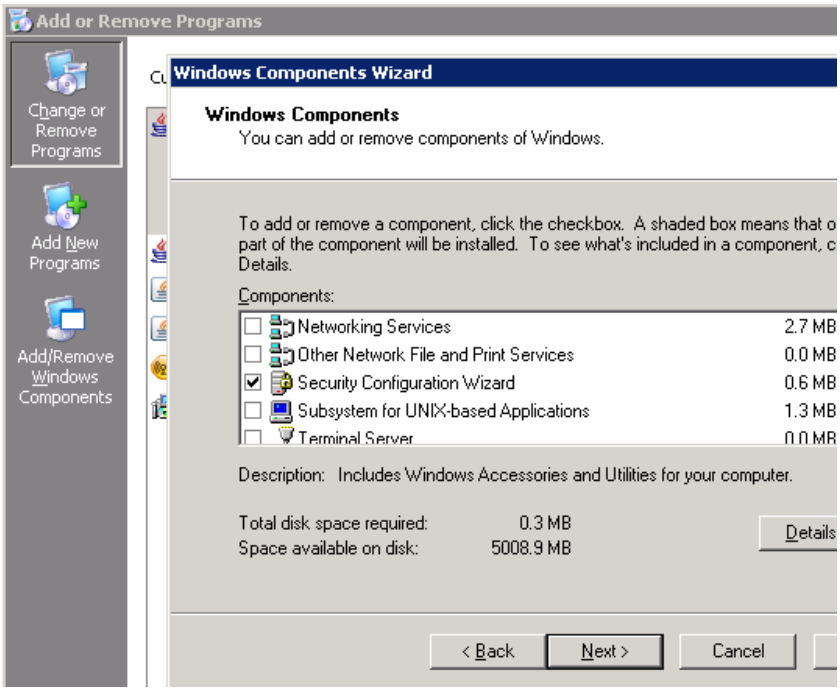
Security Configuration Wizard ile güvenliği artırmak

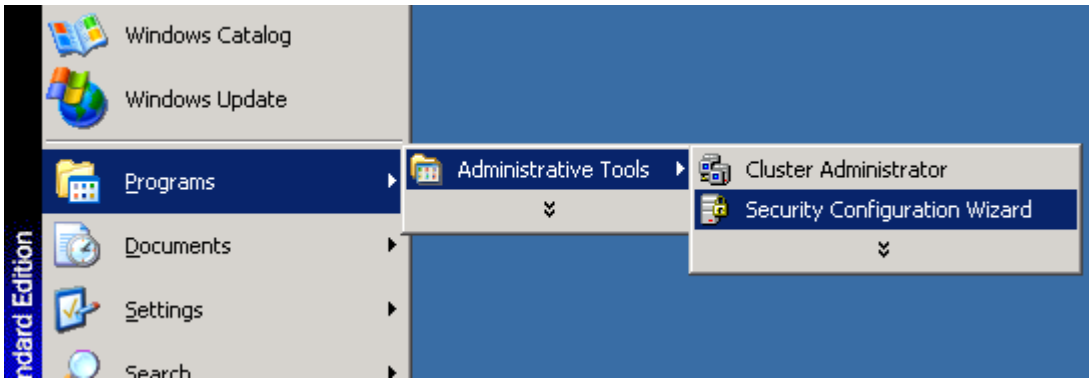
Bu makalede sizlere Security Configuration Wizard kullanımını, bu tool sunucunun nasıl daha güvenli hale getirildiğini ve bu tool ile hazırlanan xml dosyasının group policy object' i olarak Active Directoruy altında kullanımını anlatacağım.

Yönetimsel araçlar içerisinde bulunan Security Configuration Wizard kullanılarak sunucularımızı daha güvenli hale getirebiliriz. Yönetimsel araçlar içerisinde bu tool' u göremiyorsanız Add/Remove Program – Windows Component içerisinden bu tool' un kurulumunu yapmanız gerekmektedir.



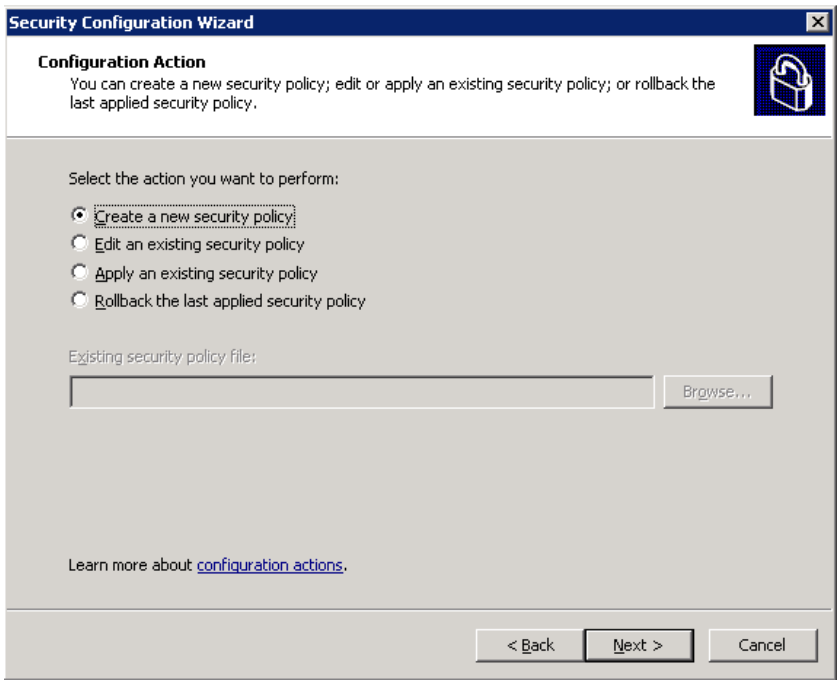
Wizard' ı çalıştırmadan evvel biraz bilgi iyi olacaktır. Bu wizard kullanılarak sunucu rollerini, client özelliklerini, network güvenliğini, registry ayarlarını, audit policy ayarlarını ve IIS ile ilgili ggvenlik ayarlarını düzenlenebilir.

- Wizard' ı çalıştıralım ve neler yapabileceğimizi daha iyi görelim;

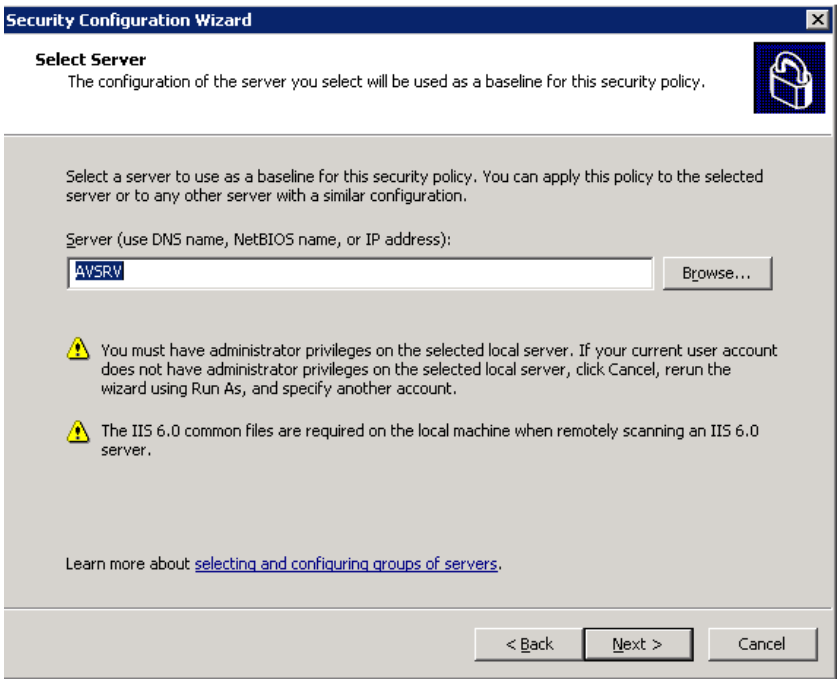


- Welcome page next butonuna basarak geçebiliriz.

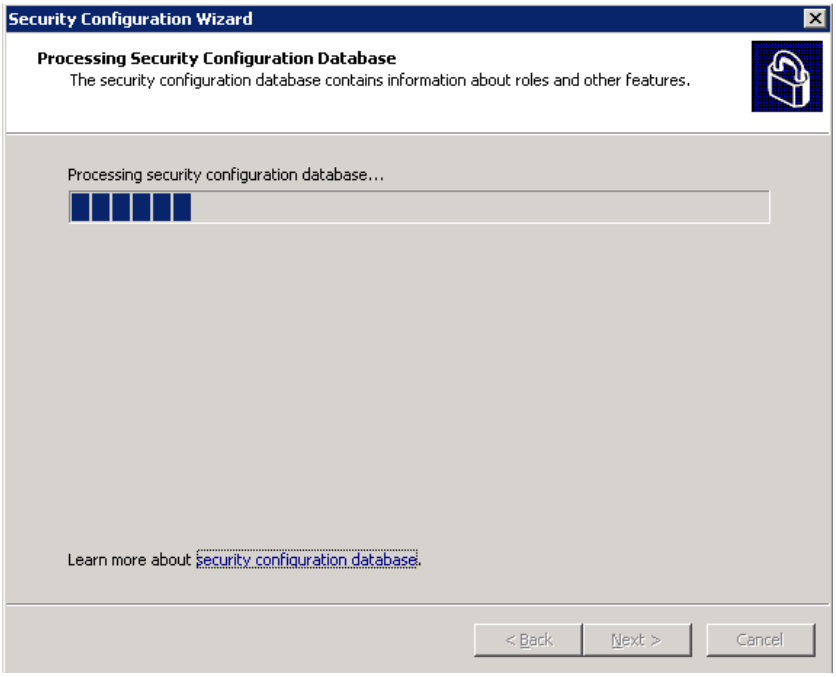
- Sonraki pencerede ben yeni bir security policy oluşturmak için create seçeneğini seçerek devam edeceğim. Burada yapabileceğimiz diğer işlemler daha evvel oluşturulmuş bir policy dosyasını değiştirmek, seçeceğimiz bir sunucuya uygulamak yada daha evvel uygulanmış olan policy' yi rollback seçilerek yapılan ayarları geri almak.



