epati

Active Directory - Kerberos SSO Entegrasyonu

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Yapılandırma Örnekleri

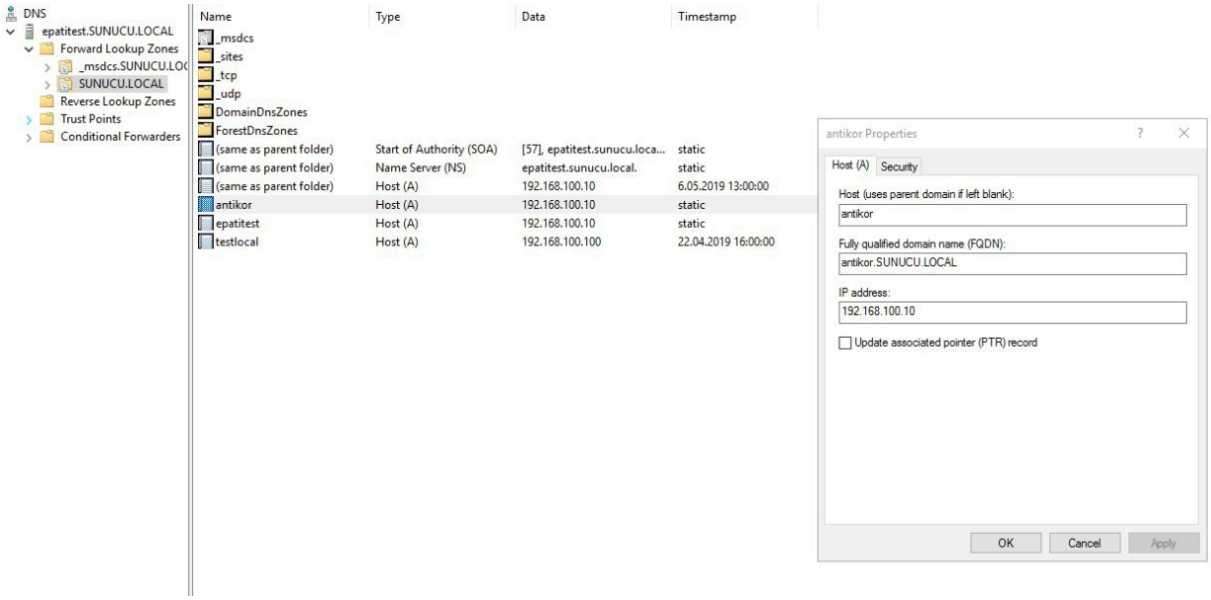
www.epati.com.tr

Active Directory - Kerberos SSO Entegrasyonu

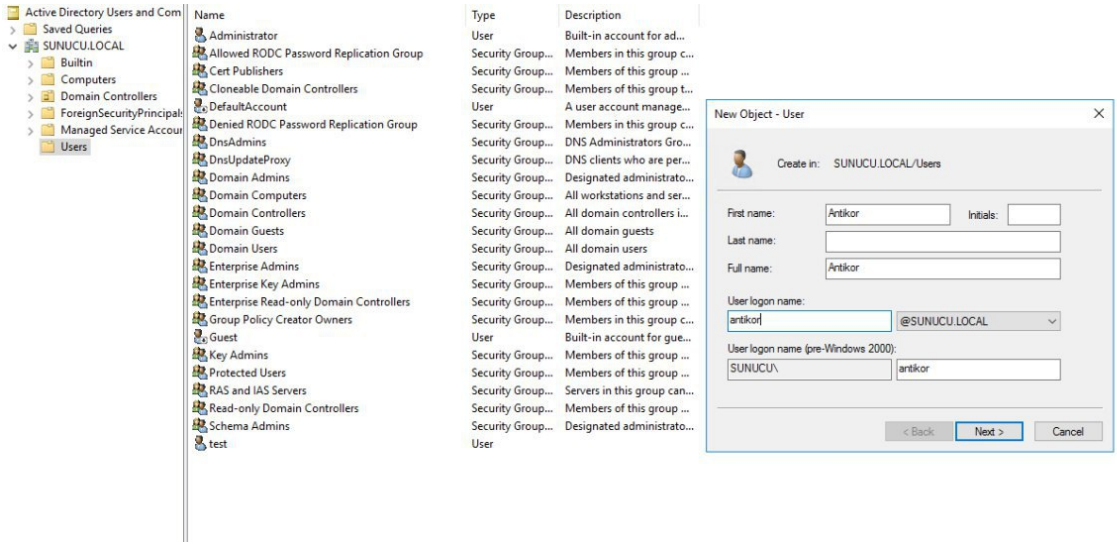
Kerberos, ağ üzerinde iletişim gerçekleştiren kaynakların kimliklerini ispatlamak için geliştirilmiş kimlik doğrulama protokolüdür. SSO (Single Sign On), tek bir kullanıcı kimliği ile oturum açma işlemi gerçekleştirilerek erişim sağlamaktadır.

