Avaya Solution & Interoperability Test Lab

Application Notes for configuring Fijowave Fijoport Remote Access with Avaya IP Office 500 V2 R9.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Fijowave's Fijoport Remote Access to access Avaya IP Office R9.1.

Readers should pay particular attention to the scope of testing as outlined in **Section 2.1**, as well as observations noted in **Section 2.2** to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Fijowave's Fijoport Remote Access to access Avaya IP Office 500 V2 R9.1. Fijoport Remote Access can be used as a remote access device with Avaya IP Office 500 V2 and can be viewed as three modules, the Fijowave Portal VPN, the Fijowave Portal Server and the Fijoport Box. The Fijowave Portal Server is responsible for establishing and maintaining secure tunnel connections to Fijoport boxes on the remote customer networks. A customer support engineer can remotely access the Fijowave Portal Server using Fijowave Portal VPN software installed on a desktop using a point-to-point tunnelling protocol virtual private network.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Fijoport Remote Access to be used as a remote access device with Avaya IP Office 500 V2.

Definitions:

- PPTP - point-to-point tunneling protocol
- VPN - Virtual Private Network
- RAS - Remote Access Session
- CSE - Customer Support Engineer
- MPPE - Microsoft Point to Point Encryption
- SMS - Short Message Service

The solution involves connecting the Fijoport box to the internet via the LAN of the IPPBX or internet gateway device on the customer premises. The Fijoport box establishes a secure tunnel link with the Fijowave Portal Server via the Public network. The Customer Support Engineer (CSE) desktop located on the Operator network can connect to the Portal server via the Fijowave Portal VPN service. This VPN service uses PPTP and is secured using MPPE. The CSE can log onto the Operator interface via the Fijowave Portal VPN and instruct the Portal server to establish a remote access session (RAS) to specified customer network equipment via the Fijoport box. The CSE can run applications locally on his desktop to manage the selected equipment as if directly connected on the customer network.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The compliance testing includes the test scenarios shown below.

- Using Avaya IP Office Manager from a remote location.
  - Log into IP Office Manager
  - Make a change to an existing user
  - Add a new user
- Using the IP Office Monitor tool.
- Using the IP Office System Status tool.

2.2. Test Results

All test cases passed successfully with the following observations noted during testing.

1. When opening IP Office Manager, the "Broadcast Discovery" must not be used. The Mapped IP address must be used to discover the IP Office and this Mapped IP address is the address provided by the Fijoport device. See **Section 7.1** for the Mapped IP Address location.
2. Opening the IP Office Manager configuration can take up to 1 minute depending on the network speed.
3. This solution was only tested with IP Office 500 V2, although a connection in theory could be made to the IP Office Server Edition if it was standalone. Similar for the IP Office Server Edition Monitor and System Status.
4. To facilitate compliance testing a 4G modem was supplied by Fijowave to allow internet access from the Supervisor PC in the DevConnect laboratory to the cloud hosted Fijowave Portal Server. This was required because the DevConnect laboratory routing network did not pass the Generic Routing Encapsulation (GRE) Point-to-Point Tunneling Protocol (PPTP) packets that are required for the Fijowave portal VPN to operate correctly. Use of this 4G modem may explain the following connection instability problems observed during compliance testing.
   (i) The connection is dropped if the IP Office Monitor is running and IP Office Manager is opened.
   (ii) The connection is dropped if the IP Office System Status is running and IP Office Manager is opened.

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 9** of these Application Notes. Technical support for the Fijowave Fijoport Remote Access product can be obtained as follows:

- Web: http://www.fijowave.com
- Email: support@fijowave.com
- Help desk: +353 1 525 3072

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Fijoport product provides a remote service platform solution that allows the user to remotely maintain products in a secure manner over an IP link. The Fijoport box is located on the customer network along with a Portal Server appliance hosted by Fijowave. A user can establish a connection to the IP Office interface via the Fijowave Portal VPN and instruct the Portal Server to establish a remote access session to specified customer network equipment via the Fijoport box.

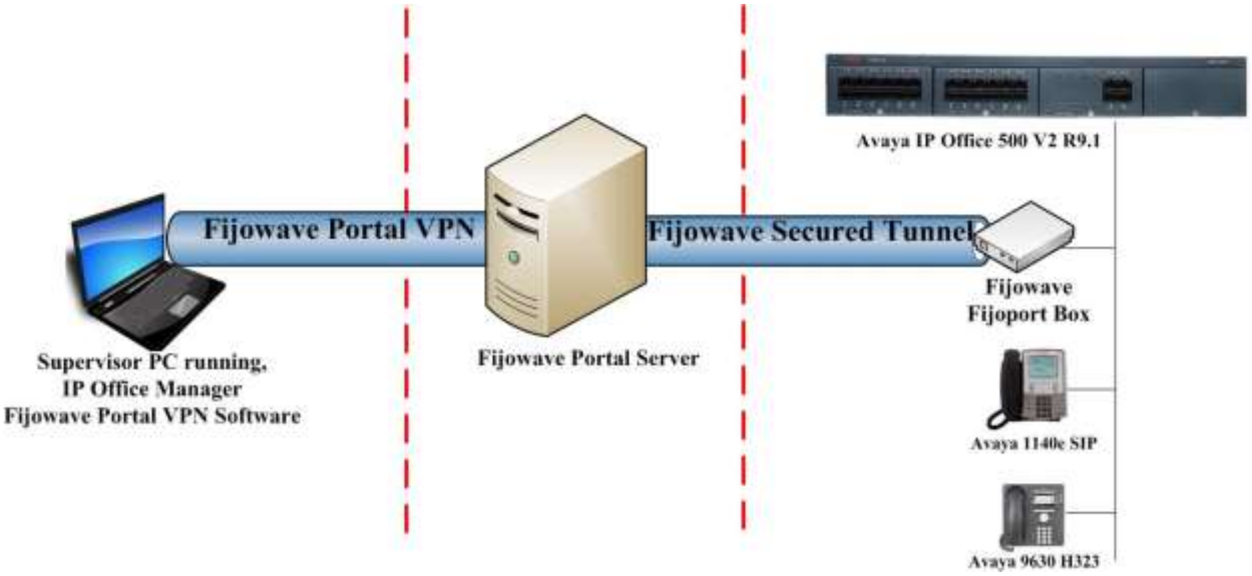


Figure 1: Reference Configuration of Fijowave Fijoport Remote Access with Avaya IP Office

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Version/Release
Avaya IP Office 500 V2	R9.1 SP6
Avaya IP Office Manager	R9.1 SP6
Avaya 9630 Deskphone	H.323 Release 6.4014U
Avaya 1140e Deskphone	SIP R04.03.12.00
Avaya 9408 Digital Deskphone	N/A
Fijowave Fijoport Box	V1.0.23-1
Fijowave Portal VPN	V1.0
Fijowave Portal Server	V2.0.7

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 only.

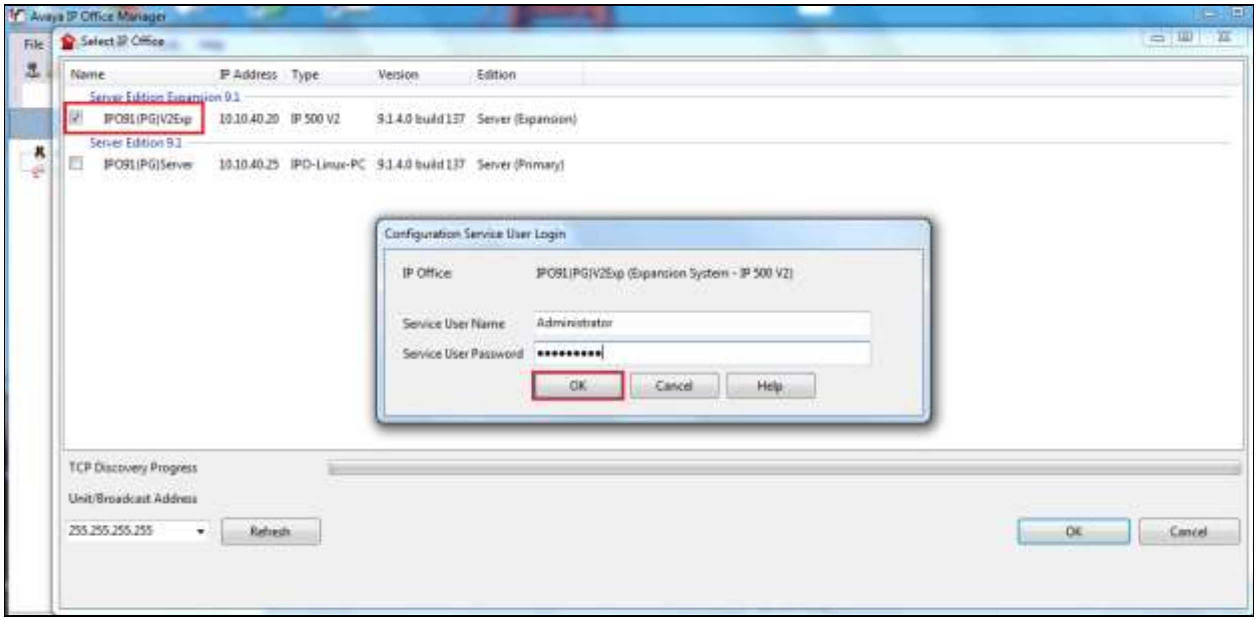
5. Configure Avaya IP Office

There is no specific configuration of IP Office required for the compliance testing of Fijoport Remote Access. The IP address of IP Office is required in order to configure the Fijoport box in **Section 6**. Configuration and verification operations on Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Launch Avaya IP Office Manager.
- Display LAN Configuration.

5.1. Launch Avaya IP Office Manager

From the Avaya IP Office Manager PC, go to **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application or use the shortcut on the desktop (not shown). Tick the required server to log in to, this will be the IP Office 500 V2 and log in to Avaya IP Office using the appropriate credentials to receive its configuration.



	Name	IP Address	Type	Version	Edition
	Server Edition Expansion 9.1				
☑	IPO91(PG)V2Exp	10.10.40.20	IP 500 V2	9.1.4.0 build 137	Server (Expansion)
	Server Edition 9.1				
□	IPO91(PG)Server	10.10.40.25	IPO-Linux-PC	9.1.4.0 build 137	Server (Primary)

IP Office: IPO91(PG)V2Exp (Expansion System - IP 500 V2)

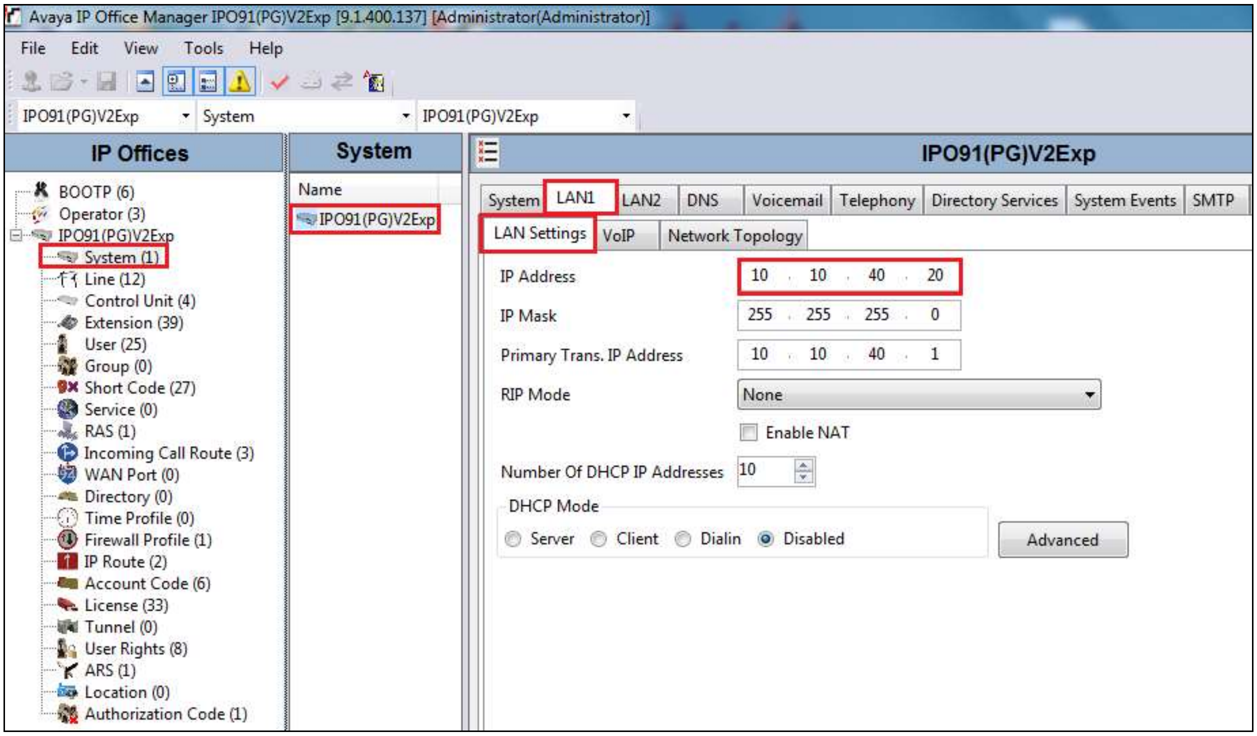
Service User Name: Administrator

Service User Password: ••••••••••

Unit/Broadcast Address: 255.255.255.255

5.2. Display LAN Configuration

Once logged in navigate to **System** in the left window and this will display the IP Office system properties in the main window. Select the **LAN1** tab in the main window and within that tab select the **LAN Settings** tab. This displays the **IP Address** information and will be used in the configuration of the Fijoport box in **Section 6.2**.



Avaya IP Office Manager IPO91(PG)V2Exp [9.1.400.137] [Administrator(Administrator)]

File Edit View Tools Help

IPO91(PG)V2Exp | System | IPO91(PG)V2Exp

IP Offices

- BOOTP (6)
- Operator (3)
- IPO91(PG)V2Exp
  - System (1)
  - Line (12)
  - Control Unit (4)
  - Extension (39)
  - User (25)
  - Group (0)
  - Short Code (27)
  - Service (0)
  - RAS (1)
  - Incoming Call Route (3)
  - WAN Port (0)
  - Directory (0)
  - Time Profile (0)
  - Firewall Profile (1)
  - IP Route (2)
  - Account Code (6)
  - License (33)
  - Tunnel (0)
  - User Rights (8)
  - ARS (1)
  - Location (0)
  - Authorization Code (1)

System

Name: IPO91(PG)V2Exp

IPO91(PG)V2Exp

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP

LAN Settings | VoIP | Network Topology

IP Address	10 . 10 . 40 . 20
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	10 . 10 . 40 . 1
RIP Mode	None
	□ Enable NAT
Number Of DHCP IP Addresses	10

DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

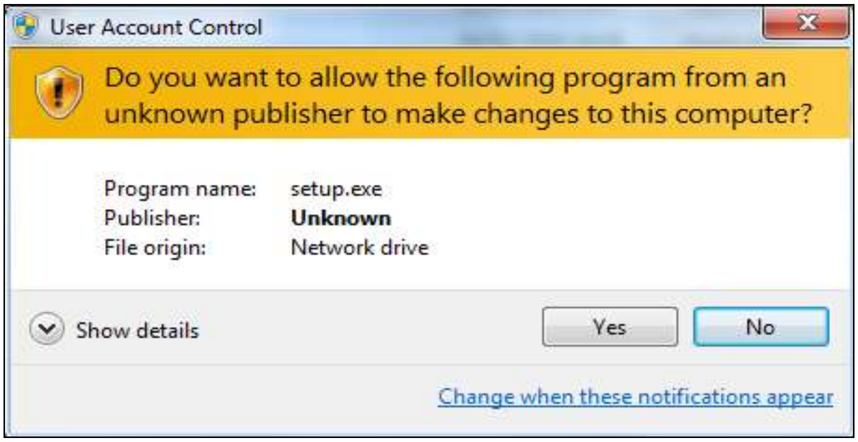
Advanced

6. Configure Fijowave Fijoport Remote Access

The configuration of the Fijoport Remote Access includes the installation and configuration of the Fijoport Portal VPN. Fijowave provides a username and password for the Fijoport Portal VPN in order to ensure connectivity to the Fijoport Portal Server. This username and password is required during the installation of the Fijoport Portal VPN.

