

epati

Hotspot SSO:Negotiate Kerberos - Active Directory Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

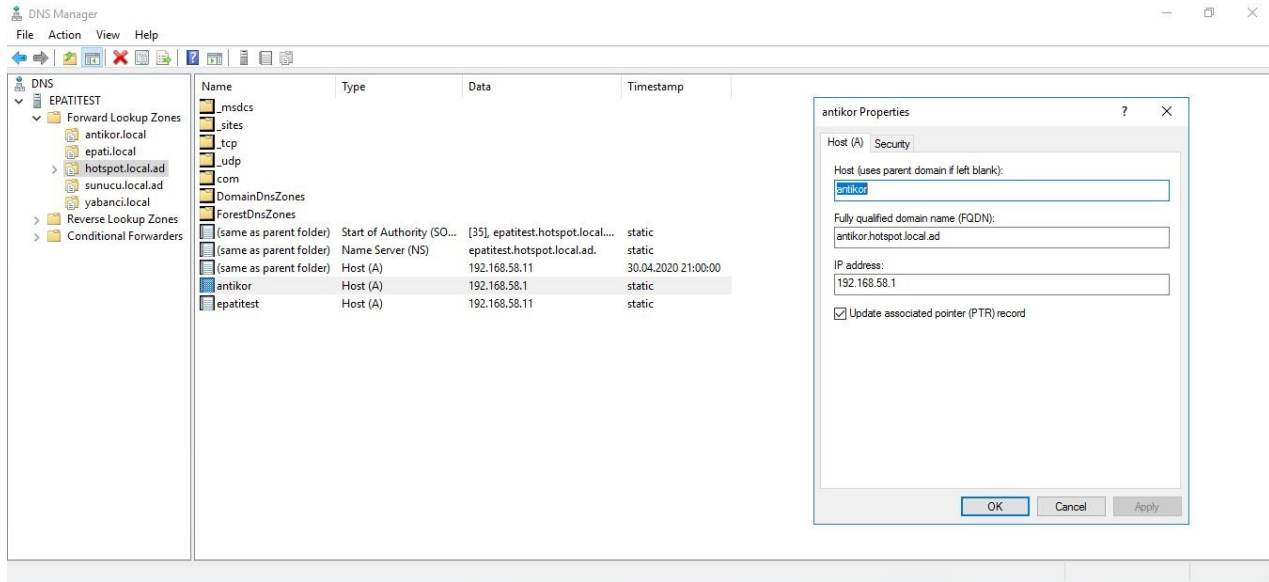
► Yapılandırma Örnekleri

Hotspot SSO:Negotiate Kerberos - Active Directory Yapılandırması

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.

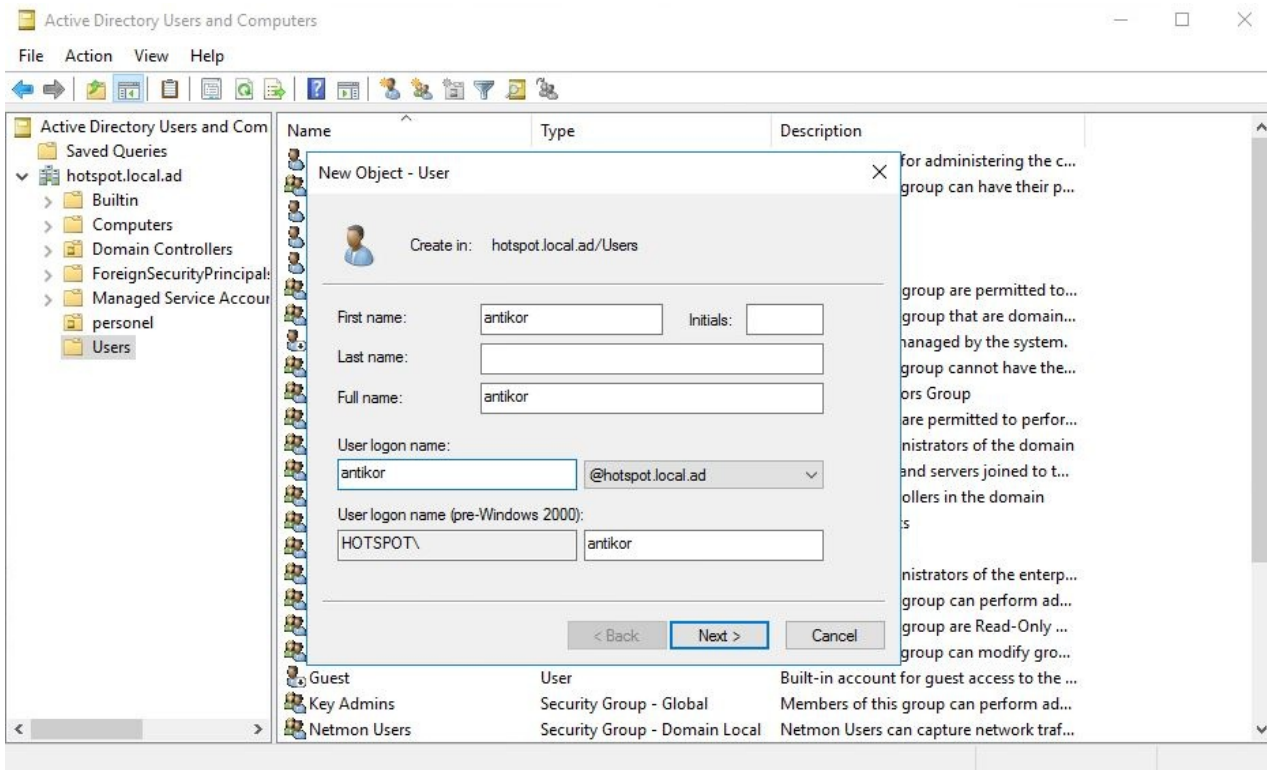
Active Directory Tarafında Yapılması Gerekenler

