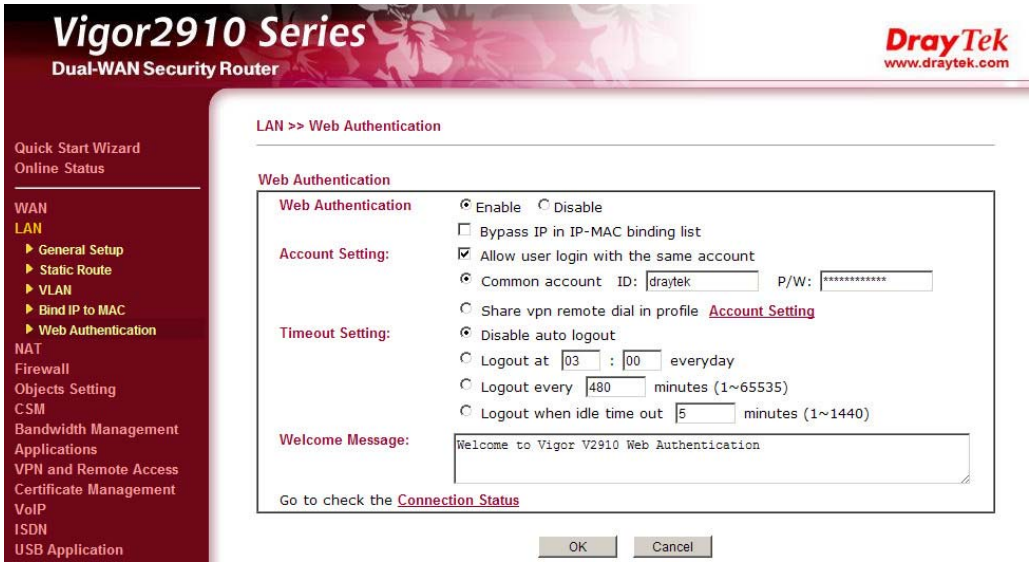
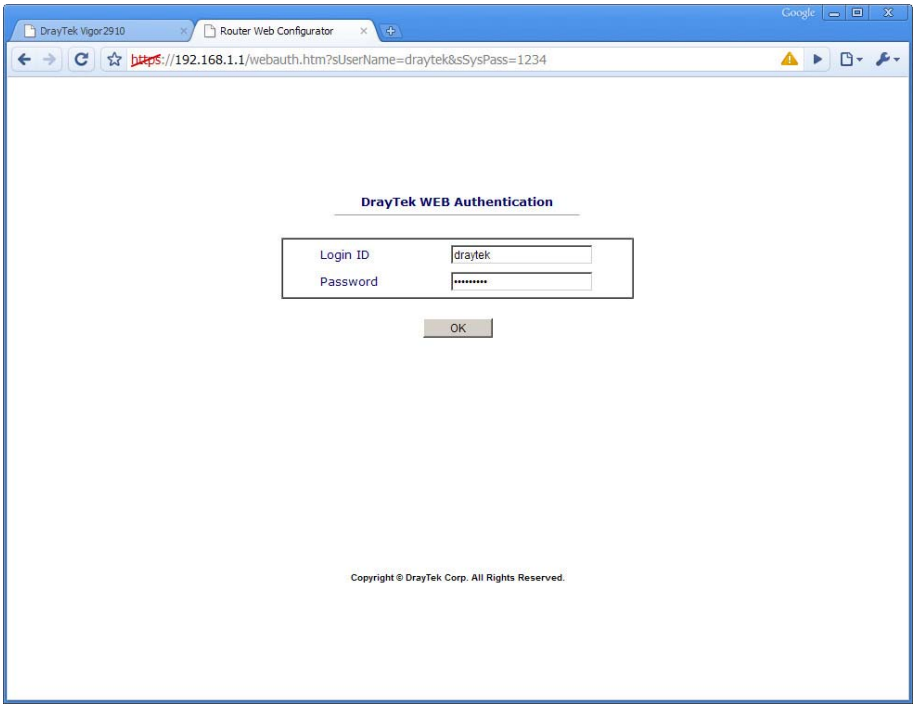
Web Authentication Application Note

What is Web Authentication?



