



## **Application Notes for configuring Fijowave Fijoport Remote Access with Avaya IP Office Server Edition R11– Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps for provisioning Fijowave’s Fijoport Remote Access to access Avaya IP Office R11.0.

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.

**Note:** The Avaya IP Office solution consists of a primary server and an IP500V2 expansion. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and user's names. This allows calls between systems and support for a range of internal call features.

Fijoport Remote Access (Fijoport) is used as both a monitoring service and a remote access device with Avaya IP Office. The Fijowave solution consists of 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 OpenVPN.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Fijoport to be used as a remote access device for IP Office. Some definitions used to describe the connection are as follows.

- VPN - Virtual Private Network
- RAS - Remote Access Session
- CSE - Customer Support Engineer
- SSH – Secure Shell
- TLS – Transport layer Security
- AES – Advanced Encryption Standard
- 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 OpenVPN and is secured using TLS. 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Fijoport included the use of SSH, TLS and AES used by Fijowave to setup a secure tunnel to IP Office.

## 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. IP Office Manager "Broadcast Discovery" cannot be used with the VPN. The IP address must be used to discover the IP Office and this IP address is the mapped IP address provided by the Fijoport device.
2. When the remote access to IP Office is established using the Fijoport, the IP Office can be accessed using IP Office Manager, this connection allows the configuration to be displayed from one IP Office server at a time.

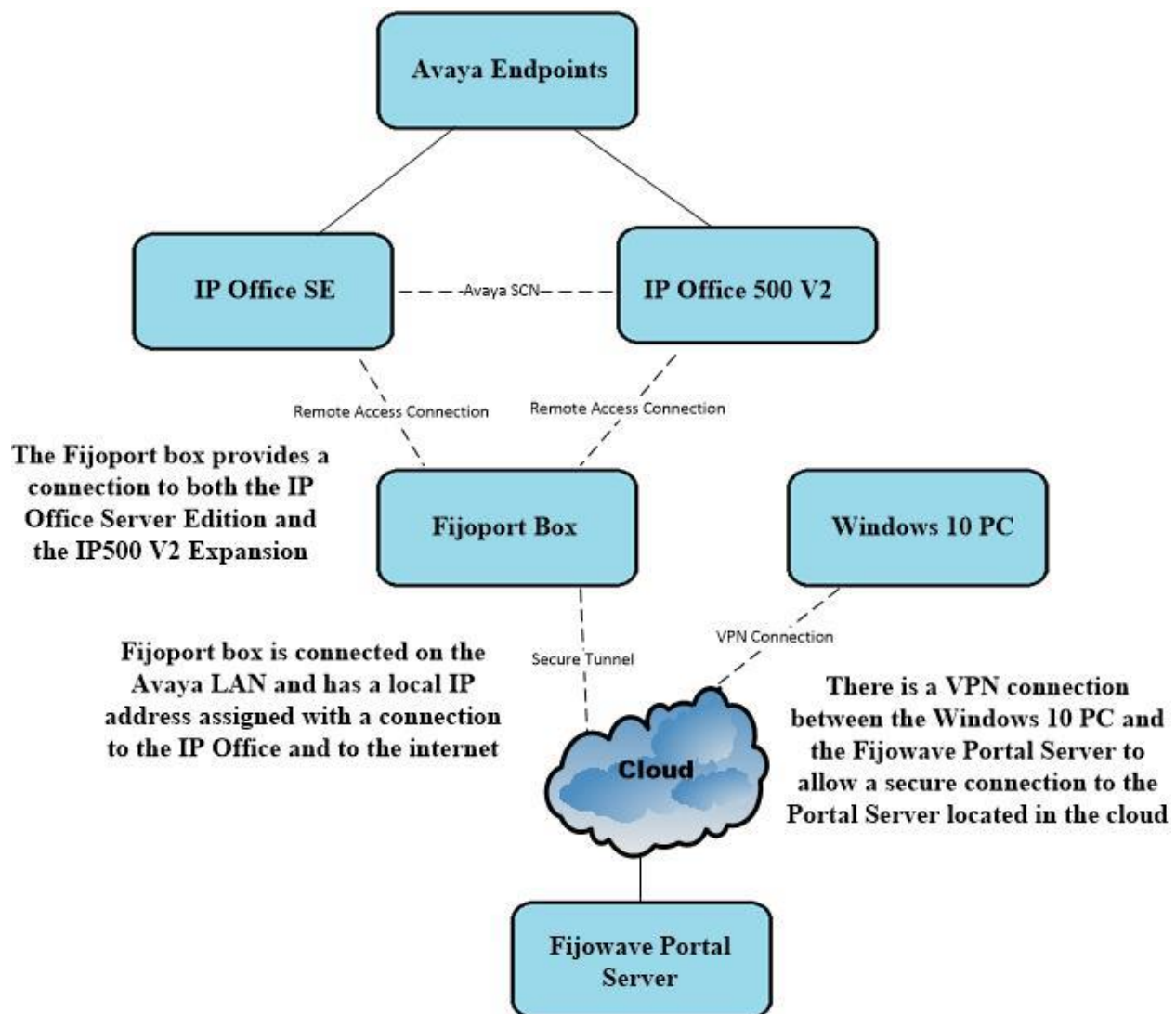
## 2.3. Support

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](mailto:support@fijowave.com)
- Help desk: +353 1 525 3072

### 3. Reference Configuration

**Figure 1** shows the network topology during compliance testing. Fijoport Remote Access provides a remote service platform solution that allows the user to remotely maintain products on their customer's premises 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 were used for the compliance test.

Equipment/Software	Version/Release
Avaya IP Office Server Edition running on a virtual platform	R11.0.4.2.0 Build 58
Avaya IP Office IP500 V2	R11.0.4.2.0 Build 58
Avaya 1140e Deskphone	SIP R04.04.23.00
Avaya 96x1 Deskphone	H.323 Release 6.6.115
Avaya 1608-I Deskphone	H.323 1608UA1_350B.bin
Avaya 9508 Digital Deskphone	V60
Fijowave Fijoport Box	V1.1
Fijowave Portal VPN	V2.2
Fijowave Portal Server	V3.5

**Note:** Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

## 5. Configure Avaya IP Office

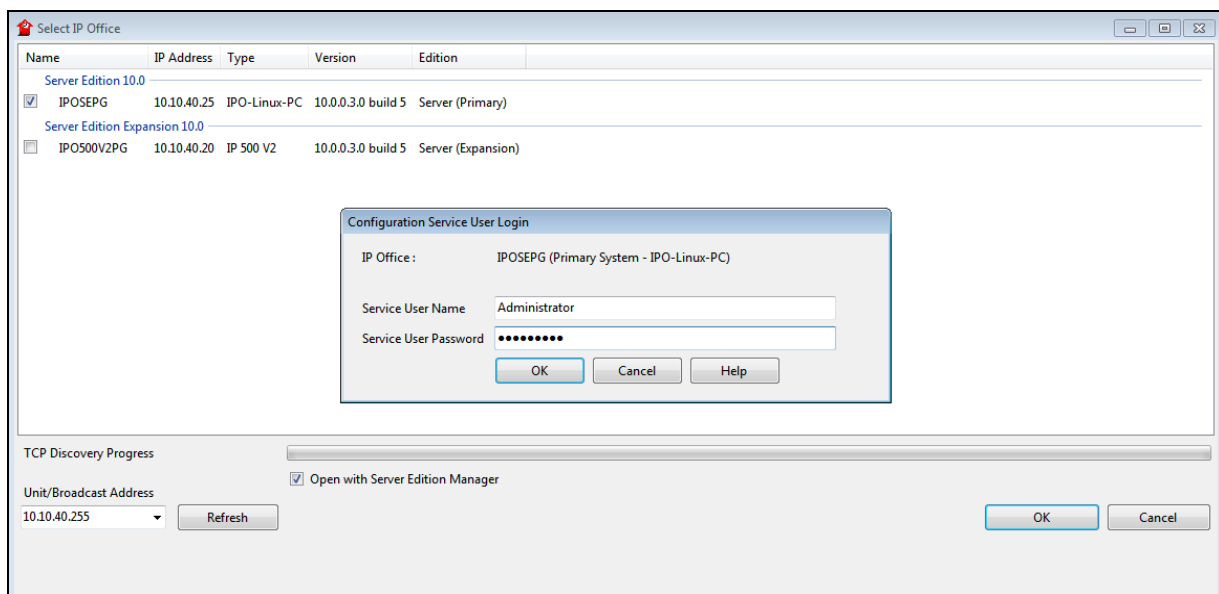
There is no specific configuration of IP Office required for the compliance testing of Fijoport Remote Access. The IP address of the IP Office is required in order to configure the Fijoport box in **Section 6.2**. Configuration and verification operations on the Avaya IP Office illustrated in this section 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.

