında aç

Seçildiğinde Windows Güvenlik Duvarı'nda bir kural oluşturulur.

Küme sihirbazı - Küme kurulum ayarları

Sertifika dağıtım modunu ve ürünün diğer düğümlere yüklenip yüklenmeyeceğini belirleyin.

Sertifika dağıtımı

- **Otomatik** uzaktan - Sertifika otomatik olarak yüklenir.
- **Manuel** - **Oluştur**'u tıklayın ve sertifikaları depolamak için uygun klasörü seçin. Kök sertifikanın yanı sıra ESET Kümesi'ni ayarlamak için kullandığınız düğüm (yerel makine) dahil olmak üzere her düğüm için bir sertifika oluşturulur. Sertifikayı yerel makineye kaydetmek için **Evet**'i tıklayın

Ürünün diğer düğümlere yüklenmesi

- **Otomatik uzaktan** - ESET Server Security Her düğüme otomatik olarak yüklenir (işletim sistemlerinin aynı mimariye sahip olması koşuluyla).
- **Manuel** - ESET Server Security ürününü manuel olarak yükleyin (örneğin, bazı düğümlerde farklı işletim sistemi mimarilerine sahipseniz).

Etkin ürün olmadan lisansı düğümlere gönder

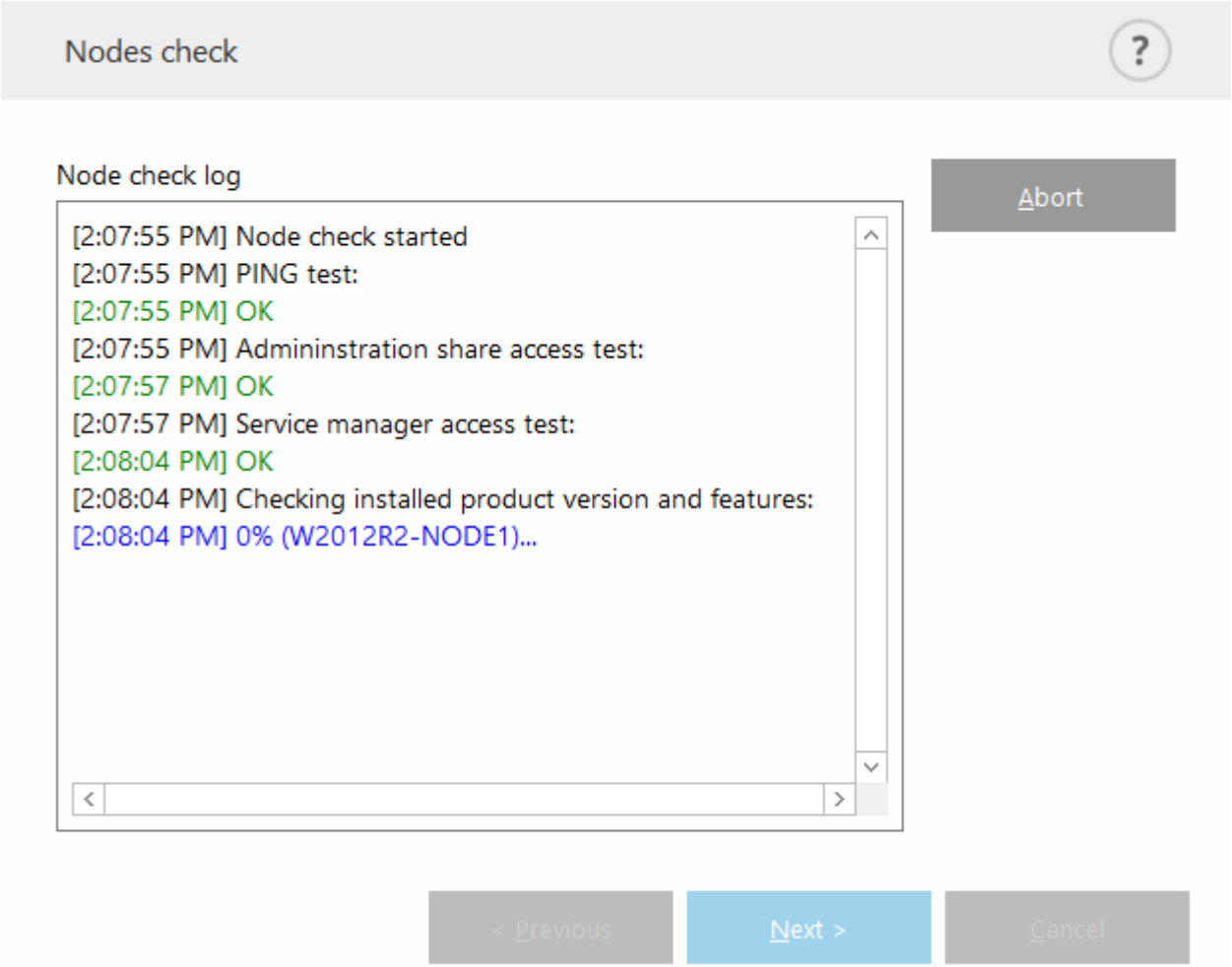
ESET Security, lisanslar olmadan düğümlerde yüklenen ESET Çözümleri'ni otomatik olarak etkinleştirir.

NOT
Karışık işletim sistemi mimarilerine sahip (32 bit ve 64 bit) bir ESET Kümesi oluşturmak istiyorsanız, ESET Server Security ürününü manuel olarak yükleyin. Kullanılan işletim sistemleri sonraki adımlarda algılanır ve siz bu bilgileri, günlük penceresinde görürsünüz.

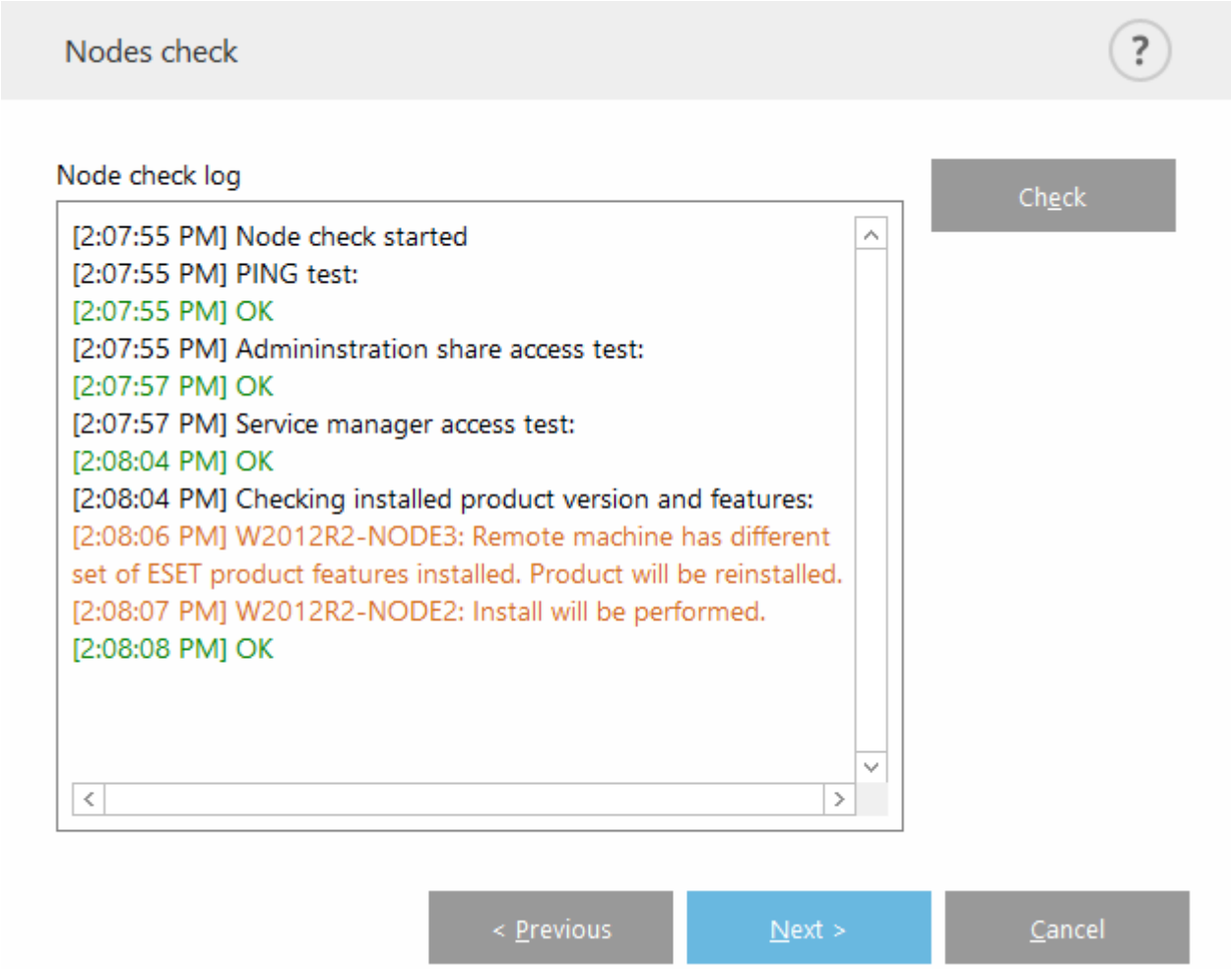
Küme sihirbazı - Düğüm denetimi

Yükleme ayrıntılarının belirlenmesinin ardından düğüm denetimi yapılır. Aşağıdaki bilgiler, **Düğüm deneyim günlüğünde** görüntülenir:

- mevcut tüm düğümlerin çevrimiçi olduğunu doğrula
- yeni düğümlerin erişilebilir olduğunu doğrula
- düğüm çevrimiçi
- yönetici paylaşımı erişilebilir
- uzaktan yürütme mümkün
- doğru ürün sürümleri yüklendi (veya ürün yüklenmedi).
- yeni sertifikaların var olduğunu doğrula

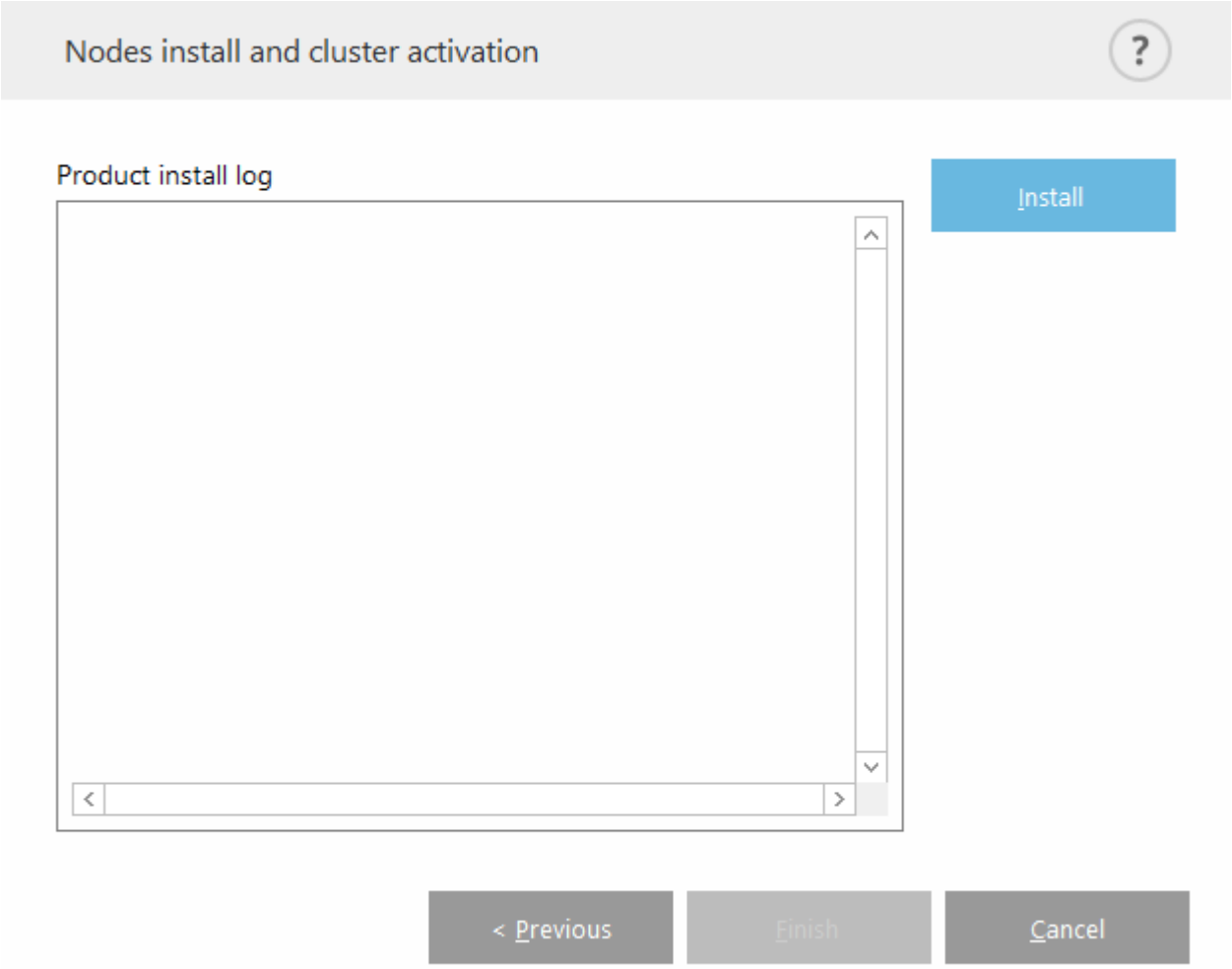


Düğüm denetimi tamamlandıktan sonra rapor görüntülenir:

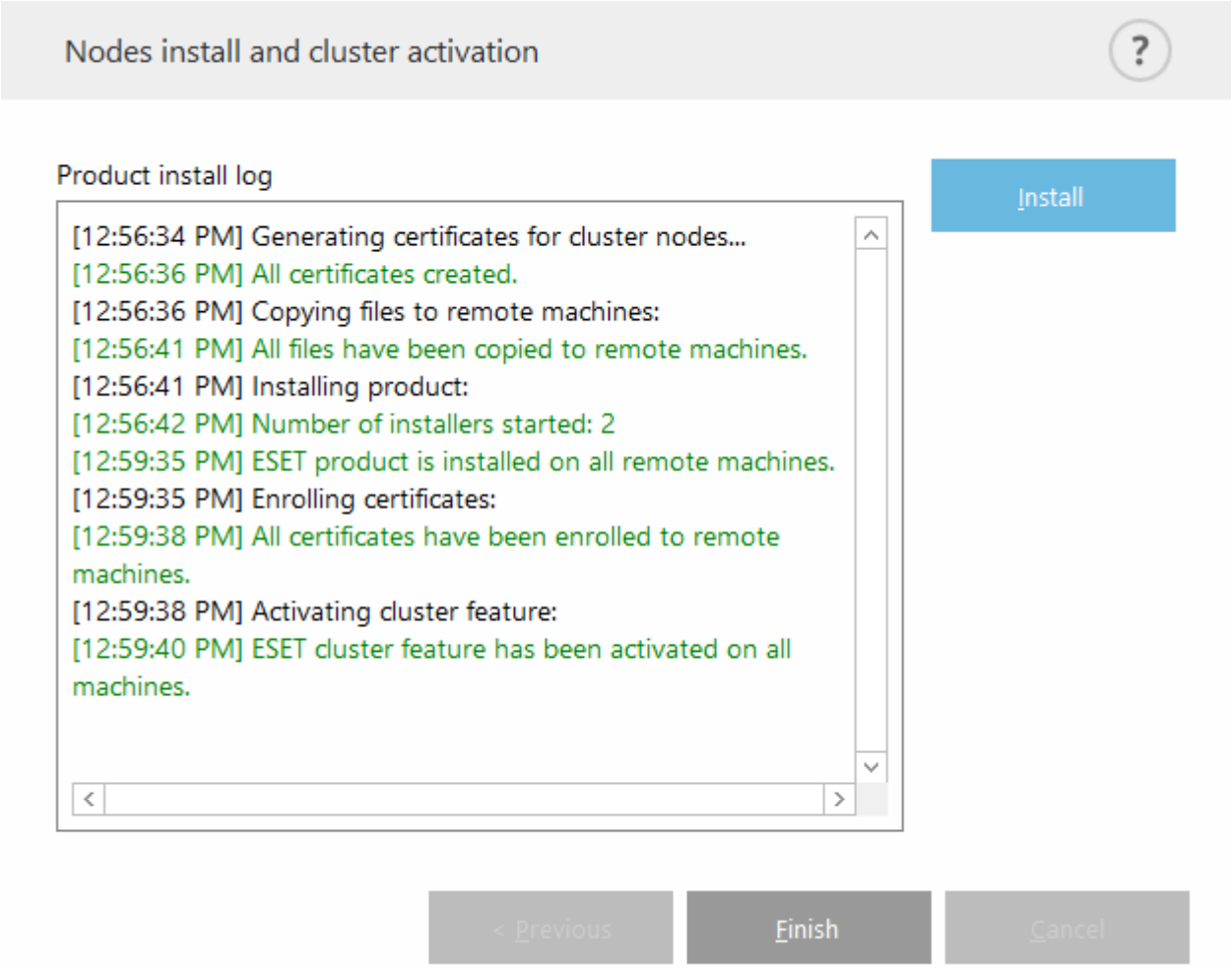


Küme sihirbazı - Düğüm yükleme

ESET Cluster'ın başlatılması sırasında uzak bir makineye yüklerken, sihirbaz *%ProgramData%\ESET\ESET Security\Installer* dizininde yükleyiciyi bulmaya çalışır. Yükleyici paketi burada bulunamazsa, yükleyici dosyasının konumunu bulmanız istenir.

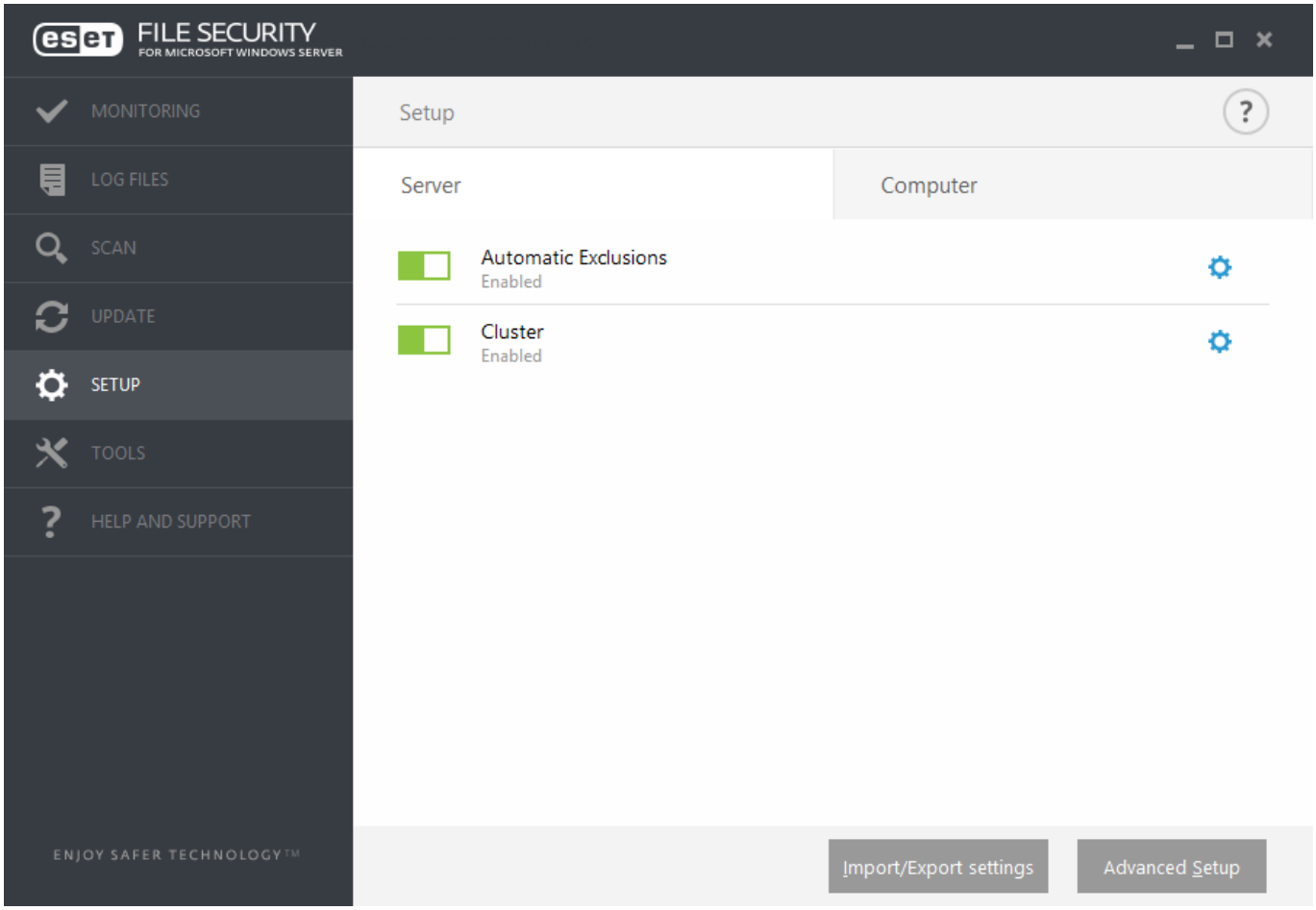


NOT
Farklı bir yapıya (32 bit - 64 bit) sahip bir düğüm için otomatik uzaktan yükleme kullanmaya çalıştığınızda, bu durum algılanır ve manuel yükleme yapmanız istenir.



ESET Kümesi'ni doğru bir şekilde yapılandırmanızın ardından **Ayarlar** > **Sunucu** sayfasında etkin olarak görüntülenir.

NOT
Bazı düğümlerde eski bir ESET Server Security sürümü halihazırda yüklenmişse, söz konusu makinelerde en yeni sürümün kullanılması gerektiği konusunda bildirim alırsınız. ESET Server Security güncellemesi otomatik bir yeniden başlatmaya neden olabilir.



Ayrıca, geçerli durumunu Küme durum sayfasından da kontrol edebilirsiniz (**Araçlar** > **Küme**).

ESET Shell

eShell (ESET Shell kısaltması), ESET Server Security için komut satırı arabirimidir. Grafik kullanıcı arabirimine (GUI) alternatif olarak kullanılır. eShell, normalde GUI'nin size sağladığı tüm özellik ve seçenekleri içerir. eShell, GUI kullanmadan tüm programı yapılandırmanıza ve yönetmenize olanak sağlar.

GUI'de mevcut olan tüm işlev ve özelliklerin yanı sıra bu arabirim; yapılandırma, yaplandırmayı değiştirme veya bir eylem gerçekleştirme amacıyla komutlar çalıştırarak otomasyon özelliğini kullanma seçeneği de sunar. Ayrıca eShell, GUI yerine komut satırı kullanmayı tercih eden kullanıcılar için yararlı olabilir.

> NOT
> Tam işlevsellik için, eShell aracını Yönetici olarak çalıştır özelliğini kullanarak açmanızı öneririz. Bu, Windows Komut İstemi (cmd) üzerinden tek komut çalıştırırken de geçerlidir. Komutu Yönetici olarak çalıştır seçeneğini kullanarak açın. Komut istemini Yönetici olarak çalıştırmamak, izinlerin eksikliği nedeniyle komutları çalıştırmanızı engeller.

eShell aracının çalıştırılabileceği iki mod vardır:

1. **İnteraktif mod** - Yalnızca tek bir komut yürütmek yerine yapılandırmayı değştirme, günlükleri görüntüleme gibi görevler için eShell aracını çalıştırmak istediğinizde, bu seçenek kullanılabilir. Henüz tüm komutlara aşina değilseniz interaktif modu kullanabilirsiniz. İnteraktif mod, eShell aracında gezinme deneyiminizi kolaylaştırır. Belirli bir bağlam içerisinde kullanabileceğiniz komutları size gösterir.

2. **Tek komut / Toplu mod -** eShell interaktif moduna girmeden yalnızca bir komut yürütmeniz gerektiğinde

bu modu kullanabilirsiniz. Bu, Windows Komut İstemi'nde doğru parametrelerle eshell yazarak yapılabilir.

ÖRNEK
`eshell get status` veya `eshell computer set real-time status disabled 1h`

Belirli komutları (örneğin yukarıdaki ikinci örnek) toplu mod/komut dosyası modunda çalıştırmak için, öncelikle yapılandırmanız gereken birkaç ayar vardır. Aksi halde, **Erişim Reddedildi** iletisi alırsınız. Bu, güvenlik açısından gereklidir.

NOT
Ayarlar değişiklikleri, eShell komutlarının Windows Komut İstemi'nden kullanılmasına izin vermek için gereklidir. Toplu dosyaları çalıştırmakla ilgili daha fazla bilgi için burayı tıklatın.

eShell aracında interaktif moda girmenin iki yolu vardır:

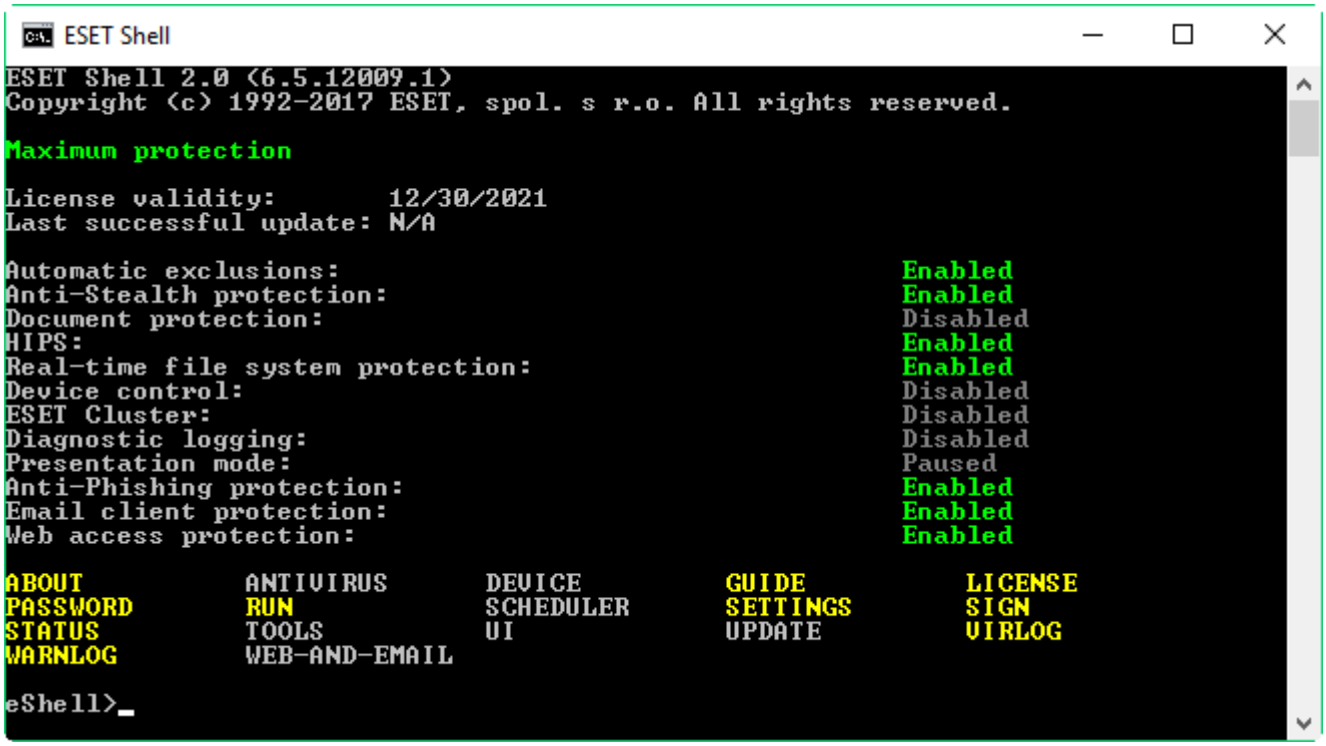
1. **Windows Başlat menüsünden**: Başlat > Tüm Programlar > ESET > ESET File Security > ESET Shell
2. **Windows Komut İstemi**'nde `eshell` yazıp Enter tuşuna basarak

ÖNEMLİ
`'eshell' is not recognized as an internal or external command` hatası alırsanız, bunun nedeni ESET Server Security kurulumunun ardından sisteminiz tarafından yüklenmeyen yeni Ortam Değişkenleridir. Yeni Komut İstemi açıp eShell aracını yeniden başlatmayı deneyin. Yine de hata alıyorsanız veya ESET Server Security Çekirdek yüklemesi varsa, mutlak yolu kullanarak eShell aracını başlatın, örneğin `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` (komutun çalışması için "" kullanmanız gerekir).

eShell aracını ilk kez interaktif modda çalıştırdığınızda, ilk çalıştırma (kılavuz) ekranı gösterilir.

NOT
Gelecekte ilk çalıştırma ekranını görmek istiyorsanız `guide` komutunu yazın. Bu, eShell aracının Sentaks, Önek, Komut yolu, Kısaltılmış biçimler, Takma adlar vs. ile nasıl kullanılacağına yönelik bazı temel örnekler gösterir.

eShell gelecekte yeniden çalıştırdığınızda şu ekranı görürsünüz:



> NOT
> Komutlar büyük-küçük harfe duyarlı değildir. Büyük harf ya da küçük harf kullanmanız fark etmez, komut her iki durumda da çalışır.

eShell'i özelleştirme

eShell yazılımını `ui eshell` bağlamında özelleştirebilirsiniz. Komutlar için takma adları, renkleri, dili, yürütme ilkesini; gizli komutlar için ayarları ve diğer özellikleri yapılandırabilirsiniz.

Kullanım

Sentaks

Komutların işlevlerini yerine getirmesi için doğru sentaks ile biçimlendirilmeleri gerekir. Komutlar; önek, bağlam, argüman, seçenek gibi öğelerden oluşabilir. eShell ürününde kullanılan genel sentaks şu şekildedir:

[<prefix>] [<command path>] <command> [<arguments>]

Örnek (bu, belge özelliğini etkinleştirir):

`SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

- `SET` - önek
- `COMPUTER SCANS DOCUMENT` - belirli bir komutun yolu, bu komutun ait olduğu bağlam
- `REGISTER` - komutun kendisi
- `ENABLED` - komut için bir argüman

`?` kullanımı, söz konusu komut için sentaksı görüntüler. Örneğin, `STATUS ?` , `STATUS` komutu için sentaksı gösterir:

SENTAKS:

```
[get] status
```

İŞLEMLER:

```
get - Tüm koruma modüllerinin durumunu göster
```

`[get]` komutunun köşeli parantez içinde olduğunu fark edebilirsiniz. Bu, `get` komutunun `status` komutu için varsayılan olduğunu gösterir. Başka bir ifadeyle, herhangi bir önek belirtmeden `status` komutunu yürütürseniz gerçekte varsayılan öneki kullanır (bu örnekte `get status`). Önek olmadan komutları kullanmak, yazarken zaman kazandırır. Genellikle, `get` çoğu komut için varsayılan önektir, ancak belirli bir komut için varsayılan önekin ne olduğunu ve bunun tam olarak yürütmek istediğiniz öğe olduğunu kesin olarak bilmeniz gerekir.

> NOT
> Komutlar büyük-küçük harfe duyarlı değildir. İster büyük harf ister küçük harf kullanın, komut bunlardan bağımsız olarak çalışır.

Önek / İşlem

Önek, bir işlemdir. `GET` öneki, ESET Server Security ürününün belirli bir özelliğinin nasıl yapılandırıldığı hakkında size bilgi verir veya durumu gösterir (örneğin `GET COMPUTER REAL-TIME STATUS` komutu mevcut koruma durumunu gösterir). `SET` öneki, işlevini yapılandırır veya durumunu değiştirir (`SET COMPUTER REAL-TIME STATUS ENABLED` korumayı etkinleştirir).

Bunlar, eShell aracının kullanmanıza olanak sağladığı öneklerdir. Bir komut, bu öneklerden herhangi birini destekliyor olabilir veya olmayabilir.

GET	geçerli ayarı/durumu döndürür
SET	değer/durum ayarlar
SELECT	bir öğeyi seçer
ADD	bir öğe ekler
REMOVE	bir öğeyi kaldırır
CLEAR	tüm öğeleri/dosyaları kaldırır
START	bir eylem başlatır
STOP	bir eylemi durdurur
PAUSE	bir eylemi duraklatır
RESUME	bir eylemi sürdürür
RESTORE	varsayılan ayarlar/nesne/dosyayı geri yükler
SEND	nesne/dosya gönderir
IMPORT	bir dosyayı içe aktarır
EXPORT	bir dosyaya aktarır

> NOT
> `GET` Ve `SET` gibi önekler birçok komutla kullanılır, ancak bazı komutlarda (örneğin `EXIT`) önek kullanılmaz.

Komut yolu / Bağlam

Komutlar, bir ağaç yapısı oluşturan bağlamlarda yer alır. Ağacın en üst düzeyi köktür. eShell aracını çalıştırdığınızda kök düzeydesinizdir:

```
eShell>
```

Buradan bir komutu yürütebilir veya ağaç içerisinde gezinmek için bağlam adını girebilirsiniz. Örneğin, `TOOLS` bağlamını girdiğinizde, burada mevcut olan tüm komutlar ve alt bağlamlar listelenir.

Sarı öğeler, yürütebileceğiniz komutlar; gri öğelerse girebileceğiniz alt bağlamlardır. Alt bağlam, başka komutları içerir.

Daha yüksek bir düzeye geri dönmeniz gerekirse `..` seçeneğini (iki nokta) kullanın.

> ÖRNEK
> Örneğin şurada olduğunuzu varsayalım:
> `eShell computer real-time>`
> `..` yazdığınızda bir düzey yukarı, yani şu konuma gidersiniz:
> `eShell computer>`

`eShell computer real-time>` Antivirus startup> komutundan köke geri dönmek isterseniz (komut kökten iki düzey aşağıda yer alır) `.. ..` (iki nokta boşluk iki nokta) yazmanız yeterlidir. Böylece iki düzey yukarı çıkararak köke ulaşmış olursunuz. `\` ters eğik çizgiyi kullanarak, bağlam ağacının ne kadar derininde bulunursanız bulunun, herhangi bir düzeyden doğrudan köke dönebilirsiniz. Daha üst düzeylerde belirli bir bağlama gitmek isterseniz, ulaşmak istediğiniz düzeye uygun olarak gereken sayıda `..` komutu girin ve ayırıcı olarak boşluk kullanın. Örneğin üç düzey yukarı çıkmak istiyorsanız, şu komutu kullanın: `.. .. ..`

Yol, geçerli bağlamla ilişkilidir. Komut, geçerli bağlamda yer alıyorsa, yol girmeyin. Örneğin,`GET COMPUTER REAL-TIME STATUS`komutunu yürütmek için şunu girin:

- `GET COMPUTER STATUS` - kök bağlamdaysanız (komut satırı şunu gösterir `eShell>`
- `GET STATUS` - bağlamdaysanız `COMPUTER` (komut satırı şunu gösterir `eShell computer>`)
- `.. GET STATUS` - bağlamdaysanız `COMPUTER REAL-TIME` (komut satırı şunu gösterir `eShell computer real-time>`)

İki nokta `..` yerine `.` tek nokta (nokta) kullanabilirsiniz. Tek nokta, iki noktanın kısaltılmışıdır.

```
ÖRNEK
. GET STATUS - bağlamdaysanız COMPUTER REAL-TIME (komut satırı şunu gösterir eShell computer
real-time>)
```

Argüman

Argüman, belirli bir komut için gerçekleştirilen bir eylemdir. Örneğin, komut `CLEAN-LEVEL` (`COMPUTER REAL-TIME ENGINE` içinde bulunur) aşağıdaki argümanlarla birlikte kullanılabilir:

`rigorous` - Algılamayı her zaman düzelt
`safe` - Güvenliyse algılamayı düzelt, aksi takdirde olduğu gibi bırak
`normal` - Güvenliyse algılamayı düzelt, aksi takdirde sor
`none` - Her zaman son kullanıcıya sor

Başka bir örnek `ENABLED` veya `DISABLED` argümanlarıdır ve bunlar, belirli bir özelliği veya işlevi etkinleştirmek ya da devre dışı bırakmak için kullanılır.

Kısaltılmış biçim / Kısa komutlar

eShell; bağlamları, komutları ve argümanları (argümanın bir düğme veya alternatif seçenek olması şartıyla) kısaltmanıza olanak sağlar. Bir sayı veya yol gibi somut değer olan önek veya argüman kısaltılamaz. Etkinleştirildi ve devre dışı bırakıldı argümanları yerine `1` ve `0`rakamlarını kullanabilirsiniz.

```
ÖRNEK
computer set real-time status enabled    =>   com set real stat 1
computer set real-time status disabled    =>   com set real stat 0
```

Kısa biçim örnekleri:

```
ÖRNEK
computer set real-time status enabled    =>   com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext    =>   com
excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1    =>   com excl rem det 1
```

İki komut veya bağlamın aynı harflerle başlaması halinde (örneğin `ADVANCED` ve `AUTO-EXCLUSIONS` kısaltılmış komut olarak `A` girersiniz), eShell aracı, komutlardan hangisini çalıştırmak istediğinize karar veremez. Bir hata iletisi görüntülenir ve aralarından seçim yapabileceğiniz "A" ile başlayan komutlar listelenir:

```
eShell>a

The following command is not unique: a
```

`COMPUTER` bağlamında aşağıdaki alt bağlamlar kullanılabilir:

`ADVANCED`

`AUTO-EXCLUSIONS`

Bir veya daha çok harf ekleyerek (örneğin sadece A yerine AD) eShell, artık benzersiz olduğu için ADVANCED alt bağlamına girer. Aynısı kısaltılmış komutlar için de geçerlidir.

> NOT
> Bir komutun sizin ihtiyacınız olan şekilde yürütüldüğünden emin olmak istiyorsanız, komutları, argümanları vs. kısaltmadan tam biçimi kullanmanızı öneririz. Bu şekilde, eShell tam istediğiniz biçimde yürütülür ve istenmeyen hatalar engellenir. Bu, özellikle toplu dosyalar / komut dosyaları için geçerlidir.

Otomatik tamamlama

eShell 2.0 ürününde sunulmuş olan bu yeni özellik, Windows Komut İsteği'ndeki otomatik tamamlama özelliğine çok benzer. Windows Komut İstemi dosya yollarını tamamlarken, eShell komut, bağlam ve işlem adlarını da tamamlar. Argüman tamamlama desteklenmemektedir. Komutu yazarken tamamlamak veya mevcut varyasyonlar arasından seçim yapmak için Tab tuşuna basmanız yeterlidir. Geriye doğru gitmek için Shift + Tab kombinasyonuna basın. Kısaltılmış biçimi ve otomatik doldurma işlevini karıştırma özelliği desteklenmemektedir. Bunlardan yalnızca birini kullanın. Örneğin, computer real-time additional yazdığınızda Tab tuşuna basarsanız bir işlem gerçekleştirilmez. Bunun yerine com yazıp ardından computer komutunu tamamlamak için TAB tuşuna basın, real + Tab ve add + Tab yazmaya devam edin. Mevcut tüm varyasyonlarda gezinmek için on + Tab yazın ve Tab tuşuna basmaya devam edin: on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default vb.

Takma adlar

Takma ad, bir komutu yürütmek için kullanılabilen alternatif addır (komutun atanmış bir takma adı olması şartıyla). Birkaç varsayılan takma ad bulunmaktadır:

(global) close - çıkış
(global) quit - çıkış
(global) bye - çıkış
warnlog - araçlar günlük olayları
virlog - araçlar günlük algılamaları

"(global)", komutun geçerli bağlamı ne olursa olsun herhangi bir yerde kullanılabileceği anlamına gelir. Bir komuta atanan birden fazla takma ad olabilir, örneğin EXIT komutu CLOSE, QUIT ve BYE gibi diğer adlara sahip olabilir. eShell aracından çıkmak istediğinizde EXIT komutunun kendisini veya diğer adlarından herhangi birini kullanabilirsiniz. VIRLOG adı, DETECTIONS komutunun diğer adıdır ve TOOLS LOG bağlamında bulunur. Bu şekilde detections komutu ROOT bağlamından kullanılabilir ve erişim daha kolaydır (TOOLS komutunu girdikten sonra LOG bağlamını girmeniz gerekmez, doğrudan ROOT bağlamından çalıştırabilirsiniz).

eShell, kendi takma adlarınızı tanımlamanıza olanak sağlar. ALIAS komutu UI ESHELL bağlamında bulunabilir.

Parola koruma ayarlar

ESET Server Security ayarları parolayla korunabilir. GUI kullanarak bir parola veya set ui access lock-password kullanarak eShell belirleyebilirsiniz. Belirli komutlar için (örneğin ayarları veya verileri değiştiren komutlar) bu parolayı interaktif bir şekilde girmeniz gerekecektir. Uzun bir süre boyunca eShell ile çalışmayı planlıyor ve parolayı tekrar tekrar girmek istemiyorsanız, set password komutunu kullanarak (root öğesinden yürütün) eShell aracının parolayı hatırlamasını sağlayabilirsiniz. Parolanız parola gerektiren yürütülen her komut için otomatik olarak doldurulur. eShell aracından çıkana kadar hatırlanır. Bu, yeni bir oturum başlattığınızda ve eShell aracının parolanızı hatırlamasını istediğinizde tekrar set password komutunu kullanmanız gerekeceği anlamına gelir.

Kılavuz / Yardım

`GUIDE` veya `HELP` komutunu çalıştırdığınızda eShell aracının nasıl kullanılacağını açıklayan bir "ilk çalıştırma" ekranı görüntülenir. Bu komut yalnızca `ROOT` bağlamında bulunabilir (`eShell>`).

Komut geçmişi

eShell, daha önce yürütülen komutların geçmişini tutar. Bu, yalnızca halihazırdaki interaktif eShell oturumu için geçerlidir. eShell aracından çıktığınızda komut geçmişi atılır. Geçmişte gezinmek için klavyenizin Yukarı ve Aşağı ok tuşlarını kullanın. Aradığınız komutu bulduktan sonra, tüm komutu baştan yazmaya gerek kalmadan onu yeniden yürütebilir veya üzerinde değişiklik yapabilirsiniz.

CLS / Ekranı temizle

`CLS` komutu, ekranı temizlemek için kullanılabilir. Windows Komut İstemi veya benzer komut satırı arabirimleriyle aynı şekilde çalışır.

EXIT / CLOSE / QUIT / BYE

eShell aracını kapatmak veya araçtan çıkmak için, şu komutlardan herhangi birini kullanabilirsiniz (`EXIT`, `CLOSE`, `QUIT` veya `BYE`).

Komutlar

Bu bölümde birkaç temel eShell komutu açıklamalarla birlikte listelenmektedir.

> NOT
> Komutlar büyük-küçük harfe duyarlı değildir. İster büyük harf ister küçük harf kullanın, komut bunlardan bağımsız olarak çalışır.

Örnek komutlar (ROOT bağlamında yer alır):

HAKKINDA

Program ile ilgili bilgileri listeler. Aşağıdaki türden bilgileri gösterir:

- Yüklenen ESET güvenlik ürününüzün adı ve sürüm numarası.
- İşletim sistemi ve temel donanım ayrıntıları.
- Kullanıcı adı (etki alanı dahil), Tam bilgisayar adı (sunucunuz bir etki alanının üyesiyse FQDN) ve Erişim hakkı adı.
- Her bir bileşenin sürüm numarası dahil ESET güvenlik ürününüzün yüklenen bileşenleri.

BAĞLAM YOLU:

```
root
```

PAROLA

Normalde parolayla korunan komutları yürütmek için güvenlik nedenlerinden ötürü bir parola girmeniz istenir. Bu, korumasını devre dışı bırakan ve ESET Server Security yapılandırmasını etkileyebilecek olan komutlar türündeki

komutlar için geçerlidir. Bu tür komutu yürütmek istediğiniz her defasında parola istenir. Parolayı her defasında girmemek için bu parolayı tanımlayabilirsiniz. eShell tarafından hatırlanır ve parola korumalı bir komut yürütüldüğünde otomatik olarak girilir.

> NOT
> Parolanız, yalnızca halihazırdaki eShell interaktif oturumu için geçerlidir. eShell aracından çıktığınızda tanımlanan parola atılır. eShell aracını tekrar başlattığınızda, parolanın yeniden tanımlanması gerekir.

Tanımlanan parola, imzalanmamış dosyalar veya komut dosyaları çalıştırılırken de kullanılabilir. İmzalanmamış toplu dosyaları çalıştırırken ESET Shell yürütme ilkesini Tam erişim olarak ayarlamayı unutmayın. Aşağıda bu tür bir toplu dosya için örnek bulabilirsiniz:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Yukarıdaki sıralanan komut parolayı tanımlar ve korumayı devre dışı bırakır.

> ÖNEMLİ
> Mümkün olduğu sürece imzalı toplu dosyaları kullanmanızı öneririz. Bu şekilde, toplu dosyada düz metin parolaları olmaz (yukarıda açıklanan yöntem kullanılırsa). Diğer ayrıntılar için Toplu dosyalar / Komutlar (İmzalı toplu dosyalar) bölümüne bakın.

BAĞLAM YOLU:

`root`

SENTAKS:

`[get] | restore password`

`set password [plain <password>]`

İŞLEMLER:

- `get` - Parolayı göster
- `set` - Parola ayarla veya temizle
- `restore` - Parolayı temizle

ARGÜMANLAR:

- `plain` - Parolayı parametre olarak girmek için değiştir
- `password` - Parola

ÖRNEKLER:

- `set password plain <yourpassword>` - Parola korumalı komutlar için kullanılacak olan parolayı ayarlar
- `restore password` - Parolayı temizler

ÖRNEKLER:

- `get password` - Bunu, parolanın yapılandırılmış olup olmadığını görmek için kullanın (parolanın kendisi değil, yalnızca "*" yıldızları gösterilir); hiçbir yıldız olmaması, ayarlanmış bir parola bulunmadığı anlamına gelir

`set password plain <yourpassword>` - Tanımlanmış parola ayarlamak için bunu kullanın

`restore password` - Bu komut tanımlanan parolayı temizler

DURUM

ESET Server Security ürününün geçerli gerçek zamanlı koruma durumu hakkında bilgiler gösterir, ayrıca korumayı duraklatmanıza / devam ettirmenize olanak tanır (GUI ile benzer bir şekilde).

BAĞLAM YOLU:

```
computer real-time
```

SENTAKS:

```
[get] status
set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]
restore status
```

İŞLEMLER:

`get` - geçerli ayarı/durumu döndürür

`set` - değeri/durumu ayarlar

`restore` - varsayılan ayarları/nesneyi/dosyayı geri yükler

ARGÜMANLAR:

`enabled` - Korumayı/özelliği etkinleştir

`disabled` - Korumayı/özelliği devre dışı bırak

`10m` - 10 dakikalığına devre dışı bırak

`30m` - 30 dakikalığına devre dışı bırak

`1h` - 1 saatliğine devre dışı bırak

`4h` - 4 saatliğine devre dışı bırak

`temporary` - Yeniden başlatılıncaya kadar devre dışı bırak

> NOT
> Tüm koruma özelliklerini tek bir komutla devre dışı bırakmak mümkün değildir. `status` komutunu kullanarak koruma özelliklerini ve modüllerini tek tek yönetebilirsiniz. Her koruma özelliği veya modülünün kendi `status` komutu vardır.

`status` komutlu özelliklerin listesi:

Özellik	Bağlam ve komut
Otomatik dışlamalar	`COMPUTER AUTO-EXCLUSIONS STATUS`

Özellik	Bağlam ve komut
Host Tabanlı Saldırı Önleme Sistemi (HIPS)	`COMPUTER HIPS STATUS`
Gerçek zamanlı dosya sistemi koruması	`COMPUTER REAL-TIME STATUS`
Cihaz Kontrolü	`DEVICE STATUS`
Botnet koruması	`NETWORK ADVANCED STATUS-BOTNET`
Ağ saldırısına karşı koruma (IDS)	`NETWORK ADVANCED STATUS-IDS`
Ağ yalıtımı	`NETWORK ADVANCED STATUS-ISOLATION`
ESET Kümesi	`TOOLS CLUSTER STATUS`
Tanı amaçlı günlüğe kaydetme	`TOOLS DIAGNOSTICS STATUS`
Sunum modu	`TOOLS PRESENTATION STATUS`
Kimlik Avı Koruması	`WEB-AND-EMAIL ANTIPHISHING STATUS`
E-posta istemci koruması	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Web erişimi koruması	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

`DETECTIONS` komutu için bir takma addır. Algılanan sızıntılarla ilgili bilgileri görüntülemeniz gerektiğinde bu seçenek kullanılabilir.

WARNLOG

`EVENTS` komutu için bir takma addır. Çeşitli olaylar hakkındaki bilgileri görüntülemeniz gerektiğinde bu seçenek kullanılabilir.

Toplu dosyalar / Komut dosyası

eShell aracını, otomasyon için güçlü bir komut dosyası aracı olarak kullanabilirsiniz. eShell ile toplu dosya kullanmak için eShell ile bir dosya ve bu dosya içinde bir komut oluşturun.

```
ÖRNEK
eshell get computer real-time status
```

Ayrıca komutları zincirleyebilirsiniz. Bu, bazı durumlarda gerekli olur. Örneğin belirli bir zamanlanmış görev türünü girmek istediğinizde şunu yazın:

```
eshell select scheduler task 4 "&" get scheduler action
```

Öğe seçimi (bu durumda 4 numaralı görev) genellikle yalnızca halihazırda çalışan eShell örneği için geçerlidir. Bu iki komutu birbiri ardına çalıştırmanız gerekirse, ikinci komut "Hiçbir görev seçilmedi veya seçilen görev artık mevcut değil" hatasını verir.

Güvenlik nedenlerinden ötürü, yürütme ilkesi varsayılan olarak **Sınırlı Komut Dosyası** şeklinde ayarlanmıştır. Bu, eShell ürününü izleme aracı olarak kullanmanıza olanak sağlar, ancak bir komut dosyası çalıştırarak ESET Server Security yapılandırmasında değişiklikler yapmanıza izin vermez. Güvenliği etkileyebilecek komutlar içeren bir komut dosyasını yürütmeye çalışırsanız, (örneğin korumayı devre dışı bırakarak) **Erişim Engellendi** iletisi görüntülenir. Yapılandırma ayarlarını yapan komutları yürütmek için imzalanmış toplı dosyaları kullanmanızı öneririz.

Windows Komut İstemi'nde manuel olarak girilen tek bir komut kullanarak yapılandırmayı değiştirmek için, eShell

aracına tam erişim sağlamalısınız (önerilmez). Tam erişim vermek için doğrudan eShell interaktif modundan veya **Gelişmiş ayarlar** (**F5**)> **Kullanıcı arabirimi** > ESET Shell üzerinden `ui eshell shell-execution-policy` komutunu kullanın.

İmzalı toplu dosyalar

eShell, ortak toplu dosyaların (*.bat) güvenliğini bir imzayla sağlamanıza olanak verir. Komut dosyaları, ayarlar koruması için kullanılan aynı parolayla imzalanır. Bir komut dosyasını imzalamak için öncelikle ayarlar korumasını etkinleştirmeniz gerekir. Bunu GUI üzerinden veya eShell içerisinde `set ui access lock-password` komutunu kullanarak yapabilirsiniz. Ayarlar koruması parolası ayarlandıktan sonra toplu dosyaları imzalamaya başlayabilirsiniz.

> NOT
> Ayarlar koruması parolanızı değiştirirseniz, tüm komut dosyalarını yeniden imzalamanız gerekir, aksi halde komut dosyaları, parola değişikliğinin ardından yürütülmez. Komut dosyası imzalanırken girilen parola, hedef sistemdeki ayarlar koruması parolasıyla eşleşmelidir.

Toplu dosyayı imzalamak için `sign <script.bat>` komutunu eShell aracının kök bağlamından çalıştırın. Buradaki *script.bat* imzalamak istediğiniz komut dosyasının yoludur. İmzalama için kullanılacak olan parolayı girin ve onaylayın. Bu parola, ayarlar koruması parolasıyla eşleşmelidir. İmza, bir yorum biçiminde toplu dosyanın sonuna yerleştirilir. Bu komut dosyası daha önceden imzalanmışsa imza yenisiyle değiştirilir.

> NOT
> Önceden imzalanmış bir toplu dosyayı değiştirdiğinizde yeniden imzalanması gerekir.

İmzalı toplu dosyayı Windows Komut İstemi'nden yürütmek veya zamanlanmış bir görev olarak çalıştırmak için şu komutu kullanın:

```
eshell run <script.bat>
```

Burada script.bat toplu dosyanın yoludur.

> ÖRNEK
> `eshell run d:\myeshellscript.bat`

ESET SysInspector

ESET SysInspector, bilgisayarınızın tamamını inceleyen ve yüklü sürücü ve uygulamalar, ağ bağlantıları veya önemli kayıt defteri girişleri gibi sistem bileşenleri hakkında ayrıntılı bilgiler toplayan ve her bileşenin risk düzeyini değerlendiren bir uygulamadır. Bu bilgiler, yazılım veya donanım uyumsuzluğundan ya da kötü amaçlı yazılımın etkilemesinden kaynaklanabilecek şüpheli sistem davranışının nedenini belirlemenize yardımcı olabilir.

Oluştur'u tıklayın ve oluşturulacak günlüğü açıklayan kısa bir **Yorum** girin. ESET SysInspector günlüğü oluşturuluncaya kadar bekleyin (durum Oluşturuldu olarak görünür). Günlük oluşturma, donanım yapılandırmanıza ve sistem verilerinize bağlı olarak biraz zaman alabilir.

ESET SysInspector penceresinde oluşturulan günlüklerle ilgili olarak şu bilgiler görüntülenir:

- **Saat** - Günlük oluşturma zamanı.

- **Yorum** - Kısa bir yorum.
- **Kullanıcı** - Günlüğü oluşturan kullanıcının adı.
- **Durum** - Günlük oluşturma durumu.

Kullanılabilir eylemler şunlardır:

- **Göster** - Oluşturulan günlüğü açar. Ayrıca belirli bir günlük dosyasını sağ tıklayıp içerik menüsünden Göster'i seçebilirsiniz.
- **Karşılaştır** - Var olan iki günlüğü karşılaştırır.
- **Oluştur** - Yeni bir günlük oluşturur. Oluşturulacak günlüğü açıklayan kısa bir yorum girin ve Oluştur'u tıklayın. ESET SysInspector günlüğü tamamlanıncaya kadar lütfen bekleyin (Durum bölümünde Oluşturuldu olarak görünür).
- **Sil** - Seçili günlükleri listeden çıkarır.

Bir veya daha fazla seçili günlük sağ tıklatıldıktan sonra, aşağıdaki seçenekler içerik menüsünden kullanılabilir:

- **Göster** - Seçili günlüğü ESET SysInspector içinde açar (bir günlüğü çift tıklatmakla aynı işlevdir).
- **Karşılaştır** - Var olan iki günlüğü karşılaştırır.
- **Oluştur -** Yeni bir günlük oluşturur. Oluşturulacak günlüğü açıklayan kısa bir yorum girin ve **Oluştur**'u tıklayın. ESET SysInspector günlüğü tamamlanıncaya kadar lütfen bekleyin (**Durum** bölümünde Oluşturuldu olarak görünür).
- **Sil** - Seçili günlükleri listeden çıkarır.
- **Tümünü sil** - Tüm günlükleri siler.
- **Dışa aktar** - Günlüğü .xml dosyası veya sıkıştırılmış .xml dosyasına aktarır.

ESET SysRescue Live

ESET SysRescue Live, önyüklenebilir bir kurtarma CD/DVD'si veya USB sürücüsü oluşturmanıza olanak tanıyan ücretsiz bir yardımcı programdır. Etkilenmiş bir bilgisayarı Kurtarma medyanızdan önyükledikten sonra zararlı yazılım için tarayabilir ve etkilenmiş dosyaları temizleyebilirsiniz.

ESET SysRescue Live uygulamasının başlıca avantajı, ESET Security çözümünün diske ve dosya sistemine doğrudan erişime sahip olurken ana bilgisayar işletim sisteminden bağımsız şekilde çalışmasıdır. Böylece, normalde silinemeyen (ör. işletim sistemi çalıştırılırken vb.) tehditleri kaldırmak mümkün olabilir.

Zamanlayıcı

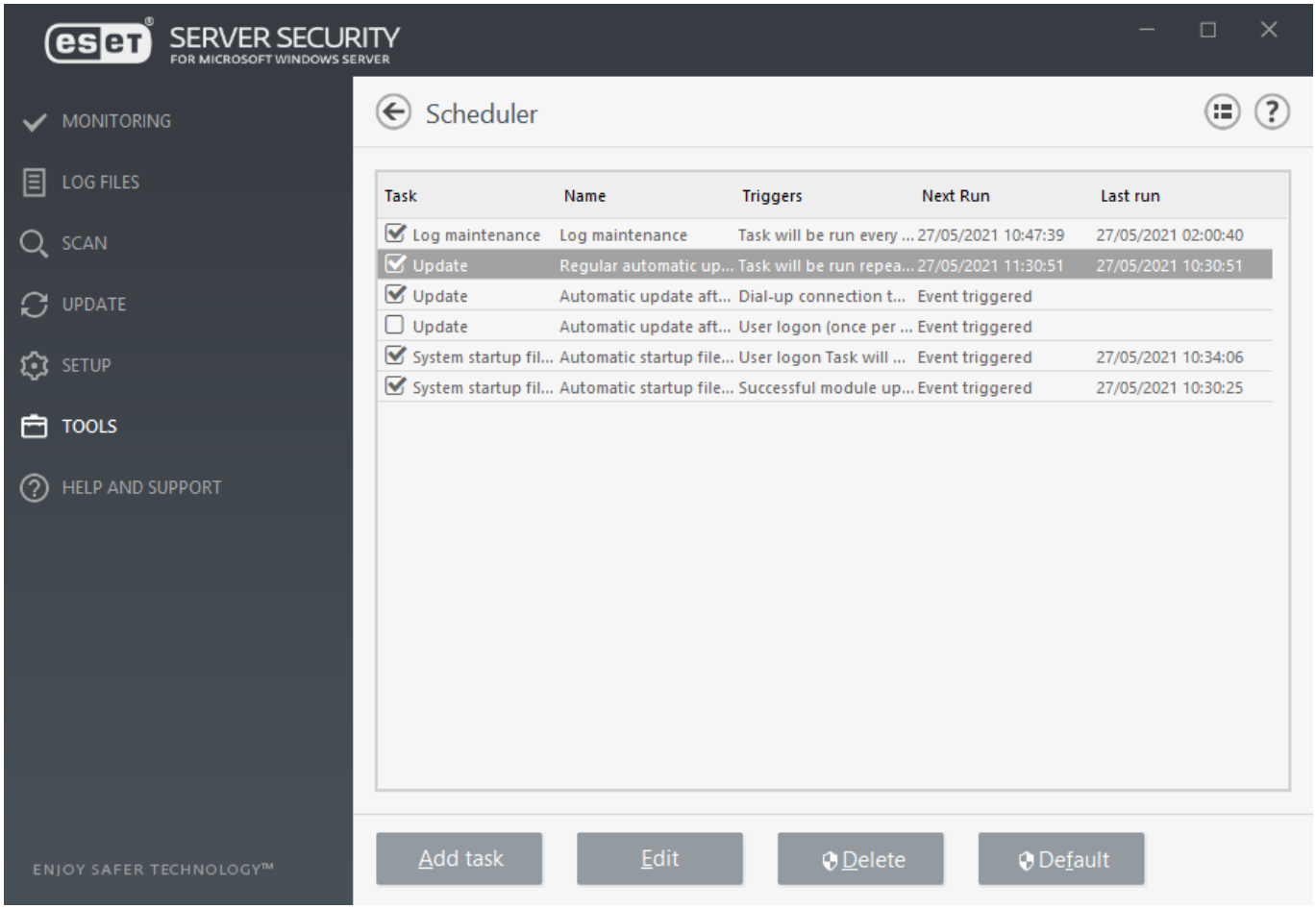
Zamanlayıcı, tanımlanan parametrelere göre zamanlanan görevleri yönetir ve başlatır. Zamanlanan tüm görevlerin listesini bir tablo biçiminde görebilirsiniz; burada Görev türü ve adı, başlatma zamanı ve gerçekleştirilen son çalıştırma gibi görevlere ait parametreler gösterilir. Ayrıca Görev ekle'yi tıklayarak yeni zamanlanan görevler de oluşturabilirsiniz. Mevcut bir zamanlanan görevin yapılandırmasını düzenlemek için **Düzenle** düğmesini tıklayın. Zamanlanan görevler listesini varsayılan ayarlarına geri döndürmek için **Varsayılan**'ı, ardından **Varsayılana döndür**'ü tıklayın. Bunun üzerine yapılan tüm değişiklikler silinir ve bu işlem geri alınamaz.

Önceden tanımlanmış bir dizi varsayılan görev bulunur:

- Günlük bakımı
- Düzenli otomatik güncelleme (güncelleme sıklığını değiştirmek için bu görevi kullanın)
- Çevirmeli bağlantıdan sonra otomatik güncelleme

- Kullanıcı oturum açtıktan sonra otomatik güncelleme
- Başlangıçta otomatik dosya denetimi (kullanıcı oturum açtıktan sonra)
- Başlangıçta otomatik dosya denetimi (modüller başarıyla güncellendikten sonra)

NOT
Görevleri etkinleştirmek veya devre dışı bırakmak için uygun onay kutularını seçin.



Aşağıdaki eylemleri gerçekleştirmek için, bir görevi sağ tıklayın:

Görev ayrıntılarını göster	Zamanlanan bir görevi çift tıkladığınızda veya sağ tıkladığınızda zamanlanan görev hakkında ayrıntılı bilgiler görüntüler.
Şimdi çalıştır	Seçilen bir zamanlayıcı görevini çalıştırır ve görevi hemen gerçekleştirir.
Ekle...	Yeni bir zamanlayıcı görevi oluşturmanıza yardımcı olacak bir sihirbazı başlatır.
Düzenle...	Mevcut bir zamanlanan görevin (hem varsayılan hem de kullanıcı tanımlı) yapılandırmasını düzenler.
Sil	Mevcut bir görevi siler.

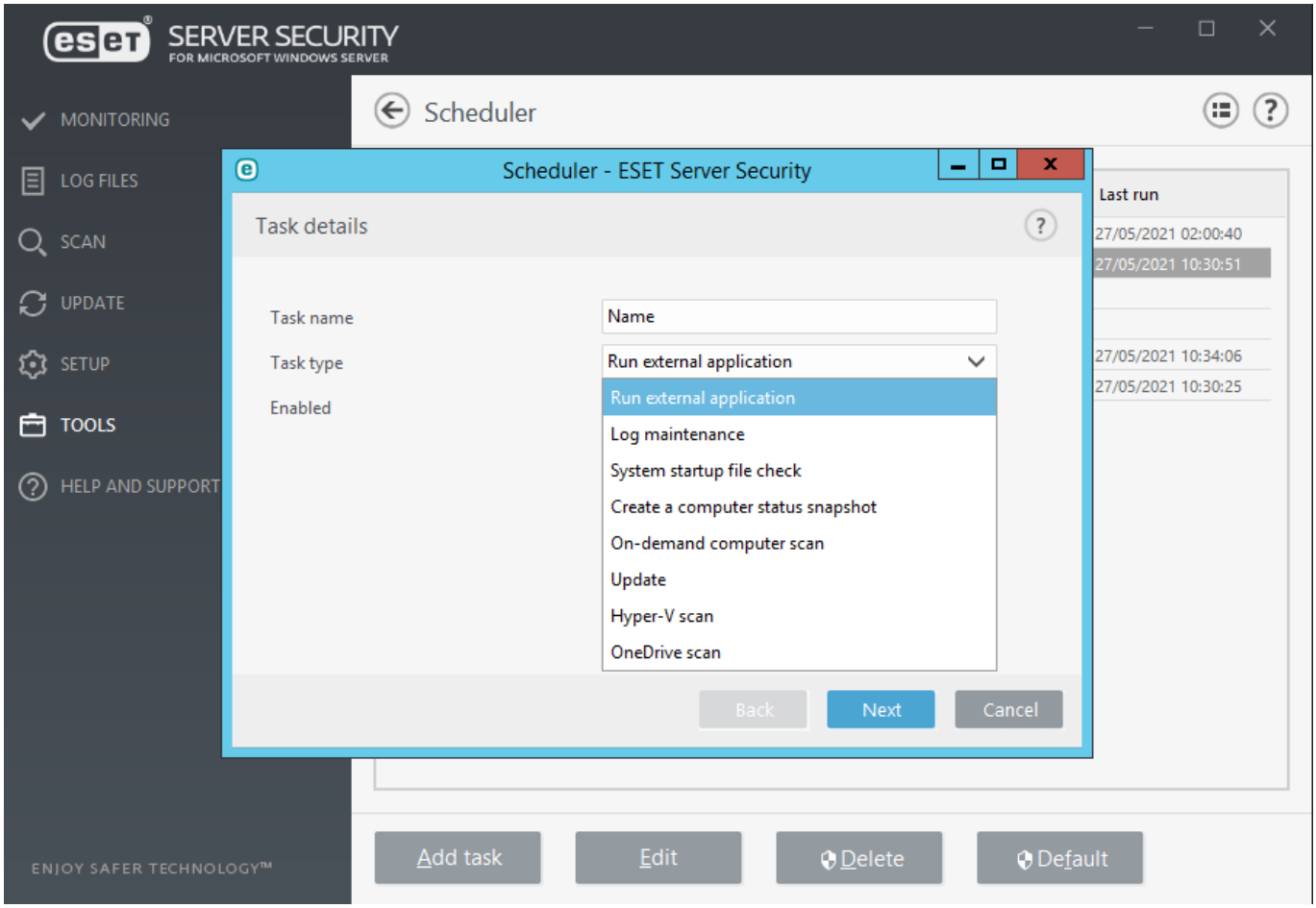
Zamanlayıcı - Görev ekle

Yeni bir zamanlanan görev oluşturmak için:

1. **Görev ekle** seçeneğini tıklayın.