1. Domain Controller makinesinde DNS sunucuya A kaydı oluşturulmalıdır.



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[35] epatitest.hotspot.local...	static
(same as parent folder)	Name Server (NS)	epatitest.hotspot.local.ad.	static
(same as parent folder)	Host (A)	192.168.58.11	30.04.2020 21:00:00
antikor	Host (A)	192.168.58.1	static
epatitest	Host (A)	192.168.58.11	static

2. DC makinesinde antikor adında user oluşturulmalıdır.



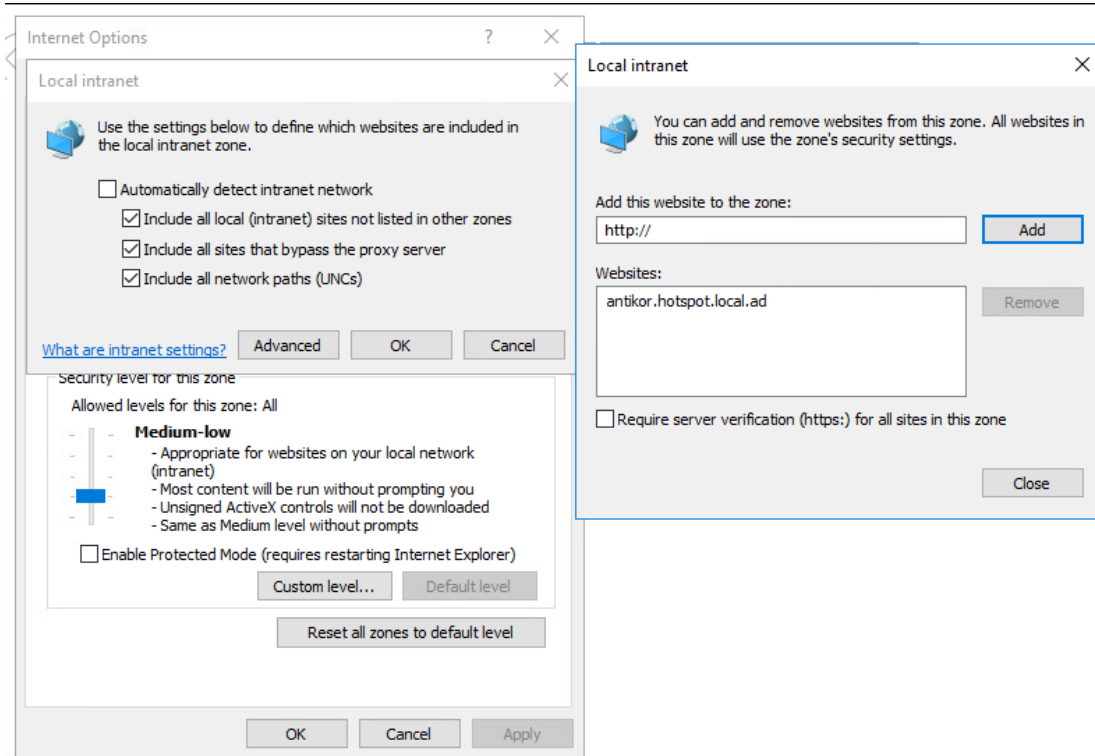
3. Yönetici olarak CMD açılarak aşağıdaki komut ile keytab dosyası oluşturulmalıdır.

```

ktpass -princ HTTP/antikor.hotspot.local@hotspot.local -mapuser antikor@hotspot.LOCAL -crypto
ll -ptype KRB5_NT_PRINCIPAL -pass SIFRE -out antikor.krb.keytab

```

4. Internet Explorer > Güvenlik > Yerel Intranet > Siteler > Gelişmiş penceresinde antikor.hotspot.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 hotspot.local.ad kaydı oluşturulur.

