FATPIPE NETWORKS

SSL VPN

Installation Guide

Phone +1 801-281-3434 • +1 801-683-5656 • Fax 801-847-6600 • Toll Free: +1 800.724.8521

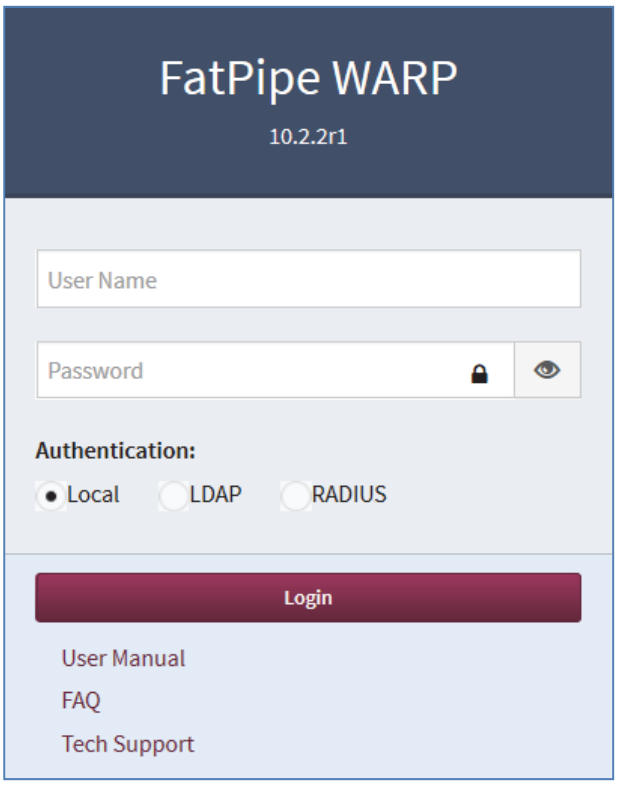
Table of Contents

Overview

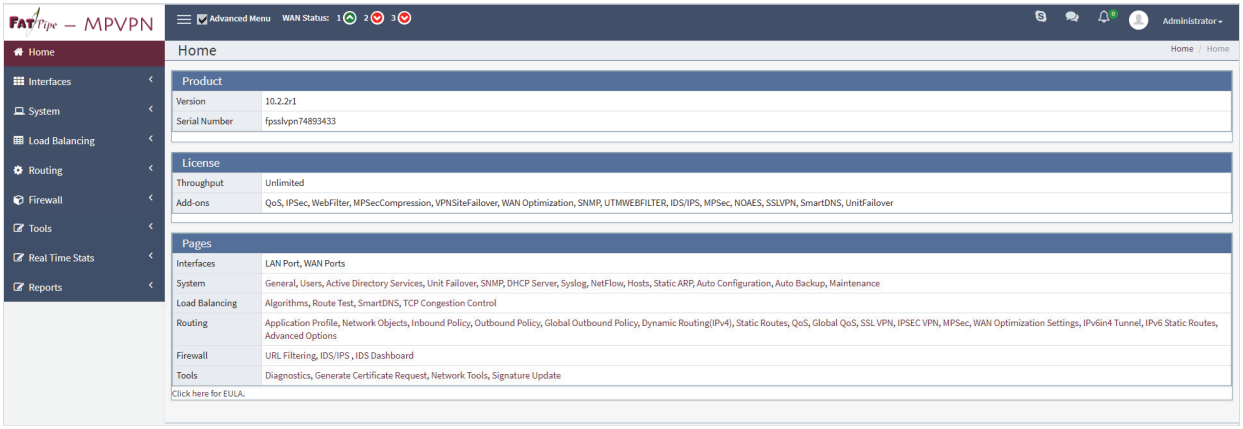
This installation guide outlines the steps to setup SSL VPN configuration to enable remote access for users.