Active Directory Tarafında Yapılması Gerekenler

1. Domain Controller makinesinde DNS sunucuya A kaydı oluşturulmalıdır.



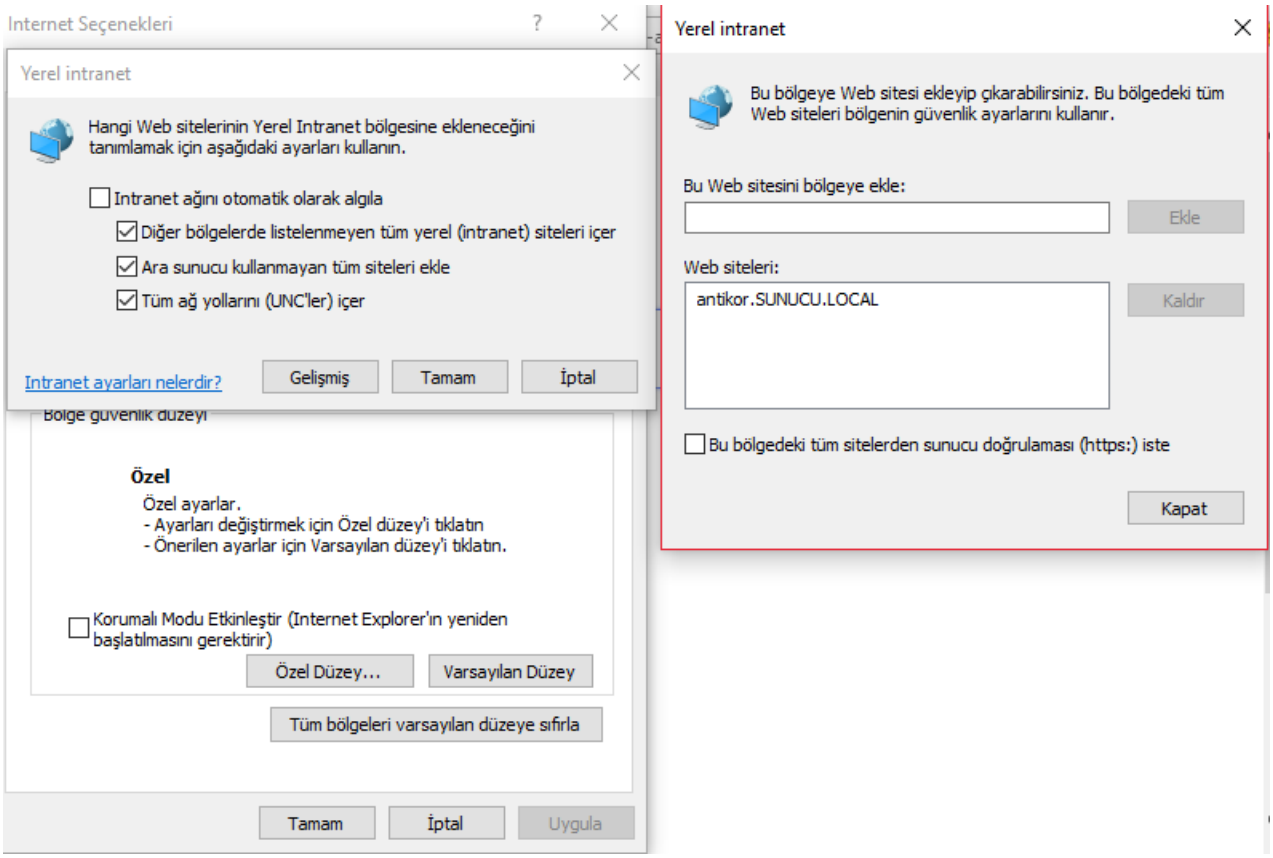
2. DC makinesinde antikor adında user oluşturulmalıdır.



