Setup PPTP Connection Over VPN for a VPN Client Access on RV220W From MAC Operating System

Objective

This document explains the procedure to use the MAC operating system's default VPN client to setup a PPTP connection over VPN Tunnel for a VPN Client Access. Suppose if there are two sites Site A and Site B. Both have a VPN Tunnel established between them. Both use the same RV220W device. A client user credential with username and password is set on Site B. Then the document explains the procedure to access Site B from Site A over the Tunnel in the MAC OS environment.

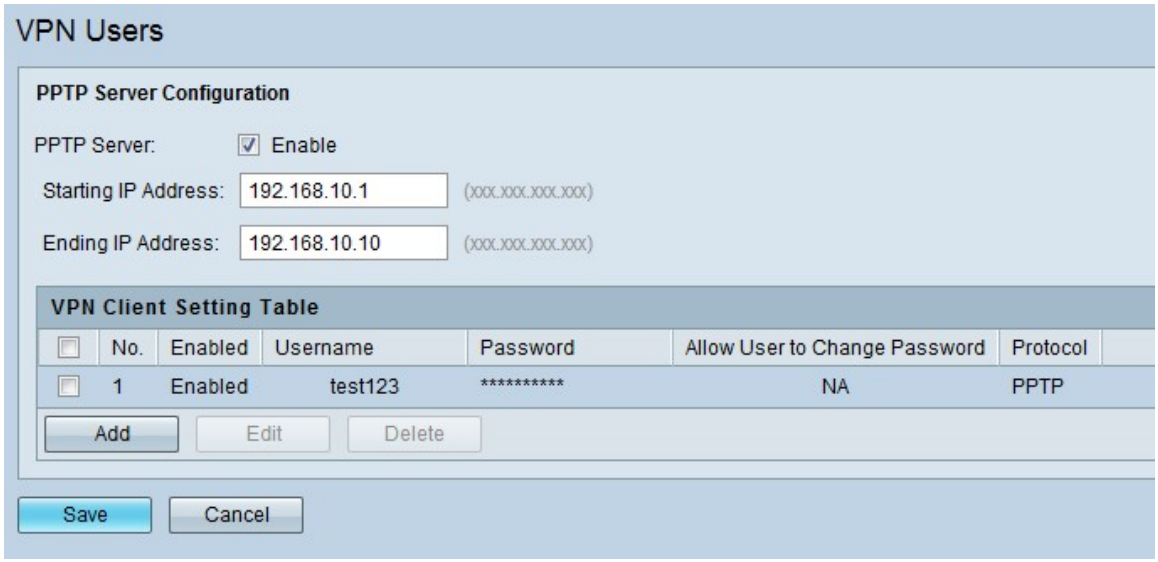
Applicable Devices

- RV220W
- RV120W

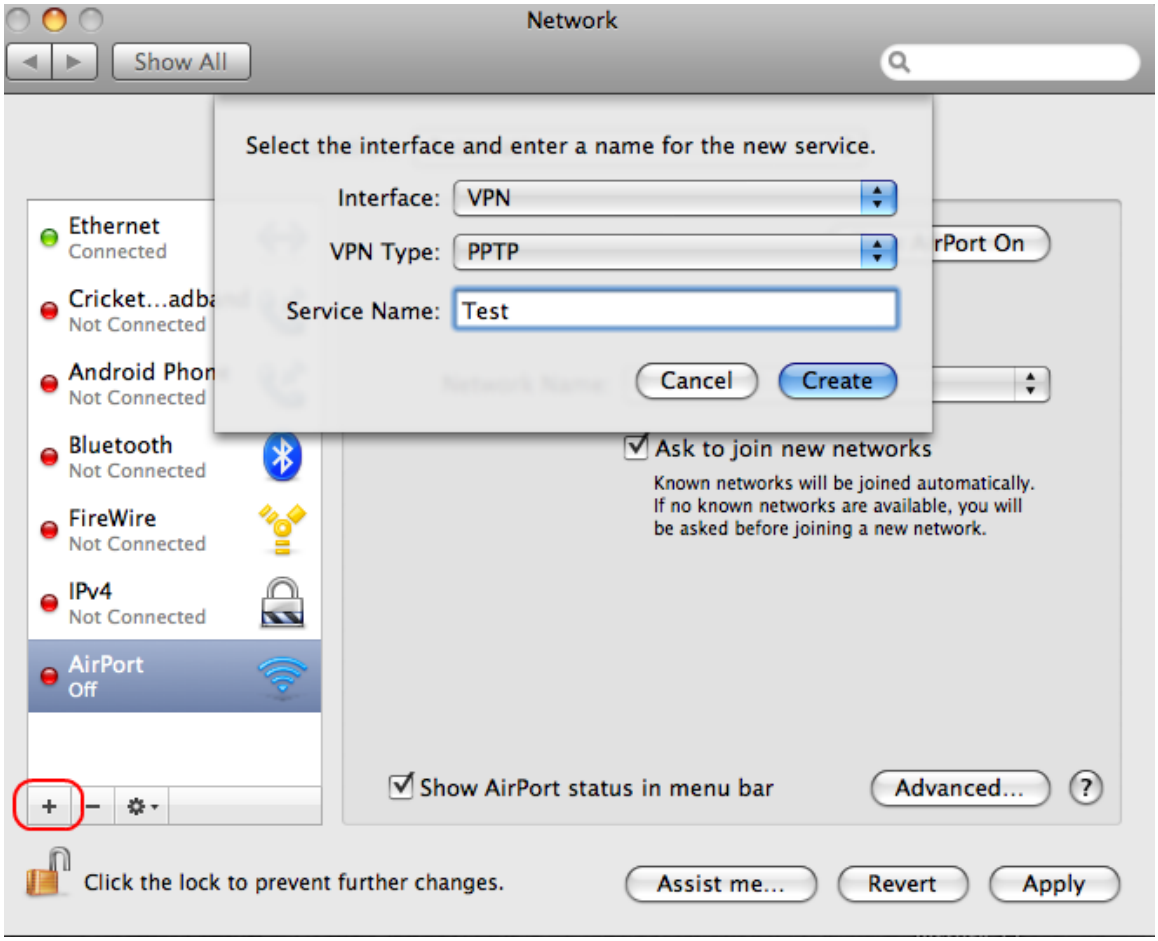