Web authentication is a Layer 3 security feature that causes the router to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. Web authentication provides simple authentication without a supplicant or client utility. Keep in mind that web authentication does not provide data encryption.

With web authentication, users of a host provide their authentication credentials using a portal or webpage on a web browser. An example of this portal or webpage is shown below.

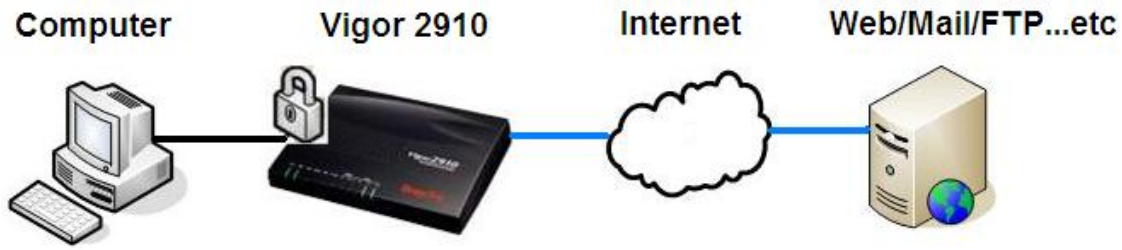


If the authentication credentials are valid, then the host is authorized on the network. If the authentication credentials are not valid, then the host will be blocked from the network until the user enters valid authentication credentials.

Quick Web Authentication Demonstration

This quick web authentication demonstration provides a very quick and easy demonstration of how to setup web authentication on Vigor 2910. For additional helpful tips and customized configuration for web authentication please refer to the **Options for Web Authentication** section.

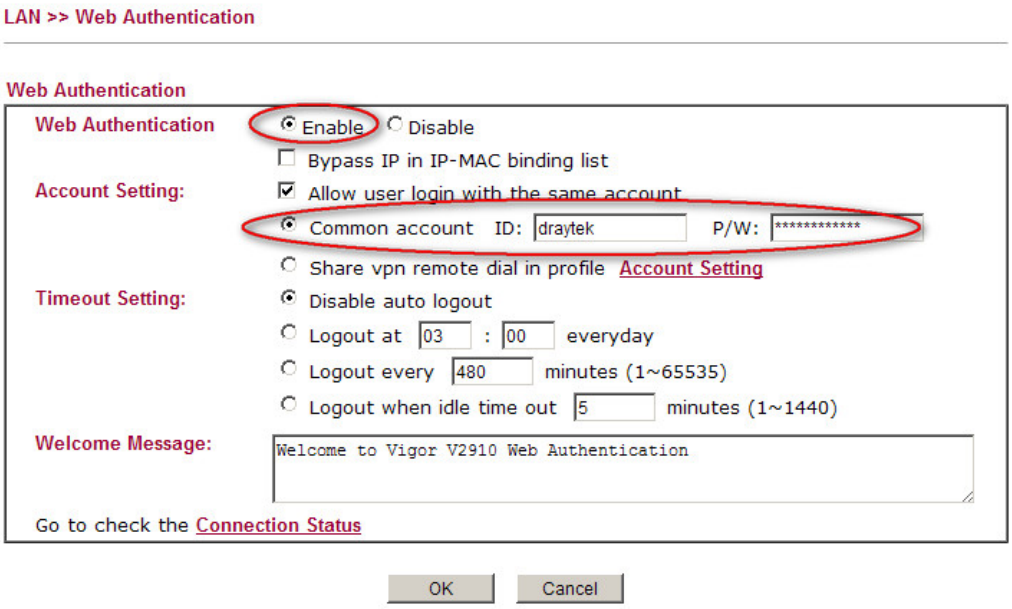
1. Connect the devices as shown in the diagram below:



2. Assign the following IP addresses to the devices:
   - LAN of Vigor 2910: **192.168.1.1/24**
   - WAN of Vigor 2910: **172.17.1.128/24**, Gateway: **172.17.1.1**
   - Computer: **192.168.1.10/24**; Gateway: **192.168.1.1**
   - You may also use DHCP to get an IP address via Vigor 2910

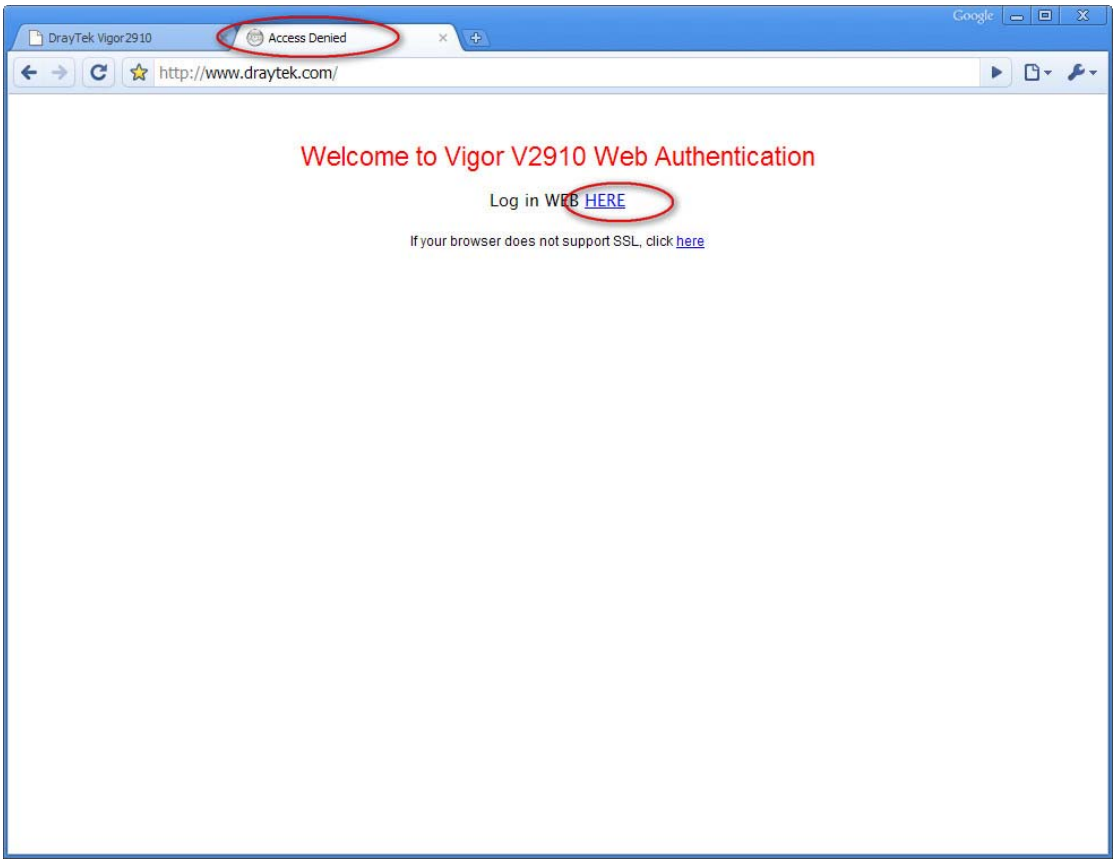
   Helpful tip: You do not have to use these exact IP address. They are just provided as an example to help explain this demonstration.

3. Connect to Vigor 2910's web configurator and setup the Web Authentication as follows:
   Choose **Enable** to enable Web Authentication. In Account Setting, choose **Common Account ID**, and input the preferred account name and password. Here we use **draytek/draytek**.
   Press **OK** to save the settings.



