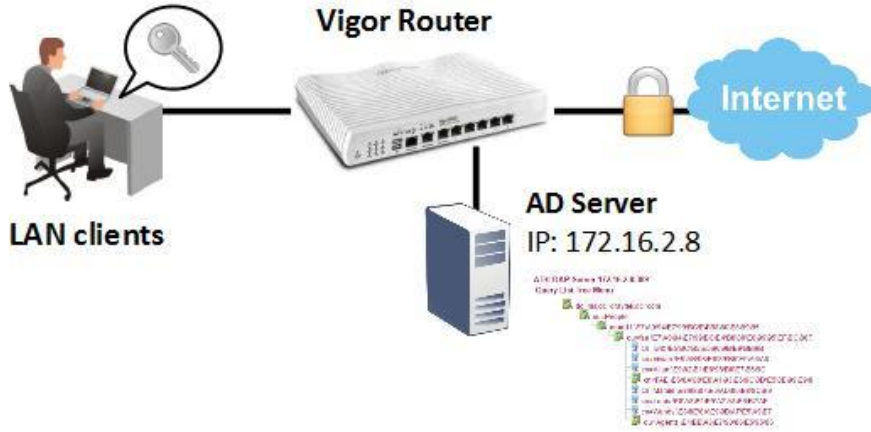


AD / LDAP Sunucusuyla Kullanıcıları Doğrulayın

User-Based Management modunda, tüm LAN istemcilerinin internete erişebilmeleri için bir kullanıcı hesabıyla giriş yapmaları gerekir. Local kullanıcı hesapları dışında, Authentication , Active Directory sunucusu gibi harici bir Authentication server tarafından da yapılabilir. Bu belge Router'ı bir AD / LDAP Server'e nasıl bağlayacağınızı ve LAN istemcilerinin kimliğini doğrulamak için sunucuyu nasıl kullanacağınızı tanıtır.



DrayOS

AD/LDAP Profil Ayarı

1. Application >> Active Directory / LDAP >> Genel Setup bölümüne gidin, AD / LDAP'ı etkinleştirin ve AD / LDAP Server bilgilerini aşağıdaki gibi girin:

- Bind Type: Regular Mode
- Server Address: AD/LDAP sunucusunun IP adresi
- Regular DN: AD/LDAP sunucusunun Administrator hesabının ayırt edici adı(DN).
- Regular Password: Administrator hesabının şifresi.

Applications >> Active Directory /LDAP

Active Directory /LDAP

[Set to Factory Default](#)

General Setup	Active Directory / LDAP Profiles
<input checked="" type="checkbox"/> Enable	
Bind Type	Regular Mode
Server Address	172.16.2.8
Destination Port	389
<input type="checkbox"/> Use SSL	
Regular DN	uid=vpntest,ou=vpnusers,dc=ms,dc=draytek,dc=
Regular Password
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Note:

After finishing the configuration of the LDAP profiles, they will be listed in the page of **VPN and Remote Access >> PPP General Setup**. If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in **VPN and Remote Access >> PPP General Setup** first.

2. Yapılandırmayı kaydetmek için OK'a tıklayın ve Router'i yeniden başlatmanız istendiğinde tekrar OK'a tıklayın.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- Using current configuration
 Using factory default configuration

OK

3. Bir AD / LDAP profili oluşturun: Application >> Active Directory / LDAP >> AD / LDAP Profiles sayfasına gidin, uygun bir index numarasına tıklayın.

Applications >> Active Directory /LDAP

Active Directory /LDAP

| [Set to Factory Default](#) |

General Setup

Active Directory /
LDAP Profiles

Index	Name	Distinguished Name
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Note:



After finishing the configuration of the LDAP profiles, they will be listed in the page of **VPN and Remote Access >> PPP General Setup**. If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in **VPN and Remote Access >> PPP General Setup** first.