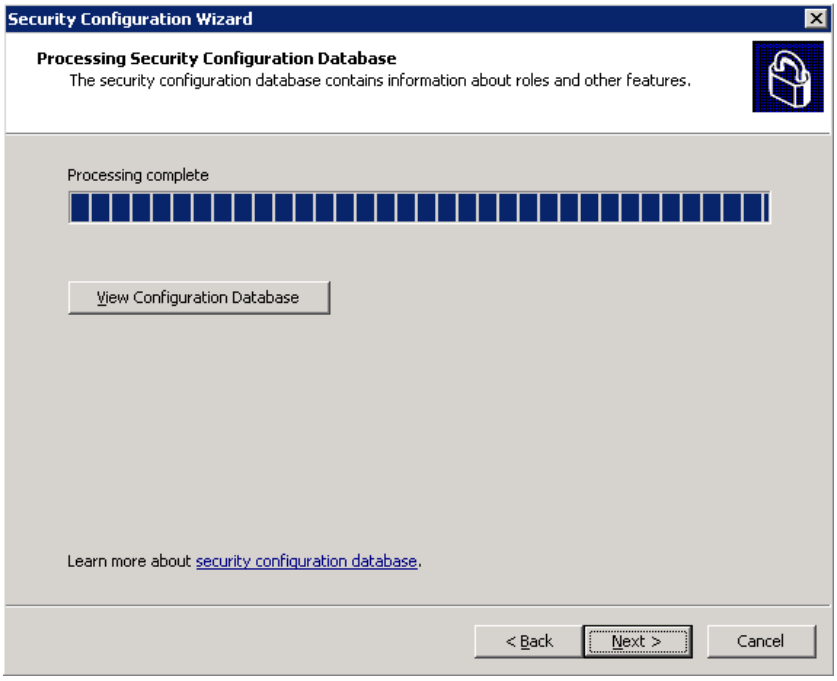
- Sonraki pencerede wizard' ın hangi sunucu için çalışacağını seçmemiz gerekmektedir. Default olarak wizard' ın çalıştırıldığı bilgisayarın bilgisayar ismi gelecektir. İsterseniz ağınızdaki başka bir sunucuyu da browse diyerek seçebilirsiniz. Burada dikkat etmemiz gereken en önemli nokta seçtiğimiz sunucunun üzerinde hizmet verilen tüm uygulamaların ve servislerin çalışır durumda olması gerektiğidir. Şayet normal zamanda çalışan bir servis, wizard çalıştırıldığında stop durumda olursa yada disable durumda olursa wizard bu servisi göz ardı edecek ve açılması için herhangi bir ayar yapmayacaktır. Unutmamanız gereken nokta security wizard' ın genel hareket şekli bir şeyleri kısmak yada kapatmak şeklinde olacaktır.



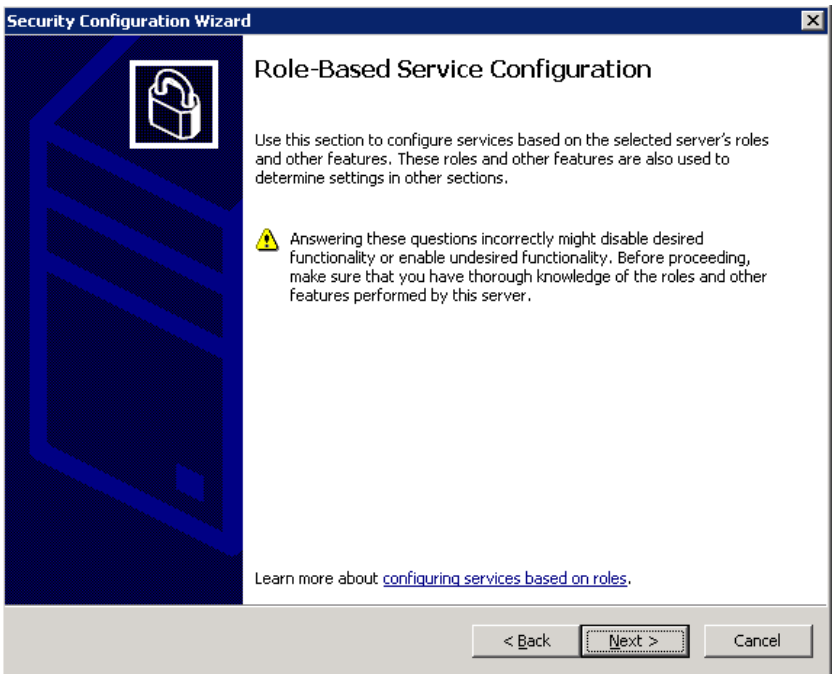
- Sunucu seçini sonrası next tuşuna bastığımızda wizard seçtiğimiz sunucu hakkında tüm bilgileri toplayacaktır.



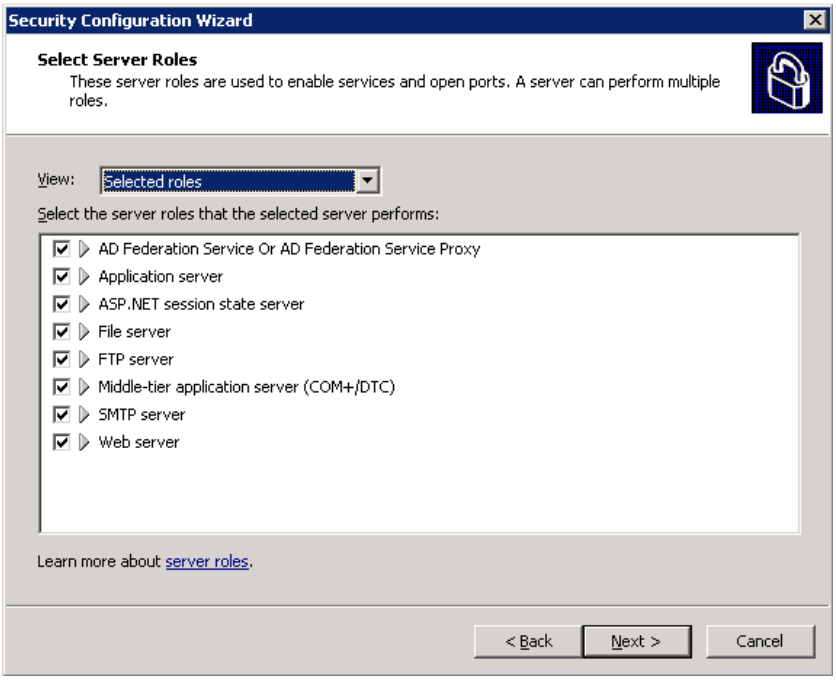
- Sunucu ile ilgili configuration database tamamlandıktan sonra isterseniz view butonu ile mevcut ayarları görebilirsiniz.



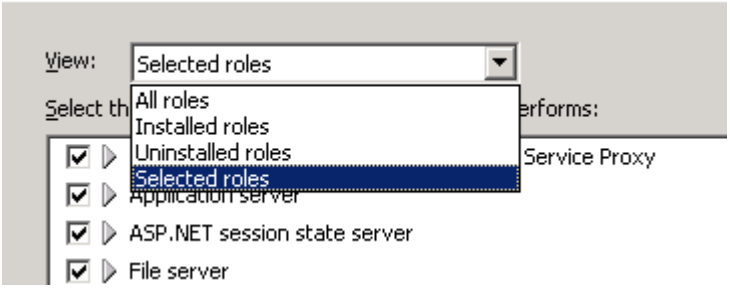
- Next ile devam ettiğimizde mevcut bilgiler üzerinden gidilerek yeni security policy' yi oluşturacağız. Policy oluşturma 5 ana kısımdan oluşmaktadır. 1nci kısım Role-Based Service kısmıdır. Bu kısımda sunucunun sunucu olarak mevcut rollerini (Server-Client mimarisindeki server kısmına giren rollerini), client olarak özelliklerini, yönetimsel özelliklerini ve servisler ile ilgili düzenlemeleri yapabiliriz.



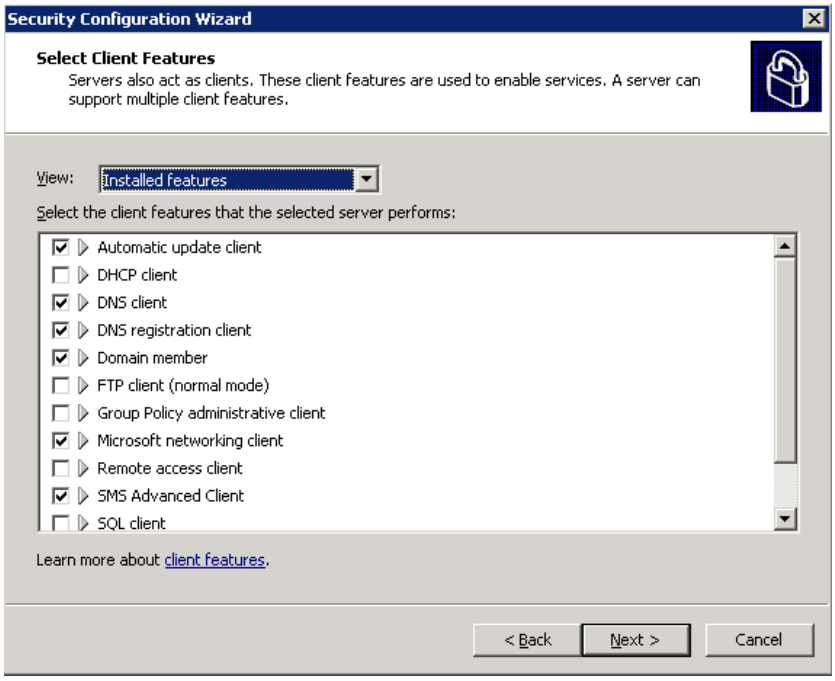
- Role-Based kısmında ilk olarak karşımıza sunucu rolleri gelecektir. Buradan şu anlamı çıkartabiliriz; bu sunucu bir file server, bir FTP server, bir web server gibi rollere sahiptir.