4. From the computer, open a web browser:

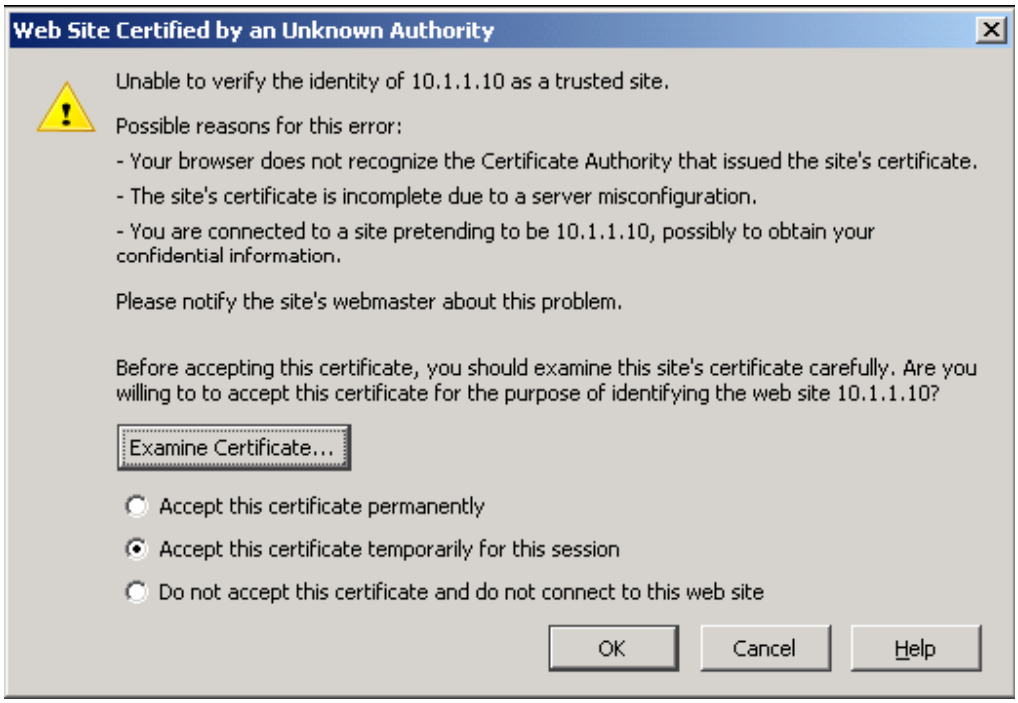
- Direct the web browser to a web server, e.g., http://www.draytek.com.
- This time, Vigor 2910 will redirect the web browser to the welcome webpage. The default **Welcome** webpage looks like this:



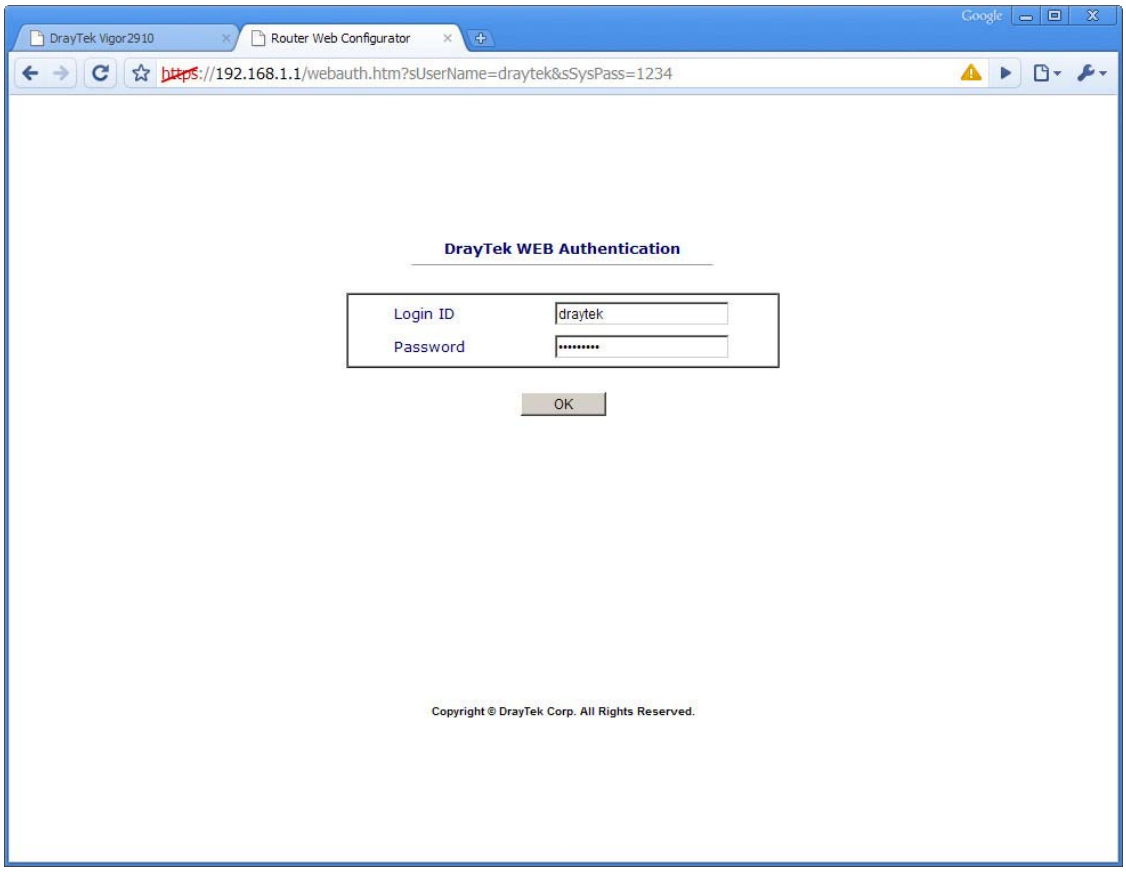
- Click the link **HERE** on the web page to proceed.
- If the web browser is Microsoft Internet Explorer, you may get the alert (depending on your web browser's security settings) below:

- When you see this alert, click **Yes**.

- If the web browser is Mozilla Firefox, you may get this alert (depending on your web browser's security settings):



- If you see this alert, click **OK**.
- The web server will redirect the web browser to the **Authentication** webpage. The **Authentication** webpage will look something like this:



- Enter a valid User ID and Password. Here is draytek/draytek. Click OK.
- The web server should redirect you to the **Successful Authentication** webpage.

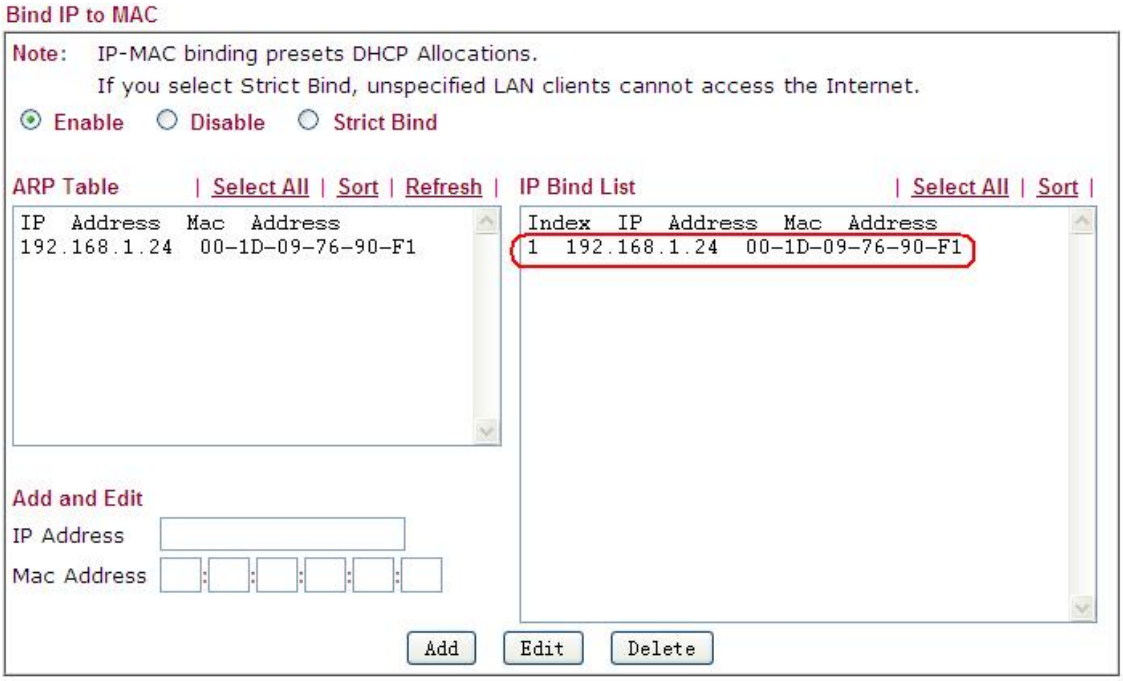
Now this user has passed the authentication and should be able to access the Internet.

