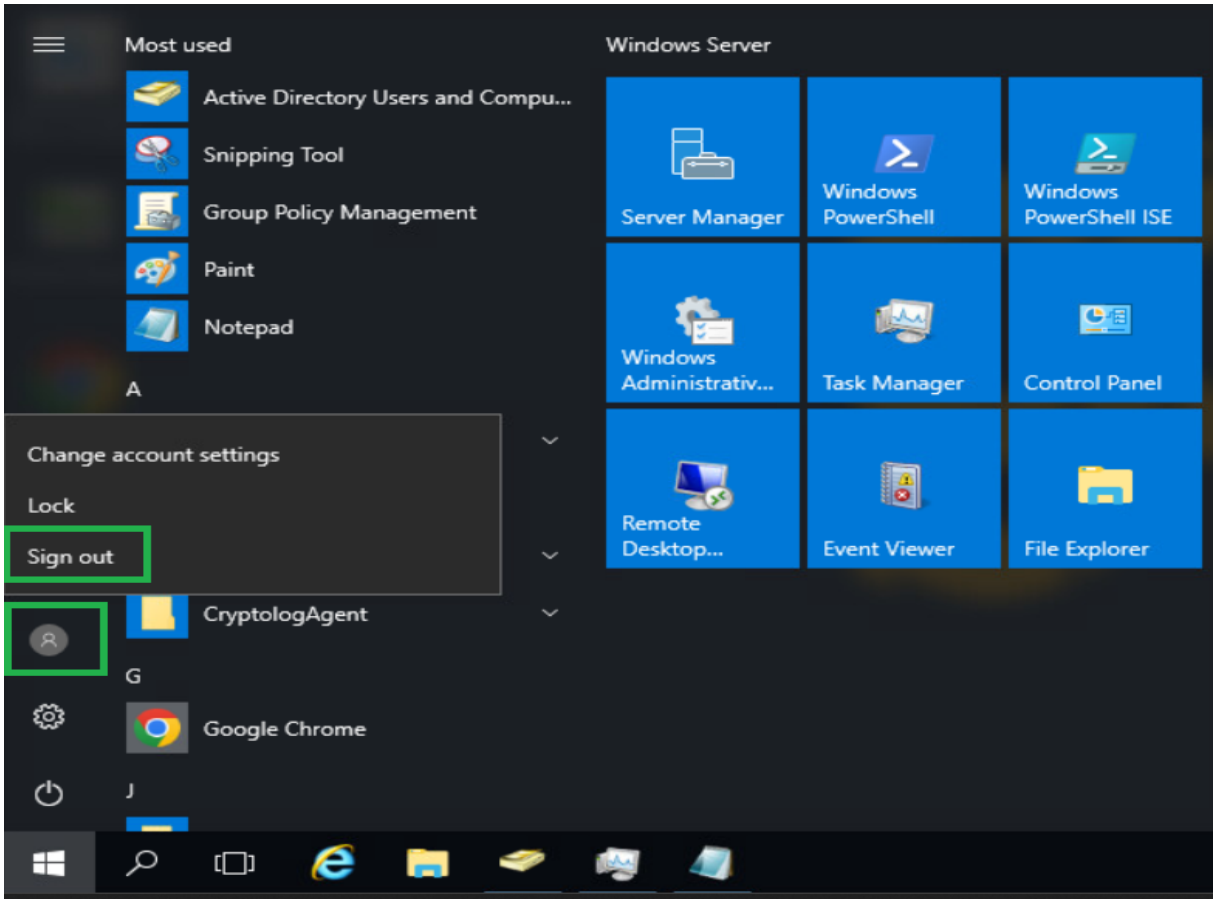
