



# **DVP Series Quick Start Guide**

**R5.10**

# Contents

<b>1</b>	<b>SCOPE .....</b>	<b>3</b>
<b>2</b>	<b>GENERAL .....</b>	<b>3</b>
<b>3</b>	<b>VIDEOFLOW'S UDP VPN SOLUTION .....</b>	<b>4</b>
3.1	QUICKSTART DESKTOP DEMO SETUP .....	5
3.1.1	WAN setup .....	5
3.1.2	LAN setup .....	5
<b>4</b>	<b>SETTING UP THE SENTINEL AT THE CENTER .....</b>	<b>6</b>
4.1	SENTINEL PORT SETUP.....	6
4.1.1	First Time Connection.....	6
4.1.2	New Management IP Address Setup.....	7
4.1.3	Sentinel Data Ports Setup.....	9
4.2	UDP VPN SETUP.....	11
4.2.1	Adding UDP VPN Server .....	11
4.2.2	Adding Remote Clients to the Server.....	13
4.3	ADDING A STREAM .....	17
4.3.1	Add Stream.....	17
<b>5</b>	<b>SETTING UP THE PROTECTOR AT THE REMOTE SITE .....</b>	<b>21</b>
5.1	PROTECTOR PORT SETUP .....	21
5.1.1	First Time Connection.....	21
5.1.2	New Management IP Address Setup.....	22
5.1.3	Protector Data Ports Setup .....	23
5.1.4	DHCP setup option .....	26
5.2	UDP VPN CLIENT SETUP.....	26
5.2.1	Adding UDP VPN Client .....	27
5.3	ADDING THE STREAM .....	29
5.4	ADDING A STREAM .....	29
5.4.1	Add Stream.....	30
5.4.2	Verify Stream Configuration.....	34
<b>6</b>	<b>TROUBLESHOOTING .....</b>	<b>35</b>
6.1	CANNOT CONNECT TO DVP'S WEB-BASED GRAPHIC USER INTERFACE (GUI).....	35
6.2	MANAGEMENT PORT IP ADDRESS IS UNKNOWN .....	36
6.2.1	Connecting Via Data Port.....	36
6.2.2	Connecting Via Console.....	36
6.2.3	No Login Window .....	36
6.2.4	Check Connectivity .....	36
6.3	CANNOT SEE A STREAM IN THE PROTECTOR.....	38
6.4	CANNOT SEE A STREAM IN THE SENTINEL.....	38
6.5	DOWNLOADING THE USER'S GUIDE .....	38

## 1 Scope

This quick start guide provides fundamental information on how to configure a Protector, Sentinel or a Fortress to protect multicast transport stream over IP network like the Internet. This quick start guide is applicable for software version 3.10 and above.

## 2 General

VideoFlow's solution is comprised at a minimum with two elements Protector and Sentinel. The digital video protection (DVP) Protector is connected to the source (e.g., encoder) and acts as a transmitter of the protected data stream; the DVP Sentinel to the receiver (e.g., Integrated receiver decoder – IRD). The quick start guide provides an easy and systematic guide for setting up the Protector and the Sentinel. Both Protector and Sentinel require three steps setup:

1. Interfaces setup
2. UDP tunnel setup
3. Stream setup

A step by step procedure to connect a DVP Protector to a DVP Sentinel is provided. The procedure includes the following sections:

1. Sentinel setup
  - a. Interfaces
  - b. UDP Tunnel server
  - c. Stream setup
  - d. Setup verification
2. Protector setup
  - a. Interfaces
  - b. UDP Tunnel client
  - c. Stream setup
  - d. Setup verification



### NOTE

*Both the Sentinel and Protector can be configured as UDP VPN Server, UDP Tunnel Client, or both. The example given in this quick start guide is for setting up a contribution network. Therefore, the Sentinel is configured as UDP VPN Server and the Protector as UDP VPN Client.*

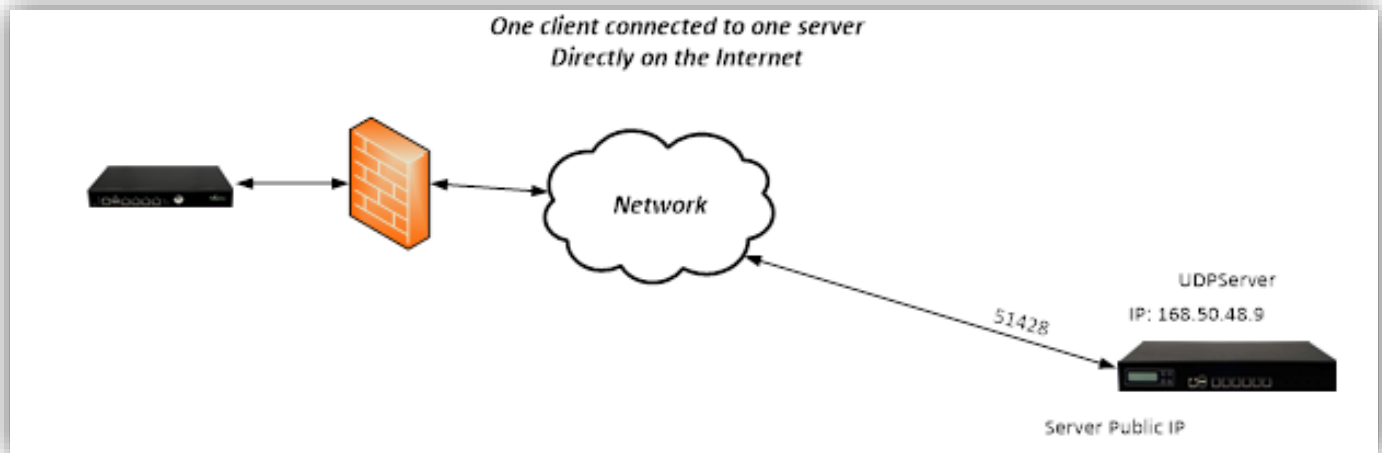
At the end of the process, the Protector and Sentinel will communicate and will protect the quality of a multicast stream. An example is used in each step of this guide as a reference.

A troubleshooting section is included as well to assist finding most likely miss configurations and/or networking issues.

### 3 VideoFlow's UDP VPN Solution

This section provides an introduction to VideoFlow's UDP VPN solution. The UDP VPN is used to connect between two DVP devices (e.g., connecting a Protector to a Sentinel) in a secure and simple manner.

The UDP VPN is based on a client-server architecture allowing a seamless traversal through firewalls and routers. The UDP VPN may require little IT support to configure and operate. The Architecture is composed of two elements; A UDP VPN server and UDP VPN client. The UDP VPN server requires a reachable static IP address which is used as an anchor for the UDP VPN clients wishing to establish a connection to the server. The UDP VPN clients can use either a static IP address or can use a DHCP configuration in case they are mobile. Each UDP VPN has a unique UDP/TCP port number assigned for it, and it may not be shared by other clients. The client-server model is independent of the function that each VideoFlow instance is configured to use (transmitter or receiver). In addition, it is important to remember that a number of clients can connect to a single server.



#### NOTE

*The UDP VPN server should be set in a location where it can be reachable. Its IP address shall be static.  
The UDP VPN client can be set anywhere.*

The contribution network architecture will normally be multipoint-to-point were many Protectors are connecting to a Sentinel in the center. Therefore the UDP tunnel server will be set in the Sentinel; the UDP VPN client in the Protector.

The distribution network architecture will normally be point-to-multipoint were one Protector in the center is connecting too many Sentinels. Therefore the UDP VPN server will be set in the Protector; the UDP VPN client in the Sentinel.

### 3.1 Quickstart desktop demo setup

For a simple benchtop demo, we propose to use a low-cost Wi-Fi Router as a network simulation.

#### 3.1.1 WAN setup

The Wi-Fi router WAN port will simulate the public internet. Throughout the document we assume that the WAN is configured to the following:

WAN is set to 'Static IP' mode

Static IP: 168.50.48.241

MASK: 255.255.255.0

GW: 168.50.48.1

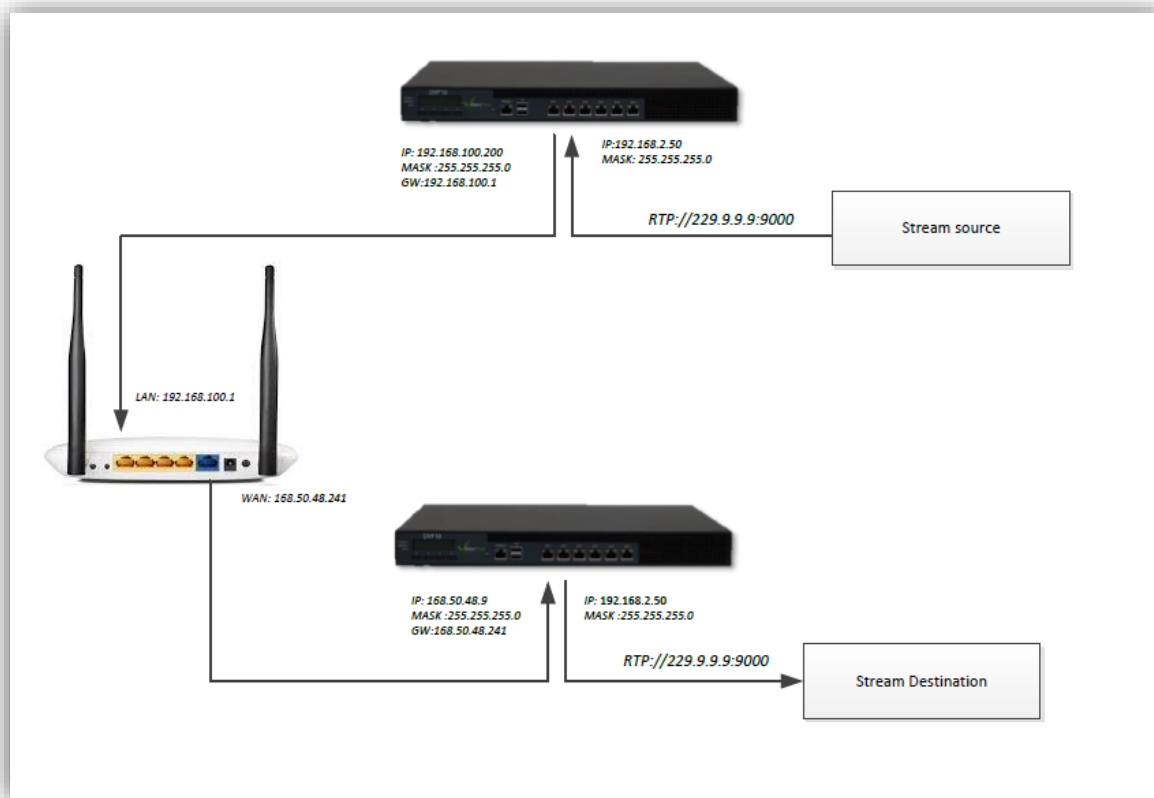
#### 3.1.2 LAN setup

The LAN is configuration:

LAN network: 192.168.100.1/24

DHCP is optional (refer to section 5.1.4 for DHCP setup)

See diagram:



## 4 Setting Up the Sentinel at the Center

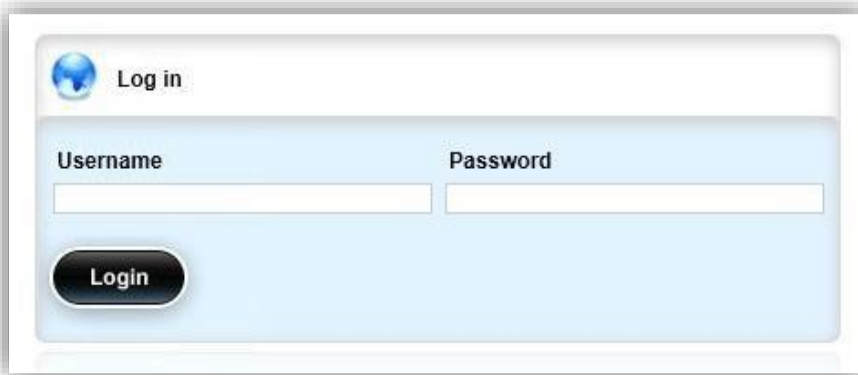
This section will describe the procedure required for configuring the Sentinel at the center. The Sentinel will act as the VPN Server to the Protectors connecting to it from the remote.

### 4.1 Sentinel Port Setup

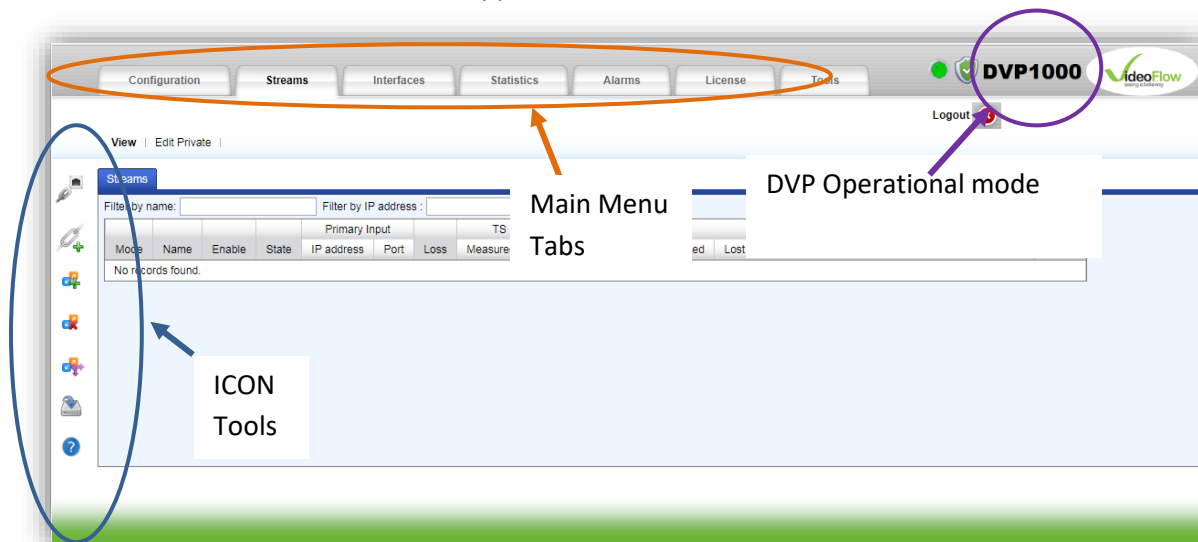
The default DVP factory management IP address is 10.0.0.200.

#### 4.1.1 First Time Connection

1. Connect an Ethernet cable between a computer running the browser program and the port labeled Mgmt in the DVP's front panel.
2. Change the local LAN settings in your PC to manual IP address
3. Select IP address from the same subnet (e.g., 10.0.0.120, Subnet Mask: 255.255.255.0)
4. Browse the Sentinel's management IP address. A login window similar to the below will appear:



5. Type the default Username: oper
6. Type the default Password: oper
7. A window similar to the below should appear:

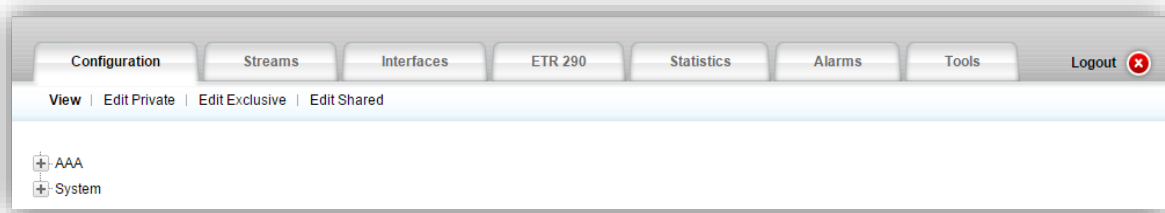


#### NOTE

*If you prefer not to leave the Mgmt IP unchanged, Go to Section 4.1.3*

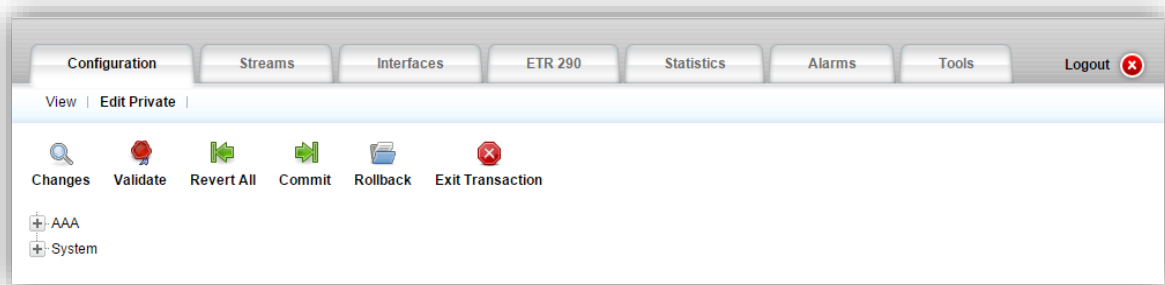
8. Click on the Configuration tab

9. A new page will appear:

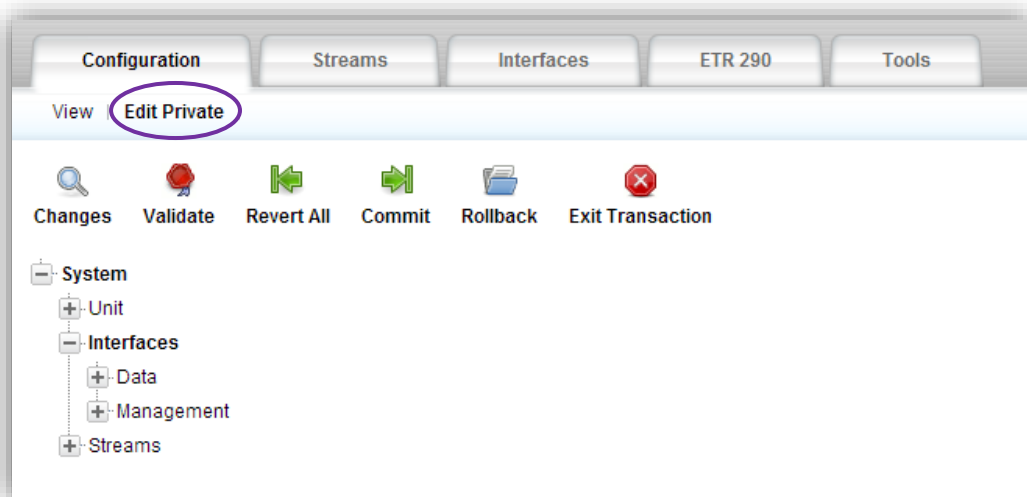


#### 4.1.2 New Management IP Address Setup

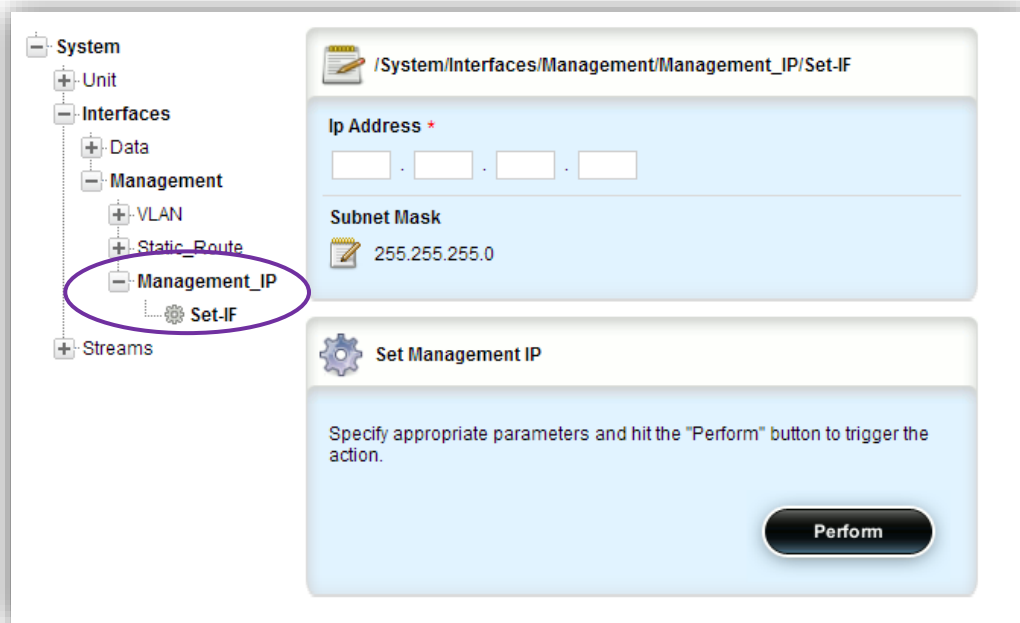
1. Click on the **Edit Private** mode



2. Clicking on the '+' expand a menu tree item. Click on System→Interfaces→Management



3. Click on Management\_IP→Set-IF to set up the management interface's IP address




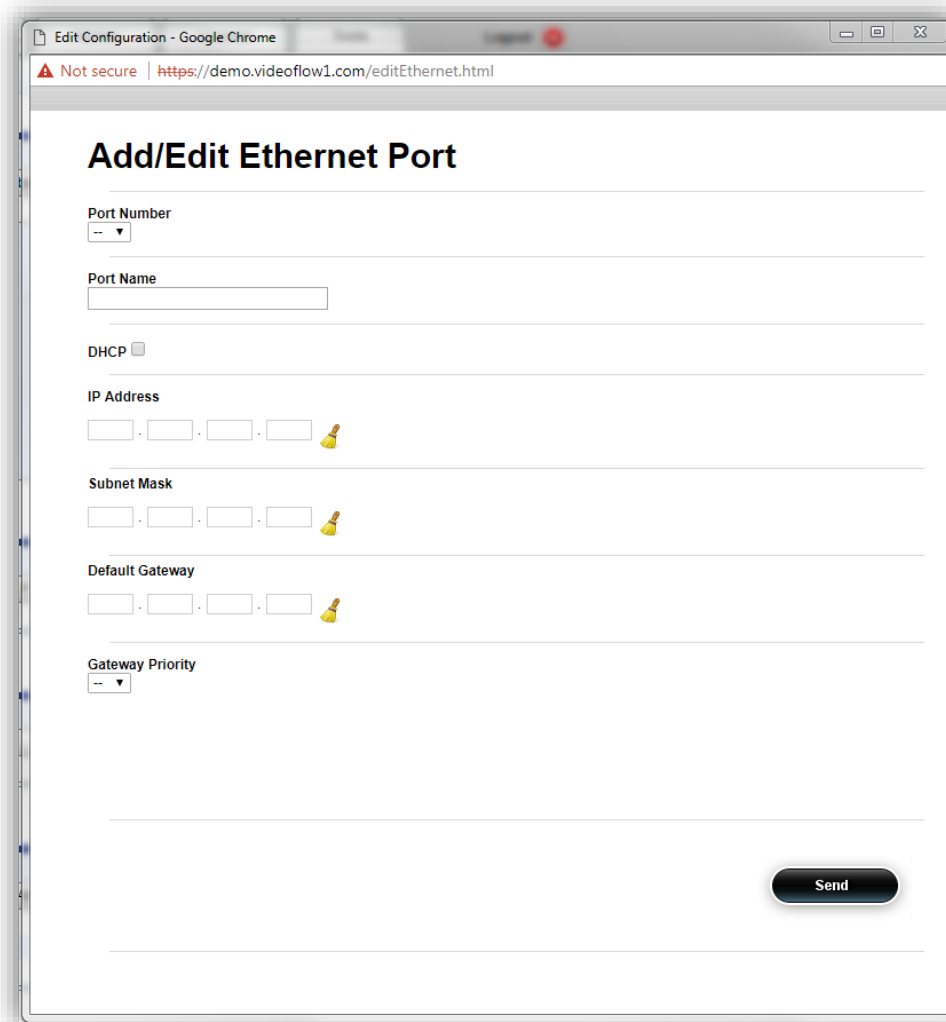
4. Type a new management IP address if required
5. Modify the management Subnet Mask if required
6. Click on the Perform button to apply the changes
7. The PC and the DVP will disconnect in the case of management IP and/or subnet mask change. Follow the below procedure to reconnect:
  - a. Close the browser window
  - b. Change the IP address in the PC to be in the same subnet as the new management IP address
  - c. Open the browser and browse the new management IP address
8. Once the connection with the Sentinel is resumed, continue to the next section



### 4.1.3 Sentinel Data Ports Setup

This section describes how to add and assign IP addresses to the DVP interfaces. The ports are used for connecting the DVP to either the local network (LAN) or to the external network (WAN).

1. Press on the  icon to bring the IP configuration



Edit Configuration - Google Chrome

Not secure | <https://demo.videoflow1.com/editEthernet.html>

## Add/Edit Ethernet Port

Port Number  
-- ▾

Port Name

DHCP ☐

IP Address  
 .  .  .  🔔

Subnet Mask  
 .  .  .  🔔

Default Gateway  
 .  .  .  🔔

Gateway Priority  
-- ▾

2. Select the interface Id number from the pull-down list.  
In this guide's network example the external network (the public Internet in this example) is connected to Port1 and the local network is connected to Port 2.
3. Port 1 (to external network) configuration (In this example):
  - a. Check the 'Enable' checkbox to enable the Port
  - b. Set the Name field to 'Port\_1'  
configure IP Address: 168.50.48.9  
configure Subnet Mask: 255.255.255.0
  - c. Configure Default Gateway: 168.50.48.241

Edit Configuration - Google Chrome

Not secure | <https://demo.videoflow1.com/editEthernet.html>

## Add/Edit Ethernet Port

Port Number  
1 ▼

Port Name  
Port\_1

DHCP ☐

IP Address  
192 . 50 . 48 . 9 🛠

Subnet Mask  
255 . 255 . 255 . 0 🛠

Default Gateway  
192 . 50 . 48 . 241 🛠

Gateway Priority  
▼

Send

To complete the configuration click on the 'Send' button to apply the configuration changes.

4. Repeat the same steps to configure Port 2 (to local network) configuration:
  - a. IP Address: 192.168.2.50
  - b. Subnet Mask: 255.255.255.0
  - c. Note that there is no need to configure default gateway to ports connecting to the local network

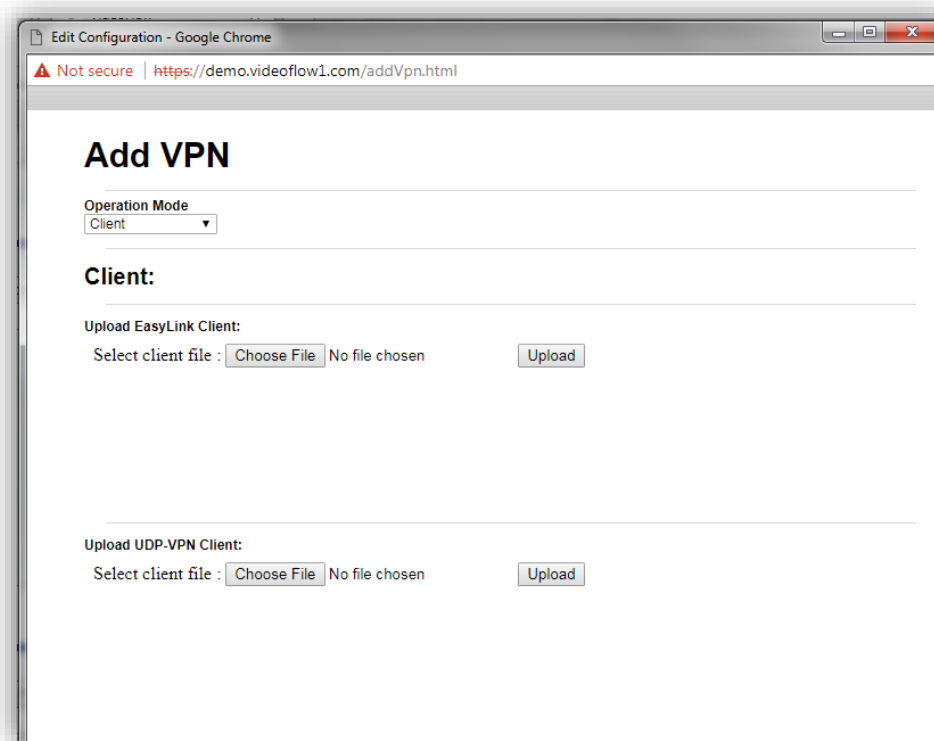
## 4.2 UDP VPN Setup

The UDP Tunnel setup is comprised of the following steps:

1. Adding a UDP VPN Server
2. Adding UDP VPN remote clients
3. Generating UDP VPN remote clients configuration files
4. Downloading remote clients configuration files

### 4.2.1 Adding UDP VPN Server

1. Click on the  ICON to open Add VPN window:



2. Using the Operation mode pull-down menu – select UDP-VPN Server



3. The Window will change to UDP-VPN Server configuration options:


Edit Configuration - Google Chrome  
Not secure | https://demo.videoflow1.com/addVpn.html

## Add VPN

Operation Mode  
UDP-VPN Server ▼



**UDP-VPN Server:**

Name

IP Address  
 .  .  .  

