McAfee VirusScan 8.7 (VS) Kullanıcı Kılavuzu

Bu belgede son kullanıcının McAfee VS 8.7 yazılımını kolay ve sorunsuz kullanmasını sağlamak amacıyla, yazılımın tanıtımı ve kullanımı anlatılmaktadır. İlk bölümde McAfee VS 8.7.i yazılımı ekranlarına erişim anlatılmaktadır, ikinci bölümde virüs taraması, virüs tanımlarının güncellenmesi gibi sıklıkla kullanılması gereken işlemler anlatılmaktadır.

McAfee VS 8.7 Erişimi

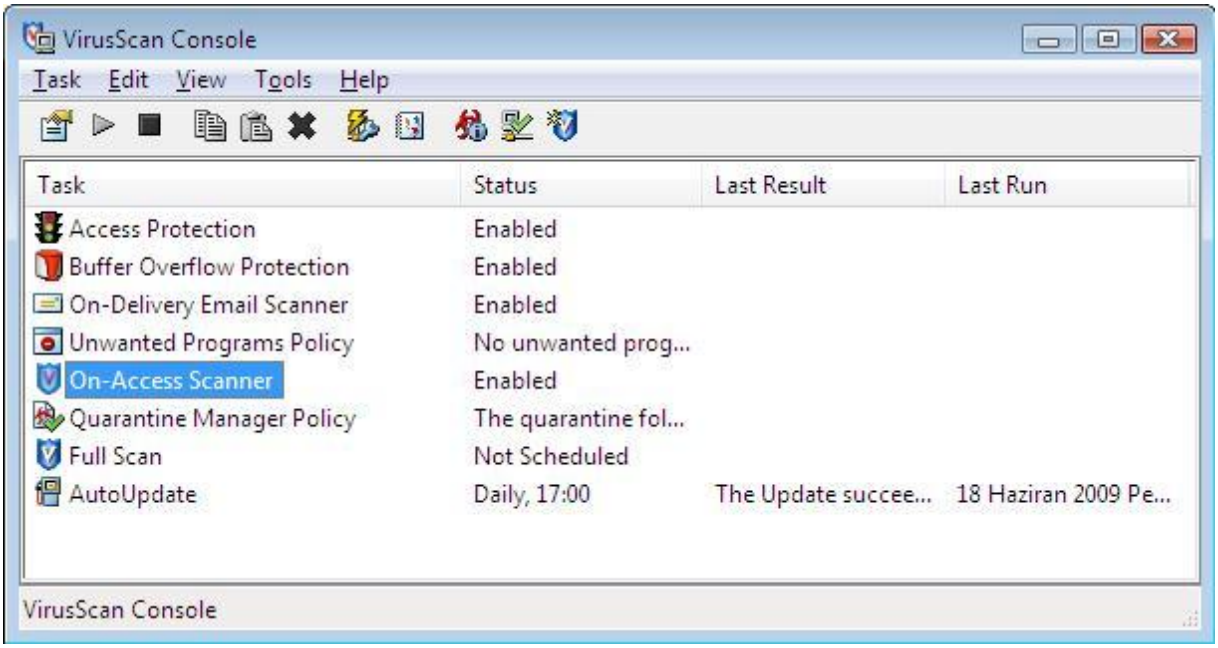
McAfee VS yazılımı seçeneklerine ulaşmanın iki yolu vardır.

- McAfee VS 8.7 yazılımı, sistem tepsisi (System Tray) içinde kalkan şeklinde bir ikon olarak görülür. İkonunun üstüne gelip sağ tıklanınca sekiz seçenekli menu görüntülenir. Varsayılan olarak "On-Access Scan Statistis" seçilidir ve çift fare tıklamasında açılır.
  Not: Antivirüs yazılımı merkezi olarak yönetiliyor ise, bölüm/birim koordinatörü bu ikonun görünmemesini sağlamış olabilir.

- Başlat menüsü tıklanır
  - All Programs > Mcafee > VirusScan Console (Windows XP / Vista)

Açılan pencerede:

"Access Protection", "Buffer Overflow Protection", "On Delivery Email Scanner", "Unwanted Programs Policy", "On-Access Scanner", "AutoUpdate", "Full Scan", "Quarantine Manager Policy" varsayılan olarak hazırlanmış "Task" (görevler) olarak görüntülenmektedir. (Resim 1)

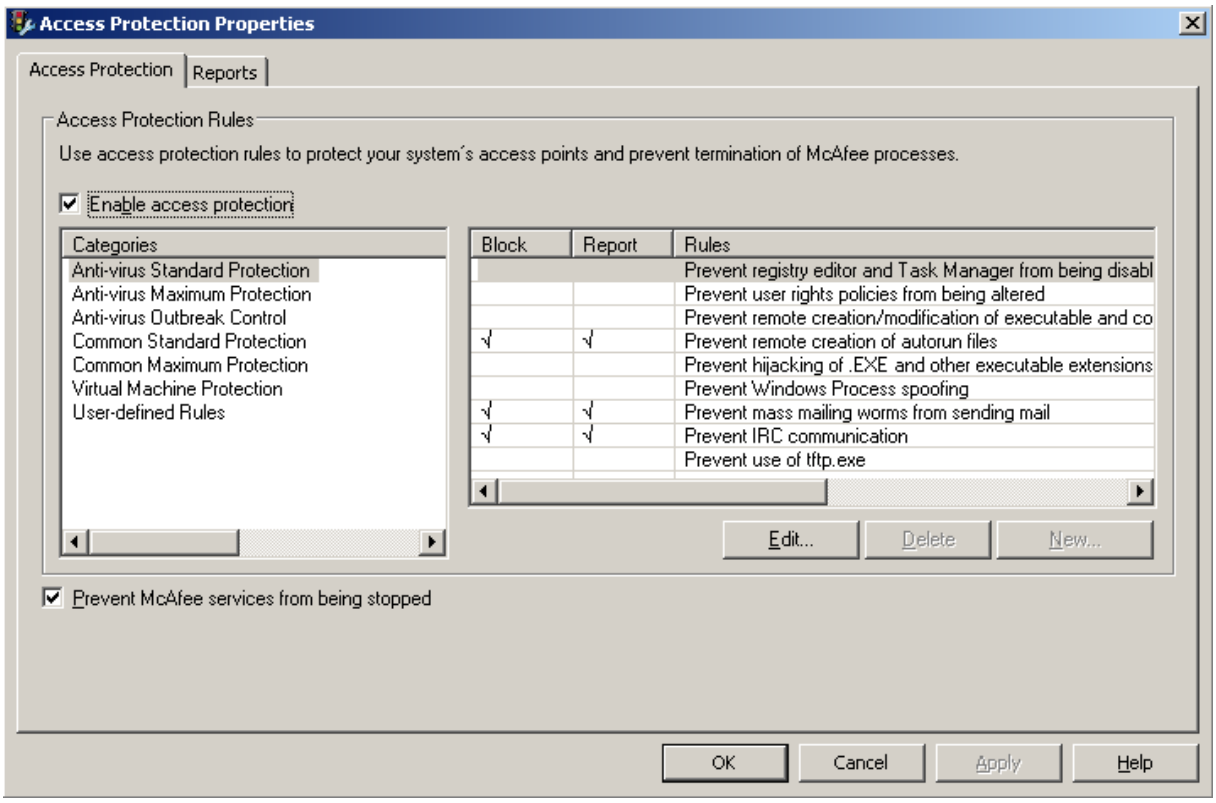


Şekil 1 - McAfee 8.7 VS konsolu

Access Protection

Belirli portlara, dosyalara, dizinlere ve paylaşımlara erişimi kısıtlayarak, izinsiz girişleri engellemeyi sağlar.