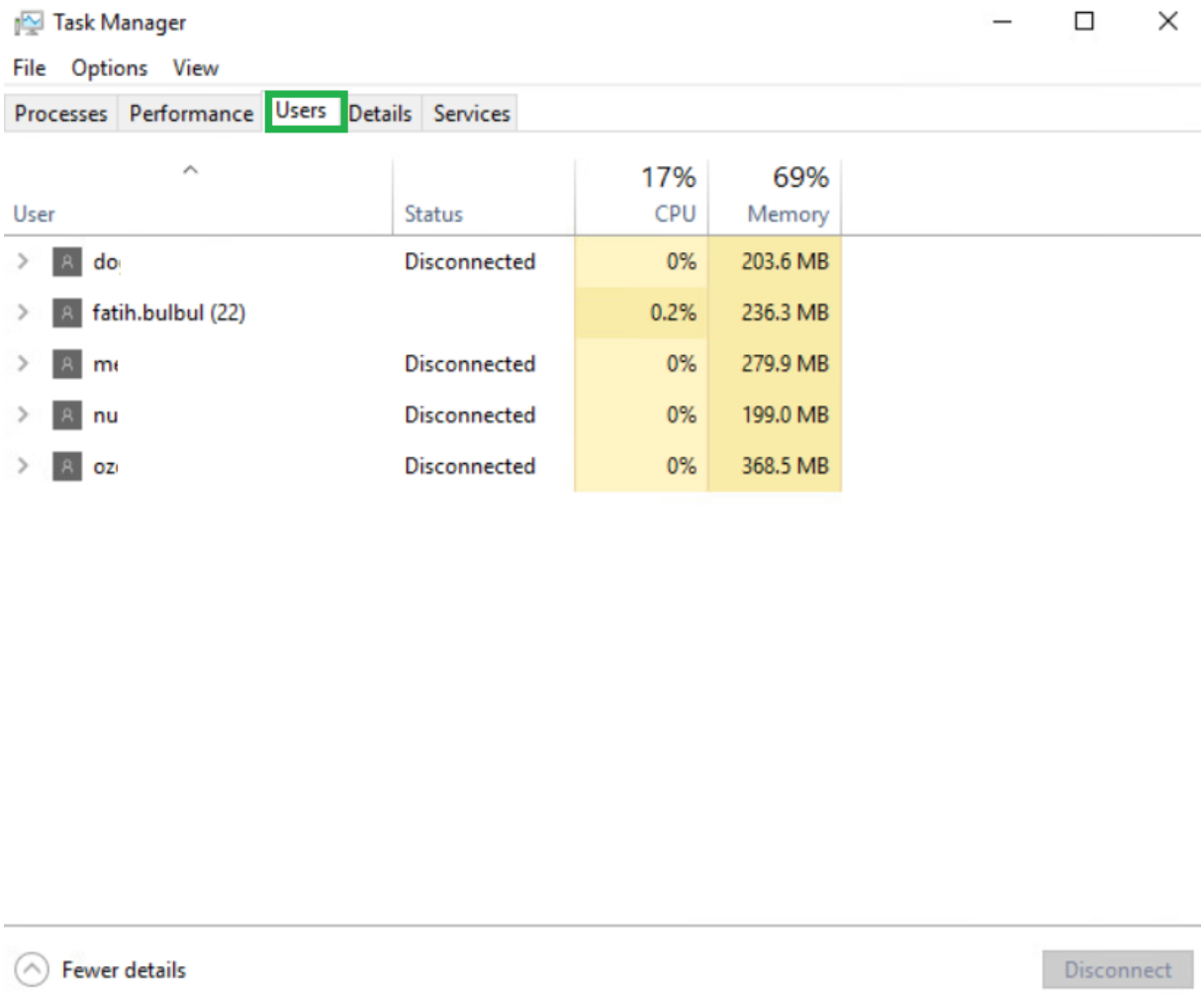
RDS Session Time Limits Ayarları

