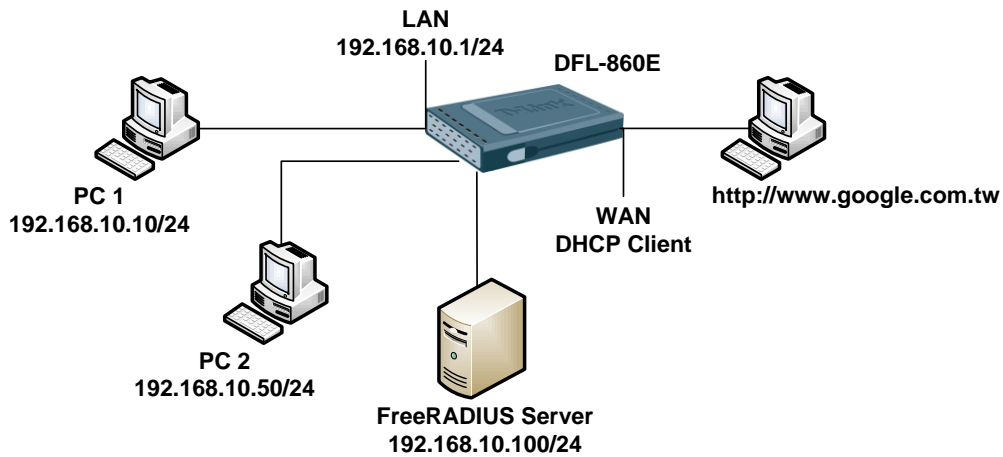


## How to set up WCF web authentication with FreeRADIUS application on the Windows system



FreeRADIUS application Information:

Website: <http://freeradius.net/index.html>

Share secret: 123456789

Test Group: webauthedgroup

Test account: test // 1111 and test2 // 1111

When we install FreeRADIUS we must to setup RADIUS configuration.

In the default install we can find out all of configurations are saving here.

<C:\FreeRADIUS.net\etc\raddb>

We need to setup those of file [dictionary](#), [users.conf](#), [clients.conf](#) and create a new file [dictionary.dlink](#).

Copy dictionary file and rename to dictionary.dlink

[FreeRADIUS setup]

[dictionary](#)

-----

```
$INCLUDE ../share/freeradius/dictionary
```

```
$INCLUDE dictionary.dlink
```

-----

[users.conf](#)

-----

```
test Cleartext-Password := "1111"
```

```
D-Link-User-Group = "webauthedgroup"
```

```
test2 Cleartext-Password := "1111"
```

```
D-Link-User-Group = "webauthedgroup"
```

-----

[clients.conf](#)

-----

```
client 192.168.10.1 {
```

```
secret = 123456789
```

```
shortname = private-network-1
```

```
}
```

-----

[dictionary.dlink](#)

-----

```
VENDOR D-Link 5089
```

```
ATTRIBUTE D-Link-User-Group 1 string D-Link
```

-----

[DFL-860E] Firmware Version: 2.27.03.25

1. System > Remote Management

Change remote HTTP and HTTPS port.

WebUI HTTP port:	<input type="text" value="8080"/>	Specifies the HTTP port for the web user interface.
WebUI HTTPS port:	<input type="text" value="4433"/>	Specifies the HTTP(S) port for the web user interface.

2. Objects > Address Book

Create a new object for authentication LAN net.

#	Name	Address	User Auth Groups	Comments
1	IT	192.168.10.0/24	webauthedgroup	

3. Objects > ALG

Create a new ALG for our HTTP service.

#	Name	Type	Parameters	Comments
1	http-alg	HTTP ALG		

http-alg  
Use an HTTP Application Layer Gateway to filter HTTP traffic.

General | File Integrity | Web Content Filtering | Anti-Virus | URL Filter

**General**

Mode: Enabled

**Categories**

Web content categories to block

Allowed: Adult content, Advertising, Business oriented, Chatrooms, Clubs and Societies, Computing/IT, Crime/Terrorism, Dating sites, Drugs/Alcohol, E-Banking, Educational

Blocked: (empty)

**Options**

Non-Managed Action: Block (Action to take for content that hasn't been classified.)