4. Profili aşağıdaki gibi düzenleyin:

- Bu profile bir Name ver.
- AD / LDAP sunucusunun kullandığı **Common Name Identifier** girin (varsayılan olarak cn olabilir)
- Router'in aramaya başlayacağı dizin olarak **Base Distinguished Name** girin.

Applications >> Active Directory /LDAP>> Server Profiles

Index No. 1

Name	<input type="text" value="user managment"/>
Common Name Identifier	<input type="text" value="cn"/>
Base Distinguished Name	<input type="text" value="ou=rd1\E7\A0\94\E7\99\BC\E4\B8\80\E8\99\95,"/> 
Additional Filter	<input type="text"/>
Note: Please type in your additional filter for BaseDN search request. For example, 1. For OpenLDAP: (gidNumber=500) 2. For AD: (msNPAllowDialin=TRUE)	
Group Distinguished Name	<input type="text"/> 
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Kullanıcı Yönetimi Kurulumu

5. User Management modunun "User-Based" olduğundan emin olmak için **User Management >> General Setup** bölümüne gidin.

User Management >> General Setup

General Setup

Mode Selection:

- Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.
- User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

6. Yeni bir kullanıcı profili oluşturun **User Management >> User Profile** bölümüne gidin, uygun bir dizine tıklayın.

User Management >> User Profile

User Profile Table | [Set to Factory Default](#) |

Select All Clear All Search

Profile	Enable	Name	Profile	Enable	Name
1.	<input checked="" type="checkbox"/>	admin	17.	<input type="checkbox"/>	
2.	<input checked="" type="checkbox"/>	Dial-In User	18.	<input type="checkbox"/>	
3.	<input type="checkbox"/>		19.	<input type="checkbox"/>	
4.	<input type="checkbox"/>		20.	<input type="checkbox"/>	
5.	<input type="checkbox"/>		21.	<input type="checkbox"/>	
6.	<input type="checkbox"/>		22.	<input type="checkbox"/>	

7. Profili aşağıdaki gibi düzenleyin:

- Bu hesabı etkinleştirin.
- Bir Username verin.
- External Server Authentication 'da "LDAP" seçeneğini seçin ve 3. Adımda oluşturduğumuz profili seçin.
- Kaydetmek için OK'a tıklayın.

User Management >> User Profile

Profile Index 3

1. Common Settings

Enable this account

Username

Password

Confirm Password

2. Web login Setting

Idle Timeout min(s) 0:Unlimited

Max User Login 0:Unlimited

Policy

External Server Authentication

user management

Log

Pop Browser Tracking Window

Authentication Web Alert Tool Telnet

The selection of items could be created as rules and which not set to active.

Kullanıcı Girişi

8. Şimdi, LAN istemcileri İnternete ilk kez eriştiğinde, Router onları bir giriş sayfasına yönlendirecektir. AD / LDAP veritabanındaki bir kullanıcı hesabıyla giriş yapmaları gerekir.



9. User Management >> User Online Status Page , Network Administrator AD / LDAP server tarafından kimliği doğrulanmış kullanıcıları görecektir.

User Management >> User Online Status

Current Time : 05-17 11:09:00 Refresh Seconds: 10 Page: 1 Refresh

Index	User	IP Address	Profile	Last Login Time	Expired Time	Data Quota	Idle Time	Action
1	admin	192.168.77.10	admin	05-17 11:08:57	Unlimited	Unlimited	Unlimited	Block Logout Delete
2	mamie_su	--	AD server	05-17 11:07:11	Unlimited	Unlimited	Unlimited	Block Logout Delete