Çoğu firmada eksik gördüğüm bir konuya değinmek istiyorum bugün. Büyük bir çoğunluğumuz bir sunucuya “RDP” ile bağlandığımızda üst köşedeki çarpı butonuna basıp öyle çıkış yapıyoruz.

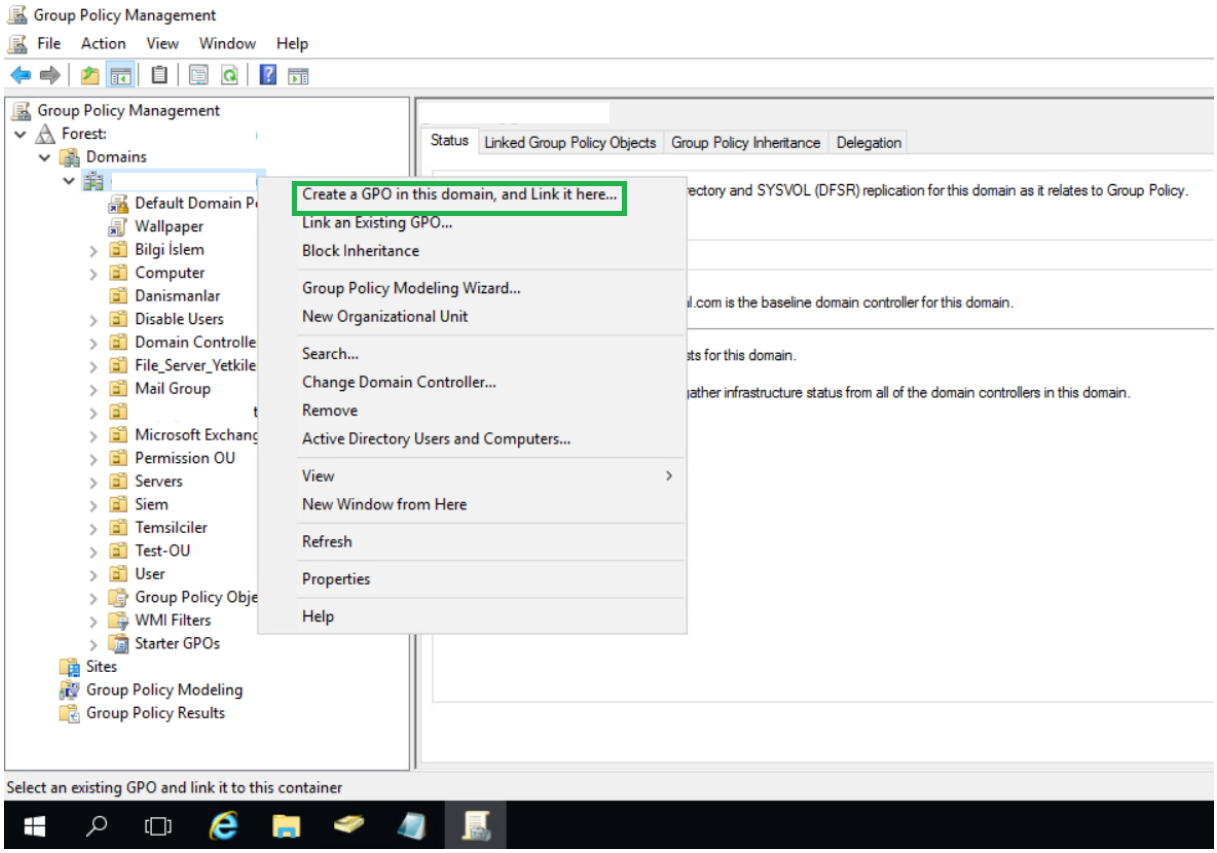
Peki ne yapmamız gerekiyor, Çarpı butonuna basmak yerine sing out olmamız gerekiyor.



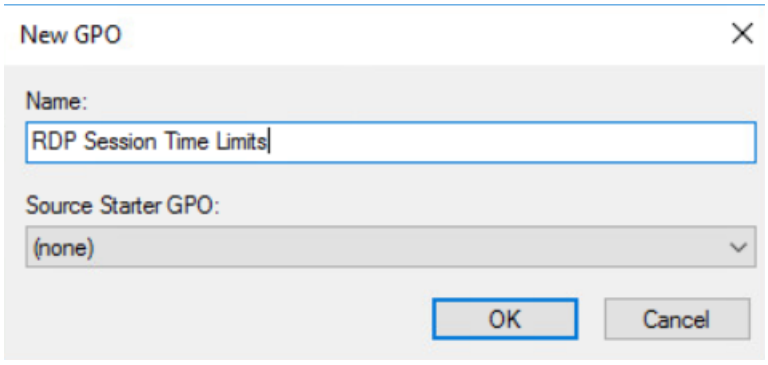
Bunu yapmadığımız taktirde başımıza neler gelebilir biraz bahsedeyim. Sunucumuzdan görev yöneticisini açıp daha sonrasında “Users” kısmına geldiğimizde bazı kullanıcıların açık olduğunu görüyoruz. Aslında bu kullanıcılar “Sing out” olmak yerine üst tarafta bulunan çarpı butonuna bastıkları için oturumları kapanmıyor ve bu durum sunucunun performansını ve güvenliğini etkilemiş oluyor. Güvenlik kısmına değinmek istiyorum, elbette dışardan destek aldığımız firma olabilir veya şirketimizde çalışan bir personel olabilir hiç fark etmez. Saldırgan eğer isterse daha yetkili bir kullanıcının powershell’ini çalıştırabilir hatta yeni kullanıcı oluşturup veya kendisini domain admin yapabilir. Bunu yapabilmesi için bazı tool’lar var ve bu saldırıyı gerçekleştirebilmek için saldırganın local admin olması yeterlidir. Saldırı nasıl yapıldığına şuanlık değinmeyeceğim isteyen olursa benimle iletişim geçebilir.