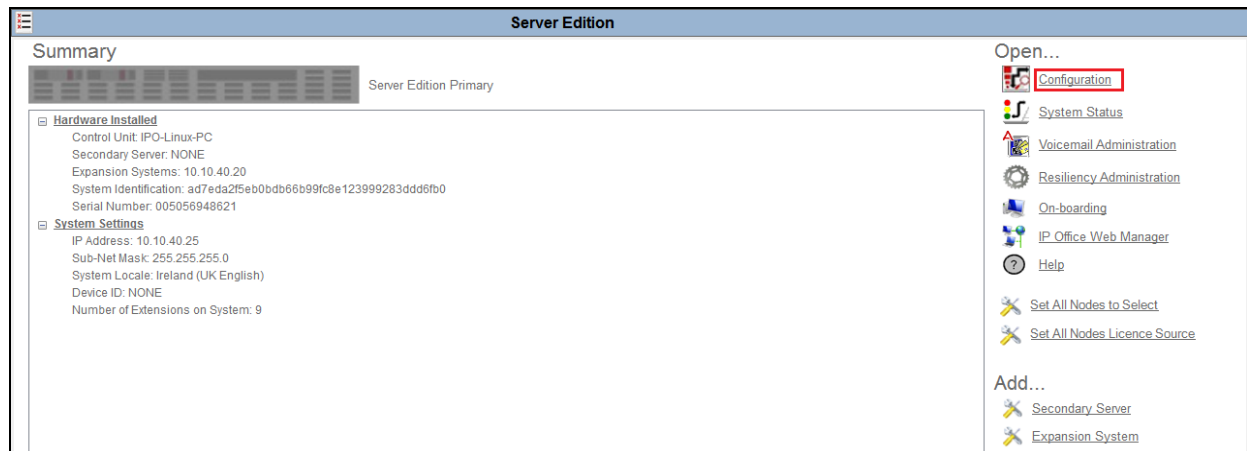
**Note:** The example below shows the IP address information for the Server Edition only, however both the Server Edition and the IP500V2 IP information must be acquired to setup a connection to both.

### 5.1. Launch Avaya IP Office Manager

From the IP Office Manager PC, click **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application (not shown). Select the required Server Edition as shown below and enter the appropriate credentials. Click on the **OK** button.

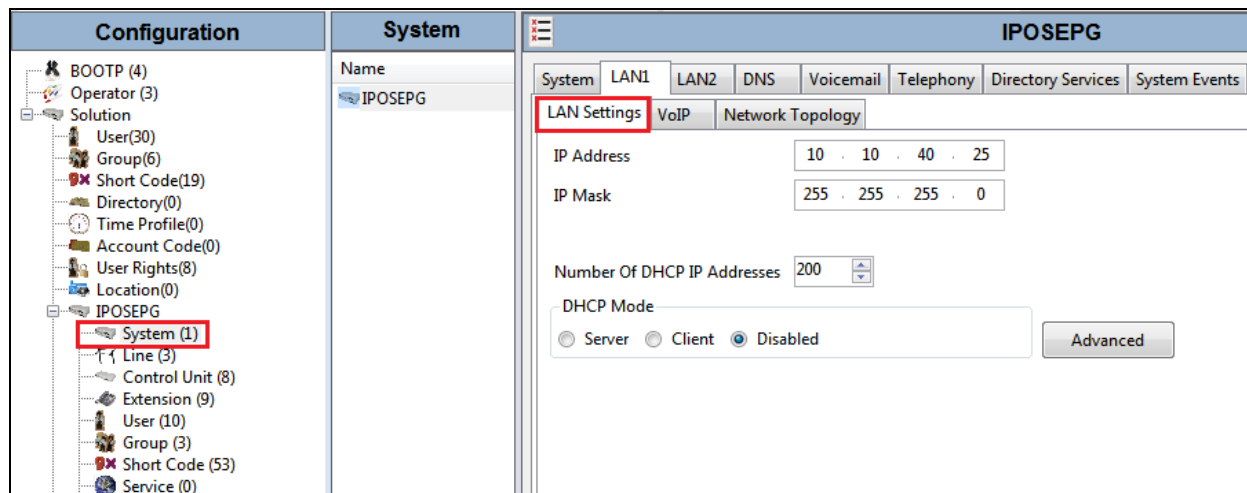


Click on **Configuration** at the top right of the page, as shown, to receive the IP Office configuration.



## 5.2. Display LAN Properties

From the left window navigate to **System** as shown and in the main window click on the **LAN1** tab and within that tab select the **LAN Settings** tab. The **IP Address** of the IP Office is shown, and this will be required for setup in **Section 6.2**.

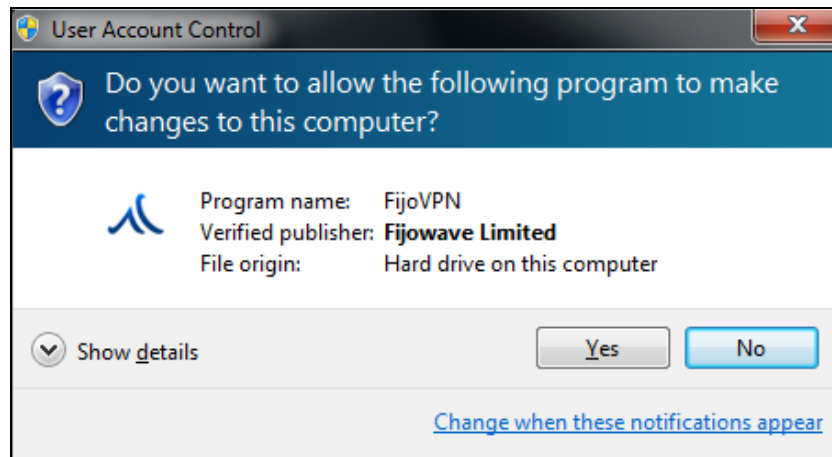


## 6. Configure Fijowave Fijoport Remote Access

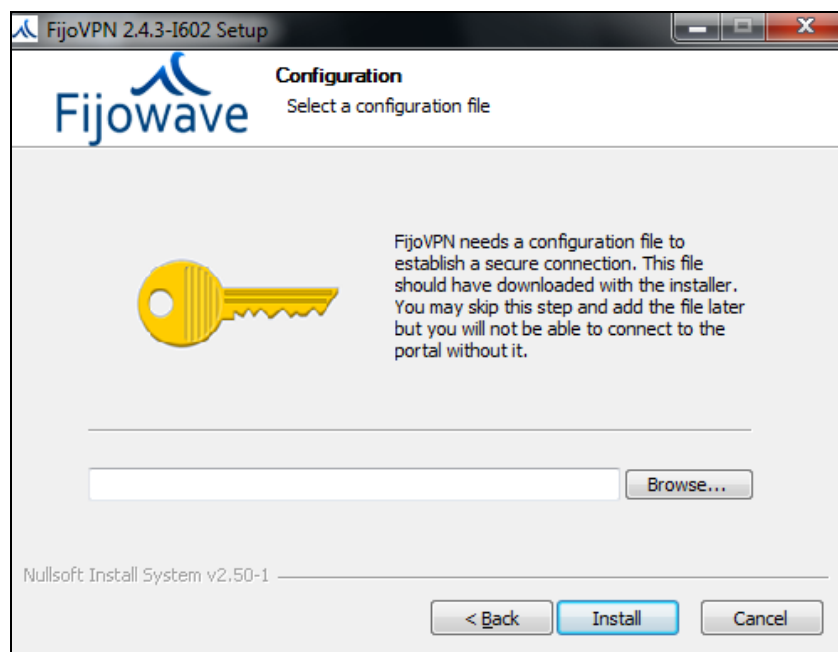
The configuration of the Fijoport Remote Access includes the installation and configuration of the Fijoport Portal VPN. Fijowave provides a username and password for the Fijoport Portal VPN in order to ensure connectivity to the Fijoport Portal Server. This username and password are required during the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