6.1. Install Fijowave Portal VPN

Unpack the contents of the ZIP file, FijowavePortal.zip, browse to the Fijowave Portal VPN directory and run setup.exe (not shown). Click **Yes** if User Account Control asks permission to proceed.

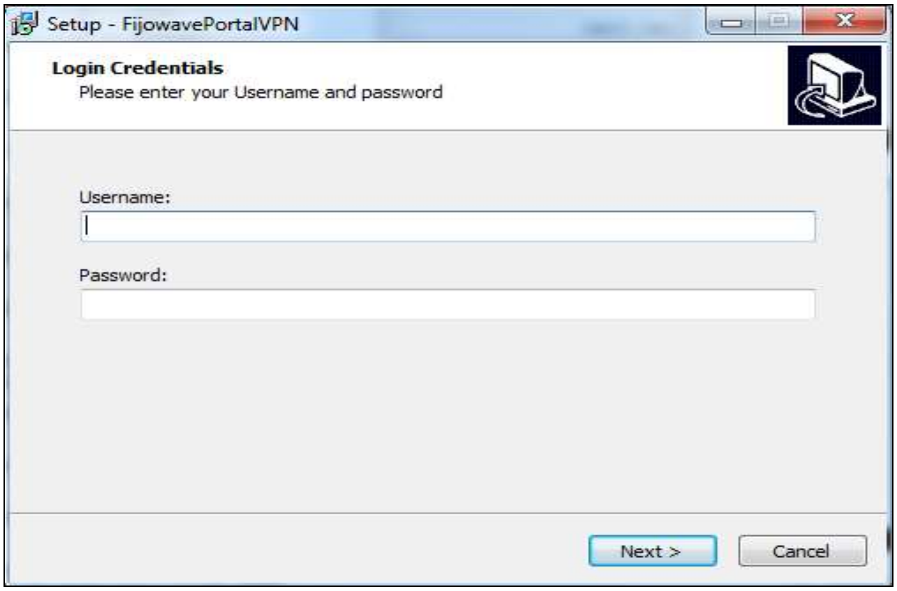


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: setup.exe
Publisher: **Unknown**
File origin: Network drive

Enter the VPN **Username** and **Password**, this information is provided by Fijowave and is used when opening the Fijowave Portal VPN. Once the correct information has been added, click on **Next** to continue.



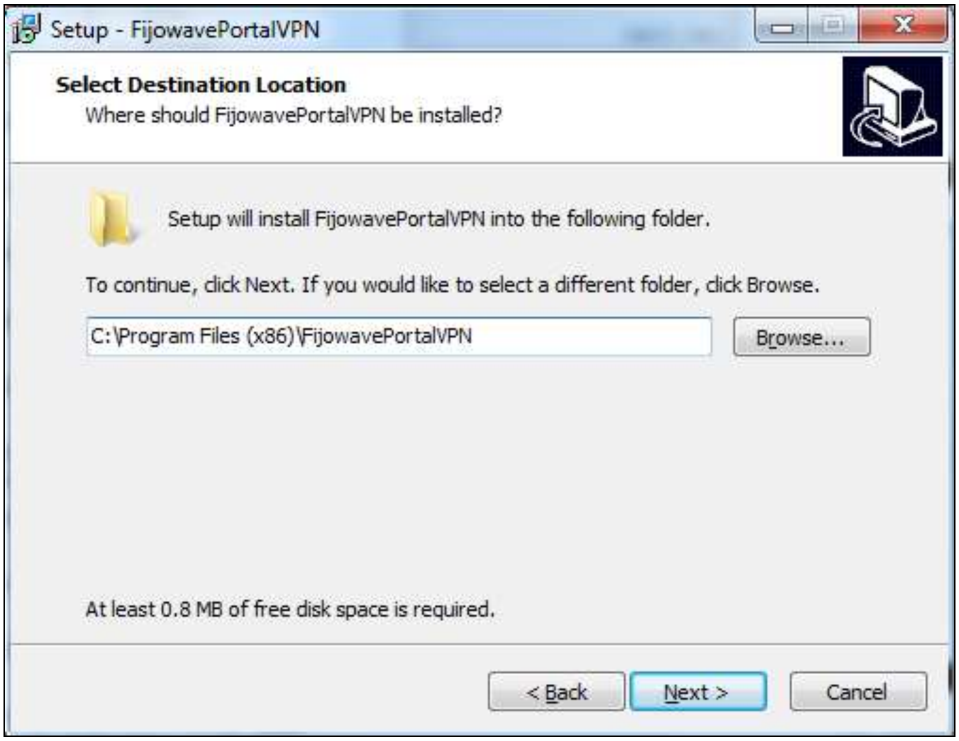
Setup - FijowavePortalVPN

Login Credentials
Please enter your Username and password

Username:

Password:

Confirm the **Destination Location** by clicking **Next**.



Setup - FijowavePortalVPN

Select Destination Location

Where should FijowavePortalVPN be installed?

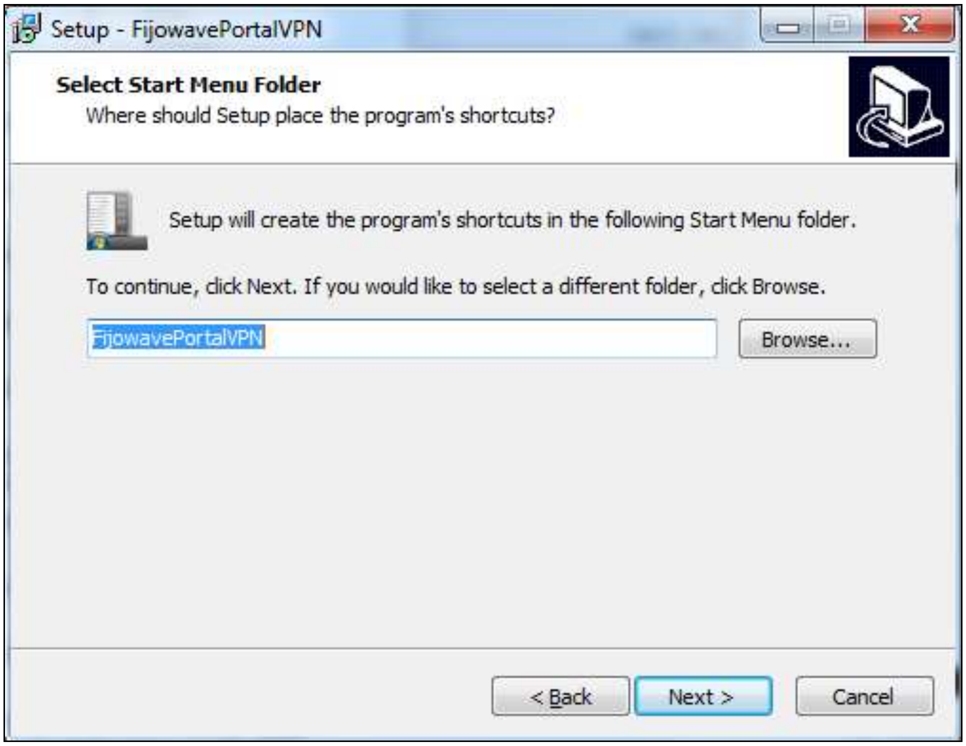
Setup will install FijowavePortalVPN into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\FijowavePortalVPN

At least 0.8 MB of free disk space is required.

Confirm the **Start Menu Folder** by clicking **Next**.



Setup - FijowavePortalVPN

Select Start Menu Folder

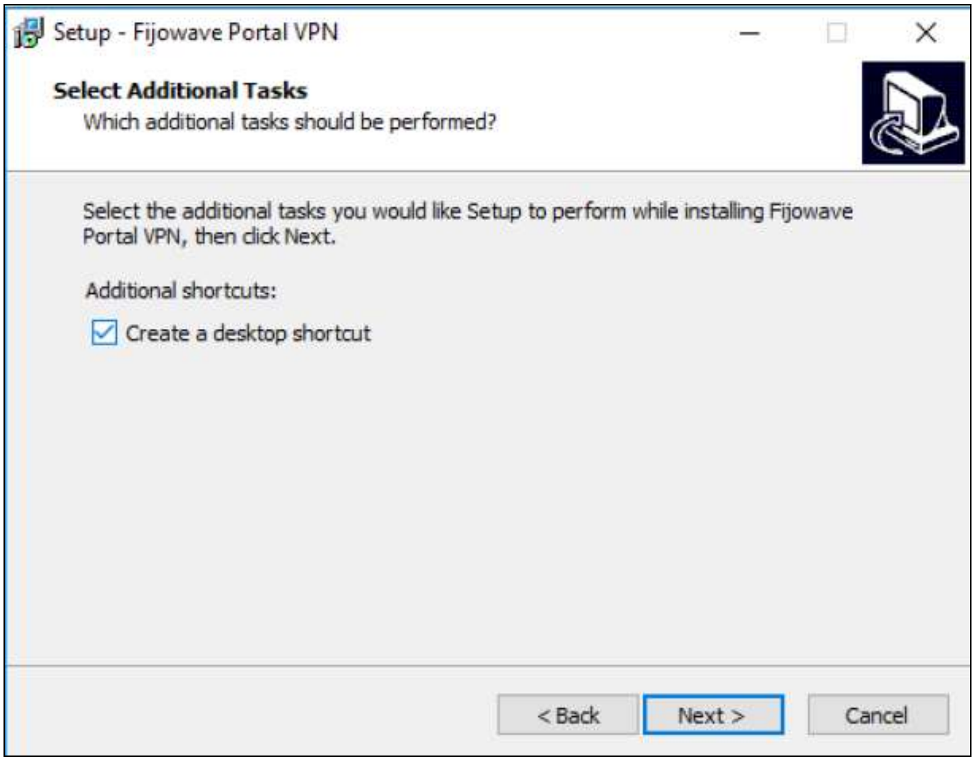
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

FijowavePortalVPN

Click **Next** to confirm the decision for creating a desktop shortcut.


Setup - Fijowave Portal VPN

Select Additional Tasks

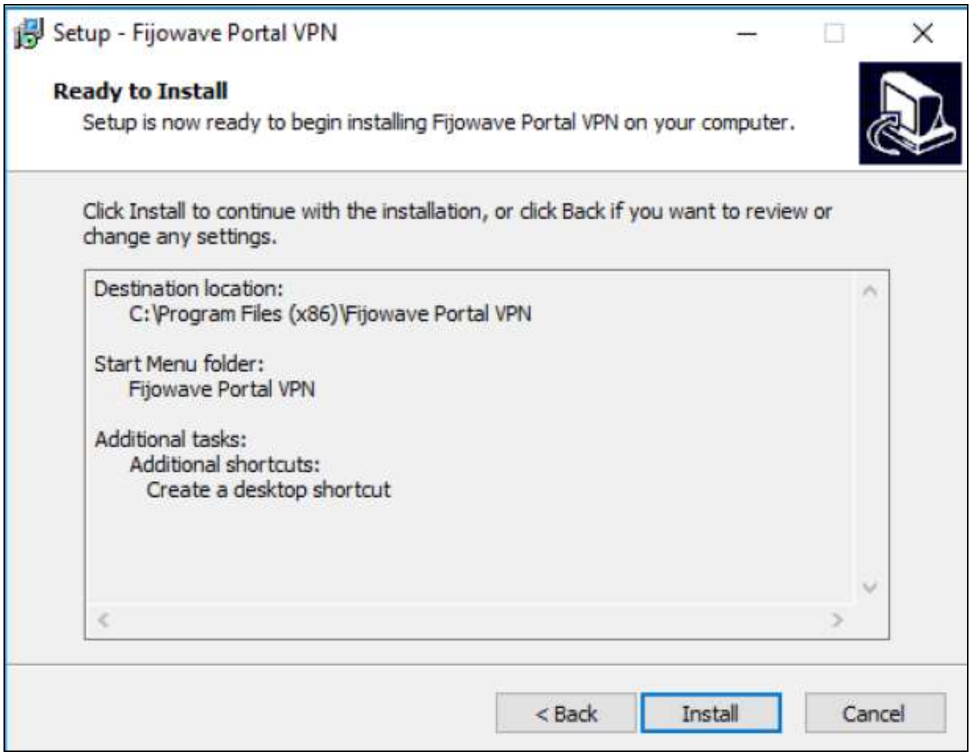
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Fijowave Portal VPN, then click Next.

Additional shortcuts:

☑ Create a desktop shortcut

Confirm the installation settings and install Fijowave Portal VPN by clicking **Install**.


Setup - Fijowave Portal VPN

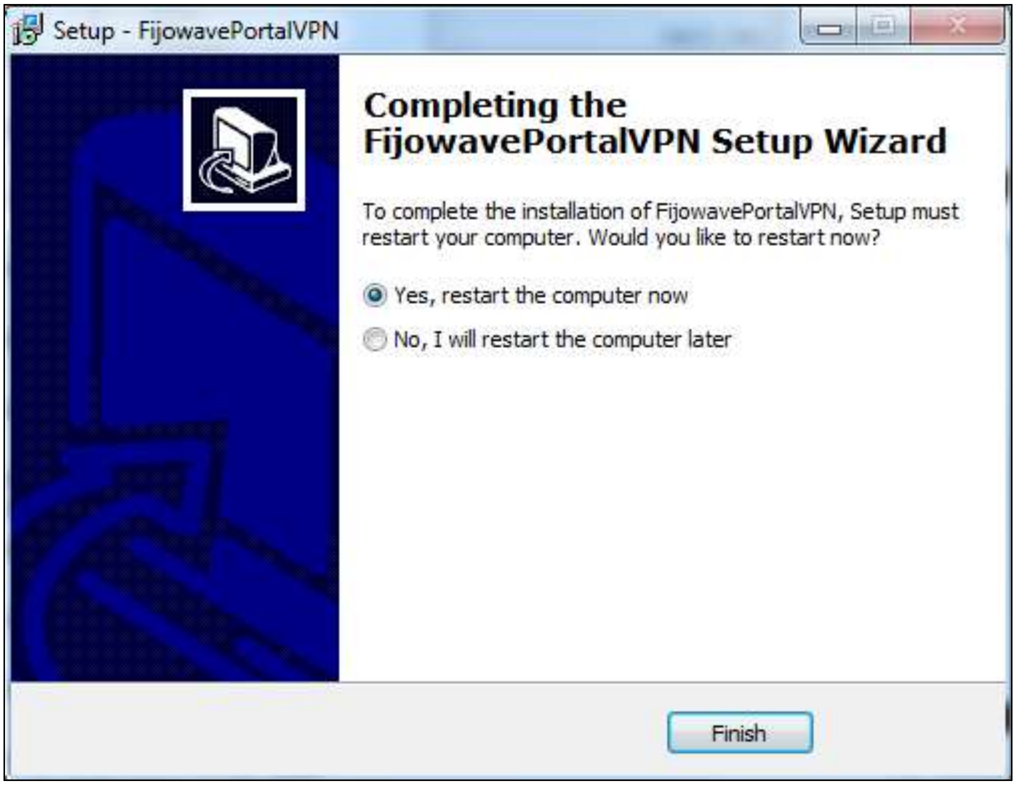
Ready to Install

Setup is now ready to begin installing Fijowave Portal VPN on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\Fijowave Portal VPN