User Login

1. Go to the **FatPipe WARP** login page as show below.

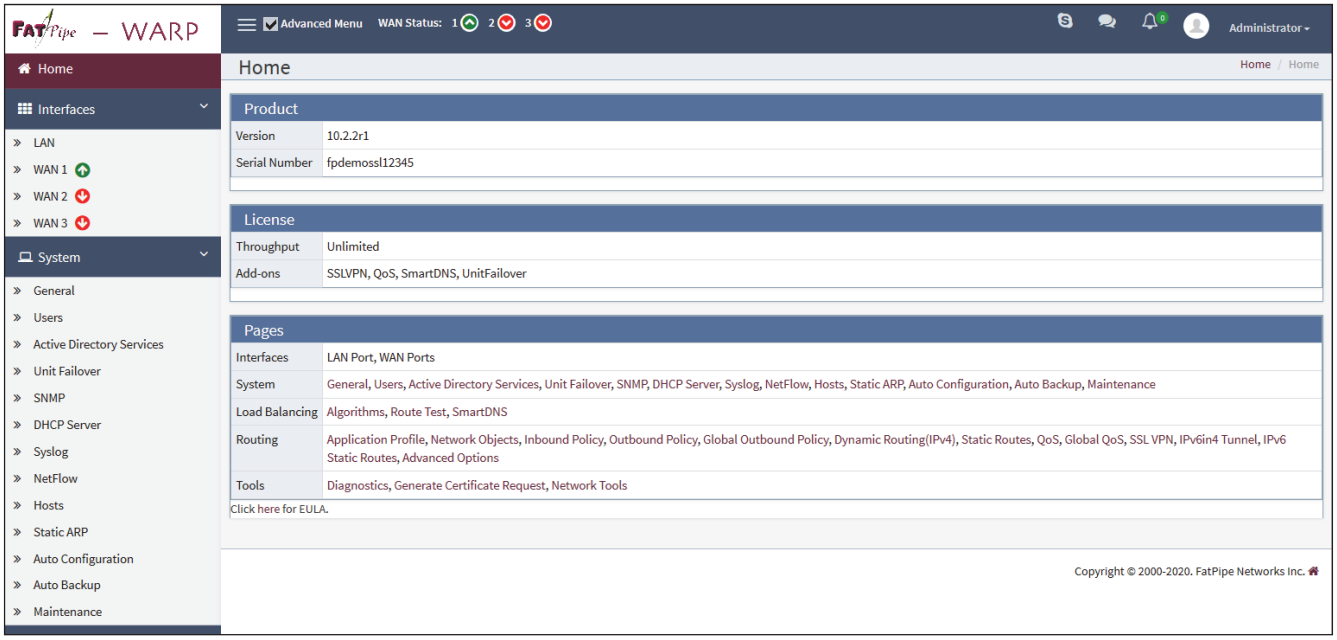


Enter the **User Name** and **Password** to login to the device. On successful login you should see the home page.

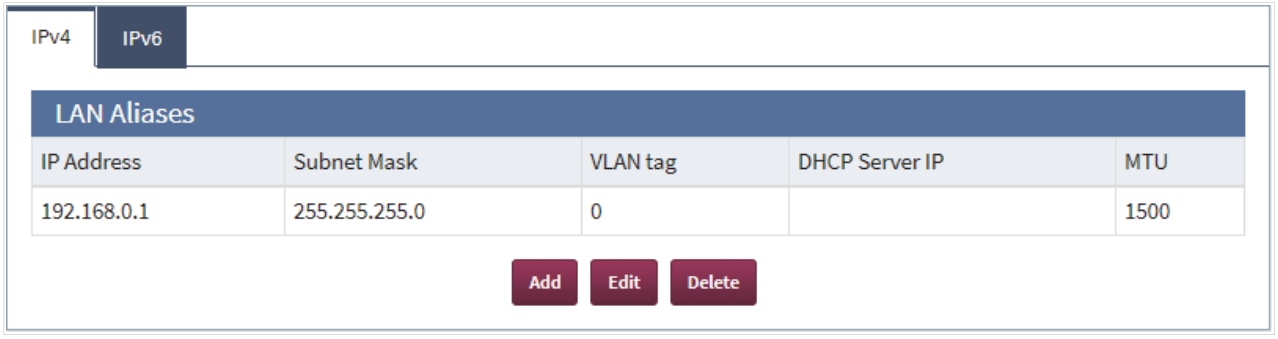


LAN Configuration

Click **Interfaces->LAN**. The **LAN** page is displayed.