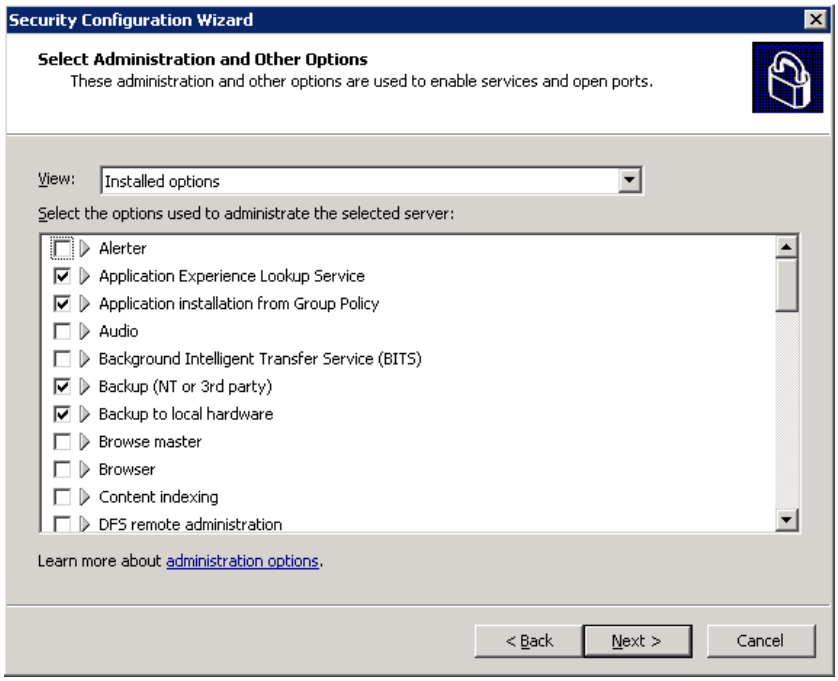
- Aynı pencere içerisinde view seçeneğini değiştirerek kurulu olan ve olmayan roller şeklinde de listeleme yapabiliriz. Kurulu olan bir servisin checkbox' ını işaretleyerek devreye alabilir yada listelenen rollerden gereksiz olarak gördüklerimizin checkbox' ını boşaltarak devre dışı bırakabiliriz.



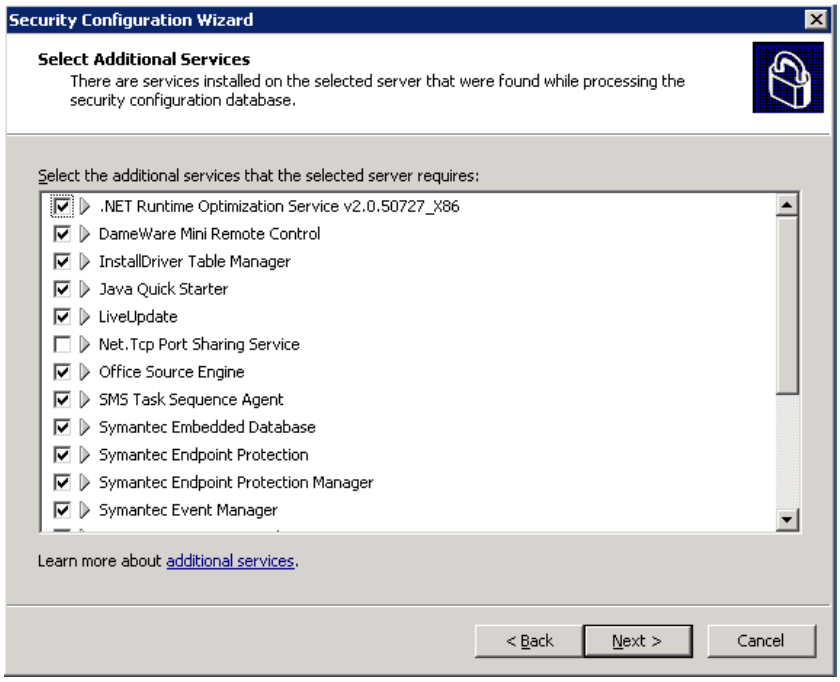
- Sonraki pencerede bu sunucunun bir client olarak özellikleri listelenir. Yine aynı şekilde istediğimizi kapatabilir ve istediğimizi devreye alabiliriz.



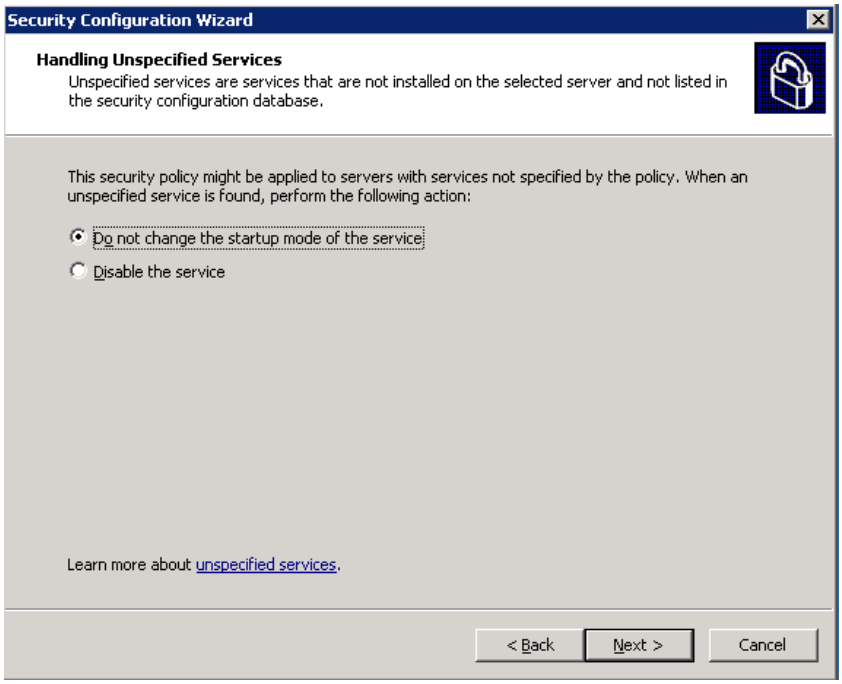
- Sonraki ekranda yönetimsel seçenekler ile ilgili ayarlamamızı yapabiliriz.



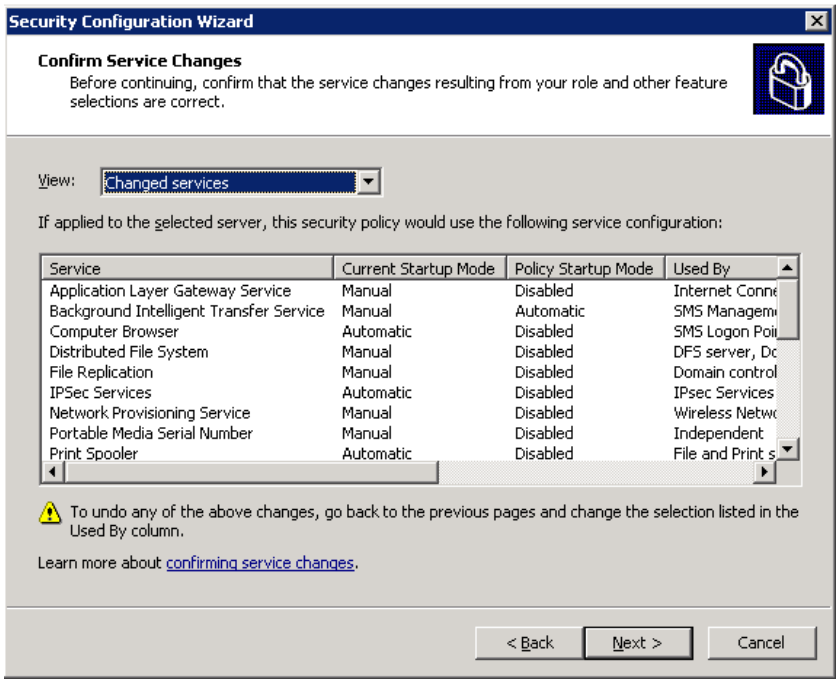
- Sonraki pencerede gelen bilgiler servisler ile ilgili bilgilerdir. Bu kısma dikkat etmeliyiz. Gereksiz gördüğümüz servisleri manuel olarak kaldırabiliriz.