Allow Override  
 Allow Reclassification

OK Cancel

4. Objects > Services

Set up service object "http-all" and select our HTTP ALG.

#	Name	Type	Parameters	ALG Info	Comments
1	http-all	TCP	80,443	http-alg - WCF:Enabled	HTTP and HTTPS

5. Rules > IP Rules

Create a special rule for WEB authentication

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	dns	NAT	lan	lannet	wan1	all-nets	dns-all
2	auth-allow	NAT	lan	IT	wan1	all-nets	http-all
3	no-auth-sat	SAT	lan	lannet	wan1	all-nets	all_services
4	no-auth-sat-allow	Allow	lan	lannet	wan1	all-nets	all_services

Index 1 & 3 is a necessary rule for WEB authentication and index 2 rule priorities must high than SAT rule.

**no-auth-sat**  
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT | SLB SAT | SLB Monitors

**General**

Translate the

Source IP

Destination IP

to:

New IP Address: lan\_ip

New Port: Applied on TCP/UDP services with port set to either a single port number or a port range without gaps

All-to-One

Name	Address
dmz_ip	172.17.100.254
lan_ip	192.168.10.1
wan1_dns1	0.0.0.0
wan1_dns2	0.0.0.0
wan1_ip	1.1.1.1
wan2_ip	192.168.120.254

OK Cancel

## 6. User Authentication > External User Databases

#	Name	IPAddress	Port	RetryTimeout	Comments
1	freedius	192.168.10.100	1812	2	

**General**

Name: freedius

IP Address: 192.168.10.100

Port: 1812

Retry Timeout: 2 seconds

Shared Secret: ●●●●●●●● Note! Existing secret will always be shown with 8 characters to hide the actual length.

Confirm Secret: ●●●●●●●●

Share Secret must setup same as RADIUS setting. (clients.conf)

## 7. User Authentication > User Authentication Rules

**free-radius-auth-rule**  
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General | Log Settings | Authentication Options | Accounting | Agent Options | Restrictions

**General**

Name: free-radius-auth-rule

Authentication agent: HTTP

Authentication Source: RADIUS

Interface: lan

Originator IP: all-nets For XAuth and PPP, this is the tunnel originator IP.

Terminator IP: (None)

**Comments**

Comments:

OK Cancel



# free-radius-auth-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

- General
- Log Settings
- Authentication Options
- Accounting
- Agent Options
- Restrictions

## General

Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

### RADIUS servers

Available

>>  
<<

Selected

freeradius

Move up Move down

### LDAP servers

Available

>>  
<<

Move up Move down

RADIUS Method:

Local User DB:

OK Cancel



# free-radius-auth-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

- General
- Log Settings
- Authentication Options
- Accounting
- Agent Options
- Restrictions

## General

Select one or more accounting servers. Also select the statistics for the authenticated user that should be sent to the accounting server.

### Accounting servers

Available

>>  
<<

Move up Move down

## User Statistics

- Bytes Sent
- Bytes Received
- Packets Sent
- Packets Received
- Enable reporting of the number of seconds the session lasted.