Start Menu folder:
    Fijowave Portal VPN

Additional tasks:
    Additional shortcuts:
      Create a desktop shortcut
```

Complete the installation process by checking, **Yes, restart the computer now** and clicking **Finish**.



Completing the FijowavePortalVPN Setup Wizard

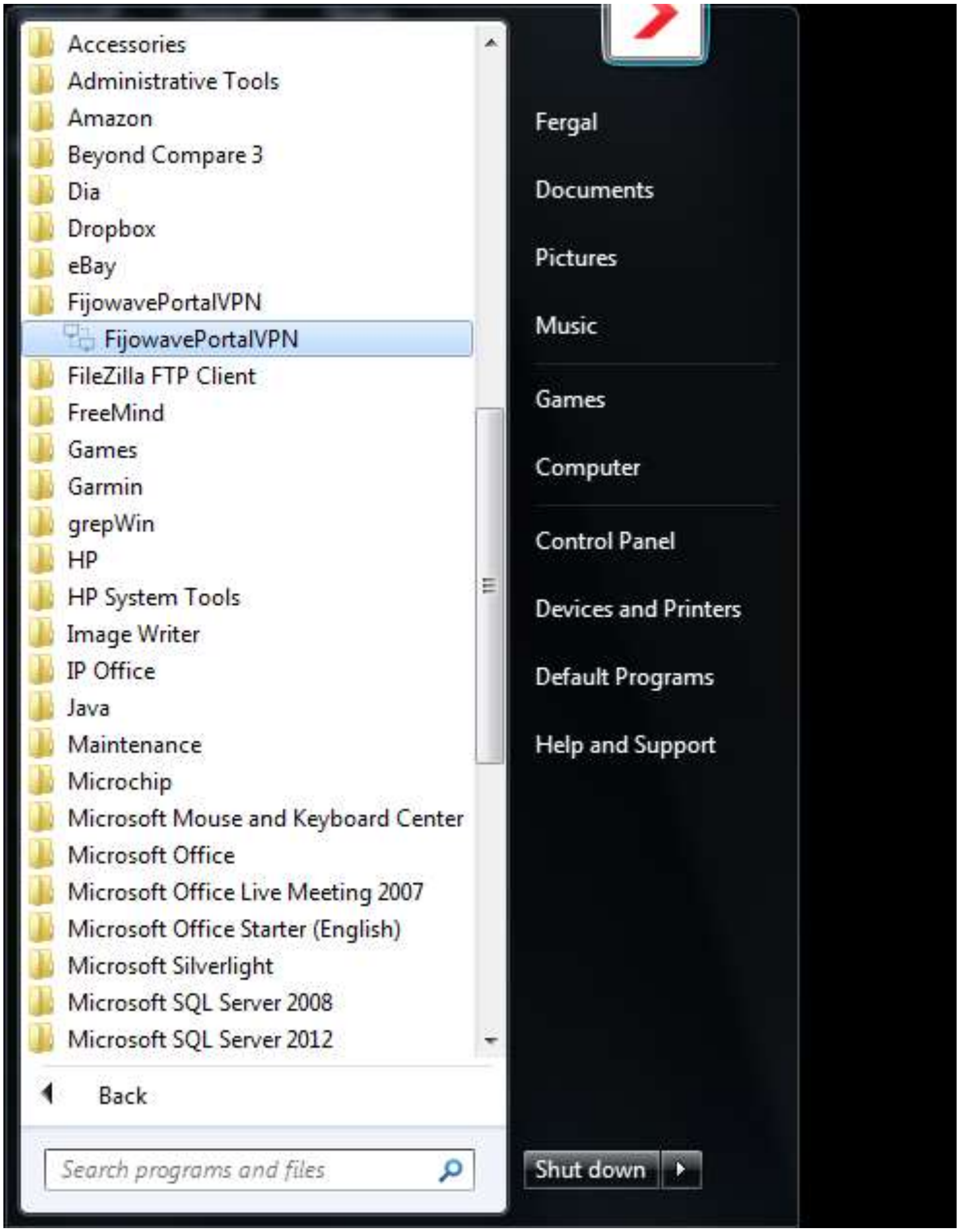
To complete the installation of FijowavePortalVPN, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now

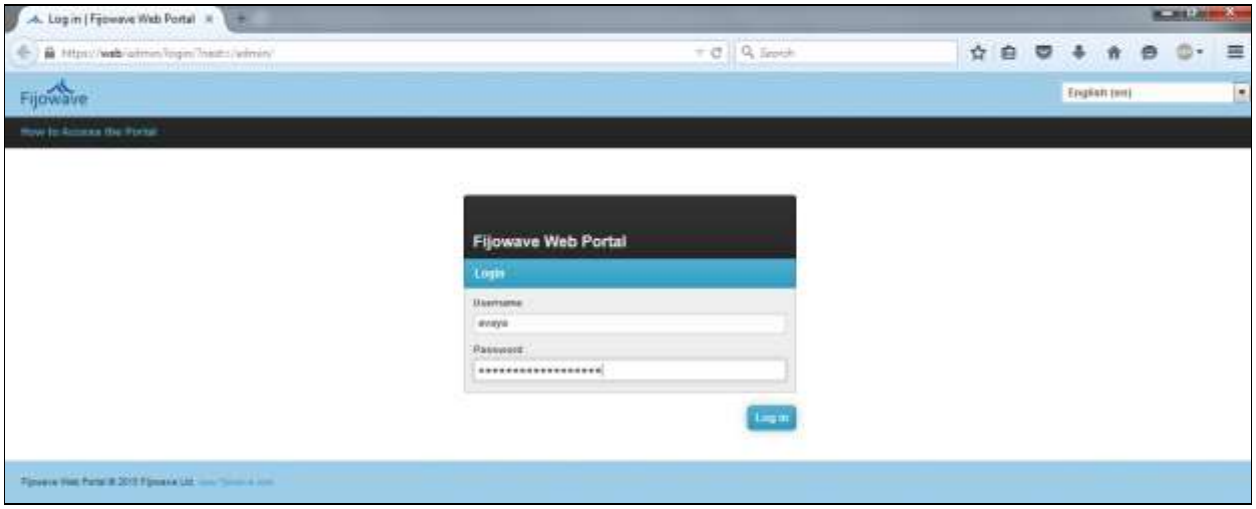
○ No, I will restart the computer later

6.2. Configure Connection to IP Office

Open the Fijowave Portal VPN by either double clicking on the shortcut on the desktop (not shown) or by clicking the desktop shortcut or by selecting the **FijowavePortalVPN** application from the Windows Start Menu.



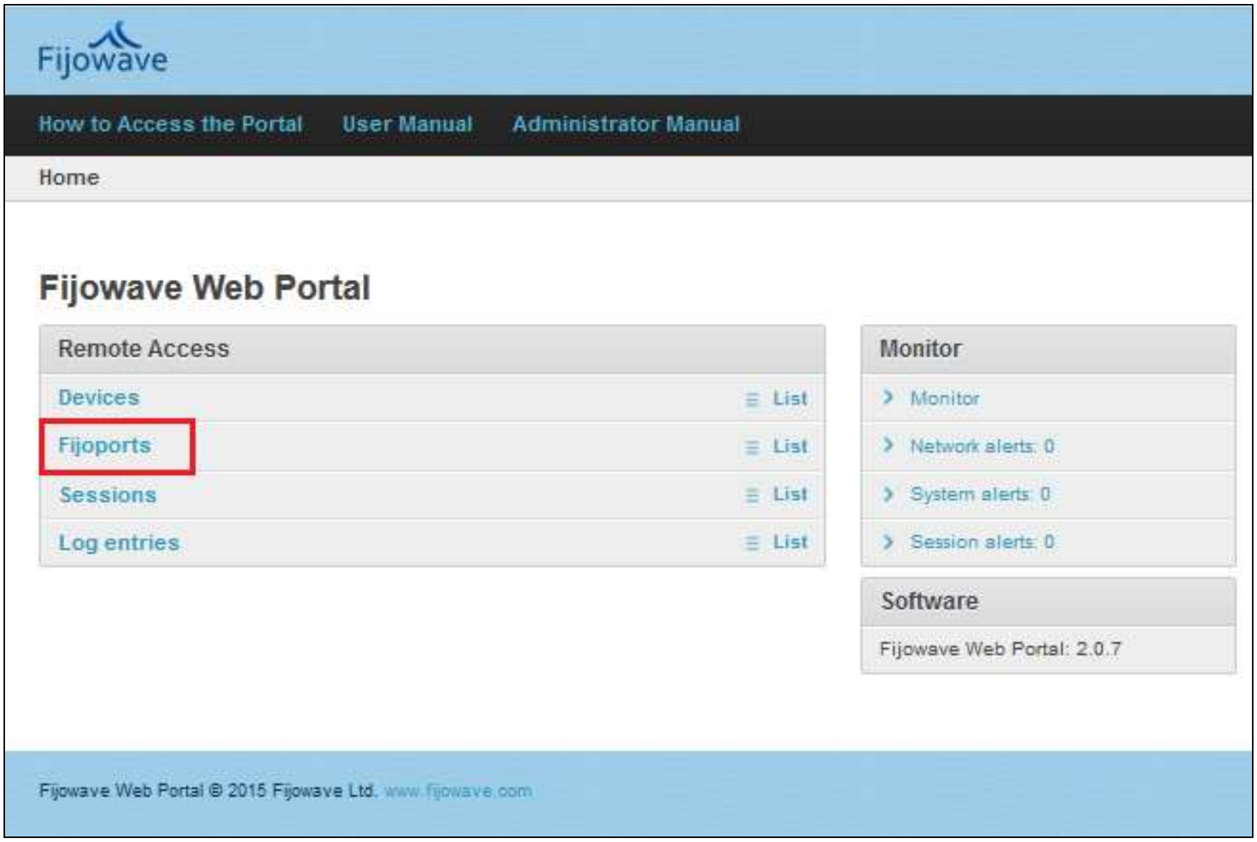
The following web page opens automatically, enter the correct credentials and click on **Log in**.



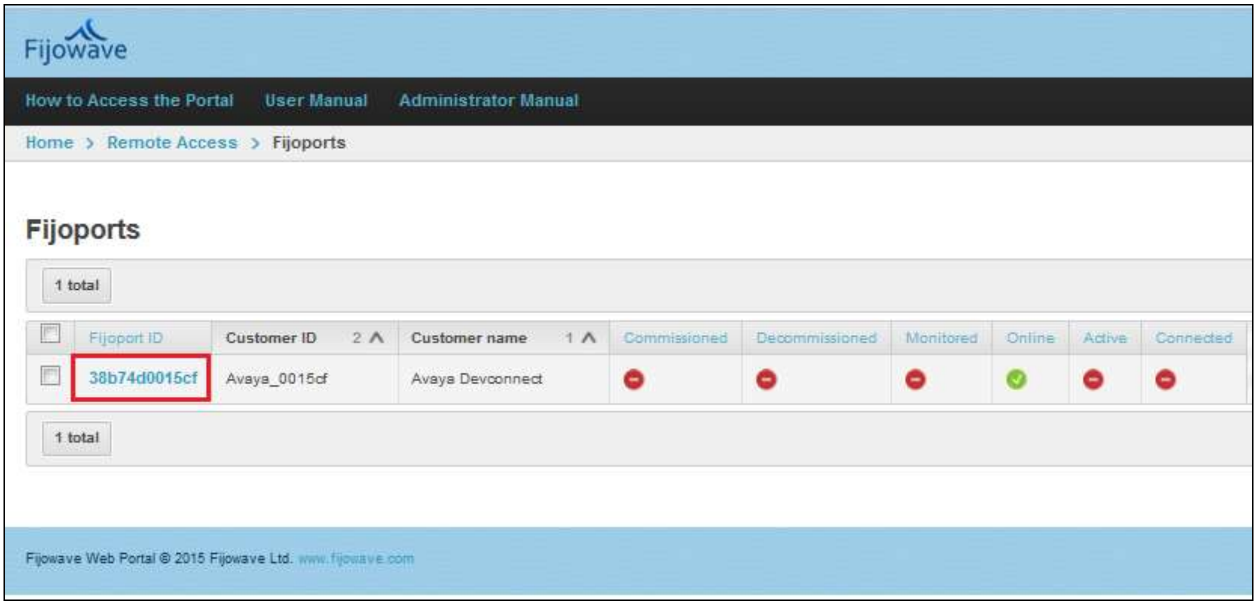
Username: avaya

Password: ••••••••••••••••••••

Click on **Fijoports**, as highlighted below.



During compliance testing only one Fijoport was used as shown below, click on that to continue. On sites where many Fijoports are in use, click on the correct **Fijoport ID**.



Fijoports

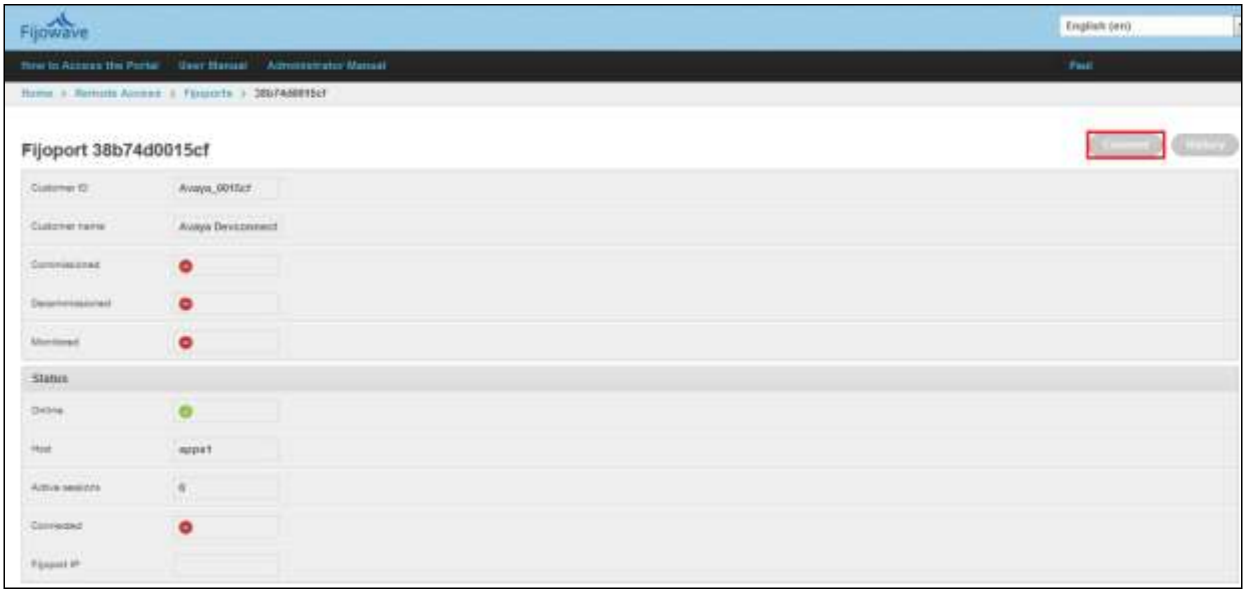
1 total

□	Fijoport ID	Customer ID 2 ^	Customer name 1 ^	Commissioned	Decommissioned	Monitored	Online	Active	Connected
□	38b74d0015cf	Avaya_0015cf	Avaya Devconnect	⊖	⊖	⊖	✓	⊖	⊖

1 total

Fijowave Web Portal © 2015 Fijowave Ltd. www.fijowave.com

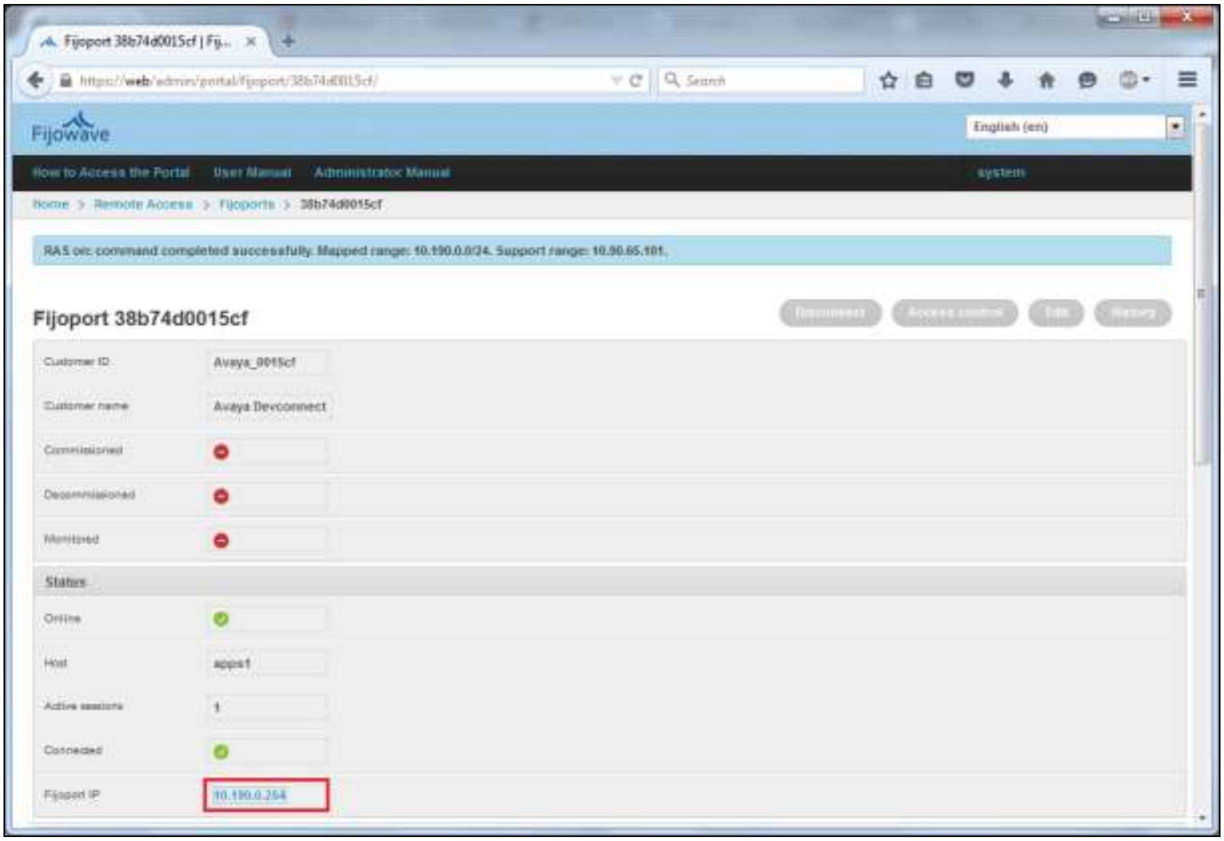
Click on **Connect** at the top right corner.



Fijoport 38b74d0015cf

Customer ID	Avaya_0015cf
Customer name	Avaya Devconnect
Commissioned	⊖
Decommissioned	⊖
Monitored	⊖
Status	
Online	✓
Host	appa1
Active sessions	6
Connected	⊖
Fijoport IP	

The message displayed at the top of the screen as well as the **Connected** status displayed at the bottom shows that the VPN as connected successfully.

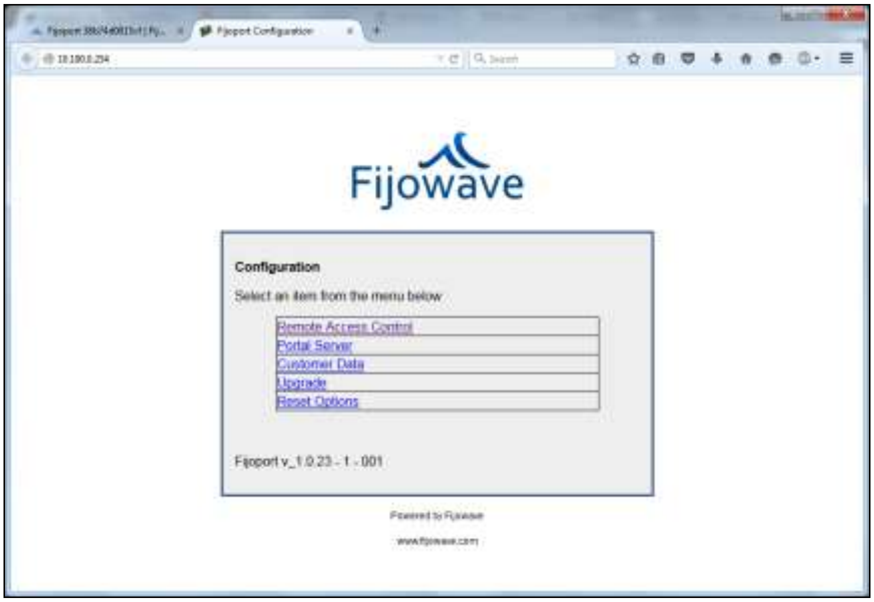

Fijoport 38b74d0015cf | Fij...
https://web/admin/portal/fijoport/38b74d0015cf/
Search
Fijowave
English (en)
How to Access the Portal
User Manual
Administrator Manual
system
Home > Remote Access > Fijoports > 38b74d0015cf
Disconnect
Access control
Edit
History

RAS on: command completed successfully. Mapped range: 10.190.0.0/24. Support range: 10.90.65.101.

Fijoport 38b74d0015cf

Customer ID	Avaya_0015cf
Customer name	Avaya Devconnect
Commissioned	⊖
Decommissioned	⊖
Monitored	⊖
Status	
Online	✓
Host	apps1
Active sessions	1
Connected	✓
