Avaya Solution & Interoperability Test Lab

Application Notes for configuring Fijowave Fijoport Advanced Monitoring with Avaya IP Office IP500 V2 R11– Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Fijowave's Fijoport Advanced Monitoring to access Avaya IP Office IP500 V2 standalone 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 Advanced Monitoring with Avaya IP Office IP500 V2 standalone.

Note: The current version of Fijoport Advanced Monitoring only supports a connection to the IP Office IP500 V2 for the monitoring of alarms and messages through the System Monitoring API. A connection to IP Office Server Edition is not currently supported.

Fijoport Advanced Monitoring (Fijoport) consists of both a monitoring service and allows for remote access 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 both a monitoring service for alarm messages and as a remote access device for IP Office. There are two modules that were tested.

1. Fijoport Advanced Monitoring
2. Fijoport Remote Access

The Fijoport Advanced Monitoring product would always include the Fijoport Remote Access module however Fijoport Remote Access product would also exist as a stand-alone product without the Fijoport Advanced Monitoring module.

Fijoport Advanced Monitoring uses the Avaya IP Office System Monitoring API. This is a REST Web Service which in response to a HTTPS GET request returns data in an XML format. This monitoring service alerts the end user to various alarms coming from the IP Office. This user can then use the remote access module to gain access to the IP Office in question and observe and fix these alarms that are being raised.

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.

- Monitoring Alarm Messages from IP Office IP500 V2
- Using Avaya IP Office Manager from a remote location
- 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. The current version of Fijoport Advanced Monitoring only supports a connection to the IP Office IP500 V2 for the monitoring of alarms and messages through the System Monitoring API. A connection to IP Office Server Edition Linux server is not currently supported.
2. 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.
3. Not every single Alarm code was tested on the Monitoring section, a flavour of current alarms and two new alarms were raised and observed.

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. Fijoport Advanced Monitoring 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.

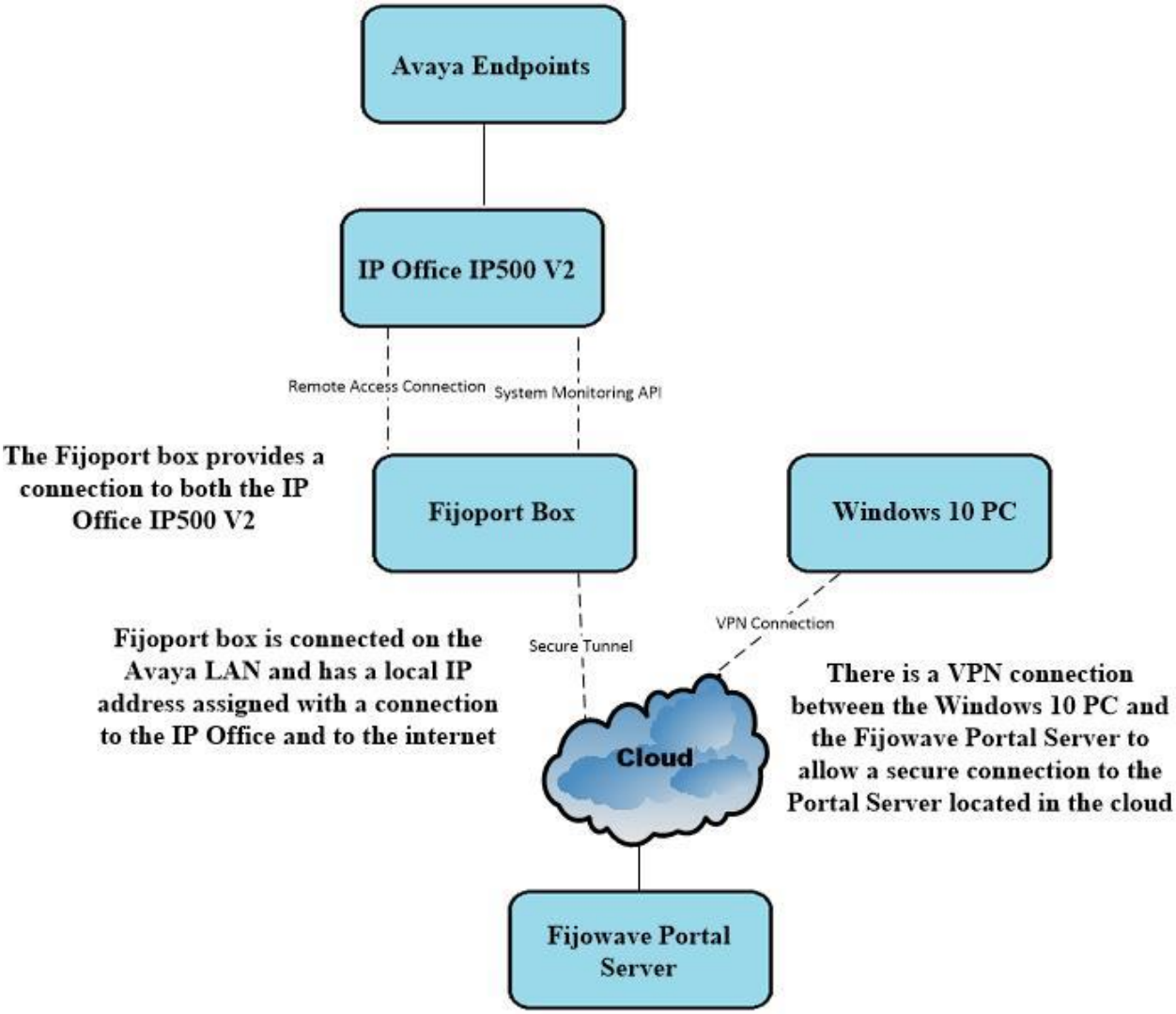


Figure 1: Reference Configuration of Fijowave Fijoport Remote Access with Avaya IP Office

4. Equipment and Software Validated

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

Equipment/Software	Version/Release
Avaya IP Office 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 only.

Note: The current version of Fijoport Advanced Monitoring only supports a connection to the IP Office IP500 V2 for the monitoring of alarms and messages through the System Monitoring API.