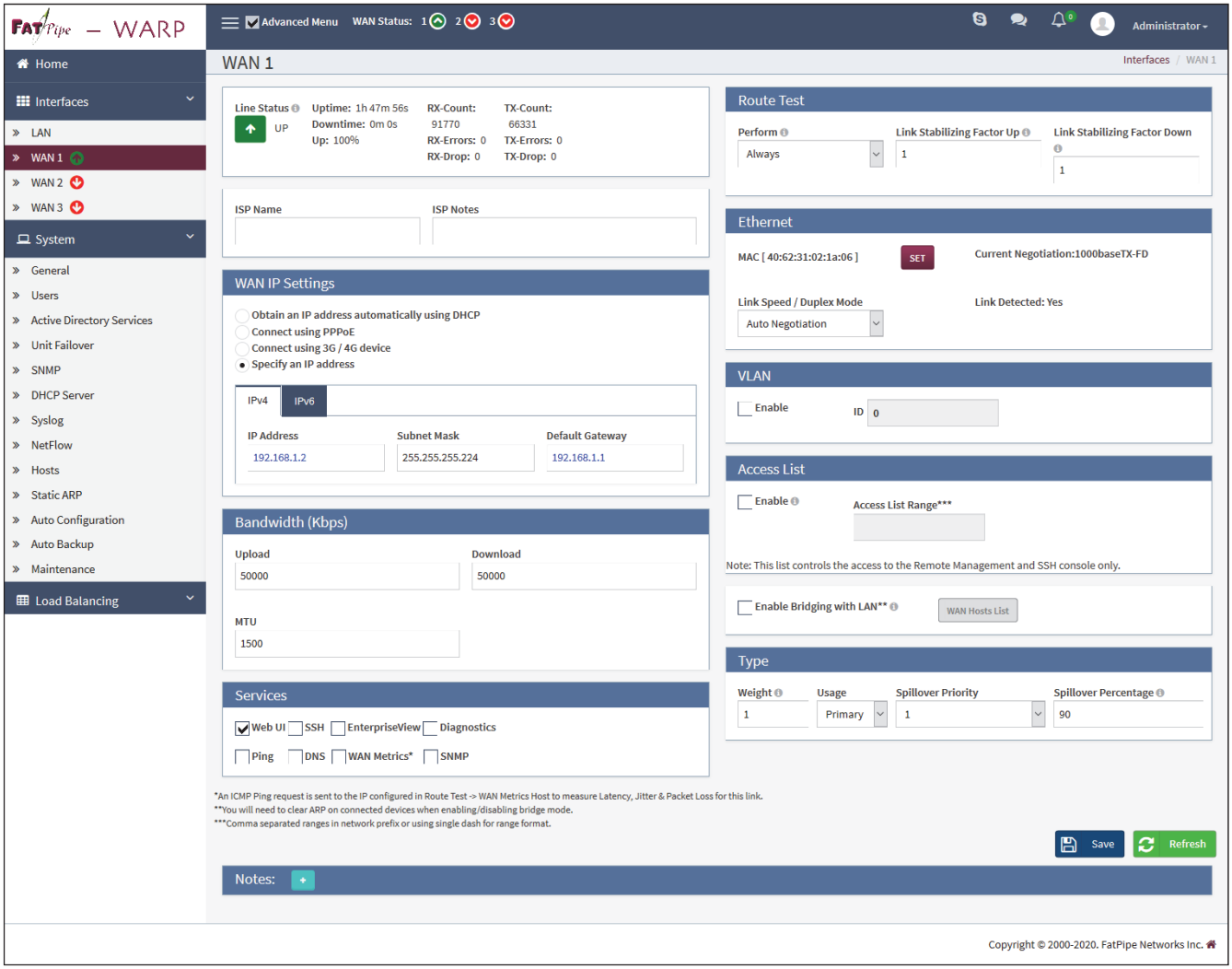
Click **Add** and enter the IP Address and Subnet Mask for each IP subnet connected to the LAN interface to configure one or more IP addresses on the LAN interface.



