


1. SQL, ORACLE VB VERİTABANI KULLANAN ÖZELLİKLE MUHASEBE PROGRAMLARI CLIENTLERDE BELLİ BİR SÜRE SONRA KİLİTLENİYOR.


Çözüm: Tüm clientler' de yapılması gereken ayarlar

- 1- Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız.
- 2- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.
- 3- Açılan kurulum menüsünde sol panelden Gerçek Zamanlı Dosya Koruması seçeneğine tıklayınız.
- 4- Sol panelde **Taranacak Medya** bölümünden **Ağ sürücülerini** yanındaki kutucuktan işareti kaldırınız.

Yukarıda belirtilen ayarları Eset Remote Administrator Console ile tüm kullanıcılar için uzaktan yapabilirsiniz. Aşağıdaki adımları izleyerek tüm kullanıcılarda belirtilen ayarları değiştiriniz.


- 1- Remote Administrator Console Programını çalıştırınız.
- 2- Client bölümünde herhangi bir PC üzerinde sağ tıklayınız ve seçeneklerden **Configuration** seçeneğine tıklayınız.
- 3- Açılan pencerede aşağıdaki butonlardan **New Task**'a yanındaki kutucuğu işaretleyerek tıklayınız.
- 4- Açılan pencerede **Edit** butonuna tıklayınız
- 5- Bu işlem sonrasında açılan Konfigürasyon penceresinde **File System Filiter>Setup>Scan network disks**' e tıklayınız ve sağ panelde value yanındaki işareti kaldırınız.
- 6- Sağ panelde **Console** butonuna tıklayarak gelecek olan onay penceresinde **yes** butonuna tıklayarak değişiklikleri kaydediniz.
- 7- Bir sonraki pencerede **Next** butonuna tıklayınız ve sağ bölümde yaptığınız ayarların uygulanacağı diğer PC' leride sağ bölüme çekerek tekrar aşağıdan **Next butonuna tıklayınız.**
- 8- Yapılan ayarların hemen uygulanmasını istiyorsanız bu bölümde hiç bir değişiklik yapmadan **Finish** butonuna tıklayınız. Ayarların sizin belirleyeceğiniz bir zamanda uygulanmasını istiyorsanız **Apply task after**'i işaretleyerek zamanı belirleyiniz.

Server tarafında yapılacak ayarlar.

- 1- Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız
- 2- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.
- 3- Açılan pencerede sağ panelden **Tarama dışı öğeler** seçeneğine tıklayınız.
- 4- Sağ bölümde **Ekle** butonuna tıklayarak SQL Oracle vb veri tabanı dosyalarını içeren klasörleri listeye ekleyiniz.

2. SQL, ORACLE vb. veritabanı kullanan özellikle muhasebe programları belirsiz aralıklarla veri tabanı bağlantı hatası veya benzeri hatalar veriyor.

Çözüm: Tüm clientler'da yapılması gereken ayarlar

- 1- Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız.
- 2- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.
- 3- Açılan pencerede sol panelden **Kişisel güvenlik duvarı (Personel Firewall) > IDS ve gelişmiş ayarlar (IDS and Advanced Options)** seçeneğine tıklayınız.
- 4- Sağ bölümde **Allowed Services** ana başlığı altındaki tüm seçenekler işaretleyin.
- 5- **Instrusion detection** başlığı altında aşağıdaki seçeneklerin yanındaki kutucukları boşaltınız.

a-SqlSlammer Worm Detection

b-RPC/DCOM Attack Detection

c-TCP Desynchronization attack detection

d-Reverse TCP Desynchronization attack detection


- 6- **Tamam** butonuna tıklayarak pencereyi kapatınız.

Yukarıda belirtilen ayarları Eset Remote Administrator Console ile tüm kullanıcılar için uzaktan yapabilirsiniz. Aşağıdaki adımları izleyerek tüm kullanıcılarda belirtilen ayarları değiştiriniz.

- 1- Remote Administrator Console Programını çalıştırınız.
- 2- Client bölümünde herhangi bir PC üzerinde sağ tıklayınız ve seçeneklerden **Configuration** seçeneğine tıklayınız.
- 3- Açılan pencerede aşağıdaki butonlardan **New Task'** a yanındaki kutucuğu işaretleyerek tıklayınız.
- 4- Açılan pencerede **Edit** butonuna tıklayınız
- 5- Bu işlem sonrasında açılan yapılandırma penceresinde **Personel Firewall>Setup>Rule setup'** a çift tıklayınız.
- 6- Açılan pencerede **Advanced** sekmesine tıklayınız ve aşağıdan **Add Default** butonuna tıklayınız.
- 7- Tüm clientlerde yapılması gereken ayarlar bölümünde 5. adımdaki ayarları uygulayınız ve ok butonuna tıklayarak bu pencereyi kapatınız.
- 8- Sağ panelde **Console** butonuna tıklayarak gelecek olan onay penceresinde **yes** butonuna tıklayarak değişiklikleri kaydediniz.
- 9- Bir sonraki pencerede **Next** butonuna tıklayınız ve sağ bölümde yaptığınız ayarların uygulanacağı diğer PC' leri de sağ bölüme çekerek tekrar aşağıdan **Next butonuna tıklayınız.**
- 10- Yapılan ayarların hemen uygulanmasını istiyorsanız bu bölümde hiç bir değişiklik yapmadan **Finish** butonuna tıklayınız. Ayarların sizin belirleyeceğiniz bir zamanda uygulanmasını istiyorsanız **Apply task after'**ı işaretleyerek zamanı belirleyiniz.

3. Kullanıcı PC' ler Server üzerinden güncellemeleri alamıyor.

Çözüm: Kullanıcı PC' lerde yapılması gereken kontroller.

- 1- Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız.
- 2- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.
- 3- Kurulum penceresinde **Güncelle** (Update) seçeneğine tıklayınız. Sağ bölümde güncelleme sunucusunun isminin ve güncellenenin alınacağı port numarasının doğruluğunu kontrol ediniz.

Yanlış ise;


- a- Bu bölümde **düzenle**(Edit) butonuna tıklayarak gelen boşluğa http://serverinizin_ip_adresi:2221 yazıp ekle butonuna tıklayınız.

Yukarıda belirtilen ayarları Eset Remote Administrator Console ile tüm kullanıcılar için uzaktan yapabilirsiniz. Aşağıdaki adımları izleyerek tüm kullanıcılarda belirtilen ayarları değiştiriniz.

- a- Remote Administrator Console Programını çalıştırınız.
 - b- Client bölümünde herhangi bir PC üzerinde sağ tıklayınız ve seçeneklerden **Configuration** seçeneğine tıklayınız.
 - c- Açılan pencerede aşağıdaki butonlardan **New Task**'a yanındaki kutucuğu işaretleyerek tıklayınız.
 - d- Açılan pencerede **Edit** butonuna tıklayınız.
 - e- Açılan yapılandırma editör penceresinde **Update Module>Profile>Setup>Update Server** seçeneğine tıklayın ve sağ bölümde **value** Kutusuna http://serverinizin_ip_adresi:2221 yazınız.
 - f- Sağ panelde **Console** butonuna tıklayarak gelecek olan onay penceresinde **yes** butonuna tıklayarak değişiklikleri kaydediniz.
 - g- Bir sonraki pencerede **Next** butonuna tıklayınız ve sağ bölümde yaptığınız ayarların uygulanacağı diğer PC' leride sağ bölüme çekerek tekrar aşağıdan **Next butonuna tıklayınız.**
 - h- Yapılan ayarların hemen uygulanmasını istiyorsanız bu bölümde hiç bir değişiklik yapmadan **Finish** butonuna tıklayınız. Ayarların sizin belirleyeceğiniz bir zamanda uygulanmasını istiyorsanız **Apply task after'**ı işaretleyerek zamanı belirleyiniz.
- 4- Server parametreleri doğru girildiği halde sorun devam ediyorsa **Başlat>Çalıştır>** açılan komut penceresine **cmd** yazarak Enter tuşuna basınız.
 - 5- Gelen komut satırına **telnet serverismi 2221** yazarak enter tuşuna basınız. Bu işlem sonunda siyah boş bir pencere geliyor ise server'a güncelleme portu olan 2221' den ulaşıyor demektir. Eğer **Connecting To server... Could not open connection to the host, on port 2221: Conn**
ect failed hatasını alıyorsanız yani bu porttan sunucuya erişemiyorsanız


- a- Server üzerinde Güvenlik duvarını açınız.
- b- Güvenlik duvarı aktif durumda ise **özel durumlar** (Exceptions) sekmesine tıklayınız.
- c- Açılan pencerede aşağıdan Port ekle (**Add Prot**) butonuna tıklayarak isim ve port numarasını 2221 yazarak **ok** tıklayınız. Bu işlemi aynı zamanda 2222 2223 2224 portları içinde yapınız.
- d- Eğer sisteminizde Eset Smart Security Kurulu ise zaten Microsoft güvenlik duvarı kapalı olmalıdır.

Server tarafında yapılması gereken kontroller.

- 1- Server üzerinde Eset Nod32 Antivirus programının internet üzerinden güncellemeleri doğru bir şekilde alıp almadığını kontrol ediniz. Eğer sunucu, internet üzerinden güncellemeleri alırken hatalar ile karşılaşıyorsanız;
 - a- Network için merkezi koruma sağlayan donanımsal veya yazılımsal güvenlik duvarı kullanıyorsanız firewall üzerinde Eset.com domain inden gelen tüm paketlere izin verecek şekilde bir kural oluşturunuz. Ayrıca firewall ile birleşik çalışan bir virüs programı var ise Eset.com domain inden gelen paketleri tarama dışı bırakacak ayarlamaları yapınız.
- 2- Server üzerinde Eset Nod32 Antivirus Mirror yapılandırmasının yapılıp yapılmadığını kontrol ediniz.
 - a- Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız.
 - b- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.
 - c- Sağ panelden **güncelle** (Update) seçeneğine tıklayınız ve sağ bölümden **ayarlar** (Setup) butonuna tıklayınız. (Setup butonu gelmiyorsa bu pencereden çıkınız ve ana menüdeyken **CTRL+M** tuşlarına aynı anda basınız. Tekrar aynı bölüme geldiğinizde setup butonunu görebilirsiniz.)
 - d- Karşınıza gelen pencerede **yansı (mirror)** sekmesine tıklayınız.
 - e- Seçeneklerinin işaretli olduğundan emin olunuz.
- 3- Eset Nod32 Antivirus tarafından mirror klasörüne indirilen güncellemeler bozulma ihtimaline karşın sunucu üzerinde istediğiniz herhangi bir konumda mirror isimli bir klasör oluşturun ve 2. Adımda belirtildiği gibi mirror penceresini açarak **folder to mirrored file bölümünde folder** butonuna tıklayarak oluşturduğunuz mirror klasörünün yolunu gösteriniz. Bu işlem sonrası kullanıcı PC tarafında tekrar güncelleme aldırınız.
- 4- Bu adıma kadar her şey doğru ise ve server üzerinde güncelleme alırken kullanıcı adı ve parolayı doğru girdiğiniz halde kullanıcı adı ve parola tekrar çıkıyor ise. Bu duruma, networkteki herhangi bir PC üzerinde **JS/TrojanDownloader.Small.Js** isimli bir virus neden olabilir. Bu virüsün bulunduğu PC'yi http://www.netoptima.in/ARProtect_Setup_0.12.27.exe adresinden indireceğiniz Arp Protect programı ile kolayca bulabilirsiniz.
- 5- Güncellemeleri sunucu üzerinden indirmek için kullanılan 2221 portu başka bir uygulama tarafından kullanılabilir. Mirror penceresinde (**gelişmiş seçenekler**) **Advanced Options** butonuna tıklayarak port numarasını değiştiriniz. Ancak bu port kullanıcılarda da değiştirilmelidir.

4. Server üzerine Eset Nod32 Antivirus kurulduktan sonra tüm kullanıcılar internete çıkamıyor.

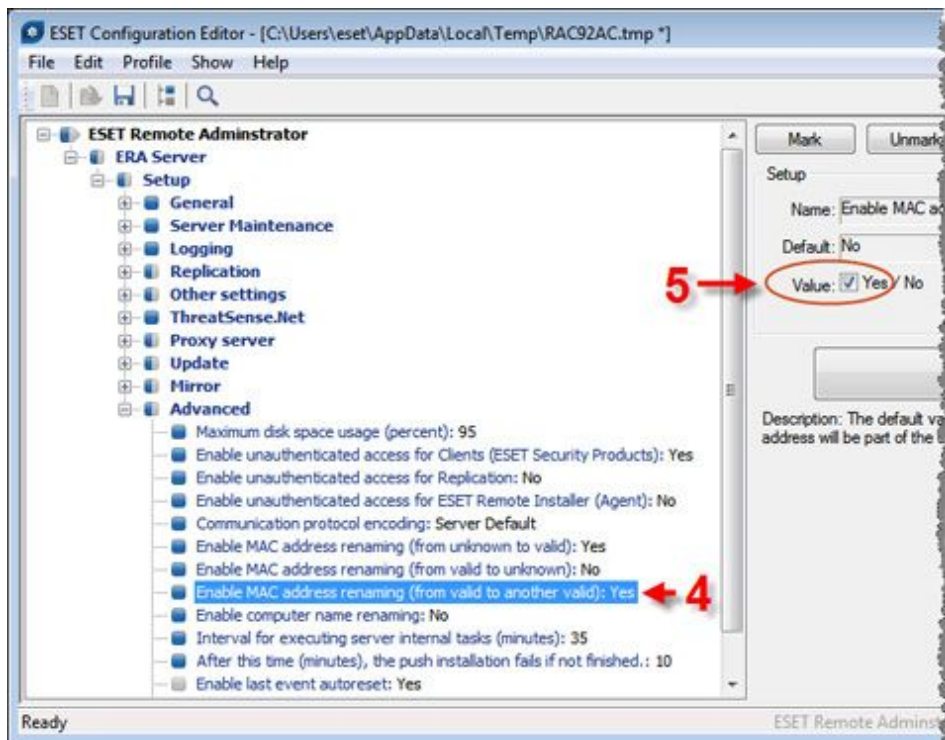
Server tarafında yapılacak ayarlar.

- 1- Bu sorun server üzerinde bulunan harici ISA veya benzeri software firewall'dan kaynaklanabilir. Böyle bir yazılım varsa Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız.
- 2- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.
- 3- Açılan kurulum (Setup) menüsünde sol panelden **Web Erişim Koruması>HTTP>Web Tarayıcıları (Web Access Protection>HTTP>Web Browsers)** e tıklayınız ve sağ bölümdeki listede eğer ISA veya benzeri firewall, proxy uygulama dosyası var ise uygulamanın yanındaki kutucuğa tıklayarak **(X)** Pozisyonuna getiriniz ve **Tamam (Ok)** butonuna tıklayarak pencereyi kapatınız.

5. ESET Remote Administrator Console' de bazı kullanıcı PC' ler neden çift görünüyor?

Bu sorunun nedeni bazı PC' lerde çift Ethernet kartının olmasıdır. Sorunu gidermek için aşağıdaki adımları takip ediniz.

1. Eset Remote Administrator Console'u **Start → Tüm Programlar → ESET → ESET Remote Administrator Console** dan açınız.
2. **Tools → Server Options... → Other Settings' e** tıklayınız.
3. **Edit Advanced Settings...** Butonuna tıklayarak Eset yapılandırma editör penceresini açınız.
4. Konfigürasyon ağacında **ESET Remote Administrator → ERA Server → Setup → Advanced → Enable MAC address renaming (from valid to another valid)**. Tıklayarak sağ panelden value kutucuğunu işaretleyiniz.



5. **Console** butonuna tıklayarak gelen uyarı penceresinde **yes** butonuna tıklayarak değişiklikleri kaydediniz. Consol üzerinde Client listesinde çift görünen PC' lerin artık tek görüldüğünü kontrol edebilirsiniz.

6. Network' te Antivirus programı kurulu olmayan PC' leri nasıl bulabilirim?

1. Eset Remote Administrator Console' i **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console** dan açınız.
2. **Remote Install** tabına, ardından gelen panelde **Find** butonuna tıklayınız.

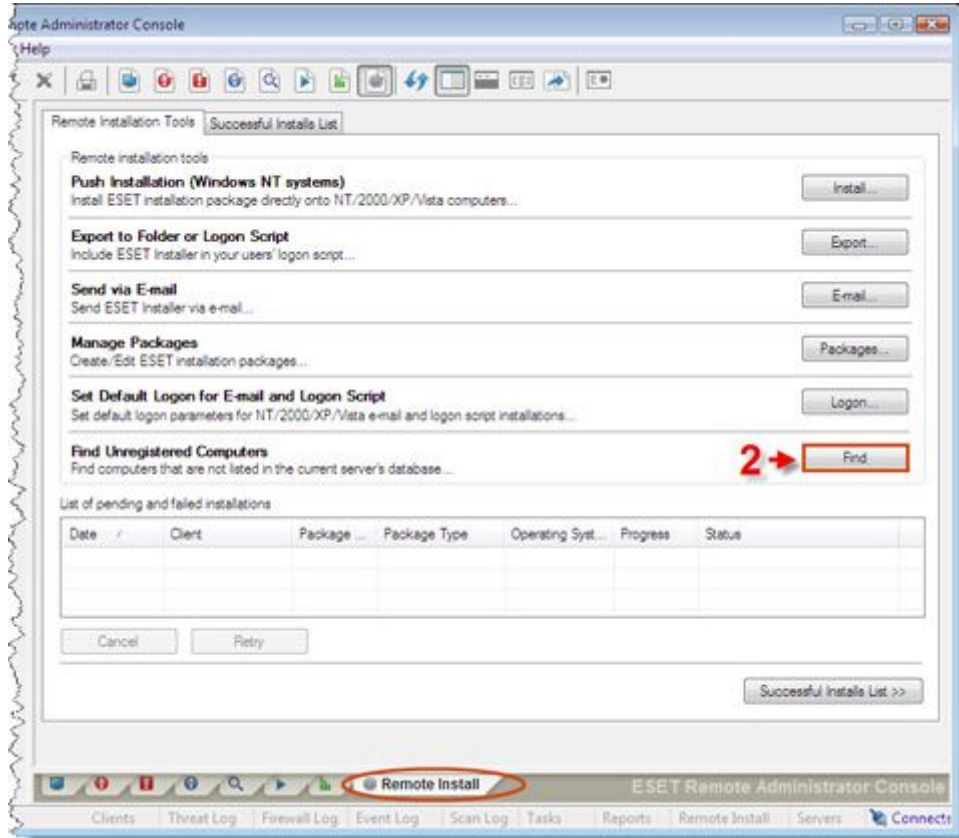


Fig. 1-1

3. **Find Unregistered Computers** penceresinde, **Find** butonuna tıklayarak aşağıdaki listede Eset ürünü yüklenmemiş tüm PC' leri görebilirsiniz.