5. Configure Avaya IP Office

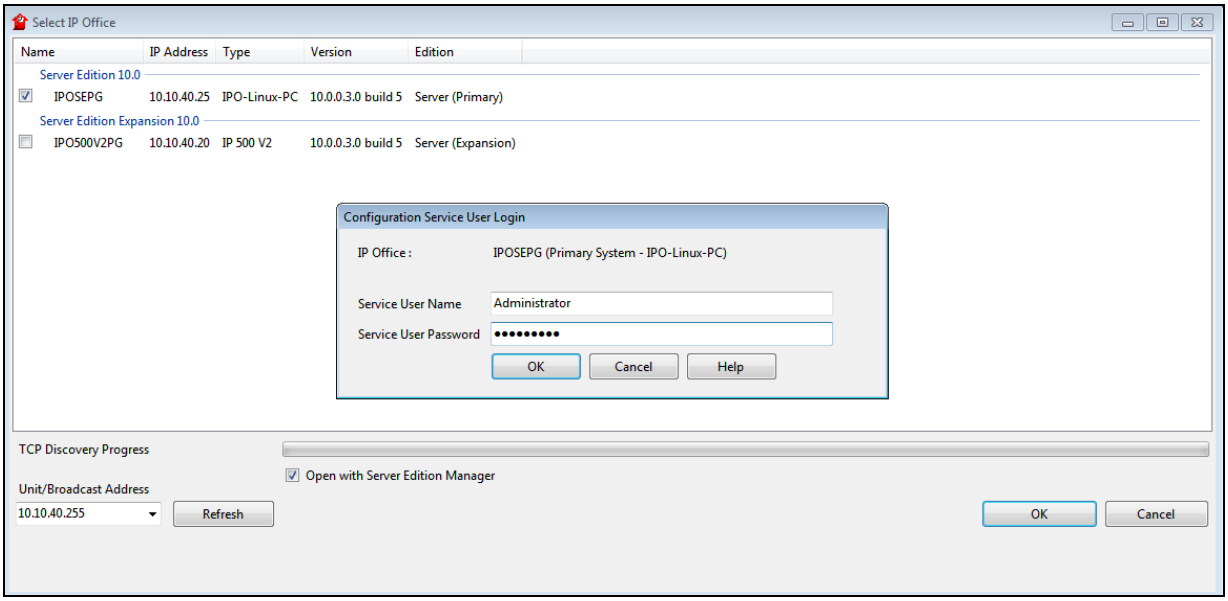
There is no specific configuration of IP Office required for the compliance testing of Fijoport Advanced Monitoring. The IP address of the IP Office is required in order to configure the Fijoport box in **Section 6**. Configuration and verification operations on the Avaya IP Office illustrated in this 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
- Create System Monitoring Web Service User

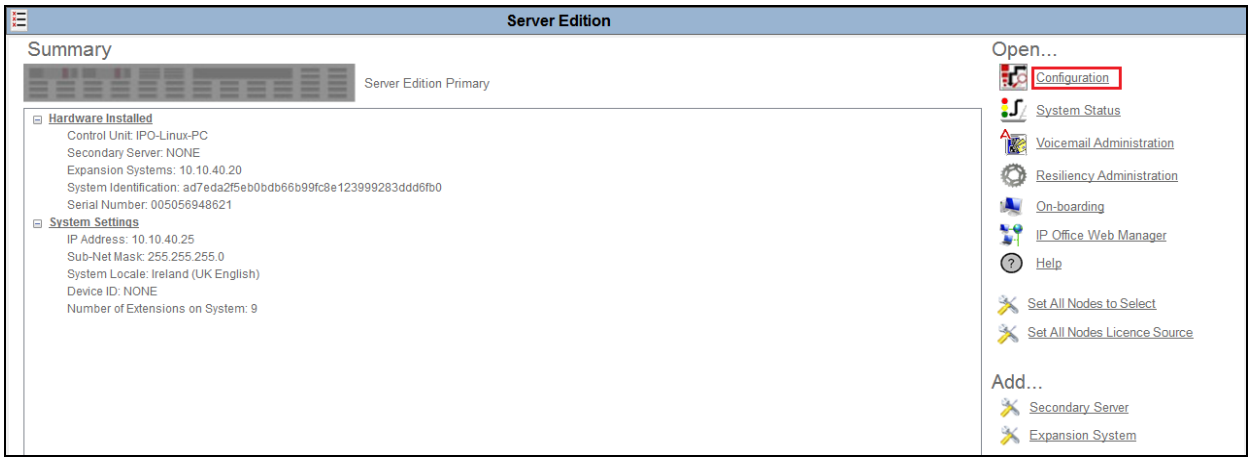
Note: The example below shows the IP address information for the Server Edition only, however both the Server Edition and the IP500V2 IP information must be acquired to setup a connection to both.

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.

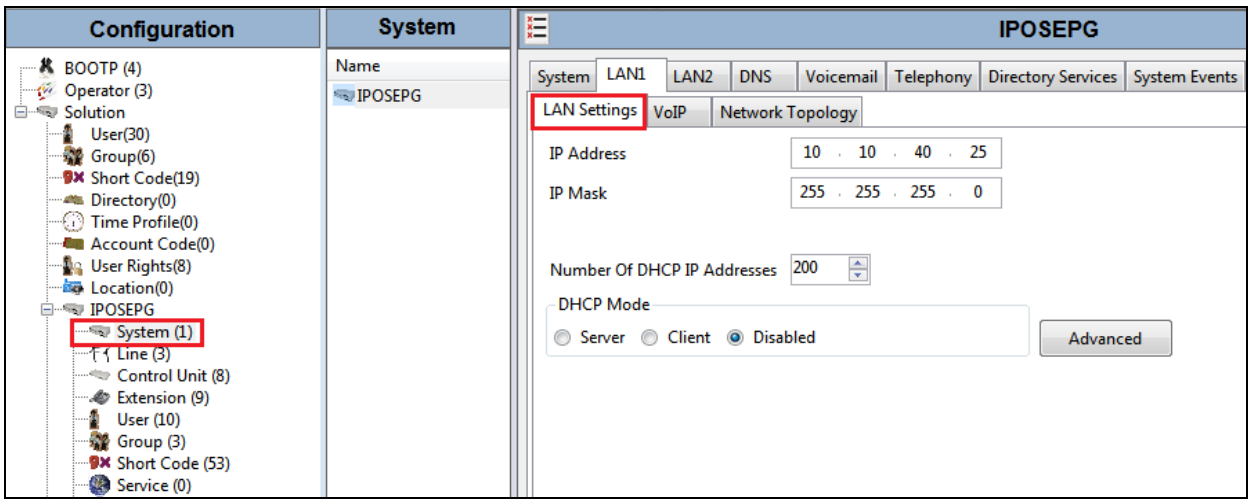


Click on **Configuration** at the top right of the page, as shown, to receive the IP Office configuration.