Şekil 2'deki pencere görüntüsü "Access Protection" çift tıklandığında kullanıcının karşısına gelen penceredir. Açılan pencerede üç sekme bulunmaktadır. "Port blocking" bilgisayara gelen ve giden trafikte belirli portların bloklanmasını sağlar. Bir port bloklandığında, o porttan gelen hem TCP hem UDP paketleri bloklanır. "File, share, and folder protection" paylaşımlara, dosyalara ve dizinlere okuma ve yazma erişimlerini engellemeyi sağlar. Varsayılan olarak tüm paylaşımları olduğu gibi bırakmaktadır ancak seçenekleri arasında "Make all shares read only" (tüm paylaşımları sadece okuma hakkı ver) ve "Block read and write access to all shares" (tüm paylaşımların okuma ve yazma haklarını durdur) vardır. "Reports" sekmesi, yukarda belirtilen sorunlar tesbit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağının ayarlanmasını sağlar.



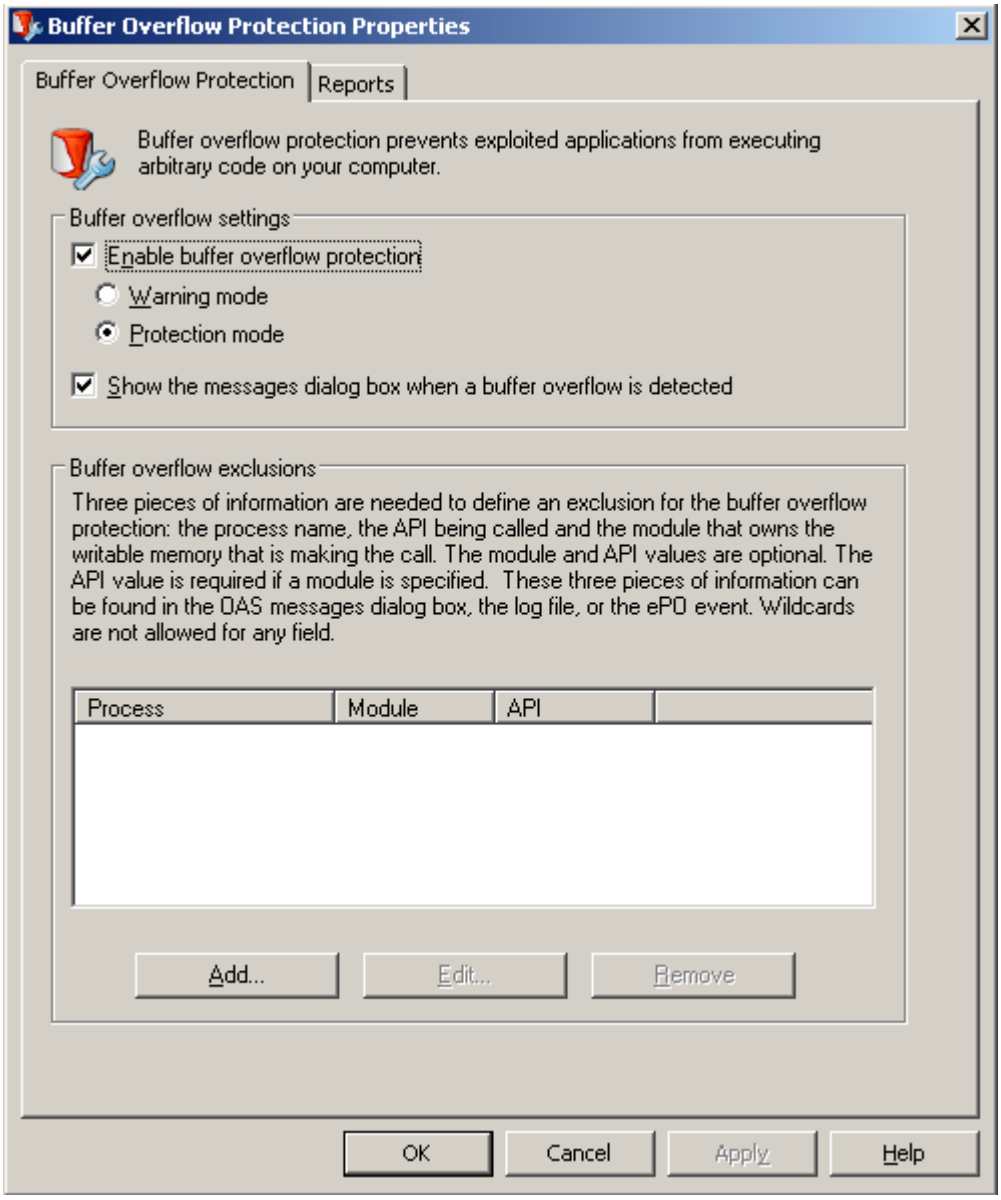
Şekil 2 - McAfee 8.7 VS konsolu

Buffer Overflow Protection

Bellek taşması saldırıları sayesinde rastgele kod çalıştırılmasını engeller. Kullanıcı modunda API isteklerini izler ve bellek taşması sırasından ne zaman yapıldığını tesbit eder. Bir çok Microsoft ürününü bu şekilde takip edebilmektedir. Varsayılan olarak bellek taşması koruması açık olarak kurulur.

Şekil 3'teki pencere görüntüsü "Buffer Overflow Protection" çift tıklandığında kullanıcın karşısına gelen penceredir. Açılan pencerede iki sekme bulunmaktadır. "Buffer Overflow Protection" sekmesi, bellek taşması saldırılarına karşı bilgisayarı koruma durumunu

göstermektedir. "Reports" sekmesi, bellek taşması saldırısı tesbit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağının ayarlanmasını sağlar.