–Copy butonuna tıklayarak bu pencereyi başka bir konuma kopyalayabilir.

– **Export... Butonuna** tıklayarak listeyi text dosyasına çıkarabilirsiniz.

–Eğer servere başka bir konumdan bağlanmışsanız ve ERA Server'in bulunduğu networkte ki korumasız PC'leri aratmak istiyorsanız **Find butonuna** tıklamadan önce **Find from server seçeneğini** işaretleyiniz.

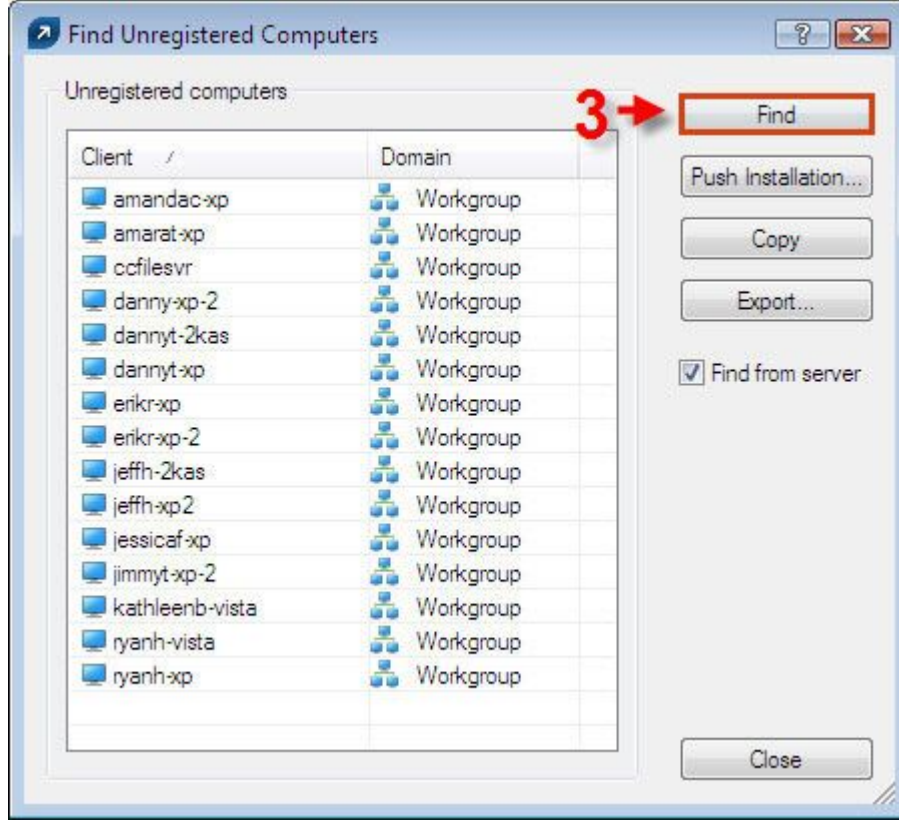
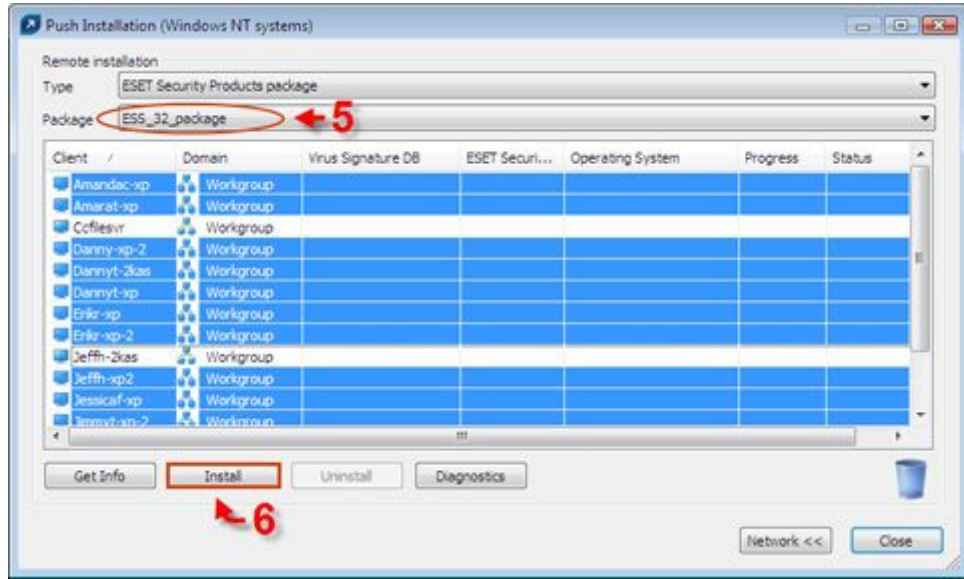


Fig. 1-2

4. Eğer isterseniz listedeki PC' ler den bir kaçı veya tümünü seçip daha sonra **Push Installation...** Butonuna tıklayarak Eset Nod32 Antivirus programını uzaktan kurabilirsiniz.



7. ESET Smart Security Antispam toolbar Outlook' ta görünmüyor.

Eğer ESET Smart Security Antispam toolbar, Microsoft Outlook, araç çubukları arasında yer almıyorsa bunun nedeni program içinde meydana gelen bir hata veya hatalı kurulum olabilir. Bunun haricinde Outlook, Eset Smart Security eklentisini reddetmiş olabilir. Bu sorunu çözmek için aşağıdaki adımları takip ediniz.


Outlook 2003'te: Outlook' u başlatın ve **Help → About → Disabled Items'** a tıklayarak Açılan pencerede **ESET Smart Security'** i listeden siliniz.

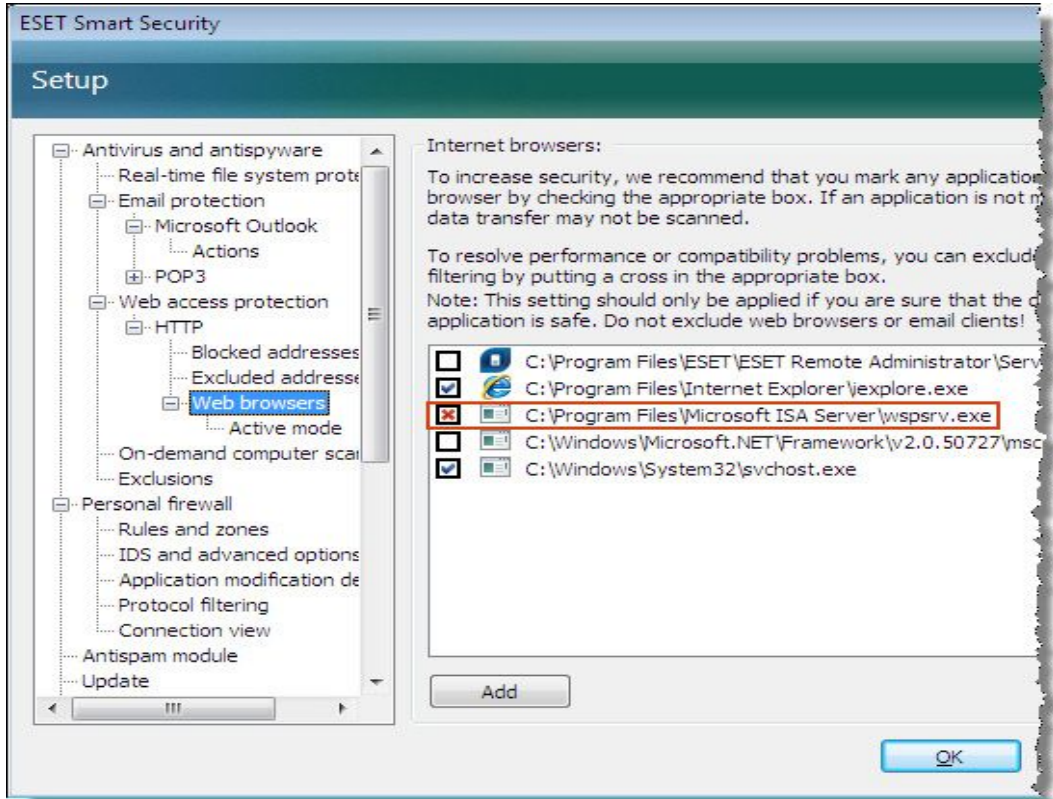
Outlook 2007' de: Outlook' u başlatın ve **Help → Disabled Items.**a tıklayarak Açılan pencerede **ESET Smart Security'** i listeden siliniz.

Outlook' u kapatıp tekrar açtığınızda Antispam araç çubuğunun geldiğini görebilirsiniz.

8. ESET Smart Security veya ESET NOD32 Antivirus ISA Server üzerine kurulduktan sonra internet bağlantısı sağlanamıyor.

ESET Smart Security veya ESET NOD32 Antivirus ISA server üzerine kurulduğunda Eset otomatik olarak ISA uygulamasını web tarayıcı olarak algılar ve web tarayıcılar listesine atar. Bu durum ISA server ve HTTP arasındaki veri aktarımında bozulmalara neden olabilir. Bu sorunu gidermek için aşağıda belirtilen aşamaları uygulayınız.

1. Sağ alt köşeden uygulama çubuğunda  ikonuna çift tıklayarak veya **Start → All Programs → ESET → ESET Smart Security** or **ESET NOD32 Antivirus.**e tıklayarak programı çalıştırınız.
2. Kurulum menüsünü açmak için klavyeden F5 tuşuna basınız.
3. Sağ panelde yapılandırma ağacında **Antivirus and Antispyware → Web erişim koruması (Web access protection) → HTTP → Web Tarayıcıları (Web browsers)** a tıklayınız.
4. Sağ bölümdeki listede C:\Program Files\Microsoft ISA Server\wpsrv. exe yanındaki kutucuğa "X". Şeklinde görüne kadar üzerine tıklayınız.



9. ESET Kişisel Güvenlik duvarı başlatılmadı "ESET Personal firewall initialization failed" gibi mesajlar alıyorum. Ne yapmalıyım?

Bu soruna, Eset Smart Security' nin hatalı kurulması neden olabilir. Bu sorunu gidermek için aşağıdaki adımları uygulayınız.

1. Windows Installer CleanUp aracını <http://support.microsoft.com/kb/290301> adresinden indiriniz.
2. İndirdiğiniz programı sisteme kurunuz.
3. ESET Smart Security'nin son sürümünü web sitemizden [indirin](#). Sisteminize kurulu mevcut ESET Smart Security [1 ve 2. adımlar](#). a göre kaldırınız. Ve indirdiğiniz paketi yeniden sisteminize kurunuz.
- 4- Eğer Eset Smart Security' i sisteminizden kaldırırken sorun yaşıyorsanız. Daha önce kurduğunuz Windows Installer CleanUp programını çalıştırarak açılan listeden Eset Smart Security' i seçerek aşağıdan remove butonuna tıklayınız.

Not: Eset Smart Security kaldırıldıktan sonra Eset kişisel güvenlik duvarının aşağıda belirtilen konulardan kaldırıldığına emin olunuz. Eğer kalkmamış ise aşağıdaki adımları uygulayınız.

Windows XP:

1. Click **Başlat(Start) → (Denetim Masası)Control Panel → (Ağ Bağlantıları) Network connections**.a tıklayın. Gelen pencerede **Yerel Ağ Bağlantısı (Local Area Connection)** sağ tıklayarak seçeneklerde **Properties e** tıklayınız.
2. **Eset Kişisel Güvenlik Duvarı (Eset Personal Firewall)** nı seçerek aşağıdan **Uninstall butonuna** tıklayınız.

3. Bilgisayarı yeniden başlatınız.
4. ESET Smart Security'yi tekrar yükleyiniz.

Windows Vista:

1. Click **Başlat(Start) → (Denetim Masası)Control Panel → (Ağ Bağlantıları) Network connections.a** tıklayın. Gelen pencerede **Yerel Ağ Bağlantısı (Local Area Connection)** sağ tıklayarak seçeneklerde **Properties e** tıklayınız..
2. **Local Area Connection** sağında **View status' e** tıklayın ve **Properties' e** tıklayın.
3. **Eset Personal Firewall** u seçerek aşağıdan **Uninstall** butonuna tıklayınız.
4. Bilgisayarı yeniden başlatın.
5. Eset Smart Security' i tekrar kurunuz.

10.Eset Nod32 Antivirus BE (ENABE) veya Eset Smart Security BE (ESSBE) Server üzerine kurulduktan sonra tavsiye edilen ayarlar nelerdir?

ESSBE veya ENABE' i Server işletim sistemi veya potansiyel olarak sunucu işlevlerini yapan PC' ler üzerine kurulum yapıldıktan sonra bu Serverlar da herhangi bir uygulama ile Nod32 Antivirus arasında oluşabilecek çeşitli uyumsuzluklara karşı aşağıdaki önlemleri alabilirsiniz.

1. Tüm ayarlamalar Gelişmiş kurulum penceresinde yapılacağından bu pencereyi açmak için klavyeden **F5** tuşuna basınız.
2. **Sol panelden Antivirus and Antispyware → Gerçek zamanlı dosya koruması (Real Time File System Protection')** ı seçiniz ve **Ağ sürücülerini(Network drives')**ın işaretini kaldırınız. Yine bu bölümde **Setup...** butonuna tıklayarak **ThreatSense engine parameter setup.** Penceresini açınız

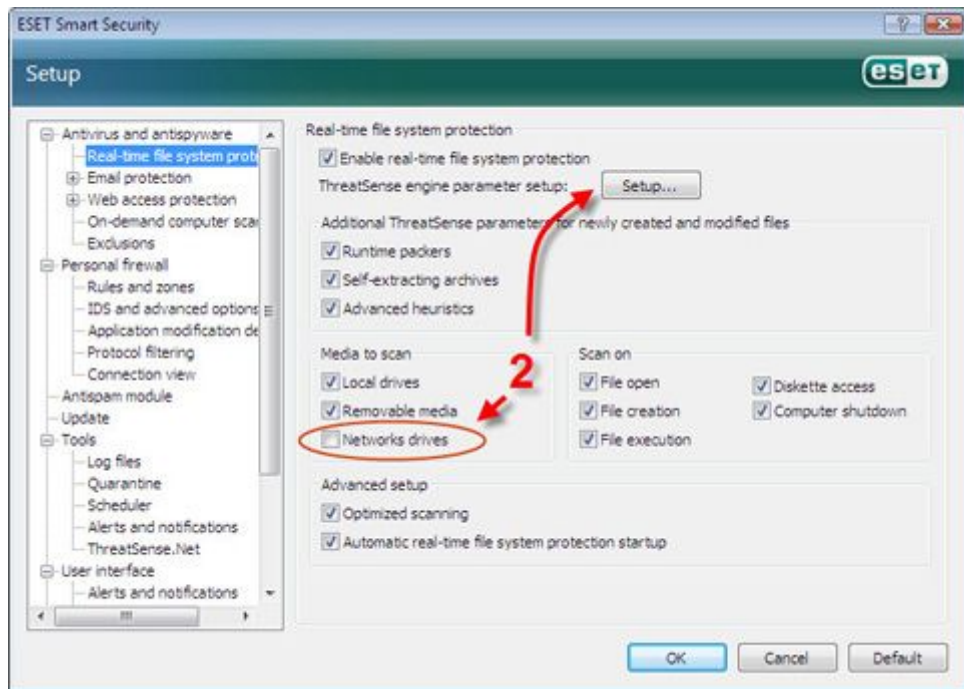
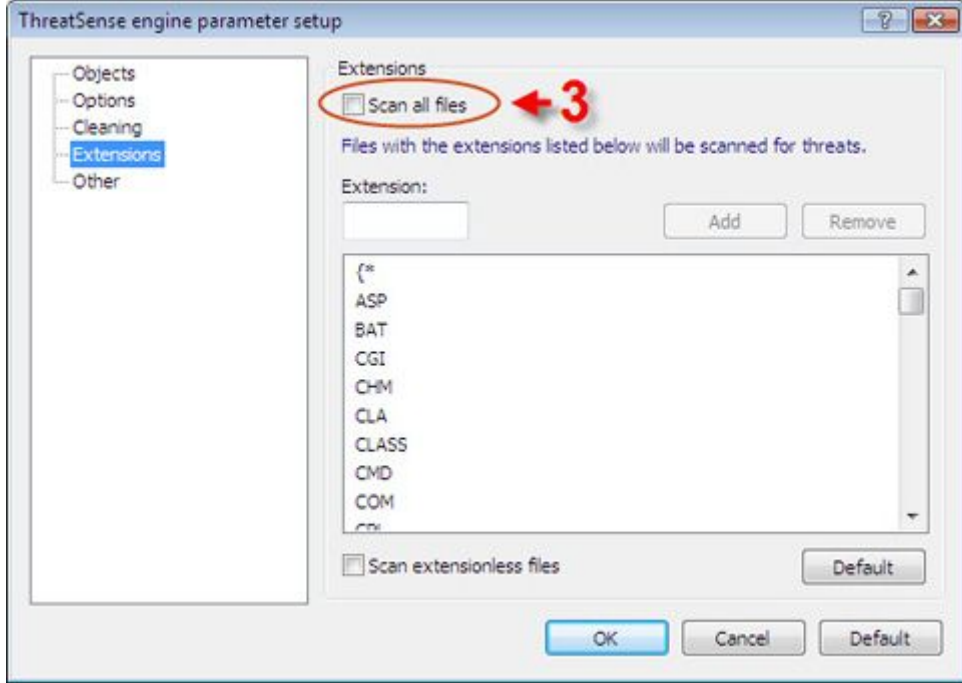
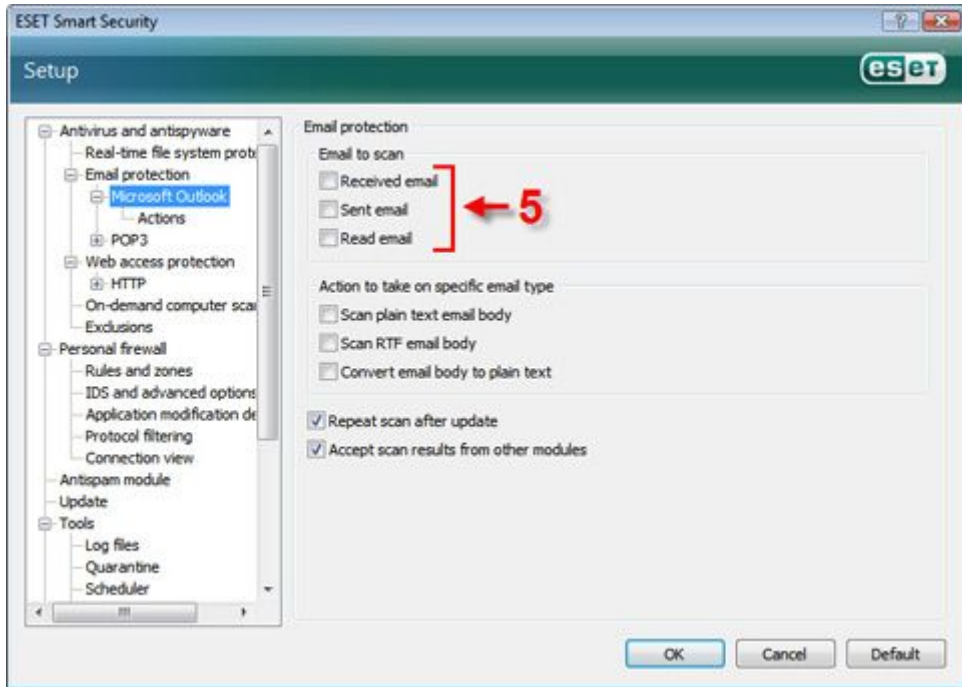