Helpful tip: If somebody in the LAN needs to use non-web applications such as IM applications, video conference and etc, he must first open the web browser and type a random external website to pass the authentication first.

Options for Web Authentication

Bypass IP in IP-MAC binding list

If this box is checked, then the IP addresses in the IP-MAC binding list will originally have the authority to access the Internet without inputting authentication credentials for web authentication first. Only the computers whose IP addresses are not in the IP-MAC binding list need to pass Web Authentication first.



Account Setting

The same account can be used for different LAN users for web authentication only if **Allow user login with the same account** is selected. Otherwise, only the first login user can pass web authentication and gain Internet access, other users will get the following error message.

DrayTek WEB Authentication

User login fails !!!

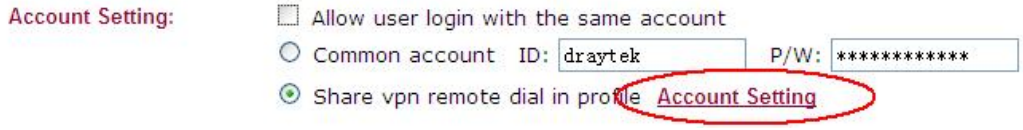
Account already logined.

There are two account settings, **Common Account** and **Share vpn remote dial in profile**.

With **Common Account** and **Allow user login with the same account** enabled, all the users share the same account.

With **Share vpn remote dial in profile**, you may set different accouts for different users as follows.

- Enable **Share vpn remote dial in profile** and press **Account Setting**.



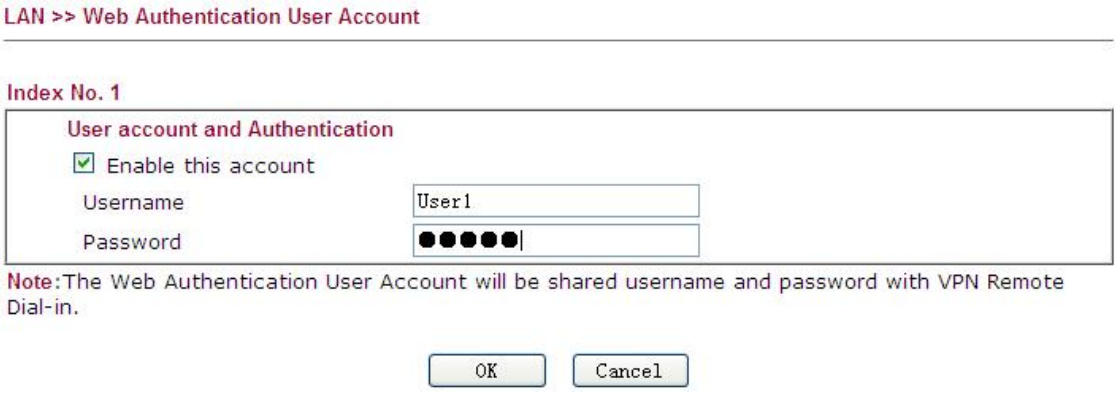
- In the **Web Authentication User Account** setup page, press one index and set the account.