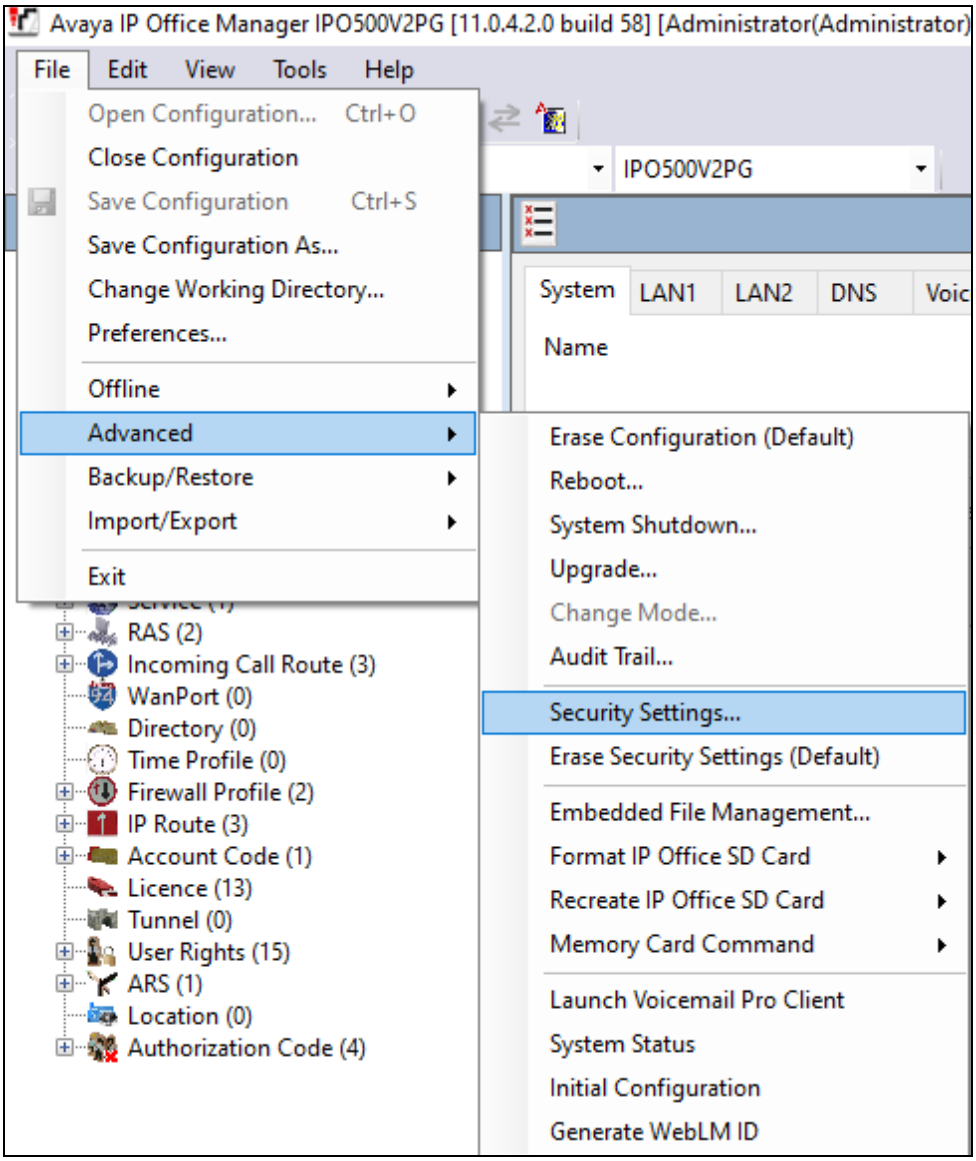
5.2. Display LAN Properties

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**.

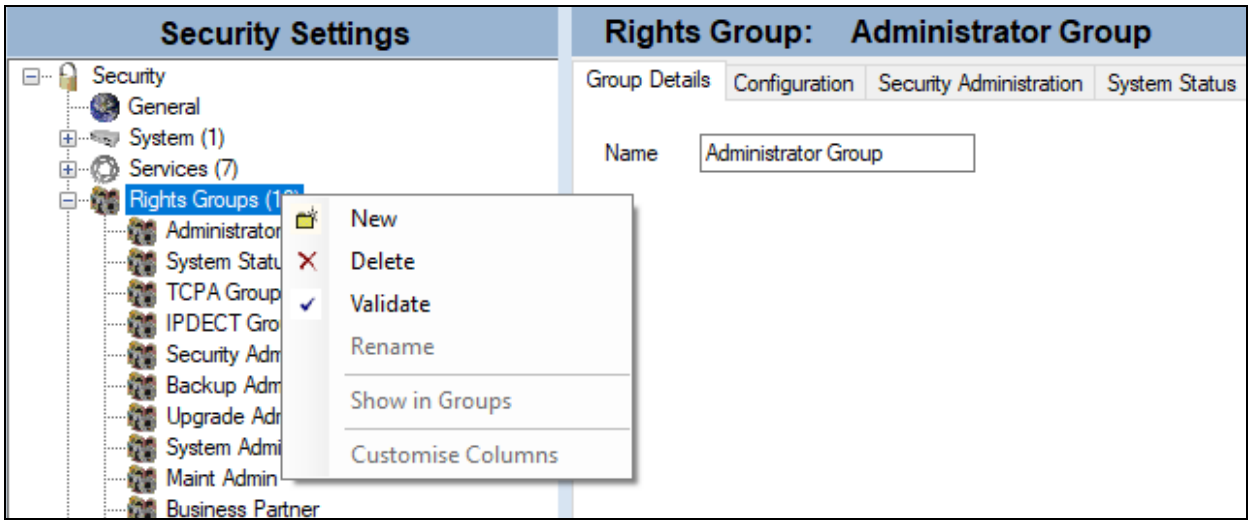


5.3. Create System Monitoring Web Service User

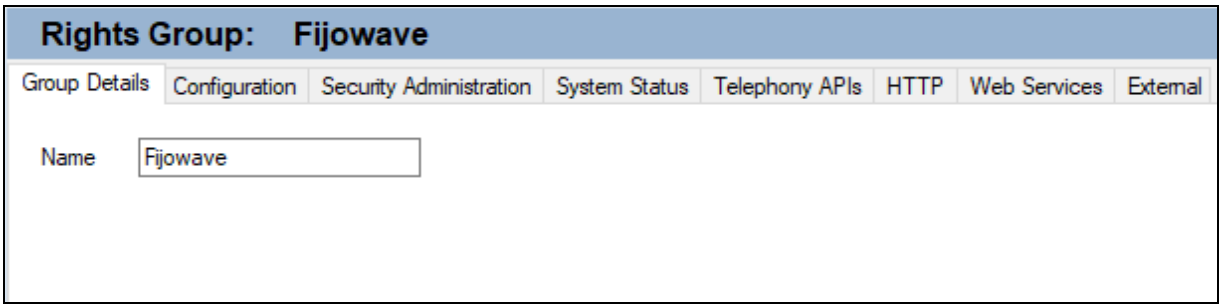
Once the configuration is opened to the IP Office IP500 V2, navigate to **File → Advanced → Security Settings**, as shown below.