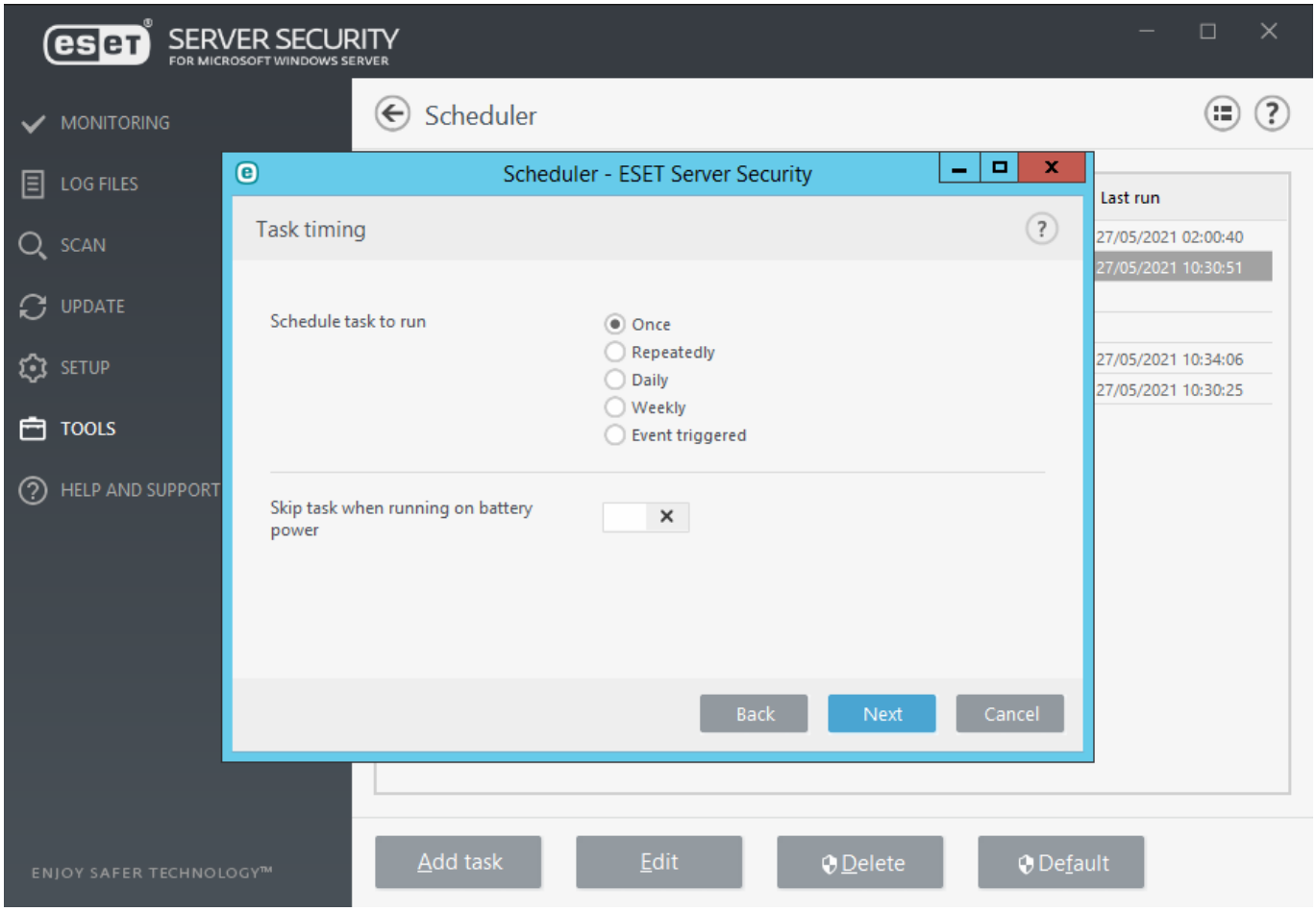
2. Bir **Görev adı** girin ve özel zamanlanan görevinizi yapılandırın.

3. Görev türü - Uygun **Görev türünü** açılır menüden seçin.

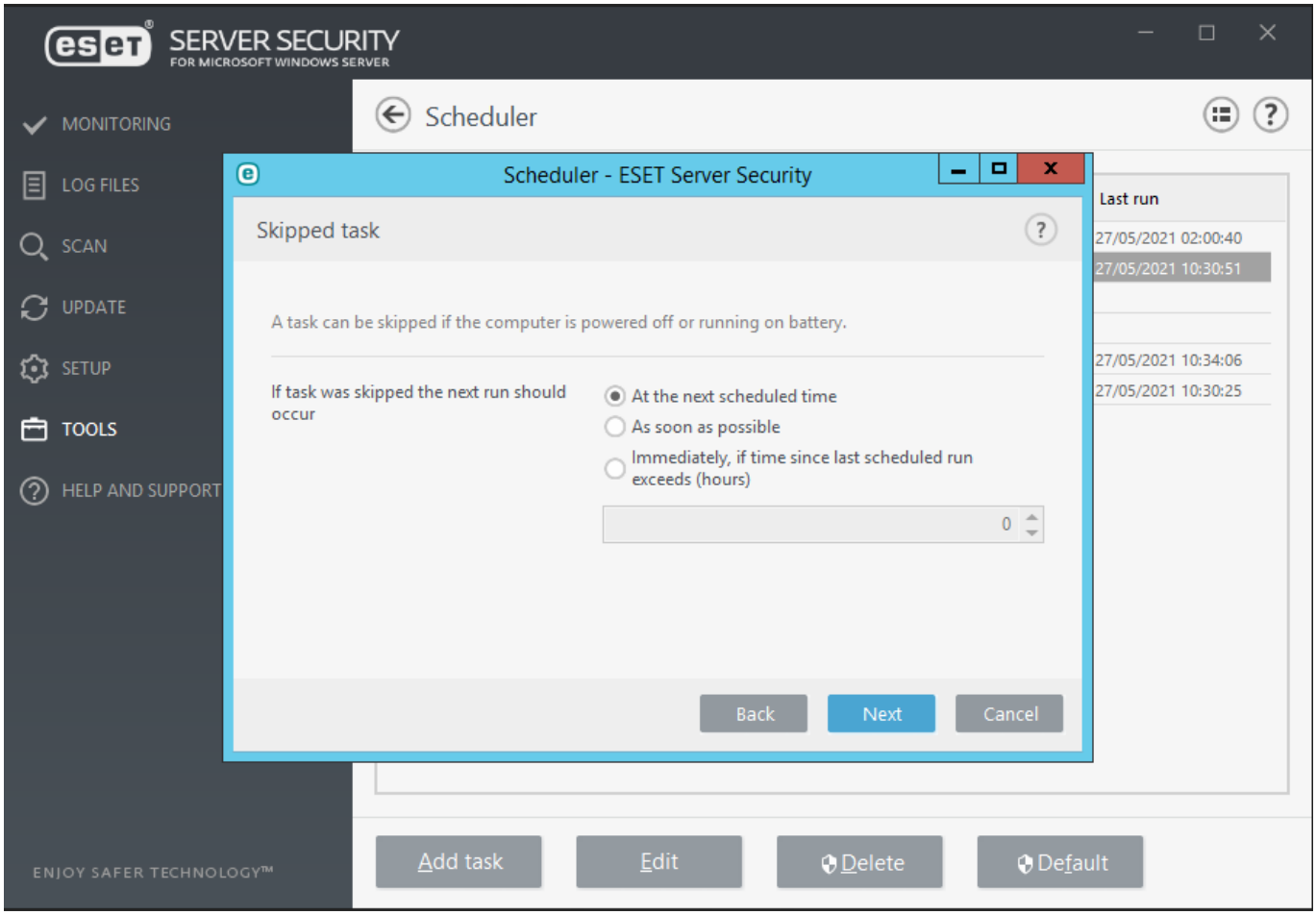


NOT
Görevi devre dışı bırakmak için **Etkin** seçeneğinin yanındaki kaydırma çubuğunu tıklayın. Görevi daha sonra etkinleştirmek için Zamanlayıcı görünümündeki onay kutusunu kullanın.

4. Görev Zamanlaması - Görevinizin çalışmasını istediğiniz zamanı tanımlamak için seçeneklerden birini belirleyin. Seçiminize bağlı olarak sizden belirli bir saat, gün, aralık veya etkinlik seçmeniz istenir.



5. Atlanan görev - Görev önceden tanımlanan bir saatte çalıştırılamadıysa, görevin ne zaman gerçekleştirileceğini belirtebilirsiniz.



6. Uygulamayı çalıştır - Görev harici bir uygulamayı çalıştırmak üzere zamanlandıysa, dizin ağacından bir yürütülebilir dosya seçin.

7.Değişiklik yapmanız gerekirse, önceki adımlara dönmek ve parametreleri değiştirmek için **Geri**'yi tıklayın.

8.Görevi oluşturmak veya değişiklikleri uygulamak için **Bitir**'i tıklayın.

Yeni zamanlanan görev, Zamanlayıcı görünümünde gösterilir.

Görev türü

Yapılandırma sihirbazı, zamanlanan görevin her **Görev türü** için farklıdır. **Görev adını** girin ve açılır menüden istediğiniz **Görev türünü** seçin:

- **Harici uygulama çalıştır** - Harici bir uygulamanın yürütülmesini zamanlar.
- **Günlük bakımı** - Günlük dosyaları, silinen kayıtlardan kalanları da içerir. Bu görev, etkin çalışma sağlamak için günlük dosyalarındaki kayıtları düzenli olarak optimize eder.
- **Sistem başlangıcında dosya denetimi** - Sistem başlangıcında veya oturum açıldığında çalıştırılmasına izin verilen dosyaları denetler.
- **Bilgisayar durumunun sistem görüntüsünü oluştur** - ESET SysInspector bilgisayar sistem görüntüsünü oluşturur; sistem bileşenleri (örneğin, sürücüler, uygulamalar) hakkında ayrıntılı bilgi toplar ve her bileşenin risk düzeyini değerlendirir.

- **İsteğe bağlı bilgisayar taraması** - Bilgisayarınızdaki dosyaların ve klasörlerin bilgisayar taramasını gerçekleştirir.
- **Güncelleme -** Algılama altyapısının ve program modüllerinin güncellenmesi için bir güncelleme görevini zamanlar.
- **Hyper-V taraması** - Hyper-V içindeki sanal disklerin taramasını zamanlar.
- **OneDrive scan** - OneDrive'da yüklenmiş olan dosyalar için bir tarama işlemi zamanlar.

Oluşturulduktan sonra görevi devre dışı bırakmak için, **Etkin** seçeneğinin yanındaki anahtarı tıklayın. Görevi daha sonra etkinleştirmek için Zamanlayıcı görünümündeki onay kutusunu tıklayın. Sonraki adıma geçmek için **İleri**'yi tıklayın.

Görev zamanlaması

Aşağıdaki zamanlama seçeneklerinden birini belirleyin:

- **Bir kere-** Görev önceden belirlenen tarih ve saatte yalnızca bir kere gerçekleştirilir. Görevi yalnızca bir kez, belirli bir zamanda çalıştırmak için kullanılır. **Görev yürütme** alanında başlangıç tarihini ve çalıştırma zamanını bir kez belirtin.
- **Tekrarlayarak -** Görev belirtilen zaman aralığında (dakika olarak) gerçekleştirilir. **Görev yürütme** alanında görevin her gün yürütüleceği saati belirtin.
- **Günlük** - Görev her gün tekrarlayan bir şekilde belirtilen saatte çalıştırılır.
- **Haftalık -** Görev seçilen günlerde ve saatte haftada bir veya birkaç kere çalıştırılır. Görevi belirtilen günde ve saatte başlayarak haftanın yalnızca belirli günlerinde tekrarlayarak çalıştırmak için kullanılır. Görevin yürütülme saati alanında başlangıç saatini belirtin. Görevin çalıştırılacağı günü veya haftanın günlerini seçin.
- Olay tetiklediğinde - Görev belirtilen bir olayın ardından gerçekleştirilir.

Pil gücüyle çalışırken görevi atla seçeneğini etkinleştirirseniz, görevin başlatılması gereken saatte sistem pil gücüyle çalışıyorsa görev başlamaz. Örneğin, UPS'te çalışan bilgisayarlar.

Olay tetiklediğinde

Olay tarafından tetiklenen bir görevi zamanlarken, görevin iki tamamlanışı arasındaki minimum aralığı belirtebilirsiniz.

Görev aşağıdaki olaylardan biri tarafından tetiklenebilir:

- **Bilgisayarın her başlatılışında**
- **Her gün, bilgisayar ilk açıldığında**
- **Çevirmeli İnternet/VPN bağlantısı**
- **Başarılı modül güncellemesi**
- **Başarılı ürün güncellemesi**

- **Kullanıcı oturum açtığında** - Kullanıcı sistemde oturum açtığı zaman görev dağıtılır. Günde birkaç kez bilgisayarınızda oturum açıyorsanız, görevi yalnızca günün ilk oturum açma işleminde ve ardından sonraki gün gerçekleştirmek için 24 saat seçeneğini belirleyin.

- **Tehdit algılama**

Uygulamayı çalıştır

Bu görev, harici bir uygulamanın çalıştırılmasını zamanlar.

- **Yürütülebilir dosya** - Dizin ağacından bir yürütülebilir dosya seçin, **tara (...) seçeneğini tıklatın** veya yolu manuel olarak girin.

- **Çalışma klasörü** - Harici uygulamanın çalışma dizinini tanımlayın. Seçili **Çalıştırılabilir dosyanın** tüm geçici dosyaları, bu dizin içinde oluşturulacaktır.

- **Parametreler** - Uygulamaya yönelik komut satırı parametreleri (isteğe bağlı).

Atlanan görev

Görev önceden tanımlanan saatte çalıştırılamadıysa, ne zaman gerçekleştirileceğini belirtebilirsiniz:

- **Bir sonraki zamanlanan saatte** - Görev belirtilen saatte (örneğin 24 saat sonra) yürütülür.

- **En kısa sürede** - Görev en kısa sürede çalıştırılır (görevlerin yürütülmesini engelleyen eylemler ortadan kalktığında).

- **Son çalıştırmadan itibaren geçen süre belirtilen değeri geçiyorsa hemen - Son çalıştırmadan itibaren geçen süre (saat)** - Bu seçeneği belirledikten sonra göreviniz her zaman belirtilen süre (saat cinsinden) geçtikten sonra yinelenir.

Zamanlanan göreve genel bakış

Bu iletişim penceresi, **Zamanlayıcı görünümündeki** görevi çift tıkladığınızda veya zamanlanan görevi sağ tıklayıp **Görev ayrıntılarını göster**'i seçtiğinizde zamanlanan görevle ilgili ayrıntılı bilgileri gösterir.

Örnekleri analiz için gönderin

Örnek gönderimi iletişim penceresi, bir dosyayı veya siteyi analiz için ESET'e gönderebilmenizi sağlar. Bilgisayarınızda şüpheli davranışları olan bir dosya veya İnternet'te şüpheli bir site bulursanız, bu dosyayı veya siteyi analiz için ESET Virüs Laboratuvarı'na gönderebilirsiniz. Dosyanın kötü amaçlı bir uygulama veya web sitesi olduğu belirlenirse, bu dosyanın algılanması yaklaşan bir güncellemeye eklenir.

Dosyayı e-posta ile göndermek için dosyaları WinRAR veya WinZip gibi bir programla sıkıştırın, arşivi *infected* parolasıyla koruyun ve samples@eset.com adresine gönderin. Açıklayıcı bir konu kullanın ve dosyayla ilgili olabildiğince çok bilgi (örneğin, dosyayı indirdiğiniz web sitesi) ekleyin.

Bir örneği ESET'e göndermeden önce aşağıdaki ölçütlerden birini veya her ikisini karşıladığından emin olun:

- dosya veya web sitesi hiç algılanmadı
- dosya veya web sitesi tehdit olarak yanlış bir şekilde algılandı

Yukarıdaki gereksinimlerden en az birisi karşılanmazsa, daha fazla bilgi sağlanıncaya kadar bir yanıt almazsınız.

Örneği gönderme nedeni açılır menüsünden iletinize en uygun olan açıklamayı seçin:

- Şüpheli dosya
- Şüpheli site (kötü amaçlı yazılımdan etkilenen web sitesi)
- Hatalı pozitif dosya (etkilenmiş olarak algılanan ancak etkilenmemiş olan dosya)
- Hatalı pozitif site
- Diğer

Dosya/Site

Göndermek istediğiniz dosyanın veya web sitesinin yolu.

İletişim e-posta adresi

Bu iletişim e-postası şüpheli dosyalarla birlikte ESET'e gönderilir ve analiz için ek bilgiler gerekirse sizinle iletişim kurmak üzere kullanılabilir. İletişim e-posta adresi girmek isteğe bağlıdır. Sunucularımıza her gün on binlerce dosya geldiğinden tüm gönderimleri yanıtlamamız olanaksız olduğu için, daha fazla bilgi gerekmedikçe ESET'ten yanıt almazsınız.

Anonim olarak gönder

E-posta adresinizi girmeden şüpheli dosyayı veya web sitesini göndermek için **Anonim olarak gönder** öğesinin yanındaki onay kutusunu kullanın.

Şüpheli dosya

Gözlemlenen kötü amaçlı yazılımdan etkilenme işaretleri ve belirtileri

Bilgisayarınızda gözlemlenen kötü amaçlı yazılım davranışlarının açıklamasını girin.

Dosya kaynağı (URL adresi veya satıcı)

Dosyanın kaynağını (nereden edindiğinizi) ve bu dosyaya ne şekilde ulaştığınızı girin.

Notlar ve ek bilgiler

Buraya şüpheli dosyanın tanımlanması sürecinde yardımcı olabilecek ek bilgileri veya açıklamaları girebilirsiniz.

> NOT
> İlk parametre olan - **Gözlemlenen kötü amaçlı yazılımdan etkilenme işaretleri ve belirtileri** - öğesinin belirtilmesi zorunludur, ancak örneklerin tanımlama sürecinde laboratuvarlarımıza önemli ölçüde yardımcı olacak ek bilgiler de sağlanmalıdır.

Şüpheli site

Bu siteyle ilgili sorun nedir açılır menüsünden aşağıdakilerden birini seçin:

Enfekte olan

Çeşitli yöntemlerle dağıtılan virüsleri veya diğer kötü amaçlı yazılımları içeren bir web sitesidir.

Kimlik avı

Genellikle banka hesabı numaraları, PIN numaraları ve diğer bilgiler gibi hassas verilere erişmek amacıyla kullanılır. Bu saldırı türüyle ilgili daha fazla bilgi sözlük'ten edinilebilir.

Dolandırıcılık

Sahtekârlık ve dolandırma amaçlı bir web sitesi.

Diğer

Yukarıdaki seçeneklerden hiçbiri göndereceğiniz site için geçerli değilse bu seçeneği belirleyin.

Notlar ve ek bilgiler

Şüpheli web sitesinin analiz edilmesine yardımcı olabilecek daha fazla bilgi veya bir açıklama girebilirsiniz.

Hatalı pozitif dosya

Tespit altyapımızı geliştirmek ve diğer kullanıcıların korunmasına yardımcı olmak için, etkilenmiş olarak algılanan ancak etkilenmemiş olan dosyaları göndermeniz istenir. Hatalı pozitif (HP) algılamaları bir dosya deseninin, algılama altyapısında yer alan aynı düzenle eşleşmesi halinde meydana gelebilir.

NOT
Yasal uygulamaların tanımlanabilmesi ve kötü amaçlı kodlardan ayrılabilmesi için ilk üç parametrenin sağlanması zorunludur. Ek bilgi sağlayarak tanımlama sürecinde ve örneklerin işlenmesinde laboratuvarlarımıza büyük oranda yardımcı olabilirsiniz.

Uygulama adı ve sürümü

Programın başlığı ve sürümü (örneğin numarası, takma adı veya kod adı).

Dosya kaynağı (URL adresi veya satıcı)

Dosyanın kaynağını (nereden edindiğinizi) girin ve bu dosyaya ne şekilde ulaştığınızı not edin.

Uygulamanın amacı

Uygulamanın genel açıklaması, uygulamanın türü (ör. tarayıcı, medya oynatıcı, ...) ve işlevleri.

Notlar ve ek bilgiler

Buraya şüpheli dosya işlenirken yardımcı olabilecek ek bilgileri veya açıklamaları ekleyebilirsiniz.

Hatalı pozitif site

Etkilenmiş, kimlik bilgilerini çalmaya veya kimlik avına yönelik olarak algılanan ancak bunlardan herhangi biri olmayan siteleri göndermeniz istenir. Yanlış tespit (YT) algılamaları bir site deseninin, algılama altyapısında yer alan aynı düzenle eşleşmesi halinde meydana gelebilir. Tespit altyapımızı geliştirmek ve diğer kullanıcıların korunmasına yardımcı olmak için lütfen bu web sitesini bize iletin.

Notlar ve ek bilgiler

Buraya şüpheli dosya işlenirken yardımcı olabilecek ek bilgileri veya açıklamaları ekleyebilirsiniz.

Diğer

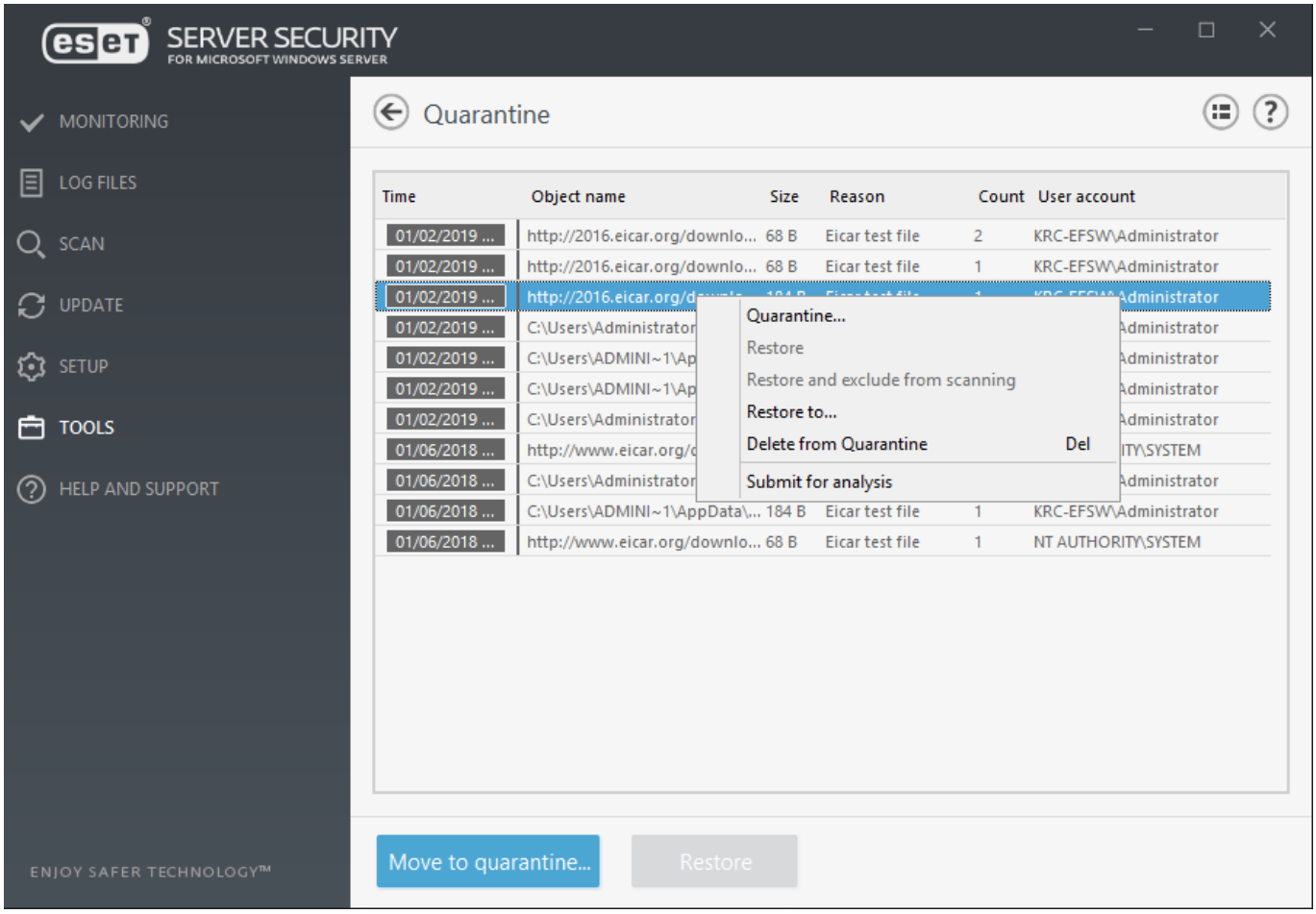
Dosya **Şüpheli dosya** veya **Hatalı pozitif** olarak sınıflandırılamıyorsa bu formu kullanın.

Dosyayı gönderme nedeni

Detaylı bir açıklama ve dosyanın neden gönderildiğini girin.

Karantina

Karantinanın ana işlevi, etkilenen dosyaları güvenli bir şekilde saklamaktır. Dosyalar temizlenemiyorsa, silinmeleri güvenli değilse ya da önerilmiyorsa veya ESET Server Security tarafından hatalı bir şekilde algılanıyorsa, bu dosyaların karantinaya alınmaları gerekir. Bir dosya şüpheli davranıyorsa ancak zararlı yazılım tarayıcısı tarafından algılanmıyorsa, bu işlem önerilebilir. Karantinaya alınan dosyalar, analiz için ESET Virüs Laboratuvarı'na gönderilebilir.



Karantina klasörüne depolanmış dosyalar karantinanın tarih ve saatini, etkilenen dosyanın özgün konumunun yolunu, bayt olarak boyutunu, nedenini (örneğin, kullanıcı tarafından eklenen nesne) ve tehdit sayısını (örneğin, birden çok sızıntıyı içeren bir arşiv olup olmadığını) görüntüleyen bir tabloda görülebilir.

E-posta iletisi nesneleri dosya karantinasına alınırsa, posta kutusu/klasör/dosya adı için bir yol görüntülenir.

Dosyaları karantinaya alma

ESET Server Security, silinen dosyaları otomatik olarak karantinaya alır (bu seçeneği uyarı penceresinde iptal etmediyseniz). Herhangi bir şüpheli dosyayı **Karantinaya al** düğmesini tıklayarak manuel olarak karantinaya alabilirsiniz. Karantinaya alınan dosyalar, orijinal konumlarından kaldırılır. Ayrıca içerik menüsü de bu amaçla kullanılabilir; **Karantina** penceresinde sağ tıklayın ve **Karantinaya al** seçeneğini belirleyin.

Karantinadan geri yükleme

Karantinaya alınan dosyalar orijinal konumlarına geri yüklenebilir. Bunun için **Geri Yükle** özelliğini kullanın; bu seçenek, Karantina penceresinde ilgili dosya sağ tıklandığında açılan içerik menüsünde yer alır. Bir dosya istenmeyen türden olabilecek uygulama olarak işaretlenirse, **Geri yükle ve tarama dışında bırak** seçeneği kullanılabilir. Ayrıca içerik menüsü, dosyayı silinmiş olduğu konumdan farklı bir konuma geri yüklemenize olanak tanıyan **Geri yükleme konumu...** seçeneğini de sunar.

NOT
Program yanlışlıkla zararsız bir dosyayı karantinaya almışsa, geri yükledikten sonra dosyayı tarama dışında bırakın ve ESET Müşteri Desteği'ne gönderin.

Karantinadaki bir dosyayı gönderme

Program tarafından algılanmayan şüpheli bir dosyayı karantinaya aldıysanız veya bir dosya yanlışlıkla etkilenmiş olarak değerlendirilmiş (örneğin, kodun sezgisel tarama analizi tarafından) ve sonra da karantinaya alınmışsa, lütfen dosyayı ESET Virüs Laboratuvarı'na gönderin. Dosyayı karantinadan göndermek için, dosyayı sağ tıklatın ve içerik menüsünden Analiz için gönder'i seçin.

Karantinadan Silme

Belirli bir öğeyi sağ tıklayın ve **Karantinadan Sil**'i seçin. Veya uygun öğeleri seçin ve klavyenizdeki **Delete** tuşuna basın.

OneDrive tarama ayarları

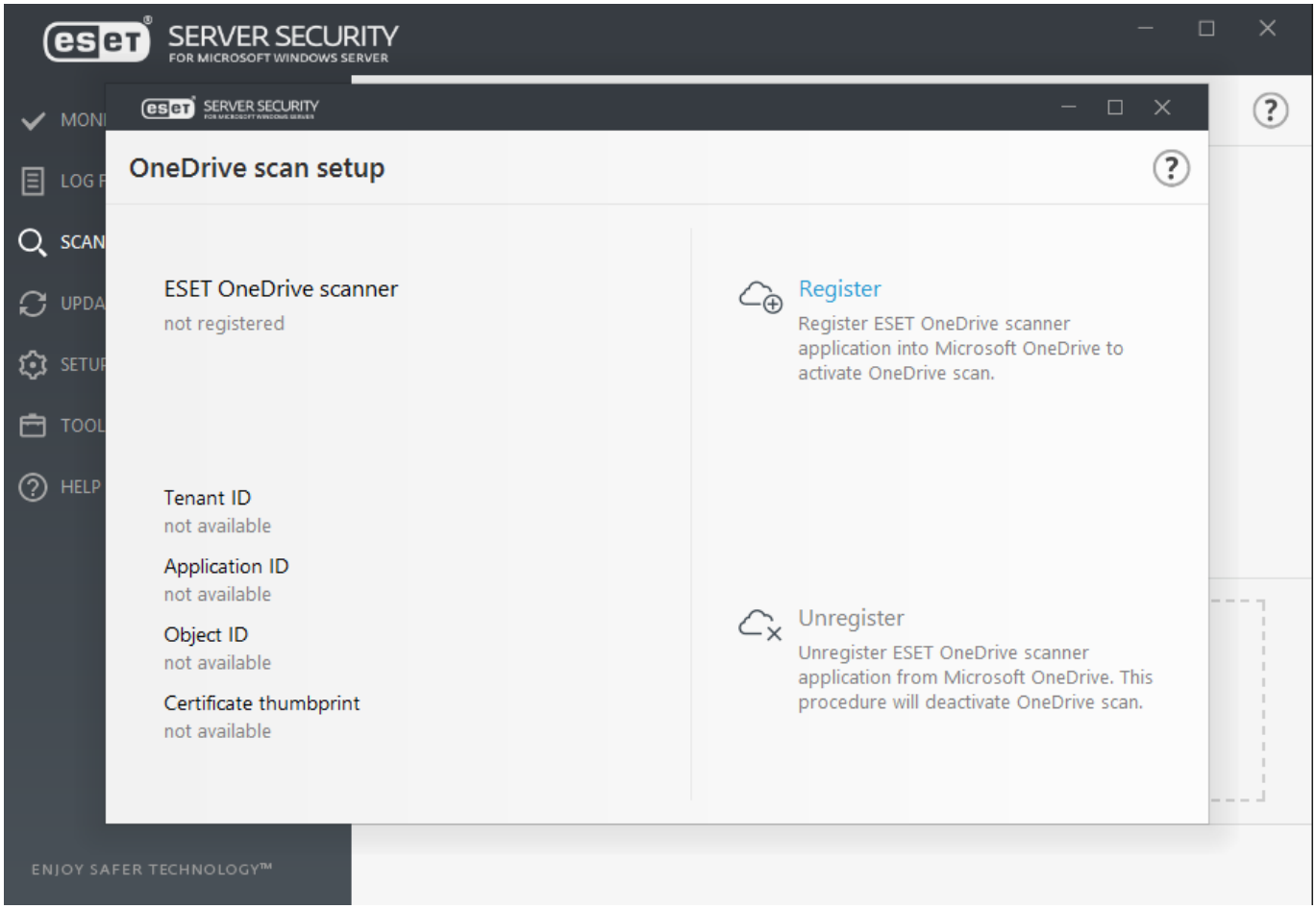
ESET Server Security Uygulamasını aç
Ayarlar > Sunucu > OneDrive Tarama ayarları

Bu özellik, Microsoft OneDrive for Business bulut depolamasında depolanan dosyaları taramanıza olanak tanır. ESET Server Security OneDrive aracının yalnızca dosya ve klasörleri taraması gerekir. E-posta, SharePoint dosyaları, kayıtlar veya takvimler gibi veri türlerini taramaz.

Hızlı bağlantılar:

ESET OneDrive tarayıcısını kaydedin
ESET OneDrive tarayıcısının kaydını kaldırın

ESET Server Security OneDrive taramasını kullanmaya başlamak için, ESET OneDrive tarayıcı uygulamasını Microsoft OneDrive / Microsoft Office 365 / Microsoft Azure'a kaydedin. OneDrive tarama ayarları kayıt durumunu gösterir. Halihazırda kaydedilmişse kayıt ayrıntılarını (Kiracı Kimliği, Uygulama Kimliği, Nesne Kimliği ve Sertifika parmak izi) görebilirsiniz. ESET OneDrive tarayıcısını Kaydedin veya Kaydı silin:



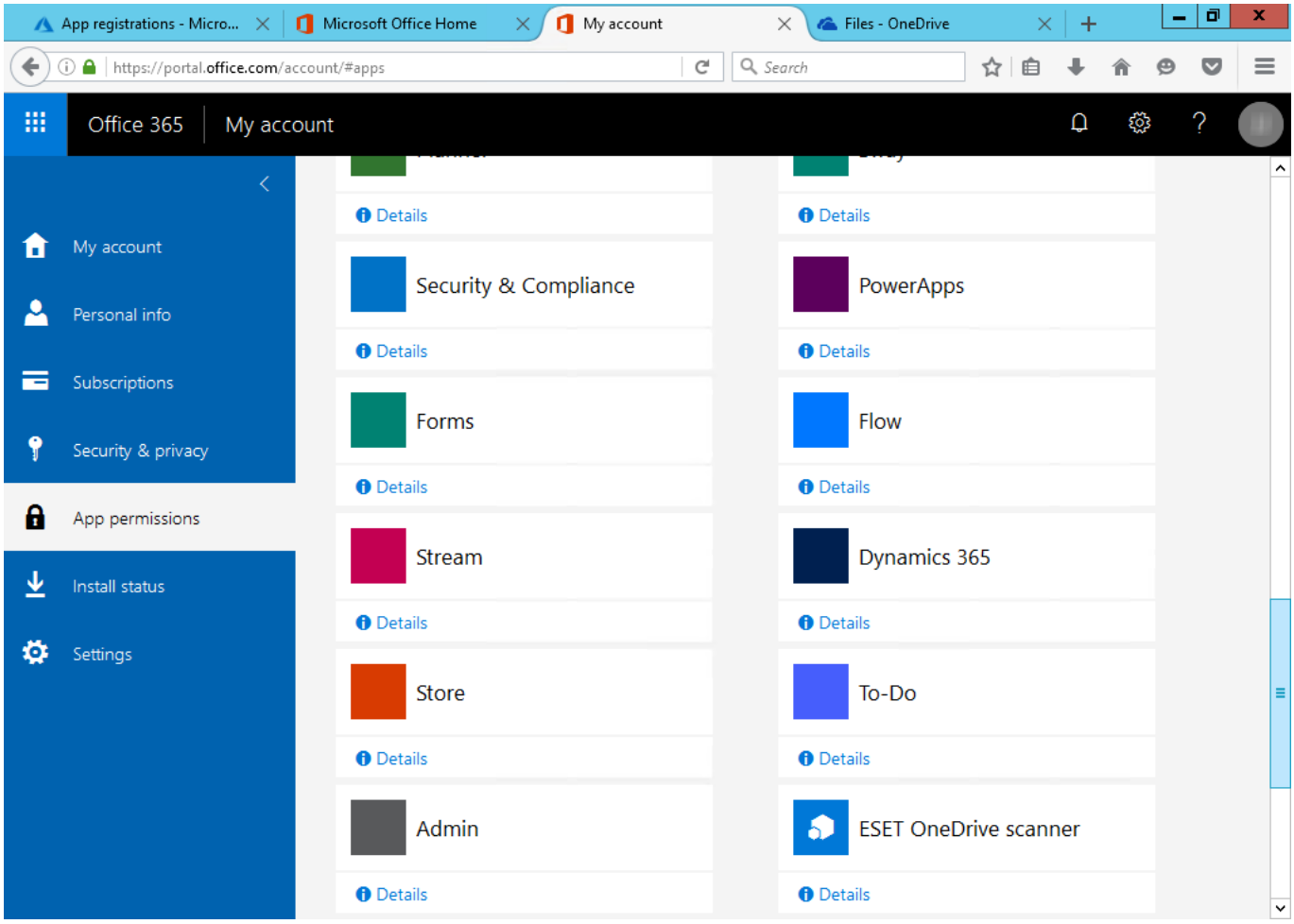
Başarılı bir kayıt işleminin ardından, OneDrive taraması Tara menüsünde kullanılabilir hale gelir ve klasör yapısıyla tarama için seçilebilecek dosyaları içeren bir kullanıcı listesi gösterilir. ESET Server Security OneDrive taraması, kullanıcıların OneDrive for Business'ta depoladığı tüm dosyaları tarayabilir.

NOT
ESET Server Security OneDrive taraması, OneDrive for Business bulut depolamasından dosyaları indirir ve taramaları yerel olarak yapar. Tarama işlemi tamamlandıktan sonra indirilen dosyalar silinir. OneDrive'dan büyük miktarda veri indirmek ağ trafiğini etkileyebilir.

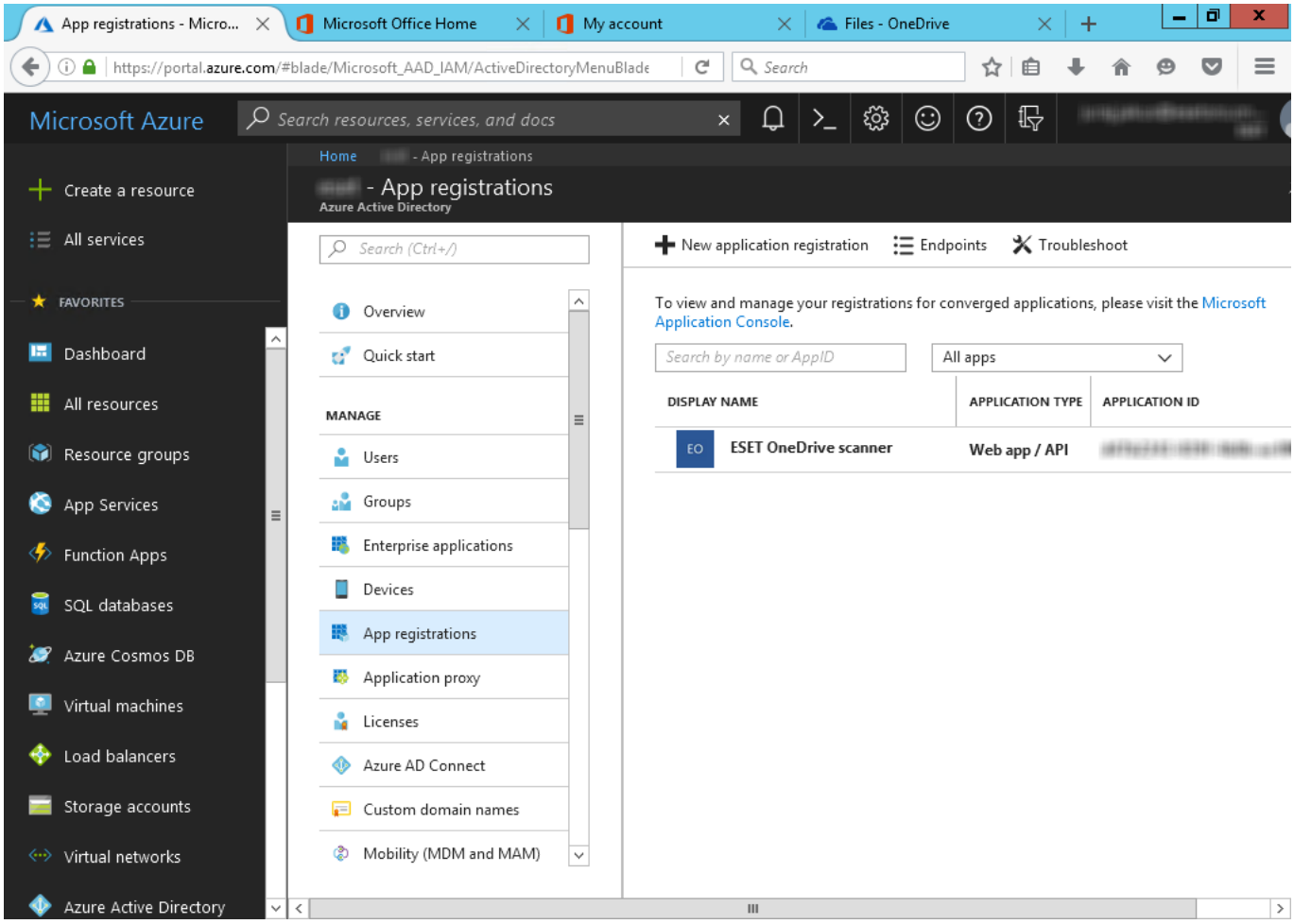
NOT
Farklı bir hesapla oturum açın: ESET Server Security OneDrive tarayıcısını yeni bir Microsoft OneDrive for Business / Office 365 hesabıyla kaydetmek istiyorsanız, önceki hesabınızla kullandığınız ESET OneDrive tarayıcısının kaydını kaldırmanız ve yeni Microsoft OneDrive for Business / Office 365 yönetici hesabıyla kayıt işlemini yapmanız gerekir.

ESET OneDrive tarayıcısının Office 365 ve Azure'da uygulama olarak kaydedildiğini görebilirsiniz:

Office 365 portalı - Hesabım sayfasındaki **Uygulama izinleri**'ni tıkladığınızda ESET OneDrive tarayıcı uygulamasının listelendiğini görürsünüz.



Azure - **Azure Active Directory** > **Uygulama kayıtları**'na gidin, **Tüm uygulamaları göster**'i tıklayın. ESET OneDrive tarayıcısının listelendiğini görebilirsiniz. Ayrıntılarını görmek için uygulamayı tıklayın.

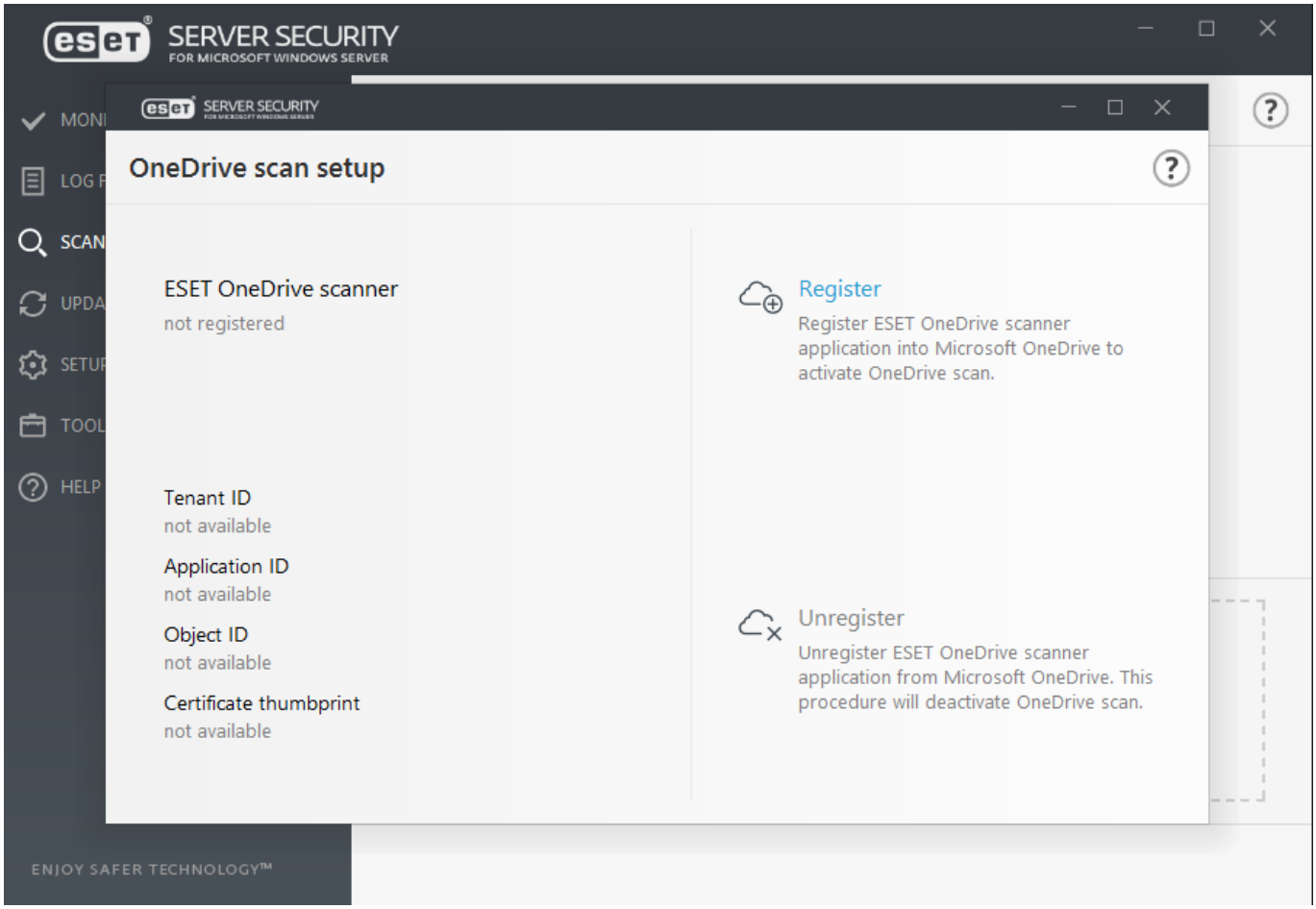


ESET OneDrive tarayıcısını kaydedin

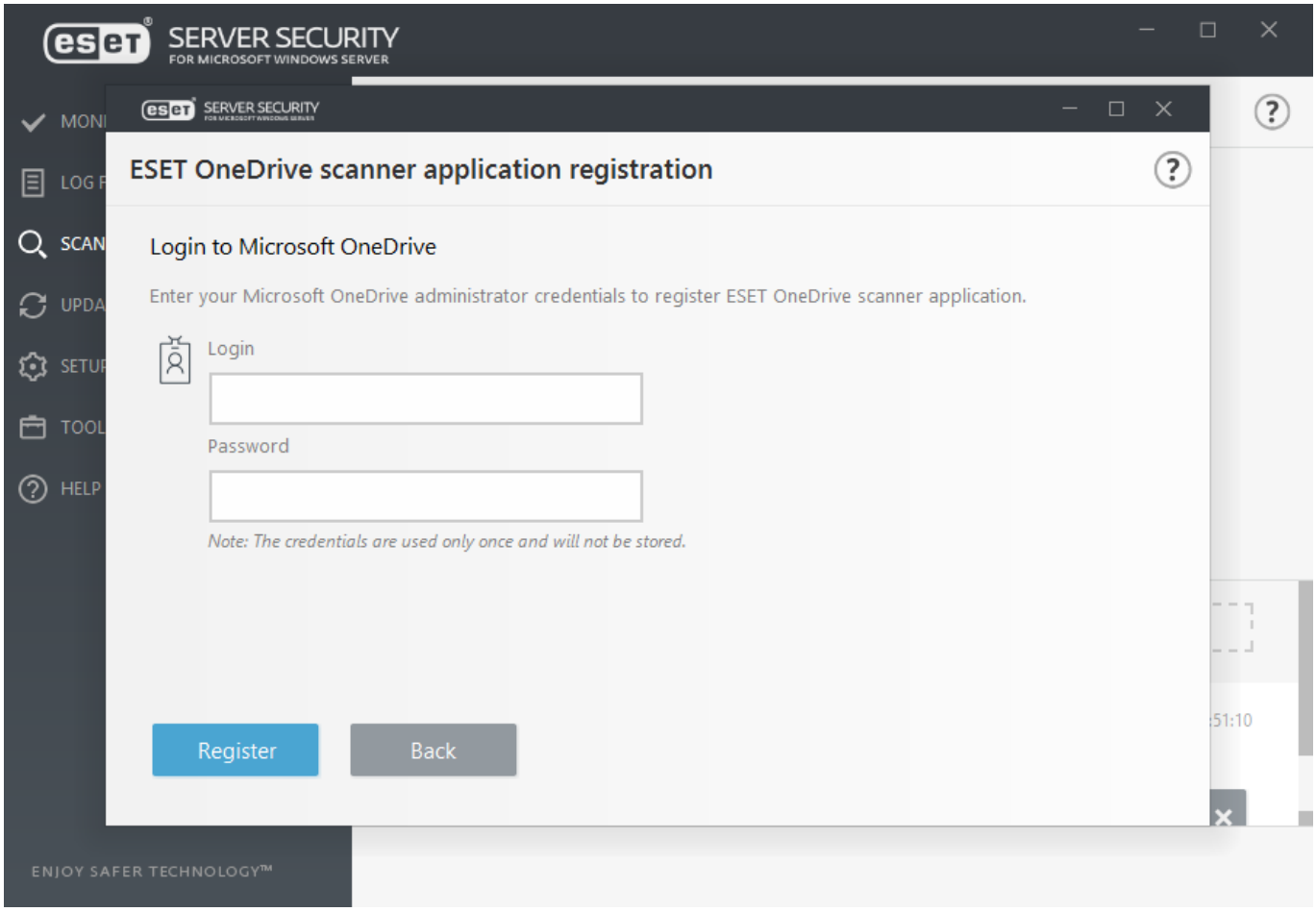
ESET Server Security Uygulamasını aç
Ayarlar > Sunucu > OneDrive Tarama ayarları > Kayıt

Aşağıdaki işlem, Microsoft OneDrive / Office 365 / Azure'da ESET OneDrive tarayıcı uygulaması kaydının yapılmasını içerir:

- ESET OneDrive tarayıcısı kaydına başlamak için **Kaydet** öğesini tıklayın. Kayıt sihirbazı açılır.

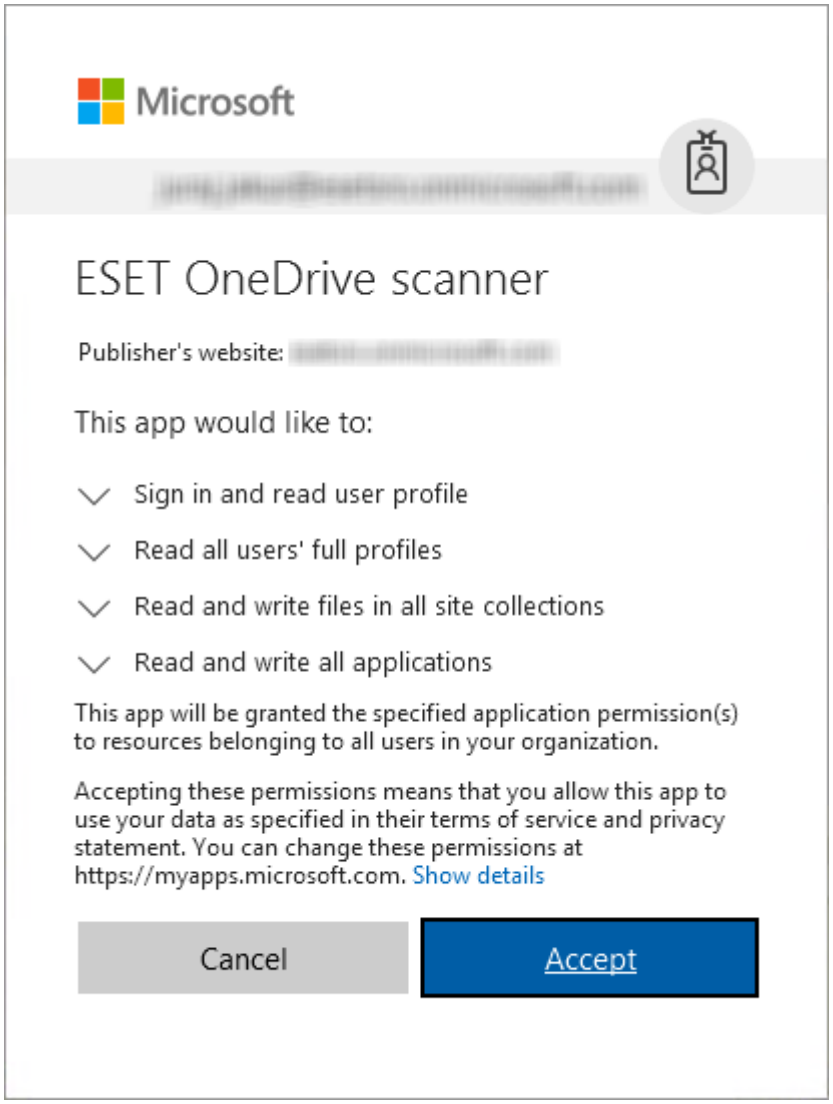


• Microsoft OneDrive / Office 365 yönetici hesabı kimlik bilgilerinizi girin. Microsoft OneDrive'da uygulama kaydı tamamlanana kadar bekleyin.

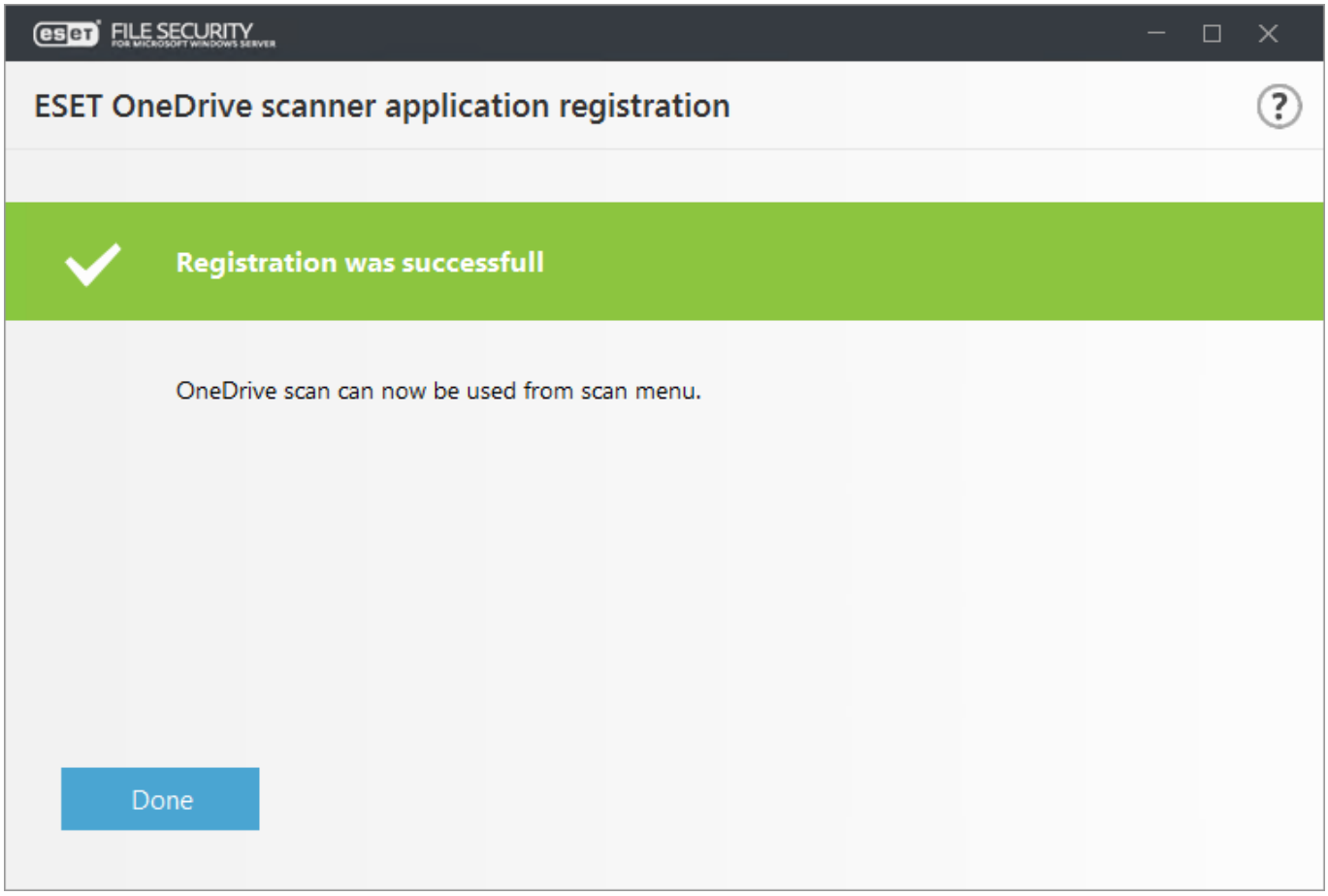


• Microsoft ile bir web tarayıcısı **Bir hesap seçin** sayfası açılır. Varsa kullandığınız hesabı tıklayın veya Microsoft OneDrive / Office 365 yönetici hesabı kimlik bilgilerinizi girin ve **Oturum aç**'ı tıklayın.

• ESET OneDrive tarayıcı uygulaması kabul iletisinde listelenen dört izin türü gerektirir. **Kabul et**'i tıklayarak ESET Server Security OneDrive tarayıcısının OneDrive bulut depolamasında bulunan verilere erişmesine izin verin.



- 'Web tarayıcısı tarafından bu bilgileri göndermeniz istenirse **Devamı** tıklayın (ESET Server Security aracının uygulama kaydını başarılı olduğunu bildirmek için bilgiler yalnızca yerel ana bilgisayarınıza gönderilir).
- Web tarayıcısını kapattıktan sonra ESET OneDrive tarayıcı kaydı sihirbazı Kayıt işlemi başarıyla tamamlandı iletisini gösterdiğinde **Bitti**'yi tıklayın.



NOT
ESET OneDrive tarayıcı kayıt işlemi, yönetici hesabı kimlik bilgilerinizle herhangi bir Microsoft portalında (OneDrive, Office 365, Azure vs.) oturum açıp açmamanıza bağlı olarak değişiklik gösterebilir. Ekrandaki talimatları ve kayıt sihirbazı penceresinin iletilerini uygulayın.

ESET OneDrive tarayıcı kaydı sırasında aşağıdaki hata iletilerinden birini alırsanız, önerilen çözüm için hata iletisi ayrıntılarına bakın:

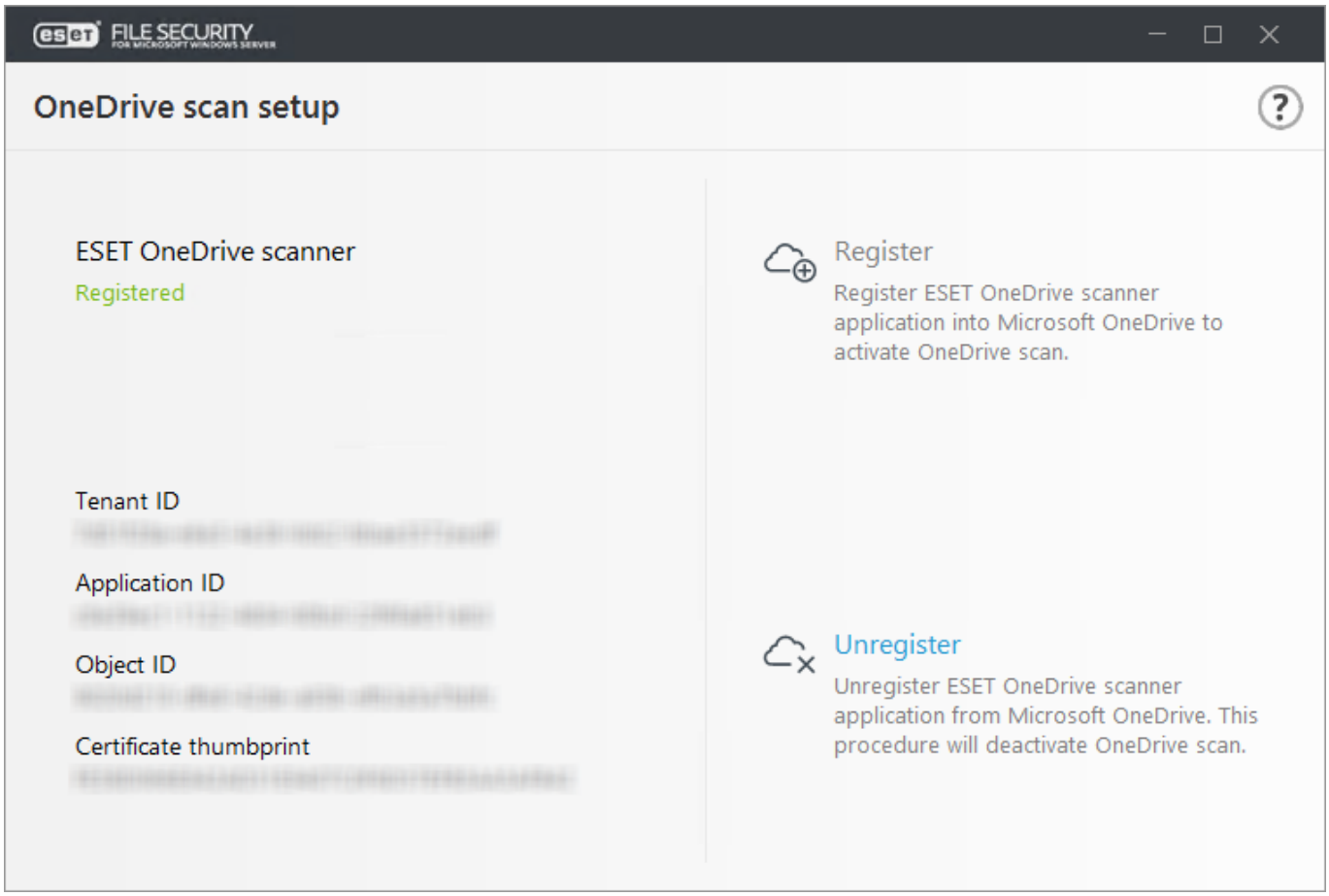
Hata iletisi	Hata iletisi ayrıntıları
Beklenmeyen bir hata oluştu.	ESET Server Security aracında bir sorun olabilir. ESET OneDrive tarayıcı kaydını daha sonra yeniden çalıştırmayı deneyin. Sorun devam ederse ESET Teknik Destek ekibine başvurun.
Microsoft OneDrive'a bağlanılamadı.	Ağ/internet bağlantınızı kontrol edip ESET OneDrive tarayıcı kaydını yeniden çalıştırın.
Microsoft OneDrive'dan beklenmeyen bir hata alındı.	HTTP 4xx hatası hata iletisi yanıtında herhangi bir cevap olmadan geri döner. Sorun devam ederse ESET Teknik Destek ekibiyle iletişime geçin.
Microsoft OneDrive'dan aşağıdaki hata alındı.	Microsoft OneDrive sunucusu belirli hata kodu/adıyla geri dönerse **Hatayı göster**'i tıklayın.
Kurulum görevi zaman aşımına uğradı.	ESET OneDrive tarayıcı kaydı kurulum görevi çok uzun sürüyor. ESET OneDrive tarayıcı kaydını daha sonra tekrar çalıştırmayı deneyin.
Kurulum görevi iptal edildi.	Çalışmakta olan bir kayıt görevini iptal ettiniz. Kaydı tamamlamak istiyorsanız ESET OneDrive tarayıcı kaydını yeniden çalıştırın.
Başka bir kurulum görevi zaten sürüyor.	Halihazırda çalışan bir kayıt görevi var. İlk kayıt işleminin tamamlanmasını bekleyin.

ESET OneDrive tarayıcısının kaydını kaldırın

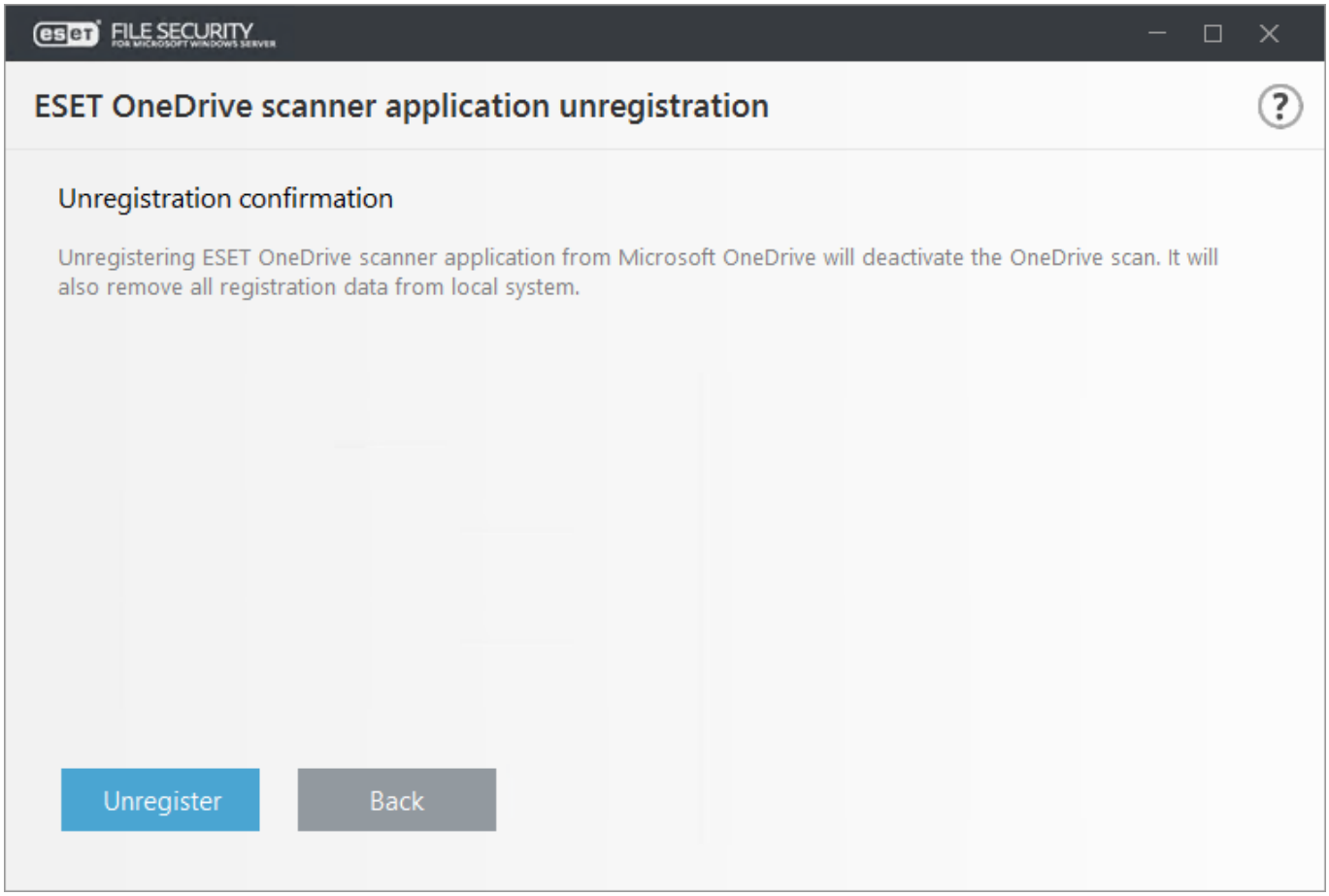
ESET Server Security Uygulamasını aç
Ayarlar > Sunucu > OneDrive Tarama ayarları > Kaydı silin

Kayıt silme işlemi, sertifikayı ve ESET OneDrive tarayıcı uygulamasını Microsoft OneDrive / Office 365 / Azure'dan kaldırmanıza olanak tanır. Ayrıca bu işlem, yerel bağlı öğeleri de kaldırır ve Kayıt seçeneğini yeniden kullanılır hale getirir.

