T.C.
MİLLÎ EĞİTİM BAKANLIĞI

BİLİŞİM TEKNOLOJİLERİ

SUNUCU İŞLETİM SİSTEMİ 4
481BB0068

Ankara, 2011

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**481BB0068**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**Sunucu İşletim Sistemi 4**
MODÜLÜN TANIMI	Bu modül; işletim sisteminde nesne erişimini denetleme, grup politikaları oluşturma ve yönetme, kullanıcı ve bilgisayar izinlerini belirleme, hesapları ve kaynakları yönetme gibi işlemleri içeren bir öğrenme materyalidir.
SÜRE	40/32
ÖN KOŞUL	Sunucu İşletim Sistemi 3 modülünü tamamlamış olmak
YETERLİK	Sunucu işletim sisteminin grup Politikalarını sağlamak
MODÜLÜN AMACI	**Genel Amaç** Gerekli ortam sağlandığında; sunucu işletim sisteminde grup politikalarını gerçekleştirebileceksiniz. **Amaçlar** **1.** Nesne erişimini yönetebileceksiniz. **2.** Grup politikası işlemini gerçekleştirebileceksiniz. **3.** Grup politikalarını kullanarak kullanıcı ve bilgisayar ortamını yönetebileceksiniz. **4.** Hesapları ve kaynakları yönetebileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam** Sunucu işletim sistemi bulunan bilgisayarlardan oluşan laboratuvar **Donanım** Sunucu işletim sistemi yazılımı
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. ➢ Modül sonunda uygulanacak ölçme araçları ile modül uygulamalarında kazandığınız bilgi ve beceriler ölçülerek değerlendirilecektir

GİRİŞ

Sevgili Öğrenci,

Sunucu işletim sistemleri, ağ üzerindeki kaynakları kullanıcılara uygun izinlerle paylaştıran, yönetimde verimliliği hedefleyen güçlü sistemlerdir. Bir firmada bilgisayar ve kullanıcılar arttıkça bunların yönetimi ve denetimi zorlaşmaktadır. Bu gibi durumlarda yönetimi mantıksal birimlere bölmek ve her birime bir yönetici atamak gerekebilir. Ayrıca her yöneticiyi, ayrı kaynakların yönetimi için farklı yetkilerle donatabiliriz. Bu sayede yönetimi kolaylaştırmış ve verimliliği artırmış oluruz.

Yönetimi mantıksal birimlere bölmek için kullanılan organizasyon birimleri, kendi içerisinde bulunan sistem kaynaklarını basite indirgenmiş bir şekilde yönetmeyi hedefler. Organizasyon birimine atayacağımız yöneticiler ise birime bağlı kullanıcı hesaplarını, bilgisayar ve diğer kaynakları yöneterek sistemin ana yöneticisine düşen ağır yönetim yükünü hafifletmiş olur.

Sistemin geneline veya organizasyon birimlerine uygulanan grup yönetim politikaları, yönetimi bilgisayarlar ve kullanıcılar bazında ele alıp bunların denetim ve yönetimi için gerekli ayarlamaları gerçekleştirir. Grup politikaları bilgisayar yazılım ayarları, windows bileşenlerinin ayarları, güvenlik ayarları, kullanıcı profilleri, komut dosyaları, ağ yönetim ayarları, kullanıcı parola ve oturum açma ayarları gibi birçok ayarları düzenlemekte kullanılan çok kullanışlı bir yönetim bileşenidir. Grup politikaları, sistemin geneline uygulanabildiği gibi farklı amaçlar için oluşturulan organizasyon birimleri için de kullanılabilir.

Bu modülde Active Directory tanımları ve nesneleri, organizasyon birimlerinin oluşturulması ve yetkilendirilmesi, grup politikası oluşturulması, kullanıcı ve bilgisayarlar için grup politikalarının düzenlenmesi, sistem yönetiminde güvenlik ilkeleri, sistem güvenliği için yapılacak ayarlamalar ve alınacak tedbirler, kullanıcı izinlerinin ve kısıtlamalarının düzenlenmesi gibi birçok güvenlik politikalarını öğrenecek ve uygulamalı olarak bu işlemleri gerçekleştireceksiniz.

ÖĞRENME FAALİYETİ-1

AMAÇ

Nesne erişimini yönetebilecektir.

ARAŞTIRMA

- Active Directory ve Active Directory Nesneleri terimlerinin ne anlama geldiğini araştırıp arkadaşlarınızla bilgilerinizi paylaşınız.
- Organizasyon biriminin ne anlama geldiğini ve bize sağlayabileceği faydaları araştırıp bilgilerinizi arkadaşlarınızla paylaşınız.

1. NESNE ERİŞİM YÖNETİMİ

1.1. Active Directory Nesneleri için Organizasyon Biriminin Rolü

1.1.1. Active Directory Nesneleri için Genel Tanımlar

Birden fazla bilgisayarı, kullanıcıları, paylaştırılmış ağ kaynakları olan büyük şirketlerin bu kaynakları daha verimli ve güvenli kullanabilmesi için işletim sistemleri içerisinde karmaşık yönetim yapılarına veya protokollerine ihtiyaç duyulmaktadır. Windows sunucu işlerim sistemleri için ağ kaynaklarını verimli bir şekilde yönetebilecek yapılara Active Directory, Organizasyon Birimi (Yapısal Birim) gibi yönetimsel yapıları örnek verebiliriz.

Active Directory; kullanıcı hesaplarını, grupları, yazıcıları ve diğer birçok ağ kaynaklarını, merkezî olarak yöneten ve denetleyen; izinlerini belirleyen, kaynaklarla ilgili verileri tutan karmaşık ve güvenli bir yapıdır.

Active Directory ile ilgili genel kavramlar:

- **Active Directory nesneleri:** Bilgisayarlar, kullanıcılar, gruplar, yazıcılar gibi Active Directory üzerinden izinler belirlenebilen veya denetlenebilen birimlerdir.

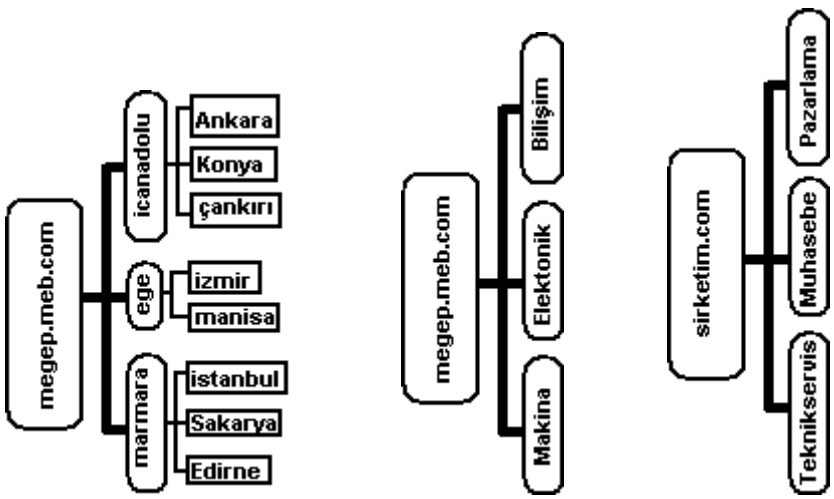
- **Active Directory şemaları:** Active Directory nesneleri hakkında verilerin tutulduğu, değişikliklerin otomatik olarak güncellendiği bir yapıdır.

- **Etki alanı:** Active Directory'nin mantıksal bileşenleri içerisinde yer alan, ağ üzerindeki kaynakları paylaştırılmış birden fazla bilgisayarın oluşturduğu birimdir.

- **Organizasyon birimi:** Belirli bir amaç için oluşturulmuş, etki alanı içerisindeki Active Directory nesnelerini gruplandıran ve yöneten mantıksal bir birimdir.

1.1.2. Active Directory Nesneleri İçin Organizasyon Birimi

Organizasyon birimi, belirli nesneleri bünyesinde toplayıp bir yöneticiye devretmekte, etki alanları içerisinde iş bölümü yapan çeşitli gruplar oluşturmakta kullanılan yönetimsel yapılardandır. Örneğin **"megep.meb.com**" isminde bir etki alanı "Domain" oluşturulsun. İç Anadolu, Ege, Marmara bölgelerindeki bilgisayarları kendi içinde gruplara ayırıp bir yönetici atamak istersek her bölge için organizasyon birimi atamalıyız. Her bölge için oluşturulan organizasyon birimlerinin yöneticileri de yalnızca kendi bölgelerini yönetmiş olur. Bu şekilde şubeleri çok olan ülke çapına yayılmış bir ağı yönetmesi de kolay olacaktır.



(a) **(b)** **(c)**

Şekil 1.1: Farklı organizasyon birimlerinin oluşturulması

Organizasyon birimleri oluştururken kendi içerisinde değişik alt organizasyon birimleri de oluşturulabilir. **Şekil 1.1'**de oluşturulmuş üç farklı organizasyon birimi görülmektedir. **Şekil 1.1.a'**da **"megep.meb.com**" ismindeki etki alanı önce üç farklı coğrafi bölgeye ayrılacak şekilde organizasyon birimleri oluşturulmuş sonra da her bölge organizasyon birimi için alt organizasyon birimleri oluşturulmuştur. Bu şekilde "İzmir" ismindeki organizasyon birimi "ege" organizasyon birimine; "ege" organizasyon birimi de **"megep.meb.com**" ismindeki etki alanına bağlanmış ve kaynak yönetimi paylaştırılmıştır. **Şekil 1.1.b'**de **"megep.meb.com**" ismindeki etki alanı için bölüm bazında üç farklı organizasyon birimi oluşturulmuştur.

Şekil 1.1.c'de **"sirketim.com**" ismindeki etki alanı için yönetim bazında üç farklı organizasyon birimi oluşturulmuştur.

Organizasyon birimleri oluşturulduktan sonra yönetmesi için organizasyon birimi içerisine Active Directory nesneleri (bilgisayar, kullanıcı, yazıcı vb.) ekleyebiliriz. Ağ içerisindeki her Active Directory nesnesinin bir tanımlama bilgisi (distinguished name) bulunmaktadır.

- **Common Name (CN) :** Active Directory nesnelerinin adını belirtir.
- **Organization Unit (OU) :** Organizasyon biriminin adını belirtir.
- **Domain Controller (DC):** Etki alanının adını belirtir.

Örneğin, **Şekil 1.1.c'**deki "Pazarlama" organizasyon birimi içerisindeki "Lab_01" isimli bilgisayarın tanımlama bilgisi;

CN="Lab_01" **OU=**"Pazarlama" **DC=**"sirketim" **DC=**"com"

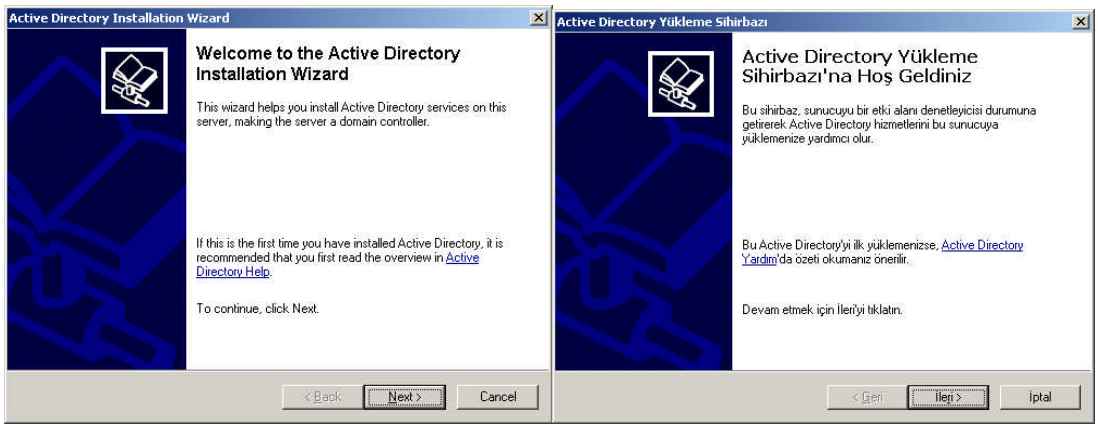
şeklinde olur. Örnekleri bu şekilde artırabiliriz.

1.2. Active Directory Nesneleri İçin İzinler

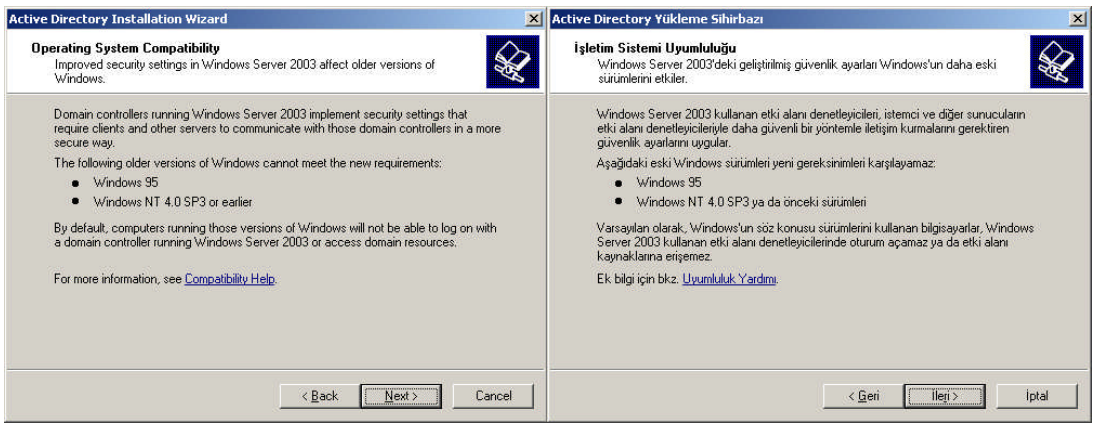
1.2.1. Active Directory Kurulumu

Active Directory kurulumu sırasında DNS varsayılan olarak kurulur. Bu nedenle Active Directory kurulumuna başlamadan önce IP'si statik yapılmalıdır. DNS Server IP'si olarak da Active Directory kurulacak bilgisayarın yerel IP'si yazılmalıdır.

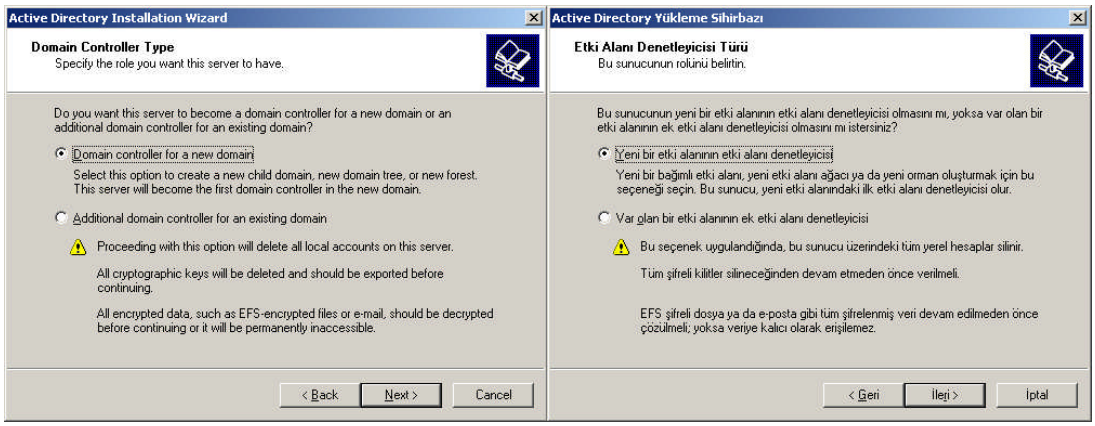
Active Directory ile yapılacak çalışmalardan önce Active Directory'nin kurulması gerekir. Active Directory kurulumu "Configure Your Server Wizard" ile yapılacağı gibi komut satırından "dcpromo" komutuyla da yapılabilmektedir. Kurulum için **"Start => Run"** (Başlat => Çalıştır) bölümüne **"dcpromo"** yazılıp "OK" (Tamam) butonunu tıkladığımızda **Resim 1.1'**deki "**Active Directory Yükleme Sihirbazı"** karşımıza gelir. **Resim 1.1** ve **Resim 1.2'**deki pencerelerde "Next" (ileri) butonuna bastıktan sonra karşımıza "Domain Controller" (Etki alanı denetleyicisi) türünü belirlemeyle ilgili **Resim 1.3'**teki pencere karşımıza gelir.



Resim 1.1: Active Directory Yükleme Sihirbazı (Win 2003 Eng ⇔ Win 2003 Tr)

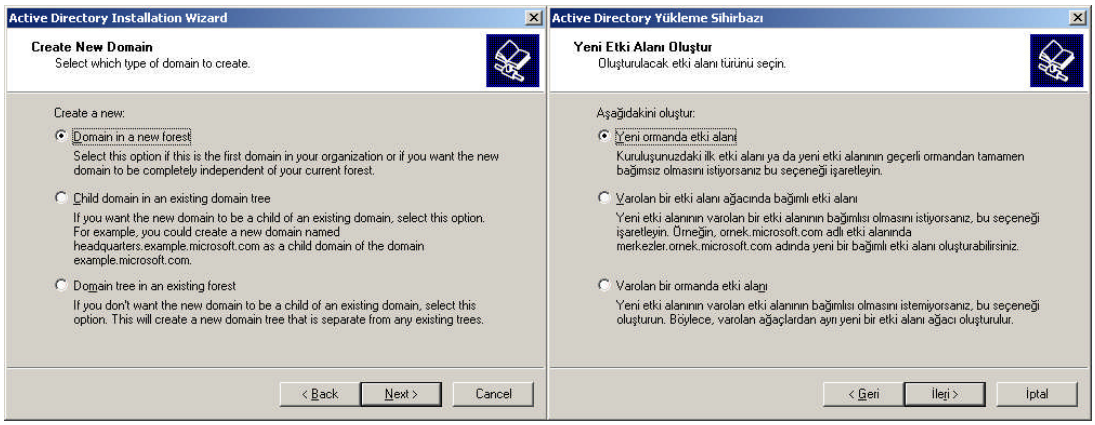


Resim 1.2: Active Directory işletim sistemi uyumluluğu (Win 2003 Eng ⇔ Win 2003 Tr)



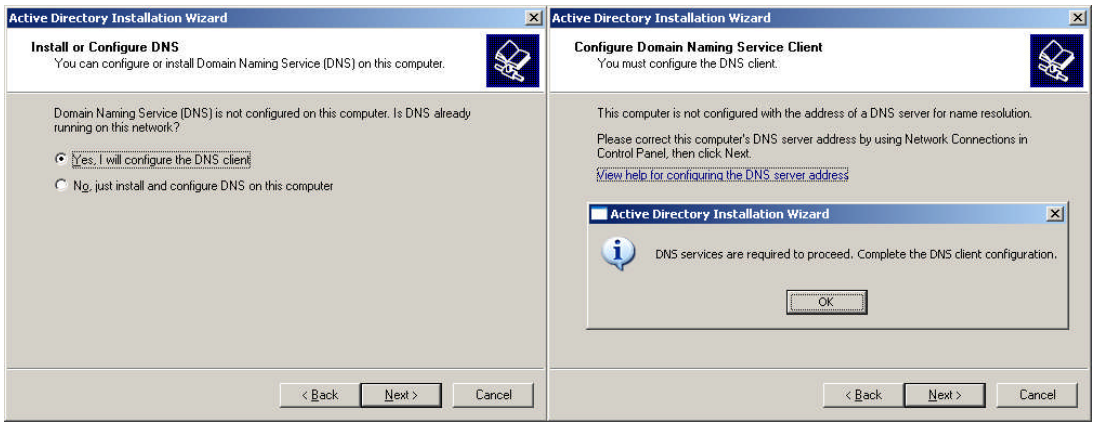
Resim 1.3: Active Directory Yükleme Sihirbazı (Win 2003 Eng ⇔ Win 2003 Tr)

"Domain Controller" (etki alanı denetleyicisi) kurulum türünü belirleyen **Resim 1.3'**teki pencerede iki farklı seçenek vardır. "Domain controller for a new domain" (yeni bir etki alanı denetleyicisi) seçeneği yeni bir etki alanı kontrolcüsü seçeneği oluşturmak için kullanılır. "Additional domain controller for an existing domain" (var olan bir etki alanının ek etki alanı denetleyicisi) seçeneği ise var olan etki alanına ek bir denetleyici oluşturmak için kullanılır. Etki alanında herhangi bir sorun olduğunda oluşturulacak bu ek etki alanı denetleyicisi devreye sokulur. Bu ek etki alanı denetleyicisi oluşturmadan önce tüm yerel hesaplar ve şifreli kilitler silineceğinden, şifreli dosyalar veya e-postalar çözülmelidir. Aksi hâlde verilere kalıcı olarak erişilemez. Biz ilk defa etki alanı denetleyicisi oluşturacağımız için "Domain Controller for a new domain" (yeni bir etki alanı denetleyicisi) seçeneğini işaretleyip "Next" (ileri) butonuna basıyoruz ve **Resim 1.4**'teki yeni etki alanının oluşturulacağı pencereyi açıyoruz.



Resim 1.4: Yeni etki alanı oluşturulması ***(Win 2003 Eng ⇔ Win 2003 Tr)***

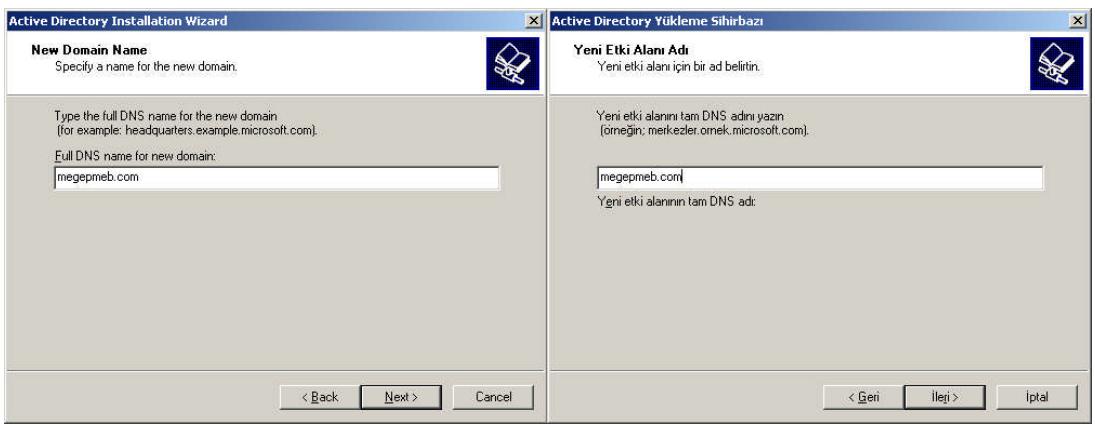
Oluşturulacak etki alanının türünün seçildiği **Resim 1.4'**teki bu pencerede üç farklı seçenek bulunmaktadır. "Domain in a new forest" (yeni ormanda etki alanı) seçeneği yeni bir etki alanı oluşturmak için kullanılır. Burada "forest" (orman) tan kastedilen bir ağdaki birden fazla etki alanlarıdır. Her etki alanı bir ağaç yapısında olduğu için ağaç yapısındaki etki alanları da ormanları oluşturur. "Child domain in an existing domain tree" (var olan bir etki alanı ağacına bağımlı etki alanı) seçeneği var olan bir etki alanına bağımlı küçük etki alanları oluşturmak içindir. "Domain tree in an existing forest" (var olan bir ormanda etki alanı) seçeneği ise var olan bir etki alanından bağımsız farklı bir etki alanı daha oluşturmak için kullanılır. Biz ilk defa etki alanı oluşturacağımız için "Domain in a new forest" (yeni ormanda etki alanı) seçeneğini işaretleyip "Next" (ileri) butonuna basıyoruz ve **Resim 1.5'**teki yeni etki alanının oluşturulacağı pencereyi açıyoruz.



(a) **(b)**

Resim 1.5: DNS kurulum veya Ayarlama Penceresi ***(Win 2003 Eng ⇔ Win 2003 Tr)***

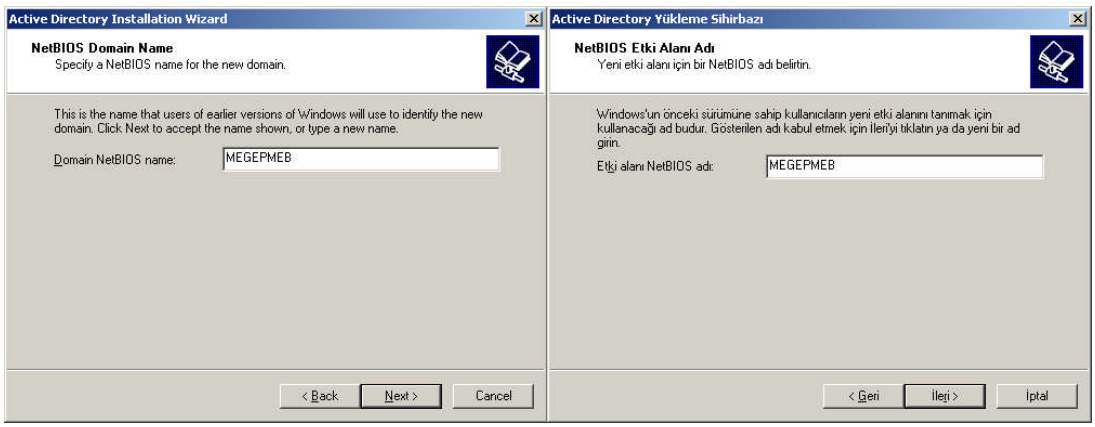
Resim 1.5.a'daki gibi mevcut bir DNS bulunup bulunmadığını soran bir pencere geliyor eğer "Yes, I will configure the DNS clint" seçeneğini seçerseniz kurulu DNS servisini arar ve bulamaz ise **Resim 1.5.b'**deki uyarı mesajını verir. Biz ilk defa DNS kuracağımız için "No, Just install and configured DNS on this computer" seçeneğini seçip "Next" (ileri) butonuna basıyoruz ve **Resim 1.6'**da ki etki alan adının yazıldığı pencereyi açıyoruz. "Windows Server 2003 Türkçe" sürümünde **Resim 1.5'**teki pencere gelmemekte, **Resim 1.6'**daki pencereye geçilmektedir.



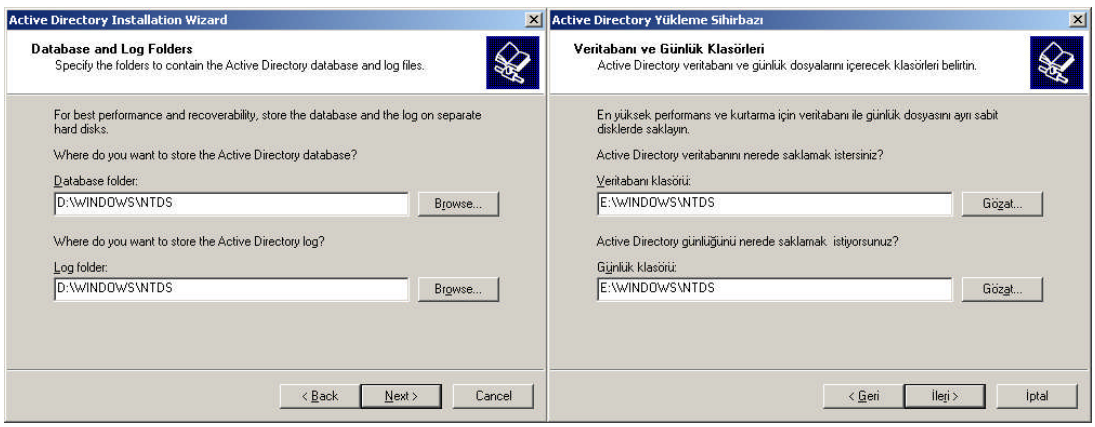
Resim 1.6: Yeni etki alan adının belirlenmesi ***(Win 2003 Eng ⇔ Win 2003 Tr)***

Oluşturulacak yeni etki alan adının belirlendiği Resim **1.6**'daki alana örnek olarak biz "megepmeb.com" verdik. Bu alana yazılan isim aynı zamanda DNS ismi de olacaktır. Alan adını belirleyip "Next" (ileri) butonuna bastıktan sonra windows eski sürümleri için NetBIOS adının belirlendiği **Resim 1.7**'deki pencere karşımıza gelecektir. Bu bölüme de istersek DNS adının aynısını verebiliriz. NetBIOS adını da belirleyip "Next" (ileri) butonuna bastıktan sonra karşımıza **Resim 1.8'**deki veritabanı ve günlük klasörlerinin yerlerinin belirlendiği pencere gelecektir.

Active Directory ve DNS kurulacak bilgisayar gerçek dünya İnternet'ine çıkacak ise kullanılan etki alanı adı benzersiz olmalıdır. Tercih edilen metot ise "etkialanadi.local" şeklinde isim verme metodudur.

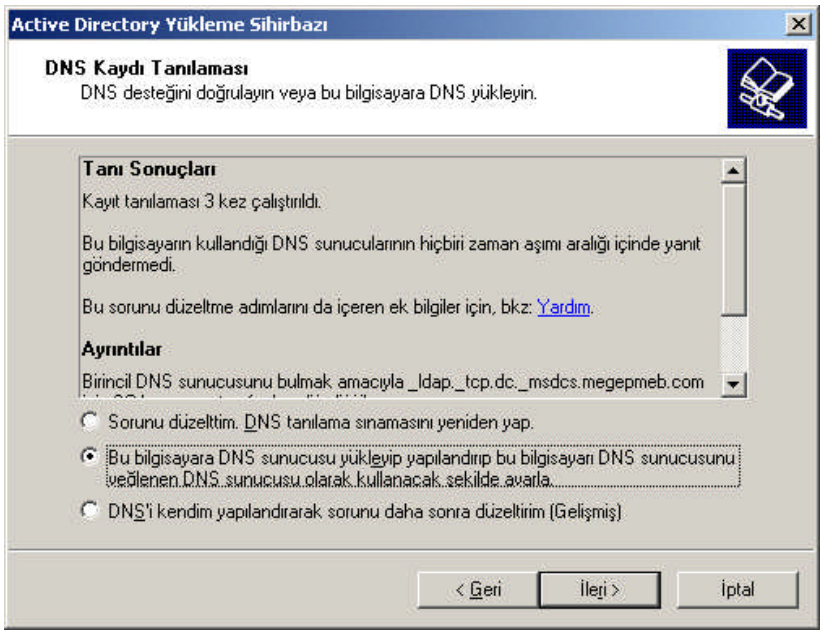


Resim 1.7: NetBIOS etki alan adının belirlenmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*



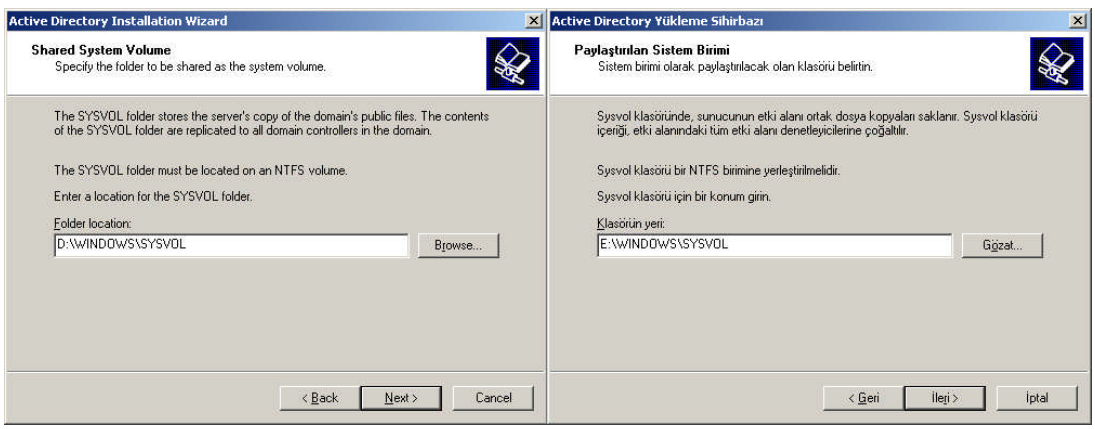
Resim 1.8: Veritabanı ve günlük klasörlerinin yerlerinin belirlenmesi
(Win 2003 Eng ⇔ Win 2003 Tr)

Active Directory ayarlarıyla ilgili veritabanı ve günlüklerin saklanması için sabit disk üzerinde klasör belirtilmesi gereklidir. **Resim 1.8'**de standart olarak Windows\NTDS klasörü altında bu dosyalar oluşturulacaktır, farklı bir yerde oluşturulması istenirse "Browse" (Gözat) butonuyla belirlenebilir.



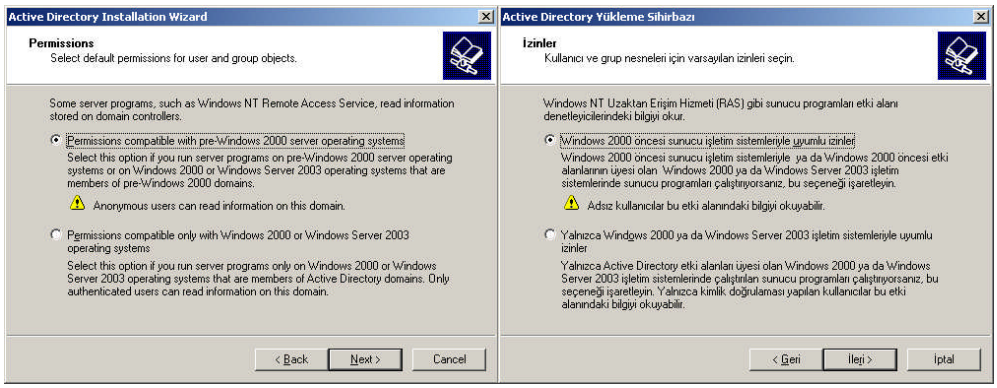
Resim 1.9: Windows 2003 Tr sürümü için DNS belirleme hatası

Veritabanı ve günlük klasörlerinin yerlerinin belirlenip "Next" (ileri) butonuna bastıktan sonra "Windows Server 2003 Türkçe" sürümünde **Resim 1.9'**daki DNS belirlemeyle ilgili bir hata gelecektir. Bu hata Türkçe sürümde **Resim 1.5'**deki pencere gelmediğinden oluşmaktadır. Bu bölümü Resim **1.9'**daki gibi ikince seçeneği seçerek belirlenip "Next" (ileri) butonuna bastıktan sonra **Resim 1.10'**daki pencere karşımıza gelir. "Windows Server 2003 İngilizce" sürümünde **Resim 1.9'**daki pencere gelmemekte, **Resim 1.10'**daki pencereye geçilmektedir.



Resim 1.10: Paylaştırılan sistem birimi için klasörün konumunun belirlenmesi
(Win 2003 Eng ⇔ Win 2003 Tr)

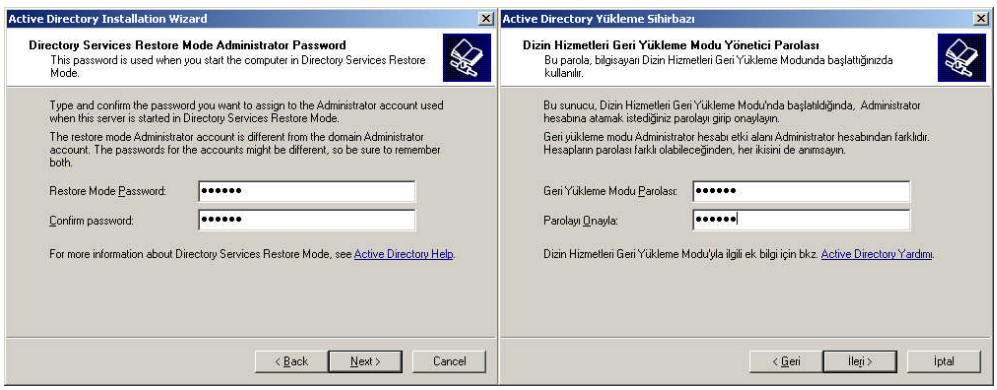
Resim 1.10'daki pencerede Etki alanının ortak dosyalarının saklanacağı klasörü belirlemekteyiz. Genelde bu klasörün yeri "**Windows\SYSVOL"**dür. Bu ayarlamadan sonraki aşama kullanıcı ve grup nesneleri için varsayılan izinlerin seçiminin yapıldığı **Resim 1.11'**deki penceredir.



Resim 1.11: Farklı işletim sistemlerine uyum sağlayacak izinlerin yüklenmesi ***(Win 2003 Eng ⇔ Win 2003 Tr)***

Varsayılan izinleri belirlerken etki alanımızda bulunan bilgisayarların üzerinde kurulu olan sunucu işletim sistemi sürümleri de önemlidir. **Resim 1.11'**de "Permissions compatible with pre-windows 2000 server operating systems" (Windows 2000 öncesi sunucu işletim sistemleriyle uyumlu izinler) seçeneği windows 2000'den önceki işletim sistemleri için geçerli izin seçeneğidir.

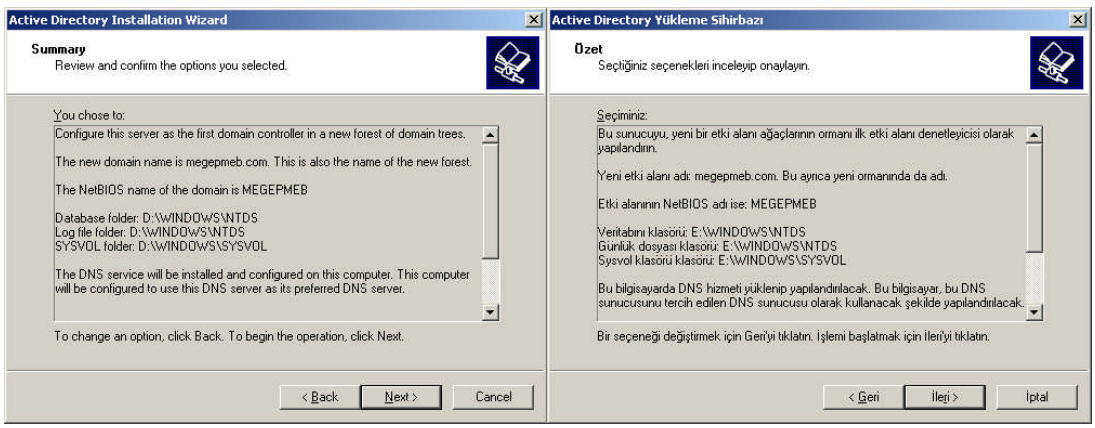
"Permissions compatible only with windows 2000 or windows 2003 operating systems" (Yalnızca Windows 2000 ya da Windows 2003 işletim sistemleriyle uyumlu izinler) seçenek ise windows 2000 ve sonraki sunucu işletim sistemleri için geliştirilen izin seçeneğidir. İlk seçeneği işaretlediğimizde sonradan ikinci seçeneğe geçmek kolaydır ama ikinci seçeneği seçtiğimizde artık windows 2000 öncesi sistemler için geri döndürülemez. **Resim 1.11'**de ilk seçeneği seçip "Next" (ileri) butonuna bastıktan sonra geri yükleme modu parolasının belirlendiği **Resim 1.12'**deki pencere karşımıza gelir.



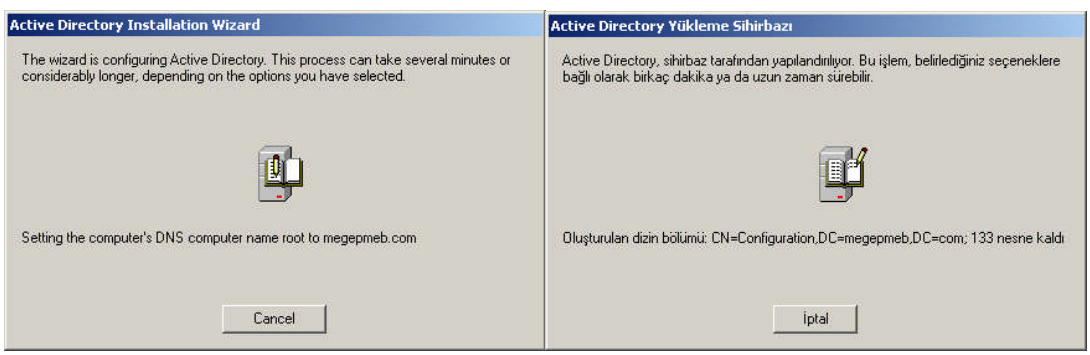
Resim 1.12: Geri yükleme modu parolasının belirlenmesi ***(W 2003 Eng ⇔ W 2003 Tr)***

Active Directory ile ilgili herhangi bir sorun oluştuğunda önceden alınmış Active Directory yedeklerini geri yüklemek için "Active Directory Restore Mode" (Active Directory Geri Yükleme Modu) çalıştırmamız gerekir. Bu çalıştırma işlemini sadece şifreyi bilen yöneticinin çalıştırabilmesi için bir Geri yükleme modu parolası belirlemek gerekir. İstersek parolada belirlemeden geçebiliriz. Parola işleminden sonraki aşama **Resim 1.13**'deki kurulum seçeneklerinin özetinin verildiği penceredir. Burada Active Directory kurulum başlangıcında yapılan ayarlamaların kısa bir özeti yer almaktadır. Bu aşamadan sonra verilen bilgiler doğrultusunda kurulum başlamış olur.

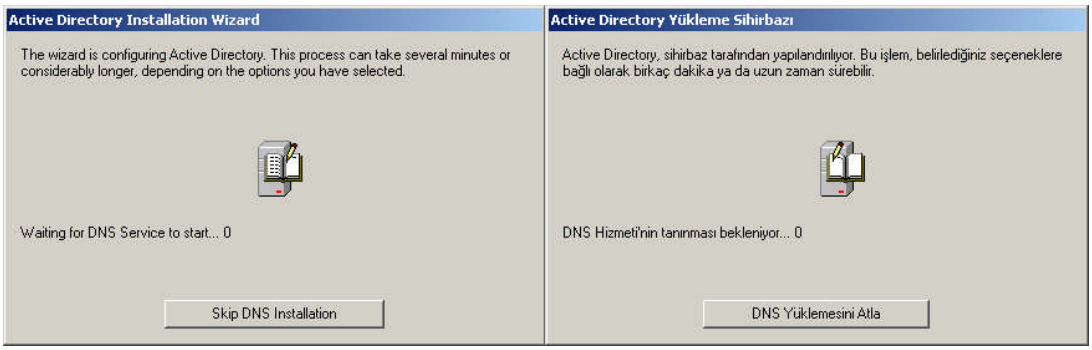
Active Directory, bir veritabanı yapısında olduğu için çalışır durumda iken yedekten geri yüklenemez. Windows sistem açılışında F8 tuşu ile gelen seçenek ile Active Directory Restore Mode ile sistem açılır. Active Directory kurulum esnasında verdiğimiz şifreyle Active Directory'i yedekten geri yükleyebiliriz.



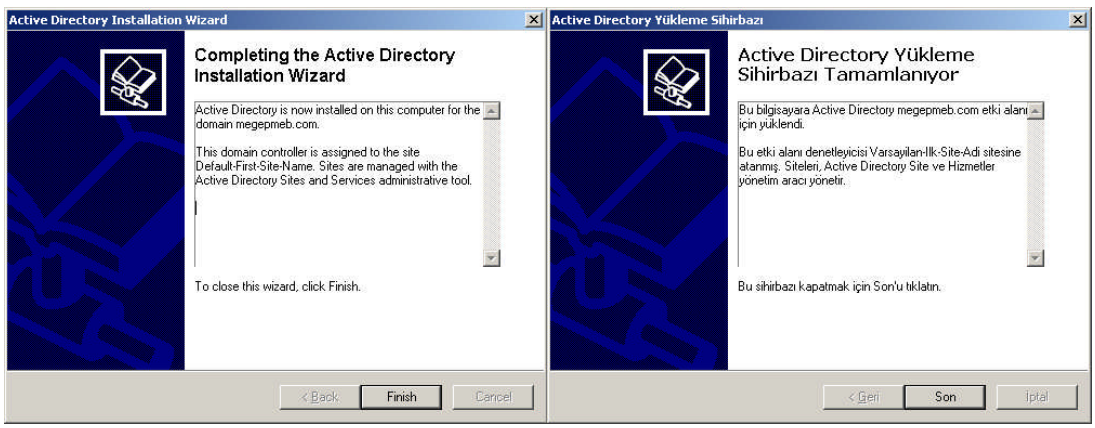
Resim 1.13: Kurulum seçeneklerinin özeti *(Win 2003 Eng ⇔ Win 2003 Tr)*



Resim 1.14: Active Directory yükleme işleminin başlatılması *(W2003 Eng ⇔ W2003 Tr)*

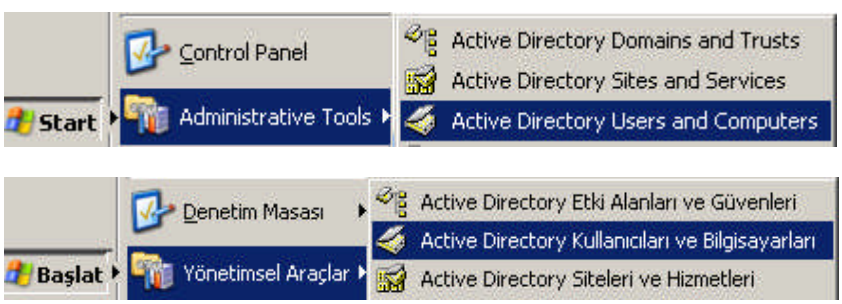


Resim 1.15: DNS yükleme işleminin başlatılması *(Win 2003 Eng ⇔ Win 2003 Tr)*



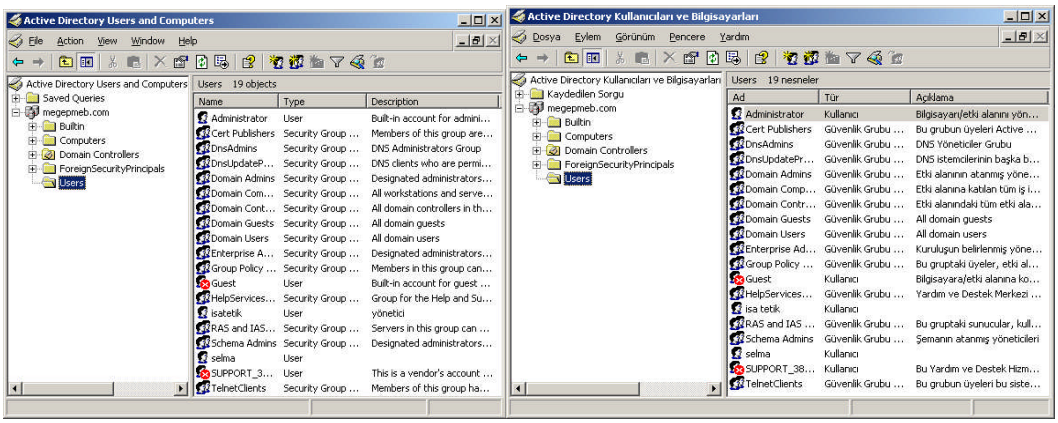
Resim 1.16: Active Directory kurulumunun tamamlanması *(W 2003 Eng ⇔ W 2003 Tr)*

Resim 1.14 ve Resim 1.15'de görüldüğü gibi Active Directory kurulumu başlar, kurulum tamamlandıktan sonra **Resim 1.16'**daki pencere karşımıza gelir. Kurulum tamamlanmış olur. Bundan sonra bilgisayarın yeniden başlatılması istenecektir. Bilgisayar yeniden başlatıldıktan sonra Active Directory kullanıma hazırdır ve tüm kullanıcı gruplar ile ilgili ayarlamalar buradan yapılacaktır.