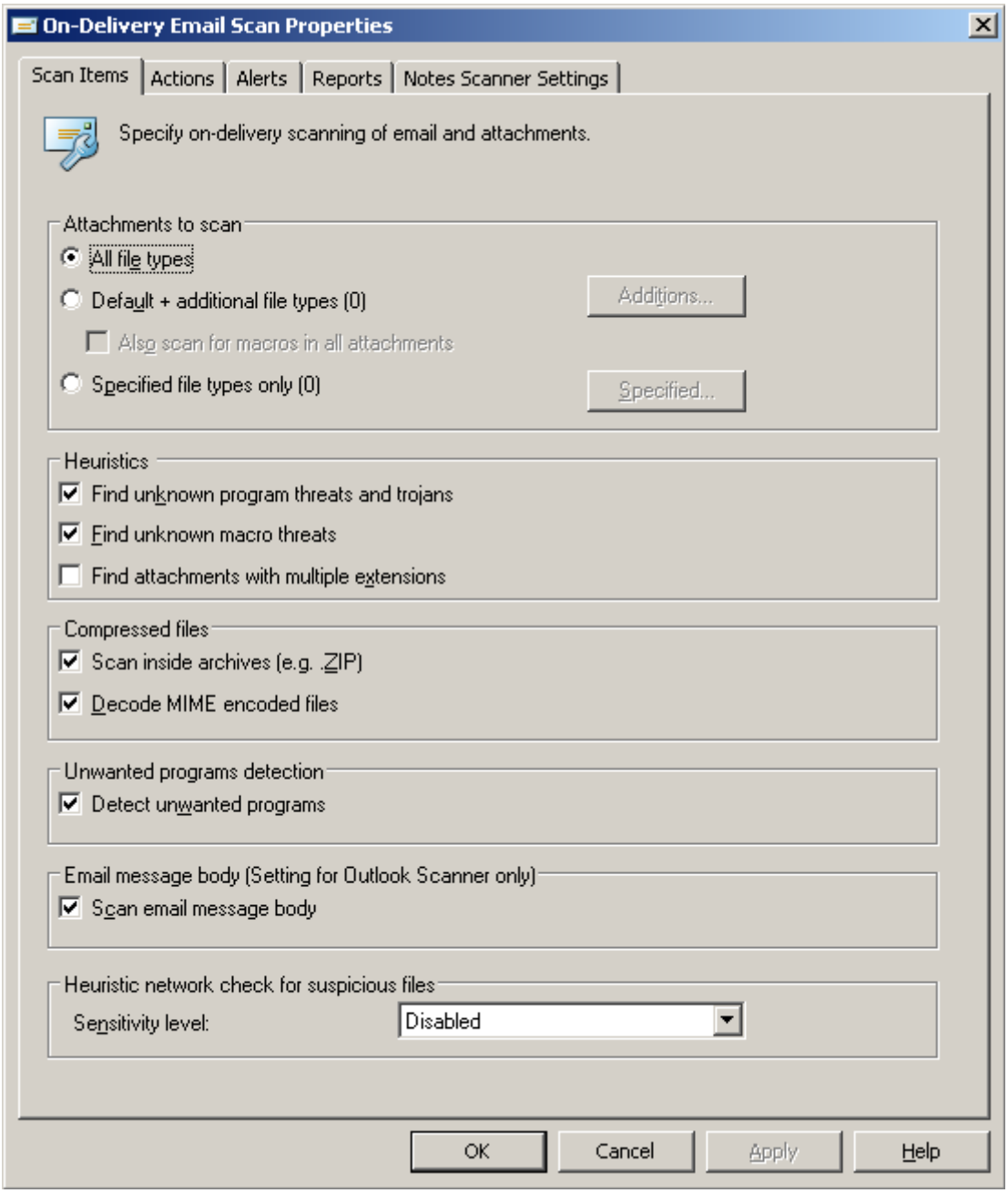
Şekil 3 - McAfee 8.7 VS konsolu

On-Delivery E-mail Scanner

Gönderilen e-postaların eklentilerinde olası virüs olmasını engeller. Varsayılan olarak tüm eklentileri kontrol eder.

Şekil 4'teki pencere görüntüsü "On-Delivery E-mail Scanner" çift tıklandığında kullanıcının karşısına gelen penceredir. Açılan pencerede altı sekme bulunmaktadır. "Detection" sekmesi, gelen e-postada taranması uygun görülen dosyaları göstermektedir. "Advanced" sekmesi altında "Heuristics" kutusu içinde virüs tanımlarında bulunmayan ama eski bir virüs motorunu kullanan virüsleri yakalamaya yarayan "Find unknown program virus" ve "Find unknown macro virus" seçenekleri varsayılan olarak seçilidir. "Non-viruses" kutusu içinde "Find

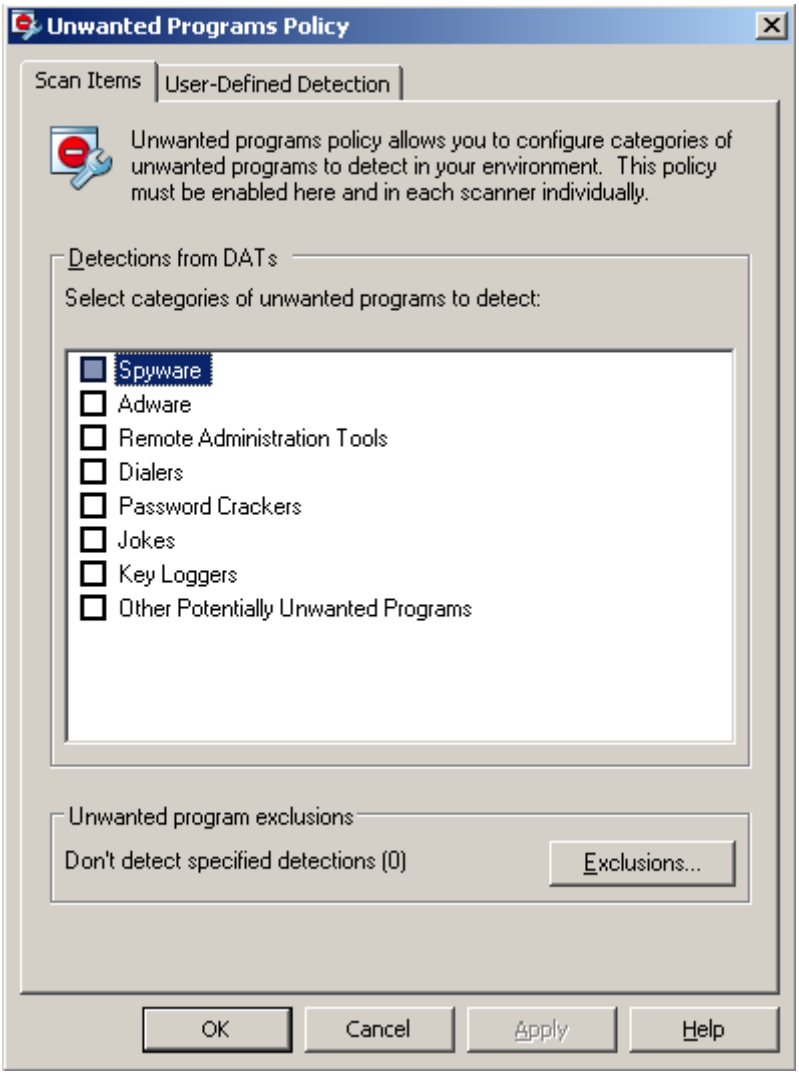
potentially unwanted programs" seçeneği varsayılan olarak seçilmemiştir. Eğer aktif hale getirilirse 'pop-up' açılan pencerelere neden olan bazı casus programlar bulunabilmektedir. "Compressed files" kutusunda sıkıştırılmış dosyaların taranması ile ilgili seçenekler bulunmaktadır. Varsayılan olarak ".UPX" dosyalarını taramaktadır ancak ".ZIP" ve MIME olarak kodlanmış dosyaları taramadan geçirmemektedir. "Actions" sekmesi altında virüs aktivitesini yaratan dosya bulunduğunda yapılacak işlemler tanımlanmıştır. Varsayılan olarak virüslü dosyanın otomatik olarak temizlenmesi seçilmiştir. Temizleme işlemi başarılı olamazsa karantina dizini olarak belirtilen dizine taşınması seçilidir. "Alert" kısmında virüs bulunması durumunda, bilgisayardan yöneticisine gönderilecek e-postanın düzenlemesini sağlayan pencere vardır. "Unwanted Programs" sekmesinde istenmeyen programların taranmasını sağlayan ayarlar bulunmaktadır."Reports" sekmesi, virüs aktivitesi tesbit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağının ayarlanmasını sağlar.



Şekil 4- McAfee 8.7 VS konsolu

Unwanted Programs Policy

Casus programları bulmayı sağlayan özelliktir. Bu bölümden tüm taramalarda bu tür programların taranmasını sağlayacak ayarlar yapılmaktadır.



Şekil 5- McAfee 8.7 VS konsolu

Şekil 5'daki pencere görüntüsü "Unwanted Programs Policy" çift tıklandığında kullanıcın karşısına gelen penceredir. Açılan pencerede iki sekme bulunmaktadır. Birincisi sekmede (Detection) genelde karşılaşılan istenmeyen programların listesi bulunur. İkinci sekme (User-Defined Detection) istenmeyen programlar arasına kullanıcı tarafından belirlenenlerin eklenebilmesini sağlar.