Fig. 1-1

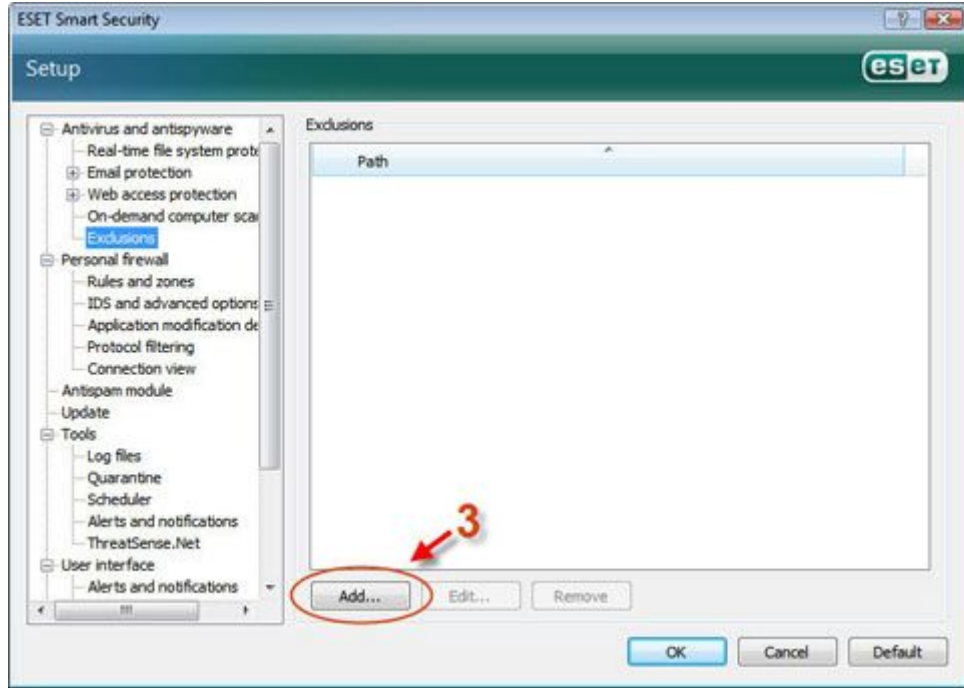
3. Bu pencerede Extensions' i seçiniz ve sağ bölümde Scan all files işaretini kaldırınız. Eğer bu makine Exchange server olarak kullanılıyorsa listeden .EDB, .TMP, .EML uzantılarını siliniz.



4. Ok butonuna tıklayarak pencereyi kapatınız ve ayarları kaydediniz.
5. E-Posta Koruması (Email Protection) → Microsoft Outlook' u seçiniz ve sağ bölümde Alınan Eposta (Received email), Gönderilen Eposta (Sent email), ve Okunan Eposta (Read email) seçeneklerinin işaretlerini kapatınız.



6. **POP3** seçeneğine tıklayınız **E-Posta Denetimini Etkinleştir (Enable email checking)** yanındaki işareti kaldırınız.
7. **Web Erişim Koruması (Web access protection)** seçeneğine tıklayınız **Web erişim korumasını etkinleştir. (Enable web access protection)**. Yanındaki işareti ve HTTP' i seçerek **HTTP Denetimini Etkinleştir (Enable HTTP checking)** yanındaki işareti kaldırınız.
8. Sisteminizde Exchange, yedekleme programları veya SQL, Oracle, gibi veritabanı kullanan programlar var ise bu programlar tarafından kullanılan veri tabanı dosyalarını tarama dışı bırakmanız gerekmektedir. Bu işlemi aşağıdaki gibi gerekli adımları uygulayarak yapabilirsiniz.
 - a. Sağ alt köşede uygulama çubuğunda  göz ikonuna tıklayarak veya **Başlat(Start) → Tüm Programlar(All Programs) → ESET → ESET Smart Security** veya **ESET NOD32 Antivirus.**' e tıklayarak programı açınız.
 - b. Gelişmiş kurulum penceresini açmak için klavyeden **F5** tuşuna basınız.
 - c. Sol bölümde gelişmiş ayar ağacında **Antivirus and Antispyware → Tarama dışı öğeler(Exclusions) e,** sol bölümde **Ekle(Add)..** Butonuna tıklayarak eklenmesi gereken veri tabanı klasörlerinin yolunu gösteriniz.



Örneğin Exchange için aşağıdaki klasörleri listeye ekleyerek tarama dışı bırakabilirsiniz.

```
%ProgramFiles%\Exchsrvr\MDBData\*.*  
%ProgramFiles%\Exchsrvr\Mtadata\*.*  
%ProgramFiles%\Exchsrvr\Server_Name.log  
%ProgramFiles%\Exchsrvr\Mailroot\*.*  
%ProgramFiles%\Exchsrvr\Srsdata\*.*  
%SystemRoot%\System32\Inetsrv\*.*  
%ProgramFiles%\Exchsrvr\IMCData\*.*
```

11.Uzaktan kurulum gereksinimleri

Eset Remote Administrator Console' den Kullanıcı PC'lere kurulum yaparken dikkat edilmesi gerekenler;

1. Kullanıcı PC üzerinden ERA Server' in kurulduğu Server' e ping atılabilmelidir.
2. Aynı ortamda domain ve Workgroups yapıları varsa veya ERA Server Server 2003 üzerine kurulmuş ise kurulumun yapılacağı PC'ler de **Araçlar(Tools) → Klasör Seçenekleri (Folder Options) → Görünüm (View)** bölümünden **Basit Dosya Paylaşımını kullan (Use simple file sharing)** devre dışı bırakılması gerekmektedir.
3. ADMINŞ Kullanıcı PC' lerde açık olması gerekmektedir (**Başlat (Start) → Denetim masası (Control Panel) → Yönetimsel Araçlar(Admin Tools)→ Yönetim (Computer Mngmnt) → Paylaşılmış Klasörler (Shared Folders) → Paylaşım(Shares)** Listesinde ADMINŞ bulunmalıdır. Yok, ise **C:\Windows** klasörü Windows\$ ismiyle paylaşımına açılmalıdır.
4. **Workgroup ortamı var ise tüm pc'ler için varsa sabit local admin kullanıcı adı ve parola yok ise her makinede local admin gurubuna üye kullanıcı adı ve parolalarını bilmek durumundasınız. Clientlere kurulum yaparken bu kullanıcı adı ve parolalar kullanılır. Domain yapısı var ise Domain admin kullanıcı adı ve parolası bu işlem için yeterlidir.**
5. Yönetimsel haklara sahip kullanıcı parolası boş olmamalıdır.
6. Kullanıcı PC' nin ERA server' e IPC,bağlantısını yapıp yapamadığını kontrol ediniz. Bu işlem için **Başlat > Çalıştır a CMD** yazıp **Enter** e basınız. Açılan komut istemi penceresinde aşağıdaki parametreleri giriniz.

net use \\serveradı\ipc\$

IPC\$ paylaşımı, ağ programları arasındaki iletişimde adlandırılmış yönlendirmeler kullanarak istemciler ile sunucular arasındaki geçici bağlantılarda kullanılır. Genelde ağ sunucularını uzaktan yönetmek için kullanılır.

7. Kullandığınız herhangi bir firewall Sunucu ve kullanıcı PC arasında veri trafiğini engellememelidir.
8. ERA Sever Kurulu olan sunucuda 2221 2222 ve 2224 portları açık olması gerekmektedir.
9. Kullanıcı PC' lerde aşağıdaki servisler çalışmalıdır.

- Remote Procedure Call (RPC).
- Remote Registry service.
- RPC Locater service "manual" el ile ayarlanmalı ve çalışmaması gerekmektedir.

12.Eset Smart Security Kurulu bir network te Eset Remote Administrator Console üzerinde tüm kullanıcılar için port ve web sitesi kısıtlaması yapabilir miyim?

ERAC kullanılarak ağınızdaki tüm kullanıcılarınız için port ve web kısıtlaması yapabilirsiniz. Bu işlemi gerçekleştirmek için aşağıdaki adımları takip ediniz.

Merkezi port kısıtlama (ESSBE)

1. Remote Administrator Console Programını çalıştırınız.
2. Client bölümünde herhangi bir PC üzerinde sağ tıklayınız ve seçeneklerden **Configuration** seçeneğine tıklayınız.
3. Açılan pencerede aşağıdaki butonlardan **New Task'** a, yanındaki kutucuğu işaretleyerek tıklayınız.
4. Açılan pencerede **Edit** butonuna tıklayınız.
5. Karşınıza gelen Konfigürasyon editör penceresinde sağ panelde **Personal Firewall>setup>filtrng mode seçeneğine** tıklayarak sağ bölümde **value'yı Policy-based mode** olarak değiştiriniz. Böylece kullanıcılar sadece sizin belirleyeceğiniz kurallar doğrultusunda veri trafiğini sağlayabilecekler.
6. Sağ panelden **Personal Firewall>setup>rule setup** a çift tıklayarak açılan pencerede üstte sekmelerden **rule'** ı seçiniz ve aşağıda **add default** butonuna tıklayınız.
7. Yukarıdan **Toggle detailed view of all rules** bağlantısına tıklayarak ESS tarafından eklenen varsayılan kurallar ile ilgili ayrıntıları görebilirsiniz. Bu pencere ile ilgili ayrıntılar aşağıda verilmiştir.

Kural adı – kuralın adı; kuralı etkinleştirmek veya devre dışı bırakmak için onay kutusunu işaretleyin veya işaretini kaldırın

Eylem – iletişimin ve eylemin yönünü gösterir

- ↑ - giden bağlantılara izin verilir
- ↓ - giden bağlantılar engellenir
- ↓ - gelen bağlantılara izin verilir
- ↓ - gelen bağlantılar engellenir
- ↑↓ - tüm bağlantılara izin verilir
- ↓↑ - tüm bağlantılar izin vermeyi veya reddetmeyi seçmenizi isteyen bir iletişim penceresi tetikler
- ↓↑ - tüm bağlantılar engellenir

Protokol – iletişim protokolü

Adres – uzak bilgisayarın adresi

Yerel bağlantı noktası – yerel bilgisayarın bağlantı noktası

Uzak bağlantı noktası – uzak bilgisayarın bağlantı noktası

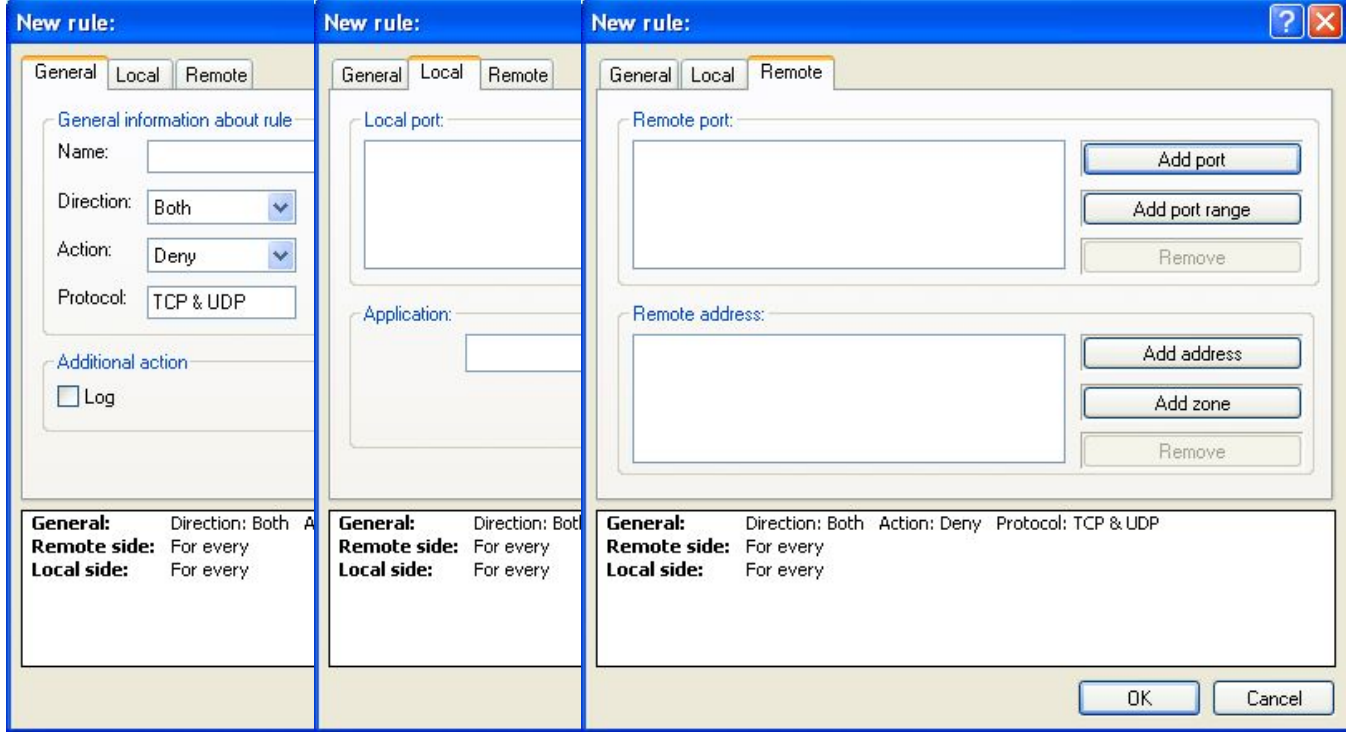
Uygulama – kuralın uygulandığı uygulamayı gösterir

Yeni – yeni kural oluşturmanızı sağlar

Düzenle – var olan kuralları düzenlemenizi sağlar

Sil – var olan kuralları silmenizi sağlar





General (Genel)

Name (Ad) – kuralın adı

Direction(Yön) – kuralın uygulanacağı yönü seçin

Action(Eylem) – iletişim kuralla eşleştğinde yürütülecek eylem

Protocol (Protokol) – kural için kullanılacak aktarım protokolü

Log(Günlük) – günlüğe kaydedilecek kuralla bağlantılı etkinlik

Notify User(Kullanıcıya bildir) – kural uygulandığında bir ileti görüntüler

Bilgi kutusu – kuralın özetini görüntüler. Bilgi kutusu üç sekmenin altında görüntülenir. Ana penceredeki kuralı tıklarızsanız, aynı bilgiyi görürsünüz (Araçlar > Kişisel Güvenlik Duvarı).

Local (Yerel)

Kuralın uygulanacağı yerel uygulamanın ve yerel bağlantı noktasının/bağlantı noktalarının adını ekleyin.

Local Port(Yerel bağlantı noktası):

Bağlantı noktası/bağlantı noktaları. Numara belirtilmezse, kural tüm bağlantı noktalarına uygulanır.