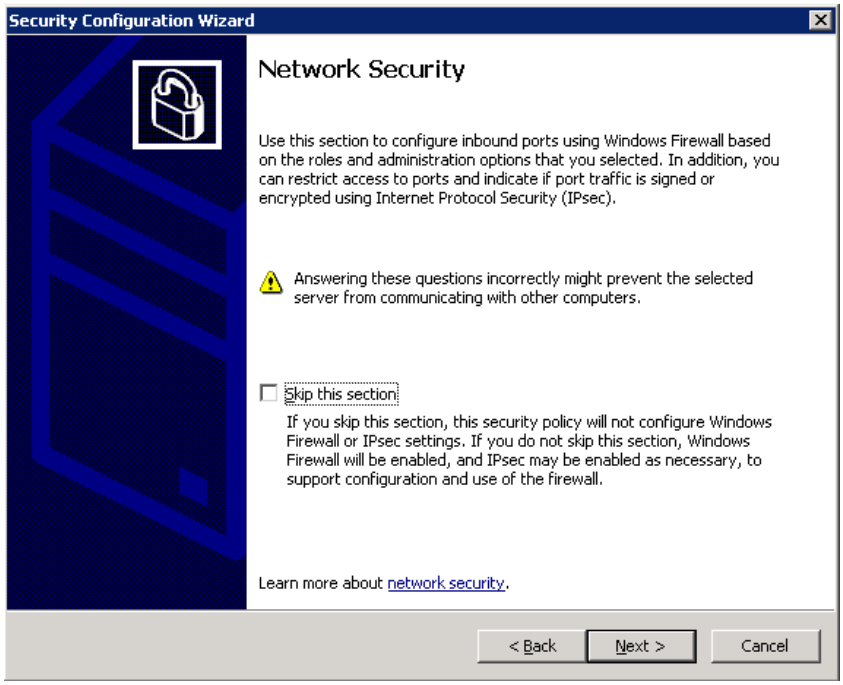
- Manuel olarak iptal ettiğimiz servisler ile alakalı olarak startup mode kısmını da istersek disable yapabilmekteyiz.



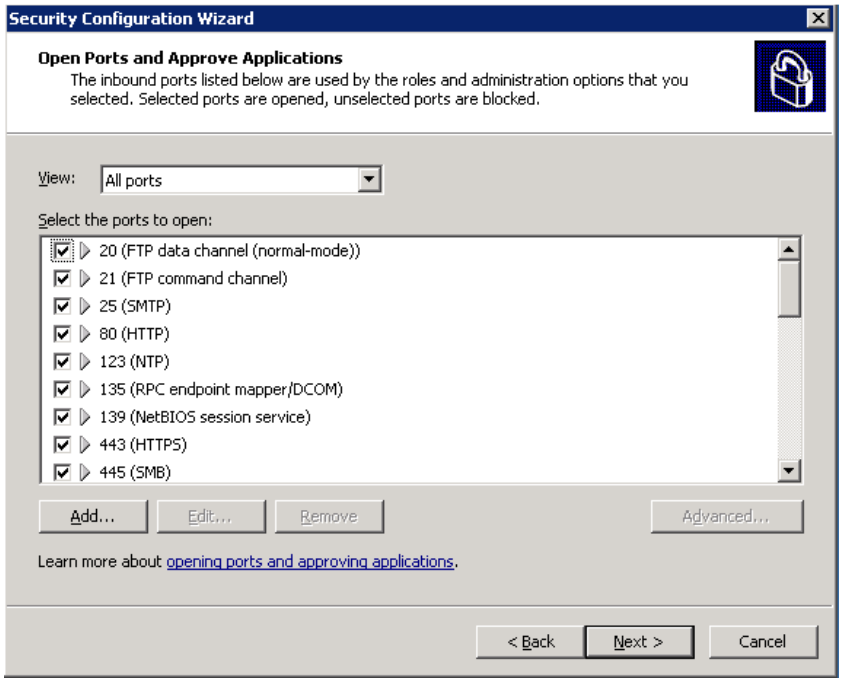
- Siz servisler ile ilgili manuel bir işlem yapmış olsanız da olmasanız da wizard size bazı ayarların değiştirildiği ile ilgili bazı bilgiler getirecektir. Bu işlemleri inceleyecek olursanız bir servisin mevcut ayarı ve policy uygulandıktan sonraki ayarını görebilirsiniz. Wizard bazı servislerin manuel iken otomatik hale gelmesinin yararlı olacağını bazılarının ise otomatik iken disable olması gerektiğini düşünerek size en uygun ayarları önerecektir. Bu kısmı incelemeniz ve şayet değişikliğinin uygun olmayacağını düşündüğünüz bir servis varsa back tuşu ile geri gelerek servisler ile ilgili düzenlemeyi tekrar yapmanız gerekmektedir.



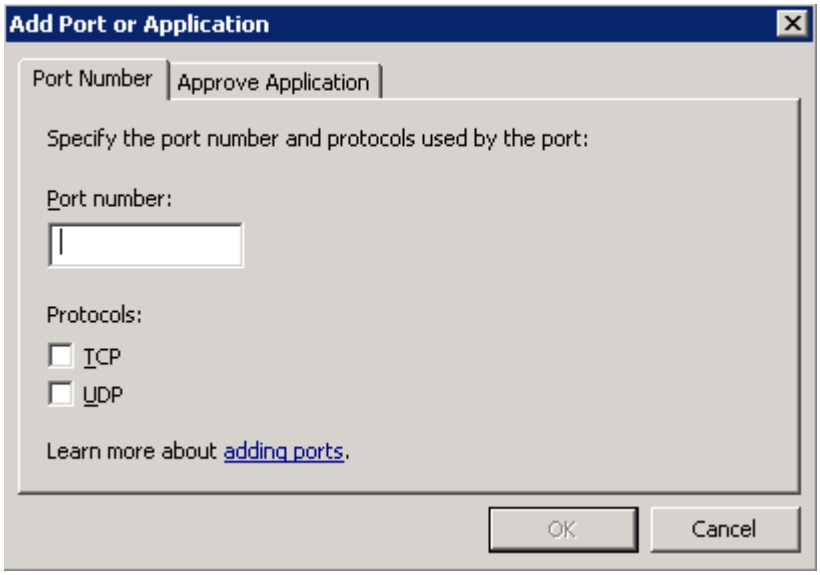
- Benim 2nci ana kısım olarak gördüğüm Network Security kısmına geldik. Bu kısımda genel olarak kullanılmasını istediğimiz ya da block' lanmasını istediğimiz portların ayarlarını yapabiliriz.



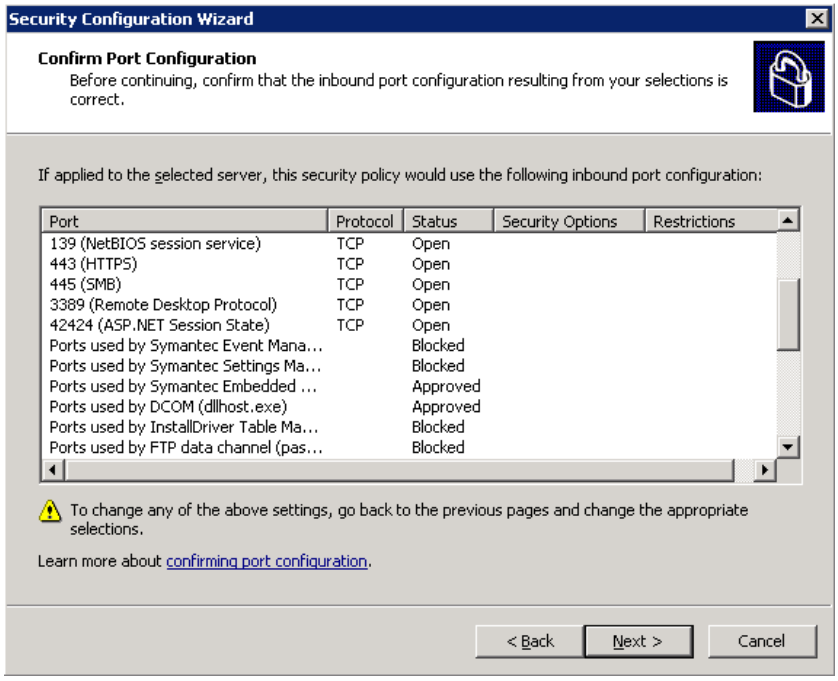
- İlk pencereyi next diyerek ilerlediğimizde sunucu üzerinde açık olan ve kullanılan portları görürüz. Bu liste üzerinde istediğimizi kaldırabilir yada onaylayabiliriz.



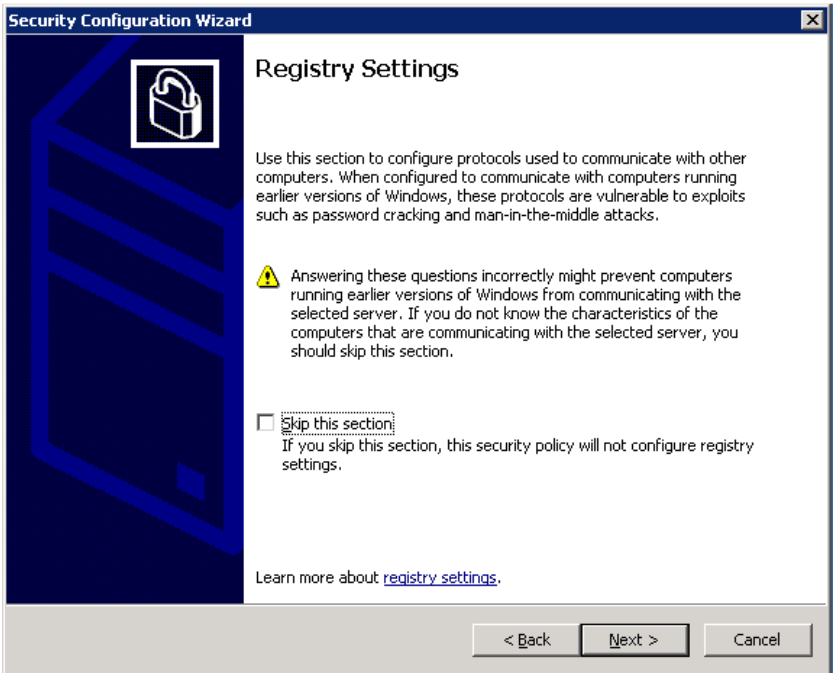
- Add kısmı kullanılarak manuel olarak port ekleyebiliriz / yada bir uygulama.