VPN Connection Setup

VPN User Set at Remote Site

A VPN user for PPTP is already set up on the Remote Site. The username being test123 and password being test123123.



VPN Connection Creation



Step 1. Click the **+** sign to create a new connection.

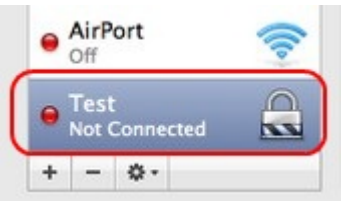
Step 2. Choose **VPN** from the Interface drop-down list as the desired connection to be set is VPN.

Step 3. Choose **PPTP** from the VPN Type drop-down list; as PPTP is the type of VPN connection to be set.

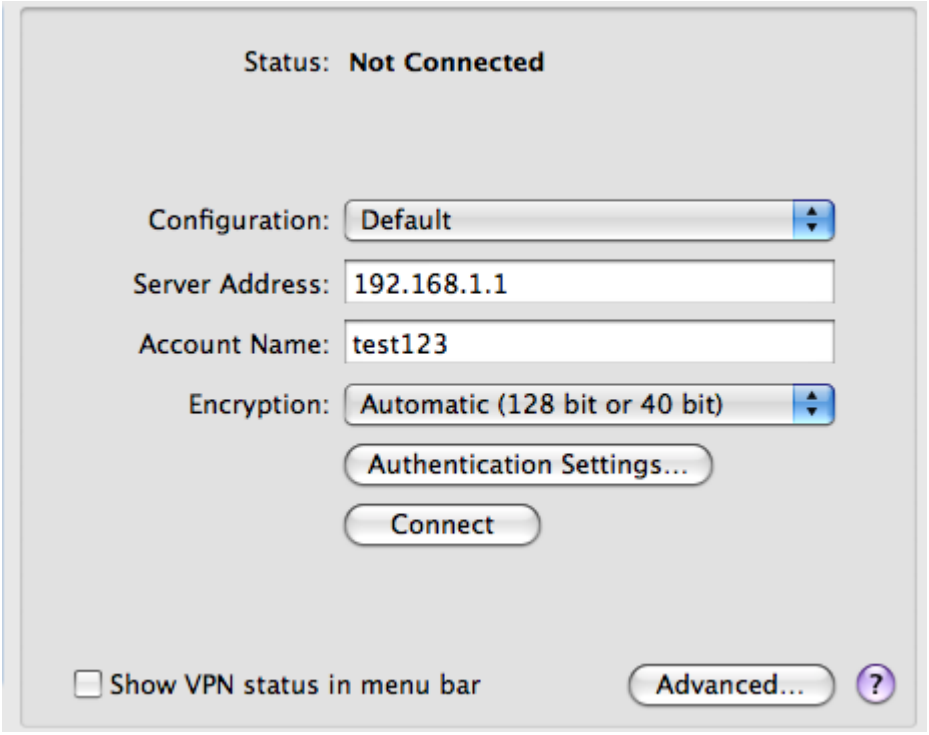
Step 4. Enter any name for the connection in the Service Name field. In the example the name Test is entered.