3. Yönetici olarak `CMD` açılarak aşağıdaki komut ile keytab dosyası oluşturulmalıdır.

```
ktpass -princ HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL -mapuser antikor@SUNUCU.LOCAL -crypto al
-ptype KRB5_NT_PRINCIPAL -pass SIFRE -out antikor.krb.keytab
```

4. Internet Explorer > Güvenlik > Yerel Intranet > Siteler > Gelişmiş penceresinde antikor.SUNUCU.LOCAL yazılmalıdır.

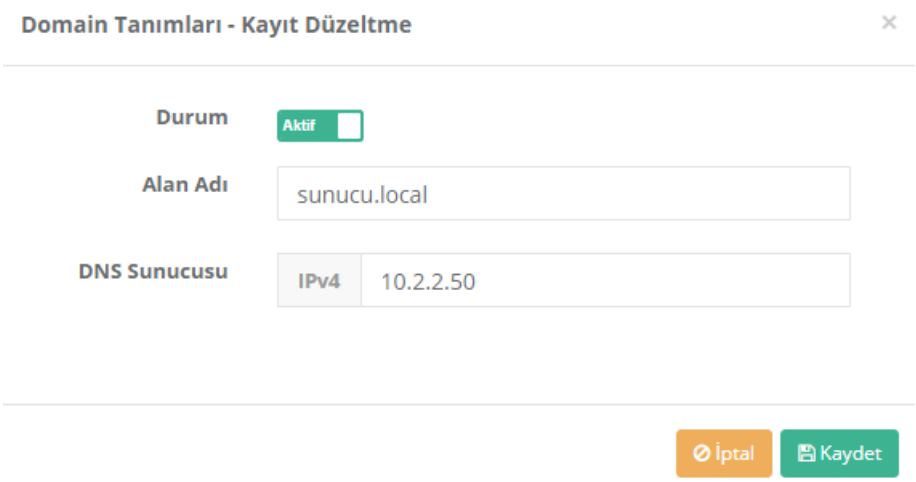


5. Group Policy ayarları ile Antikor SSL sertifikası tüm istemcilere dağıtılmalıdır.

To add trusted sites using a GPO (Group Policy Objects), Launch Active Directory Users and Computers (ADUC), right click on the domain the clients are in, select Properties > Group Policy > New, type in a name for the GPO (like “IE Security Settings”) and then select Edit > User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings. Select Import the current security zones and privacy settings > Modify Settings > Trusted Sites > Sites and add your Plexcel protected websites just as you would on a client. Then wait for the policy to propagate throughout the domain.

Antikor Tarafında Yapılması Gerekenler

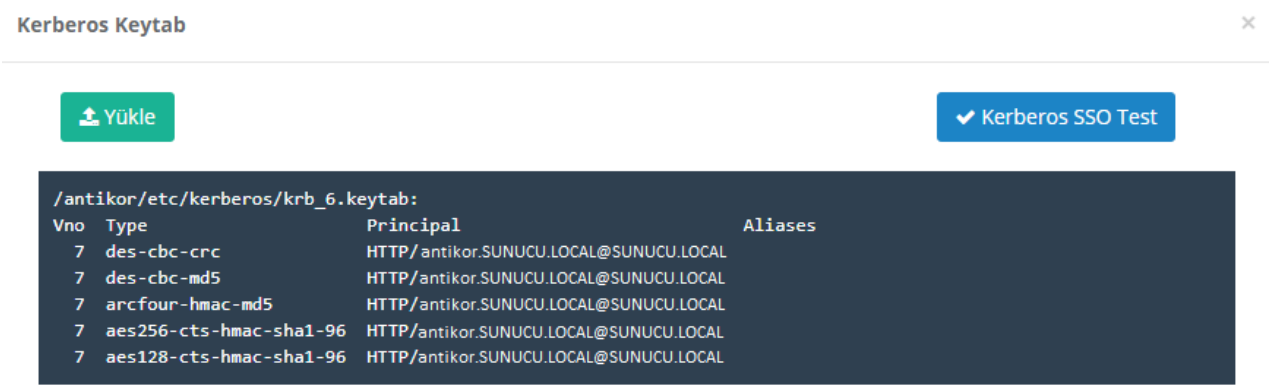
1. Antikor Domain Tanımları sayfasında SUNUCU.LOCAL kaydı oluşturulur.



2. Kimlik Sağlayıcı Tanımları sayfasında Sağlayıcı Türü SSO: Negotiate/Kerberos - Active Directory seçilerek kayıt girilir.

3. Oluşturulan Keytab dosyası Yükle butonu aracılığıyla yüklenecektir. Kök Sertifika butonu, Doğrulama Kuralları sayfasında “Tek Oturum Açma SSO” seçeneği aktif edilmesi halinde görülecektir.