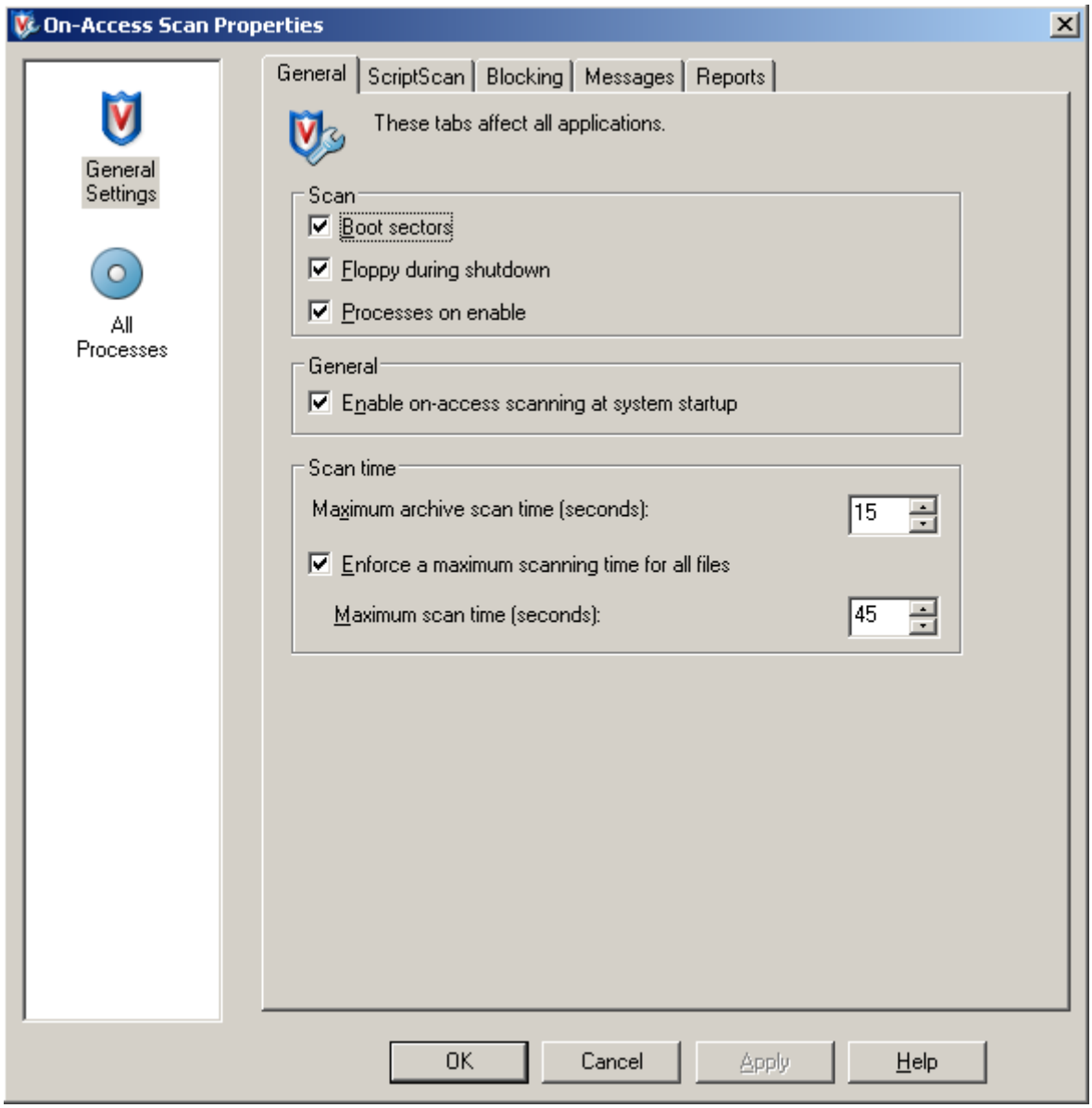
On-Access Scan:

Herhangi bir dosyaya erişimde antivirüs yazılımının ilgili dosyayı virüs taramasından geçirmesini sağlar. Kullanıcının her kullandığı programı virüs taramasından geçirildikten

sonra kullanmasını sağlar. Dosya çalıştırılmadan önce yapılan bu taramada amaç virüs tanımlarında bulunan virüsleri yakalamaktır.

Şekil 6'deki pencere görüntüsü "On-Access Scan" çift tıklandığında kullanıcın karşısına gelen penceredir. Açılan pencerede iki bölme bulunmaktadır. Birincisi solda "General Setting" ve "All Processes" ikonların bulunduğu kısım, ikincisi bu ikonların içeriklerinin bulunduğu ortadaki kısımdır.

Varsayılan olarak "General Settings" ikonunun verileri görüntülenir. "General Settings" ikonu tüm virüs taramalarını ve tarama sonuçlarında yapılacak işlemleri belirlemektedir.



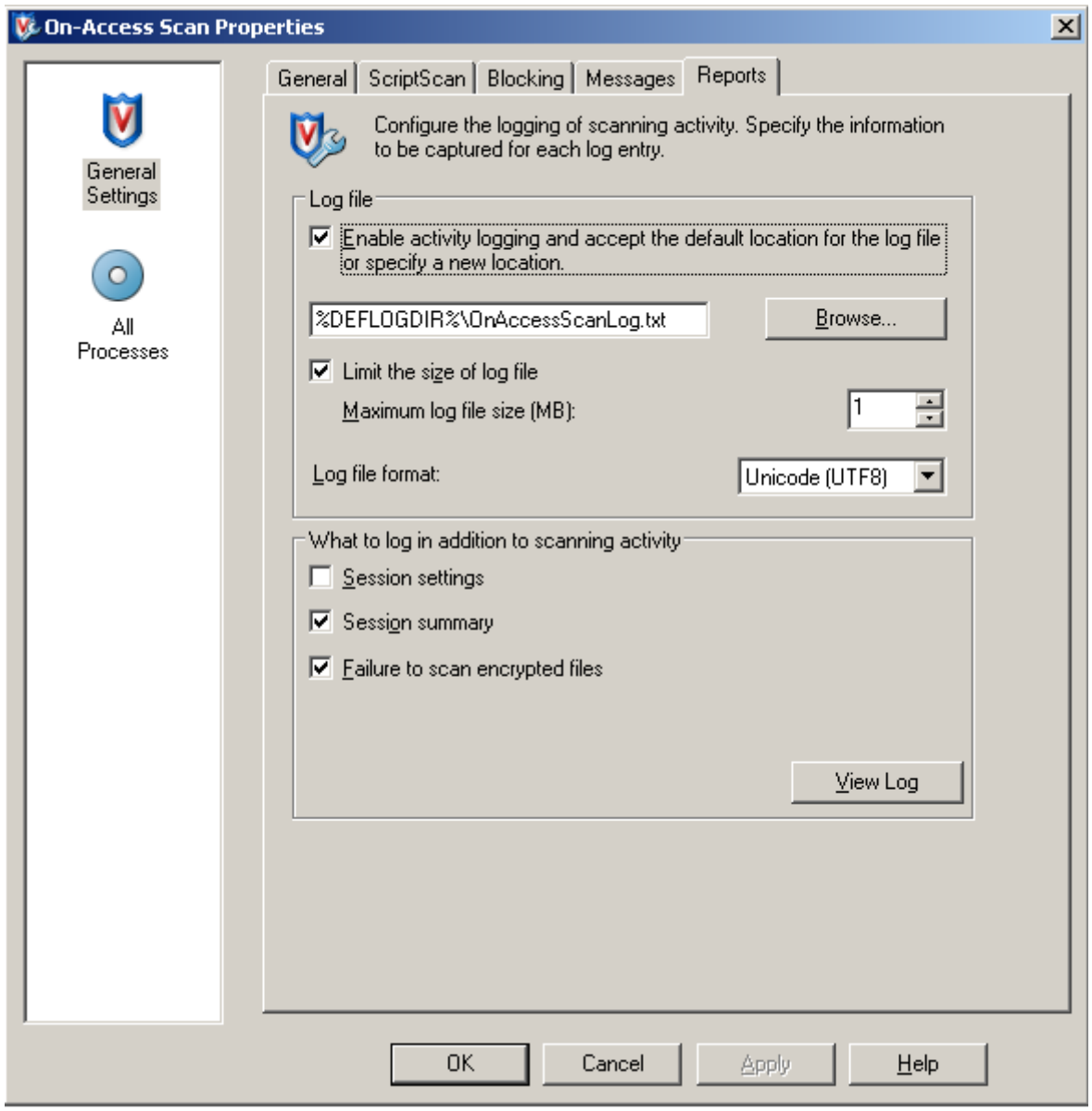
Şekil 6- McAfee 8.7 VS konsolu

"General" kutusu içinde bilgisayarın açılış ve kapanış işlemi sırasında antivirüs yazılımının yapacağı işlemler tanımlıdır. "General" kutusu, açılış sırasında "On-Access Scan" özelliğinin çalıştırılması ve karantina dizininin belirlenmesini sağlar. "Scan time" kutusu, dosyanın taranmasına en fazla kaç saniye ayrılacağını göstermektedir.