URL

Interface  
-- ▼

Port	Name	Net	Encryption
No records found.			

**Send**

4. Enter a unique name – in this Example, it will be named 'MainServer'
5. Enter the IP address of the interface connected to the external network (the Internet in our example). Note that this IP address will be used by the UDP VPN Client to connect to its server in this example it will be '168.50.48.9'
6. Select the physical interface connected to the external network, in this example, it is 'Port 1'

## Add VPN

Operation Mode

UDP-VPN Server ▼

### UDP-VPN Server:

Name

MainServer

IP Address

168 . 50 . 48 . 9 

URL

Interface


1 ▼



Port	Name	Net	Encryption
No records found.			

Send

### 4.2.2 Adding Remote Clients to the Server

1. Click on the “” ICON, a new Add Client window will pop up:

## Add VPN

Operation Mode  
UDP-VPN Server

### UDP-VPN Server

Name  
MainServer

IP Address  
168 . 50 . 48

URL

Interface  
1

Port Name  
No records found.

Send

**Add Client**

Port Number

Name

Net

Encryption  
none

Cancel OK

2. Enter a unique UDP port number (51428 in this example). Note that the port number is unique, i.e., no two remote clients with the same port number are allowed. The port number range is 20000 – 60000

**Add Client**

Port Number  
51428

Name  
UDP\_server\_1

Net  
51 . 42 . 8 . 0

Encryption  
AES-256

Cancel OK

3. Enter a unique name for the remote client in the **Name** field: in this example, we will call it 'UDP\_server\_1'
4. Enter a virtual IP address for the VPN in the **Net** fields. Note that this virtual IP address will be used to ensure connectivity hence do not enter any IP address already used in the device. in this example, we will use: 51.42.8.0 as the subnet
5. Select the type of **Encryption** (none, AES-128 or AES-256)

6. Click on OK to apply
7. Click Cancel or close the Window to exit
8. A new table entry will appear:

## Add VPN

Operation Mode  
UDP-VPN Server ▾


**UDP-VPN Server:**

Name  
MainServer

IP Address  
168 . 50 . 48 . 9 📌

URL

Interface  
1 ▾

 📌

Port	Name	Net	Encryption	
51428	UDP_server_1	51.42.8.0	AES-256	✖

Send

9. Press the 'Send' button to commit the new configuration

## Add VPN

Operation Mode

UDP-VPN Server ▾

UDP-VPN Se

Name

MainServer

IP Address

168 . 50 . 48

URL

Interface

1 ▾



Port	Name	Net	Encryption	
51428	UDP_server_1	51.42.8.0	AES-256	✗



**Note: Commit Succeeded**

The configuration has been committed.

OK

Send

10. A 'Commit Succeeded' message should appear to signal all is OK
11. Press OK, will download a configuration file to your PC.
12. Close the 'Add VPN' window to continue



### NOTE

*The remote client file will be uploaded to the remote Client. Once the file is uploaded and the remote client is configured it will always attempt connecting to the UDP VPN server upon startup*




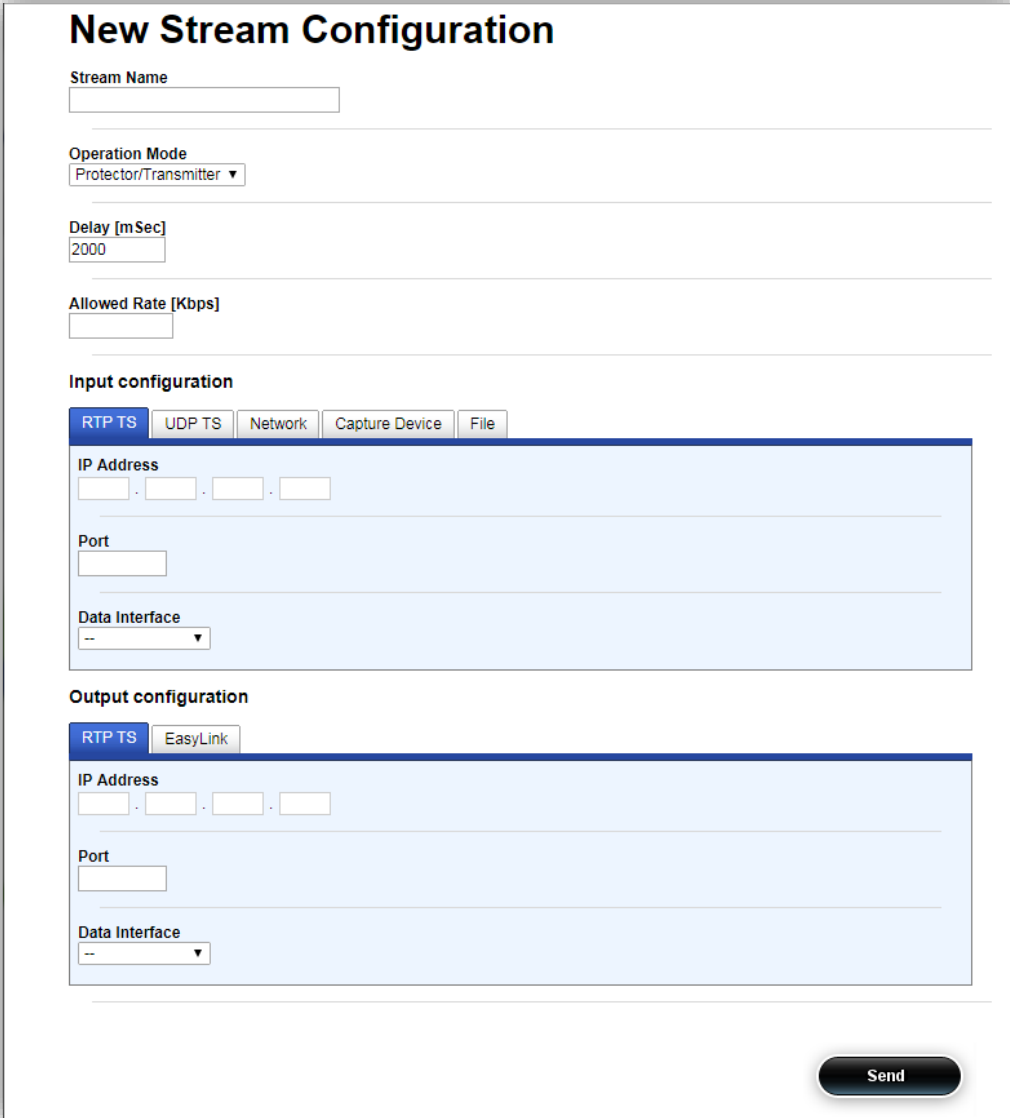
## 4.3 Adding a Stream

At this stage, the DVP unit setup and VPN connectivity are completed and we need to add streams to our setup. Adding a stream is comprised of three steps:

1. Adding stream
2. Setup the stream's input interface and properties
3. Setup the stream's output interface and properties

### 4.3.1 Add Stream

1. Click on the  ICON, a 'New Stream Configuration' Window will appear:

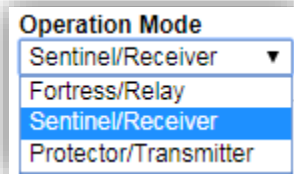


The 'New Stream Configuration' window is a form for setting up a new stream. It contains the following fields and sections:

- Stream Name:** A text input field.
- Operation Mode:** A dropdown menu with 'Protector/Transmitter' selected.
- Delay [mSec]:** A text input field with '2000' entered.
- Allowed Rate [Kbps]:** A text input field.
- Input configuration:** A section with tabs for 'RTP TS', 'UDP TS', 'Network', 'Capture Device', and 'File'. The 'RTP TS' tab is selected. It contains:
  - IP Address:** Four text input fields for IP address components.
  - Port:** A text input field.
  - Data Interface:** A dropdown menu with '--' selected.
- Output configuration:** A section with tabs for 'RTP TS' and 'EasyLink'. The 'RTP TS' tab is selected. It contains:
  - IP Address:** Four text input fields for IP address components.
  - Port:** A text input field.
  - Data Interface:** A dropdown menu with '--' selected.
- Send:** A button at the bottom right.