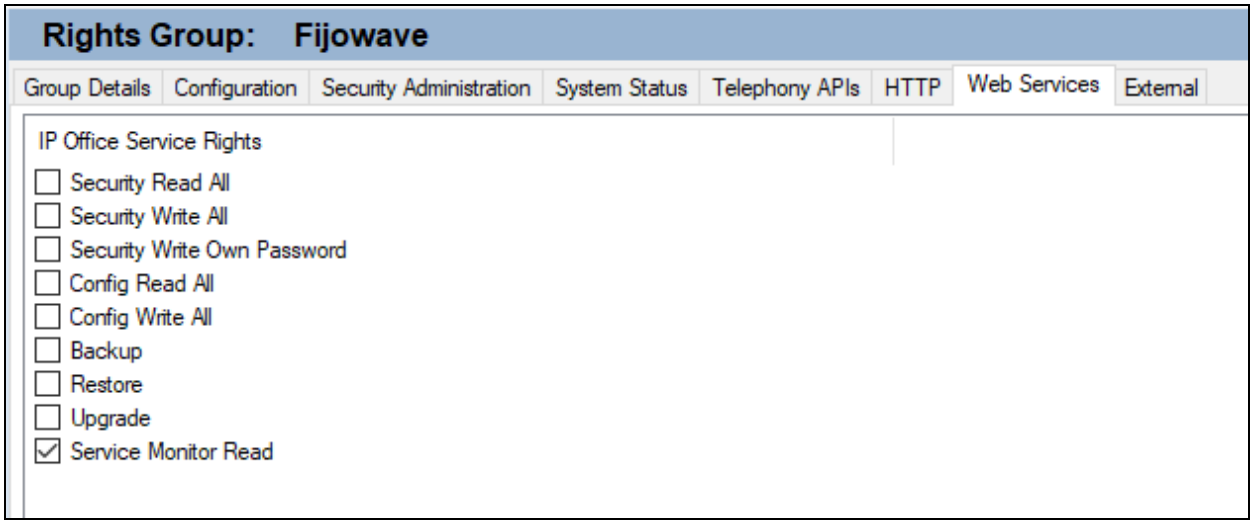
Expand the **Rights Groups** in the left window, right-click on **Rights Groups** and select **New**, as shown below.



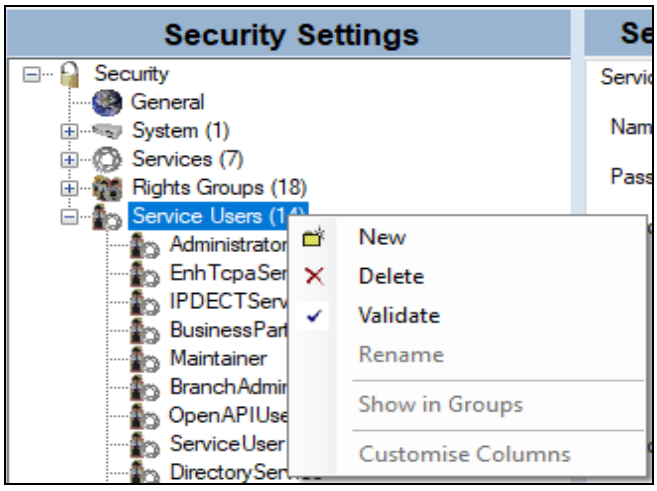
Enter a suitable **Name** under the **Group Details** tab.



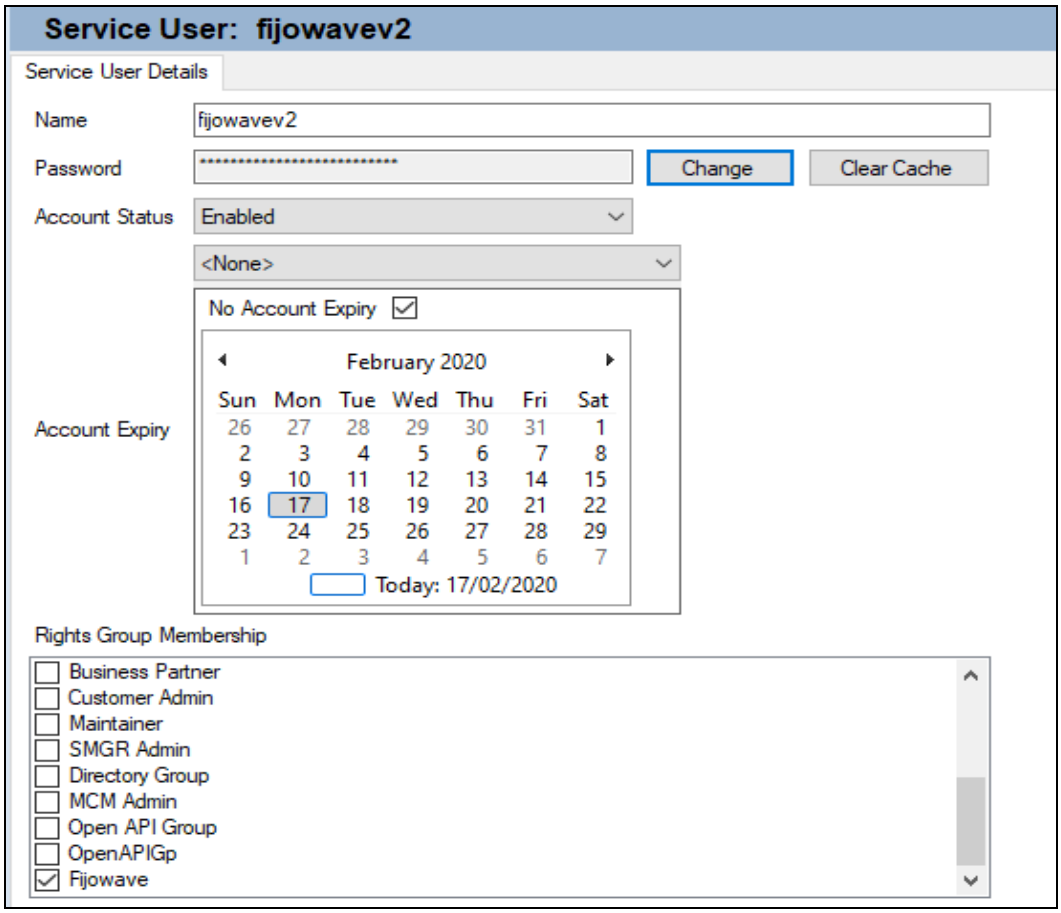
Click on the **Web Services** tab and tick the box beside **Service Monitor Read**, as shown below.