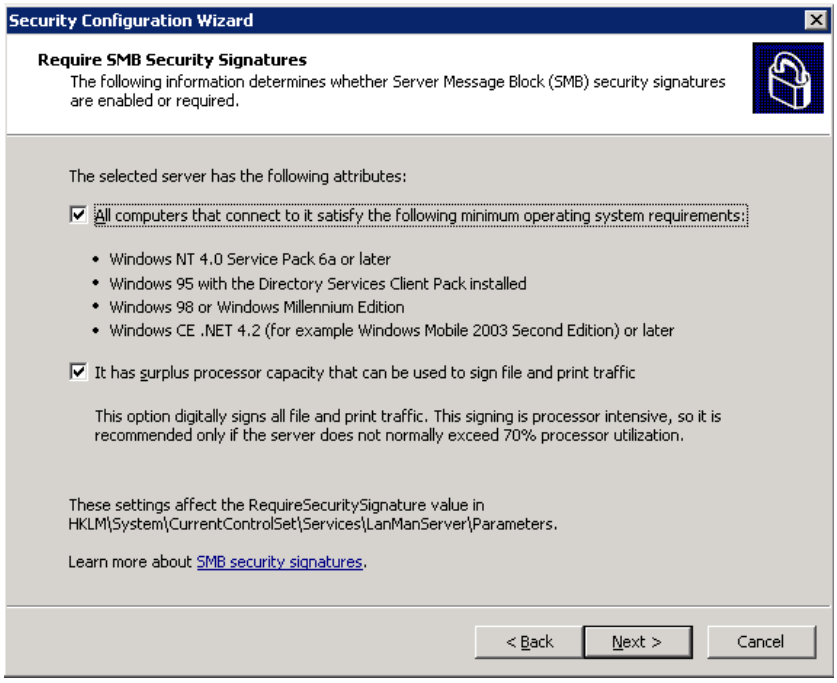
- Yaptığımız ayarlar çerçevesinde yine wizard bize son tabloyu gösterecektir. Burada block' lanacak ya da onaylanacak olan portları ve uygulamaları görebiliriz.



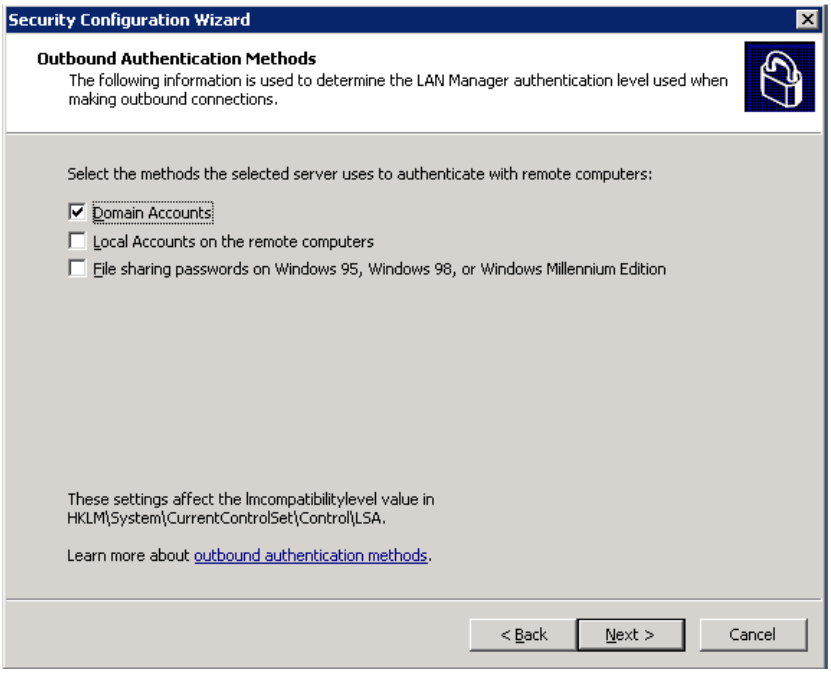
- 3ncü kısım olan Registry Setting kısmı;



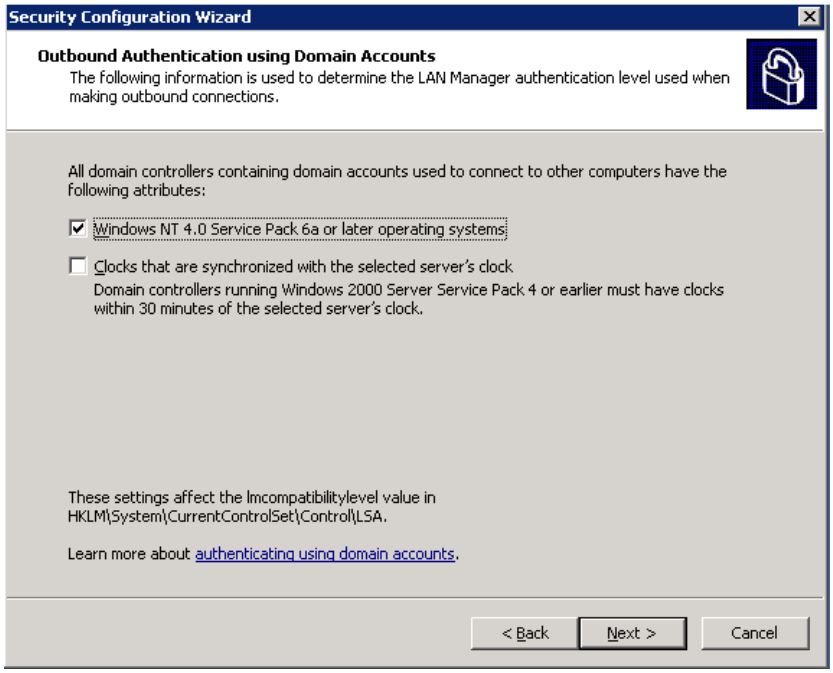
- İlk ekranda SMB (Server Message Block) ile ilgili ayarları yapabiliriz.



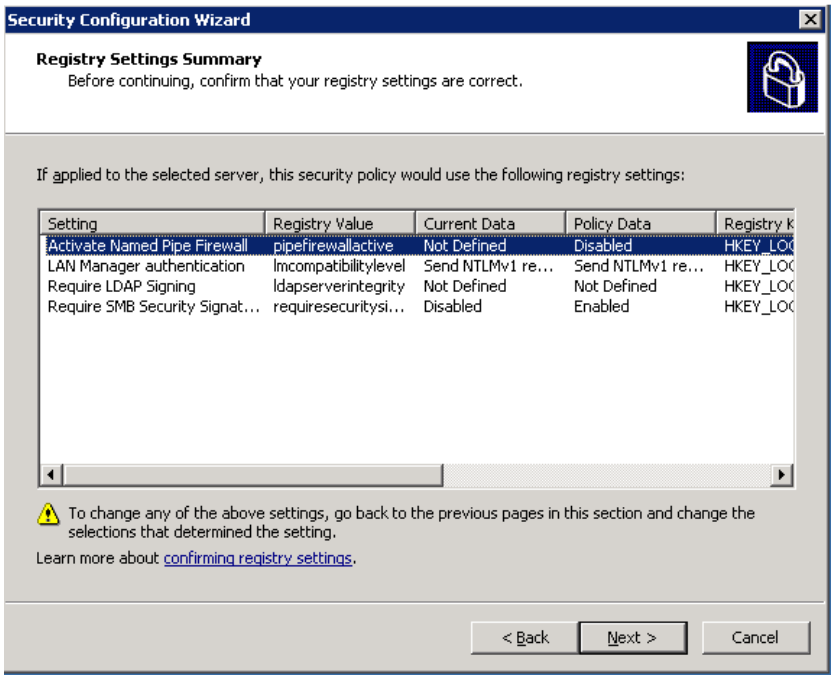
- Dışarıdan gelen istekler için kullanılacak kimlik doğrulama seçeneğini düzenleyebiliriz.



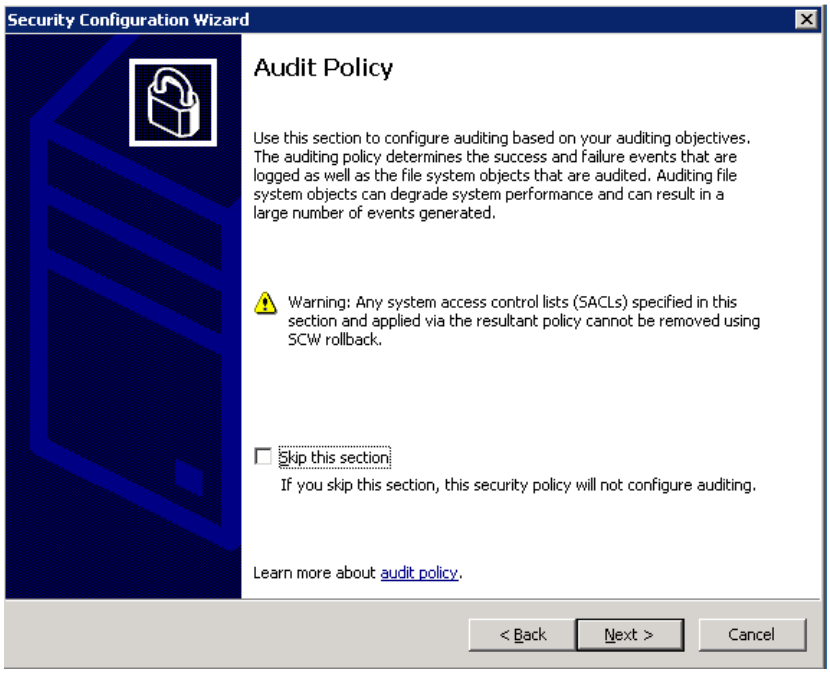
- Yine kimlik doğrulama ile ilgili ayarlar.