### 6.1. Install Fijowave Portal VPN

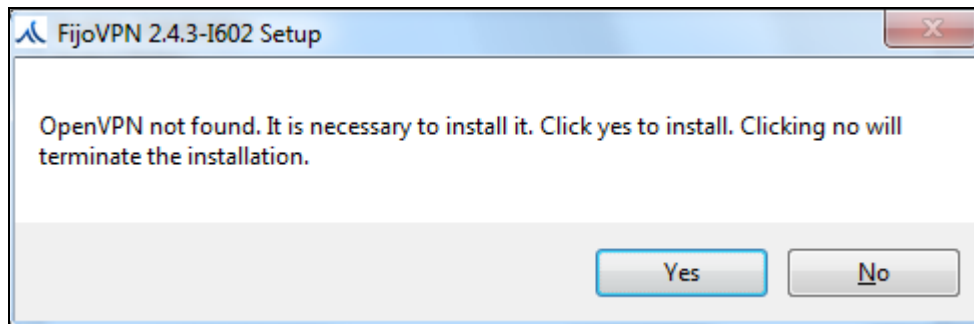
Unpack the contents of the RAR file, FijowavePortalServer2.2.rar, browse to the Fijowave Portal VPN directory and run the installer FijoVPN-2.x.x-xxxx.exe (not shown). Click **Yes** if User Account Control asks permission to proceed.



Browse and select the appropriate VPN configuration key file (not shown) and then click **Install**.



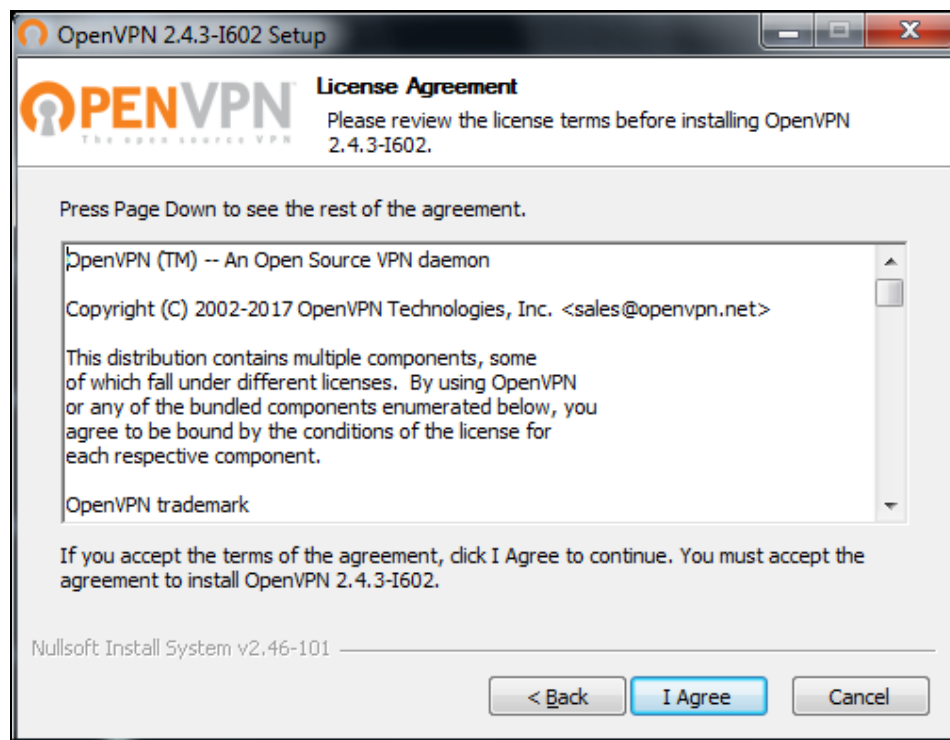
If OpenVPN is not already installed, then install it by clicking **Yes** and following the OpenVPN installation instructions.



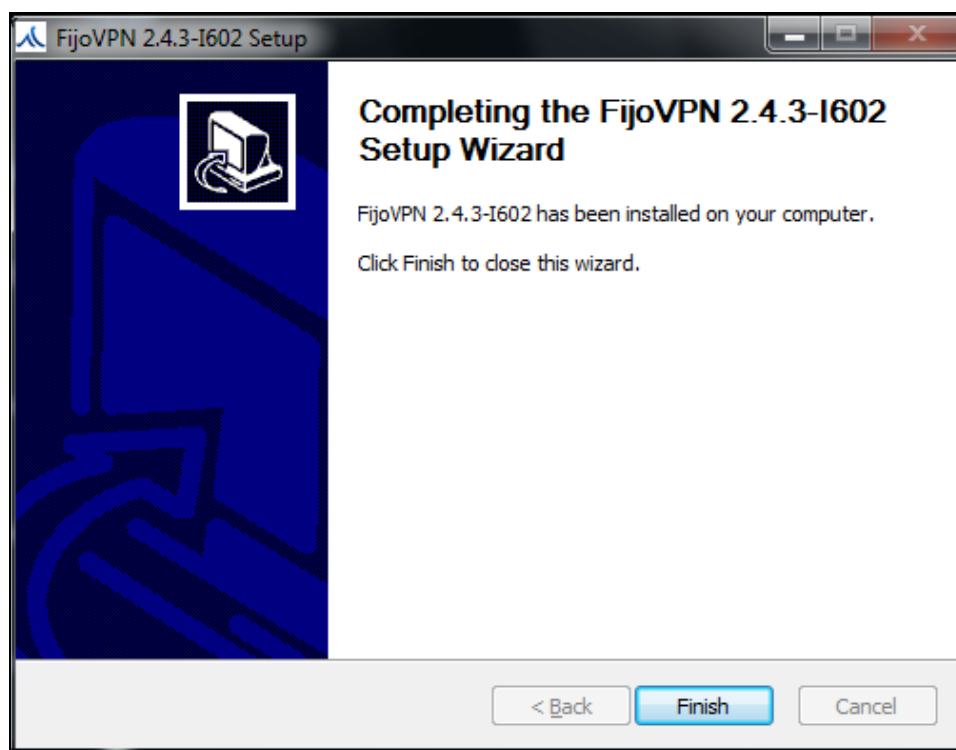
Click on **Next** to continue.



Click on **I Agree** to continue.



Close the installer by clicking **Finish**.



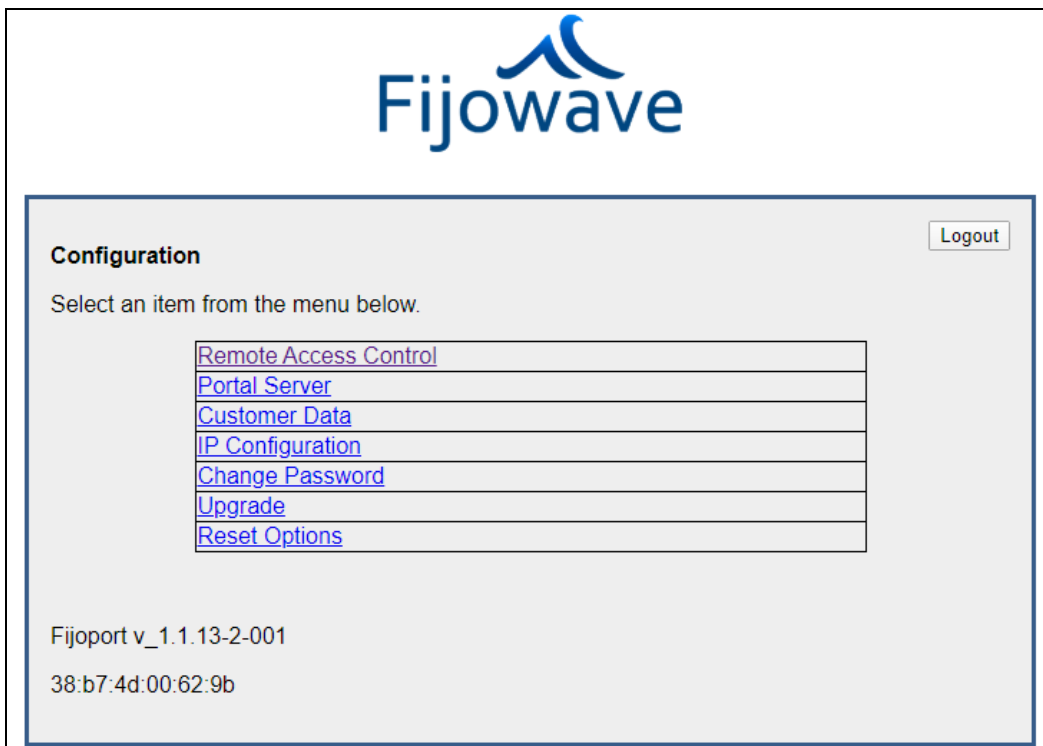
## 6.2. Configure Connection to IP Office

Open a URL to the Fijoport Box. Enter the appropriate credentials and click on **submit**.