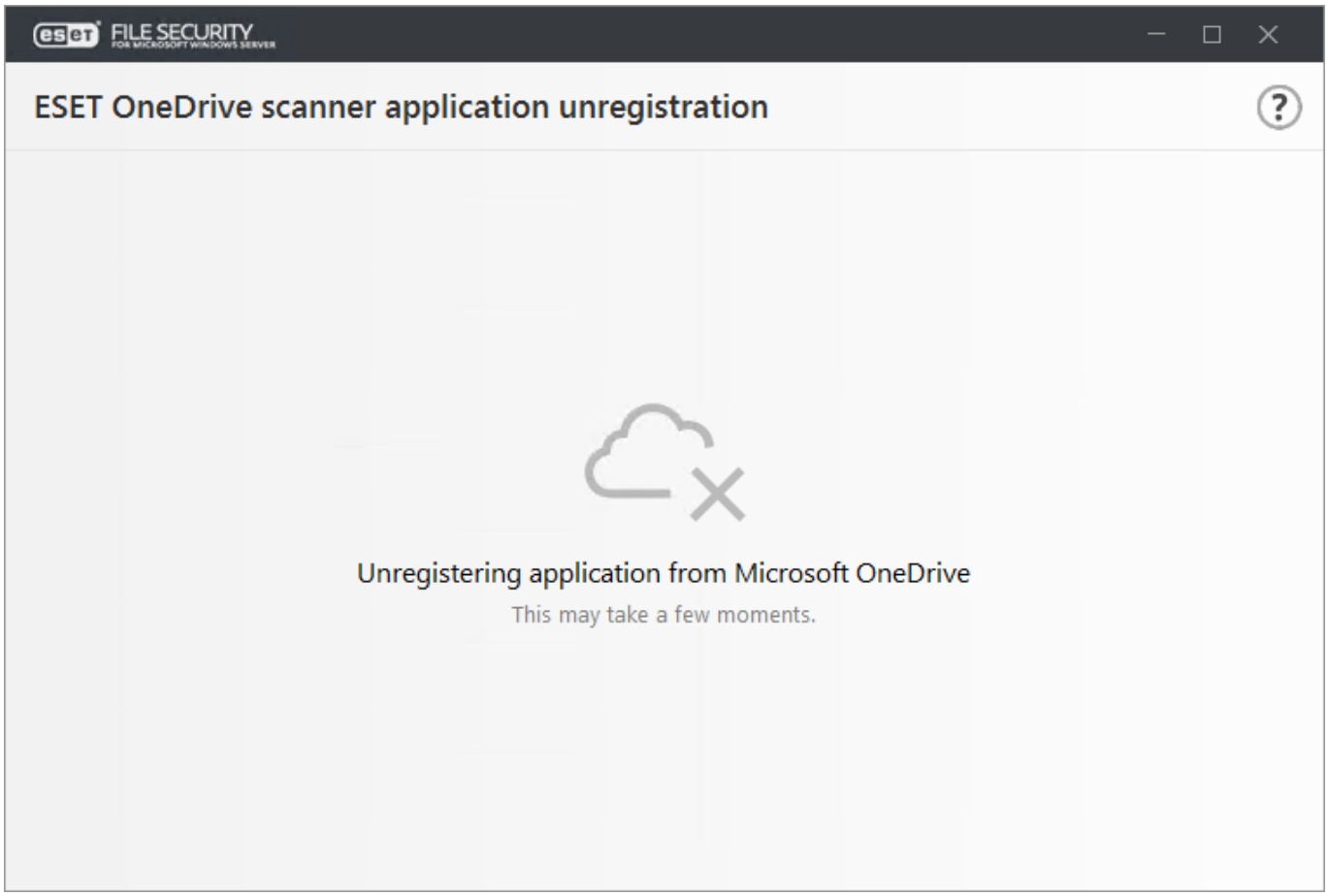
- ESET OneDrive tarayıcısı kaydını silme/kaldırma işlemine başlamak için **Kaydı sil** öğesini tıklayın. Kayıt kaldırma sihirbazı açılır.



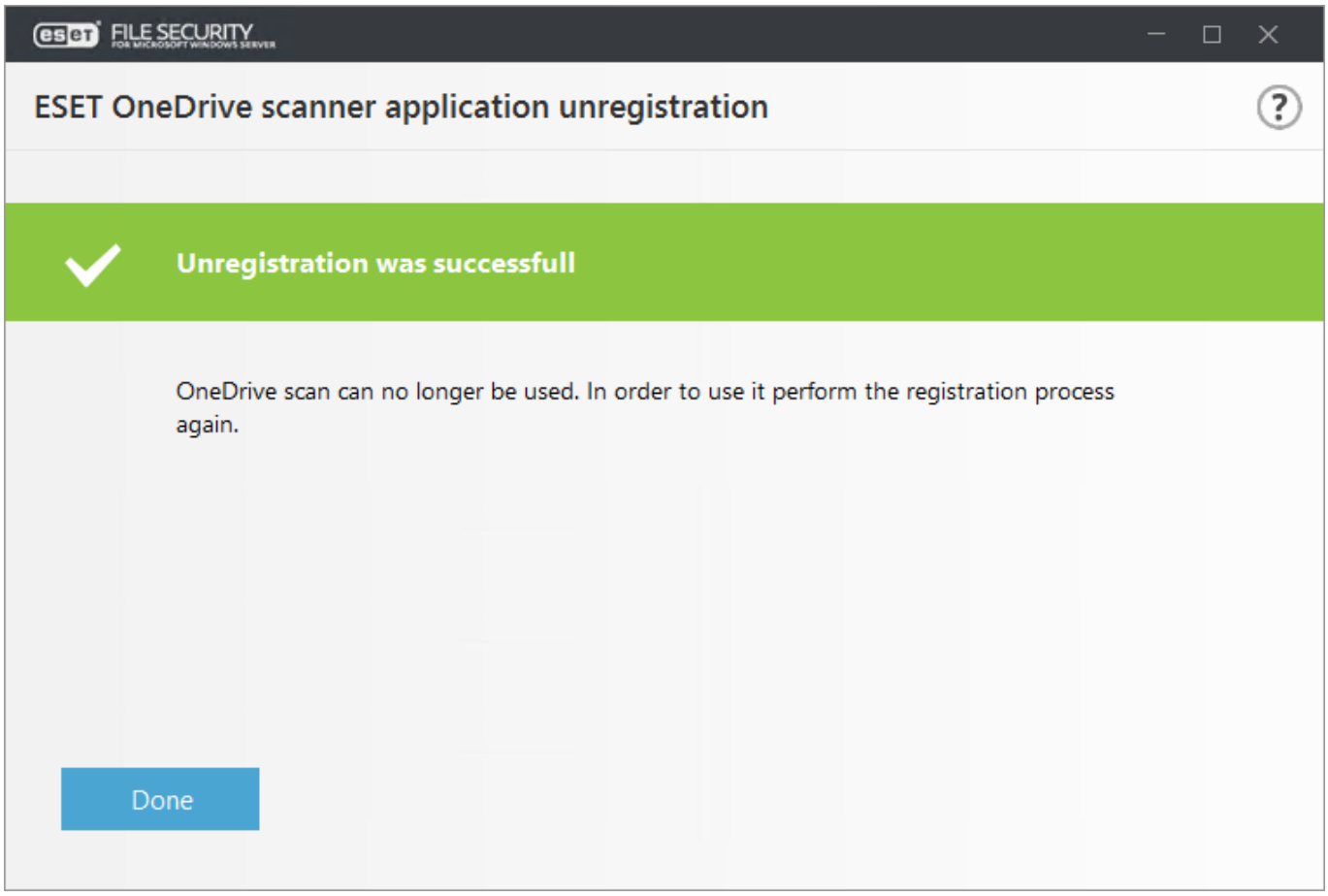
- ESET OneDrive tarayıcısını kaldırmak istediğinizi onaylamak için **Kaydı sil**'i tıklayın.



- Microsoft OneDrive'da kayıt silme işleminin tamamlanmasını bekleyin.



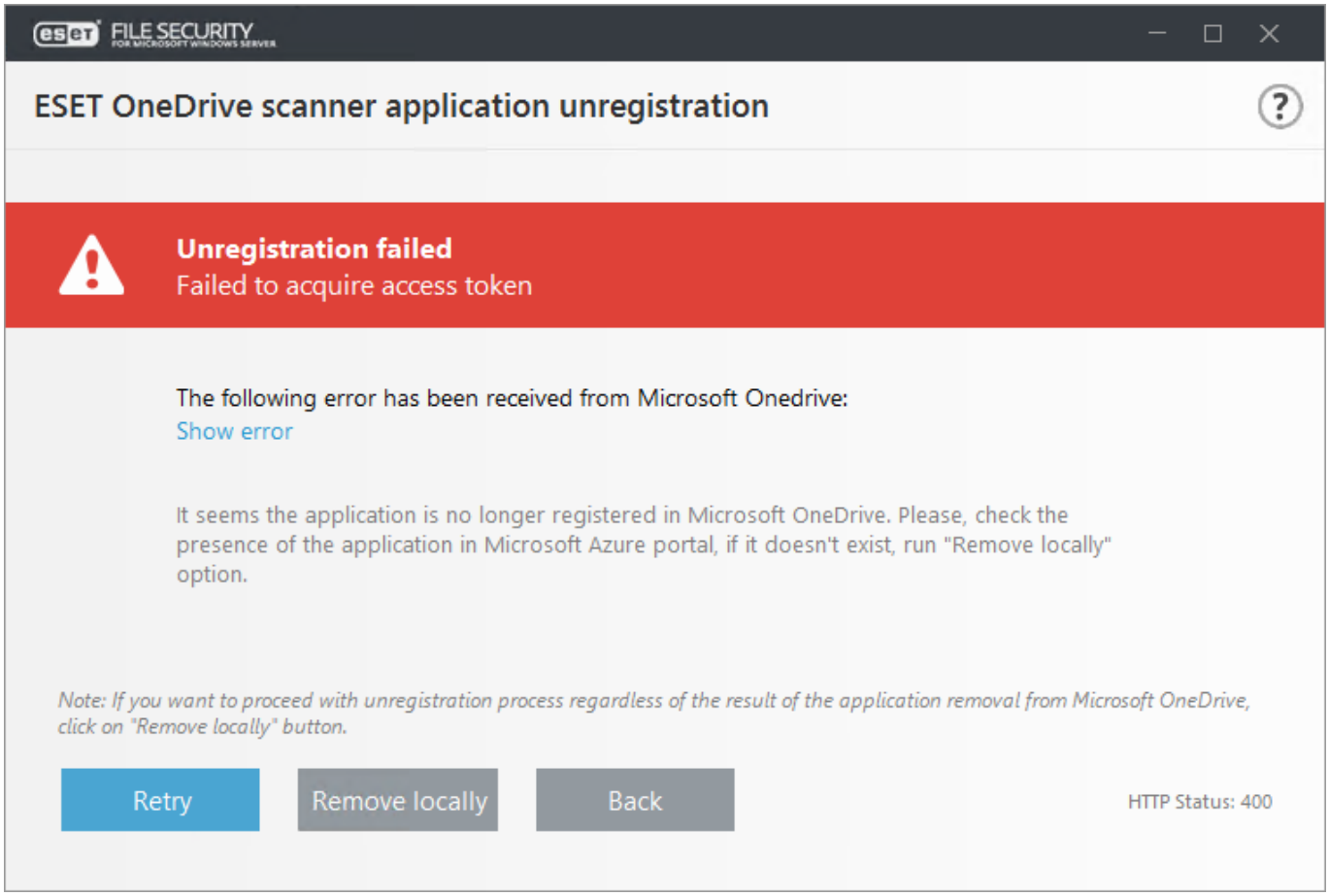
- Kayıt silme işlemi başarıyla tamamlanırsa, kayıt silme sihirbazı bununla ilgili bir ileti gösterir.



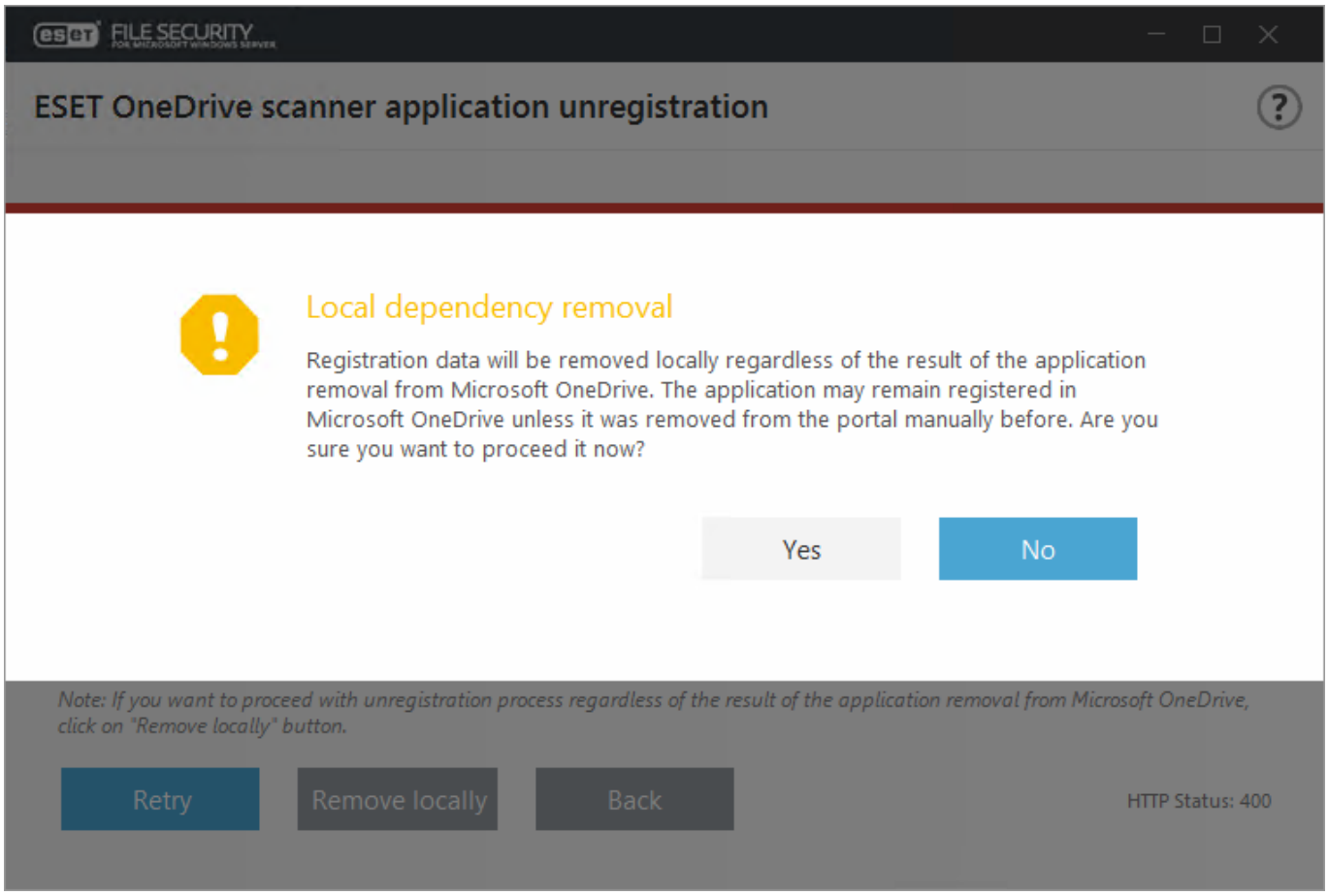
NOT
Kayıt silme işlemi başarısız oldu gibi bir hata iletisi alırsanız, bu birkaç nedenden kaynaklanıyor olabilir: genel ağ veya Microsoft OneDrive sunucularında internet bağlantısı sorunları veya ESET OneDrive tarayıcı uygulamasının artık Microsoft OneDrive'da kayıtlı olmaması. Hata iletilerinin lisesini ve bunları nasıl yöneteceğinizi görmek için aşağıdaki tabloya bakın.

Bazı hata iletişim kutuları, size yerel bağımlılıkları (bağlantı sorunları, Microsoft OneDrive'da mevcut olmayan uygulama vs.) kaldırma seçeneği sunar. ESET OneDrive tarayıcısını yerel olarak kaldırmak için şunları yapın:

- **Yeniden Dene** düğmesi çalışmazsa ve sorunlar devam ederse, kayıt kaldırma işlemine devam etmek için **Yerel Olarak Kaldır** öğesini tıklayın. Bu işlemle, ESET OneDrive tarayıcısı yerel bağımlılıkları kaldırılır.



- ESET OneDrive tarayıcısının yerel olarak kaldırılması işlemine devam etmek için **Evet**i tıklayın. ESET OneDrive taraması artık kullanılamaz. Kayıt işlemini yeniden yapmanız gerekir.



ÖNEMLİ
Yerel bağımlılığı kaldırma Azure portalındaki Uygulama kayıtlarına veya Office 365 portalındaki Uygulama izinlerinde herhangi bir değişiklik yapmaz. Microsoft OneDrive sunucularındaki ağ veya bağlantı sorunları nedeniyle ESET OneDrive tarayıcısını yerel olarak kaldırdıysanız, Azureda ESET OneDrive tarayıcı uygulamasını Uygulama kayıtlarından manuel olarak kaldırmanız gerekir. Azure portalında ESET OneDrive tarayıcısını nasıl bulacağınız ve sileceğiniz hakkında bilgi için OneDrive tarama ayarları bölümüne bakın.

ESET OneDrive tarayıcı kaydının silinmesi sırasında aşağıdaki hata iletilerinden birini alırsanız, önerilen çözüm için hata iletisi ayrıntılarına bakın:

Hata iletisi	Hata iletisi ayrıntıları
Azure uygulamasına bağlanılamadı. İnternet bağlantısı yok.	Ağ/internet bağlantınızı kontrol edip kayıt silme işlemini yeniden çalıştırın. ESET OneDrive tarayıcısı uygulamasının Microsoft OneDrive'dan kaldırmadan kayıt silme işlemine devam etmek istiyorsanız **Yerel olarak kaldır**'ı tıklayın.
Erişim belirteci alınamadı. Microsoft OneDrive'dan beklenmeyen bir hata alındı.	ESET OneDrive tarayıcı uygulaması artık Microsoft OneDrive'da kayıtlı değil. ESET OneDrive tarayıcı uygulaması Azure portalında mauel olarak silinmiş olabilir. ESET OneDrive tarayıcı uygulamasının Microsoft OneDrive veya Azure portalında olup olmadığını kontrol edin. Uygulama listelenmiyorsa, **Yerel olarak kaldır**'ı tıklayarak kayıt silme işlemine devam edin.
Erişim belirteci alınamadı. Microsoft OneDrive'dan bir sunucu hatası alındı.	Microsoft OneDrive HTTP 5xx hatası verdi. Kayıt silme işlemi şu anda tamamlanamıyor. Lütfen kayıt silmeyi daha sonra tekrar çalıştırmayı deneyin.
Microsoft OneDrive'dan aşağıdaki hata alındı.	Microsoft OneDrive sunucusu belirli hata kodu/adıyla geri dönerse **Hatayı göster**'i tıklayın.
Başka bir kurulum görevi zaten sürüyor.	Halihazırda çalışan bir kayıt silme görevi var. İlk kayıt silme işleminin tamamlanmasını bekleyin.

Genel ayarlar

İhtiyaçlarınıza göre genel ayarları ve seçenekleri yapılandırabilirsiniz. Soldaki menü, şu kategorilerden oluşur:

Algılama Altyapısı

İstenmeyen türde olabilecek, güvenilir olmayan, şüpheli uygulamaların algılanmasını ve Anti-Stealth korumasını etkinleştirin veya devre dışı bırakın. Gerçek zamanlı dosya sistemi korumasını, ThreatSense parametrelerini, Bulut tabanlı korumayı (ESET LiveGrid®), Kötü amaçlı yazılım taramalarını (İsteğe bağlı bilgisayar taraması ve diğer seçenekler), Hyper-V taraması ve HIPS'i yapılandırın.

Güncelle

Profil, algılama altyapısı yaşı, modül geri alımı için sistem görüntüleri, güncelleme türü, özel güncelleme sunucusu, bağlantı/proxy sunucusu, güncelleme aynası, güncelleme dosyalarına erişim, HTTP sunucu, ağ bağlantısı için kullanıcı hesabı ayrıntılar gibi güncelleme seçeneklerini yapılandırın.

Web ve e-posta

Protokol filtrelemesi ve istisnaları (Hariç tutulan uygulamalar ve IP adresleri), SSL/TLS protokol filtreleme seçenekleri, E-posta istemci koruması (entegrasyon, e-posta protokolleri, uyarılar ve bildirimler), Web erişim koruması (HTTP/HTTPS web protokolleri ve URL adresi yönetimi) ve e-posta istemcisi Kimlik Avı korumasını yapılandırmanıza olanak tanır.

Aygıt denetimi

Entegrasyonu etkinleştirin ve Aygıt kontrol Kuralları ve Gruplarını yapılandırın.

Araçların yapılandırılması

ESET CMD, ESET RMM, WMI sağlayıcı, ESET PROTECT tarama hedefleri, Windows Güncellemesi bildirimleri, Günlük dosyaları, Proxy sunucusu, E-posta bildirimleri, Tanılama, Küme gibi araçları özelleştirmenize olanak tanır.

Kullanıcı arabirimi

Programın Grafik kullanıcı arabirimi davranışını, Durumları, Lisans bilgilerini, Uyarılar ve bildirimleri, Parola korumasını, eShell istisna ilkesini vs. yapılandırın.

Algılama Altyapısı

Tespit altyapısı; dosyaları, e-postaları ve ağ iletişimini tarayarak kötü amaçlı sistem saldırılarına karşı koruma sağlar. Zararlı yazılım olarak sınıflandırılan bir nesne algılanırsa düzeltme başlatılır. Tespit altyapısı önce bu nesneyi engelleyerek ve ardından temizleme, silme veya karantinaya taşıma gibi işlemleri gerçekleştirerek tehdidi ortadan kaldırabilir.

Gerçek zamanlı ve makine öğrenimi koruması

Gelişmiş makine öğrenimi artık tespit altyapısının bir parçasıdır ve makine öğrenimine dayalı algılamayı iyileştiren gelişmiş bir koruma katmanı olarak işlev görür. Sözlükte bu tür koruma hakkında daha fazla bilgi edinebilirsiniz. Raporlama ve Koruma düzeylerini aşağıdaki kategorilerde yapılandırabilirsiniz:

Zararlı yazılım

Bilgisayar virüsü bilgisayarınızda bulunan dosyaların önüne veya arkasına eklenen kötü amaçlı bir kod parçasıdır. Ancak, "virüs" terimi çoğu zaman yanlış kullanılır. "Zararlı yazılım" (kötü amaçlı yazılım) daha doğru bir terimdir. Zararlı yazılım algılaması, makine öğrenimi bileşeniyle birlikte algılama altyapısı modülü tarafından gerçekleştirilir. Bu uygulama türleriyle ilgili daha fazla bilgi sözlükten edinilebilir.

İstenmeyen türden olabilecek uygulamalar (PUA'lar)

İstenmeyen türden olabilecek uygulama, kesin olarak kötü amaçlı olmayan bir yazılımdır. Ancak bu yazılımlar istenmeyen başka yazılımları yükleyebilir, dijital aygıtın davranışını değiştirebilir, kullanıcı tarafından onaylanmayan veya beklenmeyen faaliyetleri gerçekleştirebilir ya da net olmayan başka hedeflere sahip olabilir.
Bu kategori şunları içerir: reklam ekranı yazılımı, indirme sarmalayıcıları, çeşitli tarayıcı araç çubukları, yanlış yönlendiren davranışa sahip yazılımlar, bundleware, trackware vs.
Bu uygulama türleriyle ilgili daha fazla bilgi sözlükten edinilebilir.

Tehlikeli olabilecek uygulamalar

Paketleyici veya koruyucularla sıkıştırılan ve genellikle, özel sıkıştırma ve/veya şifreleme yöntemlerinden yararlanarak yürütülebilir dosyaların ters mühendisliğini engellemek veya dosya içeriğini gizlemek için (örneğin kötü amaçlı yazılımın varlığını saklamak için) kullanılan bir yazılımdır.
Bu kategoriye şunlar dahildir: çoğunlukla zararlı yazılımı sıkıştırmak için kullanılan paketleyici veya koruyucu ile sıkıştırılan tüm bilinmeyen uygulamalar.

Tehlikeli olabilecek uygulamalar

Bu sınıflandırmaya kötü amaçlara yönelik olarak suistimal edilebilen ticari, yasal yazılımlar girer. Güvenilir olmayan uygulama, kötü amaçlar doğrultusunda suistimal edilme olasılığı olan yasal ticari yazılım anlamına gelir.
Bu kategoriye şunlar dahildir: sızma araçları, lisans anahtarı oluşturucular, bilgisayar korsanlığı araçları, uzaktan erişim veya denetim araçları, şifre kırma uygulamaları ve tuş kaydediciler (kullanıcı tarafından gerçekleştirilen her bir tuş vuruşunu kaydeden programlar). Bu seçenek varsayılan olarak devre dışıdır.
Bu uygulama türleriyle ilgili daha fazla bilgi sözlükten edinilebilir.

Kategori Raporlama veya Koruma için bir eşiği (veya düzeyi) değiştirmeden önce aşağıdakileri okuyun:

Bildirme

Raporlama, algılama altyapısı ve makine öğrenimi bileşeni tarafından gerçekleştirilir. Raporlama eşiğini ortamınıza ve gereksinimlerinize daha iyi uyacak şekilde ayarlayabilirsiniz. Tek bir doğru yapılandırma yoktur. Bu nedenle, ortamınızdaki davranışı izlemenizi ve farklı bir Raporlama ayarının daha uygun olup olmadığına karar vermenizi öneririz.

Raporlama nesnelerle işlem yapmaz, bilgileri ilgili koruma katmanına aktarır. Koruma katmanı da buna uygun şekilde işlem yapar.

Agresif	**Maksimum duyarlılığa göre yapılandırılan raporlama. Daha fazla algılama bildirilir. Agresif ayar en güvenli seçenek gibi görünse de çoğu zaman fazla hassas olabildiğinden verimlilik üzerinde olumsuz etki yaratabilir.** NOT Agresif ayar, nesneleri hatalı bir şekilde kötü amaçlı olarak tanımlayabilir ve bu tür nesnelerle ilgili (Koruma ayarlarına bağlı olarak) işlem yapılır.
Dengeli	Bu ayar, performans, algılama doğruluğu oranları ve hatalı olarak bildirilen nesnelerin sayısı arasında en iyi dengeyi sağlar.
Temkinli	Hatalı olarak bildirilen nesnelerin sayısını en düşük düzeye indirecek şekilde yapılandırılan raporlama. Nesneler yalnızca çok yüksek bir olasılık olduğunda ve kötü amaçlı yazılım davranışıyla eşleştiğinde bildirilir.
Kapalı	Raporlama etkin değil. Algılamalar bulunmaz, rapor edilmez veya temizlenmez. NOT Zararlı yazılım raporlaması devre dışı bırakılamadığından **Kapalı** ayarı Zararlı yazılım için kullanılamaz.

Bu bölümdeki ayarları varsayılan değerlerine Döndürmek istiyorsanız bölüm başlığının yanındaki "U dönüşü" okunu tıklayın. Bu bölümde yaptığınız tüm değişiklikler kaybolur.

Koruma

Bir nesne yukarıdaki yapılandırmaya ve makine öğrenimi sonuçlarına göre raporlandığında engellenir ve işlem yapılır (temizlenir, silinir veya Karantinaya taşınır).

Agresif	**Bildirilen agresif (veya daha düşük) düzeydeki algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) işlemi başlatılır.**

Agresif	**Bildirilen agresif (veya daha düşük) düzeydeki algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) işlemi başlatılır.**
Dengeli	Bildirilen dengeli (veya düşük) seviyedeki algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) başlatılır.
Temkinli	Bildirilen temkinli algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) başlatılır.
Kapalı	Raporlama etkin değildir. Bu durumda, herhangi bir algılama bulunamaz, rapor edilmez veya temizlenmez. NOT Zararlı yazılım raporlaması devre dışı bırakılamadığından **Kapalı** ayarı Zararlı Yazılımlar için kullanılamaz.

Bu bölümdeki ayarları varsayılan değerlerine Döndürmek istiyorsanız bölüm başlığının yanındaki "U dönüşü" okunu tıklayın. Bu bölümde yaptığınız tüm değişiklikler kaybolur.

NOT
Varsayılan olarak, yukarıdaki makine öğrenimi koruma ayarları İsteğe bağlı bilgisayar taraması için de geçerlidir. Gerekirse, **İsteğe Bağlı ve Makine öğrenimi koruması** ayarlarını ayrı ayrı yapılandırabilirsiniz. **Gerçek zamanlı koruma ayarlarını kullan** seçeneğini devre dışı bırakıp yapılandırmaya devam etmek için geçiş simgesini tıklayın.

Makine Öğrenimini algılama

Tespit altyapısı; dosyaları, e-postaları ve ağ iletişimini tarayarak kötü amaçlı sistem saldırılarına karşı koruma sağlar. Zararlı yazılım olarak sınıflandırılan bir nesne algılanırsa düzeltme başlatılır. Tespit altyapısı önce bu nesneyi engelleyerek ve ardından temizleme, silme veya karantinaya taşıma gibi işlemleri gerçekleştirerek tehdidi ortadan kaldırabilir.

Gerçek zamanlı ve makine öğrenimi koruması

Gelişmiş makine öğrenimi artık tespit altyapısının bir parçasıdır ve makine öğrenimine dayalı algılamayı iyileştiren gelişmiş bir koruma katmanı olarak işlev görür. Sözlükte bu tür koruma hakkında daha fazla bilgi edinebilirsiniz. Raporlama ve Koruma düzeylerini aşağıdaki kategorilerde yapılandırabilirsiniz:

Zararlı yazılım

Bilgisayar virüsü bilgisayarınızda bulunan dosyaların önüne veya arkasına eklenen kötü amaçlı bir kod parçasıdır. Ancak, "virüs" terimi çoğu zaman yanlış kullanılır. "Zararlı yazılım" (kötü amaçlı yazılım) daha doğru bir terimdir. Zararlı yazılım algılaması, makine öğrenimi bileşeniyle birlikte algılama altyapısı modülü tarafından gerçekleştirilir. Bu uygulama türleriyle ilgili daha fazla bilgi sözlükten edinilebilir.

İstenmeyen türden olabilecek uygulamalar (PUA'lar)

İstenmeyen türden olabilecek uygulama, kesin olarak kötü amaçlı olmayan bir yazılımdır. Ancak bu yazılımlar istenmeyen başka yazılımları yükleyebilir, dijital aygıtın davranışını değiştirebilir, kullanıcı tarafından onaylanmayan veya beklenmeyen faaliyetleri gerçekleştirebilir ya da net olmayan başka hedeflere sahip olabilir.
Bu kategori şunları içerir: reklam ekranı yazılımı, indirme sarmalayıcıları, çeşitli tarayıcı araç çubukları, yanlış yönlendiren davranışa sahip yazılımlar, bundleware, trackware vs.
Bu uygulama türleriyle ilgili daha fazla bilgi sözlükten edinilebilir.

Tehlikeli olabilecek uygulamalar

Paketleyici veya koruyucularla sıkıştırılan ve genellikle, özel sıkıştırma ve/veya şifreleme yöntemlerinden yararlanarak yürütülebilir dosyaların ters mühendisliğini engellemek veya dosya içeriğini gizlemek için (örneğin kötü amaçlı yazılımın varlığını saklamak için) kullanılan bir yazılımdır.
Bu kategoriye şunlar dahildir: çoğunlukla zararlı yazılımı sıkıştırmak için kullanılan paketleyici veya koruyucu ile sıkıştırılan tüm bilinmeyen uygulamalar.

Tehlikeli olabilecek uygulamalar

Bu sınıflandırmaya kötü amaçlara yönelik olarak suistimal edilebilen ticari, yasal yazılımlar girer. Güvenilir olmayan uygulama, kötü amaçlar doğrultusunda suistimal edilme olasılığı olan yasal ticari yazılım anlamına gelir.
Bu kategoriye şunlar dahildir: sızma araçları, lisans anahtarı oluşturucular, bilgisayar korsanlığı araçları, uzaktan erişim veya denetim araçları, şifre kırma uygulamaları ve tuş kaydediciler (kullanıcı tarafından gerçekleştirilen her bir tuş vuruşunu kaydeden programlar). Bu seçenek varsayılan olarak devre dışıdır.
Bu uygulama türleriyle ilgili daha fazla bilgi sözlükten edinilebilir.

Kategori Raporlama veya Koruma için bir eşiği (veya düzeyi) değiştirmeden önce aşağıdakileri okuyun:

Bildirme

Raporlama, algılama altyapısı ve makine öğrenimi bileşeni tarafından gerçekleştirilir. Raporlama eşiğini ortamınıza ve gereksinimlerinize daha iyi uyacak şekilde ayarlayabilirsiniz. Tek bir doğru yapılandırma yoktur. Bu nedenle, ortamınızdaki davranışı izlemenizi ve farklı bir Raporlama ayarının daha uygun olup olmadığına karar vermenizi öneririz.

Raporlama nesnelerle işlem yapmaz, bilgileri ilgili koruma katmanına aktarır. Koruma katmanı da buna uygun şekilde işlem yapar.

Agresif	**Maksimum duyarlılığa göre yapılandırılan raporlama. Daha fazla algılama bildirilir. Agresif ayar en güvenli seçenek gibi görünse de çoğu zaman fazla hassas olabildiğinden verimlilik üzerinde olumsuz etki yaratabilir.** NOT Agresif ayar, nesneleri hatalı bir şekilde kötü amaçlı olarak tanımlayabilir ve bu tür nesnelerle ilgili (Koruma ayarlarına bağlı olarak) işlem yapılır.
Dengeli	Bu ayar, performans, algılama doğruluğu oranları ve hatalı olarak bildirilen nesnelerin sayısı arasında en iyi dengeyi sağlar.
Temkinli	Hatalı olarak bildirilen nesnelerin sayısını en düşük düzeye indirecek şekilde yapılandırılan raporlama. Nesneler yalnızca çok yüksek bir olasılık olduğunda ve kötü amaçlı yazılım davranışıyla eşleştiğinde bildirilir.
Kapalı	Raporlama etkin değil. Algılamalar bulunmaz, rapor edilmez veya temizlenmez. NOT Zararlı yazılım raporlaması devre dışı bırakılamadığından **Kapalı** ayarı Zararlı yazılım için kullanılamaz.

Bu bölümdeki ayarları varsayılan değerlerine Döndürmek istiyorsanız bölüm başlığının yanındaki "U dönüşü" okunu tıklayın. Bu bölümde yaptığınız tüm değişiklikler kaybolur.

OneDrive ve Makine öğrenimi koruması

Raporlama

Algılama altyapısı ve makine öğrenimi bileşeni tarafından gerçekleştirilir. Raporlama nesnelerle herhangi bir işlem yapmaz (bu işlem ilgili koruma katmanı tarafından yapılır).

Koruma

OneDrive bölümündeki parametreleri, bildirilen nesnelerle hangi işlemin yapılacağını belirtecek şekilde yapılandırın.

Bu bölümdeki ayarları varsayılan değerlerine Döndürmek istiyorsanız bölüm başlığının yanındaki "U dönüşü" okunu tıklayın. Bu bölümde yaptığınız tüm değişiklikler kaybolur.

Makine öğrenme korumasını kullanarak eShell aracını yapılandırın. eShell aracındaki Bağlam adı **MLP**'dir. eShell aracını etkileşimli modda açın ve MLP'ye gidin:

```
computer onedrive mlp
```

Şüpheli uygulamalar için geçerli raporlama ayarının ne olduğuna bakın:

```
get suspicious-reporting
```

Daha az katılıkta raporlama istiyorsanız ayarı Dikkatli olarak değiştirin:

```
set suspicious-reporting cautious
```

Tarama dışı öğeler

Tarama dışı öğeler, dosyaları ve klasörleri tarama dışında bırakmanızı sağlar. Tüm nesnelerin tehditlere karşı tarandığından emin olmak için, tarama dışı öğelerin yalnızca kesinlikle gerekli olduğunda oluşturulmasını öneririz. Bir nesneyi tarama dışında bırakmanızı gerektirecek durumlar, tarama sırasında sunucunuzu yavaşlatan büyük veri tabanı girişlerini taramayı veya taramayla çakışan yazılımı içerebilir (örneğin, yedekleme yazılımı).

UYARI
Tarama dışı bırakılan uzantılar, tarama dışı bırakılan işlemler veya tarama dışı bırakma filtresi ile karıştırılmamalıdır.

NOT
Bir dosya içindeki tehdit, söz konusu dosya tarama dışında bırakılma ölçütünü karşılıyorsa, Gerçek zamanlı dosya sistemi koruması modülü ya da Bilgisayar taraması modülü tarafından algılanmaz.

Tarama dışı bırakma işlemleri türünü seçin ve yeni bir işlem eklemek veya var olanı değiştirmek için **Düzenle**'yi tıklayın:

- Performansla ilgili tarama dışı bırakma işlemleri - Dosya ve klasörleri tarama dışı bırakın.
- Algılama dışı bırakma işlemleri - Nesneleri belirli ölçütler (yol, dosya hash'i veya algılama adı) kullanarak tarama dışında bırakın.

Performansla ilgili tarama dışı bırakma işlemleri

Bu özellik, dosya ve klasörleri tarama dışı bırakmanızı sağlar. Performansla ilgili tarama dışı bırakma işlemleri, görev açısından kritik uygulamaları dosya düzeyinde tarama dışı bırakmak veya taramanın anormal sistem davranışına ya da performansın düşmesine neden olacağı durumlarda kullanmak için yararlıdır.

Yol

Bu bilgisayar için belirtilen yolu (dosya veya dizin) tarama dışında bırakır. Yolun ortasında joker karakterleri - yıldız işaretini (*) kullanmayın. Daha fazla bilgi için aşağıdaki Bilgi Bankası makalesine bakın.

NOT
Klasör içeriklerini tarama dışı bırakmak için yıldız işaretini (*) yolun sonuna (*C:\Tools**) eklemeyi unutmayın. Tarayıcı açısından *Araçlar* da bir dosya adı olabileceği için *C:\Tools* tarama dışı bırakılmaz.

Yorum

Gelecekte tarama dışı bırakılan öğeyi kolayca tanımak için isteğe bağlı bir **Yorum** ekleyin.

ÖRNEK
Yolları yıldız işareti kullanarak tarama dışı bırakma:
*C:\Tools** - Bir klasör olduğunu ve tüm klasör içeriğinin (dosyalar ve alt klasörler) tarama dışı bırakılacağını göstermek için yol bir ters bölü çizgisi (\) ve yıldız (*) işaretiyle bitmelidir
C:\Tools.** - *C:\Tools** ile aynı davranış, başka bir ifadeyle, yinelemeli olarak işler
C:\Tools.dat* - Araçlar klasöründeki *dat* dosyaları tarama dışında bırakılır
C:\Tools\sg.dat - Tam yolda bulunan bu belirli dosyayı tarama dışında bırakır

ÖRNEK
Bir klasördeki tüm dosyaları tarama dışı bırakmak için söz konusu klasörün yolunu yazıp *.* maskesini kullanın
- Yalnızca doc dosyalarını tarama dışı bırakmak için *.doc* maskesini kullanın
- Yürütülebilir dosyanın adında belli sayıda karakter varsa (ve karakterler değişiyorsa) ve yalnızca ilk karakteri kesin olarak biliyorsanız (örneğin "D"), aşağıdaki biçimi kullanın:

D????.exe (soru işaretlerinin yerini eksik / bilinmeyen karakterler alır)

ÖRNEK
Tarama dışı bırakma işlemlerini tanımlamak için *%PROGRAMFILES%* gibi sistem değişkenlerini kullanın.
• Bu sistem değişkenini kullanarak Program Dosyaları klasörünü tarama dışı bırakmak isterseniz *%PROGRAMFILES%* yolunu kullanın (tarama dışı bırakma işlemlerine eklerken yolun sonuna ters eğik çizgi eklemeyi unutmayın)
• Bir *%HOMEDRIVE%* alt klasöründeki tüm dosyaları tarama dışında bırakmak istiyorsanız *%HOMEDRIVE%\Excluded_Directory*.** yolunu kullanın
Aşağıdaki değişkenler yolu tarama dışı bırakma biçiminde kullanılabilir:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Kullanıcıya özel sistem değişkenleri (*%TEMP%* veya *%USERPROFILE%* gibi) ya da ortam değişkenleri (*%PATH%* gibi) desteklenmemektedir.

Algılama dışı bırakılan öğeler

Bu, algılama adını, yolunu veya hash'ini kullanarak nesneleri tarama dışı bırakmanın başka bir yöntemidir. Algılama dışı bırakma işlemlerinde dosya ve klasörler tarama dışı bırakılmaz (örneğin performans hariç tutma işlemleri gibi). Algılama dışı bırakma işlemleri, nesneleri yalnızca algılama altyapısı tarafından algılandığında ve tarama dışı bırakma listesinde uygun bir kural bulunduğunda hariç tutar.

Algılama tabanlı tarama dışı bırakma işlemi oluşturmanın en kolay yolu **Günlük dosyaları** > Algılamalar'da mevcut olan bir algılamayı kullanmaktır. Bir günlük kaydını (algılamayı) sağ tıklayın ve **Tarama dışı bırakma işlemi oluştur**'u tıklayın. Bu, tarama dışı bırakma sihirbazını önceden tanımlanmış ölçütlerle açar.

Algılama hariç tutma işlemi oluşturmak için **Düzenle** > **Ekle**'yi (veya mevcut olanları değiştirirken **Düzenle**'yi) tıklayın ve aşağıdaki ölçütlerden bir ya da birkaçını belirtin (ölçütler birleştirilebilir):

Yol

Belirtilen yolu (dosya veya klasörü) tarama dışında bırakır. Belirli bir konum/dosyaya göz atabilirsiniz veya dizeyi manuel olarak girebilirsiniz. Yolun ortasında joker karakterleri - yıldız işaretini (*) kullanmayın. Daha fazla bilgi için aşağıdaki Bilgi Bankası makalesine bakın.

NOT
Klasör içeriklerini tarama dışı bırakmak için yıldız işaretini (*) yolun sonuna (*C:\Tools**) eklemeyi unutmayın. Tarayıcı açısından *Araçlar* da bir dosya adı olabileceği için *C:\Tools* tarama dışı bırakılmaz.

Karma

Dosya türünden, konumundan, adından veya uzantısından bağımsız olarak belirtilen bir karma (SHA1) temelinde bir dosyayı tarama dışı bırakır.

Algılama adı

Geçerli bir algılama (tehdit) adı girin. Tek başına algılama adına dayalı bir tarama dışı bırakma işlemi oluşturmak güvenlik riski doğurabilir. Algılama adını Yol ile birleştirmenizi öneririz. Bu tarama dışı bırakma ölçütleri yalnızca belirli algılama türleri için kullanılabilir.

Yorum

Gelecekte tarama dışı bırakılan öğeyi kolayca tanımak için isteğe bağlı bir **Yorum** ekleyin.

ESET PROTECT, algılama dışı bırakma işlemi oluşturmak ve bunu diğer bilgisayarlara/gruplara uygulamak için algılama dışı bırakılan öğeler yönetimi içerir.

Bir dosya grubunu kapsamak üzere joker karakterler kullanın. Soru işareti (*?*) tek bir değişken karakteri, yıldız işareti (***) ise sıfır veya daha çok karakter içeren bir değişken dizeyi gösterir.

ÖRNEK
Yolları yıldız işareti kullanarak tarama dışı bırakma:
*C:\Tools** - Bir klasör olduğunu ve tüm klasör içeriğinin (dosyalar ve alt klasörler) tarama dışı bırakılacağını göstermek için yol bir ters bölü çizgisi (\) ve yıldız (***) işaretiyle bitmelidir
C:\Tools.** - *C:\Tools** ile aynı davranış, başka bir ifadeyle, yinelemeli olarak işler
C:\Tools.dat* - Araçlar klasöründeki *dat* dosyaları tarama dışında bırakılır
C:\Tools\sg.dat - Tam yolda bulunan bu belirli dosyayı tarama dışında bırakır

ÖRNEK
Bir tehdidi tarama dışı bırakmak için şu biçimde geçerli bir algılama adı girin:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

ÖRNEK
Bir klasördeki tüm dosyaları tarama dışı bırakmak için söz konusu klasörün yolunu yazıp **.** maskesini kullanın
- Yalnızca doc dosyalarını tarama dışı bırakmak için **.doc* maskesini kullanın
- Yürütülebilir dosyanın adında belli sayıda karakter varsa (ve karakterler değişiyorsa) ve yalnızca ilk karakteri kesin olarak biliyorsanız (örneğin "D"), aşağıdaki biçimi kullanın:

D????.exe (soru işaretlerinin yerini eksik / bilinmeyen karakterler alır)

ÖRNEK
Tarama dışı bırakma işlemlerini tanımlamak için *%PROGRAMFILES%* gibi sistem değişkenlerini kullanın.
• Bu sistem değişkenini kullanarak Program Dosyaları klasörünü tarama dışı bırakmak isterseniz *%PROGRAMFILES%* yolunu kullanın (tarama dışı bırakma işlemlerine eklerken yolun sonuna ters eğik çizgi eklemeyi unutmayın)
• Bir *%HOMEDRIVE%* alt klasöründeki tüm dosyaları tarama dışında bırakmak istiyorsanız *%HOMEDRIVE%\Excluded_Directory*.** yolunu kullanın
Aşağıdaki değişkenler yolu tarama dışı bırakma biçiminde kullanılabilir:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Kullanıcıya özel sistem değişkenleri (*%TEMP%* veya *%USERPROFILE%* gibi) ya da ortam değişkenleri (*%PATH%* gibi) desteklenmemektedir.

Tarama dışı bırakma sihirbazı oluştur

Önerilen tarama dışı bırakma işlemi, algılama türüne göre önceden seçilir, ancak algılamalar için tarama dışı bırakma ölçütlerini daha ayrıntılı şekilde belirtebilirsiniz. **Ölçütleri Değiştir**'i tıklayın:

- **Spesifik dosyalar** – Her dosyayı SHA-1 hash'ine göre tarama dışı bırakın.
- **Algılama** – Bu tür algılama içeren her dosyayı tarama dışı bırakmak için algılama adını belirtin.
- **Yol + Algılama** – Belirtilen konumda bulunan bir algılamaya sahip her dosyayı tarama dışı bırakmak için algılama adını ve yolunu (dosya adı dahil) belirtin.

Gelecekte tarama dışı bırakılan öğeyi kolayca tanımak için isteğe bağlı bir **Yorum** ekleyin.

Gelişmiş seçenekler

Anti-Stealth teknolojisi

Kendini işletim sisteminden gizleyebilen kök setleri gibi tehlikeli programları algılamayı sağlayan gelişmiş bir sistemdir. Bu, bu tür programları normal sınama teknikleri kullanarak saptamanın mümkün olmadığı anlamına gelir.

AMSI

Microsoft Antimalware Scan Interface (AMSI) aracının Windows komut dosyası Ana Bilgisayarı tarafından yürütülen Powershell komut dosyalarını taramasına izin verin.

Otomatik dışlamalar

Sunucu uygulamaları ve işletim sistemleri geliştiricileri, çoğu ürün için önemli çalışma dosyalarından ve klasörlerden oluşan kümelerin, zararlı yazılım taramalarının dışında bırakılmalarını önerir. Zararlı Yazılım taramaları, sunucu performansı üzerinde negatif etkiye ya da çakışmalara neden olabilir ve bu durum bazı uygulamaların sunucuda çalışmasını engelleyebilir. Özel durumlar, potansiyel çakışma riskinin en düşük düzeye indirilmesine ve Zararlı Yazılıma Karşı Koruma yazılımı çalışırken sunucunun genel performansının artırılmasına yardımcı olur. ESET sunucu ürünleri için eksiksiz tarama dışında bırakılan dosyalar listesine bakın.

ESET Server Security önemli sunucu uygulamalarını ve sunucu işletim sistemi dosyalarını tespit eder ve bunları otomatik olarak Tarama Dışı Bırakma listesine ekler. Otomatik dışlamalar, varsayılan olarak etkinleştirilir. Her bir sunucu uygulaması tarama dışı bırakmasını, kaydırma çubuğunu kullanarak aşağıdaki sonuçla birlikte devre dışı bırakabilir/etkinleştirebilirsiniz:

- Etkinleştirildiğinde, buna ait önemli dosyalar ve klasörler, tarama dışında bırakılan dosyalar listesine eklenir. Sunucunun her yeniden başlatılışında sistem, tarama dışı öğeleri otomatik olarak denetler ve sistem veya uygulama değişiklikleri varsa listeyi günceller (örneğin yeni bir sunucu uygulaması yüklendiğinde). Bu ayar, önerilen Otomatik dışlamaların her zaman uygulanmasını sağlar.
- Devre dışı bırakıldığında, otomatik olarak dışarıda bırakılan dosyalar ve klasörler listeden kaldırılacaktır. Manuel olarak girilen kullanıcı tanımlı tarama dışı bırakmalar etkilenmeyecektir.

Otomatik tarama dışı bırakmaları tanımlamak ve oluşturmak için ESET Server Security, yükleme klasöründe bulunan özel *eAutoExclusions.exe* uygulamasını kullanır. Sizin herhangi bir etkileşimde bulunmanız gerekmez ancak sisteminizde algılanan sunucu uygulamalarını listelemek için `eAutoExclusions.exe -servers` komutunu yürüterek komut satırını kullanabilirsiniz. Tam sentaksı görüntülemek için şunu kullanın: `eAutoExclusions.exe -?`.

Paylaşılan yerel önbellek

ESET Paylaşılan yerel önbellek, ağda yinelenen taramayı ortadan kaldırarak sanallaştırılmış ortamlarda performansı artırır. Bu, her bir dosyanın yalnızca bir kez taranmasını ve paylaşılan önbellekte depolanmasını sağlar. Ağınızdaki dosyaları ve klasörleri tarama hakkındaki bilgileri yerel önbelleğe kaydetmek için **Önbelleğe alma seçeneği** düğmesini açın. Yeni bir tarama gerçekleştirirseniz, ESET Server Security önbellekte taranan dosyaları arar. Dosyalar eşleşirse bunlar tarama dışında bırakılır.

Önbellek sunucusu ayarı aşağıdakileri içerir:

- **Ana bilgisayar adı** - Önbelleğin bulunduğu bilgisayarın adı veya IP adresi.
- **Bağlantı noktası** - İletişim için kullanılan bağlantı noktası sayısı (Paylaşılan yerel önbellekte belirlenen ile aynı).
- **Parola** - Gerekirse Paylaşılan yerel önbellek parolasını belirtin.

Sızıntı algılandı

Sızıntılar sisteme web sayfaları, paylaşılan klasörler, e-posta veya çıkarılabilir aygıtlar (USB, harici diskler, CD, DVD, disket, vb.) gibi çeşitli giriş noktalarından ulaşabilir.

Standart davranış

Sızıntıların, ESET Server Security tarafından nasıl işlendiğine dair genel bir örnek olarak, sızıntılar şunların kullanımıyla algılanabilir:

- Gerçek zamanlı dosya sistemi koruması
- Web erişimi koruması
- E-posta istemci koruması
- İsteğe bağlı bilgisayar taraması

Bunların her biri standart temizleme düzeyini kullanır ve dosyayı temizleyip Karantinaya taşımaya veya bağlantıyı sonlandırmaya çalışır. Ekranın sağ alt köşesindeki bildirim alanında bir bildirim penceresi görüntülenir. Temizleme düzeyleri ve davranışı ile ilgili daha fazla bilgi için bkz. Temizleme.

Temizleme ve silme

Gerçek zamanlı dosya sistemi korumasının gerçekleştireceği önceden tanımlı bir eylem yoksa, uyarı penceresinde bir seçenek belirlemeniz istenir. Genellikle, **Temizle**, **Sil** ve **Eylem yok** seçenekleri kullanılabilir. Etkilenen dosyaları temizlenmemiş olarak bırakacağından **Eylem yok** seçeneğinin belirlenmesi önerilmez. Burada geçerli olan özel durum, dosyanın zararsız olduğundan ve yanlışlıkla algılandığından emin olduğunuz durumdur.

Bir dosya, kendisine kötü amaçlı kod ekleyen bir virüsün saldırısına uğradıysa temizleme işlemi uygulayın. Durum buysa, etkilenen dosyayı temizlemeden önceki özgün durumuna geri yüklemek için temizlemeyi deneyin. Dosya tümüyle kötü amaçlı kod içeriyorsa silinir.

Etkilenen dosya bir sistem işlemi tarafından "kilitlendiyse" veya kullanılıyorsa, genellikle ancak serbest bırakıldıktan sonra silinir (normalde sistem yeniden başlatıldıktan sonra).

Birden çok tehdit

Etkilenen dosyalar Bilgisayar taraması sırasında temizlenmediyse (veya Temizleme düzeyi **Temizleme Yok** olarak ayarlandıysa), bir uyarı penceresi, görüntülenen dosyalar için eylem seçmenizi ister. Listedeki her bir tehdit için ayrı ayrı eylem seçin veya **Listelenen tüm tehditler için eylem seç** öğesini kullanabilir ve listedeki tüm tehditler için aynı eylemi seçebilirsiniz, ardından **Bitir**'i tıklatın.

Arşivlerdeki dosyaları silme

Varsayılan temizleme modunda, tüm arşiv yalnızca etkilenen dosyalar içeriyor ve temiz dosya içermiyorsa tümüyle silinir. Başka bir deyişle, arşivler zararsız temiz dosyalar da içeriyorsa silinmez. Katı kurallı temizleme taraması gerçekleştirirken dikkatli olun; Katı kurallı temizleme etkinken arşivde tek bir etkilenen dosya bulunsa bile, arşivdeki diğer dosyaların durumuna bakılmaksızın arşiv tümüyle silinir.

Gerçek zamanlı dosya sistemi koruması

Gerçek zamanlı dosya sistemi koruması sistemde zararlı yazılımla ilgili tüm olayları denetler. Bilgisayarınızda açılan, oluşturulan veya çalıştırılan tüm dosyalar kötü amaçlı yazılım koduna karşı taranır. Varsayılan olarak, Gerçek zamanlı dosya sistemi koruması sistem başlatılırken başlatılır ve kesintisiz tarama sağlar. Özel durumlarda (örneğin, başka bir gerçek zamanlı tarayıcıyla bir çakışma varsa) **Gerçek zamanlı dosya sistemi koruması** > **Temel** altındaki **Gelişmiş ayarlar** (**F5**) içinden **Gerçek zamanlı dosya sistemi korumasını otomatik başlat** seçeneği devre dışı bırakılarak gerçek zamanlı koruma uygulanmayabilir.

ESET Server Security, bulut kademelendirmesi etkinleştirilmiş Azure File Sync agent kullanan makinelerle uyumludur. ESET Server Security, *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS* öznitelikli dosyaları tanır.

Taranacak medya

Varsayılan olarak tüm medya türleri olası tehditlere karşı taranır:

- **Yerel sürücüler** - Tüm sistem sabit sürücülerini denetler.
- **Çıkarılabilir medya** - CD/DVD'leri, USB depolamayı, Bluetooth aygıtlarını vb. denetler.
- **Ağ sürücüleri** - Tüm eşlenen sürücüleri tarar.

Varsayılan ayarları kullanmanızı ve yalnızca belirli durumlarda (örneğin belirli medya türlerini denetlerken veri aktarımı önemli ölçüde yavaşladığında) değiştirmenizi öneririz.

Şu durumda tara

Varsayılan olarak tüm dosyalar; açıldığında, oluşturulduğunda veya yürütüldüğünde taranır. Bilgisayarınız için en üst düzeyde gerçek zamanlı koruma sağladığından, şu varsayılan ayarları korumanızı öneririz:

- **Dosya açıldığında** - Dosya açıldığında / erişildiğinde taranır.
- **Dosya oluşturma** - Dosyalar oluşturulduğunda / değiştirildiğinde taranır.
- **Dosya yürütme** - Dosyalar yürütüldüğünde taranır.
- **Çıkarılabilir ortam erişimi** - Çıkarılabilir depolamaya erişirken tarama. Cihaza önyükleme kesimi içeren çıkarılabilir ortam eklendiğinde önyükleme kesimi hemen taranır. Bu seçenek çıkarılabilir ortam dosyası taramasını etkinleştirmez. Çıkarılabilir ortam dosyası tarama, **Taranacak medya** > **Çıkarılabilir medya**'da bulunur. Çıkarılabilir medya önyükleme kesimi erişiminin düzgün çalışması için ThreatSense parametrelerinde **Önyükleme kesimleri/UEFI'yi etkin** halde tutun.

Tarama dışı tutma işlemlerini yerine getirir

Belirli işlemleri tarama dışı bırakmanıza olanak sağlar. Örneğin yedekleme çözümü işlemleri ve tarama dışı bırakılan bu tür işlemle ilişkilendirilen tüm dosya işlemleri yoksayılır ve güvenli olarak algılanır, böylece yedekleme işleminin engellenmesi en düşük düzeye indirilir.

ThreatSense parametreleri

Gerçek zamanlı dosya sistemi koruması tüm medya türlerini kontrol eder ve bir dosyaya erişme gibi çeşitli sistem olayları tarafından tetiklenir. Gerçek zamanlı dosya sistemi koruması, yeni oluşturulmuş dosyalarda, mevcut dosyalardan daha farklı işlem uygulayacak şekilde yapılandırılabilir. Örneğin, Gerçek zamanlı dosya sistemi korumasını yeni oluşturulmuş dosyaları daha yakından izleyecek şekilde yapılandırabilirsiniz.

Gerçek zamanlı koruma kullanılırken sistem kaynaklarının minimum düzeyde kullanılmasını sağlamak için, zaten taranmış olan dosyalar sürekli olarak taranmaz (değiştirilmedikleri sürece). Her algılama altyapısı veri tabanı güncellemesinden sonra dosyalar hemen tekrar taranır. Bu davranış **Akıllı optimizasyon** kullanılarak denetlenir. Bu **Akıllı optimizasyon** devre dışı bırakılırsa tüm dosyalar her erişildiğinde taranır. Bu seçeneği değiştirmek isterseniz, **F5** tuşuna basarak **Gelişmiş ayarları** açın ve **Algılama Altyapısı** > **Gerçek zamanlı dosya sistemi koruması** seçeneğini genişletin. **ThreatSense parametresi** > **Diğer** öğesine tıklatın ve **Akıllı optimizasyonu etkinleştir** seçeneğini belirleyin veya seçimini kaldırın.

Ek ThreatSense parametreleri

Yeni oluşturulan ve değiştirilen dosyalar için ek ThreatSense parametreleri veya **Yürütülen dosyalar için ek ThreatSense parametreleri**'nin ayrıntılı seçeneklerini değiştirebilirsiniz.

ThreatSense parametreleri

ThreatSense, birçok karmaşık tehdit algılama yönteminden oluşan bir teknolojidir. Bu teknoloji proaktiftir; yani, yeni bir tehdidin ilk yayılmaya başladığı zamanlarda da koruma sağlar. Sistem güvenliğini önemli ölçüde yükseltmek için birlikte çalışan kod analizinin, kod öykünmesinin, genel imzaların ve virüs imzalarının bir bileşimini kullanır. Tarama altyapısı birkaç veri akışını aynı anda denetleme, böylece verimliliği ve algılama hızını en üst seviyeye çıkarma becerisine sahiptir. Ayrıca ThreatSense teknolojisi kök setleri de başarıyla ortadan kaldırır.

> NOT
> Başlangıçta otomatik dosya denetimi hakkında bilgi edinmek için Başlangıç taraması bölümüne bakın.

ThreatSense altyapısı ayar seçenekleri birkaç tarama parametresi belirtmenize olanak tanır:

- **Taranacak dosya türleri ve uzantıları**
- **Çeşitli algılama yöntemlerinin bileşimi**
- **Temizleme düzeyleri, vb.**

Ayarlar penceresine girmek için **ThreatSense teknolojisi kullanan herhangi bir modül için Gelişmiş ayarlar** (**F5**) penceresinde **ThreatSense altyapısı parametre ayarları** seçeneğini tıklayın (aşağı bakın). Farklı güvenlik senaryoları farklı yapılandırmalar gerektirebilir. Bu göz önüne alınarak, ThreatSense aşağıdaki koruma modülleri için ayrı ayrı yapılandırılabilir nitelikte hazırlanmıştır:

- Hyper-V taraması
- OneDrive taraması
- Gerçek zamanlı dosya sistemi koruması
- Kötü amaçlı yazılım taramaları
- Boşta durumu taraması
- Başlangıç taraması
- Belge koruması
- E-posta istemci koruması
- Web erişimi koruması

ThreatSense parametreleri her modül için optimize edilmiştir ve bu parametrelerin değiştirilmesi sistemin çalışmasını önemli ölçüde etkileyebilir. Örneğin, parametreleri çalışma zamanı paketleyicilerini her zaman tarayacak şekilde değiştirmek veya Gerçek zamanlı dosya sistemi koruması modülünde gelişmiş sezgisel taramayı etkinleştirmek sistemin yavaşlamasına neden olabilir (normalde, bu yöntemler kullanılarak yalnızca yeni oluşturulmuş dosyalar taranır). Bilgisayar taraması dışındaki tüm modüller için varsayılan ThreatSense parametrelerini değiştirmeden bırakmanızı öneririz.

Taranacak nesneler

Bu bölüm, hangi bilgisayar bileşenlerinin ve dosyaların sızıntılara karşı taranacağını tanımlamanıza olanak tanır.

İşletim belleği

Sistemin işletim belleğine saldırıda bulunan tehditler için tarama yapar.

Önyükleme kesimleri/UEFI

Önyükleme kesimlerini MBR'de (Ana Önyükleme Kaydı) virüslere karşı tarar. Hyper-V Virtual Machine varsa, MBR diski yalnızca salt okunur modda taranır.

E-posta dosyaları

Program, şu uzantıları destekler: DBX (Outlook Express) ve EML.

Arşivler

Program aşağıdaki uzantıları destekler: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE ve diğer birçok uzantı.

Kendiliğinden açılan arşiv dosyaları

Kendiliğinden açılan arşiv dosyaları (SFX), kendilerini açmak için özel programlar (arşivler) gerekmeyen arşiv dosyalarıdır.

Çalışma zamanı paketleyicileri

Çalışma zamanı paketleyicileri, yürütüldükten sonra (standart arşiv türlerinin aksine) bellekte açılır. Standart statik paketleyicilere ek olarak (UPX, yoda, ASPack, FSG vb.) tarayıcı, kod öykünmesini kullanarak başka birçok paketleyici türünü tanıyabilir.

Tarama seçenekleri

Sistemi sızıntılara karşı tararken kullanılacak yöntemleri seçin. Kullanılabilir seçenekler şunlardır:

Sezgisel tarama

Sezgisel tarama, programların etkinliğini (kötü amaçlı) analiz eden bir algoritmadır. Bu teknolojinin en temel getirisi, var olmayan veya önceki algılama altyapısı tarafından bilinmeyen kötü amaçlı yazılımları tanıma özelliğine sahip olmasıdır.

Gelişmiş sezgisel tarama/DNA imzalar

Gelişmiş sezgisel tarama ESET tarafından geliştirilen benzersiz bir sezgisel tarama algoritmasından oluşur, bilgisayar solucanlarını ve truva atlarını algılamak için optimize edilmiş ve yüksek düzeyli programlama dillerinde yazılmıştır. Gelişmiş sezgisel tarama kullanımı ESET ürünlerinin tehdit algılama özelliklerini büyük oranda artırır. İmzalar, virüsleri güvenilir bir şekilde algılayabilir ve belirleyebilir. Otomatik güncelleme sistemini kullanarak, tehdidin tespitinden sonraki birkaç saat içinde yeni imzalar kullanılabilir. İmzaların tek olumsuz tarafı, yalnızca bildikleri virüsleri (veya bu virüslerin çok az değiştirilmiş sürümlerini) algılamalarıdır.

Temizleme

Temizleme ayarları, etkilenen dosyaları temizlerken tarayıcı davranışını belirler. 3 temizleme düzeyi vardır:

Temizleme yok

Etkilenen dosyalar otomatik olarak temizlenmez. Program uyarı penceresi görüntüler ve kullanıcının bir eylem seçmesine olanak verir. Bu düzey, sızıntı durumunda hangi adımların gerçekleştirilmesi gerektiğini bilen daha

ileri düzey kullanıcılar için tasarlanmıştır.