Fijoport IP	10.190.0.254

Click on the **Fijoport IP** address, highlighted above, to open a new tab and log in to the Fijoport Web Configuration Service. Click on the **Remote Access Control** link.



Configuration

Select an item from the menu below

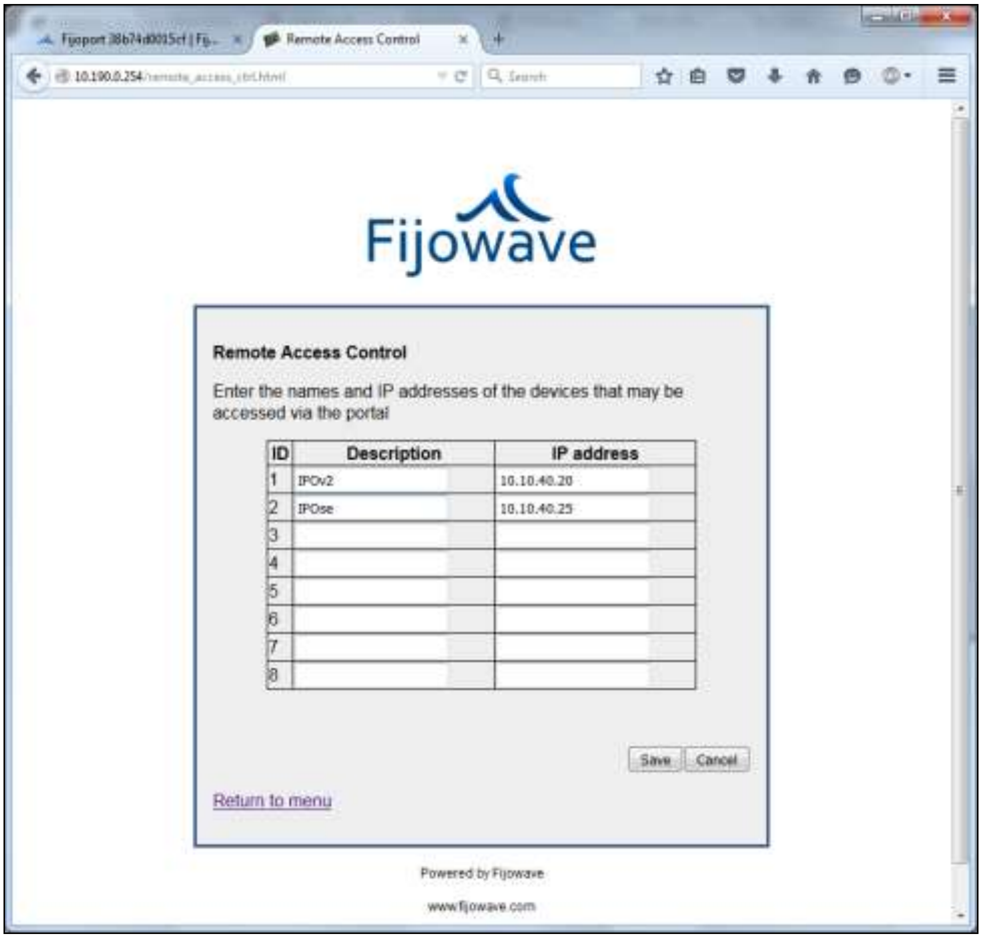
- Remote Access Control
- Portal Server
- Customer Data
- Upgrade
- Reset Options

Fijoport v_1.0.23 - 1 - 001

Powered by Fijowave

www.fijowave.com

After clicking on the Remote Access Control link on the previous page, enter the local IP address of the IP Office 500 v2 address in device **ID 1** position and the local IP address of the IP Office Server Edition in device ID 2 position (if applicable) and press the **Save** button and then close the browser tab.

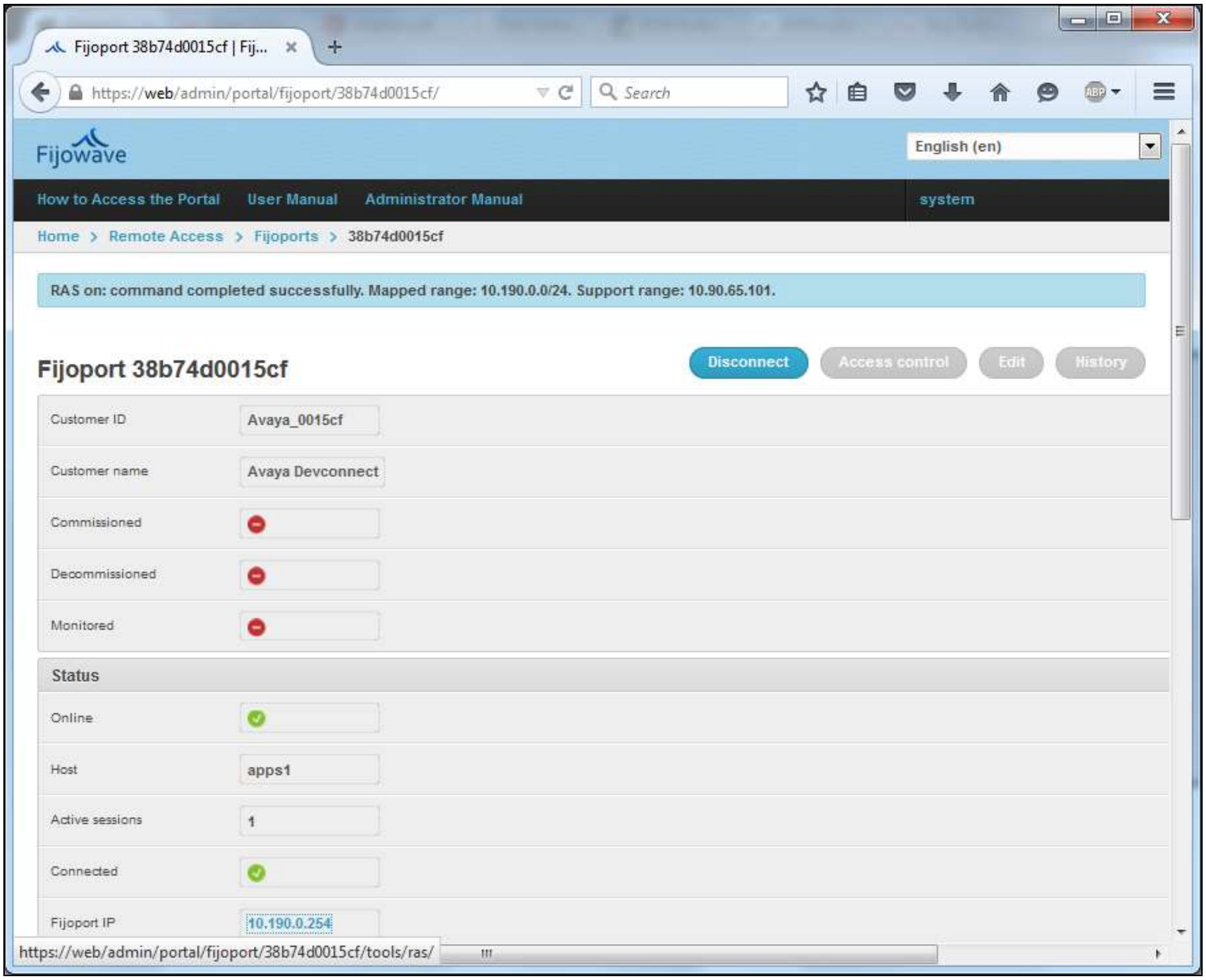

Fijoport 38b74d0015cf | Fij...
Remote Access Control
10.190.0.254/remote_access_ctrl.html
Search
Fijowave

Remote Access Control

Enter the names and IP addresses of the devices that may be accessed via the portal

ID	Description	IP address
1	IPOv2	10.10.40.20
2	IPOse	10.10.40.25
3		
4		
5		
6		
7		
8		

Click **Disconnect** in the top right corner.



Fijoport 38b74d0015cf | Fij...
https://web/admin/portal/fijoport/38b74d0015cf/
Search
Fijowave
English (en)
How to Access the Portal
User Manual
Administrator Manual
system
Home > Remote Access > Fijoports > 38b74d0015cf
Disconnect
Access control
Edit
History
https://web/admin/portal/fijoport/38b74d0015cf/tools/ras/

RAS on: command completed successfully. Mapped range: 10.190.0.0/24. Support range: 10.90.65.101.

Fijoport 38b74d0015cf

Customer ID	Avaya_0015cf
Customer name	Avaya Devconnect
Commissioned	⊖
Decommissioned	⊖
Monitored	⊖

Status

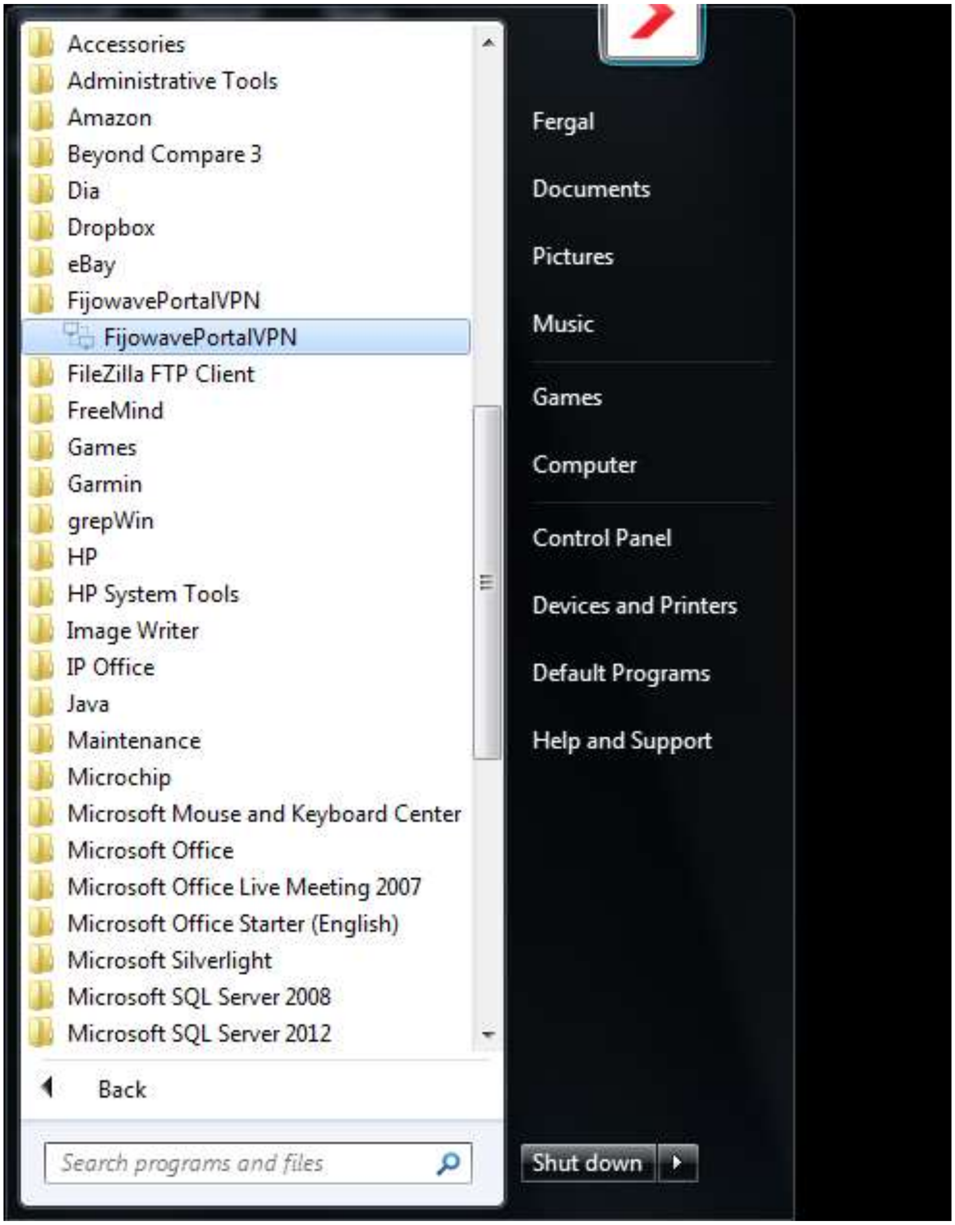
Online	✓
Host	apps1
Active sessions	1
Connected	✓
Fijoport IP	10.190.0.254

7. Verification Steps

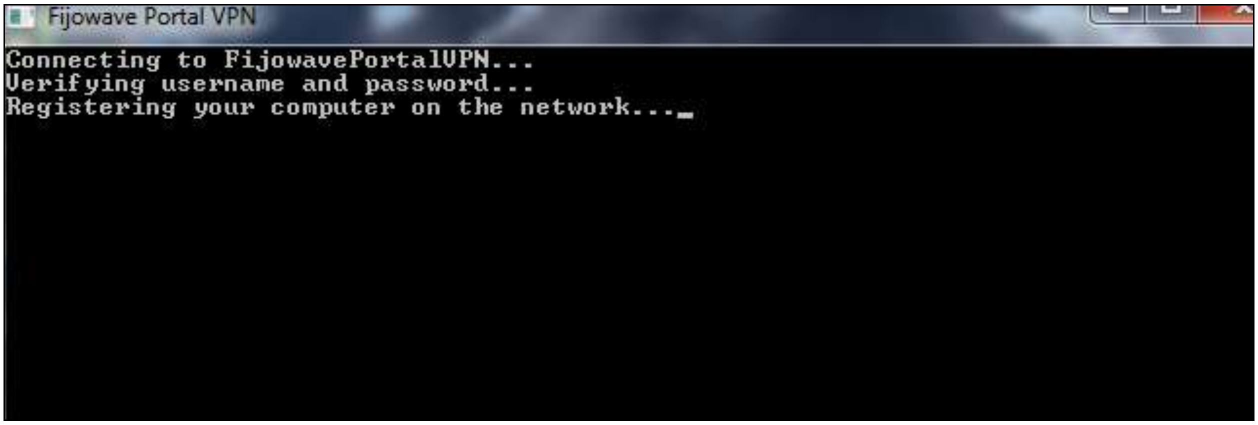
The following steps can be taken to ensure that connections between Fijowave Fijoport Remote Access and IP Office are up. The Fijowave Portal VPN is executed in order to setup the VPN connection. This connection can be verified and the IP Office applications can be run.

7.1. Run Fijowave Portal VPN

Open the Fijowave Portal VPN by either double clicking on the shortcut on the desktop (not shown) or by clicking the desktop shortcut or by selecting the **FijowavePortalVPN** application from the Windows Start Menu.

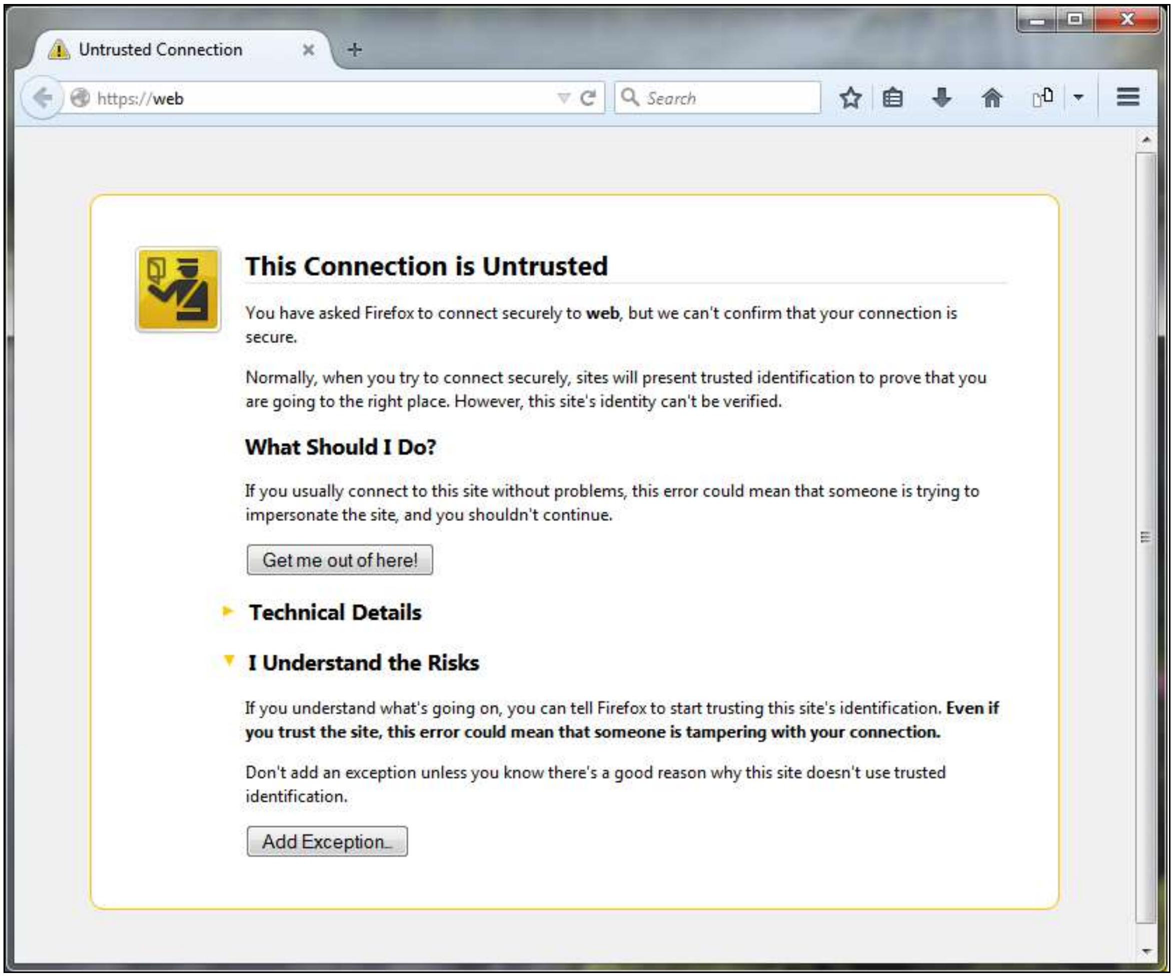


The following window will appear for a few moments before the default browser is opened.