Gelelim güvenliğin sağlanmasına, öncelikle group policy açalım ve bir adet policy oluşturalım.

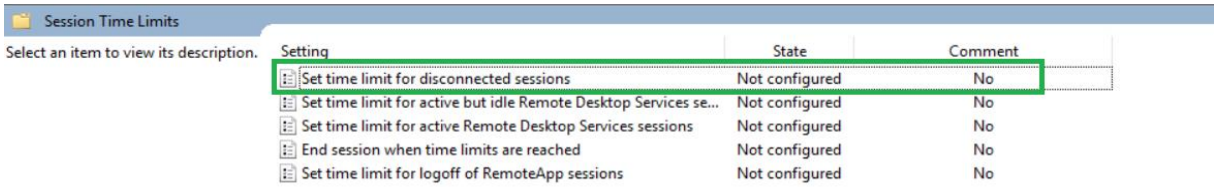


Oluşturmuş olduğum policy'nin ismini "RDP Session Time Limits" veriyorum siz istediğinizi verebilirsiniz.

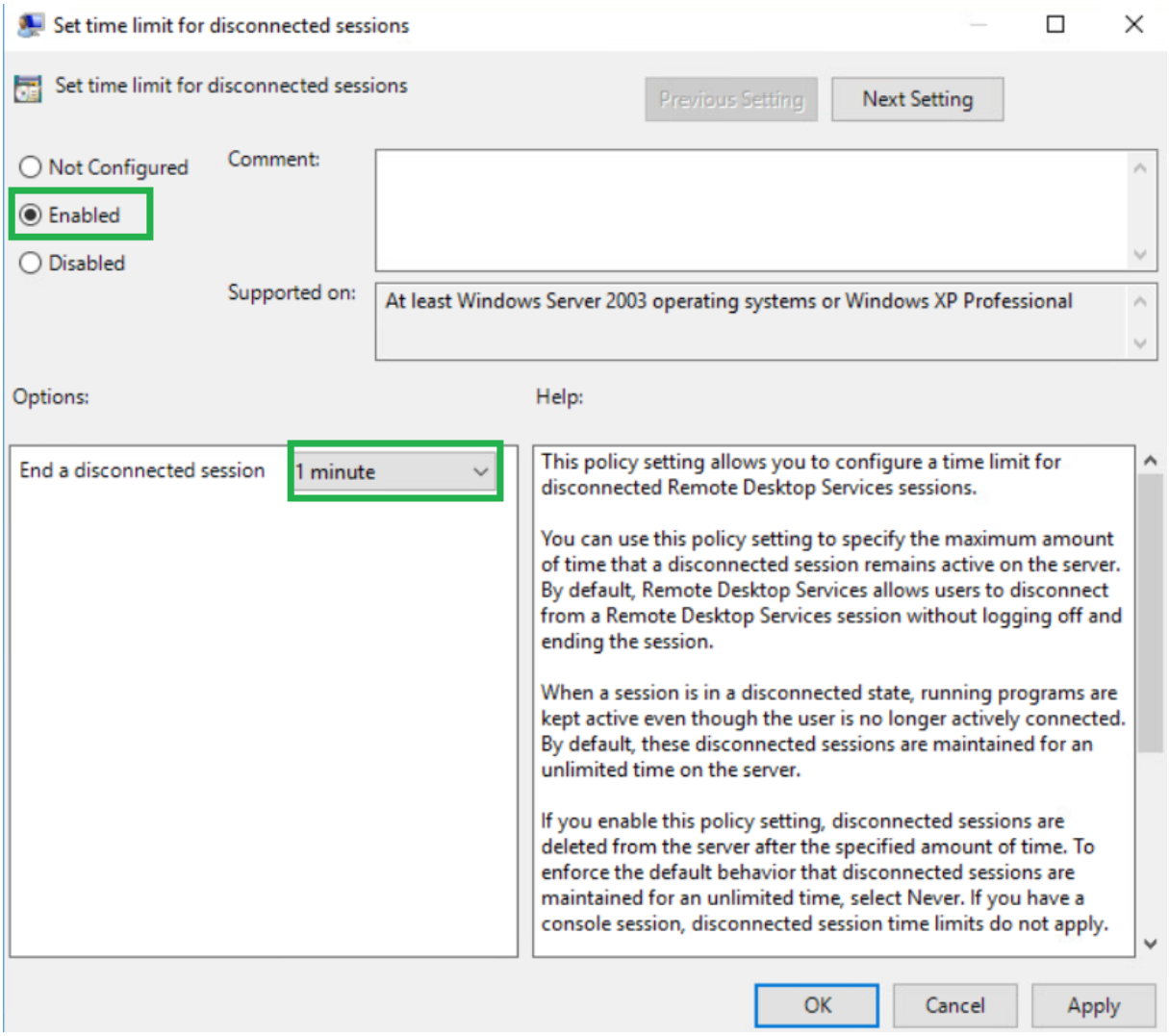


Oluşturduğumuz policy'de sağ tıklayıp edit diyelim ve belitmiş olduğum dizine gelelim.

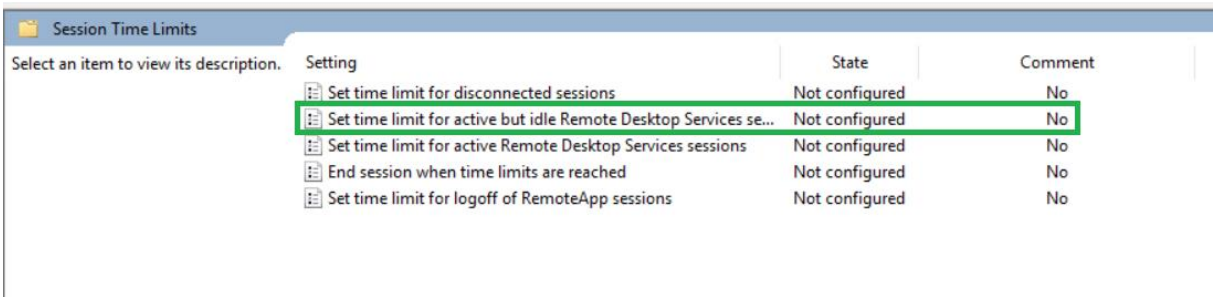
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits



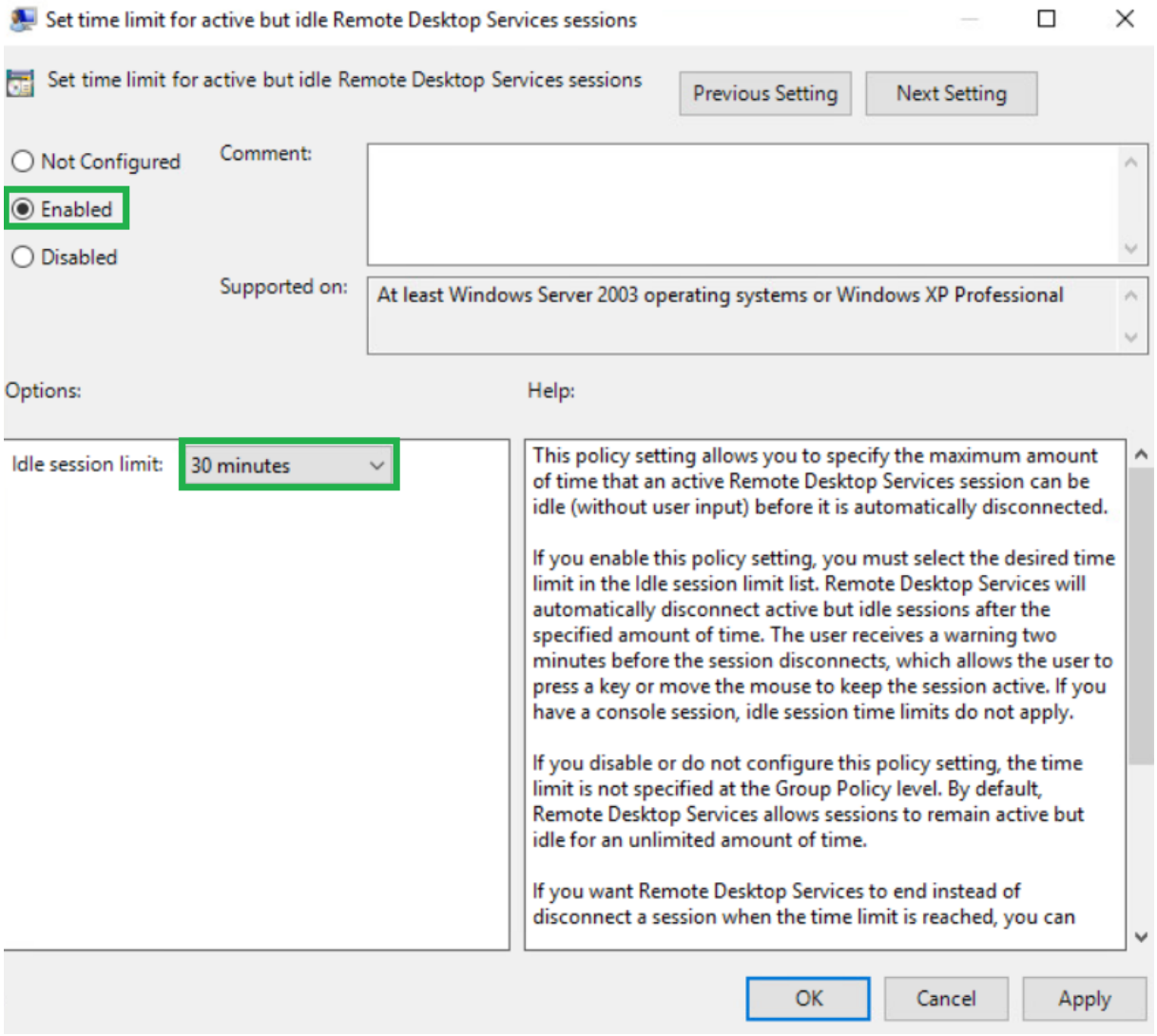
En üst seçenekte belirttiğim gibi “Set time limit for disconnected sessions” seçelim. Seçtiğimiz seçenek şuna yarıyor. Kullanıcı “RDP” bağlantısını üst köşeden çarpıya bastıktan sonra kaç dk sonra kullanıcının hesabı sing out olmasını istediğimiz belirlediğimiz kısım.



Resimde görüldüğü gibi kuralı “Enabled” edip süre olarak 1 dk seçtim. Yani kullanıcı oturumdan çıktıktan 1 dk sonra oturumu otomatikman sing out olacak. Bir başka seçeneğide göz atalım 2. sırada bulunan “Set time limit for active ut idle Remote Desktop Services sessions” seçiyorum.



Bu seçenek ise şuna yarıyor. Kullanıcı üst köşeden oturumu kapatmayıp ama herhangi bir işlem'de yapmadığı zaman kaç dk sonra sing out olunmasını belirlediğimiz ekran. Kısaca özetlemek gerekirse sunucuda bir işim oldu ve giriş yaptım, işim bittikten sonra oturumu kapatmayıp alt sekmeye aldığımı farz edelim. Bu durumlar için kullanılır.



Yukarıda görüldüğü üzere "Enabled" seçip süreyi'de 30 dk olarak belirledim. Buradaki süreyi çok kısa tutmanızı tavsiye etmem çünkü. Belki o sırada kullanıcı bir uygulama indiriyordur veya bir kurulum yaparken beklemesi gerekti diyelim bu gibi kazalar yaşanmaması için 30 dk belittim.

Fatih Bülbül