Normal temizleme

Program, etkilenen dosyayı önceden tanımlanan bir eylemi temel alarak (sızıntı türüne göre) otomatik olarak temizlemeye veya silmeye çalışır. Etkilenen dosyanın algılanması ve silinmesi, ekranın sağ alt köşesindeki bir bildirim ile belirtilir. Doğru eylem otomatik olarak seçilemiyorsa, program başka izleme eylemleri sağlar. Önceden tanımlanan bir eylem tamamlanamadığında da bu yapılır.

Katı kurallı temizleme

Program etkilenen tüm dosyaları temizler veya siler. Yalnızca sistem dosyaları bu işlemin dışında tutulur. Bir dosyayı temizlemek mümkün değilse kullanıcıya, ne tür bir eylem gerçekleştirileceği sorulur.

UYARI
Bir arşivde virüsten etkilenmiş dosya veya dosyalar varsa, arşivle ilgili olarak iki seçenek vardır. Varsayılan mod olan **Standart temizleme** modunda, arşivde bulunan tüm dosyaların etkilenmesi durumunda arşiv tümüyle silinir. **Katı kurallı temizleme** modunda, arşivde virüsten etkilenmiş en az bir dosya varsa, arşivdeki diğer dosyaların durumuna bakılmaksızın arşiv silinir.

ÖNEMLİ
Hyper-V ana bilgisayarı Windows Server 2008 R2 SP2'de çalışıyorsa, **Standart temizleme** ve **Katı kurallı temizleme** desteklenmez. Sanal Makine disklerinin taranması salt okunur modda yapılır, temizleme yapılmaz. Seçilen temizleme düzeyinden bağımsız olarak tarama işlemi her zaman salt okunur modda gerçekleştirilir.

Tarama dışı öğeler

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı bir dosyanın türünü ve içeriğini tanımlar. ThreatSense parametre ayarlarının yer aldığı bu bölüm, tarama dışı bırakılacak dosyaların türlerini tanımlamanızı sağlar.

Diğer

İsteğe bağlı bilgisayar taraması için ThreatSense altyapısı parametre ayarlarını yapılandırırken **Diğer** bölümünde bulunan aşağıdaki seçenekler de kullanılabilir:

Alternatif veri akışlarını (ADS) tara

NTFS dosya sistemi tarafından kullanılan alternatif veri akışları (ADS), normal tarama teknikleriyle görülemeyen dosya ve klasör ilişkilendirmeleridir. Pek çok sızıntı, kendisini alternatif veri akışları olarak göstererek algılanmamaya çalışır.

Arka plan taramalarını düşük öncelikle çalıştır

Her tarama dizisi belirli miktarda sistem kaynağı tüketir. Sistem kaynaklarını aşırı yükleyen programlarla çalışıyorsanız, düşük öncelikli arka plan taramasını etkinleştirebilir ve uygulamalarınız için kaynak tasarrufu yapabilirsiniz.

Tüm nesneleri günlüğe kaydet

Bu seçenek belirlenirse günlük dosyası, etkilenmeyenler de dahil olmak üzere taranan tüm dosyaları gösterir.

Smart optimizasyonu etkinleştir

Akıllı Optimizasyon etkin durumdayken en yüksek tarama hızları korunur ve en etkili tarama düzeyinin sağlanması için en uygun ayarlar kullanılır. Çeşitli koruma modülleri, farklı tarama yöntemlerinden faydalanarak ve bunları belirli dosya türlerine uygulayarak akıllı tarama yapabilir. Smart Optimizasyon devre dışı bırakılırsa, bir tarama gerçekleştirilirken yalnızca belirli modüllerin ThreatSense çekirdeğindeki kullanıcı tanımlı ayarlar uygulanır.

Son erişim zaman damgasını koru

Taranan dosyaların erişim zamanını güncellemek yerine orijinal erişim zamanını tutmak için bu seçeneği belirleyin (örneğin, veri yedekleme sistemleri ile kullanmak için).

Sınırlar

Sınırlar bölümü, taranacak nesnelerin maksimum boyutunu ve taranacak arşivlerin iç içe geçme düzeylerini belirtmenize olanak sağlar:

Varsayılan nesne ayarları

Varsayılan ayarları kullanmak için etkinleştirin (sınır yok). ESET Server Security özel ayarlarınızı yoksayar.

Maksimum nesne boyutu

Taranacak nesnelerin maksimum boyutunu tanımlar. Belirli bir koruma modülü yalnızca belirtilen boyuttan küçük olan nesneleri tarayacaktır. Bu seçenek, yalnızca büyük nesneleri tarama dışında tutmaya yönelik belirli gerekçeleri olabilecek ileri düzey kullanıcılar tarafından değiştirilmelidir. Varsayılan değer: sınırsız.

Nesne için maksimum tarama süresi (sn.)

Bir nesneyi taramaya yönelik maksimum zaman değerini tanımlar. Buraya kullanıcı tanımlı bir değer girilirse söz konusu süre geçtikten sonra koruma modülü, taramanın bitmiş olup olmadığına bakmaksızın nesneyi taramayı durdurur. Varsayılan değer: sınırsız.

Arşiv tarama ayarları

Arşiv tarama ayarlarını değiştirmek için **Varsayılan arşiv tarama ayarları** seçeneğinin seçimini kaldırın.

Arşiv iç içe geçme düzeyi

Arşiv taramasının maksimum derinliğini belirtir. Varsayılan değer: 10. Bir e-postadaki arşiv eki birinci düzey olarak değerlendirildiğinden, Posta kutusu aktarım koruması tarafından algılanan nesneler için gerçek iç içe geçme düzeyi +1'dir.

ÖRNEK
İç içe geçme düzeyini 3 olarak ayarlamışsanız, iç içe geçme düzeyi 3 olan bir arşiv dosyası bir aktarım katmanında yalnızca gerçek düzeyi 2'ye kadar taranacaktır. Bu nedenle, Posta kutusu aktarım koruması tarafından iç içe geçme düzeyi 3'e kadar taranan arşivleriniz varsa, **Arşiv iç içe geçme düzeyi** değerini 4'e ayarlayın.

Arşivde maksimum dosya boyutu

Bu seçenek, taranacak arşivlerde bulunan dosyaların (ayıklandıklarında) maksimum dosya boyutunu

belirtmenize olanak tanır. Varsayılan değer: sınırsız

NOT
Varsayılan değerlerin değiştirilmesi önerilmez; normal koşullarda bunları değiştirmenize neden olacak bir durumla karşılaşmazsınız.

Ek ThreatSense parametreleri

Yeni oluşturulan ve değiştirilen dosyalar için ek ThreatSense parametreleri

Yeni oluşturulmuş veya değiştirilmiş dosyaların etkilenme olasılığı, mevcut dosyalarla kıyaslandığında daha yüksektir. Bundan dolayı, program bu dosyaları ilave tarama parametreleriyle kontrol eder. Yaygın imza tabanlı tarama yöntemlerinin yanı sıra modül güncellemesi yayınlanmadan önce yeni tehditleri algılayabilen gelişmiş sezgisel tarama kullanılır. Yeni oluşturulmuş dosyaların yanı sıra, kendiliğinden ayıklanan dosyalarda (.sfx) ve çalışma zamanı paketleyicilerinde (dahili kullanımda sıkıştırılan yürütülebilir dosyalar) tarama yapılır. Varsayılan olarak, arşivler 10. iç içe geçme düzeyine kadar taranır ve gerçek boyutlarına bakılmaksızın denetlenir. Arşiv tarama ayarlarını değiştirmek için **Varsayılan arşiv tarama ayarları** öğesini devre dışı bırakın.

Yürütülen dosyalar için ek ThreatSense parametreleri

Varsayılan olarak, dosyalar yürütüldüğünde Gelişmiş sezgisel tarama kullanılır. Etkinleştirildiğinde, sistem performansı üzerindeki etkiyi azaltmak için Akıllı optimizasyon ve ESET LiveGrid® uygulamasının etkin olmasını kesinlikle öneririz.

Tarama dışında bırakılan dosya uzantıları

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı, bir dosyanın türünü tanımlar. Normalde tüm dosyalar taranır. Ancak belirli bir uzantıya sahip dosyaları tarama dışında bırakmanız gerekiyorsa ThreatSense parametre ayarları, uzantılarına bağlı olarak dosyaları tarama dışında bırakmanızı sağlar. Tarama dışı bırakma, belirli dosya türlerini tarama bir uygulamanın düzgün çalışmasını engelliyorsa kullanışlı olabilir.

ÖRNEK
Listeye yeni bir uzantı eklemek için **Ekle**'yi tıklayın. Uzantıyı metin alanına (örneğin `tmp`) yazıp **Tamam**'ı tıklayın. **Birden fazla değer gir** öğesini seçtiğinizde çizgiler, virgüller veya noktalı virgüller ile ayrılmış birden fazla dosya uzantısı ekleyebilirsiniz. (örneğin, açılır menüden ayırıcı olarak **Noktalı virgül** seçeneğini belirleyin ve`edb;eml;tmp` yazın.
? (soru işareti) özel sembolü kullanabilirsiniz. Soru işareti, herhangi bir sembolü temsil eder (örneğin `?db`).

NOT
Windows işletim sisteminde tüm dosyalar için uzantıyı (dosya türü) görüntülemek üzere **Denetim Masası** > **Klasör Seçenekleri** > **Görüntüle** alanında **Bilinen dosya türleri için uzantıları gizle** seçeneğinin işaretini kaldırın.

Tarama dışı tutma işlemlerini yerine getirir

İşlemler özel durumları özelliği, uygulama işlemlerini yalnızca Anti-Malware Erişim tabanlı tarama dışında bırakır. Özel sunucuların (uygulama sunucusu, depolama sunucusu vs.) kritik rolüne bağlı olarak her türden olaydan

zamanında kurtarmayı garantilemek için düzenli yedekleme zorunludur. Yedekleme hızını, işlem bütünlüğünü ve hizmetin kullanılabilirliğini iyileştirmek için yedekleme sırasında, dosya düzeyinde zararlı yazılım korumasıyla çakıştığı bilinen bazı teknikler vardır. Benzer sorunlar, sanal makinelerin canlı olarak taşınması denemelerinde de ortaya çıkabilir. Her iki durumu da önlemenin etkili tek yolu anti-malware yazılımını devre dışı bırakmaktır. Belirli işlemler hariç tutularak (örneğin yedekleme çözümü işlemleri) hariç tutulan bu tür işlemlerle ilişkilendirilen tüm dosya işlemleri, yoksayılır ve bunların güvenli olduğu düşünülür. Bu sayede yedekleme süreciyle olası çakışmalar en düşük düzeye indirilir. İstisnaları oluştururken dikkatli olmanızı öneririz (hariç tutulan bir yedekleme aracı herhangi bir uyarıyı tetiklemeden enfekte dosyalara erişebilir. Süresi uzatılan izinlere yalnızca gerçek zamanlı koruma modülünde izin verilmesinin nedeni budur.

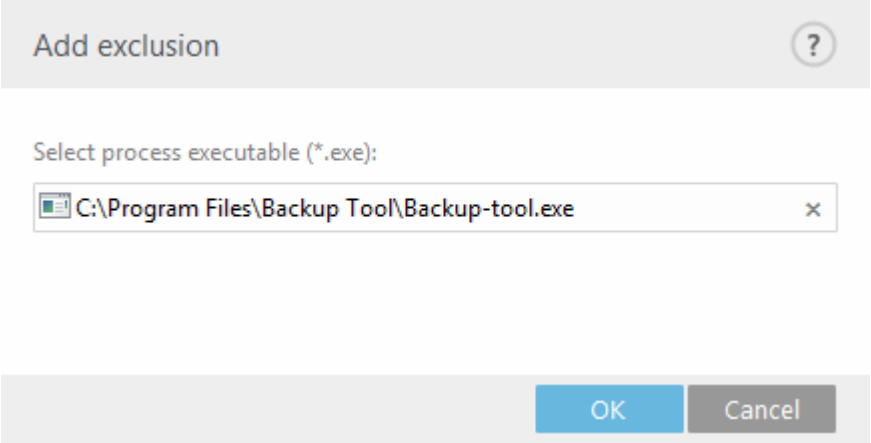
Tarama dışı bırakılan işlemler, potansiyel çakışma riskini en düşük düzeye indirir ve tarama dışı bırakılan uygulamaların performansını iyileştirerek işletim sisteminin genel performansı ve istikrarı üzerinde olumlu bir etki yaratır. Bir işlemin / uygulamanın tarama dışında bırakılması kendisine ait yürütülebilir dosyanın (*.exe*) tarama dışında bırakılmasıdır.

Gelişmiş ayarlar (F5) > **Algılama Altyapısı** >**Gerçek zamanlı dosya sistemi koruması** > **Temel** > **Tarama dışı bırakılan işlemler** aracılığıyla veya ana menüde **Araçlar** > **Çalışan işlemler** kısmından çalışan işlemler listesini kullanarak tarama dışı bırakılan işlemlerin listesine yürütülebilir dosyalar ekleyebilirsiniz.

Bu özellik, yedekleme araçlarını tarama dışında bırakmak için tasarlanmıştır. Yedekleme aracının işlemini tarama dışında bırakmak sistem kararlılığını sağlamakla kalmaz aynı zamanda çalışırken yedekleme yavaşlatılmadığından yedekleme performansını etkilemez.

ÖRNEK
Tarama dışı bırakılan işlemler yönetim penceresini açmak için **Düzenle**'yi tıklayın. Bu pencerede tarama dışı öğeler **ekleyebilir** ve tarama dışında bırakılacak yürütülebilir dosyalara gözatabilirsiniz (örneğin, *Backup-tool.exe*).
.exe dosyası tarama dışı öğelere eklenir eklenmez bu işlemin faaliyetleri ESET Server Security tarafından izlenmez ve bu işlem tarafından gerçekleştirilen herhangi bir dosya işleminde hiçbir tarama işlemi gerçekleştirilmez.

ÖNEMLİ
Yürütülebilir işlemi seçerken gözatma işlevini kullanmazsanız, yürütülebilir dosyaya ilişkin tam yolu el ile girmeniz gerekir. Aksi takdirde tarama dışı bırakma doğru çalışmaz ve HIPS hata bildirebilir.



Ayrıca tarama dışı öğelerden mevcut işlemleri **Düzenleyebilir** veya **Silebilirsiniz**.

NOT
Web erişimi koruması bu dışarıda bırakma işlemini dikkate almaz. Bu nedenle, web tarayıcınızın yürütülebilir dosyasını tarama dışı bırakırsanız, indirilen dosyalar taranmaya devam eder. Böylece sızıntı varsa yine de algılanır. Bu senaryo yalnızca bir örnektir. Web tarayıcılarının tarama dışı bırakılmalarını önermiyoruz.

Bulut tabanlı koruma

ESET LiveGrid® çeşitli bulut tabanlı teknolojilerden oluşan gelişmiş bir erken uyarı sistemidir. Bilinirliğe dayalı ortaya çıkan tehditleri algılamaya yardımcı olur ve beyaz liste kullanarak tarama performansını geliştirir. Yeni tehdit bilgileri, gerçek zamanlı olarak buluta aktarılır; bulut, ESET Malware Research Lab'in daima zamanında yanıt vermesine ve tutarlı koruma sağlamasına olanak tanır. Kullanıcılar ESET LiveGrid® içinden kullanılabilir ek bilgiler alarak programın arabirimindeki ya da içerik menüsündeki çalışan işlemlerin ve dosyaların bilinirliğini denetleyebilir.

ESET Server Security uygulamasını yüklerken aşağıdaki seçeneklerden birini belirleyin:

- ESET LiveGrid® ürününü etkinleştirmemeye karar verebilirsiniz. Yazılımda herhangi bir işlevsellik kaybı olmaz, ancak bazı durumlarda ESET Server Security ürünü yeni tehditlere, algılama altyapısı veri tabanı güncellemesine göre daha yavaş bir şekilde yanıt verebilir.
- ESET LiveGrid® ürününü, yeni tehditler ve bu yeni tehlikeli kodun nerede bulunduğu hakkındaki bilgileri anonim olarak gönderecek şekilde yapılandırabilirsiniz. Bu dosya ayrıntılı analiz için ESET'e gönderilebilir. Bu tehditlerin incelenmesi, ESET'in kendi tehdit algılama becerilerini güncellemesine yardımcı olacaktır.

ESET LiveGrid® yeni algılanan tehditlerle ilişkili olarak bilgisayarınız hakkında bilgi toplar. Bu bilgiler, tehdidin görüldüğü dosyanın bir örneğini veya kopyasını, o dosyanın yolunu, dosya adını, tarih ve saatini, tehdidin bilgisayarınızda hangi işlem yoluyla göründüğünü ve bilgisayarınızın işletim sistemi hakkındaki bilgileri içerebilir.

Varsayılan olarak ESET Server Security, şüpheli dosyaların analizi için ESET Virüs Laboratuvarı'na gönderilecek şekilde yapılandırılmıştır. *.docx* veya *.xlsx* gibi uzantılara sahip dosyalar daima hariç tutulur. Siz veya şirketinizin göndermek istemediği belirli dosyalar varsa, onların uzantılarını da ekleyebilirsiniz.

ESET LiveGrid® Bilinirlik sistemini etkinleştirin (önerilir)

ESET LiveGrid® bilinirlik sistemi, taranan dosyaları buluttaki beyaz ve kara listelerde yer alan öğelerden oluşan veri tabanıyla karşılaştırarak ESET anti-malware çözümlerinin etkisini artırır.

ESET LiveGrid® Geri bildirim sistemini etkinleştirin

Veriler, daha ayrıntılı inceleme için ESET Araştırma Laboratuvarı'na gönderilir.

Kilitlenme raporlarını ve tanılama verilerini gönder

Kilitlenme raporları, modüller veya bellek dökümleri gibi verileri gönderin.

Anonim istatistikleri gönder

ESET'in; sisteminizle ilgili bilgiler de dahil olmak üzere tehdit adı, tarih, algılama saati, algılama yöntemi ve ilişkili meta veriler, taranan dosyalar (karma, dosya adı, dosyanın kaynağı, telemetri), engellenen ve şüpheli URL'ler, ürün sürümü ve yapılandırması gibi yeni algılanan tehditler hakkında anonim bilgiler toplamasına izin verir.

İletişim e-posta adresi (isteğe bağlı)

İletişim e-posta adresiniz şüpheli dosyalar arasına eklenebilir ve analiz için daha fazla bilgi gerekmesi durumunda sizinle iletişim kurma amacıyla kullanılabilir. Daha fazla bilgi gerekmedikçe ESET'ten bir yanıt almayacağınızı lütfen unutmayın.

Örneklerin Gönderimi

Enfekte olan örneklerin otomatik gönderimi

Bu, enfekte olan tüm örnekleri analiz etmek ve gelecekteki algılama düzeyini iyileştirmek için ESET'e gönderir.

- Enfekte olan tüm örnekler
- Belgeler dışındaki tüm örnekler
- Gönderme

Şüpheli örneklerin otomatik gönderimi

Tehditlere benzeyen şüpheli örnekler ve/veya sıradışı özellikleri ya da davranışları olan örnekler inceleme amacıyla ESET'e gönderilir.

- **Yürütülebilir dosyalar** - Şu yürütülebilir dosyaları içerir: *.exe, .dll, .sys*
- **Arşivler** - Şu arşiv dosyası türlerini içerir: *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- **Betikler** - Şu betik dosyayı türlerini içerir: *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.js*, *.ps1*
- **Diğer** - Şu dosya türlerini içerir: *.jar*, *.reg*, *.msi*, *.swf*, *.lnk*
- **Olası spam e-postaları** - Genel spam algılamasını iyileştirir.
- **Belgeler** - Microsoft Office belgeleri veya etkin içerikli PDF'ler içerir.

Tarama dışı öğeler

ESET LiveGrid® içindeki Tarama Dışı Öğeler'in yanında bulunan Düzenle seçeneğini tıklayarak tehditlerin analiz için ESET Virüs Laboratuvarları'na ne şekilde gönderileceğini yapılandırabilirsiniz.

Örneklerin maksimum boyutu (MB)

Taranacak örneklerin maksimum boyutunu tanımlayın.

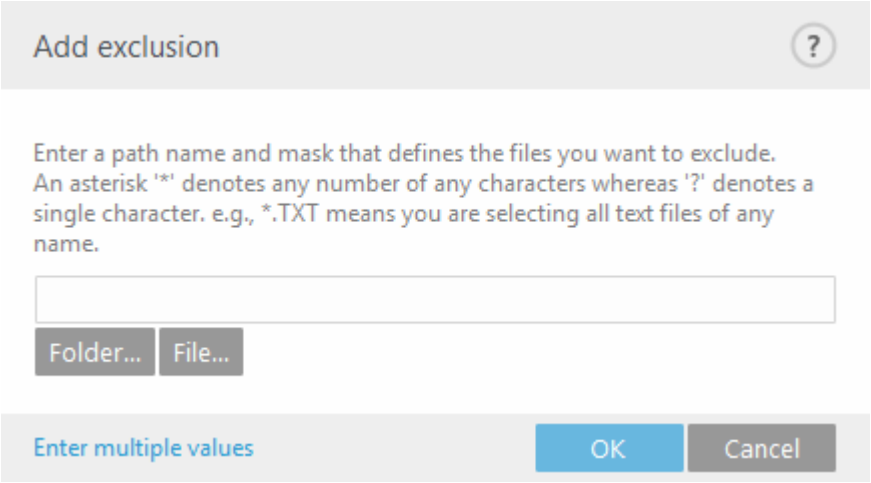
ESET Dynamic Threat Defense

ESET PROTECT Web Konsolu kullanarak bir istemci makinede ESET Dynamic Threat Defense hizmetini etkinleştirmek için ESET PROTECT Web Konsolunda yeni bir ilke oluşturun veya mevcut bir ilkeyi düzenleyin ve ESET Dynamic Threat Defense kullanmak istediğiniz makinelere atayın.

Tarama dışı bırakma filtresi

Tarama dışı öğe filtresi, belirli dosyaları/klasörleri gönderimden hariç tutmanıza olanak tanır (örneğin belgeler veya elektronik tablolar gibi gizli bilgiler içerebilecek dosyaları hariç tutmak için faydalı olabilir). Listelenen dosyalar, şüpheli kod içerse bile hiçbir zaman analiz için ESET laboratuvarına gönderilmez. En yaygın kullanılan dosya türleri (*.doc* vb.) varsayılan olarak tarama dışı bırakılır. İstendiğinde tarama dışında bırakılan dosyalar listesine ekleyebilirsiniz.

Önceden ESET LiveGrid® ürününü kullandıysanız ve devre dışı bıraktıysanız hala gönderilecek veri paketleri olabilir. Devre dışı bıraktıktan sonra bile bu paketler ESET'e gönderilir. Mevcut tüm bilgiler gönderildikten sonra başka paket oluşturulmaz.



Şüpheli bir dosya bulduğunuzda, analiz edilmesi için Tehdit Laboratuvarımıza gönderebilirsiniz. Kötü amaçlı bir uygulama olması halinde, algılanması bir sonraki algılama modülü güncellemesine eklenir.

Kötü amaçlı yazılım taramaları

Bu bölüm, tarama parametrelerini seçmek için seçenekler sunar.

> NOT
> Bu tarama profili seçicisi, **İsteğe bağlı tarama**, Hyper-V taraması ve OneDrive taraması için geçerlidir.

Seçili profil

İsteğe bağlı tarayıcı tarafından kullanılan belirli bir parametre kümesi. Önceden tanımlı tarama profillerinden birini kullanabilir veya yeni bir profil oluşturabilirsiniz. Tarama profilleri farklı ThreatSense altyapı parametreleri kullanır.

Profil listesi

Yeni bir profil oluşturmak için **Düzenle**'yi tıklayın. Profil adını yazıp **Ekle**'yi tıklayın. Yeni profil, mevcut tarama profillerini listeleyen **Seçili profil** açılır menüsünde görüntülenir.

Tarama hedefleri

Belirli bir hedefi taramak için **Düzenle** seçeneğini tıklayın ve açılır menüden bir seçenek belirleyin veya klasör (ağaç) yapısından belirli bir hedefi seçin.

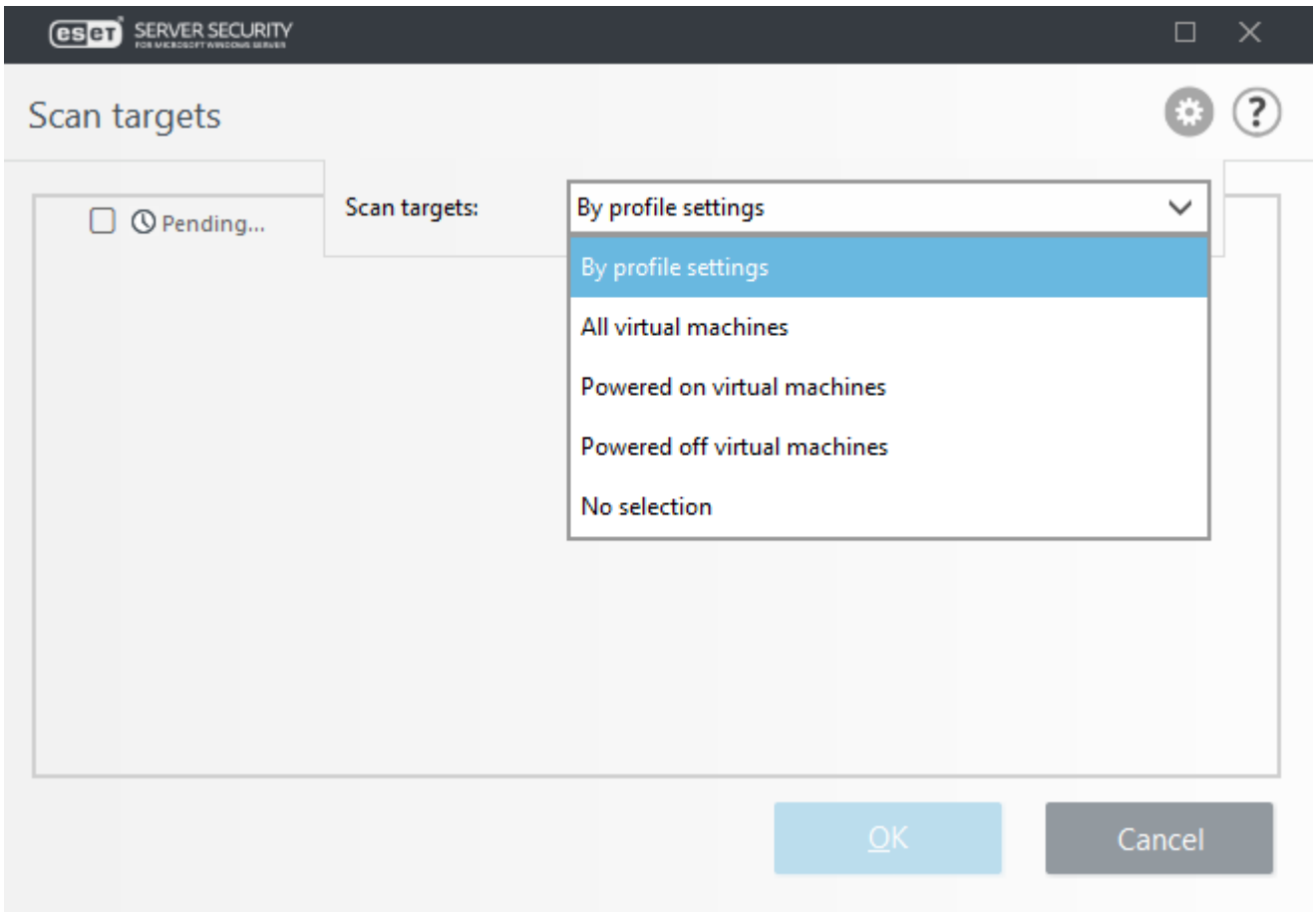
ThreatSense parametreleri

İsteğe bağlı bilgisayar tarayıcısı için tarama parametrelerini değiştirin.

İsteğe bağlı ve Makine öğrenimi koruması

Raporlama, algılama altyapısı ve makine öğrenimi bileşeni tarafından gerçekleştirilir.

Hyper-V taraması açılır penceresi:



Hyper-V için **Tarama hedefleri** açılır menüsü, önceden tanımlı tarama hedeflerini seçmenize olanak tanır:

Profil ayarlarına göre	Seçili tarama profilinde ayarlanan hedefleri seçer.
Tüm sanal makineler	Tüm sanal makineleri seçer.
Sanal makinelerde desteklenen	Tüm sanal VM'leri seçer.
Sanal makinelerde desteklenmeyen	Tüm çevrimdışı VM'leri seçer.
Seçim yok	Tüm seçimleri temizler.

Taramayı ayarladığınız özel parametreleri kullanarak yürütmek için **Tara** seçeneğini tıklayın. Tüm taramalar tamamlandığında **Günlük dosyaları** > Hyper-V taraması öğelerini işaretleyin.

Profil yöneticisi

Tarama profili açılır menüsü, önceden tanımlı tarama profillerini seçmenize olanak tanır.

- **Smart tarama**

- **İçerik menüsü taraması**
- **Kapsamlı tarama**
- **Profilim** (şunlar için geçerlidir: Hyper-V taraması, Güncelleme profilleri ve OneDrive taraması)

İhtiyaçlarınıza uygun bir tarama profili oluşturmanıza yardımcı olması için, tarama ayarlarının her bir parametresine yönelik bir açıklama içeren ThreatSense altyapısı parametre ayarları bölümüne bakın.

Profil yöneticisi ESET Server Security içinde üç yerde kullanılır.

İsteğe bağlı bilgisayar taraması

Tercih edilen tarama parametreleriniz daha sonraki taramalar için kaydedilebilir. Düzenli olarak kullanılan her tarama için farklı bir profil (çeşitli tarama hedefleriyle, tarama yöntemleriyle ve diğer parametrelerle) oluşturmanızı öneririz.

Güncelle

Profil düzenleyicisi, kullanıcıların yeni güncelleme profilleri oluşturmasına olanak tanır. Yalnızca bilgisayarınız güncelleme sunucularına bağlanmak için birden çok araç kullanıyorsa özel güncelleme profilleri oluşturmanız gerekir.

Hyper-V taraması

Yeni profil oluşturun; **Profil listesi** yanındaki **Düzenle** seçeneğini belirleyin. Yeni profil, var olan tarama profillerini listeleyen **Seçili profil** açılır menüsünde görüntülenir.

OneDrive taraması

Yeni profil oluşturun; **Profil listesi** yanındaki **Düzenle** seçeneğini belirleyin. Yeni profil, var olan tarama profillerini listeleyen **Seçili profil** açılır menüsünde görüntülenir.

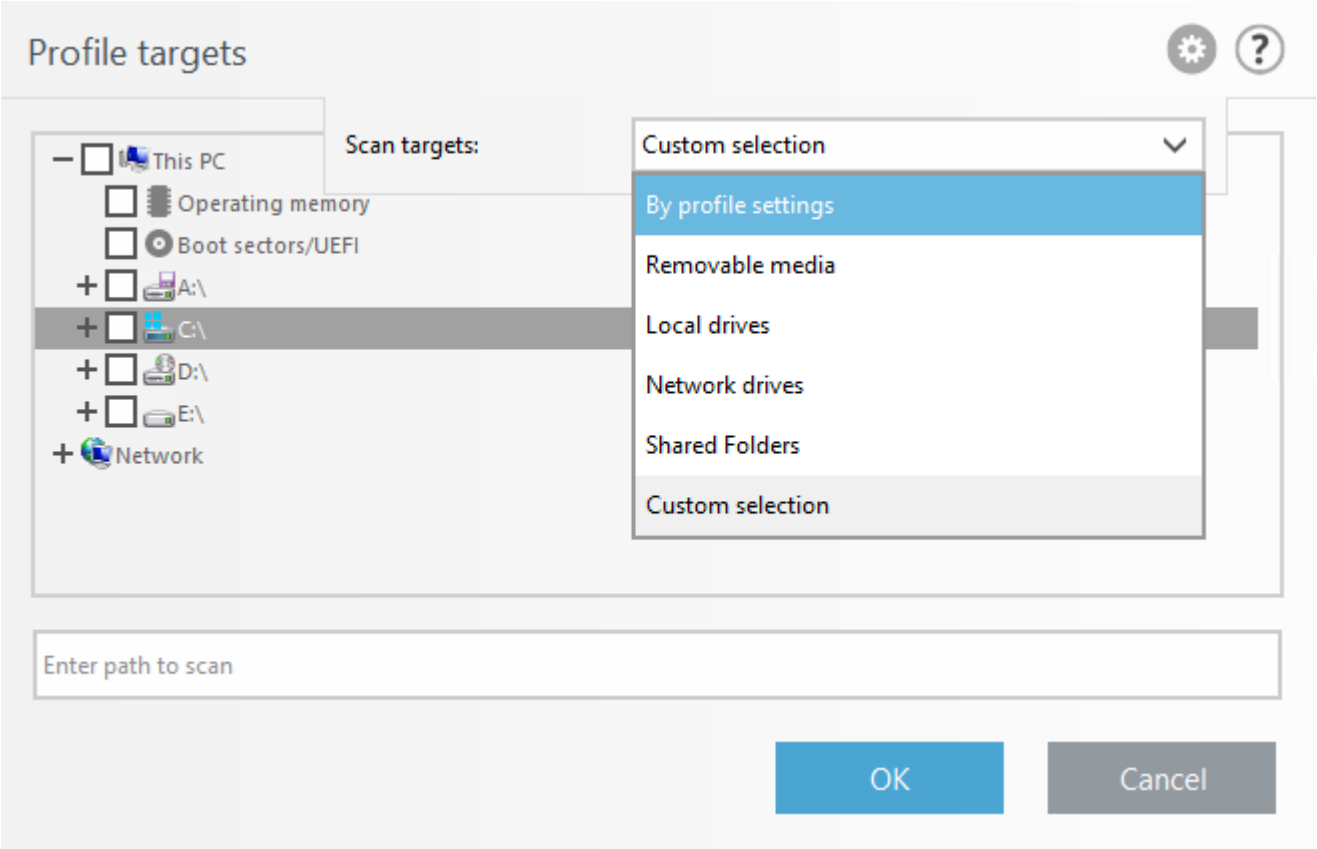
Profil hedefleri

Sızıntılar için nelerin taranacağını belirtebilirsiniz. Sisteminizde mevcut tüm hedefleri listeleyen ağaç yapısından nesneler (bellek, önyükleme kesimleri ve UEFI, sürücüler, dosyalar ve klasörler ve ağ) seçin. **Hedefleri tara** ve **Profili tara** açılır menülerine erişmek için sol üst köşedeki dişli simgesini tıklayabilirsiniz.

NOT
Bu tarama profili seçicisi, **İsteğe bağlı tarama**, Hyper-V taraması ve OneDrive taraması için geçerlidir.

İşletim belleği	İşletim belleği tarafından halihazırda kullanılan tüm işlemleri ve verileri tarar.
Önyükleme kesimleri/UEFI	Önyükleme kesimlerini ve UEFI'yi zararlı yazılımlara karşı tarar. UEFI tarayıcı ile ilgili daha fazla bilgi için sözlüğe başvurabilirsiniz.
WMI veri tabanı	Tüm Windows Yönetim Araçları (WMI) veri tabanını, tüm ad alanlarını, tüm sınıf örneklerini ve tüm mülkleri tarar. Enfekte olan dosyalara veya veri olarak yerleştirilmiş zararlı yazılımlara referans arar.
Sistem kayıt defteri	Tüm sistem kayıt defterini, tüm anahtarları ve alt anahtarları tarar. Enfekte olan dosyalara veya veri olarak katıştırılmış zararlı yazılımlara referans arar. Tespitleri temizlerken önemli verilerin kaybolmadığından emin olmak için referans kayıt defterinde kalır.

Hızlı bir şekilde tarama hedefine gitmek veya bir hedef klasör ya da dosya eklemek için klasör listesinin altındaki boş alana hedef dizini girin.



Tarama hedefleri açılır menüsü, önceden tanımlı tarama hedefleri seçmenizi sağlar:

Profil ayarlarına göre	**Seçili tarama profilinde ayarlanan hedefleri seçer.**
Çıkarılabilir medya	Disketi, USB depolama aygıtını, CD/DVD'yi seçer.
Yerel sürücüler	Tüm sistem sabit sürücülerini seçer.
Ağ sürücüleri	Tüm eşlenen ağ sürücülerini seçer.
Paylaşılan Klasörler	Yerel sunucuda paylaşılan tüm klasörleri seçer.
Özel seçim	Tüm seçimleri temizler. Temizleme işleminin ardından özel seçiminizi yapabilirsiniz.

Bir tarama hedefine (dosya veya klasör) hızlıca gidip hedefi taramaya dahil etmek için ağaç yapısının altındaki metin alanına yolunu girin. Yol girişi, büyük küçük harf duyarlıdır.

Tarama profili açılır menüsü, önceden tanımlı tarama profilleri seçmenizi sağlar:

- **Smart tarama**
- **İçerik menüsü taraması**
- **Kapsamlı tarama**

Bu tarama profilleri farklı ThreatSense altyapı parametreleri kullanır.

Temizlemeden tara

Ek temizleme eylemi olmadan yalnızca sistemi taramak istiyorsanız **Temizlemeden tara** seçeneğini belirleyin. Yalnızca etkinleşmiş öğeler olup olmadığına dair bir genel bakış elde etmek ve varsa etkilenmeler hakkındaki ayrıntıları almak istiyorsanız, bu seçenek kullanılabilir. Ayrıca **Ayarlar** > **ThreatSense parametreleri** >

Temizleme seçeneğini tıklatarak üç temizleme düzeyinden birini seçebilirsiniz. Taramayla ilgili bilgiler bir tarama günlüğüne kaydedilir.

İstisnaları yoksay

Özel durumları yoksay'ı seçtiğinizde özel durumları yok sayan bir tarama yapabilirsiniz, aksi halde bu özel durumlar geçerli olur.

Tarama hedefleri

Yalnızca belirli bir hedefi taramak istiyorsanız, **Tarama hedefleri** açılır menüsünden bir seçenek belirleyerek ya da klasör (ağaç) yapısından belirli hedefler seçerek **Özel tarama** aracını kullanabilirsiniz.

Tarama hedefleri profili seçicisi şunlar için geçerlidir:

- İsteğe bağlı tarama
- Hyper-V taraması
- OneDrive taraması

Hızlı şekilde bir tarama hedefine gitmek veya yeni bir hedef dosya ya da klasörü eklemek için, klasör listesinin altındaki boş alana söz konusu hedefi girin. Bu yalnızca ağaç yapısında hedef seçilmemesi ve **Tarama hedefleri** menüsünün **Seçim yok** olarak ayarlanması durumunda mümkündür.

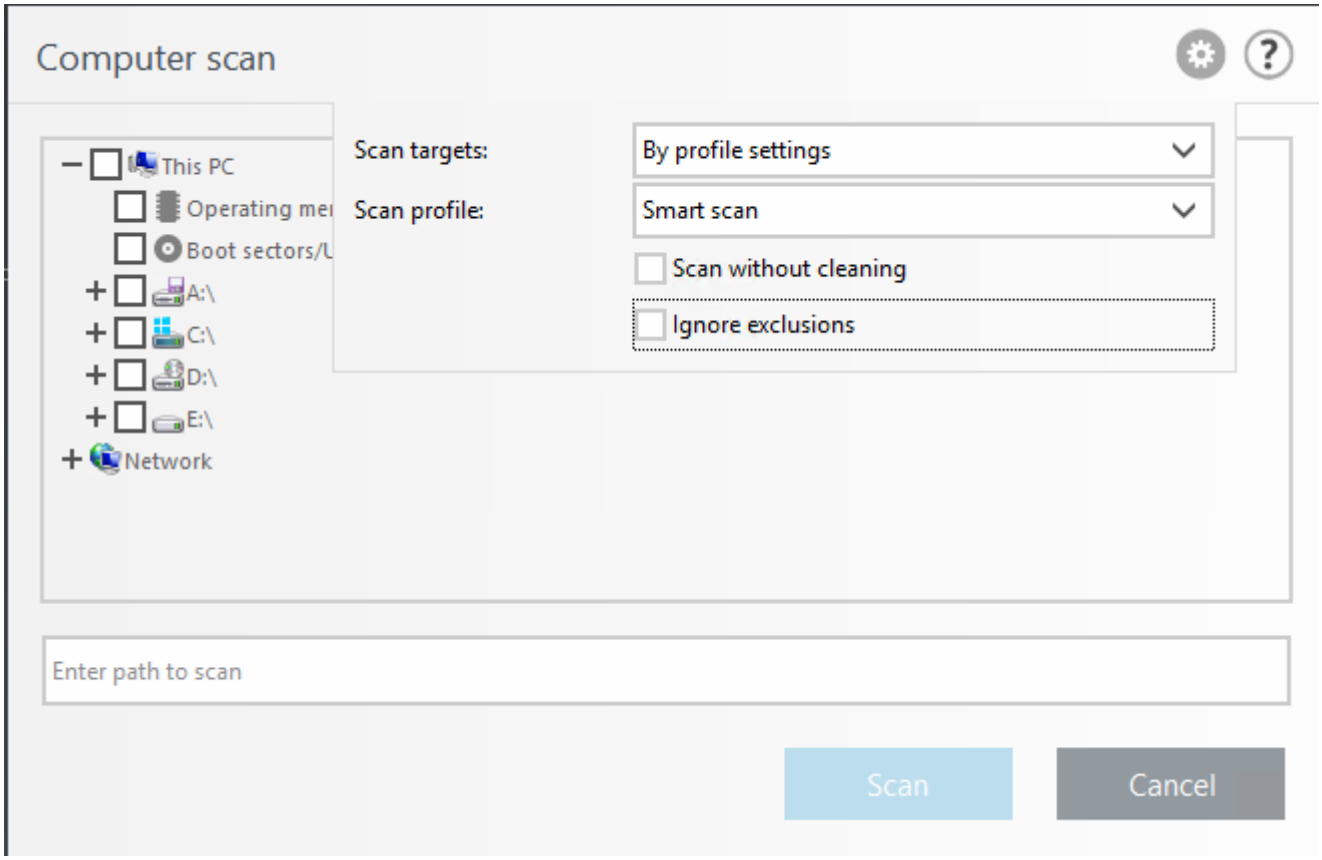
İşletim belleği	İşletim belleği tarafından halihazırda kullanılan tüm işlemleri ve verileri tarar.
Önyükleme kesimleri/UEFI	Önyükleme kesimlerini ve UEFI'yi zararlı yazılımlara karşı tarar. UEFI tarayıcı ile ilgili daha fazla bilgi için sözlüğe başvurabilirsiniz.
WMI veri tabanı	Tüm Windows Yönetim Araçları (WMI) veri tabanını, tüm ad alanlarını, tüm sınıf örneklerini ve tüm mülkleri tarar. Enfekte olan dosyalara veya veri olarak yerleştirilmiş zararlı yazılımlara referans arar.
Sistem kayıt defteri	Tüm sistem kayıt defterini, tüm anahtarları ve alt anahtarları tarar. Enfekte olan dosyalara veya veri olarak katıştırılmış zararlı yazılımlara referans arar. Tespitleri temizlerken önemli verilerin kaybolmadığından emin olmak için referans kayıt defterinde kalır.

Tarama hedefleri açılır menüsü, önceden tanımlı tarama hedeflerini seçmenize olanak tanır.

Profil ayarlarına göre	Seçili tarama profilinde ayarlanan hedefleri seçer.
Çıkarılabilir medya	Disketi, USB depolama aygıtını, CD/DVD'yi seçer.
Yerel sürücüler	Tüm sistem sabit sürücülerini seçer.
Ağ sürücüleri	Tüm eşlenen ağ sürücülerini seçer.
Paylaşılan Klasörler	Yerel sunucuda paylaşılan tüm klasörleri seçer.
Özel seçim	Tüm seçimleri temizler. Temizleme işleminin ardından özel seçiminizi yapabilirsiniz.

Seçilen hedeflerin taranması için kullanılmak üzere **Tarama** profili açılır menüsünden bir profil seçin. Varsayılan profil, **Smart tarama**'dır. **Kapsamlı tarama** ve **Bağlam menüsü taraması** adlı iki önceden tanımlı tarama profili daha vardır. Bu tarama profilleri farklı ThreatSense altyapı parametreleri kullanır.

Özel tarama açılır penceresi:



Temizlemeden tara

Ek temizleme eylemi olmadan yalnızca sistemi taramak istiyorsanız **Temizlemeden tara** seçeneğini belirleyin. Yalnızca etkinleşmiş öğeler olup olmadığına dair bir genel bakış elde etmek ve varsa etkilenmeler hakkındaki ayrıntıları almak istiyorsanız, bu seçenek kullanılabilir. Ayrıca **Ayarlar** > **ThreatSense parametreleri** > **Temizleme** seçeneğini tıklatarak üç temizleme düzeyinden birini seçebilirsiniz. Taramayla ilgili bilgiler bir tarama günlüğüne kaydedilir.

İstisnaları yoksay

Aksi halde geçerli olan tarama dışı öğelerini yoksayarak tarama gerçekleştirebilirsiniz.

Tarama

Taramayı ayarladığınız özel parametreleri kullanarak yürütmek için kullanılır.

Yönetici olarak tara

Taramayı Yönetici hesabı altında yürütmenize izin verir. Geçerli kullanıcının taranacak uygun dosyalara erişmek için ayrıcalığı yoksa bunu tıklayın. Bu düğmenin, geçerli kullanıcı Yönetici olarak UAC işlemlerini çağıramıyorsa kullanılabilir olmadığını unutmayın.

Boşta durumu taraması

Bilgisayar boşta durumundayken, tüm yerel sürücülerde sessiz bilgisayar taraması gerçekleştirilir. **Boşta durumu algılaması** bilgisayarınız aşağıdaki durumlardayken çalışır:

- **Ekran veya ekran koruyucu kapatıldı**

- **Bilgisayar kilidi**
- **Kullanıcı oturumunu kapatma**

Bilgisayar pil gücüyle çalışıyor olsa da çalıştır

Varsayılan olarak, Boşta durumu tarayıcısı bilgisayar (dizüstü bilgisayar) pil gücüyle çalışıyorsa çalışmaz.

Günlüğe kaydetmeyi etkinleştir

Günlük dosyaları bölümünde bilgisayar tarama çıktısı kaydetmek için kullanılır (ana program penceresinde Günlük dosyalarını tıklayın ve aşağı açılır menüden Bilgisayar taraması günlük türünü seçin).

ThreatSense parametreleri

Boşta durumu tarayıcısı için tarama parametrelerini değiştirin.

Başlangıç taraması

Varsayılan olarak, sistem başlatıldığında (kullanıcı girişi) ve başarılı bir modül güncellemesinden sonra otomatik başlatma dosyası denetimi gerçekleştirilir. Bu tarama, Zamanlayıcı yapılandırması ve görevleri tarafından denetlenir.

Başlangıç taraması seçenekleri, **Sistem başlangıcında dosya denetimi** zamanlayıcı görevinin bir parçasıdır.

Başlangıç taraması seçeneklerini değiştirmek için **Araçlar** > **Zamanlayıcı** seçeneğine gidin, **Başlangıçta otomatik dosya denetimi** adlı görevlerden birini seçin (kullanıcı girişi veya modül güncellemesi) ve **Düzenle**'yi tıklayın. Sihirbazın adımlarını izleyin. Son adımda Başlangıçta otomatik dosya denetimi için ayrıntılı seçenekleri değiştirebilirsiniz.

Başlangıçta otomatik dosya denetimi

Sistem başlangıç dosyası denetimi zamanlanmış görevi oluştururken aşağıdaki parametreleri ayarlamak için birkaç seçeneğiniz vardır:

Tarama hedefi açılır menüsü, sistem başlatıldığında çalışan dosyaların tarama derinliğini belirtir. Dosyalar aşağıdaki ölçütlere göre artan sırada düzenlenir:

- **Kayıtlı tüm dosyalar** (birçok dosya taranır)
- **Az kullanılan dosyalar**
- **Yaygın olarak kullanılan dosyalar**
- **Sık kullanılan dosyalar**
- **Yalnızca en sık kullanılan dosyalar** (az sayıda dosya taranır)

İki belirli Tarama hedefi grubu da dahildir:

Kullanıcı oturum açmadan önce çalıştırılan dosyalar

Kullanıcı oturum açmadan erişilebilen konumlardaki dosyaları içerir (hizmetler, tarayıcı yardımcı nesneleri, winlogon bildirimi, Windows zamanlayıcı girdileri, bilinen dll'ler gibi neredeyse tüm başlangıç konumlarını içerir).

Kullanıcı oturum açtıktan sonra çalıştırılan dosyalar

Yalnızca kullanıcı oturum açtıktan sonra erişilebilen konumlardaki dosyaları içerir (yalnızca belirli kullanıcı tarafından çalıştırılan dosyaları, özellikle *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* içindeki dosyaları içerir).

Söz konusu her bir grup için taranacak dosya listeleri belirlenir.

Tarama önceliği

Bir taramanın ne zaman başlayacağını belirlemek için kullanılan öncelik düzeyi:

- **Normal** - ortalama sistem yüklemesinde,
- **Düşük** - düşük sistem yüklemesinde,
- **En düşük** - sistem yüklemesi olası en düşük düzeyde olduğunda,
- **Boştayken** - görev yalnızca sistem boştayken gerçekleştirilir.

Çıkarılabilir medya

ESET Server Security, otomatik çıkarılabilir medya (CD/DVD/USB) tarama işlemini sağlar. Bu modül, takılı bir medyayı taramanıza olanak verir. Bilgisayar yöneticisi, kullanıcıların istenmeyen içeriklere sahip çıkarılabilir medyayı kullanmalarını engellemek istiyorsa bu özellik faydalı olabilir.

Çıkarılabilir medya takıldıktan sonra yapılacak eylem

Bilgisayara çıkarılabilir bir medya aygıtı (CD/DVD/USB) takıldığında gerçekleştirilecek eylemi belirleyin.

- **Tarama** - Herhangi bir eylem gerçekleştirilmez ve **Yeni aygıt algılandı** penceresi kapatılır.
- **Otomatik aygıt taraması** - Takılı çıkarılabilir medya aygıtının isteğe bağlı bilgisayar taraması gerçekleştirilir.
- **Tarama seçeneklerini göster** - Çıkarılabilir medya ayarları bölümünü açar.

Çıkarılabilir medya takıldığında aşağıdaki iletişim kutusu gösterilir:

- **Şimdi tara** - Bu seçenek, çıkarılabilir medyanın taranması işlemini başlatır.
- **Daha sonra tara** - Çıkarılabilir medya taraması ertelenir.
- **Ayarlar** - Gelişmiş ayarları açar.
- **Her zaman belirlenen seçeneği kullan** - Bu seçenek belirlendiğinde çıkarılabilir medyanın her takılışında aynı eylem gerçekleştirilir.

Ayrıca, ESET Server Security belirli bir bilgisayarda harici aygıtları kullanmaya yönelik kuralları tanımlayabilme olanağı sağlayan Aygıt denetimi işlevine de sahiptir. Aygıt denetimi ile ilgili daha fazla ayrıntı Aygıt denetimi bölümünde bulunabilir.

Belge koruması

Belge koruması özelliği, Microsoft Office belgelerini ve Microsoft ActiveX öğeleri gibi Internet Explorer tarafından otomatik olarak indirilen dosyaları açılmadan önce tarar. Belge koruması Gerçek zamanlı dosya sistemi korumasına ek olarak bir koruma katmanı sağlar ve çok sayıda Microsoft Office belgelerine maruz kalmayan sistemlerde performansı artırmak için devre dışı bırakılabilir.

Sisteme tümleştir

Bu seçenek, Microsoft Office belgelerinin korumasını geliştirir (normal koşullarda gerekmez).

ThreatSense parametreleri

Belge koruması için parametreleri değiştirin.

> NOT
> Bu özellik, Microsoft Antivirus API kullanan uygulamalar (örn. Microsoft Office 2000 ve üzeri veya Microsoft Internet Explorer 5.0 ve üzeri) tarafından etkinleştirilir.

Hyper-V taraması

Hyper-V taramasının geçerli sürümü, Hyper-V'de çevrimiçi veya çevrimdışı sanal sistemlerin taranmasını destekler. Barındırılan Windows Hyper-V sistemine ve sanal sistem durumuna göre desteklenen tarama türleri aşağıda gösterilmektedir:

Hyper-V özelliğine sahip sanal sistemler	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
Online VM	tarama yok	salt okunur	salt okunur	salt okunur	salt okunur
Offline VM	salt okunur/temizleme	salt okunur/temizleme	salt okunur/temizleme	salt okunur/temizleme	salt okunur/temizleme

Donanım gereklilikleri

Sunucuda, Sanal Makineleri çalıştırmakla ilgili herhangi bir performans sorunu olmamalıdır. Tarama etkinliği esas olarak CPU kaynaklarını kullanır. Çevrimiçi VM'leri taramak için, boş disk alanı gereklidir. Disk alanı, denetim noktaları/sistem görüntüleri ve sanal diskler tarafından kullanılan alanın en az iki katı büyüklüğünde olmalıdır.

Belirli sınırlamalar

- RAID depolaması, Dağıtılmış Birimler ve Dinamik Diskler üzerinde tarama, Dinamik Disklerin yapısı nedeniyle desteklenmemektedir. Bu nedenle, mümkünse VM'lerinizde Dinamik Disk türünü kullanmaktan kaçınmanızı öneririz.
- Tarama her zaman geçerli VM'de gerçekleştirilir ve denetim noktalarını ya da anlık görüntüleri etkilemez.
- Bir kümedeki ana bilgisayar üzerinde çalışan Hyper-V şu anda ESET Server Security tarafından desteklenmemektedir.
- Windows Server 2008 R2 SP1'de çalışan bir Hyper-V ana bilgisayarındaki Sanal Makineler, ThreatSense parametrelerinde seçilen temizleme düzeyinden bağımsız olarak yalnızca salt okunur modda taranabilir (Temizleme işlemi yapılmaz).

NOT
ESET Security sanal disk MBR'lerinin taranmasını desteklese de bu hedefler için yalnızca salt okunur tarama yöntemi desteklenir. Bu ayar **Gelişmiş Ayarlar** (**F5**) > **Algılama Altyapısı** > **Hyper-V taraması** > ThreatSense parametreleri > **Önyükleme kesimleri**'nde değiştirilebilir.

Taranacak Sanal Makine "çevrimdışı" - Kapalı durumu

ESET Server Security, sanal makineleri algılamak ve onlara bağlanmak için Hyper-V Yönetimi'ni kullanır. Bu şekilde, ESET Server Security tıpkı herhangi bir genel sürücünün verilerine ve dosyalarına erişir gibi, sanal disklerin içeriklerine erişir.

Taranacak Sanal Makine "çevrimiçi" - Çalışıyor, Duraklatıldı, Kaydedildi durumu

ESET Server Security, sanal diskleri algılamak için Hyper-V Yönetimi'ni kullanır. Bu disklere gerçek bağlantı mümkün değildir. Bu nedenle, ESET Server Security Sanal Makine'nin denetim noktasını/sistem görüntüsünü oluşturur ve ardından denetim noktasına/sistem görüntüsüne bağlanır. Tarama tamamlandığında, denetim noktası/sistem görüntüsü silinir. Bu, çalışan Sanal Makineler tarama etkinliği tarafından etkinlenmediğinden salt okunur taramanın gerçekleştirilebileceği anlamına gelir.

Tarama sırasında ESET Server Security uygulamasının anlık görüntü veya denetim noktası oluşturması için bir dakika kadar bekleyin. Hyper-V taramasını çok sayıda Sanal Makine üzerinde çalıştırırken bunu göz önünde bulundurmalısınız.

Adlandırma kuralı

Hyper-V Tarama modülü şu adlandırma kuralına bağlıdır:

```
VirtualMachineName\DiskX\VolumeY
```

X, disk sayısını, Y ise birim sayısını gösterir. Örneğin:

```
Computer\Disk0\Volume1
```

Sayı öneki, algılama sırasına dayalı olarak eklenir ve bu sıra, VM'nin Disk Yöneticisi'nde görülen sırayla aynıdır. Bu adlandırma kuralı, taranacak hedeflerden oluşan ağaç yapılı listede, ilerleme çubuğunda ve günlük dosyalarında kullanılır.

Taramanın yürütülmesi

- İsteğe Bağlı - Tarama için mevcut olan Sanal Makinelerin ve birimlerin listesini görüntülemek için **Hyper-V Taraması**'nı tıklayın. Taramak istediğiniz Sanal Makineleri, diskleri veya birimleri seçip **Tara** öğesini tıklayın.
- Zamanlayıcı görevi oluşturmak için kullanılır.
- Sunucu Taraması adlı bir İstemci Görevi olarak ESET PROTECT üzerinden.
- Hyper-V taraması, eShell aracılığıyla yönetilebilir ve başlatılabilir.

Birkaç Hyper-V taramasını eşzamanlı yürütmek mümkün değildir. Tarama işlemi tamamlandığında dosyaları günlüğe kaydetmek için bağlantı içeren bir bildirim alırsınız.

Potansiyel sorunlar

- Çevrimiçi Sanal Makine'nin taraması yürütülürken, söz konusu Sanal Makine'nin denetim noktası/sistem görüntüsü oluşturulmalıdır ve denetim noktası/sistem görüntüsü oluşturma esnasında bazı genel Sanal Makine eylemleri sınırlandırılmış veya devre dışı bırakılmış olabilir.
- Çevrimdışı Sanal Makine taranmaktaysa tarama işlemi bitene kadar açılamaz.
- Hyper-V Yöneticisi iki farklı Sanal Makine'nin aynı şekilde adlandırılmasına olanak sağlar ve bu, tarama günlüklerini gözden geçirirken makineleri birbirinden ayırmakta güçlüklere neden olur.

OneDrive taraması

Temel

Eylemi ve karantinayı yapılandırabilirsiniz

Dosya enfekte olmuşsa yapılacak işlem

- **Eylem yok** - Dosyada herhangi bir değişiklik yapılmaz.
- **Sil** - Karantina bölümüne taşır ve dosyaları OneDrive'dan siler. Ancak dosyalar OneDrive geri dönüşüm kutusunda kalmaya devam eder.

Etkilenen dosyaları karantinaya al

Etkinleştirildiğinde silinmek üzere işaretlenen dosyalar karantinaya alınır. Dosyaların karantinada toplanmaması için karantinayı devre dışı bırakmak üzere bu ayarın işaretini kaldırın.

Gelişmiş

Bu bölümde OneDrive tarama kaydı (Uygulama Kimliği, Azure portalındaki Nesne Kimliği, Sertifika parmak izi) ile ilgili bilgiler yer alır. Süre aşımına uğrayanları ve eş zamanlı indirme sınırlarını yapılandırabilirsiniz.

Profiller

Yeni kural oluşturmak için, **Profil listesi** öğesinin yanındaki **Düzenle** seçeneğini tıklayıp kendi **Profil adınızı** girdikten sonra **Ekle** öğesini seçin. Yeni profil, mevcut tarama profillerini listeleyen **Seçili profil** açılır menüsünde görüntülenir.

Tarama hedefi açılır menüsü, önceden tanımlı tarama hedefi seçmenizi sağlar:

- **Profile göre** - Seçili tarama profilinde ayarlanan hedefleri seçer.
- **Tüm kullanıcılar** - Tüm kullanıcıları seçer.
- **Seçim yok** - Geçerli seçiminizi temizler.

Taramayı ayarladığınız özel parametreleri kullanarak yürütmek için **Tara** seçeneğini tıklayın. Tüm taramalar tamamlandığında **Günlük dosyaları** > OneDrive taraması öğelerini işaretleyin.

ThreatSense parametreleri

OneDrive tarayıcısı için tarama parametrelerini değiştirin.

OneDrive taraması ve Makine öğrenimi koruması

Raporlama, algılama motoru ve makine öğrenimi bileşeni tarafından gerçekleştirilir.

HIPS

Ana Bilgisayar Tabanlı Saldırı Önleme Sistemi (HIPS), sisteminizi bilgisayarınızı olumsuz yönde etkilemeyi hedefleyen kötü amaçlı yazılımlardan ve istenmeyen etkinliklerden korur. HIPS; çalışan işlemleri, dosyaları ve kayıt defteri anahtarlarını izlemek için ağ filtrelemesinin algılama özellikleriyle birlikte gelişmiş davranışsal analiz yöntemini kullanır. HIPS, Gerçek zamanlı dosya sistemi korumasından ayrıdır ve bir güvenlik duvarı değildir. Yalnızca işletim sisteminde çalışan işlemleri izler.

UYARI
HIPS ayarlarında yapılan değişiklikler yalnızca deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. HIPS ayarlarında yanlış bir yapılandırma, sistemde istikrarsızlığa neden olabilir.

Savunmayı etkinleştir

ESET Server Security, kötü amaçlı yazılımların zararlı yazılım korumanızı bozmalarını ya da devre dışı bırakmalarını engelleyen tümleşik Kendini koruma teknolojisine sahiptir. Bu sayede sisteminizin her an korunuyor olduğundan emin olabilirsiniz. HIPS'i etkinleştir ve SD'yi (Kendini Koruma) etkinleştir ayarlarında yapılan değişiklikler, Windows işletim sistemi yeniden başlatıldığında geçerli hale gelir. HIPS sisteminin tamamının devre dışı bırakılması da bilgisayarın yeniden başlatılmasını gerektirir.

Korumalı Hizmeti Etkinleştir

Microsoft, Microsoft Windows Server 2012 R2 ile bir korunan hizmetler konseptini kullanıma sunmuştur. Zararlı yazılım saldırılarına karşı olan bir hizmet sunar. ESET Server Security çekirdeği varsayılan olarak korumalı bir hizmet olarak çalışır. Bu özellik, Microsoft Windows Server 2012 R2 ve daha yeni sunucusu olan işletim sistemlerinde kullanılabilir.

Advanced Memory Scanner etkinleştir

Gizleme veya şifreleme kullanarak zararlı yazılımlara karşı koruma ürünleri tarafından algılanmaktan kurtulmak için tasarlanan zararlı yazılımlara karşı korumayı güçlendirmek üzere Exploit Engelleyici ile birlikte çalışır. Advanced Memory Scanner, varsayılan olarak etkindir. Sözlük'ten bu koruma türü hakkında daha fazla bilgi edinin.

Exploit Engelleyici'yi etkinleştir

Web tarayıcıları, PDF okuyucuları, e-posta istemcileri ve MS Office bileşenleri gibi yaygın olarak kötüye kullanılan uygulama türlerini güçlendirmek üzere tasarlanmıştır. Exploit Engelleyici, varsayılan olarak etkindir. Sözlük'ten bu koruma türü hakkında daha fazla bilgi edinin.

Fidye Yazılım Korumasını Etkinleştir

Bu işlevi kullanmak için HIPS ve ESET Live Grid'i etkinleştirin. Sözlük'te Ransomware hakkında daha fazla bilgi edinin.

Filtreleme modu

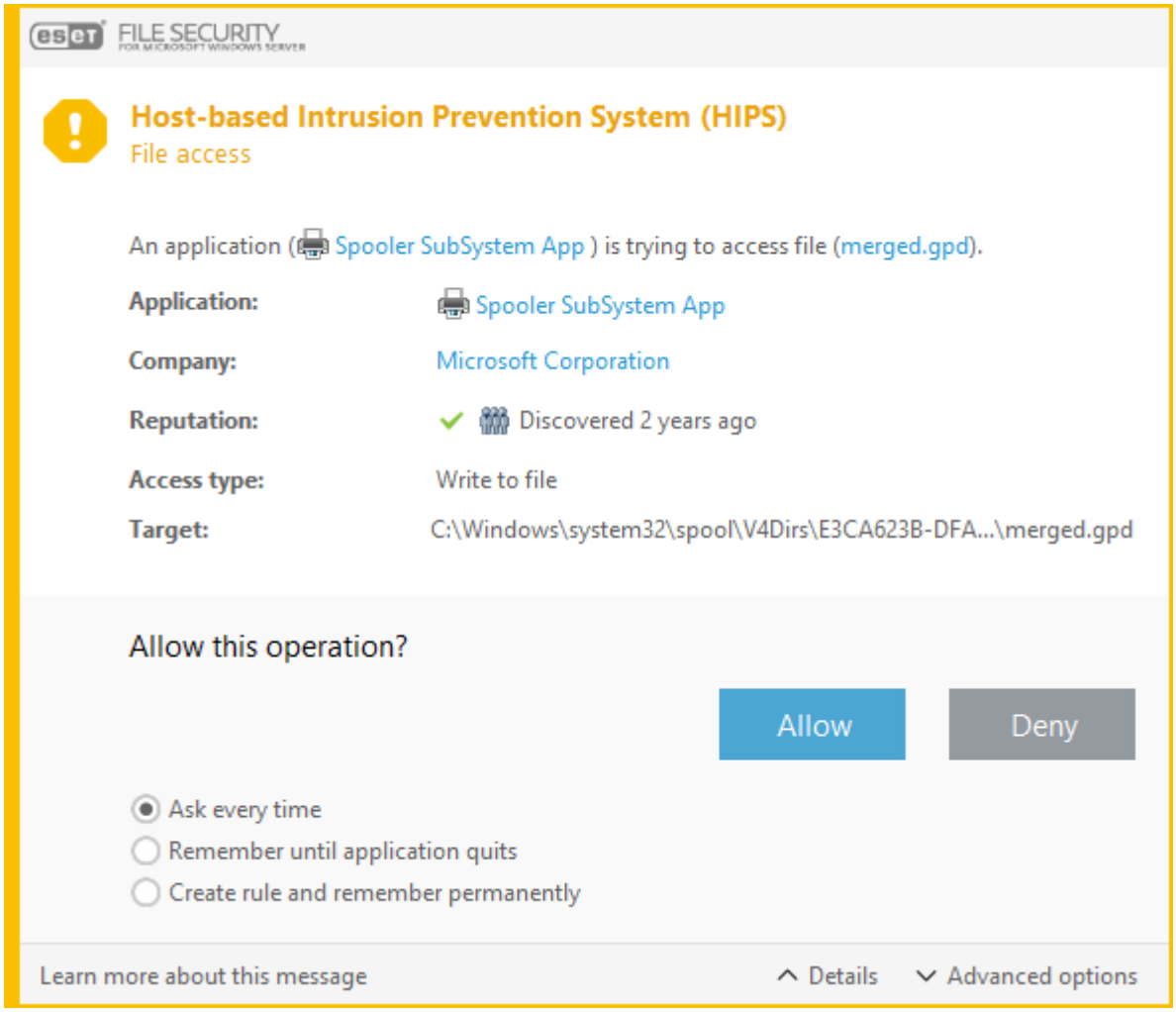
Aşağıdaki filtreleme modlarından birini seçebilirsiniz:

- **Otomatik mod** - Sisteminizi koruyan önceden tanımlı kurallar tarafından engellenenler dışındaki işlemler etkinleştirilir. Kural tarafından reddedilen eylemler hariç her şeye izin verilir.
- **Akıllı mod** - Kullanıcıya yalnızca çok şüpheli olaylarla ilgili bildirim gönderilir.
- **Etkileşimli mod** - Kullanıcının işlemleri onaylaması istenir. Erişime izin ver/erişimi reddet, Kural oluştur, Bu eylemi geçici olarak hatırla.
- **İlke tabanlı mod** - İşlemler engellenir. Yalnızca kullanıcı kurallarını/önceden tanımlı kuralları kabul eder.
- **Öğrenme modu** - İşlemler etkinleştirilir ve her işlemden sonra bir kural oluşturulur. Bu modda oluşturulan kurallar, Kural düzenleyicisinde görüntülenebilir, ancak bunların önceliği manuel olarak veya otomatik modda oluşturulan kurallardan daha düşüktür. HIPS Filtreleme modu açılır menüsünden **Öğrenme modunu** seçtiğinizde, **Ööğrenme modu şu sürenin ardından sona erecek** ayarı kullanılabilir hale gelir. Öğrenme modunda kalmak istediğiniz süreyi seçin (maksimum süre 14 gündür). Belirtilen süre geçtiğinde öğrenme modundayken HIPS tarafından oluşturulan kuralları düzenlemeniz istenir. Ayrıca başka bir filtreleme modu seçebilir veya kararı erteleyebilir ve öğrenme modunu kullanmaya devam edebilirsiniz.