Add Prot (Bağlantı noktası ekle) – tek bir bağlantı noktası ekler

Add Port Range (Bağlantı noktası aralığı) ekle – bağlantı noktası aralığı ekler

Remove (Kaldır) – bağlantı noktalarını listeden kaldırır

Aplication (Uygulama) – kuralın uygulanacağı uygulamanın adı

Brows (Gözet) – kuralın uygulandığı uygulamanın konumunu eklemek için tıklatın

Uzak (Remote)

Remote Port(Uzak bağlantı noktası) – uzak bağlantı noktası numarası/numaraları. Numara belirtilmezse, kural tüm bağlantı noktalarına uygulanır.

Add Port Bağlantı noktası ekle – tek bir bağlantı noktası ekler

Add Port Range Bağlantı noktası aralığı ekle – iletişim bağlantı noktası aralığı ekler

Remove Kaldır – bağlantı noktalarını listeden kaldırır

Remote Address (Uzak adres) – kuralın uygulandığı adresi/adres aralığı/alt ağ veya uzak bölge. Değer belirtilmezse, kural tüm iletişime uygulanır.

Add address (Adres ekle) – uzak adres, adres aralığı veya alt ağ eklemenize olanak verir.

Add Zone (Bölge ekle) – oluşturulan bir bölge ekler. Bölge oluşturmak için Bölge sekmesini kullanın.

Remove (Kaldır) – bağlantı noktalarını listeden kaldırır

9. “Kişisel güvenlik duvarı engellenen bağlantı günlüğünü kaydetme” bölümünden güvenlik duvarı kayıtlarını her kullanıcı için takip edebilirsiniz. Böylece bu kayıtlarda gerekli bağlantılar ile ilgili kural oluşturabilirsiniz.

Merkezi web kısıtlaması (ESSBE-ENABE)

Tüm Kullanıcılarda sadece sizin istediğiniz web sitelerine girilmesini sağlayabilirsiniz. Bunun için aşağıdaki adımları takip ediniz.

1. Remote Administrator Console Programını çalıştırınız.
2. Client bölümünde herhangi bir PC üzerinde sağ tıklayınız ve seçeneklerden **Configuration** seçeneğine tıklayınız.
3. Açılan pencerede aşağıdaki butonlardan **New Task'** a, yanındaki kutucuğu işaretleyerek tıklayınız.
4. Açılan pencerede **Edit** butonuna tıklayınız.
5. Karşınıza gelen Konfigürasyon editör penceresinde sağ panelde **Personal Firewall>setup>List of blocked URL addresses** e çift tıklayınız. Açılan pencerede [http://*. *](http://*.) yazıp **add** butonuna tıklayınız. Böylece tüm kullanıcıların web erişimini kısıtlamış olursunuz. **Ok** butonuna tıklayarak pencereyi kapayınız.
6. Aynı bölümde **List of URL addresses excluded from filtering** e çift tıklayarak gelen pencerede kullanıcıların sadece sizin belirleyeceğiniz web adreslerini <http://www.google.com.tr> şeklinde ekleyiniz. **Ok** butonuna tıklayarak pencereyi kapatınız.
7. Sağ panelde **Console** butonuna tıklayarak gelecek olan onay penceresinde **yes** butonuna tıklayarak değişiklikleri kaydediniz.
8. Bir sonraki pencerede **Next** butonuna tıklayınız ve sağ bölümde yaptığınız ayarların uygulanacağı diğer PC' leride sağ bölüme çekerek tekrar aşağıdan **Next butonuna tıklayınız.**

Yapılan ayarların hemen uygulanmasını istiyorsanız bu bölümde hiç bir değişiklik yapmadan **Finish** butonuna tıklayınız. Ayarların sizin belirleyeceğiniz bir zamanda uygulanmasını istiyorsanız **Apply task after'** i işaretleyerek zamanı belirleyiniz.

13. ESET Remote Administrator Console üzerinden tarama zamanlayıcısı oluşturma (3.0 sürüm)

İsteğe bağlı tarama, virüs imza veri tabanı güncelleme, sistem başlangıcında dosya denetimi gibi konularda otomatik görev zamanlayıcıları oluşturabilirsiniz. Bu işlemi tüm bilgisayarlarda uygulamak için Eset Remote Administrator Console (ERAC') ı kullanabiliriz.

1. ESET Remote Administrator Console (ERAC) ı **Start → All Programs → ESET → ESET Remote Administrator Console.** e tıklayarak açınız.
2. ERAC ana pencereden **Tools → ESET Configuration Editor' ü** açınız.
3. Client bölümünde herhangi bir PC üzerinde sağ tıklayınız ve seçeneklerden **Configuration** seçeneğine tıklayınız.
4. Açılan pencerede aşağıdaki butonlardan **New Task' butonuna**, yanındaki **kutucuğu işaretleyerek** tıklayınız.
5. Açılan pencerede **Edit** butonuna tıklayınız

6. Konfigürasyon editörde **ESET Smart Security, ESET NOD32 Antivirus → ESET Kernel → Setup → Scheduler/Planner** altında **Scheduler/Planner: Total 0/0 (tasks/to delete)** e tıklayınız.
7. Sağ panelde Edit **butonuna** tıklayınız.

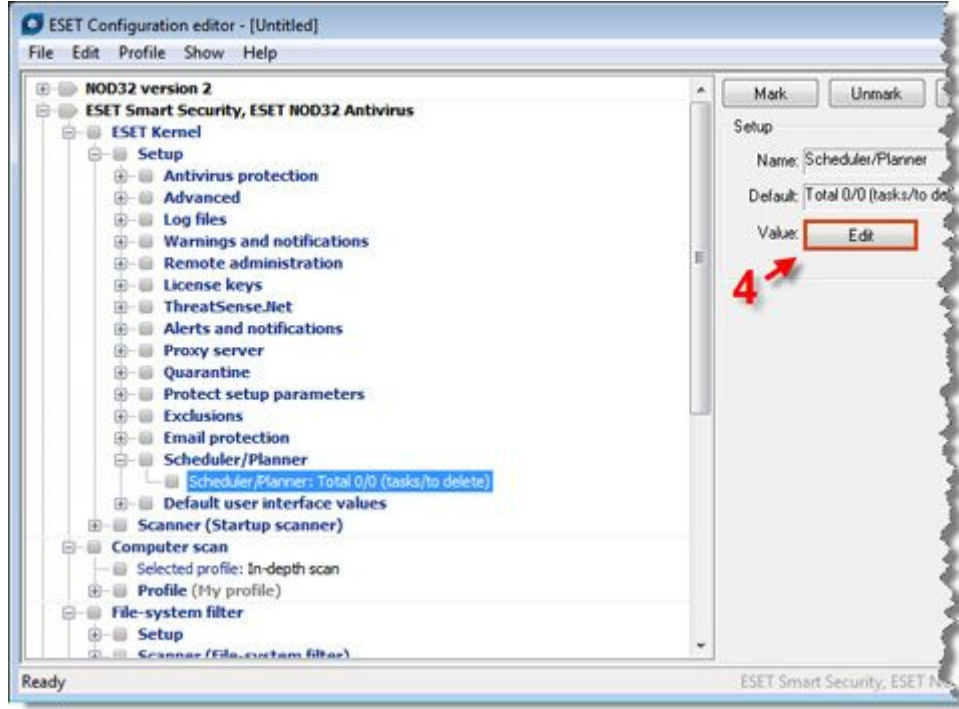
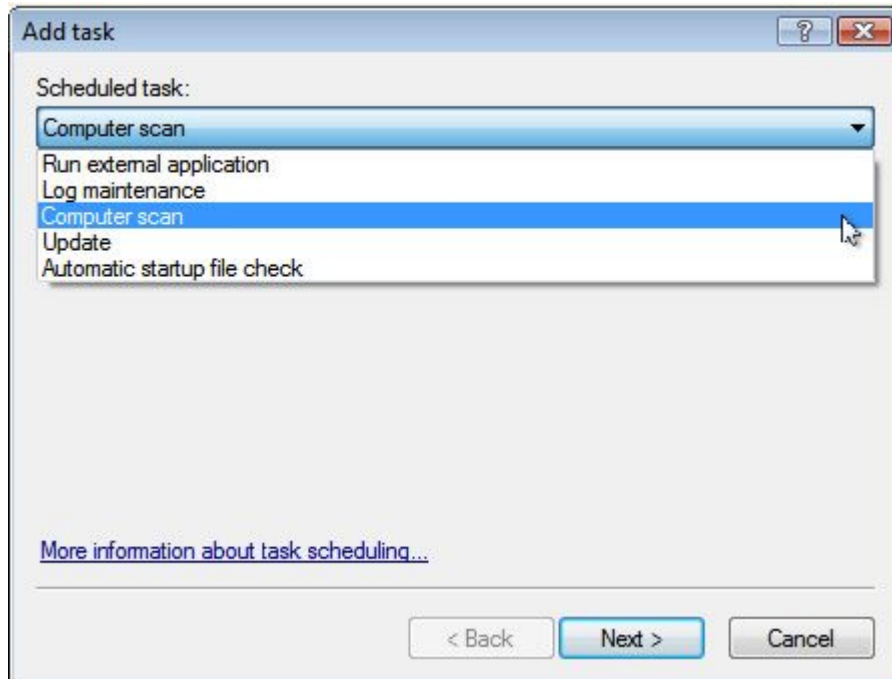
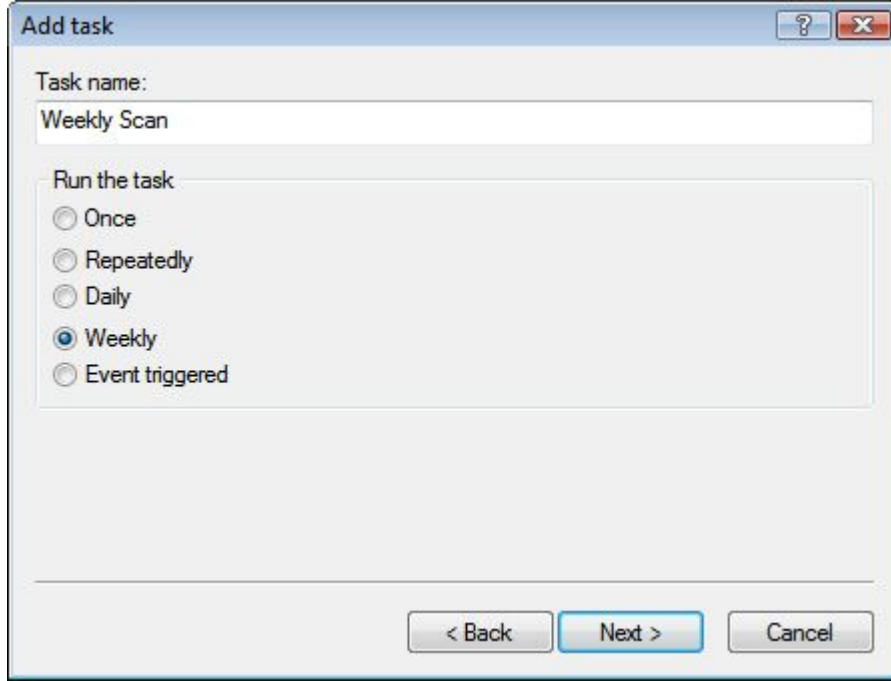


Fig. 1-1

8. Açılan **Schedule tasks** penceresinde **Add** butonuna tıklayarak zamanlayıcı oluşturma işlemini başlatalım.
9. Bu bölümde zamanlama yapılacak kategori seçilir. Biz **Computer Scan**'i seçerek bir tarama zamanlayıcısı oluşturalım.

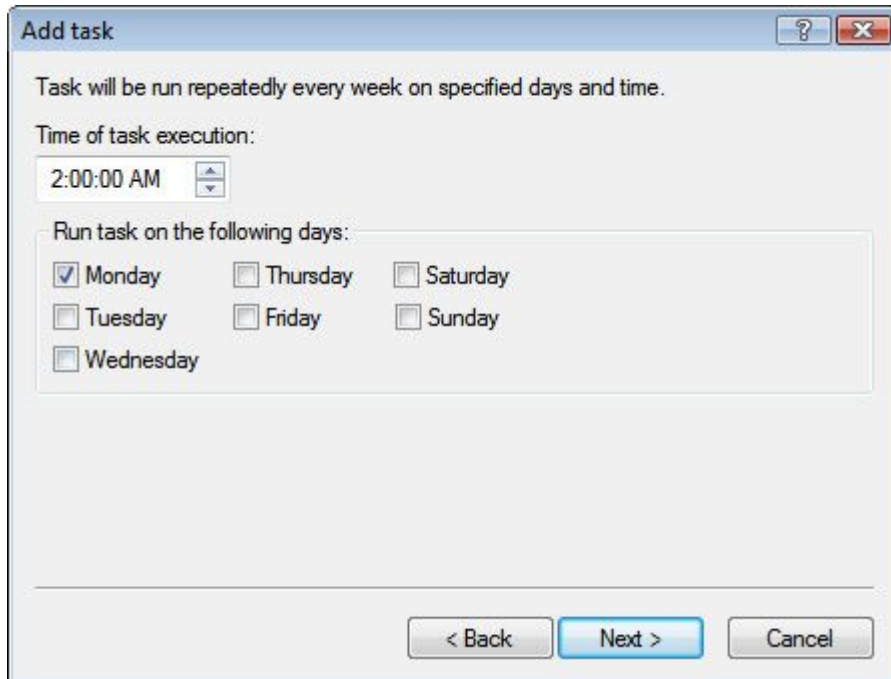


10. Task name bölümüne yapacağımız zamanlayıcıya bir isim verebiliriz. Aşağıdan zamanlayıcı için zaman kapsamını belirleriz. **Next** butonu ile bir sonraki pencereye geçiniz.



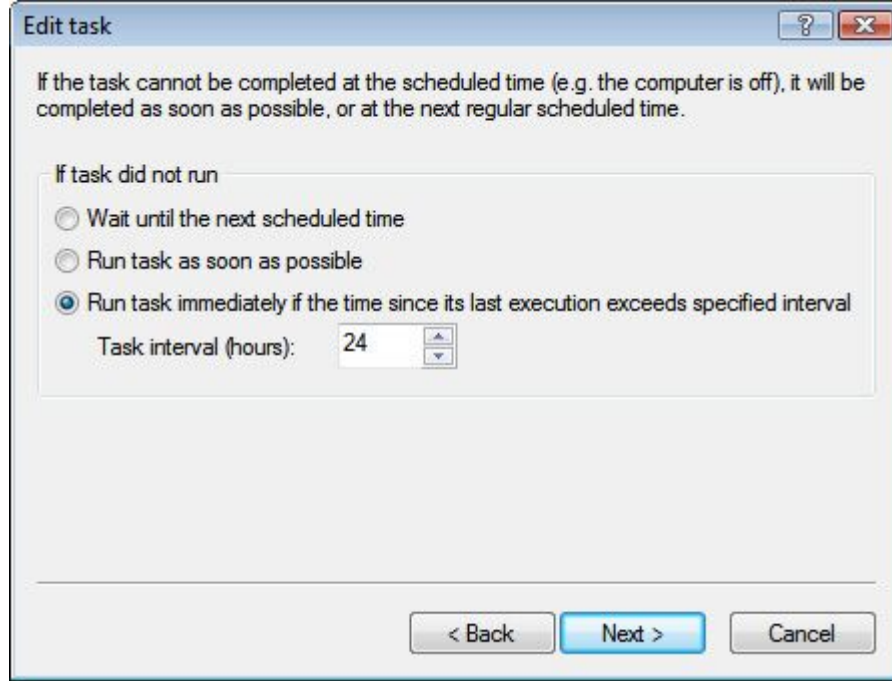
The screenshot shows a dialog box titled "Add task". It has a "Task name:" label and a text input field containing "Weekly Scan". Below this, there is a section titled "Run the task" with five radio button options: "Once", "Repeatedly", "Daily", "Weekly" (which is selected), and "Event triggered". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

11. Bir sonraki pencerede taramanın tekrarlanacağı süre belirlenir. Bu aşamaya kadar yapılan ayarlamalarda **Her hafta Pazartesi günü saat 2:00 da tarama yap** görevini belirledik **Next butonu ile bir sonraki pencereye geçiniz.**

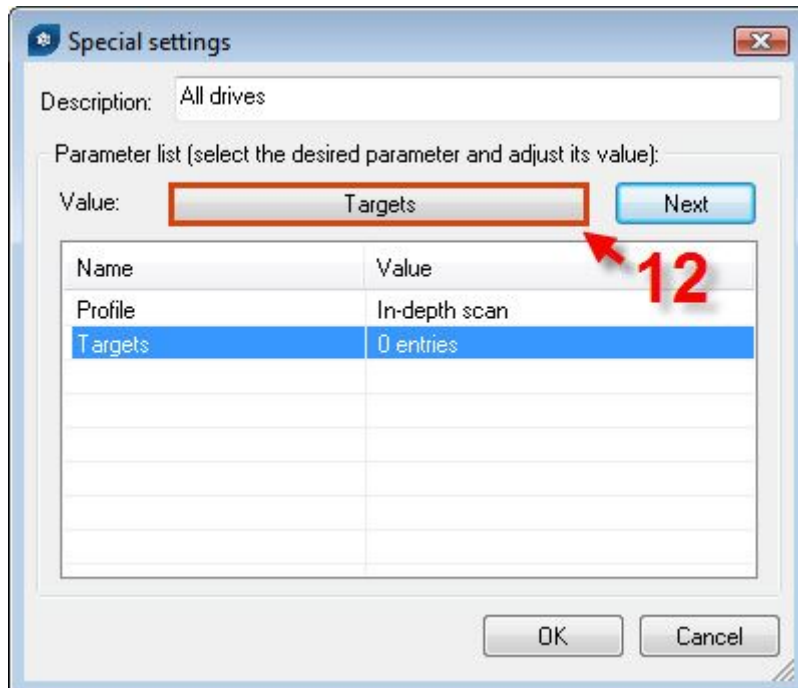


The screenshot shows a dialog box titled "Add task". It contains the text "Task will be run repeatedly every week on specified days and time." Below this, there is a section titled "Time of task execution:" with a time picker set to "2:00:00 AM". Underneath, there is a section titled "Run task on the following days:" with seven checkboxes for the days of the week: Monday (checked), Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