Expand the **Service Users** in the left window, right-click on **Service Users** and select **New**, as shown.



Enter a suitable **Name** and **Password** for this new user, note that these details will be required in the configuration of the Fijowave Monitoring in **Section 6.3**. Ensure that the **Rights Group** created above is ticked as shown below. Click on **OK** at the bottom of the screen (not shown).

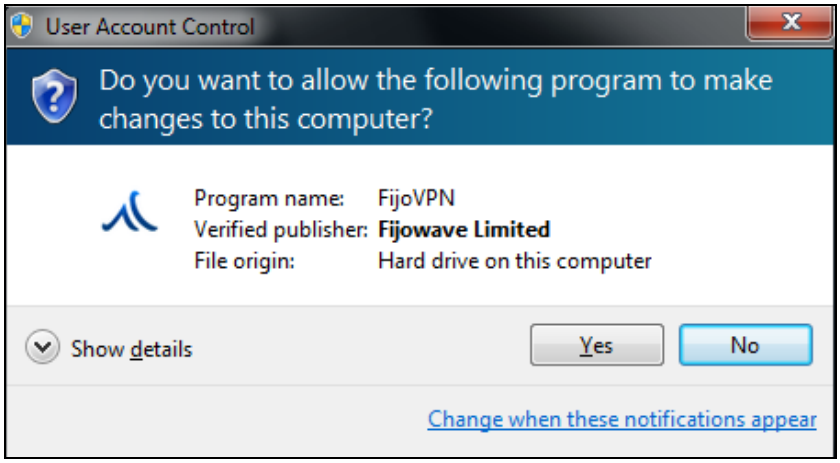


6. Configure Fijowave Fijoport Remote Access

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.

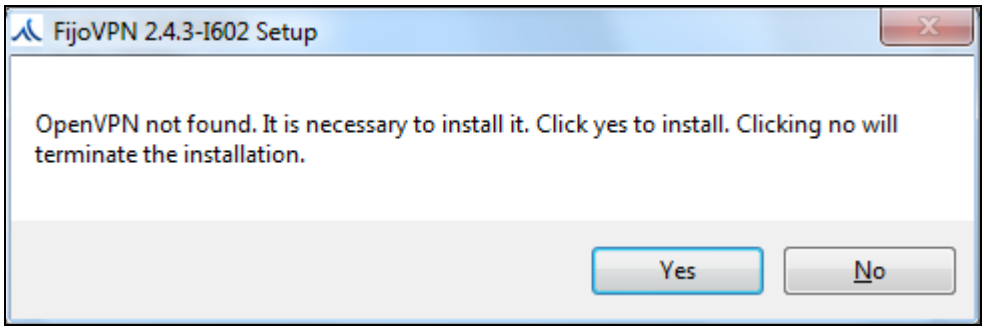
6.1. Install Fijowave Portal VPN

Unpack the contents of the 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.



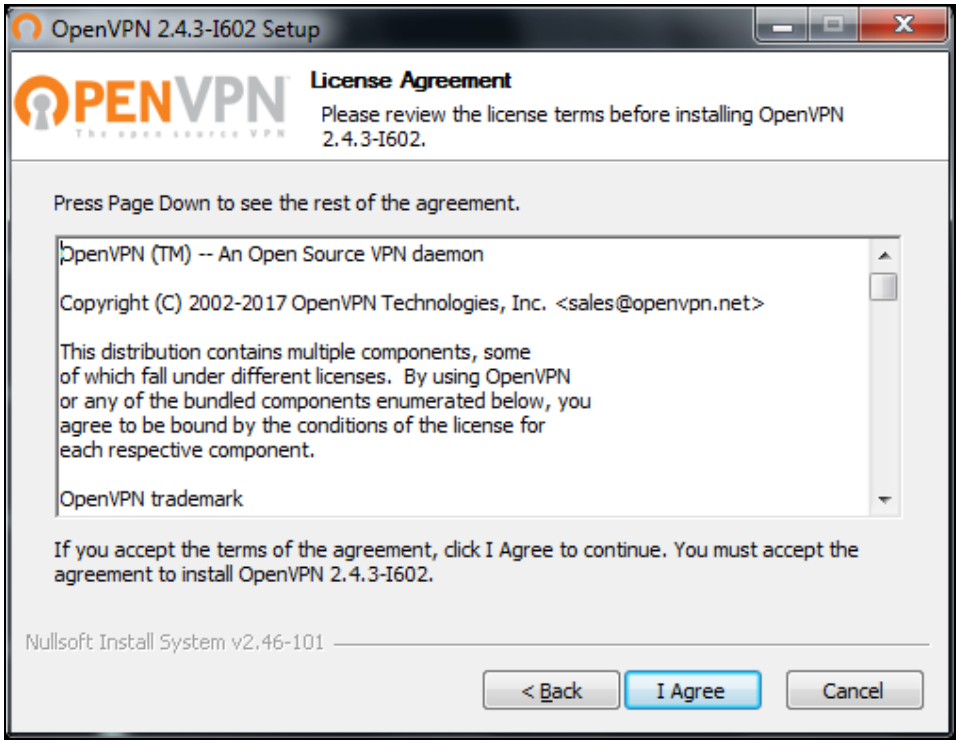
Browse and select the appropriate VPN configuration key file (not shown) and then click **Install**.