```
Connecting to FijowavePortalVPN...
Verifying username and password...
Registering your computer on the network...
```

The first time the Fijowave Portal Server web page opens the Firefox web browser displays that the connection is not trusted or unsafe. Click **I Understand the Risks** and **Add Exception**. On the following screen click **Confirm Security Exception** (not shown).



This Connection is Untrusted

You have asked Firefox to connect securely to **web**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

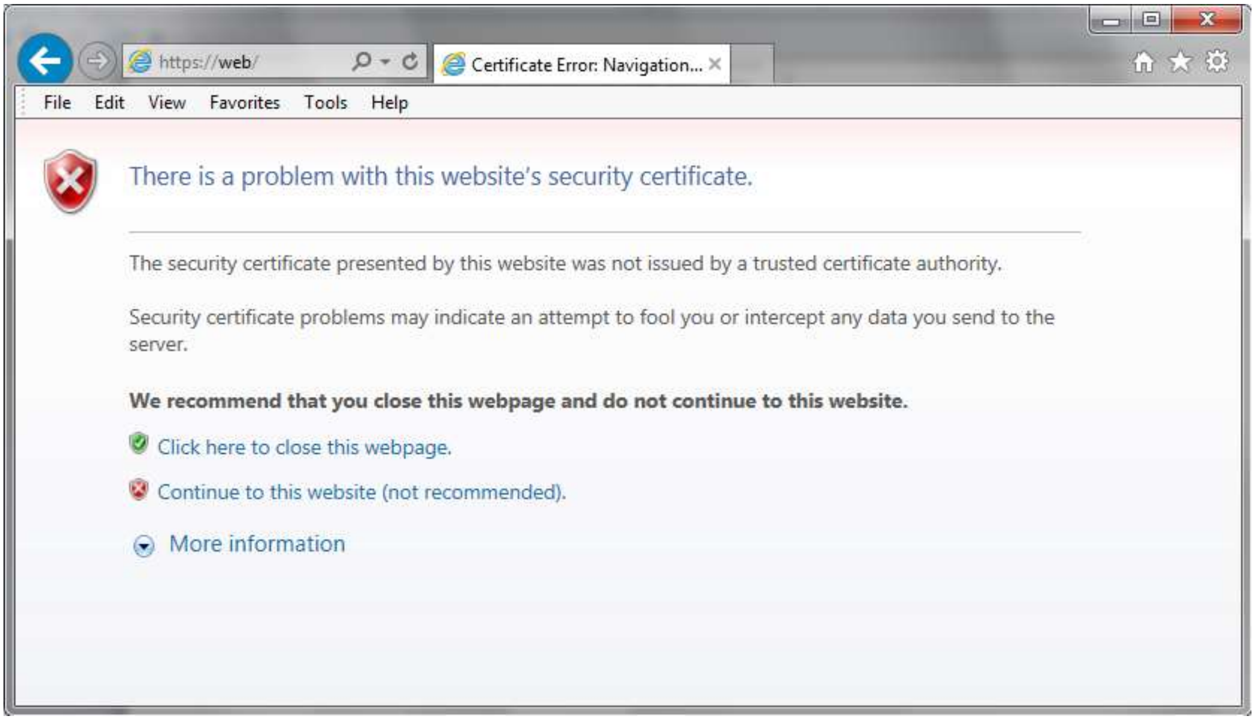
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

The Internet Explorer web browser says, **There is a problem with this website's security certificate**, click **Continue to this website (not recommended)**.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

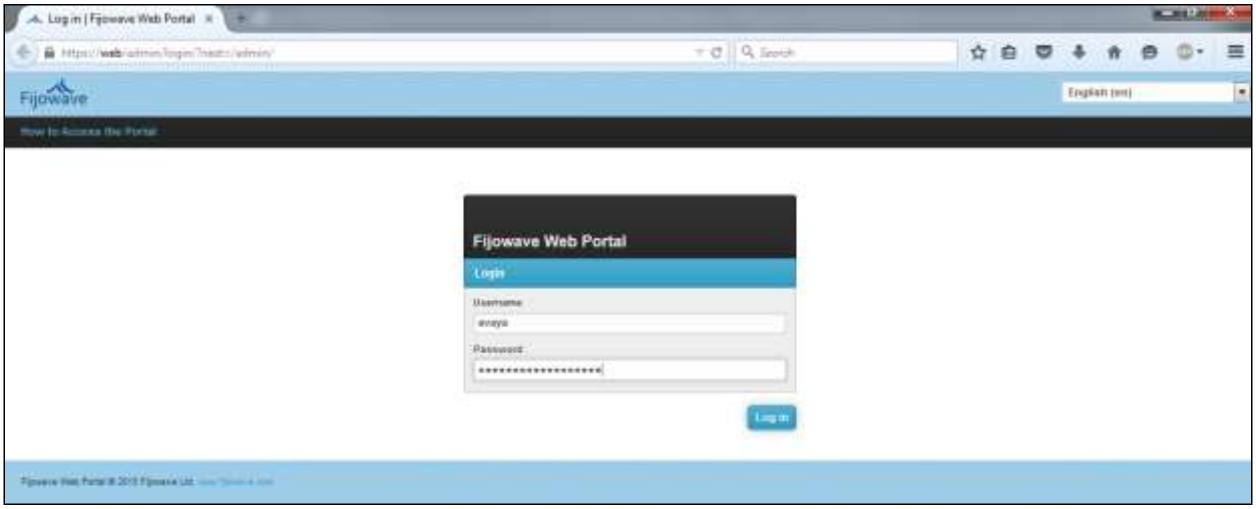
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

The following web page then opens, enter the correct credentials and click on **Log in**.


Log in | Fijowave Web Portal
https://web/admin/login/?next=/admin/
Search
Fijowave
English (en)
How to Access the Portal
Log in
Fijowave Web Portal © 2015 Fijowave Ltd.

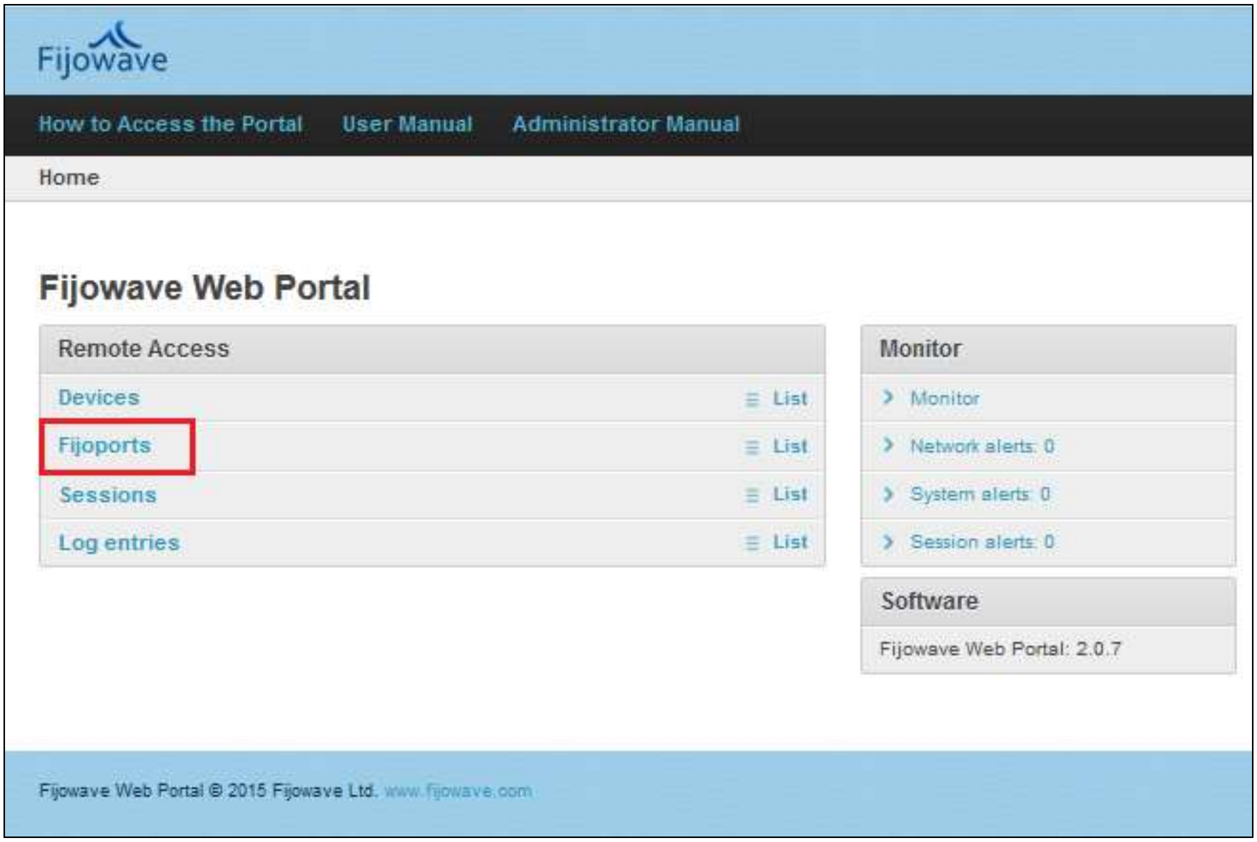
Fijowave Web Portal

Login

Username: avaya

Password: •••••••••••••••••••

Click on **Fijoports**, as highlighted below.



Fijowave

How to Access the Portal | User Manual | Administrator Manual

Home

Fijowave Web Portal

Remote Access	
Devices	≡ List
Fijoports	≡ List
Sessions	≡ List
Log entries	≡ List

Monitor

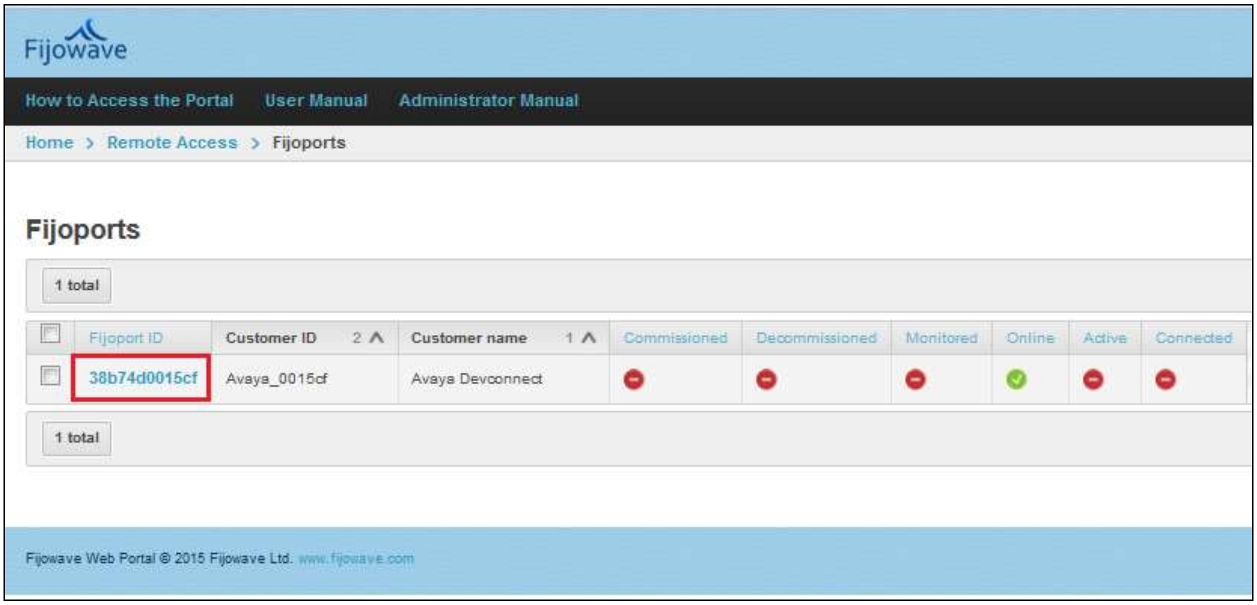
- Monitor
- Network alerts: 0
- System alerts: 0
- Session alerts: 0

Software

Fijowave Web Portal: 2.0.7

Fijowave Web Portal © 2015 Fijowave Ltd. www.fijowave.com

During compliance testing only one Fijoport was used as shown below, click on that to continue. On sites where many Fijoports are in use, click on the correct **Fijoport ID**.



Fijowave

How to Access the Portal | User Manual | Administrator Manual

Home > Remote Access > Fijoports

Fijoports

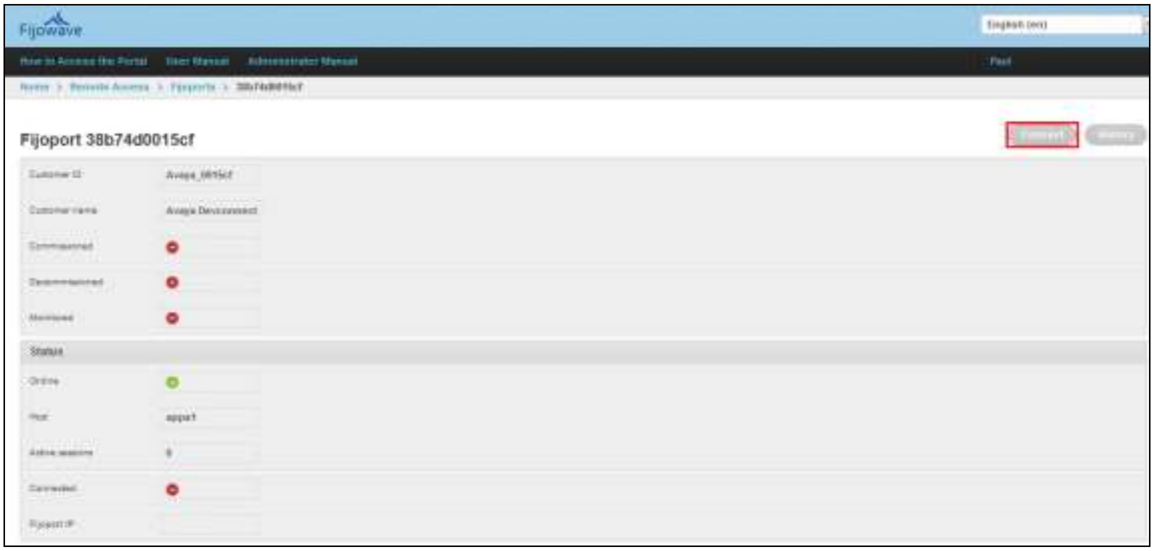
1 total

□	Fijoport ID	Customer ID 2 ^	Customer name 1 ^	Commissioned	Decommissioned	Monitored	Online	Active	Connected
□	38b74d0015cf	Avaya_0015cf	Avaya Devconnect	⊖	⊖	⊖	✓	⊖	⊖

1 total

Fijowave Web Portal © 2015 Fijowave Ltd. www.fijowave.com

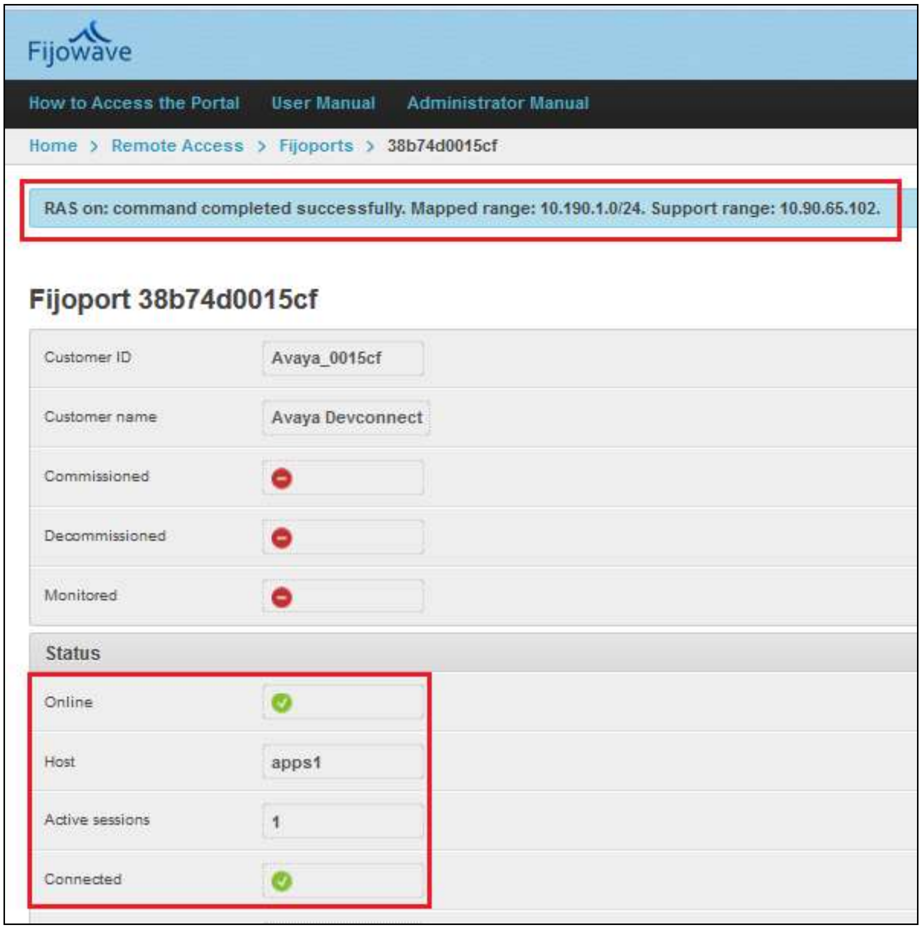
Click on **Connect** at the top right corner.



Fijoport 38b74d0015cf

Customer ID	Avaya_0015cf