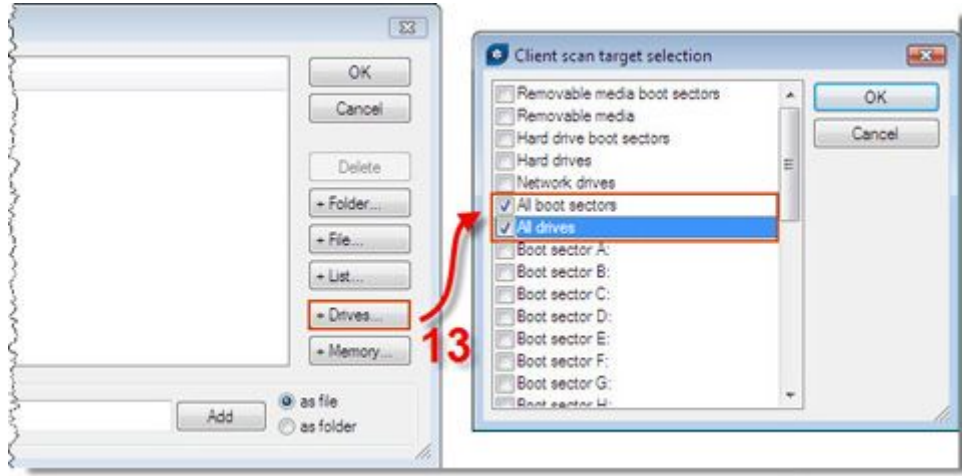
12. Bir sonraki aşamada eğer görev herhangi bir nedenden dolayı çalışmaz ise (bilgisayar kapalıdır veya network bağlantısı kopmuş olabilir vb) zamanlayıcının ne yapması gerektiğine dair ayarlama yapılır. **Wait until the next sc... Sonraki zamanlanan saate kadar bekle** yani bir hafta sonra Pazartesi gününe kadar hiç bir işlem yapılmaz **Run task as so... Şartlar uygun olur olmaz görevi hemen çalıştır. Run task immediately if the time since... Görevin son yürütülmesi üzerinden belirtilen aralıktan daha uzun geçtiyse görevi hemen çalıştır. Biz üçüncü seçeneği seçerek Next butonuna tıklayalım.**



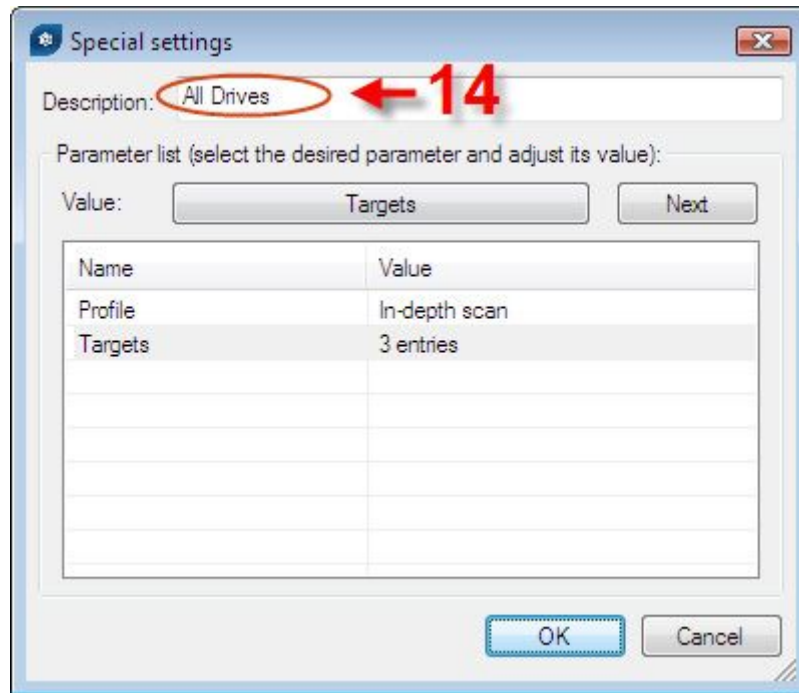
13. **Oluşturulan görev ile ilgili genel bilgiler penceresini Finish'e tıklayarak geçiniz.**
14. **Special settings** penceresinde tarama profili belirlenir. Tarama profilleri taranacak nesnelere temizleme seviyesi gibi faktörler ile birbirlerinden ayrılırlar **In-depth scan i** (derinlemesine tarama) seçiniz.
15. **Profil seçildikten sonra Targets** butonuna tıklanarak Tarama yapılacak lokasyon belirlenebilir.



16. Açılan pencerede **+Drives...** a tıklayarak **Taranacak sürücülerini belirleyiniz. Biz All boot sectors ve All drivers'i seçiyoruz.** Ayrıca **Memory** butonuna tıklayarak memory'de taranacağını belirtiyoruz. **OK.**' e tıklayarak pencereyi kapatınız.



17. Son olarak Description bölümünde bir tanım belirleyip **ok** butonuna tıklayarak pencereleri kapatınız.



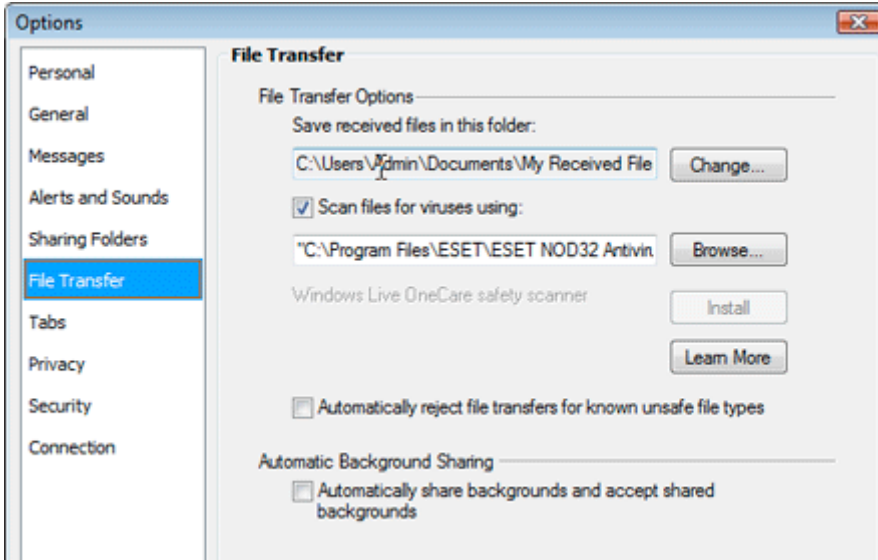
18. Sağ panelde **Console** butonuna tıklayarak gelecek olan onay penceresinde **yes** butonuna tıklayarak değişiklikleri kaydediniz.
19. Bir sonraki pencerede **Next** butonuna tıklayınız ve sağ bölümde yaptığınız ayarların uygulanacağı diğer PC' leri de sağ bölüme çekerek tekrar aşağıdan **Next butonuna** tıklayınız.
20. Yapılan ayarların hemen uygulanmasını istiyorsanız bu bölümde hiç bir değişiklik yapmadan **Finish** butonuna tıklayınız. Ayarların sizin belirleyeceğiniz bir zamanda uygulanmasını istiyorsanız **Apply task after'**ı işaretleyerek zamanı belirleyiniz

14. LiveMessenger üzerinden gelen dosyaların taranması için nasıl bir ayar yapmalıyım.

Çözüm

Live Messenger' e, gelen dosyaların taranması için Eset Nod32 Antivirus' e ait ecl.s. exe uygulamasını tanımlayabilirsiniz.

1. **Live Messenger** Programını açınız.
2. **Araçlar (Tools) > Seçenekler (Options)**' e tıklayınız.
3. Açılan pencerede sol bölümden **Dosya Transferi (File Transfer)** e tıklayınız.
4. **Dosyalarda virus taramasında bu uygulamayı kullan (Scan files for viruses using)** yanındaki kutucuğa tıklayarak işaretleyiniz.
5. **Gözet (Browse)** butonuna tıklayarak ecl.s.exe dosyasının yolunu gösteriniz. **C:\Program Files\ESET\ESET Smart Security\ec.s.exe** ayrıca **--log-file=log.txt --action=clean** gibi parametrelerde kullanılabilir.
6. **Ok** butonuna tıklayarak pencereyi kapatınız.



log-file=log.txt parametresini msn üzerinden alınan dosyalar ile ilgili bir kayıt oluşturmak istiyorsanız ecl.s.exe den sonra kullanabilirsiniz. **Action=clean** parametresini ise algılanan virüslerin temizlenmesini sağlar.

15. NOD32 Antivirus 2.7 kendisini otomatik olarak Eset Smart Security veya Eset Nod32 Antivirus 3.0' a sürüm güncellemesi yapabilir mi?

Eset, 2.70.xx(Eski) 3.0.xx(Yeni) gibi özellikle çekirdek yapısı farklı sürümler çıkarır. Bu sürümler kendi kapsamlarında virüs imza veritabanı güncellemeleri ile birlikte programın yapısını değiştirebilecek güncellemeleri de içerebilir. Temel yapıları tamamen farklı sürümler arası otomatik geçiş yeniden kurulum gerektirdiği için mümkün değildir. Ancak;

Bireysel kullanıcılar için ; <http://www.Nod32.com.tr/download/downloads.asp>

Kurumsal kullanıcılar için; <http://www.Eset.com/download/business.php>

adreslerinden son sürümü indirerek çalıştırabilir ve var olan eski sürüm üzerine kolayca kurarak versiyon güncellemesini gerçekleştirebilirsiniz.

16. ESET NOD32 Antivirus 3,0 / ESET Smart Security, SSL (Secure Sockets Layer) trafiğini tarayabilir mi?

Varsayılan ayarlar ile ESET Smart Security/ESET NOD32 Antivirus 3.0, POP3 protokolü TCP portları 110 ve HTTP protokolü TCP portu olan 80, 8080 ve 3128' üzerinden gelen tehditleri algılar ve engeller.

SSL kullanan (HTTPS, S/POP3, SSH, vb.) Protokollerinden sağlanan veri akışı, **SSL** kapsamında özel bir şifrelenmeye tabi tutulduğu için ESET Smart Security/ESET NOD32 Antivirus te Taranması için SSL portları belirtilse bile taranamaz. Ancak şifrelenmiş veri sistemde açıldığı an şifrede çözüleceği için anında Eset Nod32 tarafından taranır. Örneğin S/Pop3 protokolü üzerinden aldığınız mail'i sistemde acar açmaz şifrede çözüleceği için Eset Nod32 tarafından taranacaktır.

17. Virus imza veri tabanı güncellemesi yapamıyorum

PROBLEM:

Virus imza veri tabanını, gerek otomatik gerekse elle güncelleme yapıldığında **Virüs imza veri tabanı güncellenemedi** (Virus signature database could not be updated) hatasını almaktadır.

NEDEN

Bu hata Eset Nod32 Antivirus /Eset Smart Security' nin internet üzerinde Eset güncelleme sunucularına erişilemediği zaman meydana gelir.

Böyle bir problem ile karşılaştığınızda aşağıda belirtilen adımları takip ediniz.

1. Örneğin web tarayıcınızdan www.Eset.eu. Web sitesine erişip erişemediğinizi kontrol ederek internet bağlantınızı denetleyiniz.
2. Güncelleme sunucu ayarlarının doğru bir şekilde yapılandırılıp yapılandırılmadığını kontrol ediniz. Bunun için. Ana menüdeyken F5 tuşuna basınız ve açılan kurulum penceresinde **güncelle (Update)**'e tıklayınız ve sağ bölümde **güncelleme sunucusu(update server)** bölümünde **Otomatik Seç (Choose Automatically)** nin seçili olduğundan emin olunuz. Seçili değil ise yandaki ok işaretine tıklayarak seçiniz.
3. Eğer ikinci adımda da belirtilen ayarlar doğru bir şekilde yapılandırılmış ise aynı pencerede **Ayarlar(Setup)** butonuna tıklayarak **gelişmiş ayarlar (Advanced Setup)** penceresini açınız.
4. Bu pencerede **HTTP Proxy** sekmesine tıklayınız ve aşağıdaki seçeneklerden, eğer Proxy sunucusu kullanıp kullanmadığınızı bilmiyorsanız **Genel proxy sunucu ayarlarını kullan (Use global proxy server settings)**' i kullanmıyorsanız **Proxy sunucusu kullanma (Do not use proxy server)** Proxy sunucusu kullanıyorsanız, **Proxy sunucuyla bağlan (Connection through a proxy server)**'ı seçiniz ve bu bölümde gerekli parametreleri giriniz. [Global proxy server settings](#) ile ilgili daha ayrıntılı bilgi alabilirsiniz.
5. Eğer sisteminizde bir firewall kullanıyorsanız. Firewall üzerinde Eset güncelleme sunucularına **EKRN bağlantısının açık olduğundan emin olunuz**. Özellikle zone alarm firewall var ise

Programs tabında “**Allow Connect**” and “**Allow Server**” local network ve internet bağlantısı için EKRN’ e izin verecek şekilde bir kural oluşturunuz.

6. Güncellemeler, yerel network üzerinde belirlenen bir sunucudan alınıyor ise bu sorun ile ilgili sistem yöneticinize başvurunuz.


18. Kişisel güvenlik duvarı ile ilgili günlük tutma (Loglama) nasıl yapılır?

Bazı özel durumlar için Kişisel güvenlik duvarı tarafından meydana gelen olaylar ile ilgili günlük tutma işlemi aktif etmeniz gerekir. Örneğin sisteminize dışarıdan veya içerden gelen saldırılar ve türü ile ilgili bilgi almak isteyebilirsiniz veya bilgisayarınızın dışarıdan (İnternet) veya içerden gerçekleştiremediği bir bağlantı var ise firewall’un bunu engelleyip engellemediği engelledi ise hangi kurala göre bu işlemi yaptığını görmek isteyebilirsiniz. Ayrıca günlükleri program içinden görebileceğiniz gibi, bir dosyada depolanacak şekilde de ayarlayabilirsiniz.

- 1) **Başlat(Start) > Çalıştır(Run)**, komut çubuğuna ‘**regedit**’ yazarak **OK** a tıklayınız. HKLM\SOFTWARE\Eset\ESETSecurity\CurrentVersion\Plugins\01000200\Profiles\@My profile anahtarını açınız.
- 2) Sağ tarafta sağ tıklayarak **WriteBlockedToPcap** isimli yeni bir **DWORD** oluşturup değer olarak **1** veriniz.
- 3) Bilgisayarı yeniden başlatınız
- 4) Artık tüm bloklanan trafik ile ilgili log lar c:\Document and Settings\All Users\ApplicationData\Eset\EsetSmartSecurity\EpfwLog.Pcap dosyasında tutulacaktır.
- 5) Firewall ile ilgili problem yaşadığınız durumlarda **WriteBlockedToPcap** değerini **0** olarak değiştirerek **bilgisayarınızı kapatıp açınız ve yukarıda belirtilen EpfwLog.pcap dosyasını support@Eset.com adresine gönderiniz.**

19. İstenmeyen (SPAM) e-postaların depolandığı klasörü nasıl belirleyebilirim?

Eset Smart Security’de Antispam modülü tarafından algılanan istenmeyen e-postaların depolanacağı klasörü belirleyebilirsiniz. Bu işlem için aşağıdaki adımları takip ediniz.

1. ESET Smart Security programını  ikonuna tıklayarak veya **Start → All Programs → ESET → ESET Smart Security**’ye tıklayarak açınız.
2. Ana menüde **Ayarlar(Setup) > Antispam Modülüne** ardından sağ bölümde **Gelişmiş istenmeyen e-postaları önleme modülü ayarları (Advanced antispam module setup...)** na tıklayınız.(Eğer setup altında belirtilen seçenekler gelmiyor ise gelişmiş görünüme geçiş yapmak için klavyeden CTRL+M tuşlarına aynı anda basınız.)