The image shows the Fijowave login interface. At the top is the Fijowave logo. Below it is a light gray rectangular box containing the login form. The form has the title "Login" centered at the top. Below the title are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. Below these fields is a "submit" button. At the bottom of the page, outside the login box, is the text "Powered by Fijowave" and the website "www.fijowave.com".


Click on the **Remote Access Control** link.



The image shows the Fijowave configuration interface. At the top is the Fijowave logo. Below it is a light gray rectangular box containing the configuration menu. The menu has the title "Configuration" at the top left and a "Logout" button at the top right. Below the title is the instruction "Select an item from the menu below." followed by a table of links. The links are: "Remote Access Control", "Portal Server", "Customer Data", "IP Configuration", "Change Password", "Upgrade", and "Reset Options". At the bottom of the page, outside the configuration box, is the text "Fijoport v\_1.1.13-2-001" and the MAC address "38:b7:4d:00:62:9b".

<a href="#">Remote Access Control</a>
<a href="#">Portal Server</a>
<a href="#">Customer Data</a>
<a href="#">IP Configuration</a>
<a href="#">Change Password</a>
<a href="#">Upgrade</a>
<a href="#">Reset Options</a>

Enter the local IP address of the IP Office Server Edition for **ID 1** and the local IP address of the IP Office IP500 V2 for **ID 2** (if applicable). Press the **Save** button and then close the browser tab.



Logout

**Remote Access Control**

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

ID	Description	IP address	Device Type
1	Server Edition	10.10.40.25	Avaya IPO SE ▼
2	IP500V2	10.10.40.20	Avaya IPO 500 V2 ▼
3			▼
4			▼
5			▼
6			▼
7			▼
8			▼

Save Cancel

[Return to menu](#)

Powered by Fijowave

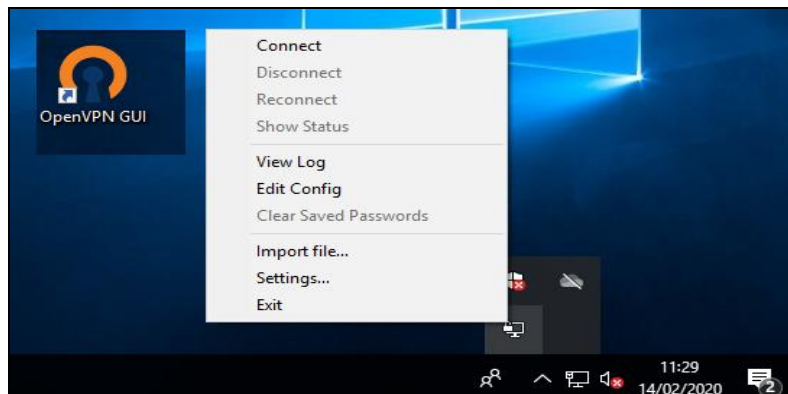
[www.fijowave.com](http://www.fijowave.com)

## 7. Verification Steps

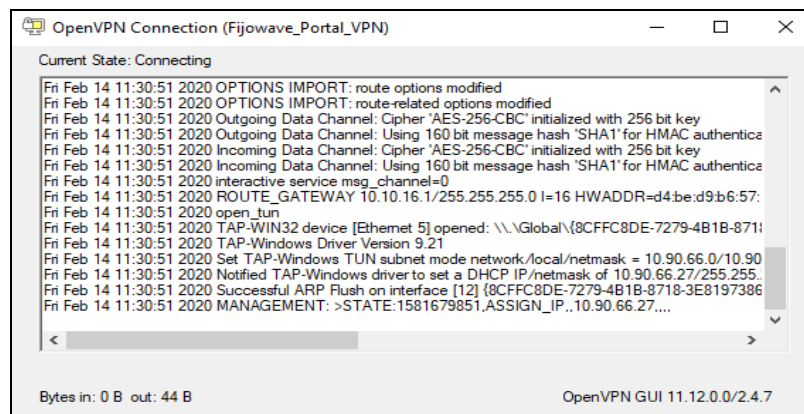
The following steps can be taken to ensure that connections between Fijowave Fijoport Remote Access and IP Office are up. The Fijowave Portal VPN is executed in order to setup the VPN connection. This connection can be verified, and the IP Office applications can be run.

### 7.1. Verify Fijowave Portal VPN

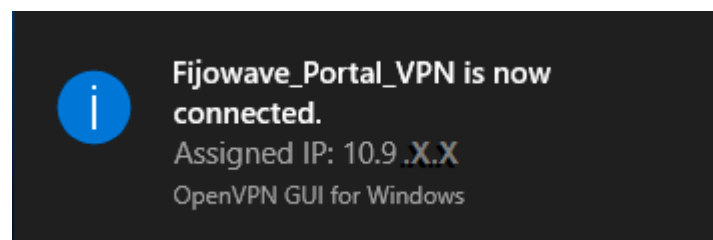
Start the VPN application by double-clicking on the shortcut. Once this is started it will appear in the system tray at the bottom right of the screen where it can be accessed and **Connect** is chosen.



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

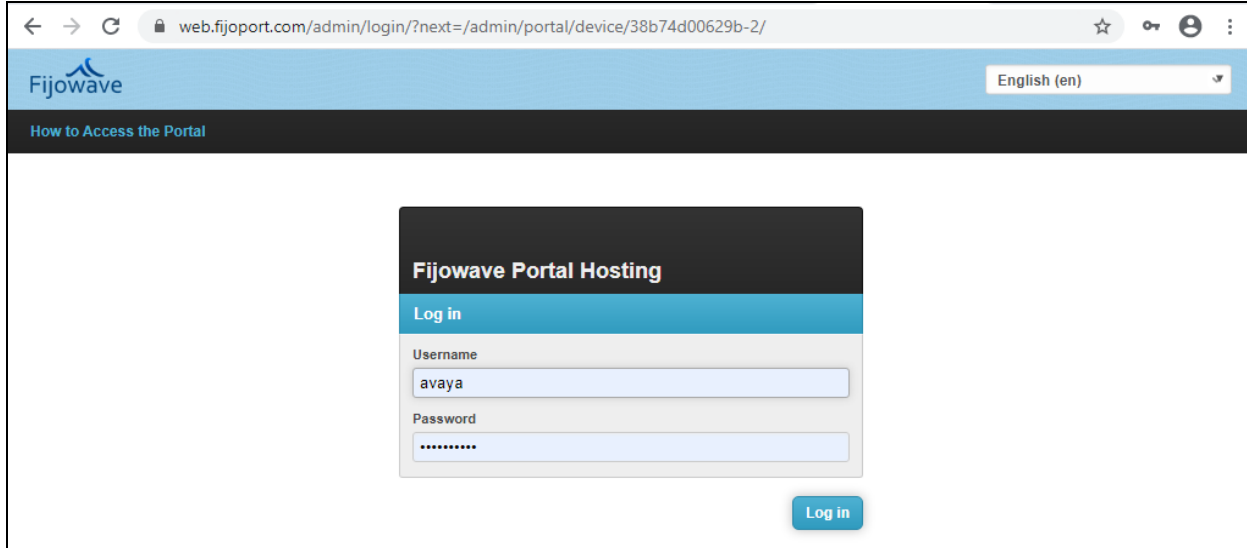


The following message verifies that the VPN is up and running and connected correctly.



