



FATPIPE NETWORKS

---

**SSL VPN**

Installation Guide

---



# Table of Contents

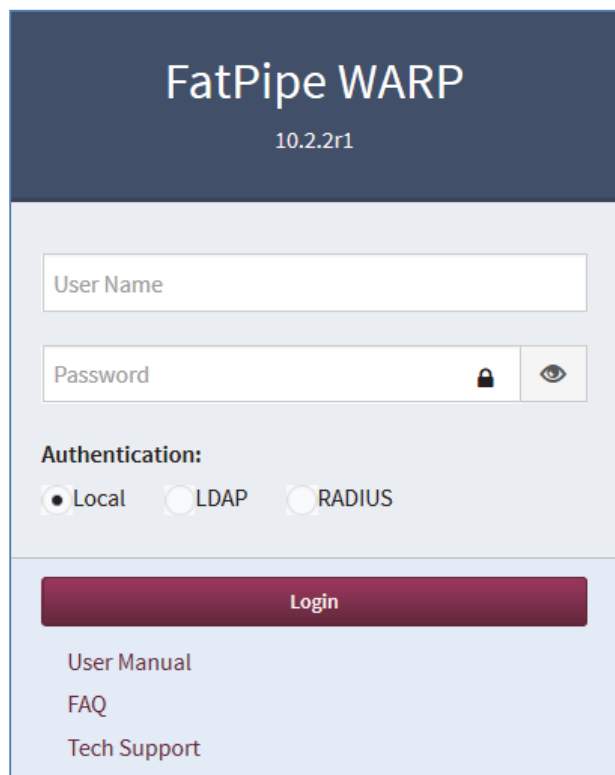
1. Overview
2. User Login
3. LAN Configuration
4. WAN Configuration
5. SSL VPN Configuration
6. Creating Server Profiles
7. Creating Client Profiles
8. Creating User Profiles
9. Downloading the OVPN File for Client
10. Viewing Connected Clients

## Overview

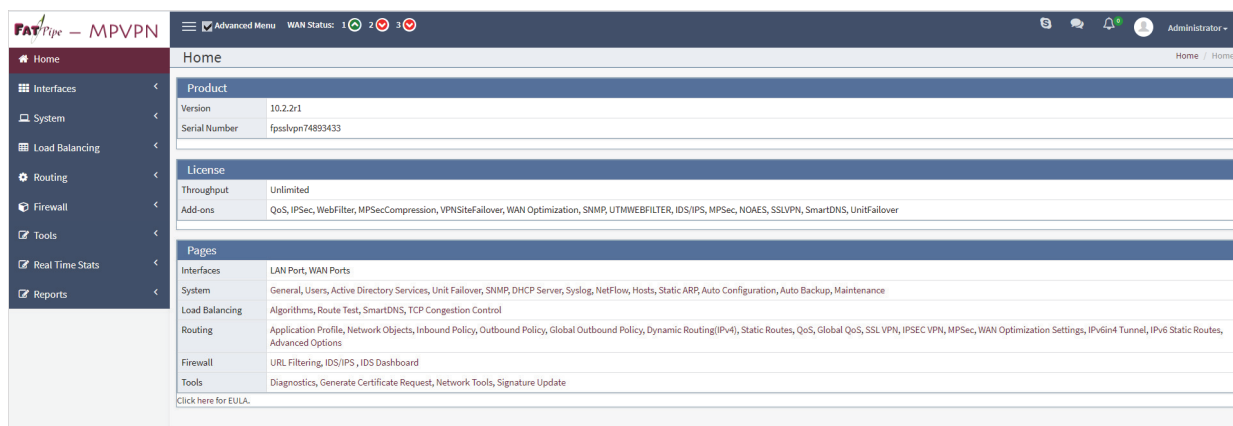
This installation guide outlines the steps to setup SSL VPN configuration to enable remote access for users.

## 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.



Product	
Version	10.2.2r1
Serial Number	fpslvpn74893433
License	
Throughput	Unlimited
Add-ons	QoS, IPSec, WebFilter, MPSECCompression, VPNSiteFailover, WAN Optimization, SNMP, UTMWEBFILTER, IDS/IPS, MPSEc, NOAES, SSLVPN, SmartDNS, UnitFailover
Pages	
Interfaces	LAN Port, WAN Ports
System	General, Users, Active Directory Services, Unit Failover, SNMP, DHCP Server, Syslog, NetFlow, Hosts, Static ARP, Auto Configuration, Auto Backup, Maintenance
Load Balancing	Algorithms, Route Test, SmartDNS, TCP Congestion Control
Routing	Application Profile, Network Objects, Inbound Policy, Outbound Policy, Global Outbound Policy, Dynamic Routing(IPv4), Static Routes, QoS, Global QoS, SSL VPN, IPSEC VPN, MPSEc, WAN Optimization Settings, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options
Firewall	URL Filtering, IDS/IPS, IDS Dashboard
Tools	Diagnostics, Generate Certificate Request, Network Tools, Signature Update
<a href="#">Click here for EULA.</a>	