"Script Scan" kutusu JavaScript ve VBScript betiklerinin bilgisayarda çalıştırılması sırasında taranmasını sağlar.

"Blocking" kutusu bilgisayara uzaktan erişen bir kullanıcının virüslü dosya kopyalaması durumunda erişiminin bloklanmasını sağlar.

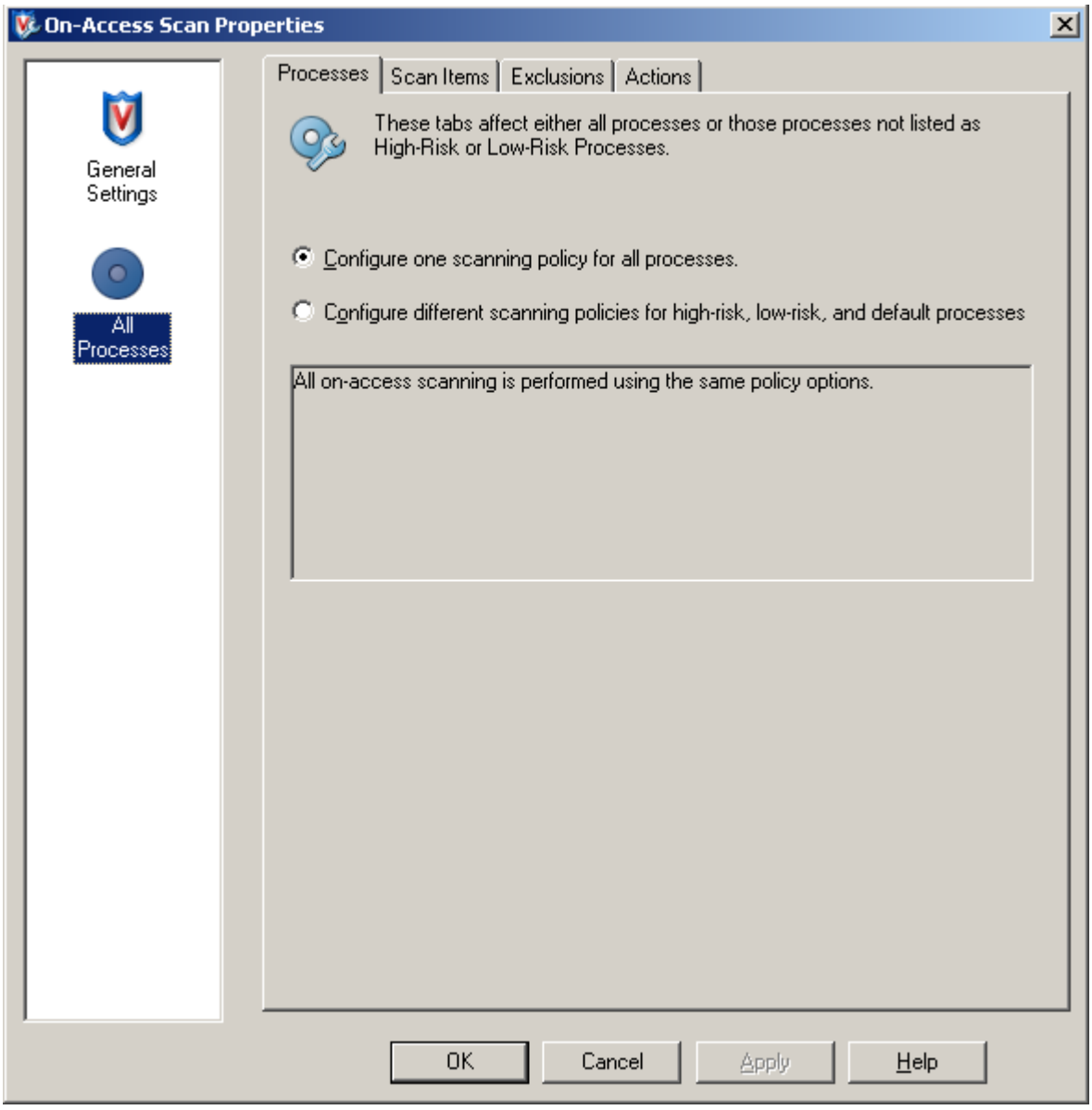
"Messages" sekmesi tıklandığında ekrana gelen "Message for local users" kutusu, virüs bulunduğunda o anda bilgisayarı kullanan kullanıcıya verilecek mesajı ve bu kullanıcı yönetici haklarına sahip değilse yapabileceği işlemleri içermektedir. Bu seçenekler arasında dosyanın silinmesine izin verme vardır ancak sistem dosyalarını etkileyen bir virüsün bilinçsiz bir kullanıcı ile birleşerek sistemi bozma olasılığı göz önünde tutulduğundan varsayılan olarak aktif değildir. "Response to network users" kutusu ağ üzerinde bilgisayarı kullanan kullancılara gönderilecek mesajı ve iletişimin kesip kesilmeyeceğini belirler.



Şekil 7 - McAfee 8.7 VS On-Access Scan Özellikleri- Reports

"Reports" sekmesi, bilgisayarda virüs aktivitesi tesbit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağının ayarlanmasını sağlar. Virüs aktivitesine ek olarak günlük dosyasına o an bilgisayarı kullanan kullanıcı adını, virüs taraması yapılmamış şifrelenmiş dosyaları ve oturum özetini yazar.

"All Process" ikonuna tıklandığında "Process" sekmesi altında tüm işlemlere ya da düşük risk düzeyi ve yüksek risk düzeyi olarak ayrılmış işlemlere uygulanacak kurallara erişilmektedir. Varsayılan olarak tüm işlemlere aynı kurallar uygulanmaktadır (Şekil 8).