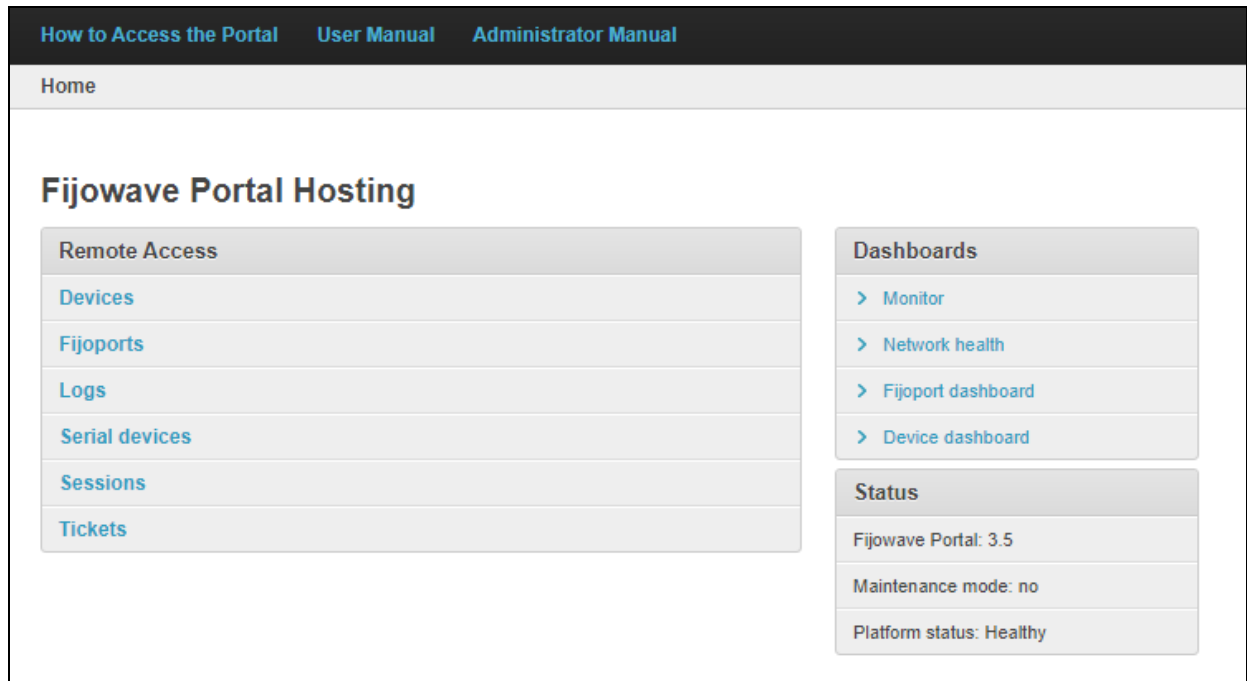
## 7.2. Verify connection to Fijoport

Open a URL to **web.fijoport.com** as shown below, enter the appropriate credentials and click on **Log in**.



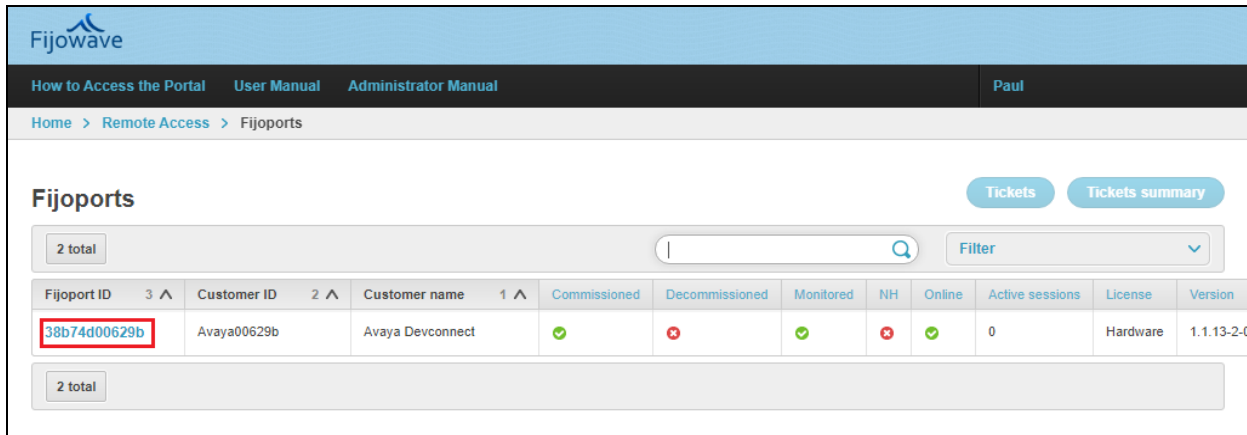
The screenshot shows a web browser window with the URL `web.fijoport.com/admin/login/?next=/admin/portal/device/38b74d00629b-2/`. The page features the Fijowave logo and a language dropdown set to "English (en)". A dark header bar contains the link "How to Access the Portal". The main content area displays a "Fijowave Portal Hosting" login form. The form includes a "Log in" header, a "Username" field with the value "avaya", a "Password" field with masked characters, and a "Log in" button.

Click on **Fijoports**.



The screenshot shows the Fijowave Portal Hosting dashboard. The top navigation bar includes links for "How to Access the Portal", "User Manual", and "Administrator Manual". Below the navigation bar is a "Home" section. The main content area is titled "Fijowave Portal Hosting" and is divided into three columns. The left column, "Remote Access", lists "Devices", "Fijoports", "Logs", "Serial devices", "Sessions", and "Tickets". The middle column, "Dashboards", lists "Monitor", "Network health", "Fijoport dashboard", and "Device dashboard". The right column, "Status", displays "Fijowave Portal: 3.5", "Maintenance mode: no", and "Platform status: Healthy".

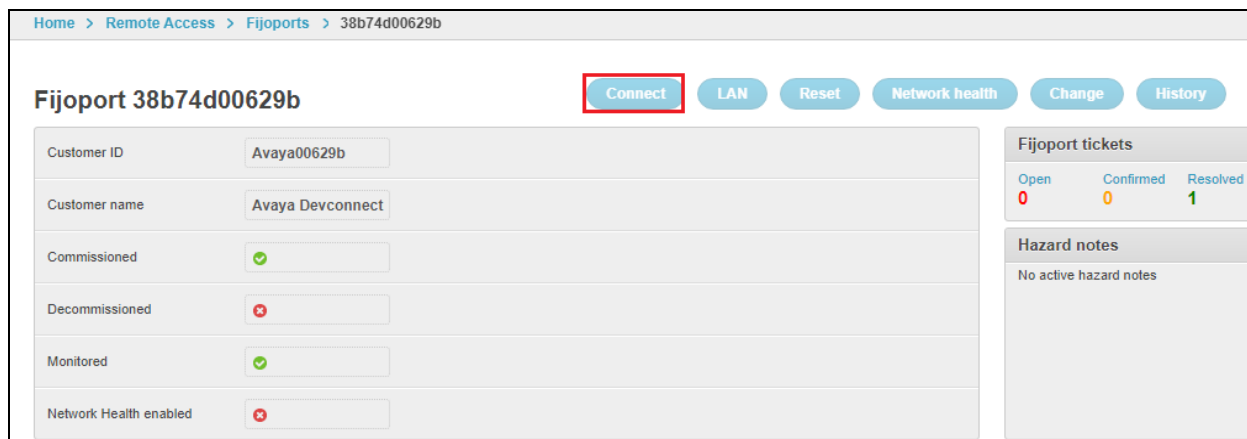
Click on the appropriate **Fijoport ID**. For compliance testing only one Fijoport was used, so there is only one choice displayed. On sites where many Fijoports are in use, click on the Fijoport ID to be accessed.