## 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.

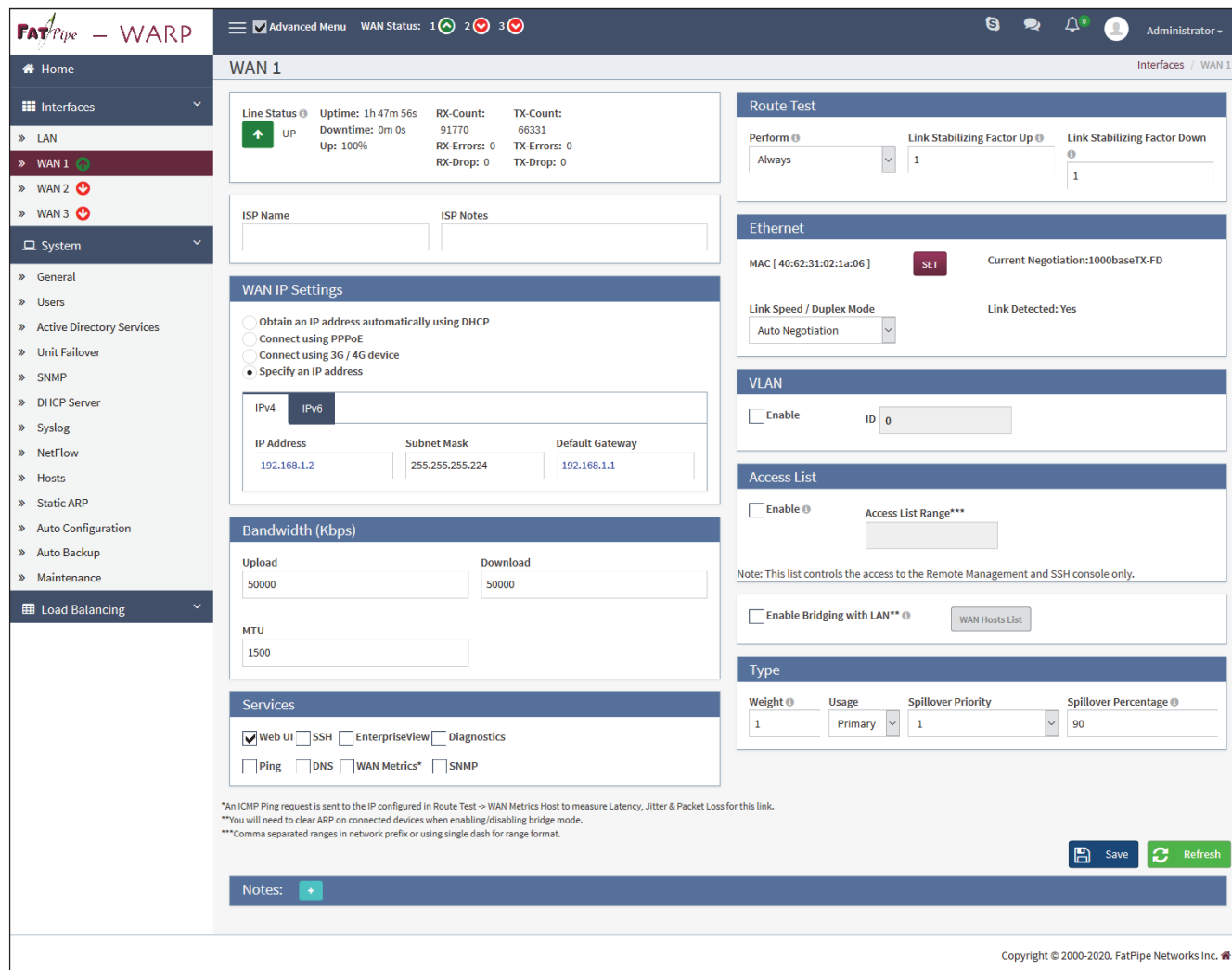
LAN Aliases				
IP Address	Subnet Mask	VLAN tag	DHCP Server IP	MTU
192.168.0.1	255.255.255.0	0		1500

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.