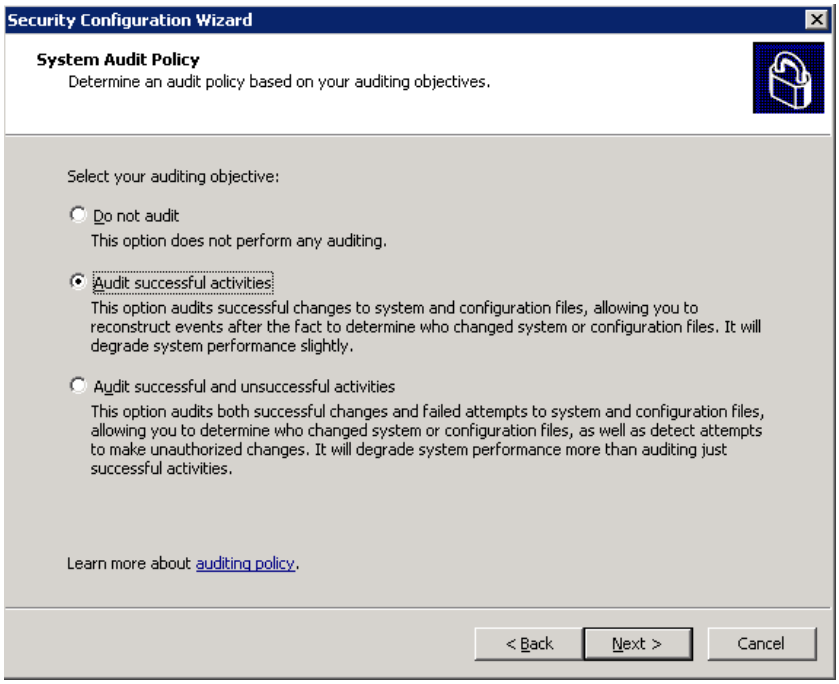
- Yine her kısmın sonunda olduğu gibi yapılan ayarların özet bilgisinin görüntülendiği pencere;



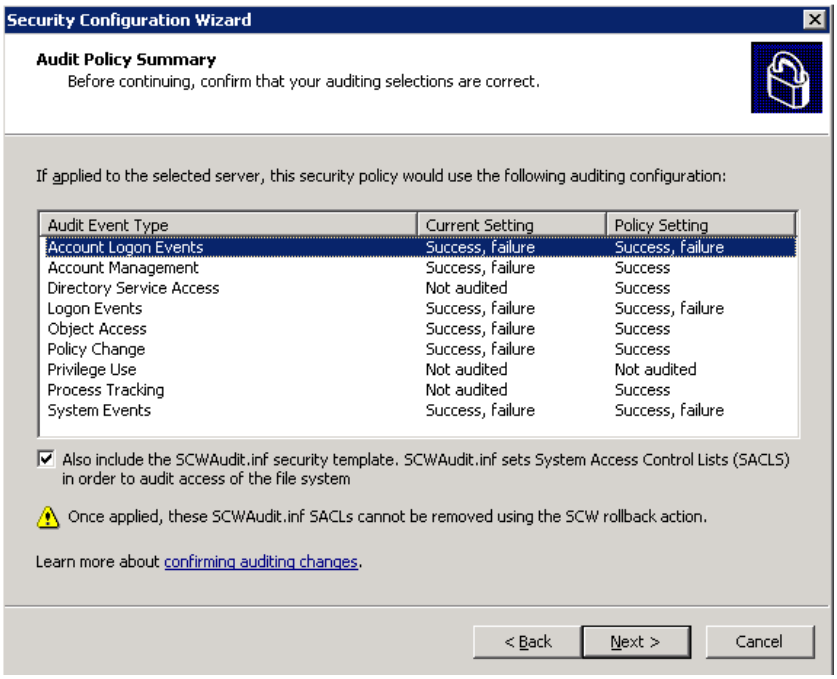
- 4ncü bölüm olan Audit Policy kısmı;



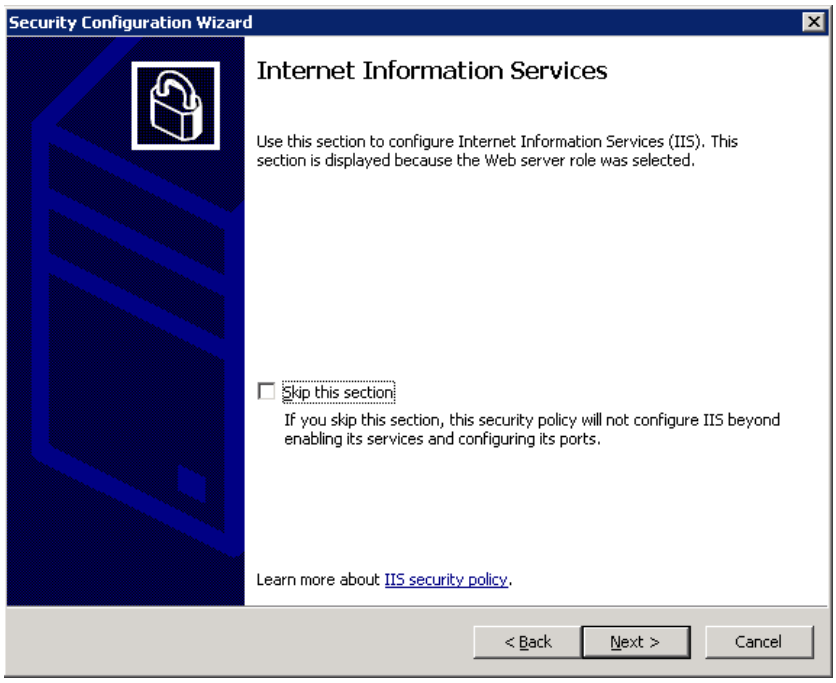
- Bu kısımda sadece sistem ile ilgili olan audit (denetim) aktivitelerinin kapsamını ayarlayabileceğimiz seçenekler mevcut.



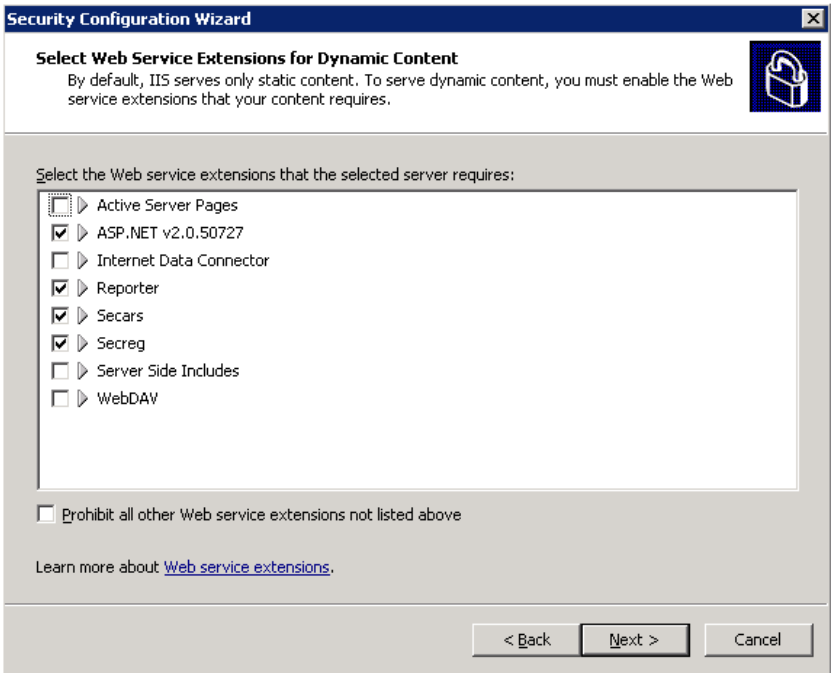
- Standart özet bilgi ekranı;



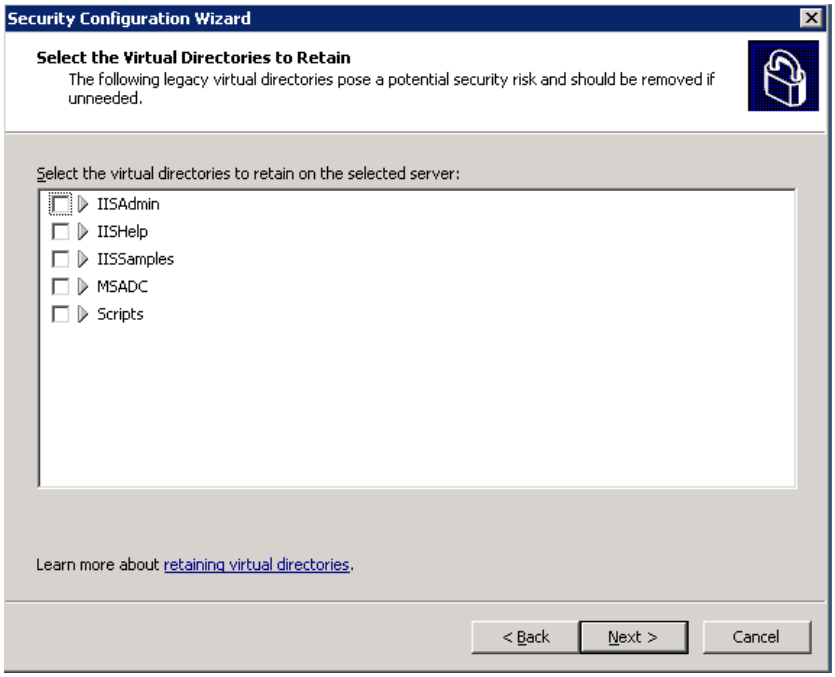
- 5nci ve son kısım olan IIS ile ilgili ayarları yapabileceğimiz kısım;