Step 5. Click **Create** to create the VPN connection.

Configuration of the VPN Connection



Step 1. Click the connection Test created from the connections displayed to configure the settings.

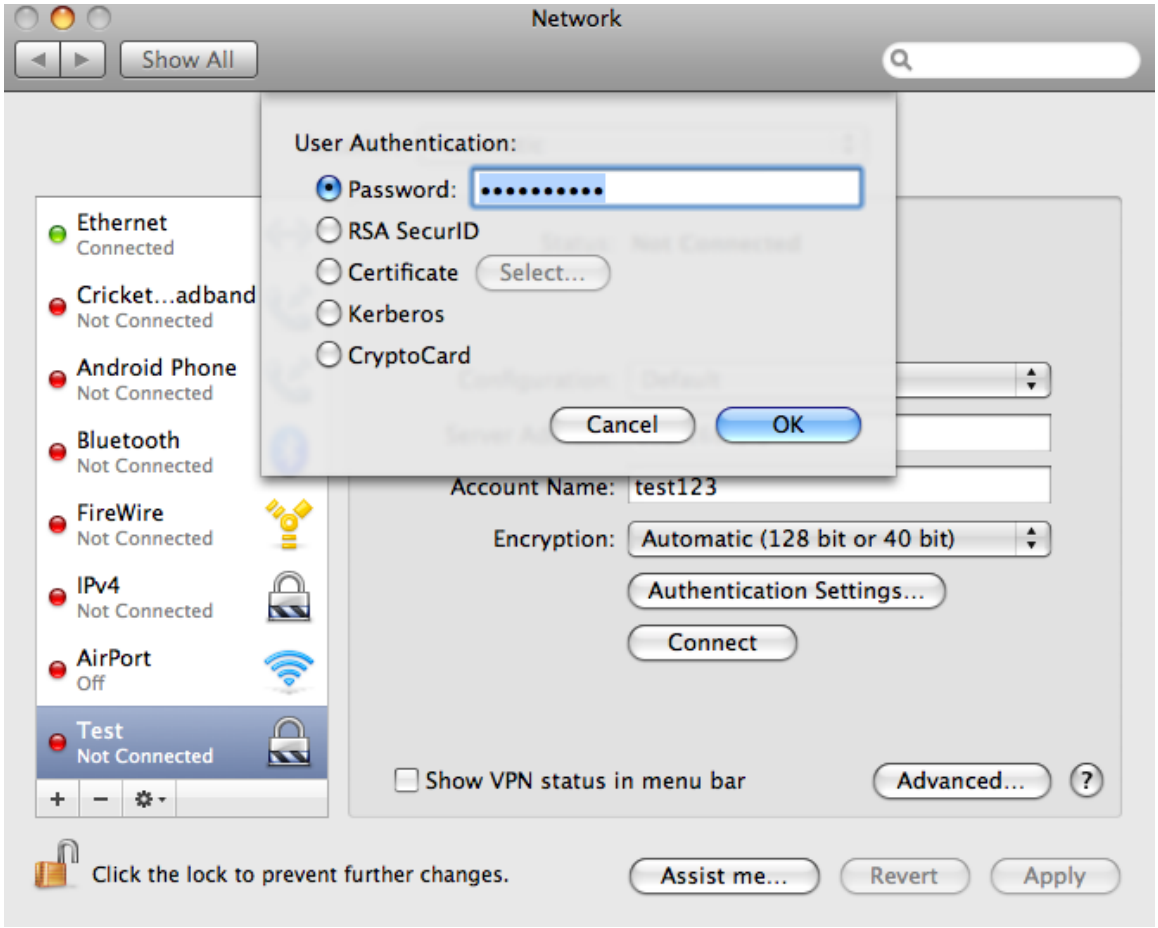


Step 2. The Configuration drop-down list gives information about any previous configuration settings saved for any connection. If it is required to save the configuration settings of the connection, then choose **Add Configuration** option from the Configuration drop-down list. In this case it is not required to save the configuration settings and therefore the **Default** option is chosen.

Step 3. Enter the IP Address of the server in the Server Address field. The Server Address is the Remote Local Area Network IP Address of the device on end point of the tunnel. Here in this case the Local Local Area Network IP Address is 192.168.10.1 and Remote Local Area Network Address is 192.168.1.1.