The screenshot displays the WAN 1 configuration page in the FatPipe WARP interface. The page is organized into several sections:

- Line Status:** Shows the interface is UP with an uptime of 1h 47m 56s. Statistics include RX-Count (91770), TX-Count (66331), RX-Errors (0), TX-Errors (0), RX-Drop (0), and TX-Drop (0).
- ISP Information:** Fields for ISP Name and ISP Notes.
- WAN IP Settings:** Offers three options: Obtain an IP address automatically using DHCP (selected), Connect using PPPoE, and Connect using 3G / 4G device. Below, there are input fields for IPv4 (IP Address: 192.168.1.2, Subnet Mask: 255.255.255.224, Default Gateway: 192.168.1.1) and IPv6.
- Bandwidth (Kbps):** Upload and Download rates are both set to 50000.
- MTU:** Set to 1500.
- Services:** Web UI is checked. Other services like SSH, EnterpriseView, Diagnostics, Ping, DNS, WAN Metrics\*, and SNMP are unchecked.
- Route Test:** Perform is set to Always, Link Stabilizing Factor Up and Down are both set to 1.
- Ethernet:** MAC address is 40:62:31:02:1a:06. Current Negotiation is 100baseTX-FD. Link Speed / Duplex Mode is Auto Negotiation. Link Detected is Yes.
- VLAN:** Enable checkbox is unchecked. ID is 0.
- Access List:** Enable checkbox is unchecked. Access List Range is empty.
- Type:** Weight is 1, Usage is Primary, Spillover Priority is 1, and Spillover Percentage is 90.

At the bottom right, there are 'Save' and 'Refresh' buttons. A copyright notice at the bottom right reads: Copyright © 2000-2020. FatPipe Networks Inc.

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.

The screenshot shows the 'SSL VPN' configuration page in the FatPipe WARP interface. The 'Enable SSL VPN' checkbox is checked. Below it, a table displays the configuration for a tunnel named 'demo1'. The table has columns for Name, Virtual Network, External IP, Port, TCP MSS, Authentication Type, Two factor Auth, and Client Status. The configuration for 'demo1' is: Virtual Network: 192.168.70.0/24, External IP: 192.168.2.2, Port: 11136, TCP MSS: 1372, Authentication Type: Local, Two factor Auth: Disabled. Below the table are buttons for 'Add', 'Edit', and 'Delete'. At the bottom right, there are 'Save' and 'Refresh' buttons. The interface also shows a sidebar with navigation options like 'Load Balancing', 'Routing', 'Application Profile', 'Network Objects', 'Inbound Policy', 'Outbound Policy', 'Global Outbound Policy', 'Dynamic Routing(IPv4)', 'Static Routes', 'QoS', 'Global QoS', 'SSL VPN', 'IPv6in4 Tunnel', 'IPv6 Static Routes', 'Advanced Options', 'Tools', 'Real Time Stats', and 'Reports'.

The screenshot shows the 'Add/Edit Configuration' dialog box. The 'Enable Tunnel' checkbox is checked. The 'Tunnel Name' field contains 'demo1'. The 'Server Profile' section includes fields for Mode (server), Virtual Network (192.168.70.0/24), Port (11136), Protocol (TCP), External IP (192.168.2.2), Authentication (SHA256), Encryption (AES-128-CBC), TCP MSS (1372), Log Level (1), and Radius server (None selected). The 'Type' is set to 'Subnets' with 'Local LAN Networks' (10.2.0.0/21, 172.30.0.0/24) and 'Type' (Local). The 'Two factor Auth' checkbox is checked. The 'Client Profile' section shows a table with columns for Profile Name, Local LAN Address, User Name, Download, and Show QR Image. Two client profiles are listed: 'Test1' and 'demotest'. Buttons for Add, Edit, and Delete are at the bottom. A note at the bottom states: 'Note: If you make any changes to the Server profile, Client profile files need to be downloaded and client VPNs need to be reconfigured. Please ensure the time on your Google Authenticator App is synced correctly for the Authenticator code to work properly.'

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 <b>Mode</b> 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 <b>Protocol</b> 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 <b>Authentication</b> drop-down. The available options are <b>SHA1</b> <b>SHA256</b> <b>SHA384</b> <b>SHA512</b>
Encryption	Select the encryption type from the Encryption drop-down. The available options are <b>BF-CBC</b> <b>AES-128-GCM</b> <b>AES-192-GCM</b> <b>AES-256-GCM</b> <b>AES-128-CBC</b> <b>AES-192-CBC</b> <b>AES-256-CBC</b>
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 <b>Type</b> . In the <b>Local LAN Networks</b> 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.