3. Click **Save** to make the changes permanent.

WAN Configuration

From the FatPipe **WARP** home page, click on the respective WAN page to display the wan settings.



Select **Obtain an IP address automatically using DHCP** to have WAN IP settings assigned dynamically by a DHCP server.

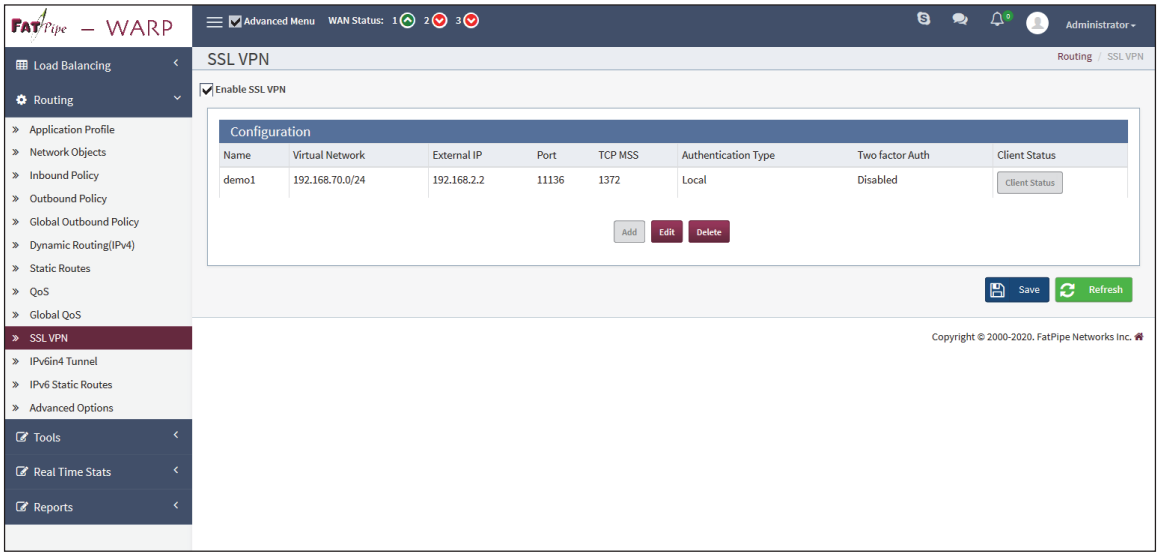
To connect to your ISP using PPPoE, select **Connect using PPPoE**.