The screenshot shows the Fijowave portal interface. At the top, there's a navigation bar with links like 'How to Access the Portal', 'User Manual', and 'Administrator Manual'. Below this, a breadcrumb trail reads 'Home > Remote Access > Fijoports'. The main section is titled 'Fijoports' and includes a search bar and a 'Filter' dropdown. A table lists the available Fijoports. The first entry, with ID '38b74d00629b', is highlighted with a red box. The table columns include Fijoport ID, Customer ID, Customer name, Commissioned status, Decommissioned status, Monitored status, NH status, Online status, Active sessions, License, and Version.

Fijoport ID	Customer ID	Customer name	Commissioned	Decommissioned	Monitored	NH	Online	Active sessions	License	Version
38b74d00629b	Avaya00629b	Avaya Devconnect	✓	✗	✓	✗	✓	0	Hardware	1.1.13-2.0

Click on **Connect** at the top.



The screenshot shows the detailed view for Fijoport 38b74d00629b. At the top, there's a breadcrumb trail 'Home > Remote Access > Fijoports > 38b74d00629b'. The main section is titled 'Fijoport 38b74d00629b'. Below the title, there's a row of buttons: 'Connect', 'LAN', 'Reset', 'Network health', 'Change', and 'History'. The 'Connect' button is highlighted with a red box. Below the buttons, there's a form with fields for Customer ID, Customer name, Commissioned status, Decommissioned status, Monitored status, and Network Health enabled. To the right, there's a section for 'Fijoport tickets' showing counts for Open, Confirmed, and Resolved tickets, and a section for 'Hazard notes'.

Customer ID	Customer name	Commissioned	Decommissioned	Monitored	Network Health enabled
Avaya00629b	Avaya Devconnect	✓	✗	✓	✗

The message displayed at the top shows that the VPN as connected successfully. The **Mapped IP** will be required in order to connect to each of the Server Edition and the IP500 V2 devices.

How to Access the Portal   User Manual   Administrator Manual

Paul

Home > Remote Access > Fijoport > 38b74d00629b

RA S on: command completed successfully. Mapped range: 10.190.40.0/24. Support range: 10.90.66.27. Race range: 10.90.66.27.

Fijoport 38b74d00629b

Disconnect   LAN   Reset   Network health   Change   History

Customer ID

Avaya00629b

Customer name

Avaya Devconnect

Commissioned

☒

Decommissioned

☐

Monitored

☒

Network Health enabled

☐

Status

Online

☒

Public IP

165.225.196.97

License

Hardware

Fijoport tickets

Open

0

Confirmed

0

Resolved

1

Device tickets

Open

3

Confirmed

0

Resolved

7

Hazard notes

No active hazard notes

RAS

Connected

☒

Fijoport mapped IP

10.190.40.254

Active sessions

1

Devices

Device	Device name	Local IP	Device model	Monitored	Network Health	Online	Mapped IP	Actions
Device 1	Server Edition	10.10.40.25	Avaya IPO SE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.190.1.1	<a href="#">Browse</a>
Device 2	IP500V2	10.10.40.20	Avaya IPO 500 V2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.190.1.2	<a href="#">Browse</a>
Device 3		-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

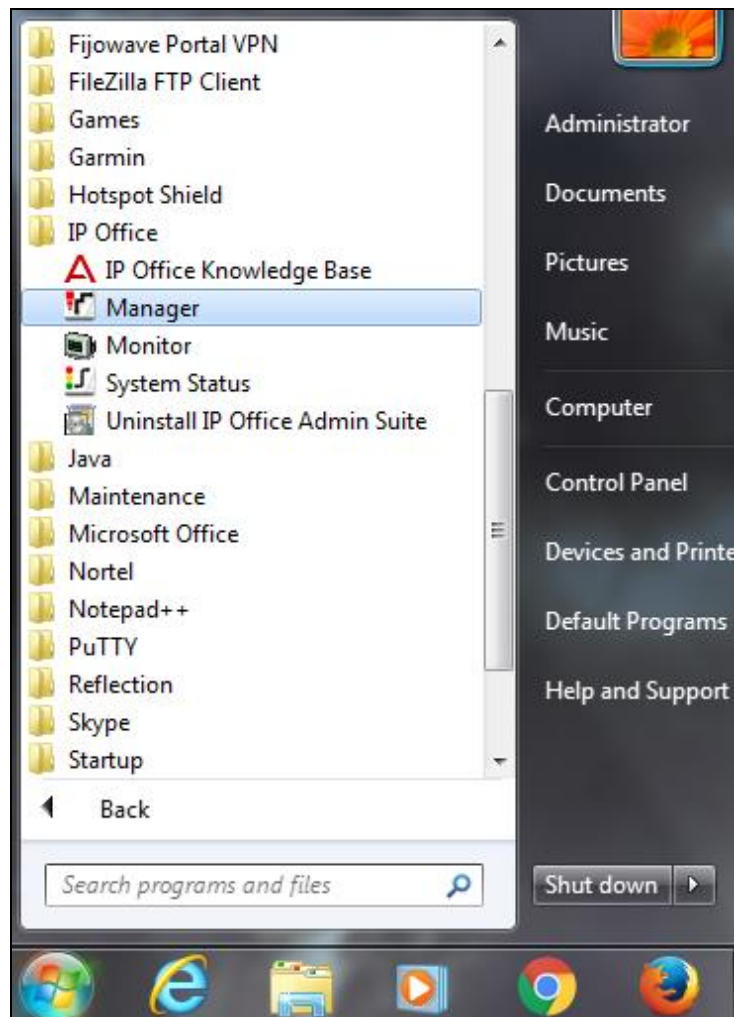
Using the **Mapped IP** from above the IP Office Manager and System Monitor can be used to access the IP office using these IP addresses to connect to each device, see **Section 7.3**.

### 7.3. Verify IP Office Remote Access Connections

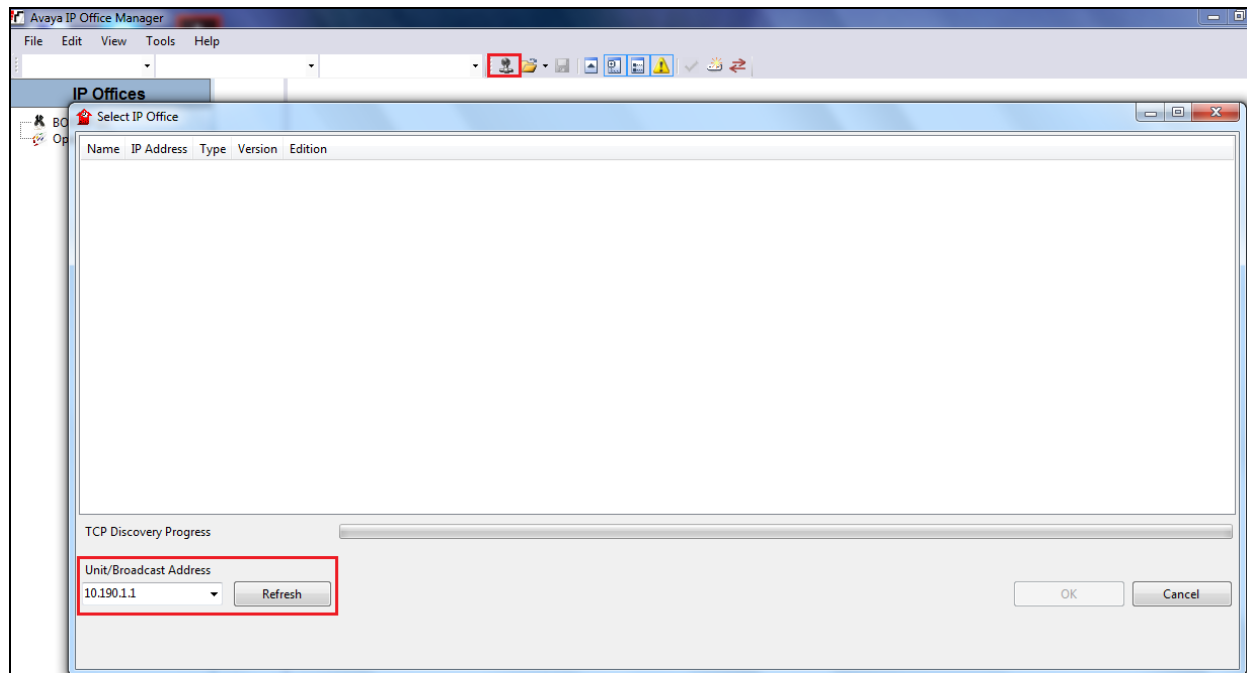
Once the secure tunnel is established to the IP Office, the IP Office clients can be used to connect to each of the Server Edition and the IP500 V2. To verify that Fijoport Remote Access is fully working, from the PC running the Fijowave Portal VPN, open the three IP Office applications, IP Office Manager, Monitor and System Status.