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

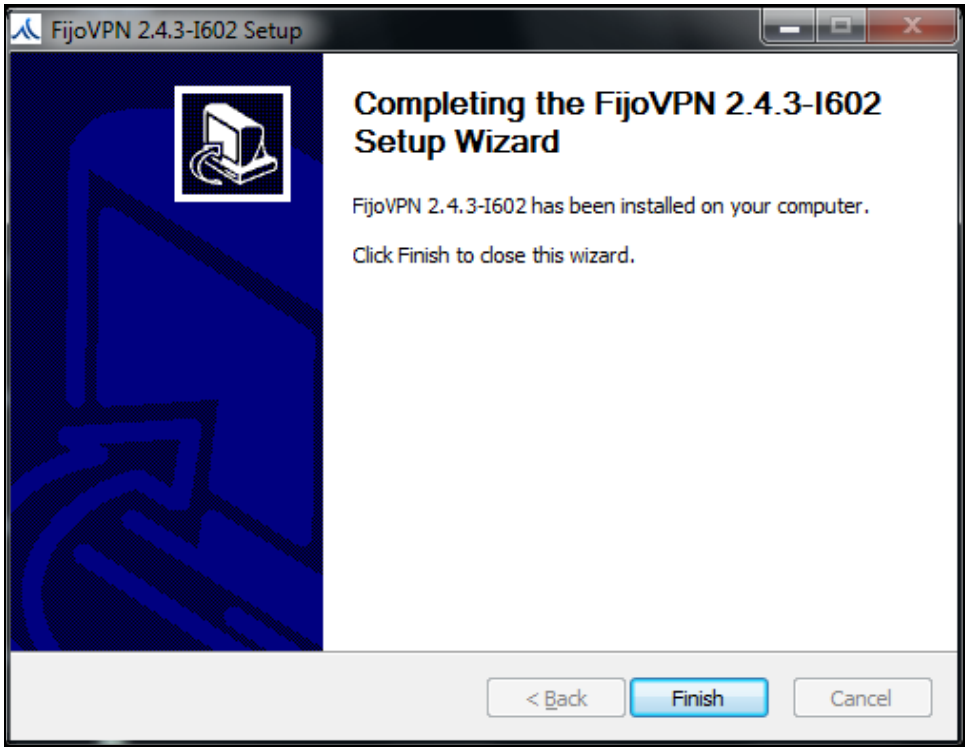


Click on **Next** to continue.

Click on **I Agree** to continue.



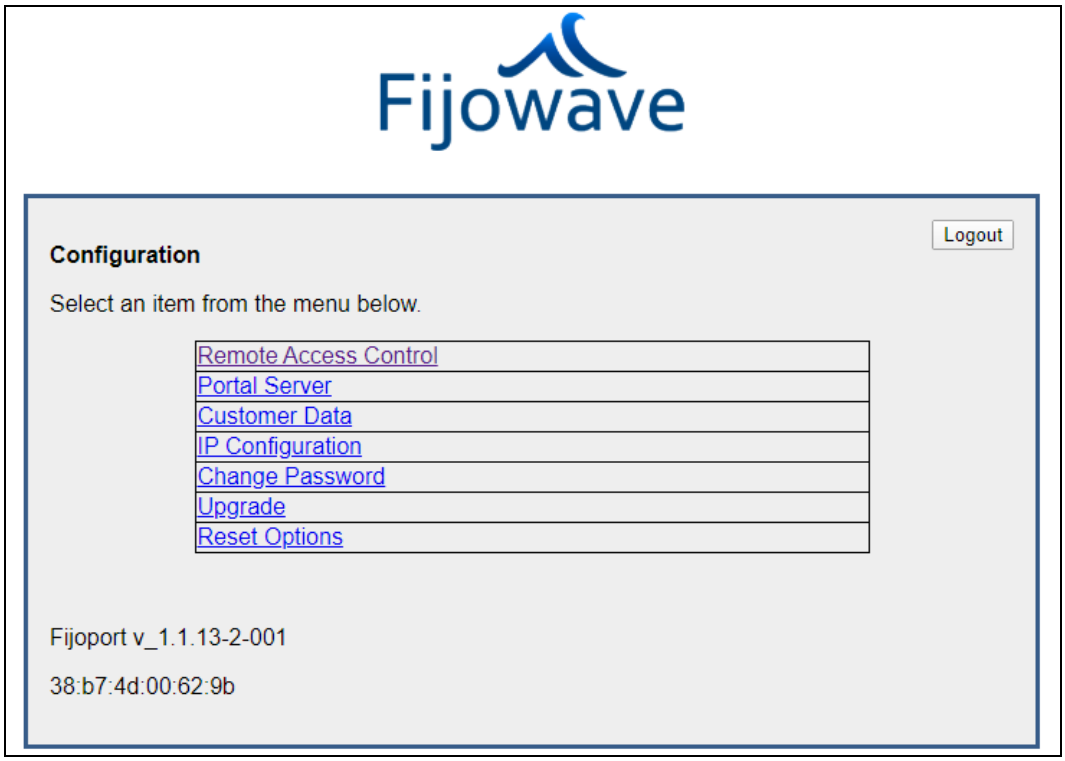
Close the installer by clicking **Finish**.