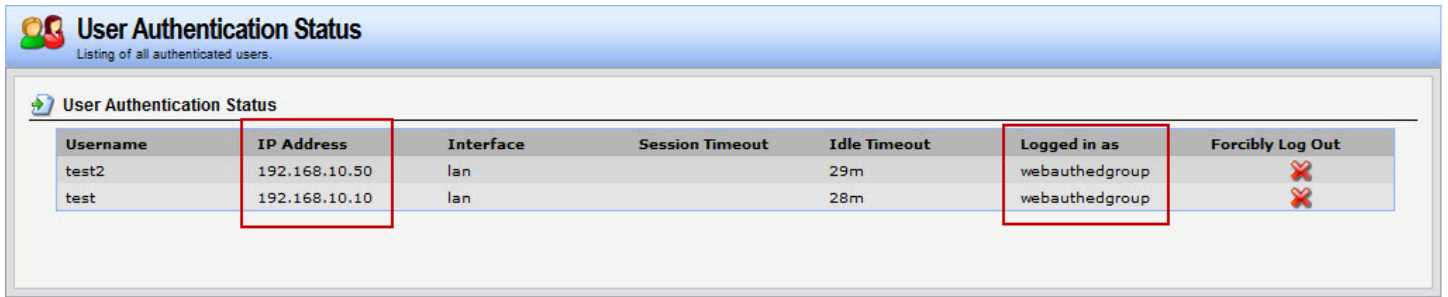
- Support Interim Accounting
  - Server controlled value

Interim Value:  seconds The interval in seconds which the unit should send interim accounting events. Note that this value should not be less than 600 seconds.

OK Cancel

[Test]

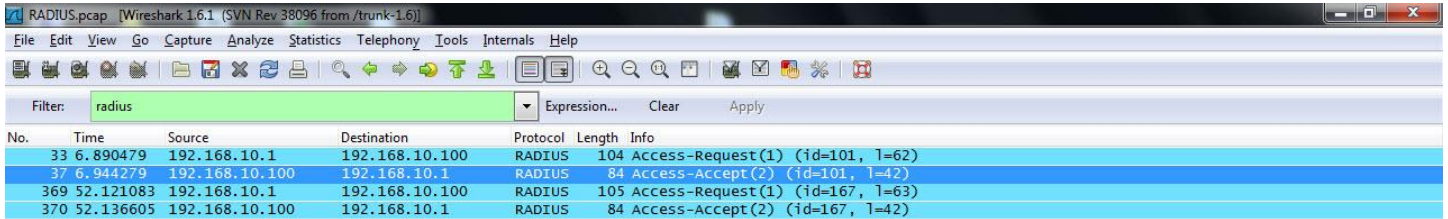
PC1 & PC2 login on WEB authentication.



The screenshot shows a web interface titled "User Authentication Status" with the subtitle "Listing of all authenticated users." Below the title is a table with the following columns: Username, IP Address, Interface, Session Timeout, Idle Timeout, Logged in as, and Forcibly Log Out. Two rows of data are visible, both with red boxes highlighting the IP Address and Logged in as columns.