Step 4. Enter the appropriate account user name in the Account Name field. Here the Account Name is the username (test123).

Step 5. Click **Authentication Settings**. A dialog box that allows the user to enter a password appears.



Step 6. Click the **Password** radio button as the user authentication method is set as password. Then enter the password in the corresponding field. In this example, the password is test123123. This password is for the account user.

• RSA SecurID — There is a portable device sometimes given to the users which generates a numeric value. If the authentication mechanism is set by the server is through this numeric value then this option is used.

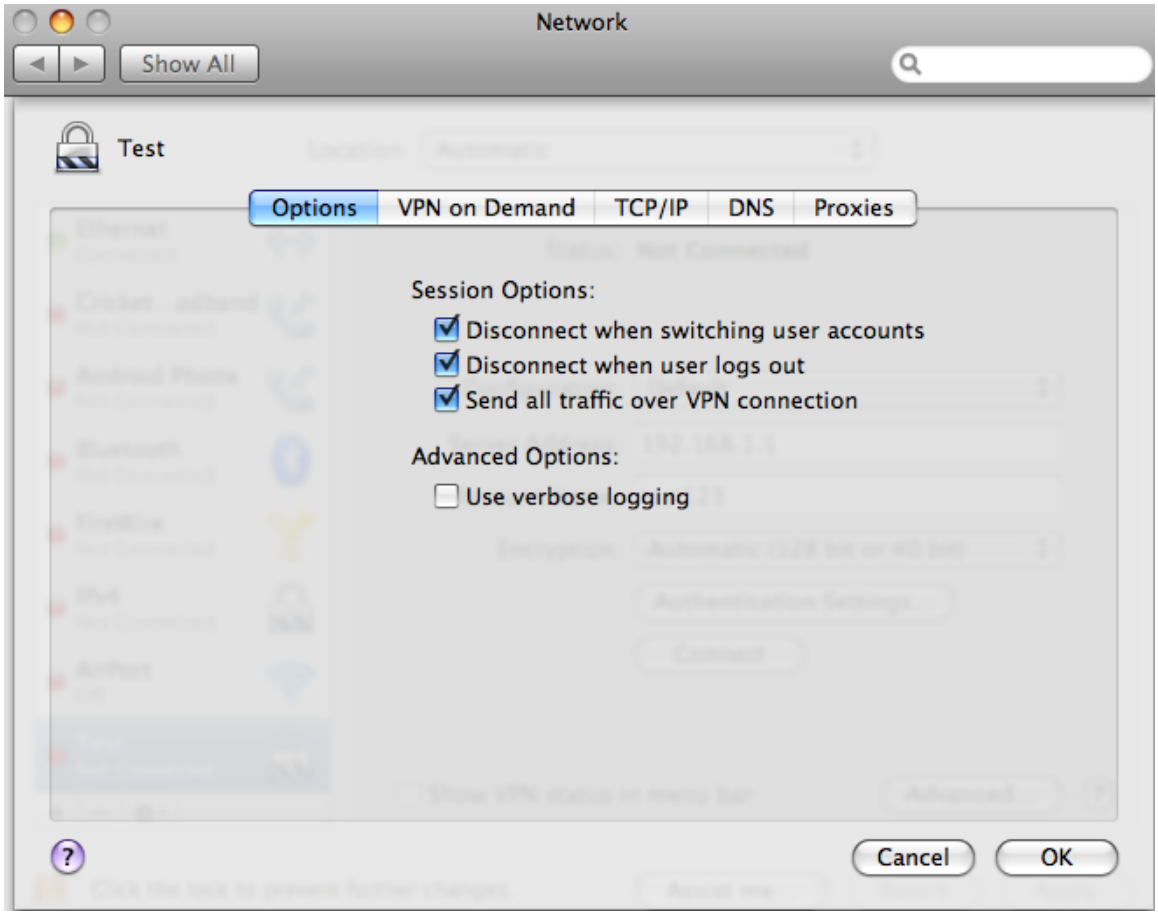
• Certificate — The server sometimes issues authentication certificates to the user. If the user has downloaded certificate present then those can be uploaded for authentication. Click the **Select** button to choose the appropriate certificate downloaded.