LINUX

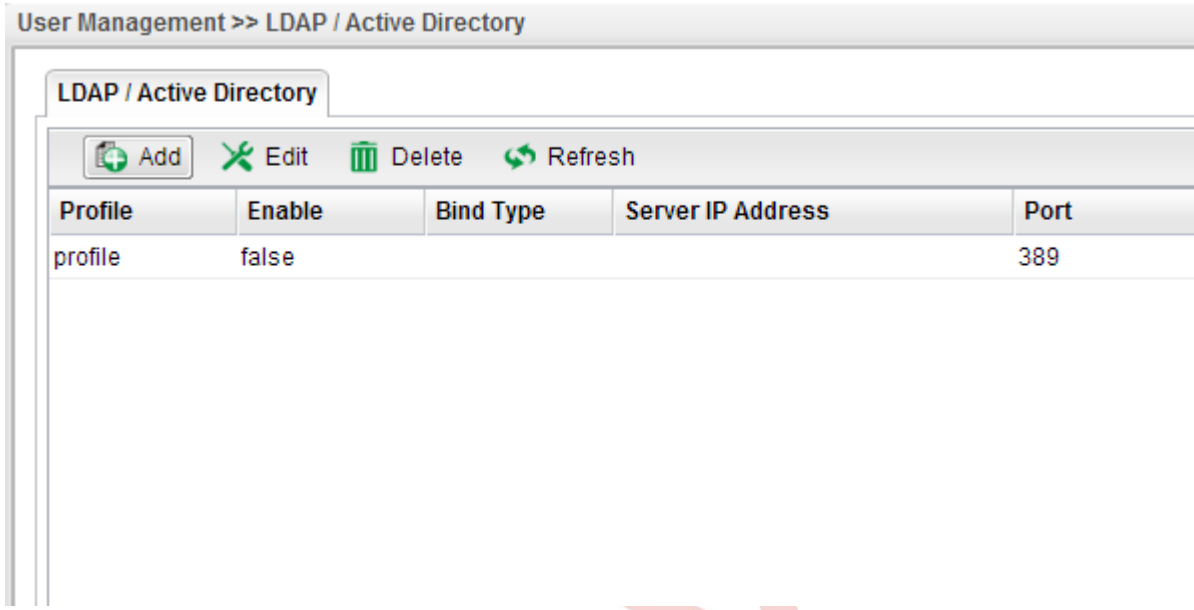
Vigor3900 / Vigor2960, LDAP / AD kimlik doğrulaması için üç bağlantı türünü destekler:

- Simple Mode – Herhangi bir arama yapmadan Bind Authentication yapın.
- Anonymous – Adsız arama yapın ve ardından kimlik doğrulama işlemini yapın.
- Regular mode Router,ilk önce arama yetkisine sahip olup olmadığını görmek için sunucu tarafından kontrol edilir,Ardından arama işlemini gerçekleştirebilir ve Bind Authenticationu yapabilir.

Aşağıda Simple mod ve normal mod kullanma örneklerini sunuyoruz.

LDAP/AD Kurulumu

1. User Management >>LDAP/Active Directory'e gidin ve yeni bir profil eklemek için Add'e tıklayın.



User Management >> LDAP / Active Directory

LDAP / Active Directory

Add Edit Delete Refresh

Profile	Enable	Bind Type	Server IP Address	Port
profile	false			389

2. LDAP profilini yapılandırın.

(1) Basit Mod

LDAP/AD sunucusu basit bir yapıya sahipse bu modu kullanın. Örneğin, LDAP/AD sunucusunda "ms.draytek.com" domaini altında yalnızca bir default kullanıcı grubu varsa "Users" ve user accounts bu grubun altındaki profili aşağıdaki gibi yapılandırabiliriz:

- Bind Type: Simple Mode
- Server IP address and Port: LDAP/AD sunucusunun IP'si ve dinlediği port
- Common Name Identifier: cn
- Base DN: cn=Users,dc=ms,dc=draytek,dc=com

LDAP / Active Directory

Profile : simple

Enable

Bind Type : Simple Mode

Server IP Address : 172.16.2.8

Port : 389

Common Name Identifier : cn (Optional)

Base DN : cn=Users,dc=ms,dc=dr...