Resim 1.17: Active Directory'nin başlatılması *(W 2003 Eng ⇔ W 2003 Tr)*

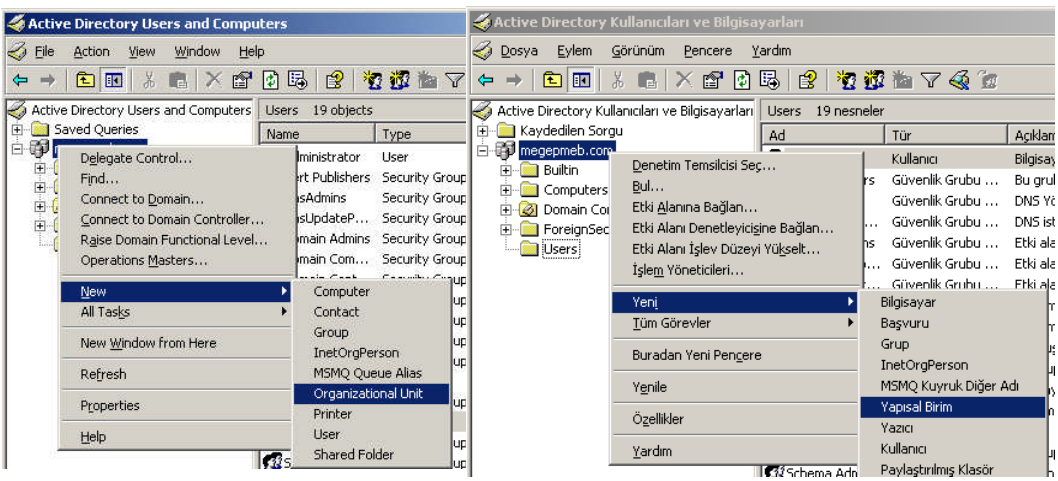
Active Directory kurulumu tamamlanıp bilgisayar yeniden başlatıldıktan sonra Active Directoryi çalıştırmak için **"Start => Administartive Tools => Active Directory Users and Computers"** (Başlat => Yönetimsel Araçlar => Active Directory kullanıcı ve bilgisayarları) seçeneğine tıklamamız gerekir.



Resim 1.18: Active Directory kullanıcı ve bilgisayarlar penceresi
(Win 2003 Eng ⇔ Win 2003 Tr)

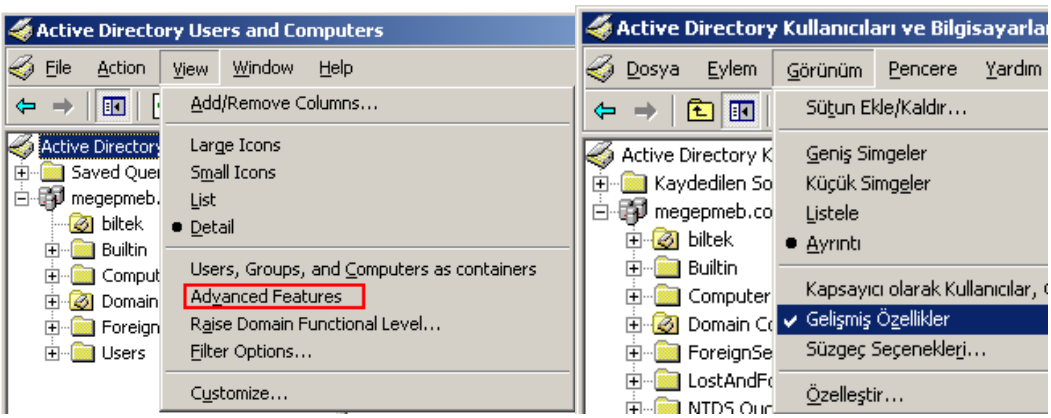
1.2.2. Active Directory Nesnelerine Verilecek İzinler

Active Directory nesnelerine ağ kaynaklarını verimli ve düzenli kullanabilmeleri için çeşitli izinler belirlenmiştir. **Resim 1.19'**da yeni oluşturulabilecek Active Directory Nesneleri görülmektedir. Her nesnenin bilgisayar kaynaklarına erişim yapabileceği izinler bulunduğu gibi diğer nesnelerin izinlerini düzenlemek veya denetlemek gibi özel yetkileri de bulunmaktadır. Belirlenecek izinler, Active Directory nesnesi üzerinde yapılacak özel bir işlem içindir; bu işlem, söz konusu nesnedeki belirli bir öz niteliği okuma veya yazma erişimiyle ilgili olabilir.

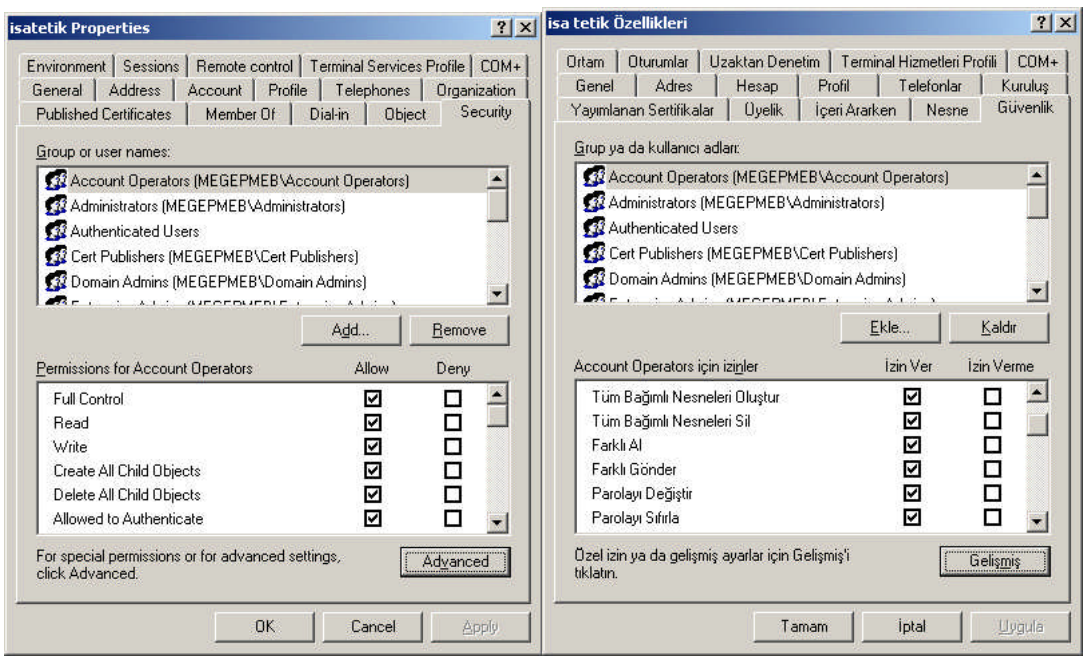


Resim 1.19: Active Directory nesneleri ***(Win 2003 Eng ⇔ Win 2003 Tr)***

Active Directory nesneleriyle ilgili izinleri ayarlamadan önce "Start => **Administartive Tools => Active Directory Users and Computers"** (Başlat => Yönetimsel Araçlar => Active Directory kullanıcı ve bilgisayarları) açıp "View" (Görünüm) menüsünden "Advanced Features" (Gelişmiş Özellikler) seçeneğini tıklamamız gerekmektedir. Bu şekilde Active Directory nesnelerinin izinlerine erişebiliriz.



Resim 1.20: Active Directory gelişmiş özelliklerin başlatılması
(Win 2003 Eng ⇔ Win 2003 Tr)



Resim 1.21: Active Directory penceresinden seçilen bir kullanıcının özellikleri
(Win 2003 Eng ⇔ Win 2003 Tr)

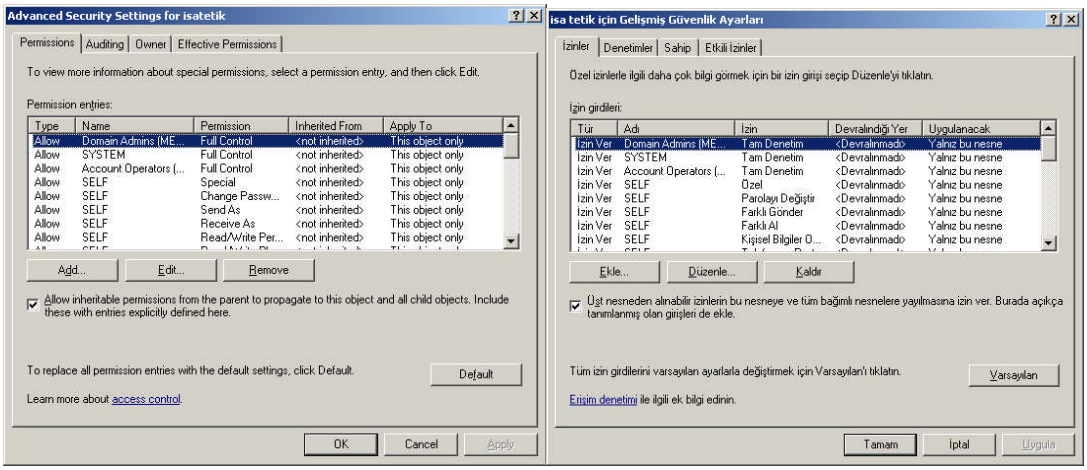
Active Directory penceresinden herhangi bir nesneye (örneğin Resim 1.18'deki pencereden "isatetik" ismindeki kullanıcıya) sağ tıklayıp "Properties" (Özellikler) dediğimizde **Resim 1.21**'deki kullanıcı özellikleri penceresi açılır. Burada izinlerle ilgili olan sekme "Security" (Güvenlik) sekmesidir. Active Directory altındaki her nesnenin özellikler penceresinde "Security" (Güvenlik) sekmesi bulunur. **Resim 1.21'**deki pencerenin üst kısmından izinlerini görüntülemek istediğimiz nesneyi seçtiğimizde alt kısımda o nesneye ait izinler görüntülenir.

Kullanıcı için standart izinler aşağıdaki gibidir:

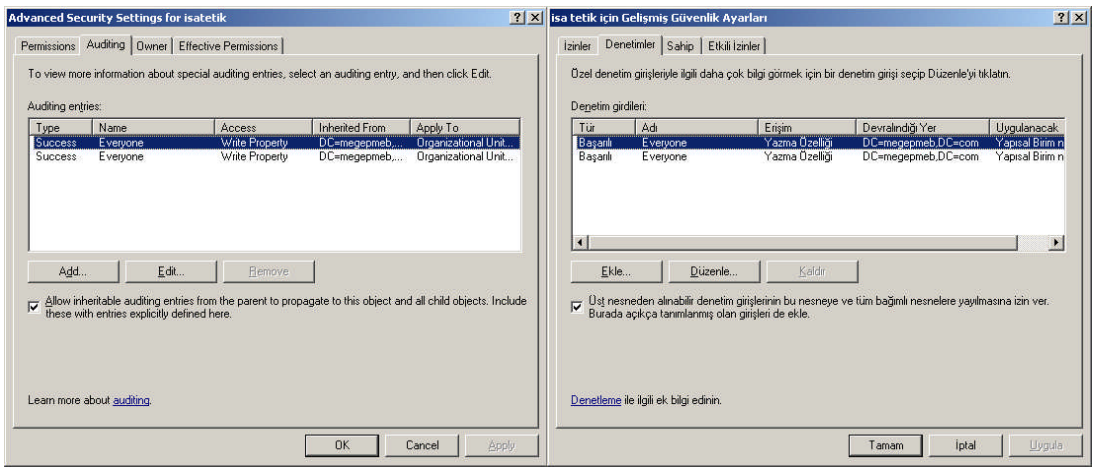
- Full Control (Tam Denetim)
- Read (Oku)
- Write (Yaz)
- Create All Child Object (Tüm Bağımlı Nesneleri Oluştur)
- Delete All Child Object (Tüm Bağımlı Nesneleri Sil)
- Receive As (Farklı Al)
- Send As (Farklı Gönder)
- Change Password (Parolayı Değiştir)
- Reset Password (Parolayı Sıfırla)
- Allowed to Authenticate (Kimlik doğrulamasına izin ver)
- Read General Information (Genel bilgi oku)
- Write General Information (Genel bilgi yaz)
- Read Public Information (Genel bilgiler oku)
- Write Public Information (Genel bilgiler yaz)
- Read Group Membership (Grup üyeliği oku)
- Write Group Membership (Grup üyeliği yaz)
- Read Accont Restrictions (Hesap kısıtlamaları oku)
- Write Accont Restrictions (Hesap kısıtlamaları yaz)
- Read Personal Information (Kişisel bilgiler oku)
- Write Personal Information (Kişisel bilgiler yaz)
- Read Logon Information (Oturum açma bilgileri oku)
- Write Logon Information (Oturum açma bilgileri yaz)
- Read Phone and Mail Options (Telefon ve posta seçenekleri oku)
- Write Phone and Mail Options (Telefon ve posta seçenekleri yaz)
- Read Remote Access Information (Uzak erişim bilgileri oku)
- Write Read Remote Access Information (Uzak erişim bilgileri yaz)
- Read Web information (Web bilgileri oku)
- Write Web information (Web bilgileri yaz)
- Special Permissions (Özel izinler)

Bu izinleri nesneye vermek istediğimizde "Allow", vermek istemediğimizde ise "Deny" (İzin verme) seçeneğini işaretleriz. İzinler her nesne için değişmektedir. İzinlerle ilgili daha ayrıntılı bir ayarlama istenirse **Resim 1.21'**deki pencerenin "Advanced" (Gelişmiş) seçeneğini tıklayarak **Resim 1.22**'deki gelişmiş güvenlik ayarları penceresini açmamız gerekir. **Resim 1.22**'de (İzinler) sekmesi nesnelerin izinleriyle ilgili durumlarını görüntüler. **Resim 1.23'**deki "Auditing" (Denetimler) sekmesi nesnelerin üzerinde denetim sahibi olanları görüntüler. **Resim 1.24'**deki "Owner" (Sahip) sekmesi belirtilen nesnelerin

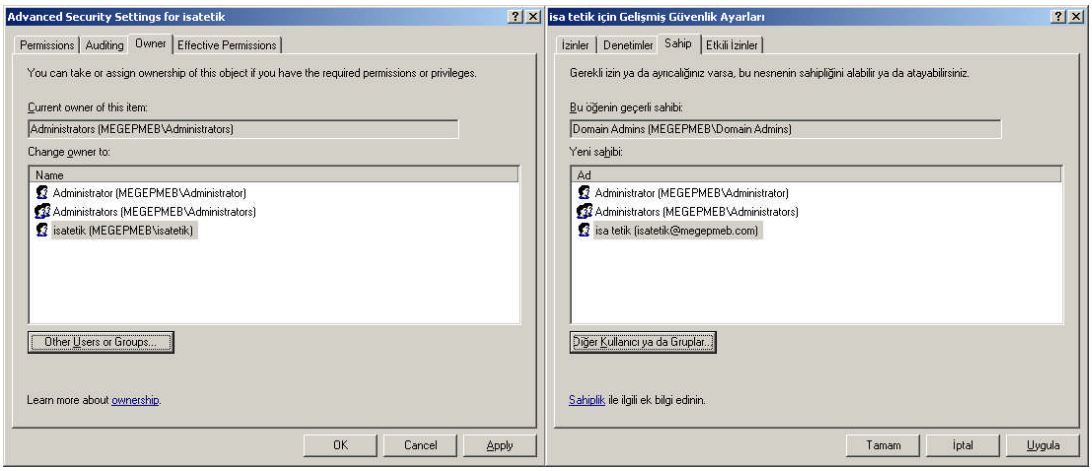
sahipliğini görüntüler. **Resim 1.24**'deki "Effective Permission" (Etkili İzinler) sekmesi ise daha ayrıntılı ve farklı izinler atamak için kullanılır.



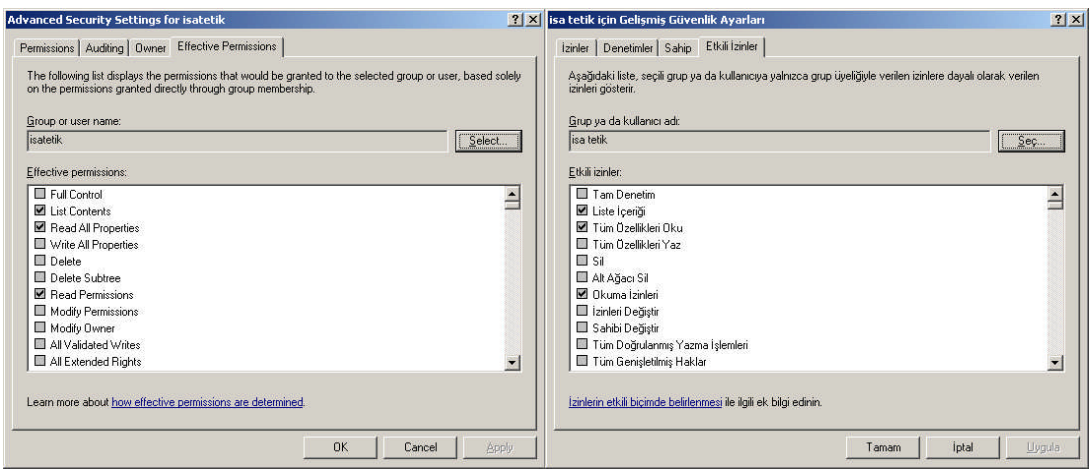
Resim 1.22: Gelişmiş güvenlik ayarları; izinler sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*



Resim 1.23: Denetimler sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*



Resim 1.24: Nesne sahipliği sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*

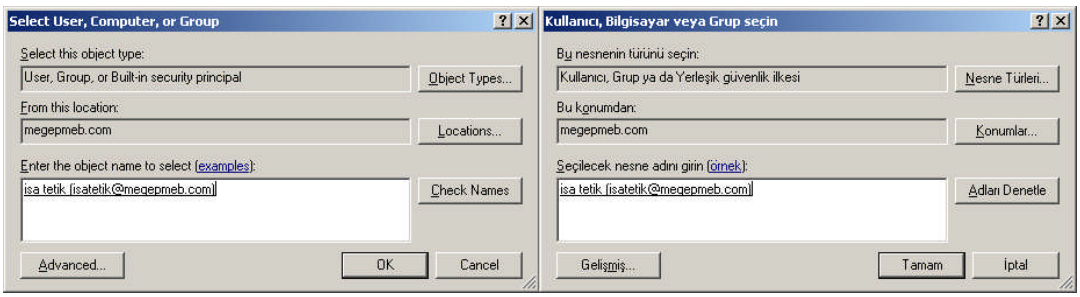


Resim 1.25: Etkili izinler sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*

Tam Denetim	Görünen Ad Oku
Liste İçeriği	Görünen Ad Yaz
Tüm Özellikleri Oku	İkinci Ad Oku
Tüm Özellikleri Yaz	İkinci Ad Yaz
Sil	İlk Ad Oku
Alt Ağacı Sil	İlk Ad Yaz
Okuma izinleri	IP Telefon Numarası Oku
İzinleri Değiştir	IP Telefon Numarası Yaz
Sahibi Değiştir	İş Ünvanı Oku
Tüm Doğrulanmış Yazma İşlemleri	İş Ünvanı Yaz
Tüm Genişletilmiş Haklar	Name Oku
Tüm Bağımlı Nesneleri Oluştur	Name Yaz
Tüm Bağımlı Nesneleri Sil	Notlar Oku
Farklı Al	Notlar Yaz
Farklı Gönder	Oturum Açma Adi Oku
Parolayı Değiştir	Oturum Açma Adi Yaz
Parolayı Sıfırla	Oturum Açma İş İstasyonları Oku
Kimlik Doğrulamasına İzin Verilen	Oturum Açma İş İstasyonları Yaz
Genel Bilgi Oku	Posta Kodu Oku
Genel Bilgi Yaz	Posta Kodu Yaz
Genel Bilgiler Oku	Posta Kutusu Oku
Genel Bilgiler Yaz	Posta Kutusu Yaz
Grup Üyeliği Oku	Sokak Adresi Oku
Grup Üyeliği Yaz	Sokak Adresi Yaz
Hesap Kısıtlamaları Oku	Şirket Oku
Hesap Kısıtlamaları Yaz	Şirket Yaz
Kişisel Bilgiler Oku	Tanım Oku
Kişisel Bilgiler Yaz	Tanım Yaz
Oturum Açma Bilgileri Oku	Telefon Numarası Oku
Oturum Açma Bilgileri Yaz	Telefon Numarası Yaz
Telefon ve Posta Seçenekleri Oku	Uluslararası ISDN Numarası Oku
Telefon ve Posta Seçenekleri Yaz	Uluslararası ISDN Numarası Yaz
Uzak Erişim Bilgileri Oku	Unvan Oku
Uzak Erişim Bilgileri Yaz	Unvan Yaz
Web Bilgileri Oku	Üyesi olunan gruplar Oku
Web Bilgileri Yaz	Üyesi olunan gruplar Yaz
Açıklama Oku	Web Sayfası Adresi Oku
Açıklama Yaz	Web Sayfası Adresi Yaz
Adı Oku	Yardımcı Oku
Adı Yaz	Yardımcı Yaz
Ev Telefonu Oku	Yönetici Oku
Ev Telefonu Yaz	Yönetici Yaz
Faks Numarası Oku	
Faks Numarası Yaz	

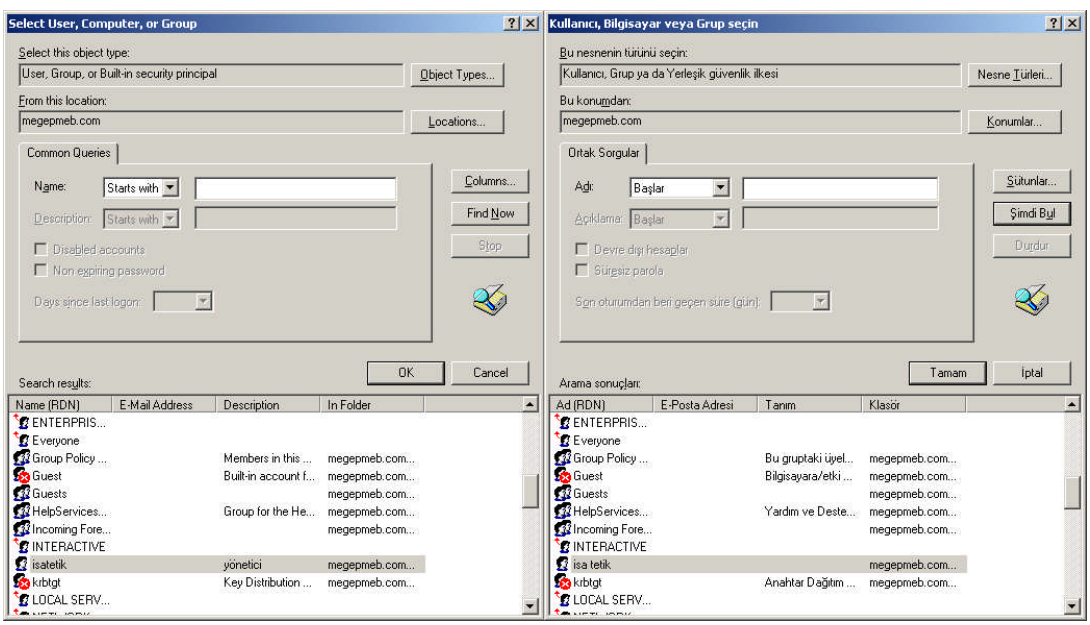
Tablo 1.1: Etkili izinler sekmesinde bulunan farklı izinlerin listesi

Bir kullanıcı, bilgisayar, grup veya diğer bir nesnenin sahip olduğu bütün izinleri görüntülemek için **Resim 1.2.25'**deki Etkili izinler sekmesinden "Select" (Seç) butonunu tıklayarak **Resim 1.2.26'**daki pencereyi açmamız gerekir.



Resim 1.2.26: Etkili izinleri görüntülenecek kullanıcı seçimi
(Win 2003 Eng ⇔ Win 2003 Tr)

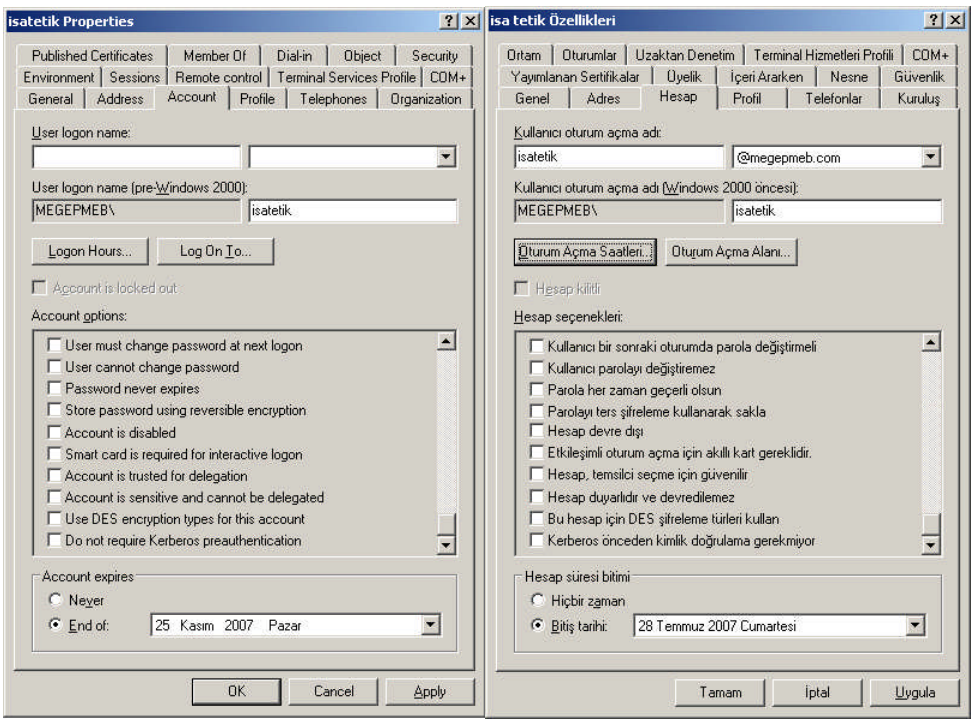
Etkili izinleri görüntülenecek kullanıcı seçimini gerçekleştirmemizi sağlayan **Resim 1.26'**daki pencereden "Check Names" (Adları Denetle) butonunu tıklayarak **Resim 1.27'**deki pencereyi açmamız gerekir. **Resim 1.27'**deki pencereden "Find Now" (Şimdi Bul) butonunu tıkladığımızda Active Directory içerisindeki nesne isimlerini bulur. **Resim 1.2.27'**deki listeden bir nesne ismi seçerek "OK" (Tamam) butonuna bastığımızda **Resim 1.2.24'**te olduğu gibi seçilen nesnenin (kullanıcı, bilgisayar, grup veya diğer bir nesne) izinlerini görüntülemiş oluruz. Active Directory içerisindeki nesnelerle ilgili etkili izinlerin bir kısmı **Tablo 1.1'**de verilmiştir. **Resim 1.2.24'**te görüntülenen izinler sadece bilgi amaçlıdır. Değiştirilme imkânı yoktur.



Resim 1.27: Etkili izinleri görüntülenecek kullanıcı listesi
(Win 2003 Eng ⇔ Win 2003 Tr)

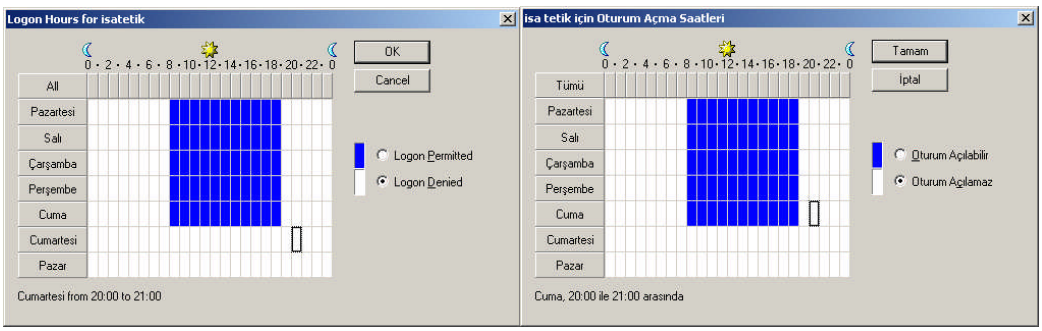
Active Directory içerisindeki bir kullanıcının izinlerini belirlemenin yanında kullanıcı hesabıyla ilgili ayarlamaları da vardır. **"Start => Administartive Tools => Active Directory Users and Computers"** (Başlat => Yönetimsel Araçlar => Active Directory kullanıcı ve bilgisayarları) açıp kullanıcı hesabıyla ilgili ayarlamalar yapacağımız kişiyi seçerek sağ tıklayıp "Properties" (Özellikler) dediğimizde **Resim 1.28'**deki kullanıcı özellikleri penceresini açalım. **Resim 1.28'**deki hesap seçenekleri aşağıdaki gibidir:

- User must Change password at next logon (Kullanıcı bir sonraki oturumda parola değiştirmeli)
- User cannot Change password (Kullanıcı parolayı değiştiremez)
- Password never expires (Parola her zaman geçerli olsun)
- Store password using resersible encryption (Parolayı ters şifreleme kullanarak sakla)
- Account is disabled (Hesap devre dışı)
- Smart card is required for interactive logon (Etkileşimli oturum açma için akıllı kart gereklidir)
- Account is trusted for delegation (Hesap, temsilci seçme için güvenilir)
- Account is sensitive and cannot be delegated (Hesap duyarlıdır ve devredilemez)
- Use DES encryption types for this account (Bu hesap için DES şifreleme türleri kullan)
- Do not require Kerberos preauthentication (Kerberos önceden kimlik doğrulama gerekmiyor)

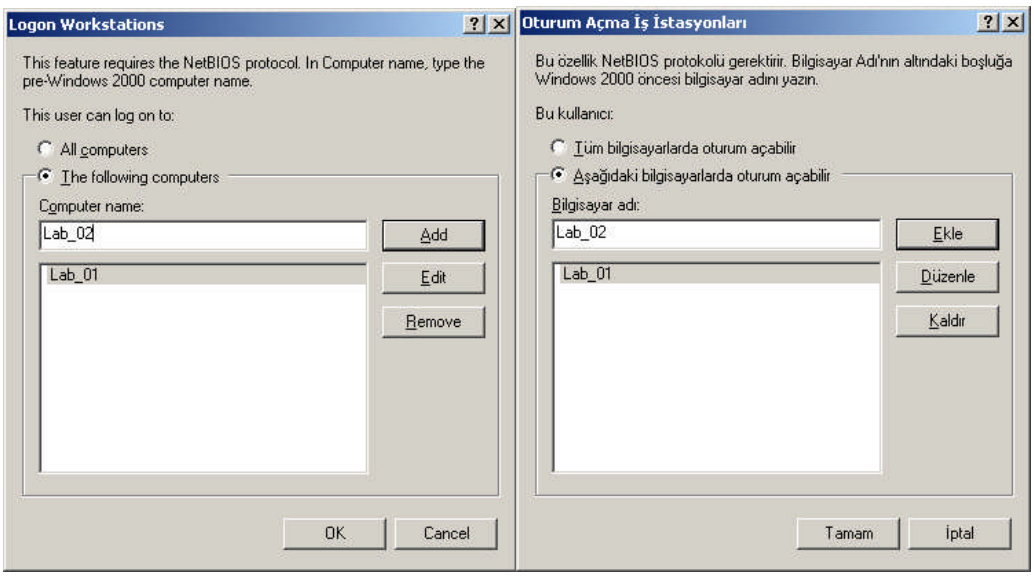


Resim 1.28: Kullanıcı hesabı ayarları *(Win 2003 Eng ⇔ Win 2003 Tr)*

Kullanıcı hesaplarıyla ilgili diğer izinlerde “Logon Hours” (Oturum açma saatleri)’tur. **Resim 1.29’**da kullanıcının hangi gün ve saatlerde sisteme giriş yapacağı düzenlenebilmektedir. Ayrıca **Resim 1.28’**de “Log on to” (Oturum açma alanı) butonu tıklandığında **Resim 1.29**’deki kullanıcının hangi bilgisayarlarda oturum açabileceğini belirleyen pencere açılır. **Resim 1.28’**de “Account expires” (Hesap bitim süresi) bölümü ise kullanıcı hesabının geçerlilik süresini belirlemek için kullanılır.



Resim 1.29: Kullanıcı hesabı oturum açma saatleri *(Win 2003 Eng ⇔ Win 2003 Tr)*

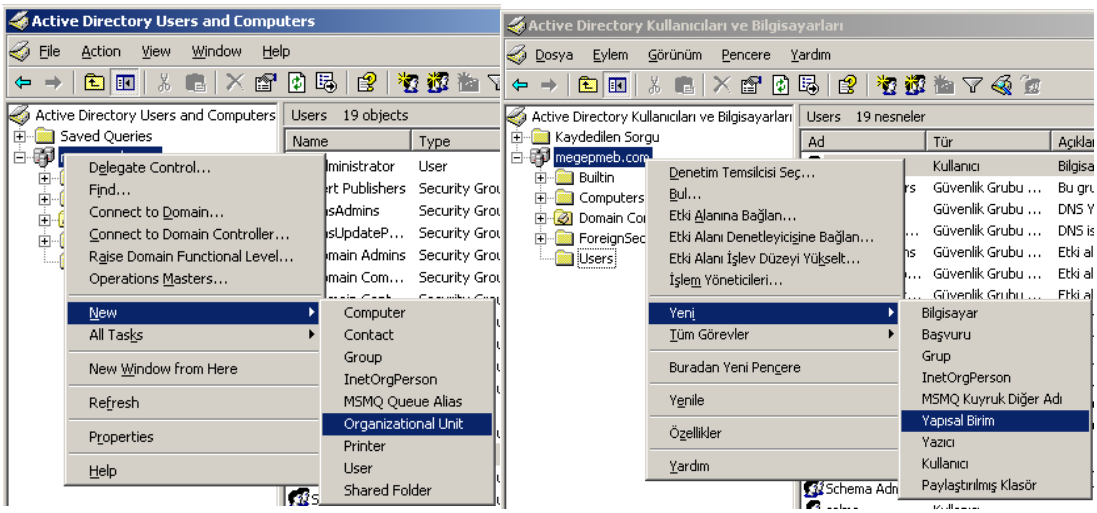


Resim 1.30: Kullanıcı hesabı oturum açma alanı *(Win 2003 Eng ⇔ Win 2003 Tr)*

1.3. Organizasyon Birim Yetkilendirmesi

Belirli Active Directory nesnelerinin, oluşturulacak organizasyon birimi yönetimine verilmesi ve bu organizasyon biriminin başına bir yönetici yetkilendirilmesi, yönetimin paylaştırılması ve denetimin kolaylaştırılması açısından yararlı olacaktır. Bu gibi işlemlerde önce bir organizasyon birimi oluşturmak, sonra organizasyon biriminin kontrol edeceği

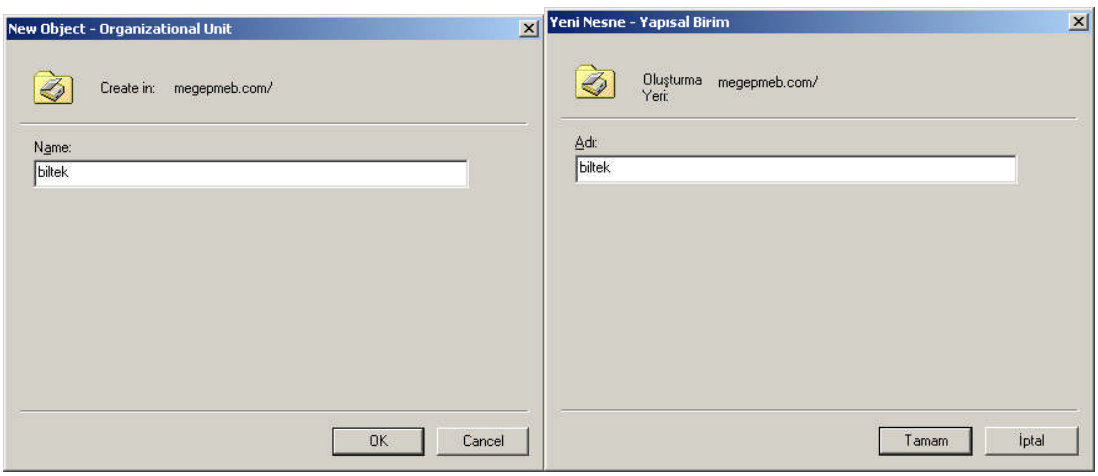
nesneleri belirlemek, en son olarak da organizasyonun biriminin başına yönetici veya değişik yetkilere sahip yöneticiler tayin etmek gerekir.



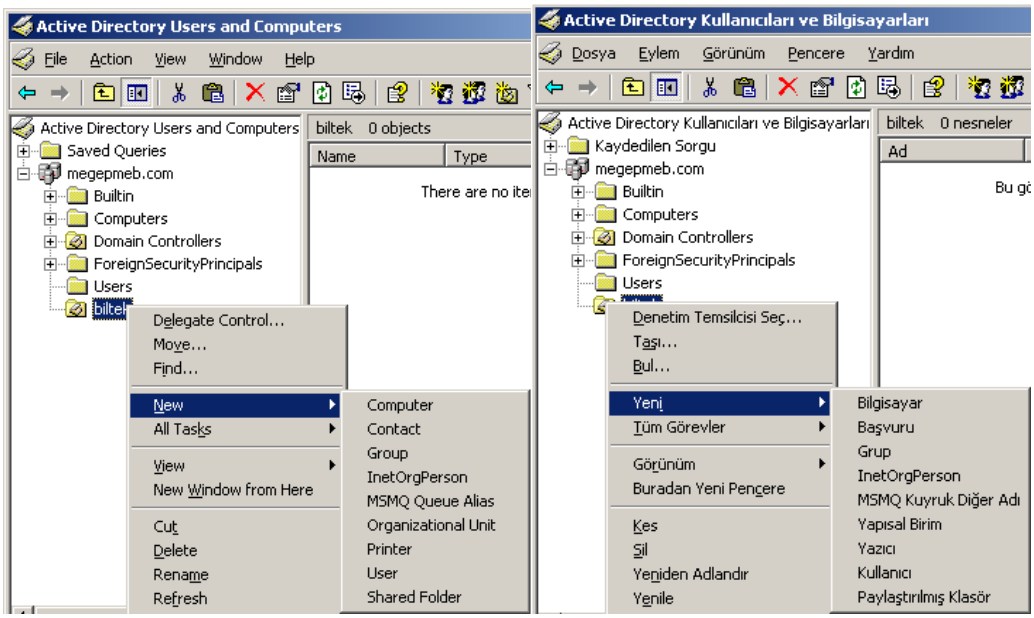
Resim 1.31: Organizasyon biriminin oluşturulması *(Win 2003 Eng ⇔ Win 2003 Tr)*

Bu bölümde, organizasyon birimin nasıl oluşturulacağı ve içerisine nasıl nesne ekleneceği anlatılacaktır. Organizasyon biriminin başına bir yönetici yetkilendirme ve yetkilerin belirlenmesi işlemi bir sonraki modülde ayrıntılı olarak incelenecektir.

Organizasyon birimi oluşturmak için **Resim 1.31'**de olduğu gibi etki alanına sağ tıklatıp "Organizational Unit" (Yapısal birim) seçeneğini seçip açarız. **Resim 1.31'**deki pencereye oluşturulacak organizasyon birimimin ismini yazıp "OK" (Tamam) butonuna bastığımızda organizasyon birimi kurulmuş olur.



Resim 1.32: Oluşturulması organizasyon birimine isim verilmesi
(Win 2003 Eng ⇔ Win 2003 Tr)



Resim 1.33: Oluşturulmuş organizasyon birimi içinde yeni nesne oluşturulması
(Win 2003 Eng ⇔ Win 2003 Tr)

Resim 1.33'te olduğu gibi oluşturulmuş organizasyon birimine sağ tıkladığımızda istersek organizasyon birimi içerisine yeni bilgisayar, grup, kullanıcı gibi Active Directory nesneleri oluşturabiliriz. İstersek mevcut Active Directory nesnelerini, oluşturduğumuz organizasyon birimi içerisine sürükle-bırak yöntemiyle organizasyon birimi yönetimine bırakılabiliriz.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ **"TeknikBilgisayar.com"** isminde yeni bir etki alanı oluşturunuz, altına **"Teknik"** ve **"Muhasebe"** isminde organizasyon birimi oluşturunuz.	➢ Etki alanı ve organizasyon birimi isimlerine dikkat ediniz.
➢ Oluşturacağımız **"Muhasebe"** isimli organizasyon birimi içerisine **"Ahmet"** isimli kullanıcı oluşturup kullanıcıya sadece "Full Control", Read, Write izinlerini veriniz	➢ Organizasyon birimi ve kullanıcı isimlerine, kullanıcıya verilecek izinlerin neler olduğuna dikkat ediniz.
➢ Oluşturacağımız **"Teknik"** isimli organizasyon birimi içerisine "Hasan" isimli kullanıcı oluşturup kullanıcının oturum açma saatlerini hafta içi **9.00-18.00** arası, hesap süresi bitimini **28.10.2009** olacak şekilde ve sadece **M_01** bilgisayarında oturum açabilecek şekilde ayarlayınız.	➢ Organizasyon birimi ve kullanıcı isimlerine, kullanıcıya verilecek izinlerin neler olduğuna dikkat ediniz.
➢ Öncelikle **"Muhasebe"** isimli organizasyon birimini **"Teknik"** isimli organizasyon birimi içerisine taşıyınız	➢ Organizasyon birimi ve kullanıcı isimlerine dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruların doğru seçeneklerini işaretleyiniz.

1. Active Directory nesneleri hakkında verilerin tutulduğu, değişikliklerin otomatik olarak güncellendiği yapı aşağıdakilerden hangisidir?
A) Aktif Rehber Birimi **B)** Organizasyon Birimi
C) Etki Alanı **D)** Aktif Rehber Şemaları **E)** Domain Controller

2. "Sirketim.com" isimli etki alanında bulunan **"Pazarlama"** Organizasyon birimi içerisindeki **"Lab_01"** isimli bilgisayarın tanımlama bilgisi aşağıdakilerden hangisidir?
A) DC="Lab_01" **OU**="Pazarlama" **CN**="sirketim.com"
B) CN="Lab_01" **DC**="Pazarlama" **OU**="sirketim.com"
C) CN="Lab_01" **OU**="Pazarlama" **DC**="sirketim" **DC**="com"
D) OU="Lab_01" **CN**="Pazarlama" **DC**="sirketim.com
E) DC="Lab_01" **OU**="Pazarlama" **CN**="sirketim" **CN**="com"

3. Active Directory kurulumunu gerçekleştiren komut aşağıdakilerden hangisidir?
A) dcpromo **B)** adirectory
C) ADsetup **D)** ARsetup **E)** directorysetup

4. Aşağıdakilerden hangisi Etki alanı altında oluşturulabilecek yeni Active Directory nesnelerinden değildir?
A) Yazıcı **B)** Bilgisayar
C) Grup **D)** Kullanıcı **E)** Farklı bir etki alanı

5. Aşağıdakilerden hangisi kullanıcı hesabı yetkilerinin belirlendiği özellikler sekmesidir?
A) General **B)** Security
C) Sessions **D)** Account **E)** Profile

6. Aşağıdakilerden hangisi kullanıcı hesabı yetkilerinden olamaz?
A) Full control **B)** Send As
C) Change Password **D)** Account read **E)** Write

7. Aşağıdakilerden hangisi kullanıcı parolasını sıfırlayan standart izinlerdendir?
A) Reset Password **B)** Delete Password
C) Change Password **D)** Read Password **E)** Write Password

8. Aşağıdakilerden hangisi kullanıcı hesabının, oturum açma saatlerinin, oturum açma alanının ve hesap süresi bitiminin belirlendiği özellikler sekmesidir?

A) Permissions **B)** Security
C) Sessions **D)** Profile **E)** Account

9- Aşağıdakilerden hangisi kullanıcı hesabını devre dışı bırakan hesap seçeneklerinden biridir?

A) Account is sensitive **B)** Account is trusted
C) Account is deleted **D)** Account is disabled **E)** Account is resersible

10- Aşağıdakilerden hangisi organizasyon birimi içerisine taşınabilecek bir Active Directory nesnesi değildir?

A) Printer **B)** User
C) Delegation **D)** Group **E)** Computer

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları, faaliyete geri dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-2

AMAÇ

Grup Politikası İşlemini gerçekleştirebileceksiniz.

ARAŞTIRMA

- Grup Politikalarının ne anlama geldiğini ve nasıl uygulandığını araştırınız.
- Grup Politikalarının Etki alanlarına nasıl uygulandığını araştırınız.
- Grup Politikalarının Organizasyon birimlerine nasıl uygulandığını araştırınız.

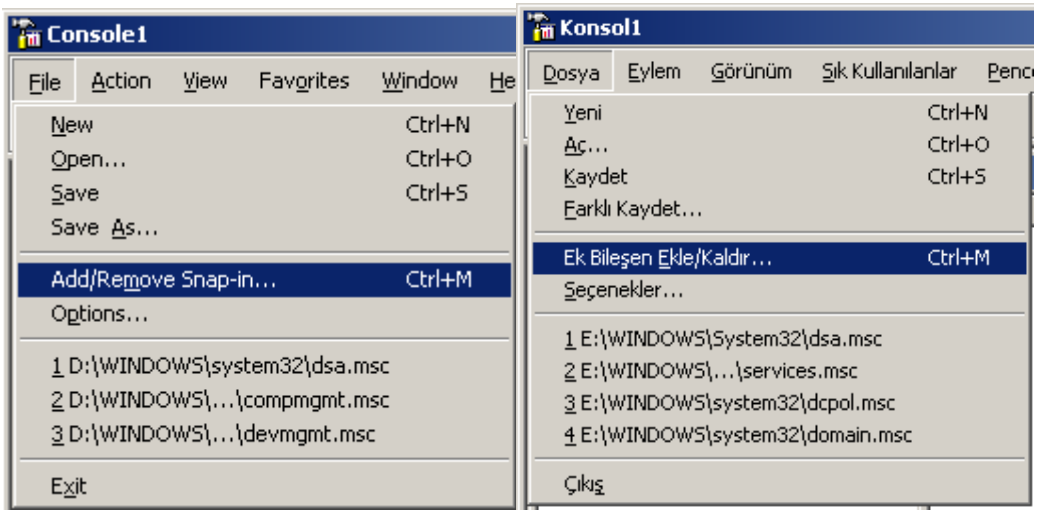
2. GRUP POLİTİKASI İŞLEMİNİ GERÇEKLEŞTİRME

2.1. GPO'ların Uygulaması

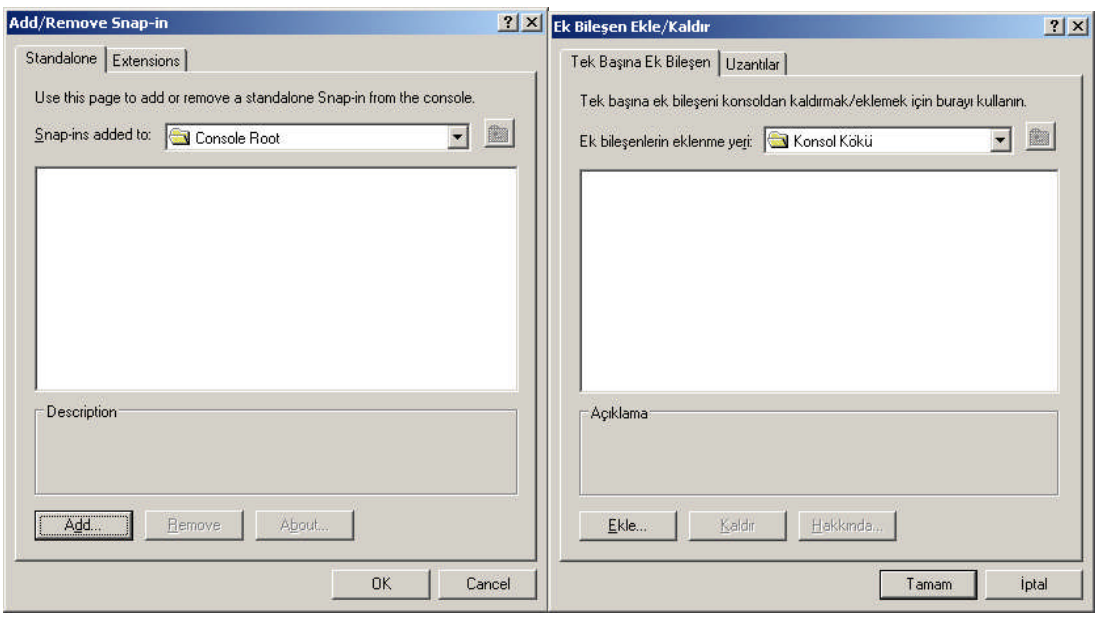
Grup politikaları Active Directory içerisindeki kullanıcı ve bilgisayarları merkezî bir yönetim sağlayarak program kulumu ve ayarlarını otomatikleştiren bir yönetim biçimidir. Grup politikalarını kullanabileceğimiz bilgisayarlar da kurulu işletim sistemi windows 2000 üzeri olması gerekir. Grup politikalarının bize sağlayacağı yararları aşağıdaki gibi sıralayabiliriz:

- Kullanıcı hesaplarıyla ilgili denetim ve güvenlik ayarlarını yapılandırır.
- Kullanıcıların ihtiyaç duyacağı gerekli program ve ayarlamaların merkezî olarak yapılandırılmasına yardımcı olur.
- Kullanıcıların başlat menüsü ve masaüstü seçeneklerini yapılandırır.
- Bilgisayar yazılımlarının gerekli güncelleştirmelerini ve kurulumlarını otomatik olarak gerçekleştirir.
- Organizasyon birimlerindeki gerekli yönetim ve güvenlik ayarlarını yapılandırır.

Güncel sunucu işletim sistemlerinde yerel bir grup politikası bulunmaktadır. Yerel bilgisayardaki bu grup politikalarını yönetmek için öncelikle yüklemek gereklidir. Grup politikasını yüklemek için **"Start => Run"** (Başlat => Çalıştır) bölümüne **"MMC"** yazılıp "OK" (Tamam) butonuna tıkladığımızda **Resim 2.1'**deki "Microsoft Management Consol" (Microsoft Yönetim Konsolu) karşımıza gelir. Yönetim Konsolundaki **"File=>Add/Remove Snap-in"** (Dosya=>Ek Bileşen Ekle/Kaldır) seçeneğiyle **Resim 2.2'**deki Bileşen Ekle/Kaldır pencere karşımıza gelir.



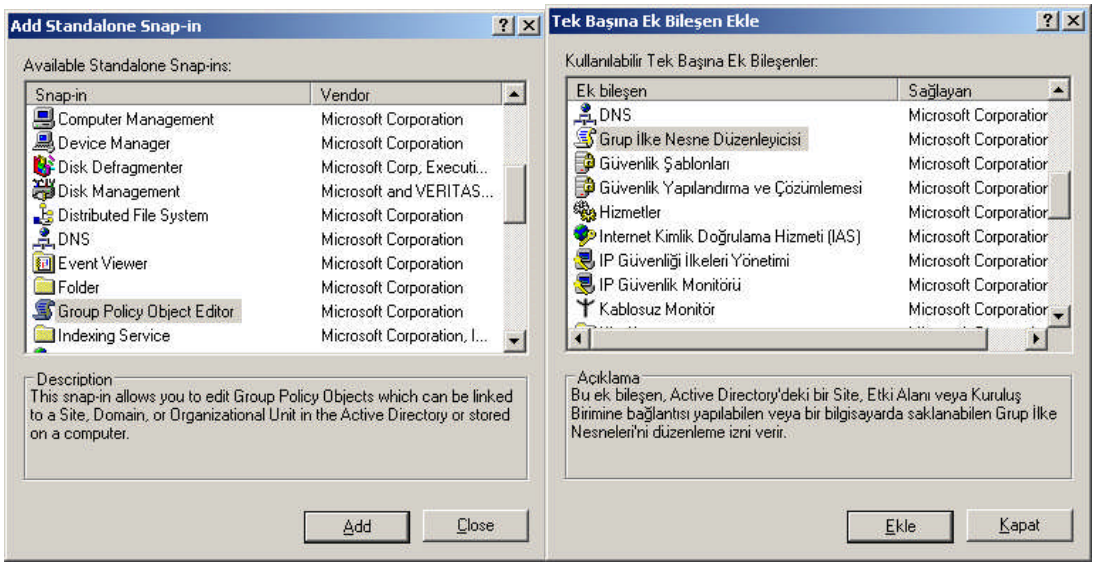
Resim 2.1: Microsoft Yönetim Konsolu ***(Win 2003 Eng ⇔ Win 2003 Tr)***



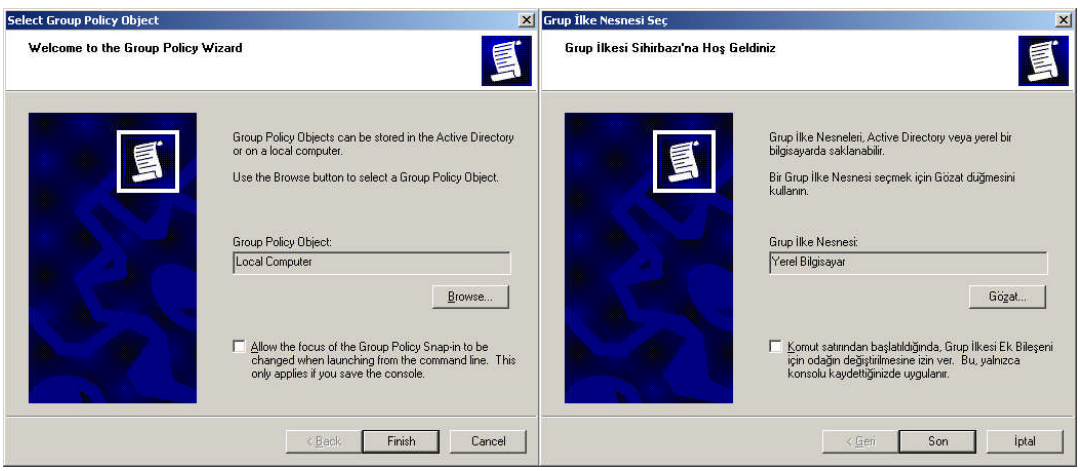
Resim 2.2: Bileşen Ekle/Kaldır Penceresi ***(Win 2003 Eng ⇔ Win 2003 Tr)***

Resim 2.2'deki Ek bileşen Ekle/Kaldır Pencerede **"Add"** (Ekle) butonuna tıklandığımızda yüklenecek standart bileşenlerin bulunduğu **Resim 2.3'**teki pencere karşımıza gelir. Ek bileşen Ekle/Kaldır Penceresinden "Group Policy Object Editör" (Grup İlke Nesne Düzenleyicisi) bileşenini seçip **"Add"** (Ekle) butonuna tıkladığımızda **Resim 2.4'**teki grup politikası kurulacak bilgisayarın seçildiği grup ilkesi sihirbazı açılır. Aksi belirtilmediği sürece grup politikasını yerel bilgisayara kurar. İstenirse grup politikası etki alanı içerisindeki farklı bir bilgisayara da kurulabilir. Grup politikası kurulacak

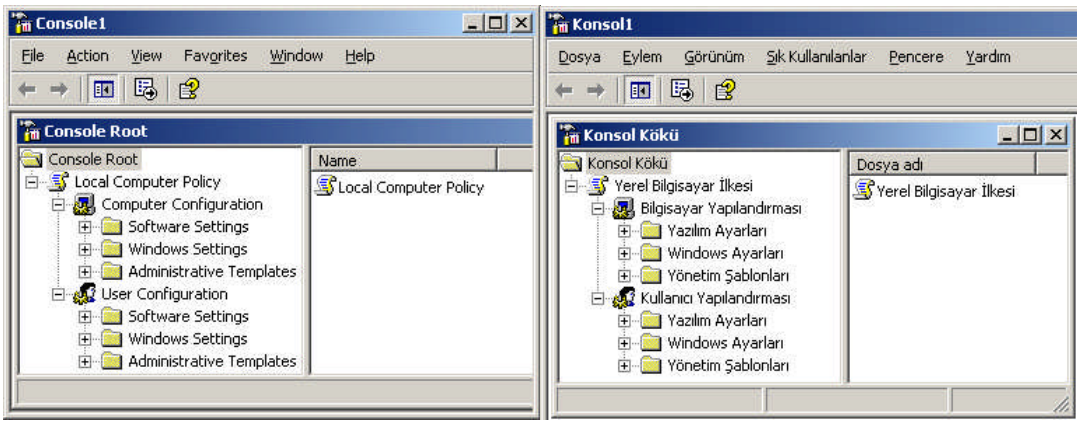
bilgisayarın seçimi yapıldıktan sonra **"Finish"** (Son) butonuna tıklandığımızda yükleme işlemi tamamlanmış ve **Resim 2.5'**teki yüklenen grup politikasının yüklendiği konsol penceresi açılmış olur.



Resim 2.3: Eklenecek standart bileşenler ***(Win 2003 Eng ⇔ Win 2003 Tr)***

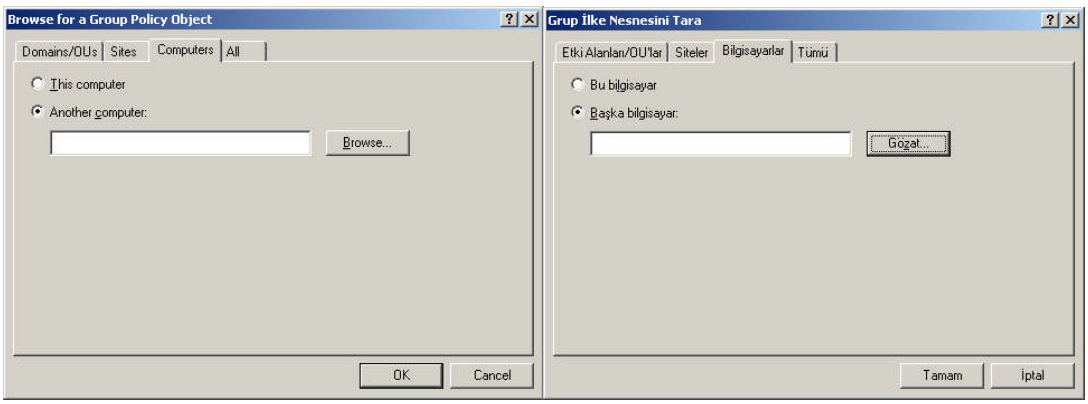


Resim 2.4: Grup politikası kurulacak bilgisayarın seçimi ***(W 2003 Eng ⇔ W 2003 Tr)***

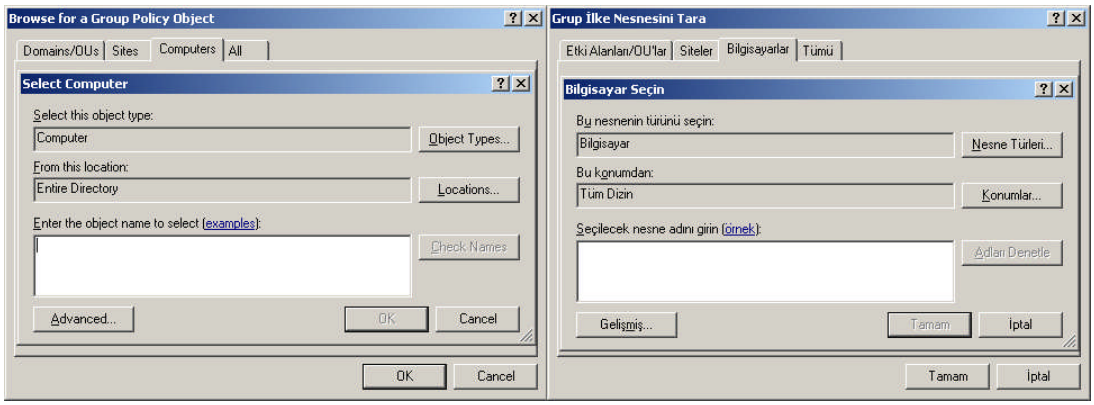


Resim 2.5: Temsilci için atanacak özel görevler *(Win 2003 Eng ⇔ Win 2003 Tr)*

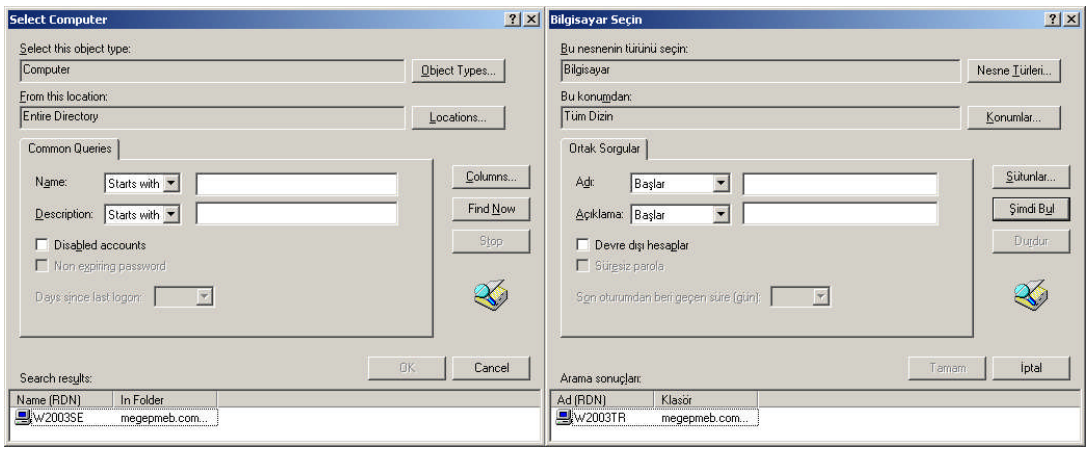
Grup Politikalarını Etki Alanı içerisindeki farklı bir bilgisayara yüklemek istiyorsak Resim **2.4**'deki Pencerede "Browse" (Gözat) butonuna bastığımızda **Resim 2.6'**daki "Grup ilke nesnesi tara" penceresi açılır. "Grup ilke nesnesi tara" penceresinde "Computers" (Bilgisayarlar) sekmesini açarak "Another computer" (Başka bilgisayar) seçeneği yanındaki "Browse" (Gözat) butonuna bastığımızda **Resim 2.7'**deki grup politikası yüklenecek bilgisayar seçimi penceresi karşımıza gelir. **Resim 2.7'**deki pencereden "Advanced" (Gelişmiş) butonuna bastığımızda **Resim 2.8'**deki Grup politikaları yüklenecek bilgisayarı aramamıza yardımcı olacak pencere açılır. **Resim 2.1.8'**deki bu pencereden "Find Now" (Şimdi Bul) dediğimizde Etki alanı içerisindeki tüm bilgisayarlar listelenir. Listelenen bilgisayardan birini seçerek "OK" (Tamam) butonuna bastıktan sonra yükleme işlemine başlanmış olur.



Resim 2.6: Grup ilke nesnesi bilgisayarlar sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*



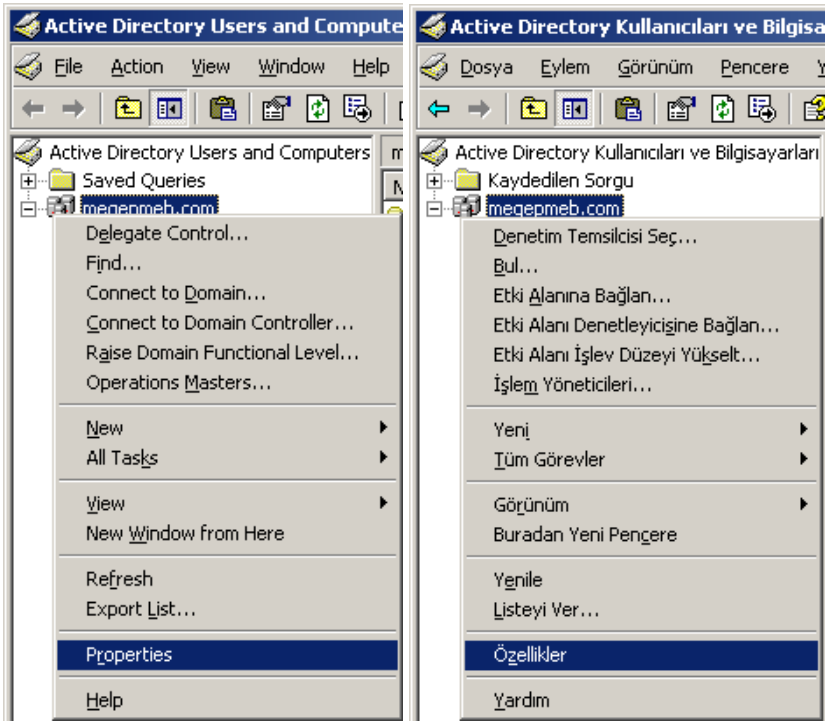
Resim 2.7: GPO yüklenecek bilgisayar seçimi *(W 2003 Eng ⇔ W 2003 Tr)*



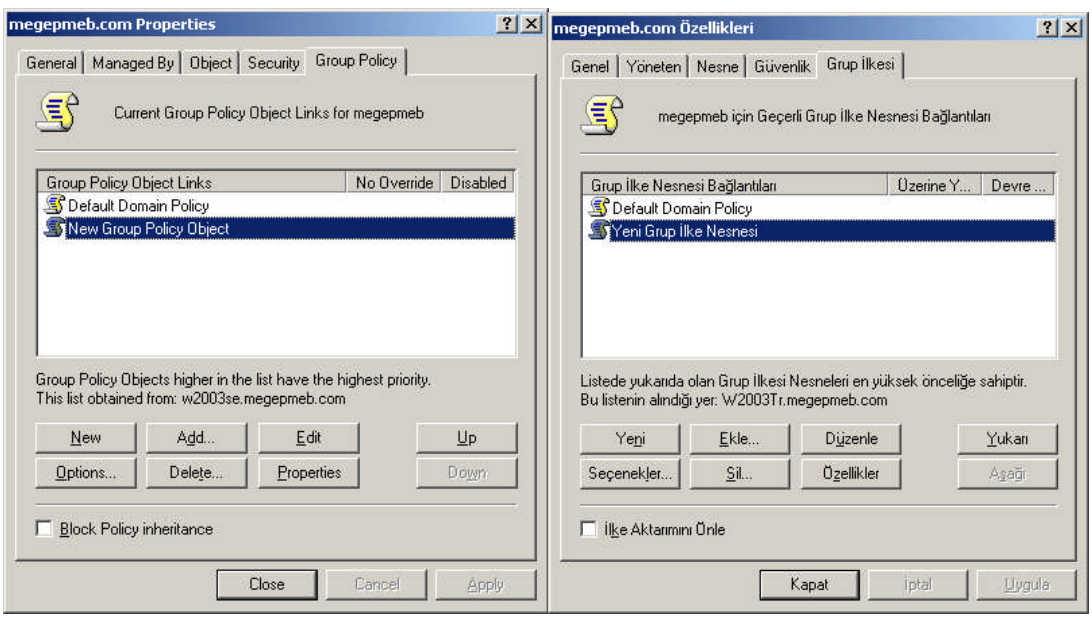
Resim 2.8: GPO yüklenecek bilgisayarın aranması *(Win 2003 Eng ⇔ Win 2003 Tr)*

2.2. Etki Alanı İçerisindeki GPO'ların Uygulaması

Etki alanı içerisindeki kullanıcı ve bilgisayarlar için varsayılan Grup Politikalarını düzenleyebilir veya her biri farklı işlevleri gerçekleştirebilecek yeni Grup Politikaları oluşturabiliriz. Etki alanı içerisindeki Grup Politikalarını düzenlemek için **"Start => Administartive Tools => Active Directory Users and Computers"** (Başlat => Yönetimsel Araçlar => Active Directory kullanıcı ve Bilgisayarları) seçeneğine tıklayıp **Resim 2.9'**daki karşımıza gelen pencerenin Etki alanına (Bizim Etki Alanı: **megepmeb.com**) sağ tıklayıp "Properties" (Özellikler) seçmemiz ve özellikler penceresini açmamız gerekir.

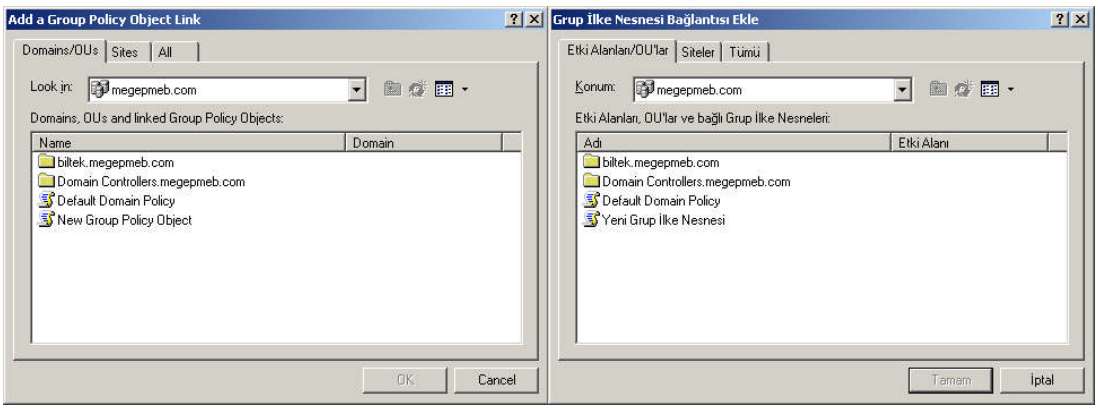


Resim 2.9: Etki alanı "Özellikler" penceresinin açılması *(Win 2003 Eng ⇔ Win 2003 Tr)*

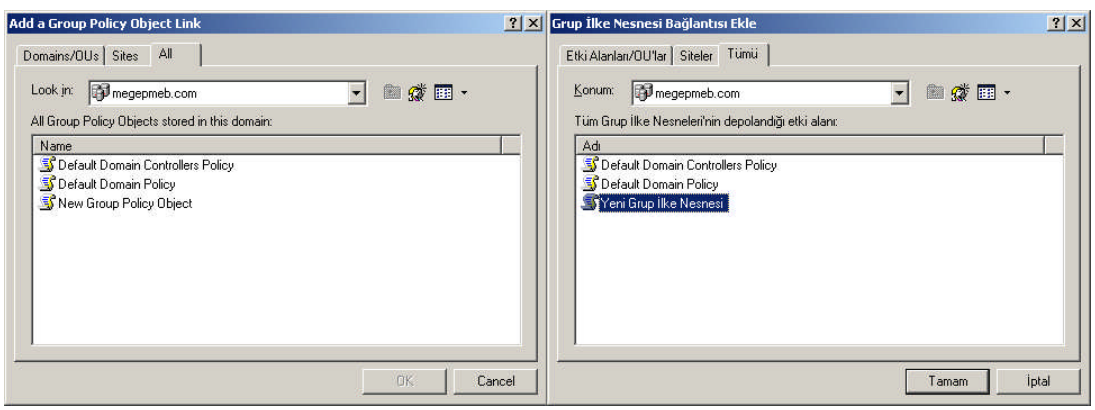


Resim 2.10: Özellikler penceresi "Grup İlkesi" sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*

Resim 2.10'daki etki alanı özellikler penceresinin grup ilkesi sekmesinde **"megepmeb.com"** etki alanı için tanımlanmış grup ilkeleri görülmektedir. Yeni bir GPO oluşturmak için "New" (Yeni) butonuna basmamız gereklidir. Şu anda yüklü olarak "Default Domain Policy" (varsayılan etki alanı politikası) görülmektedir. Yeni GPO yüklemek için "Add" (Ekle) butonuna basmamız ve **Resim 2.11'**deki pencereyi açmamız gerekir. **Resim 2.11'**deki GPO nesne bağlantısı "ekle" penceresinde üç farklı sekme bulunmaktadır. "Domain/OUs" (Etki Alanı/OU'lar) sekmesinde mevcut Etki alanı, Organizasyon birimi ve bunlar için tanımlanmış GPO'lar bulunmaktadır. "Sites" (Siteler) sekmesinde ileriki etkinliklerde öğreneceğiniz site alanlarını ve bunlar için yüklü "All" (Tümü) sekmesinde sistemde yüklü tüm GPO'ları göstermektedir. Bu sekmelerdeki GPO'lardan herhangi birini seçip ekleme işlemini gerçekleştirebiliriz.



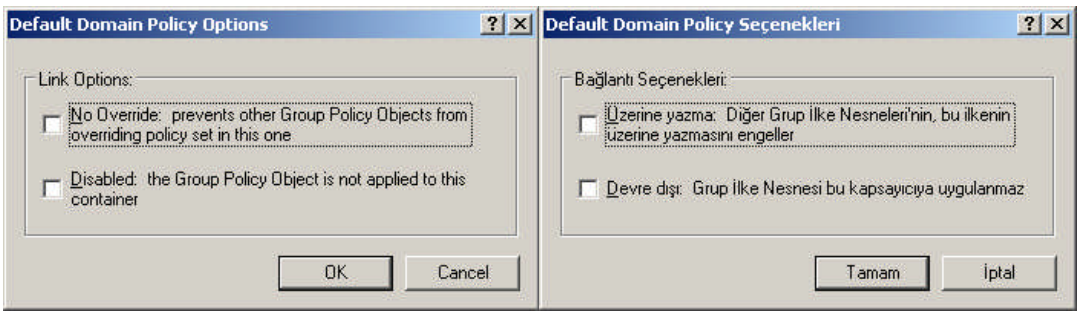
Resim 2.11: GPO sekmesi Add butonu *(Win 2003 Eng ⇔ Win 2003 Tr)*



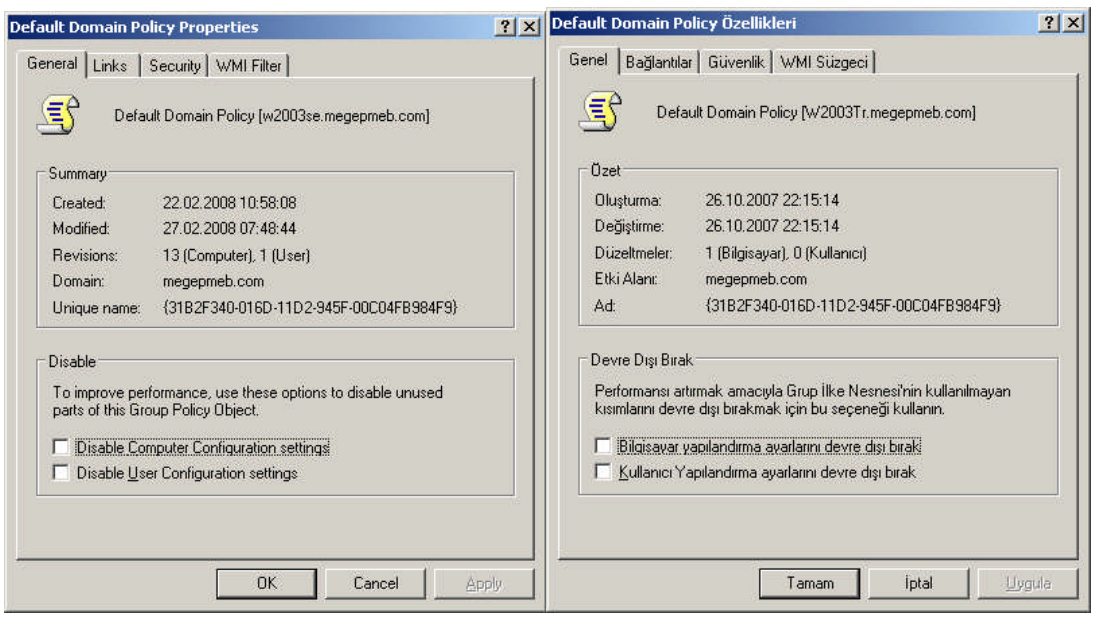
Resim 2.12: GPO sekmesi Add butonu All sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*

Resim 2.10'daki Pencerede "Options" (Seçenekler) butonuna bastığımızda **Resim 2.13'**teki seçenek penceresi açılır. Burada birden fazla tanımlanmış GPO için hiyerarşik bir sıralama yapmak için kullanılan seçenekler bulunmaktadır. GPO ayarları arasında herhangi bir çakışma olursa "No Overide" (Üzerine yazma) seçeneğine tıklanmış

GPO ayarları geçerli olur. “Disabled” (Devre dışı) seçeneği ise GPO ayarlarını devre dışı bırakmak için kullanılır.



Resim 2.13: GPO sekmesi Options butonu *(Win 2003 Eng ⇔ Win 2003 Tr)*

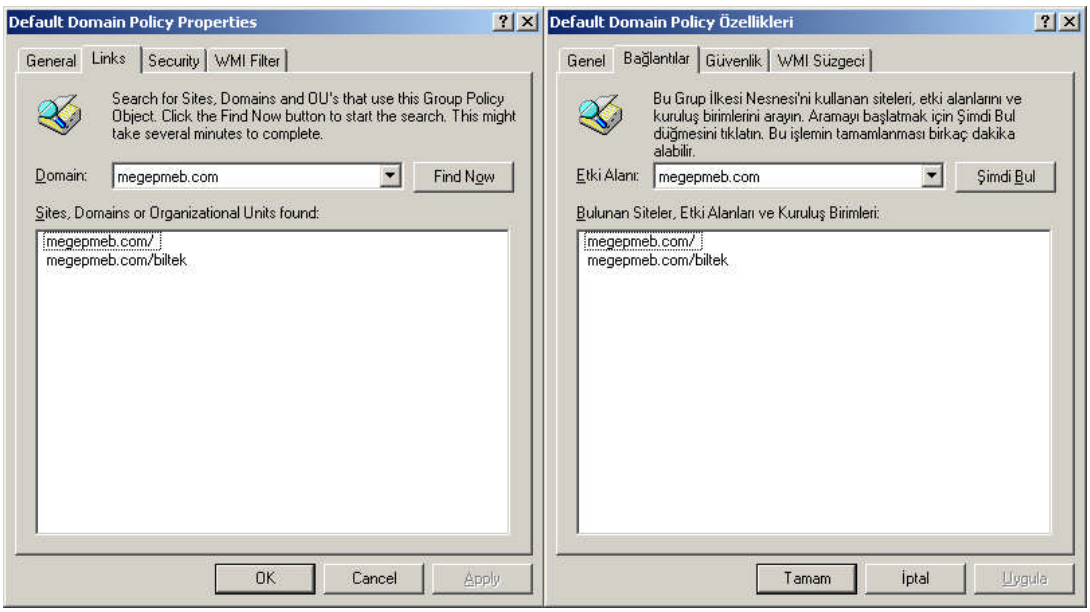


Resim 2.14: Seçilen GPO özellikleri *(Win 2003 Eng ⇔ Win 2003 Tr)*

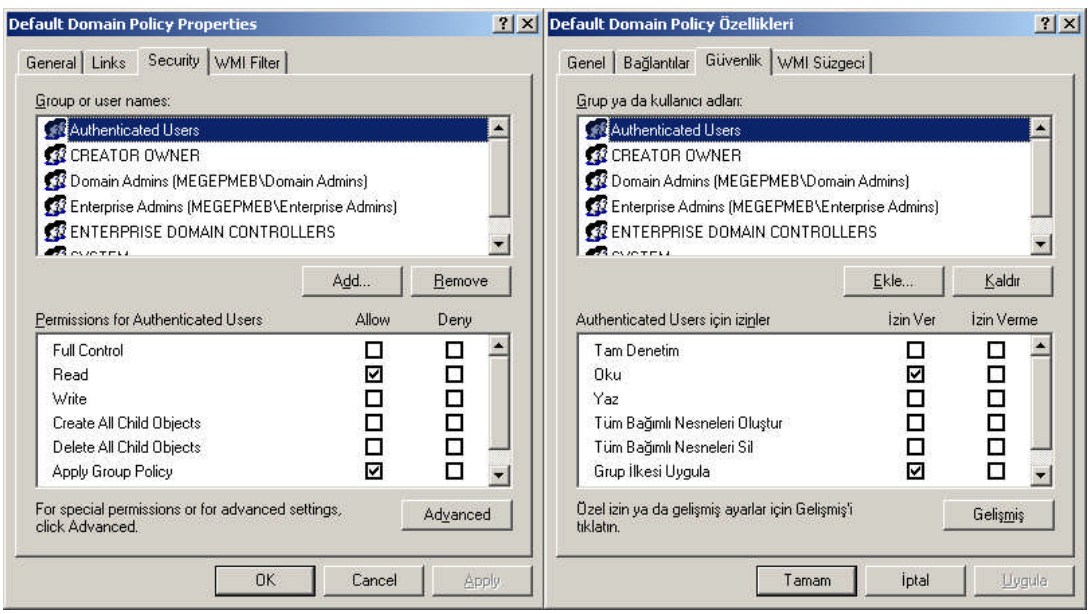
Resim 2.10’daki Pencerede “Properties” (Özellikler) butonuna bastığımızda **Resim 2.14’**teki **“Seçilen GPO için özellikler”** penceresi açılır. Bu penceredeki ilk sekmede GPO hakkında genel bilgi vererek devre dışı bırakmak için iki seçenek yer almaktadır. “Disable Computer Configuration Settings” (Bilgisayar yapılandırma ayarlarını devre dışı bırak) seçeneği GPO’nun sadece bilgisayarlarla ilgili yönetimsel ayarlamalarını devre dışı bırakır.

“Disable User Configuration Settings” (Kullanıcı yapılandırma ayarlarını devre dışı bırak) seçeneği ise GPO’nun sadece kullanıcılarla ilgili yönetimsel ayarlamalarını devre dışı bırakır. **Resim 2.15’**teki “Links” (Bağlantılar) sekmesinde Etki alanı içerisinde seçilen

GPO'yu kullanan birimleri görüntüler. "Find Now" (Şimdi Bul) butonuyla GPO'yu kullanan birimleri arama işlemini gerçekleştirebiliriz.



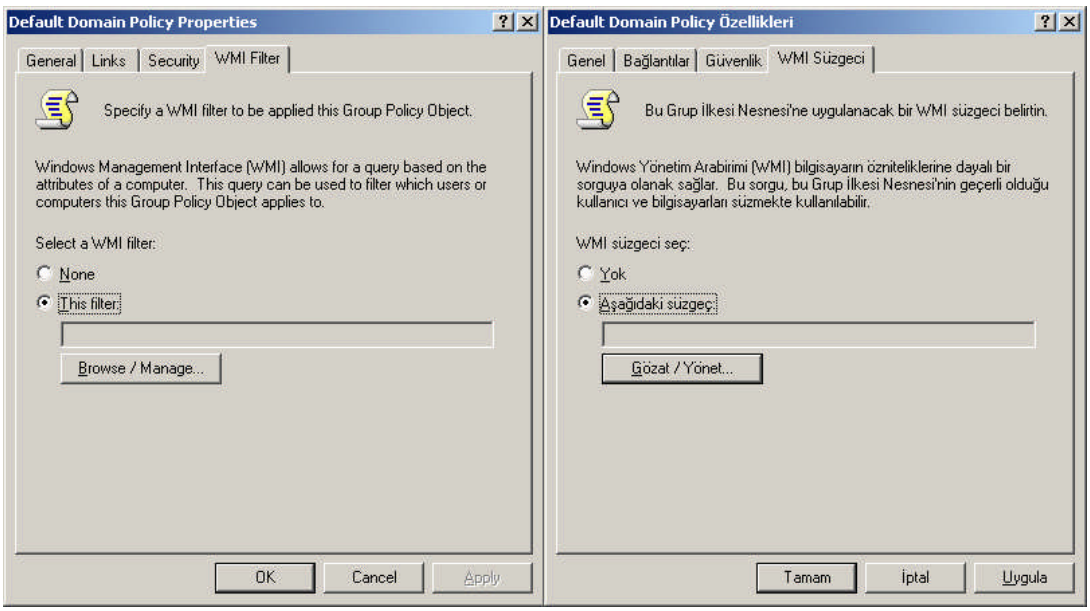
Resim 2.15: Seçilen GPO özellikleri Links sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*



Resim 2.16: Seçilen GPO özellikleri Güvenlik sekmesi *(Win 2003 Eng ⇔ Win 2003 Tr)*

Resim 2.16'daki "Security" (Güvenlik) sekmesinde GPO'nun seçilen bir kullanıcı üzerinde hangi denetimler gerçekleştirebileceğini ayarlamak için kullanılır. Örneğin

Resim 2.16'da "Add" (Ekle) butonuyla üst listeye bir kullanıcı dâhil edip "izinler" penceresinden "Apply Group Policy" (Grup ilkesi uygula) seçeneğinin "Deny" (İzin verme) seçeneğini tıklarsak GPO ayarları artık sadece o kullanıcı için geçerli olmaz.

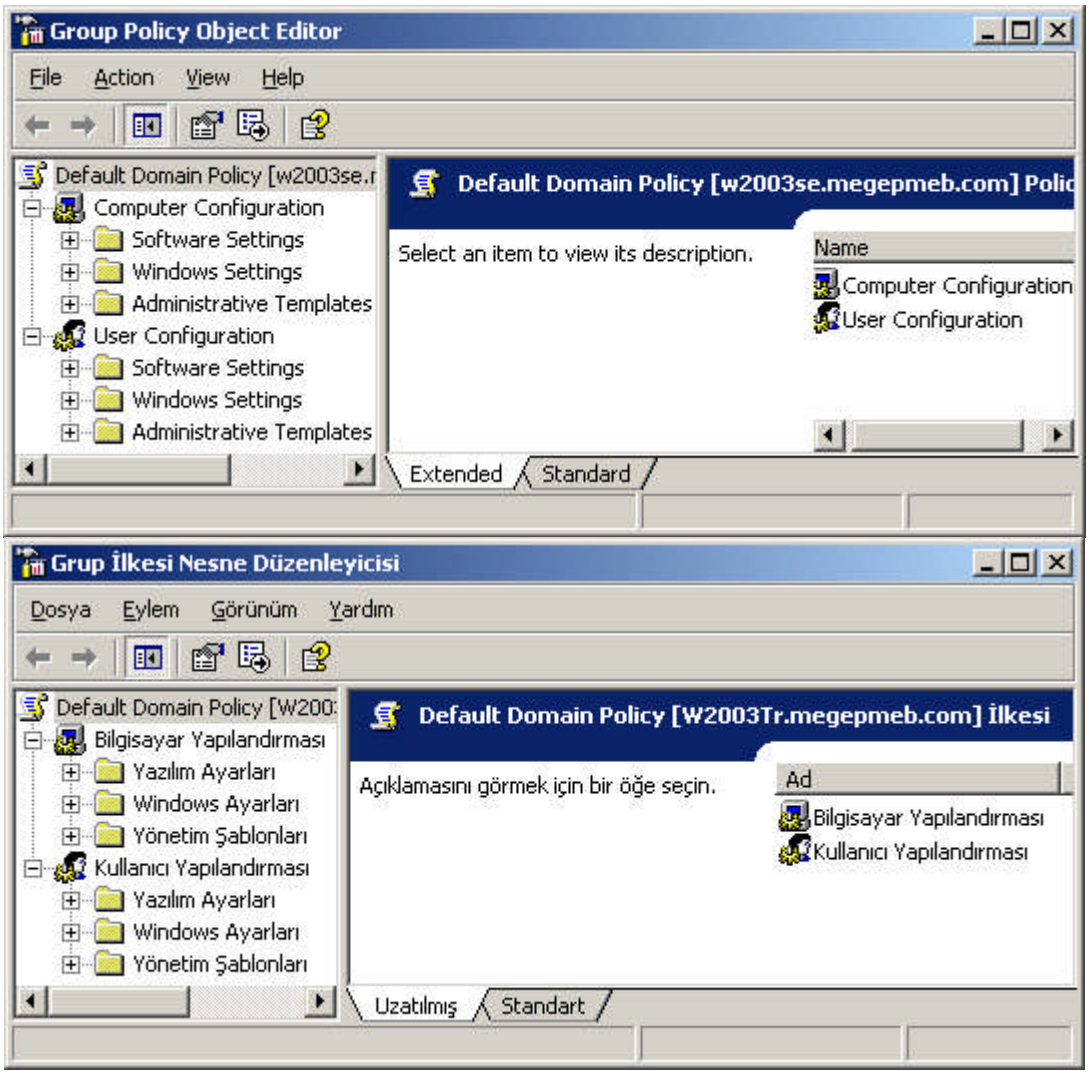


Resim 2.17: Seçilen GPO özellikleri WMI süzgeci *(Win 2003 Eng ⇔ Win 2003 Tr)*

Resim 2.17'deki "WMI Filter" (WMI süzgeci) sekmesinde Etki alanı içerisindeki bilgisayarlar ve kullanıcılara uygulanacak sorgular oluşturmak ve bu sorgulara uyan bilgisayarlar ve kullanıcıları süzmek için kullanılır.

Resim 2.10'daki Pencerede "Edit" (Düzenle) butonuna bastığımızda **Resim 2.18'**deki GPO nesne düzenleyici penceresi açılır. Bu pencereden kullanıcı ve bilgisayarlarla ilgili gerekli düzenlemeler yapılmaktadır. GPO nesne düzenleyici penceresinde bilgisayarlar ve kullanıcılar ile ilgili üç farklı ayarlama grubu vardır:

- Software Settings (Yazılı Ayarları)
- Windows Settings (Windows Ayarları)
- Administrative Templates (Yönetim Şablonları)



Resim 2.18: GPO nesne düzenleyicisi ***(Win 2003 Eng ⇔ Win 2003 Tr)***

2.3. Grup Politikasının Yayılımı

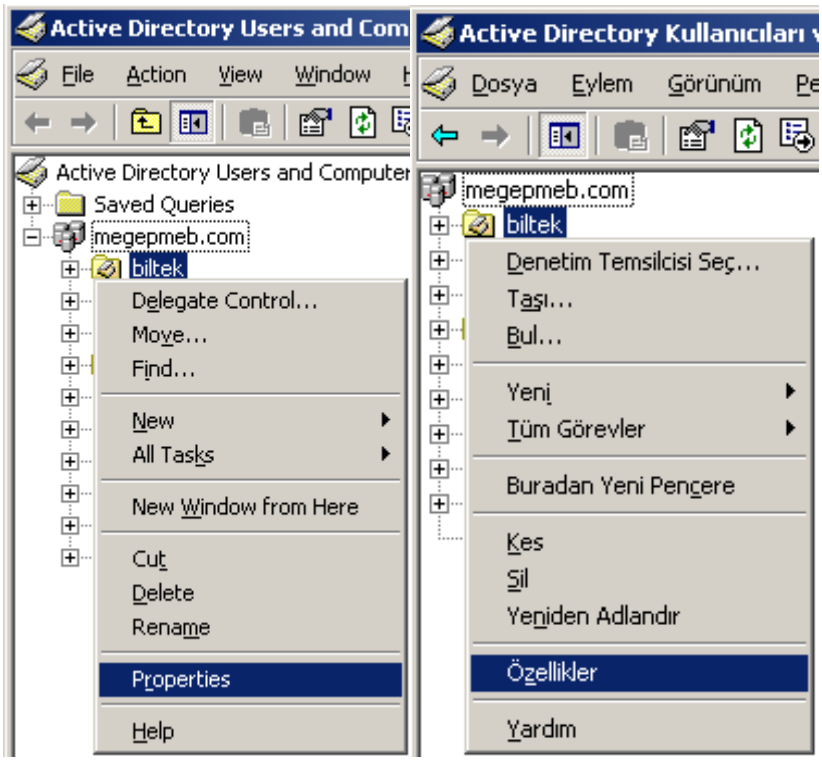
Grup politikaları (Group Policy);

- Etki alanı (Domain),
- Site,
- Organizasyon Birimi (OU-Organizational Unit)

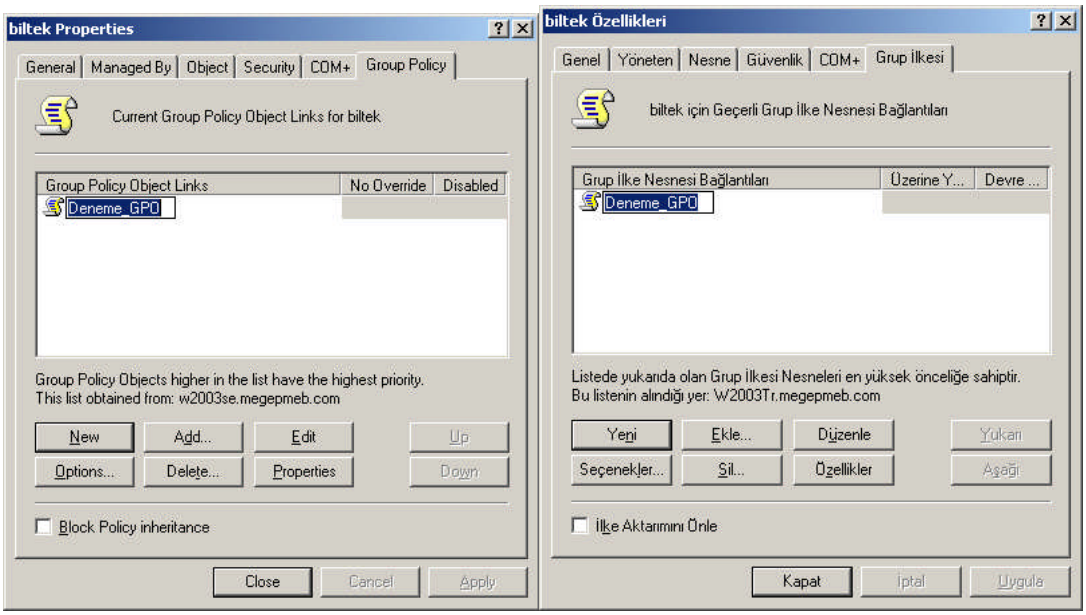
nesneleri içindeki kullanıcı ve bilgisayarları yönetmek için kullanılır.

Grup politikaları bilgisayar ve kullanıcılara direkt olarak uygulanamaz.

Bir organizasyon birimi için GPO tanımlamak istersek **Resim 2.19'**daki gibi önceden oluşturulmuş "Biltek" ismindeki Organizasyon birimlerine sağ tıklatıp "Properties" (Özellikler) seçmemiz ve **Resim 2.20'**deki özellikler penceresini açmamız gerekir.

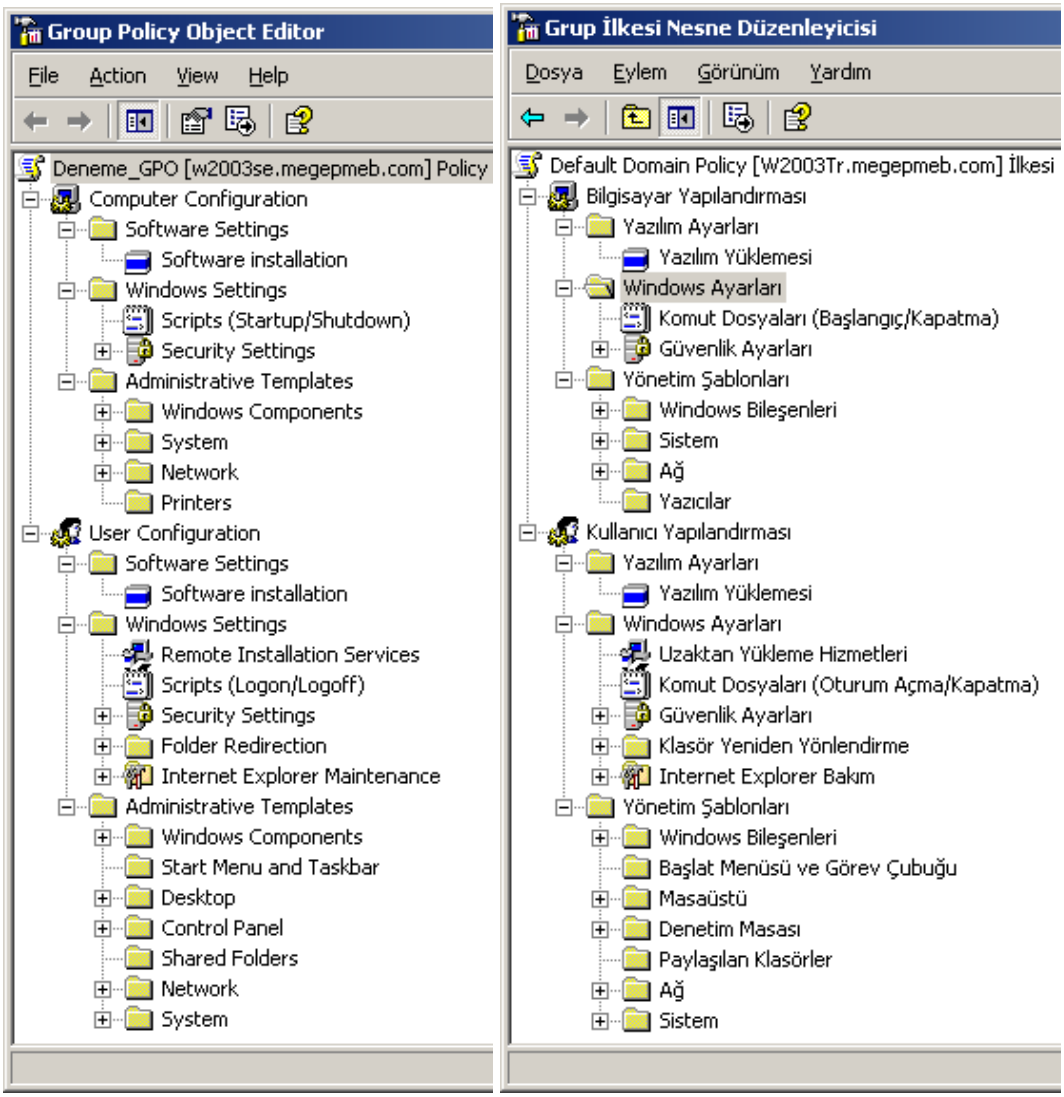


Resim 2.19: Organizasyon birimi için özellikler penceresinin açılması
(Win 2003 Eng ⇔ Win 2003 Tr)



Resim 2.20: Organizasyon birimi için özellikler penceresi
(Win 2003 Eng ⇔ Win 2003 Tr)

Resim 2.20'deki Organizasyon birimi için özellikler penceresinin "Group Policy" (Grup ilkesi) sekmesinde öncelikle "Add" (Ekle) butonuyla "Deneme_GPO" isminde bir Grup politikası oluşturalım. Oluşturulan GPO üzerine tıklayıp "Edit" (Düzenle) butonuna bastığımızda **Resim 2.21'**deki Grup ilkesi Nesne Düzenleyicisi açtığımızda karşımıza "Computer Configuration" (Bilgisayar Yapılandırması) ve "User Configuration" (Kullanıcı Yapılandırması) isminde iki farklı yönetim grubu gelir.



Resim 2.21: Organizasyon birimi için alt özellikler penceresi
(Win 2003 Eng ⇔ Win 2003 Tr)

Bilgisayar ve kullanıcılarla ilgili ayarları genel olarak **Resim 2.21'**de verdik ileriki etkinliklerde bu gibi ayarlamaları ayrıntılı olarak inceleyeceğiz.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Etki alanınızın altına **“ayarlar_1”** ve **“ayarlar_2”** isminde iki farklı Grup politikası oluşturup **“ayarlar_1”** Grup politikasını sadece kullanıcılar için **“ayarlar_2”** ise sadece bilgisayar için etkili olacak şekilde ayarlayınız.	➢ Etki alanı ve politikası isimlerine, ayrıca Grup politikalarının kimler için geçerli olacağına dikkat ediniz.
➢ Oluşturacağımız **“Pazarlama”** isimli organizasyon birimi içerisine **“user_1”** ve **“user_2”** isimli iki kullanıcı oluşturup ayrıca organizasyon birimi için önceden oluşturulmuş **“ayarlar_1”** Grup politikasını ekleyiniz ve **“user_2”** isimli kullanıcıyı bu Grup politikasından muaf tutunuz.	➢ Organizasyon birimi ve kullanıcı isimlerine, kullanıcıya verilecek Grup politikalarının neler olduğuna dikkat ediniz.
➢ Oluşturacağımız **“Arsiv”** isimli organizasyon birimi için **“GPO_1”, “GPO_2”** ve **“GPO_3”** isminde üç farklı Grup politikası oluşturup bu politikaları hiyerarşik bir sıralamaya koyunuz.	➢ Organizasyon birimi ve Grup politikaları isimlerine dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıda verilen ifadeler için, yanlarında verilmiş boşluğa doğru ise "**D**"; yanlış ise "**Y**" yazınız.

1. Grup politikaları sadece kullanıcı ve bilgisayara uygulanabilir. (…) D/Y

2. Grup politikaları etki alanı için belirlenebilir ama organizasyon birimleri için belirlenemez (…) D/Y

3. Yerel bilgisayar veya diğer bilgisayarlar için Grup politikası Microsoft Yönetim Konsolundan gerçekleştirilir. (…) D/Y

4. Etki alanı için yeni oluşturacağımız bir Grup politikası diğer organizasyon birimleri içinde kullanılamaz. (…) D/Y

5. Bir birim için oluşturulmuş iki Grup politikası için bir çakışma olduğunda hiyerarşi olarak en büyük olan Grup politikası ayarları uygulanır. (…) D/Y

6. Bir Grup politikası sadece bilgisayarlar ya da sadece kullanıcılar için etkili olabilecek şekilde ayarlanabilir. (…) D/Y

7. Etki alanı için yeni oluşturacağımız bir Grup politikasından sadece bir kullanıcının etkilenmesi sağlanamaz. (…) D/Y

8. Etki alanındaki bir Grup politikasının kullanıcı ve bilgisayar özelliklerini düzenleyebilmek için etki alanı özelliklerinden "Group Policy" sekmesini açmak gerekir. (…) D/Y

9. Bir Grup politikasının izinlerini belirleyebilmek için GPO özelliklerinin "Security" sekmesini açmak gerekir. (…) D/Y

10. Bir Grup politikasını devre dışı bırakmak için GPO özelliklerinin "Links" sekmesini açmak gerekir. (…) D/Y

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları, faaliyete geri dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-3

AMAÇ

Grup politikalarını kullanarak kullanıcı ve bilgisayar ortamını yönetebilecektir.

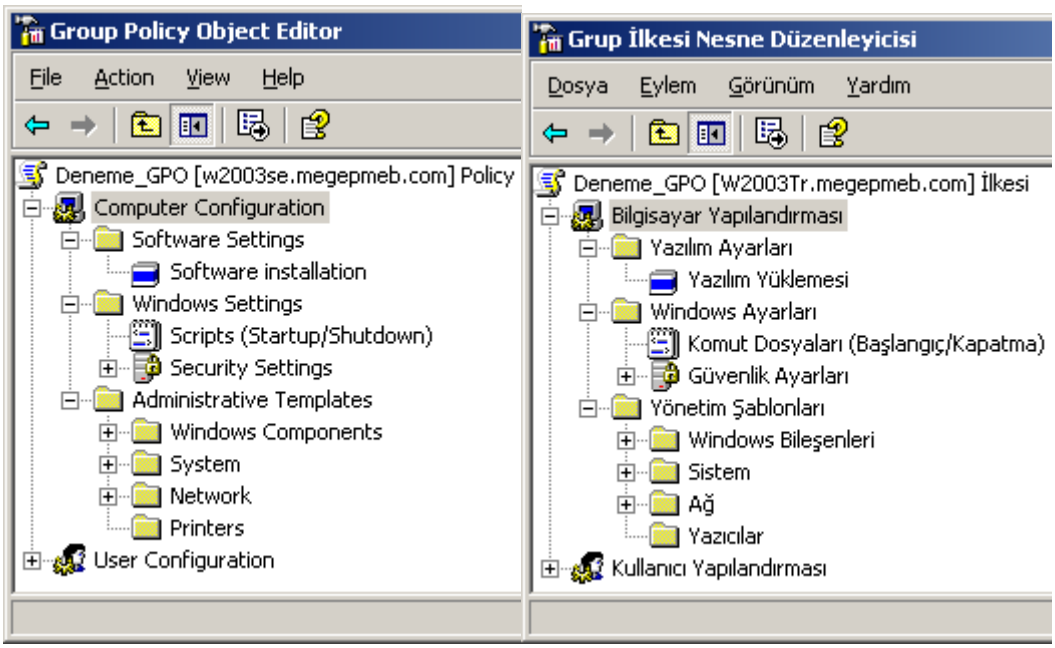
ARAŞTIRMA

- Grup politikaları için Script belirlemelerin nasıl yapıldığını araştırınız.
- Grup politikaları için klasör yönlendirmenin nasıl yapıldığını araştırınız.
- Grup politikaları için bilgisayar yönetim ayarlarının nasıl yapıldığını araştırınız.
- Grup politikaları için kullanıcı yönetim ayarlarının nasıl yapıldığını araştırınız.

3. GRUP POLİTİKALARINI KULLANARAK KULLANICI VE BİLGİSAYAR ORTAMINI YÖNETME

3.1. Grup Politika Özelliklerini Ayarlamak

Grup politikalarının kullanıcı ve bilgisayar özelliklerini düzenleyen bir yönetim şekli olduğundan bahsetmiştik. Kullanıcı ve bilgisayarlarla ilgili açılış, kapanış, windows bileşenleri, otomatik kurulum, sistem ayarları, ağ ayarları, yazıcı ayarları gibi birçok yönetim ayarları grup politikaları içerisinde yer alır. Şimdi bu alt yönetim gruplarını açıklamaya çalışalım.

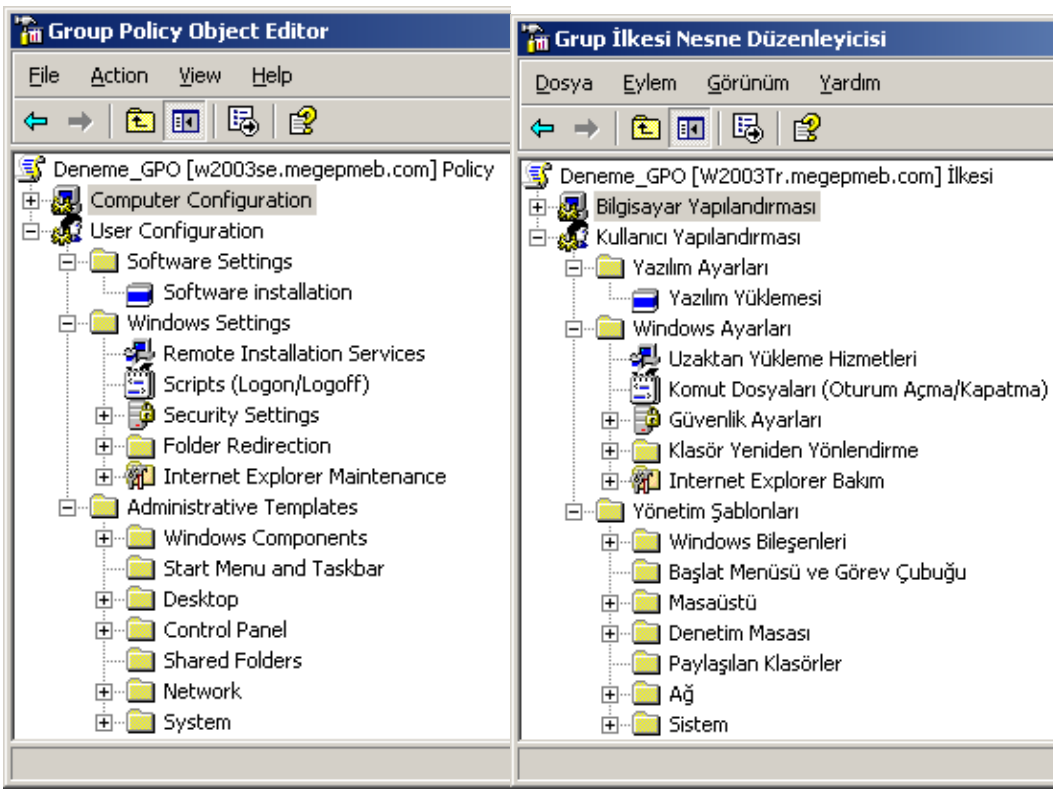


Resim 3.1: Bilgisayarlar için GPO ayarları *(Win 2003 Eng ⇔ Win 2003 Tr)*

Bilgisayar yapılandırma ayarları

- **Software Settings (Yazılım Ayarları):** Bu ayarlar Etki alanındaki bilgisayarlara otomatik olarak yazılım yüklemek için kullanılır.
- **Windows Settings (Windows Ayarları):** Bu ayarlar Etki alanındaki bilgisayarların windows ayarları için kullanılır.
  - **Script (Komut Dosyaları):** Bilgisayarın açılış ve kapanışta çalıştırılacak komut dosyalarını belirlemek için kullanılır.
  - **Security Setting (Güvenlik Ayarları):** Açılış şifresiyle ilgili ayarlar, hesap kilitleme, kullanıcı haklarının belirlenmesi, olay günlükleri, dosya sistemi, kayıt defteri, sistem hizmetleri gibi birçok yönetimsel ve güvenlik ayarlarının bulunduğu bölümdür.
- **Administrative Templates (Yönetim Şablonları):** Bilgisayarda yüklü programların ayarları, ağ ayarları, yazıcı ayarları gibi geniş bir yönetim imkânı sağlayan bölümdür.
  - **Windows Components (Windows Bileşenleri):** Netmeeting, İnternet Explorer, IIS, Messanger, Media Player gibi bileşenlerin yönetim ayarlarının yapıldığı bölümdür.
  - **Systems (Sistem):** Kullanıcı profilleri, komut dosyaları, oturum açma, uzaktan yardım, disk sınırları, grup ilkeleri gibi yönetim ayarlarının yapıldığı bölümdür.
  - **Network (Ağ):** DNS istemcisi, çevrim dışı dosyalar, ağ bağlantıları, SNMP gibi ağ yönetim ayarlarının yapıldığı bölümdür.

- **Printers (Yazıcılar):** Yazdırma seçenekleri, web tabanlı yazdırma, yazıcılara Gözat, yazdırma havuzu gibi yazıcı yönetim ayarlarının bulunduğu bölümdür.



Resim 3.2: Kullanıcılar için GPO ayarları (Win 2003 Eng ⇔ Win 2003 Tr)

Kullanıcı yapılandırma ayarları

- **Software Settings (Yazılı Ayarları):** Bu ayarlar Etki alanındaki bilgisayarlara otomatik olarak yazılım yüklemek için kullanılır.
- **Windows Settings (Windows Ayarları):** Bu ayarlar Etki alanındaki kullanıcıların windows ayarları için kullanılır.
  - **Remote installation services (Uzaktan yükleme hizmetleri):** Uzaktan etki alanındaki bilgisayara yazılım yüklemek için kullanılır.
  - **Script (Komut dosyaları):** Kullanıcıların oturum açılış ve kapanışında çalıştırılacak komut dosyalarını belirlemek için kullanılır.
  - **Security Setting (Güvenlik ayarları):** Kullanıcılar için ortak anahtar ilkeleri, yazılım kısıtlama gibi güvenlik ayarlarının bulunduğu bölümdür.
  - **Folder Redirection (Klasör yeniden yönlendirme):** Kullanıcıların dosyalarını ağ ortamındaki paylaştırılmış klasörler içerisine yönlendirmek için kullanılan bölümdür.

- **İnternet Explorer Maintenance (İnternet Explorer Bakım):** İnternet Explorer ile ilgili araç çubuklarını özelleştirilmesi, bağlantı ayarları, sık kullanılanlar, güvenlik bölgeleri gibi ayarlamaları içerir.

➢ **Administrative Templates (Yönetim şablonları):** Bilgisayarda yüklü programların ayarları, ağ ayarları, yazıcı ayarları gibi geniş bir yönetim imkânı sağlayan bölümdür.

- **Windows Components (Windows Bileşenleri):** Netmeeting, internet Explorer, IIS, Messanger, Media Player gibi bileşenlerin sadece kullanıcılara özgü ayarlarını içerir.
- **Start menu and taskbar (Başlat menüsü ve görev çubuğu):** Kullanıcıların Başlat menüsü ve görev çubuğu ile ilgili ayarlarını içeren bölümdür.
- **Desktop (Masaüstü):** Kullanıcıların masaüstüyle ilgili gerekli ayarlamaların ve bu ayarlara erişim hakkıyla ilgili düzenlemelerin yapıldığı bölümdür.
- **Control panel (Denetim masası):** Kullanıcıların Denetim masasındaki gerekli ayarlamaların ve bu ayarlara erişim hakkıyla ilgili düzenlemelerin yapıldığı bölümdür.
- **Shared Folders (Paylaşılan klasörler):** Paylaşılan klasörlerle ilgi gerekli ayarlamaların yapıldığı bölümdür.
- **Network (Ağ):** Kullanıcılarla ilgili çevrim dışı dosyalar ve ağ bağlantılarıyla ilgili ağ yönetim ayarlarının yapıldığı bölümdür.
- **Systems (Sistem):** Kullanıcı profilleri, komut dosyaları, oturum açma, Crtl+Alt+Del seçenekleri, grup ilkeleri, güç yönetimi gibi ayarların kullanıcıları ilgilendiren düzenlemelerin yapıldığı bölümdür.

3.2. Grup Politikası İle Senaryo (Script) Atama

Grup politikalarının bizlere sağladığı bir diğer avantaj da tümleşik kod içeren dosyaları bilgisayar açılış veya kapanışında çalıştırmasıdır. Önceden bu gibi işlemler için toplu işlem dosyaları kullanılırdı. Şimdilerde Windows Server 2003 sayesinde farklı script dillerini de desteklemektedir. Desteklenen kod dosyaları ve görünümleri **Resim 3.3'**de verilmiştir

Resim 3.3: Windows Server 2003'ün desteklediği kod dosyaları

Windows Server 2003'ün desteklediği kod dosyaları:

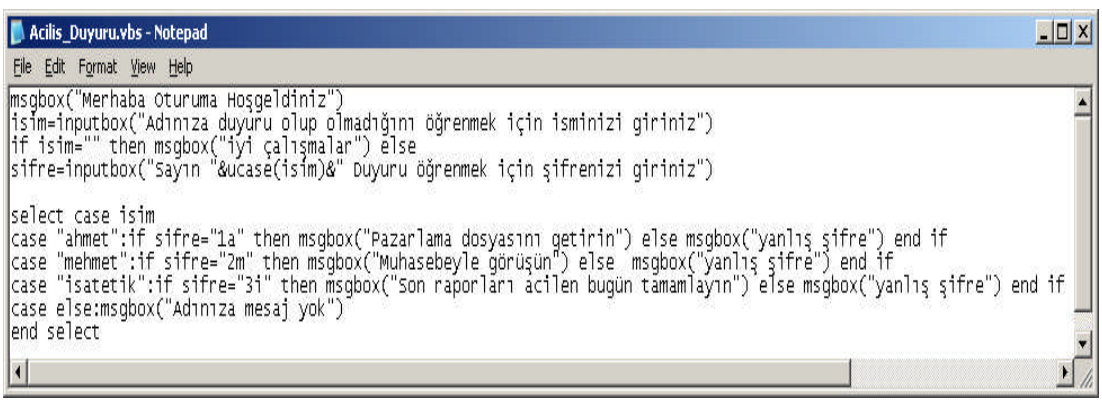
- Toplu işlem dosyaları (BAT uzantılı)
- Çalıştırılabilir dosyalar (EXE veya COM uzantılı)
- Visual Basic Script dosyaları (VBS uzantılı)
- Java Script dosyaları (JS uzantılı)

Grup politikalarında script oluşturabilmek için Windows Server 2003 desteklediği bir script dilini seçtikten sonra bir metin editöründe örneğin "Notepad" (Not defteri)de kodlarımızı yazabiliriz tabii ki dosyayı kaydederken uzantısına dikkat etmek şartıyla. Şimdi Visual Basic Script kodlarıyla örnek bir uygulama oluşturalım.

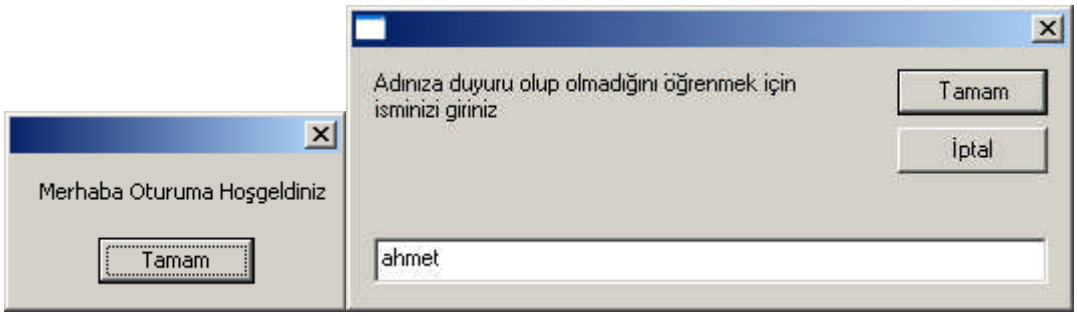
```
Msgbox ("Merhaba Oturuma Hoş geldiniz")
isim=inputbox ("Adınıza duyuru olup olmadığını öğrenmek için isminizi giriniz")
if isim="" then msgbox("iyi çalışmalar") else
sifre=inputbox ("Sayın "&ucase (isim) &" Duyuru öğrenmek için şifrenizi giriniz")

select case isim
case "ahmet":if sifre="1a" then msgbox("Pazarlama dosyasını getirin") else msgbox("yanlış şifre") end if
case "mehmet":if sifre="2m" then msgbox("Muhasebeyle görüşün") else  msgbox("yanlış şifre") end if
case "isatetik":if sifre="3i" then msgbox("Son raporları acilen bugün tamamlayın") else msgbox("yanlış şifre")
end if
case else:msgbox("Adınıza mesaj yok")
end select
```

Tablo 3.1: Örnek bir Visual Basic Script uygulaması

Tablo 3.1'deki örnek uygulamamızda kullanıcıların oturumu açtıklarında kendilerine özel duyuru mesajlarını, kendi şifrelerini girerek okuyabilen bir dosya oluşturalım. Bu işlemi **Resim 3.4'**te olduğu gibi "Not defteri" programında gerçekleştirebiliriz. Örnek kodlarımızı yazdıktan sonra dosyamızı kaydederken **"Acilis_Duyuru.vbs"** isminde kaydedelim. Siz farklı bir isim de verebilirsiniz ama mutlaka uzantısı "VBS" olmalıdır. Uzantısı VBS olduğunda sembolü **Resim 3.4'**teki gibi olur. Kaydetme işlemini de tamamladıktan sonra kodlarımızın çalıştığını görmek için üzerine çift tıklamak yeterli olacaktır.



Resim 3.4: Örnek kod dosyasının Not defterinde yazılması

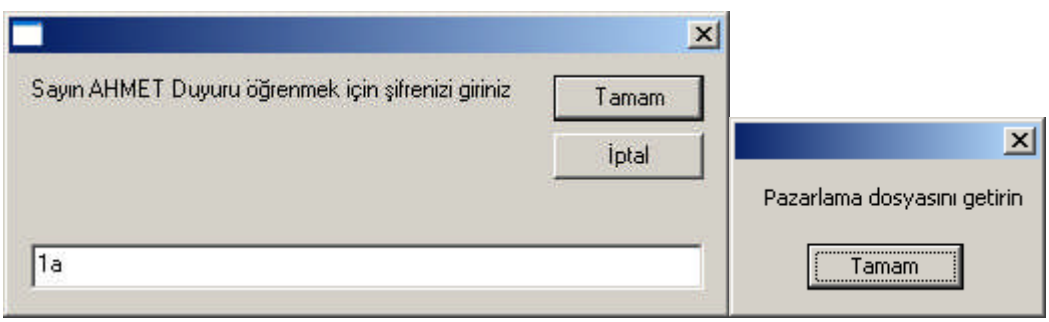


Resim 3.5: Örnek kod dosyasının çalıştırılması (1. ve 2. adım)

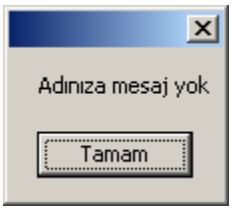
Örnek kodlarımız çalıştırıldığında **Resim 3.5'**teki ilk adımda karşılama mesajı gelecek ikinci adımda ise adımıza bir duyuru olup olmadığını öğrenmemiz için isminizi girmemizi isteyecektir. İkinci aşamadaki kısımda iptal butonuna basarsak **Resim 3.6'**daki üçüncü aşamaya geçip duyuru işlemini atlayacaktır. Eğer ikinci aşamada isim yazar tamam butonuna basarsak **Resim 3.7'**deki dördüncü aşamada o kullanıcı için şifre isteyecektir. Dördüncü aşamada şifre doğru ise beşinci aşamadaki o kullanıcıya ait duyuru, ekranda görüntülenecek eğer şifre yanlış ise veya kullanıcı ismi yok ise **Resim 3.8'**deki altıncı aşamada ekranda "mesaj yok" görüntülenecektir.

GP oluşturulduktan sonra bu işlemingerçekleşmesi konsol ekranında (cmd) "gpudate/force" komutu ile sağlanır.

Resim 3.6: Örnek kod dosyasının çalıştırılması (3. adım)

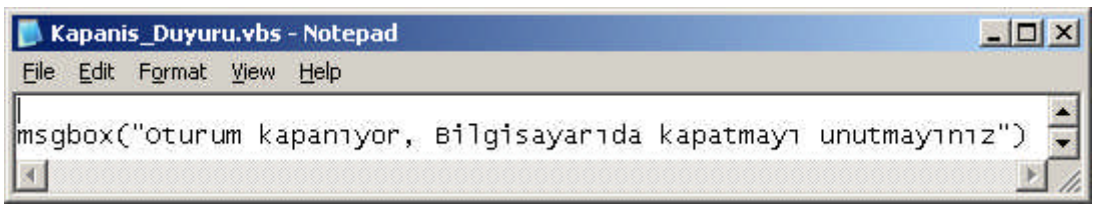


Resim 3.7: Örnek kod dosyasının çalıştırılması (4. ve 5. adım)

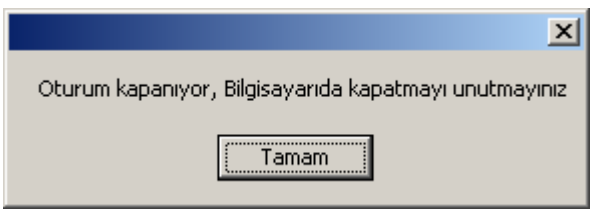


Resim 3.8: Örnek kod dosyasının çalıştırılması (6. adım)

Görüldüğü gibi kullanıcıları bilgilendirme amaçlı kısa bir program parçası oluşturduk. Visual Basic Script kodlarını bildikten sonra farklı birçok program parçası yazabiliriz. Şimdide oturumu kapatmak için **Resim 3.9'**daki gibi ekrana mesaj veren bir program parçası yazalım ve **"Kapanis_Duyuru.vbs"** isminde kaydedelim. Bu dosyayı çalıştırdığımızda da **Resim 3.9'**daki gibi bir bilgi mesajı elde ederiz.

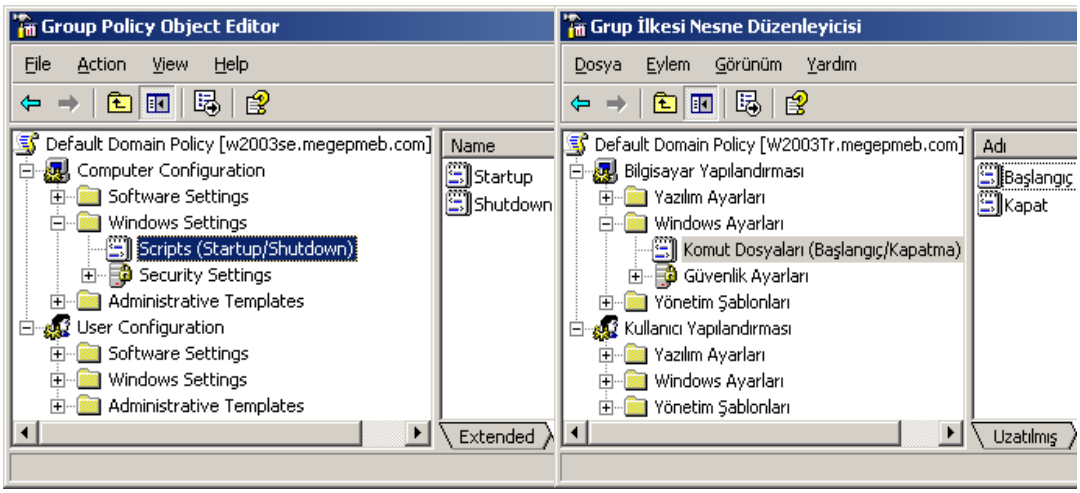


Resim 3.9: Kapanış için örnek kod dosyasının Not defterinde yazılması



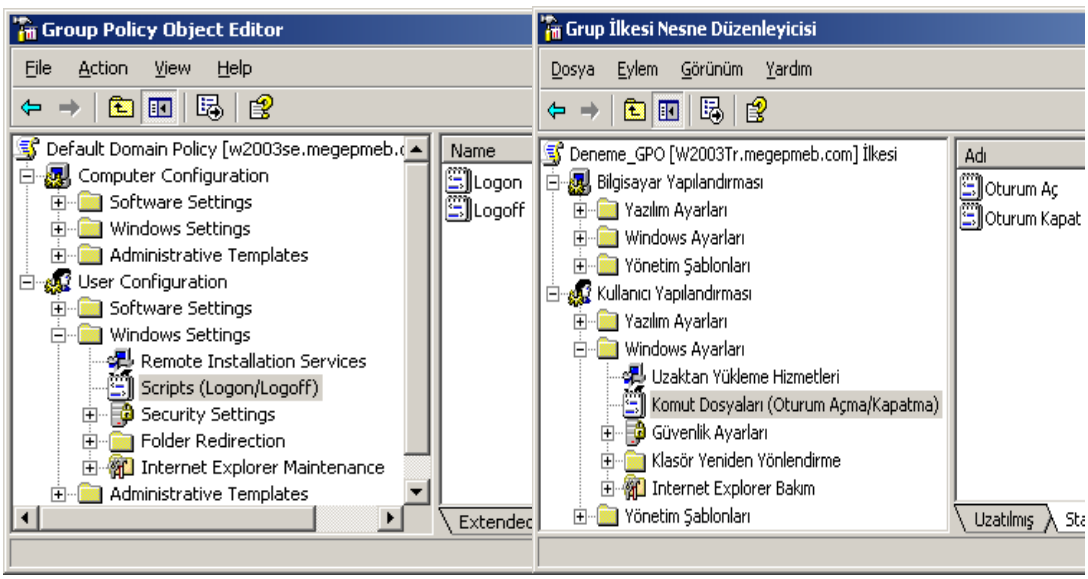
Resim 3.10: Kapanış için örnek kod dosyasının çalıştırılması

Grup politikalarında, oluşturduğumuz örnek kod dosyalarını, kullanmak için öncelikle hangi durumlarda kullanacağımızı belirlememiz gerekir. Örneğin, bilgisayar açıldığında kodların çalışmasını istiyorsak **Resim 3.11'**deki bölümden "Startup" (Başlangıç) seçeneğini, bilgisayar kapandığında kodların çalışmasını istiyorsak "Shutdown" (Kapat) seçeneğini kullanmamız gerekir.



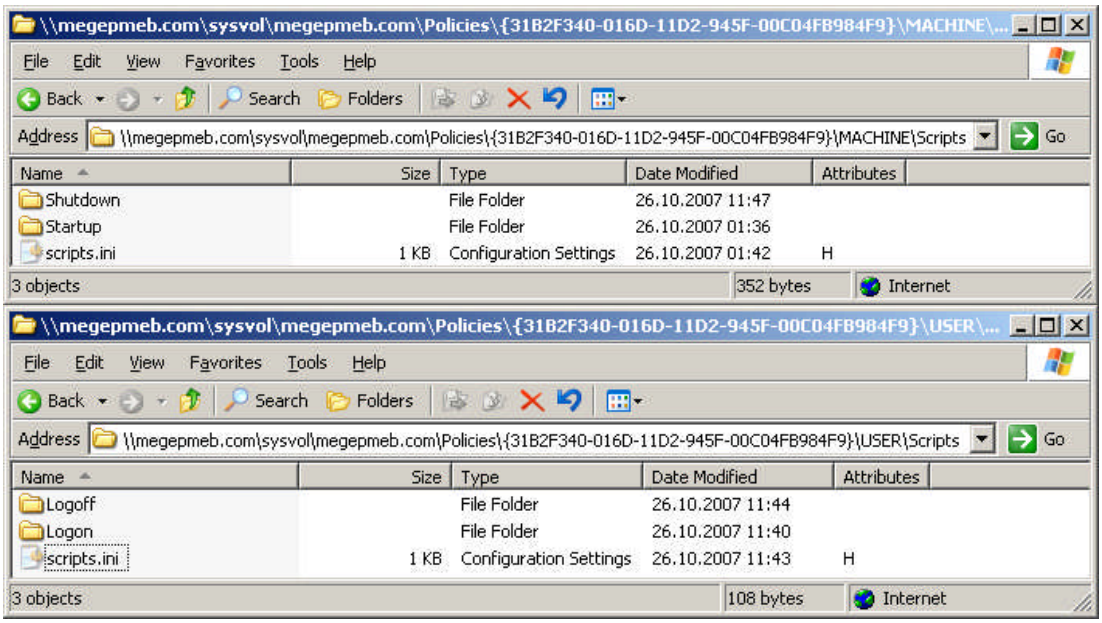
Resim 3.11: Bilgisayarlar için Script tanımlama (Win 2003 Eng ⇔ Win 2003 Tr)

Eğer kod dosyalarını kullanıcılar için uygulamak istiyorsak **Resim 3.12'**deki bölümleri kullanırız. Örneğin kullanıcı oturum açtığında kodların çalışmasını istiyorsak **Resim 3.12'**deki bölümden "Logon" (Oturum Aç) seçeneğini, kullanıcı oturumu kapattığında kodların çalışmasını istiyorsak "Logoff" (Oturum Kapat) seçeneğini kullanmamız gerekir.

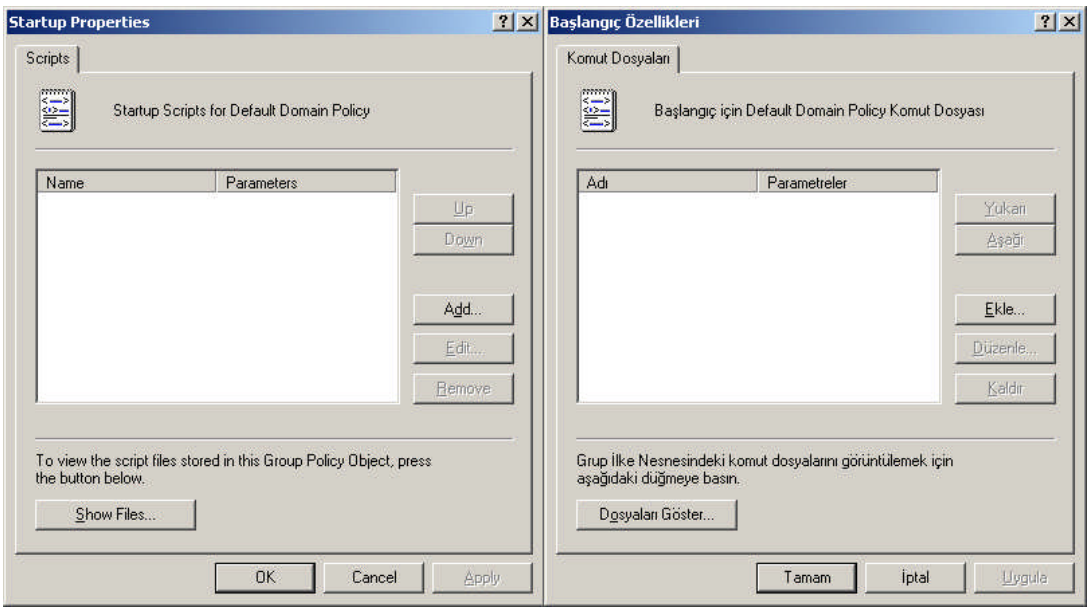


Resim 3.12: Kullanıcılar için Script tanımlama (Win 2003 Eng ⇔ Win 2003 Tr)

Script dosyalarının çalışabileceği bir konum bulunmaktadır. Bu konumlar **Resim 3.13'**te belirtilmiştir. Script dosyalarının bulunacağı bu konumlara erişebilmek için **Resim 3.11** veya **Resim 3.12'**den (Startup, shutdown, Logon, Logoff) herhangi birini çift tıklayıp ilgili seçenek için **Resim 3.14'**teki pencereyi açmamız gerekir.

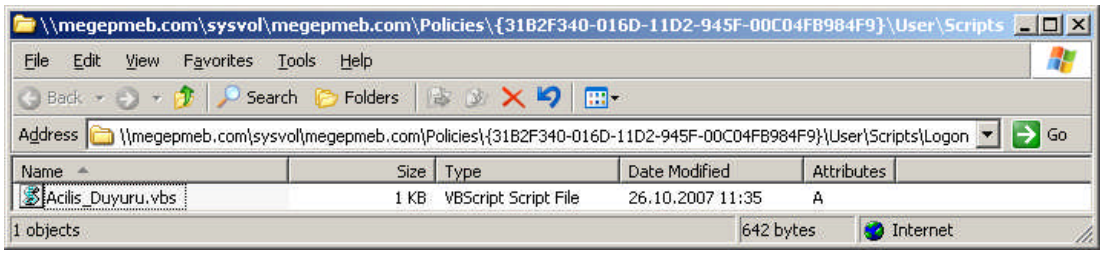


Resim 3.13: Script dosyalarının çalışacağı konumlar

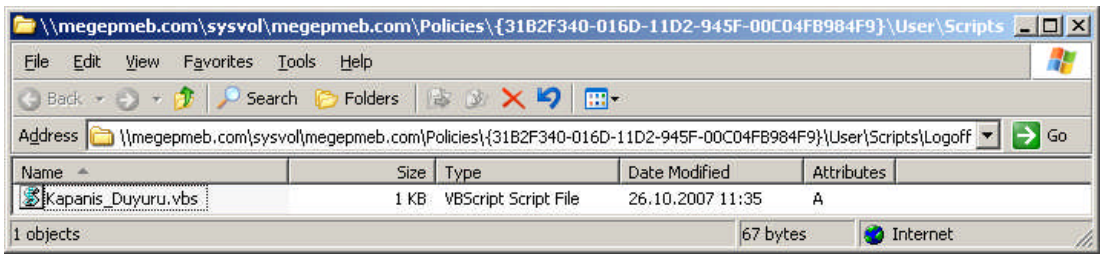


Resim 3.14: Bilgisayarlar için Script tanımlama penceresi (W 2003 Eng ⇔ W 2003 Tr)

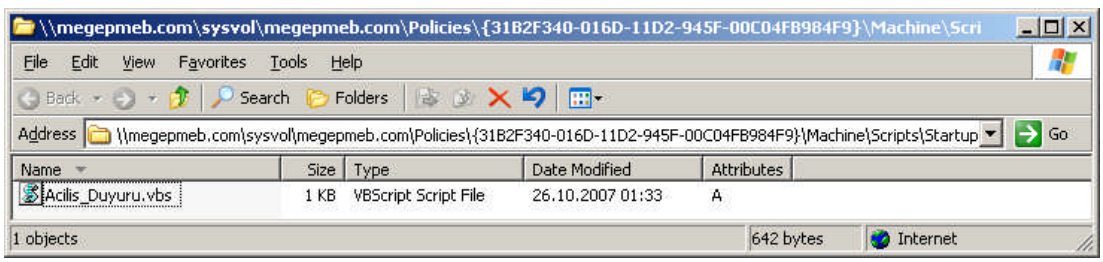
Resim 3.14'teki bu pencere (Startup, shutdown, Logon, Logoff) seçenekleri için ortaktır. Bu pencerenin "Show Files" (Dosyaları göster) butonuna basarsanız **Resim 3.15, Resim 3.16, Resim 3.17** ve **Resim 3.18'**den herhangi biri açılacaktır. Çalıştıracağımız kod dosyasını açılan bu klasörler altına kopyalamamız gerekir.



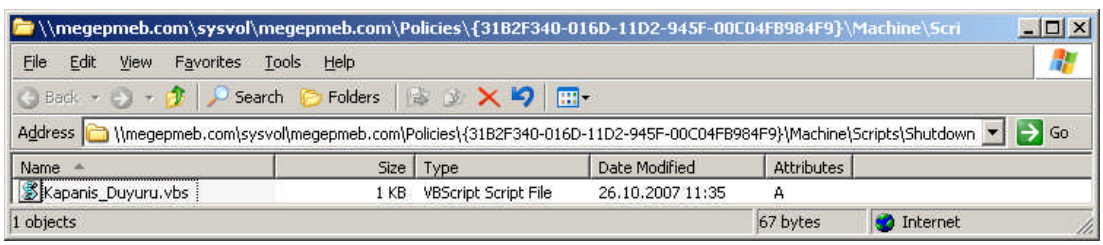
Resim 3.15: Kullanıcıların oturum açılımında Script tanımlayacağımız konum



Resim 3.16: Kullanıcıların oturum kapandığında Script tanımlayacağımız konum



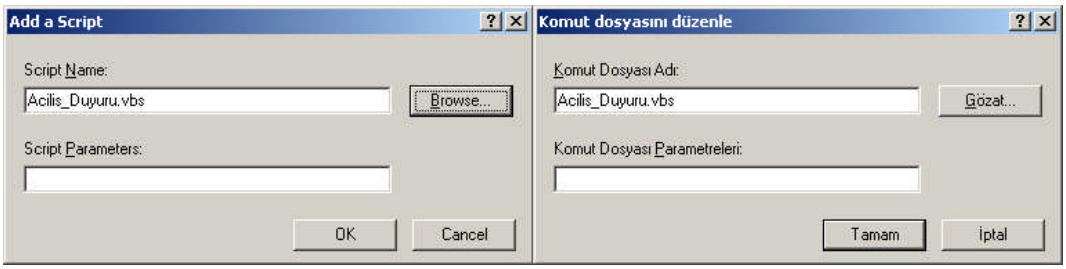
Resim 3.17: Bilgisayar açıldığında Script tanımlayacağımız konum



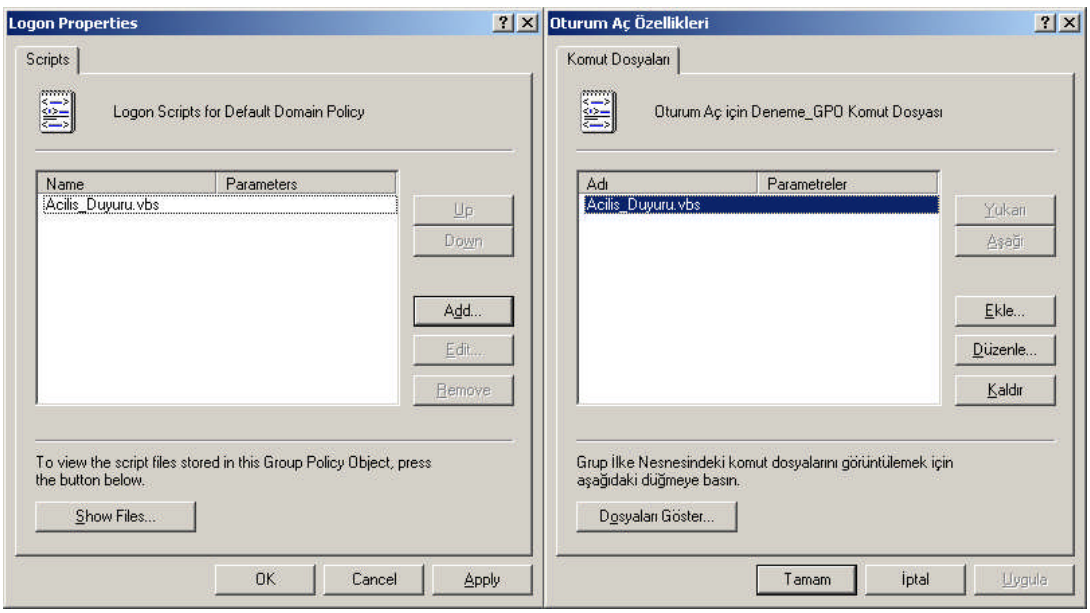
Resim 3.18: Bilgisayar kapandığında Script tanımlayacağımız konum

Kod dosyaları ilgili klasörler altına yerleştirildikten sonra **Resim 3.14'**teki "Add" (Ekle) butonuna basıp **Resim 3.19'**daki pencereyi açmamız gerekir. **Resim 3.19'**daki çalıştırılacak kod dosyasının eklenecek pencereden "Browse" (Gözat) butonuyla klasör içerisindeki dosyalardan birini seçerek (varsa komut parametreleri "script parameters"

(Komut dosyası parametreleri) bölümüne girilerek) “OK” (Tamam) butonuna basmamız gerekir. Komut dosyası ile ilgili parametreler “Script Parameters” (Komut Dosyası Parametreleri) Bu işlemlerden sonra **Resim 3.20’**de olduğu gibi kod dosyası yüklenmiş olur. **Resim 3.20’**deki “OK” (Tamam) butonuna bastığımızda kod çalışır hâle gelmiş olur.



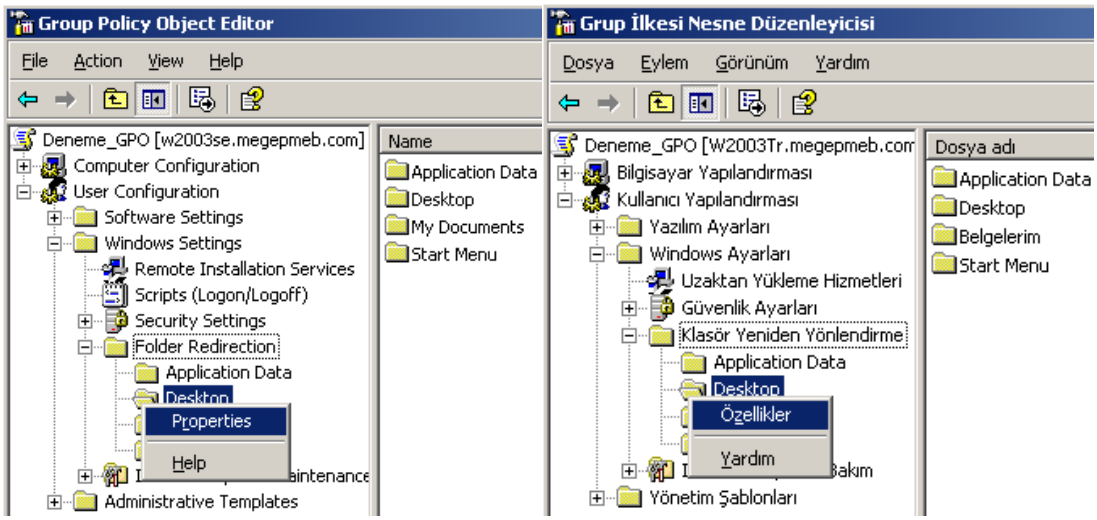
Resim 3.19: Çalıştırılacak kod dosyasının eklenmesi



Resim 3.20: Kullanıcılar için Script tanımlama penceresi (W 2003 Eng ⇔ W 2003 Tr)

3.3. Klasörlerin Yeniden Yönlendirmesini Ayarlama

Kullanıcılarla ilgili kişisel ayarları, dosyaları ve klasörleri merkezî bir ortamda saklanmasını sağlayan sisteme “Folder Redirection” (Klasör yeniden yönlendirme) denir. Bu şekilde önemli verilerin yedeklenmesi daha kolaylaşır. Kullanıcılara ait gezi profil kullanımı azalacağı için ağ trafiği rahatlar ve kullanıcıların oturum açma süreleri kısalır.

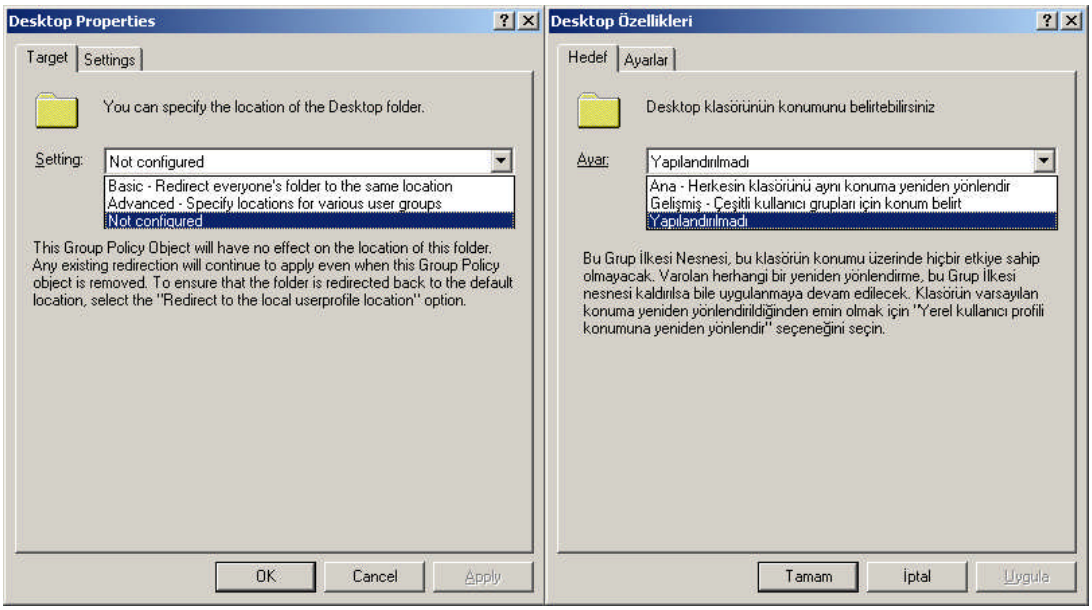


Resim 3.21: Kullanıcılar için klasör yönlendirme penceresi (W 2003 Eng ⇔ W 2003 Tr)

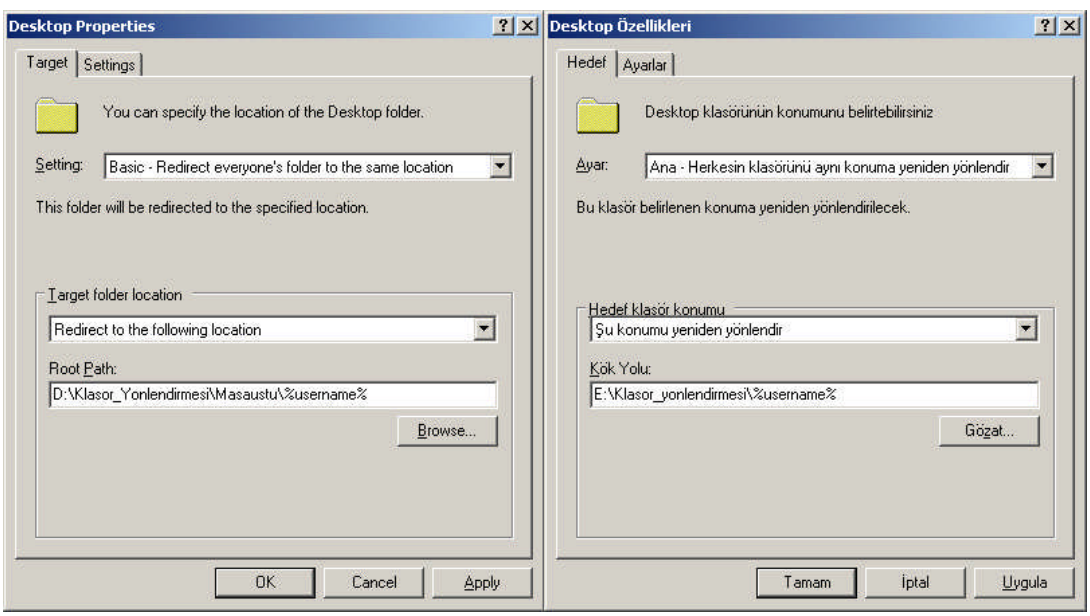
Klasörlerin yönlendirilmesi işlemini yapabileceğimiz dört farklı klasör seçeneği vardır:

- **Application Data (Uygulama program verileri) :** Kullanıcılara ait uygulama programlarının verilerinin yönlendirileceği bölümdür.
- **Desktop (Masaüstü):** Kullanıcılara ait masaüstünde bulunan dosyaların ve klasörlerin yönlendirileceği bölümdür.
- **My Documents (Belgelerim):** Kullanıcılara ait "Belgelerim" klasöründe bulunan dosyaların ve klasörlerin yönlendirileceği bölümdür.
- **Start Menu (Başlangıç menüsü): K**ullanıcılara ait "Başlangıç" menüsünde bulunan kısa yollar ve klasörlerin yönlendirileceği bölümdür.

Yönlendirme işlemleri temelde birbirinin benzeridir. Örnek olarak kullanıcı masaüstü bilgilerini yönlendirmek istersek **Resim 3.21'**deki Grup ilkesi nesne düzenleyicisini ve "user configuration=>Windows Setting=> Folder Redirection" (Kullanıcı Yapılandırması=> Windows Ayarları=>Klasör yeniden yönlendir) seçeneğini açmamız gerekir. "Folder Redirection" (Klasör yeniden yönlendirme) altındaki "Desktop" klasörüne sağ tıklayıp "Properties" (Özellikler) seçeneğini tıkladığımızda **Resim 3.22'**deki Masaüstü yönlendirme özelliklerinin bulunduğu pencere karşımıza gelir. "Basic" (Ana) seçeneği GPO'nun tanımlı olduğu birimlerdeki (Etki alanı, organizasyon birimi gibi) tüm kullanıcılar için aynı yere yönlendirme yapar. "Advanced" (Gelişmiş) seçeneği ise GPO'nun tanımlı olduğu birimlerdeki belirli kullanıcılar için yönlendirme işlemini yapar. Öncelikle "Basic" (Ana) seçeneği seçelim ve **Resim 3.23'**teki pencereden ilgili düzenlemeyi yapalım.



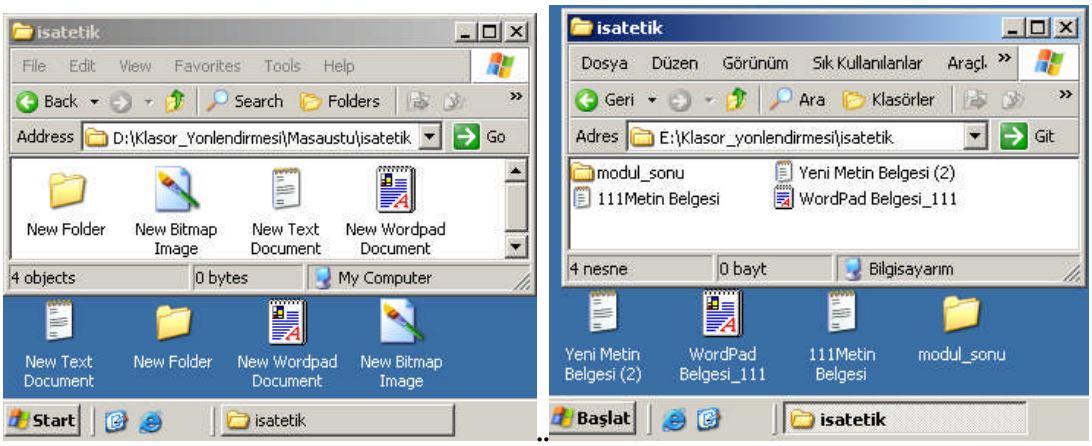
Resim 3.23: Masaüstü yönlendirme özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



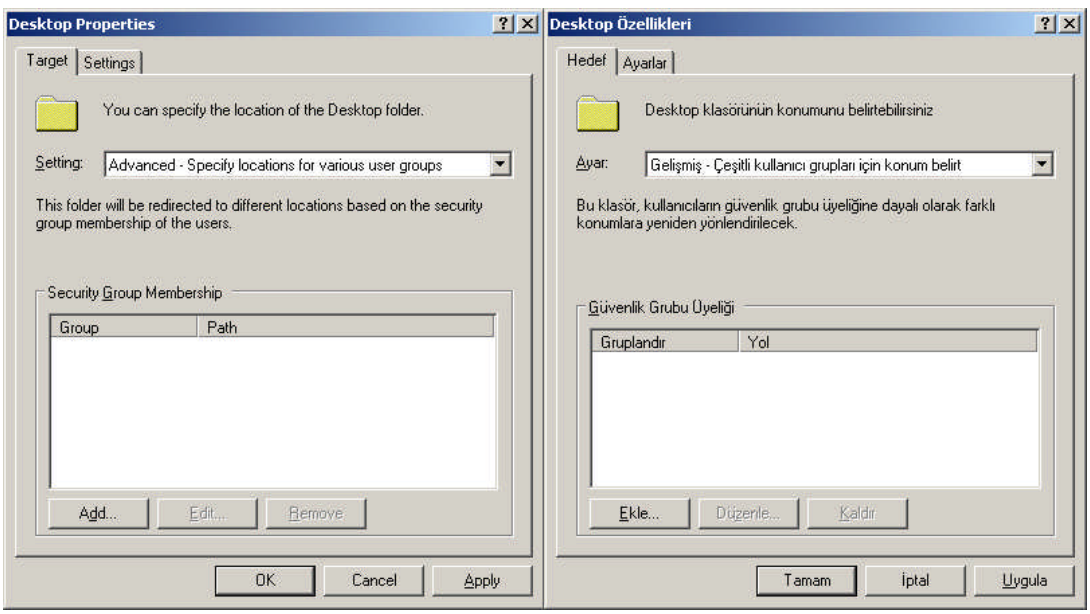
Resim 3.24: Masaüstü yönlendirmesi; hedef klasör konumunun belirlenmesi (Win 2003 Eng ⇔ Win 2003 Tr)

"Basic" (Ana) seçeneği seçtikten sonra **Resim 3.24'**teki pencerede, yönlendirme işlemi yapılacak hedef klasörün konumunu belirlemek gerekir. Biz örneğin sabit disk üzerinde **"D:\Klasor_Yonlendirmesi\Masaustu\%username%"** şeklinde bir yol belirleyelim. Burada **%username%"** ifadesi "her kullanıcının isminde bir klasör oluştur"

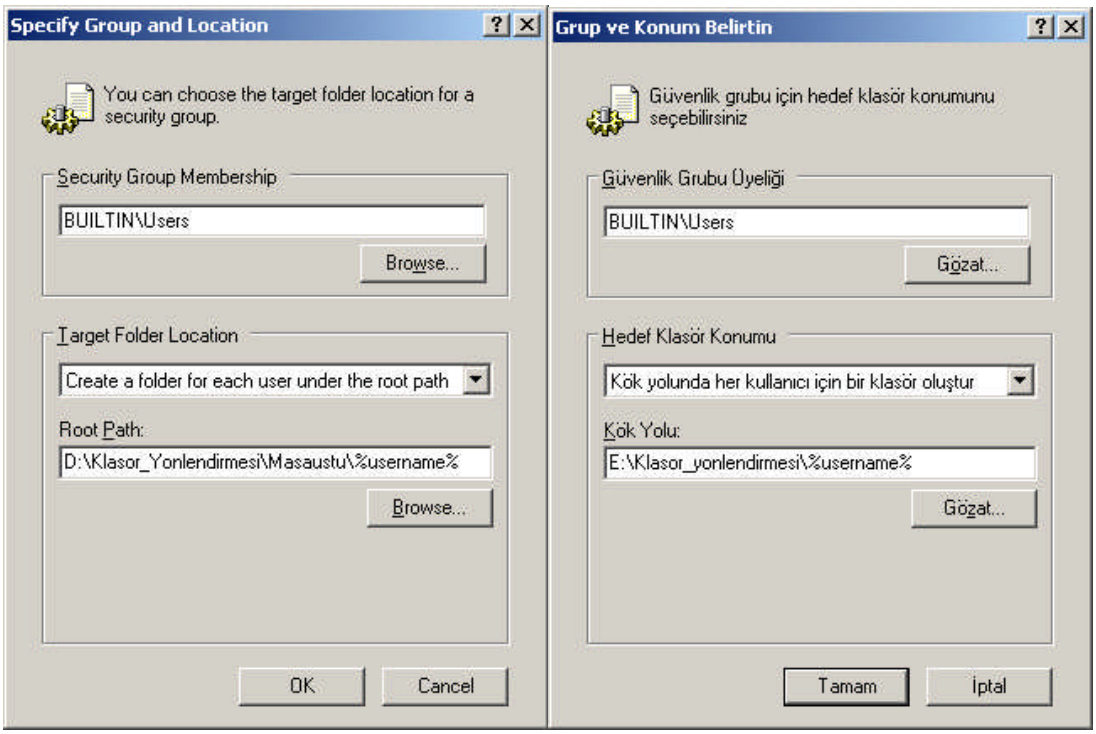
anlamına geliyor. Yani **"Aligel"** isimli bir kullanıcının masaüstünde bulunan dosya ve klasörleri **"D:\Klasor_Yonlendirmesi\Masaustu\ Aligel"** hedef konumuna yönlendirilecektir. Bu şekilde hedef klasör konumu da belirlendikten sonra "OK" (Tamam) butonuna basarsak **Resim 3.25'**teki gibi yönlendirme işlemi tamamlanmış olacaktır.



Resim 3.25: Masaüstü yönlendirilmiş kullanıcı (Win 2003 Eng ⇔ Win 2003 Tr)

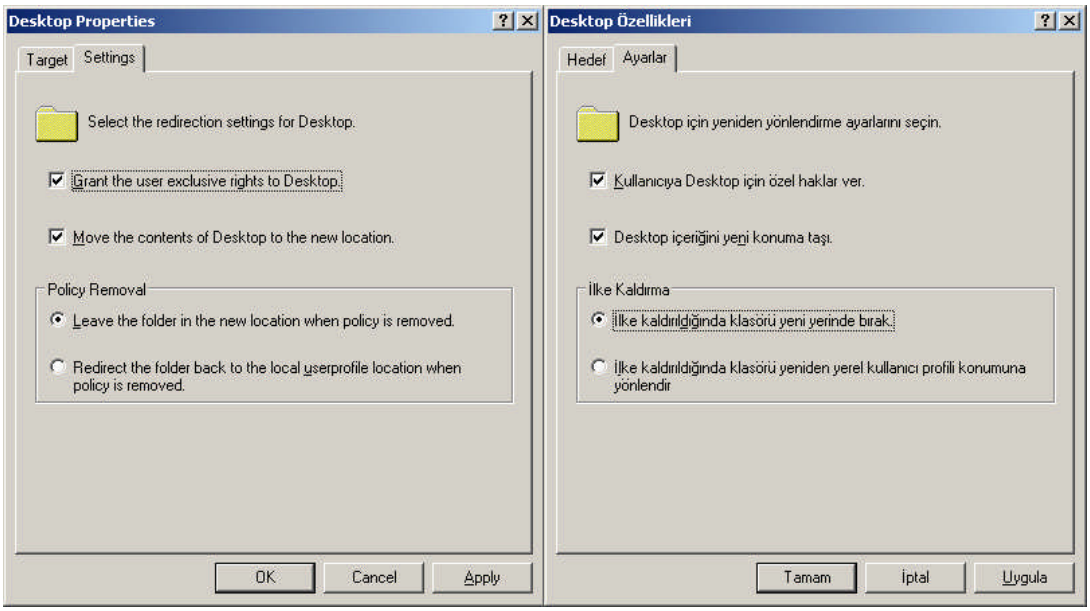


Resim 3.26: Farklı kullanıcılar ve gruplar için masaüstü yönlendirmesi (Win 2003 Eng ⇔ Win 2003 Tr)



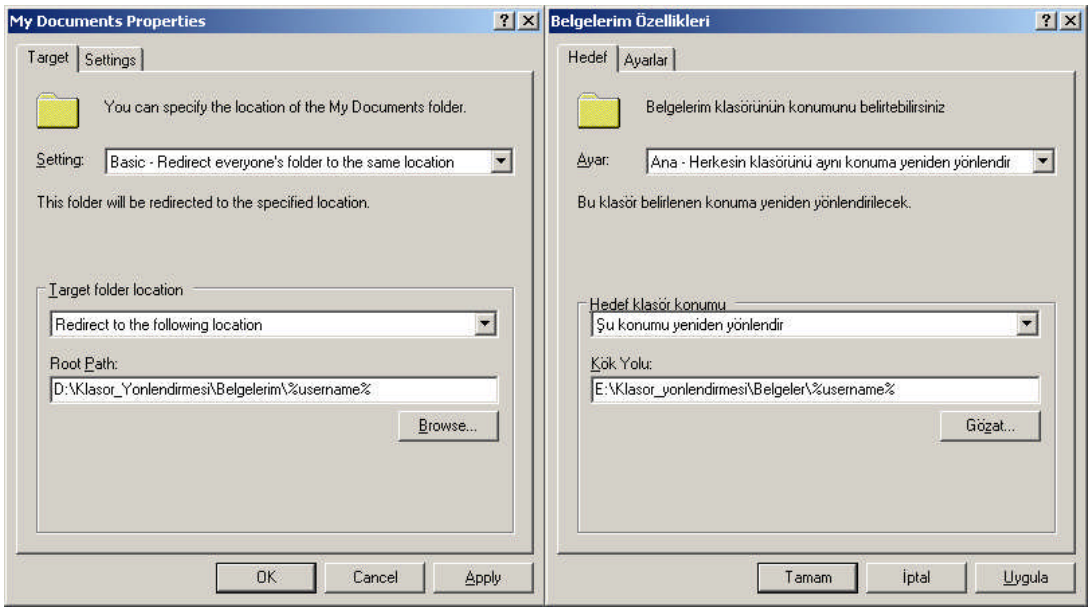
Resim 3.27: Farklı kullanıcılar ve gruplar için hedef klasörün konumu (Win 2003 Eng ⇔ Win 2003 Tr)

Yönlendirme işlemini **Resim 3.26'**daki gibi farklı kullanıcılar ve gruplar için yapmak istiyorsak, "Advanced" (Gelişmiş) seçeneğini seçip **Resim 3.26'**daki pencereden "Add" (Ekle) butonuna basıp **Resim 3.27'**deki pencereyi açmamız gerekir. **Resim 3.27'**deki pencereden "Security Group Membership" (Güvenlik grubu üyeliği) bölümünde "Browse" (Gözat) butonuyla yönlendirme işlemi uygulanacak grup veya kullanıcı seçmemiz gerekir. Target Folder Location" (Hedef klasör konumu) bölümü "Redirect to the Following location" (Şu konumu yeniden yöndendir) şeklinde olmalıdır. En son olarak da yolu belirleyip yönlendirme işlemini tamamlamış oluruz. Klasör yönlendirme işlemi seçenekleri "Target" (Hedef) sekmesinden yapılır. Bir de ek ayarların bulunduğu **Resim 3.28'**deki "Setting" (Ayarlar) sekmesi bulunmaktadır. **Resim 3.28'**deki seçenekler kullanıcıya özel haklar vermeyle, dosya içeriğinin yeni konuma taşınmasıyla ve grup ilkesi kaldırıldığında yönlendirme durumunun ne olacağıyla ilgilidir.

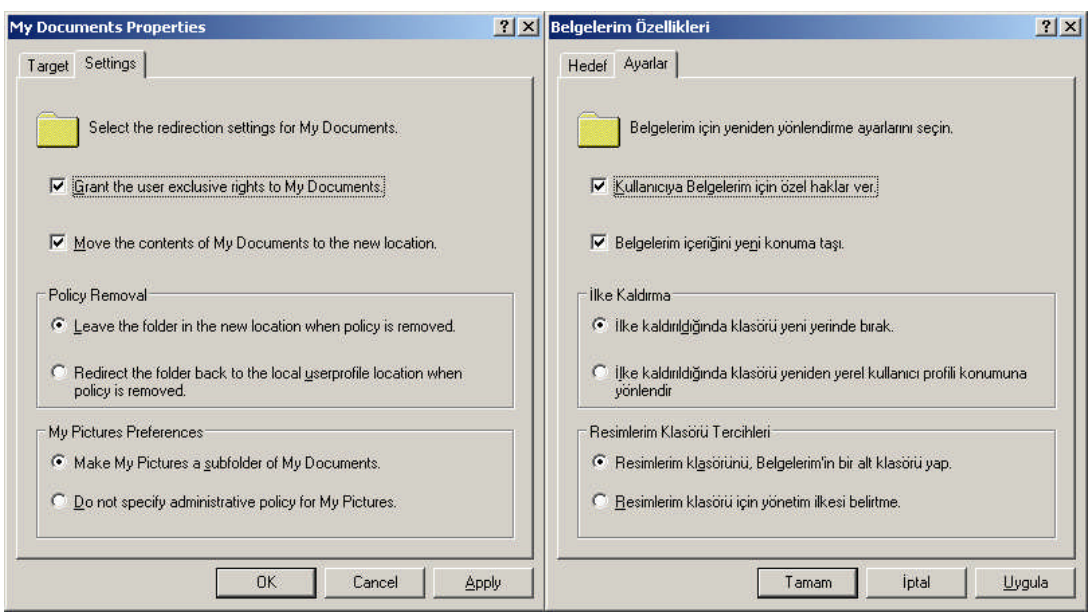


Resim 3.28: Masaüstü yönlendirme ayarları (Win 2003 Eng ⇔ Win 2003 Tr)

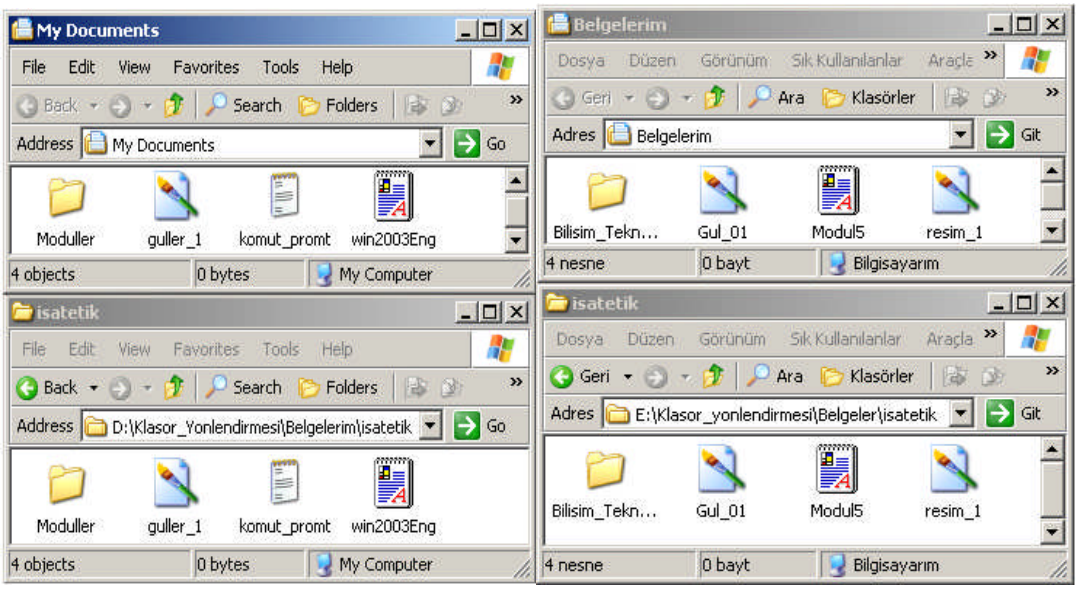
Yönlendirme işlemini kullanıcılara ait "My Documents" (Belgelerim) klasörü için yapmak istersek **Resim 3.21'**deki Grup ilkesi nesne düzenleyicisini açmamız gerekir. "Folder Redirection" (Klasör yeniden yönlendirme) altındaki "My Documents" (Belgelerim) klasörüne sağ tıklayıp "Properties" (Özellikler) seçeneğine tıkladığımızda **Resim 3.29'**daki Belgelerim yönlendirme özelliklerinin bulunduğu pencere karşımıza gelir. "Basic" (Ana) seçeneği seçelim ve **Resim 3.29'**daki pencereden hedef klasör konumunu ve klasör yolunu belirleyelim. Sonrada **Resim 3.30'**daki "Setting" (Ayarlar) sekmesini açalım. Buradaki ayarlar Masaüstü yönlendirme ayarlarından biraz farklıdır. **Resim 3.30'**daki pencereden de uygun ayarlamalar yapıldıktan sonra "OK" (Tamam) butonuna basarsak **Resim 3.31'**deki gibi yönlendirme işlemi tamamlanmış olacaktır.



Resim 3.29: Belgelerim yönlendirme; hedef klasör konumunun belirlenmesi (Win 2003 Eng ⇔ Win 2003 Tr)



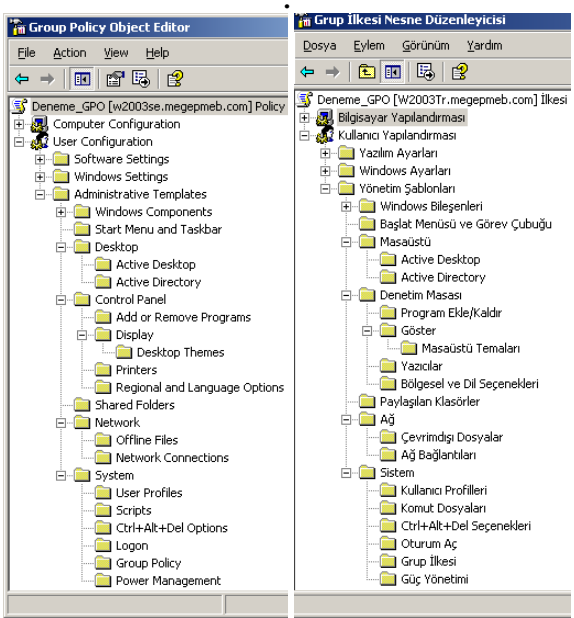
Resim 3.30: Belgelerim yönlendirme ayarları (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 3.31: Belgelerim yönlendirme ayarları (Win 2003 Eng ⇔ Win 2003 Tr)

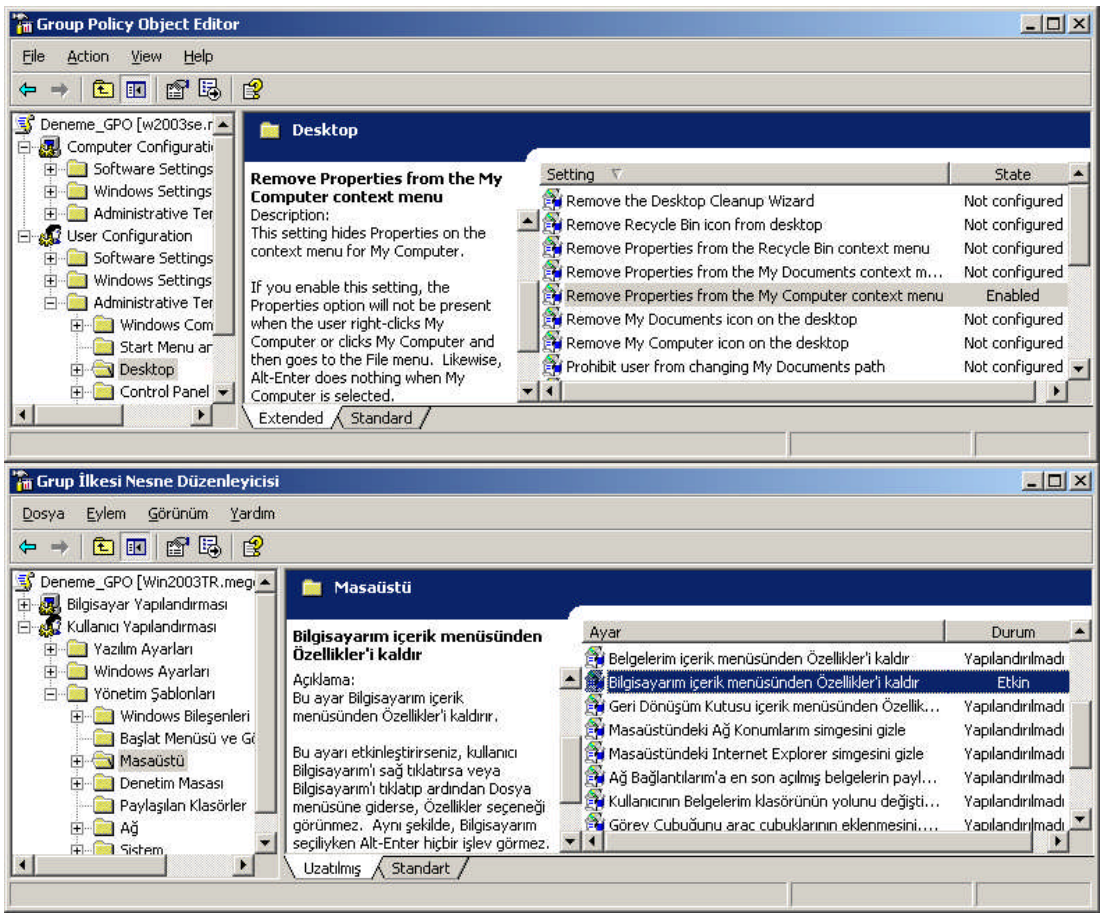
3.4. Uygulamalı GPO' ların Kararını Verme

Grup Politikaları sayesinde kullanıcılara izinsiz işlem yapmaması ya da bilgisayar ayarlarıyla oynamaması gibi birçok yönden müdahale edilebilir. Bu durum güvenlik ve yönetimin verimliliği açısından önemlidir.



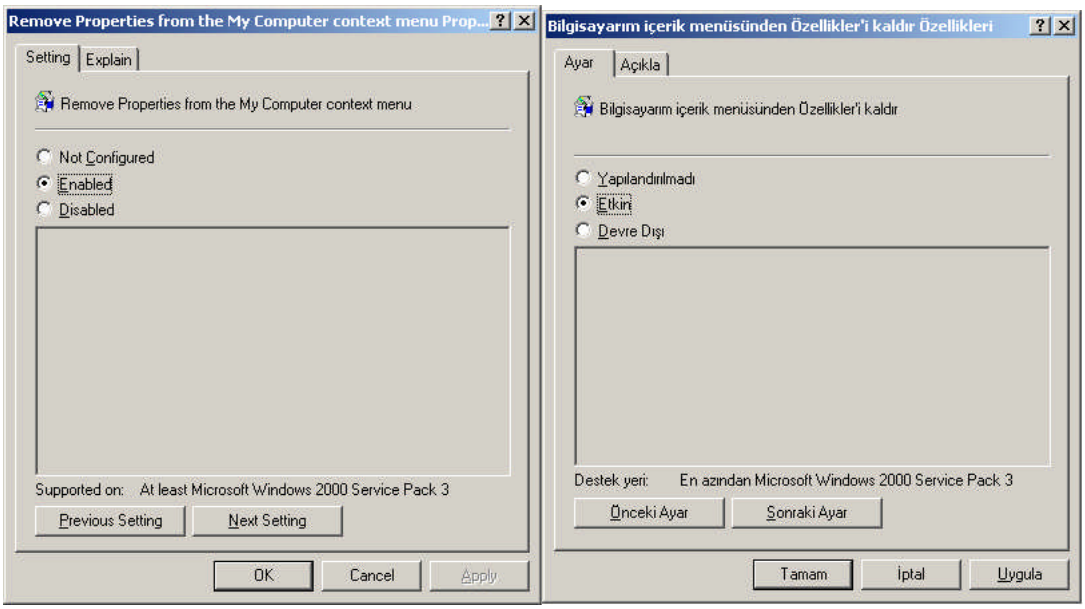
Resim 3.32: Kullanıcılar için yönetim şablonları (Win 2003 Eng ⇔ Win 2003 Tr)

Kullanıcılarla ilgili birçok yönetim kontrolü “Administrative Templates” (Yönetim Şablonları) altında yer almaktadır. Yönetim Şablonları altındaki kullanıcı ayarları **Resim 3.32’**de görülmektedir. Şimdi kullanıcının masaüstü ayarlarıyla ilgili bir örnek yapalım. Kullanıcının masaüstündeki “Bilgisayarım” simgesine sağ tıkladığında normalde özellikler seçeneği görülür ama biz bunu GPO sayesinde kullanıcının bilgisayarım özelliklerine erişememesi için özellikler seçeneğini görünmez yapacağız. Öncelikle **Resim 3.33’**teki GPO düzenleyicisini açalım.

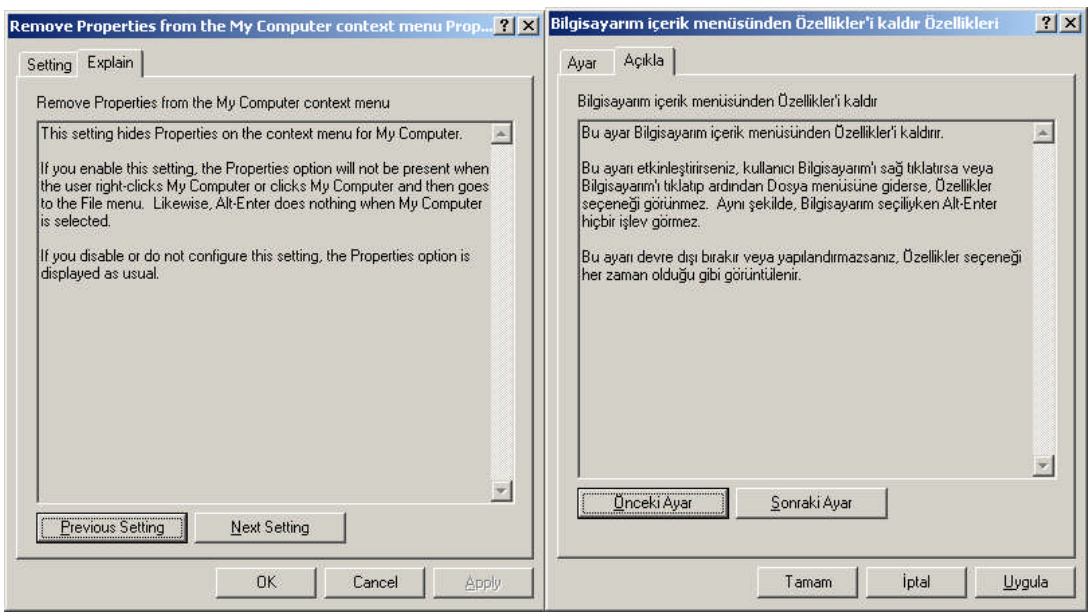


Resim 3.33: Kullanıcılar için GPO düzenleyici (Win 2003 Eng ⇔ Win 2003 Tr)

GPO düzenleyici penceresi üç bölümden oluşur. Sol bölümdeki ağaç yapısında ayar gruplarının başlıkları yer alır. Sağ bölümde seçilen yönetim başlıkları altındaki ayarları görüntüler. Orta bölüm ise seçilen kullanıcı ayarları hakkında gerekli açıklamaları içerir. **Resim 3.33’**teki GPO düzenleyici penceresinde “User Configuration =>Administartive Templates=>Desktop” (Kullanıcı Yapılandırılması =>Yönetim Şablonları =>Masaüstü) bölümünden “Remove Properties from the My Computer context menu” (Bilgisayarım içerik menüsünden Özellikleri kaldır) seçeneğini tıklarsak **Resim 3.34**’teki pencere karşımıza gelir.



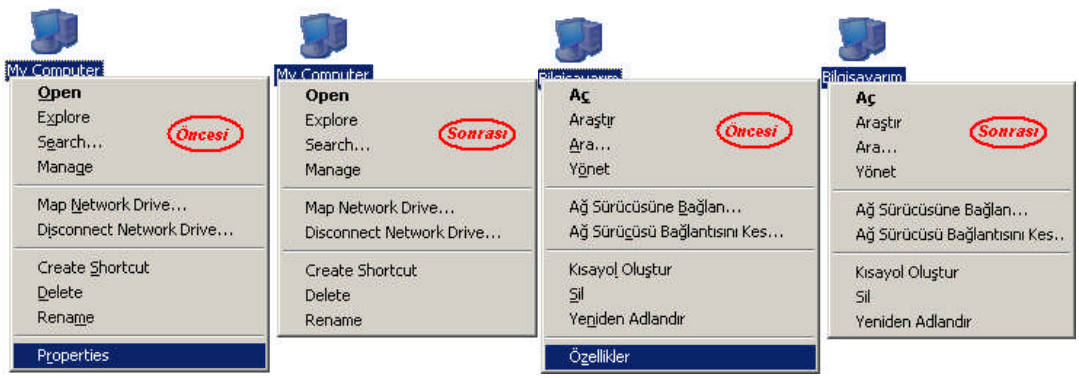
Resim 3.34: Seçilen kullanıcı ayarının etkinleştirilmesi (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 3.35: Seçilen kullanıcı ayarıyla ilgili açıklama (Win 2003 Eng ⇔ Win 2003 Tr)

Seçilen kullanıcı ayarının etkinleştirilmesinde kullanılan **Resim 3.34'**deki bu pencerede üç farklı seçenek vardır. "Not Configured" (Yapılandırılmamış) seçeneğiyle ilgili ayarlamanın kullanıcıya hiçbir etkisi olmaz. "Enabled" (Etkinleştir) seçeneği ile ilgili ayarlama, kullanıcıları etkiler. "Disabled" (Devre dışı) seçeneği ile kullanıcılar ilgili ayarlamadan muaf tutulur. **Resim 3.35'**teki "Explain" (Açıklama) sekmesi ilgili ayarlama

hakkında bilgi verir. **Resim 3.34'**deki pencereden "Enabled" (Etkinleştir) seçeneğini işaretleyip "OK" (Tamam) butonuna bastıktan sonra ayarlamamız GPO' yu ilgili birimdeki (Etki alanı veya Organizasyon birimi) tüm kullanıcılar için uygulanmış olur. **Resim 3.36'** de kullanıcı ayarlaması uygulanmadan önceki durumda özellikler seçeneği görülmekte ama kullanıcı ayarlaması uygulandıktan sonra özellikler seçeneği görülmemektedir. Kullanıcılarla ilgili diğer ayarlamalar da bu şekilde yapılmaktadır.



Resim 3.36: Seçilen kullanıcı ayarının uygulanmış hâli (Win 2003 Eng ⇔ Win 2003 Tr)

Kullanıcılarla ilgili diğer ayarlamalar da bu şekilde yapılmaktadır. Şimdi "Administartive Templates" (Yönetim Şablonları) içerisindeki kullanıcılarla ilgili diğer ayarlamaların bir listesini verelim.

- **Start Menu and Taskbar (Başlat menüsü ve görev çubuğu) ayarları**

Remove user's folders from the Start Menu	⇔	Kullanıcı klasörlerini Başlat menüsünden kaldır
Remove links and access to Windows Update	⇔	Windows Güncelleştirmeye olan bağlantıları ve erişimi kaldır
Remove common program groups from Start Menu	⇔	Başlat menüsünden ortak program gruplarını kaldır
Remove My Documents icon from Start Menu	⇔	Belgelerim simgesini Başlat menüsünden kaldır
Remove Documents menu from Start Menu	⇔	Belgeler menüsünü Başlat menüsünden kaldır
Remove programs on Settings menu	⇔	Ayarlar menüsündeki programlan kaldır
Remove Network Connections from Start Menu	⇔	Başlat Menüsü'nden Ağ Bağlantılarını kaldır
Remove Favorites menu from Start Menu	⇔	Başlat Menüsü'nden Sık Kullanılanlar menüsünü kaldır
Remove Search menu from Start Menu	⇔	Ara menüsünü Başlat menüsünden kaldır
Remove Help menu from Start Menu	⇔	Başlat menüsünden Yardım menüsünü kaldır
Remove Run menu from Start Menu	⇔	Çalıştır menüsünü Başlat menüsünden kaldır

Remove My Pictures icon from Start Menu	⇔	Başlat menüsünden Resimlerimi kaldır
Remove My Music icon from Start Menu	⇔	Müziğim simgesini Başlat menüsünden kaldır
Remove My Network Places icon from Start Menu	⇔	Başlat menüsünden Ağ Bağlantılarını kaldır
Add Logoff to the Start Menu	⇔	Başlat menüsüne Oturumu Kapat'ı Ekle
Remove Logoff on the Start Menu	⇔	Başlat menüsünde Oturum Kapatmayı Kaldır
Remove and prevent access to the Shut Down command	⇔	Oturumu Kapat komutunu kaldır ve erişimi engelle
Remove Drag-and-drop context menus on the Start Menu	⇔	Başlat menüsünde Sürükle ve bırak içerik menülerini kaldır
Prevent changes to Taskbar and Start Menu Settings	⇔	Görev Çubuğu ve Başlat menüsü Ayarlarındaki değişiklikleri engelle
Remove access to the context menus for the taskbar	⇔	Görev çubuğu için içerik menülerini erişimi kaldır
Do not keep history of recently opened documents	⇔	Son açılan belgelerin geçmişini tutma
Clear history of recently opened documents on exit	⇔	Çıkışta son açılan dosyaların geçmişini sil
Turn off personalized menus	⇔	Kişiselleştirilmiş menüleri kapat
Turn off user tracking	⇔	Kullanıcı izlemeyi kapat
Add "Run in Separate Memory Space" check box to Run dialog box	⇔	Çalıştır iletişim kutusuna "Ayrı Bellek Alanında Çalıştır" onay kutusunu ekle
Do not use the search-based method when resolving shell shortcuts	⇔	Kabuk kısa yollarını çözümlerken arama tabanlı yöntemi kullanma
Do not use the tracking-based method when resolving shell shortcuts	⇔	Kabuk kısa yollarını çözümlerken izleme tabanlı yöntemi kullanma
Gray unavailable Windows Installer programs Start Menu shortcuts	⇔	Windows Installer programlan Başlat menüsü kısa yolları kullanılabilir değil
Prevent grouping of taskbar items	⇔	Görev çubuğu öğelerinin gruplandırılmasını engelle
Turn off notification area cleanup	⇔	Bildirim alanı temizlemeyi kapat
Lock the Taskbar	⇔	Görev Çubuğunu Kilitle
Force classic Start Menu	⇔	Klasik Başlat menüsünü uygula
Remove Balloon Tips on Start Menu items	⇔	Başlat menüsü öğelerinde Balon ipuçlarını kaldır
Remove pinned programs list from the Start Menu	⇔	Başlat menüsünden tutturulan programlar listesini kaldır
Remove frequent programs list from the Start Menu	⇔	Sık kullanılan programlar listesini Başlat menüsünden kaldır
Prevent changes to Taskbar and Start Menu Settings	⇔	Başlat menüsünden Tüm Programlar listesini kaldır
Remove access to the context menus for	⇔	Başlat menüsünden "PC'yi Çıkar"

the taskbar		düğmesini kaldır
Do not keep history of recently opened documents	⇔	Başlat menüsünden kullanıcı adını kaldır
Clear history of recently opened documents on exit	⇔	Sistem bildirim alanından Saati kaldır
Turn off personalized menus	⇔	Bildirim alanını gizle
Turn off user tracking	⇔	Görev çubuğunda hiçbir Özel araç çubuğu Görüntüleme
Add "Run in Separate Memory Space" check box to Run dialog box	⇔	Program Erişimi ve Varsayılanları Ayırma simgesini Başlat menüsünden kaldır

- **Desktop (Masaüstü) Ayarları**

Hide and disable all items on the desktop	⇔	Masaüstündeki tüm simgeleri gizle ve devre dışı bırak
Remove My Documents icon on the desktop	⇔	Masaüstündeki Belgelerim simgesini kaldır
Remove My Computer icon on the desktop	⇔	Bilgisayarım simgesini masaüstünden kaldır
Remove Recycle Bin icon from desktop	⇔	Masaüstünden Geri Dönüşüm Kutusunu kaldır
Remove Properties from the My Documents context menu	⇔	Belgelerim içerik menüsünden Özellikleri kaldır
Remove Properties from the My Computer context menu	⇔	Bilgisayarım içerik menüsünden Özellikleri kaldır
Remove Properties from the Recycle Bin context menu	⇔	Geri Dönüşüm Kutusu içerik menüsünden Özellikleri kaldır
Hide My Network Places icon on desktop	⇔	Masaüstündeki Ağ Konumlarım simgesini gizle
Hide Internet Explorer icon on desktop	⇔	Masaüstündeki İnternet Explorer simgesini gizle
Do not add shares of recently opened documents to My Network Places	⇔	Ağ Bağlantılarıma en son açılmış belgelerin paylaşımlarını ekleme
Prohibit user from changing My Documents path	⇔	Kullanıcının Belgelerim klasörünün yolunu değiştirmesini engelle
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	⇔	Görev Çubuğunu araç çubuklarının eklenmesini, sürüklenip bırakılmasını ve kapatılmasını engelle
Prohibit adjusting desktop toolbars	⇔	Masaüstü araç çubuklarının ayarlanmasını yasakla
Don't save settings at exit	⇔	Çıkışta kaydetme
Remove the Desktop Cleanup Wizard	⇔	Masaüstü Temizleme Sihirbazı'nı kaldır
Active Desktop	⇔	***Active Desktop***
Enable Active Desktop	⇔	Active Desktopu Etkinleştir
Disable Active Desktop	⇔	Active Desktop özelliğini devre dışı bırak

Disable all items	⇔	Tüm öğeleri devre dışı bırak
Prohibit changes	⇔	Değişiklikleri yasakla
Prohibit adding items	⇔	Öğelerin eklenmesini engelle
Prohibit deleting items	⇔	Öğelerin silinmesini engelle
Prohibit editing items	⇔	Öğelerin düzenlenmesini engelle
Prohibit closing items	⇔	Öğelerin kapatılmasını engelle
Add/Delete items	⇔	Öğe ekle/sil
Active Desktop Wallpaper	⇔	Active Desktop Duvar Kâğıdı
Allow only bitmapped wallpaper	⇔	Yalnızca bit eşlemli duvar kâğıdına izin ver
Active Directory	⇔	***Active Directory***
Maximum size of Active Directory searches"	⇔	Active Directory aramalarının en büyük boyutu
Enable filter in Find dialog box"	⇔	Bul iletişim kutusundaki süzgeci etkinleştir
Hide Active Directory folder"	⇔	Active Directory klasörünü gizle

- **Control Panel (Denetim Masası) ayarları**

Prohibit access to the Control Panel	⇔	Denetim Masasına erişimi yasakla
Hide specified Control Panel applets	⇔	Belirlenen denetim masası uygulamalarını gizle
Show only specified Control Panel applets	⇔	Yalnızca belirtilen denetim masası uygulamalarını göster
Force classic Control Panel Style	⇔	Klasik Denetim Masası Stilini uygula
Add or Remove Programs	⇔	***Program Ekle/Kaldır***
Remove Add or Remove Programs	⇔	Program Ekle/Kaldırı Kaldır
Hide Change or Remove Programs page	⇔	Programlan Değiştir veya Kaldır sayfasını Gizle
Hide Add New Programs page	⇔	Yeni Program Ekle sayfasını gizle
Hide Add/Remove Windows Components page	⇔	Windows Bileşenlerini Ekle/Kaldır sayfasını gizle
Hide the Set Program Access and Defaults page	⇔	Program Erişimi ve Varsayılanları Ayarla sayfasını gizle
Hide the "Add a program from CD-ROM or floppy disk" option	⇔	" CD-ROM ya da disketten program ekle" seçeneğini gizle
Hide the "Add programs from Microsoft" option	⇔	" Microsoft'tan program ekle" seçeneğini gizle
Hide the "Add programs from your network" option	⇔	"Kendi Ağından program ekle" seçeneğini gizle
Go directly to Components Wizard	⇔	Doğrudan Bileşenler sihirbazına git
Remove Support Information	⇔	Destek Bilgilerini Kaldır
Specify default category for Add New Programs	⇔	Yeni Programlar Ekle için varsayılan kategoriyi belirle
Display	⇔	***Göster***
Remove Display in Control Panel	⇔	Denetim Masasında görüntüyü kaldır

Hide Desktop tab	⇔	Masaüstü Sekmesini gizle
Prevent changing wallpaper	⇔	Duvar kâğıdı değiştirmeyi engelle
Hide Appearance and Themes tab	⇔	Görünüm ve Temalar sekmesini gizle
Hide Settings tab	⇔	Ayarlar sekmesini gizle
Hide Screen Saver tab	⇔	Ekran Koruyucu sekmesini gizle
Screen Saver	⇔	Ekran Koruyucusu
Screen Saver executable name	⇔	Ekran Koruyucusu çalıştırılabilir adı
Password protect the screen saver	⇔	Ekran Koruyucusunu parolayla koru
Screen Saver timeout	⇔	Ekran Koruyucu zaman aşımı
Desktop Themes	⇔	***Masaüstü Temaları***
Remove Theme option	⇔	Temayı Kaldır seçeneği
Prevent selection of windows and buttons styles	⇔	Pencere ve düğme stilleri seçimini engelle
Prohibit selection of font size	⇔	Yazı tipi boyutu seçimini önle
Prohibit Theme color selection	⇔	Tema rengi seçimini önle
Load a specific visual style file or force Windows Classic	⇔	Belirli bir Görsel stil dosyası yükle veya Windows Klasik kullanmaya zorla
Printers	⇔	***Yazıcılar***
Printers Browse a common web site to find printers	⇔	Yazıcı bulmak için ortak bir web sitesine gözat
Browse the network to find printers	⇔	Yazıcı bulmak için ağa gözat
Default Active Directory path when searching for printers	⇔	Yazıcıları ararken kullanılacak Varsayılan Active Directory yolu
Point and Print Restrictions	⇔	İşaretle ve Yazdır Sınırlamaları
Prevent addition of printers	⇔	Yazıcı eklenmesini engelle
Prevent deletion of printers	⇔	Yazıcıların silinmesini engelle
Regional and Language Options	⇔	***Bölgesel Seçenekler ve Dil Seçenekleri***
Restrict selection of Windows menus and dialogs language	⇔	Windows menülerinin ve iletişim kutusu dilinin seçimini sınırla
Shared Folders	⇔	***Paylaşılan klasörler***
Allow shared folders to be published	⇔	Paylaşılan klasörlerin yayımlanmasına izin ver
Allow DFS roots to be published	⇔	DFS köklerinin yayımlanmasına izin ver

- **Network (Ağ) Ayarları**

Offline Files	⇔	***Çevrim dışı Dosyalar***
Prohibit user configuration of Offline Files	⇔	Çevrim dışı dosyaların kullanıcı tarafından yapılandırılmasını yasaklar
Synchronize all offline files when logging on	⇔	Oturum açarken tüm çevrim dışı dosyaları eşitle
Synchronize all offline files before logging off	⇔	Oturumu kapatmadan önce tüm çevrim dışı dosyaları eşitle
Synchronize offline files before suspend	⇔	Askıya almadan önce çevrimdışı dosyaları

		eşitle
Action on server disconnect	⇔	Sunucu bağlantısı kesildiğinde gerçekleştirilecek eylem
Non-default server disconnect actions	⇔	Varsayılan dışındaki sunucu bağlantısı kesme eylemleri
Remove 'Make Available Offline'	⇔	“Çevrim dışı Kullan”ı Kaldır
Prevent use of Offline Files folder	⇔	Çevrim dışı Dosyalar klasörünün kullanımını engelle
Administratively assigned offline files	⇔	Yönetici tarafından atanmış çevrimdışı dosyalar
Turn off reminder balloons	⇔	Anımsatma balonlarını kapat
Reminder balloon frequency	⇔	Anımsatma balonunun sıklığı
Initial reminder balloon lifetime	⇔	İlk anımsatma balonunun ömrü
Reminder balloon lifetime	⇔	Anımsatma balonu ömrü
Event logging level	⇔	Olay günlüğüne alma düzeyi
Prohibit 'Make Available Offline' for these file and folders	⇔	Bu klasör ve dosyalar için “Çevrim dışı Kullan”ı engelle
Do not automatically make redirected folders available offline	⇔	Yeniden yönlendirilmiş klasörleri otomatik olarak çevrim dışı kullanılabilir yapma
Network Connections	⇔	***Ağ Bağlantıları***
Ability to rename LAN connections or remote access connections available to all users	⇔	LAN bağlantılarını veya uzaktan erişim bağlantılarını yeniden adlandırabilme tüm kullanıcılar tarafından kullanılabilir
Prohibit access to properties of components of a LAN connection	⇔	Bir yerel ağ bağlantısı bileşenlerinin özelliklerine erişimi yasakla
Prohibit access to properties of components of a remote access connection	⇔	Bir uzak erişim bağlantısı bileşenlerinin özelliklerine erişimi yasakla
Prohibit TCP/IP advanced configuration	⇔	TCP/IP gelişmiş yapılandırmasını engelle
Prohibit access to the Advanced Settings item on the Advanced menu	⇔	Gelişmiş menüsünde Gelişmiş Ayarlar öğesine erişimi engelle
Prohibit adding and removing components for a LAN or remote access connection	⇔	LAN veya uzaktan erişim bağlantısı için bileşen ekleme ve kaldırmayı engelle
Prohibit access to properties of a LAN connection	⇔	Bir yerel ağ bağlantısının özelliklerine erişimi yasakla
Prohibit Enabling/Disabling components of a LAN connection	⇔	LAN bağlantısı bileşenlerini Etkinleştirmeyi/Devre Dışı Bırakmayı engelle
Ability to change properties of an all user remote access connection	⇔	Tüm kullanıcı uzaktan erişim bağlantısının özelliklerini değiştirebilme
Prohibit changing properties of a private remote access connection	⇔	Özel uzaktan erişim bağlantısının özelliklerini değiştirmeyi engelle
Prohibit deletion of remote access connections	⇔	Uzaktan erişim bağlantılarının silinmesini engelle

Ability to delete all user remote access connections	⇔	Tüm kullanıcı uzaktan erişim bağlantılarını silebilme
Prohibit connecting and disconnecting a remote access connection	⇔	Uzaktan erişim bağlantısına bağlanmayı ve bağlantıyı kesmeyi engelle
Ability to Enable/Disable a LAN connection	⇔	LAN bağlantılarını Etkinleştirebilme/Devre Dışı Bırakabilme
Prohibit access to the New Connection Wizard	⇔	Yeni Bağlantı Sihirbazına erişimi engelle
Ability to rename LAN connections	⇔	LAN bağlantılarını yeniden adlandırabilme
Ability to rename all user remote access connections	⇔	Tüm kullanıcı uzaktan erişim bağlantılarını yeniden adlandırabilme
Prohibit renaming private remote access connections	⇔	Özel uzaktan erişim bağlantılarını yeniden adlandırmayı engelle
Prohibit access to the Remote Access Preferences item on the Advanced menu	⇔	Gelişmiş menüsünde Uzaktan Erişim Tercihleri öğesine erişimi engelle
Prohibit viewing of status for an active connection	⇔	Etkin bir bağlantının durumunu görüntülemeyi engelle
Enable Windows 2000 Network Connections settings for Administrators	⇔	Windows 2000 Ağ Bağlantıları ayarlarını Yöneticiler için etkinleştir

- **System (sistem) ayarları**

Don't display the Getting Started welcome screen at logon	⇔	Açılışa Başlarken ekranını görüntüleme
Century interpretation for Year 2000	⇔	2000 Yılı Yüzyıl yorumu
Gonfigure driver search locations	⇔	Sürücü arama konumlarını yapılandır
Code signing for device drivers	⇔	Aygıt sürücüleri için kod imzalama
Gustom user interface	⇔	Özel kullanıcı ara birimi
Prevent access to the command prompt	⇔	Komut satırına erişimi engelle
Prevent access to registry editing tools	⇔	Kayıt Defteri düzenleme araçlarına erişimi engelle
Run only allowed Windows applications	⇔	Yalnızca izin verilen Windows uygulamasını çalıştır
Don't run specified Windows applications	⇔	Belirlenen Windows uygulamalarını çalıştırma
Turn off Autoplay	⇔	Otomatik çalıştır Özelliğini kapat
Restrict these programs from being launched from Help	⇔	Bu programların Yardım'dan çalıştırılmasına izin verme
Download missing CÖM components	⇔	Eksik COM bileşenlerini yükle
Windows Automatic Updates	⇔	Windows Otomatik Güncelleştirmesi
User Profiles	⇔	***Kullanıcı Profilleri***
Connect home directory to root of the share	⇔	Ana dizini paylaşımın köküne bağla
Limit profile size	⇔	Profil boyutunu sınırla

Exclude directories in roaming profile	⇔	Gezici profildeki dizinleri çıkar
Scripts	⇔	***Komut Dosyaları***
Run logon scripts synchronously	⇔	Oturum açma komut dosyalarını eş zamanlı olarak çalıştır
Run legacy logon scripts hidden	⇔	Eski oturum açma komut dosyalarını saklı çalıştır
Run logon scripts visible	⇔	Oturum açma komut dosyalarını görünür olarak çalıştır
Run logoff scripts visible	⇔	Oturum kapatma komut dosyalarını görünür olarak çalıştır
Ctrl+Alt+Del Options	⇔	***Ctrl+Alt+Del Seçenekleri***
Remove Task Manager	⇔	Oturum açma komut dosyalarını eş zamanlı olarak çalıştır
Remove Lock Computer	⇔	Eski oturum açma komut dosyalarını saklı çalıştır
Remove Change Password	⇔	Oturum açma komut dosyalarını görünür olarak çalıştır
Remove Logoff	⇔	Oturum kapatma komut dosyalarını görünür olarak çalıştır
Logon	⇔	***Oturum Aç***
Run these programs at user logon	⇔	Kullanıcı oturumu sırasında bu programları çalıştır
Do not process the run önce list	⇔	Bir kez çalıştır listesini işletme
Do not process the legacy run list	⇔	Bilinen çalıştırma listesini işletme
Group Policy	⇔	***Grup İlkesi***
Group Policy refresh interval for users	⇔	Kullanıcılar için Grup İlkesi yenileme aralığı
Group Policy slow link detection	⇔	Grup İlkesi yavaş bağlantı algılama
Group Policy domain controller selection	⇔	Grup İlkesi etki alanı denetleyicisi seçimi
Create new Group Policy object links disabled by default	⇔	Varsayılan değer olarak devre dışı bırakılmış yeni Grup İlkesi Nesnesi bağlantısı oluştur
Default name for new Group Policy objects	⇔	Yeni Grup İlkesi nesneleri için varsayılan ad
Enforce Show Policies Only	⇔	Yalnızca ilkeleri Göstermeyi Zorla
Turn off automatic update of ADM files	⇔	ADM dosyalarının otomatik güncelleştirilmesini kapat
Disallow Interactive Users from generating Resultant Set of Policy data	⇔	Etkileşimli kullanıcıların İlke Sonuç Kümesi verileri oluşturmalarına izin verme
Power Management	⇔	***Güç Yönetimi***
Prompt for password on resume from hibernate / suspend	⇔	Hazırda bekleme / askıya alma durumundan devam edilirken parola sor

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Oluşturacağımız **"kullanıcılar_1"** isimli organizasyon birimi içerisine **"ozel_GPO"** isimli bir Grup politikası oluşturup bu Grup politikasına kullanıcıların oturum açtıklarında "Hoş geldiniz"; oturumu kapattıklarında "Güle güle" mesajını veren bir Script ekleyiniz.	➢ Organizasyon birimi ve Grup politikası isimlerine, Grup politikasının nasıl bir işlem yapacağına dikkat ediniz.
➢ Oluşturacağımız **"kullanıcılar_2"** isimli organizasyon birimi için **"GPO_KY",** isminde bir politikası oluşturup bu GPO kullanan kullanıcıların Belgelerim içeriğini "d:\yedek\belgeler" hedef klasörü içerisinde her kullanıcının kendi adına açılmış klasörler altında yönlendirilmesi işlemini gerçekleştiriniz.	➢ Organizasyon birimi ve GPO ismine, Grup politikalarının kullanıcılara nasıl bir etki yapacağına dikkat ediniz.
➢ **"kullanıcılar_2"** isimli organizasyon birimi içerisinde oluşturacağımız **"user_1" , "user_2"** ve **"user_3"** kullanıcılarından yalnız **"user_2"** ve **"user_3"** kullanıcılarının masaüstü dosyalarını **"d:\yedek\Desktop"** hedef klasörü içerisinde her kullanıcının kendi adına açılmış klasörler altına yönlendirilmesi işlemini gerçekleştiriniz.	➢ Organizasyon birimi ve kullanıcı isimlerine, Grup politikalarının kullanıcılara nasıl bir etki yapacağına dikkat ediniz.
➢ **"kullanıcılar_3"** isimli organizasyon birimi içerisinde tüm kullanıcıların başlat menülerinden Ara, Çalıştır ve yardım seçeneklerini kaldıran **"GPO_KA",** isminde bir Grup politikası oluşturunuz.	➢ Organizasyon birimi ve GPO isimlerine, Grup politikalarının kullanıcılara nasıl bir etki yapacağına dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorularda doğru seçenekleri işaretleyiniz.

1. Etki alanındaki bilgisayarlara otomatik olarak yazılım yüklemek için kullanılan GPO seçeneği aşağıdakilerden hangisidir?

A) Systems Settings **B)** Windows Settings **C)** Administrative Templates
D) Software Settings **E)** Security Setting

2. Kullanıcı profilleri, komut dosyaları, oturum açma, uzaktan yardım, disk sınırları, grup ilkeleri gibi yönetim ayarlarının yapıldığı GPO seçeneği aşağıdakilerden hangisidir?

A) Windows Components **B)** Systems **C)** Desktop
D) Administrative Templates **E)** Script

3. Aşağıdaki GPO alt ayar gruplarından hangisi **Windows Settings (Windows Ayarları)** altında **yer almaz?**

A) Folder Redirection **B)** Script **C)** Remote installation services
D) Security Setting **E)** Software Settings

4. Aşağıda dosya uzantıları verilen kod dosyalarından hangisi GPO tarafından sistem açılış veya kapanışlarında **kullanılamaz?**

A) VBS **B)** BAT **C)** DLL **D)** JS **E)** COM

5. Bir kod dosyasının kullanıcı oturum açtığında çalışabilmesi için hangi klasör altında olması gerekir?

A) Logon **B)** Startup **C)** Shutdown **D)** Logoff **E)** Logstart

6. "Oturumu Kapat komutunu kaldır ve erişimi engelle" işlemi GPO ayarlarından hangi alt gruba girer.

A) Desktop **B)** Power Management
C) Start menu and Taskbar **D)** System **E)** Control Panel

7. "Yazıcı eklenmesini engelle" işlemi GPO ayarlarından hangi alt gruba girer?

A) Desktop **B)** Control Panel **C)** System
D) Network **E)** Start menu and Taskbar

8. Aşağıdaki **"Administrative Templates"** altındaki kullanıcı ayarlarından hangisi "**system"** alt ayar grubu içinde yer almaz?

A) Scripts **B)** User Profiles **C)** Ctrl+Alt+Del Options
D) Printers **E)** Group Policy

9. Aşağıdaki klasör yönlendirme seçeneklerinden hangisi bir organizasyon biriminde sistemin yalnızca seçilen kullanıcılar için kullanılmasını sağlar?

A) Advanced **B)** Basic **C)** Selections
D) Multiple **E)** Redirect

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları, faaliyete geri dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-4

AMAÇ

Hesapları ve kaynakları yönetebileceksiniz.

ARAŞTIRMA

- Sunucu işletim sistemlerinde güvenlik gereksinimlerinin neler olduğunu araştırınız.
- Güvenlik şablonlarının ne olduğunu ve nasıl kullanıldığını araştırınız
- Bilgisayar güvenlik politikalarının ne olduğunu ve nasıl oluşturulduğunu araştırınız
- Sunucu işletim sistemlerinde güvenlik kayıtlarının nasıl yapıldığını araştırınız

4. HESAPLARI VE KAYNAKLARI DENETLEME

4.1. Sunucu İşletim Sisteminde Güvenlik

Bir şirket ya da kuruluş için ticari sırların önemli olması sebebiyle şirket kayıtları ve bilgisayar verileri de bir o kadar hayati değere sahiptir. Şirket bilgisayarlarındaki verilerin herhangi bir şekilde bilgisayar korsanlarının eline geçmesi ya da herhangi bir virüs programlarıyla tahrip edilmesi, o şirketi büyük bir zarara uğratacaktır. Bilgisayar verilerinin çok önemli olduğu günümüzde, güvenli bilgisayarların gerekliliği yanında her yönüyle güçlü ve güvenli işletim sistemlerine de ihtiyaç duyulmaktadır. Ağ üzerindeki tüm bilgisayar ve kullanıcıları, kontrol edebilen sunucu işletim sistemleri, büyük şirketlerin bu ihtiyaçlarını karşılamak için geliştirilmiştir. Daha önceki etkinliklerde öğrendiğiniz kullanıcı haklarını sınırlama ve izinlerini düzenleme işlemleri ile kullanıcılar denetim altına alınmaktadır. Ayrıca sistem giriş çıkışları kontrol edilip sisteme izinsiz giriş çıkış önlenmekte, veri kaybı veya veri hırsızlığının önüne geçilebilmektedir.

Windows tabanlı sunucu işletim sistemlerinde bilgisayar güvenliğini sağlamak için bazı noktalara dikkat edilmesi gereklidir:

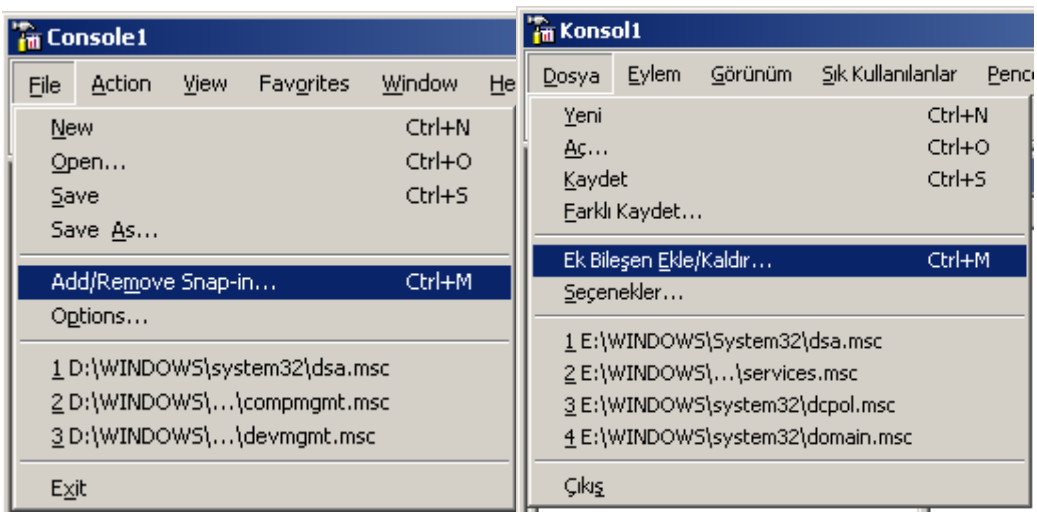
- **Sunucu işletim sisteminizi belirli aralıklarla güncelleştirin:** Sunucu işletim sistemi geliştirici firmalar, ortaya çıkan güvenlik açıklarını kapatmak için İnternet üzerinden bağlantı yaparak otomatik veya manuel güncelleme işlemleri gerçekleştirebilirler. Bununla birlikte iletim sistemi kullanıcılarına belirli

güvenlik politikalarını içeren servis paketleri sunarlar. Sunulan bu paketlerin sisteme dâhil edilerek sürekli güncel kalması gereklidir.

- **Sistem güvenliğiyle ilgili haberleri takip etmek:** İşletim sistemi üreticilerinin veya antivirüs üreticilerinin sisteme yönelik tehditlere karşı İnternetten yayınladıkları haberleri takip edip gerekli önlemleri almak gerekir. Bu sayede ilerde çıkabilecek zorluklara karşı tedbir almış oluruz.
- **Güncel virüs koruma programlarının kullanılması:** Virüslerin sistem verilerine zarar vermemesi için etili virüs koruma programları kullanılmalı ve son çıkan virüslere karşı etkili olabilmesi için belirli periyotlarla güncelleştirilmelidir.
- **Belirli periyotlarla sistem yedeğinin alınması:** Sistem güvenliğinin bir yönü de veri kayıplarının en aza indirilmesidir. Belirli periyotlarla sistemin ve diğer önemli verilenlerin yedeği alınmalıdır.
- **İzinsiz ve denetimsiz yazılım yüklenmesinin engellenmesi:** Kullanıcıların izinsiz ve denetimsiz yazılım yüklemeleri engellenmeli, her kullanıcının sadece ihtiyaç duyacağı programları kullanmasına izin verilmelidir. İzinsiz yüklenecek bir program, bazı casus kodları içerebileceği gibi sistem güvenliğini de tehlikeye sokabilir.
- **Sisteme veri giriş çıkışlarının kontrol edilmesi:** Sisteme izinsiz veri girişi ve veri çıkışı, sistem yöneticisi tarafından denetlenmeli, sistemi etkileyecek zararlı verilerin girişi ve sistemden dışarı çıkabilecek veri sızıntıları önlenmelidir. Bununla ilgili gerekli güvenlik ayarları yapılmalıdır.
- **Yönetimin belirli bölümlere ve kullanıcılara paylaştırılması:** Küçük etki alanları için merkezden yönetim çok verimli ve etkilidir ancak etki alanı büyüdükçe yönetim ve denetim bir hayli zorlaşır. Bu gibi durumlarda belirli işlemleri yapabilecek birimler oluşturulup yönetimin paylaştırılması gerekmektedir.
- **Sistemde Administrator (Sistem yöneticisi) girişi minimum seviyede tutulmalı:** Administrator (Sistem yöneticisi) tüm haklara sahip ve diğer kullanıcı haklarını da düzenleyen bir kullanıcı hesabıdır. Bu yönetici şifresinin bir şekilde ele geçirilmesi tüm sistemi çökertebilir. İşte bu yüzden Administrator hesabı mümkün olduğu kadar az kullanılmalı bunun yerine gerekli işlemler için izin işlemleri atanmış kullanıcı hesapları kullanılmalıdır.
- **Güvenlik kayıtları sürekli denetlenmeli:** Sistemde bilgisayar ve kullanıcılarla ilgili oluşabilecek her türlü bilgi, uyarı ve hatalar bir olay günlüğüne kaydedilir. Bu olay günlükleri belirli aralıklarla denetlenmeli, sisteme zarar verecek durumlara karşı önlem alınmalıdır.
- **Kullanıcıların oturum açma izninin ve diğer izinlerinin uygun bir şekilde düzenlenmesi:** sisteme giriş yapacak kullanıcıların şifre işlemleri, şifre uzunluk ve karmaşıklığı, belirli aralıklarla kullanıcının şifresini değiştirmeye zorlanması gibi güvenlik ayarları düzenlenmelidir. Ayrıca kullanıcının sistemin hangi kaynaklarına ne şekilde erişebileceği iyi bir şekilde düzenlenmelidir.

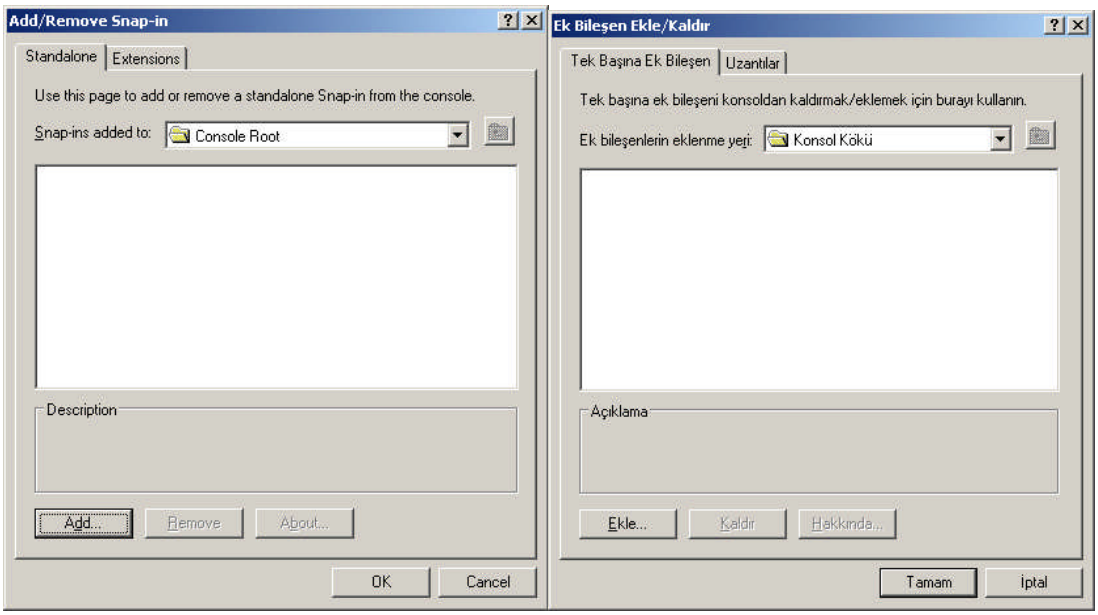
4.2. Güvenli Bilgisayar İçin Güvenlik Şablonunu Kullanma

Güvenlik şablonları windows tabanlı sunucu işletim sistemleri için geliştirilmiş bilgisayar ve kullanıcılarla ilgili standart güvenlik ayarlarını içeren bileşendir. Yöneticicinin seçeneğine göre birden fazla güvenlik şablon dosyası bulunmaktadır. Güvenlik şablonlarından herhangi biri seçildiğinde güvenlik ayarları bu şablona göre düzenlenir. Güvenlik şablonlarından birini sisteme dâhil edebilmek için yönetim konsolunu çalıştırmamız gerekir. **"Start => Run"** (Başlat => Çalıştır) bölümüne **"MMC"** yazılıp "OK" (Tamam) butonuna tıkladığımızda **Resim 4.1'**deki "Microsoft Management Consol" (Microsoft Yönetim Konsolu) karşımıza gelir. Yönetim Konsolundaki **"File=>Add/Remove Snap-in"** (Dosya=>Ek Bileşen Ekle/Kaldır) seçeneğiyle **Resim 4.2'**deki Bileşen Ekle/Kaldır pencere karşımıza gelir.

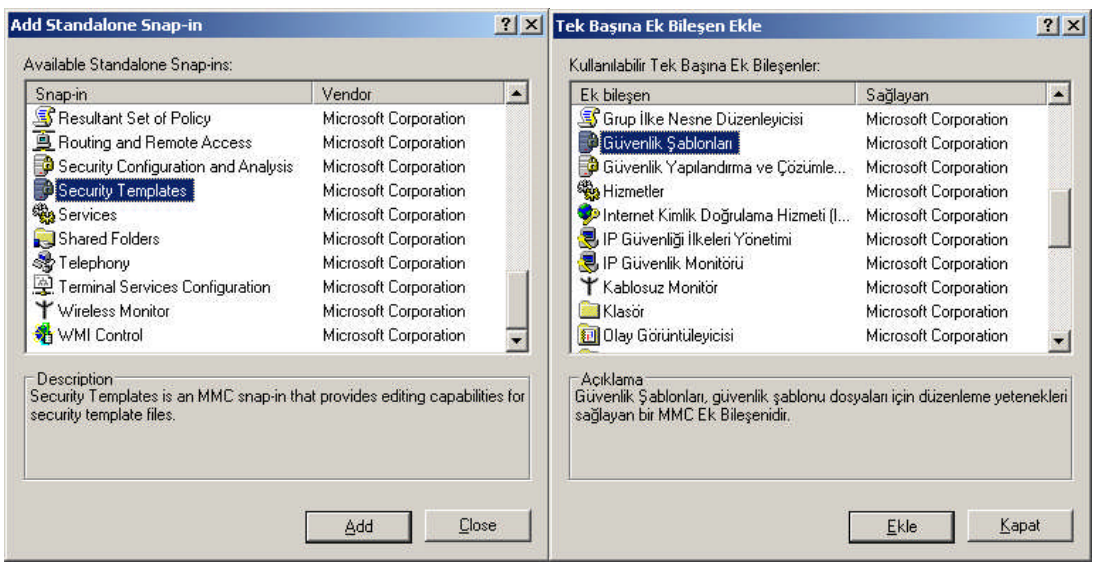


Resim 4.1: Microsoft Yönetim Konsolu (Win 2003 Eng ⇔ Win 2003 Tr)

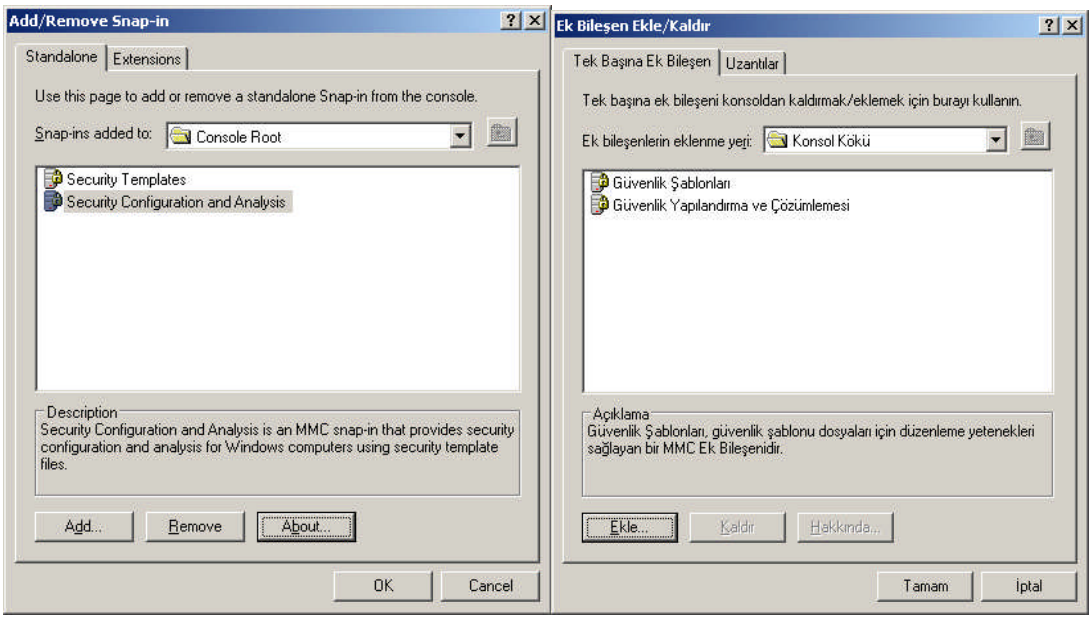
Resim 4.1'deki Ek bileşen Ekle/Kaldır Pencerede **"Add"** (Ekle) butonunu tıkladığımızda yüklenecek standart bileşenlerin bulunduğu **Resim 4.3'**teki pencere karşımıza gelir. Ek bileşen Ekle/Kaldır önce "Security Templates" (Güvenlik şablonları) bileşenini seçip **"Add"** (Ekle) butonunu tıklarız sonra da "Security Configuration and Analysis" (Güvenlik Yapılandırma ve Çözümleme) bileşenini seçip **"Add"** (Ekle) butonuna tıklarız. Böylece **Resim 4.4**'te görüldüğü gibi güvenlik şablonları için gerekli iki bileşenimizi konsola eklemiş oluruz. Bileşenleri ekledikten sonra **Resim 4.4'**teki pencerenin "OK" (Tamam) butonuna basıp **Resim 4.4**'teki konsol ekranına dönmüş oluruz.



Resim 4.2: Bileşen Ekle/Kaldır penceresi (Win 2003 Eng ⇔ Win 2003 Tr)

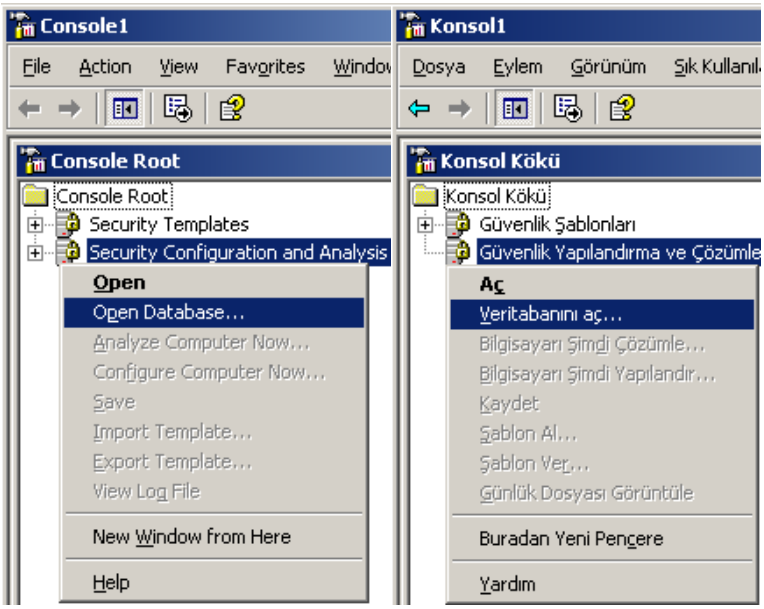


Resim 4.3: Güvenlik Şablonu bileşeninin eklenmesi (Win 2003 Eng ⇔ Win 2003 Tr)

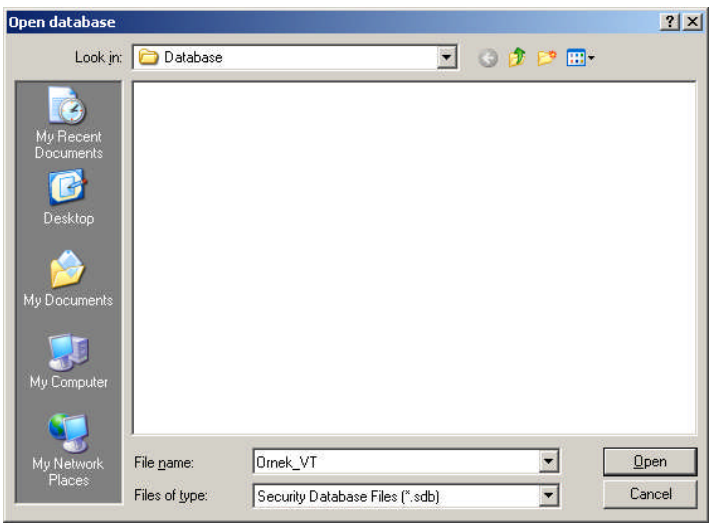


Resim 4.4: MMC eklenmiş Güvenlik Şablonu bileşeni (Win 2003 Eng ⇔ Win 2003 Tr)

Resim 4.5: Konsol üzerinde Güvenlik Şablonu işlemleri (W 2003 Eng ⇔ W 2003 Tr)



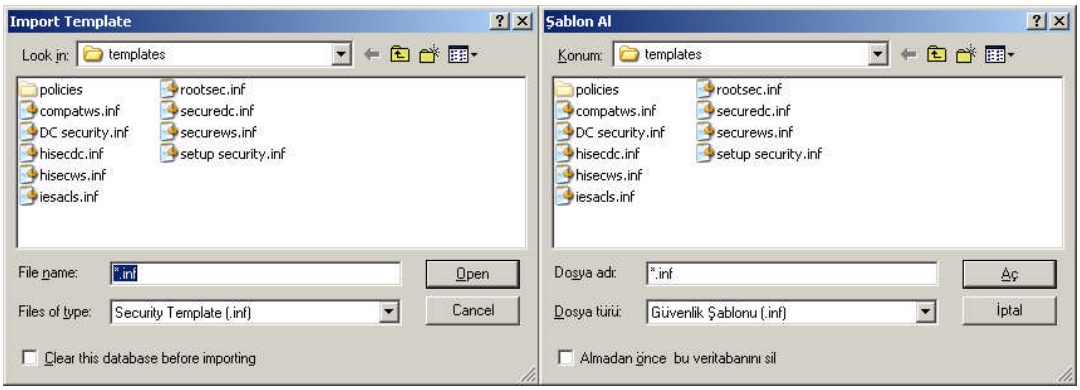
Resim 4.6: MMC Güvenlik Şablonu için VT açılması (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.7: Veritabanı seçme veya oluşturma penceresi (Win 2003 Eng)

Güvenlik şablonları yüklenip konsol ekranına döndükten sonra seçeceğimiz güvenlik şablonu ayarları için bir veri tabanı oluşturmamız veya mevcut veritabanını seçmemiz gerekir. Veri tabanı oluşturabilmek için **Resim 4.6'**daki konsol penceresinden "Security Configuration and Analysis" (Güvenlik Yapılandırma ve Çözümleme) bileşenine sağ tıklayıp "Open Database" (Veritabanı aç) seçeneğini seçmemiz gerekir. **Resim 4.6'**da görüldüğü gibi veritabanı oluşturulmadan birçok seçenek aktif konumda olmaz.

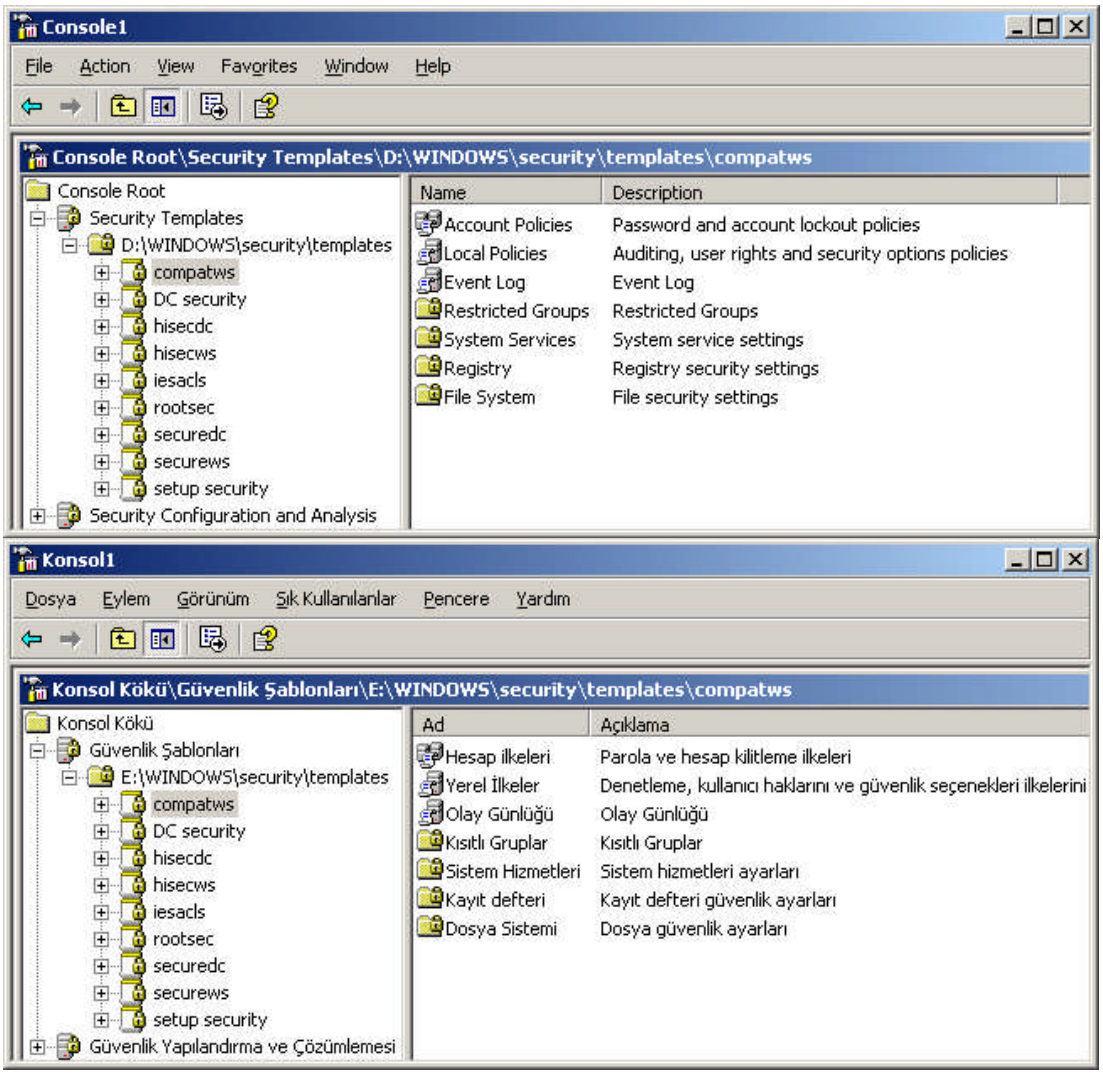
"Open Database" (Veritabanı aç) seçeneğini tıkladığımızda **Resim 4.7'**deki veritabanı seçme penceresi karşımıza gelir. Eğer mevcut bir veritabanı dosyası bulunmuyorsa "File name" (Dosya adı) bölümüne yazdığımız dosya isminde bir veritabanı dosyası oluşturulur. Veritabanı oluşturulduktan sonra **Resim 4.8'**de görüldüğü gibi bizden bir şablon dosyası seçmemiz istenecektir.



Resim 4.8: Eklenecek Güvenlik Şablonları (Win 2003 Eng ⇔ Win 2003 Tr)

Güvenlik şablonlarıyla ilgili dosyaları kısaca açıklayalım:

- **securedc:** Gelişmiş etki alanı hesabı ilkeleri sağlar, LanManager kimlik denetimini kısıtlar ve adsız kullanıcılarda daha ileri kısıtlamalar sağlar. Bir etki alanı denetleyicisi securedc ile yapılandırılmışsa o etki alanından hesabı olan kullanıcı, LanMananeger istemcisinden herhangi bir üye sunucuya bağlanamaz.
- **securews:** Gelişmiş yerel hesap ilkeleri sağlar ve LanManager kimlik denetimi kullanımını kısıtlar, sunucu tarafı SMB imzalamasını etkinleştirir ve adsız kullanıcılarda daha ileri kısıtlamalar sağlar.
- **compatws:** Varsayılan dosya ve kayıt defteri izinlerini, Kullanıcılar grubunda sertifikası olmayan uygulamaların gerekliliklerine uygun bir şekilde serbest bırakır. Power Users grubu, sertifikasız uygulamalar için kullanılmalıdır.
- **rootsec:** İşletim sistemi biriminin köküne uygulanır ve alt nesnelere doğru yayılır. Yayılma zamanı korunmasız alt nesne sayısına bağlıdır.
- **DC security:** Varsayılan güvenlik ayarlarının, etki alanı denetleyicileri için güncelleştirilmesinde kullanılır.
- **hisecdc:** Securedc süper kümesi. LanManager kimlik denetiminde ve güvenli kanal imzalama ve SMB verilerinde daha gelişmiş kısıtlamalar sağlar. Hisecdc'nin bir etki alanı denetleyicisine uygulanması için, güvenilen ve güvenen bütün etki alanı denetleyicilerinin Windows 2000 veya sonrası olması gerekir.
- **hisecws:** Securews süper kümesi. LanManager kimlik denetiminde ve güvenli kanalların şifrelenmesi ve imzalanmasında ve SMB verisinde gelişmeler sağlar. Hisecws uygulanması için bütün kullanıcıların hesaplarını içeren etki alanı denetleyicilerinin oturum açan istemcilerinin en az NT4 SP4 veya sonrası olması gerekir.
- **setup security:** Ürün kurulduğunda varsayılan güvenlik ayarlarını içerir.

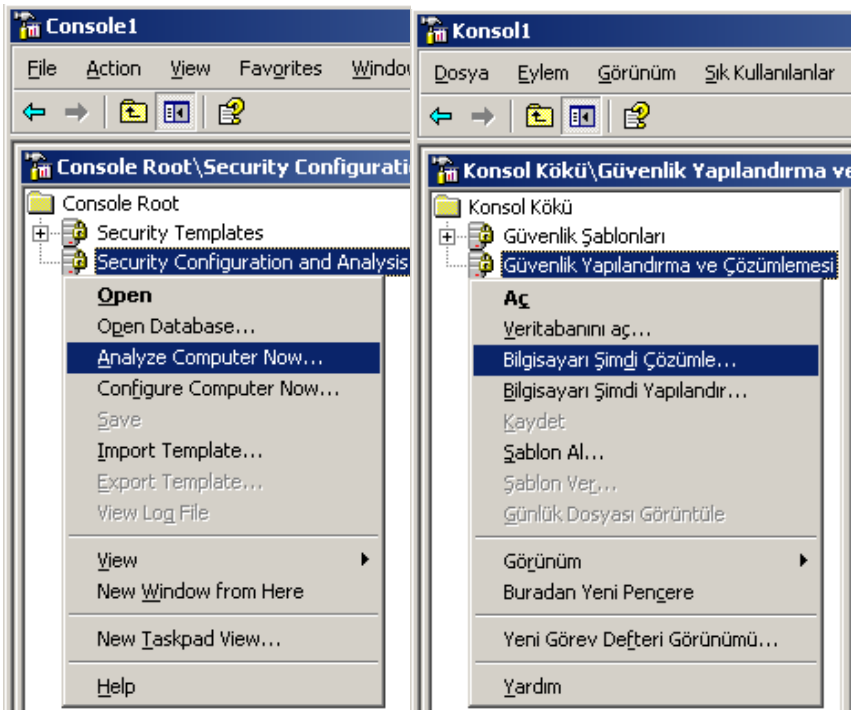


Resim 4.9: Güvenlik şablonlarının içerikleri (Win 2003 Eng ⇔ Win 2003 Tr)

Resim 4.9'daki güvenlik şablonu çeşitleri ve onların içerikleri görülmektedir. Tüm şablonların içerikleri aynıdır sadece kullanıcı ve bilgisayarlar için uygulanacak ayarlar farklıdır. Güvenlik şablonlarının içerikleri aşağıda verilmiştir:

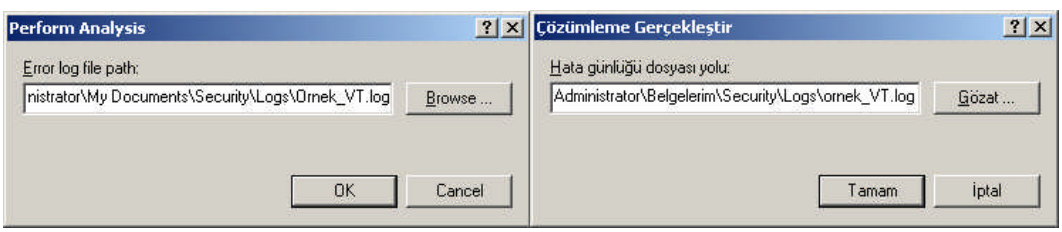
- **Account Policy (Hesap ilkeleri):** Şifre özellikleri ve hesap kilitleme ayarlarının bulunduğu ilkelerdir.
- **Local Policy (Yerel ilkeler):** Denetleme, kullanıcı hakları ve güvenlik seçeneklerinin bulunduğu ilkelerdir.
- **Event Log (Olay günlüğü):** Olay günlüğü ayarlarının bulunduğu ilkelerdir.
- **Restricted Groups (Kısıtlı gruplar):** Kısıtlı gruplarla ilgili ayarlarının bulunduğu ilkelerdir.

- **Systems Services (Sistem Hizmetleri):** Sistem hizmetleri ayarlarının bulunduğu ilkelerdir.
- **File Systems (Dosya sistemi):** Dosya güvenlik ayarlarının bulunduğu ilkelerdir.

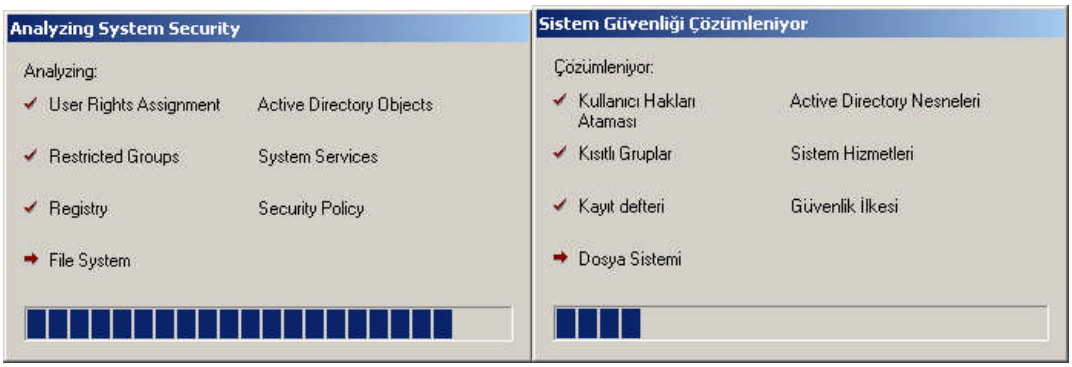


Resim 4.10: Güvenlik Yapılandırma ve Çözümleme seçenekleri (Win 2003 Eng ⇔ Win 2003 Tr)

Uygun güvenlik şablonu dosyası seçildikten sonra bunu sisteme uygulayabilmek için birkaç işlem yapmak gerekir. Öncelikle **Resim 4.10'**daki konsol penceresinden "Security Configuration and Analysis" (Güvenlik Yapılandırma ve Çözümleme) bileşenine sağ tıklayıp "Analyze Computer Now" (Bilgisayarı Şimdi Çözümle) seçeneğiyle bilgisayarın şu anki ayarlarıyla güvenlik şablonu ayarlarını karşılaştırmamız ve **Resim 4.11'**deki gibi belirtileceğimiz dosyaya kaydetmemiz gerekir. **Resim 4.12**'de çözümleme işleminin gerçekleşme aşaması görülmektedir.



Resim 4.11: Yapılacak Çözümleme sonuçlarının kaydedileceği dosya seçimi (Win 2003 Eng ⇔ Win 2003 Tr)

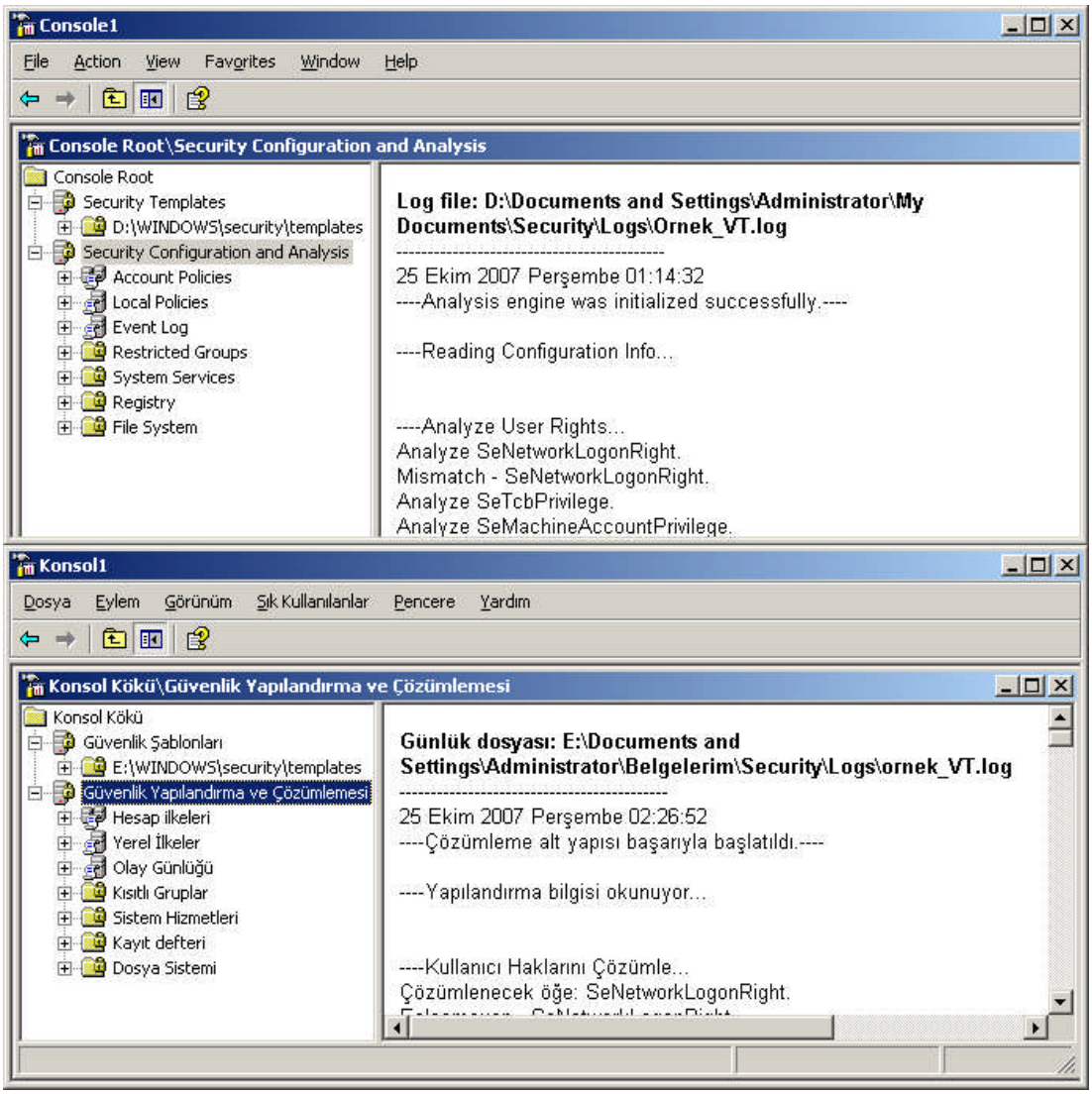


Resim 4.12: Sistem Güvenliğinin Çözümlenmesi (Win 2003 Eng ⇔ Win 2003 Tr)

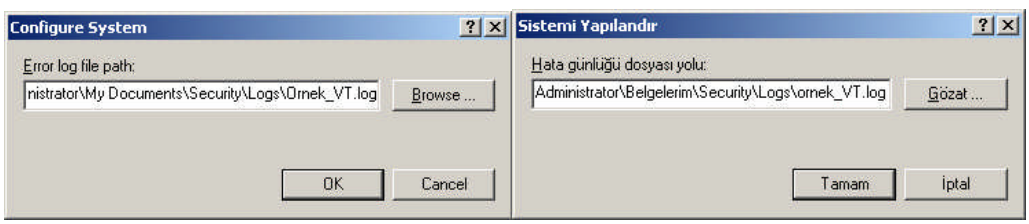
Çözümleme işlemi gerçekleştikten sonra elde edilen analiz kayıtlarını **Resim 4.12**'de görüldüğü gibi

"E:\Documents and Settings\Administrator\Belgelerim\Security\Logs\ornek_VT.log"

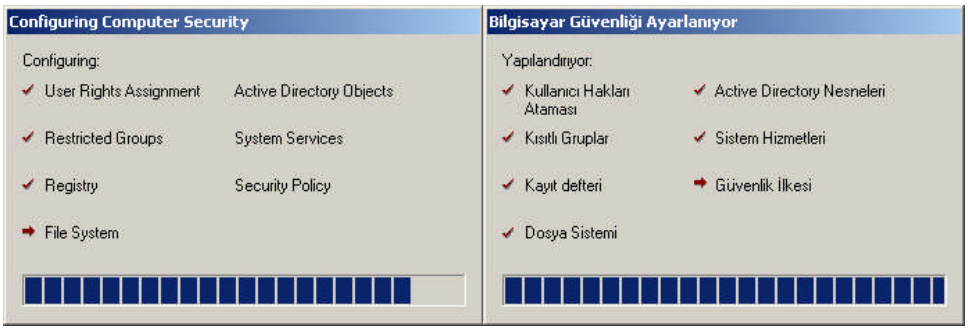
dosyası içerisine kaydeder. Log dosyası incelenip gerekli değişikliklerin neler olacağı öğrenildikten sonra bir karar vermemiz gerekir. Eğer bu şablonun sistemimize uygulanmasını istiyorsak **Resim 4.10'**daki konsol penceresinden "Security Configuration and Analysis" (Güvenlik Yapılandırma ve Çözümleme) bileşenine sağ tıklayıp "Configure Computer Now" (Bilgisayarı Şimdi Yapılandır) seçeneğiyle şablonun sisteme uygulanması işlemini başlatmak için ilk adımı atmış oluruz. Bizden **Resim 4.14'**te olduğu gibi Bilgisayar yapılandırma sonuçlarının kaydedileceği **Log** dosyasının adını isteyecektir. Dosya ismi de belirlendikten sonra **Resim 4.14'**te olduğu gibi sistem yapılandırması başlatılmış olur. Bundan sonraki işlemler, GPO güvenlik ayarları ile yapılabilir.



Resim 4.13: Çözümleme sonucunda oluşan Log dosyası (W 2003 Eng ⇔ W 2003 Tr)



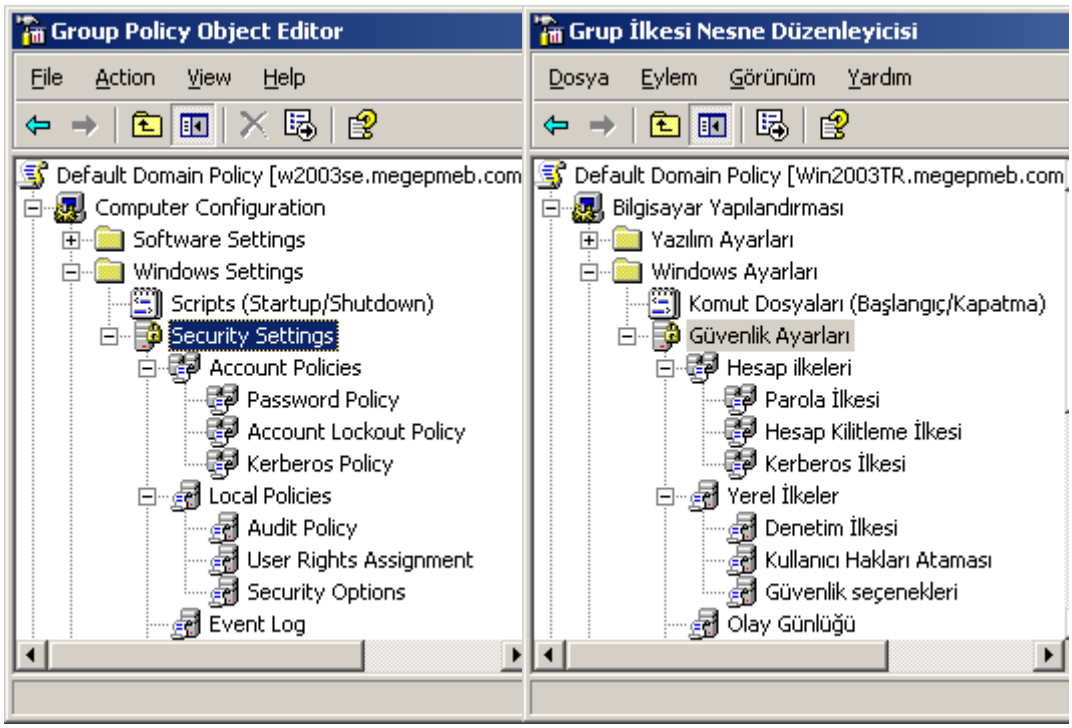
Resim 4.14: Bilgisayar yapılandırma sonuçlarının kaydedileceği dosya seçimi (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.15: Bilgisayar güvenliğinin yapılandırılması (Win 2003 Eng ⇔ Win 2003 Tr)

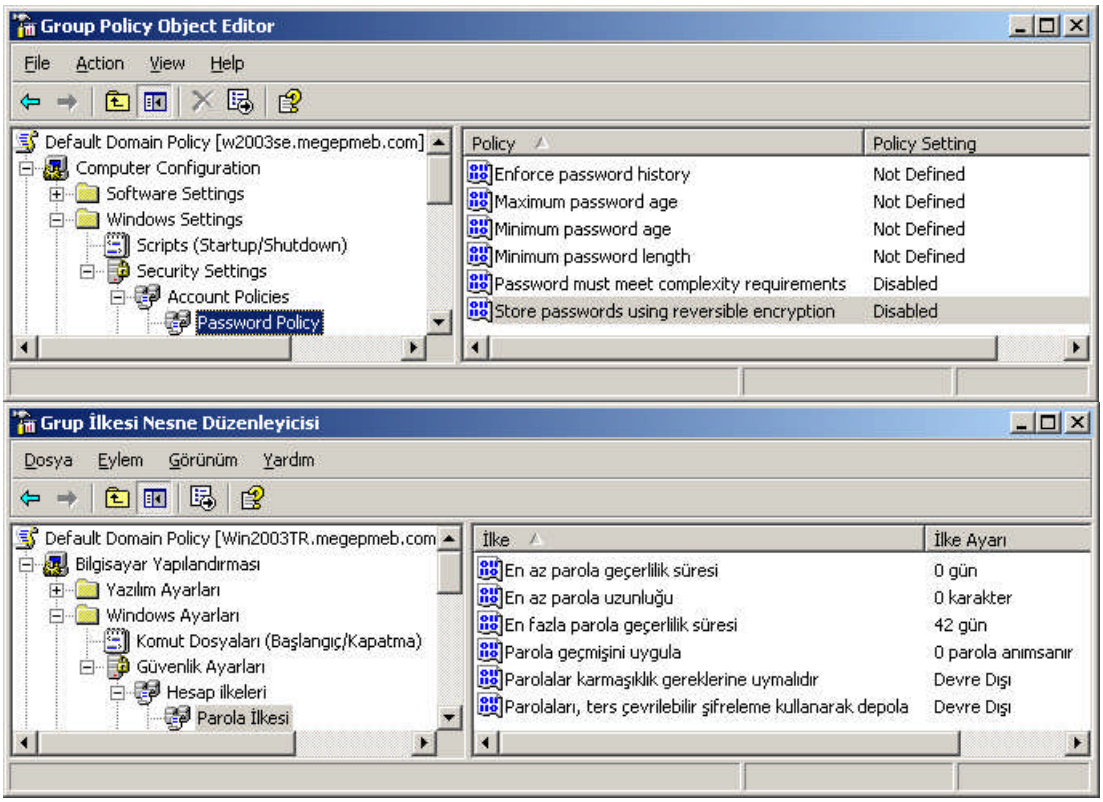
4.3. Bilgisayar Güvenlik Politikası

Bilgisayar güvenlik politikaları bilgisayarda oturum açma, parola işlemleri, hesap kilitleme ayarları, kullanıcı haklarının atanması gibi birçok güvenlik seçeneklerinin olduğu bölümdür. Bilgisayar güvenlik politikaları, her birim için ayrı kullanılabileceği gibi sistemin ortak bir güvenlik politikası da bulunabilir. Bilgisayar güvenlik politikalarını düzenleyebilmek için etki alanı veya organizasyon birimine eklenmiş Grup politikası nesne düzenleyicisini **Resim 4.16**'daki gibi açmamız gerekir.



Resim 4.16: GPO bilgisayar güvenlik ayarları (Win 2003 Eng ⇔ Win 2003 Tr)

Bilgisayar güvenlik ayarlarını Hesap ilkeleri ve Yerel ilkeler olmak üzere iki ana başlıkta toplayabiliriz. Hesap ilkeleri içerisinde parola ilkesi, Hesap kilitleme ilkesi ve Kerberos ilkesi yer alır. Yerel ilkeler içerisinde ise denetim ilkesi, kullanıcı hakları ataması ve güvenlik seçenekleri yer almaktadır. **Resim 4.17'**de "Password Policy" (Parola ilkesi) ayar seçenekleri görülmektedir.

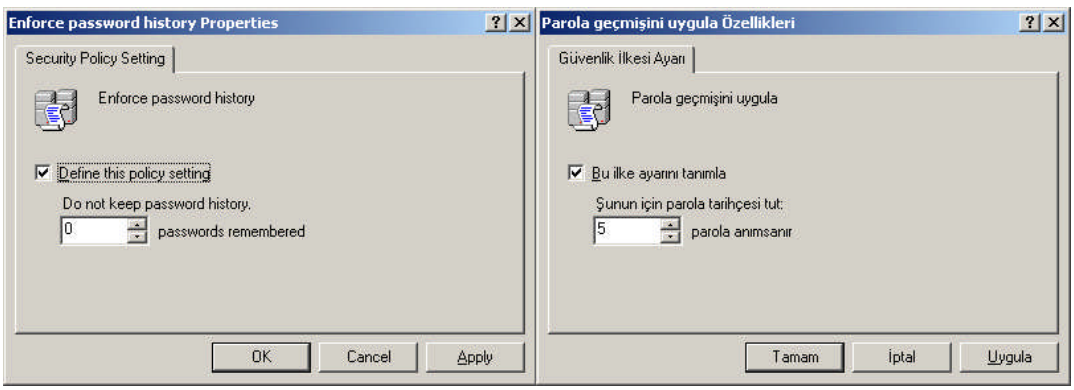


Resim 4.17: Parola ilkesi seçenekleri (Win 2003 Eng ⇔ Win 2003 Tr)

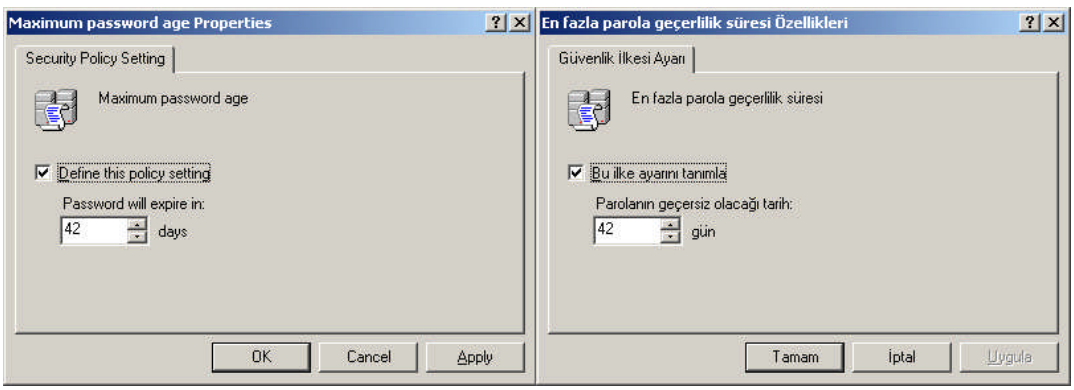
Parola ilkesi seçenekleri şöyle incelenebilir:

- **Enforce password history (Parola geçmişini uygula):** Bu seçenek kullanıcının parola değiştirirken belirtilen sayıdaki önceki parolalarını tutar **(Resim 4.18).**
- **Maximum password age (En fazla parola geçerlilik süresi):** Kullanıcı tarafından belirlenen parolanın en fazla ne kadar zamanda geçerli kalacağını ayarlar, bu süre dolduğunda kullanıcı parola değiştirmeye zorlanır (**Resim 4.19).**
- **Minimum password age (En az parola geçerlilik süresi):** Kullanıcı tarafından belirlenen parolanın en az ne kadar zamanda geçerli kalacağını ayarlar **(Resim 4.20).**
- **Minimum password length (En az parola uzunluğu):** kullanıcı tarafından belirlenen parolanın en az ne kadar uzunlukta olacağını ayarlar **(Resim 4.21).**

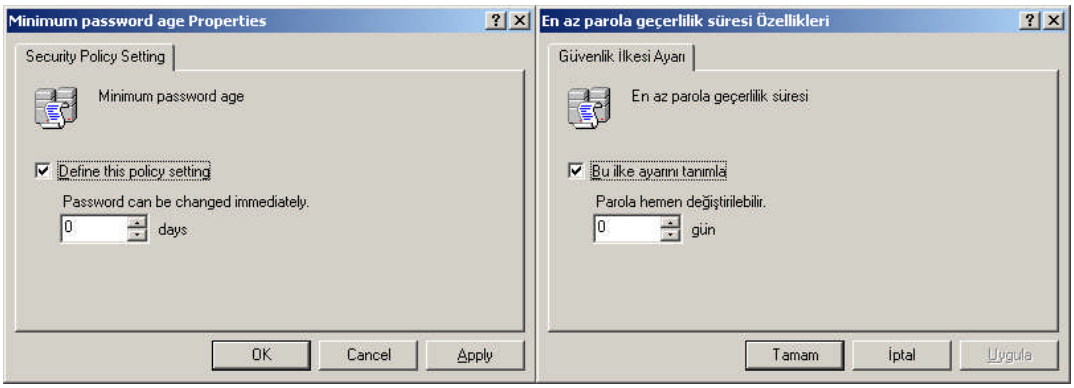
- **Password must meet complexity requirements (Parolalar karmaşıklık gereklerine uymalıdır) :** kullanıcı tarafından belirlenen parolanın karmaşıklığını ayarlar. Parola karmaşıklık gereklerine uymazsa kabul edilmez **(Resim 4.22).**
- **Store passwords using reversible encryption (Parolaları, ters çevrilebilir şifreleme kullanarak depola):** Kullanıcı tarafından belirlenen parolayı kaydederken ters çevrilebilir şifreleme kullanarak işlem yapar. **Resim 4.22'**deki ile benzer bir işlemdir.



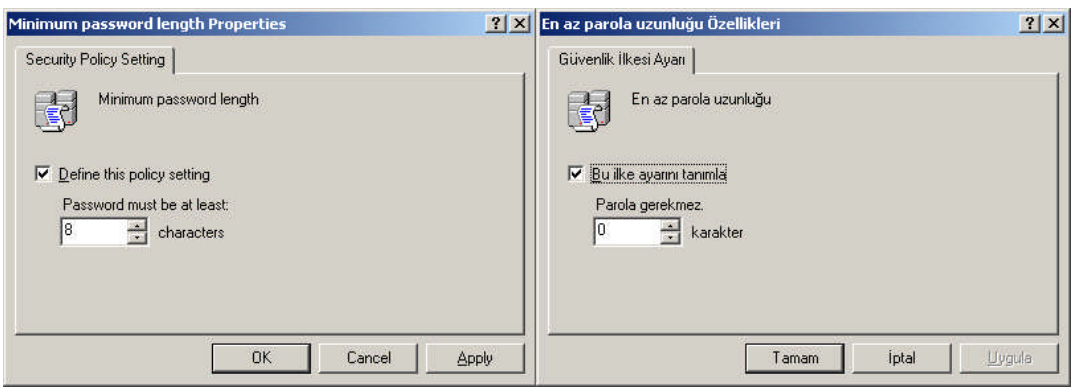
Resim 4.18: Parola geçmişini uygula özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



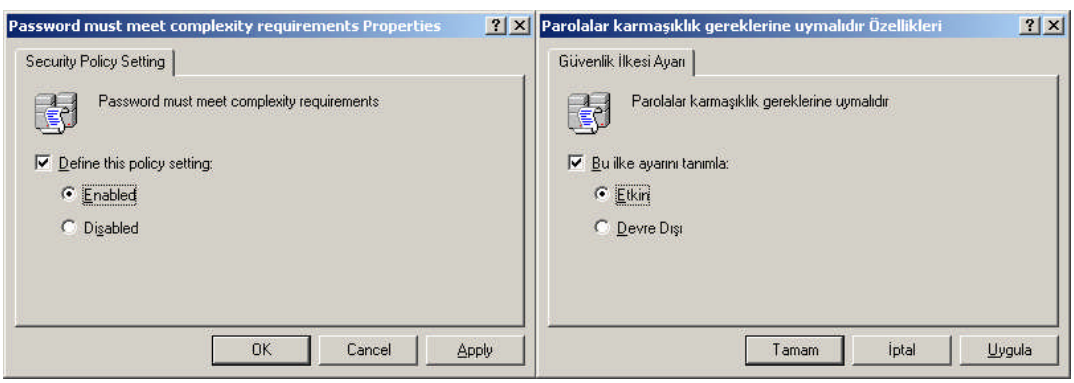
Resim 4.19: En fazla parola geçerlilik süresi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



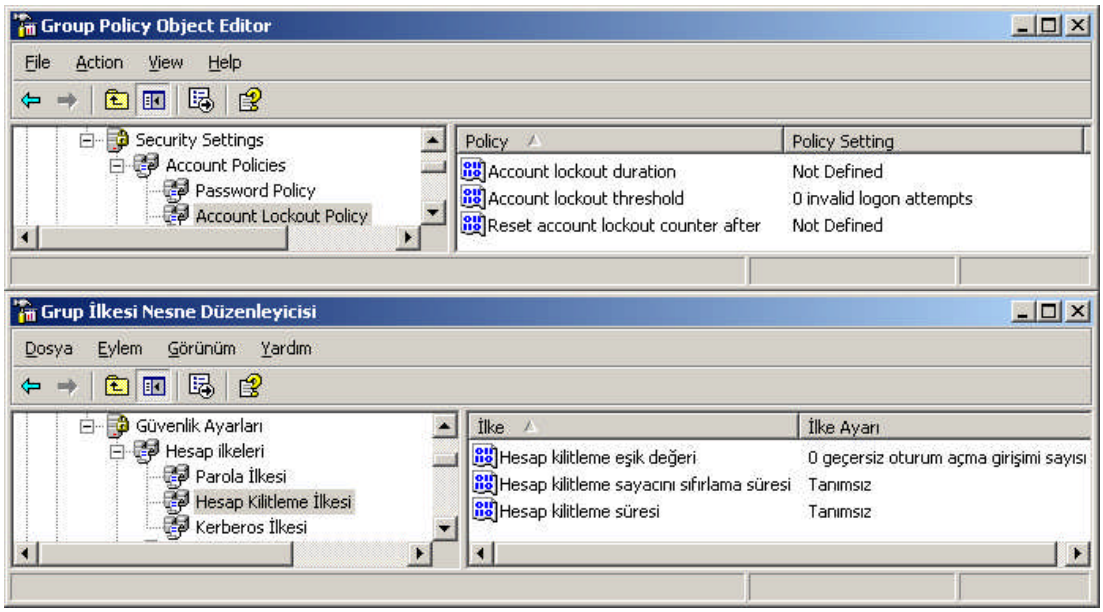
Resim 4.20: En az parola geçerlilik süresi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.21: En az parola uzunluğu özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



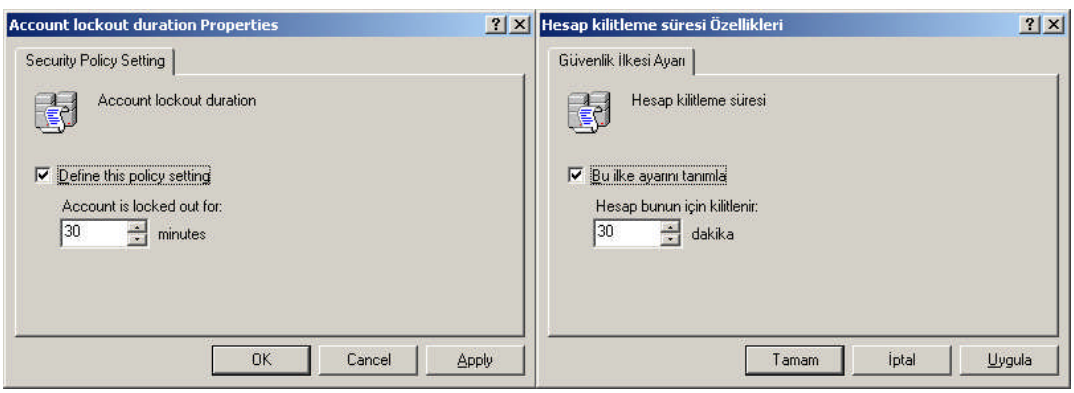
Resim 4.22: Parola karmaşıklığı özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



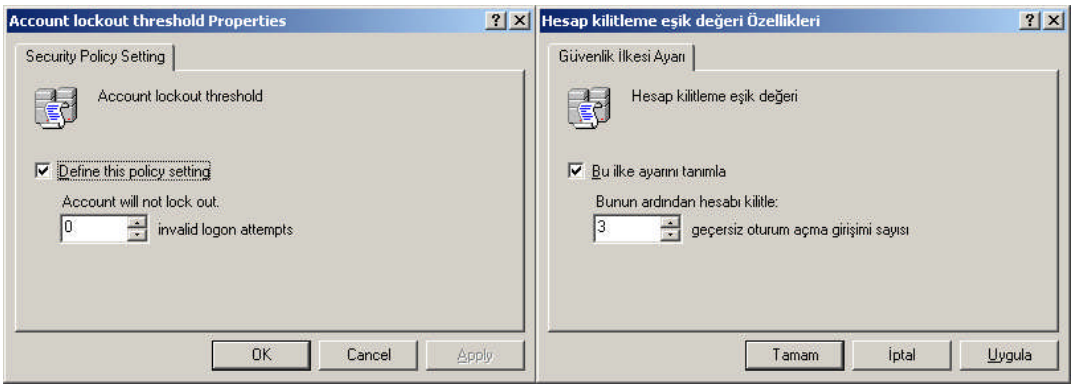
Resim 4.23: Hesap kilitleme ilkesi seçenekleri (Win 2003 Eng ⇔ Win 2003 Tr)

Hesap ilkelerinden bir diğer ayar grubu da **Resim 4.23**'de görülen "Account lockout policy" (Hesap kilitleme ilkesi) dir.

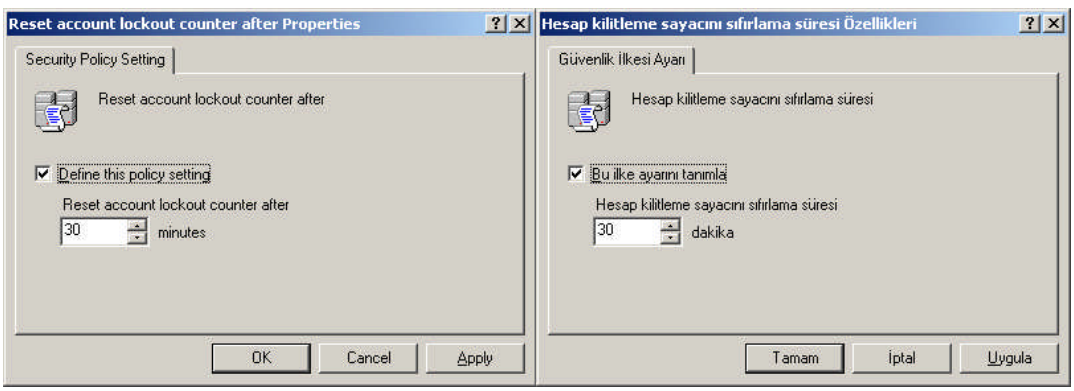
- **Account lockout duration (Hesap kilitleme süresi):** kullanıcının boşta olduğu zamanda belirtilen süreden sonra hesabı kilitlemek için kullanılır **(Resim 4.24).**
- **Account lockout threshold (Hesap kilitleme eşik değeri):** kullanıcının yanlış parola girişlerinde hesabı kilitleme süresini ayarlar **(Resim 4.25).**
- **Reset account lockout counter after (Hesap kilitleme sayacını sıfırlama süresi):** Hesap kilitleme sayacını sıfırlama süresini ayarlar **(Resim 4.26).**



Resim 4.24: Hesap kilitleme süresi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



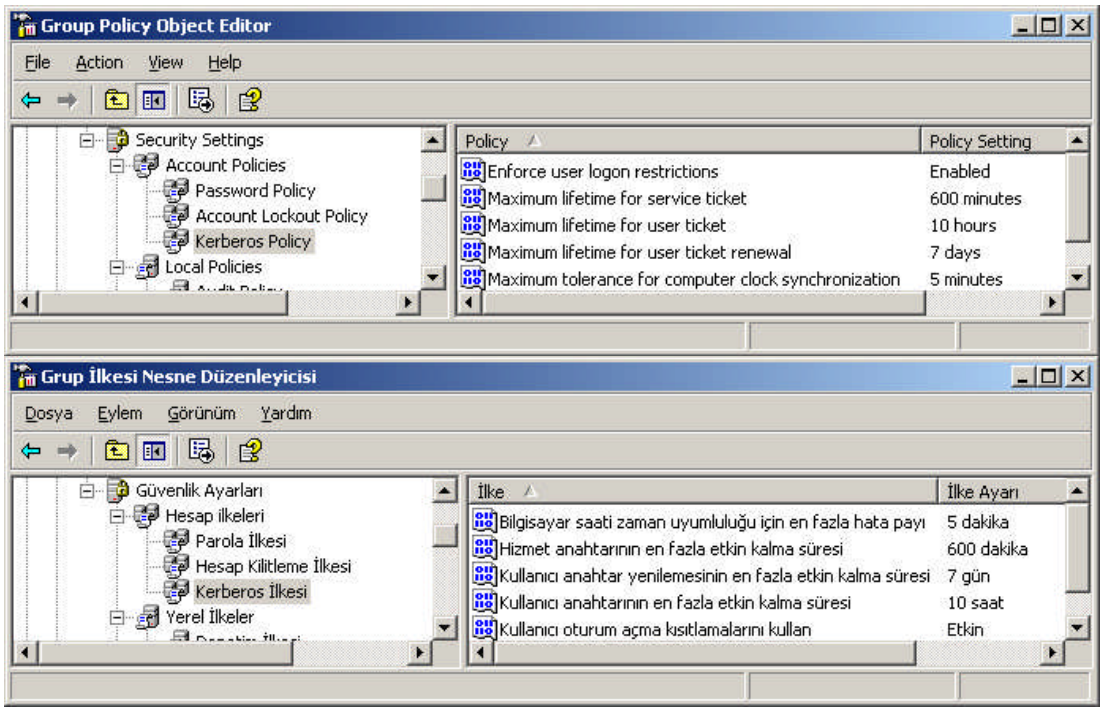
Resim 4.25: Hesap kilitleme eşik değeri özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



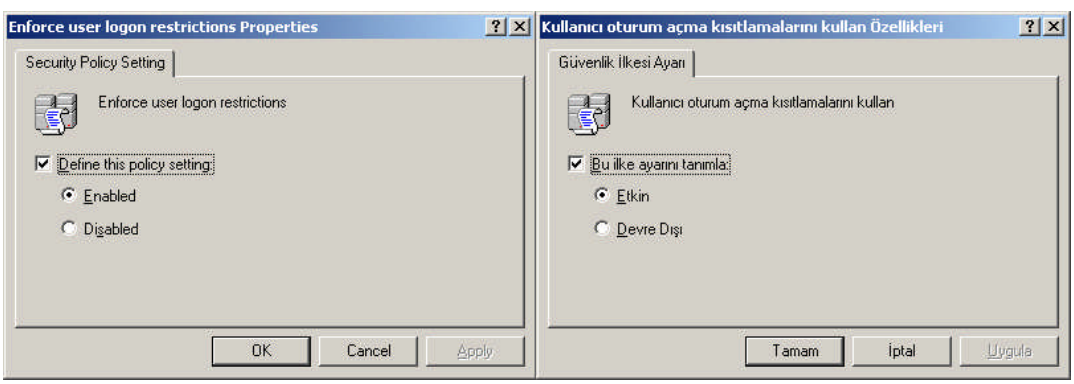
Resim 4.26: Hesap kilitleme sayacı sıfırlama süresi (Win 2003 Eng ⇔ Win 2003 Tr)

Hesap ilkelerinden en sonuncusu olan ayar grubu da **Resim 4.27**'de görülen "Kerberos policy" (Kerberos ilkesi) dir. Kerberos ilkesi, kullanıcının oturum açma ve oturumun açık kalma sürelerini düzenleyen bir hesap ilkesi bileşenidir. Kerberos ilkesi seçenekleri aşağıdaki gibidir:

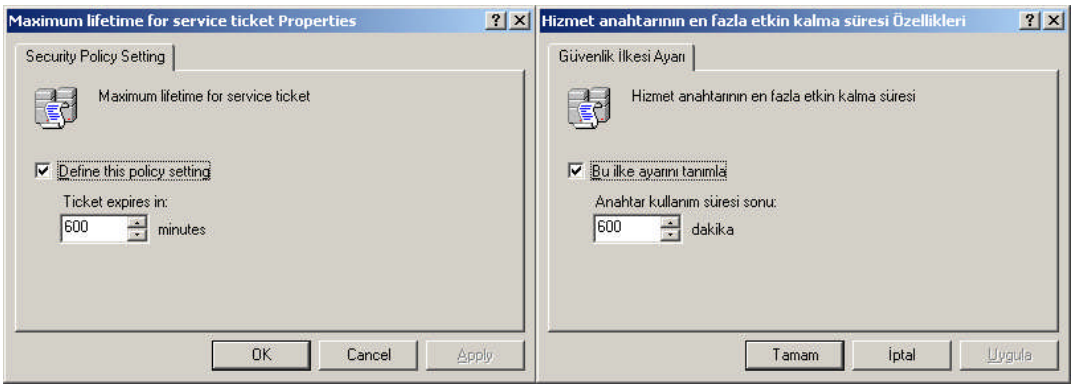
- **Enforce user logon restrictions (Kullanıcı oturum açma kısıtlamalarını kullan):** (Resim 4.28).
- **Maximum lifetime for service ticket (Hizmet anahtarının en fazla etkin kalma süresi)** (Resim 4.29).
- **Maximum lifetime for user ticket (Kullanıcı anahtarının en fazla etkin kalma süresi)** (Resim 4.30).
- **Maximum lifetime for user ticket renewal (Kullanıcı anahtar yenilemesinin en fazla etkin kalma süresi)** (Resim 4.31).
- **Maximum tolerance for computer clock synchronization (Bilgisayar saati zaman uyumluluğu için en fazla hata payı)** (Resim 4.32).



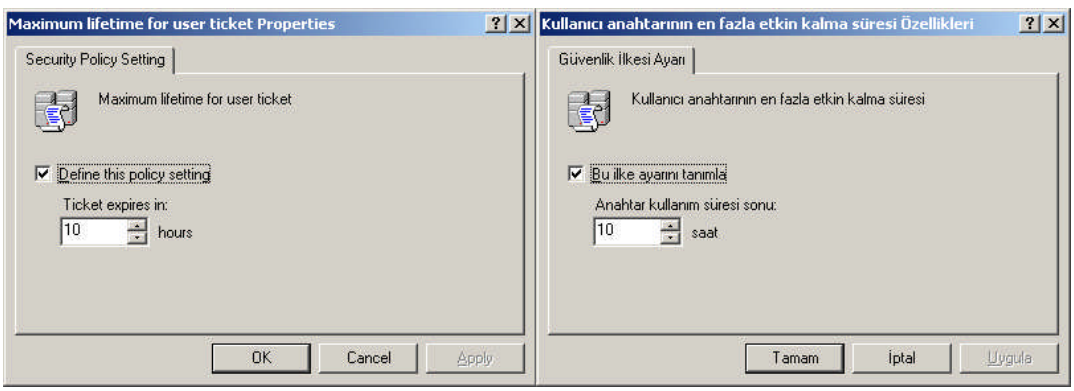
Resim 4.27: Kerberos ilkesi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



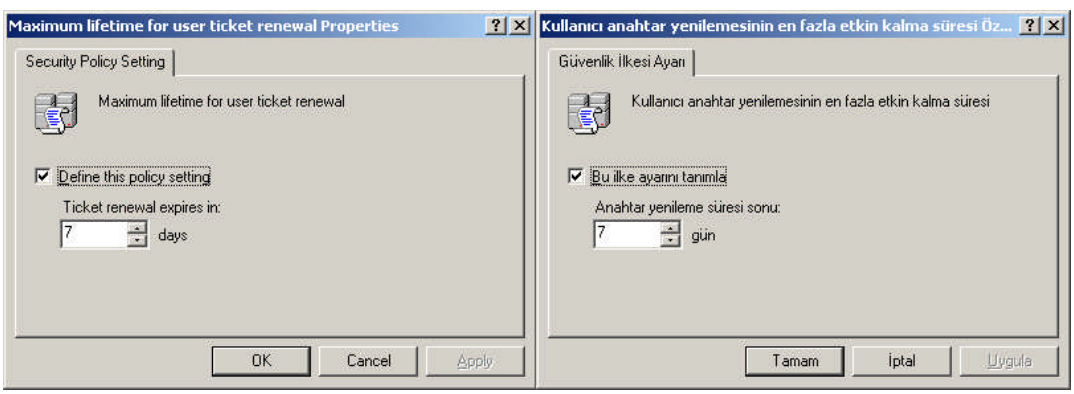
Resim 4.28: Kullanıcı oturum açma kısıtlamalarını kullan özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



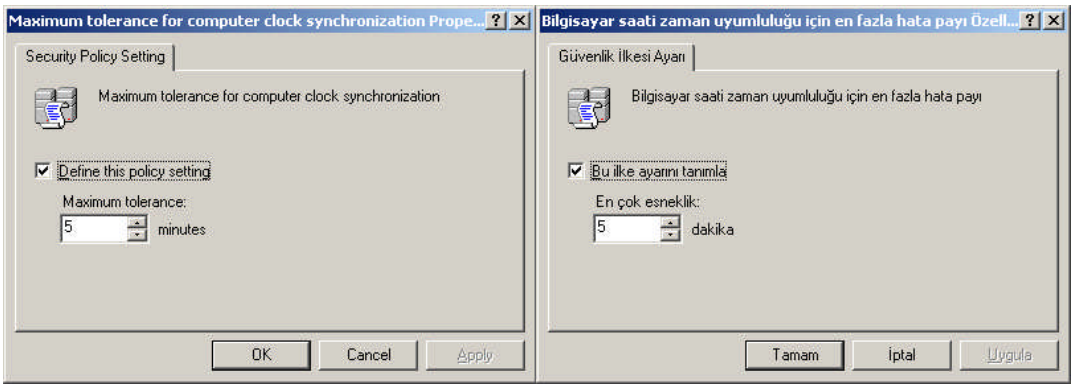
Resim 4.29: Hizmet anahtarının en fazla etkin kalma süresi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



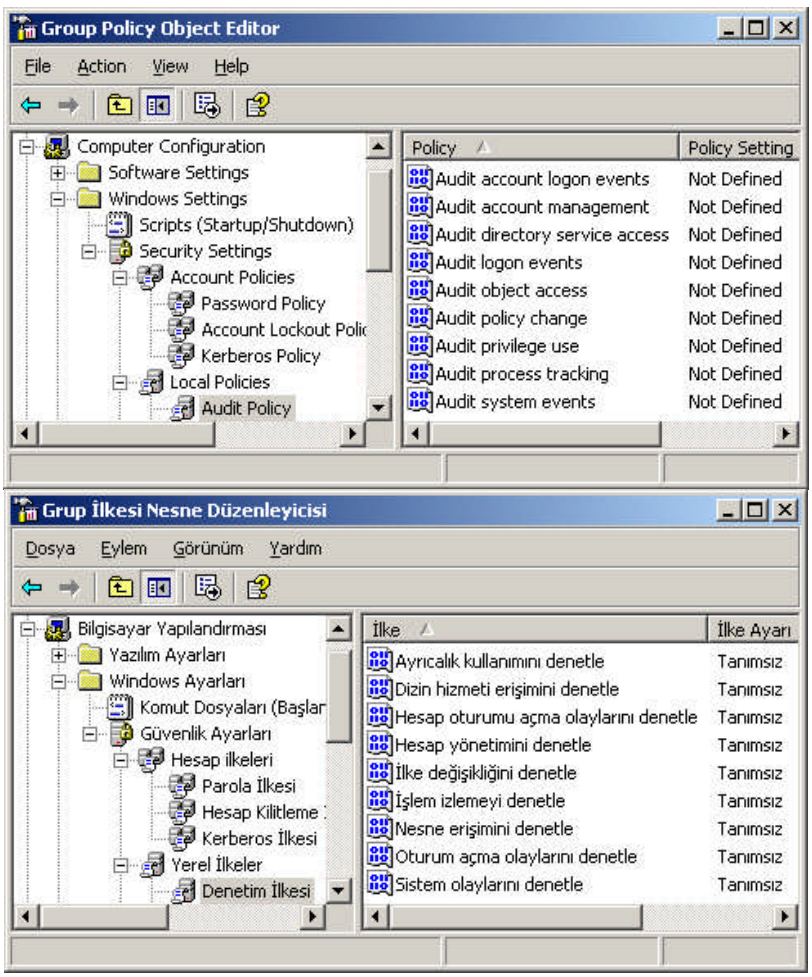
Resim 4.30: Kullanıcı anahtarının en fazla etkin kalma süresi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.31: Kullanıcı anahtar yenilemesinin en fazla etkin kalma süresi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)

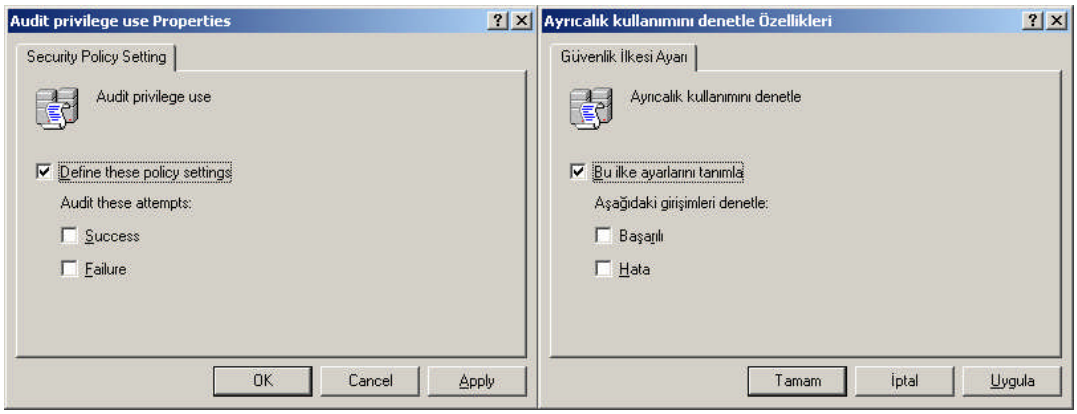


Resim 4.32: Bilgisayar saati zaman uyumluluğu için en fazla hata payı özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.33: Denetim ilkesi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)

Yerel ilkeler (Local policy), bilgisayarların birçok birime erişimi kontrol etmek amacıyla oluşturulmuş ilkelerdir. Bu yerel ilkelerin ilki **Resim 4.33**'te görülen "Audit policy"(Denetim ilkesi) dir. Bu ilke genelde hesap ve dizin denetimi, oturum açma ve kapatma işlemleri gibi birçok denetimi içerir. Denetim ilkesinde bulunan ayarlamalar **Resim 4.34'**te gösterilmiştir.

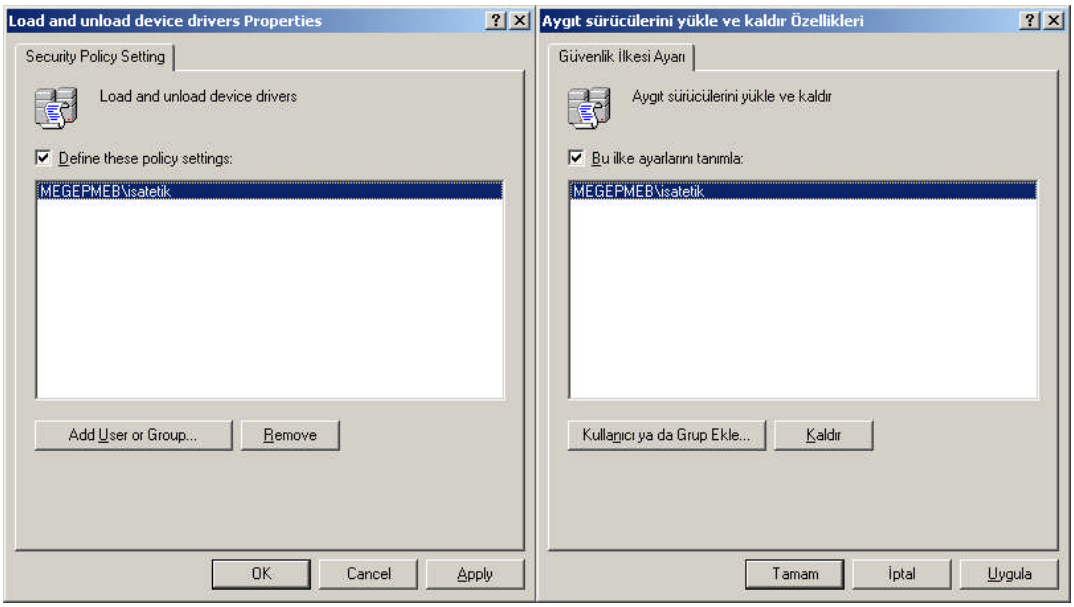


Resim 4.34: Ayrıcalık kullanıcılarını denetle özellikleri (W 2003 Eng ⇔ W 2003 Tr)

"Audit policy" (Denetim ilkesi) içerisinde bulunan ayarlamalar aşağıdaki gibidir:

- Audit account logon events (Hesap oturumu açma olaylarını denetle)
- Audit account management (Hesap yönetimini denetle)
- Audit directory service access (Dizin hizmeti erişimini denetle)
- Audit logon events (Oturum açma olaylarını denetle)
- Audit object access (Nesne erişimini denetle)
- Audit policy change (İlke değişikliğini denetle)
- Audit privilege use (Ayrıcalık kullanımını denetle)
- Audit process tracking (İşlem izlemeyi denetle)
- Audit system events (Sistem olaylarını denetle)

Yerel ilkelerin ikinci denetim grubu olan "User Rights Assignment" (Kullanıcı hakları ataması) kullanıcı haklarının atanmasıyla ilgili ayarlamaları içerir. Kullanıcı hakları ataması ile ilgili ayarlamalar **Resim 4.35'**te gösterilmiştir. **Resim 4.35'**te "Add User or Group" (Kullanıcı veya grup ekle) butonundan bu denetim ilkesinin etkileneceği kullanıcılar veya gruplar seçilir.



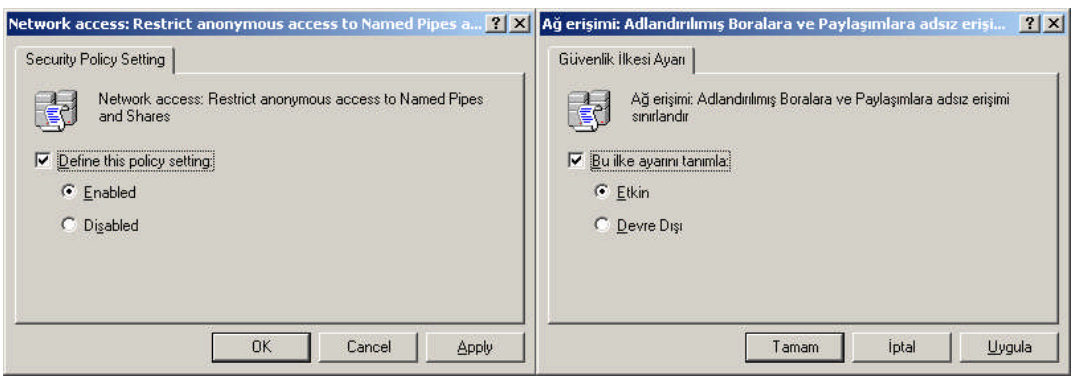
Resim 4.35: Denetim ilkesinin kullanıcı veya gruplar için uygulanması (Win 2003 Eng ⇔ Win 2003 Tr)

"User Rights Assignment" (Kullanıcı hakları ataması) içerisinde bulunan ayarlamalar aşağıdaki gibidir:

- Access this computer from the network (Bu bilgisayara ağ üzerinden erişim)
- Act as part of the operating system (İşletim sisteminin parçası olarak davran)
- Add workstations to domain (İş istasyonlarını etki alanına ekle)
- Adjust memory quotas for a process (İşlem için bellek kotası ayarla)
- Allow log on locally (Yerel olarak oturum açmaya izin ver)
- Allow log on through Terminal Services (Terminal hizmetler üzerinden oturum açmaya izin ver)
- Back up files and directories (Dosya ve dizinleri yedekle)
- Bypass traverse checking (Çapraz denetlemeyi geç)
- Change the system time (Sistem saatini değiştir)
- Create a pagefile (Bir disk belleği dosyası oluştur)
- Create a token object (Bir anahtar nesnesi oluştur)
- Create global objects (Genel nesne oluştur)
- Create permanent shared objects (Kalıcı paylaştırılmış nesneler oluştur)
- Debug programs (Programların hatalarını ayıkla)
- Deny access to this computer from the network (Bu bilgisayara ağ üzerinden erişime izin verme)
- Deny log on as a batch job (Toplu iş olarak oturum açmayı kabul etme)
- Deny log on as a service (Hizmet olarak oturum açmayı kabul etme)
- Deny log on locally (Yerel olarak oturum açmaya izin verme)
- Deny log on through Terminal Services (Terminal hizmetler üzerinden oturum açmayı reddet)

- Enable computer and user accounts to be trusted for delegation (Bilgisayar ve kullanıcı hesaplarının dağıtım güvenilirliğini etkinleştir)
- Force shutdown from a remote system (Uzaktaki bir sistemden oturum kapatmayı zorla)
- Generate security audits (Güvenlik denetimlerini üret)
- Impersonate a client after authentication (Kimlik doğrulamanın ardından bir istemciyi temsil et)
- Increase scheduling priority (Zamanlama önceliğini artır)
- Load and unload device drivers (Aygıt sürücülerini yükle ve kaldır)
- Lock pages in memory (Bellekteki sayfaları kilitle)
- Log on as a batch job (Toplu iş olarak oturum aç)
- Log on as a service (Hizmet olarak oturum aç)
- Manage auditing and security log (Denetim ve güvenlik günlüklerini yönet)
- Modify firmware environment values (Üretim ortam bilgisini değiştir)
- Perform volume maintenance tasks (Birim bakım görevlerini gerçekleştir)
- Profile single process (Tek işlem profilini çıkar)
- Profile system performance (Sistem performans profilini çıkar)
- Remove computer from docking station (Bilgisayarı yerleştirme istasyonundan çıkar)
- Replace a process level token (Bir işlem düzeyi anahtarını değiştir)
- Restore files and directories (Dosya ve dizinleri geri yükle)
- Shut down the system (Sistemi kapat)
- Synchronize directory service data (Dizin servisi verisini eşitle)
- Take ownership of files or other objects (Diğer nesnelerin ve dosyaların sahipliğini al)

Yerel ilkelerin sonuncu denetim grubu olan "Security options" (Güvenlik seçenekleri) ağ erişimi ve güvenliği, aygıtlar, etki alanı denetleyicisi, etkileşimli oturum açma, hesaplar, sistem ayarları ve şifrelemesi gibi birçok ayarlamaları içerir. Güvenlik seçenekleri ile ilgili ayarlamalar **Resim 4.36'**da gösterilmiştir. **Resim 4.36**'da "Enabled" (Etkin) seçeneği tıklandığında ayarlama etkinleştirilir.



Resim 4.36: Denetim ilkesinin kullanıcı veya gruplar için uygulanması (Win 2003 Eng ⇔ Win 2003 Tr)

"Security options" (Güvenlik seçenekleri) içerisinde bulunan ayarlamalar aşağıdaki gibidir:

- **Accounts:** Administrator account status {Hesaplar: Yönetici hesap durumu}
- Accounts: Guest account status {Hesaplar: Konuk hesabı durumu}
- Accounts: Limit local account use of blank passwords to console logon only {Hesaplar: Sadece konsol oturumu açmak için yerel hesapları boş parola ile sınırla}
- Accounts: Rename administrator account {Hesaplar: Yönetici hesabının adını değiştirin}
- Accounts: Rename guest account {Hesaplar: Konuk hesabının adını değiştirin}
- **Audit:** Audit the access of global system objects {Denetle: Genel sistem nesnelerinin erişimini denetle}
- Audit: Audit the use of Backup and Restore privilege {Denetle: Yedekleme ve Geri Yükleme ayrıcalığının kullanımını denetle}
- Audit: Shut down system immediately if unable to log security audits {Denetle: Güvenlik denetimleri günlüğü tutulamazsa sistemi hemen kapat}
- **Devices:** Allow undock without having to log on {Aygıtlar: Oturum açmak zorunda olmadan çıkarmaya izin ver}
- Devices: Allowed to format and eject removable media {Aygıtlar: Çıkarılabilir ortamı biçimlendirme ve çıkartma izni var}
- Devices: Prevent users from installing printer drivers {Aygıtlar: Kullanıcıların yazıcı sürücüleri yüklemesini önle}
- Devices: Restrict CD-ROM access to locally logged-on user only {Aygıtlar: CD-ROM erişimini yalnızca yerel olarak oturum açan kullanıcıya sınırla}
- Devices: Restrict floppy access to locally logged-on user only {Aygıtlar: Disket erişimini yalnızca yerel olarak oturum açan kullanıcıya sınırla}
- Devices: Unsigned driver installation behavior {Aygıtlar: İmzasız sürücü yükleme davranışı}
- **Domain controller:** Allow server operators to schedule tasks {Etki alanı denetleyicisi: Sunucu işletmenlerinin görev zamanlarına izin ver}
- Domain controller: LDAP server signing requirements {Etki alanı denetleyicisi: LDAP sunucusu imzalama gereklilikleri}
- Domain controller: Refuse machine account password changes {Etki alanı üyesi: Makine hesabı parola değişikliklerini devre dışı bırak}
- **Domain member:** Digitally encrypt or sign secure channel data (always) {Etki alanı üyesi: Güvenli kanal verisini (her zaman) dijital olarak şifrele ya da imzala}
- Domain member: Digitally encrypt secure channel data (when possible) {Etki alanı üyesi: Güvenli kanal verisini (uygun olduğunda) dijital olarak şifrele}
- Domain member: Digitally sign secure channel data (when possible) {Etki alanı üyesi: Güvenli kanal verisini (uygun olduğunda) dijital olarak imzala}
- Domain member: Disable machine account password changes {Etki alanı denetleyicisi: Makine hesabı parola değişikliklerini reddet}
- Domain member: Maximum machine account password age {Etki alanı Üyesi: En çok makine hesap parolası yaşı}

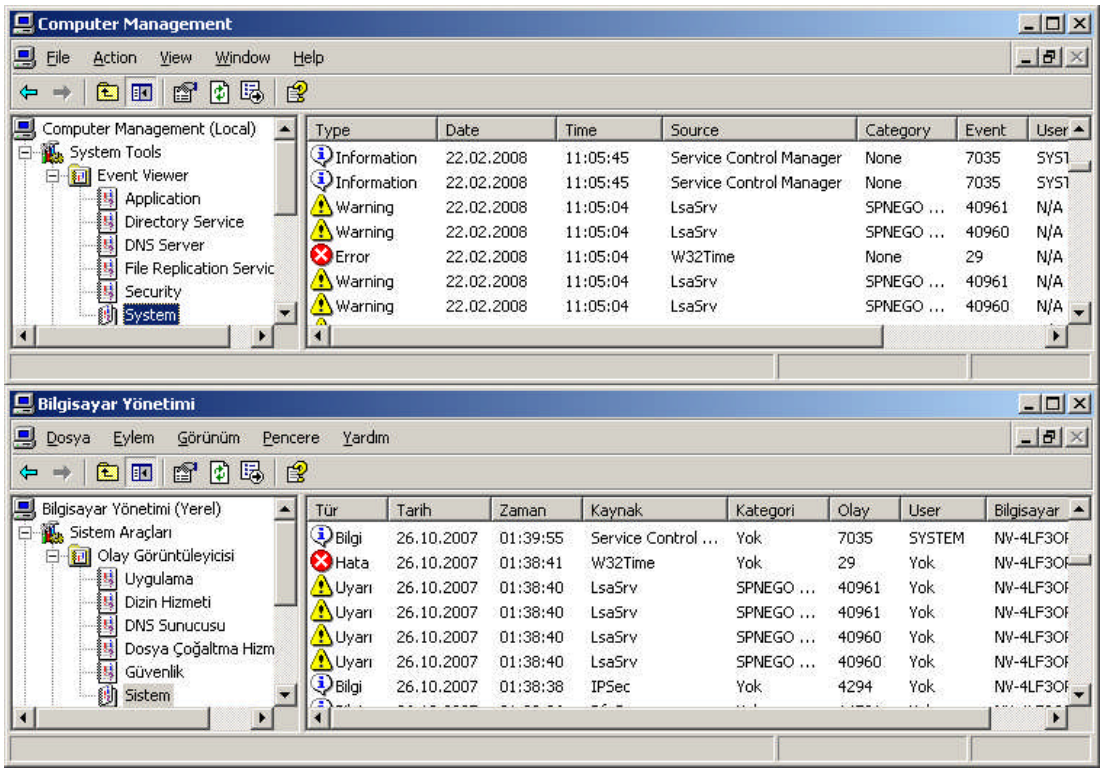
- Domain member: Require strong (Windows 2000 or later) session key {Güvenli kanal: Sağlam (Windows 2000 ya da yenisi) oturum anahtarı gerekir}
- **Interactive logon:** Do not display last user name {Etkileşimli oturum açma: Oturum açma ekranında son kullanıcının adını görüntüleme}
- Interactive logon: Do not require CTRL+ALT+DEL {Etkileşimli oturum açma:Oturum açmada CTRL+ALT+DEL gerektirme}
- Interactive logon: Message text for users attempting to log on {Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti metni}
- Interactive logon: Message title for users attempting to log on {Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti başlığı}
- Interactive logon: Number of previous logons to cache (in case domain controller is not available) {Etkileşimli oturum açma: Önbelleğe alınacak oturum açmaların sayısı (etki alanı denetleyicisinin kullanılamaması).}
- Interactive logon: Prompt user to change password before expiration {Etkileşimli oturum açma: Kullanıcıdan süresi bitmeden parola değiştirmesini iste}
- Interactive logon: Require Domain Controller authentication to unlock workstation {Etkileşimli oturum açma: İş istasyonunun kilidini açmak için Etki Alanı Denetleyicisi yetkilendirmesi kilitli değil}
- Interactive logon: Require smart card {Etkileşimli oturum açma: Akıllı kart iste}
- Interactive logon: Smart card removal behavior {Etkileşimli oturum açma: Akıllı kart kaldırma davranışı}
- **Microsoft network client:** Digitally sign communications (always) {Microsoft ağ İstemcisi: İletişimi dijital olarak imzala (her zaman)}
- Microsoft network client: Digitally sign communications (if server agrees) {Microsoft ağ istemcisi: İletişimi dijital olarak imzala (sunucu uygunsa)}
- Microsoft network client: Send unencrypted password to third-party SME servers {Microsoft ağ istemcisi: Üçüncü parti SME sunucularına şifrelenmemiş parola gönder}
- **Microsoft network server:** Amount of idle time required before suspending session {Microsoft ağ sunucusu: Oturum açma saatleri dışında istemci bağlantısını kes}
- Microsoft network server: Digitally sign communications (always) {Microsoft Ağ sunucusu: İletişimi dijital olarak imzala (her zaman)}
- Microsoft network server: Digitally sign communications (if client agrees) {Microsoft Ağ sunucusu: İletişimi dijital olarak imzala (istemci uygunsa)}
- Microsoft network server: Disconnect clients when logon hours expire {Microsoft Ağ Sunucusu: Oturumu askıya almadan önce gereken boş süre}
- **Network access:** Allow anonymous SID/Name translation {Ağ erişimi adsız SID/Name çevirisine izin ver}
- Network access: Do not allow anonymous enumeration of SAM accounts {Ağ erişimi SAM hesaplarının adsız numaralandırılmasına izin verme}
- Network access: Do not allow anonymous enumeration of SAM accounts and shares {Ağ erişimi SAM hesap ve paylaşımlarının adsız numaralandırılmasına izin verme}

- Network access: Do not allow storage of credentials or .NET Passports for network authentication {Ağ erişimi ağ kimlik doğrulaması için kimlik bilgileri veya .NET Passports bilgilerinin depolanmasına izin verme}
- Network access: Let Everyone permissions apply to anonymous users {Ağ erişimi adsız kullanıcılara diğer kullanıcıların izinleri uygulansın}
- Network access: Named Pipes that can be accessed anonymously {Ağ erişimi adsız erişilebilen adlandırılmış yöneltme}
- Network access: Remotely accessible registry paths {Ağ erişimi Uzaktan erişilebilir kayıt defteri yolları}
- Network access: Remotely accessible registry paths and sub-paths {Ağ erişimi uzaktan erişilebilir kayıt defteri yolları ve alt yolları}
- Network access: Restrict anonymous access to Named Pipes and Shares {Ağ erişimi adlandırılmış hatlara ve paylaşımlara adsız erişimi sınırlandır}
- Network access: Shares that can be accessed anonymously {Ağ erişimi Adsız bağlanılabilecek paylaşımlar}
- Network access: Sharing and security model for local accounts {Ağ erişimi yerel hesaplar için paylaşım ve güvenlik modeli}
- **Network security:** Do not store LAN Manager hash value on next password change {Ağ güvenliği: Sonraki parola değişikliğinde LAN Manager sağlama değerini depolama}
- Network security: Force logoff when logon hours expire {Ağ güvenliği: Oturum açma saatleri bitiminde oturumdan çıkmaya zorla}
- Network security: LAN Manager authentication level {Ağ güvenliği: Yerel ağ yöneticisi kimlik doğrulama düzeyi}
- Network security: LDAP client signing requirements {Ağ güvenliği: LDAP istemci imzalama gereklilikleri}
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients {Ağ güvenliği: NTLM SSP (güvenli RPC'yi içeren) tabanlı istemciler için en düşük oturum güvenliği}
- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers {Ağ güvenliği: NTLM SSP (güvenli RPC'yi içeren) tabanlı sunucular için en düşük oturum güvenliği}
- **Recovery console:** Allow automatic administrative logon {Kurtarma Konsolu: Otomatik olarak yönetim oturumu açılmasına izin ver}
- Recovery console: Allow floppy copy and access to all drives and all folders {Kurtarma Konsolu: Disket kopyalama ile tüm sürücü ve klasörlere erişime izin ver}
- **Shutdown:** Allow system to be shut down without having to log on {Kapat: Oturum açmaya gerek kalmadan sistemin kapatılmasını sağla}
- Shutdown: Clear virtual memory pagefile {Kapat: Sanal bellek disk bellek dosyasını temizle}
- **System cryptography:** Force strong key protection for user keys stored on the computer {Sistem şifrelemesi: Bilgisayarda depolanan kullanıcı anahtarlarında sağlam anahtar korumasını zorla}
- System cryptography: Use FIPS compliant algorithms for encryption hashing, and signing {Sistem şifrelemesi: Şifreleme, sağlama ve imzalama için FIPS uyumlu algoritmalar kullanın}

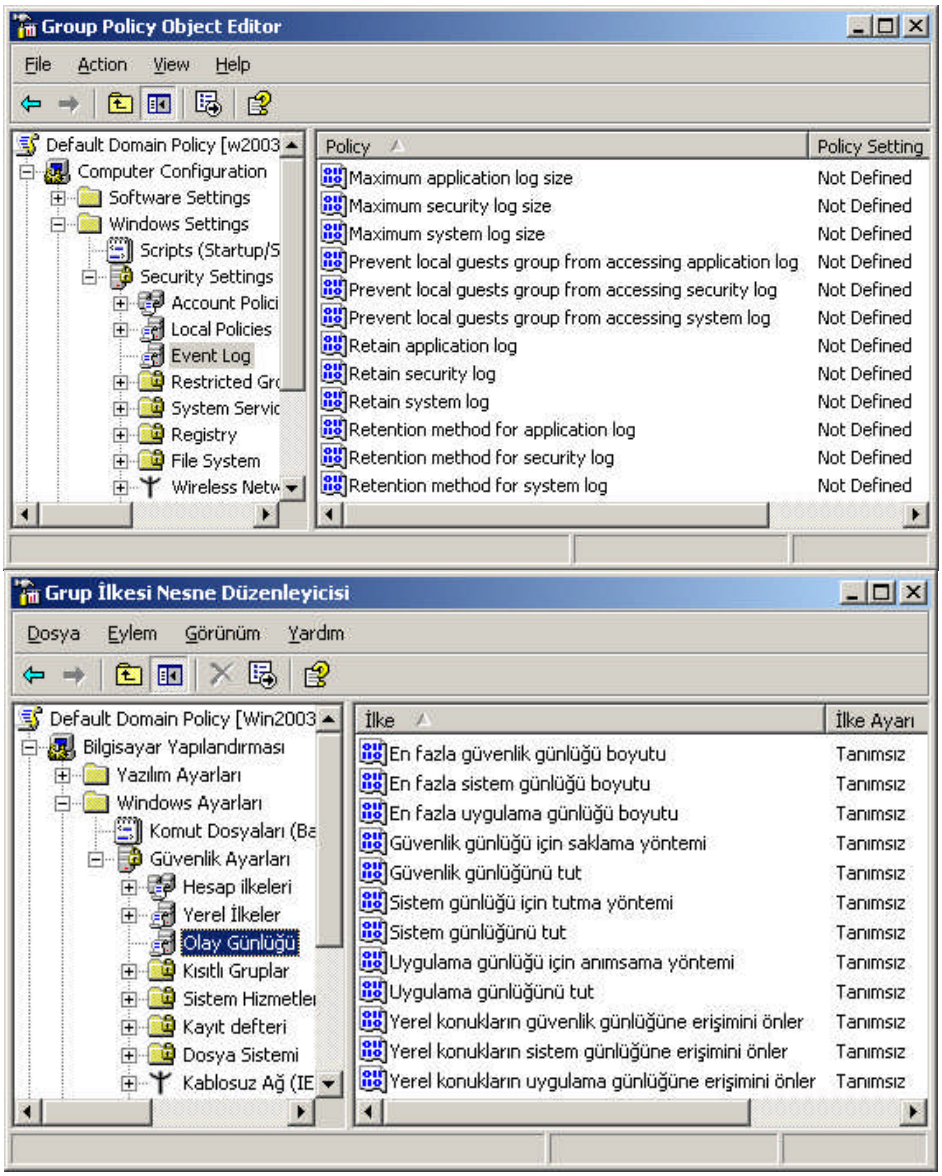
- **System objects:** Default owner for objects created by members of the Administrators group {Sistem nesneleri: Yöneticiler grubunun üyeleri tarafından oluşturulan nesnelerin varsayılan sahibi}
- System objects: Require case insensitivity for non-Windows subsystems {Sistem nesneleri: Windows olmayan alt sistemler için büyük/ küçük harf duyarlılığı gerekmesin}
- System objects: Strengthen default permissions of internal system objects {Sistem nesnesi: İç sistem nesnelerinin varsayılan izinlerini sağlamlaştır (örneğin. simgesel bağlantılar)}
- **System settings:** Optional subsystems {Sistem ayarları: Seçeneğe bağlı alt sistemler}
- System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies {Sistem ayarları: Yazılım Sınırlama İlkeleri için Windows Çalıştırılabilirlerinde Sertifika Kurallarını Kullan}

4.4. Denetleme Yönetim ve Güvenlik kayıtlarını ayarlama

Sunucu işletim sistemde bilgisayar ve kullanıcılarla ilgili oluşabilecek her türlü bilgi, uyarı ve hatalar **Resim 4.37'**de görüldüğü gibi bir olay günlüğüne kaydedilir. Olay günlüğü bilgileri kendi içerisinde uygulama, dizin hizmetleri, DNS sunucusu, dosya çoğaltma hizmetleri, güvenlik ve sistem olmak üzere sınıflara ayrılmıştır. Olay günlüğünü "My Computer=>Manage" (Bilgisayarım=>Yönet) ile veya **"Start => Administartive Tools => Event Viewer"** (Başlat => Yönetimsel Araçlar =>Olay görüntüleyicisi) ile çalıştırabiliriz. Olay günlükleri belirli aralıklarla denetlenmeli, sisteme zarar verecek durumlara karşı önlem alınmalıdır.



Resim 4.37: Olay günlükleri (Win 2003 Eng ⇔ Win 2003 Tr)

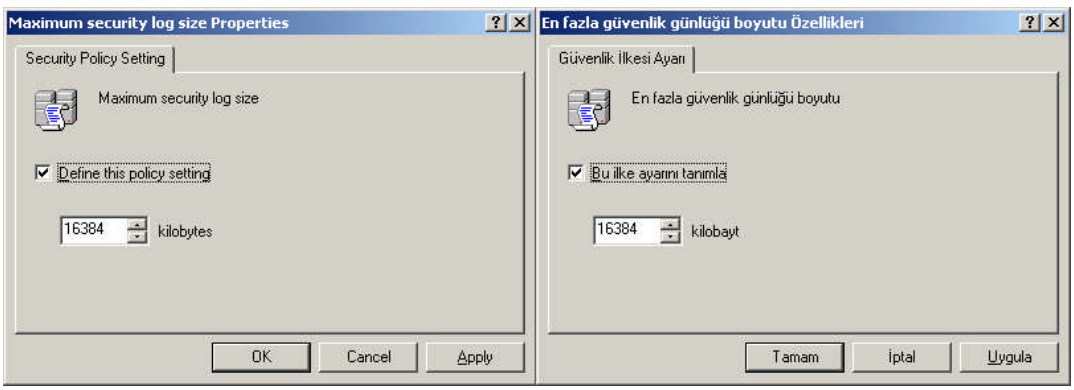


Resim 4.38: Olay günlüğü seçeneklerinin düzenlenmesi (W 2003 Eng ⇔ W 2003 Tr)

Olay günlüklerinin nasıl tutulacağı, günlük boyutu, günlük erişimi gibi çeşitli ayarlamaları da düzenleyebiliriz. Bu ayarları düzenlemek için uygulayacağımız birimim GPO'sunu çalıştırıp **Resim 4.38**'de olduğu gibi "Event Log" (Olay günlüğü) seçeneğini tıklamamız gerekir. Buradaki ayarlamalar **Resim 4.39, Resim 4.40 , Resim 4.41** ve **Resim 4.42**'de verilmiştir.

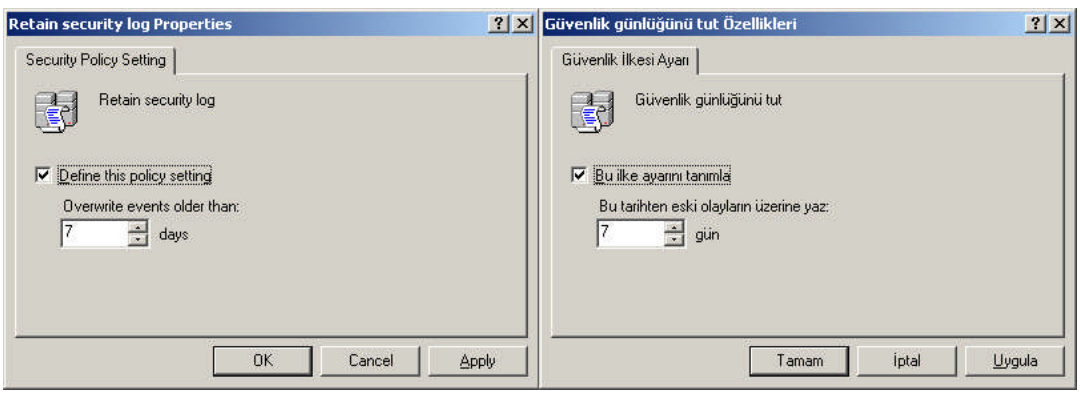
"Event Log" (Olay günlüğü) içerisinde bulunan ayarlamalar aşağıdaki gibidir:

- **Maximum application log size** {En fazla uygulama günlüğü boyutu} **Resim 4.39**'daki ile benzerdir.
- **Maximum security log size** {En fazla güvenlik günlüğü boyutu} **(Resim 4.39).**
- **Maximum system log size** {En fazla sistem günlüğü boyutu} **Resim 4.39**'daki ile benzerdir.
- **Prevent local guests group from accessing application log** {Yerel konukların uygulama günlüğüne erişimini önler} **Resim 4.40**'daki ile benzerdir.
- **Prevent local guests group from accessing security log** {Yerel konukların güvenlik günlüğüne erişimini önler} **(Resim 4.40).**
- **Prevent local guests group from accessing system log** {Yerel konukların sistem günlüğüne erişimini önler} **Resim 4.40**'daki ile benzerdir.
- **Retain application log** {Uygulama günlüğünü tut} **Resim 4.41**'deki ile benzerdir.
- **Retain security log** {Güvenlik günlüğünü tut} **(Resim 4.41).**
- **Retain system log** {Sistem günlüğünü tut} **Resim 4.41**'deki ile benzer bir işlemdir.
- **Retention method for application log** {Uygulama günlüğü için anımsama yöntemi} **Resim 4.42**'deki ile benzerdir.
- **Retention method for security log** {Güvenlik günlüğü için saklama yöntemi} **(Resim 4.42).**
- **Retention method for system log** {Sistem günlüğü için tutma yöntemi} **Resim 4.42**'deki ile benzer bir işlemdir.

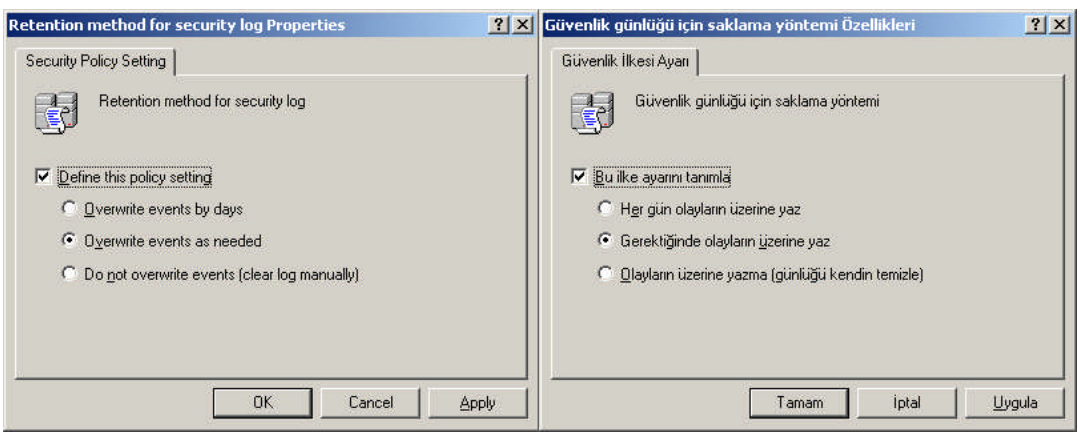


Resim 4.39: En fazla güvenlik günlüğü boyutu özellikleri (W 2003 Eng ⇔ W 2003 Tr)

Resim 4.40: Yerel konukların güvenlik günlüğüne erişimini önle özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.41: Güvenlik günlüğünü tut özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)



Resim 4.42: Güvenlik günlüğü için saklama yöntemi özellikleri (Win 2003 Eng ⇔ Win 2003 Tr)

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Sisteme "Security Templates" (Güvenlik şablonları) ve "Security Configuration and Analysis" (Güvenlik Yapılandırma ve Çözümleme) bileşenlerini yükleyerek yeni oluşturacağınız **"ozel_VT"** isimli veritabanı için **securews** şablon dosyasını seçip sisteme uygulayınız.	➢ Yüklenecek bileşenlere, nereden yüklenebileceğine, veri tabanı ismine ve organizasyon birimi ve veritabanı için şablon dosyasının seçimine dikkat ediniz.
➢ Oluşturacağımız **"kullanıcılar_5"** isimli organizasyon birimi için **"GPO_KY_1",** isminde bir politikası oluşturup bu GPO kullanan kullanıcıların en az 8 haneli parola seçip 35 saniye süreyle değiştirmesini sağlayan ve kullanıcı 3 kez parolasını yanlış girdiğinde sistemi kilitleyen ayarlamaları yapınız.	➢ Organizasyon birimi ve GPO ismine, Grup politikasının kullanıcılara nasıl bir etki yapacağına dikkat ediniz.
➢ **"kullanıcılar_6"** isimli organizasyon birimi içerisinde oluşturacağımız **"user_1" , "user_2"** ve **"user_3"** kullanıcılarından yalnız **"user_2"** ve **"user_3"** kullanıcılarının bilgisayara ağ üzerinden erişmesini, yerel olarak oturum açmaya izin verilmesini, sistem saatini değiştirmesini sağlayan kullanıcı hakları atamasını gerçekleştiriniz.	➢ Organizasyon birimi ve kullanıcı isimlerine, Grup politikasının kullanıcılara nasıl bir etki yapacağına dikkat ediniz.
➢ **"kullanıcılar_7"** isimli organizasyon birimi içerisinde tüm kullanıcıların yazıcı sürücüleri yüklemesini önleyen, Oturum açma saatleri bitiminde oturumdan çıkmaya zorlayan, **"GPO_KA_2",** isminde bir Grup politikası oluşturunuz.	➢ Organizasyon birimi ve GPO isimlerine, Grup politikasının kullanıcılara nasıl bir etki yapacağına dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorular için doğru cevap seçeneklerini işaretleyiniz.

1. Sistem güvenliği önlemlerinden hangisi doğrudan veri kayıplarını önlemeye yönelik **değildir?**
A) Belirli periyotlarla sistem yedeğinin alınması
B) Güncel virüs koruma programlarının kullanılması
C) Sisteme veri giriş çıkışlarının kontrol edilmesi
D) İzinsiz ve denetimsiz yazılım yüklenmesinin engellenmesi
E) Yönetimin belirli bölümlere ayrılması ve kullanıcılara paylaştırılması

2. Aşağıdakilerden hangisi güvenlik şablonu dosyalarından **değildir?**
A) securedc **B)** systems security
C) securews **D)** compatws **E)** setup security

3. İşletim sistemi biriminin köküne uygulanan ve alt nesnelere doğru yayılan güvenlik şablonu dosyası aşağıdakilerden hangisidir?
A) hisecws **B)** compatws
C) hisecdc **D)** rootsec **E)** DC security

4. Denetleme, kullanıcı hakları ve güvenlik seçeneklerinin bulunduğu güvenlik şablonu dosyası ilkeleri aşağıdakilerden hangisidir?
A) Local Policy **B)** Account Policy
C) File Systems **D)** Systems Services **E)** Restricted Groups

5. Aşağıdakilerden hangisi "Parola ilkesi" seçeneklerinden **değildir?**
A) Maximum password age
B) Minimum password age
C) Maximum password length
D) Minimum password length
E) Enforce password history

6. Aşağıdakilerden hangisi kullanıcının yanlış parola girişlerinde hesabı kilitleme süresini ayarlayan Hesap ilkesidir?
A) Account lockout time
B) Account lockout threshold
C) Enforce user logon
D) Reset account lockout
E) Account lockout duration

7. Aşağıdakilerden hangisi Kerberos ilkesi seçeneklerinden **değildir?**
A) Maximum tolerance for computer clock synchronization
B) Enforce user logon restrictions
C) Maximum lifetime for user ticket
D) Minimum lifetime for user ticket
E) Maximum lifetime for user ticket renewal

8. Aşağıdakilerden hangisi oturum olaylarını denetleyen Denetim ilkesi seçeneğidir?
A) Audit account events **B)** Audit system events
C) Audit security events **D)** Audit aplication events **E)** Audit logon events

9- Aşağıdakilerden hangisi Güvenlik günlüğü için saklama yöntemi belirleyen "Event Log" Olay günlüğü seçeneğidir?
A) Retain system log
B) Maximum security log size
C) Retention method for security log
D) Retain security log
E) Prevent local guests group from accessing security log

10- Aşağıdakilerden hangisi Güvenlik günlüklerini saklama yöntemlerindendir?
A) Her gün olayları üzerine yaz
B) Her hafta olayları üzerine yaz
C) Her ay olayları üzerine yaz
D) Her saat olayları üzerine yaz
E) Her oturum açıldığında olayları üzerine yaz

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ (YETERLİK ÖLÇME)

DEĞERLENDİRME KRİTERLERİ		Evet	Hayır
1	Bilgisayara Active Directoryi sorunsuz yükleyebildiniz mi?		
2	DNS ve Etki alan adlarını belirleyebildiniz mi?		
3	Active Directory içerisindeki kullanıcı izinlerini düzenleyebildiniz mi?		
4	Etki alanı içine yeni Organizasyon birimi oluşturabildiniz mi?		
5	Bilgisayara Yerel Grup Politikalarını yükleyebildiniz mi?		
6	Yeni Grup Politikası oluşturabildiniz mi?		
7	Etki alanına yeni Grup Politikası ekleyebildiniz mi?		
8	Organizasyon birimine yeni Grup Politikası ekleyebildiniz mi?		
9	Grup Politikası izinlerini düzenleyebildiniz mi?		
10	Grup Politikası özelliklerini düzenleyebildiniz mi?		
11	Grup Politikasında kullanıcı özelliklerini düzenleyebildiniz mi?		
11	Grup Politikasında bilgisayar özelliklerini düzenleyebildiniz mi?		
12	Grup politikası ile script atama işlemini gerçekleştirebildiniz mi?		
13	Grup Politikasında güvenli ayarlarını düzenleyebildiniz mi?		
14	GPO ile klasör yönlendirme işlemini gerçekleştirebildiniz mi?		
15	Güvenlik Şablonu bileşenlerini sisteme ekleyebildiniz mi?		
16	Güvenlik Şablonu dosyasını sisteme uygulayabildiniz mi?		
17	GPO ile hesap ilkelerini düzenleyebildiniz mi?		
18	GPO ile yerel ilkeleri düzenleyebildiniz mi?		
19	Olay günlüklerini görüntüleyebildiniz mi?		
20	Olay günlükleri ayarlarını düzenleyebildiniz mi?		

DEĞERLENDİRME

Uygulamalı testteki cevaplarınızın tümü “Evet” olmalıdır. Eğer “Hayır” cevabınız varsa uygulamayı tekrar ediniz.Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

Sunucu İşletim Sistemi – 4 modülü faaliyetleri ve araştırma çalışmaları sonunda; kazandığınız bilgi ve becerileri ölçme soruları ile değerlendiriniz. Bu değerlendirme sonucuna göre bir sonraki modüle geçebilirsiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

Sorular	Cevaplar
1	D
2	C
3	A
4	E
5	B
6	D
7	A
8	E
9	D
10	C

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

Sorular	Cevaplar
1	D
2	Y
3	D
4	Y
5	D
6	D
7	Y
8	D
9	D
10	Y

ÖĞRENME FAALİYETİ-3'ÜN CEVAP ANAHTARI

Sorular	Cevaplar
1	D
2	B
3	E
4	C
5	A
6	E
7	C
8	B
9	D
10	A

ÖĞRENME FAALİYETİ-4'ÜN CEVAP ANAHTARI

Sorular	Cevaplar
1	E
2	B
3	D
4	A
5	C
6	B
7	D
8	E
9	C
10	A

KAYNAKÇA

- İNAN Yüksel, DEMİRLİ Nihat, **Windows Server 2003 & Windows XP, PALME Yayıncılık,** Ankara, 2003.
- STANEK William R. , **Windows Server 2003, ARKADAŞ Yayıncılık,** 2003.
- **http://www.microsoft.com/turkiye/**
- Windows Server 2003 Türkçe Sürümü Yardım Dosyaları