#### 7.3.1. Verify IP Office Manager

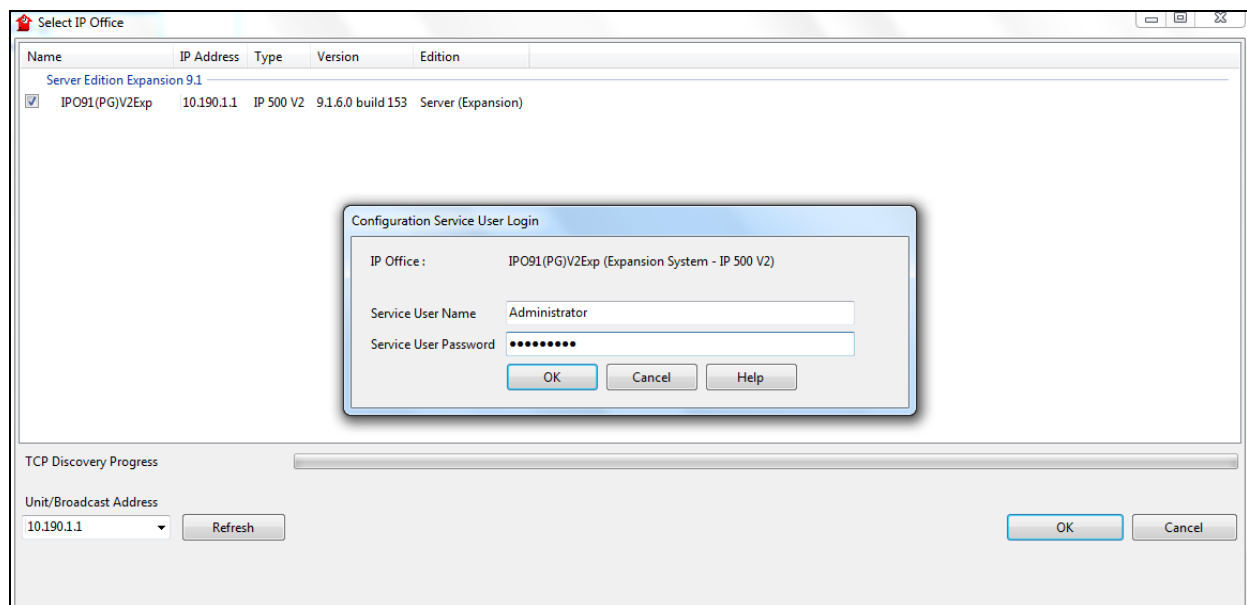
Open the IP Office Manager either from the desktop shortcut or from **Programs → IP Office** as shown below.



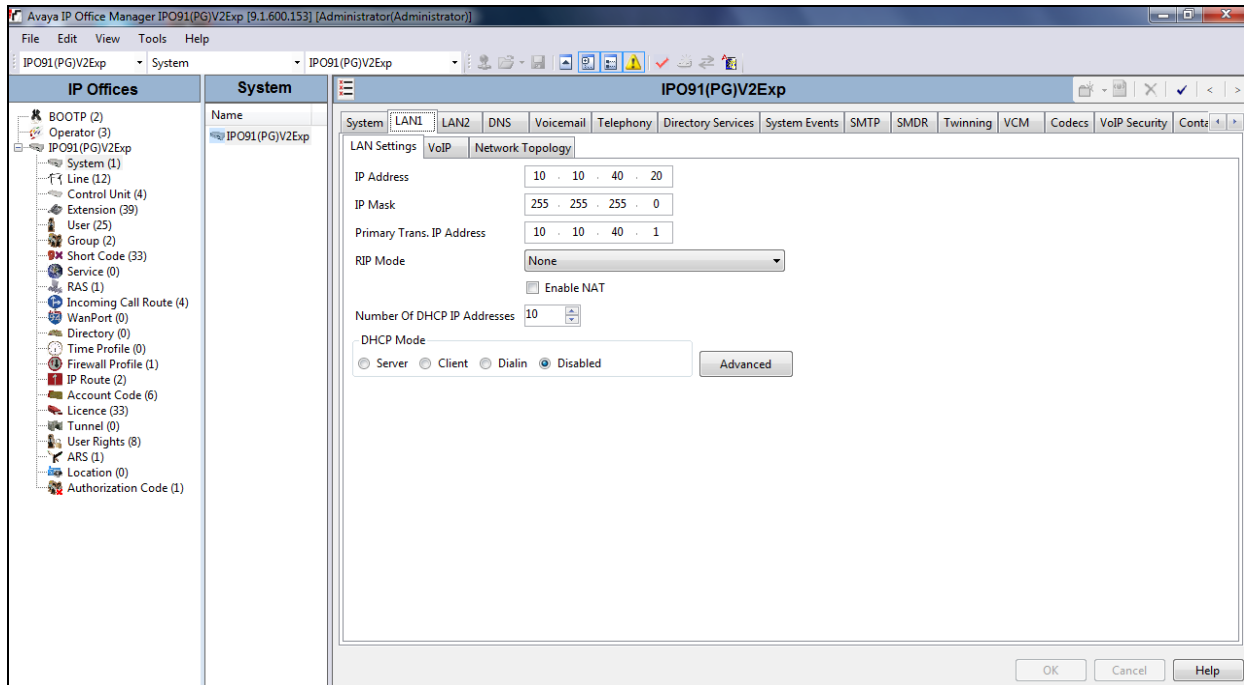
The **Unit Broadcast Address** will need to be set to that of the **Mapped IP** found in **Section 7.2**. The mapped IP address is entered, and **Refresh** is pressed and that should bring up the IP Office unit.



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.



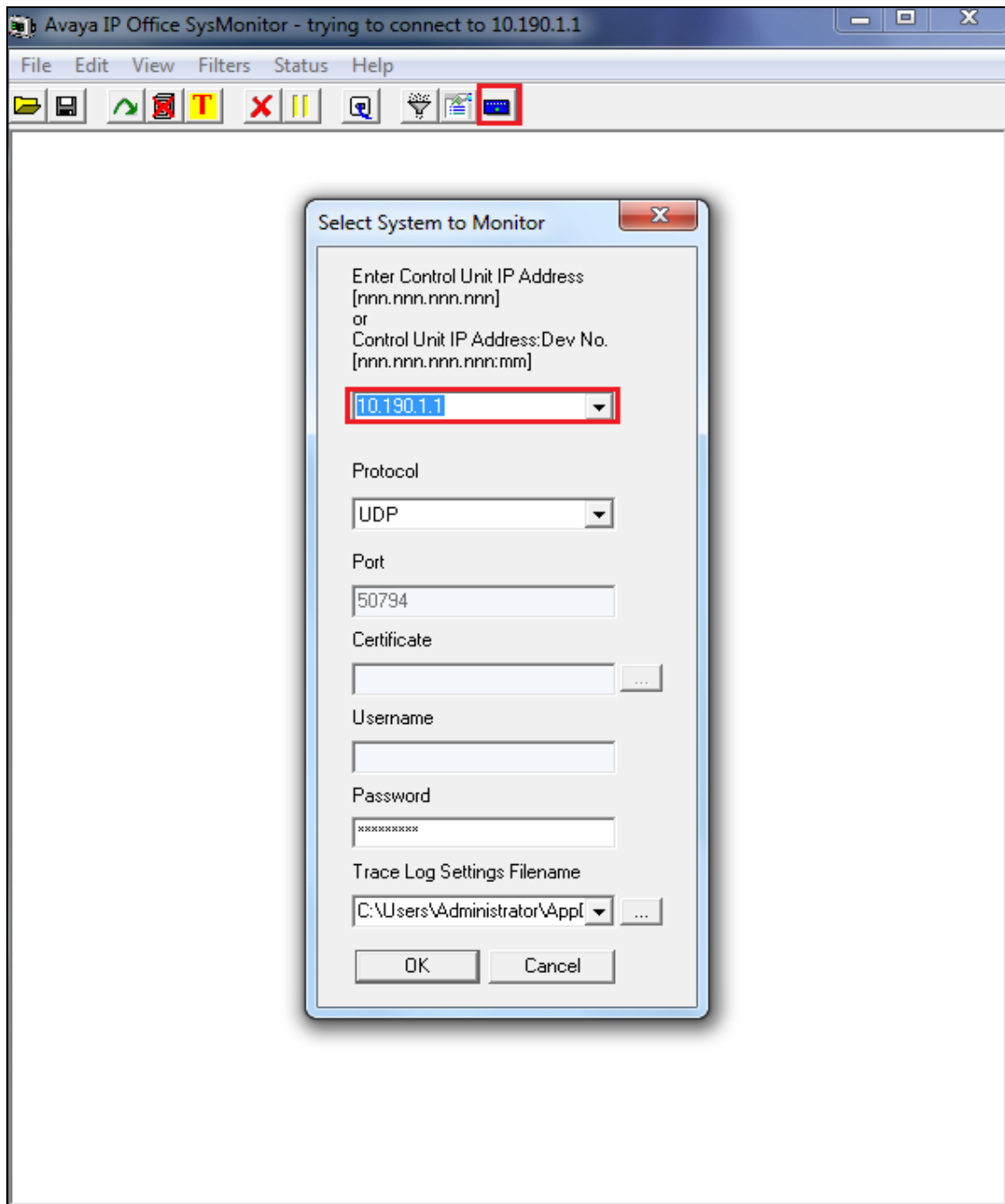
The IP Office Manager screen should be opened and should appear something like shown below where changed can be made and saved (not shown).