LAN >> Web Authentication User Account

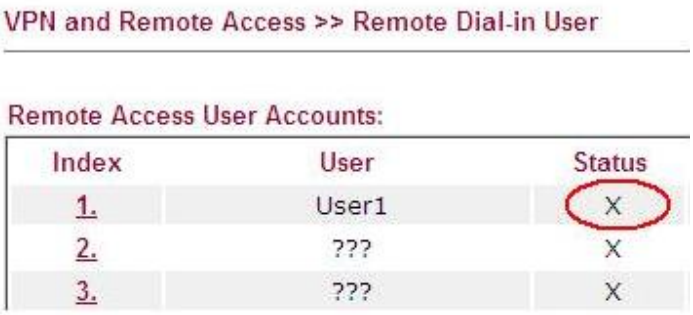
Web Authentication User Account:

Index	User	Status	Index	User	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

- Tick **Enable this account** and set the Username/Password.



Helpful tip: Web Authentication User Account shares the same profile as VPN remote dial-in profile. So, if you go to the **VPN and Remote Access >> Remote Dial-in User** setup page, you will find the profile set in Web Authentication User Account page is also shown in this page. But the status is 'X', as shown below.

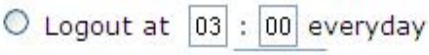


Helpful tip: Though web authentication user account and vpn dial-in user share the same profile, you should always setup them respectively in correct setup page. Don't setup the web authentication user account from vpn dial-in user setup page, and vice verse.

Timeout Setting

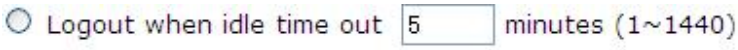
Currently we provide four modes here for the timeout mechanism of the authenticated clients. Admininstarator can configure the router to log the clients out in:

- A special time every day

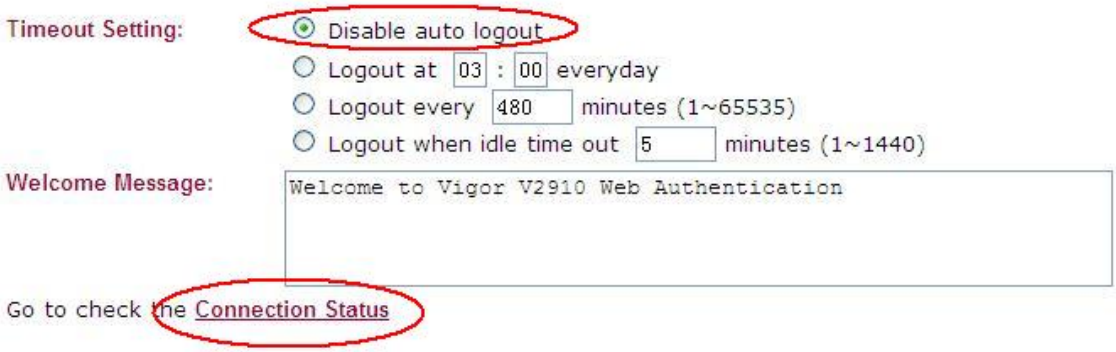


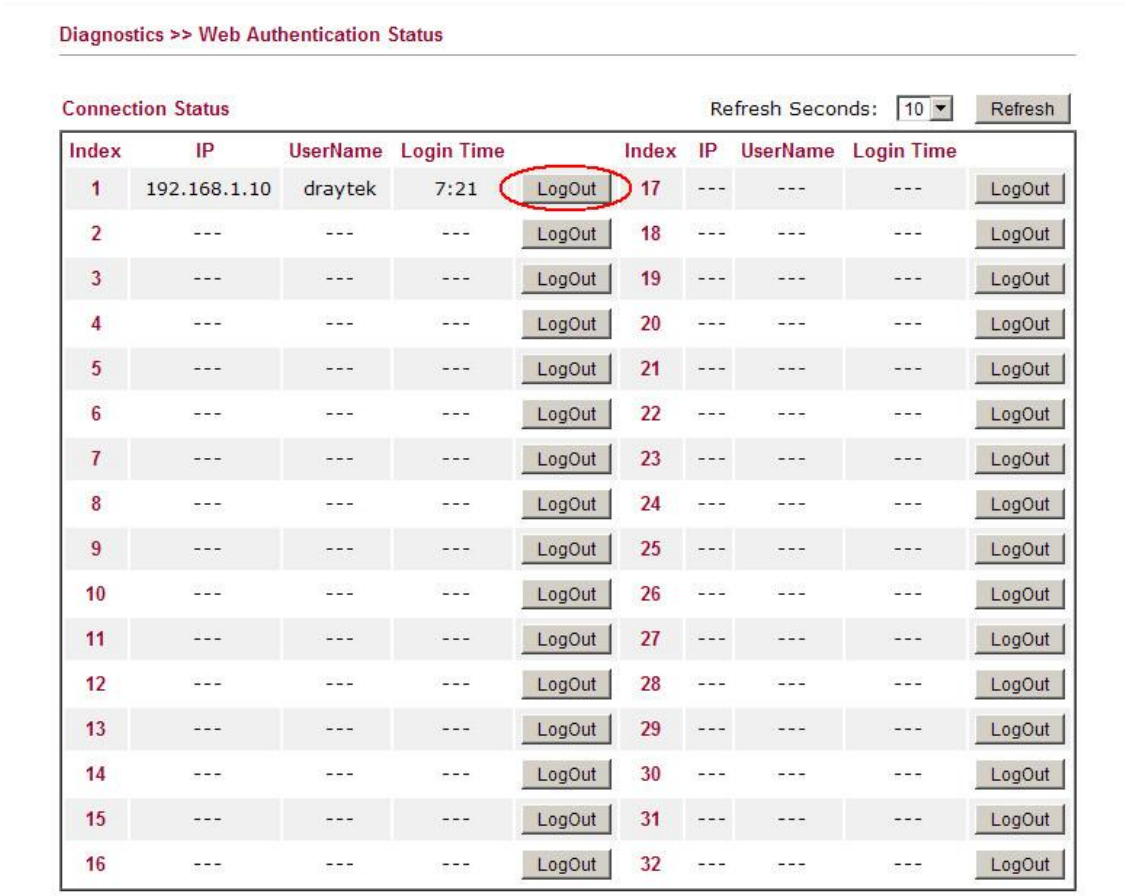
- After a duration of time

- After or a certain length of idle time.



When you select **Disable auto logout**, you may manually log the user out from **Connection Status** page.





Index	IP	UserName	Login Time		Index	IP	UserName	Login Time	
1	192.168.1.10	draytek	7:21	LogOut	17	---	---	---	LogOut
2	---	---	---	LogOut	18	---	---	---	LogOut
3	---	---	---	LogOut	19	---	---	---	LogOut
4	---	---	---	LogOut	20	---	---	---	LogOut
5	---	---	---	LogOut	21	---	---	---	LogOut
6	---	---	---	LogOut	22	---	---	---	LogOut
7	---	---	---	LogOut	23	---	---	---	LogOut
8	---	---	---	LogOut	24	---	---	---	LogOut
9	---	---	---	LogOut	25	---	---	---	LogOut
10	---	---	---	LogOut	26	---	---	---	LogOut
11	---	---	---	LogOut	27	---	---	---	LogOut
12	---	---	---	LogOut	28	---	---	---	LogOut
13	---	---	---	LogOut	29	---	---	---	LogOut
14	---	---	---	LogOut	30	---	---	---	LogOut
15	---	---	---	LogOut	31	---	---	---	LogOut
16	---	---	---	LogOut	32	---	---	---	LogOut

Welcome Message

The message specified here will be displayed to unauthenticated users when they open a web site for the first time.