Domain Tanımları - Kayıt Düzeltme

Durum Aktif

Alan Adı

DNS Sunucusu

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

Kimlik Sağlayıcı Tanımları - Kayıt Düzeltme

Durum Aktif

Sağlayıcı Türü

Domain Controller / Kerberos Key Distribution Center ile saat uyumsuzluğu halinde Tek Oturum Açma (SSO) başarısız olabilir. Lütfen Tarih Saat Ayarları menüsünden NTP senkronizasyonu yapıldığından emin olun.

Etki Alanı

KDC / DC DNS Adı

Antikora atanan DNS Adı

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

2 Aktif SSO: Negotiate/Kerberos - Active Directory HOTSPOT.LOCAL.AD

Keytab dosyası yüklendiğinde aşağıdaki gibi bilgiler görülecektir;

Yükle

Kerberos SSO Test

```
/antikor/etc/kerberos/krb_winR52N_RHLJ.keytab:
Vno Type Principal Aliases
69 des-cbc-crc HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD
69 des-cbc-md5 HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD
69 arcfour-hmac-md5 HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD
69 aes256-cts-hmac-sha1-96 HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD
69 aes128-cts-hmac-sha1-96 HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD
```

İptal

Not: Kerberos SSO Test butonu ile test işlemi gerçekleştirilebilir.

4. Doğrulama kuralları Hotspot sekmesinde sağlayıcı olarak SSO:Negotiate Kerberos - Active Directory seçilir.

Doğrulama Kuralları

Hotspot Proxy Kayıt Servisi LZTP / PPTP VPN SSL VPN RADIUS İstemci Değişikliği Formu

Network: Tümü

0 Tek Oturum Açma SSO Seçiniz...

1 Mernis

2 SMS

3 IP Bilgi mesajı... Kaydet

4 Sağlayıcılar SSO: Negotiate/Kerberos - Acti

##	Adı	Etki Alanı	Kullanımda	→	Adı	Sağlayıcı Türü	Etki Alanı	İşlemler
<input type="checkbox"/>		HOTSPOT.LOCALAD	Hayır					

Doğrulama Kuralları

Hotspot Proxy Kayıt Servisi LZTP / PPTP VPN SSL VPN RADIUS İstemci Değişikliği Formu

Network: Tümü

0 Tek Oturum Açma SSO Seçiniz...

1 Mernis

2 SMS

3 IP Bilgi mesajı... Kaydet

4 Sağlayıcılar SSO: Negotiate/Kerberos - Acti

##	Adı	Etki Alanı	Kullanımda	→	Adı	Sağlayıcı Türü	Etki Alanı	İşlemler
<input checked="" type="checkbox"/>		HOTSPOT.LOCALAD	Hayır					

Hotspot Proxy Kayıt Servisi L2TP / PPTP VPN SSL VPN RADIUS İstemci Değişikliği Formu

Network: Tümü

0 Tek Oturum Açma SSO: HOTSPOT.LOCALAD

1 Mernis

2 SMS

3 IP: Bilgi mesajı... Kaydet

4 Sağlayıcılar: SSO: Negotiate/Kerberos - Acti

#	Adı	Etki Alanı	Kullanımda	Adı	Sağlayıcı Türü	Etki Alanı	İşlemler
1		HOTSPOT.LOCALAD	Evet	SSO: Negotiate/Kerberos - Active Directory	HOTSPOT.LOCALAD		Sil

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

Antikor Tarafında Dikkat Edilmesi Gerekenler

1. NTP Sunucu ayarı yapılmalıdır.

04.05.2020
16:31 29 +3

Otomatik AI: Aktif

Saat Dilimleri: +3 Kaydet

NTP Sunucular: Yeni Ekle

XLS CSV PDF Göster/Gizle Sayfa Başı Kayıt Sayısı Tamam Filtrele Filtreyi Temizle

#	Durum	Sunucu Adresi	İşlemler
1	Aktif	192.168.58.11	Düzenle Sil Senkronize Et

#	Kimlik Bilgileri	Kullanıcı Adı	İşlem Adı	İşlem Zamanı
1	Antikor Admin	admin	Güncelleme	2020-04-30 23:44:35.292484+03
2	Antikor Admin	admin	Güncelleme	2020-04-30 23:44:25.333333+03
3	Antikor Admin	admin	Güncelleme	2020-04-30 23:44:21.104845+03
4	Antikor Admin	admin	Güncelleme	2020-04-30 21:51:20.539566+03
5	Antikor Admin	admin	Güncelleme	2020-04-30 21:51:08.428983+03

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

Doğrulama Kuralları

Hotspot Proxy Kayıt Servisi L2TP / PPTP VPN SSL VPN RADIUS İstemci Değişikliği Formu

Network: Tümü

0 Tek Oturum Açma SSO: HOTSPOT.LOCALAD

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.