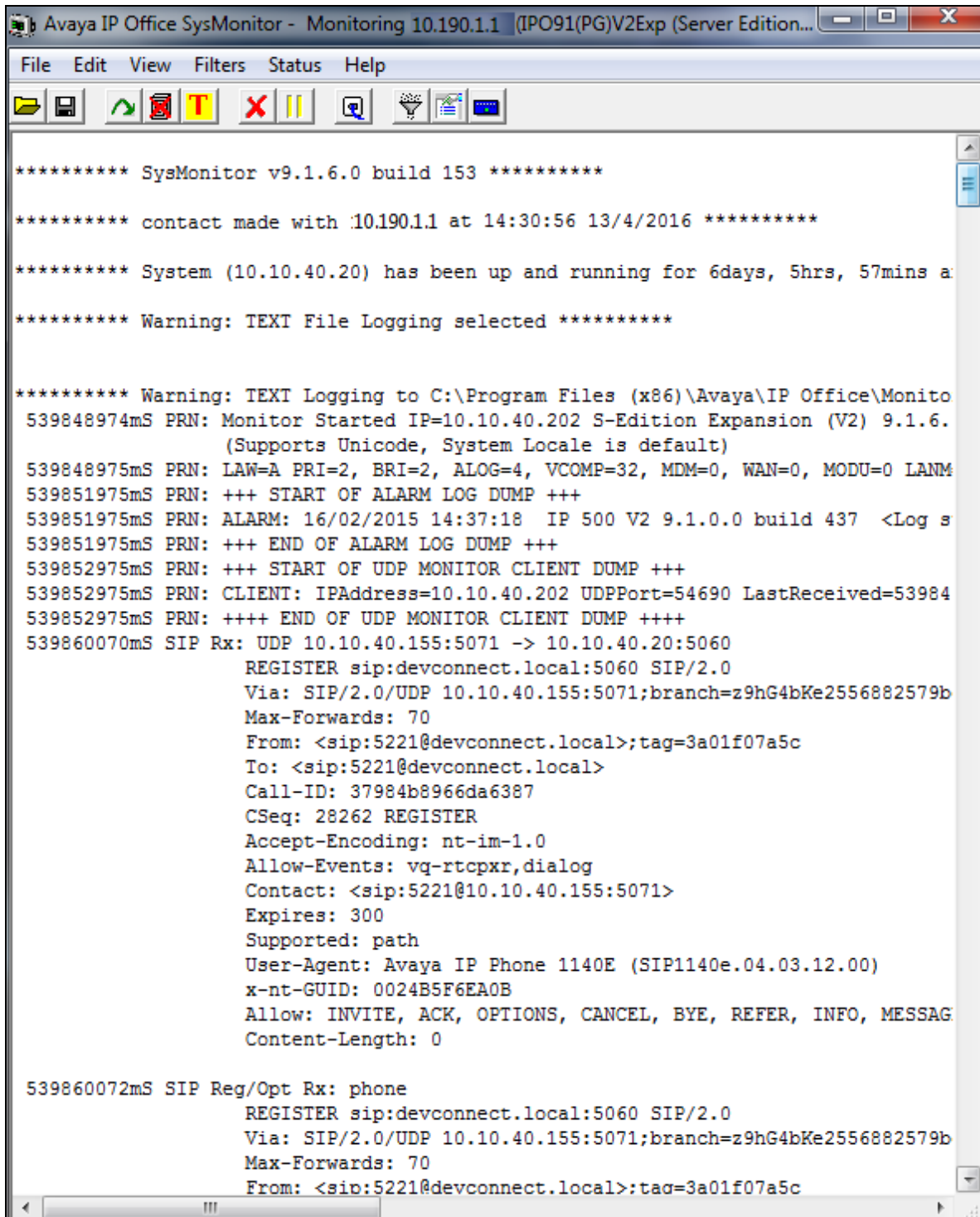
### 7.3.2. Verify IP Office Monitor

IP Office Monitor is accessed in the same way 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 7.2**. Click on OK and the monitor should start correctly.



The monitor should now display information on IP Office correctly.



```
***** 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-rtcp,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 way 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 7.2**, enter the log in credentials and click on **Logon** and the monitor should start correctly.

The screenshot shows the Avaya IP Office System Status application window. The window title is "Avaya IP Office System Status". The main content area displays the Avaya logo and the title "IP Office System Status". Below the title bar, there is a menu bar with "Help", "Exit", and "About". The main content area is mostly blank, with a "Logon" dialog box open in the center. The dialog box has a title bar with "Online" and "Offline" buttons. The "Logon" dialog box contains the following fields and controls:

- Control Unit IP Address:** A dropdown menu showing "10.190.1.1".
- Services Base TCP Port:** A text field showing "50804".
- User Name:** A text field showing "Administrator".
- Password:** A text field with masked characters (dots).
- Auto reconnect:** A checkbox that is unchecked.
- Secure connection:** A checkbox that is checked.
- Logon:** A button to initiate the login process.

The status bar at the bottom of the window indicates "IP Office System Status Version 9.1.6.0 build 153".

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

**AVAYA** IP Office System Status

Help Snapshot LogOff Exit About

**System**

**Alarms (4)**

Configuration (0)

Service (0)

**Trunks (4)**

Link (0)

Call Quality of Service

**Security (0)**

**Extensions (19)**

5201

5202

5203

5204

5205

5206

5207

5208

5211

5212

5213

5214

5215

5216

5217

5218

5221

5250

5251

**Trunks (12)**

Active Calls

**Resources**

**Voicemail**

**IP Networking**

**Locations**

**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

Trinning: 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				

Trace Trace All Pause Call Details Print... Save As...

14:33:20 Online

## 8. Conclusion

These Application Notes describe the configuration steps required for provisioning Fijowave's Fijoport Remote Access to interoperate with Avaya IP Office R11.0. It has been verified that the Fijoport solution allows a secure connection to IP Office and allows the end user to connect to IP Office using 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] Administering Avaya IP Office™ Platform with Manager, Release 11
- [2] Avaya IP Office™ Platform Documentation Catalog Release 11
- [3] Avaya IP Office™ Platform 11 Deploying Avaya IP Office™ Platform Servers as Virtual Machines

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

- Web: <http://www.fijowave.com>
- Email: [support@fijowave.com](mailto:support@fijowave.com)
- Help desk: +353 1 525 3072

---

**©2020 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).