Kurallar

Kurallar, hangi uygulamaların hangi dosyalara, kayıt defteri bölümlerine veya diğer uygulamalara erişebileceğini belirler. HIPS sistemi, işletim sistemi içindeki olayları izler ve kişisel güvenlik duvarı tarafından kullanılan kurallara benzer kurallara dayanarak uygun şekilde yanıt verir. HIPS kural yönetimi penceresini açmak için Düzenle'yi tıklayın. Bir kural için varsayılan eylem **Sor** olarak belirlenmiştir, kuralın her tetiklenişinde bir iletişim penceresi görüntülenir. İşlem için **Engelle** veya **İzin Ver** seçeneklerini belirleyebilirsiniz. Belirtilen sürede bir eylem seçmezseniz yeni eylem kurallara göre seçilir.

İletişim kutusu penceresi, HIPS'in algıladığı herhangi bir yeni eyleme göre kural oluşturmanıza ve ardından eyleme **İzin verileceği** veya eylemin **Engelleneceği** koşulları tanımlamanıza izin verir. Daha fazla bilgi için Ayrıntılar'ı tıklayın. Bu şekilde oluşturulan kurallar, manuel olarak oluşturulan kurallara eşit sayılır. Bu nedenle, bir iletişim penceresinden oluşturulan kural, söz konusu iletişim penceresini tetikleyen kuraldan daha az spesifik olabilir. Bu; bu tür bir kural oluşturulduktan sonra aynı işlemin aynı pencereyi tetikleyebileceği anlamına gelir.



Her defasında sor

Kuralın her tetiklenişinde bir iletişim penceresi görüntülenir. İşlem için **Reddet** veya **İzin Ver** seçeneklerinden birini belirleyebilirsiniz.

Uygulamadan çıkılana kadar anıma

Reddet veya **İzin ver** işlemlerinden birini seçmek, söz konusu uygulama kapatılana kadar kullanılacak olan geçici bir HIPS kuralı oluşturur. Ayrıca, filtreleme modunu ya da kuralları değiştirirseniz veya HIPS modülü güncellenirse ve sistemi yeniden başlatırsanız geçici kurallar silinir.

Kural oluştur ve daima hatırla

Yeni bir HIPS kuralı oluşturun. Bu kuralı daha sonra HIPS kural yönetimi bölümünde değiştirebilirsiniz.

HIPS kural ayarları

Bu pencere, size mevcut HIPS kurallarının genel bakışını sunar.

Kural	Kullanıcı tanımlı veya otomatik olarak seçilen kural adı.
Etkin	Kuralı listede tutmak istiyor ancak kullanmak istemiyorsanız bu düğmeyi devre dışı bırakın.
Eylem	Kural, koşulların doğru olması durumunda gerçekleştirilmesi gereken bir eylemi (**İzin ver**, **Engelle** veya **Sor**) belirtir.

Kural	Kullanıcı tanımlı veya otomatik olarak seçilen kural adı.
Kaynaklar	Kural, yalnızca olayın bir uygulama tarafından tetiklenmesi durumunda kullanılır.
Hedefler	Kural, yalnızca işlemin belirli bir dosyayla, uygulamayla ya da kayıt defteri girişiyle ilgili olması halinde kullanılır.
Günlüğe kaydetme düzeyi	Bu seçeneği etkinleştirirseniz bu kuralla ilgili bilgiler HIPS günlüğüne yazılır.
Bildir	Bir olay tetiklenirse sağ alt köşede küçük bir açılır pencere görünür.

Yeni kural oluşturmak için Yeni HIPS kuralları **ekle**'yi veya Seçili girişleri **düzenle**'yi tıklayın.

Kural adı

Kullanıcı tanımlı veya otomatik olarak seçilen kural adı.

Eylem

Kural, koşulların doğru olması durumunda gerçekleştirilmesi gereken bir eylemi (**İzin ver**, **Engelle** veya **Sor**) belirtir.

Etkileyen işlemler

Kuralın uygulanacağı işlem türünü seçmelisiniz. Kural, yalnızca bu tür işlem ve seçili hedef için kullanılır. Kural, bu kuralı tetikleyen koşulları açıklayan bölümlerden oluşur.

Kaynak uygulamalar

Kural, yalnızca olayın bu uygulamalar tarafından tetiklenmesi durumunda kullanılır. Açılır menüden **Belirli uygulamaları** seçin ve **Ekle** öğesini tıklayarak yeni dosya veya klasörleri ekleyin ya da tüm uygulamaları eklemek için açılır menüden **Tüm uygulamalar** seçeneğini belirleyin.

NOT
HIPS tarafından önceden tanımlanan belirli kuralların bazı işlemleri engellenemez ve bunlara varsayılan olarak izin verilir. Ek olarak, HIPS tarafından tüm sistem işlemleri izlenmez. HIPS tehlikeli olarak değerlendirilebilecek işlemleri izler.

Önemli işlemlerin açıklaması:

Dosya işlemleri:

Dosyayı sil	Uygulama hedef dosyayı silmek için izin istiyor.
Dosyaya yaz	Uygulama hedef dosyaya yazmak için izin istiyor.
Diske doğrudan erişim	Uygulama sıradan Windows prosedürlerini atlatan, standart olmayan bir şekilde diskten okumaya veya diske yazmaya çalışıyor. Bu, ilgili kurallar uygulanmadan dosyaların değiştirilmesiyle sonuçlanabilir. Bu işlem, algılamadan kurtulmaya çalışan zararlı yazılımdan, diskin tam kopyasını elde etmeye çalışan bir yedekleme yazılımından veya disk birimlerini yeniden düzenlemeye çalışan bir bölüm yöneticisinden kaynaklanıyor olabilir.
Genel kanca yükle	MSDN kitaplığından SetWindowsHookEx işlevini çağırmayı ifade eder.
Sürücüyü yükle	Sisteme sürücülerin kurulması ve yüklenmesi.

Kural, yalnızca işlemin bu hedefle ilgili olması durumunda kullanılır. Açılır menüden **Belirli dosyaları** seçin ve yeni dosya veya klasörleri eklemek için **Ekle** seçeneğini tıklayın. Ayrıca tüm uygulamaları eklemek için açılır menüden

Tüm dosyalar seçeneğini de belirleyebilirsiniz.

Uygulama işlemleri:

Başka bir uygulama için hata ayıkla	İşleme bir hata ayıklayıcı ekler. Bir uygulamanın hataları ayıklanırken, birçok davranış ayrıntıları görüntülenebilir ve verilerine erişilebilir.
Başka bir uygulamanın olaylarını durdur	Kaynak uygulama belirli bir uygulamaya hedeflenen olayları yakalamaya çalışır (örneğin tuş kaydedicinin tarayıcı olaylarını yakalamaya çalışması gibi).
Başka bir uygulamayı sonlandır/askıya al	Bir işlemi askıya alır, sürdürür veya sonlandırır (doğrudan İşlem Gezgininden veya İşlemler penceresinden erişilebilir).
Yeni uygulama başlat	Yeni uygulamaların veya işlemlerin başlatılması.
Başka bir uygulamanın durumunu değiştir	Kaynak uygulama hedef uygulamanın belleğine yazmaya çalışır veya onun adına kodu çalıştırır. Bu işlevsellik, bu işlemin kullanımını engelleyen bir kuralda hedef bir uygulama olarak yapılandırmak yoluyla önemli bir uygulamayı korumak için kullanışlı olabilir.

Kural, yalnızca işlemin bu hedefle ilgili olması durumunda kullanılır. Açılır menüden **Belirli uygulamaları** seçin ve yeni dosya veya klasörleri eklemek için **Ekle** seçeneğini tıklayın. Ayrıca tüm uygulamaları eklemek için açılır menüden **Tüm uygulamalar** seçeneğini de belirleyebilirsiniz.

Kayıt defteri işlemleri:

Başlatma ayarlarını değiştir	Ayarlardaki, Windows açılışında çalıştırılacak uygulamaları tanımlayan tüm değişikliklerdir. Bunlar Windows Kayıt Defteri'nde örneğin Çalıştırma anahtarı aranarak bulunabilir.
Kayıt defterinden sil	Kayıt defteri anahtarını veya değerini siler.
Kayıt defteri anahtarını yeniden adlandır	Kayıt defteri anahtarlarını yeniden adlandırır.
Kayıt defterini değiştir	Kayıt defteri anahtarlarının yeni değerlerini oluşturabilir, mevcut değerleri değiştirebilir, veri tabanı ağacından veri taşıma veya kayıt defteri anahtarı için kullanıcı veya grup hakları ayarlayabilirsiniz.

Kural, yalnızca işlemin bu hedefle ilgili olması durumunda kullanılır. Açılır menüden **Belirli girişleri** seçin ve yeni dosya veya klasörleri eklemek için **Ekle** seçeneğini tıklayın. Ayrıca tüm uygulamaları eklemek için açılır menüden **Tüm girişler** seçeneğini de belirleyebilirsiniz.

NOT
Bir hedef girerken, belirli kısıtlamalarla joker karakterler kullanabilirsiniz. Belirli bir anahtarın yerine * (yıldız işareti) simgesi kayıt defteri yollarında kullanılabilir. Örneğin *HKEY_USERS*\software can mean HKEY_USER\.default\software* anlamına gelebilir ancak *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software* anlamına gelemez. *HKEY_LOCAL_MACHINE\system\ControlSet** geçerli bir kayıt defteri anahtarı yolu değildir. *** içeren bir kayıt defteri anahtarı yolu, "bu yolu veya bu sembolden sonraki herhangi bir düzeydeki herhangi bir yolu" tanımlar. Dosya hedefleri için joker karakter kullanmanın tek yolu budur. Öncelikle, bir yolun belirli bir parçası, ardından joker karakter simgesini (*) izleyen yol değerlendirilir.

UYARI
Çok genel bir kural oluşturursanız, bir bildirim alabilirsiniz.

HIPS gelişmiş ayarları

Aşağıdaki seçenekler, hata ayıklamak ve uygulamanın davranışını analiz etmek için faydalıdır:

Sürücüler her zaman yüklenebilir

Seçili sürücülerin, kullanıcı kuralı tarafından açıkça engellenmedikleri sürece yapılandırılmış filtreleme modundan bağımsız olarak her zaman yüklenmesine izin verilir. Bu listede gösterilen sürücülerin, kullanıcı kuralı tarafından açıkça engellenmediği sürece HIPS filtreleme modundan bağımsız olarak her zaman yüklenmesine izin verilir. Yeni sürücü **Ekleyebilir**, listeden seçili sürücü **Düzenleyebilir** veya **Silebilirsiniz**.

NOT
Manuel olarak eklediğiniz sürücülerin dahil edilmesini istemiyorsanız **Sıfırla** öğesini tıklatın. Birçok sürücü eklediyseniz ve bunları listeden manuel olarak silemiyorsanız bu seçenek kullanılabilir.

Engellenen tüm işlemleri günlüğe kaydet

Engellenen tüm işlemler HIPS günlüğüne yazılır.

Başlangıç uygulamalarında değişiklik meydana geldiğinde bildir

Sistem başlangıcına her uygulama eklendiğinde veya buradan her uygulama kaldırıldığında bir masaüstü bildirimi görüntüler.

Güncelleme yapılandırması

Bu bölüm, kullanılan güncelleme sunucuları gibi güncelleme kaynağı bilgilerini ve bu sunucular için kimlik doğrulama verilerini belirtir.

NOT
Güncellemelerin düzgün bir şekilde indirilmesi için tüm güncelleme parametrelerini doğru doldurmanız önemlidir. Güvenlik duvarı kullanıyorsanız ESET programınızın İnternet iletişimi (örneğin, HTTP iletişimi) kurmasına izin verildiğinden emin olun.

Temel

Varsayılan güncelleme profilini seç

Güncellemeler için varsayılan olarak uygulanacak mevcut profili seçin veya yeni profil oluşturun.

Güncelleme önbelleğini temizle

Güncellemeyle ilgili sorunlar yaşıyorsanız geçici güncelleme önbelleğini temizlemek için **Temizle** öğesini tıklayın.

Maksimum algılama altyapısı yaşını otomatik olarak ayarla / Maksimum algılama altyapısı yaşı (gün)

Algılama altyapısı yaşının ne kadar zaman sonra (maksimum gün sayısı) güncel değil şeklinde bildirileceğini belirlemenize olanak tanır. Varsayılan değer 7'dir.

Modülü Geri Alma

Algılama altyapısının ve/veya program modüllerinin yeni güncellemesinin kararsız veya bozuk olduğundan şüpheleniyorsanız, önceki sürüme geri alabilir ve belirlediğiniz bir süre boyunca güncellemeleri devre dışı bırakabilirsiniz. Alternatif olarak, önceden devre dışı bıraktığınız güncellemeleri süresiz bir şekilde ertelemişseniz etkin hale getirebilirsiniz. ESET Server Security, Geri al özelliğiyle kullanmak için algılama altyapısının ve program modüllerinin sistem görüntülerini kaydeder. Algılama altyapısı sistem görüntüleri oluşturmak için **Modüllerin sistem görüntülerini oluştur** seçeneğini etkin durumda bırakın.

Yerel olarak depolanan sistem görüntülerinin sayısı

Depolanan önceki modül sistem görüntülerinin sayısını tanımlar.

Profiller

Özel güncelleme profili oluşturmak için, **Profil listesi** yanındaki **Düzenle** seçeneğini belirleyin, **Profil adınızı** girin ve **Ekle**'yi tıklayın. **Düzenlenecek profili seçin** ve **modül güncellemeleri** türleri için parametreleri değiştirin veya **Güncelleme yansıtması** oluşturun.

Güncellemeler

Açılır menüden kullanılacak olan güncelleme türünü seçin:

- **Düzenli güncelleme** - Varsayılan olarak, güncelleme dosyalarının en az ağ trafiğine sahip ESET sunucusundan otomatik olarak indirilmesini sağlamak için Güncelle türü Düzenli güncelle olarak ayarlanır.
- **Sınama modu güncellemesi** - Dahili sınamadan geçen ve kısa bir süre sonra genel olarak kullanılabilir duruma gelecek güncellemelerdir. En son algılama yöntemlerine ve düzeltmelere erişim elde ederek sınama modu güncellemelerini etkinleştirme avantajından faydalanabilirsiniz. Ancak, sınama modu güncellemeleri her zaman yeterince kararlı olmayabilir ve maksimum kullanılabilirlik ve kararlılık gerektiren üretim sunucularında ve iş istasyonlarında KULLANILMAMALIDIR.
- **Gecikmeli güncelleme** - Özel güncelleme sunucularından güncelleme gerçekleştirilmesine izin verir ve en az X saat gecikme ile virüs veri tabanlarının yeni sürümlerini sağlar (ör. gerçek bir ortamda test edilmiş ve bu nedenle kararlı olarak değerlendirilen veri tabanları).

Güncellemeyi karşıdan yüklemeden önce sor

Yeni güncelleme mevcut olduğunda, indirmeden önce size sorulur.

Güncelleme dosyası şu boyuttan büyükse sor (kB)

Güncelleme dosyasının boyutu, alanda belirtilen değerden büyükse bir bildirim görüntülenir.

Başarılı güncelleme hakkındaki bildirimi devre dışı bırak

Ekranın sağ alt köşesindeki sistem tepsisi bildirimini kapatır. Tam ekran bir uygulama çalıştırılıyorsa bu seçeneğin belirlenmesi yararlı olacaktır. Sunum modunun tüm bildirimleri kapattığını unutmayın.

Modül güncellemeleri

Modül güncellemeleri, varsayılan olarak **Otomatik seç** şeklinde ayarlanır. Güncelleme sunucusu, güncellemelerin depolandığı konumdur. ESET sunucusu kullanıyorsanız varsayılan seçeneği seçili bırakmanızı öneririz.

Yerel HTTP sunucusu (Yansıtma olarak da bilinir) kullanırken, güncelleme sunucusu şu şekilde ayarlanmalıdır: ***http://computer_name_or_its_IP_address:2221***
SSL kullanan yerel HTTP sunucusu kullanırken, güncelleme sunucusu şu şekilde ayarlanmalıdır: *https://computer_name_or_its_IP_address:2221*
Yerel paylaşılan klasör kullanırken, güncelleme sunucusu şu şekilde ayarlanmalıdır: *computer_name_or_its_IP_address**shared_folder*

Algılama imzalarının daha sık güncellenmesini etkinleştir

Algılama altyapısı daha kısa aralıklarla güncellenir. Bu seçeneği devre dışı bırakmak algılama oranını olumsuz yönde etkiler.

Çıkarılabilir medyadan güncellemelere izin ver

Oluşturulan yansıtmayı içermesi halinde çıkarılabilir medyadan güncelleme yapın. **Otomatik** seçildiğinde güncellemeler arka planda çalışır. Güncelleme iletişim kutularını göstermek istiyorsanız **Her zaman sor** seçeneğini belirleyin.

Program bileşeni güncellemesi

Yeni bir güncelleme olduğunda ESET Server Security Program Bileşeni Güncellemelerinin (PCU) ve micro Program Bileşeni Güncellemelerinin (µPCU) nasıl uygulanacağını seçmek için **Güncelleme modu** açılır menüsünü kullanın. Bileşen güncellemeleri genellikle mevcut özellikleri değiştirir ancak yeni özellikler ve düzeltmeler de içerebilir. Seçilen güncelleme moduna bağlı olarak, bileşen güncellemesi müdahale veya onay olmaksızın otomatik olarak gerçekleştirilebilir (yeniden başlatma gerekirse size sorulacaktır). Alternatif olarak, güncellemeler yüklenmeden önce bildirim almayı seçebilirsiniz.

NOT
Bazı durumlarda, bileşen güncellemesinin ardından sunucunun yeniden başlatılması gerekebilir.

Şu güncelleme modları kullanılabilir:

- **Güncellemeden önce sor** - Kullanılabilir olduklarında ürün güncellemelerini onaylamanız veya reddetmeniz için sorulur. Bu, varsayılan seçenektir. Bileşen güncellemesinin ardından sunucunun yeniden başlatılması gerekebilir.
- **Otomatik güncelleme** - Bileşen güncellemeleri otomatik olarak indirilir ve yüklenir. Sunucunun yeniden başlatılması gerekebileceğini unutmayın.
- **Hiçbir zaman güncelleme** - Bileşen güncellemeleri hiçbir şekilde gerçekleştirilmez. Bu seçenek, bileşen güncellemelerini manuel olarak çalıştırmanıza ve zamanlanan bakım dönemi sırasında sunucunuzu yeniden başlatmanıza olanak tanır.

ÖNEMLİ
Otomatik güncelleme modu, bileşen güncellemesi tamamlandıktan sonra sunucunuzu otomatik olarak yeniden başlatır.

Bağlantı seçenekleri

Proxy sunucu

Belirli bir güncelleme profili için proxy sunucu ayar seçeneklerine erişmek amacıyla. **Proxy modu** açılır menüsünü tıklatın ve aşağıdaki üç seçenekten birini belirleyin:

- **Proxy sunucu kullanma** - Güncellemeler gerçekleştirilirken ESET Server Security tarafından hiçbir proxy sunucu kullanılmaz.
- **Genel proxy sunucu ayarlarını kullan** - **Gelişmiş ayarlar** (F5) > **Araçlar** > Proxy sunucu alanında belirtilen proxy sunucu yapılandırması kullanılır.
- **Proxy sunucu aracılığıyla bağlantı** - Bu seçeneği şu durumlarda kullanın:

ESET Server Security Uygulamasını güncellemek için genel ayarlarda (Araçlar > Proxy sunucu) belirtilen proxy sunucudan farklı bir proxy sunucu kullanılmalıdır. Böyle bir durumda burada şu ayarlar belirtilmelidir: Proxy sunucusu adresi, Bağlantı noktası (varsayılan olarak 3128) iletişimi, gerekirse, proxy sunucusu için Kullanıcı adı ve Parola.
Proxy sunucu ayarları genel olarak belirlenmedi, ancak ESET Server Security güncellemeler için bir proxy sunucuya bağlanacak.
Bilgisayarınız İnternet'e bir proxy sunucu üzerinden bağlanır. Ayarlar program yüklemesi sırasında Internet Explorer'dan alınır, ancak daha sonra değiştirilmeleri durumunda (örneğin ISP'nizi değiştirirseniz) bu pencerede listelenen HTTP proxy ayarlarının doğru olup olmadığını kontrol edin. Aksi takdirde, program güncelleme sunucularına bağlanamaz.

NOT
Kullanıcı Adı ve **Parola** gibi kimlik doğrulama verileri, proxy sunucuya erişme amaçlıdır. Bu alanları, yalnızca kullanıcı adı ve parola gerekiyorsa tamamlayın. Lütfen bu alanların ESET Server Security uygulamasına yönelik Kullanıcı Adınız/Parolanız olmadığını ve yalnızca İnternet'e proxy sunucu aracılığıyla erişmek için parolaya gereksinim duyduğunuzu biliyorsanız doldurulması gerektiğini unutmayın.

Proxy mevcut değilse doğrudan bağlantıyı kullanın

Bir ürün HTTP Proxy kullanacak şekilde yapılandırılmışsa, ancak proxy'ye ulaşılamıyorsa, ürün proxy'yi atlayarak doğrudan ESET sunucularıyla iletişim kurar.

Windows Paylaşımları

Windows işletim sistemine sahip yerel bir sunucudan güncellerken, varsayılan olarak her ağ bağlantısı için kimlik doğrulaması gerekir.

LAN'a bağlanma yöntemi

Hesabınızı yapılandırmak için aşağıdaki seçeneklerden birini belirleyin:

- **Sistem hesabı (varsayılan)** - Kimlik doğrulaması için sistem hesabını kullanın. Genellikle, ana güncelleme ayarları bölümünde sağlanmış kimlik doğrulama verisi yoksa, hiçbir kimlik doğrulama işlemi gerçekleşmez.
- **Mevcut kullanıcı** - Programın halihazırda giriş yapmış olan kullanıcı hesabını kullanarak kimlik doğrulamasını sağlamak için bu seçeneği belirleyin. Bu çözümün sakıncası, giriş yapmış kullanıcı olmadığında programın güncelleme sunucusuna bağlanamamasıdır.

- **Belirli kullanıcı** - Kimlik doğrulaması için belirli bir kullanıcı hesabı kullanmak üzere bu seçeneği belirleyin. Varsayılan sistem hesabı bağlantısı başarısız olduğunda bu yöntemi kullanın. Belirtilen kullanıcı hesabının, yerel sunucudaki güncelleme dosyaları dizinine erişimi olması gerektiğini unutmayın. Kullanıcının erişimi yoksa, program bağlantı kuramaz veya güncellemeleri indiremez.

UYARI
Geçerli kullanıcı veya **Belirtilen kullanıcı** seçildiğinde, programın kimliğini istenen kullanıcı olarak değiştirirken bir hata oluşabilir. LAN kimlik doğrulama verilerinin ana güncelleme ayarları bölümüne girilmesini öneririz. Bu güncelleme ayarları bölümünde, kimlik doğrulama verileri şöyle girilmelidir: *domain_name\user* (bu bir çalışma grubuysa, *workgroup_name\name* girin) ve parola. Yerel sunucunun HTTP sürümünden güncellerken, kimlik doğrulaması gerekmez.

Güncellemeden sonra sunucu bağlantısını kes

Güncellemeler indirildikten sonra bile sunucu bağlantısı etkin durumda kalırsa, bağlantıyı kesmeye zorlamak için bu seçeneği belirleyin.

Güncelle yansıtması

Yerel Yansıtma sunucusu için yapılandırma seçenekleri **Gelişmiş ayarlar** ağacında (F5) **Güncelle** > **Profiller** > Güncelleme Yansıtması sekmesinde bulunmaktadır.

Güncelle geri dönüşü

Geri al seçeneğini tıklatırsanız, algılama altyapısı veri tabanı ve program modülü güncellemelerinin duraklatılacağı süreyi temsil eden açılır menüden bir zaman aralığı seçmeniz gerekir.

Güncelle işlevini manuel olarak geri yükleyene kadar düzenli güncellemeleri süresiz bir şekilde ertelemek için **İptal edilene kadar** öğesini seçin. Olası bir güvenlik riski taşıdığından, bu seçeneği belirlemenizi önermeyiz.

Algılama altyapısı veri tabanı sürümü kullanılabilir olan en eski sürüme indirilir ve yerel bilgisayar dosya sisteminde sistem görüntüsü olarak kaydedilir.

Zamanlanan Görev - Güncelleme

Programı iki güncelleme sunucusundan güncellemek istiyorsanız, iki farklı güncelleme profili oluşturulması gerekir. Birincisi güncelleme dosyalarını indiremezse, program otomatik olarak diğerine geçiş yapar. Bu, örneğin normalde yerel bir LAN güncelleme sunucusundan güncelleme yapan ancak sahipleri genellikle başka ağlar kullanarak İnternet'e bağlanan dizüstü bilgisayarlar için uygundur. Bu nedenle, birinci profil başarısız olursa, ikinci profil otomatik olarak ESET'in güncelleme sunucularından güncelleme dosyalarını indirecektir.

ÖRNEK
Aşağıdaki adımlar, mevcut **Düzenli otomatik güncelleme** düzenleme görevinde size kılavuzluk eder.
1.Ana **Zamanlayıcı** ekranında, **Düzenli otomatik güncelleme** adlı **Güncelleme** görevini seçip **Düzenle**'yi tıklayın. Yapılandırma sihirbazı açılır.
2.Zamanlayıcı görevini yürütmeye ayarlayın, zamanlanan görevin yürütüleceği zamanı tanımlamak için aşağıdaki zamanlama seçeneklerinden birini seçin.
3.Sistem pillerden çalışırken (örneğin UPS) görevin yürütülmesini önlemek istiyorsanız, **Pil gücünde çalışırken görevi atla** seçeneğinin yanındaki anahtarı tıklatın.
4.Güncelleme için kullanılacak güncelleme profilini seçin. Zamanlanan görevin yürütülmesi herhangi bir nedenle başarısız olursa, gerçekleştirilecek bir eylem seçin.
5.Görevi uygulamak için **Bitir**'i tıklatın.

Güncelle yansıtması

ESET Server Security Uygulamasını aç
F5 > Güncelleme > Profiller > Güncelleme yansıtması'na basın

ESET Server Security, ağda bulunan diğer iş istasyonlarını güncellemek üzere kullanılabilecek güncelleme dosyası kopyaları oluşturmanıza olanak tanır. "Yansıtma"'nın kullanımı - Satıcının güncelleme sunucusundan güncelleme dosyalarını indirme işleminin her iş istasyonu için yinelenmesi gerekmediğinden, LAN ortamında güncelleme dosyalarının kopyası yararlı olur. Güncelleler, yerel yansıtma sunucusuna yüklenir ve ardından ağ trafiğine aşırı yüklenme riskini ortadan kaldırmak için tüm iş istasyonlarına dağıtılır. İstemci iş istasyonlarını bir yansıtmadan güncellemek ağ yükü dengesini optimize eder ve İnternet bağlantısı bant genişliğinden tasarruf eder.

⊟ Güncelle yansıtması

Güncelle yansıtması oluştur

Yansıtma yapılandırma seçeneklerini etkinleştirir.

Depolama klasörü

Yansıtılan dosyaları *C:\ProgramData\ESET\ESET Security\mirror depolamak için tanımlanmış varsayılan klasörü değiştirmek isterseniz, Temizle seçeneğini tıklayın. Yerel bilgisayarda veya paylaşılan bir ağ klasöründe bir klasörü bulmak için* **Düzenle** seçeneğini tıklayın. Belirtilen bir klasör için yetki gerekiyorsa yetkilendirme verileri Kullanıcı adı ve Parola alanlarına girilmelidir. Seçilen hedef klasör Windows NT/2000/XP işletim sistemi çalıştıran bir ağ diskinde bulunuyorsa, belirtilen kullanıcı adı ve parola, seçilen klasör için yazma ayrıcalıklarına sahip olmalıdır.
Kullanıcı adı ve parola, *Domain/User* veya *Workgroup/User* biçiminde girilmelidir. Lütfen ilgili parolaları sağlamayı unutmayın.

Program bileşeni güncellemesi

Dosyalar

Yansıtmayı yapılandırırken yüklemek istediğiniz güncellemelerin dil sürümlerini belirtebilirsiniz. Seçilen dillerin, kullanıcının yapılandırdığı yansıtma sunucusu tarafından desteklenmesi gerekir.

Bileşenleri otomatik olarak güncelle

Yeni özelliklerin ve güncellemelerin var olan özelliklere yüklenmesine olanak tanır. Güncelleme, kullanıcı

müdahalesi olmadan otomatik gerçekleştirilebilir veya uyarıda bulunulmasını seçebilirsiniz. Ürün güncellemesi yüklendikten sonra bilgisayarı yeniden başlatmak gerekebilir.

Bileşenleri şimdi güncelle

Program bileşenlerinizi en son sürüme günceller.

HTTP sunucusu

Sunucu bağlantı noktası

Varsayılan bağlantı noktası 2221'dir. Farklı bir bağlantı noktası kullanıyorsanız bu değeri değiştirin.

Kimlik doğrulaması

Güncelleme dosyalarına erişmek için kullanılan kimlik doğrulama yöntemini tanımlar. Kullanılabilir seçenekler şunlardır: **Yok**, **Temel** ve **NTLM**.

- Temel kullanıcı adı ve parola kimlik doğrulamasıyla base64 kodlamasını kullanmak için **Temel** öğesini seçin.
- **NTLM** seçeneği, güvenli bir kodlama yöntemi kullanarak kodlama sağlar. Kimlik doğrulama için, güncelleme dosyalarını paylaşan iş istasyonunda oluşturulan kullanıcı kullanılır.
- Varsayılan ayar, kimlik doğrulama gerekmeden güncelleme dosyalarına erişim izni veren **Yok** seçeneğidir.

UYARI
HTTP sunucusu aracılığıyla güncelleme dosyalarına erişime izin vermek istiyorsanız, Yansıtma klasörünün onu oluşturan ESET Server Security örneğiyle aynı bilgisayarda bulunması gerekir.

HTTP sunucusu için SSL

HTTPS (SSL) destekli HTTP sunucusu çalıştırmak istiyorsanız, **Sertifika zincir dosyanızı** ekleyin veya otomatik olarak imzalı sertifika oluşturun. Şu sertifika türleri mevcuttur: PEM, PFX ve ASN. Ek güvenlik amacıyla, güncelleme dosyalarını indirmek için HTTPS protokolünü kullanabilirsiniz. Bu protokol kullanılarak veri aktarımlarının ve oturum açma kimlik bilgilerinin takip edilmesi neredeyse imkansızdır.
Özel anahtar türü, varsayılan olarak **Tümleşik** biçiminde ayarlanmıştır (bu nedenle Özel anahtar dosyası seçeneği varsayılan olarak devre dışıdır). Bu, özel anahtarın seçili sertifika zincir dosyasının bir parçası olduğu anlamına gelir.

Bağlantı seçenekleri

Windows Paylaşımları

Windows işletim sistemine sahip yerel bir sunucudan güncellerken, varsayılan olarak her ağ bağlantısı için kimlik doğrulaması gerekir.

LAN'a bağlanma yöntemi

Hesabınızı yapılandırmak için aşağıdaki seçeneklerden birini belirleyin:

- **Sistem hesabı (varsayılan)** - Kimlik doğrulaması için sistem hesabını kullanın. Normalde, ana güncelleme ayarları bölümünde sağlanmış kimlik doğrulama verisi yoksa, hiçbir kimlik doğrulama işlemi gerçekleşmez.

- **Mevcut kullanıcı** - Programın halihazırda giriş yapmış olan kullanıcı hesabını kullanarak kimlik doğrulamasını sağlamak için bu seçeneği belirtin. Bu çözümün sakıncası, oturum açmış kullanıcı olmadığında programın güncelleme sunucusuna bağlanamamasıdır.

- **Belirli kullanıcı** - Kimlik doğrulaması için belirli bir kullanıcı hesabı kullanın. Varsayılan sistem hesabı bağlantısı başarısız olduğunda bu yöntemi kullanın. Belirtilen kullanıcı hesabının, yerel sunucudaki güncelleme dosyaları dizinine erişimi olması gerektiğini unutmayın. Kullanıcının erişimi yoksa, program bağlantı kuramaz ve güncellemeleri indiremez.

UYARI
Geçerli kullanıcı veya **Belirtilen kullanıcı** seçildiğinde, programın kimliğini istenen kullanıcı olarak değiştirirken bir hata oluşabilir. LAN kimlik doğrulama verilerinin ana güncelleme ayarları bölümüne girilmesini öneririz. Bu güncelleme ayarları bölümünde, kimlik doğrulama verileri şöyle girilmelidir: *domain_name\user* (bu bir çalışma grubuysa, *workgroup_name\name* girin) ve parola. Yerel sunucunun HTTP sürümünden güncellerken, kimlik doğrulaması gerekmez.

Güncellemeden sonra sunucu bağlantısını kes

Güncellemeler indirildikten sonra bile sunucu bağlantısı etkin durumda kalırsa, bağlantıyı kesmeye zorlamak için bu seçeneği belirleyin.

Ağ saldırısına karşı koruma

Ağ saldırısına karşı korumayı etkinleştir (IDS)

Bilgisayarınızda çalışan hizmetlerden bazılarına Güvenilir bölgeden erişimi yapılandırmanıza ve bilgisayarınıza zarar vermek için kullanılabilecek çeşitli saldırı ve açıklardan yararlanma türlerinin algılanmasını etkinleştirmenize/devre dışı bırakmanıza izin verir.

Botnet korumasını etkinleştir

Bilgisayara virüs bulaştığında ve bir bot iletişim kurma girişiminde bulunduğunda tipik modellere dayalı olarak kötü amaçlı komut ve kontrol sunucuları içeren iletişimi algılar ve engeller

IDS özel durumları

Yetkisiz Giriş Algılama (IDS) özel durumlarını ağ koruma kuralları olarak düşünebilirsiniz. IDS özel durumlarını tanımlamak için düzenle'yi tıklayın.

NOT
Ortamınız yüksek hızlı bir ağ (10 GbE ve üzeri) çalıştırıyorsa, ağ hızı performansı ve ESET Server Security ile ilgili bilgiler için Bilgi Bankası makalesini okuyun.

Deneme yanılma saldırısına karşı koruma

ESET Server Security ağ trafiği içeriğini inceler ve parola tahmini amaçlı saldırı girişimlerini engeller.

Gelişmiş seçenekler

Bilgisayarınıza karşı gerçekleştirilebilecek çeşitli saldırı türlerini ve güvenlik açıklarını algılamak için gelişmiş filtreleme seçenekleri yapılandırın.

Yetkisiz giriş algılama:

SMB Protokolü - SMB protokolündeki çeşitli güvenlik sorunlarını algılar ve engeller
RPC Protokolü – Dağıtılmış Bilgi İşlem Ortamı (DCE) için geliştirilen uzaktan prosedür arama sistemindeki çeşitli CVE'leri algılar ve engeller.
RDP Protokolü – RDP protokolündeki çeşitli CVE'leri algılar ve engeller (yukarıya bakın).
Saldırının algılanmasından sonra güvenli olmayan adresi engelle – Saldırıların kaynağı olarak algılanan IP adresleri, belirli bir süreliğine bağlantının önlenmesi için Kara Liste'ye eklenir.
Saldırının algılamasından sonra bildirim görüntüle – Ekranın sağ alt köşesindeki sistem tepsisindeki bildirimi açar.
Güvenlik boşluklarına yönelik saldırılar için bildirimleri göster – Güvenlik boşluklarına yönelik saldırılar algılanırsa veya bir tehdit bu şekilde sisteme girmek için girişimde bulunursa sizi uyarır.

Paket denetleme:

KOBİ protokolünde yönetici paylaşımlarının gelen bağlantısına izin ver - Yönetici paylaşımları (yönetici paylaşımları) sabit sürücü kısımlarını (C$, D$, ...) sistem klasörü ile birlikte (ADMIN$) sistem içinde paylaşan varsayılan ağ paylaşımlarıdır. Yönetici paylaşımları bağlantısını devre dışı bırakmak, birçok güvenlik riskini ortadan kaldırabilir. Örneğin, Conficker kurdu yönetici paylaşımlarına bağlanmak için sözlük saldırıları gerçekleştirir.
Eski (desteklenmeyen) SMB lehçelerini reddet – IDS tarafından desteklenmeyen eski bir SMB lehçesi kullanan SMB oturumlarını reddeder. Modern Windows işletim sistemleri Windows 95 gibi eski işletim sistemleriyle geriye dönük uyumluluk nedeniyle eski SMB diyalektlerini destekler. Saldırgan, trafik denetlemesinden kaçınmak için SMB oturumunda eski bir diyalekti kullanabilir. Bilgisayarınızın, dosyaları eski bir Windows sürümüne sahip bir bilgisayarla paylaşması gerekmiyorsa (veya genellikle SMB iletişimi kullanıyorsa) eski SMB diyalektlerini reddedin.
Genişletilmiş güvenlik olmadan SMB oturumlarını reddet – Genişletilmiş güvenlik, LAN Manager Sınama/Yanıt (LM) kimlik doğrulamasından daha güvenli kimlik doğrulama mekanizması sağlamak için SMB oturumu anlaşması sırasında kullanılabilir. LM şeması zayıf olarak değerlendirilir ve kullanılması önerilmez.
Güvenlik Hesabı Yöneticisi hizmeti ile iletişime izin ver – Bu hizmet hakkında daha fazla bilgi için [MS-SAMR] bölümüne bakın.
Yerel Güvenlik Yetkilisi hizmeti ile iletişime izin ver – Bu hizmet hakkında daha fazla bilgi için [MS-LSAD] ve [MS-LSAT] bölümüne bakın.
Uzak Kayıt Defteri hizmeti ile iletişime izin ver – Bu hizmet hakkında daha fazla bilgi için [MS-RRP] bölümüne bakın.
Hizmet Denetimi Yöneticisi hizmeti ile iletişime izin ver – Bu hizmet hakkında daha fazla bilgi için [MS-SCMR] bölümüne bakın.
Sunucu hizmeti ile iletişime izin ver – Bu hizmet hakkında daha fazla bilgi için [MS-SRVS] bölümüne bakın.
Diğer hizmetlerle iletişime izin ver – Diğer MSRPC hizmetleri.

IDS özel durumları

Yetkisiz Giriş Algılama (IDS) özel durumları esas olarak ağ koruma kurallarıdır. Özel durumlar yukarıdan aşağıya değerlendirilir. IDS özel durumları düzenleyici, çeşitli IDS özel durumları üzerinden ağ koruma davranışını özelleştirmenize olanak tanır. İlk eşleme özel durumu her bir işlem türü için (Engelleme, Bildirme, Günlük) ayrı ayrı uygulanır. **Üst/Yukarı/Aşağı/Alt** özel durumların öncelik düzeyini ayarlamanızı sağlar. Yeni bir IDS özel durumu oluşturmak için **Ekle**'yi tıklayın. Mevcut bir IDS özel durumunu değiştirmek için **Düzenle**'yi veya kaldırmak için **Sil**'i tıklayın.

Açılır listeden **Uyarı** türünü seçin. **Tehdit adı** ve **Yönlendirme**'yi belirtin. Özel durum oluşturmak istediğiniz **Uygulama**'yı bulun. IP adreslerinden (IPv4 veya IPv6) veya alt ağlardan oluşan bir liste belirleyin. Birden çok giriş için ayırıcı olarak virgül kullanın.

Açılır menüdeki seçeneklerden birini belirleyerek (**Varsayılan**, **Evet**, **Hayır**) IDS özel durumu için **Eylem**'i yapılandırın. Bunu her Eylem türü için yapın (**Engelle**, **Bildirim gönder**, **Günlüğe kaydet**).

ÖRNEK
Bir IDS özel durum uyarısı olması halinde bildirim gösterilmesini istiyorsanız ayrıca olayın günlüğe kaydedilme zamanını da görmek istiyorsanız, **Engelle** eylem türünü **Varsayılan** olarak bırakın ve diğer iki eylem türü için (**Bildirim gönder** ve **Günlüğe kaydet**) açılır menüden **Evet**'i seçin.

Geçici IP adresi kara listesi

Saldırı kaynakları olduğu algılanan ve bağlantıların belirli bir süreliğine engellenmesi için kara listeye eklenen IP adreslerinin bir listesini görüntüler. Kilitlenen **IP adresini** gösterir.

Engelleme nedeni

Adresten engellenen saldırı türünü (örneğin, TCP Bağlantı Noktası Tarama saldırısı) gösterir.

Süre aşımı

Adresin kara listedeki süresinin dolacağı saati ve tarihi gösterir.

Kaldır/Tümünü kaldır

Süresi dolmadan önce, seçili IP adresini geçici kara listeden kaldırır veya tüm adresleri kara listeden anında kaldırır.

Özel durum ekle

Seçili IP adresi için IDS filtrelemesine güvenlik duvarı özel durumu ekler.

Web ve e-posta

İnternet iletişimi sırasında sunucunuzu korumak için protokol filtrelemesini, E-posta istemci korumasını, Web erişimi korumasını ve Kimlik avı korumasını yapılandırabilirsiniz.

E-posta istemci koruması

Tüm e-posta iletişimini denetler, kötü amaçlı koda karşı koruma sağlar ve virüs bulaşma durumu algılandığında gerçekleştirilecek eylemi seçmenize olanak tanır.

Web erişimi koruması

Web tarayıcıları ile uzak sunucular arasındaki iletişimi izler ve de HTTP ve HTTPS kurallarına uyar. Bu özellik ayrıca belirli URL adreslerine izin vermenizi, bunları engelleyebilmenizi veya denetleme dışında bırakmanızı sağlar.

Protokol filtrelemesi

Uygulama protokolleri için gelişmiş bir koruma sunar ve ThreatSense tarama altyapısı tarafından sağlanır. Bu denetim web tarayıcısı veya e-posta istemcisinden bağımsız bir şekilde otomatik olarak çalışır. Ayrıca şifreli (SSL/TLS) iletişimi için de çalışır.

Kimlik Avı Koruması

Kimlik avı amaçlı içeriği yaydığı bilinen web sayfalarını engellemenizi sağlar.

Protokol filtrelemesi

Uygulama protokolleri için zararlı yazılım koruması, çeşitli gelişmiş kötü amaçlı yazılım tarama tekniklerini bütünleştiren ThreatSense tarama altyapısı tarafından sağlanır. Protokol filtreleme, kullanılan İnternet tarayıcısından veya e-posta istemcisinden bağımsız olarak otomatik çalışır. Protokol filtrelemesi etkinse, ESET Server Security SSL/TLS protokolü kullanan iletişimleri denetler. **Web ve e-posta** > SSL/TLS bölümüne gidin.

Uygulama protokolü içerik filtresini etkinleştir

Protokol filtrelemesini devre dışı bırakırsanız birçok ESET Server Security bileşeninin (**Web erişimi koruması**, **E-posta protokolleri koruması** ve **Kimlik Avı koruması**) buna bağlı olduğunu ve tüm özelliklerinin kullanılamayacağını unutmayın.

Tarama dışı bırakılan uygulamalar

Ağı algılayan belirli uygulamaları içerik filtreleme dışında bırakmak için bu uygulamaları listeden seçin. Seçili uygulamaların HTTP/POP3 iletişimi tehditlere karşı denetlenmeyecektir. Belirli uygulamaları protokol filtrelemesi dışında bırakmanızı sağlar. Protokol filtrelemesi dışında bırakmak için uygulama listesinden bir yürütülebilir dosya seçmek üzere **Düzenle** ve **Ekle** seçeneklerini tıklayın.

ÖNEMLİ
Bu seçeneğin yalnızca, iletişimleri denetlendiğinde düzgün şekilde çalışmayan uygulamalar için kullanılmasını öneririz.

Tarama dışı bırakılan IP adresleri

Belirli uzak adresleri protokol filtrelemesi dışında bırakmanızı sağlar. Bu listedeki IP adresleri protokol içerik filtresi dışında bırakılır. Seçili adreslerle olan HTTP/POP3/IMAP iletişimi tehditlere karşı denetlenmez.

ÖNEMLİ
Bu seçeneği yalnızca güvenilir olduğu bilinen adresler için kullanmanızı öneririz.

Dışlamanın uygulanacağı IP adresini, adres aralığını veya alt ağı belirtmek için **Düzenle ve Ekle** seçeneklerini tıklayın. **Birden fazla değer gir** öğesini seçtiğinizde yeni satırlar, virgüller veya noktalı virgüller ile ayrılmış birden fazla IP adresi ekleyebilirsiniz. Birden fazla seçim etkinleştirildiğinde adresler hariç tutulan IP adresleri listesinde görünür.

NOT
Tarama dışı bırakma işlemleri, protokol filtrelemenin uyumluluk sorunlarına neden olması durumunda yararlıdır.

Web ve e-posta istemcileri

İnternet'te çok yüksek sayıda kötü amaçlı kod dolaştığından, İnternet'te güvenli gezinmek bilgisayarı korumak açısından çok önemlidir. Web tarayıcısındaki güvenlik açıkları ve sahte bağlantılar, kötü amaçlı kodların hiç farkında olunmadan sisteme girmesine yardımcı olur; bu nedenle ESET Server Security, web tarayıcı güvenliği üzerine odaklanır. Ağa erişen tüm uygulamalar İnternet tarayıcısı olarak işaretlenebilir. İletişim için zaten protokolleri kullanan uygulamalar veya seçilen yollardaki uygulamalar, Web ve e-posta istemcileri listesine eklenebilir.

SSL/TLS

ESET Server Security, Güvenli Yuva Katmanı (SSL) / Aktarım Katmanı Güvenliği (TLS) protokolünü kullanan iletişimlerde tehditleri denetleme becerisine sahiptir.

Güvenilir sertifikaları, bilinmeyen sertifikaları veya SSL korumalı iletişim denetimi dışında tutulan sertifikaları kullanan SSL korumalı iletişimleri incelemek için çeşitli tarama modlarını kullanabilirsiniz.

SSL/TLS protokolü filtrelemesini etkinleştir

Protokol filtrelemesi devre dışı bırakılmışsa program SSL/TLS üzerinden iletişimleri taramaz. Güvenli Yuva Katmanı (SSL) / Aktarım Katmanı Güvenliği (TLS) protokol filtrelemesi modu şu seçeneklerde kullanılabilir:

- **Otomatik mod** - Denetim dışında bırakılan sertifikalar tarafından korunan iletişimler hariç, tüm SSL/TLS korumalı iletişimleri taramak için bu seçeneği belirleyin. Bilinmeyen, imzalı bir sertifika kullanan yeni bir iletişim kurulduğunda, bilgilendirilmezsiniz ve iletişim otomatik olarak filtrelenir. Güvenilir olmayan sertifika sahibi olduğu halde güvenilir olarak işaretlenmiş (güvenilir sertifikalar listesindedir) bir sunucuya erişim sağladığınızda, sunucuyla iletişime izin verilir ve iletişim kanalı içeriği filtrelenir.
- **Etkileşimli mod** - Yeni bir (bilinmeyen sertifikaya sahip) SSL/TLS korumalı siteye girerseniz, eylem seçimi iletişim kutusu görüntülenir. Bu mod, tarama dışında tutulacak SSL/TLS sertifikaları listesi oluşturmanıza olanak sağlar.
- **İlke modu** - Yapılandırılmış tarama dışı bırakma işlemleri haricinde tüm SSL/TLS bağlantıları filtrelenir.

SSL/TLS filtrelenmiş uygulamaların listesi

Filtreli uygulama ekleyin ve tarama eylemlerinden birini belirleyin. SSL/TLS filtreli uygulamalar listesi; belirli uygulamalar için ESET Server Security davranışını özelleştirmek ve **SSL/TLS protokolü filtreleme modunda Etkileşimli modun** seçilmesi durumunda belirlenecek eylemleri hatırlamak için kullanılabilir.

Bilinen sertifikalar listesi

Belirli SSL sertifikaları için ESET Server Security davranışını özelleştirmenizi sağlar. Liste, **Bilinen sertifikalar listesi** yanındaki Düzenle seçeneği tıklanarak görüntülenebilir ve yönetilebilir.

Güvenilir etki alanlarıyla iletişimi hariç tut

Uzatılmış doğrulama sertifikalarını kullanarak iletişimi protokol denetimi (İnternet bankacılığı) dışında bırakmak için kullanılır.

Eski SSL v2 protokolünü kullanarak şifrelenmiş iletişimi engelle

SSL protokolünün bu önceki sürümü kullanılarak gerçekleştirilen iletişim otomatik olarak engellenir.

Kök sertifika

SSL/TLS iletişiminin tarayıcınızda/e-posta istemcilerinizde düzgün bir şekilde çalışması için, ESET kök sertifikasının bilinen kök sertifikalar (yayımcılar) listesine eklenmesi önemlidir. Kök sertifikayı bilinen tarayıcılara ekle seçeneğinin etkinleştirilmesi gerekir. ESET kök sertifikasını bilinen tarayıcılara (örneğin, Opera ve Firefox) otomatik olarak eklemek için bu seçeneği belirleyin. Sistem sertifika deposunu kullanan tarayıcılar için, sertifika otomatik olarak eklenir (örneğin, Internet Explorer).

Sertifikayı desteklenmeyen tarayıcılara uygulamak için **Sertifikayı Görüntüle** > **Ayrıntılar** > **Dosyaya Kopyala**... öğelerini tıklatıp manuel olarak tarayıcıya aktarın.

Sertifika geçerliliği

TRCA sertifika deposu kullanılarak sertifika doğrulanamazsa

Bazı durumlarda bir web sitesi sertifikası **Güvenilir Kök Sertifika Yetkilileri** (TRCA) deposu kullanılarak doğrulanamayabilir. Bu, sertifikanın birisi tarafından (örneğin, bir web sunucusunun veya küçük ölçekli bir şirketin yöneticisi) imzalandığı anlamına gelir ve bu sertifikanın güvenilir olduğunu düşünmek her zaman bir risk oluşturmaz. Çoğu büyük ölçekli şirket (örneğin, bankalar) TRCA tarafından imzalanmış sertifika kullanır. **Sertifika geçerliliğini sor** seçeneği (varsayılan olarak seçilir) belirlendiyse, şifreli bir iletişim kurulduğunda kullanıcıdan gerçekleştirilecek eylemi seçmesi istenecektir. Doğrulanamayan sertifikalara sahip sitelere şifreli bağlantıları her zaman sonlandırmak için **Sertifikayı kullanan iletişimi engelle** seçeneğini belirleyebilirsiniz.

Sertifika geçersiz veya bozuksa

Bu, sertifika süresinin dolduğu veya hatalı bir şekilde imzalandığı anlamına gelir. Bu durumda **Sertifikayı kullanan iletişimi engelle** öğesini seçili bırakmanızı öneririz.

Bilinen sertifikalar listesi

Belirli Güvenli Yuva Katmanı (SSL)/Aktarım Katmanı Güvenliği (TLS) sertifikaları için ESET Server Security davranışını özelleştirme ve SSL/TLS protokol filtreleme modunda **Etkileşimli mod** seçeneği belirlenmişse tercih edilen eylemlerin hatırlanması amacıyla kullanılır. Seçili sertifikayı düzenleyebilir veya URL'den ya da Dosyadan sertifika **Ekleyebilirsiniz**. Sertifika ekle penceresindeyken, URL veya Dosya düğmesini tıklayın ve sertifika URL'sini belirtin veya sertifika dosyasını bulun. Aşağıdaki alanlar sertifikadaki veriler kullanılarak otomatik olarak doldurulur:

- **Sertifika adı** - sertifikanın adı.
- **Sertifika sağlayıcı** - sertifikayı oluşturanın adı.
- **Sertifikanın konusu** - Konu alanı, konu genel anahtarı alanına kaydedilen genel anahtarla ilişkili bir bölümü tanımlar.

Erişim eylemi

- **Otomatik** - Güvenilir sertifikalara izin vermek ve güvenilmeyenleri sormak için kullanılır.
- **İzin ver veya Engelle** - Güvenilirliğine bakılmaksızın, bu sertifika tarafından güvence altına alınan iletişimlere izin vermek/bunları engellemek için kullanılır.

- **Sor** - Belirli bir sertifikayla karşılaşıldığında istem almak için kullanılır.

Tarama eylemi

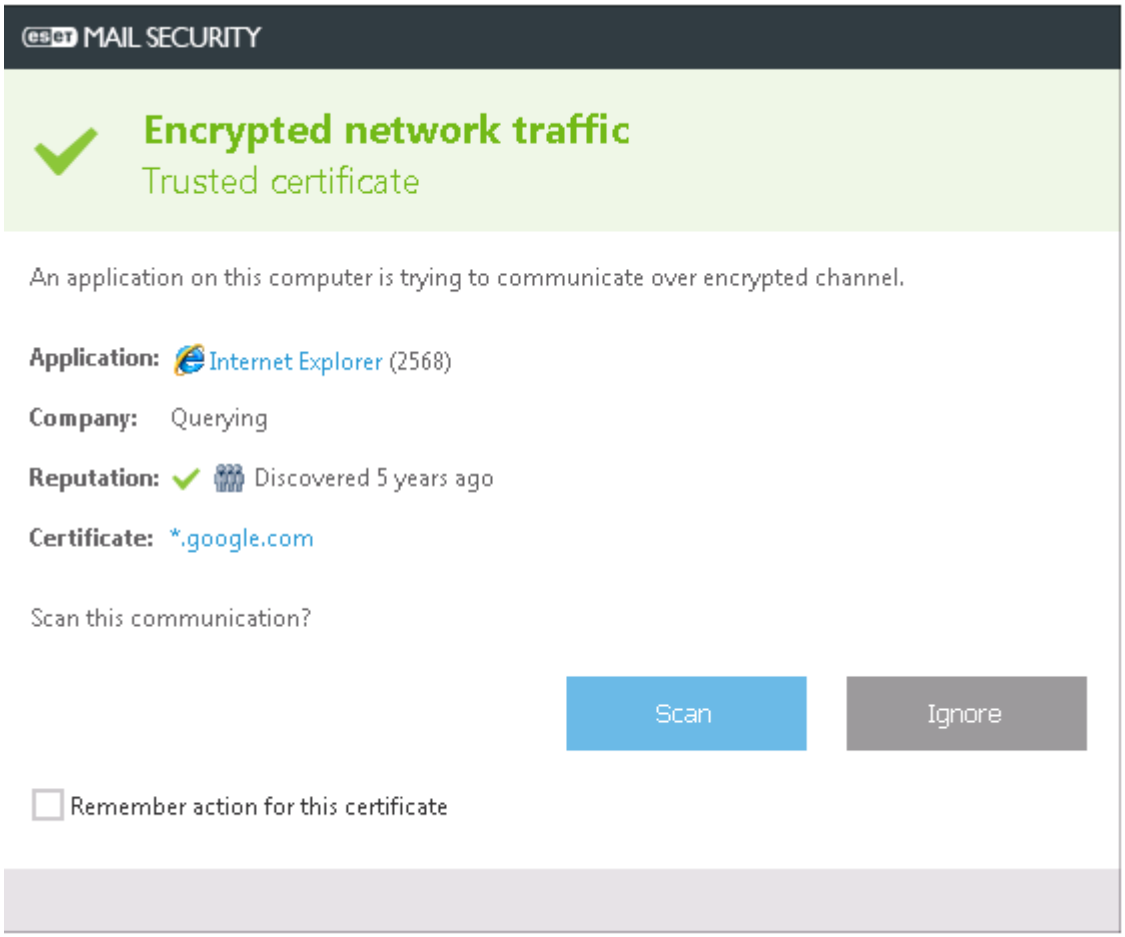
- **Otomatik** - Otomatik modda taramak ve etkileşimli modda sormak için kullanılır.
- **Tara veya Yoksay** - Bu sertifika tarafından güvence altına alınan iletişimi taramak veya yoksaymak için kullanılır.
- **Sor** - Belirli bir sertifikayla karşılaşıldığında istem almak için kullanılır.

Şifrelenmiş SSL iletişimi

Sisteminiz SSL protokol taraması kullanmak üzere yapılandırıldıysa aşağıdaki iki durumda sizden bir eylem seçmenizi isteyen iletişim penceresi görüntülenir:

İlk olarak, bir web sitesi doğrulanamayan veya geçersiz bir sertifika kullanıyorsa ve ESET Server Security bu gibi durumlarda kullanıcıya bunu sormak üzere yapılandırıldıysa (varsayılan olarak doğrulanamaz sertifika için evet, geçersiz olanlar için hayır), iletişim kutusunda bağlantı için **İzin ver** veya **Engelle** seçeneklerinden birini belirlemeniz istenir.

İkincisi, **SSL protokolü filtreleme modu**, **Etkileşimli mod** olarak ayarlandıysa iletişim kutusunda her web sitesi için trafiği **Tara** veya **Yoksay** seçeneklerinden birini belirlemeniz istenir. Bazı uygulamalar kendi SSL trafiğinin değiştirilmediğini ya da herhangi biri tarafından denetlenmediğini doğrular; bu durumlarda uygulamanın çalışmaya devam etmesi için, ESET Server Security ürününün bu trafiği **Yoksayması** gerekir.



Her iki durumda da kullanıcı seçilen eylemin hatırlanmasını seçebilir. Kaydedilen eylemler Bilinen sertifikalar listesi içinde depolanır.

E-posta istemci koruması

ESET Server Security uygulamasının e-posta istemcileriyle tümleştirilmesi, e-posta iletilerindeki kötü amaçlı kodlara karşı gerçekleştirilen etkin koruma düzeyini artırır. E-posta istemciniz destekleniyorsa tümleştirme ESET Server Security içinden etkinleştirilebilir. Tümleştirme etkinleştirildiğinde daha etkili e-posta koruması sağlamak için ESET Server Security araç çubuğu, doğrudan e-posta istemcisine eklenir (Windows Live Mail'in yeni sürümleri için araç çubuğu eklenmez).

E-posta istemcisiyle entegrasyon

Şu anda desteklenen e-posta istemcilerine Microsoft Outlook, Outlook Express, Windows Mail ve Windows Live Mail dahildir. E-posta koruması bu programların bir eklentisi olarak çalışır. Eklentinin en temel getirisi, kullanılan protokolden bağımsız olmasıdır. E-posta istemcisi şifreli bir ileti aldığında, bu iletinin şifresi çözülür ve ileti virüs tarayıcıya gönderilir. Tümleştirme etkin olmasa bile, e-posta iletişimleri e-posta istemci koruması modülü (POP3, IMAP) ile korunmaya devam eder. Desteklenen e-posta istemcilerinin ve bunların sürümlerinin tam listesi için şu Bilgi Bankası makalesine bakın.

Gelen kutusu içeriği değişirken denetimi devre dışı bırak

E-posta istemcinizle çalışırken (yalnızca MS Outlook) sistem yavaşlaması sorunu yaşamanız durumunda kullanılır. Bu durum Kerio Outlook Connector Store'dan e-posta alınırken ortaya çıkabilir.

İstemci eklentileri ile e-posta korumasını etkinleştir

E-posta istemcinizdeki tümleştirmeyi kaldırmadan e-posta istemci korumasını devre dışı bırakmanızı sağlar. Tüm eklentileri aynı anda veya aşağıdakilerden istediğinizi seçerek devre dışı bırakabilirsiniz:

- **Alınan e-posta** - Alınan iletilerin denetlenmesi özelliğini açar veya kapatır.
- **Gönderilen e-posta** - Gönderilen iletilerin denetlenmesi özelliğini açar veya kapatır.
- **Okunan e-posta** - Okunan iletilerin denetlenmesi özelliğini açar veya kapatır.

Etkilenen e-postada gerçekleştirilecek eylem

- **Eylem yok** - Etkinleştirilirse, program etkilenen ekleri belirler, ancak e-postaları hiçbir işlem yapmadan olduğu gibi bırakır.
- **E-postayı sil** - Program kullanıcıyı sızıntılarla ilgili olarak uyarır ve iletiyi siler.
- **E-postayı Silinmiş öğeler klasörüne taşı** - Etkilenen e-postalar Silinmiş öğeler klasörüne otomatik olarak taşınır.
- **E-postayı klasöre taşı** - Etkilenen e-postalar belirtilen klasöre otomatik olarak taşınır.
- **Klasör** - Etkilenen e-postalar algılandığında bunları taşımak isteyeceğiniz özel bir klasör belirtin.

Güncellemeden sonra taramayı tekrar et

Algılama Altyapısı güncellemesinden sonra yeniden taramayı etkinleştirir/devre dışı bırakır.

Diğer modüllerin tarama sonuçlarını kabul et

Bu seçilirse, e-posta koruması modülü, diğer koruma modüllerinden (POP3, IMAP protokollerinin taramaları) tarama sonuçlarını kabul eder.

E-posta protokolleri

Protokol filtresiyle e-posta korumasını etkinleştir

IMAP ve POP3 protokolleri, bir e-posta istemci uygulamasında e-posta iletişimlerini almak için en yaygın şekilde kullanılan protokollerdir. ESET Server Security kullanılan e-posta istemcisinden bağımsız olarak bu protokoller için koruma sağlar.

ESET Server Security, IMAPS ve POP3S protokolleri taramasını da destekler; bu durumda sunucu ve istemci arasında bilgilerin aktarılması için şifreli kanal kullanılır. ESET Server Security, iletişimi SSL (Güvenli Yuva Katmanı) ve TLS (Aktarım Katmanı Güvenliği) protokollerini kullanarak denetler. Program işletim sistemi sürümü fark etmeksizin, yalnızca **IMAPS/POP3S** protokolü tarafından kullanılan Bağlantı noktaları içinde tanımlı bağlantı noktalarında trafiği tarar.

IMAPS/POP3S tarayıcı ayarları

Şifreli iletişimler, varsayılan ayarlar kullanımdayken taranmaz. Şifreli iletişimlerin taranmasını etkinleştirmek için SSL/TLS protokol denetimine gidin.

Bağlantı noktası numarası ne tür bir bağlantı noktası olduğunu belirtir. Şunlar için varsayılan e-posta bağlantı noktaları:

Bağlantı noktası adı	Bağlantı noktası numaraları	Açıklama
POP3	110	Varsayılan POP3 şifresiz bağlantı noktası.
IMAP	143	Varsayılan IMAP şifresiz bağlantı noktası.
Güvenli IMAP (IMAP4-SSL)	585	SSL/TLS protokol filtrelemesini etkinleştir Birden fazla bağlantı noktası numaraları virgülle ayrılmalıdır.
SSL üzerinden IMAP4 (IMAPS)	993	SSL/TLS protokol filtrelemesini etkinleştir Birden fazla bağlantı noktası numaraları virgülle ayrılmalıdır.
Güvenli POP3 (SSL-POP)	995	SSL/TLS protokol filtrelemesini etkinleştir Birden fazla bağlantı noktası numaraları virgülle ayrılmalıdır.

Uyarılar ve bildirimler

E-posta koruması, POP3 ve IMAP protokolleri ile alınan e-posta iletişimlerinin denetimini sağlar. ESET Server Security, Microsoft Outlook ve diğer e-posta istemcileri için eklenti programını kullanarak e-posta istemcisinden yapılan tüm iletişimi denetler (POP3, MAPI, IMAP, HTTP). Program, gelen iletileri incelerken ThreatSense tarama altyapısında yer alan tüm gelişmiş tarama yöntemlerini kullanır. Bu, kötü amaçlı programların algılanmasının, virüs algılama veri tabanıyla eşleştirilmeden önce gerçekleştiği anlamına gelir. POP3 ve IMAP protokolü iletişimlerinin taranması, kullanılan e-posta istemcisinden bağımsızdır.

E-posta denetlendikten sonra, iletiye tarama sonucuyla birlikte bir bildirim eklenebilir. **Alınan ve okunan e-postalara alt bilgi ekle**, **Alınan ve okunan etkilenen e-postanın konusuna not ekle** veya **Gönderilen e-postaya etiket bilgileri ekle** seçeneklerinden birini belirleyebilirsiniz. Etiket iletilerinin nadir olarak, sorunlu HTML iletilerinde atlanabileceğini veya iletilerin kötü amaçlı yazılımlar tarafından taklit edilebileceğini unutmayın. Etiket iletileri, alınan ve okunan e-postaya, giden e-postaya veya her ikisine de eklenebilir. Kullanılabilen seçenekler şunlardır:

- **Hiçbir zaman** - Etiket iletileri hiçbir zaman eklenmez.
- **Yalnızca etkilenen e-postaya** - Yalnızca kötü amaçlı yazılım içeren iletiler, "denetlendi" şeklinde işaretlenir (varsayılan).
- **Taranan tüm e-postalara** - Program taranan tüm e-postalara ileti ekler.