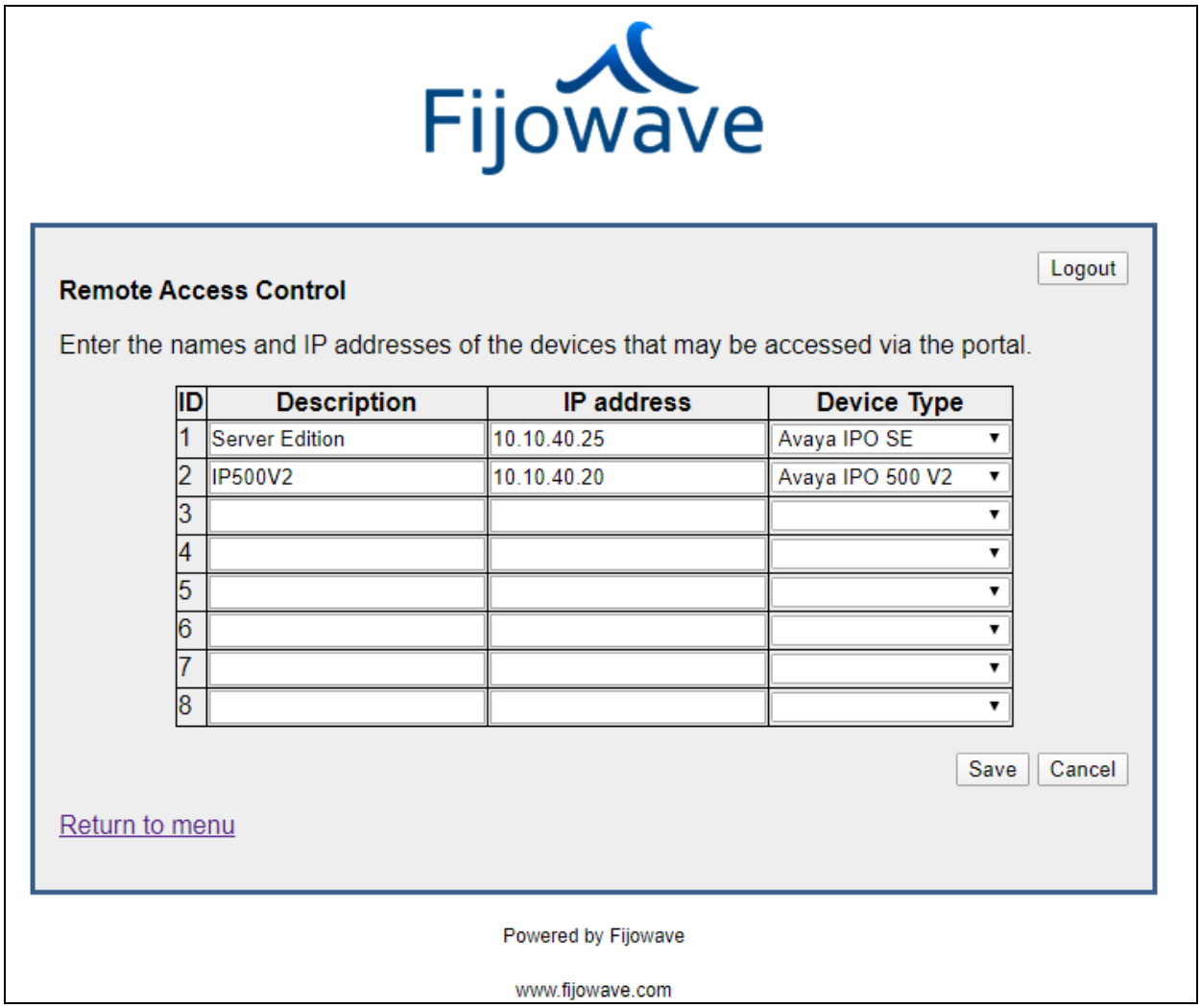
6.2. Configure Connection to IP Office

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

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

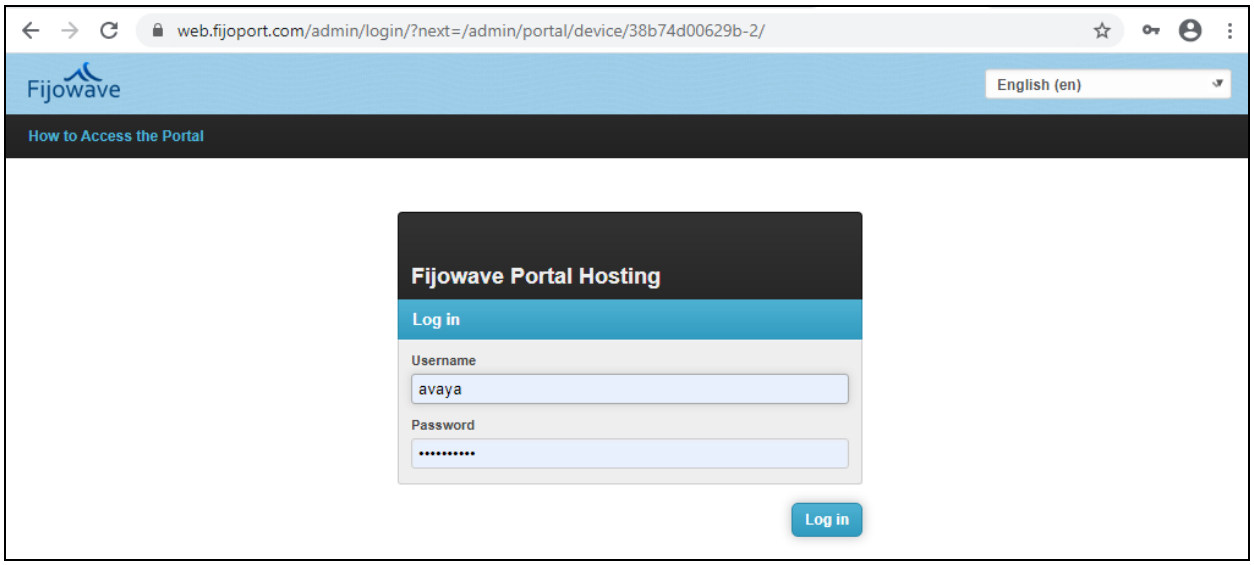


Enter the local IP address of the IP Office Server Edition for **ID 1** and the local IP address of the IP Office IP500 V2 for **ID 2** (if applicable). Press the **Save** button and then close the browser tab.