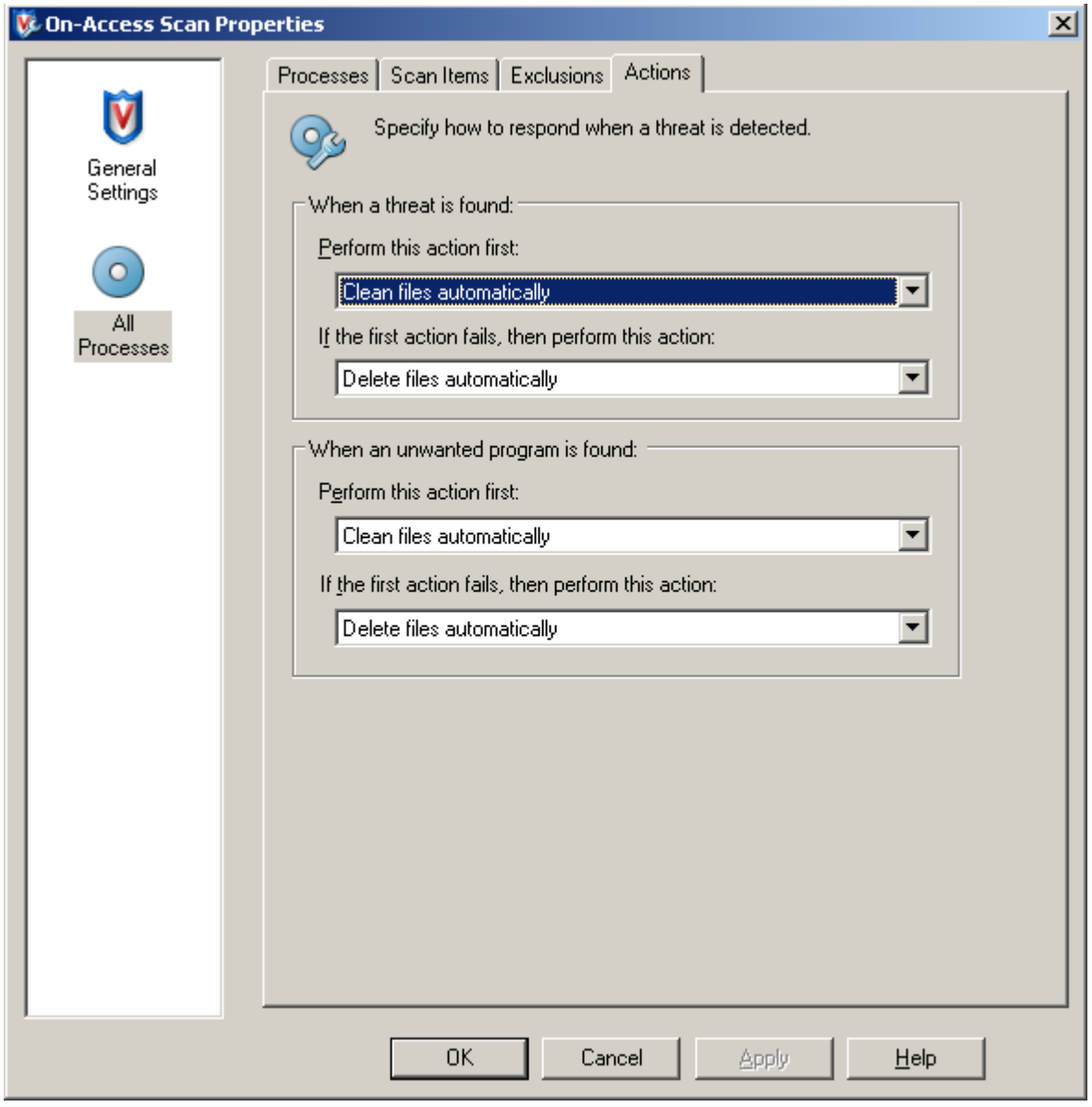
Şekil 8 - McAfee 8.7 VS On-Access Scan Özellikleri - All Process

"Process" sekmesi altında, süreçlere uygulanacak politika bulunmaktadır. Varsayılan olarak tüm süreçlere aynı virüs tarama politikası uygulanmaktadır.

"Detection" sekmesi altındaki "Scan Files" kutusunda diske yazıldığı sırada ve diskten okunduğu sırada dosyaların taranması varsayılan olarak seçilidir. Bu seçeneklere ek olarak ağ sürücülerinin de taranması olanağı vardır. "What to scan" kutusu altında varsayılan olarak tüm

dosyalar işaretlidir ancak isteğe bağlı olarak varsayılan dosyalar ve bunlara ek olarak kullanıcının belirlediği dosyaları tarama seçeneği ya da yine isteğe bağlı olarak sadece özel dosya tiplerinin taranmasını sağlayan bir seçenek bulunmaktadır. Varsayılan ayarlarla kullanması önerilir. "What not to scan" seçeneği, kullanıcının belirleyeceği dizinler ve/veya dosya türleri için tarama yaptırmama olanağı sağlar.

"Advanced" sekmesi altında "Heuristics" kutusu içinde virüs tanımlarında bulunmayan ama eski bir virüs motorunu kullanan virüsleri yakalamaya yarayan "Find unknown program virus" ve "Find unknown macro virus" seçenekleri varsayılan olarak seçilidir. "Non-viruses" kutusu içinde "Find potentially unwanted programs" seçeneği varsayılan olarak seçilmemiştir. Eğer aktif hale getirilirse 'pop-up' açılan pencerelere neden olan bazı casus programlar bulunabilmektedir. "Compressed files" kutusunda sıkıştırılmış dosyaların taranması ile ilgili seçenekler bulunmaktadır. Varsayılan olarak ".UPX" dosyalarını taramaktadır ancak ".ZIP" ve MIME olarak kodlanmış dosyaları taramadan geçirmemektedir.



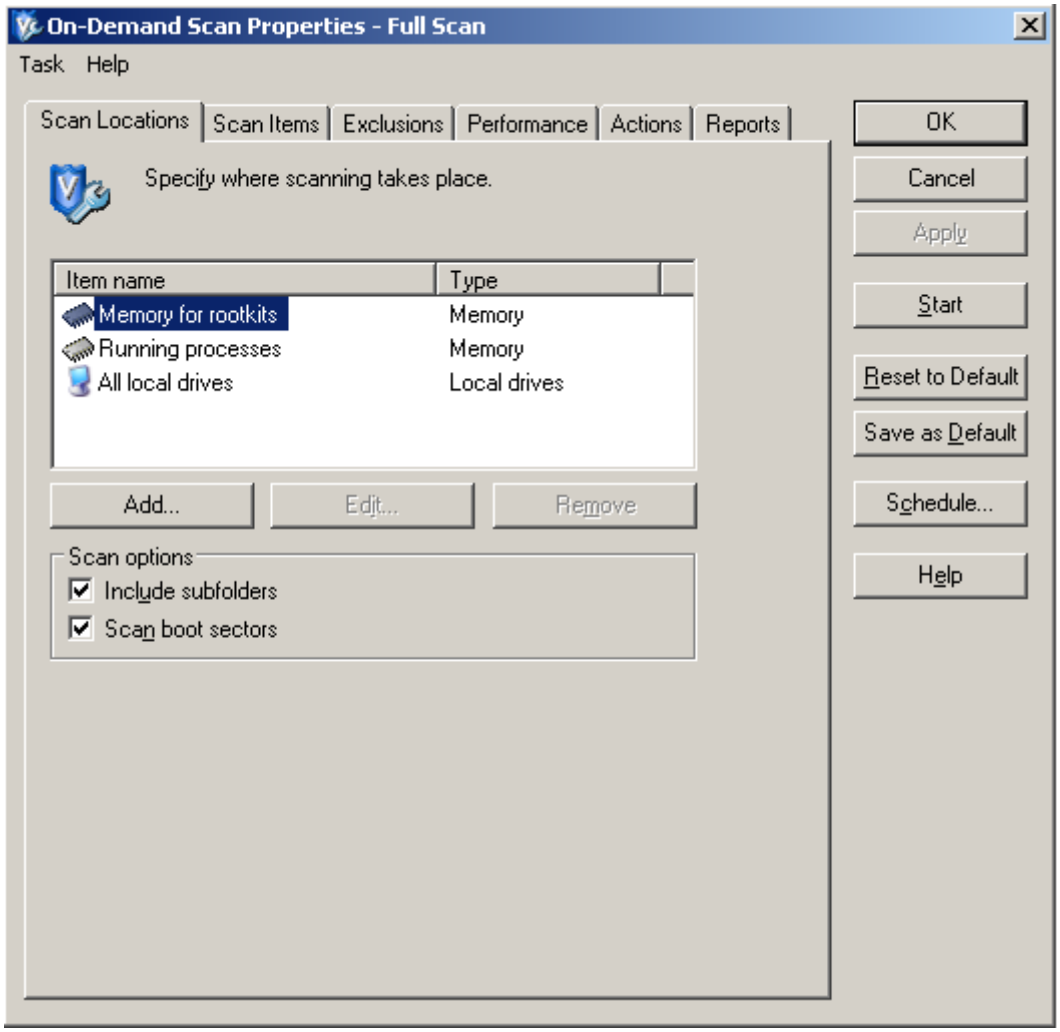
Şekil 9 - McAfee 8.7 VS On-Access Scan Özellikleri - All Settings - Actions

"Actions" sekmesi altında, virüs aktivitesini yaratan dosya bulunduğunda yapılacak işlemler tanımlanmıştır. Varsayılan olarak virüslü dosyanın otomatik olarak temizlenmesi seçilmiştir. Temizleme işlemi başarılı olamazsa karantina dizini olarak belirtilen dizine taşınması seçilidir.