Gönderilen etkilenen e-postanın konusuna not ekle

E-posta korumasının etkilenen e-posta konusuna virüs uyarısı dahil etmesini istemiyorsanız bunu devre dışı bırakın. Bu özellik, etkilenen e-postaya basit, konuya göre filtre uygulanmasına olanak verir (e-posta programınız tarafından destekleniyorsa). Ayrıca alıcı için güvenilirlik düzeyini arttırır ve bir sızıntı algılandığında belirli bir e-posta veya gönderen için tehdit düzeyi hakkında çok değerli bilgiler sağlar.

Etkilenen e-postanın konusuna eklenen şablon

Etkilenen bir e-postanın konu önek biçimini değiştirmek isterseniz bu şablonu düzenleyin. Bu işlev iletinin `[virus]` gibi belirli bir önek değeriyle birlikte `Hello` şeklindeki mesaj konusunu şu biçimle değiştirir: `[virus] Hello`. Değişken `%VIRUSNAME%` algılanan tehdidi temsil eder.

MS Outlook araç çubuğu

Microsoft Outlook koruması eklenti modülü olarak çalışır. ESET Server Security yüklendikten sonra, zararlı yazılım koruması seçeneklerini içeren bu araç çubuğu Microsoft Outlook'a eklenir:

ESET Server Security

Simgeyi tıklatarak ESET Server Security ana program penceresini açabilirsiniz.

İletileri yeniden tara

E-posta denetlemesini manuel olarak başlatmanıza olanak sağlar. Denetlenecek iletileri belirtebilir ve alınan postanın yeniden taranmasını etkinleştirebilirsiniz. Daha fazla bilgi için, bkz. E-posta istemci koruması.

Tarayıcı ayarları

E-posta istemci koruması ayar seçeneklerini görüntüler.

Outlook Express ve Windows Mail araç çubuğu

Outlook Express ve Windows Mail koruması bir eklenti modülü olarak çalışır. ESET Server Security yüklendikten sonra, zararlı yazılım koruması seçeneklerini içeren bu araç çubuğu Outlook Express veya Windows Mail uygulamasına eklenir:

ESET Server Security

Simgeyi tıklatarak ESET Server Security ana program penceresini açabilirsiniz.

İletileri yeniden tara

E-posta denetlemesini manuel olarak başlatmanıza olanak sağlar. Denetlenecek iletileri belirtebilir ve alınan postanın yeniden taranmasını etkinleştirebilirsiniz. Daha fazla bilgi için, bkz. E-posta istemci koruması.

Tarayıcı ayarları

E-posta istemci koruması ayar seçeneklerini görüntüler.

Görünümü özelleştir

E-posta istemciniz için araç çubuğunun görünümü değiştirilebilir. E-posta program parametrelerinden bağımsız olarak görünümü özelleştirmek için bu seçeneğin seçimini kaldırın.

- **Metni göster** - Simgelerin açıklamalarını görüntüler.
- **Sağa metin** - Seçenek açıklamaları, simgelerin alt kısmından sağ tarafına taşınır.
- **Büyük simgeler** - Menü seçenekleri için büyük simgeler görüntüler.

Onay iletişim penceresi

Bu uyarı, kullanıcının seçilen eylemi gerçekten yapmak isteyip istemediğini doğrulamasını sağlayarak olası hataları ortadan kaldıracaktır. İletişim kutusu aynı zamanda onayları devre dışı bırakma seçeneği de sunar.

İletileri yeniden tara

E-posta istemcileriyle tümleşik olan ESET Server Security araç çubuğu, kullanıcıların e-posta denetimi için birçok seçenek belirtmesini sağlar. **İletileri yeniden tara** seçeneği, iki tarama modu sunar:

- **Geçerli klasördeki tüm iletiler** - Halihazırda görüntülenen klasördeki iletileri tarar.
- **Yalnızca seçili iletiler** - Yalnızca kullanıcı tarafından işaretlenen iletileri tarar.
- **Önceden taranmış iletileri yeniden tara** - Kullanıcıya önceden taranmış iletiler üzerinde bir tarama daha çalıştırma seçeneğini sunar.

Web erişimi koruması

Web erişimi koruması, sizi çevrimiçi tehditlere karşı korumak için web tarayıcıları ile uzak sunucular arasındaki iletişimi izleyerek çalışır ve HTTP (Köprü Metni Aktarım Protokolü) ile HTTPS (şifreli iletişim) kurallarına uyar.

Kötü amaçlı içeriğe sahip olduğu bilinen web sayfalarına erişim, içerik indirilmeden önce engellenir. Tüm diğer web sayfaları; yüklendiklerinde ve kötü amaçlı içerik algılanması durumunda engellendiklerinde ThreatSense tarama altyapısı ile taranır. Web erişimi koruması iki koruma düzeyi sunar: kara listeye göre engelleme ve içeriğe göre engelleme.

Temel

Web erişimi korumasını etkin durumda bırakmanızı kesinlikle öneririz. Bu seçeneğe ESET Server Security ana program penceresinde, **Ayarlar** > **Web ve e-posta** > **Web erişimi koruması**'na giderek de erişebilirsiniz.

Tarayıcı komut dosyalarının gelişmiş taramasını etkinleştirin

Varsayılan olarak, web tarayıcıları tarafından yürütülen tüm JavaScript programları algılama altyapısı tarafından kontrol edilecektir.

Web protokolleri

Birçok İnternet tarayıcısı tarafından kullanılan bu standart protokoller için izlemeyi yapılandırmanızı sağlar. Varsayılan olarak ESET Server Security, birçok İnternet tarayıcısı tarafından kullanılan HTTP protokolünü izleyecek şekilde yapılandırılmıştır.

ESET Server Security HTTPS protokol denetimini de destekler. HTTPS iletişimi, sunucu ile istemci arasında bilgi aktarmak için şifreli bir kanal kullanır. ESET Server Security, Güvenli Yuva Katmanı (SSL) ve Aktarım Katmanı Güvenliği (TLS) protokollerini kullanarak iletişimleri denetler. Program işletim sistemi sürümü fark etmeksizin, yalnızca **HTTPS protokolü tarafından kullanılan bağlantı noktaları** içinde tanımlı bağlantı noktalarında trafiği tarar.

Varsayılan ayarlar kullanılıyorsa şifreli iletişim taranmaz. Şifreli iletişimin taramasını etkinleştirmek için **Gelişmiş ayarlar** (**F5**) > **Web ve e-posta** > SSL/TLS seçeneklerini kullanın.

ThreatSense parametreleri

Tarama (e-posta, arşiv, tarama dışı bırakma, sınırlar vs.) ve Web erişimi koruması için algılama yöntemleri gibi ayarları yapılandırın.

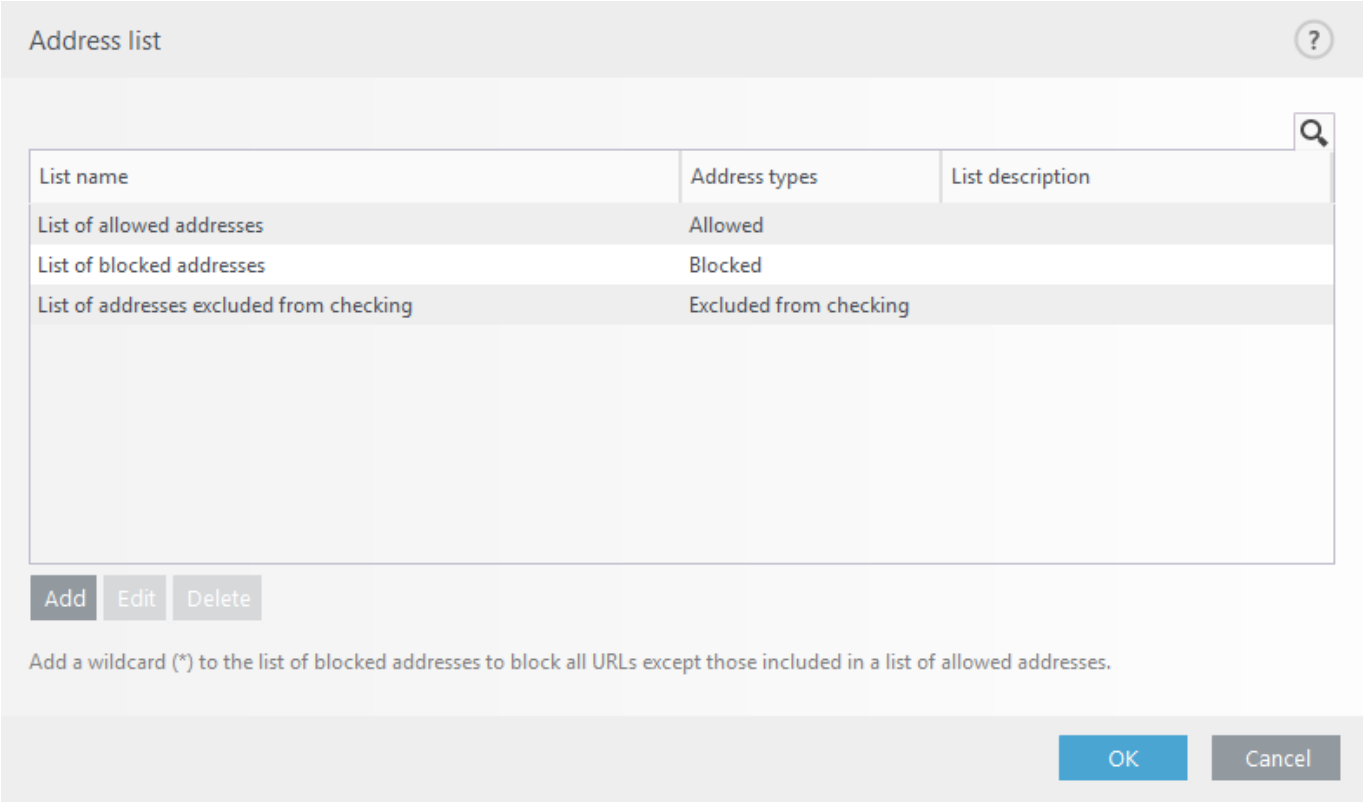
URL adresi yönetimi

URL adres yönetimi; denetim için engellenecek, izin verilecek veya dışarıda bırakılacak HTTP adreslerini belirtmenize olanak tanır. Engellenen adresler listesindeki web sitelerine, İzin verilen adresler listesine dahil edilmedikleri sürece erişilemez. Denetim dışında bırakılan adresler listesindeki web sitelerine erişildiğinde bunlara kötü amaçlı kod taraması yapılmaz. HTTP web sayfalarına ek olarak, HTTPS adreslerini filtrelemek isterseniz SSL/TLS protokol filtrelemesi etkinleştirilmelidir. Aksi takdirde, yalnızca ziyaret ettiğiniz HTTPS sitelerinin etki alanları eklenir, tam URL eklenmez.

Engellenen adresler listelerinden biri bazı harici ortak kara listelerdeki adresler içerirken, ikincisi kendi kara listenizi içerebilir. Bu sayede kendi kara listenizi bozulmadan tutarken harici listeyi kolayca güncelleyebilirsiniz.

Önceden tanımlı olanlara ek olarak yeni bir adres listesi oluşturmak için **Düzenle** ve **Ekle** seçeneğini tıklayın. Adresleri mantıksal olarak farklı gruplara ayırmak isterseniz bu yararlıdır. Varsayılan olarak aşağıdaki üç liste kullanılabilir:

- **Denetim dışında bırakılan adreslerin listesi** - Bu listeye eklenen adresler için kötü amaçlı kod denetlemesi gerçekleştirilmez.
- **İzin verilen adresler listesi** - Yalnızca izin verilen adresler listesindeki HTTP adreslerine erişim izni ver seçeneği etkinleştirilirse ve engellenen adresler listesinde * simgesi (her şeyle eşleş) yer alıyorsa, kullanıcının yalnızca bu listede belirtilen adreslere erişmesine izin verilir. Engellenen adresler listesinde yer alsalar bile bu listedeki adreslere izin verilir.
- **Engellenen adresler listesi** - Ayrıca izin verilen adresler listesinde yer almadıkça kullanıcının bu listede belirtilen adreslere erişmesine izin verilmez.



Listeye yeni bir URL adresi **ekleyebilirsiniz**. Ayırıcı ile birden çok değer de girebilirsiniz. Listede mevcut olan bir adresi değiştirmek için **Düzenle**'yi, silmek için ise **Sil**'i tıklayın. Silme işlemi yalnızca **Ekle** seçeneği kullanılarak oluşturulan adresler için kullanılabilir, içe aktarılan adresler için kullanılamaz.

Tüm listelerde, * (yıldız işareti) ve ? (soru işareti) özel simgeleri kullanılabilir. Yıldız işareti herhangi bir sayıyı veya karakteri; soru işareti herhangi bir karakteri temsil eder. Dışarıda bırakılan adresler listesinin yalnızca güvenilen ve güvenli adresleri içermesi gerektiğinden, buradaki adresleri belirlerken çok dikkatli olmak gerekir. Aynı şekilde * ve ? simgelerinin de bu listede doğru kullanıldığından emin olunmalıdır.

> NOT
> Etkin İzin verilen adresler listesi'ndeki adresler hariç tüm HTTP adreslerini engellemek isterseniz etkin Engellenen adresler listesi'ne * simgesini ekleyin.

Yeni liste oluştur

Bu liste, engellenecek, izin verilecek veya denetleme dışında bırakılacak olan istenen URL adreslerini/etki alanı maskelerini içerir. Yeni bir liste oluştururken şunları belirtin:

- **Adres listesi türü** - Açılır menüden türü (Denetleme dışında tutulan, Engellenen veya İzin verilen) seçin.
- **Liste adı** - Listenin adını belirtin. Önceden tanımlı üç listeden biri düzenlenirken bu alan gri olur.
- **Liste açıklaması** - Liste için kısa bir açıklama yazın (isteğe bağlı). Önceden tanımlı üç listeden biri düzenlenirken bu alan gri olur.
- **Liste aktif** - Listeyi devre dışı bırakmak için anahtarı kullanın. Gerektiğinde daha sonra etkinleştirebilirsiniz.
- **Uygularken bildir** - Belirli bir liste ziyaret ettiğiniz HTTP/HTTPS sitesinin değerlendirilmesinde

kullanıldığında size bildirilmesini istiyorsanız kullanılır. Bir web sitesi engellenen veya izin verilen adresler listesine dahil edildiği için engellenir veya buna izin verilirse bildirimde bulunulur. Bildirim, belirtilen web sitesini içeren listenin adını içerir.

- **Günlüğe kaydetme düzeyi** - Açılır listeden günlüğe kaydetme düzeyini (Yok, Tanılama, Bilgi veya Uyarı) seçin. **Uyarı** ayrıntı düzeyine sahip kayıtlar ESET PROTECT tarafından toplanabilir.

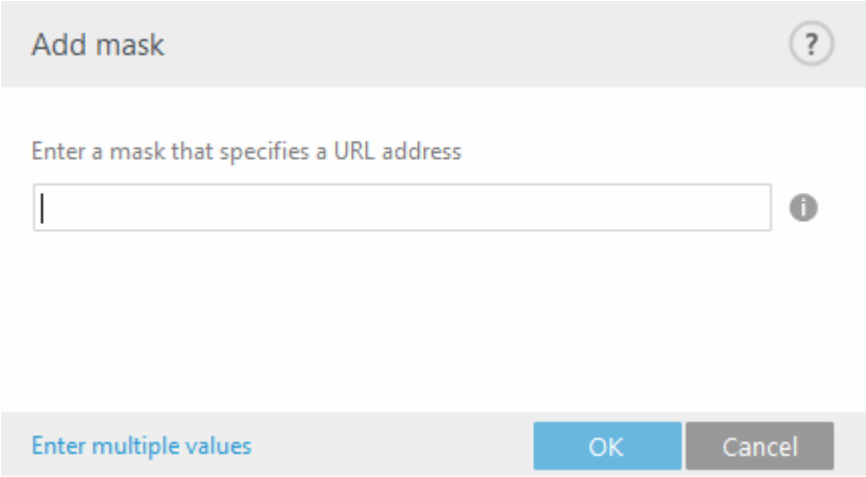
ESET Server Security, kullanıcıların belirtilen web sitelerine erişimi engellemesini ve İnternet tarayıcısının bu sitelerin içeriğini görüntülemesini önlemesini sağlar. Ek olarak, kullanıcının denetim dışında bırakılması gereken adresleri belirtmesine de olanak verir. Uzak sunucunun tam adı bilinmiyorsa veya kullanıcı tam bir uzak sunucular grubu belirtmek istiyorsa, böyle bir grubu tanımlamak için maskeler kullanılabilir.

Maskelerde ? ve * sembolleri bulunur:

- simgenin yerine ? kullanın
- metin dizesinin yerine ** kullanın

ÖRNEK
**.c?m*, son bölümü c harfi ile başlayan, sonu m harfi ile biten ve bunların arasında bilinmeyen bir simge bulunan bütün adresler için geçerlidir (*.com*, *.cam* gibi).

Etki alanı adının başında kullanılırsa başa gelen *. dizisi özel olarak ele alınır. Öncelikle, * joker karakteri bu durumda eğik çizgi karakteriyle ('/') eşleşmez. Bunun amacı maskeyi aşmaktan kaçınmaktır. Örneğin, **.domain.com* maskesi *https://anydomain.com/anypath#.domain.com* ile eşleşmez (bu tür bir sonek, indirme işlemini etkilemeden herhangi bir URL'ye eklenebilir). İkinci olarak *. aynı zamanda bu özel durumda boş bir dize ile eşleşir. Bunun amacı, tüm alt etki alanlarını içeren etki alanının tümünü tek bir maske kullanarak eşleştirmektir. Örneğin **.domain.com* maskesi *https://domain.com* ile de eşleşir. *https://anotherdomain.com* ile de eşleşeceğinden, **domain.com* kullanmak yanlış olur.

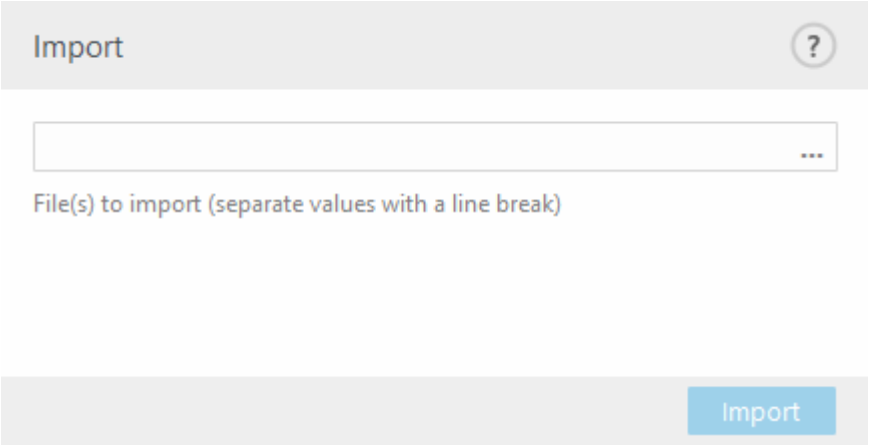


Birden fazla değer gir

Yeni çizgiler, virgüller veya noktalı virgüller ile ayrılmış birden fazla URL adresi ekleyebilirsiniz. Birden fazla seçim etkinleştirildiğinde adresler listede görünür.

İçe aktar

İçe aktarılacak URL adresleri içeren metin dosyası (değerleri satır sonuyla ayırın, örneğin UTF-8 kodlaması kullanan `*.txt`).

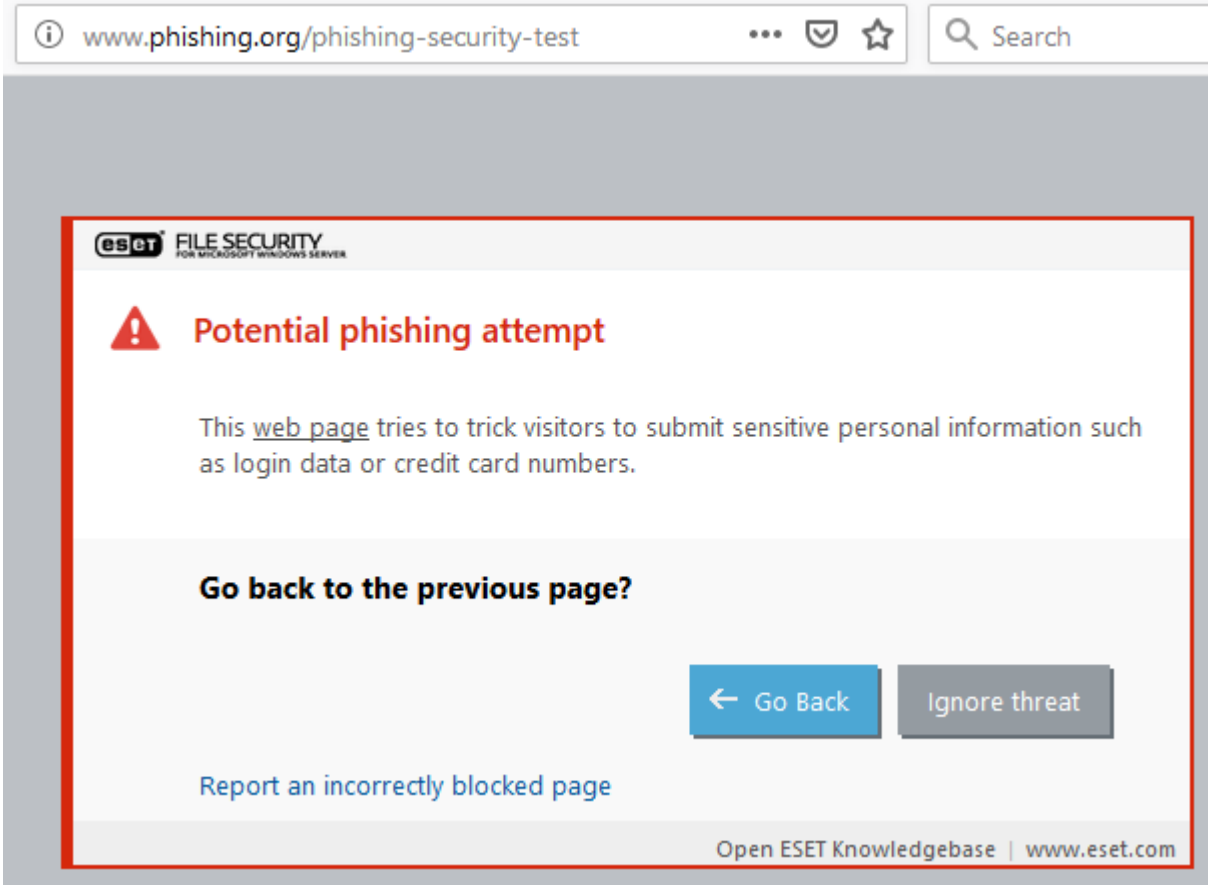


Kimlik avı web koruması

Kimlik avı terimi sosyal mühendisliği (kullanıcıların gizli bilgilerini elde etmek için kandırılması) kullanılan bir suç eylemine karşılık gelir. Kimlik avının amacı genellikle banka hesabı numaraları, PIN numaraları ve diğer bilgiler gibi hassas verilere erişmektir.

ESET Server Security kimlik avı korumasını içerir. Bu koruma, bu tür içerik dağıttığı bilinen web sayfalarını engeller. ESET Server Security uygulamasında Kimlik Avı Korumasını etkinleştirmenizi kesinlikle öneririz. ESET Server Security ürününde Kimlik Avı koruması hakkında daha fazla bilgi edinmek için Bilgi bankası makalemize bakın.

Tespit edilen bir kimlik avı web sitesine eriştiğinizde web tarayıcınızda şu iletişim kutusu görüntülenir. Web sitesine yine de erişmek istiyorsanız **Tehdidi yoksay** seçeneğini tıklayın (önerilmez).



NOT
Beyaz listeye eklenen potansiyel kimlik avı web sitelerinin süreleri varsayılan olarak birkaç saatten sonra dolar. Bir web sitesine kalıcı olarak izin vermek için URL adresi yönetimi aracını kullanabilirsiniz.

Kimlik avı sitesi bildir

Kimlik avı yaptığını veya başka kötü amaçlı yazılım içerdiğiniz düşündüğünüz şüpheli bir web sitesiyle karşılaşırsanız bu durumu analiz etmesi için ESET'e bildirebilirsiniz. Bir web sitesini ESET'e göndermeden önce aşağıdaki ölçütlerden birine veya birden fazlasına uyduğundan emin olun:

- web sitesi hiç algılanmamış,
- web sitesi tehdit olarak yanlışlıkla algılanmış. Bu durumda Kimlik avını hatalı pozitif olarak bildirebilirsiniz.

Alternatif olarak, web sitesini e-posta ile de gönderebilirsiniz. E-postanızı samples@eset.com adresine gönderin. Açıklayıcı bir konu kullanmayı ve web sitesiyle ilgili mümkün olduğunca fazla bilgi (örneğin, hangi web sitesinden bu web sitesine geldiğiniz, web sitesini nasıl duyduğunuz vs.) eklemeyi unutmayın.

Cihaz Kontrolü

ESET Server Security, otomatik aygıt (CD/DVD/USB/) denetimi sağlar. Bu modül genişletilmiş filtreleri/izinleri taramanıza, engellemenize veya ayarlamanıza ve bir kullanıcının belirli bir aygıta erişip erişemeyeceğini ve bu aygıtla çalışıp çalışamayacağını tanımlamanıza olanak tanır. Bilgisayar yöneticisi, istenmeyen içerik bulunduran aygıtların kullanımını engellemek istiyorsa bu özellik faydalı olabilir.

NOT
Aygıt denetimini, **Sisteme tümleştir** düğmesini kullanarak etkinleştirdiğinizde ESET Server Security Aygıt denetimi özelliği etkinleşir. Ancak bu değişikliğin geçerli olması için sisteminizin yeniden başlatılması gerekir.

Aygıt denetimi etkin hale gelerek ayarları düzenlemenize olanak tanır. Mevcut bir kural tarafından engellenen bir aygıt algılanırsa, bildirim penceresi görüntülenir ve aygıta erişim verilmez.

Kurallar

Aygıt denetimi kuralı, kural ölçütlerini karşılayan bir aygıt bilgisayara bağlandığında gerçekleştirilecek olan eylemi tanımlar.

Gruplar

Düzenle seçeneğini tıkladığınızda, Aygıt gruplarını yönetebilirsiniz. Yeni bir Aygıt grubu oluşturun ya da listeye aygıt eklemek veya listeden aygıt kaldırmak için mevcut bir aygıtı seçin.

NOT
Günlük dosyaları'nda aygıt denetimi günlük girişlerini görüntüleyebilirsiniz.

Aygıt kuralları

Bazı aygıtlara kural yapılandırmasında belirlenebilen kullanıcı, kullanıcı grubu veya bazı ek parametrelerden herhangi biri tarafından izin verilebilir veya bu aygıtlar engellenebilir. Kural listesi, bir kuralın çeşitli açıklamalarını

içerir, ör. adı, harici aygıt türü, bir aygıtın algılandığında gerçekleştirilecek eylem ve günlük kaydı önem derecesi.

Mevcut bir aygıt için yeni kural **Ekleyebilir** veya ayarlarını değiştirebilirsiniz. Daha iyi tanımlama için **Ad** alanına kuralın bir açıklamasını girin. Bu kuralı devre dışı bırakmak veya etkinleştirmek için **Kural etkin** seçeneğinin yanındaki düğmeyi tıklayın. Bu, kuralı kalıcı olarak silmek istemediğinizde kullanılabilir.

Şu sırada uygula

Saat yuvalarını kullanarak kuralları sınırlayabilirsiniz. Saat yuvasını oluşturduktan sonra kural açılır menüde görünür.

Aygıt türü

Aşağı açılır menüden harici aygıt türünü seçin (Disk depolama/Taşınabilir aygıt/Bluetooth/FireWire/...). Aygıt türleri, işletim sisteminden devralınır ve aygıtın bilgisayara bağlı olması şartıyla sistem Aygıt yöneticisinde görülebilir. Depolama aygıtları USB veya FireWire ile bağlanan harici diskleri veya geleneksel bellek kartı okuyucularını içerir. Akıllı kart okuyucuları SIM kartlar veya kimlik doğrulama kartları gibi entegre edilmiş tümleşik devreye sahip tüm akıllı kart okuyucularını içerir. Görüntüleme aygıtları örnekleri tarayıcılar veya kameralardır. Bu aygıtlar kullanıcılar hakkında değil, yalnızca kullanıcıların işlemleri hakkında bilgi verir. Bu, görüntüleme aygıtlarının yalnızca genel olarak engellenebileceği anlamına gelir.

Eylem

Depolama özelliği olmayan aygıtlara erişime izin verilebilir veya erişim engellenebilir. Buna karşılık, depolama aygıtlarına yönelik kurallar, aşağıdaki haklara ilişkin ayarlardan birini seçebilmenize olanak tanır:

- **Okuma/Yazma** - Aygıta tam erişime izin verilir.
- **Engelle** - Aygıta erişim engellenir.
- **Salt Okunur** - Aygıt için yalnızca okuma erişimine izin verilir.
- **Uyar** - Bir aygıtın her bağlanışında kullanıcı, izin verildiği/engellendiği konusunda bilgilendirilir ve bir günlük girişi yapılır. Aygıtlar hatırlanmaz, aynı aygıtın sonraki bağlanışlarında yine bir bildirim gösterilir.

NOT
Tüm hakların (eylemlerin) tüm aygıt türleri için kullanılabilir olduğunu unutmayın. Bir aygıt, depolama alanına sahipse eylemlerin dördü de kullanılabilir hale getirilir. Depolama özelliği olmayan aygıtlar için yalnızca iki eylem bulunur (örneğin, **Salt Okunur** eylemi Bluetooth için kullanılamaz; bu nedenle, yalnızca Bluetooth aygıtları için erişime izin verilebilir veya erişim engellenebilir).

Aşağıdaki ek parametreler, kurallarla ilgili hassas ayarlama yapmak ve bunları aygıtlara uyarlamak için kullanılabilir. Tüm parametreler küçük-büyük harf duyarsızdır:

- **Satıcı** - Satıcı adı veya kimliğine göre filtreler.
- **Model** - Aygıtın adı.
- **Seri numarası** - Harici aygıtların genellikle kendi seri numaraları vardır. CD/DVD'lerde bu, CD sürücünün değil, belirli bir medyanın seri numarasıdır.

NOT
Bu üç tanımlayıcı boşsa kural, eşleştirme sırasında bu alanları yoksayar. Tüm metin alanlarındaki filtreleme parametreleri büyük-küçük harfe duyarsızdır ve joker karakterler (*, ?) desteklenmez.

Bir aygıt parametrelerini anlamak üzere aygıtın türüne izin veren bir kural oluşturun, aygıtı bilgisayarınıza bağlayın ve Aygıt denetim günlüğünde aygıt detaylarını kontrol edin.

Açılır listeden **Günlüğe kaydetme düzeyini** seçin:

- **Her zaman** - Tüm olayları günlüğe kaydeder.
- **Tanılama** - Programda hassas ayarlama yapmak için gereken bilgileri günlüğe kaydeder.
- **Bilgiler** - Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarı** - Kritik hataları ve uyarı iletilerini kaydeder.
- **Yok** - Günlüğe herhangi bir şey kaydedilmez.

Kurallar, **Kullanıcı listesi** alanına eklenme yoluyla belirli kullanıcılarla veya kullanıcı gruplarıyla sınırlandırılabilir. Kullanıcı listesini yönetmek için **Düzenle**'yi tıklayın.

- **Ekle** - İstenen kullanıcıları seçmenize olanak tanıyan **Nesne türleri**: Kullanıcılar veya Gruplar iletişim penceresini açar.
- **Sil** - Filtreden seçili kullanıcıyı siler.

> NOT
> Tüm aygıtlar, kullanıcı kuralları tarafından filtrelenebilir (örneğin görüntüleme aygıtları kullanıcılar hakkında değil, yalnızca başlatılan eylemler hakkında bilgi verir).

Şu işlevler mevcuttur:

Düzenle

Seçilen grubun adını veya bu kuralda yer alan aygıtların parametrelerini (satıcı, model, seri numarası) değiştirmenize olanak sağlar.

Kopyala

Seçili kuralın parametrelerine göre yeni kural oluşturur.

Sil

Seçili kuralı silmek istediğinizde bu düğmeyi kullanabilirsiniz. Alternatif olarak, belirli bir kuralı devre dışı bırakmak için yanındaki onay kutusunu kullanabilirsiniz. Bu, gelecekte kullanmak isteyebileceğiniz bir kuralı kalıcı olarak silmek istemediğiniz zaman yararlı olabilir.

Doldur

Bağlı olan tüm aygıtlar için bir genel bakış sunar ve şunlar hakkındaki bilgileri sağlar: aygıt türü, aygıt satıcısı, modeli ve seri numarası (varsa). Bir aygıt seçtiğinizde (Algılanan aygıtlar listesinden) ve **Tamam**'ı tıkladığınızda, önceden tanımlı bilgileri içeren bir kural düzenleyici penceresi açılır (tüm ayarları yapabilirsiniz).

Kurallar yüksek önceliğe sahip olanlar en yukarıda olacak şekilde sıralanır. Birden fazla kural seçebilir ve silme ya da **Üst/Yukarı/Aşağı/Alt** ok düğmelerini tıklayarak yukarı veya aşağı taşıma gibi eylemleri uygulayabilirsiniz.

Aygıt grupları

Aygıt grupları penceresi iki bölüme ayrılır. Pencerenin sağındaki bölüm, söz konusu gruba ait aygıtların listesini verir; pencerenin sol tarafındaki bölümse mevcut grupların listesini içerir. Sağ bölmede görüntülemek istediğiniz aygıtları içeren grubu seçin.

Farklı kuralların uygulanacağı aygıtlardan oluşan farklı gruplar oluşturabilirsiniz. **Okuma/Yazma** veya **Salt okuma** olarak ayarlanan tek bir aygıt grubu da oluşturabilirsiniz. Bu, tanınmayan aygıtlar bilgisayarınıza bağlandığında Aygıt denetimi tarafından engellenmelerini sağlar.

> UYARI
> Bilgisayarınıza bağlanan harici bir aygıt, bir güvenlik riski oluşturabilir.

Şu işlevler mevcuttur:

Ekle

Düğmeye pencerenin hangi bölümünde bastığınıza bağlı olarak, adını girerek yeni bir aygıt grubu oluşturabilir veya bir aygıtı mevcut bir gruba ekleyebilirsiniz (isteğe bağlı olarak; satıcı adı, model ve seri numarası gibi ayrıntıları belirtebilirsiniz).

Düzenle

Seçilen grubun adını veya bu grupta yer alan aygıtların parametrelerini (satıcı, model, seri numarası) değiştirmenize olanak sağlar.

Sil

Pencerede tıkladığınız yere bağlı olarak seçili grubu veya aygıtı siler. Alternatif olarak, belirli bir kuralı devre dışı bırakmak için yanındaki onay kutusunu kullanabilirsiniz. Bu, gelecekte kullanmak isteyebileceğiniz bir kuralı kalıcı olarak silmek istemediğiniz zaman yararlı olabilir.

İçe aktar

Bir dosyadan aygıtlara ilişkin seri numara listesini içe aktarır.

Doldur

Bağlı olan tüm aygıtlar için bir genel bakış sunar ve şunlar hakkındaki bilgileri sağlar: aygıt türü, aygıt satıcısı, modeli ve seri numarası (varsa). Bir aygıt seçtiğinizde (Algılanan aygıtlar listesinden) ve **Tamam**'ı tıkladığınızda, önceden tanımlı bilgileri içeren bir kural düzenleyici penceresi açılır (tüm ayarları yapabilirsiniz).

Özelleştirme işlemini tamamladığınızda **Tamam** seçeneğine tıklatın. Değişiklikleri kaydetmeden **Aygıt grupları** penceresinden ayrılmak isterseniz **İptal** seçeneğini tıklatın.

> NOT
> Tüm hakların (eylemlerin) tüm aygıt türleri için kullanılabilir olduğunu unutmayın. Bir aygıt, depolama alanına sahipse eylemlerin dördü de kullanılabilir hale getirilir. Depolama özelliği olmayan aygıtlar için yalnızca iki eylem bulunur (örneğin, Salt Okunur eylemi Bluetooth için kullanılamaz; bu nedenle, yalnızca Bluetooth aygıtları için erişime izin verilebilir veya erişim engellenebilir).

Araçların yapılandırılması

Şunlar için gelişmiş ayarları özelleştirebilirsiniz:

- Zaman aralığı
- ESET PROTECT tarama hedefleri

- Geçersiz kılma modu
- ESET CMD
- ESET RMM
- Lisans
- WMI Sağlayıcı
- Günlük dosyaları
- Proxy sunucu
- E-posta bildirimleri
- Sunum modu
- Tanılamalar
- Küme

Zaman aralığı

Zaman aralığı, Aygıt denetimi kuralları dahilinde kullanılır ve uygulandıkları sırada kuralları sınırlar. Bir saat yuvası oluşturun ve yeni kural oluştururken veya mevcut kuralları değiştirirken saat yuvasını seçin (**Şu sırada uygula** parametresi). Bu, yaygın olarak kullanılan saat yuvalarını (çalışma zamanı, hafta sonu vb.) tanımlamanıza ve bunları her kural için saat aralıklarını yeniden tanımlamadan kolaylıkla yeniden kullanmanıza olanak tanır. Saat yuvası, zaman tabanlı denetimi destekleyen herhangi bir ilgili kural türü için geçerli olmalıdır.

Microsoft Windows güncellemesi

Windows güncellemeleri, tehlikeli olabilecek güvenlik açıkları için önemli onarımlar sağlar ve bilgisayarınızın genel güvenlik düzeyini iyileştirir. Bu nedenle, Microsoft Windows güncellemelerini kullanılabilir olduklarında hemen yüklemeniz büyük önem taşır. ESET Server Security, belirttiğiniz düzeye göre eksik güncellemeleri size bildirir. Şu düzeyler kullanılabilir:

- **Güncelle yok** - İndirme için sistem güncellemesi sunulmaz.
- **İsteğe bağlı güncellemeler** - Düşük ve üzeri önceliğe sahip olarak işaretlenen güncellemeler, indirilmek üzere sunulur.
- **Önerilen güncellemeler** - Genel ve üzeri önceliğe sahip olarak işaretlenen güncellemeler indirilmek üzere sunulur.
- **Önemli güncellemeler** - Önemli ve üzeri önceliğe sahip olarak işaretlenen güncellemeler, indirilmek üzere sunulur.
- **Kritik güncellemeler** - Yalnızca kritik güncellemeler indirilmek üzere sunulur.

Değişiklikleri kaydetmek için **Tamam**'ı tıklatın. Güncelle sunucusuyla durum doğrulamasının ardından Sistem güncellemeleri penceresi görüntülenir. Sistem güncelleme bilgileri, değişiklikler kaydedildikten hemen sonra kullanılamayabilir.

Komut satırı tarayıcısı

eShell'e alternatif olarak, yükleme klasöründe bulunan `ecls.exe`'yi kullanarak komut satırı üzerinden ESET Server Security İsteğe bağlı tarayıcıyı çalıştırabilirsiniz.

Aşağıda parametre ve anahtarların bir listesi yer almaktadır:

Seçenekler:

/base-dir=FOLDER	KLASÖR içindeki modülleri yükle
/quar-dir=FOLDER	karantina KLASÖRÜ
/exclude=MASK	MASKE ile eşleşen dosyaları tarama dışında bırak
/subdir	alt klasörleri tara (varsayılan)
/no-subdir	alt klasörleri tarama
/max-subdir-level=LEVEL	taranacak klasörlerdeki maksimum klasör alt seviyesi
/symlink	sembolik bağlantıları izle (varsayılan)
/no-symlink	sembolik bağlantıları atla
/ads	ADS'leri tara (varsayılan)
/no-ads	ADS'leri tarama
/log-file=FILE	çıkışı DOSYA günlük dosyasına kaydet
/log-rewrite	çıkış dosyasının üzerine yaz (varsayılan - sonuna ekle)
/log-console	çıktının konsolda günlük kaydını yap (varsayılan)
/no-log-console	çıktının konsolda günlük kaydını yapma
/log-all	ayrıca temiz dosyaları da günlüğe kaydet
/no-log-all	temiz dosyaları günlüğe kaydetme (varsayılan)
/aind	aktivite göstergesini göster
/auto	Bütün yerel diskleri otomatik olarak tara ve temizle

Tarayıcı seçenekleri:

/files	dosyaları tara (varsayılan)
/no-files	dosyaları tarama
/memory	belleği tara
/boots	önyükleme kesimlerini tara
/no-boots	önyükleme kesimlerini tarama (varsayılan)
/arch	arşivleri tara (varsayılan)
/no-arch	arşivleri tarama
/max-obj-size=SIZE	yalnızca megabayt BOYUTTAN küçük dosyaları tara (varsayılan 0 = sınırsız)
/max-arch-level=LEVEL	taranacak arşivlerdeki (derin arşivler) maksimum arşiv alt seviyesi
/scan-timeout=LIMIT	arşivleri en çok SINIR saniye süreyle tara
/max-arch-size=SIZE	arşivlerde yalnızca şu BOYUTTAN (varsayılan 0 = sınırsız) küçük dosyaları tara
/max-sfx-size=SIZE	yalnızca BOYUT megabayttan küçükse, kendiliğinden açılan arşivdeki dosyaları tara (varsayılan 0 = sınırsız)
/mail	e-posta dosyalarını tara (varsayılan)
/no-mail	e-posta dosyalarını tarama
/mailbox	posta kutularını tara (varsayılan)
/no-mailbox	posta kutularını tarama

/sfx	kendiliğinden açılan arşiv dosyalarını tara (varsayılan)
/no-sfx	kendiliğinden açılan arşiv dosyalarını tarama
/rtp	çalışma zamanı paketleyicilerini tara (varsayılan)
/no-rtp	çalışma zamanı paketleyicilerini tarama
/unsafe	tehlikeli olabilecek uygulamaları tara
/no-unsafe	tehlikeli olabilecek uygulamaları tarama (varsayılan)
/unwanted	istenmeyen türden olabilecek uygulamaları tara
/no-unwanted	istenmeyen türden olabilecek uygulamaları tarama (varsayılan)
/suspicious	şüpheli uygulamaları tara (varsayılan)
/no-suspicious	şüpheli uygulamaları tarama
/pattern	imzaları kullan (varsayılan)
/no-pattern	imzaları kullanma
/heur	sezgisel taramayı etkinleştir (varsayılan)
/no-heur	sezgisel taramayı devre dışı bırak
/adv-heur	Gelişmiş sezgisel taramayı etkinleştir (varsayılan)
/no-adv-heur	Gelişmiş sezgisel taramayı devre dışı bırak
/ext-exclude=EXTENSIONS	üst üste iki noktayla ayrılmış dosya UZANTILARI tarama dışında kalsın
/clean-mode=MODE	etkilenen nesneler için temizleme MODUNU kullan Kullanılabilir seçenekler şunlardır: • none (varsayılan) – Otomatik temizleme oluşmaz. • standard – ecls.exe etkilenen dosyaları otomatik olarak temizlemeyi veya silmeyi dener. • strict – ecls.exe, kullanıcı müdahalesi olmadan, etkilenen dosyaları otomatik olarak temizlemeyi veya silmeyi dener (dosyalar silinmeden önce sizden herhangi bir komut istenmez). • rigorous – ecls.exe, dosya ne olursa olsun, temizlemeye çalışmadan dosyaları siler. • delete – ecls.exe, temizlemeye çalışmadan dosyaları siler, ancak Windows sistem dosyaları gibi hassas dosyaları silmekten kaçınır.
/quarantine	etkilenen dosyaları (temizlendiyse) Karantinaya kopyala (temizleme sırasında gerçekleştirilen eylemi tamamlar)
/no-quarantine	etkilenen dosyaları Karantinaya kopyalama

Genel seçenekler:

/help	yardımı göster ve çık
/version	sürüm bilgisini göster ve çık
/preserve-time	son erişim zaman damgasını koru

Çıkış kodları:

0	tehdit bulunmadı
1	tehditler bulundu ve temizlendi
10	bazı dosyalar taranamadı (tehdit bulunabilir)
50	tehdit bulundu

100	hata (100'den büyük çıkış kodları dosyanın taranmamış olduğu ve temiz olarak değerlendirilemeyeceği anlamına gelir)

ESET CMD

Bu, gelişmiş ecmd komutlarını etkinleştiren bir özelliktir. Komut satırını (ecmd.exe) kullanarak ayarları dışa ve içe aktarmanıza olanak sağlar. Şimdiye kadar, GUI kullanılarak ayarları yalnızca dışarı aktarmak mümkündü. ESET Server Security yapılandırması bir *.xml* dosyasına dışa aktarılabilir.

ESET CMD özelliğini etkinleştirdiğinizde, iki yetkilendirme yöntemi kullanılabilir:

- **Yok** - Yetkilendirme yoktur. Bu yöntem imzalanmamış tüm yapılandırmaların içe aktarılmasına izin vereceğinden ve bu durum potansiyel risk taşıyacağından, bu yöntemi kullanmanızı önermiyoruz.
- **Gelişmiş ayarlar parolası** - Bir yapılandırmayı *.xml* dosyasından içe aktarmak için parola gereklidir. Bu dosya imzalanmış olmalıdır (aşağıda ..*xml* yapılandırma dosyasının imzalanması bölümüne bakın). Erişim Ayarları'nda belirtilen parola, yeni yapılandırma içe aktarılmadan önce sağlanmalıdır. Erişim ayarlarınız etkin değilse, parolanız eşleşmez veya *.xml* yapılandırma dosyası imzalanmaz, bu durumda yapılandırma içe aktarılmayacaktır.

ESET CMD etkinleştirildikten sonra, ESET Server Security yapılandırmalarını içe veya dışa aktarmak için komut satırını kullanabilirsiniz. Bunu manuel olarak yapabilir veya otomasyon amacıyla bir betik oluşturabilirsiniz.

ÖNEMLİ
Gelişmiş ecmd komutlarını kullanmak için bu komutları yönetici ayrıcalıklarıyla çalıştırmanız veya **Yönetici olarak çalıştır** seçeneğini kullanarak Windows Komut İstemi'ni (cmd) açmanız gerekir. Aksi halde, **Error executing command.** iletisi alırsınız. Ayrıca yapılandırmayı dışa aktarmak için hedef klasör mevcut olmalıdır. Dışa aktarma komutu, ESET CMD ayarı kapatıldığında da çalışmaya devam eder.

ÖRNEK
Dışa aktarma ayarları komutu:
```
ecmd /getcfg c:\config\settings.xml
```

İçe aktarma ayarları komutu:
```
ecmd /setcfg c:\config\settings.xml
```

NOT
Gelişmiş ecmd komutları yalnızca yerel olarak çalıştırılabilir. ESET PROTECT kullanımıyla **Komut çalıştır** istemci görevi yürütülemez.

.xml yapılandırma dosyasını imzalama:

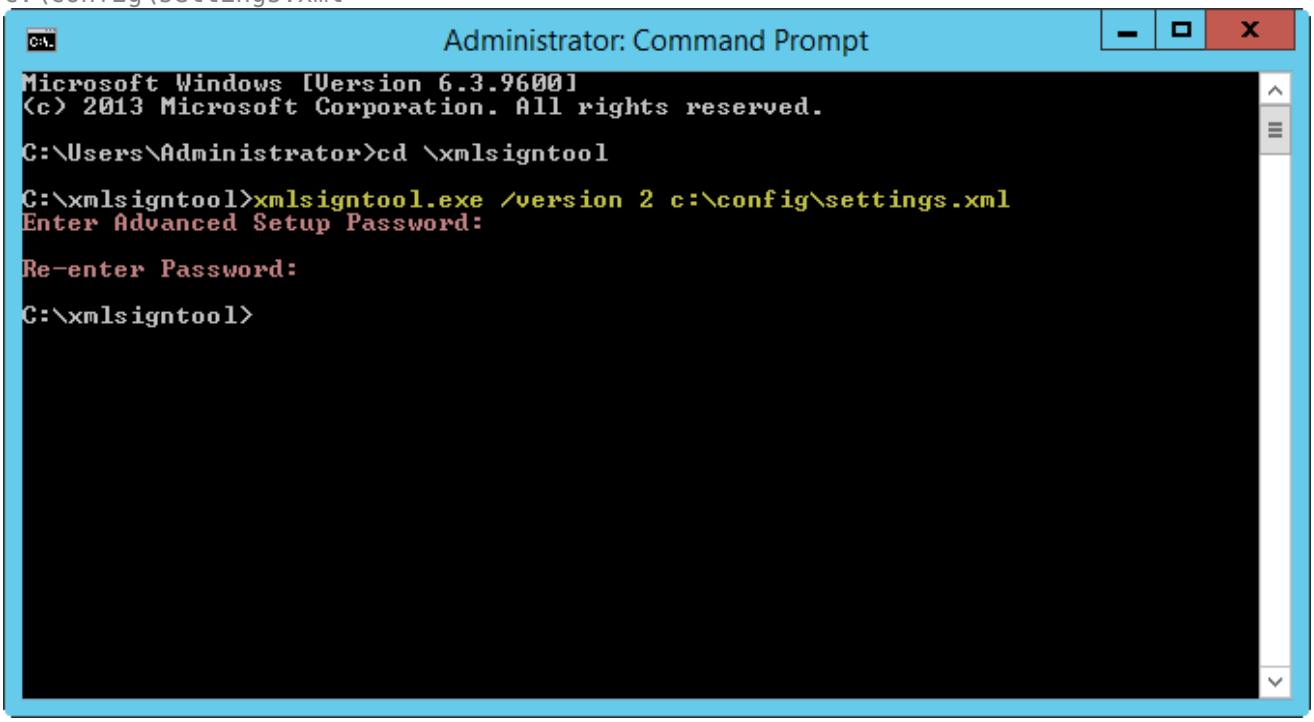
1. XmlSignTool yürütülebilir dosyasını indirin.
2. **Yönetici olarak çalıştır** seçeneğini kullanarak bir Windows Komut İstemi (cmd) açın.
3. Şu dosyayı kullanarak bir konuma gidin: `xmlsigntool.exe`

4..*xml* yapılandırma dosyasını imzalamak için bir komut yürütün. Kullanım: `xmlsigntool /version 1|2 <xml_file_path>`

ÖNEMLİ
`/version` parametre değeri, kullandığınız ESET Server Security sürümüne bağlıdır. ESET Server Security ve üstü için `/version 2` kullanın.

5.Gelişmiş Ayarlar Parolanızı XmlSignTool tarafından istendiğinde girin ve yeniden girin. .*xml* yapılandırma dosyanız şimdi imzalanmıştır ve parola yetkilendirme yöntemi kullanılarak ESET CMD ile başka bir ESET Server Security bilgisayarında içe aktarma için kullanılabilir.

ÖRNEK
Dışa aktarılan yapılandırma dosyası imzalama komutu: `xmlsigntool /version 2 c:\config\settings.xml`



NOT
Erişim Ayarı parolası değiştirilirse ve önceden eski bir parolayla imzalanmış olan bir yapılandırmayı içe aktarmak isterseniz, .*xml* yapılandırma dosyasını geçerli parolayı kullanarak yeniden imzalayabilirsiniz. Bu, içe aktarma işleminden önce ESET Server Security aracını çalıştırarak dosyayı başka bir makineye aktarmanıza gerek kalmadan, eski yapılandırma dosyasını kullanmanıza olanak sağlar.

ESET RMM

Uzaktan izleme ve yönetim (RMM), yönetim hizmeti sağlayıcısı tarafından erişilen yerel olarak yüklü bir aracı tarafından yazılım sistemlerini denetleme ve kontrol etme sürecidir (ör. masaüstü bilgisayarlardaki, sunuculardaki ve mobil aygıtlardaki).

RMM'yi etkinleştir

Uzaktan izleme ve yönetimi etkinleştir komutu işlevseldir. RMM yardımcı programını kullanmak için yönetici ayrıcalıklarına sahip olmanız gerekir.

Çalışma modu

Açılır menüden RMM çalışma modunu seçin:

- **Yalnızca güvenli ayırma -** Güvenli ve yalnızca okuma erişimi olan işlemler için RMM arabirimini etkinleştirmek istiyorsanız
- **Tüm işlemler -** Tüm işlemler için RMM arayüzünü etkinleştirmek istiyorsanız

Kimlik doğrulama yöntemi

Açılır menüden RMM kimlik doğrulama yöntemini belirleyin:

- **Yok** - Uygulama yolu denetimi gerçekleştirilmez, *ermm.exe* dosyasını herhangi bir uygulamadan çalıştırabilirsiniz
- **Uygulama yolu** - *ermm.exe* dosyasını çalıştırma izni olan uygulamayı belirtin

Varsayılan ESET Endpoint Security yüklemesi, ESET Server Security (varsayılan C yolu *:\Program Files\ESET\ESET Server Security*) içinde bulunan *ermm.exe* dosyayı içerir. *ermm.exe*; RMM Sunucusuna bağlı RMM Aracısı ile iletişim kuran RMM Eklentisi ile veri alışverişi yapar.

- *ermm.exe* - Endpoint ürünlerinin yönetimini ve herhangi bir RMM Eklentisi ile iletişimi sağlayan ESET tarafından geliştirilen komut satırı yardımcı programı.
- RMM Eklentisi - Endpoint Windows sisteminde yerel olarak çalışan üçüncü taraf uygulaması. Eklenti, belirli RMM Aracısı (ör. yalnızca Kaseya) ve *ermm.exe* ile iletişim kurmak için tasarlanmıştır.
- RMM Aracısı - Endpoint Windows sisteminde yerel olarak çalışan üçüncü taraf uygulaması (ör. Kaseya'dan). Aracı, RMM Eklentisi ve RMM Sunucusu ile iletişim kurar.
- RMM Sunucusu - Üçüncü taraf sunucusunda hizmet olarak çalışır. Desteklenen RMM sistemleri; Kaseya, Labtech, Autotask, Max Focus ve Solarwinds N-able'dır.

ESET Server Security ürünündeki ESET RMM hakkında daha fazla bilgi edinmek için Bilgi Bankası makalemizi ziyaret edin.

Üçüncü taraf RMM çözümleri için ESET Direct Endpoint Management eklentileri

RMM Server, üçüncü taraf sunucuda hizmet olarak çalışıyor. Daha fazla bilgi için aşağıdaki ESET Direct Endpoint Management online kullanım kılavuzlarına bakın:

- ConnectWise Automate için ESET Direct Endpoint Management Eklentisi
- DattoRMM için ESET Direct Endpoint Management Eklentisi
- Solarwinds N-Central için ESET Direct Endpoint Management
- NinjaRMM için ESET Direct Endpoint Management

Lisans

ESET Server Security, denetleme işlemlerini gerçekleştirmek için saatte birkaç kez ESET License sunucusuna bağlanır. **Aralık denetimi** parametresi varsayılan olarak **Otomatik** şeklinde ayarlanır. Lisans denetimlerinden kaynaklanan ağ trafiğini azaltmak istiyorsanız Aralık denetimini **Sınırlı** olarak değiştirin. Bu durumda, lisans denetimi günde yalnızca bir kez (ve ayrıca sunucu yeniden başlatıldıktan sonra) yapılır.

Sınırlı olarak ayarlanan Aralık denetimiyle, ESET Business Account ve ESET MSP Administrator üzerinden ESET Server Security ürününüzde yapılan, lisansla ilişkili tüm değişikliklerin uygulanması bir gün kadar sürebilir.

WMI Sağlayıcı

Windows Yönetim Yardımcıları (WMI), Microsoft tarafından geliştirilen Web Tabanlı Kurumsal Yönetim (WBEM) uygulamasıdır. Bu uygulama, kurumsal ortamda yönetim bilgilerine erişmek için standart bir teknoloji geliştirmeye yönelik sektörel bir girişimdir.

WMI ile ilgili daha fazla bilgi için http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx sayfasına bakın

ESET WMI Sağlayıcı

ESET WMI Sağlayıcı'nın amacı, ESET tanımlı herhangi bir yazılım ya da araca gerek olmadan, kurumsal bir ortamda ESET ürünlerinin uzaktan izlenmesine olanak sağlamaktır. Temel ürünü, durumu ve istatistiksel bilgileri WMI üzerinden göstererek kurumsal yöneticilere ESET ürünlerini izlerken çok daha fazla imkan sunuyoruz. Yöneticiler, ESET ürünlerinin durumunu izlemek için, WMI tarafından sunulan bir dizi erişim yönteminden yararlanabilir (komut satırı, komut dosyaları ve üçüncü taraf kurumsal izleme araçları).

Mevcut uygulama; temel ürün bilgilerine, yüklenmiş özelliklere ve bunların koruma durumlarına, ayrı ayrı tarayıcıların ististstiklerine ve ürün günlük dosyalarına salt okunur erişim sağlar.

WMI Sağlayıcı, ürünün ve ürün günlüklerinin durumunu okumak için standart Windows WMI altyapısını ve araçlarının kullanılmasına olanak tanır.

Sağlanan veriler

ESET ürünleriyle ilişkili olan tüm WMI sınıfları "root\ESET" ad alanında yer alır. Aşağıda daha ayrıntılı şekilde açıklanan şu sınıflar halihazırda uygulanmıştır:

Genel

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

Günlükler

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**

- **ESET_HyperVScanLogs**
- **ESET_HyperVScanLogRecords**

ESET_Product sınıfı

Yalnızca tek bir ESET_Product sınıfı örneği olabilir. Bu sınıfın özellikleri, yüklenmiş ESET ürününüzle ilgili temel bilgilere başvurur:

- **Kimlik** - ürün türü tanıtıcısı, örneğin "emsl"
- **Ad** - ürünün adı, örneğin "ESET Mail Security"
- **Tam adı** - ürünün tam adı, örneğin "IBM Domino için ESET Mail Security"
- **Sürüm** - Ürünün sürümü, örneğin "6.5.14003.0"
- **VirusDBVersion** - Virüs veri tabanının sürümü, örneğin "14533 (20161201)"
- **VirusDBLastUpdate** - Virüs veri tabanının son güncellemesinin zaman damgası. Bu dize, zaman damgasını WMI tarih-saat biçiminde içerir. Örneğin "20161201095245.000000+060"
- **LicenseExpiration** - Lisans son kullanma tarihi. Dize, zaman damgasını WMI tarih-saat biçiminde içerir
- **KernelRunning** - ekrn hizmetinin makinede çalışıp çalışmadığını gösteren boolean değeri, örneğin “TRUE”
- **StatusCode** - Ürünün koruma durumunu gösteren numara: 0 - Yeşil (Tamam), 1 - Sarı (Uyarı), 2 - Kırmızı (Hata)
- **StatusText** - sıfırdan farklı durum kodunun nedenini açıklayan ileti, aksi halde boş olur

ESET_Features sınıfı

ESET_Features sınıfı, ürün özelliklerinin sayısına bağlı olarak birden çok tekrara sahiptir. Her tekrar şunları içerir:

- **Ad** - özelliğin adı (adların listesi aşağıda sağlanmaktadır)
- **Durum** - özelliğin durumu: 0 - pasif, 1 - devre dışı, 2 - etkin

Halihazırda algılanan ürün özelliklerini temsil eden dizelerin listesi:

- **CLIENT_FILE_AV** - gerçek zamanlı dosya sistemi antivirus koruması
- **CLIENT_WEB_AV** - istemci web antivirus koruması
- **CLIENT_DOC_AV** - istemci belge antivirus koruması
- **CLIENT_NET_FW** - istemci kişisel güvenlik duvarı
- **CLIENT_EMAIL_AV** - istemci e-posta antivirus koruması
- **CLIENT_EMAIL_AS** - istemci e-posta antispam koruması
- **SERVER_FILE_AV** - korunan dosya sunucusu ürünündeki dosyaların gerçek zamanlı antivirus koruması, örneğin ESET Server Security durumunda SharePoint'in içerik veri tabanındaki dosyalar
- **SERVER_EMAIL_AV** - korunan sunucu ürününün e-postalarının antivirus koruması, örneğin MS Exchange veya IBM Domino'daki e-postalar
- **SERVER_EMAIL_AS** - korunan sunucu ürününün e-postalarının antispam koruması, örneğin MS Exchange veya IBM Domino'daki e-postalar
- **SERVER_GATEWAY_AV** - ağ geçidindeki korunan ağ protokollerinin antivirus koruması
- **SERVER_GATEWAY_AS** - ağ geçidindeki korunan ağ protokollerinin antispam koruması

ESET_Statistics sınıfı

ESET_Statistics sınıfı, üründeki tarayıcıların sayısına bağlı olarak birden çok örneğe sahiptir. Her örnek şunları içerir:

- **Tarayıcı** - belirli tarayıcı için dize kodu, örneğin "CLIENT_FILE"

- **Toplam** - taranan dosyaların toplam sayısı
- **Etkilenen** - etkilenen dosyaların sayısı
- **Temizlenen** - temizlenen dosyaların sayısı
- **Zaman damgası** - bu istatistiğin son değiştirildiği zamanı gösteren zaman damgası. WMI tarih-zaman biçiminde, örneğin "20130118115511.000000+060"
- **ResetTime** - İstatistiklerin en son sıfırlandığı zamanı gösteren zaman damgası. WMI tarih-zaman biçiminde, örneğin "20130118115511.000000+060"

Halihazırda algılanan tarayıcıları temsil eden dizelerin listesi:

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog sınıfı

ESET_ThreatLog sınıfının birden çok örneği vardır ve her biri "Algılanan tehditler" günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Scanner** - bu olay günlüğünü oluşturan tarayıcının adı
- **ObjectType** - bu olay günlüğünü üreten nesnenin türü
- **ObjectName** - bu olay günlüğünü üreten nesnenin adı
- **Tehdit** - ObjectName ve ObjectType özellikleri tarafından açıklanan nesnede bulunan tehdidin adı
- **Eylem** - tehdidin algılanmasının ardından gerçekleştirilen eylem
- **Kullanıcı** - Bu olay günlüğünün oluşturulmasına neden olan kullanıcı hesabı
- **Bilgiler** - Olayla ilgili ek bilgiler
- **Karma** - Bu günlük olayını üreten nesne karması

ESET_EventLog

ESET_ThreatLog sınıfının birden çok örneği vardır ve her biri "Olaylar" günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Günlük Düzeyi** - günlük kaydının [0-8] aralığından bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Modül** - bu olay günlüğünü oluşturan modülün adı
- **Olay** - olayın açıklaması
- **Kullanıcı** - Bu olay günlüğünün oluşturulmasına neden olan kullanıcı hesabı

ESET_ODFileScanLogs

ESET_ODFileScanLogs sınıfının birden çok örneği vardır ve her biri, bir isteğe bağlı dosya taraması kaydını temsil eder. Bu, günlüklerin "İsteğe bağlı bilgisayar taraması" GUI'sine eşdeğerdir. Her örnek şunları içerir:

- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Hedefler** - taramanın hedef klasörleri/nesneleri
- **Toplam Taranan** - taranan nesnelerin toplam sayısı
- **Etkilenen** - etkilenmiş nesnelerin sayısı
- **Temizlenen** - temizlenen nesnelerin sayısı
- **Status** - tarama işleminin durumu

ESET_ODFileScanLogRecords

ESET_ODFileScanLogRecords sınıfının birden çok örneği vardır ve her biri ESET_ODFileScanLogs sınıfının örneklerince temsil edilen tarama günlüklerinden birindeki günlük kaydını temsil eder. Bu sınıfın örnekleri, tüm isteğe bağlı taramaların/günlüklerin günlük kayıtlarını sağlar. Yalnızca belirli bir tarama günlüğü örneğine gerek duyuluyorsa, LogID özelliğine göre filtrelenmelidir. Her sınıf örneği şunları içerir:

- **LogID** - bu kaydın ait olduğu tarama günlüğünün kimliği (ESET_ODFileScanLogs sınıfının örneklerinden birinin kimliği)
- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Günlük** - Gerçek günlük iletisi

ESET_ODServerScanLogs

ESET_ODServerScanLogs sınıfının birden çok örneği vardır ve her biri bir isteğe bağlı tarama çalıştırmasını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Hedefler** - taramanın hedef klasörleri/nesneleri
- **Toplam Taranan** - taranan nesnelerin toplam sayısı
- **Etkilenen** - etkilenmiş nesnelerin sayısı
- **Temizlenen** - temizlenen nesnelerin sayısı
- **RuleHits** - kural isabetlerinin toplam sayısı
- **Status** - tarama işleminin durumu

ESET_ODServerScanLogRecords

ESET_ODFileScanLogRecords sınıfının birden çok örneği vardır ve her biri ESET_ODServerScanLogs sınıfının örneklerince temsil edilen tarama günlüklerinden birindeki günlük kaydını temsil eder. Bu sınıfın örnekleri, tüm isteğe bağlı taramaların/günlüklerin günlük kayıtlarını sağlar. Yalnızca belirli bir tarama günlüğü örneğine gerek duyuluyorsa, LogID özelliğine göre filtrelenmelidir. Her sınıf örneği şunları içerir:

- **LogID** - bu kaydın ait olduğu tarama günlüğünün kimliği (ESET_ ODServerScanLogs sınıfının örneklerinden birinin kimliği)
- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği

- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Günlük Düzeyi** - günlük kaydının [0-8] aralığından bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Günlük** - Gerçek günlük iletisi

ESET_SmtpProtectionLog

ESET_SmtpProtectionLog sınıfının birden çok örneği vardır ve her biri "Smtp koruma" günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu tarama günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **HELODomain** - HELO etki alanının adı
- **IP** - kaynak IP adresi
- **Sender** - e-posta göndericisi
- **Alıcı** - e-posta alıcısı
- **KorumaTürü** - Kullanılan koruma türü
- **Eylem** - gerçekleştirilen eylem
- **Neden** - Eylemin nedeni
- **TimeToAccept** - e-postanın kabul edilmesi için geçecek dakika sayısı

ESET_HIPSLog

ESET_HIPSLog sınıfının birden çok örneği vardır ve her biri "HIPS" günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Günlük Düzeyi** - günlük kaydının [0-8] aralığından bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Uygulama** - Kaynak uygulama
- **Hedef** - İşlem türü
- **Eylem** - HIPS tarafından gerçekleştirilen eylem; ör. izin ver, reddet vb.
- **Kural** - Eylemden sorumlu kuralın adı
- **Ek Bilgi**

ESET_URLLog

ESET_URLLog sınıfının birden çok örneği vardır ve her biri "Filtrelenen web siteleri" günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman

biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **URL** - Söz konusu URL
- **Durum** - URL'ye ilişkin durum; ör. "Web denetimi tarafından engellendi"
- **Uygulama** - URL'ye erişmeyi deneyen uygulama
- **Kullanıcı** - Uygulamanın çalıştığı kullanıcı hesabı

ESET_DevCtrlLog

ESET_DevCtrlLog sınıfının birden çok örneği vardır ve her biri “Aygıt denetimi” günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik**- bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Aygıt** - Aygıt adı
- **Kullanıcı** - Kullanıcı hesabı adı
- **Kullanıcı SID'si** - Kullanıcı hesabı SID'si
- **Grup** - Kullanıcı grubu adı
- **Grup SID'si** - Kullanıcı grubu SID'si
- **Durum** - Aygıta ilişkin durum; ör. "Yazma engellendi"
- **Aygıt Ayrıntıları** - Aygıtla ilgili ek bilgi
- **Olay Ayrıntıları** - Olayla ilgili ek bilgi

ESET_MailServerLog

ESET_MailServerLog sınıfının birden çok örneği vardır ve her biri “Posta sunucusu” günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **IP Adresi** - Kaynak IP adresi
- **HELODomain** - HELO etki alanının adı
- **Sender** - e-posta göndericisi
- **Alıcı** - e-posta alıcısı
- **Konu** - E-posta konusu
- **Koruma Türü** - Geçerli günlük kaydı tarafından tanımlanan eylemi (yani zararlı yazılım, antispam veya kurallar) gerçekleştiren koruma türü.
- **Eylem** - gerçekleştirilen eylem
- **Neden** - Belirtilen Koruma Türü tarafından nesne üzerinde gerçekleştirilen eylemin nedeni.