Customer name	Avaya Devconnect
Commissioned	⊖
Decommissioned	⊖
Monitored	⊖
Status	
Online	✓
Host	apps1
Active sessions	0
Connected	⊖
Fijoport IP	

The message displayed at the top as well as the **Connected** status displayed at the bottom shows that the VPN as connected successfully.

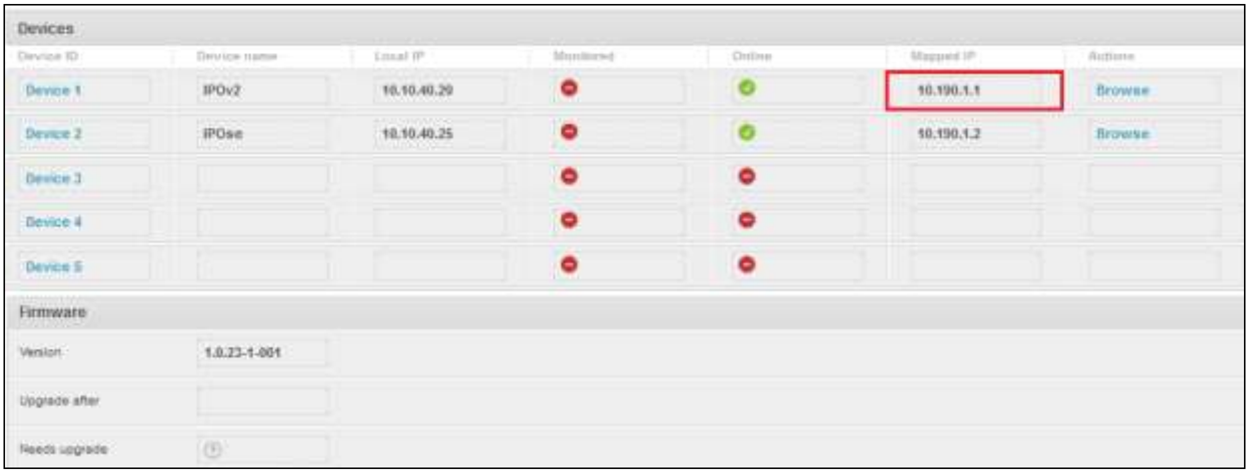


RAS on: command completed successfully. Mapped range: 10.190.1.0/24. Support range: 10.90.65.102.

Fijoport 38b74d0015cf

Customer ID	Avaya_0015cf
Customer name	Avaya Devconnect
Commissioned	⊖
Decommissioned	⊖
Monitored	⊖
Status	
Online	✓
Host	apps1
Active sessions	1
Connected	✓

The Mapped IP is very important as this is the IP Address of the IP Office as far as the remote access is concerned. When opening IP Office Manager, Monitor or System Status this is the IP address that will be used, see **Section 7.3**.



Devices

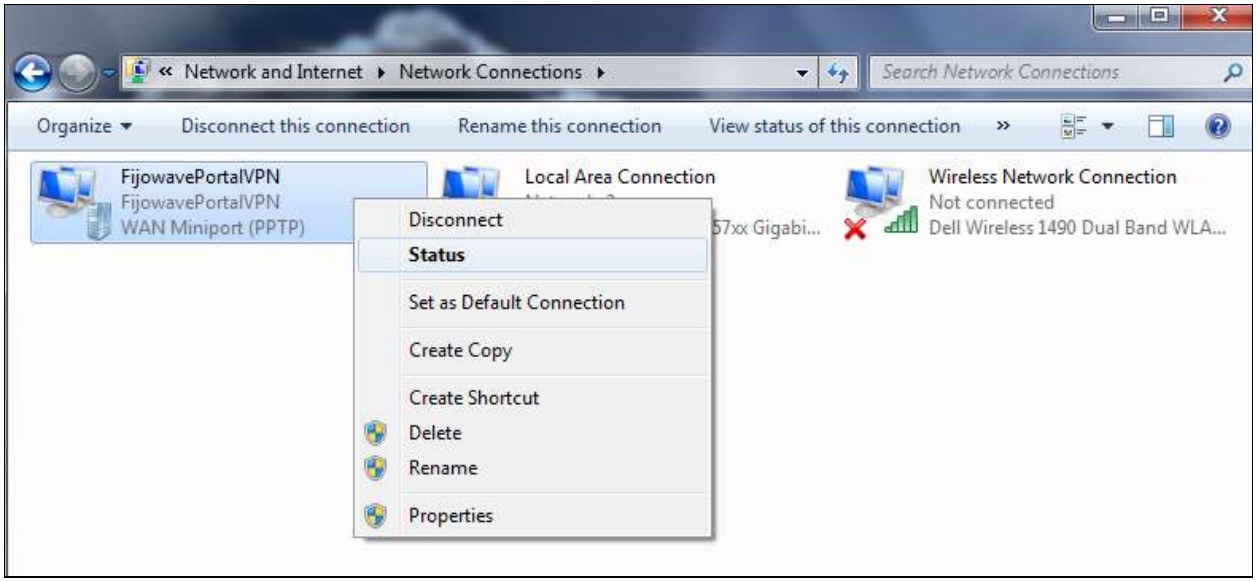
Device ID	Device name	Local IP	Monitored	Online	Mapped IP	Actions
Device 1	IPOv2	10.10.40.29	⊖	✓	10.190.1.1	Browse
Device 2	IPOse	10.10.40.25	⊖	✓	10.190.1.2	Browse
Device 3			⊖	⊖		
Device 4			⊖	⊖		
Device 5			⊖	⊖		

Firmware

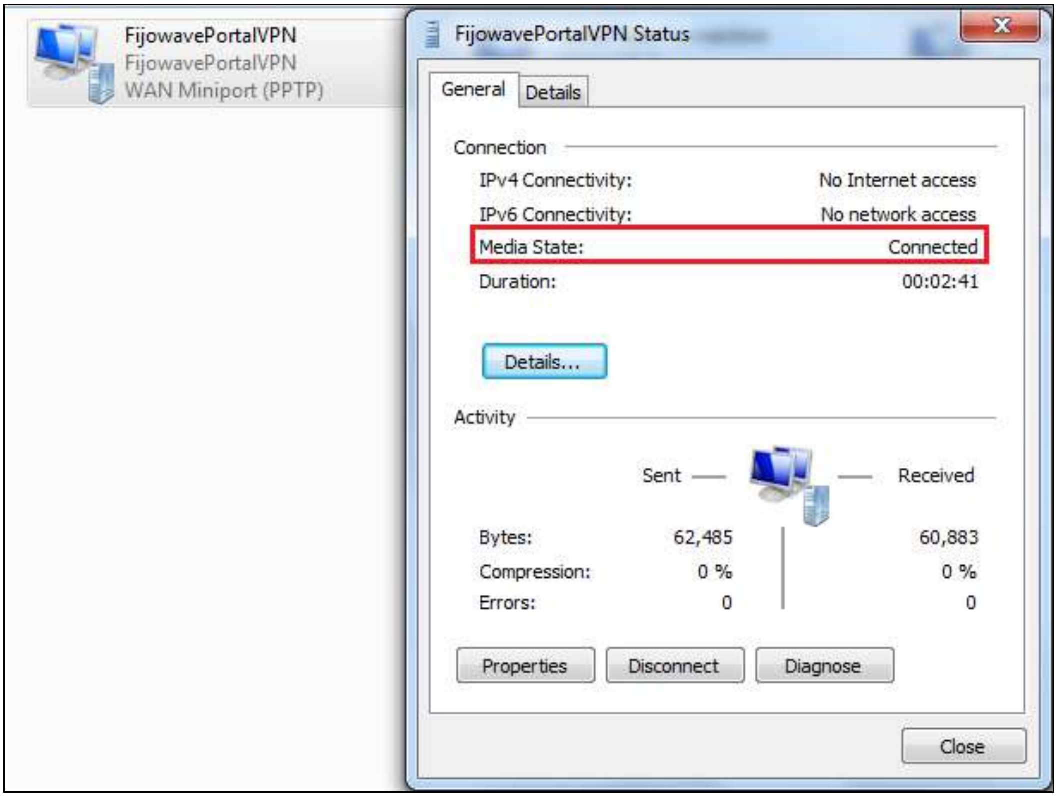
Version	1.0.23-1-001
Upgrade after	
Needs upgrade	?

7.2. Verify Fijowave Portal VPN is running

The **FijowavePortalVPN** connection will appear under Network Connections as shown below. Right click on this connection and select **Status**.


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disconnect this connection
Rename this connection
View status of this connection
»
FijowavePortalVPN
FijowavePortalVPN
WAN Miniport (PPTP)
Local Area Connection
57xx Gigabi...
Wireless Network Connection
Not connected
Dell Wireless 1490 Dual Band WLA...
Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties

The **Media State** should show up as **Connected** as shown below.



Connection

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No network access

Media State: Connected

Duration: 00:02:41

Activity

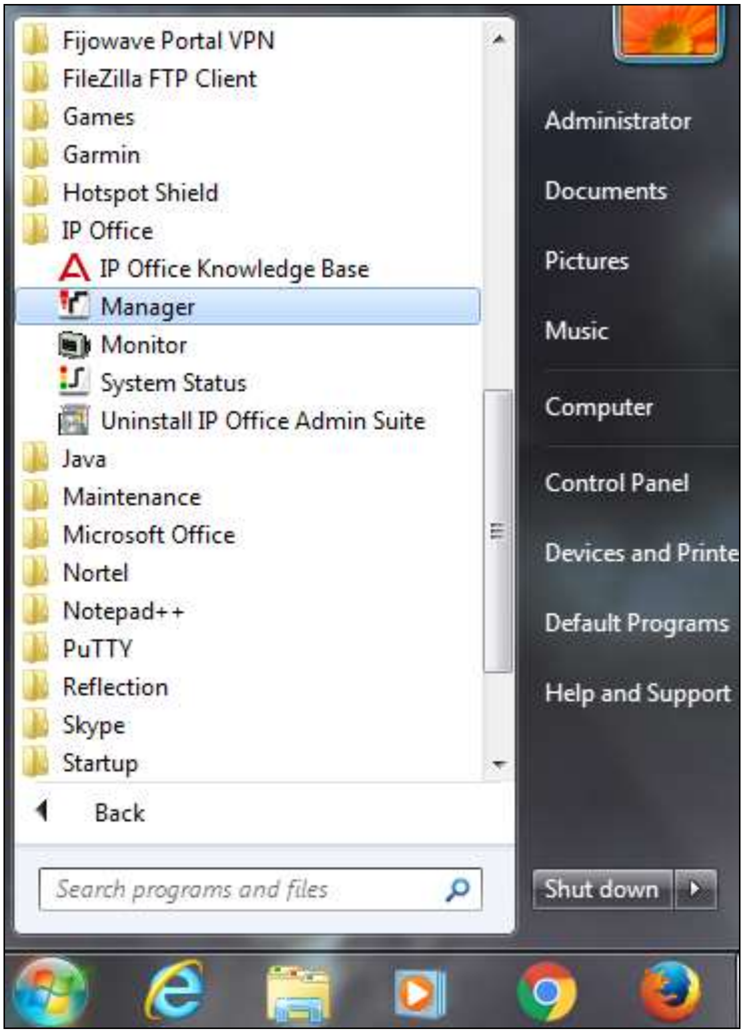
	Sent	Received
Bytes:	62,485	60,883
Compression:	0 %	0 %
Errors:	0	0

7.3. Verify IP Office Connections

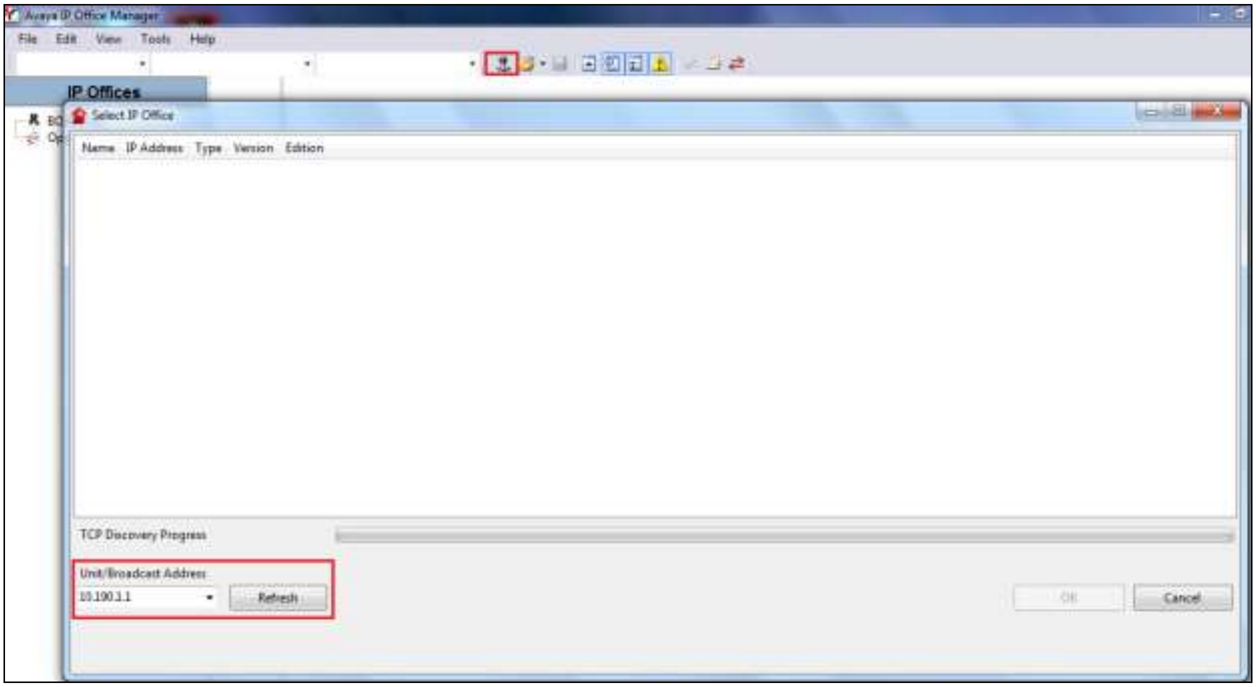
Once the VPN connection is established IP Office and all the monitoring tools should be accessible. To verify that Fijoport Remote Access is fully working, from the PC running the Fijowave Portal VPN, open the three IP Office applications, IP Office Manager, Monitor and System Status.