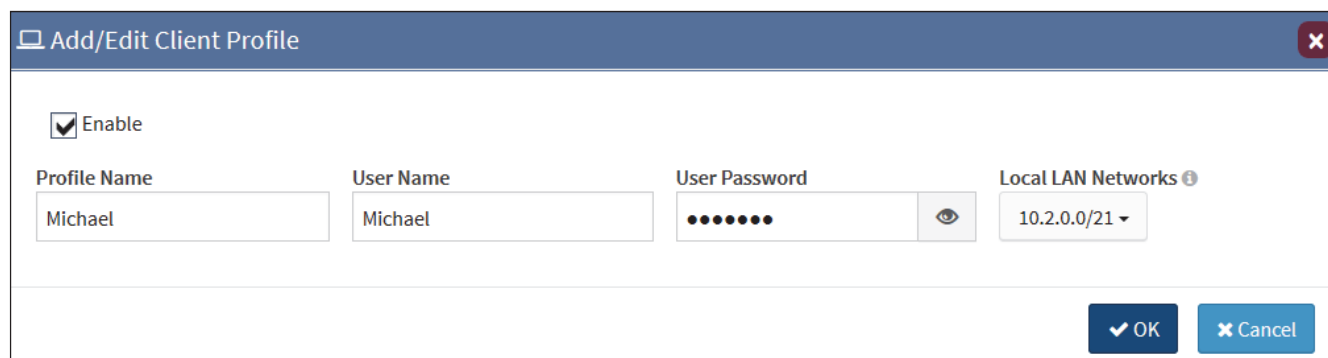
Select the **Type** as **Radius** if you have Radius configured. Select the ADS User from the **ADS User** drop-down.

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

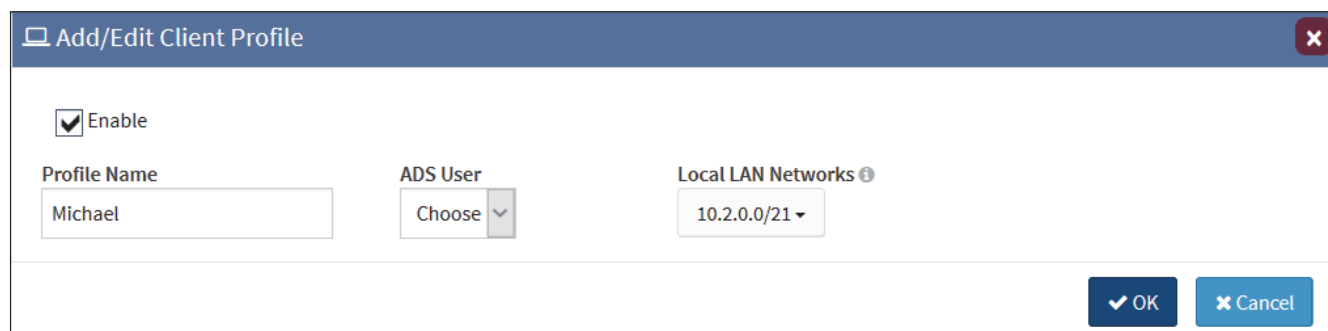
## Client Profiles

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:

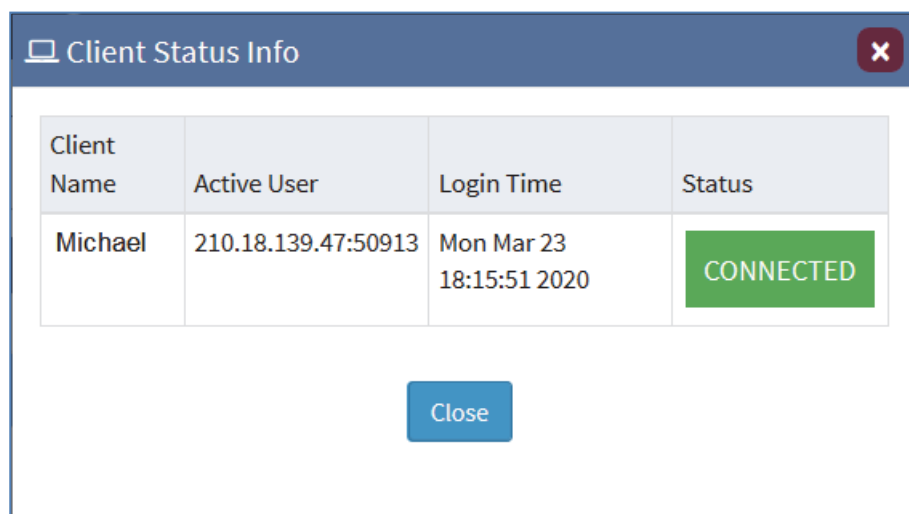
Click the **Download File** button to download the OVPN file for the client.

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.



The screenshot shows a window titled "Client Status Info" with a close button in the top right corner. Below the title bar is a table with the following data:

Client Name	Active User	Login Time	Status
Michael	210.18.139.47:50913	Mon Mar 23 18:15:51 2020	CONNECTED

Below the table is a "Close" button.