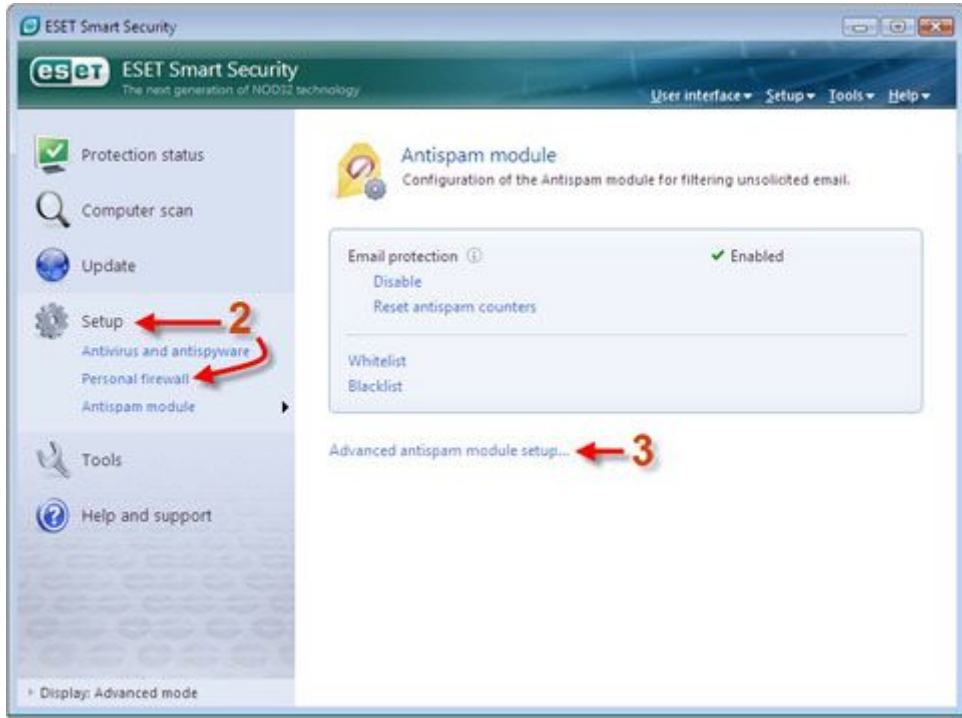
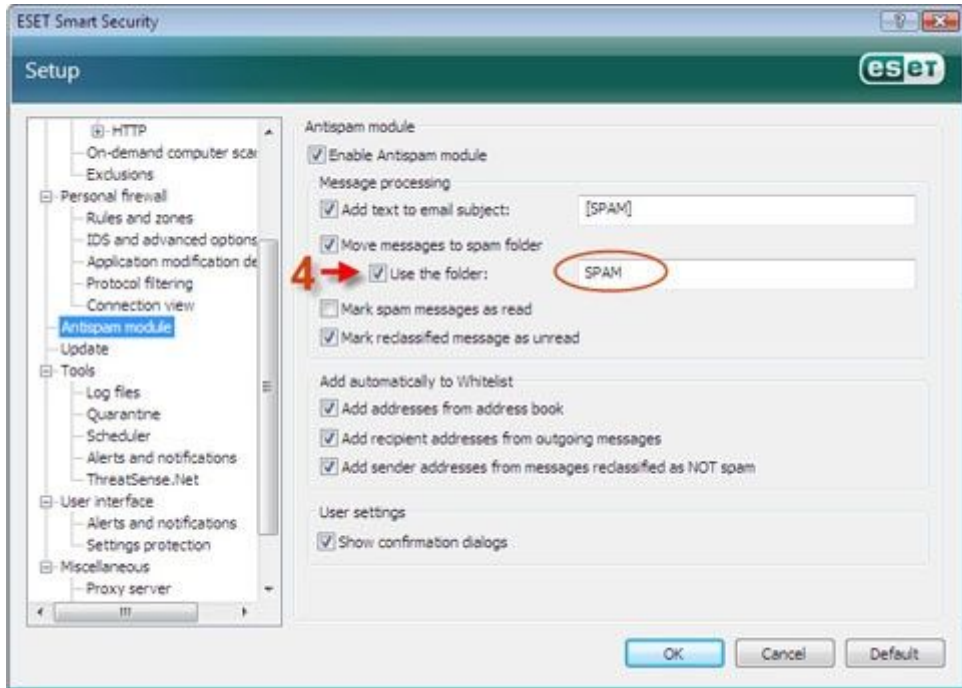
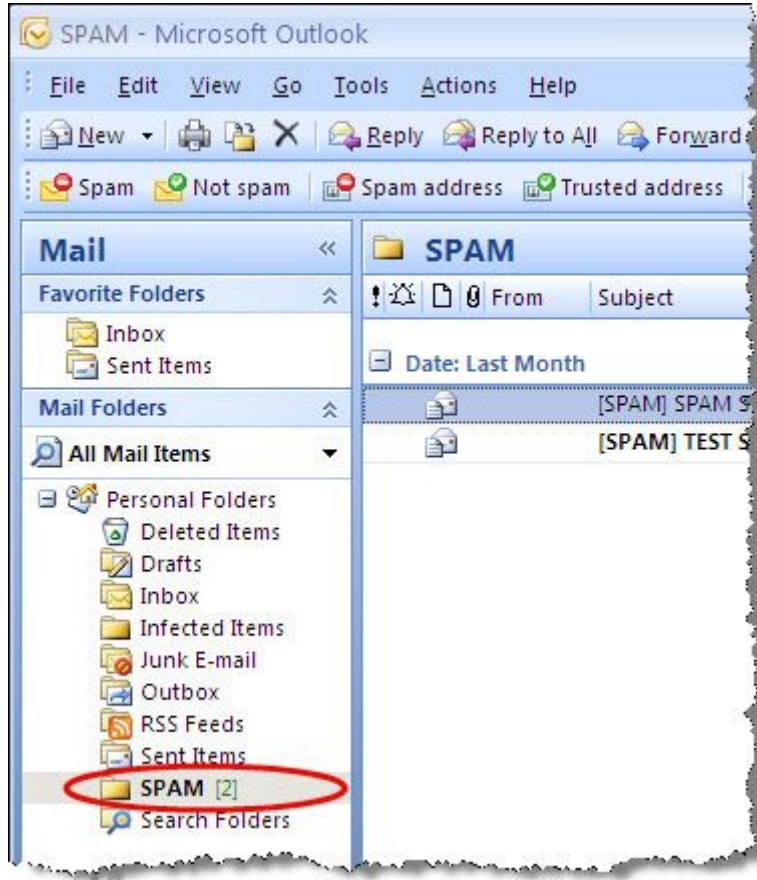


Fig. 1-1

3. Açılan kurulum penceresinde **iletleri istenmeyen eposta klasörüne taşı (Move message to spam folder)** ve **Kullanılacak Klasör (Use the Folder)** yanındaki kutucukları işaretleyerek sağ bölümde klasör ismini belirleyiniz. Örneğin bu klasörün adına aşağıda belirtildiği gibi SPAM verebilirsiniz. **Ok** butonuna tıklayarak pencereyi kapatınız.



4. Bu aşamadan sonra Microsoft Outlook veya Outlook Express'te Personal Folder içinde **Spam** isimli bir klasör oluşacaktır. Ancak bu klasör ancak istenmeyen bir eposta (Spam) geldiğinde otomatik olarak oluşur.



20. Eset Smart Security çalışır halde iken Windows Security Center Windows'un virüs koruması devre dışı uyarısı veriyor.

Bu sorun, Security Center tarafından kullanılan C:\Windows\system32\Wbem\Repository, klasöründeki dosyaların bozulmasından kaynaklanabilir.

Bu sorunu gidermek için;

- **Start > Run** a tıklayarak açılan komut penceresine **services.msc** yazarak enter'e basınız.
- Aşağıdaki listeden **Windows Yönetim Araçları/Yardımcıları (Windows Management Instrumentation)** servisini bulunuz ve üzerinde sağ tıklayarak **stop** a tıklayınız.
- C:/Windows/system32/Wbem/Repository dizinindeki tüm dosyaları siliniz
- Bilgisayarınızı kapatıp tekrar başlatınız. Böylece yukarıda belirtilen dizindeki tüm dosyalar tekrar oluşacaktır.

21. ESET Smart Security veya ESET NOD32 Antivirus' ün (32-bit veya 64-bit) sürümlerinden hangisini yüklemem gerekir?

İndireceğiniz Eset Programları İşletim sisteminizin yapısına göre değişmektedir. İşletim sisteminiz hangi işlemci türünü destekliyor ise (32bit-64bit) Nod32 Antivirus programının uygun olan (32bit 64bit) sürümünü indirmanız gerekmektedir.

İşletim sisteminizin 32bit veya 64bit olup olmadığını anlamak için aşağıdaki adımları takip edebilirsiniz.


Windows XP

1. **Bilgisayarım (My Computer)** üzerinde sağ tıklayınız gelen seçeneklerden **Properties** e tıklayınız.

Açılan pencerede **Genel(General)** sekmesinde **System** bölümünde **Microsoft Windows XP x64 Edition Version** yazıyorsa sisteminiz 64 bittir.

Eğer sistem bölümünde **Microsoft Windows XP Version [Yıl]** yazıyor ise sisteminiz 32 bittir

Windows Vista

1. **Start**  **Computer.** Üzerinde sağ tıklayınız ve seçeneklerden **Properties** e tıklayınız.

İşletim sisteminiz 64-bit ise **64-bit Operating System** yazısını **system type** bölümünde görebilirsiniz.

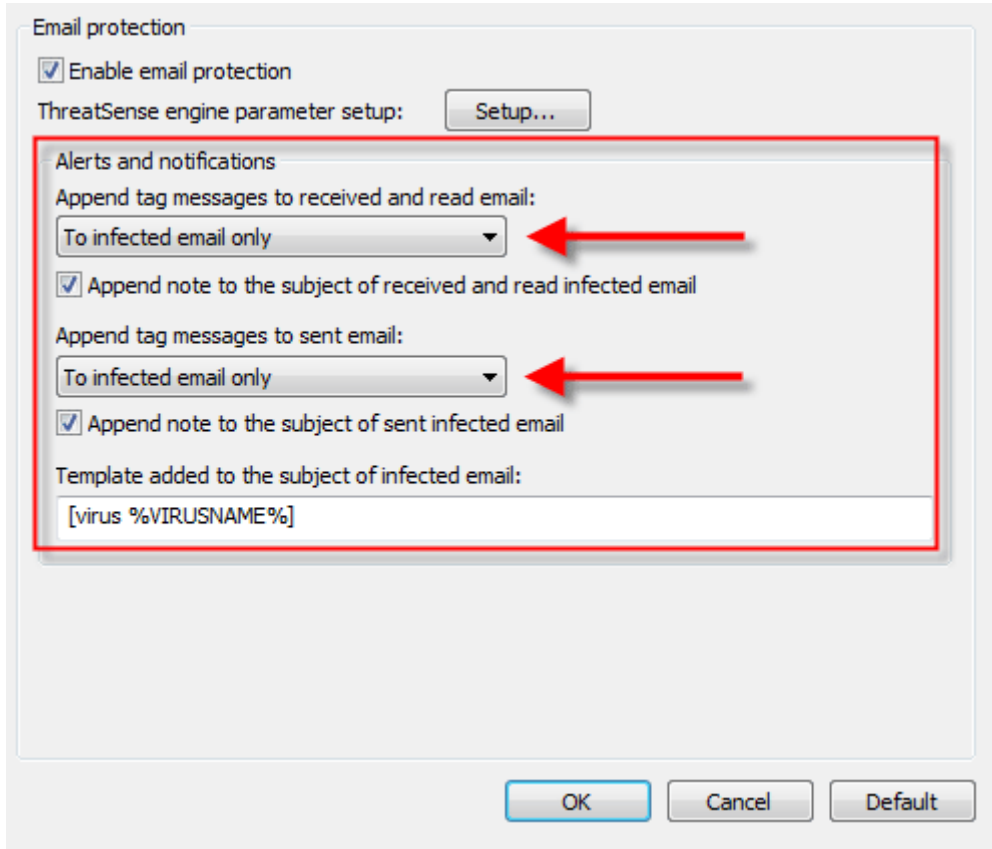
Eğer 32-bit ise : **32-bit Operating System** ibaresini **System type** bölümünde görebilirsiniz.

22. ESET Smart Security veya ESET NOD32 Antivirus'ün giden ve gelen e-postalara bilgi notu eklemesini nasıl engelleyebilirim?

Varsayılan olarak Nod32 Antivirus giden ve gelen tüm taranmış postalara bilgilendirme notu ekler. İsterseniz sadece virüslü e-postalara bu notun eklenmesini sağlayabilir. Veya bu işlemi tamamen devre dışı bırakabilirsiniz.

1. Kurulum penceresini açmak için ana menüdeyken klavyeden F5 tuşuna basınız.
2. Açılan pencerede sol panelden **Eposta Koruması (Email protection,)** a tıklayınız.

3. **Alınan ve okunan e-postalara alt bilgi ekle** (Append tag messages to received and read email) **Gönderilen etkilenen e-postanın konusuna not ekle** (Append tag messages to sent email) isterseniz bu ibareler yanındaki kutucukları boşaltarak ibarelerde belirtilen eylemi tamamen devre dışı bırakabilirsiniz. Ancak bu durum size gönderilen veya sizin gönderdiğiniz eklentili bir e postanın eklentisi virüslü ise Nod32 bu eklentiye silebilir bu yüzden eklentinin size veya gönderdiğiniz kişiye ulaşmamasının nedenini bilemeyeceksiniz. Bu nedenle her iki eylem için en uygun seçenek olan **Sadece virüslü mailer (To infected email only)** seçeneğini seçebilirsiniz. **Ok** butonuna tıklayarak pencereyi kapatınız.



23. ESET Smart Security and ESET NOD32 Antivirus kurulum problemleri.

Kurulum problemlerinin birçoğu Eset Smart Security ve Eset Nod32 Antivirus network filtreleme sürücülerini ile harici güvenlik yazılımlarına ait sürücüler arasındaki uyumsuzluktan kaynaklanmaktadır. Bu nedenle kurulum yapmadan önce mutlaka sisteminizde harici bir Antivirus veya firewall gibi bir güvenlik programının olmadığından emin olunuz. Bu durum haricinde yine Eset Smart Security ve Eset Nod32 Antivirus tarafından kurulum esnasında ihtiyaç duyulan **Temp** klasörlerinin olmaması veya aşırı derecede dolu olmasından veya harddisk ve ram gibi donanımsal arızalardan da kaynaklı kurulum hataları alabilirsiniz. Böyle durumlarda Eset kurulumu ile ilgili detaylı bilgiler içeren bir günlük (Log) oluşturabilirsiniz. Bu işlem için aşağıdaki adımları takip ediniz.

Windows içinde setupapi.log'u kullanarak kurulum loglaması oluşturulabilir. Bu işlem için;

1. Kayıt defterini, (**Start – Run** komut penceresine **regedit** yazıp enter tuşuna basarak açınız.
2. **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\LogLevel** anahtarını bulunuz ve değerini hexadecimal **0x0000FFFF** olarak belirleyiniz. Ve kayıt defterini kapatınız.

3. **Start > Run** a tıklayarak açılan komut penceresine **Eset Smart Security veya Eset Nod32 Antivirus Programının kurulum dosyasının yolunu yazıp hemen arkasına /lvx* install.log parametresini giriniz.**

Örnek: `C:\ess_nt32_ENU.msi /lvx* install.log`

24. Group Policy aracını kullanarak ESET Smart Security and ESET NOD32 Antivirus Programını yükleme.

1. Tüm Domain kapsamındaki kullanıcıların erişebileceği paylaştırılmış bir klasör oluşturulması gerekmektedir.
2. Smart Security, or ESET NOD32 Antivirus msi uzantılı kurulum paketini paylaşım klasörüne kopyalayınız.
3. **Start -> Administrative tools -> Active Directory Users and Computers' ı açınız.**
4. Domain ismi üzerinde sağ tıklayınız ve **Properties -> Group Policy -> Edit -> User Configuration altında Software Settings üzerinde sağ tıklayınız ve New Package' i seçiniz**
5. **Open** penceresinde paylaşım klasöründeki msi uzantılı kurulum dosyasının network yolunu belirleyiniz. **Örneğin \\Bilgisayar_adi\paylaştırılmış_klasör\kurulum_paketi.msi daha sonra Open butonuna tıklayarak paketi ekleyiniz. Bir sonraki pencerede Assigned' ı işaretleyip ok butonuna tıklayınız. Assigned seçeneği paketin otomatik olarak kullanıcı tarafına kurulmasını sağlar eğer Publish i seçecek olursak paket, kullanıcı tarafında Control Panel - Add or Remove programs - Add new program - Add programs from your network listesine gelir ve kurulum kullanıcıya bırakılır.**

25. ESET NOD32 Antivirus 3.0 ve ESET Smart Security arasındaki fark nedir?

Eset Smart Security ile Eset Nod32 Antivirus' e ait genel özellikler aşağıda belirtilmiştir.

(Eset Smart Security—Eset Nod32 Antivirus)

1- Antivirus & Antispyware: Bu modül, ilk defa Nod32 Antivirus sisteminde kullanılan ThreatSense tarama çekirdeği üzerine inşa edilmiş ve yeni Eset Smart Security alt yapısında daha da geliştirilmiştir. ESS ile birlikte gelen yeniliklerden bir kaçını aşağıda gösterilmiştir.

- **Gelişmiş Temizleme:** Bu özellik, sisteme sızabilecek virüslerin birçoğunun kullanıcı müdahalesi olmaksızın arka plandan otomatik olarak temizlenmesini sağlar.
- **Arka Plan Tarama Modu:** Virüs taraması yaparken, arka plan tarama modunu seçerek sistem performansını etkilemeden sistem tarama işlemi gerçekleştirilebilir.
- **Daha Küçük Güncelleme Dosyaları:** Çekirdek optimizasyon işlemleri, güncelleme dosyalarının 2.7 versiyonuna göre daha küçük olmasını sağlar. Ayrıca bu dosyaların bozulmasına neden olabilecek dış etkenlere karşı daha da güçlendirilmiştir.
- **URL filtreleme:** Girilmesi sakıncalı siteleri, engellenen url listesine girerek engelleyebilirsiniz.
- **E-posta Program Entegrasyonu:** Sadece MS Outlook değil, aynı zamanda Outlook Express ve Windows mail ile tam bütünleşik çalışıp tüm mail protokollerinden gelen e-postaların virüs taramasını yapar.
- **Diğer:** Ek opsiyonlar ile daha da esnek hale getirilmiş Gerçek zamanlı dosya koruması, virüs bulaşmış dosyalara erişimin engellenmesi, taramalar esnasında sistem erişiminde minimum performans .

Sadece Eset Smart Security' de bulunmaktadır.

2- Kişisel Güvenlik Duvarı (Personal Firewall): Eset Smart Security ile bütünleşik çalışan en önemli modüllerden biridir. Sisteminize gelen ve sisteminizden giden tüm veri trafiğini monitöre edebilir, ip, uygulama ve protokol bazında yasaklar ve izinleri yönetebilirsiniz.