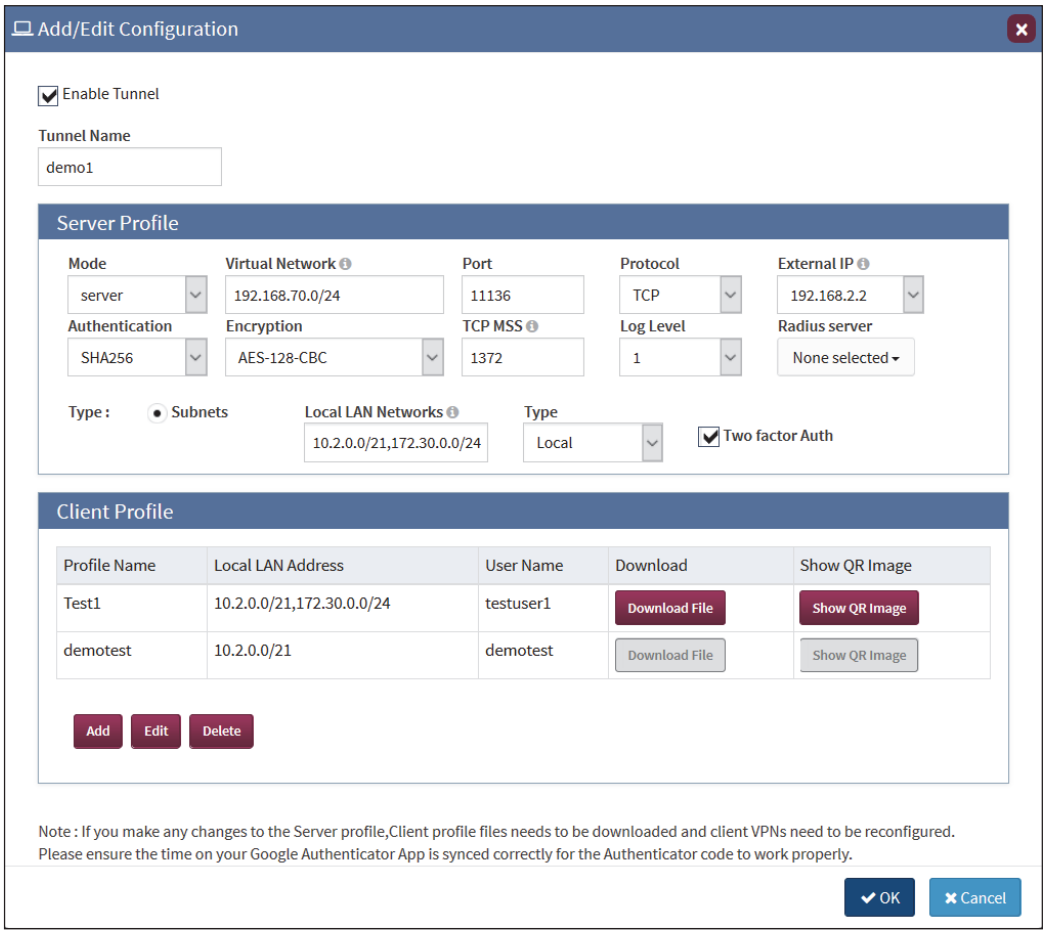
To connect a 3G/4G line, plug a 3G USB Modem to any of the USB interfaces on the WARP device. The USB Modem will be automatically detected. Select **Connect using 3G/4G device**.

Choose the device model from the **Detected 3G/4G USB Modem** drop down, IMEI/ESN and Model Name of the USB Modem will be displayed. This information cannot be modified. The APN and Phone Number will also be displayed. This information can be modified. Click **SAVE** to make the changes permanent. Select **Specify an IP address** to assign IP Address, Subnet Mask, and Default Gateway settings to each WAN interface. The Default Gateway is typically the IP address of your WAN router.

SSL VPN Configuration

From the FatPipe **WARP** home page, click **SSL VPN** to display the **SSL VPN** . Click **Add** or **Edit** to add or edit an SSL VPN configuration. The **Add/Edit Configuration** page is displayed.





Select the **Enable Tunnel** checkbox. Enter the tunnel name in the **Tunnel Name** field.

Server Profile

Enter the following details in the **Server Profile** section in the **Add/Edit Configuration** window to configure the server.

Field	Description
Mode	Select the server mode from the **Mode** drop-down.
Virtual Network	Enter the subnet from which the client will be assigned an IP address.
Port	Enter the port number in which the server is running.
Protocol	Select UDP or TCP from the **Protocol** drop-down.
External IP	Select the WAN IP through which the tunnel is established, in this case, 14.14.14.1.
Authentication	Select the authentication method from the **Authentication** drop-down. The available options are **SHA1** **SHA256** **SHA384** **SHA512**
Encryption	Select the encryption type from the Encryption drop-down. The available options are **BF-CBC** **AES-128-GCM** **AES-192-GCM** **AES-256-GCM** **AES-128-CBC** **AES-192-CBC** **AES-256-CBC**
TCP MSS	The MSS value helps set the maximum segment size. The size range is from 576 to 1460. The default value is 1372.
Log Level	The user can choose log levels from 1 to 7 for debugging purposes.
Radius Server	Select the radius server from the Radius Server drop-down if already configured.
Type and Local LAN Networks	Select the Subnet button next to **Type**. In the **Local LAN Networks** box, mention the local LAN subnets you want to allow the client to access.

Select the user configuration type from the **Type** drop-down. The available options are **Local** and **Radius**.

Select the Type as Local for on-device Authentication of user accounts.