• Kerberos — Kerberos is a security protocol used for user authentication. The user sends the Account User Name entered to the server. The server authenticates the user and sends the user a session key and a Ticket which basically has information about the user's ID, user's Network Address and session validity period.

• CryptoCard — The CryptoCard method will inform the user a password from the server each time the user logs into the server.

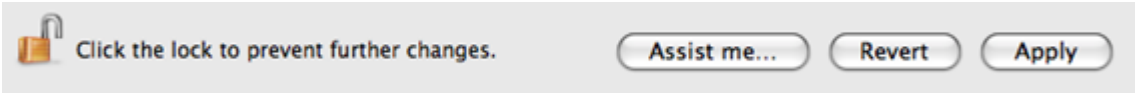
Step 7. Click **Ok**.

Step 8. To make sure all the traffic is being sent through VPN, Click the **Advanced**.

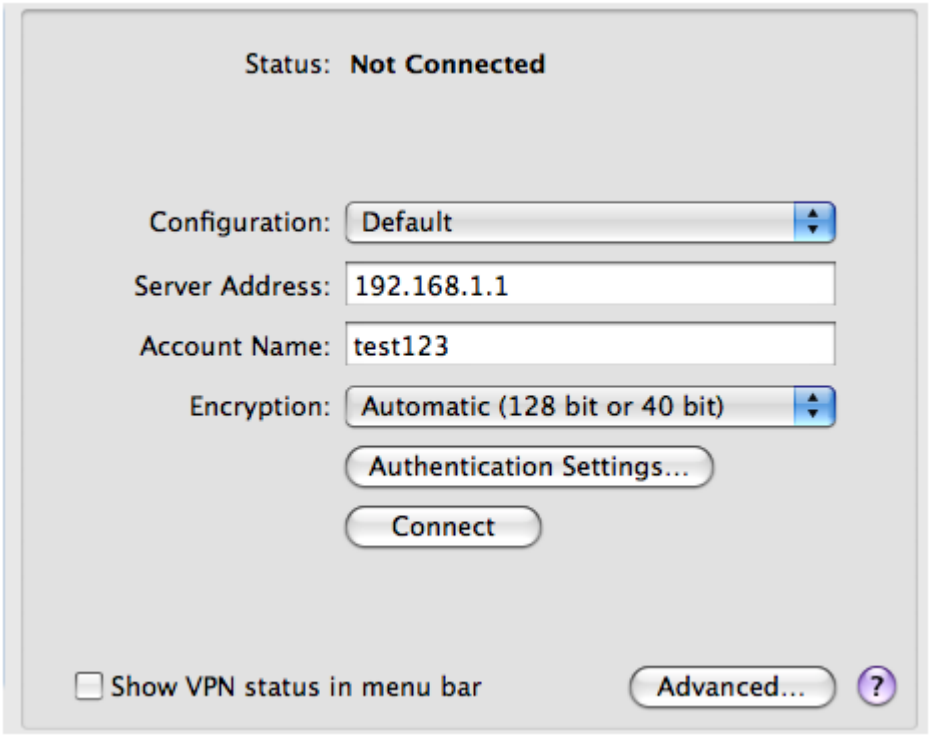


Step 9. Check the **Send all traffic over VPN** check box. This will enable all the packets to go through the VPN connection.

Step 10. Click **Ok**.



Step 11. Click **Apply** button to apply the configurations made to the connection.



Step 12. Click **Connect** to connect.