ESET_HyperVScanLogs

ESET_HyperVScanLogs sınıfının birden çok örneği vardır ve her biri, bir Hyper-Vdosya taraması yürütmesini temsil eder. Bu, günlüklerin "Hyper-V taraması" GUI'sine eşdeğerdir. Her örnek şunları içerir:

- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Hedefler** - Taramanın hedef makineleri/diskleri/birimleri
- **Toplam Taranan** - taranan nesnelerin toplam sayısı
- **Etkilenen** - etkilenmiş nesnelerin sayısı
- **Temizlenen** - temizlenen nesnelerin sayısı
- **Status** - tarama işleminin durumu

ESET_HyperVScanLogRecords

ESET_HyperVScanLogRecords sınıfının birden çok örneği vardır ve her biri ESET_HyperVScanLogs sınıfının örneklerince temsil edilen tarama günlüklerinden birindeki günlük kaydını temsil eder. Bu sınıfın örnekleri, tüm Hyper-V taramalarının/günlüklerinin günlük kayıtlarını sağlar. Yalnızca belirli bir tarama günlüğü örneğine gerek duyuluyorsa, LogID özelliğine göre filtrelenmelidir. Her sınıf örneği şunları içerir:

- **LogID** - bu kaydın ait olduğu tarama günlüğünün kimliği (ESET_HyperVScanLogs sınıfının örneklerinden birinin kimliği)
- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Günlük** - Gerçek günlük iletisi

ESET_NetworkProtectionLog

ESET_NetworkProtectionLog sınıfının birden çok örneği vardır ve her biri “Ağ koruması” günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Olay** - Ağ koruması eylemini tetikleyen olay
- **Eylem** - Ağ koruması tarafından gerçekleştirilen eylem
- **Kaynak** - Ağ aygıtının kaynak adresi
- **Hedef** - Ağ aygıtının hedef adresi
- **Protokol** - Ağ iletişim protokolü
- **RuleOrWormName** - Olayla ilgili kural veya solucan adı
- **Uygulama** - Ağ iletişimini başlatan uygulama
- **Kullanıcı** - Bu olay günlüğünün oluşturulmasına neden olan kullanıcı hesabı

ESET_SentFilesLog

ESET_SentFilesLog sınıfının birden çok örneği vardır ve her biri “Gönderilen dosyalar” günlüğünden bir günlük kaydını temsil eder. Her örnek şunları içerir:

- **Kimlik** - bu günlük kaydının benzersiz kimliği
- **Zaman damgası** - günlük kaydının oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Sha1** - Gönderilen dosyanın Sha-1 karması
- **Dosya** - Gönderilen Dosya
- **Boyut** - Gönderilen dosyanın boyutu
- **Kategori** - Gönderilen dosyanın kategorisi
- **Neden** - Dosyanın gönderilme nedeni
- **SentTo** - Dosyanın gönderildiği ESET departmanı
- **Kullanıcı** - Bu olay günlüğünün oluşturulmasına neden olan kullanıcı hesabı

ESET_OneDriveScanLogs

ESET_OneDriveScanLogs sınıfının birden çok örneği vardır ve her biri, bir OneDrive taramasının yürütmesini temsil eder. Bu, günlüklerin "OneDrive taraması" GUI'sine eşdeğerdir. Her örnek şunları içerir:

- **Kimlik** - Bu OneDrive günlük kaydının benzersiz kimliğidir
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **Hedefler** - taramanın hedef klasörleri/nesneleri
- **Toplam Taranan** - taranan nesnelerin toplam sayısı
- **Etkilenen** - etkilenmiş nesnelerin sayısı
- **Temizlenen** - temizlenen nesnelerin sayısı
- **Status** - tarama işleminin durumu

ESET_OneDriveScanLogRecords

ESET_OneDriveScanLogRecords sınıfının birden çok örneği vardır ve her biri ESET_OneDriveScanLogRecords sınıfının örneklerince temsil edilen tarama günlüklerinden birindeki günlük kaydını temsil eder. Bu sınıfın örnekleri, tüm isteğe bağlı taramaların/günlüklerin günlük kayıtlarını sağlar. Yalnızca belirli bir tarama günlüğü örneğine gerek duyuluyorsa, LogID özelliğine göre filtrelenmelidir. Her sınıf örneği şunları içerir:

- **LogID** - Bu kaydın ait olduğu tarama günlüğünün kimliği (ESET_OneDriveScanLogs sınıfının örneklerinden birinin kimliği)
- **Kimlik** - Bu OneDrive günlük kaydının benzersiz kimliğidir
- **Zaman damgası** - günlüğün oluşturulduğu zamanı gösteren zaman damgası (WMI tarih/zaman biçiminde)
- **LogLevel** - günlük kaydının [0-8] kümesinden bir sayı olarak ifade edilen önem derecesi. Değerler, aşağıdaki adlandırılan düzeylere tekabül eder: Hata Ayıklama, Bilgi-Dipnot, Bilgi, Bilgi - Önemli, Uyarı, Hata, Güvenlik/Uyarı, Hata-Ciddi, Güvenlik Uyarısı-Ciddi
- **Günlük** - Gerçek günlük iletisi

Sağlanan Verilere Erişme

Burada, Windows komut satırından ve PowerShell'den ESET WMI verilerine nasıl erişileceğine dair birkaç örnek verilmektedir. Bunlar, mevcut herhangi bir Windows işletim sisteminde kullanılabilir. Ancak verilere diğer komut

dosyası dillerinden ve araçlarından erişmenin başka yolları da vardır.

Komut dosyası olmayan komut satırı

`Wmic` komut satırı aracı, çeşitli önceden tanımlanmış veya özel WMI sınıflarına erişmek için kullanılabilir.

Yerel makinedeki ürünle ilgili tüm bilgileri görüntülemek için:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Yerel makinedeki ürünün yalnızca ürün sürüm numarasını görüntülemek için:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

10.1.118.180 IP'sine sahip uzak makinedeki ürünle ilgili tüm bilgileri görüntülemek için:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Yerel makinedeki ürünle ilgili tüm bilgileri almak ve görüntülemek için:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