- Network Monitör: Lokal sistem için network trafiğini ayrıntılı bir şekilde gözlemlemenizi sağlar. Veri akışının hangi makineden, hangi porttan, hangi uygulamadan, hangi ip den gerçekleştiğini ayrıntılı bir şekilde izleyebilirsiniz.
- Network Filtreleme Mod ları: Otomatik, Etkileşimli, İlke Tabanlı olmak üzere üç temel filtreleme seçeneği vardır. Otomatik modu seçerek veri trafiği filtrelemesi sadece ESS tarafından belirlenen kurallara göre yapılır. Etkileşimli Mod, sisteminize gelen ve sisteminizden giden tüm veri akışı ile ilgili uyarıları görmenize, eğer güvendiğiniz bir bağlantı ise kural oluştur seçeneğini kullanarak kalıcı bir kural oluşturmanızı sağlar. Böylece aynı bağlantı için her defasında uyarı ile karşılaşmazsınız.

Sadece Eset Smart Security' de bulunmaktadır.

3- Antispam Modülü: Günümüzde reklam, tuzak vb. amaçlı gönderilen istenmeyen e-postalar, her geçen gün artmaktadır. Bu nedenle antispam koruması da doğru orantılı olarak büyük bir önem kazanmaktadır. Ess antispam modülü tüm e-posta istemci programlarıyla uyumlu olarak çalışır. ESS, E-posta istemci programına kendi antispam araç çubuğunu ekleyerek istenmeyen e-postaları kolaylıkla belirlemenizi ve engellenizi sağlar. Bu özelliğinin dışında sizin istemediğiniz e-postaların içeriğine ilişkin başlıklar oluşturur ve benzer mailler geldiğinde bu başlıklar ile karşılaştırma yaparak gelen e-postanın spam değerlendirmesini yapar.

26. Belirleyeceğim sitelere girilmesini nasıl engelleyebilirim?

Eset Nod32 Antivirus veya Eset Smart Security' de Web Erişim Koruması özelliğiyle belirleyeceğiniz sitelerin engellenmesini aşağıdaki adımları takip ederek yapabilirsiniz.

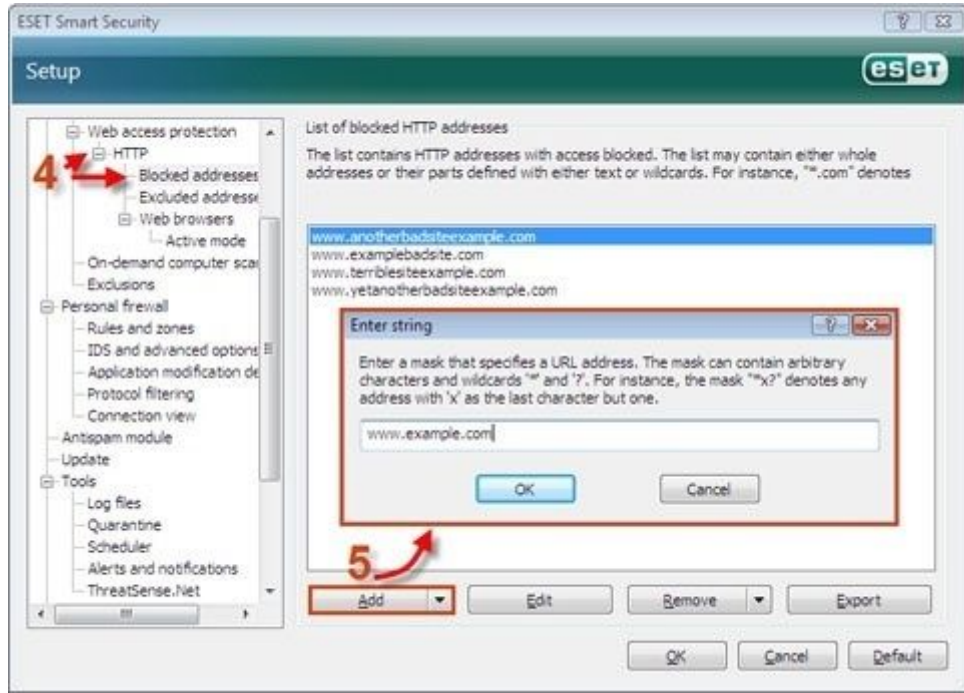
1. Masaüstünde sağ alt köşede  ikonuna veya **Start → All Programs → Eset → ESET Smart Security** veya **Eset Nod32 Antivirus'** a tıklayarak programı çalıştırınız.
2. Ana pencerede **Setup → Antivirus and Antispyware ardından sağ bölümde Web Erişim Koruması (Web Access Protection) altında Yapılandır (Configure).**e tıklayarak gelişmiş kurulum penceresini açınız.



3. Sağ bölümde yapılandırma ağacından **HTTP > Engellenen Adresler (Blocked Addresses)** i seçiniz
4. Sağ bölümde engellenen adreslerin listesi bulunmaktadır. Bu bölümde **Ekle (Add)** butonuna tıklayarak açılan pencerede eklemek istediğiniz web adresini aşağıdaki gibi yazarak **OK** butonuna tıklayınız.

NOTE: Adres eklemelerde "*" ve "?" parametrelerini de kullanabilirsiniz örneğin nk01.warshare.com den nk98.warshare.net e kadar tüm web sitelerini engellemek istiyorsunuz bu durumda eklemeyi "nk??.warshare.*" şeklinde yapmanız gerekmektedir.

Ayrıca **Ekle (ADD)** butonu yanındaki aşağı ok işaretine tıklayarak açılan seçeneklerden **Dosyadan (From file)** a tıklayarak gelen pencerede daha önceden oluşturulmuş içinde bu listeye ekleyeceğimiz web adreslerinin bulunduğu bir txt dosyasını gösterip listeye bu adresleri ekleyebilirsiniz. Bu gibi zararlı sitelerin listesini içeren txt dosyaları çeşitli güvenlik sitelerinde yayımlanmaktadır.



27. Windows Installer Kurulum sonlandırıldı (installation is stopped) hatasını vermektedir.

ESET Smart Security veya ESET NOD32 Antivirus Windows 2000 işletim sistemi üzerine kurulurken Windows Installer **installation is stopped** hatası veriyor ise Windows Installer 2.0 programını [indirerek](#) sisteminize kurunuz. Veya Windows 2000 service pack güncelleme paketini [indirip](#) sisteminizi güncellemeniz de bu sorunu giderecektir.

28. Windows işletim sistemlerinin ESET NOD32 Antivirus/ESET Smart Security güncellemelerini alabilmesi için ESET Security for Linux/FreeBSD v. 3.x üzerinden mirror klasörü oluşturmak.

- Konfigürasyon dosyasını /etc/Esets/Esets.cfg dizininden text editör ile birlikte açınız.

- av_mirror_enabled seçeneğinin karşısına **yes** yazarak mirror'u etkinleştiriniz.

```
# av_mirror_enabled = yes/no  
# Enables ESETS mirror.  
av_mirror_enabled = yes
```

- Mirror klasörü için bir yol belirleyiniz

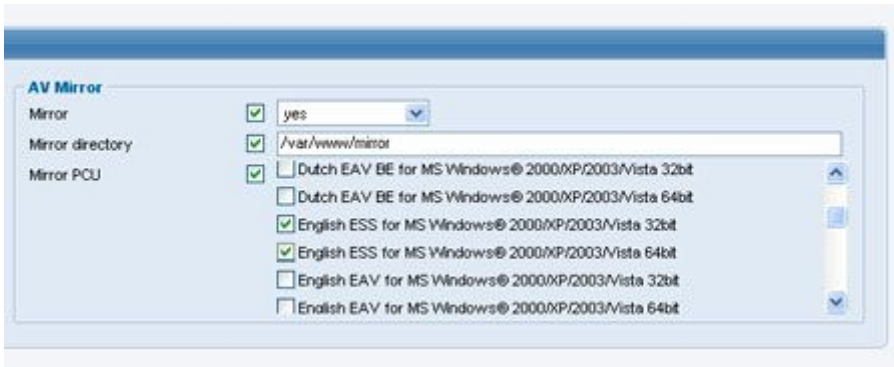
```
# av_mirror_dir = "directory"  
# Directory of ESETS mirror.  
av_mirror_dir = "/var/lib/Esets/mirror"
```

- EAV/ESS için Program bileşen güncelleme isimlerini aşağıdaki gibi belirleyiniz

```
# av_mirror_pcu = "mod1:mod2:..."  
# List of so called ESETS anti-virus Program Component Update modules  
# to be mirrored from ESET server.  
av_mirror_pcu = "ESS_WINNT32_1033:ESS_WINNT64_1033:EAV_..."
```

ESS_WINNT32_1033:ESS_WINNT64_1033 ESS nin İngilizce (32 and 64 bit) versiyonları içindir. Yükleme istediğiniz diğer bileşenler ile ilgili ayrıntıları http://download.Eset.com/manuals/Eset_file_security.pdf Adresinden edinebilirsiniz.

Yukarıda yapılan ayarlar ESET Web ara yüzünden de yapılabilir.



Mirror klasörü, **Esets_update** Komutu ile de güncellenebilir. Additional info can be founded in the man page „man Esets_update“.

```
/usr/sbin/Esets_update -u username -p password --mirror-dir /var/lib/Esets/mirror --mirror-pcu  
ESS_WINNT32_1033:ESS_WINNT64_1033:EAV_WINNT32_1033:EAV_... --mirror
```


Esets_update komutu ile ilgili ayrıntılı bilgi almak için **man** komutunu kullanabilirsiniz.

Örnek: man Esets_update

29. ESET NOD32 Antivirus Business Edition ve ESET Smart Security Business Edition' de Mirror özelliğini nasıl aktif edebilirim?

Eset, Kurumsal ürünlerinde (EAVBE-ESSBE) mirror özelliği aktif edilerek kullanıcıların yerel network'te merkezi bir noktadan virüs imza veritabanı güncellemelerinin alınmasını sağlar.

Mirror özelliğini etkinleştirmek için aşağıdaki adımları takip ediniz.

- 1- Eset Nod32 Antivirus programını sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak açınız.
- 2- Program açıldıktan sonra klavyeden **F5** tuşuna basınız.

- 3- Açılan kurulum menüsünde sol panelden **Diğer (miscellaneous) ' a** tıklayınız ve sağ bölümde **Ekle (add)** butonuna tıklayarak lisans dosyanızın yolunu belirleyiniz. Lisans dosyasının yolu **CD sürücüsü\lisans\Security veya RA\Nod32.lic** dir.
- 4- Lisans dosyasını ekledikten sonra **ok** butonuna tıklayarak pencereyi kapatınız.
- 5- Ana menüdeyken tekrar **F5** tuşuna basarak kurulum penceresini açınız.
- 6- Sağ panelden **güncelle** (Update) seçeneğine tıklayınız ve sağ bölümden **ayarlar (Setup)** butonuna tıklayınız. (Setup butonu gelmiyorsa bu pencereden çıkınız ve ana menüdeyken **CTRL M** tuşlarına aynı anda basınız. Tekrar aynı bölüme geldiğinizde setup butonunu görebilirsiniz.)
- 7- Karşınıza gelen pencerede **ayna lama** (mirror) sekmesine tıklayınız.
- 8- **Güncelleme yansımaları oluştur (Create update mirror)** i işaretleyiniz.

Ok butonuna tıklayarak pencereleri kapatınız.

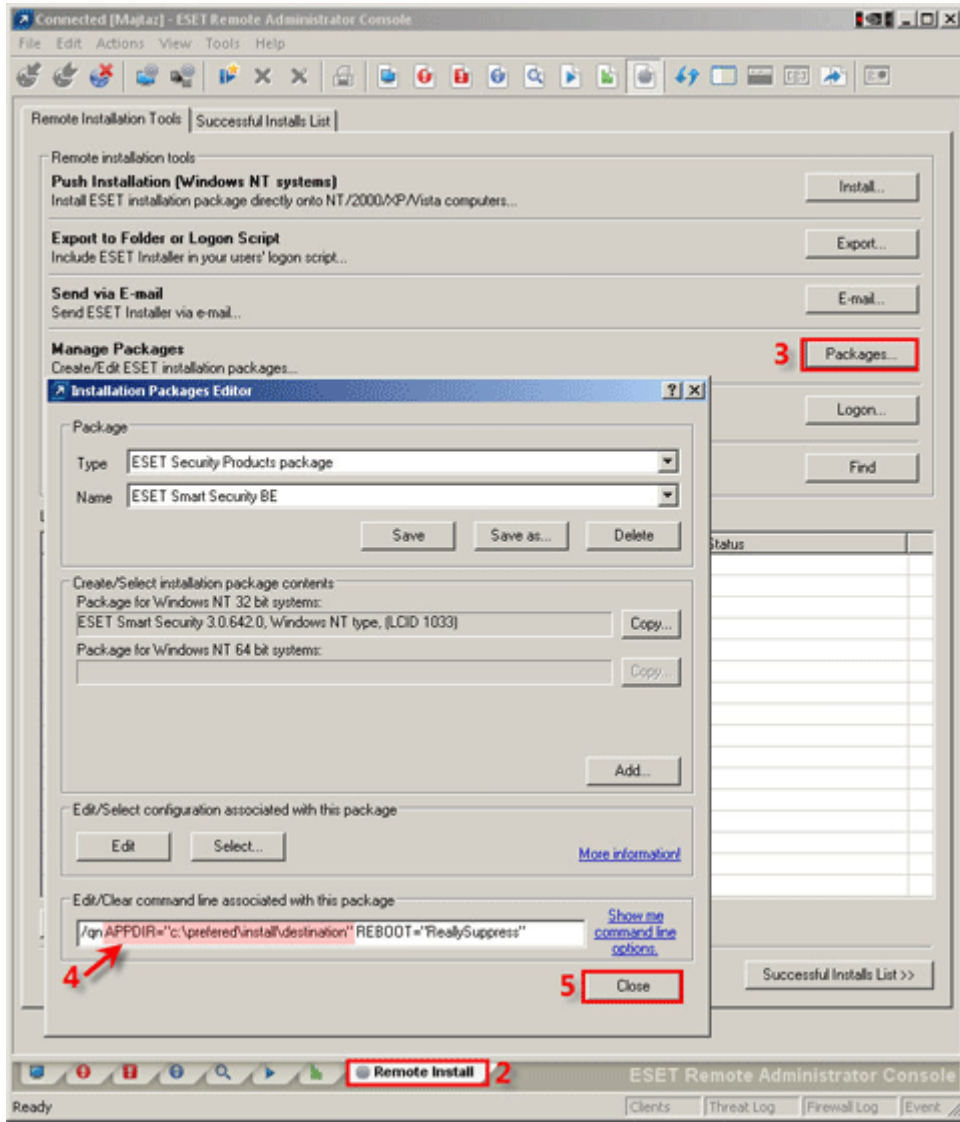
30. ESET Smart Security/ESET NOD32 Özel kurulum paketi oluşturma.

ESET Remote Administrator Console ERAC kullanarak ESET Smart Security/ESET NOD32 Antivirus otomatik kurulum paketleri oluşturabilirsiniz.

1. ESET Remote Administrator Console (ERAC)' ı çalıştırınız
2. **Remote Install tabından Packages butonuna tıklayınız.**
3. Name bölümünden daha önce oluşturduğunuz paketi seçiniz.
4. **Edit/Clear command line ass...** Komut satırına aşağıdaki parametreyi ekleyiniz.

APPDIR="c:\tercih edilen\kurulum\yolu"

5. **Close butonuna tıklayınız ve gelen uyarı penceresinde yes' e tıklayarak değişiklikleri kaydediniz.**
6. Install butonuna tıklayarak oluşturduğunuz paketi kullanıcı PC' lere kurabilirsiniz.



Komut satırından otomatik kurulum

1. **Start >Run** Komut satırında **CMD** yazarak enter tuşuna basınız.
2. Komut penceresi açıldıktan sonra aşağıdaki komut ve parametreleri yazarak enter tuşuna basınız.

```
msiexec /i "\\server\path\to\package.msi" APPDIR="c:\preferred\install\destination"  
ADMINCFG="\\server\path\to\cfg.xml" /qn
```

Yukarıdaki komut ve parametreleri bat uzantılı bir dosyaya kopyalayabilir istediğiniz kullanıcıda çalıştırarak Eset kurulumunu gerçekleştirebilirsiniz. Ayrıca bu bat dosyasını Active directory de tüm kullanıcıların oturum açılırken çalışmasını GPO üzerinden sağlayabilirsiniz.

Örnek Kurulum

1. **Server** isimli sunucu üzerinde **Paylaşım** isimli bir klasör oluşturarak paylaşıma açınız.
2. **Remote Administrator Console** Programını çalıştırarak üstteki menülerden **Tools** ardından **Eset Configuration Editor** e tıklayarak Konfigürasyon Editor penceresini açınız.