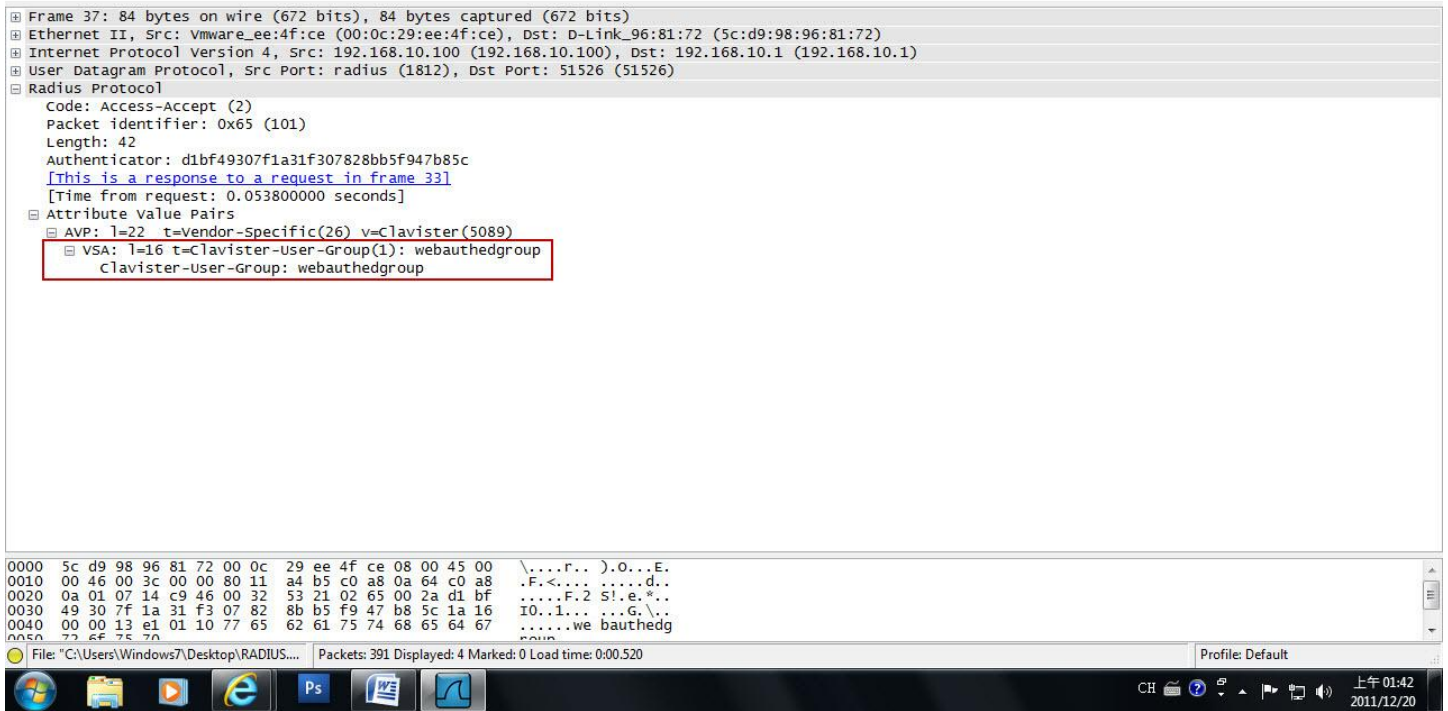
Username	IP Address	Interface	Session Timeout	Idle Timeout	Logged in as	Forcibly Log Out
test2	192.168.10.50	lan		29m	webauthedgroup	✘
test	192.168.10.10	lan		28m	webauthedgroup	✘

### RADIUS Server packet



The screenshot shows a Wireshark packet capture window for "RADIUS.pcap". The filter is set to "radius". The packet list shows four packets related to RADIUS authentication:

No.	Time	Source	Destination	Protocol	Length	Info
33	6.890479	192.168.10.1	192.168.10.100	RADIUS	104	Access-Request(1) (id=101, l=62)
37	6.944279	192.168.10.100	192.168.10.1	RADIUS	84	Access-Accept(2) (id=101, l=42)
369	52.121083	192.168.10.1	192.168.10.100	RADIUS	105	Access-Request(1) (id=167, l=63)
370	52.136605	192.168.10.100	192.168.10.1	RADIUS	84	Access-Accept(2) (id=167, l=42)



The screenshot shows the packet details pane for the selected RADIUS packet (Frame 37). The details are as follows:

- Frame 37: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
- Ethernet II, Src: vmware\_ee:4f:ce (00:0c:29:ee:4f:ce), Dst: D-Link\_96:81:72 (5c:d9:98:96:81:72)
- Internet Protocol Version 4, Src: 192.168.10.100 (192.168.10.100), Dst: 192.168.10.1 (192.168.10.1)
- User Datagram Protocol, Src Port: radius (1812), Dst Port: 51526 (51526)
- Radius Protocol
  - Code: Access-Accept (2)
  - Packet identifier: 0x65 (101)
  - Length: 42
  - Authenticator: d1bf49307fia31f307828bb5f947b85c
  - [This is a response to a request in frame 33]
  - [Time from request: 0.053800000 seconds]
  - Attribute Value Pairs
    - AVP: l=22 t=Vendor-Specific(26) v=Clavister(5089)
    - VSA: l=16 t=Clavister-User-Group(1): webauthedgroup
    - Clavister-User-Group: webauthedgroup

The hex dump at the bottom shows the raw data of the packet, with the ASCII column displaying ".....we bauthedg" and ".....".

END