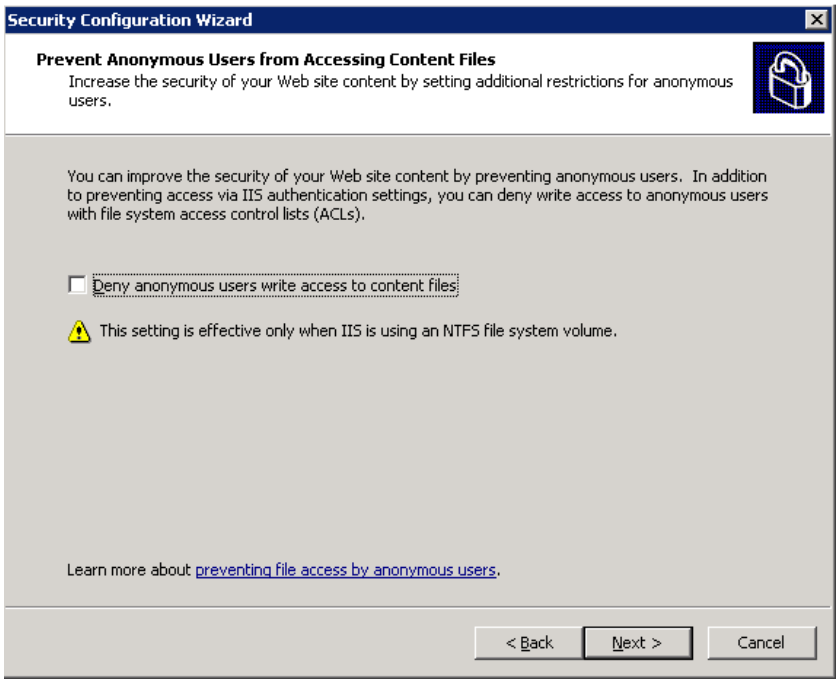
- IIS' in hizmet vereceği servisleri açıp kapatabileceğimiz pencere;



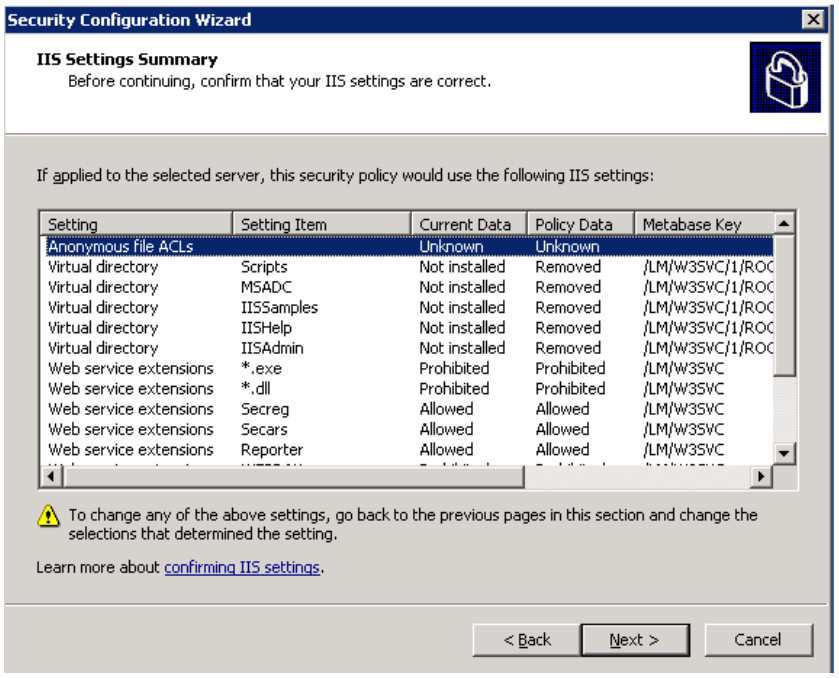
- Sanal dizinler ile ilgili seçeneklerin olduğu bir pencere;



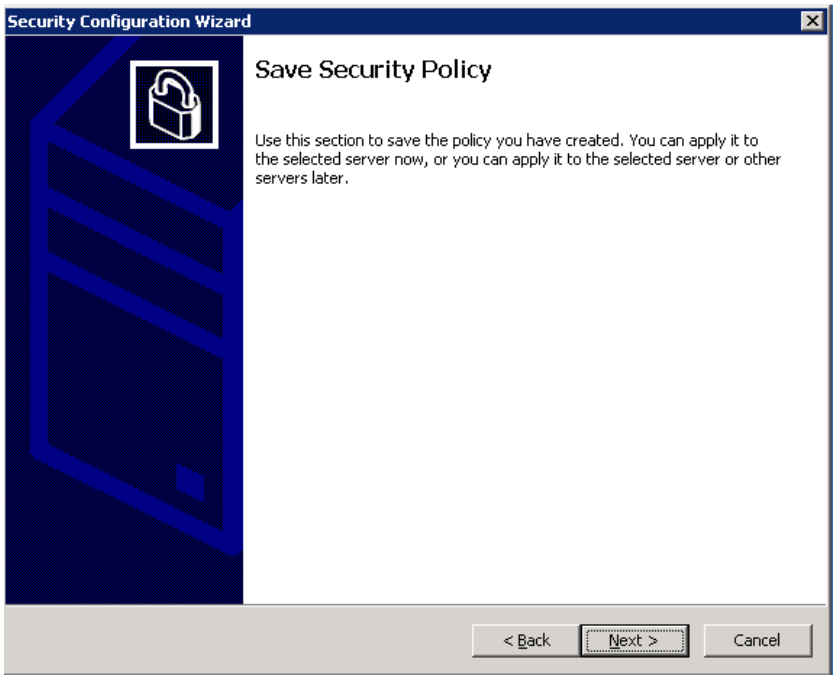
- Anonymous user' lar için içerik dosyalarına yazma hakkını engelleyebileceğimiz bir pencere;



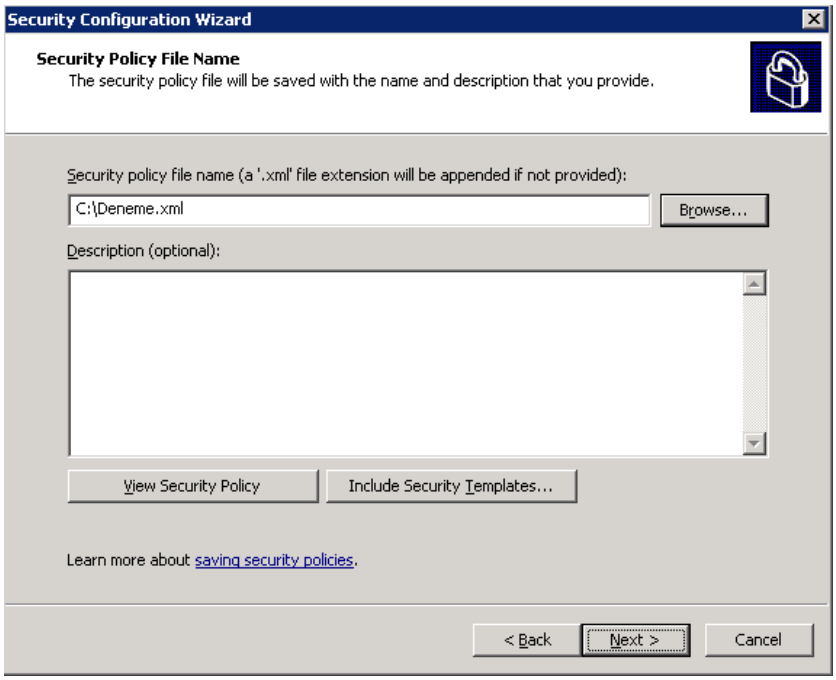
- IIS ile ilgili bizim ve yine wizard' ın yaptığı ayarlar görüntülenir.



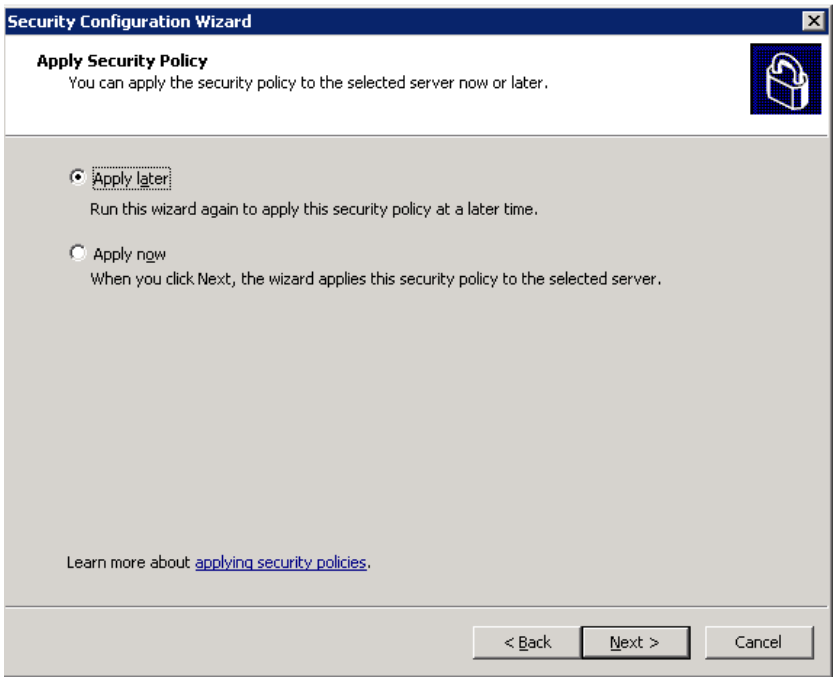
- Hazırladığımız policy' yi kaydetmek için next diyoruz;



- Policy' nin kaydedilmesini istediğimiz dizini seçerek bir isim veriyoruz. Ben deneme ismini verdim. Dosya otomatik olarak xml formatında kaydolacaktır.