10.1.118.180 IP'sine sahip uzak makinedeki ürünle ilgili tüm bilgileri almak ve görüntülemek için:

```
$cred = Get-Credential # kullanıcıdan kimlik bilgileri ister ve bunları şu
değişkende depolar
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

ESET PROTECT tarama hedefleri

Bu işlev, ESET Server Security bulunan bir sunucuda **Sunucu Taraması** istemci görevi çalıştırırken, ESET PROTECT ürününün tarama hedefi (İsteğe bağlı posta kutusu veri tabanı taraması ve Hyper-V taraması) kullanmasına olanak sağlar. ESET PROTECT tarama hedefleri ayarı yalnızca ESET Management Agent yüklenmişse kullanılabilir. Aksi halde, gri renkle gösterilecektir.

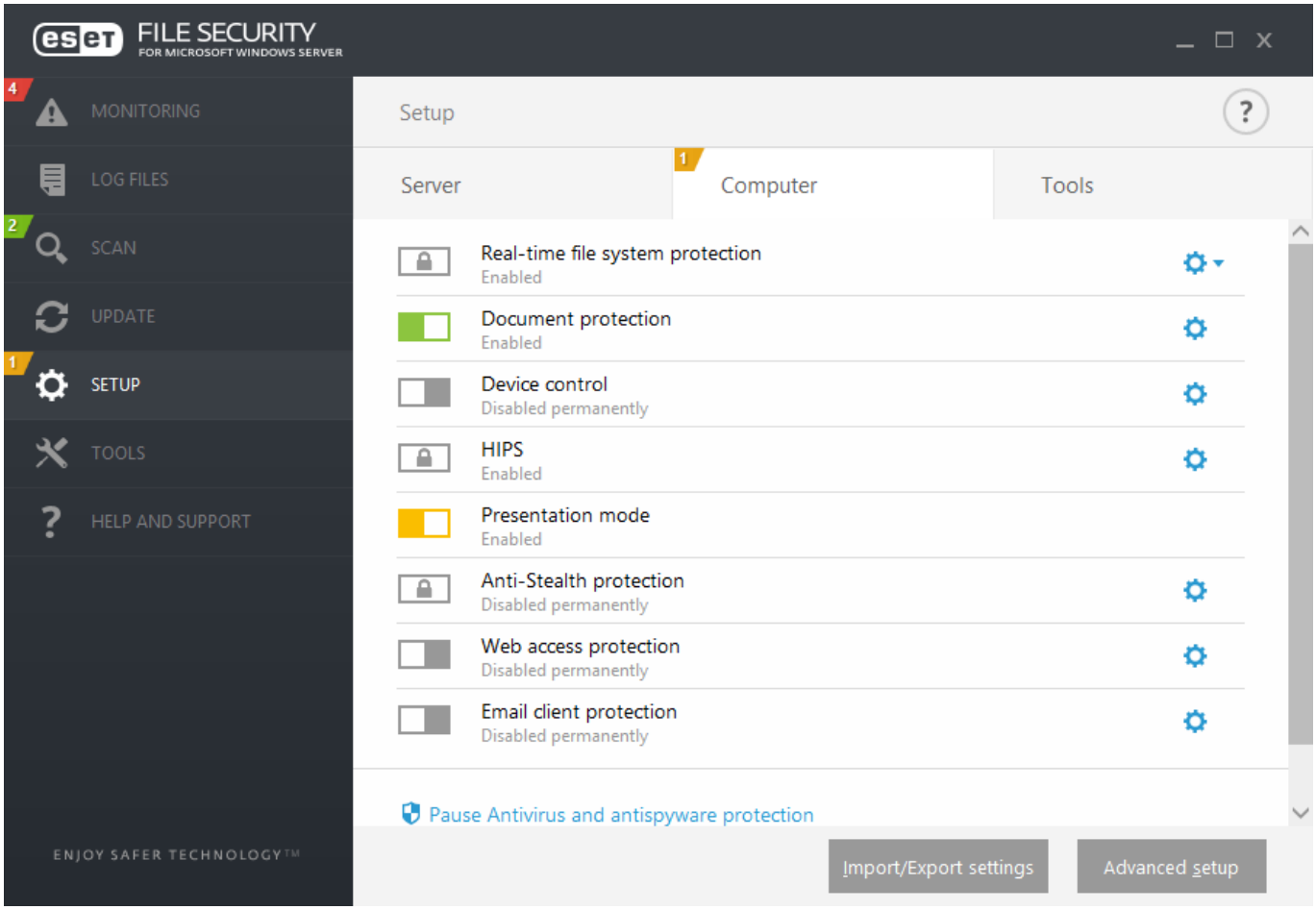
Hedef listesi oluştur işlevini etkinleştirdiğinizde, ESET Server Security kullanılabilir tarama hedeflerinin bir listesini oluşturur. Bu liste, tanımladığınız **Güncelle dönemine** uygun şekilde dönemsel olarak oluşturulur.

> NOT
> **Hedef listesi oluştur** seçeneği ilk kez etkinleştirildiğinde, ESET PROTECT'nin bu seçimi algılaması belirtilen **Güncelle süresinin** yaklaşık yarısı kadar bir süreyi alır. Yani **Güncelleme süresi** 60 dakika olarak ayarlanırsa ESET PROTECT'nin tarama hedefleri listesini alması yaklaşık 30 dakika sürer. ESET PROTECT'nin listeyi daha erken toplamasını isterseniz, güncelleme süresi için daha küçük bir değer belirtin. Bu değeri dilediğiniz zaman artırabilirsiniz.

ESET PROTECT, **Sunucu Taraması** istemci görevi çalıştırdığında, listeyi toplar ve söz konusu sunucuda Hyper-V taraması için tarama hedefleri seçmeniz istenir.

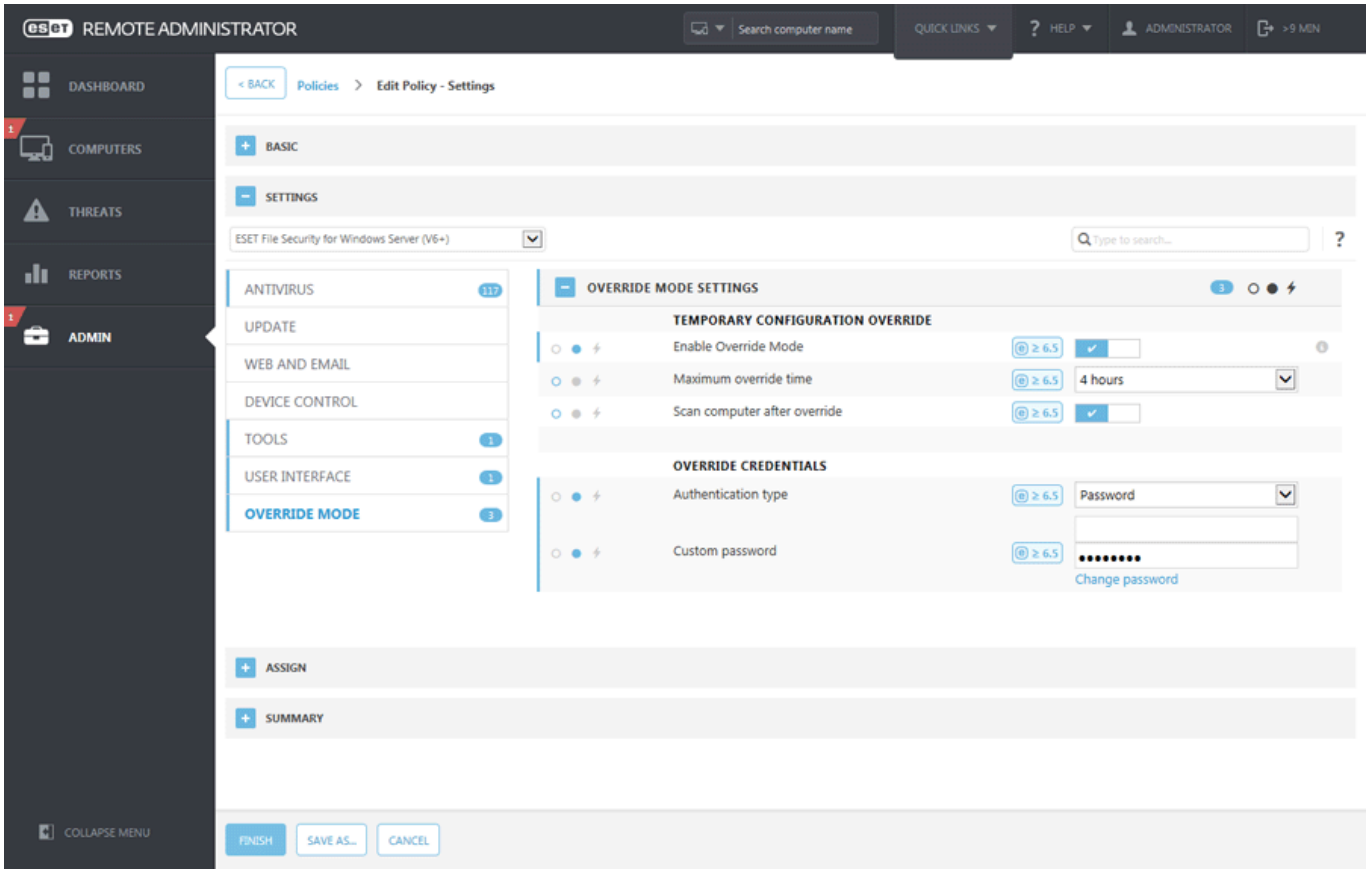
Geçersiz kılma modu

ESET PROTECT Ilkesi ESET Server Security aracına uygulanmışsa, Ayarlar sayfasında Etkinleştir/Devre Dışı bırak anahtarı yerine bir kilit simgesi görürsünüz, ayrıca **Gelişmiş ayarlar** penceresindeki anahtarın yanında da bir kilit simgesi yer alır.

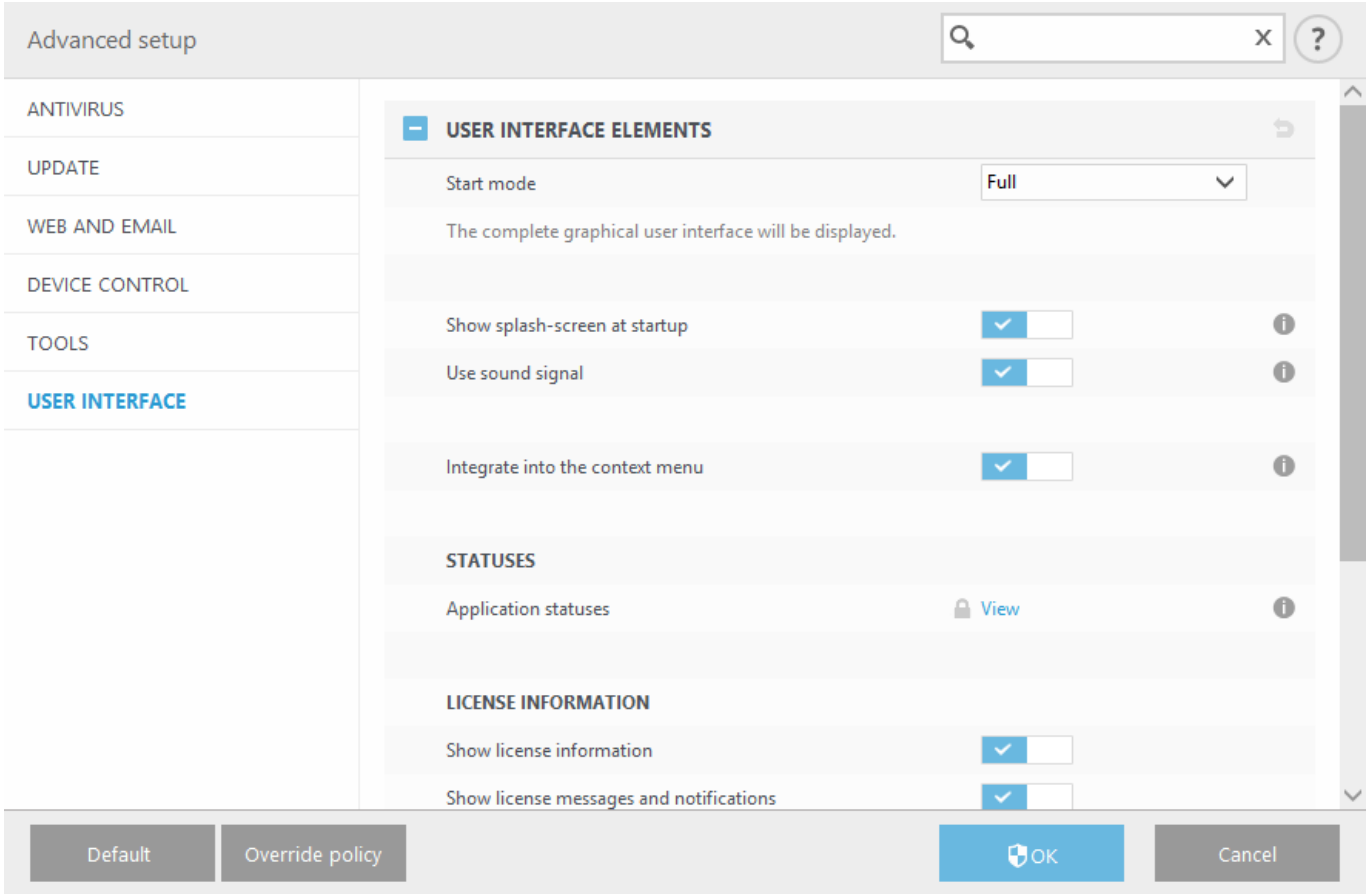


Normalde ESET PROTECT ilkesi üzerinden yapılandırılan ayarlar değiştirilemez. Geçersiz kılma modu, bu ayarların kilidini geçici olarak açmanıza olanak tanır. Ancak ESET PROTECT ilkesini kullanarak **Geçersiz kılma modunu** etkinleştirmeniz gerekir.

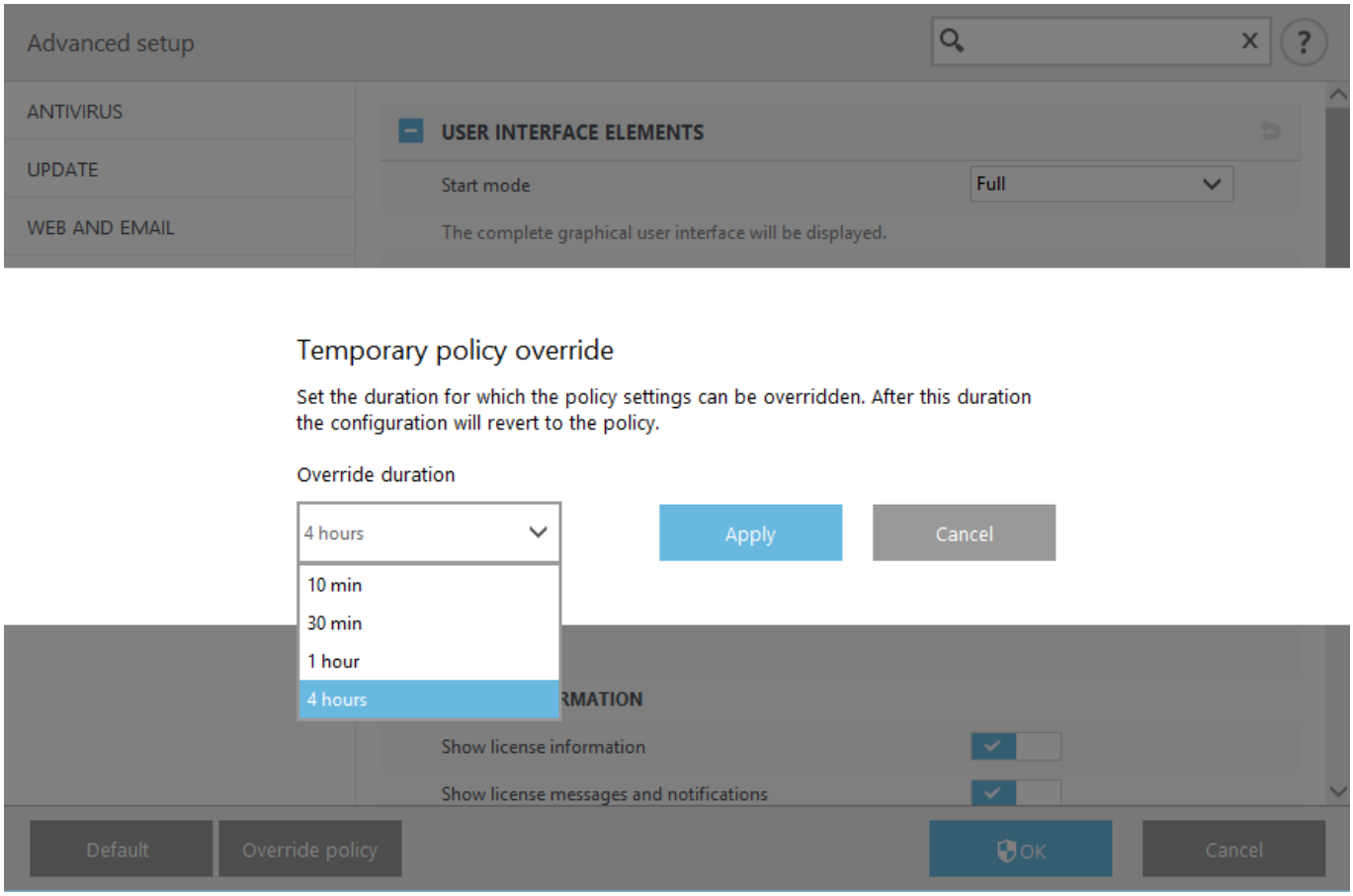
ESET PROTECT Web Konsolu'na giriş yapın, **İlkeler** bölümüne gidin, ESET Server Security aracına uygulanan mevcut ilkeyi seçip düzenleyin veya yeni bir ilke oluşturun. **Ayarlar**'da, **Geçersiz Kılma Modu**'nu tıklayıp etkinleştirin ve Kimlik Doğrulama türü dahil (**Active Directory kullanıcısı** veya **Parola**) diğer ayarları yapılandırın.



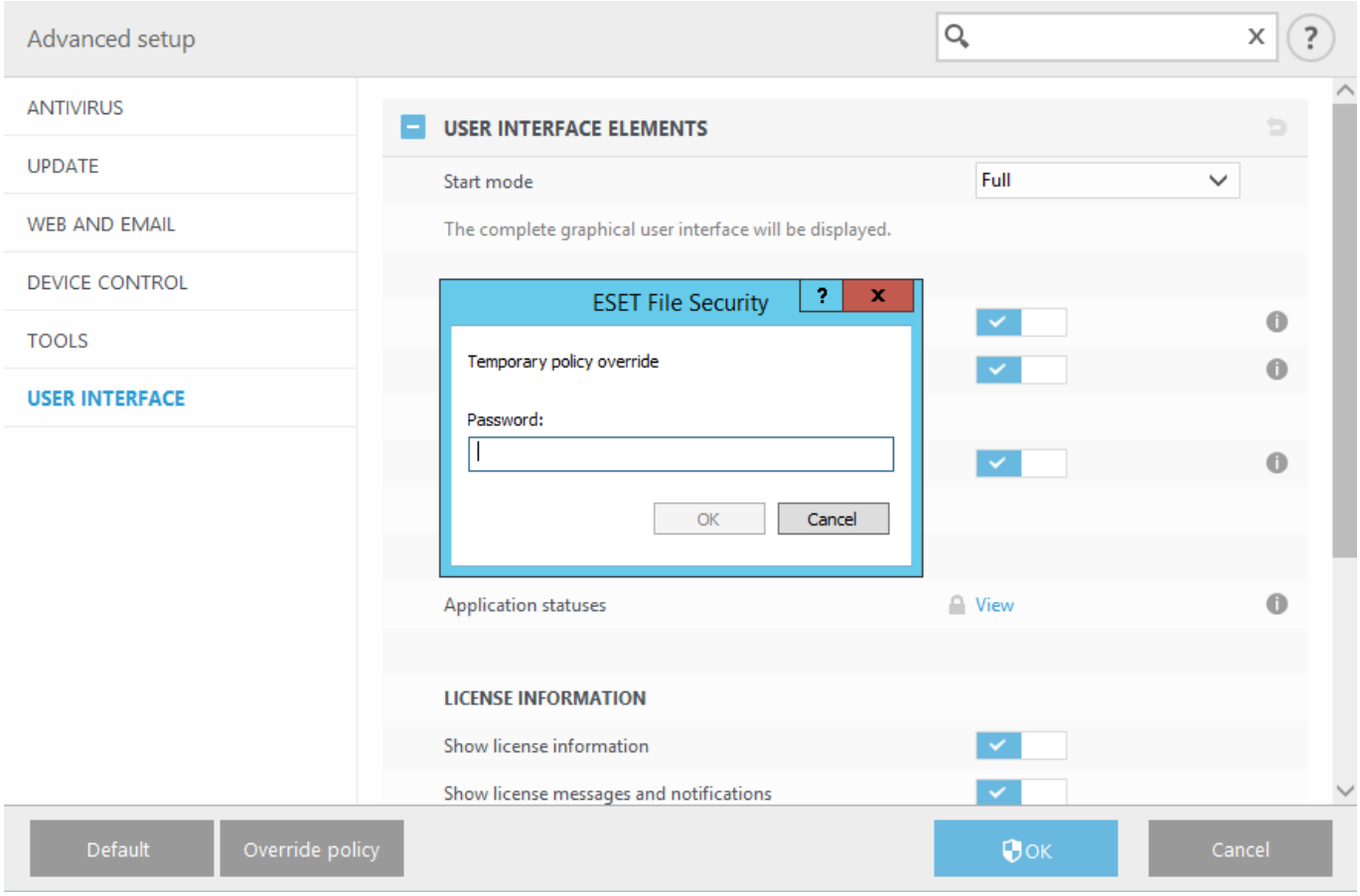
İlke değiştirildikten veya yeni ilke ESET Server Security aracına uygulandıktan sonra, İlkeyi geçersiz kıl düğmesi Gelişmiş ayarlar penceresinde görüntülenir.



İlkeyi geçersiz kıl düğmesini tıklatın, süreyi ayarlayın ve **Uygula**'yı tıklatın.



Kimlik Doğrulama türü olarak **Parola**'yı seçerseniz, ilke geçersiz kılma parolasını girin.



Geçersiz kılma modunun süresi dolunca, yaptığınız tüm yapılandırma değişiklikleri orijinal ESET PROTECT ilkesi

ayarlarına geri döner. Geçersiz kılma modunun süresi dolmadan önce bir bildirim görürsünüz.

İzleme sayfasında veya **Gelişmiş ayarlar** penceresinde süresi dolmadan önce dilediğiniz zaman **Geçersiz kılma modunu sonlandırabilirsiniz**.

Günlük dosyaları

Bu bölüm, ESET Server Security günlüğe kaydetme yapılandırmasını değiştirmenize olanak tanır.

Günlük kaydı filtreleme

Tüm günlüğe kaydetme seçenekleri varsayılan olarak etkinleştirildiğinden önemli miktarda veri üretir. Kullanışlı veya sorunla ilgili olmayan bileşenlerin günlüğe kaydedilmesini seçim yaparak devre dışı bırakmanızı öneririz.

> NOT
> Gerçek günlüğe kaydetmeyi başlatmak için ana menüde ürün düzeyinde **Ayarlar** > Araçlar bölümünde **Tanılama amaçlı günlüğe kaydetme**'yi etkinleştirmeniz gerekir. Günlüğe kaydetme özelliği etkinleştirildikten sonra, ESET Server Security bu bölümde etkinleştirilmiş olan özelliklere uygun olarak ayrıntılı günlükleri toplar.

Belirli özellikleri etkinleştirmek veya devre dışı bırakmak için düğmeleri kullanın. Bu seçenekler, ESET Server Security içindeki ayrı bileşenlerin kullanılabilirliğine bağlı olarak birleştirilebilir.

- **Küme Tanılama günlük kaydı** - Küme günlüğe kaydetme özelliği, genel tanı amaçlı günlüğe kaydetmeye eklenir.

Günlük dosyaları

Günlüklerin nasıl yönetileceğini tanımlayın. Bu özellik, diskin sonuna kadar kullanılmasını önlemek açısından çok önemlidir. Varsayılan ayarlar, disk alanı açmak için eski günlüklerin otomatik olarak silinmesine olanak sağlar.

(Gün) günden eski kayıtları otomatik olarak sil

Belirtilen gün sayısından eski günlük girişleri silinir.

Günlük boyutu aşılırsa eski kayıtları otomatik olarak sil

Günlük boyutu **Maks. günlük boyutunu [MB]** aştığında eski günlük kayıtları **Azaltılmış günlük boyutuna [MB]** ulaşılana kadar silinir.

Otomatik olarak silinen kayıtları yedekle

Otomatik olarak silinen günlük kayıtları ve dosyalar, belirtilen dizine yedeklenir ve isteğe bağlı olarak ZIP dosyaları biçiminde sıkıştırılır.

Tanılama günlüklerini yedekle

Otomatik olarak silinen tanı amaçlı günlükler yedeklenir. Etkinleştirilmezse tanı amaçlı günlük kayıtları

yedeklenmez.

Yedekleme klasörü

Günlük yedeklemelerinin depolanacağı klasör. Günlük yedeklemelerinin ZIP kullanılarak sıkıştırılmasını etkinleştirebilirsiniz.

Günlük dosyalarını otomatik olarak optimize et

Bağlanıldığında bölümlere ayırma yüzdesi **Kullanılmayan kayıt sayısı şu değeri aşarsa (%):** alanında belirtilen değerden daha büyükse günlük dosyaları otomatik olarak birleştirilir. Günlüklerin birleştirilmesi işlemini başlatmak için **Optimize et** seçeneğini tıklayın. Tüm boş günlük girişleri performansı ve günlük işleme hızını artırmak için kaldırılır. Bu iyileştirme, özellikle çok sayıda giriş içeren günlüklerde belirgin olarak gözlenir.

Metin protokolünü etkinleştir

Günlük dosyalarından başka bir dosya biçiminde günlük depolamayı etkinleştirmek için:

- **Hedef dizin** - Günlük dosyalarının depolanacağı dizin (yalnızca **Metin/CSV** için geçerlidir). Her günlük bölümünün önceden tanımlı dosya adına sahip kendi dosyası vardır (örneğin, günlükleri depolamak için düz metin dosya biçimi kullanıyorsanız, Günlük dosyalarının Algılanan tehditler bölümü için *virlog.txt* kullanılır).
- **Tür** - **Metin** dosya biçimini seçerseniz, günlükler metin dosyasına depolanır; veriler sekmelerle ayrılır. Aynısı, virgülle ayrılan **CSV** dosya biçimi için de uygulanır. **Olay** seçeneğini belirlerseniz günlük, dosya yerine Windows Olay günlüğüne depolanır (Denetim masasındaki Olay Görüntüleyicisi kullanılarak görüntülenebilir).
- **Tüm günlük dosyalarını sil** - **Tür** açılır menüsünde halihazırda seçili olan tüm depolanan günlükleri siler.

NOT
Sorunları daha hızlı çözmeye yardımcı olmak için ESET Teknik Destek, bilgisayarınızdan günlükler sağlamanızı isteyebilir. ESET Log Collector, istenen bilgileri toplamanızı kolaylaştırır. ESET Log Collector hakkında daha fazla bilgi için Bilgi Bankası makalemize bakın.

Denetleme günlüğü

Yapılandırma veya korumadaki değişiklikleri izlemenize olanak tanır. Ürün yapılandırmasının değiştirilmesi ürünün nasıl çalıştığını önemli düzeyde etkileyebileceği için denetleme amaçlarına yönelik olarak değişiklikleri izleyebilirsiniz. **Günlük dosyaları** > Denetleme günlüğü bölümünde değişikliklerin günlük kayıtlarına bakabilirsiniz.

Proxy sunucu

Büyük LAN ağlarında, bilgisayarınızın İnternet'e bağlantısı proxy sunucu aracılığıyla gerçekleştirilir. Bu durumda, aşağıdaki ayarların tanımlanması gerekir. Ayarları tanımlamazsanız, program kendini otomatik olarak güncelleyemez. ESET Server Security içinde proxy sunucu ayarları **Gelişmiş ayarlar** penceresinde (**F5**) iki farklı bölümde kullanılabilir.

1. **Gelişmiş ayarlar** (**F5**) > **Güncelleme** > **Profiller** > **Güncellemeler** > **Bağlantı seçenekleri** > HTTP Proxy'si
   Bu ayar belirli güncelleme profili için geçerlidir ve çoğu zaman farklı konumlardan modüller alan dizüstü bilgisayarlar için önerilir.

2. **Gelişmiş ayarlar** (**F5**) > **Araçlar** > **Proxy sunucu**
Proxy sunucuyu bu düzeyde belirtmek, tüm ESET Server Security için genel proxy sunucu ayarlarını tanımlar. Buradaki parametreler İnternet'e bağlanan tüm modüller tarafından kullanılır.

Bu düzey için proxy sunucu ayarını belirlemek üzere **Proxy sunucu kullan** anahtarını açık konumuna getirin ve ardından **Proxy sunucu** alanına proxy sunucu adresini ve proxy sunucunun **Bağlantı noktası** numarasını girin.

Proxy sunucu kimlik doğrulaması gerektirir

Proxy sunucu aracılığıyla ağ iletişimi kimlik doğrulaması gerektiriyorsa, bu seçeneği etkinleştirin ve **Kullanıcı Adını** ve **Parolayı** belirleyin.

Proxy sunucuyu sil

Proxy sunucu ayarlarını otomatik olarak algılamak ve doldurmak için **Algıla** düğmesini tıklatın. Internet Explorer'da belirtilen parametreler kopyalanır.

NOT
Bu özellik kimlik doğrulama verilerini (kullanıcı adı ve parola) alamaz; bunları sizin sağlamanız gerekir.

Proxy mevcut değilse doğrudan bağlantıyı kullanın

Bir ürün HTTP Proxy kullanacak şekilde yapılandırılmışsa, ancak proxy'ye ulaşılamıyorsa, ürün proxy'yi atlayarak doğrudan ESET sunucularıyla iletişim kurar.

Bildirimler

Masaüstündeki bildirimler ve ipucu balonları bilgilendirme amaçlıdır ve kullanıcı etkileşimi gerektirmez. Ekranın sağ alt köşesindeki bildirim alanında görüntülenirler. Bildirim görüntüleme zamanı ve pencere saydamlığı gibi daha ayrıntılı seçenekler aşağıda değiştirilebilir. Etkileşimli olmayan tüm bildirimleri bastırmak için **Uygulamalar tam ekran modunda çalıştırılırken bildirimleri gösterme** düğmesini açın.

Başarılı güncelleme hakkındaki bildirimi göster

Bir güncelleme başarılı olduğunda açılır pencere bildirimi gösterilir.

Olay bildirimlerini e-postayla gönder

E-posta bildirimlerini etkinleştirmek için etkinleştirin.

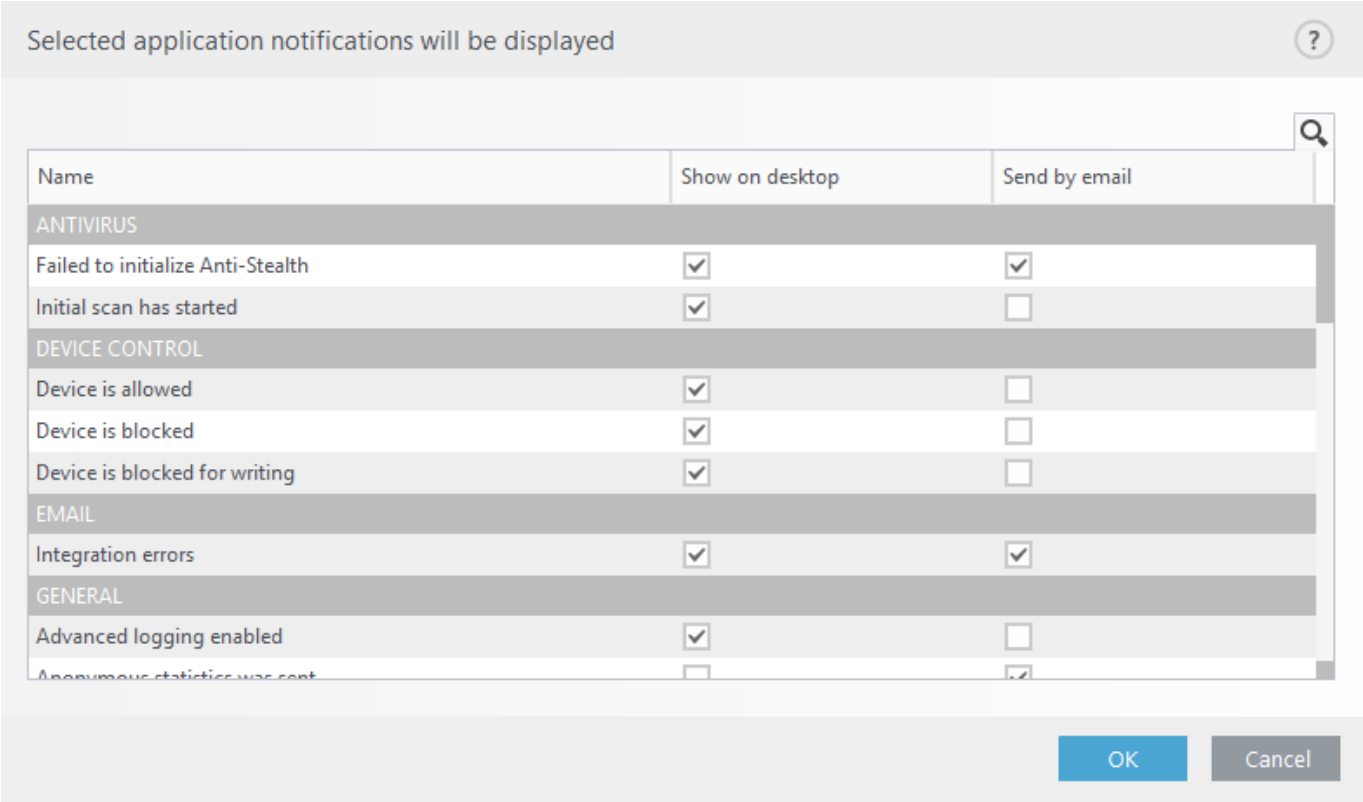
Uygulama bildirimleri

Ekran uygulama bildirimlerini etkinleştirmek veya devre dışı bırakmak için Düzenle'yi tıklayın.

Uygulama bildirimleri

ESET Server Security bildirimlerini masaüstünde gösterilecek ve/veya e-postayla gönderilecek şekilde yapılandırabilirsiniz.

NOT
E-posta bildirimleri için **Temel** bölümünde **Olay bildirimlerini e-postayla gönder** seçeneğini etkinleştirdikten sonra gerekli olması halinde SMTP sunucusunu ve diğer ayrıntıları yapılandırın.



Masaüstü bildirimleri

Tehdit uyarıları ve sistem bildirimlerini (başarılı güncelleme iletileri gibi) ESET Server Security tarafından nasıl işleneceğini yapılandırabilirsiniz. Örneğin, sistem tepsisi bildirimlerinin görüntülenme **Süresini** ve **Saydamlığını** ayarlayabilirsiniz (bu, yalnızca sistem tepsisi bildirimlerini destekleyen sistemlerde geçerlidir).

Görüntülenecek olayların minimum ayrıntı düzeyi açılır menüsü, uyarıların ve bildirimlerin şiddet düzeylerini belirlemenize olanak tanır. Kullanılabilir seçenekler şunlardır:

- **Tanılama** - Programı ve yukarıdaki tüm kayıtları hassas bir şekilde ayarlamak için gereken bilgileri günlüğe kaydeder.
- **Bilgilendirici** - Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarılar** - Kritik hataları ve uyarı iletilerini kaydeder.
- **Hatalar** - "Dosya indirme hatası" gibi hatalar ve kritik hatalar kaydedilir.
- **Kritik** - Yalnızca kritik hataları günlüğe kaydeder.

Birden fazla kullanıcının olduğu sistemlerde bildirimleri şu kullanıcının ekranında görüntüle alanı, aynı anda birden çok kullanıcının bağlanmasına olanak veren sistemlerde sistem bildirimlerini ve diğer bildirimleri alacak kullanıcıyı belirtir. Normalde bu, sistem veya ağ yöneticisi olacaktır. Bu seçenek, tüm sistem bildirimlerinin yöneticiye gönderilmesi koşuluyla özellikle terminal sunucular için kullanışlıdır.

E-posta bildirimleri

ESET Server Security, seçili ayrıntı düzeyine sahip bir olay meydana gelirse otomatik olarak bildirim e-postaları gönderebilir.

> NOT
> TLS şifrelemesine sahip SMTP sunucuları ESET Server Security tarafından desteklenir.

SMTP sunucusu

Uyarı ve bildirim göndermek için kullanılan SMTP sunucusunun adı. Bu, genellikle Microsoft Exchange Server'ınızın adıdır.

Kullanıcı adı ve parola

SMTP sunucusu kimlik doğrulaması gerektiriyorsa SMTP sunucusuna erişmek için bu alanlar geçerli bir kullanıcı adı ve parola ile doldurulmalıdır.

Gönderen adresi

Bildirim e-postalarının başlığında görüntülenecek olan gönderici adresini girin. Alıcı **Kimden** alanında bu adresi görür.

Alıcı adresi

Bildirimlerin iletileceği **Kime** bölümünde alıcının e-posta adresini belirtin.

TLS'yi etkinleştir

TLS şifrelemesi tarafından desteklenen uyarı ve bildirim iletilerini etkinleştirir.

E-posta ayarları

Bildirimler için minimum ayrıntı düzeyi

Gönderilecek bildirimlerin minimum ayrıntı düzeyini belirtir.

Şu aralıktan sonra yeni bildirim e-postaları gönder (dk.):

Dakika cinsinden belirtilen aralığın ardından yeni bildirim, e-posta üzerinden gönderilir. Bu bildirimleri hemen göndermek istiyorsanız, değeri 0 olarak ayarlayın.

Her bildirimi ayrı bir e-posta olarak gönder

Etkinleştirildiğinde alıcı her bir bildirim için yeni bir e-posta alır. Bu, kısa bir sürede çok sayıda e-posta alınmasına neden olabilir.

İleti biçimi

Program ile uzak kullanıcı veya sistem yöneticisi arasındaki iletişimler, e-posta veya LAN iletileri aracılığıyla yapılır (Windows Messenger Service kullanılarak). Uyarı iletilerinin ve bildirimlerin varsayılan biçimi, pek çok durum için en uygun biçimdir. Bazı durumlarda olay iletilerinin ileti biçimini değiştirmeniz gerekebilir.

Olay iletilerinin biçimi

Uzak bilgisayarlarda görüntülenen olay iletilerinin biçimidir.

Tehdit uyarı iletilerinin biçimi

Tehdit uyarısı ve bildirim iletileri önceden tanımlı varsayılan bir biçime sahiptir. Bu biçimi değiştirmemenizi öneririz. Ancak bazı durumlarda (örneğin, otomatik e-posta işleme sisteminiz varsa), ileti biçimini değiştirmeniz gerekebilir.

İletideki anahtar sözcüklerin (% işaretiyle ayrılan dizeler) yerine, uyarıya özel gerçek bilgiler koyulur. Kullanılabilen anahtar sözcükler şunlardır:

- **%TimeStamp%** - Olayın tarihi ve saati.
- **%Scanner%** - İlgili modül.
- **%ComputerName%** - Uyarının oluştuğu bilgisayarın adı.
- **%ProgramName%** - Uyarıyı oluşturan program.
- **%InfectedObject%** - Etkilenen dosyanın, iletinin vs. adı.
- **%VirusName%** - Etkilenmenin tanımı.
- **%ErrorDescription%** - Virüs olmayan olayın açıklaması

%InfectedObject% ve **%VirusName%** anahtar sözcükleri yalnızca tehdit uyarısı iletilerinde kullanılır ve **%ErrorDescription%** yalnızca olay iletilerinde kullanılır.

Karakter kümesi

Açılır menüden kodlamayı seçebilirsiniz. E-posta mesajı seçilen karakter kodlamasına göre dönüştürülür.

Tırnaklı basılabilir (QP) şifrelemeyi kullan

E-posta iletisi kaynağı ASCII karakterlerini kullanan ve özel ulusal karakterleri e-posta yoluyla 8 bit biçiminde (áéíóú) düzgün bir şekilde iletebilen Tırnaklı Basılabilir (QP) biçiminde kodlanır.

Özelleştirme

Bu mesaj, seçilen tüm bildirimlerin alt bilgisinde gösterilir.

Varsayılan bildirim mesajı

Bildirim altbilgisinde gösterilecek varsayılan mesaj.

Tehditler

Kötü amaçlı yazılımları otomatik olarak kapatma

Siz manuel olarak kapatana kadar zararlı yazılım bildirimlerinin ekranda kalmasını sağlar.

Varsayılan mesajı kullan

Varsayılan iletiyi kapatıp bir tehdit engellendiğinde görüntülenecek özel **Tehdit bildirim iletisi** belirtebilirsiniz.

Tehdit bildirim mesajı

Bir tehdit engellendiğinde görüntülenecek özel bir mesaj girin.

Sunum modu

Sunum modu yazılımlarını kesintisiz olarak kullanabilmeyi talep eden, açılır pencerelerle rahatsız edilmek istemeyen ve CPU kullanımının en aza inmesini isteyen kullanıcılara yönelik bir özelliktir. Sunum modu ayrıca ESET Server Security etkinliği tarafından kesilmemesi gereken sunumlar sırasında da kullanılabilir. Etkinleştirildiğinde tüm açılır pencereler devre dışı bırakılır ve zamanlanan görevler çalıştırılmaz. Sistem koruması arka planda çalışmaya devam eder, ancak kullanıcı etkileşimi gerektirmez.

Uygulamalar tam ekran modunda çalıştırılırken Sunum modunu otomatik olarak etkinleştir

Tam ekran uygulaması çalıştırdığınız her sefer sunum modu otomatik olarak etkinleştirilir. Sunum modu etkinken bildirimleri veya ESET Server Security durum değişikliğini göremezsiniz.

Şu süre sonunda Sunum modunu otomatik olarak devre dışı bırak

Sunum modunun ne kadar zaman sonra otomatik olarak devre dışı bırakılacağını dakika olarak tanımlamak için kullanılır.

Tanılamalar

Tanılamalar, ESET işlemleri için uygulamanın kilitlendiği durumların dökümünü sağlar (örneğin: *ekrn*). Bir uygulama kilitlendiğinde döküm oluşturulur. Bu, geliştiricilerin hataları düzeltmesine ve çeşitli ESET Server Security sorunlarını gidermesine yardımcı olabilir.

Döküm türü öğesinin yanındaki açılır menüyü tıklayın ve mevcut üç seçenekten birini belirleyin:

- **Devre dışı bırak** - Bu özelliği devre dışı bırakmak için kullanılır.
- **Mini** - (varsayılan) Uygulamanın neden beklenmedik bir şekilde kilitlendiğini belirlemeye yardımcı olabilecek faydalı bilgilerin yer aldığı en küçük kümeyi kaydeder. Alan sınırlı olduğunda bu tür döküm faydalı olabilir. Ancak, dahil edilen bilgiler kısıtlı olduğundan bu dosya analiz edildiğinde, sorun oluştuğu sırada çalıştığı halde doğrudan tehdit nedeniyle oluşmayan hataların tespit edilmesi mümkün olmayabilir.
- **Tam** – Uygulama beklenmedik bir şekilde durduğunda sistem belleğinin tüm içeriklerini kaydeder. Tam bellek dökümü, bellek dökümü toplanırken çalışmakta olan tüm işlemler hakkında veri içerebilir.

Hedef dizin

Kilitlenme sırasında dökümün oluşturulacağı dizin.

Tanılamalar klasörünü aç

Yeni bir *Windows Explorer* penceresinde bu dizini açmak için **Aç**'ı tıklayın.

Tanılama dökümü oluştur

Hedef dizinde tanılama bilgi döküm dosyaları oluşturmak için **Oluştur**'u tıklayın.

Gelişmiş günlük kaydı

Aygıt denetimi gelişmiş günlük kaydını etkinleştir

Tanılama ve sorunları çözme işlemlerine izin vermek için Cihaz Kontrolü gerçekleşen tüm olayları kaydedin.

Kernel gelişmiş günlük kaydını etkinleştir

Tanılama ve sorunları çözme işlemlerine izin vermek için ESET kernel hizmetinde (`ekrn`) gerçekleşen tüm olayları kaydedin.

Lisans gelişmiş günlük kaydını etkinleştir

Lisans sunucusu ile tüm ürün iletişimlerini kaydet.

Ağ koruması gelişmiş günlük kaydını etkinleştir

Geliştiricilerin ağ koruması ile ilgili sorunları tespit edip onarmasına yardımcı olmak için ağ korumasından geçen tüm ağ verilerini PCAP biçiminde kaydeder.

İşletim sistemi gelişmiş günlük kaydını özelliğini etkinleştir

Çalışan işlemler, CPU etkinliği, disk işlemleri gibi İşletim sistemi ile ilgili ek bilgiler toplanır.

Protokol filtreleme gelişmiş günlük kaydını etkinleştir

Geliştiricilerin Protokol filtrelemesi ile ilgili sorunları tespit edip onarmasına yardımcı olmak için Protokol filtreleme altyapısından geçen tüm verileri PCAP biçiminde kaydeder.

Güncelleme altyapısı gelişmiş günlük kaydını etkinleştir

Geliştiricilerin Güncelleme altyapısıyla ilgili sorunları tespit edip gidermesine yardımcı olması için güncelleme işlemi sırasında gerçekleşen tüm olayları kaydedin.

Teknik destek

Sistem konfigürasyon verilerini gönder

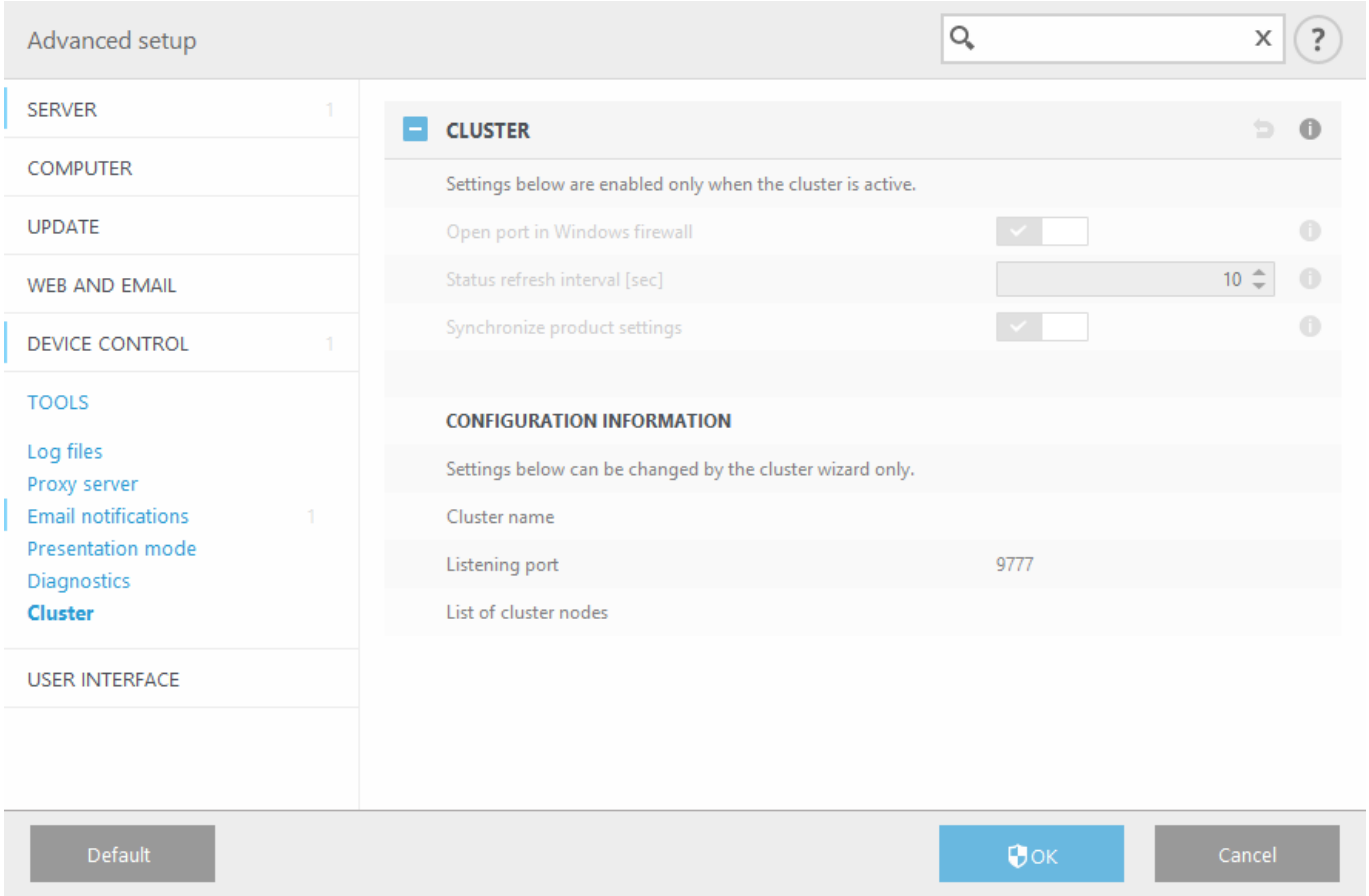
ESET Server Security yapılandırma verilerinizi müşteri destek birimine göndermeden önce soru sorulmaması için **Her zaman gönder** seçeneğini belirleyin veya **Göndermeden önce sor** seçeneğini kullanın.

Küme

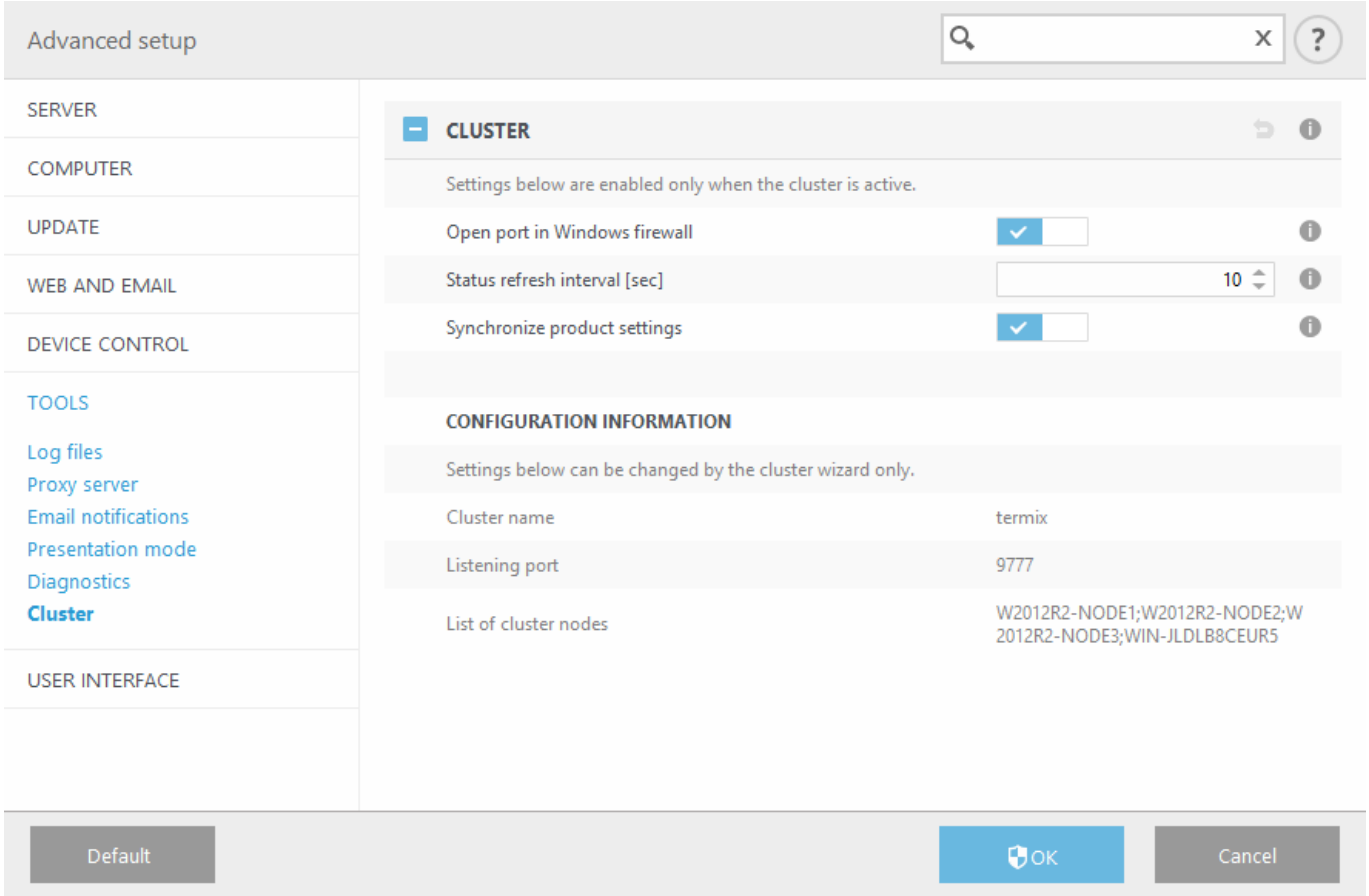
Kümeyi Etkinleştir seçeneği, ESET Kümesi yapılandırıldığında otomatik olarak etkinleştirilir. Bu seçeneği, **Gelişmiş ayarlar** (**F5**) penceresinde düğme simgesini tıklayarak manuel olarak devre dışı bırakabilirsiniz (örneğin, ESET Kümesi'ndeki diğer düğümleri etkilemeden yapılandırmayı değiştirmeniz gerektiğinde). Bu düğme, yalnızca ESET Kümesi işlevini etkinleştirir veya devre dışı bırakır. Kümeyi düzgün bir şekilde oluşturmak veya yok etmek için

Küme sihirbazını veya ana program penceresinde **Araçlar** > **Küme** bölümünde bulunan **Kümeyi yok et** seçeneğini kullanmak gerekir.

ESET kümesi yapılandırılmadı ve devre dışı bırakıldı:



ESET Kümesi ayrıntılarıyla ve seçenekleriyle birlikte düzgün bir şekilde yapılandırıldı:



Kullanıcı arabirimi

ESET Server Security Grafik kullanıcı arabirimi (GUI) davranışını yapılandırın. Programın görünümünü ve efektlerini ayarlayabilirsiniz.

Kullanıcı arabirimi öğeleri

Aşağıdaki Grafik kullanıcı arabirimi (GUI) başlatma modlarından seçim yapmak için GUI başlatma modu açılır menüsünü kullanın:

- **Tam** - Tam GUI görüntülenir.
- **Terminal** - Bildirim veya uyarı görüntülenmez. GUI, yalnızca Yönetici tarafından başlatılabilir. Grafik öğeleri bilgisayarınızın performansını yavaşlatıyorsa veya başka sorunlara neden oluyorsa, kullanıcı arabirimi Terminal olarak ayarlanmalıdır. Ayrıca Terminal sunucuda grafik kullanıcı arabirimini kapatmayı da düşünebilirsiniz. Terminal sunucuda yüklenen ESET Server Security hakkında daha fazla bilgi için Terminal Sunucuda GUI'yi devre dışı bırakma başlığına bakın.

Açılış ekranını başlangıçta göster

ESET Server Security uygulamanızın GUI'si başlatıldığında (örneğin sisteme giriş yaparken) açılır ekranın görüntülenmemesini tercih ediyorsanız bu seçeneği devre dışı bırakın.

Ses sinyali kullan

ESET Server Security, bir tarama sırasında önemli olaylar gerçekleştiğinde (örneğin, bir tehdit algılandığında

veya tarama sona erdiğinde) sesli uyarı verir.

İçerik menüsüne tümleştir

Etkinleştirildiğinde, ESET Server Security denetim öğeleri içerik menüsüne tümleştirilir. Bir nesne (dosya) sağ tıklandıktan sonra içerik menüsü görüntülenir. Menü, bir nesneyle ilgili gerçekleştirebileceğiniz tüm eylemleri listeler.

Uygulama durumları

İzleme penceresinde görüntülenen durumları seçmek için Düzenle'yi tıklayın. Alternatif olarak, uygulamanızın durumlarını yapılandırmak için ESET PROTECT ilkelerini kullanabilirsiniz. Uygulama durumu, ürününüz etkinleştirilmediğinde veya lisansınızın süresi dolduğunda da görüntülenir.

Lisans Bilgileri/Lisans bilgilerini göster

Etkinleştirildiğinde, lisansınızla ilgili iletiler ve bildirimler görüntülenir.

Uyarılar ve mesaj kutuları

Uyarılar ve bildirimler'i yapılandırarak, algılanan tehdit uyarılarının ve sistem bildirimlerinin davranışını değiştirebilirsiniz. Bu öğeler, ihtiyaçlarınıza uygun şekilde özelleştirilebilir. Bazı bildirimleri görüntülememeyi seçerseniz, bunlar Devre dışı bırakılmış iletiler ve durumlar alanında görüntülenir. Buradan durumlarını denetleyebilir, daha fazla ayrıntı görebilir veya pencereden kaldırabilirsiniz.

Erişim ayarları

Yüksek güvenlik düzeyini korumak için Erişim ayarları aracını kullanarak yetkisiz değişiklik yapılmasını önleyebilirsiniz.

ESET Shell

Ürün ayarları, özellikler ve verilere erişim haklarını, eShell üzerinden, ESET Shell yürütme ilkesi'ni değiştirerek yapılandırabilirsiniz.

Sistem tepsisi simgesi

Bu bölümdeki tüm ayarları geri al

Uyarılar ve mesaj kutuları

Tehdit uyarıları ve sistem bildirimlerini (başarılı güncelleme iletileri gibi) ESET Server Security tarafından nasıl işleneceğini yapılandırabilirsiniz. Örneğin, sistem tepsisi bildirimlerinin görüntülenme **Süresini** ve **Saydamlığını** ayarlayabilirsiniz (bu, yalnızca sistem tepsisi bildirimlerini destekleyen sistemlerde geçerlidir).

Etkileşimli uyarıları göster

Windows bildirim alanında ESET Server Security tarafından uyarı görüntülenmesini önlemek istiyorsanız, bu özelliği devre dışı bırakın.

Etkileşimli uyarıların listesi

Otomasyon için kullanışlıdır. Otomatikleştirmek istediğiniz öğeler için **Kullanıcıya sor** seçeneğinin işaretini kaldırın ve etkileşiminizi bekleyen uyarı penceresi yerine hangi eylemin gerçekleştirileceğini seçin.

Mesaj kutuları kısa metin mesajlarını veya soruları görüntülemek için kullanılır.

İleti kutularını otomatik olarak kapat

Açılan pencereleri belirli bir süre sonra otomatik olarak kapatmak içindir. El ile kapatılmazlarsa, belirtilen süre geçtikten sonra uyarı pencereleri otomatik olarak kapatılır.

Onay iletileri

Düzenle seçeneğini tıkladığınızda, bir eylem gerçekleştirilmeden önce ESET Server Security tarafından görüntülenen onay iletilerinin bir listesinin bulunduğu açılır pencere açılır. Onay iletilerine ilişkin tercihlerinizi özelleştirmek için onay kutularını kullanın.

Erişim ayarları

Sisteminizin maksimum güvenliği için ESET Server Security uygulamasının doğru yapılandırılması önemlidir. Yapılan herhangi yetkisiz bir değişiklik sorunlara ve hatta önemli verilerin kaybına yol açabilir. Yetkisiz değişiklikleri önlemek için ESET Server Security yapılandırma parolanızın korunmasını sağlayabilirsiniz.

ÖNEMLİ
Erişim ayarları parola koruması kullanırken ESET Server Security uygulamasını kaldırıyorsanız parolayı girmeniz istenir. Aksi takdirde ESET Server Security uygulamasını kaldıramazsınız.

Parola koruma ayarları

Programın ayar parametrelerini kilitler/kilidini kaldırır. **Parola ayarları** penceresini açmak için tıklayın.

Parola ayarlayın

Ayar parametrelerini korumak üzere bir parola belirlemek veya parolayı değiştirmek için **Ayarla**'yı tıklayın. Yetkisiz değişiklikleri engellemek için ESET Server Security ayar parametrelerini korumak üzere yeni bir parola ayarlanmalıdır. Var olan parolayı değiştirmek isterseniz eski parolanızı **Eski parola** alanına yazın, **Yeni parola** ve **Parolayı onayla** alanlarına yeni parolanızı girip **Tamam** seçeneğini tıklayın. ESET Server Security ürününde ileride gerekli olabilecek tüm değişiklikler için bu parola gerekecektir.

Sınırlı yönetici hesapları için tam yönetici hakları iste

Geçerli kullanıcıdan (yönetici haklarına sahip olmayan), koruma modüllerini devre dışı bırakma gibi belirli parametreleri değiştirirken yönetici hesabı kimlik bilgilerini girmesini istemek için bu seçeneği belirleyin.

NOT
Erişim ayarları parolası değiştirilirse ve mevcut *.xml* yapılandırma dosyasını (parola değişikliğinden önce imzalanmış olan dosyayı) ESET CMD komut satırını kullanarak içe aktarmak isterseniz, geçerli parolayı kullanarak dosyayı yeniden imzaladığınızdan emin olun. Bu, içe aktarma işleminden önce ESET Server Security çalıştırarak dosyayı başka bir makineye aktarmanıza gerek kalmadan, eski yapılandırma dosyasını kullanmanıza olanak sağlar.

ESET Shell

Ürün ayarları, özellikler ve verilere erişim haklarını, eShell üzerinden, **ESET Shell yürütme ilkesi**'ni değiştirerek yapılandırabilirsiniz. Varsayılan ayar **Sınırlı komut dosyası**'dır, ancak gerekirse bu ayarı Devre dışı, Salt okunur veya Tam erişim olarak değiştirebilirsiniz.

Devre dışı

eShell hiçbir şekilde kullanılamaz. Yalnızca eShell yapılandırmasının kendisine `ui eshell` bağlamında izin verilir. eShell görünümünü özelleştirebilirsiniz ancak ürün ayarlarına veya verilere erişemezsiniz.

Salt okunur

eShell izleme aracı olarak kullanılabilir. Tüm ayarları hem İnteraktif hem de Toplu modda görüntüleyebilirsiniz, ancak hiçbir ayar veya özelliği değiştiremez, veriler üzerinde değişiklik yapamazsınız.

Sınırlı komut dosyası

İnteraktif modda tüm ayarları, özellikleri ve verileri görüntüleyebilir ve değiştirebilirsiniz. Toplu modda, eShell Salt okunur mod kullanıyormuşsunuz gibi işlev gerçekleştirir, ancak imzalı toplu dosyalar kullanmanız halinde ayarları düzenleyebilir, verileri değiştirebilirsiniz.

Tam erişim

Tüm ayarlara erişim, hem İnteraktif modda hem de Toplu modda (toplu dosyaları çalıştırırken) sınırsızdır. Herhangi bir ayarı görüntüleyebilir ve değiştirebilirsiniz. eShell özelliğini tam erişimle çalıştırmak için bir yönetici hesabı kullanmalısınız. UAC etkinse yükseltme de gerekli olur.

Terminal Sunucuda GUI'yi devre dışı bırakma

Bu bölümde, kullanıcı oturumları için Windows Terminal Sunucusu'nda çalışan ESET Server Security GUI'sinin nasıl devre dışı bırakılacağı açıklanmaktadır.

Normal olarak, ESET Server Security GUI'si uzak kullanıcının sunucuya giriş yaptığı her seferinde başlatılır ve bir terminal oturum oluşturur. Bu, Terminal Sunucularda genelde istenmeyen bir durumdur. Terminal oturumları için GUI'yi kapatmak istiyorsanız bunu eShell üzerinden `set ui ui gui-start-mode none` komutunu çalıştırarak yapabilirsiniz. Bu, GUI'yi terminal moda geçirir. GUI başlatmak için kullanılabilen iki mod şu şekildedir:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

Hangi modun kullanılmakta olduğunu öğrenmek istiyorsanız, `get ui ui gui-start-mode` komutunu çalıştırın.

> NOT
> Citrix sunucusunda ESET Server Security yüklemişseniz, Bilgi Bankası makalemizde açıklanan ayarları kullanmanızı öneririz.

Devre dışı bırakılan iletiler ve durumlar

Onay iletileri

Görüntülenmesini veya görüntülenmemesini seçebileceğiniz onay iletileri listesini gösterir.

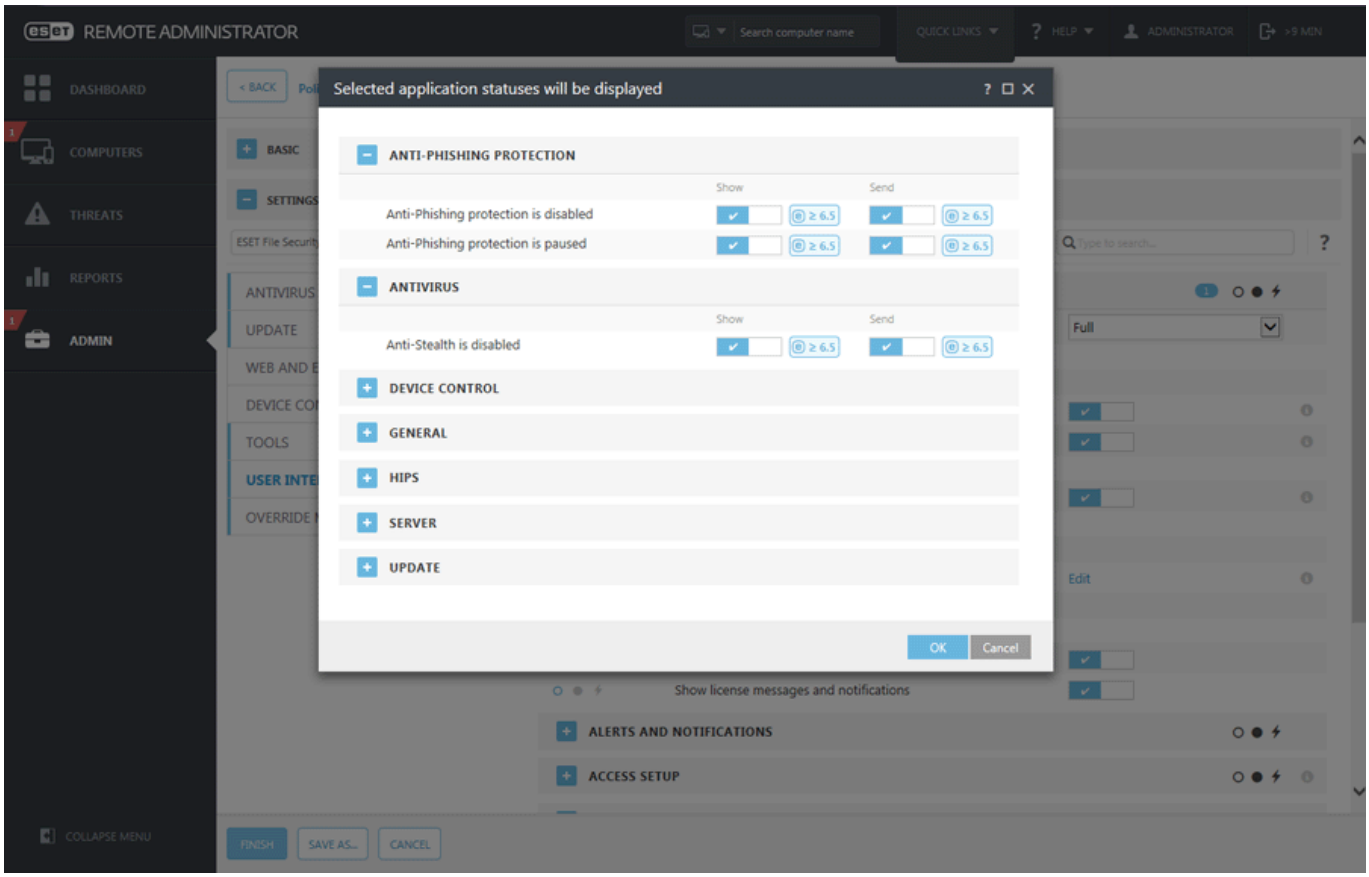
Uygulama durumları ayarları

Ana menüde İzleme sayfasında ekran durumunu etkinleştirmenizi veya devre dışı bırakmanızı sağlar.

Uygulama durumları ayarları

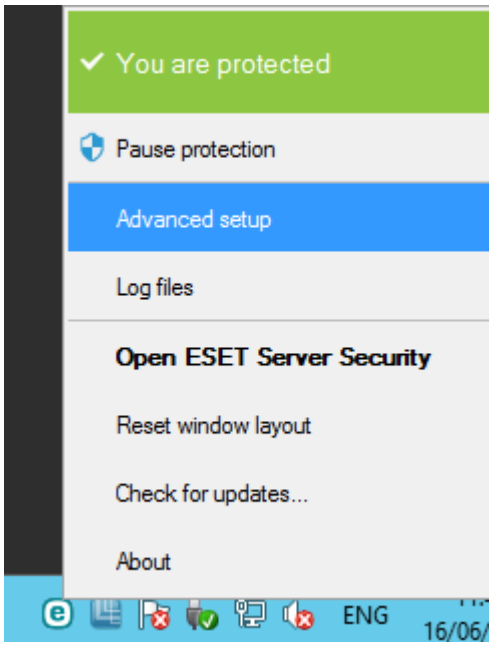
Bu iletişim kutusu, hangi uygulama durumlarının görünüp görünmeyeceğini seçmenize veya durumları kaldırmanıza olanak sağlar. Örneğin, Antivirus ve antispyware korumasını duraklattığınızda, bir koruma durumu değişikliği ortaya çıkar ve bu değişiklik İzleme sayfasında görünür. Uygulama durumu, ürününüz etkinleştirilmediğinde veya lisansınızın süresi dolduğunda da görüntülenir.

Uygulama durumları, ESET PROTECT ilkeleri üzerinden yönetilebilir. Kategori ve durumlar, Durumu **göster** ve **gönder** şeklinde iki seçenekle bir listede gösterilir. Uygulama durumları için Gönder sütunu, yalnızca ESET PROTECT ilke yapılandırması durumunda görünür. ESET Server Security kilit simgesine sahip ayarları gösterir. Uygulama durumlarını geçici olarak değiştirmek için Modu geçersiz kıl seçeneğini kullanabilirsiniz.



Sistem tepsisi simgesi

ESET Server Security uygulamasının sıklıkla kullanılan öğelerine ve özelliklere hızlı erişim hizmeti verir. Bunlar, sistem tepsisi simgesi sağ tıklanarak kullanılabilir.



Daha fazla bilgi

Geçerli koruma durumunu ve iletilerini göstermek için İzleme sayfasını açar.

Korumayı duraklat

Antivirus ve antispyware koruması ifadesini görüntüleyen onay iletişim kutusu görüntülenir. Bu koruma dosya, web ve posta iletişimini denetleyerek saldırılara karşı koruma sağlar. sistem tepsisi simgesini kullanarak Antivirus ve antispyware korumasını geçici olarak duraklattığınızda, **Korumayı duraklat** iletişim kutusu görüntülenir. Bu işlem, belirtilen süre boyunca zararlı yazılımla ilgili korumayı devre dışı bırakır. Korumayı kalıcı olarak devre dışı bırakmak için **Gelişmiş ayarlar**'ı kullanabilirsiniz. Korumayı devre dışı bırakırken dikkatli olun, sisteminiz tehditlere maruz kalabilir.

Gelişmiş ayarlar'da farklı güncelleme profillerini

Gelişmiş ayarlar'ı girmek için bu seçeneği kullanın.

Günlük dosyaları

Meydana gelen tüm önemli program olayları hakkında bilgi içerir ve algılanan tehditlere ilişkin genel bakış sağlar.

ESET Server Security Ürününü gizle

Ekrandan ESET Server Security penceresini gizleyin.

Pencere düzenini sıfırla

ESET Server Security penceresini ekran üzerindeki varsayılan boyutuna ve konumuna sıfırlar.

Güncellemeleri denetle

Kötü amaçlı koda karşı koruma düzeyini sürdürmek üzere modül güncellemesini başlatır.

Hakkında

Sistem bilgileri, ESET Server Security ürününün yüklenen sürümü ve yüklenen program modülleri hakkında ayrıntıların yanı sıra lisansınızın sona erme tarihi hakkında bilgiler sağlar. İşletim sisteminiz ve sistem kaynaklarınız hakkındaki bilgileri sayfanın alt bölümünde bulabilirsiniz.

Varsayılan ayarlara döndür

Ayarları, **Gelişmiş ayarlar** bölümünde varsayılan değerlerine geri yükleyebilirsiniz. İki seçenek vardır. Tüm ayarları varsayılana döndürebilir veya yalnızca belirli bir bölümün ayarlarını döndürebilirsiniz (diğer bölümlerdeki ayarlar değişmez).

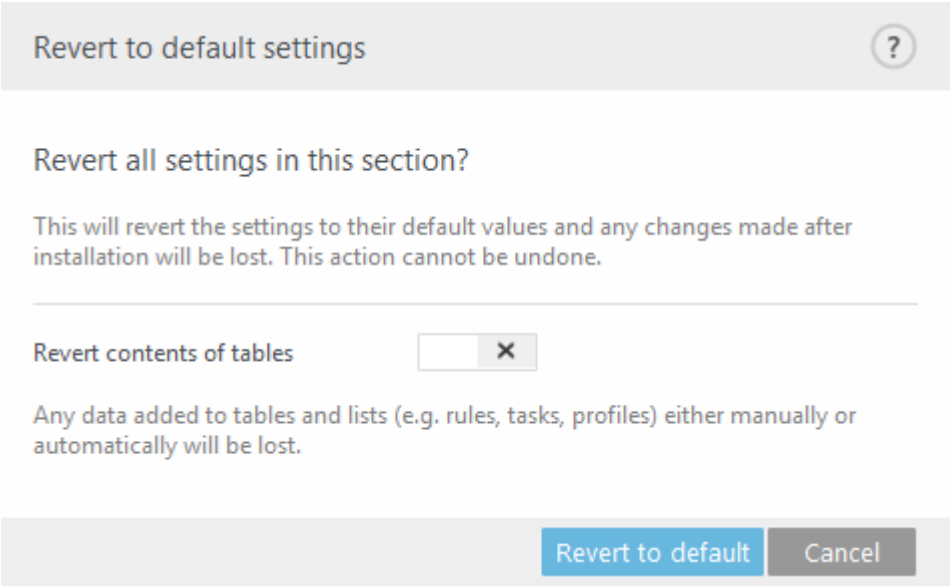
Tüm ayarları döndür

Gelişmiş ayarların tüm bölümlerindeki ayarların tamamı, ESET Server Security ürününü yüklemenizin ardından önceden oldukları duruma geri yüklenirler. Bunu *Fabrika Varsayılanlarını Geri Yükleme* olarak düşünebilirsiniz.

NOT
Varsayılana döndür seçeneğini tıkladıktan sonra, yapılmış olan tüm değişiklikler kaybolur. Bu eylem geri alınamaz.

Bu bölümdeki tüm ayarları geri al

Seçili bölümdeki modül ayarlarını varsayılan değerlere döndürür. Bu bölümde yaptığınız tüm değişiklikler kaybolur.



Tabloların içeriklerini döndür

Etkinleştirildiğinde, manuel veya otomatik olarak eklenmiş kurallar, görevler veya profiller kaybolur.

Yardım ve destek

ESET Server Security, karşılaşabileceğiniz sorunları çözmede size yardımcı olacak sorun giderme araçlarını ve destek bilgilerini içerir.

Yardım

ESET Bilgi Bankası'nda arayın

ESET Bilgi Bankası, en sık sorulan soruların yanıtlarının yanı sıra, çeşitli konular için önerilen çözümleri içerir. ESET teknik uzmanları tarafından düzenli olarak güncellenen Bilgi Bankası, çeşitli türlerde sorunları gidermek için kullanılabilecek en güçlü araçtır.

Yardımı aç

ESET Server Security için çevrimiçi yardım sayfalarını açar.

Hızlı çözüm bulun

En sık karşılaşılan sorunlara çözüm bulmak için bu seçeneği belirleyin. Teknik destek ile iletişim kurmadan önce bu bölümü okumanızı öneririz.

Teknik destek

Destek isteği gönderin

Sorununuza yanıt bulamıyorsanız Teknik Destek bölümümüzle hızlı bir şekilde iletişim kurabilmek için ESET web sitesindeki bu formu da kullanabilirsiniz.

Teknik Destek Ayrıntıları

Teknik Destek ile ilgili ayrıntılı bilgiler (Ürün adı, Ürün sürümü vb.) görüntüler.

Destek Araçları

Tehdit ansiklopedisi

Farklı sızıntı türlerinin tehlikeleri ve belirtileri ile ilgili bilgiler içeren ESET Tehdit Ansiklopedisi'ne bağlantı sağlar.

ESET Log Collector

ESET Log Collectorindirme sayfasına bağlantı sağlar. ESET Log Collector, sorunların daha hızlı çözülmesine yardımcı olmak için sunucunuzdan yapılandırma ve günlükler gibi bilgileri otomatik olarak toplayan bir uygulamadır.

Algılama Altyapısı geçmişi

ESET algılama modüllerinin sürümleri hakkında bilgiler içeren ESET Virus radarına bağlanır.

ESET Specialized Cleaner

ESET Özelleştirilmiş Temizleyici; genel zararlı yazılım etkilenmelerine yönelik, Conficker, Sirefef veya Necurs

gibi bir kaldırma aracıdır.

Ürün ve Lisans bilgileri

Ürünü etkinleştir / Lisansı değiştir

Ürün etkinleştirme penceresini açmak için bunu tıklayın. ESET Server Security ürününü etkinleştirmek için kullanılabilir yöntemlerden birini seçin.

ESET Server Security Hakkında

ESET Server Security ürününüzün kopyası hakkındaki bilgileri görüntüler.

Destek isteği gönderme

ESET, mümkün olduğu kadar hızlı ve doğru bir şekilde destek sağlamak amacıyla, ESET Server Security yapılandırmanız hakkındaki bilgilere, ayrıntılı sistem bilgilerine ve çalışan işlemlere (ESET SysInspector günlük dosyası) ve kayıt defteri verilerine ihtiyaç duyar. ESET, bu verileri yalnızca müşteriye teknik destek sağlamak amacıyla kullanır. Bu ayar **Gelişmiş ayarlar** (**F5**) > **Araçlar** > **Tanılamalar** > **Teknik Destek** bölümünden de yapılandırılabilir.

> NOT
> Sistem verilerini göndermeye karar verdiyseniz, web formunu doldurup göndermeniz gerekir, aksi takdirde biletiniz oluşturulmaz ve sistem verileriniz kaybolur.

Web formunu ilettiğinizde sistem yapılandırma verileriniz ESET'e gönderilir. Bu işlem için bu eylemin hatırlanmasını istiyorsanız **Bu bilgileri her zaman gönder** öğesini seçin.

Verileri gönderme

Verileri göndermek istemiyorsanız bu seçeneği kullanın. ESET Teknik Destek web sayfasına yönlendirilirsiniz.

ESET Server Security Hakkında

Bu pencere, ESET Server Security ürününün yüklenmiş olan sürümü hakkındaki ayrıntıları sağlar. Pencerenin üst tarafında işletim sisteminiz ve sistem kaynaklarıyla ilgili bilgilerin yanı sıra halihazırda giriş yapmış olan kullanıcı ile bilgisayarın tam adı yer alır.

Yüklü bileşenler

Yüklenen bileşenlerin ve ayrıntılarının bir listesini görüntülemek için modüller hakkında bilgiler içerir. Listeyi panonuza kopyalamak için **Kopyala** seçeneğini tıklayın. Bu özellik Teknik Destek birimiyle iletişim kurarken veya sorun giderme sırasında faydalı olabilir.

Sözlük

Teknik terimler, tehditler ve internet güvenliği hakkında daha fazla bilgi için Sözlük sayfasını ziyaret edin.

Son Kullanıcı Lisans Sözleşmesi

ÖNEMLİ: İndirme, yükleme, kopyalama veya kullanmadan önce, lütfen bu ürüne ilişkin aşağıdaki hükümleri dikkatlice okuyun. **YAZILIMI İNDİREREK, YÜKLEYEREK, KOPYALAYARAK VEYA KULLANARAK BU HÜKÜM VE KOŞULLARI ONAYLADIĞINIZI VE ŞUNU KABUL EDERSİNİZ GİZLİLİK POLİTİKASI.**

Son Kullanıcı Lisans Sözleşmesi

Einsteinova 24, 85101 Bratislava, Slovak Republic Cumhuriyeti adresinde mukim ve Bratislava I. Bölge Mahkemesinin Ticari Sicil Kaydında Bölüm Sro, Giriş No 3586/B, İşyeri Sicil Numarası: 31333532 olarak kayıtlı ESET, spol. s r. o. (buradan sonra "ESET" veya "Sağlayıcı" olarak anılacaktır) tarafından ve fiziksel veya tüzel bir kişi olan siz (buradan sonra "Siz" ya da "Son Kullanıcı" olarak anılacaktır) arasında yapılan bu Son Kullanıcı Lisans Sözleşmesi (buradan sonra "Sözleşme" olarak anılacaktır) koşullarına göre, Size bu Sözleşmenin 1. Maddesinde tanımlanan Yazılımı kullanım hakkı tanınır. Bu Sözleşmenin 1. Maddesinde tanımlanan Yazılım bir veri taşıyıcısında saklanabilir, elektronik posta üzerinden gönderilebilir, İnternet üzerinden yüklenebilir, Sağlayıcının sunucularından yüklenebilir ya da aşağıda ifade edilen hüküm ve koşullara bağlı olarak diğer kaynaklardan elde edilebilir.

BU BİR SATIN ALMA SÖZLEŞMESİ DEĞİL, SON KULLANICI HAKLARI İLE İLGİLİ BİR SÖZLEŞMEDİR. Sağlayıcı ticari ambalajda bulunan Yazılım kopyası ile fiziksel ortamın ve Son Kullanıcının bu Sözleşme uyarınca oluşturmaya hak kazandığı diğer tüm kopyaların sahibi olarak kalır.

Yazılımı yüklerken, indirirken, kopyalarken veya kullanırken "Kabul Ediyorum" veya "Kabul Ediyorum…" düğmesini tıkladığınız zaman, bu Sözleşmenin hükümlerini ve koşullarını kabul etmiş olursunuz. Bu Sözleşmedeki tüm hükümleri ve koşulları kabul etmiyorsanız, hemen "Kabul Etmiyorum" düğmesini tıklayın; yükleme ya da indirme işlemini iptal edin veya Yazılım, yükleme ortamı, birlikte gelen belgeler ve satın alma makbuzunu yok edin ya da Sağlayıcıya veya Yazılımı edindiğiniz satış yerine iade edin.

YAZILIMI KULLANMANIZIN, BU SÖZLEŞMEYİ OKUDUĞUNUZ, ANLADIĞINIZ VE HÜKÜMLERİNE VE KOŞULLARINA TABİ OLMAYI KABUL ETTİĞİNİZ ANLAMINA GELDİĞİNİ KABUL ETMİŞ SAYILIRSINIZ.

1. **Yazılım.** Bu Sözleşmede kullanıldığı şekliyle "Yazılım" şu anlama gelmektedir: (i) bu Sözleşme ile birlikte sağlanan bilgisayar programı ve ilgili tüm bileşenleri; (ii) disklerin, CD-ROM'ların, DVD'lerin, e-postaların ve tüm eklerin veya veri taşıyıcısında, elektronik postayla veya İnternet üzerinden indirilmek üzere sağlanan Yazılımın nesne kodu biçimi de dahil olmak üzere, beraberinde bu Sözleşmenin sağlandığı diğer medyaların içerikleri; (iii) ilgili tüm açıklayıcı yazılı malzeme ve Yazılımla ilgili olası tüm Dokümantasyon ve Yazılımla ilgili tüm açıklamalar, Yazılımın teknik özellikleri, Yazılım özellikleri veya çalışması ile ilgili açıklamalar, Yazılımın kullanıldığı işletim ortamıyla ilgili tüm açıklamalar, Yazılımın kullanımı veya yüklenmesi ile ilgili tüm talimatlar veya Yazılımın nasıl kullanılacağına ilişkin tüm açıklamalar (buradan sonra "Dokümantasyon" olarak anılır); (iv) Yazılımın kopyaları, Yazılımda olabilecek hatalar için yamalar, Yazılıma ekler, Yazılımın uzantıları, varsa Yazılımın değiştirilen sürümleri ve Yazılım bileşenlerinin güncellemeleri. Maddesi uyarınca size Lisans hakkını tanıdığı Yazılım bileşenleri güncellemelerini içerir. Yazılım yalnızca yürütülebilir nesne kodu biçiminde sağlanır.

2. **Yükleme, Bilgisayar ve Lisans anahtarı**. Veri taşıyıcısında sağlanan, elektronik posta ile gönderilen, internetten indirilen, Sağlayıcının sunucularından indirilen veya başka kaynaklardan elde edilen Yazılım yükleme işlemi gerektirir. Yazılımı en azından Belgeler'de belirtilen gereksinimleri karşılayan doğru şekilde yapılandırılmış bir Bilgisayara yüklemeniz gerekir. Yükleme yöntemi Belgeler'de açıklanmaktadır. Yazılım üzerinde ters bir etki yapabilecek hiçbir bilgisayar programı veya donanım, Yazılımı yüklediğiniz bilgisayara yüklenemez. Bilgisayar; kişisel bilgisayarlar, dizüstü bilgisayarlar, iş istasyonları, avuç içi bilgisayarlar, akıllı telefonlar, elektronik el cihazları veya Yazılımın tasarlanmış olduğu ve yükleneceği, kurulacağı ve/veya kullanılacağı diğer elektronik cihazlar dahil ancak bunlarla sınırlı olmamak üzere donanım anlamına gelmektedir. Lisans anahtarı Yazılımın yasal kullanımına, spesifik sürümüne veya Lisans süresinin uzatılmasına bu Sözleşmeye uygun şekilde izin vermek için Son Kullanıcıya

sağlanan benzersiz dizi veya sembol, harf, sayı ya da özel işaretler anlamına gelir.

3. **Lisans**. Bu Sözleşmenin hükümlerini kabul etmeniz ve burada belirtilen tüm hükümlere ve koşullara uymanız durumunda, Sağlayıcı size aşağıdaki hakları (buradan sonra "Lisans" olarak anılacaktır) sağlar:

a) **Yükleme ve kullanım.** Yazılımı bir bilgisayarın sabit sürücüsüne veya veri depolama için benzer bir kalıcı ortama yüklemek, Yazılımı bir bilgisayar sisteminin belleğine yüklemek ve depolamak ve Yazılımı uygulamak, depolamak ve görüntülemek için münhasır olmayan ve devredilemeyen bir hakka sahip olursunuz.

b) **Lisans sayısı koşulu.** Yazılımı kullanma hakkı, Son Kullanıcı sayısına bağlıdır. Bir Son Kullanıcı şunları ifade eder: (i) bir bilgisayar sistemindeki Yazılım kurulumu veya (ii) bir lisansın kapsamı posta kutusu sayısıyla sınırlıysa, tek Son Kullanıcı bir Posta Kullanıcı Aracısı (“PKA”) üzerinden elektronik posta alan bir bilgisayar kullanıcısını ifade eder. PKA elektronik postayı kabul eder ve ardından otomatik olarak birçok kullanıcıya gönderirse, Son Kullanıcı sayısı elektronik postanın dağıtıldığı gerçek kullanıcı sayısına göre belirlenir. Bir posta sunucusu bir posta geçidinin işlevini gerçekleştiriyorsa, Son Kullanıcı sayısı söz konusu geçidin hizmet verdiği posta sunucusu kullanıcılarının sayısına eşit olur. Belirli olmayan bir sayıda elektronik posta adresi tek bir kullanıcıya yönlendirilir ve tek bir kullanıcı tarafından kabul edilirse (ör. öteki adlar yoluyla) ve postalar istemci tarafından daha fazla sayıda kullanıcıya otomatik olarak dağıtılmıyorsa, Lisans tek bir bilgisayar için gereklidir. Bir Lisansı aynı anda birden fazla bilgisayarda kullanmamalısınız. Son Kullanıcı, Sağlayıcı tarafından verilen Lisansların sayısından doğan sınırlamaya uygun olarak Yazılımı kullanma hakkına sahip olunan ölçüye kadar Yazılıma Lisans Anahtarı girmekle yükümlüdür. Lisans Anahtarının gizli olduğu kabul edilir. Lisansı üçüncü taraflarla paylaşamaz veya bu Sözleşme ya da Sağlayıcı tarafından izin verilmediği sürece Lisans anahtarını kullanması için üçüncü taraflara izin veremezsiniz. Lisans anahtarınız tehlikeye girerse Sağlayıcıyı hemen bilgilendirin.

c) **Kurumsal Sürüm.** Yazılımın posta sunucularında, posta geçişlerinde, posta ağ geçitlerinde veya İnternet ağ geçitlerinde kullanılması için, bir Kurumsal Sürümünün edinilmesi gerekir.

d) **Lisans Hükmü.** Yazılımı kullanma hakkınız zamanla sınırlıdır.

e) **OEM Yazılımı.** OEM Yazılımı, yalnızca Yazılımı kullanmaya başladığınız bilgisayarla sınırlıdır. Başka bir bilgisayara aktarılamaz.

f) **SO, DENEME Yazılımı.** "Satılık Olmayan", SO veya DENEME olarak sınıflandırılan Yazılım ücretle satılamaz ve sadece Yazılımın özelliklerinin tanıtılması veya test edilmesi için kullanılmalıdır.

g) **Lisansın Sonlandırılması.** Lisans, kullanımı için verilen sürenin sonunda otomatik olarak sonlandırılır. Bu Sözleşmedeki hükümlerden herhangi birine uymamanız durumunda Sağlayıcı, bu gibi bir koşulda Sağlayıcı için geçerli olan herhangi bir yetkiye veya yasal çözüme halel gelmeksizin Sözleşmeden çekilme hakkına sahiptir. Lisansın iptal edilmesi durumunda, Yazılımı ve yedeklenmiş tüm kopyalarını derhal silmeniz, yok etmeniz ya da ESET’e veya Yazılımı edindiğiniz satış yerine masrafları size ait olmak üzere iade etmeniz gerekir. Lisansın sonlandırılması durumunda, Sağlayıcı, Son Kullanıcının Yazılım işlevlerini kullanma yetkisini iptal etme hakkına sahiptir ve bu iptal işlemi, Sağlayıcının sunucularına veya üçüncü taraf sunucularına bağlantı gerektirir.

4. **Veri toplama işlevleri ve internet bağlantısı gereksinimleri.** Yazılımı düzgün şekilde kullanmak, İnternet bağlantısı gerektirir ve düzenli aralıklarla Sağlayıcının sunucularına veya üçüncü taraf sunucularına ve Gizlilik Politikasına uygun olarak geçerli veri toplama işleminin yapılması gerekir. İnternete bağlanmak ve geçerli veri toplama Yazılımın şu işlevleri için gereklidir:

a) **Yazılım Güncellemeleri.** Sağlayıcı zaman zaman Yazılım için güncellemeler yayımlama hakkına sahiptir ("Güncellemeler") ancak Güncellemeler yayımlamakla yükümlü değildir. Bu işlev Yazılımın standart ayarlarında etkinleştirilmiştir ve bu nedenle Son Kullanıcı Güncellemelerin otomatik olarak yüklenmesini devre dışı bırakmadığı sürece, Güncellemeler otomatik olarak yüklenirler. Güncellemelerin gerçekleştirilmesi amacına yönelik olarak, Bilgisayar ve/veya Yazılımın yüklendiği platformla ilgili bilgiler dahil olmak üzere, Gizlilik Politikasına

uygun olarak bir Lisans kimlik doğrulama işlemi gereklidir.

b) **İzinsiz girişlerin ve bilgilerin Sağlayıcıya iletilmesi**. Yazılım; bilgisayar virüslerinin ve diğer kötü amaçlı bilgisayar programlarının ve dosyalar, URL'ler, IP paketleri ve ethernet çerçeveleri gibi şüpheli, sorunlu, istenmeyen türden olabilecek veya tehlikeli olabilecek nesnelerin (bundan sonra "Sızıntılar" olarak anılacaktır) örneklerini toplayan işlevler içerir; bu işlevler söz konusu sızıntıları yükleme süreci, bilgisayar ve/veya Yazılımın yüklendiği platform hakkındaki bilgiler ile Yazılımın işlemleri ve işlevleri hakkındaki bilgiler de dahil, ancak bunlarla sınırlı olmamak üzere (bundan sonra "Bilgiler" olarak anılır) Sağlayıcıya gönderilir. Bilgiler ve Sızıntılar Son Kullanıcı veya Yazılımın yüklü olduğu bilgisayarın diğer kullanıcıları hakkında veriler (tesadüfen veya yanlışlıkla elde edilen kişisel bilgiler de dahil) ve ilişkili meta verilere sahip Sızıntılardan etkilenen dosyaları içerebilir.

Bilgiler ve Sızıntılar Yazılımın şu işlevleri tarafından toplanabilir:

i. LiveGrid Saygınlık Sistemi işlevi Sızıntılarla ilişkili tek yönlü karmaların toplanmasını ve Sağlayıcıya gönderilmesini içerir. Bu işlev, Yazılımın standart ayarları altında etkinleştirilmiştir.

ii. LiveGrid Geri Bildirim Sistemi işlevi, Sızıntıların toplanmasını ve ilişkilendirilen meta veriler ve Bilgiler ile birlikte Sağlayıcıya gönderilmesini içerir. Bu işlev, Yazılımı yükleme esnasında Son Kullanıcı tarafından etkinleştirilebilir.

Sağlayıcı alınan Bilgileri ve Sızıntıları yalnızca Sızıntıların analizi ve araştırılması, Yazılımın ve Lisans kimlik doğrulamasının iyileştirilmesi amaçlarına yönelik olarak kullanacaktır ve alınan Sızıntıların ve Bilgilerin güvende kalmasını sağlamak için uygun olan önlemleri alacaktır. Yazılımın bu işlevini etkinleştirdiğinizde, Sızıntılar ve Bilgiler Sağlayıcı tarafından, Gizlilik Politikasında belirtildiği şekilde ve ilgili yasal düzenlemelere uygun olarak toplanabilir ve işlenebilir. Bu işlevleri dilediğiniz zaman devre dışı bırakabilirsiniz.

Bu Sözleşmenin amacına uygun olarak, Sağlayıcının Sizi Gizlilik Politikasına uygun olarak tanımlamasına olanak tanıyan verileri toplamak, işlemek ve depolamak gerekir. Sağlayıcının kendi araçlarını kullanarak Yazılımın Sizin tarafınızdan bu Sözleşmenin şartlarına uygun şekilde kullanılıp kullanılmadığını kontrol edeceğini burada kabul edersiniz. Bu Sözleşmenin amacına uygun olarak verilerinizin Yazılım ve Sağlayıcının bilgisayar sistemleri arasındaki iletişim esnasında aktarılması gerektiğini ve Yazılımın işlevinin sağlanması için ağa destek ve Yazılımı kullanmak ve Sağlayıcının haklarının korunması için yetki vermek gerektiğini kabul edersiniz.

Bu Sözleşmenin neticelendirilmesinin ardından, Sağlayıcı veya Sağlayıcının dağıtım ve destek ağının parçası olarak herhangi bir iş ortağı, faturalandırma amaçlı olarak veya bu Sözleşmenin uygulanması amacıyla Sizi tanımlamak için gerekli olan verileri aktarma, işleme ve depolama hakkına sahip olur. Pazarlama bilgileri de dahil ancak bunlarla sınırlı olmamak üzere bildirim ve iletileri almayı kabul edersiniz.

Gizlilik, kişisel veri koruması ve veri öznesi olarak Sizin Haklarınız hakkındaki detaylar, Sağlayıcının web sitesinde yer alan ve yükleme işleminden doğrudan erişilebilen Gizlilik Politikasında bulunabilir. Ayrıca Yazılımın yardım bölümünden de ziyaret edebilirsiniz.

5. **Son Kullanıcı haklarının kullanılması**. Son Kullanıcı haklarını bizzat veya çalışanlarınız yoluyla kullanmalısınız. Yazılımı yalnızca işlemlerinizi güvence altına almak ve Lisansı aldığınız Bilgisayarlar veya bilgisayar sistemlerine koruma sağlamak için kullanma hakkına sahipsiniz.

6. **Hakların kısıtlanması.** Yazılımı kopyalayamaz, dağıtamaz, bileşenlerine ayıramaz veya türetilmiş sürümlerini oluşturamazsınız. Yazılımı kullanırken aşağıdaki kısıtlamalara uymanız gerekmektedir:

a) Arşivlenen yedek kopyanızın başka bir bilgisayara yüklenmemesi veya başka bir bilgisayarda kullanılmaması kaydıyla, arşiv amaçlı olarak kalıcı bir saklama ortamına Yazılımın bir kopyasını kaydedebilirsiniz. Oluşturacağınız diğer her türlü kopya, bu Sözleşmeyi ihlal eder.

b) Bu Sözleşmede ifade edilen yolların dışında, Yazılımı kullanamaz, değiştiremez, çeviremez, çoğaltamaz ya da

Yazılımın veya Yazılımın kopyalarını kullanım haklarını aktaramazsınız.

c) Yazılımı satamaz, alt lisansını veremez, kiralayamaz, ödünç veremez veya ödünç alamaz ya da ticari hizmet sağlamak için kullanamazsınız.

d) Bu kısıtlamanın yasalarla açık bir şekilde yasaklandığı durumlar haricinde, Yazılımda ters mühendislik uygulayamaz, geri derleme yapamaz, Yazılımın derlemesini açamaz ya da başka bir şekilde kaynak kodunu bulmaya çalışamazsınız.

e) Yazılımı, yalnızca Yazılımı kullandığınız yerde geçerli olan yargı alanının, telif hakkı ve diğer fikri mülkiyet haklarıyla ilgili geçerli kısıtlamalar dahil ancak bunlarla sınırlı olmamak kaydıyla, tüm geçerli yasalarıyla uyumlu bir yolla kullanacağınızı kabul etmiş olursunuz.

f) Yazılımı ve işlevlerini, yalnızca diğer Son Kullanıcıların bu hizmetlere erişim olanaklarını sınırlamayacak şekilde kullanacağınızı kabul edersiniz. Sağlayıcı, hizmetlerin mümkün olan en çok sayıda Son Kullanıcı tarafından kullanılmasını sağlamak üzere, Son Kullanıcılara ayrı ayrı sağlanan hizmetlerin kapsamını sınırlama hakkını saklı tutar. Hizmetlerin kapsamının sınırlanması aynı zamanda, Yazılım işlevlerinden herhangi birinin kullanılma olasılığının tamamen sonlandırılması ve Sağlayıcının sunucularındaki ya da üçüncü şahıs sunucularındaki Yazılımın belirli bir işleviyle ilgili Verilerin ve bilgilerin silinmesi anlamına da gelir.

g) Lisans anahtarının kullanımını içeren, bu Sözleşmenin şartlarına aykırı olan veya Yazılımı kullanma yetkisi olmayan herhangi bir kişiye Lisans anahtarı sağlamaya yol açan, kullanılan ya da kullanılmayan Lisans anahtarını herhangi bir biçimde aktarma, yetkisiz yeniden üretme ya da çoğaltılan veya oluşturulan Lisans anahtarlarını dağıtma ya da Yazılımı Sağlayıcı dışında bir kaynaktan elde edilen Lisans anahtarının kullanımının sonucu olarak kullanma gibi hiçbir faaliyette bulunmayacağınızı kabul edersiniz.

7. **Telif Hakkı**. Yazılım ve mülkiyet hakları ve fikri mülkiyet hakları dahil ancak bunlarla sınırlı kalmamak kaydıyla Yazılımın tüm hakları ESET ve/veya onun adına lisans veren taraflara aittir. ESET ve/veya lisans veren taraflar uluslararası anlaşma hükümleri ve Yazılımın kullanıldığı ülkedeki ilgili tüm diğer ulusal yasalar tarafından korunur. Yazılımın yapısı, düzeni ve kodu ESET'e ve/veya onun adına lisans veren taraflara ait değerli ticari sırlarıdır ve gizli bilgilerdir. 6(a) Maddesi altında belirtilen durumlar dışında Yazılımı kopyalayamazsınız. Bu Sözleşme kapsamında oluşturma hakkınızın olduğu tüm kopyaların Yazılımda bulunan telif hakkı ve diğer mülkiyet hakkı bildirimlerini içermesi gerekir. Bu Sözleşmenin hükümlerini ihlal edecek şekilde Yazılıma ters mühendislik uygulamanız, geri derleme yapmanız, Yazılımın derlemesini açmanız ya da başka bir şekilde kaynak kodunu bulmaya çalışmanız halinde, bu şekilde elde edilen her türlü bilginin ortaya çıktığı andan itibaren, Sağlayıcının bu Sözleşmenin ihlaline dair haklarından bağımsız olarak, otomatik olarak ve geri alınamaz şekilde tamamen Sağlayıcıya devredilmiş ve Sağlayıcıya ait sayılacağını kabul etmiş olursunuz.

8. **Hakların saklı tutulması**. Sağlayıcı, bu Sözleşme hükümleri kapsamında Yazılımın Son Kullanıcısı olarak Size açıkça verilen hakların dışında, Yazılıma dair tüm haklarını saklı tutar.

9. **Çoklu dil sürümleri, çift ortamlı yazılım, çoklu kopyalar**. Yazılımın birden fazla platformu veya dili desteklemesi durumunda veya Yazılımın birden fazla kopyasını edinmişseniz, Yazılımı yalnızca Lisansını aldığınız sayıda bilgisayar sistemi ve sürümü için kullanabilirsiniz. Kullanmadığınız Yazılım sürümlerini veya kopyalarını satamaz, kiralayamaz, finansal kiralama yoluyla veremez, alt lisansını veremez, ödünç veremez ya da aktaramazsınız.

10. **Sözleşmenin başlangıcı ve sonlandırılması**. Bu Sözleşme, Sözleşmenin hükümlerini kabul ettiğiniz andan itibaren geçerli olur. Yazılımı, tüm yedeklenmiş kopyalarını ve Sağlayıcı veya iş ortakları tarafından sağlanan tüm ilgili malzemeleri kalıcı olarak silerek, yok ederek ve masrafları size ait olmak üzere geri yollayarak, istediğiniz zaman bu Sözleşmeyi sonlandırabilirsiniz. Bu Sözleşme ne biçimde sonlandırılmış olursa olsun, 7, 8, 11, 13, 19 ve 21. maddelerin hükümleri süre sınırı olmaksızın geçerli kalır.

11. **SON KULLANICI BEYANLARI**. SON KULLANICI OLARAK, YAZILIMIN HİÇBİR AÇIK VEYA ZIMNİ BİR GARANTİ

OLMAKSIZIN VE İLGİLİ YASALARIN İZİN VERDİĞİ AZAMİ ÖLÇÜDE, "OLDUĞU GİBİ" SAĞLANDIĞINI KABUL ETMİŞ OLURSUNUZ. SAĞLAYICI, ONUN ADINA LİSANS VEREN TARAFLAR VEYA BAĞLI ŞİRKETLERİ YA DA TELİF HAKKI SAHİPLERİ, PAZARLANABİLİRLİK GARANTİSİ VEYA BELLİ BİR AMACA UYGUNLUK GARANTİSİ YA DA YAZILIMIN ÜÇÜNCÜ TARAF PATENTLERİNİ, TELİF HAKLARINI, TİCARİ MARKALARINI VEYA DİĞER HAKLARINI İHLAL ETMEMESİ DAHİL ANCAK BUNLARLA SINIRLI OLMAMAK KAYDIYLA HİÇBİR AÇIK VEYA ZIMNİ BEYANDA BULUNMAZ VEYA GARANTİ VERMEZ. SAĞLAYICI VEYA DİĞER BİR TARAF, YAZILIMIN İŞLEVLERİNİN İHTİYAÇLARINIZI KARŞILAYACAĞI VEYA YAZILIMIN KESİNTİSİZ ÇALIŞACAĞI YA DA HATASIZ OLACAĞI GARANTİSİNİ VERMEZ. HEDEFLEDİĞİNİZ SONUÇLARA ERİŞMEK İÇİN YAZILIMIN SEÇİLMESİ VE YAZILIMIN YÜKLENMESİ, KULLANILMASI VE BUNUN SONUCUNDA ELDE EDİLEN SONUÇLARA DAİR HER TÜRLÜ SORUMLULUĞUN VE RİSKİN TARAFINIZA AİT OLDUĞUNU KABUL ETMİŞ OLURSUNUZ.

12. **Başka yükümlülük kabul edilmez**. Bu Sözleşme, burada özel olarak belirtilenlerin dışında Sağlayıcı ve onun adına lisans veren taraflar için hiçbir yükümlülük teşkil etmez.

13. **YÜKÜMLÜLÜKLERİN SINIRLANDIRILMASI**. GEÇERLİ YASALARIN İZİN VERDİĞİ AZAMİ ÖLÇÜDE, SAĞLAYICI, SAĞLAYICININ ÇALIŞANLARI VEYA ADINA LİSANS VEREN TARAFLAR HİÇBİR DURUMDA SÖZLEŞMEDEN, HAKSIZ FİİLDEN, İHMALDEN VEYA YÜKÜMLÜLÜK DOĞURAN BAŞKA BİR NEDENDEN ÖTÜRÜ OLUŞAN VEYA BUNLARDAN KAYNAKLANAN, YAZILIMIN KULLANILMASINDAN VEYA KULLANILAMAMASINDAN KAYNAKLANAN HER TÜRLÜ KÂR, GELİR, SATIŞ VEYA VERİ KAYBINDAN YA DA YEDEK PARÇA VEYA SERVİS ALINMASI MASRAFLARINDAN, MALA GELEN HASARLARDAN, KİŞİSEL YARALANMADAN, TİCARİ BİLGİLERİN KAYBINDAN YA DA ÖZEL, DOĞRUDAN, DOLAYLI, ARIZİ, EKONOMİK, TELAFİ GEREĞİ, CEZAİ, ÖZEL VEYA DOLAYLI HASARLARDAN ÖTÜRÜ, SAĞLAYICININ VEYA ADINA LİSANS VEREN TARAFLARIN YA DA BAĞLI ŞİRKETLERİN BU GİBİ ZARARLARIN MÜMKÜN OLDUĞUNA DAİR HABERDAR EDİLMELERİ DURUMUNDA BİLE, SORUMLU TUTULAMAZLAR. BAZI ÜLKELERDE VE YARGI ALANLARINDA YÜKÜMLÜLÜKLERİN REDDİNE DEĞİL ANCAK SINIRLANDIRILMASINA İZİN VERİLDİĞİNDEN, SAĞLAYICI, SAĞLAYICININ ÇALIŞANLARI VEYA ADINA LİSANS VEREN TARAFLAR VEYA BAĞLI ŞİRKETLERİN YÜKÜMLÜLÜĞÜ LİSANS İÇİN ÖDEDİĞİNİZ ÜCRETLE SINIRLANDIRILMIŞTIR.

14. Bu Sözleşmede bulunan hiçbir hüküm, aksine yorumlanabilmesine bakılmaksızın, müşteri olarak kabul edilen bir tarafın yasal haklarını ihlal etmez.

15. **Teknik destek**. ESET veya ESET tarafından yetkilendirilen üçüncü taraflar, teknik desteği herhangi bir garanti veya beyanat olmaksızın, kendi takdirlerine göre sağlarlar. Son Kullanıcının, teknik desteğin tedarik edilmesinden önce tüm mevcut verileri, yazılım ve program tesislerini yedeklemesi gerekir. ESET ve/veya ESET tarafından yetkilendirilen üçüncü taraflar, teknik destek tedariki nedeniyle veri, mal, yazılım veya donanım hasarı veya kaybı ya da gelir kaybından ötürü yükümlülük kabul etmezler. ESET ve/veya ESET tarafından yetkilendirilen üçüncü taraflar, sorunun çözülmesinin teknik desteğin kapsamının dışında olduğuna hükmetme hakkını saklı tutarlar. ESET kendi takdirine bağlı olarak teknik destek tedarikini reddetme, askıya alma veya sonlandırma hakkını saklı tutar. Lisans bilgileri, Bilgiler ve Gizlilik Politikasına uygun diğer veriler, teknik destek sağlama amacına yönelik olarak gerekebilir.

16. **Lisansın Aktarılması**. Sözleşmedeki hükümlerle çelişmediği sürece, Yazılım bir bilgisayar sisteminden başka bir bilgisayar sistemine aktarılabilir. Bu Sözleşmenin hükümlerine aykırı olmadığı sürece, Son Kullanıcı yalnızca Sağlayıcının onayı olması durumunda, (i) orijinal Son Kullanıcının Yazılımın hiçbir kopyasını elde tutmaması; (ii) hakların aktarılmasının doğrudan yapılması, yani orijinal Son Kullanıcıdan yeni Son Kullanıcıya aktarılması; (iii) yeni Son Kullanıcının bu Sözleşme hükümlerine göre sorumlu olduğu tüm hakları ve yükümlülükleri kabul etmesi; (iv) orijinal Son Kullanıcının 17. Maddede belirtilen şekilde Yazılımın gerçek olduğunu kanıtlamasını sağlayacak belgeleri yeni Son Kullanıcıya sağlaması koşullarına bağlı olarak, Lisansı ve bu Sözleşmeden doğan tüm hakları kalıcı olarak başka bir Son Kullanıcıya aktarma hakkına sahip olur.

17. **Yazılımın orijinal olduğunun doğrulanması**. Son Kullanıcı şu yöntemlerden biriyle Yazılımı kullanma hakkına sahip olduğunu gösterebilir: (i) Sağlayıcı veya Sağlayıcı tarafından görevlendirilmiş bir üçüncü tarafın verdiği lisans sertifikası; (ii) daha önce düzenlenmişse, yazılı bir lisans sözleşmesi; (iii) lisans ayrıntılarını (kullanıcı adı ve parola)

içeren, Sağlayıcı tarafından gönderilen bir e-postanın sunulması. Gizlilik Politikasına uygun olarak lisans bilgileri ve Son Kullanıcı tanımlama verileri Yazılımın orijinalliğinin doğrulanması amacına yönelik olarak gerekebilir.

18. **Kamu kuruluşları ve ABD Hükümeti için lisans verme**. Yazılım Amerika Birleşik Devletleri Hükümeti dahil olmak üzere devlet makamlarına, bu Sözleşmede açıklanan lisans hakları ve kısıtlamalar uyarınca sağlanır.

19. **Ticari denetim uygunluğu**.

a) Yazılımı doğrudan veya dolaylı olarak ihraç edemez, yeniden ihraç edemez, transfer edemez veya başka bir şekilde herhangi bir kişinin kullanımına sunamaz ya da ESET'i veya holding şirketlerini, bağlı şirketleri ve herhangi bir holding şirketinin bağlı şirketlerinin yanı sıra holding şirketleri tarafından kontrol edilen kuruluşları (buradan sonra "Bağlı Kuruluşlar" olarak anılacaktır), aşağıdakileri içeren Ticari Denetim Kanunlarını ihlal eder bir durumda veya bu kanunlar nezdinde negatif sonuçlara maruz bırakan bir şekilde kullanamaz ya da bunlardan herhangi biriyle sonuçlanabilecek bir edime dahil olamaz:

i. Amerika Birleşik Devletleri, Singapur, Birleşik Krallık, Avrupa Birliği veya bağlı devlerinin ya da Sözleşme yükümlülüklerinin yerine getirileceği veya ESET'in veya Bağlı Kuruluşlarından herhangi birinin dahil olduğu ya da faaliyet gösterdiği bir ülkenin hükümeti, eyaleti ya da yetkili düzenleme kurumu tarafından çıkarılan ya da benimsenen; malların, yazılımların, teknolojinin ya da hizmetlerin ihracatı, yeniden ihracatı veya transferiyle ilgili lisans gereksinimlerini kontrol eden, sınırlandıran ya da dayatan tüm kanunlar (buradan sonra "İhracat Denetimi Kanunları" olarak anılacaktır) ve

ii. Amerika Birleşik Devletleri, Singapur, Birleşik Krallık, Avrupa Birliği veya bağlı devlerinin ya da Sözleşme yükümlülüklerinin yerine getirileceği veya ESET'in veya Bağlı Kuruluşlarından herhangi birinin dahil olduğu ya da faaliyet gösterdiği bir ülkenin hükümeti, eyaleti ya da yetkili düzenleme kurumu tarafından getirilen tüm ekonomik, mali, ticari veya diğer yasaklar, kısıtlamalar, ambargolar, ithalat veya ihracat yasakları, fon ya da varlıkların aktarımıyla veya hizmetlerin sağlanmasıyla ilgili yasaklamalar ya da eş değer tedbirler (buradan sonra "Yaptırım Kanunları" olarak anılacaktır).

b) ESET aşağıdakilerin gerçekleşmesi durumunda hemen geçerli olmak üzere bu Şartlar nezdindeki yükümlülüklerini askıya alma veya bu Şartları sonlandırma hakkını saklı tutar:

i. ESET, kendi makul gerekçelerine dayalı fikrince, Kullanıcının Sözleşmenin Madde 19.a altında belirtilen ihlal şartını ihlal ettiğine veya ihlal etme olasılığının yüksek olduğuna karar verirse veya

ii. Son Kullanıcı ve/veya Yazılım Ticari Denetim Kanunlarının öznesi haline gelirse ve bunun sonucu olarak ESET kendi makul gerekçelerine dayalı fikrince, Sözleşme nezdindeki yükümlülüklerini uygulamaya devam etmesinin, ESET'i veya Bağlı Kuruluşlarını Ticari Denetim Kanunlarını ihlal eder bir durumda bırakacağına ya da bu Kanunlar nezdinde olumsuz sonuçlara maruz bırakacağına karar verirse.

c) Sözleşmedeki herhangi bir ifade, taraflardan herhangi birinin geçerli Ticari Denetim Kanunları ile tutarsız olan, bu Kanunlar nezdinde cezalandırılacak olan ya da yasaklanmış olan herhangi bir edimde bulunmasına neden olacak veya böyle bir edimde bulunmasını gerektirecek ya da Kanunlar nezdinde uygun olan bir edimde bulunmamasına neden olacak ya da bulunmamasını gerektirecek şekilde davranması (veya bunları yapmayı kabul etmesi) için tasarlanmamıştır ve bu şekilde yorumlanamaz ya da tahlil edilemez.

20. **Bildirimler**. Tüm bildirimler, iade edilen Yazılım ve Belgeler şu adrese gönderilmelidir: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. **Geçerli yasa**. Bu Sözleşme Slovakya Cumhuriyeti yasalarına tabidir ve bu yasalara uygun şekilde yorumlanır. Son Kullanıcı ve Sağlayıcı, yasalar ve Malların Uluslararası Satışına İlişkin Anlaşmalar hakkındaki Birleşmiş Milletler Konvansiyonu arasındaki ihtilaflı hükümlerin geçerli olmadığını kabul etmiş sayılır. Sağlayıcıyla ilgili olarak bu Sözleşmeden kaynaklanan tüm anlaşmazlıkların veya iddiaların ya da Yazılımın kullanımı ile ilgili tüm

anlaşmazlıkların veya iddiaların Bratislava I. Bölge Mahkemesinde çözümleneceğini ve adı geçen mahkemenin yargı yetkisini uygulamasını açıkça kabul etmiş olursunuz.

22. **Genel hükümler**. Bu Sözleşmenin herhangi bir hükmünün geçersiz veya uygulanamaz olması durumunda, bu Sözleşmenin diğer hükümlerinin geçerliliği etkilenmez ve bu hükümler bu belgede belirtilen koşullar doğrultusunda geçerli ve uygulanabilir kalırlar. Bu Sözleşmenin dil versiyonları arasında bir çatışma olması halinde İngilizce versiyon esas kabul edilecektir. Bu Sözleşmede, yalnızca Sağlayıcının yetkili bir temsilcisi veya avukatlık yetkisine sahip, aynı ehliyetle hareket etmek için açık bir biçimde yetkilendirilmiş bir kişi tarafından imzalanmak suretiyle, yazılı olarak değişiklik yapılabilir.

Bu Sözleşme, Sağlayıcı ve Sizin aranızdaki Yazılım için geçerli olan tüm Sözleşmeyi temsil eder ve Yazılıma ilişkin daha önceki tüm beyanları, görüşmeleri, yükümlülükleri, haberleşmeleri veya tanıtımları geçersiz kılar ve bunların yerine geçer.

EULA ID: BUS-STANDARD-20-01

Gizlilik Politikası

Einsteinova 24, 851 01 Bratislava, Slovakya Cumhuriyeti adresinde mukim ve Bratislava I. Bölge Mahkemesinin Ticari Sicil Kaydında Bölüm Sro, Giriş No 3586/B, İşyeri Sicil Numarası: 31333532 olarak kayıtlı ESET, spol. s r. o. ("ESET" veya "Biz") müşterilerimizin kişisel verilerini işlemek ve onların gizliliği konusunda şeffaf olmak istemektedir. Bu amaçla, bu Gizlilik Politikasını yalnızca müşterimizi ("Son Kullanıcı" veya "Siz") şu konularda bilgilendirmek için yayınlamaktayız:

- Kişisel Verilerin İşlenmesi,
- Veri Gizliliği,
- Veri Öznesinin Hakları.

Kişisel Verilerin İşlenmesi

ESET tarafından sağlanan ve ürünümüze eklenen hizmetler, Son Kullanıcı Lisans Sözleşmesi ("EULA") altında sağlanmaktadır, ancak hizmetlerimizden bazıları özel dikkat gerektirmektedir. Hizmetlerimizin sağlanmasıyla bağlantılı veri toplama hakkında size daha fazla detay sunmak istiyoruz. EULA'da ve ürün belgelerinde açıklanan, güncelleme/yükseltme hizmeti, ESET LiveGrid®, verilerin kötüye kullanımına karşı koruma, destek gibi çeşitli hizmetler sunmaktayız. Bunu yapabilmek için aşağıdaki bilgileri toplamamız gerekmektedir:

- Güncelleme ve yükleme işlemi ve ürünümüzün yüklendiği platform dahil olmak üzere bilgisayarınız ile ilgili bilgileri kapsayan istatistikler ve işletim sistemi, donanım bilgileri, yükleme kimlikleri, lisans kimlikleri, IP adresi, MAC adresi, ürünün yapılandırma ayarları gibi işlemler ve işlevler ile ilgili bilgiler.
- ESET LiveGrid® itibar sistemi kapsamında sızıntılarla ilişkili tek yönlü karmalar, taranan dosyaları buluttaki beyaz ve kara listelerde yer alan öğelerden oluşan veri tabanıyla karşılaştırarak anti-malware çözümlerimizin etkisini artırır.
- ESET LiveGrid® İtibar Sistemi kapsamında dağınık haldeki ortamdan alınan şüpheli örnekler ve meta veriler, ESET'in son kullanıcılarımızın ihtiyaçlarına hemen yanıt vermesine ve en son tehditlere anında tepki verebilmemize olanak tanır. Hizmetlerimizi sağlamamız Sizin bize şu bilgileri iletmenize bağlıdır:
  - potansiyel virüs örnekleri ve diğer kötü amaçlı yazılım programları gibi sızıntılar; sorunlu, istenmeyen türden olabilecek veya tehlikeli olabilecek güvenilir olmayan nesneler (örneğin yürütülebilir dosyalar, Sizin tarafınızdan spam olarak bildirilen veya ürünümüz tarafından işaretlenen e-posta iletileri;

- otür, satıcı, model ve/veya cihaz adı gibi, yerel ağda bulunan cihazlar hakkındaki bilgiler;
- oIP adresi ve coğrafi bilgiler, IP paketleri, URL'ler ve ethernet çerçeveleri gibi internet kullanımı ile ilgili bilgiler;
- okilitlenme bilgi döküm dosyaları ve içindeki bilgiler.

Bu kapsamın dışındaki verilerinizi toplamayı istemeyiz, ancak kimi zaman bunu önlemek mümkün olmamaktadır. Yanlışlıkla toplanan veriler kötü amaçlı yazılıma dahil edilebilir (bilginiz veya onayınız olmadan toplanabilir) veya dosya adlarının ya da URL'lerin bir parçası olarak gelebilir ve bu Gizlilik Politikası'nda açıklanan amaca yönelik olarak bu bilgilerin sistemlerimizin parçası haline gelmelerini veya bu bilgileri işlemeyi amaçlamayız.

- Lisans kimliği gibi lisans bilgileri ve ad, soyadı, adres, e-posta adresi gibi kişisel veriler faturalandırma amaçları, lisans orijinalliğini doğrulama ve hizmetlerimizin sunulması için gereklidir.
- İletişim bilgileri ve destek isteklerinizde yer alan veriler, destek hizmetleri için gereklidir. Bizimle iletişim kurmak için seçtiğiniz kanala bağlı olarak e-posta adresinizi, telefon numaranızı, lisans bilgilerinizi, ürün ayrıntılarını ve destek olayınızın açıklamasını toplayabiliriz. Destek hizmetini kolaylaştırmak için bize başka bilgiler sağlamanız da istenebilir.

Veri Gizliliği,

ESET; dağıtım, hizmet ve destek ağımızın bir parçası olarak bağlı kurumlar veya iş ortakları üzerinden dünya genelinde faaliyet gösteren bir şirkettir. ESET tarafından işlenen bilgiler, hizmet, destek veya faturalandırma tedariki gibi EULA'nın performansı için, bağlı kuruluşlar veya iş ortaklarına ya da bu kurumlardan aktarılabilir. Kullanmayı seçtiğiniz konumu ve hizmete bağlı olarak, verilerinizi Avrupa Komisyonu tarafından uygulanan yeterlik noksanlığı kararının bulunduğu bir ülkeye göndermemiz gerekebilir. Bu durumda bile, bilgilerin her aktarımı veri koruma kanunu düzenlemesine tabidir ve yalnızca gerektiğinde gerçekleşir. Standart Sözleşme Maddeleri, Bağlayıcı Tüzel Kişi Kuralları veya diğer uygun koruma mekanizması herhangi bir istisna olmaksızın oluşturulmalıdır.

EULA kapsamında hizmetlerimizi sunarken verilerin gerektiğinden daha uzun süre depolanmasını önlemek için elimizden gelenin en iyisini yaparız. Elde bulundurma süremiz, size kolay ve zahmetsiz yenileme imkanı sunabilmek için lisansınızın geçerlilik süresinden daha uzun olabilir. ESET LiveGrid® ürününden minimize edilmiş ve anonim hale getirilmiş olan istatistikler ve diğer bilgiler istatistiksel amaçlar için işlenmeye devam edebilir.

ESET, potansiyel risklere uygun bir güvenlik düzeyi sağlamak için uygun teknik ve organizasyonel önlemleri alır. Gizlilik, doğruluk, sistemlerin ve hizmetlerin kullanılabilirliği ve dayanıklılığını sürekli olarak sağlamak için elimizden gelenin en iyisini yaparız. Ancak haklarınız ve özgürlüklerinize yönelik bir riskle sonuçlanan veri ihlali durumunda yetkilileri ve veri öznelerini bilgilendirmeye hazırız. Bir veri öznesi olarak yetkili kuruluşa şikayette bulunma hakkınız vardır.

Veri Öznesinin Hakları

ESET Slovak kanunlarının düzenlemesine tabidir ve Biz de Avrupa Birliği'nin üyesi olarak veri koruma mevzuatına tabiyiz. Geçerli veri koruma kanunlarınca belirtilen şartlara tabi olmak koşuluyla, bir veri öznesi olarak şu haklara sahipsiniz:

- ESET'ten kişisel verilerinize erişim isteme hakkı,
- doğru olmaması halinde kişisel verilerinizin düzeltilmesi hakkı (Ayrıca eksik verileri tamamlama hakkına da sahipsiniz),
- kişisel verilerinizin silinmesini isteme hakkı,

- kişisel verilerinizin işlenmesinde kısıtlama isteme hakkı
- veri işlenmesine itiraz etme hakkı
- şikayette bulunma hakkı ve
- veri taşınabilirliği hakkı.

Veri öznesi olarak hakkınızı kullanmak istemeniz halinde veya sorunuz ya da endişeniz varsa bize şu adresten mesaj gönderebilirsiniz:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk