canyoupwn.me

# TR | Group Policy

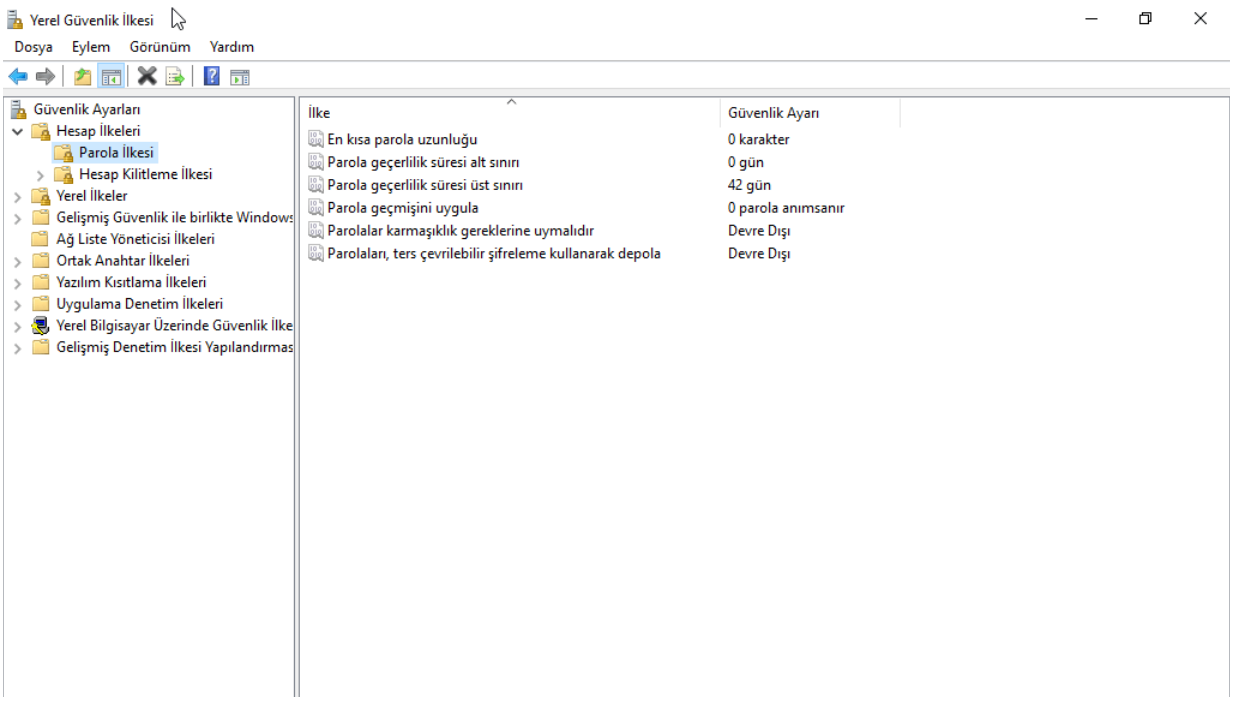
*CypmUni İYTE*

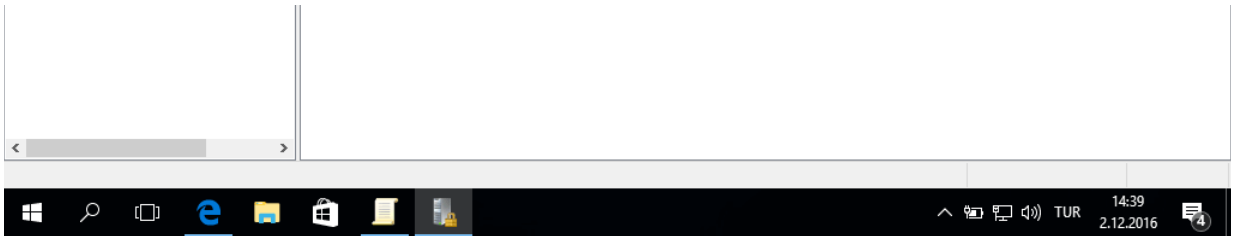
Group Policy; ihtiyaçlar doğrultusunda güvenlik ayarları, kısıtlamalar, standart konfigürasyonlar, kullanıcı güvenliği gibi işlemlerin gerçekleştirildiği, merkezi yönetimi kolaylaştıran bir takım düzenlemelerin yapıldığı bölümdür. Group Policy, Active Directory ile gelen bir özelliktir. Group Policy domain seviyesinde ve organizational unit seviyesinde uygulanır. Farklı organizational unitler oluşturup bunlara organizational unit seviesinde Group Policy uygulamak çok daha kolay olmaktadır. Örneğin 2000 bilgisayara aynı programı yüklemeniz veya kaldırmanız gerekirse ayrı ayrı yapmak kesinlikle çok zor olacağı için kısayol bulmalısınız. Böyle durumlarda aynı program yüklenecek bilgisayarlar aynı organizational unitlere eklenirse kolaylıkla toplu kurulum yapılabilir, yönetim sağlanabilir.

**Group Policy Management (Temel Güvenlik Ayarları)**

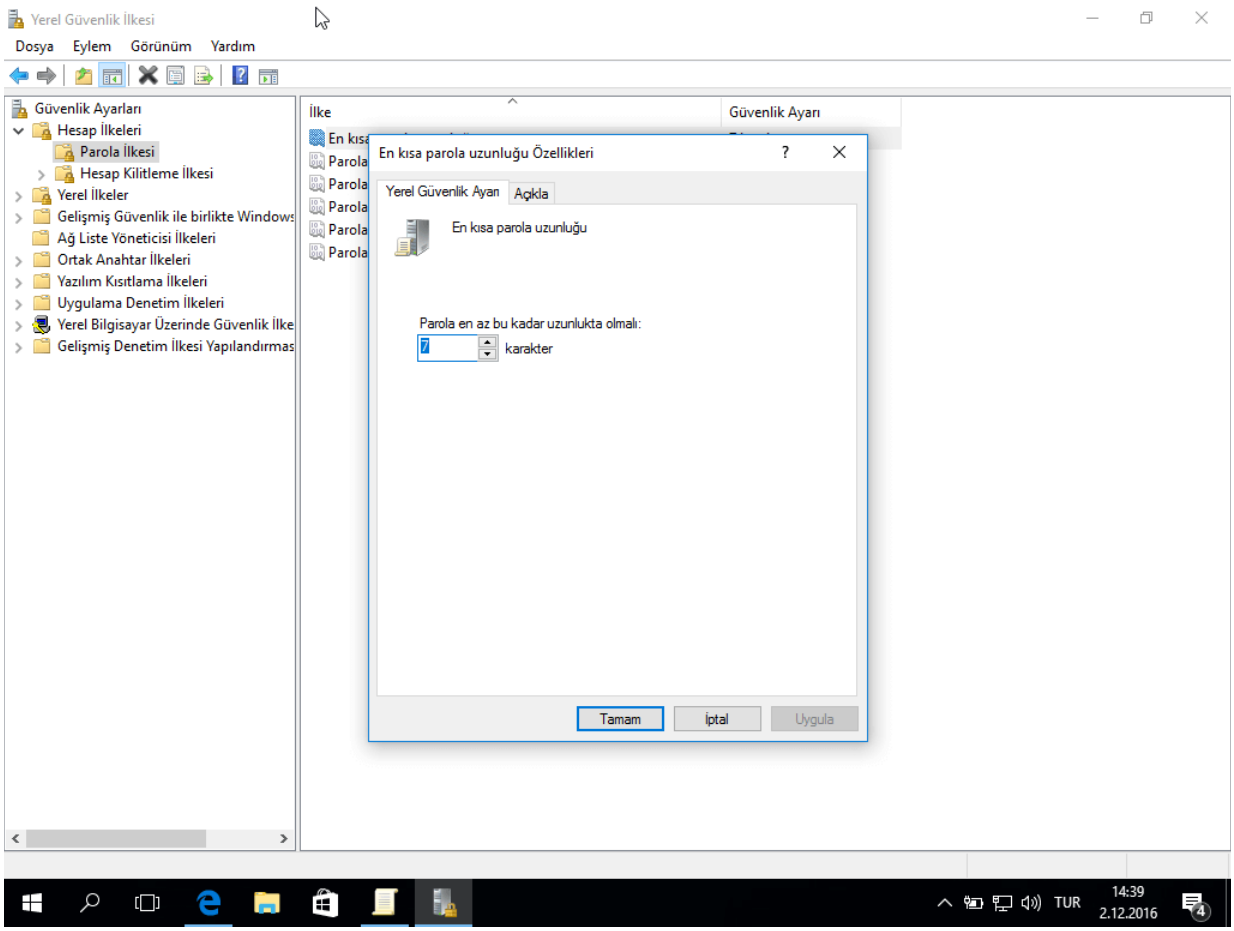
**Password Policy (Parola İlkesi)**

**Yerel güvenlik ilkesi > güvenlik ayarları > hesap ayarları > parola ilkesi** yolu izlenerek buraya ulaşılır. Buradaki password policy(parola ilkesi) bilgisayar ayarları altında çalışan bilindik bir policy tipidir. Domaine üye bilgisayarlarda oturum açabilen kullanıcılarla ilgili  uygulanabilecek bütün kuralları içerir.



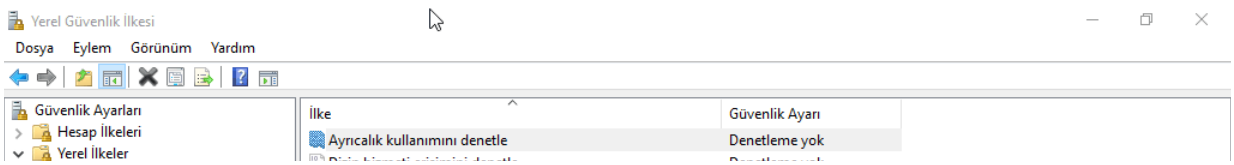


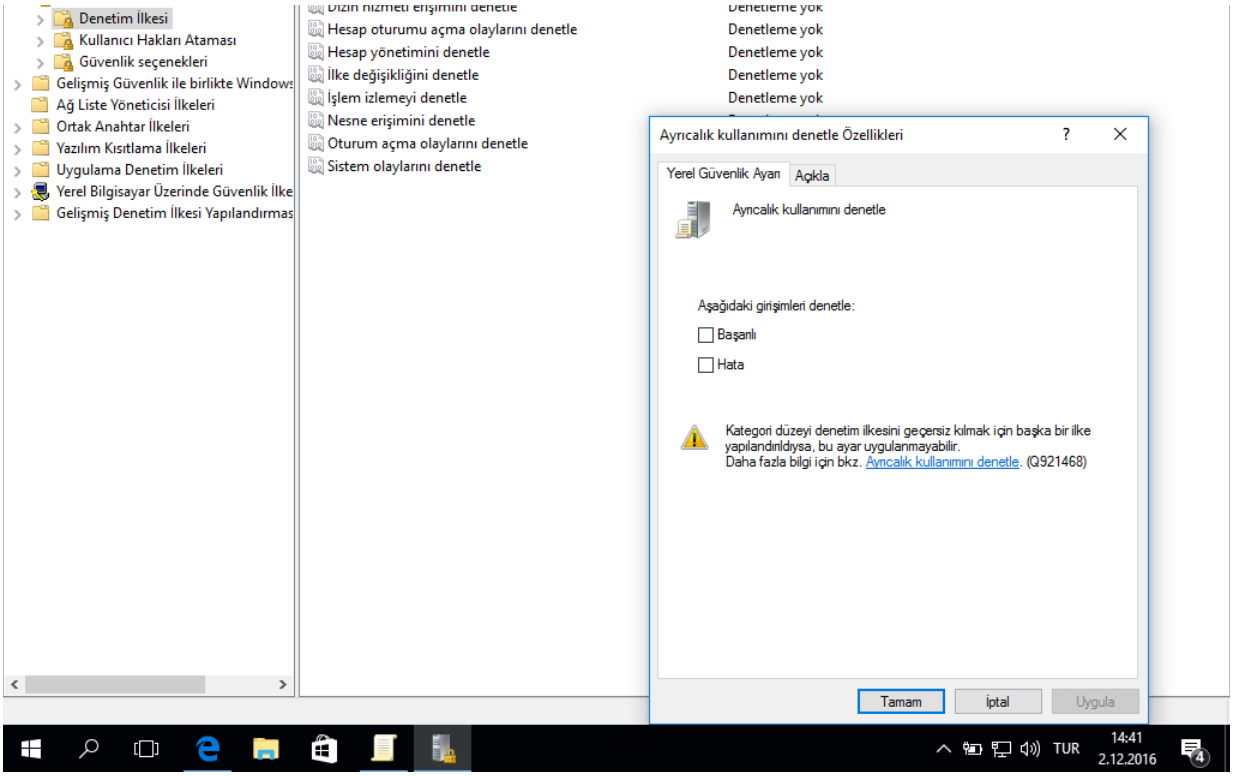
Burada parolamız ile ilgili her türlü güvenlik tedbirini alabiliriz. Parolanın geçerlilik süresini ayarlayabilir, parolamızı güçlendirebiliriz. Aynı zamandan parolamızın minimum uzunluğunu da buradan ayarlayabiliriz.




**Denetim İlkesi(Audit Policy)**

**Yerel güvenlik ilkesi > güvenlik ayarları > denetim ilkesi** ile de domain ortamında olan biteni görebileceğimiz policy bölümü olan denetim ilkesine geliriz. Bu bölümde dizin hizmeti, hesap yönetimi, nesne erişimi, oturum açma vb. olayları denetleyerek daha güvenli hale getirebiliriz.

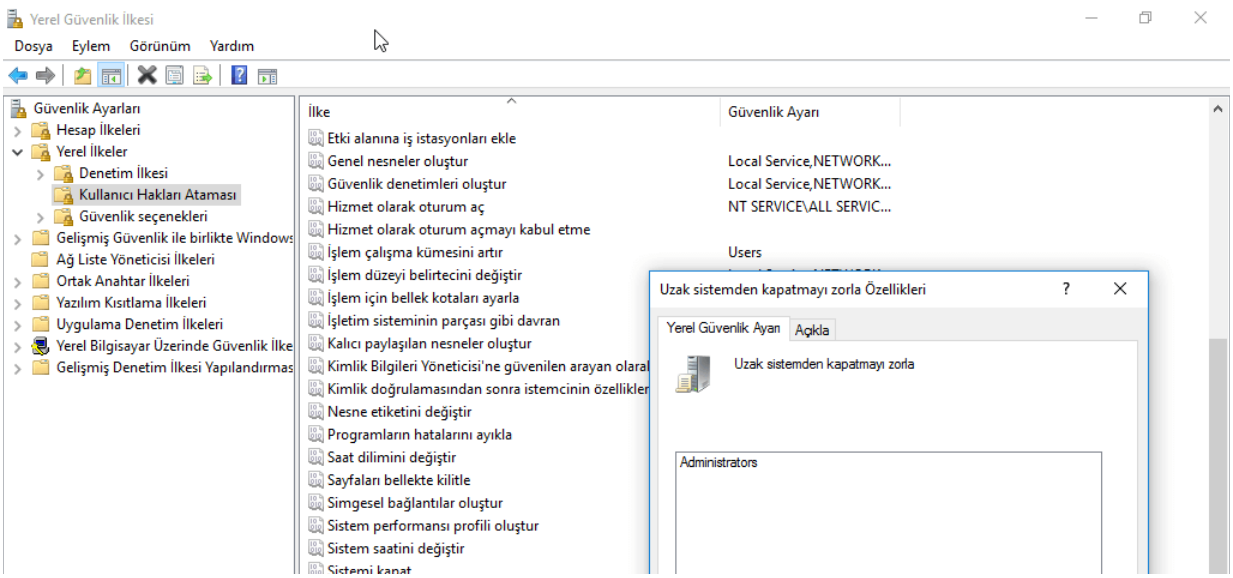


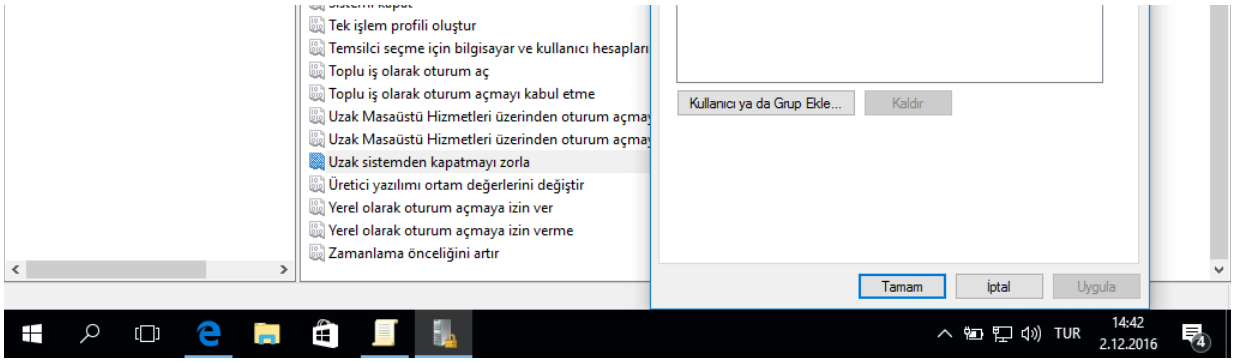



**Kullanıcı Hakları Aşaması(User Right Assignment)**

Kullanıcı haklarıyla ilgili tedbirlerin alındığı yerdir. Aygıt sürücüleri, belirteçler, bilgisayara ağ üzerinden bağlantı, nesne etiketleri gibi birçok ilke olmakla birlikte önemli ilkelerden uzak sistemden kapatmaya zorla ve aynı oturumda farklı bir kullanıcı için bir kimliğe bürünme ilkelerinin örneklerini alacağız.

**Yerel güvenlik ilkesi > güvenlik ayarları > yerel ilkeler > kullanıcı hakları ataması** yolunu izleyerek bu sayfaya geliriz. Burada istenilen ayarlar yapılabilir. Uzak sistemden kapatmak için buraya kullanıcı adı girilmelidir. Çünkü Administrator dışında herhangi bir kullanıcı böyle bir hakka sahip değildir.



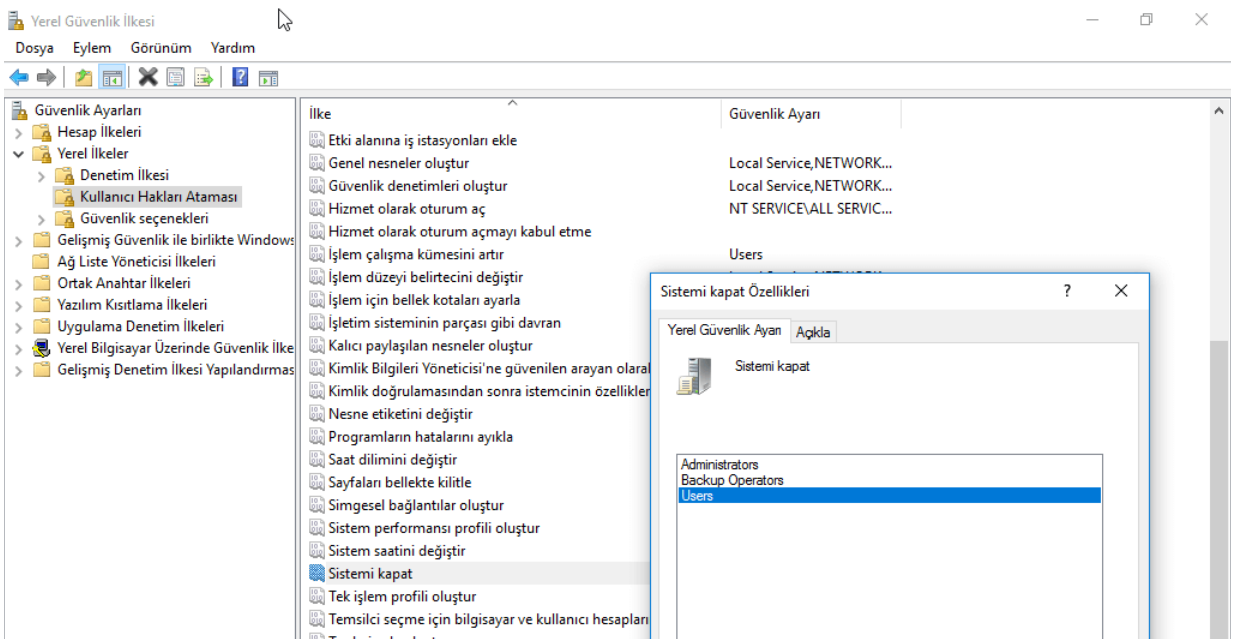


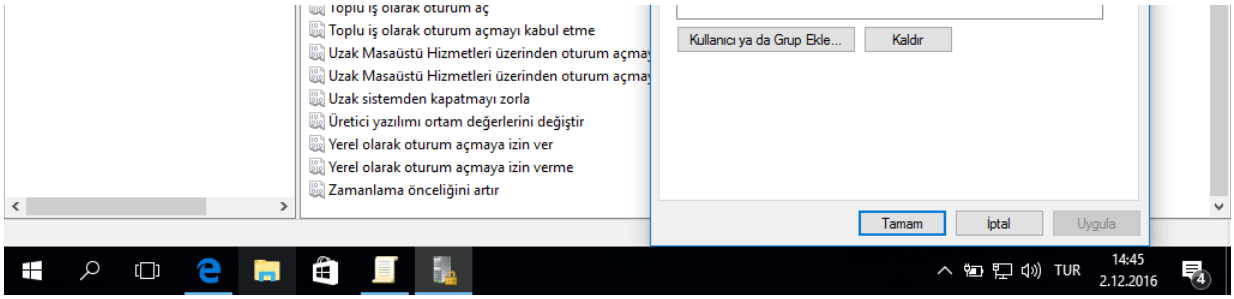

Aynı oturumda farklı bir kullanıcı için bir kimliğe bürünme ilkesi için

**Yerel güvenlik ilkesi > güvenlik ayarları > yerel ilkeler > kullanıcı hakları** ataması yolunu izleyerek yine şekildeki sayfaya ulaştık. Burada da diğer ilkelerde olduğu gibi kullanıcıya yetki vermemiz gerekiyor. Kullanıcı adımız olan “amele” yi buraya yazarak adları denetle diyoruz ve tamam diyerek bu hakkı amele kullanıcısı ile paylaşmış oluyoruz.

Kullanıcı hakları aşamasında dikkat etmemiz gereken birkaç ilkeyi şöyle sıralayabiliriz:

- Çapraz geçiş denetimi
- Saat dilimi kontrolü
- Sayfaları bellekte kilitleme
- Kalıcı paylaşılan nesneler
- Aynı oturumda farklı bir kullanıcı için bir kimliğe bürünme
- Sistemi kapatmak
- Toplu iş ilkeleri
- Yerel olarak oturum açma
- Zamanlama önceliği



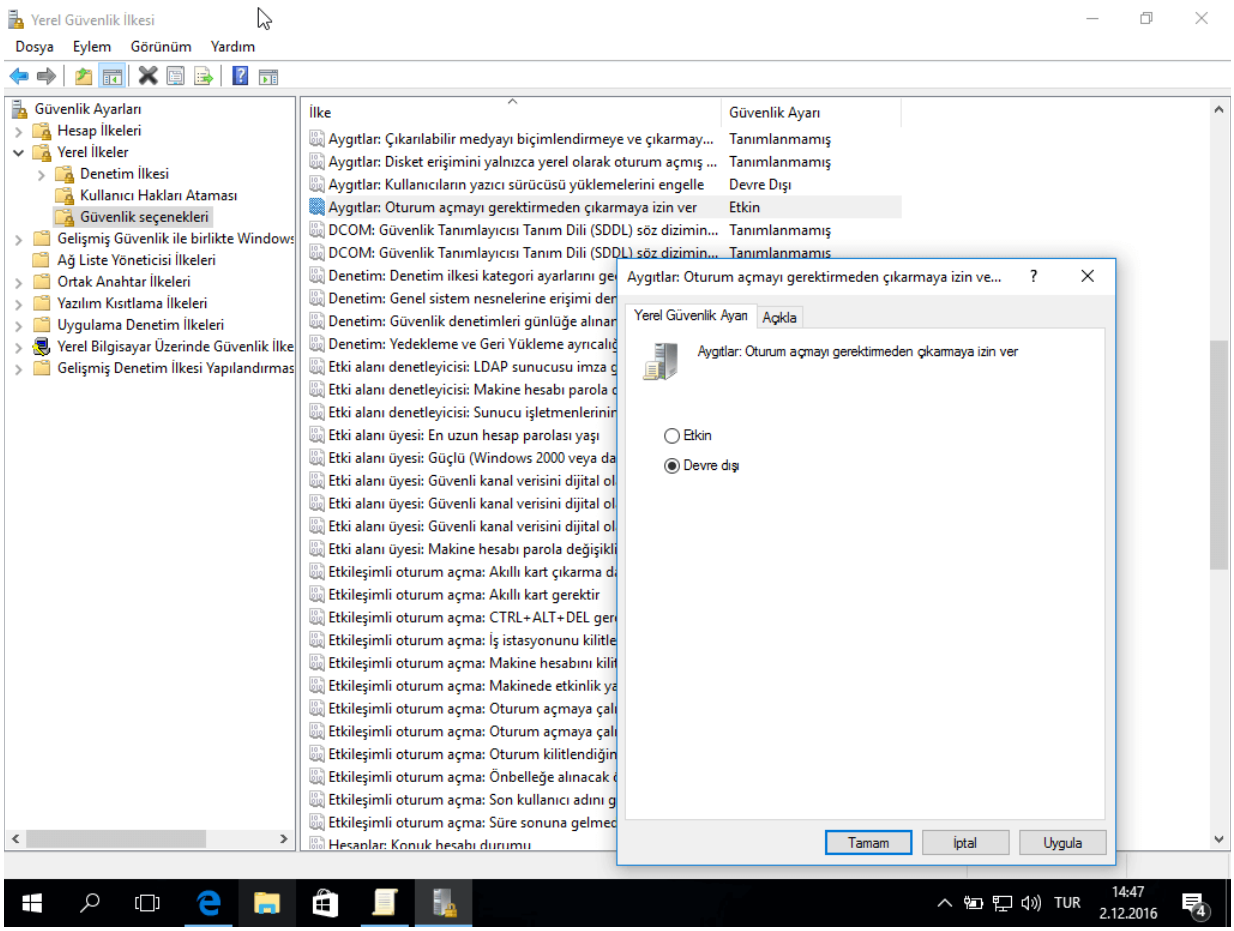



Bu ilkelere öncelik vererek bütün ilkeleri gözden geçirmeliyiz.

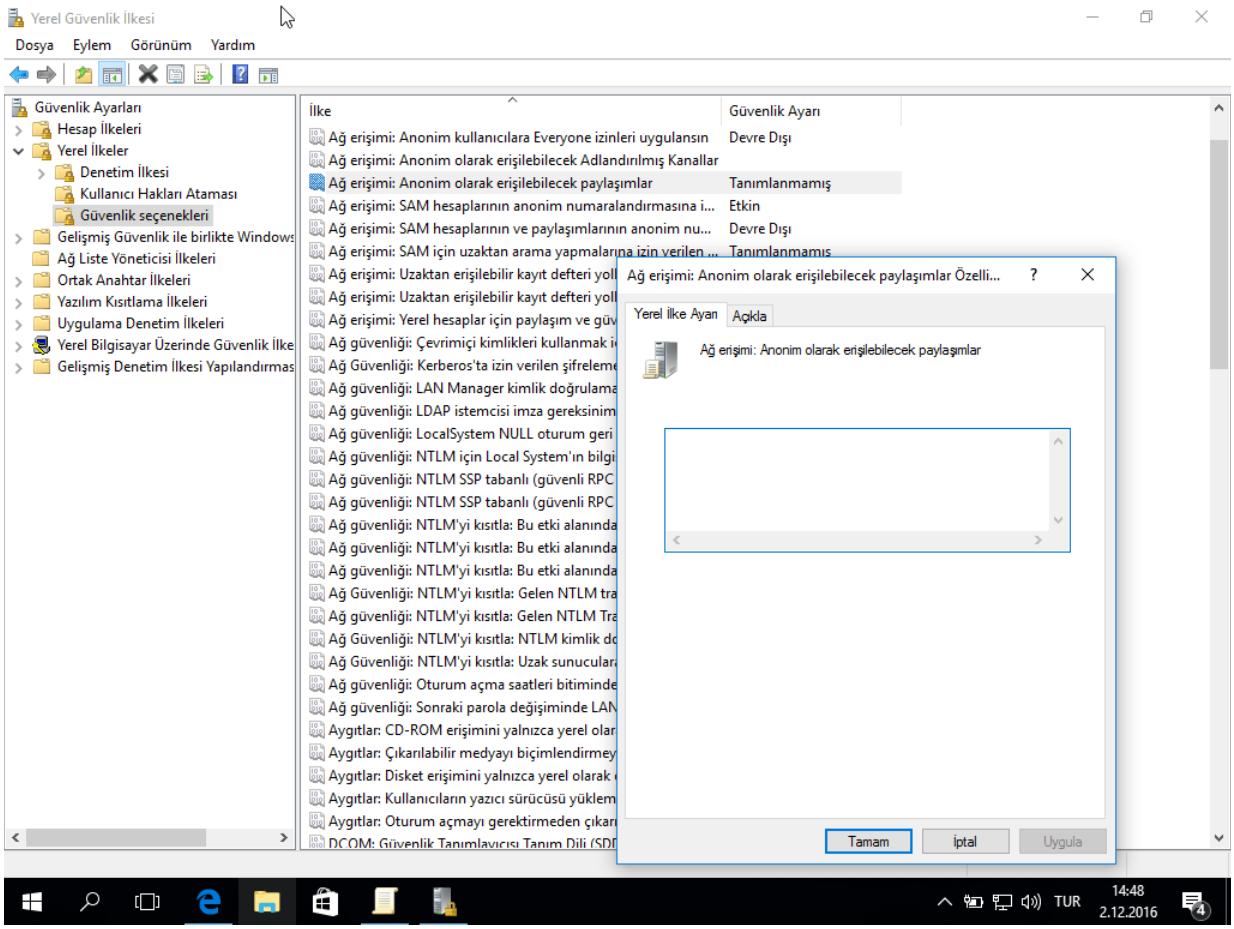
### Güvenik Seçenekleri(Security Options)

Burada çok fazla ayar yapılabilir. Kişisel güvenlik için çok önemli seçenekler vardır. Dikkatli bir şekilde seçim yapılmalıdır.

**Yerel güvenlik ilkesi> güvenlik ayarları > yerel ilkeler> güvenlik seçenekleri** diyerek bu sayfaya erişiriz. Konuk hesabı ile ilgili ayarlar, kullanıcı hesabı denetimi, etkileşimli oturum açma, Microsoft ağ istemcisi ve sunucusu, ağ erişimi , ağ güvenliği, aygıtlar vb birçok önemli konuda birçok alt dalda konfigürasyonlar vardır.

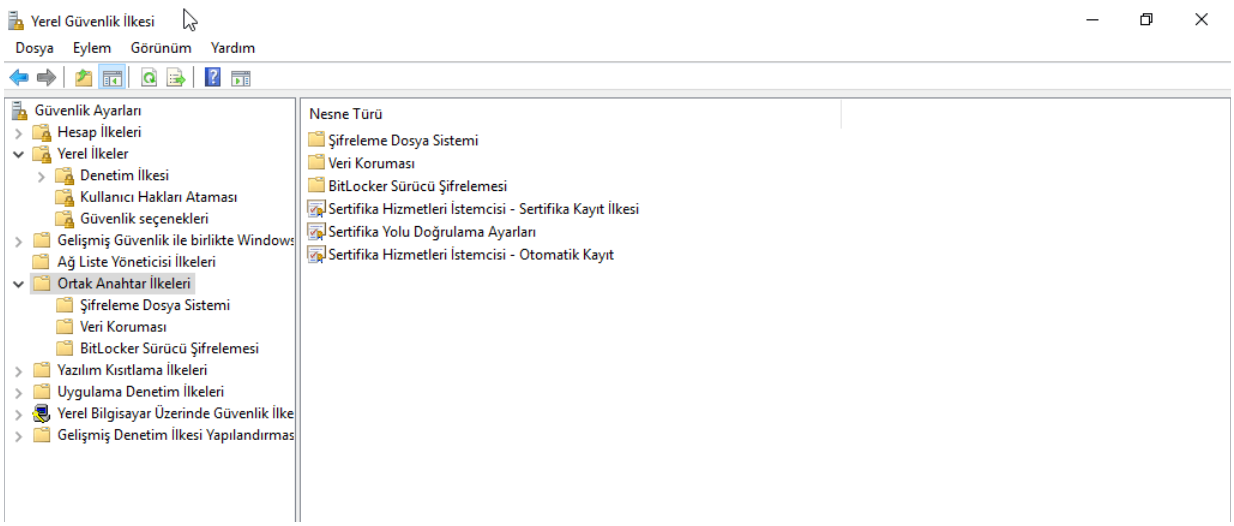


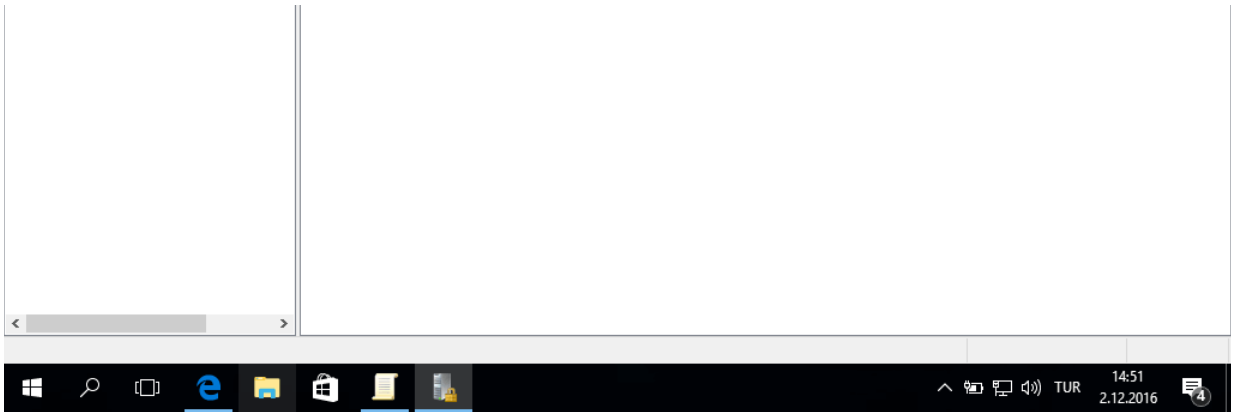
Burada aygıtları oturum açma gibi işlemler yapmadan çıkarma işlemi için izin ayarları var.




### Ortak Anahtar İlkesi(Public Key Policies)

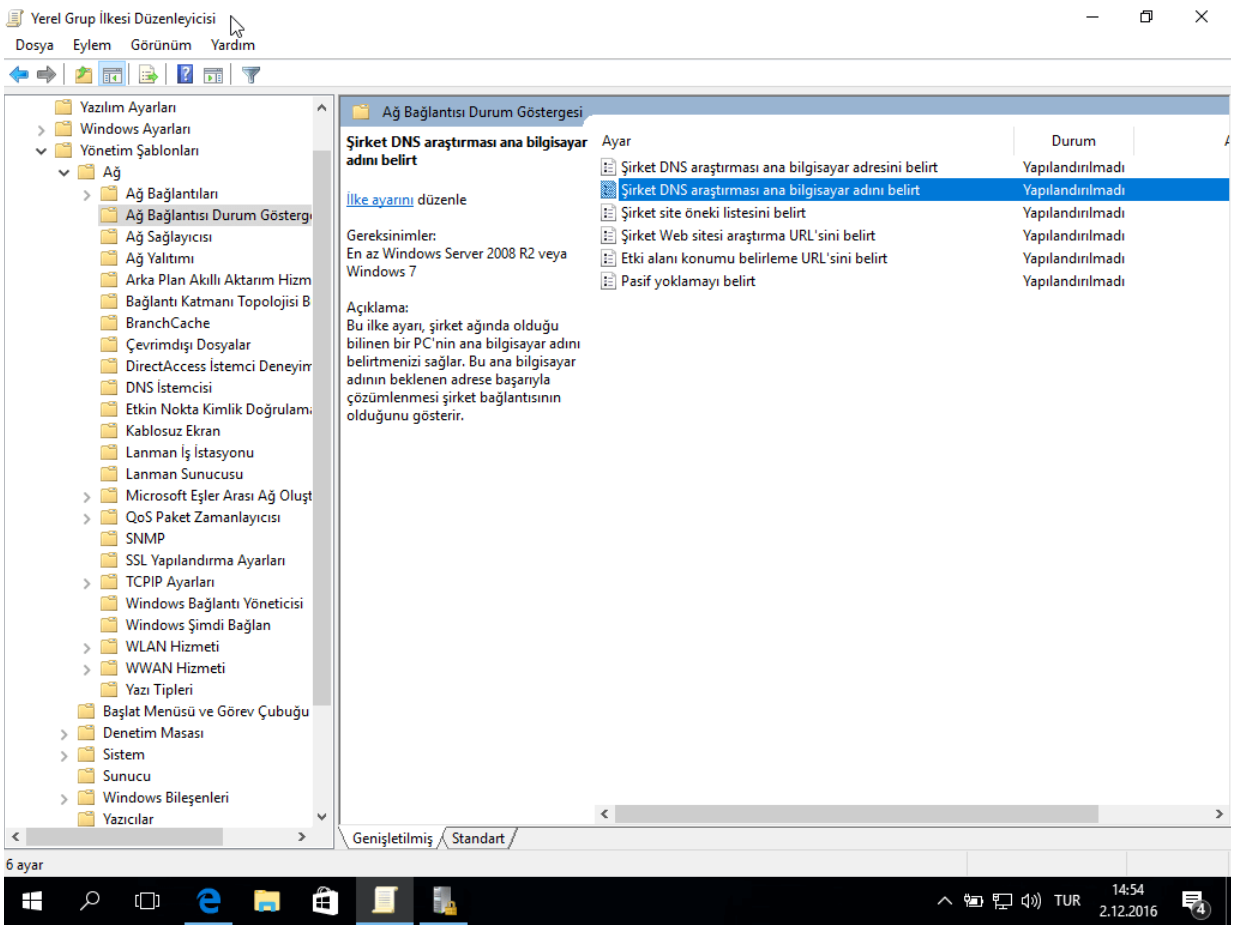
Bu ilke sayesinde her türlü şifreleme ayarları yapabiliriz. Şifreleme algoritma türü veri koruması vb. birçok şifre ayarlarını yapılandırabiliriz.
**Yerel güvenlik ilkesi > güvenlik ayarları > ortak anahtar ilkeleri** diyerek bu sayfaya ulaşabiliriz.





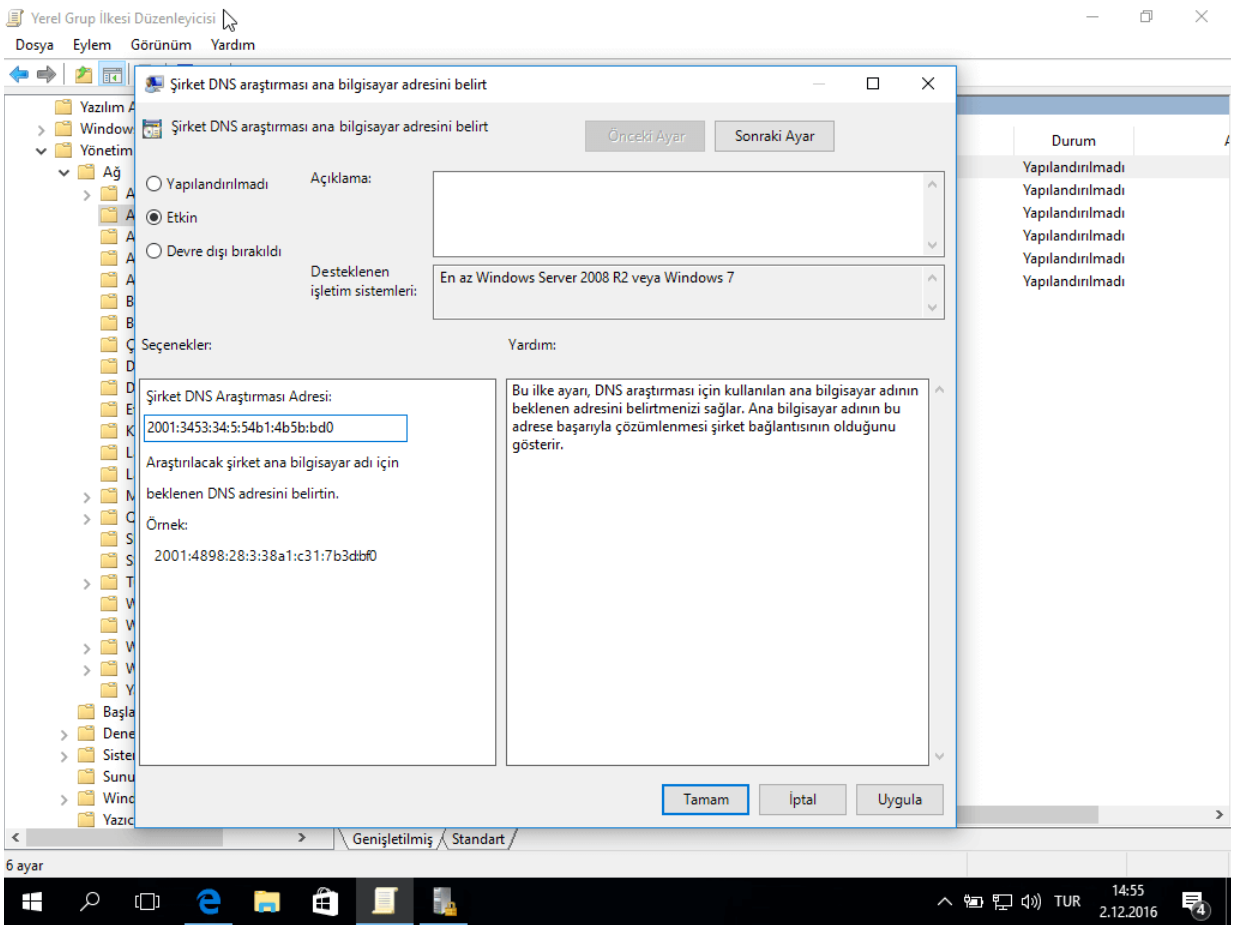
### Ağ(Network)

**Yerel güvenlik ilkesi > güvenlik ayarları > administrator şablonları > ağ yolu** ile bulunur ve sistemdeki ağ güvenliği hakkında yapılandırmamız gereken ayarları içerir. DNS Server ayarlamalar vb. burada yapılır.




Burada şirket vb. topluluklar için ortak DNS adresi atayabiliriz. Burada şirket DNS araştırma adresi yazan yere adresi yazarız. DNS araştırması için kullanılan ana bilgisayarın adının beklenen adresini belirtmemizi sağlar. Ana bilgisayar adının bu adrese başarıyla çözümlenmesi şirket bağlantısının

olduğunu gösterir.




Bu bölümde her türlü güvenlik ilkelerini kullanarak Windows işletim sistemimizi çok daha güvenilir hale getirerek sıkılaştırabiliriz.

Bize uygun olan ayarları Group Policy sayesinde yaparak sistemimizi dış saldırılardan koruyabiliriz.