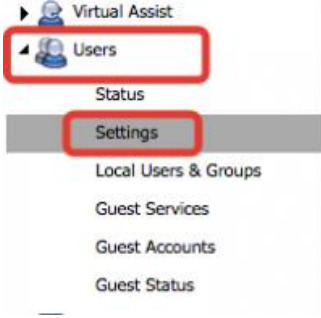


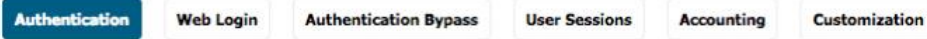
Sonicwall Active Directory Yapılandırması

Sonicwall ile active directory ile oluşturulan kullanıcıların Firewall a çekebilirsiniz. Bunun için öncelikle Sonicwall Firewall web arayüzüne giriyoruz.

Sonrasında açılan ekranda **User** başlığı altında **Settings** kısmını tıklıyoruz.



Açılan ekranda **User Authentication Method** kısmında **LDAP+Local User** seçiyoruz ve sonrasında hemen yan tarafta bulunan **Configure LDAP** butonuna tıklayarak ayarlarımızı yapmaya başlıyoruz.



User Authentication Settings

User authentication method:

Local Users

CONFIGURE RADIUS

CONFIGURE LDAP

Single-sign-on method(s):

- SSO Agent
- Terminal Services Agent
- RADIUS Accounting
- 3rd-Party API
- Browser NTLM Authentication

CONFIGURE SSO

Case-sensitive user names

ADD diyerek sunucu ayarlarını yapılandırılalım.

LDAP Servers

LDAP Servers

General Settings

#	Status	Host Name/IP Address	Role	Port	Timeout	TLS	Domain	Enable
---	--------	----------------------	------	------	---------	-----	--------	--------

ADD...

Açılan pencerede öncelikle Sunucumuzun ip adresini port numarasını belirliyoruz. **Name or Ip address** kısmına active directory ip adresimizi giriyoruz. Sonrasında portu 389 olarak yanındaki menüden seçiyoruz ve son olarak seçili olarak gelen **Use TLS(SSL)** seçimini kaldırıyoruz.

Add server

Settings Login/Bind Schema Directory

Role: Primary LDAP server Secondary LDAP server Backup/replica server

Name or IP address: 0.0.0.0

Port Number: 389 Standard port choices...

Server timeout (seconds): 10

Overall operation timeout (minutes): 5

Use TLS (SSL)

Send LDAP 'Start TLS' request

SAVE CANCEL

Settings kısmındaki ayarlarımız yaptıktan sonra **Login/Bind** kısmını tıklıyoruz ve burada Active directory admin hesabımızın kullanıcı adı ve şifresini giriyoruz. **User tree for login to server** kısmına activedirectory user yolumuzu yazıyoruz. **Örnek olarak e-data.local/User**

Add server

Settings **Login/Bind** Schema Directory

Anonymous login Give login name/location in tree Give bind distinguished name

Login user name: _____

User tree for login to server: _____

Password: _____

When referred to other servers: Bind with this account Bind with an equivalent account on that server (same password)

Schema kısmında Microsoft Active Directory veya sizin user kütüphaneniz neyse onu seçiyoruz.

Add server

Settings Login/Bind **Schema** Directory

LDAP Schema:

User Objects

Object class:

Attributes:

Login name:

Qualified login name:

User Group Objects

Object class:

Attributes:

Member:

is: Distinguished name User ID

Directory kısmında domain adresimizi yazarak **AUTO-CONFIGURE** kısmına tıklıyoruz. Bu işlem ile active directory tree miz aşağıda listenecektir. Sonrasın da **SAVE** diyerek ayarlarımızı kaydediyoruz.

Add server

Settings Login/Bind Schema **Directory**

Primary domain:

Trees containing users:

↑ ↓

Trees containing user groups:

↑ ↓

Ayarlarımızı yaptıktan sonra **Test** butonuna tıklayarak Active Direktory haberleşmesini test edebiliriz. Bunun için test kısmını tıkladıktan sonra açılan sayfada sunucu adresimizi seçerek test dememiz yeterli olacaktır. İşlem başarılı uyarısı gelecektir.



LDAP Servers



#	Status	Host Name/IP Address	Role	Port	Timeout	TLS	Domain	Enable	
1		192.168.1.145	Primary	389	10	<input type="checkbox"/>	aryalab.local	<input checked="" type="checkbox"/>	

ADD...

Status kısmında yeşil ışık yandı ve test butonunu tıklayarak active directory kullanıcılarımızı görebiliriz. Eğer test ettiğinizde active directory grup ve kullanıcılarınızı göremiyorsanız ayarlarınızı tekrar kontrol ediniz.