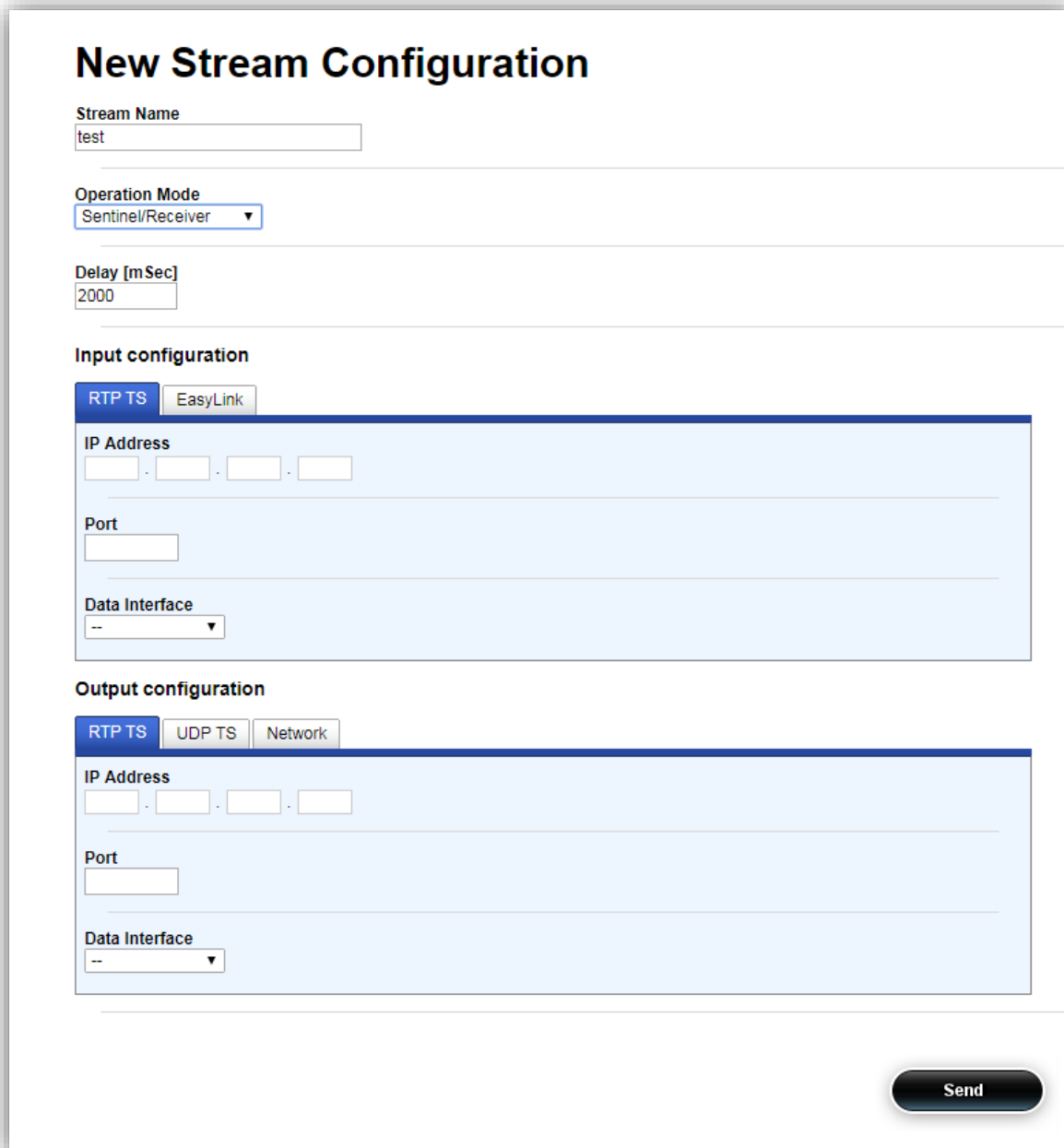
2. Set a name for the stream, in this case, 'test'.

3. Select the stream function Protector/Sentinel/Fortress from a drop-down menu. In our example **Sentinel**



A screenshot of a dropdown menu titled "Operation Mode". The menu is open, showing four options: "Sentinel/Receiver" (selected and highlighted in blue), "Fortress/Relay", "Sentinel/Receiver", and "Protector/Transmitter".

4. The Window will change its appearance to;



A screenshot of the "New Stream Configuration" window. The window has a title bar and a main content area. The title "New Stream Configuration" is in large, bold, black font. Below the title, there are several input fields and a dropdown menu. The "Stream Name" field contains the text "test". The "Operation Mode" dropdown menu is set to "Sentinel/Receiver". The "Delay [mSec]" field contains the value "2000". Below these fields, there are two sections: "Input configuration" and "Output configuration". The "Input configuration" section has a tabbed interface with "RTP TS" and "EasyLink" tabs. The "RTP TS" tab is active, showing fields for "IP Address" (four empty boxes separated by dots), "Port" (one empty box), and "Data Interface" (a dropdown menu with "--" selected). The "Output configuration" section also has a tabbed interface with "RTP TS", "UDP TS", and "Network" tabs. The "RTP TS" tab is active, showing fields for "IP Address" (four empty boxes separated by dots), "Port" (one empty box), and "Data Interface" (a dropdown menu with "--" selected). At the bottom right of the window, there is a "Send" button.

5. Configure the stream's **Input configuration** parameters:
- Select the Data interface from the Input Interface Name drop-down menu (**UDP\_server\_1** in our example)
  - Configure Listen Ip according to the stream's destination IP address (229.9.9.9 in this example)
  - Configure Listen Port according to the stream's UDP port (9000 in this example)

6. Configure the stream's **Output configuration** parameters:
  - a. Configure Listen Ip according to the stream's destination IP address (229.9.9.9 in this example)
  - b. Configure Listen Port according to the stream's UDP port (9000 in this example)
  - c. Select the Data interface from the Name drop-down menu (**Port\_2** in our example)

## New Stream Configuration

Stream Name

test

Operation Mode

Sentinel/Receiver

Delay [mSec]

2000

Input configuration

RTP TS

EasyLink

IP Address

229 . 9 . 9 . 9

Port

9000

Data Interface

UDP\_server\_1

Output configuration

RTP TS

UDP TS

Network

IP Address

229 . 9 . 9 . 9

Port

9000

Data Interface

Port\_2

Send

- d. Press Send when done

7. Wait for the 'Commit Succeeded' window to appear:

## New Stream Configuration

Stream Name

test

Operation Mode

Sentinel/Receiver

Delay [mSec]

2000

Input configuration

RTP TS

EasyLin

IP Address

229 . 9 . 9 . 9

Port

9000

Data Interface

UDP\_server\_1

Output configuration

RTP TS

UDP TS

Network

IP Address

229 . 9 . 9 . 9

Port

9000

Data Interface

Port\_2



**Note: Commit Succeeded**

The configuration has been committed.

OK

Send

8. Close the window
9. A new stream should appear:

Configuration Streams Interfaces Statistics Alarms License Tools Logout

View | Edit Private | Edit Exclusive | Edit Shared

Streams

Filter by name: Filter by IP address:

Mode	Name	Enable	State	Primary Input		Loss	TS Rate		Packet rate	Protection statistics				Active Input	Action
				IP address	Port		Measured	PCR		Processed	Lost Detected	Requested	Unrecovered		
+	test	✓	✗	229.9.9.9	9000	0	0	0	0	0	0	0	0	All	Select

Total streams bitrate is 0 Mbit/s out of 1600 Mbit/s.

## 5 Setting Up the Protector at the Remote Site

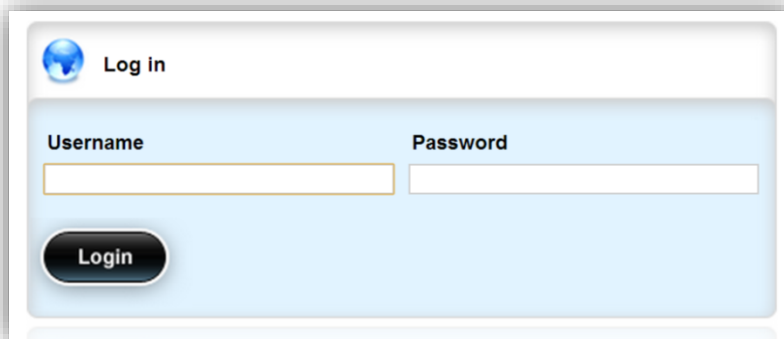
This section will describe the procedure required for configuring the Protector at the remote site. The Protector will act as the VPN Client of the Sentinel connecting to it from remote.

### 5.1 Protector Port Setup

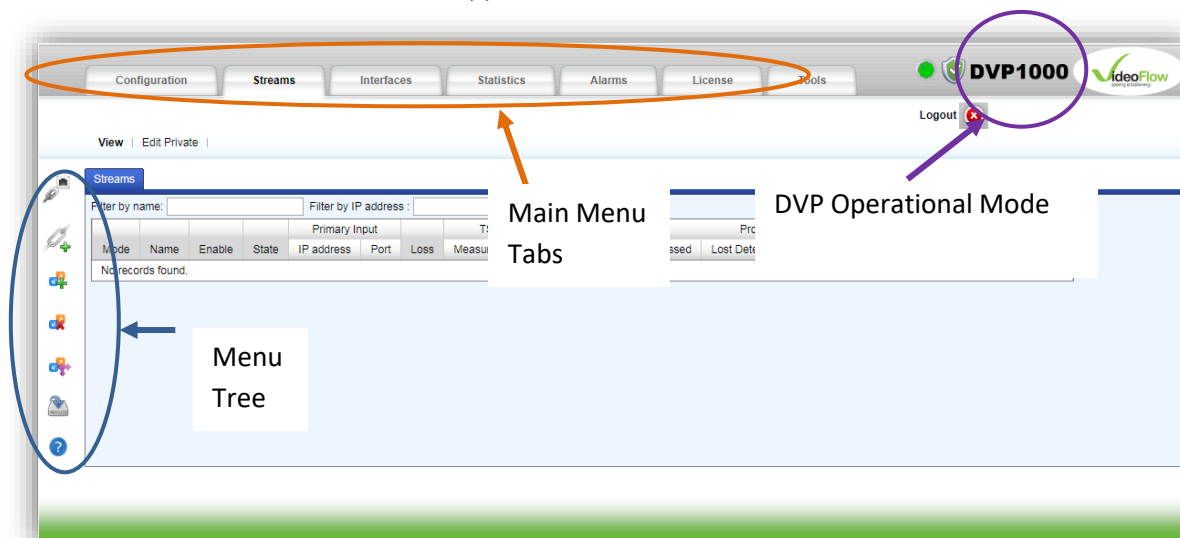
The default DVP factory management IP address is 10.0.0.200.