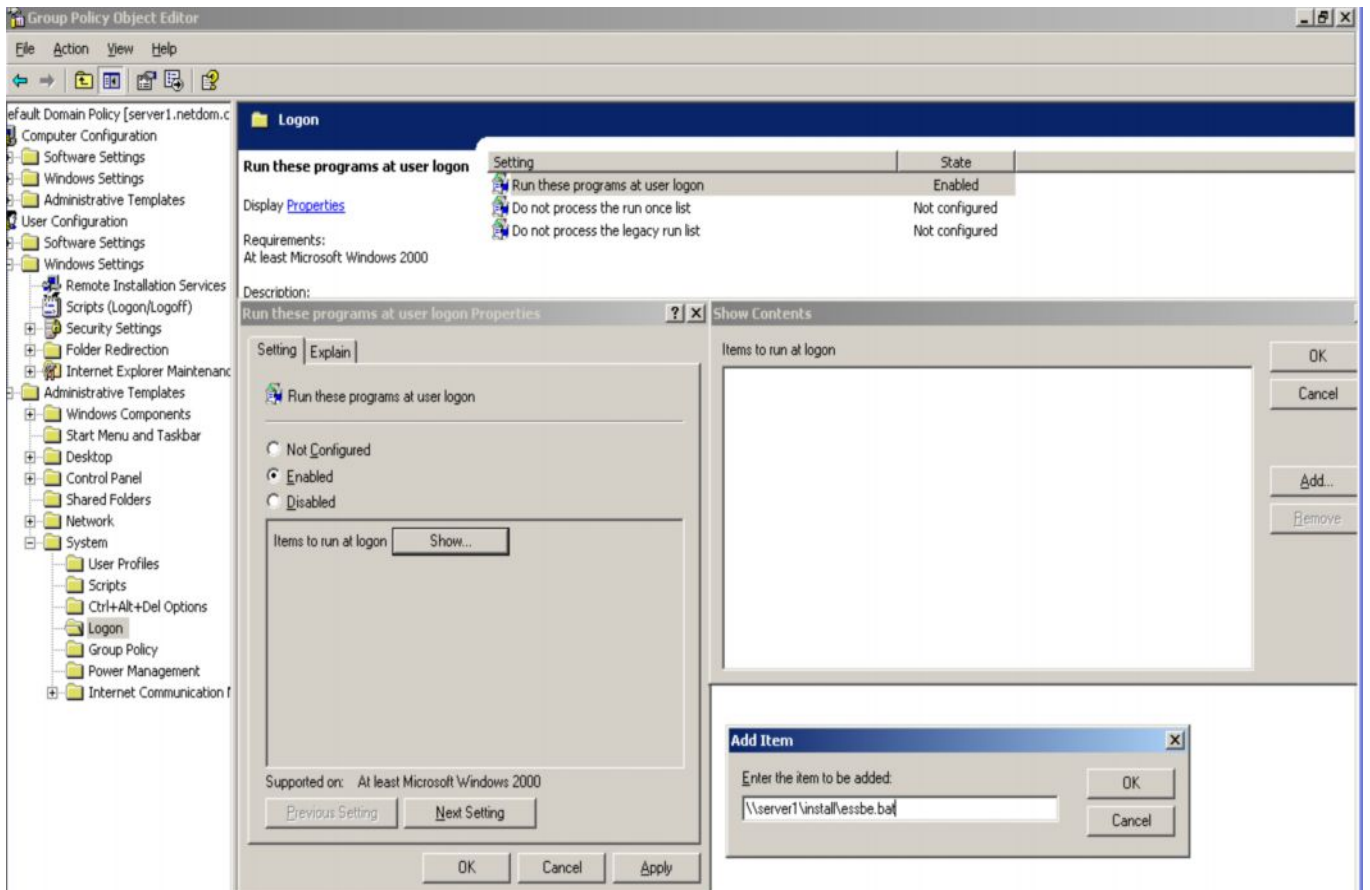
3. Bu pencerede istediğiniz ayarlamaları yaptıktan sonra **file > Export Selected To** seçerek açılan pencerede yapılandırma dosyasının adına **cfg** vererek daha önce paylaşım açtığınız **paylaşım** klasörü içine kaydediniz.
4. CD veya internetten temin ettiğiniz ESSBE/EAVBE msi uzantılı kurulum dosyasını da **paylaşım** klasörüne atınız ve ismini **Esetinstall.msi** olarak değiştiriniz. Bu aşamadan sonra artık kurulum parametreleri için gerekli bilgilere sahibiz.
5. Yeni bir text dosyası oluşturarak içine aşağıdaki gibi gerekli komut ve parametreleri giriniz.

```
msiexec /i "\\server\paylaşım\Esetinstall.msi" APPDIR="c:\program files\Eset" ADMINCFG="\\server\paylaşım\cfg.xml" /qn
```

6. Yukarıdaki komut ve parametreleri girdikten sonra dosyayı kaydedip kapatınız. Bu dosyayı istediğiniz kullanıcı PC' de çalıştırarak Eset kurulumunu gerçekleştirebilirsiniz.


Group policy üzerinden oluşturulan bat dosyasının tüm kullanıcılarda çalışmasını sağlamak için;

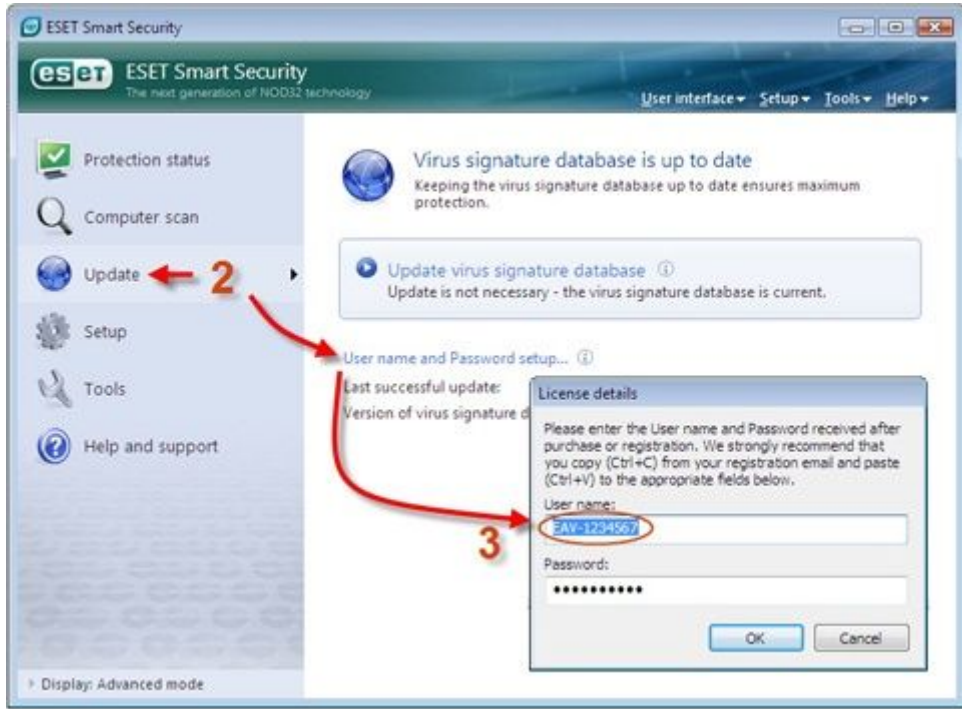
1. Active directory users and computers' i açınız ve domain ismi üzerinde sağ tıklayınız ve **Properties -> Group Policy -> Edit -> User Configuration > Administrative Templates > System > logon > Run these programs at user logon' e çift tıklayınız**
2. Açılan pencerede **Enable' i işaretleyerek aşağıdan show butonuna tıklayınız.**
3. **Show contents penceresinde add butonuna tıklayarak tekrar açılan add item penceresinde bat dosyasının network yolunu belirleyiniz.**
4. **Ok butonlarına tıklayarak pencereleri kapatınız.**
5. **Start >run komut penceresine gpupdate /force yazarak enter' e basınız.**
6. **Artık kullanıcı PC' lerde bir sonraki sistem açılışında ESSBE/EAVBE otomatik olarak kurulacaktır.**




31. Kullanıcı Adı ve Parolamı ESS/ENA üzerinde nasıl gösterebilirim?

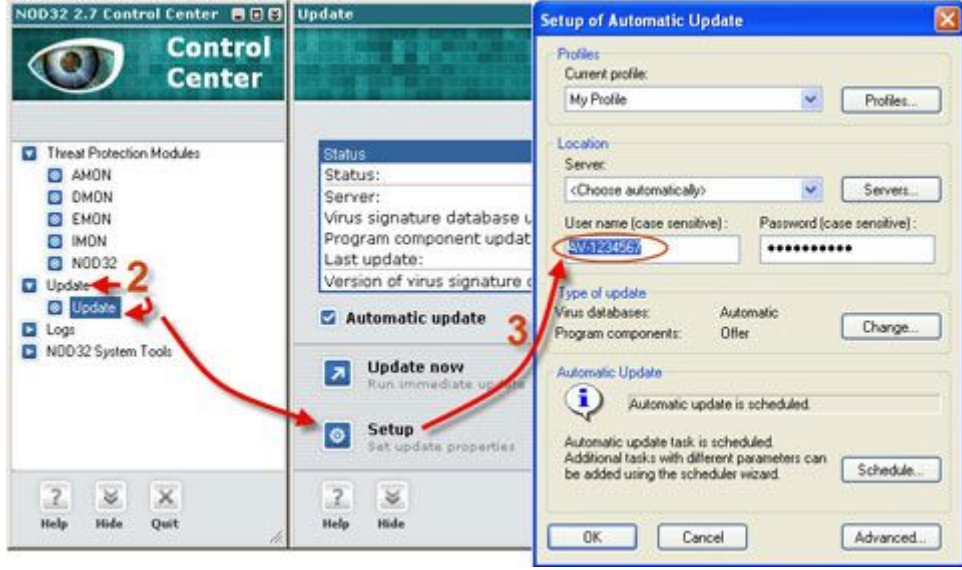
ESS veya ENA ilgili yaşayacağınız herhangi bir sorun için sisteminizde mevcut kurulu olan Nod32 Antivirus Programı içinden kullanıcı adınızı öğrenip destek@Nod32.com.tr adresine yaşadığınız sorun ile birlikte gönderebilirsiniz. Kullanıcı adınızı öğrenmek için aşağıdaki adımları takip ediniz.

1. Masaüstünde sağ alt köşede uygulama çubuğundan  ikonuna çift tıklayarak veya **Start → All Programs → ESET → ESET Smart Security** veya **ESET NOD32 Antivirus**. a tıklayarak programı çalıştırınız.
2. Ana menüden **Güncelle (Update)** ardından sağ bölümde **Kullanıcı adı ve parola kurulumu (User name and Password Setup...)** a tıklayınız.
3. Açılan **Lisans ayrıntıları (License Details)** penceresinde **Kullanıcı adı (Username)** alanındaki bilgiyi aşağıdaki bilgiyi destek@Nod32.com.tr adresine göndereceğiniz epostaya ekleyerek gönderiniz.





ESET NOD32 v2.7 üzerinde lisans bilgilerinin konumu;

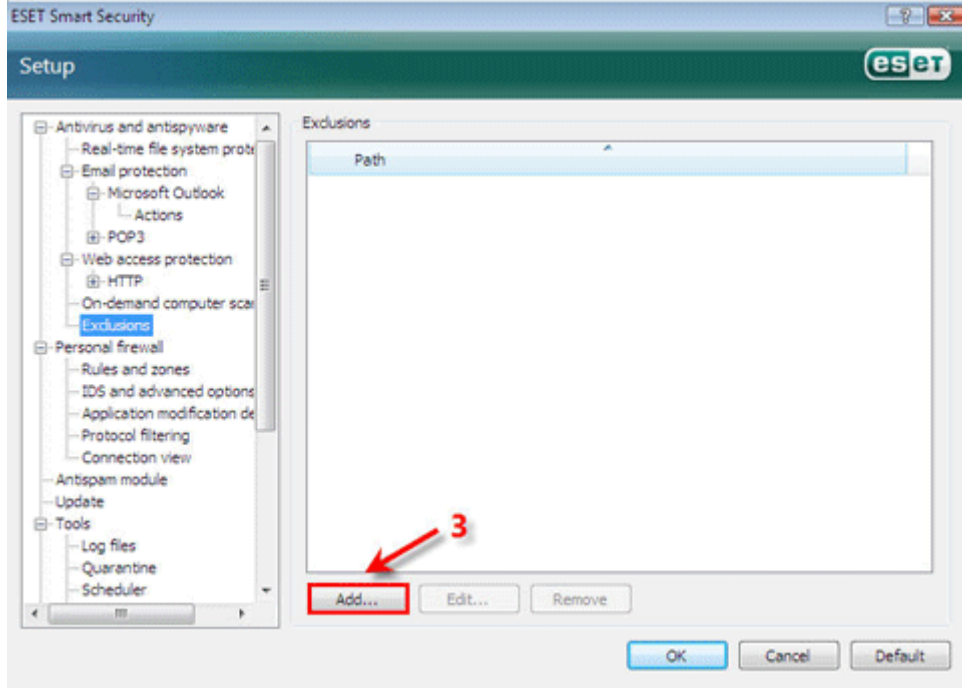
1.  ikonuna tıklayarak veya **Start → All Programs → Eset → NOD32 Control Center** a tıklayarak kontrol merkezini açınız.
2. **Update → Update** a tıklayınız ve ardından sağ bölümde **Setup** butonuna tıklayınız
3. Açılan pencerede user name bölümündeki bilgiyi destek@Nod32.com.tr adresine gönderebilirsiniz



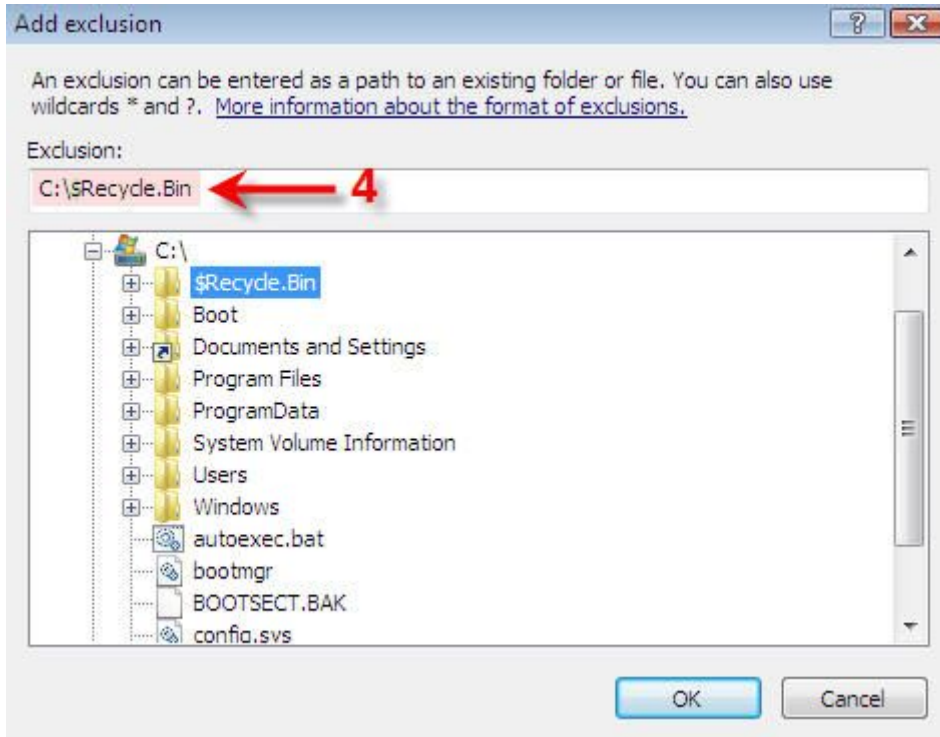
32. Gerçek zamanlı dosya taramasında (real-time scanning) önemli dosya veya klasörleri nasıl tarama dışı bırakabilirim?

File server, Mail server, Backup server' lar da kullanılan yüksek boyutlu sıkıştırılmış veri dosyaları ESS/ENA tarafından taranırken bu dosyaları kullanan programlarda sorunlarla karşılaşabilirsiniz. Bu sorunu gidermek için aşağıdaki adımları uygulayınız.

1. Eset Smart Security' i  ikonundan Eset Nod32 Antivirus' ü  ikonuna çift tıklayarak veya **Start → All Programs → ESET → ESET Smart Security** veya **ESET NOD32 Antivirus**. a tıklayarak programı açınız.
2. Gelişmiş kurulum penceresini açmak için klavyeden F5 tuşuna basınız.
3. **Antivirus and Antispyware → Tarama Dışı öğeler (Exclusions)** e tıklayarak sağ bölümde **Add...** Butonuna tıklayınız.



4. Açılan pencerede listeye ekleyeceğimiz klasör veya dosyaları belirleyiniz. Ayrıca (*, *,*) gibi parametreleri de kullanabilirsiniz. Örneğin C:\ altındaki tüm doc uzantılı dosyalar tarama dışı kalsın diyorsanız. Aşağıdaki pencereye c:*.doc yazmanız yeterlidir.



5. **OK** butonuna tıklayarak pencereyi kapatınız.

33. Microsoft Outlook açılırken hata veriyor.

The Add-in "ESET Outlook Plugin" (C:\PROGRA~1\ESET\ESETNO~1\EPLGOU~1.DLL) cannot be loaded and has been disabled by Outlook. If no update is available, please uninstall the Add-in.

Outlook açılırken yukarıdaki gibi bir hata ile karşılaşıyorsanız aşağıdaki adımları uygulayınız.

EXTEND. DAT' dosyasını siliniz.

EXTEND. DAT Microsoft Outlook tarafından kullanılan eklentileri barındırır. Eğer bu dosyayı silip M. Outlook' u yeniden başlatırsanız bu dosya en yeni şekliyle yeniden oluşur. Böylece eklentilerden kaynaklanan bir sorun var ise bu işlem ile birlikte bu sorun giderilmiş olur.

Extend.dat dosyasını silmek için;

1. **Outlook' tan çıkınız.**
2. **Başlat > ARA > Tüm Dosya ve Klasörler > Gizli dosya ve klasörleri ara (Search hidden files and folders) arama seçeneğini işaretleyiniz**
3. **Dosya adı bölümüne 'extend.dat' yazarak ara butonuna tıklayınız.**
4. Bulunan dosyayı siliniz.

Eğer Outlook için birden fazla profil oluşturulmuş ise Extend. dat dosyası da birden fazla olur dolayısıyla oluşan bu dosyaları da silmeniz gerekmektedir. Extend. dat dosyasının yolu (C:\Documents and Settings\Username\Local Settings\Application Data\Microsoft\Outlook) ayrıca aynı dosyayı tüm Windows profillerinde de silmeniz gerekmektedir.

İkinci Çözüm olarak

MS Outlook 2003, kullanıyorsanız Office 2003 Service Pack 3'ü <http://office.microsoft.com/en-us/downloads/default.aspx> adresinden indirerek Outlook' u güncelleyiniz.