7.3.1. Verify IP Office Manager

Open the IP Office Manager either from the desktop shortcut or from **Programs → IP Office** as shown below.

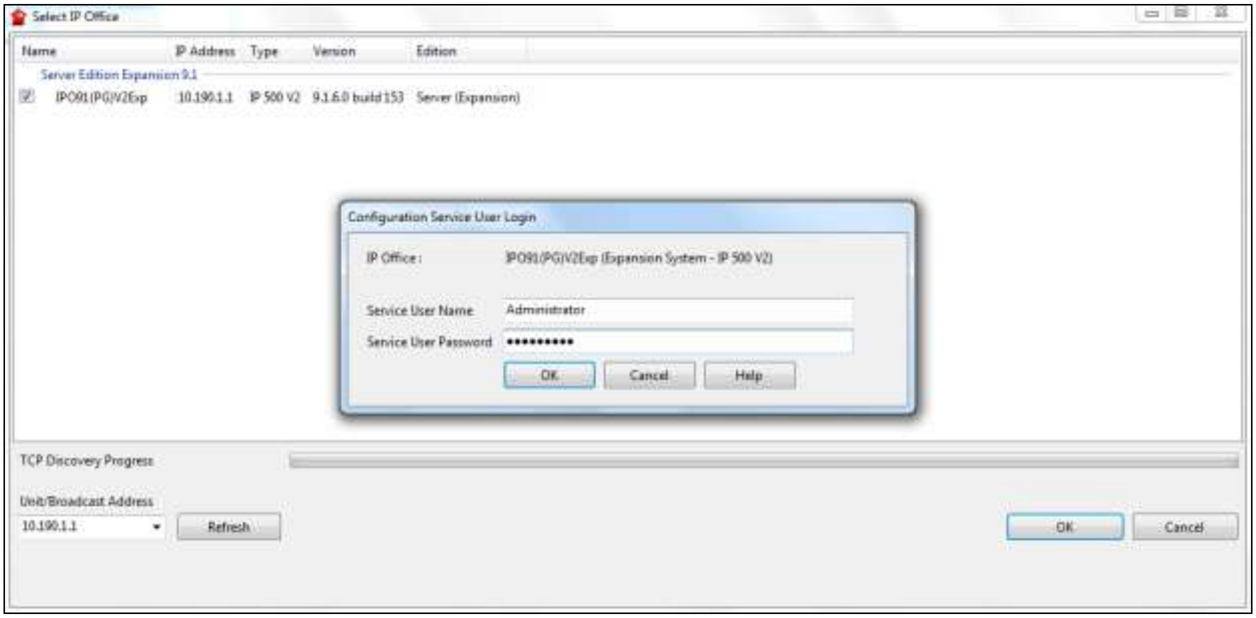


The **Unit Broadcast Address** will need to be set to that of the **Mapped IP** found in **Section 7.1**. The mapped IP address is entered and **Refresh** is pressed and that should bring up the IP Office unit.



Unit/Broadcast Address: 10.190.1.1

Select the IP Office unit and click on **OK** at the bottom of the screen and this will bring up another smaller window where the IP Office username and password are entered and again **OK** is pressed on the smaller window.

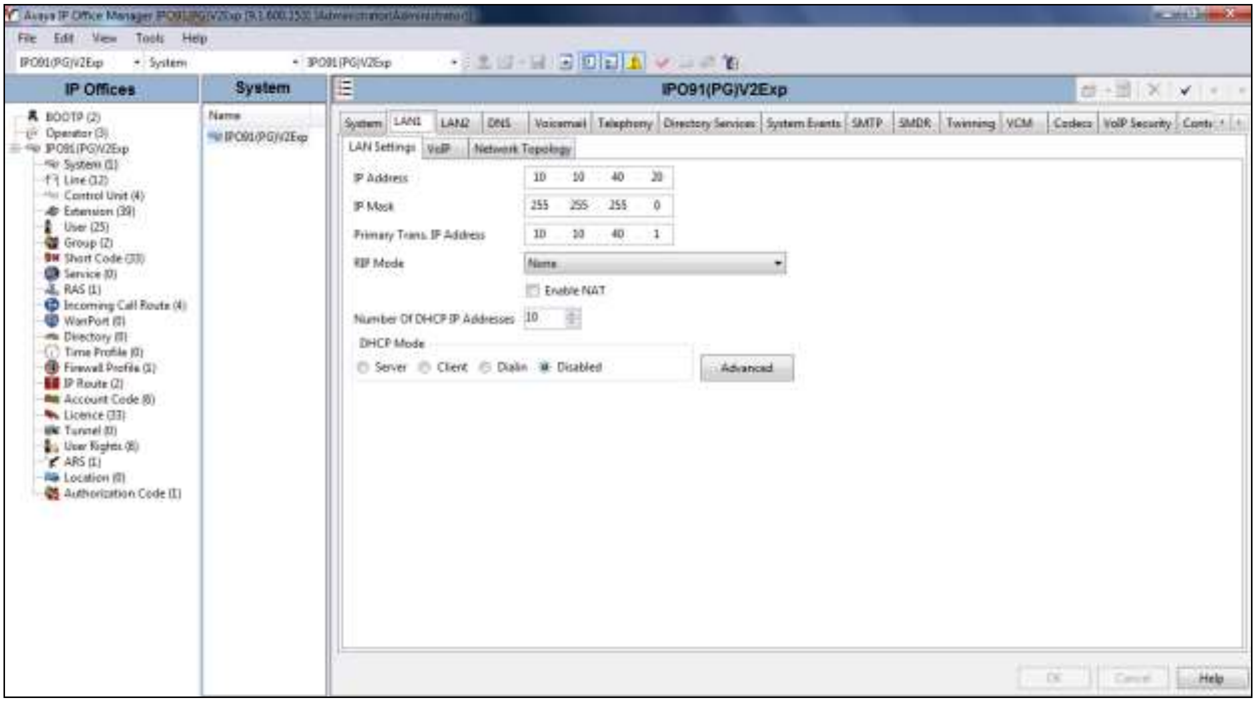


Name	IP Address	Type	Version	Edition
Server Edition Expansion 9.1				
☑ IPO91(PG)V2Exp	10.190.1.1	IP 500 V2	9.1.6.0 build 153	Server (Expansion)

IP Office: IPO91(PG)V2Exp (Expansion System - IP 500 V2)
Service User Name: Administrator
Service User Password: ••••••••••

Unit/Broadcast Address: 10.190.1.1

The IP Office Manager screen should be opened and should appear something like shown below where changed can be made and saved (not shown).



IP Address: 10 . 10 . 40 . 20

IP Mask: 255 . 255 . 255 . 0

Primary Trans. IP Address: 10 . 10 . 40 . 1

RIP Mode: None

□ Enable NAT

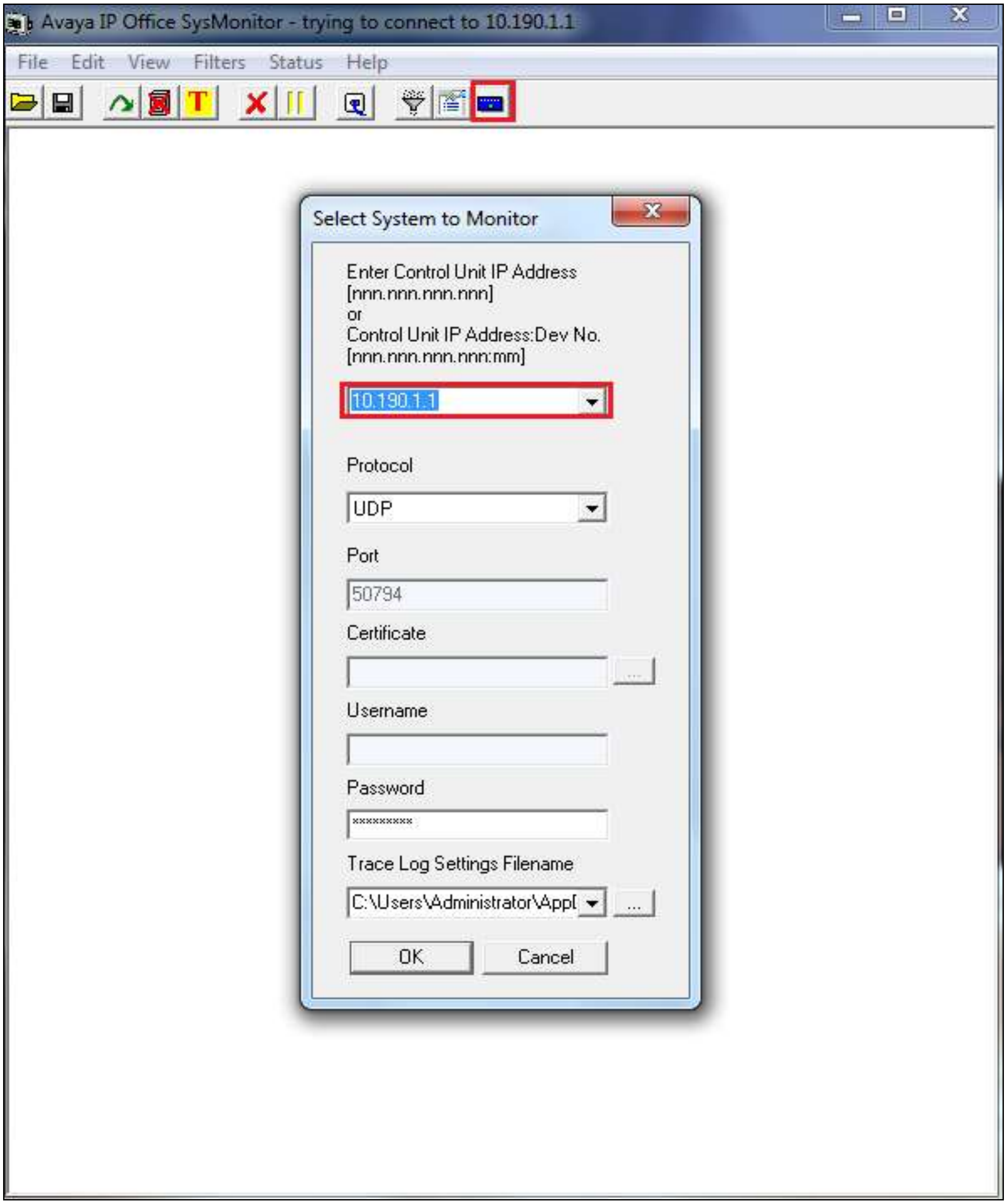
Number Of DHCP IP Addresses: 10

DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

7.3.2. Verify IP Office Monitor

IP Office Monitor is accessed in the same was as IP Office Manager is from **Section 7.3.1**. Once opened the connection information must be changed to reflect the mapped IP address instead of the real IP Office address.

Click on the connection icon highlighted at the top of the screen and enter the mapped IP address for the IP Office as per **Section 7.1**. Click on OK and the monitor should start correctly.



Avaya IP Office SysMonitor - trying to connect to 10.190.1.1

Select System to Monitor

Enter Control Unit IP Address [nnn.nnn.nnn.nnn] or Control Unit IP Address:Dev No. [nnn.nnn.nnn.nnn:mm]

10.190.1.1

Protocol: UDP

Port: 50794

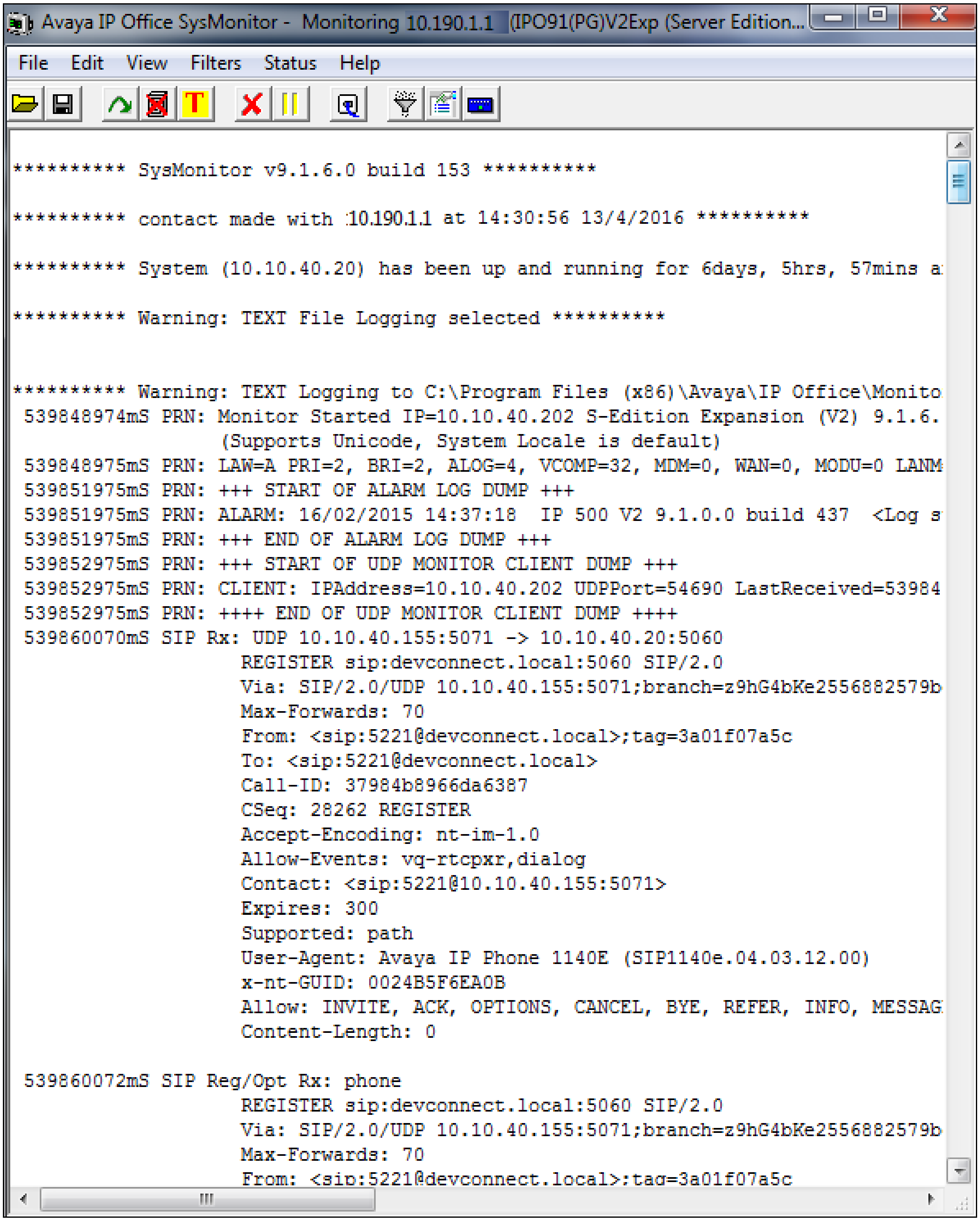
Certificate:

Username:

Password: **********

Trace Log Settings Filename: C:\Users\Administrator\AppI

The monitor should now display information on IP Office correctly.

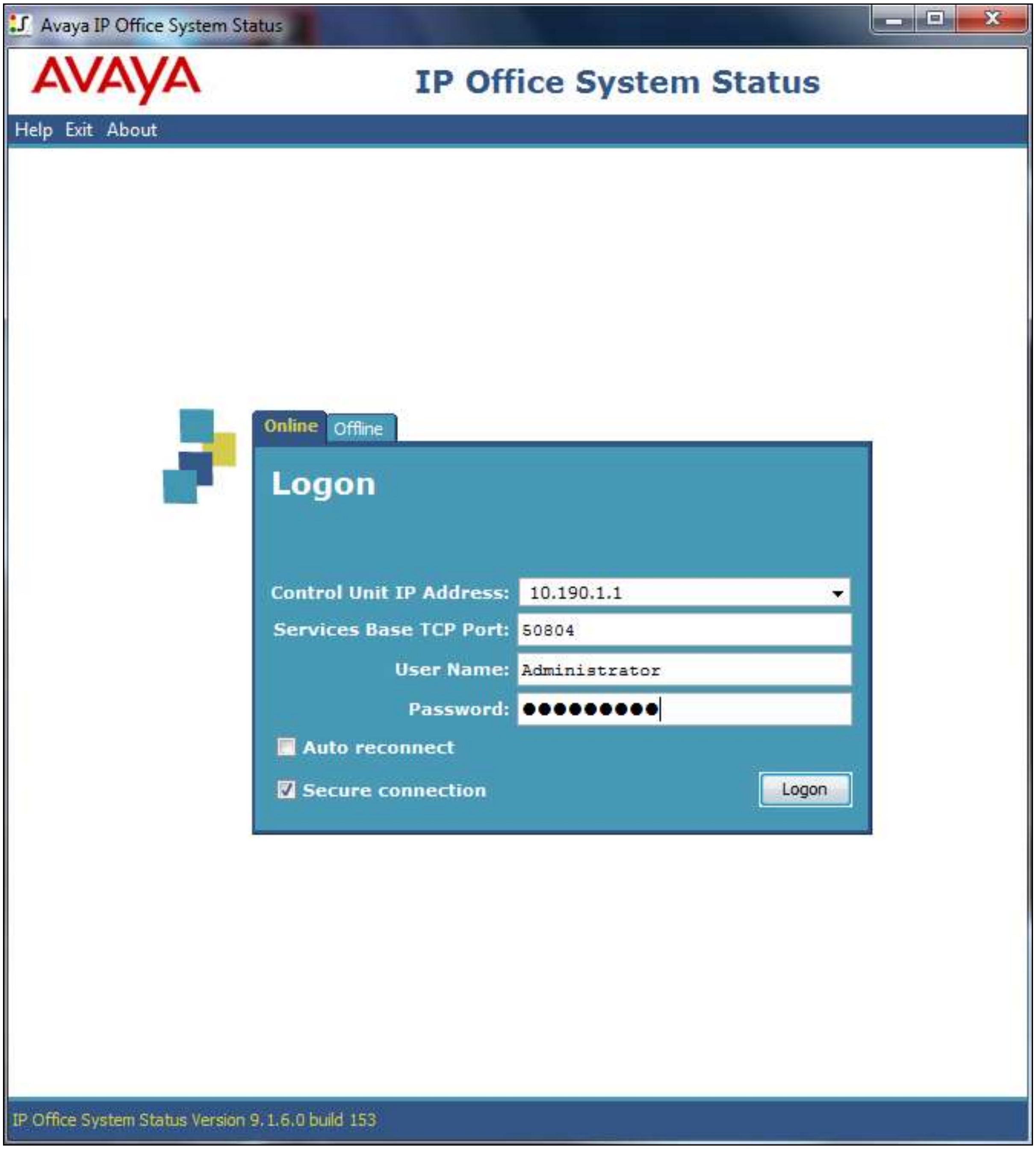

Avaya IP Office SysMonitor - Monitoring 10.190.1.1 (IPO91(PG)V2Exp (Server Edition...
File
Edit
View
Filters
Status
Help