"Unwanted Programs" sekmesinde istenmeyen programların taranmasını sağlayan ayarlar bulunmaktadır.

Scan All Fix Disks:

Kullanıcının bilgisayarındaki dosyaların hepsini kendi istediği zaman taramasını sağlar. "Add" düğmesi, belirlenen tarama yapılacak alanlar dışında tarama yapılması istenilen alanların eklenmesini sağlar. "Remove" düğmesi, taranması istenmeyen listede bulunan alanların çıkarılmasını sağlar (Şekil 10).

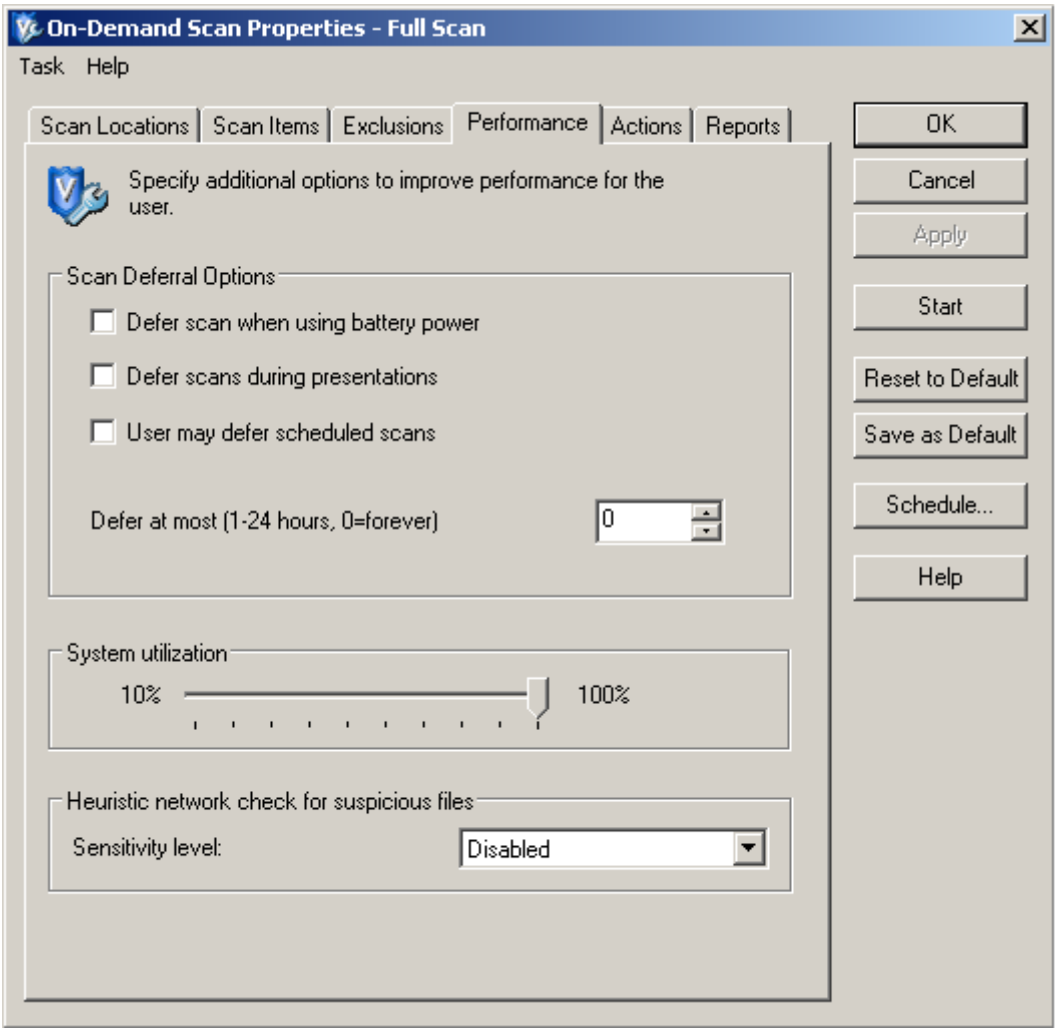


Şekil 10 - McAfee 8.7 VS - On-Demand Scan Özellikleri

"Start" düğmesi kullanıcının o anda tarama başlatmasını sağlar. "Reset to Default" düğmesi kullanıcının varsayılan ayarlara dönmesini, "Save as Default" varsayılan ayarların kullanıcının belirlediği ayarlar olmasını sağlar. Tarama işlemi "Schedule" düğmesine basılarak zamanlanmış görevler arasına alınabilir (Şekil 10).

"Detection" sekmesi altındaki "Scan Files" kutusunda diske yazıldığı sırada ve diskten okunduğu sırada dosyaların taranması varsayılan olarak seçilidir. Bu seçeneklere ek olarak ağ sürücülerinin de taranması olanağı vardır. "What to scan" kutusu altında varsayılan olarak tüm dosyalar işaretlidir ancak isteğe bağlı olarak varsayılan dosyalar ve bunlara ek olarak kullanıcın belirlediği dosyaları tarama seçeneği ya da yine isteğe bağlı olarak sadece özel dosya tiplerinin taranmasını sağlayan bir seçenek bulunmaktadır. Varsayılan ayarlarla kullanması önerilir. "What not to scan" seçeneği içinde kullanıcının belirleyeceği dizinler ve/veya dosya türleri için tarama yaptırmama olanağını sağlar.

"Advanced" sekmesi altında "Heuristics" kutusu içinde virüs tanımlarında bulunmayan ama eski bir virüs motorunu kullanan virüsleri yakalamaya yarayan "Find unknown program virus ve "Find unknown macro virus" seçenekleri varsayılan olarak seçilidir. "Non-viruses kutusu içinde "Find potentially unwanted programs" seçeneği varsayılan olarak seçilmemiştir. Eğer aktif hale gelirse pop-up açılan pencerelere neden olan bazı casus programlar bulunabilmektedir. "CPU utilization" tarama sırasında işlemcinin hangi oranda kullanılacağının belirlenmesini sağlar. "Compressed files" kutusunda sıkıştırılmış dosyaların taranması ile ilgili seçenekler bulunmaktadır. Varsayılan olarak ".UPX" dosyalarını taramaktadır ancak ".ZIP" ve MIME olarak kodlanmış dosyaları taramadan geçirmemektedir.