Keytab dosyası yüklendiğinde aşağıdaki gibi bilgiler görülecektir;

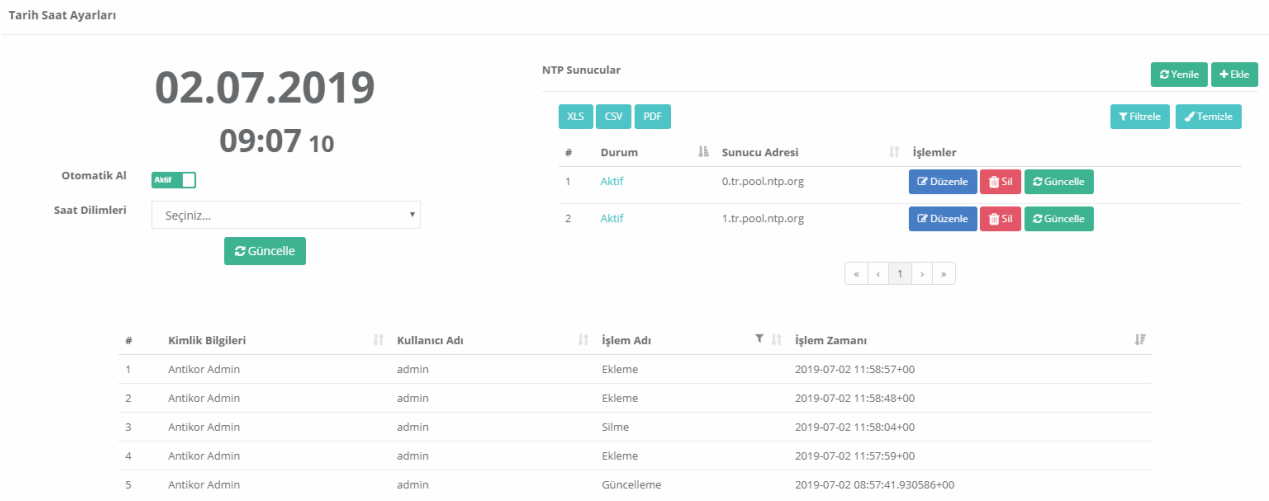


Kerberos SSO Test butonu ile test işlemi gerçekleştirilebilir.

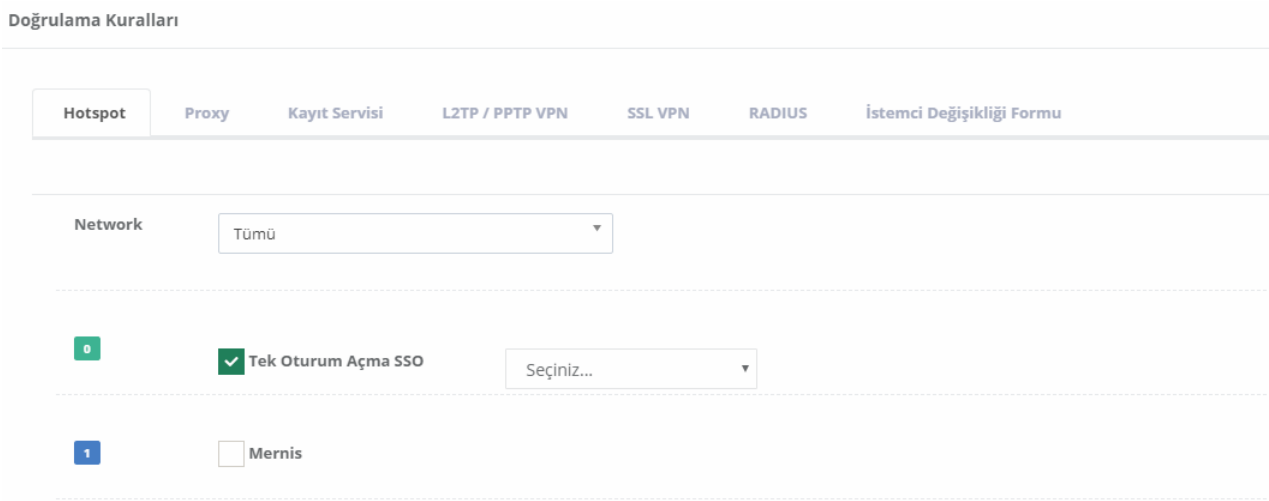
4. Bütün adımlar gerçekleştirildikten sonra oturum açma işlemi başarı ile gerçekleştirilecektir.

Antikor Tarafında Dikkat Edilmesi Gerekenler

1. NTP Sunucu ayarı yapılmalıdır.



2. Doğrulama Kuralları sayfasında Hotspot sekmesinde Tek Oturum Açma SSO özelliği aktif edilmelidir.



3. Domain Sunucu, İstemci ve Antikor için tarih/saat ayarları aynı olmalıdır.

4. SSO doğrulama yapılmak istenen IP adresleri veya IP blokları Hotspot İstemcileri sayfasına eklenmelidir.