#### 5.1.1 First Time Connection

1. Connect an Ethernet cable between a computer running a browser program to the port labeled Mgmt in the DVP's front panel
2. Change the local LAN settings in your PC to manual IP address
3. Select IP address that is in the same subnet (e.g., 10.0.0.140, Subnet Mask: 255.255.255.0)
4. Browse the Protector's management IP address. A login window similar to the below will appear:



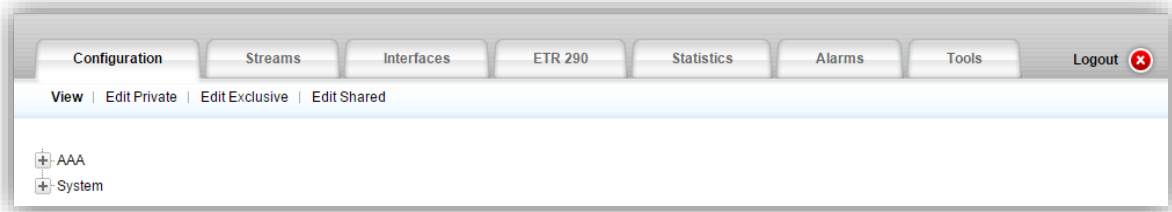
5. Type the default Username: oper
6. Type the default Password: oper
7. A window similar to the below should appear:



#### NOTE

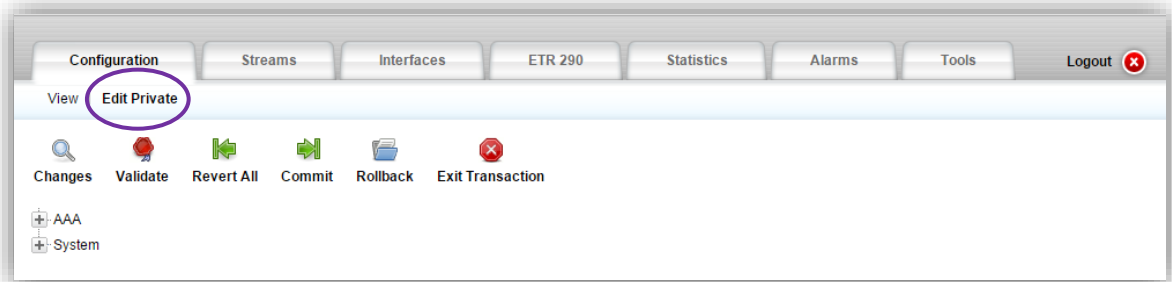
*If you prefer not to leave the Mgmt IP unchanged, Go to Section 5.1.3*

- Click on the Configuration tab
- A new page will appear:

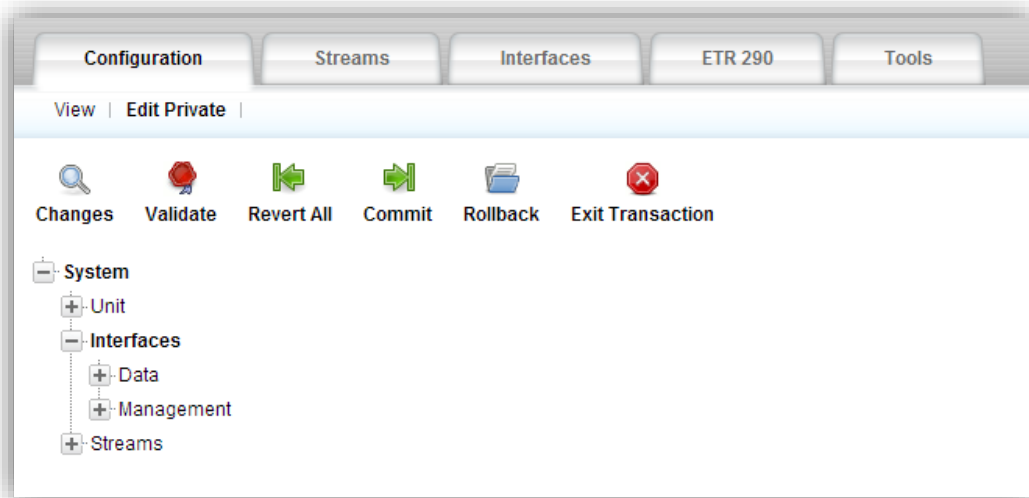


### 5.1.2 New Management IP Address Setup

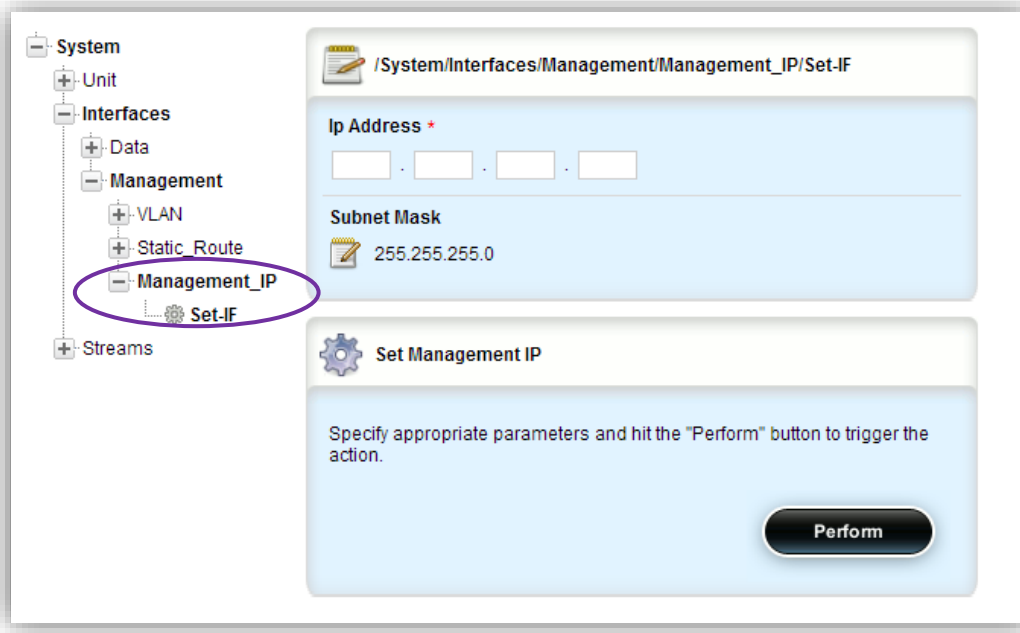
- Click on the Edit Private mode.



- Click on the '+' to expand the menu tree. Expand the menu tree further by clicking on Management




3. Click on Management\_IP→Set-IF to set up the management interface's IP address.



4. Type a new management IP address if required.
5. Modify the management Subnet Mask if required.
6. Click on Perform to apply the changes.
7. The PC and the DVP will disconnect in the case of management IP and/or subnet mask change. Follow the below procedure to reconnect:
  - a. Close the browser window.
  - b. Change the IP in the PC to the same subnet as the new management IP address.
  - c. Open the browser and browse the new management IP address.
8. Once the connection with the Protector is resumed, continue to the next section.

### 5.1.3 Protector Data Ports Setup

This section describes how to Add and assign IP addresses to the DVP interfaces. The ports are used for connecting the DVP to either the local network (LAN) or to the external network (WAN).

1. Press on the  icon to bring the IP configuration

Edit Configuration - Google Chrome

Not secure | <https://demo.videoflow1.com/editEthernet.html>

## Add/Edit Ethernet Port

Port Number  
-- ▾

Port Name

DHCP ☐

IP Address  
 .  .  .  🔔

Subnet Mask  
 .  .  .  🔔

Default Gateway  
 .  .  .  🔔

Gateway Priority  
-- ▾

Send

Select the interface Id number from the pull-down list.

In this guide's network example the external network (the public Internet in this example) is connected to Port1 and the local network is connected to Port 2.

2. Port 1 (to external network) configuration (In this example: ):
  - Check the 'Enable' checkbox to enable the Port
  - Set the Name field to 'Port\_1'
  - configure IP Address: 192.168.100.200
  - configure Subnet Mask: 255.255.255.0
  - Configure Default Gateway: 192.168.100.1



## Add/Edit Ethernet Port

Port Number


1 ▼

Port Name

Port\_1

DHCP ☐


IP Address

192 . 168 . 100 . 200 

Subnet Mask

255 . 255 . 255 . 0 

Default Gateway

192 . 168 . 100 . 1 

Gateway Priority

▼

Send

To complete the configuration click on the 'Send' button to apply the configuration changes

3. Repeat the same steps to configure Port 2 (to local network) configuration:

IP Address: 192.168.2.50

Subnet Mask: 255.255.255.0

Note that there is no need to configure default gateway to ports connecting to the local network

#### 5.1.4 DHCP setup option

In the case of using DHCP, just follow the same direction as in previous sections (any IP may be in use for temporary status).

To set DHCP mode – just check the DHCP check box

### Add/Edit Ethernet Port

Port Number

1 ▼

Port Name

Port\_1

DHCP

☒

IP Address

192 . 168 . 100 . 200 🔔

Subnet Mask

255 . 255 . 255 . 0 🔔

Default Gateway

192 . 168 . 100 . 1 🔔

Gateway Priority

▼

Send

Press **Send** to apply.


Close the window when done.