Group DN : (Optional)

Regular DN : (Optional)

Regular Password : (Optional)

Logout After(min) : -1 (User Management)

Apply Cancel

(2) Düzenli Mod

LDAP/AD sunucusu birden fazla seviyeye sahipse ve kullanıcı hesabının yolunu bulmak için aranıyorsa bu modu kullanın. Örneğin, domain altında OU "People" ve "Group" var; OU "RD1", "RD2", "RD3" OU altında "People", OU "MIS", "PQC", "FAE" OU "RD1" altında ve OU "People" altındaki tüm kullanıcı hesaplarının doğrulanmasını istiyorsak profili aşağıdaki gibi yapılandırabiliriz:

- Bind Type: Regular Mode
- Server IP address and Port: LDAP/AD sunucusunun IP'si ve dinlediği port.
- Common Name Identifier: cn (Not: "cn" önerilen ayardır. Eğer Ortak Ad Tanımlayıcı "cn" olarak ayarlanmamışsa, Vigor Router varsayılan olarak "cn =", "uid =" veya "sAMAccountName =" ile filtre gönderir)
- Base DN: ou=People,dc=ms,dc=draytek,dc=com
- Regular DN: cn=vivian,cn=vivian,ou=fae,ou=rd1,ou=people,dc=ms,dc=draytek,dc=com ("vivian", OU FAE altında bir kullanıcı hesabı olduğunda)
- Regular Password: Normal DN'de belirtilen hesabın şifresi.

LDAP / Active Directory

Profile : simple

Enable

Bind Type : Regular Mode

Server IP Address : 172.16.2.8

Port : 389

Common Name Identifier : cn (Optional)

Base DN : cn=Users,dc=ms,dc=dr...

Group DN : (Optional)

Regular DN : cn=vivian,cn=vivian,ou=fa... (Optional)

Regular Password : (Optional)

Logout After(min) : -1 (User Management)

Apply Cancel

Düzenli modda, bir User Authentication isteği olduğunda, Router ilk önce LDAP / AD sunucusu tarafından doğrulanması için Regular DN ve Password'ü kullanır (a.k.a. basit bağlama isteği). User authentication başarılı olduktan sonra, router bir arama isteği gönderecek ve kullanıcı hesabının Base DN kapsamında olup olmadığını kontrol edecektir. LDAP sunucusu Entry 0'ı yanıtlarsa, kullanıcı hesabının Base DN'de bulunmadığı anlamına gelir. Kullanıcı hesabı varsa, LDAP sunucusu Entry/Path ile cevap verecektir. Router, path ile, kullanıcı hesabının kimliğini doğrulamak için Bind isteğini LDAP sunucusuna gönderir.

Yapılandırmadan sonra, LDAP'yi "Preview" ile doğrulayabiliriz.

User Management >> LDAP / Active Directory

LDAP / Active Directory

Add Edit Delete Refresh

Profile	Enable	Bind Type	Server IP Address	Port	Common Name Identifier	Base DN	Group DN	Regular DN
v1	true	Simple Mode	172.16.2.8	389	cn	ou=Users,dc=ms,dc=dr...		
v2	true	Regular Mode	172.16.2.8	389	cn	ou=People,dc=ms,dc=dr...		ou=People,dc=ms,dc=dr...

LDAP / Active Directory

Profile : v2

Enable

Use SSL

Bind Type : Regular Mode

Server IP Address : 172.16.2.8

Port : 389

Common Name Identifier : cn

Base DN : ou=People,dc=ms,dc=dr...