- Sonraki pencerede bu policy' nin üzerinde hazırlanan sunucuya uygulanıp uygulanmayacağını seçebileceğimiz ekran gelmektedir. Ben bu policy' yi group policy object' i olarak kullanacağım ve bir OU' ya ekleyeceğim için bu sunucuya direk olarak uygulamıyorum.

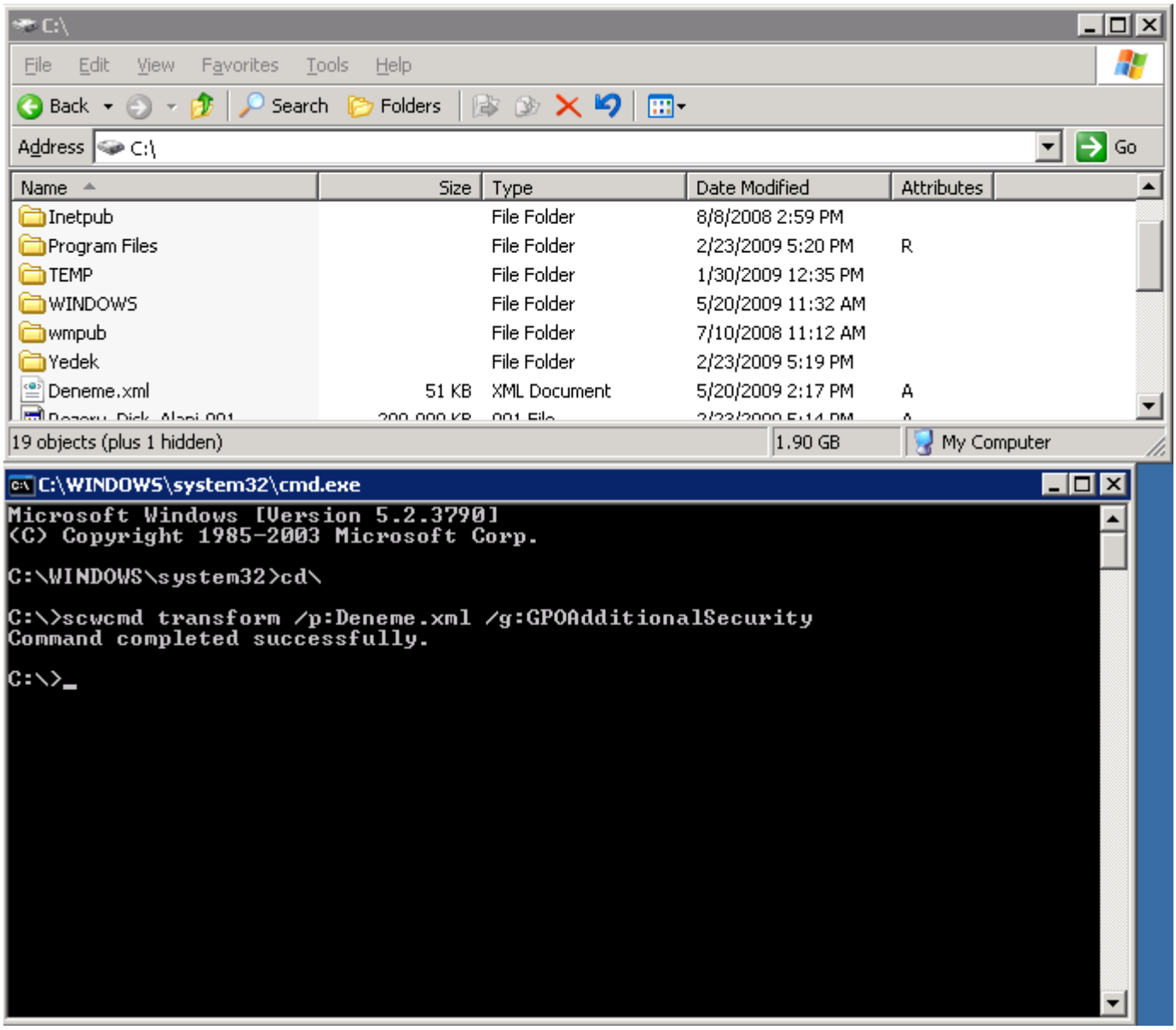


- Son olarak finish diyerek wizard' ı tamamlıyoruz.

Hazırladığımız dosya ile ilgili bazı bilgiler vermek gerekirse; bu dosyayı benzer özellikler taşıyan başka sunucularda yine wizard kullanılarak uygulayabiliriz, birazdan yapacağımız gibi group policy object' i haline getirerek AD ortamında da kullanabiliriz. AD ortamında bir OU' ya uygulamadan dikkat edilmesi gereken nokta, uygulanacak olan OU altındaki sunucuların aynı özellikleri taşıyor olması gerektiğidir. Yani üzerinde SQL uygulaması çalışan bir sunucu üzerinde oluşturduğumuz dosyayı içerisinde Exchange Sunucusu olan bir OU' ya uygular isek problem yaşayacağımız neredeyse kesindir diyebiliriz.

Bunun dışında 32 bit / 64 bit farkıda göz önünde bulundurmamız gereken bir ayrımdır.

Bu bilgilerden sonra hazırladığımız dosyayı group policy object' i haline getirmek için aşağıdaki işlemi yapmamız gerekmektedir.

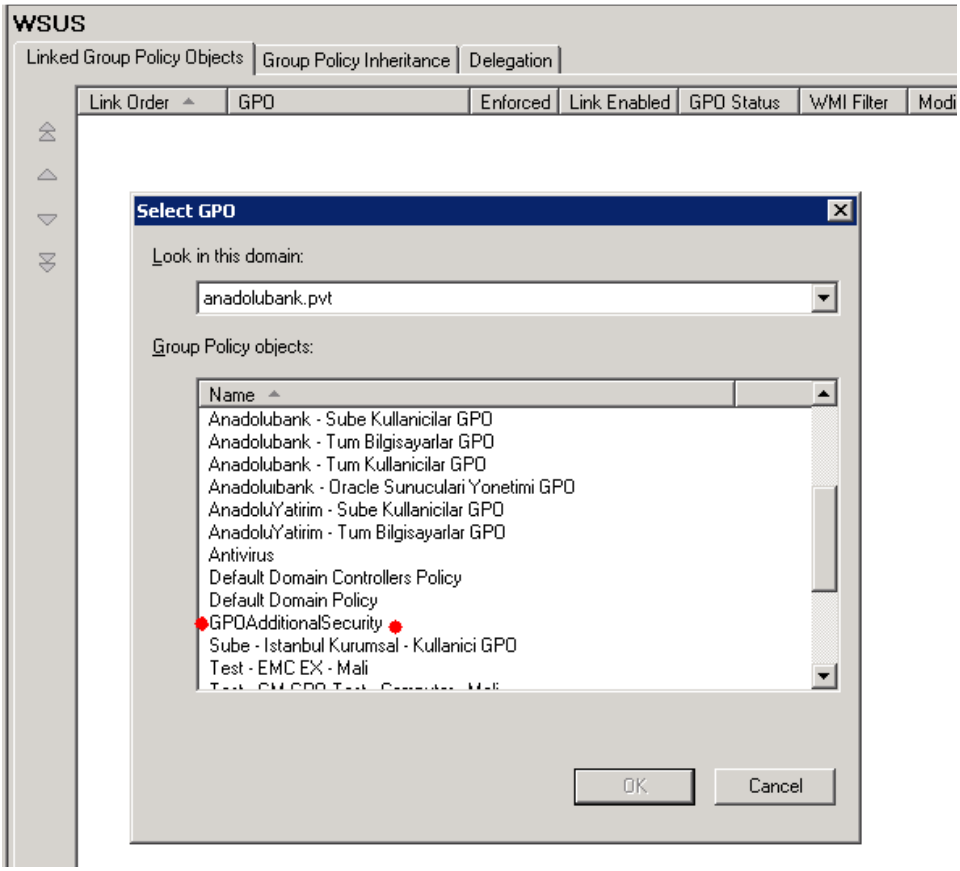


Ben hazırladığım dosyayı direk olarak C: altına kaydetmiştim. Komut satırını açıp aşağıdaki formata uygun olarak komutu girdiğimizde xml dosyamız group policy object' i olacak ve domain ortamına aktarılacaktır.

Scwcms transform /p:xxxxx.xml /g:GPOObjectName

Burada alabileceğiniz hata yazım yanlışı (sözdizimi) hatası ya da yetkisiz kullanıcı hatası olacaktır. Bu işlemi domain admins grubuna üye olan bir kullanıcı ile yapmanız gerekmektedir.

İşlemi başarılı bir şekilde tamamladığınızın mesajını aldığınızda kontrol etmek yada bu object' i bir OU' ya uygulamak için Group Policy Management Console' u açınız. Seçeceğiniz herhangi bir OU üzerinde Link GPO dediğinizde domain ortamındaki tüm policy' ler ile birlikte az önce oluşturduğunuz object' i de görebilirsiniz.



Hepinize iyi çalışmalar.