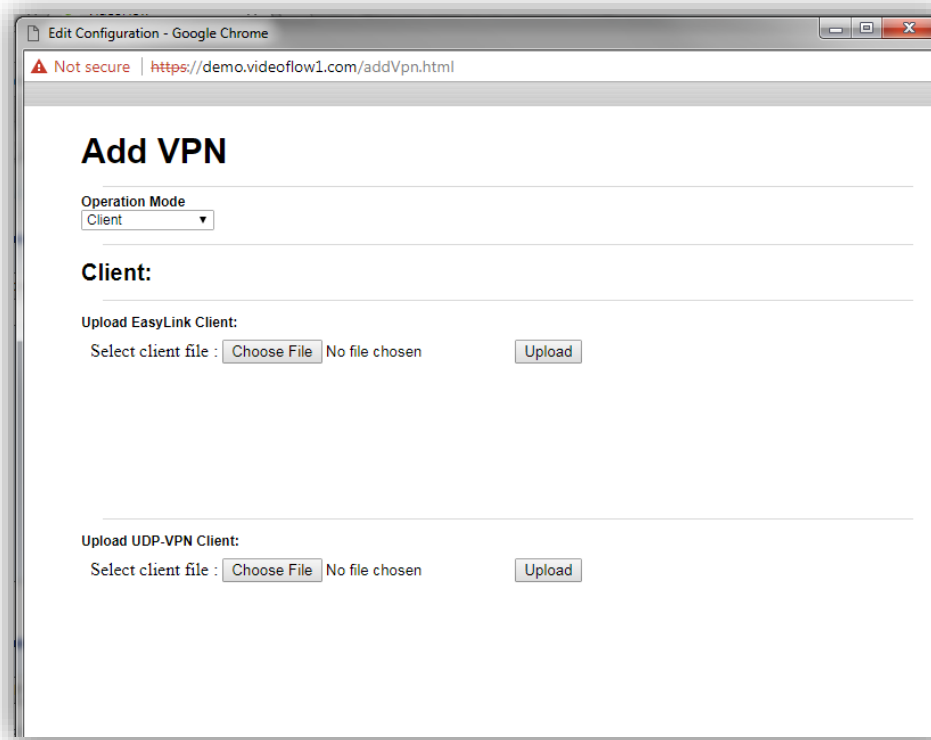
## 5.2 UDP VPN Client Setup

The UDP VPN Client setup is comprised of the following steps:

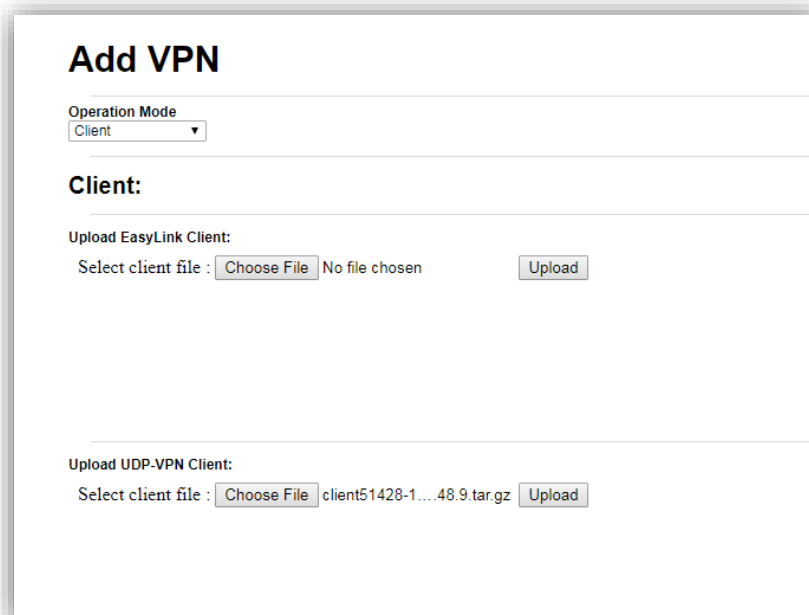
1. Adding a UDP VPN Client
2. Uploading the file generated by the UDP VPN Server in the Sentinel.

## 5.2.1 Adding UDP VPN Client

1. Click on the  ICON to open Add VPN window:



2. Turn to the '**Upload UDP-VPN Client**' and press the Choose File button
3. Locate the file 'Client51428-168.50.48.9.tar'



4. Now press the **Upload** button.
5. The window will change to :

## Add VPN

Operation Mode  
Client ▼

---

**Client:**

Upload EasyLink Client:

Select client file :  No file chosen

---

Upload UDP-VPN Client:

UDP VPN file has been uploaded!!

VPN Name:

Bind To Interface:  ▼

To update the new database [click here](#)

6. Set the VPN name to 'MainTunnel'
7. Set the 'Bind to Interface to '1'

## Add VPN

Operation Mode  
Client ▼

---

**Client:**

Upload EasyLink Client:

Select client file :  No file chosen

---

Upload UDP-VPN Client:

UDP VPN file has been uploaded!!

VPN Name:

Bind To Interface:  ▼

To update the new database [click here](#)

8. Press '[Click\\_here](#)'
9. The Window should show:

# Add VPN

---

Operation Mode  
Client ▼

---

## Client:

---

Upload EasyLink Client:

Select client file :  No file chosen

---

Upload UDP-VPN Client:

File was successfully activated!!

Close the window.


## 5.3 Adding the Stream

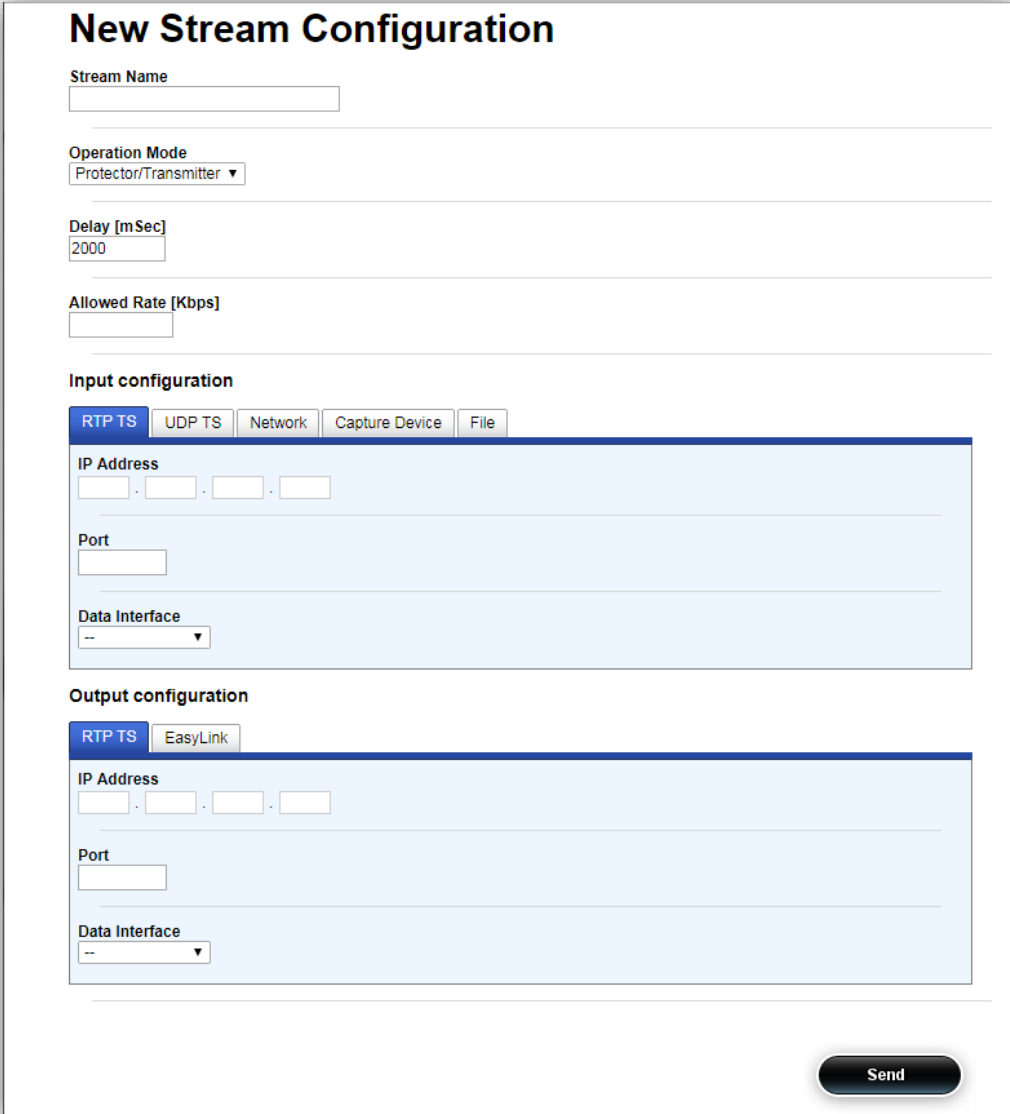
### 5.4 Adding a Stream

At this stage, the DVP unit setup and VPN connectivity are completed and we need to add streams to our setup. Adding a stream is comprised of three steps:

1. Adding stream
2. Setup the stream's input interface and properties
3. Setup the stream's output interface and properties

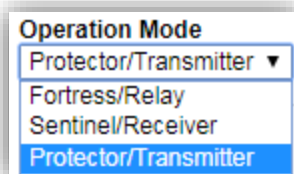
### 5.4.1 Add Stream

1. Click on the  ICON, a 'New Stream Configuration' Window will appear:



The 'New Stream Configuration' window is a form for setting up a new stream. It includes fields for 'Stream Name', 'Operation Mode' (a dropdown menu), 'Delay [mSec]' (a text box with '2000'), and 'Allowed Rate [Kbps]' (a text box). Below these are two sections: 'Input configuration' and 'Output configuration'. Each section has tabs for 'RTP TS', 'UDP TS', 'Network', 'Capture Device', and 'File'. The 'Input configuration' section has fields for 'IP Address', 'Port', and 'Data Interface'. The 'Output configuration' section also has fields for 'IP Address', 'Port', and 'Data Interface'. A 'Send' button is located at the bottom right of the window.

2. Set a name for the stream, in this case, 'test'.
3. Select the stream function Protector/Sentinel/Fortress from a drop-down menu. In our example **Protector**



4. The Window will change its appearance to;

## New Stream Configuration

Stream Name

test

Operation Mode

Protector/Transmitter ▼

Delay [mSec]

2000

Allowed Rate [Kbps]

### Input configuration

RTP TS

UDP TS

Network

Capture Device

File

IP Address

. . .

Port

Data Interface

-- ▼

### Output configuration

RTP TS

EasyLink

IP Address

. . .