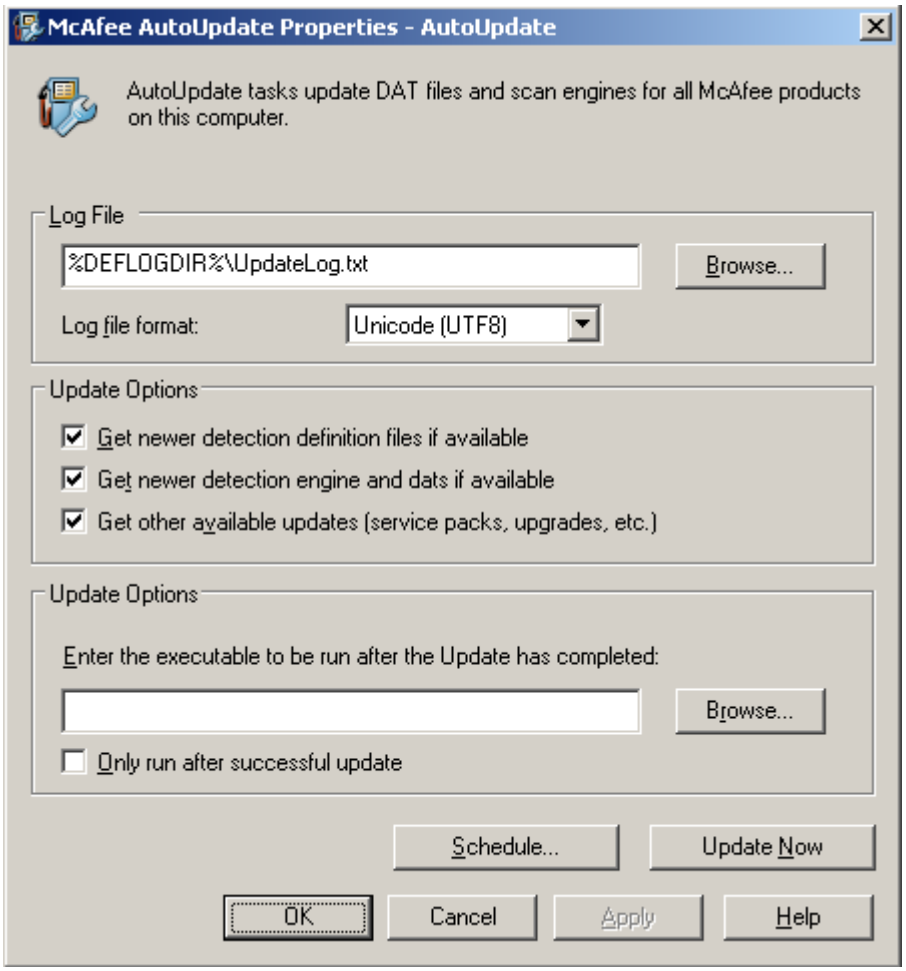
Şekil 11- McAfee 8.7 VS - On-Demand Scan Özellikleri - Advanced

"Action" sekmesi altında virüs aktivitesini yaratan dosya bulunduğunda yapılacak işlemler tanımlanmıştır. Varsayılan olarak virüslü dosyanın otomatik olarak temizlenmesi seçilmiştir. Virüslü dosyaya uygulanan temizleme işlemi başarılı olamazsa karantina dizini olarak belirtilen dizine taşınması seçilidir.

"Report" sekmesi, bilgisayarda virüs aktivitesi tesbit edildiği zaman, hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağının ayarlanmasını sağlar. Virüs aktivitesine ek olarak günlük dosyasına o andaki kullanıcını adını, virüs taraması yapılmamış şifrelenmiş dosyaları ve oturum özetini yazar.

AutoUpdate:

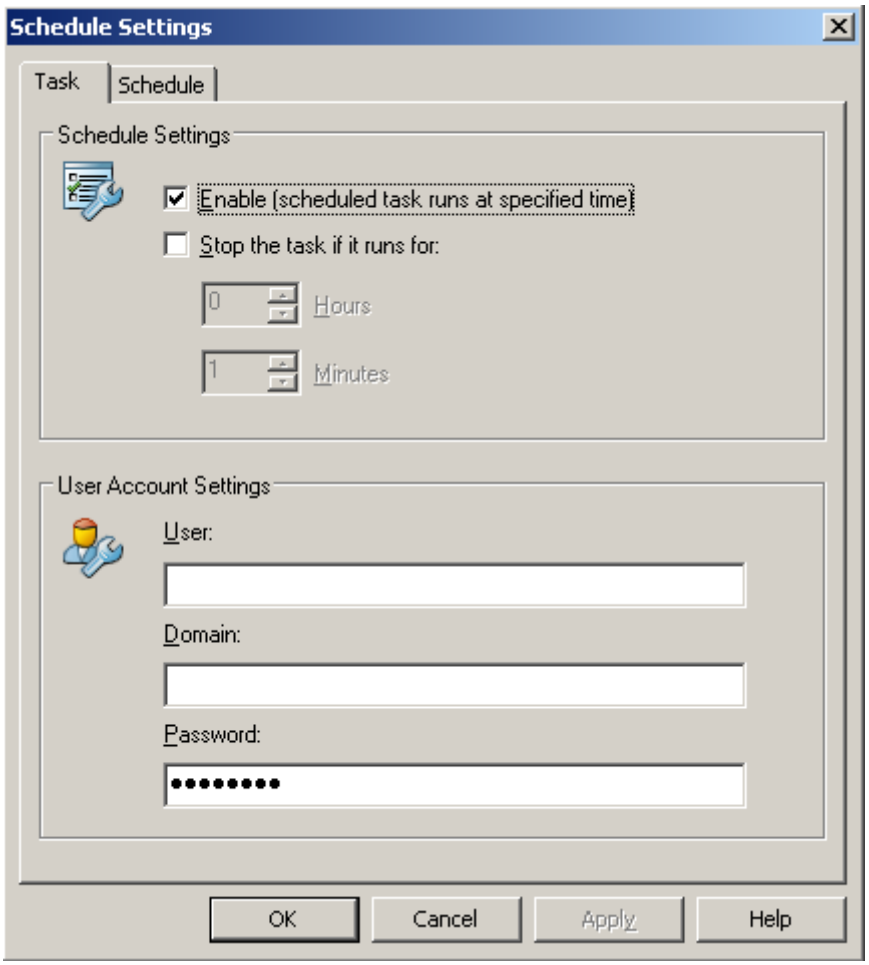
Kullanıcının virüs tanımlama dosyalarını güncellemesini unutması ya da atlaması sonucu antivirüs yazılımın yeni çıkan virüslere karşı etkisiz kalmasını engellemek için hazırlanmış bölümdür (Şekil 12). "Update Now" düğmesi o anda güncelleme yapılmasını sağlar.



Şekil 12 - McAfee 8.7 VS - AutoUpdate Özellikleri

"Log file" kutusu güncellemenin günlüğünü tutar. Bu dosyayı başarısız güncellemelerde, sorunu bulmak açısından incelemekte fayda vardır. "Run options" güncelleme sonrasında istenilen bir programın çalıştırılmasını sağlar. Genelde virüs tarama programının çalıştırılması bilgisayarın yeni çıkan virüs aktivitesinden etkilenip etkilenmediğini görmek açısından faydalıdır.

Güncellemenin periyodik olarak yapılması için "Schedule" düğmesine basılır. Açılan pencerede, kullanılan bilgisayar bir domain üyesi bilgisayarsa ait olduğu domainde güncelleme yetkilerine sahip kullanıcı adı ve parolası girilmelidir. Ardından "Schedule" sekmesi tıklanarak hangi sıklıkla güncelleme yapılacağı belirlenmelidir. Normal durumlarda haftada bir defa güncelleme yapmak yeterlidir. Ancak acil önlem planları uygulanmaya başladığında gerekli görülürse bu süre düşürülmelidir (Şekil 13).



Şekil 13 - McAfee 8.7 VS - AutoUpdate Özellikleri - Zamanlanmış Güncelleme