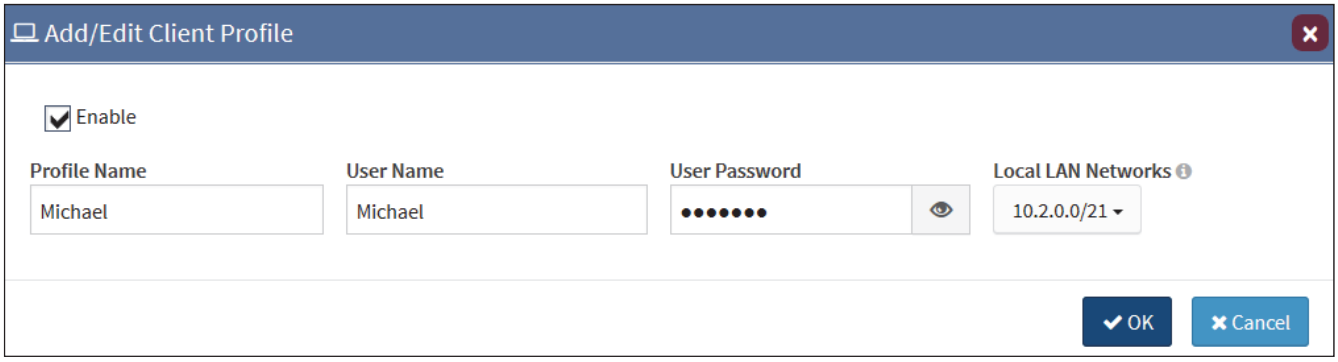
Select the **Type** as **Radius** if you have Radius configured. Select the ADS User from the **ADS User** drop-down.

Select the **Two factor Auth** checkbox to enable two factor authentication through Google Authenticator.

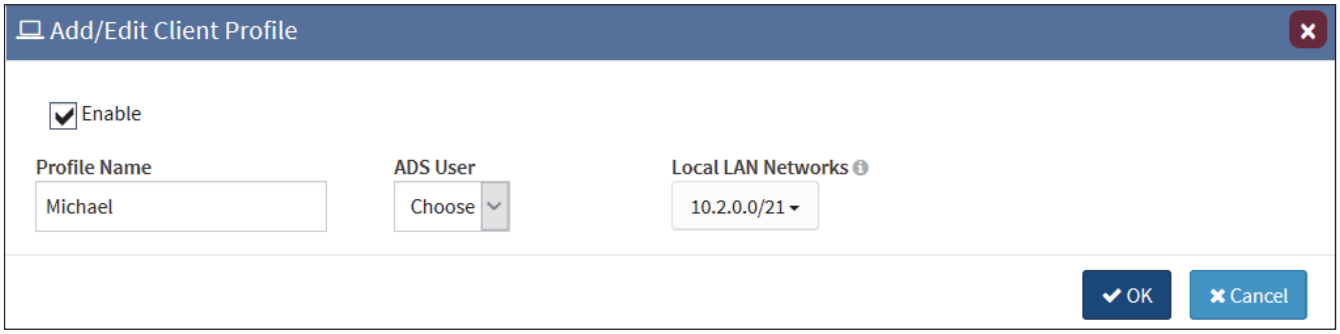
Client Profiles

In the **Client Profile** section, click **Add** to add a client profile. The **Add/Edit Client Profile** window is displayed.

User Entry screen for local authentication users



User Entry screen for RADIUS Authentication Users



Select the **Enable** checkbox.

Enter the profile name in the **Profile Name** field.

If you select the **Type** as **Local**, you will have to configure the username and password in the **User Name** and **Password** fields.

Select one or multiple LAN subnets from the **Local LAN Networks** list.

Click **OK** to save the details.

Downloading the OVPN File for Client

After adding clients and users in the **Client Profile** section, the Download File button gets enabled as shown below:

Click the **Download File** button to download the OVPN file for the client.

Click the **Show QR Image** field to view the QR code.

Note: For logging in, the end user needs to have the OVPN file, username and password to login, and time based OTP from Google Authenticator.

Viewing Connected Clients

1. After configuring the SSL VPN, click the **Client Status** button to view the list of connected clients.