Port

Data Interface

-- ▼

Send

5. Configure the stream's **Input configuration** parameters:
  - a. Configure Listen Ip according to the stream's destination IP address (229.9.9.9 in this example)
  - b. Configure Listen Port according to the stream's UDP port (9000 in this example)
  - c. Select the Data interface from the Input Interface Name drop-down menu (**Port\_2** in our example)
6. Configure the stream's **Output configuration** parameters:
  - a. Configure Listen Ip according to the stream's destination IP address (229.9.9.9 in this example)
  - b. Configure Listen Port according to the stream's UDP port (9000 in this example)
  - c. Select the Data interface from the Name drop-down menu (**MainTunnel** in our example)

# New Stream Configuration

**Stream Name**

**Operation Mode**

**Delay [mSec]**

**Allowed Rate [Kbps]**

**Input configuration**

**IP Address**  
 .  .  .

**Port**

**Data Interface**

**Output configuration**

**IP Address**  
 .  .  .

**Port**

**Data Interface**

d. Press the **Send** button when done

10. Wait for the 'Commit Succeeded' window to appear:



# New Stream Configuration

Stream Name

test

Operation Mode

Protector/Transmitter

Delay [mSec]

2000

Allowed Rate [Kbps]



**Note: Commit Succeeded**

The configuration has been committed.

OK

## Input configuration

RTP TS

UDP TS

Network

Capture Device

File

IP Address

229 . 9 . 9 . 9

Port

9000

Data Interface

Port\_2

## Output configuration

RTP TS

EasyLink

IP Address

229 . 9 . 9 . 9

Port

9000

Data Interface

MainTunnel

Send

11. Close the window

12. A new stream should appear:

Configuration Streams Interfaces Easy Link Easy Connect ETR 290 Statistics Alarms License Tools

View | Edit Private |

Streams

Filter by name: Filter by IP address:

Mode	Name	Enable	State	Primary Input		Loss	TS Rate		Packet rate	Protection statistics				Active Input	Action
				IP address	Port		Measured	PCR		Processed	Lost Detected	Requested	Unrecovered		
test	test	<input checked="" type="checkbox"/>		229.9.9.9	9000	0	2989952	3000000	284	0	0	0	0	All	Select

Total streams bitrate is 0 Mbit/s out of 1600 Mbit/s.

## 5.4.2 Verify Stream Configuration

- Click on the Streams Tab from the Main Menu:

Configuration Streams Interfaces Easy Link Easy Connect ETR 290 Statistics Alarms License Tools

View | Edit Private |

Streams

Filter by name: Filter by IP address:

Mode	Name	Enable	State	Primary Input		Loss	TS Rate		Packet rate	Protection statistics				Active Input	Action
				IP address	Port		Measured	PCR		Processed	Lost Detected	Requested	Unrecovered		
test	test	<input checked="" type="checkbox"/>		229.9.9.9	9000	0	2989952	3000000	284	0	0	0	0	All	Select

Total streams bitrate is 0 Mbit/s out of 1600 Mbit/s.

- Verify
  - The stream is shown
  - Packet rate is shown and valid
  - Both measured and PCR TS rate are shown and valid

## 6 Troubleshooting

This section provides a guide for troubleshooting issues commonly found when setting up DVP Protector and Sentinel.

### 6.1 Cannot Connect to DVP's Web-based Graphic User Interface (GUI)

In many situations, the inability to connect to the DVP's web-based GUI is highly likely to be due to connectivity issues.

1. Ethernet Cable Test
  - a. Connect the Ethernet cable between the DVP and a local host directly.
  - b. Verify that the Data or management port LED's are on (left and right).
  - c. In the case, the LED's are OFF
    - i. Verify that the DVP is ON.
    - ii. Replace the Ethernet cable.
  - d. Ping the DVP's port to verify the connectivity issue is resolved.
    - i. If resolved then connect to the DVP's web-based GUI by typing the DVP's management IP address as URL.
    - ii. If not, continue to step 2.
2. IP/Subnet Configuration

The DVP does not currently support DHCP hence IP address and subnet masks are not set automatically.

  - a. Using the IP configuration tool in your host verify that:
    - i. The host's IP address is at the same subnet as the DVP port's subnet.
    - ii. The host's subnet mask is the same as the DVP port's subnet.
  - b. Ping the DVP to verify connectivity issue is resolved.
    - i. If resolved then connect to the DVP's web-based GUI.
    - ii. If not then continue to step 3.
3. If the problem is not resolved consult customer support.

Configuration example:

- DVP Management IP address is set for 10.0.0.200
- Local host IP address is set to 10.0.0.20
- Local host subnet mask is set for 255.255.255.0

## 6.2 Management Port IP Address is Unknown

### 6.2.1 Connecting Via Data Port

In the case, the management port IP is unknown then the DVP web-based GUI is accessible via the data port.

1. Connect an Ethernet cable between the DVP data port and a local host directly.
2. Verify that the Data port LED's are on (left and right).
3. In the case, the LED's are OFF
  - a. Verify that the DVP is ON.
  - b. Replace the Ethernet cable.
4. Modify the host's IP address to be in the same subnet as the Data port.
5. Ping the DVP Data port from the host.
6. Connect to the DVP web-based GUI by typing the DVP's Data port IP address as URL.
7. Modify the management IP address as desired.

### 6.2.2 Connecting Via Console

In the case, neither management nor data port IP address is known then the data port IP address can be retrieved via the DVP console.

1. Connect an RJ-45 to RS-232, DB9 (Cisco type console cable) to the DVP.
2. Configure the RS-232 port parameters in the terminal to 115200, 8-bit, 1 Stop, No Parity.
3. Using a terminal software of your choice
  - a. Press <Enter>
  - b. User: root
  - c. Password: videoflow
4. Type `ifconfig eth0` <Enter>
5. Copy the IP address shown. This is **data port 1** IP address
6. Retry Section 6.2.1


### 6.2.3 No Login Window

In the case a login window is not shown even though the DVP is ON follow the below procedure:

1. Clear the Web browser history
2. Clear the Web browser cache
3. Try to reconnect
4. In the case of no Login window try to update the Java version used by the host

### 6.2.4 Check Connectivity

Now you need to confirm that the VPN tunnel has been established.

1. Click on the interfaces tab
2. See the section labeled VPNs
  - a. If this is severe there will be tabs marking the names of the different servers. Click the tab of the appropriate server.
  - b. If this the client, there will be a list of UDP Port numbers that match the clients that were configured
3. The table in the window shows the status of the UDP VPN tunnel. If the tunnel is up a green "+" symbol will be indicated. If the tunnel is down then a red "-" will be indicated. If there is a red triangle with a  then there is a potential configuration or conflict and advanced troubleshooting will be required.

Once the configuration of the tunnel has been completed and the tunnel is up and running it is time to configure the video streams to flow through the tunnel.

This is first achieved by assigning a logical name to the VPN tunnel on both the client and the server side.

1. Click on the Configuration tab
2. Click on system→interfaces→all
3. Click add interface
4. Enter a unique identifier to name this interface (BP Tip – Choose a name that easily represents the functionality of the tunnel. Some ideas could be to use the name of the destination or to use a video stream name as part of the name of the interface. This could help to diagnose the issues later much simpler.)
5. Click add
6. Select the port type.
  - a. If this is the server select UDP\_VPN\_Server from the drop down. Then select the name of the appropriate server (If there is more than one). Then select the remote client to which this interface will be connecting. Then click Commit
  - b. If this is the client select UDP\_VPN\_Client from the drop down. Then select the client interface port number that was configured in the previous steps. Then click Commit.

Now that the interfaces have been configured, you can proceed to configure the stream for video. (See How to configure a stream cookbook).

### 6.3 Cannot See a Stream in the Protector

1. Verify that the stream's encapsulation method in the source is identical to the one used by the DVP.
2. In the case, it is not, then click on configurations/Stream/stream\_name/Advanced and set the working mode to either Standard if encapsulation is RTP or UDP\_2\_RTP if encapsulation is UDP
3. Make sure the stream is sent as constant bit rate (CBR) and not as variable bit rate (VBR).
4. Make sure the source is configured for sending constant packet length according to Pro-MPEG or SMPTE2022 (1..7 MPEG packets in a single IP frame)
5. Make sure the stream includes PAT, PMT, and PCR
6. Verify that the time to live (TTL) set by the source is not set for low number (1, 2). It is advised to set this parameter to the maximum possible.
7. Using a sniffer tool (e.g., Wireshark or tcpdump) verify that the stream's source IP address and destination IP address are set as required.

### 6.4 Cannot see a Stream in the Sentinel

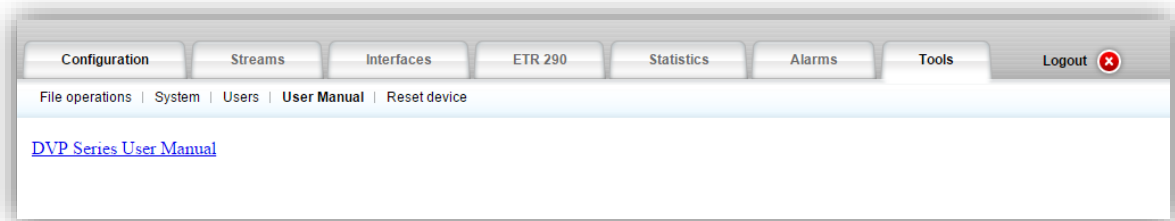
1. Verify the stream configuration in the connected Data port
2. If a tunnel is in use then verify that the source port is the tunnel interface and not a data port
3. Verify the DVP bandwidth license is above the stream's bandwidth
  - a. Click on the Configuration tab
  - b. Click on Unit
  - c. Click on Permission
4. Verify that the TS Rate (PCR) is the same as the TS rate (measured)
  - a. Click on Stream tab
  - b. Compare the values

TS rate (pcr)	TS rate (measured)
  - c. In the case the TS rate (PCR) is significantly higher than the TS rate (measured) then reset the stream (Please consult with the DVP user's manual for more information on how to reset the stream)

### 6.5 Downloading the User's Guide

The DVP includes a copy of the latest user's manual at the time it was shipped. The following procedure describes how to download it from the DVP to your computer.

1. Click on the main menu Tools tab



2. Click on **DVP\_Series\_User\_Manual** to download the DVP user manual to your computer.