Group DN : (Optional)

Regular DN : ou=People,dc=ms,dc=dr... (Optional)

Regular Password : (Optional)

Logout After(min) : -1 (User Management)

Apply Cancel

Preview

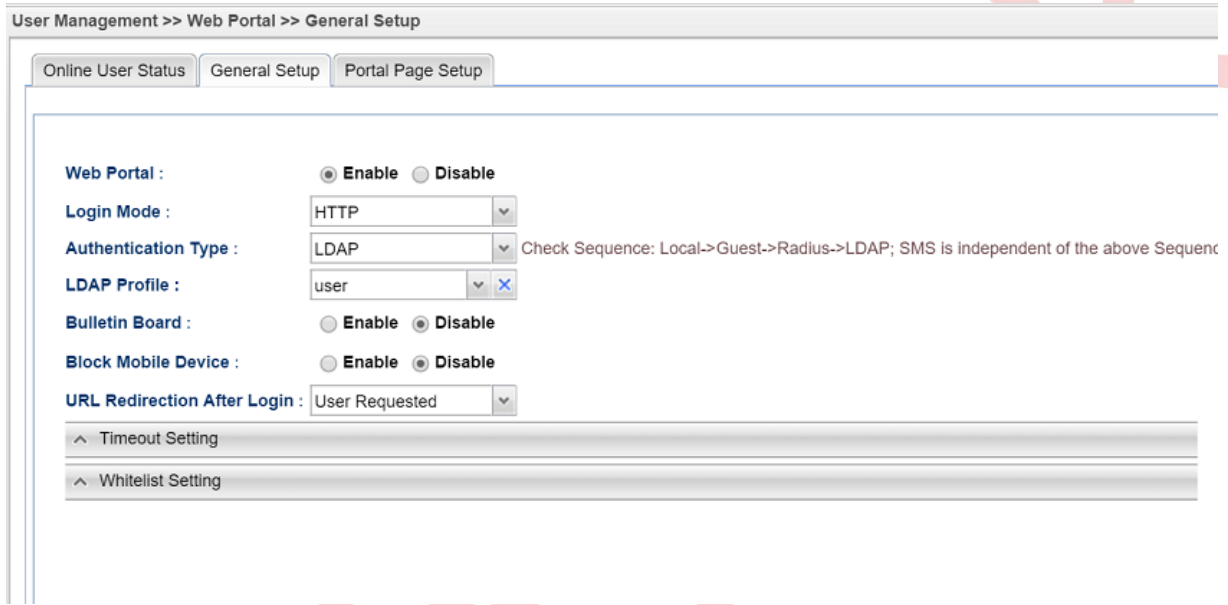
dc=ms,dc=draytek,dc=com

- cn=Administrator
- ou=Groups
- ou=Users
- ou=People
- ou=Groups
- ou=Users
- samba:DomainName=TS
- samba:DomainName=KID

OK

LDAP / AD ile Kullanıcı Yönetimi'ni kullanın

1. **User Management >> Web Portal >> General Setup'a git**
 - a. **Web Portal'ı etkinleştir.**
 - b. **Bir Login mode seçin.**
 - c. **Authentication Type için LDAP'ı seçin.**
 - d. **User Management >> LDAP / Active Directory oluşturun LDAP Profile seçin.**
 - e. **Kurulumu tamamlamak için Apply'a tıklayın.**



User Management >> Web Portal >> General Setup

Online User Status General Setup Portal Page Setup

Web Portal : Enable Disable

Login Mode : HTTP

Authentication Type : LDAP Check Sequence: Local->Guest->Radius->LDAP; SMS is independent of the above Sequenc

LDAP Profile : user

Bulletin Board : Enable Disable

Block Mobile Device : Enable Disable

URL Redirection After Login : User Requested

Timeout Setting

Whitelist Setting

2. Şimdi LAN istemcileri bir tarayıcı açıp Internet'e ilk kez eriştiğinde, bir giriş sayfası olacaktır. LAN istemcileri LDAP / AD sunucusundaki kullanıcı hesabıyla oturum açabilir ve başarılı bir şekilde oturum açtıktan sonra Internet'e erişebilir.

Welcome



Username louis_hsu

Password

Login

Powered by DrayTek Corp. Copyright 2014 All rights reserved.