```
********** SysMonitor v9.1.6.0 build 153 **********

********** contact made with 10.190.1.1 at 14:30:56 13/4/2016 **********

********** System (10.10.40.20) has been up and running for 6days, 5hrs, 57mins a

********** Warning: TEXT File Logging selected **********


********** Warning: TEXT Logging to C:\Program Files (x86)\Avaya\IP Office\Monito
 539848974mS PRN: Monitor Started IP=10.10.40.202 S-Edition Expansion (V2) 9.1.6.
                  (Supports Unicode, System Locale is default)
 539848975mS PRN: LAW=A PRI=2, BRI=2, ALOG=4, VCOMP=32, MDM=0, WAN=0, MODU=0 LANM
 539851975mS PRN: +++ START OF ALARM LOG DUMP +++
 539851975mS PRN: ALARM: 16/02/2015 14:37:18  IP 500 V2 9.1.0.0 build 437  <Log s
 539851975mS PRN: +++ END OF ALARM LOG DUMP +++
 539852975mS PRN: +++ START OF UDP MONITOR CLIENT DUMP +++
 539852975mS PRN: CLIENT: IPAddress=10.10.40.202 UDPPort=54690 LastReceived=53984
 539852975mS PRN: ++++ END OF UDP MONITOR CLIENT DUMP ++++
 539860070mS SIP Rx: UDP 10.10.40.155:5071 -> 10.10.40.20:5060
                    REGISTER sip:devconnect.local:5060 SIP/2.0
                    Via: SIP/2.0/UDP 10.10.40.155:5071;branch=z9hG4bKe2556882579b
                    Max-Forwards: 70
                    From: <sip:5221@devconnect.local>;tag=3a01f07a5c
                    To: <sip:5221@devconnect.local>
                    Call-ID: 37984b8966da6387
                    CSeq: 28262 REGISTER
                    Accept-Encoding: nt-im-1.0
                    Allow-Events: vq-rtcpxr,dialog
                    Contact: <sip:5221@10.10.40.155:5071>
                    Expires: 300
                    Supported: path
                    User-Agent: Avaya IP Phone 1140E (SIP1140e.04.03.12.00)
                    x-nt-GUID: 0024B5F6EA0B
                    Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, REFER, INFO, MESSAG
                    Content-Length: 0

 539860072mS SIP Reg/Opt Rx: phone
                    REGISTER sip:devconnect.local:5060 SIP/2.0
                    Via: SIP/2.0/UDP 10.10.40.155:5071;branch=z9hG4bKe2556882579b
                    Max-Forwards: 70
                    From: <sip:5221@devconnect.local>;tag=3a01f07a5c
```

7.3.3. Verify IP Office System Status

IP Office System Status is accessed in the same was as IP Office Manager is from **Section 7.3.1**. Once opened the connection information must be changed to reflect the mapped IP address instead of the real IP Office address.

Enter the mapped IP address for the IP Office as per **Section 7.1**, enter the log in credentials and click on **Logon** and the monitor should start correctly.


Avaya IP Office System Status
AVAYA
IP Office System Status
Help
Exit
About
Online
Offline
Logon
Logon
IP Office System Status Version 9.1.6.0 build 153

Control Unit IP Address: 10.190.1.1

Services Base TCP Port: 50804

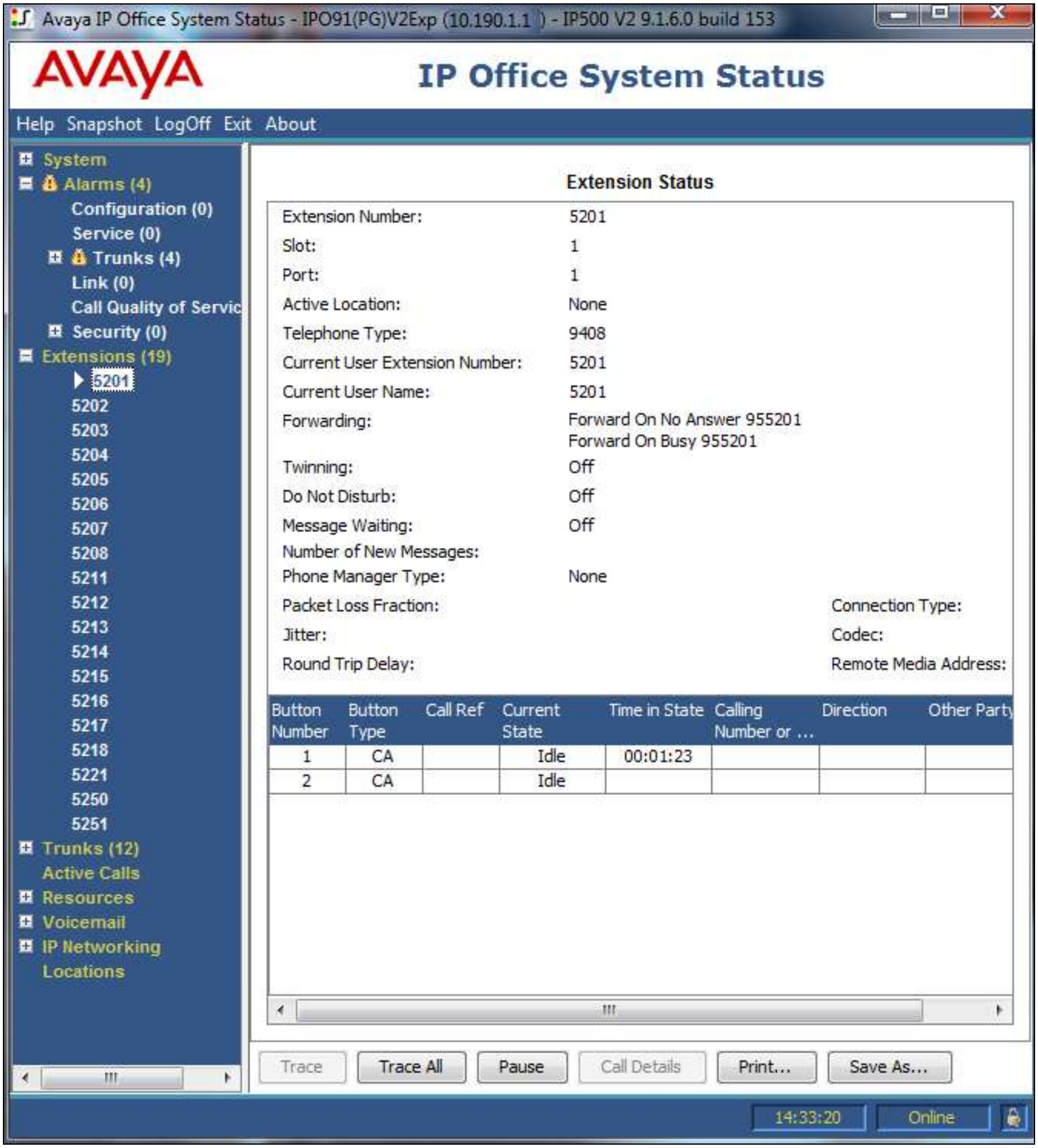
User Name: Administrator

Password: ●●●●●●●●●

□ Auto reconnect

☑ Secure connection

The IP Office System Status should open correctly and display the correct IP Office information as shown below.



Extension Status

Extension Number: 5201
Slot: 1
Port: 1
Active Location: None
Telephone Type: 9408
Current User Extension Number: 5201
Current User Name: 5201
Forwarding: Forward On No Answer 955201
Forward On Busy 955201
Twinning: Off
Do Not Disturb: Off
Message Waiting: Off
Number of New Messages:
Phone Manager Type: None
Packet Loss Fraction:
Jitter:
Round Trip Delay:
Connection Type:
Codec:
Remote Media Address:

Button Number	Button Type	Call Ref	Current State	Time in State	Calling Number or ...	Direction	Other Party
1	CA		Idle	00:01:23			
2	CA		Idle				

8. Conclusion

These Application Notes describe the configuration steps required for provisioning Fijowave's Fijoport Remote Access to interoperate with Avaya IP Office 500 V2 R9.1. It has been verified that the Fijoport solution interoperates with IP Office Manager, IP Office Monitor tool and IP Office System Status tools. Please refer to **Section 2.2** for test results and observations.

9. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com where the following documents can be obtained.
Product documentation for Avaya products may be found at http://support.avaya.com.

[1] Avaya IP Office R9.1 Manager 10.1, Document Number 15-601011
[2] Avaya IP Office R9.1 Doc library

Technical support for the Fijowave Fijoport Remote Access product can be obtained as follows:

- Web: http://www.fijowave.com
- Email: support@fijowave.com
- Help desk: +353 1 525 3072

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.