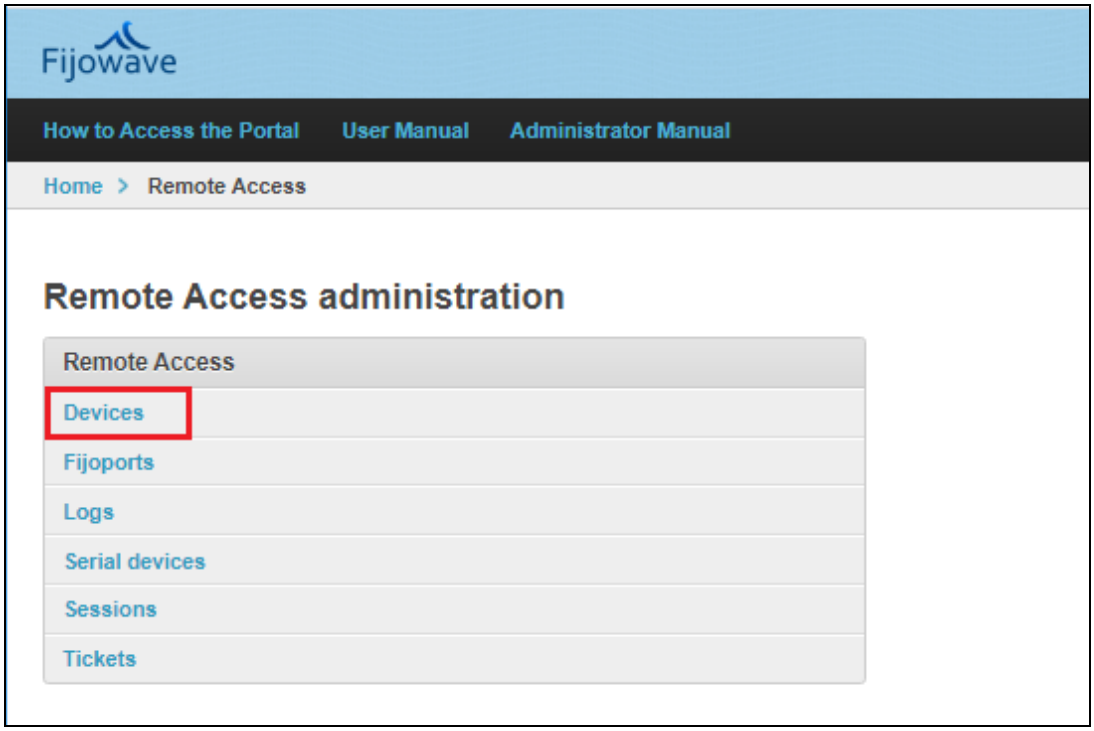


6.3. Configure Monitoring on Fijowave Portal Server

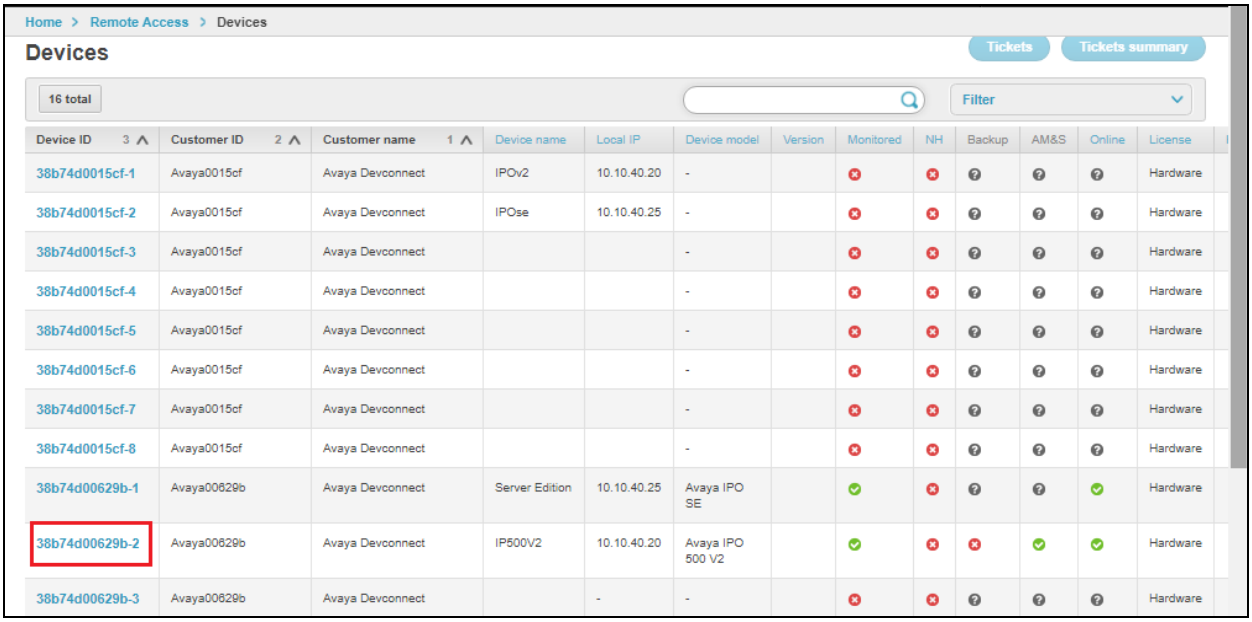
Open a URL to **web.fijoport.com** as shown below, enter the appropriate credentials and click on **Log in**.



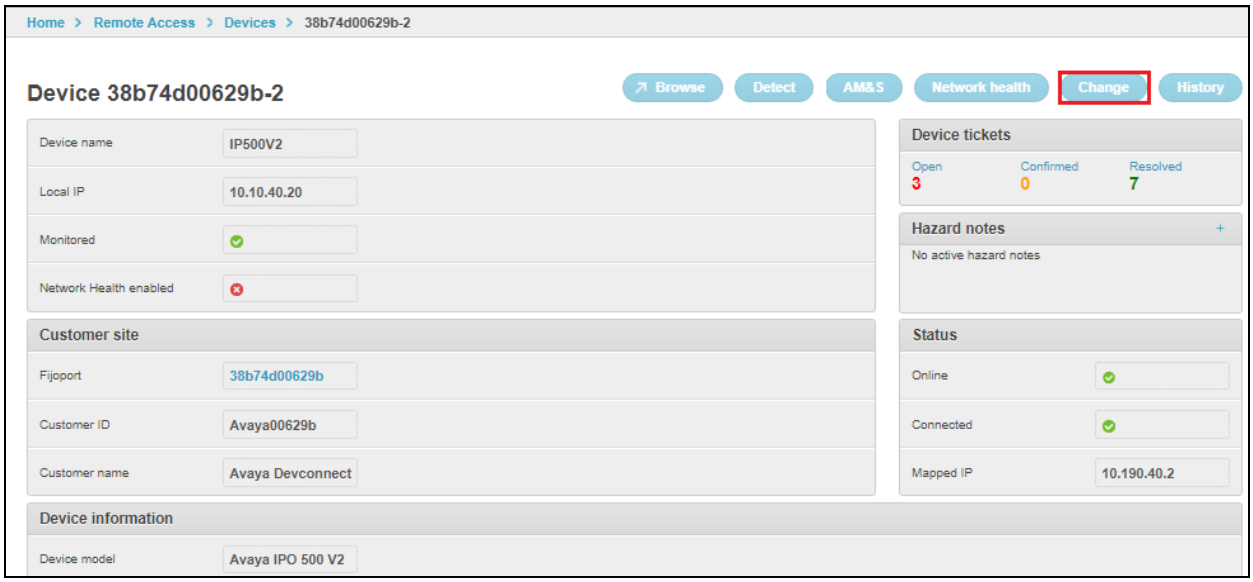
Click on **Devices**.



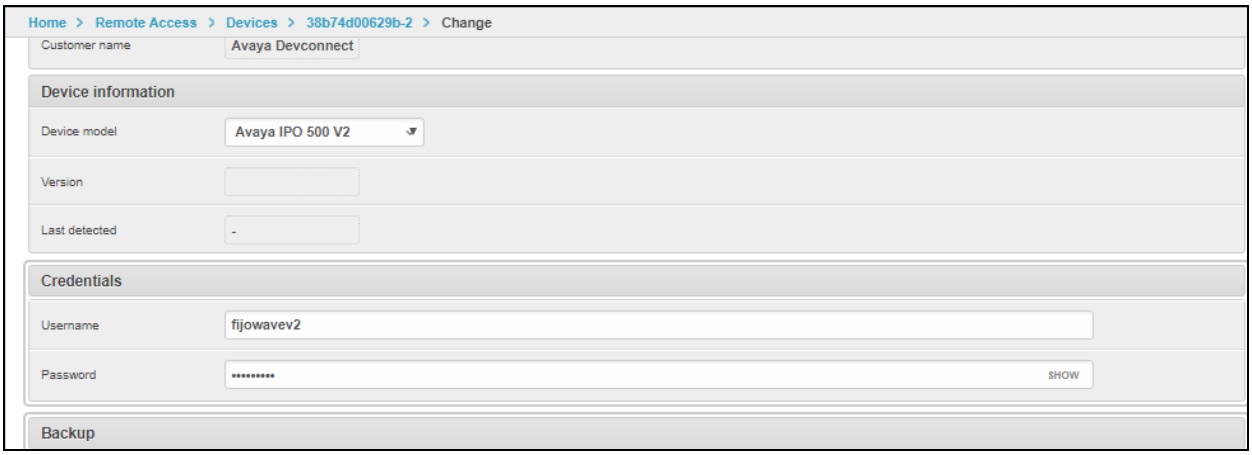
On sites where many Fijoports are in use, click on the **Device ID** to be accessed.



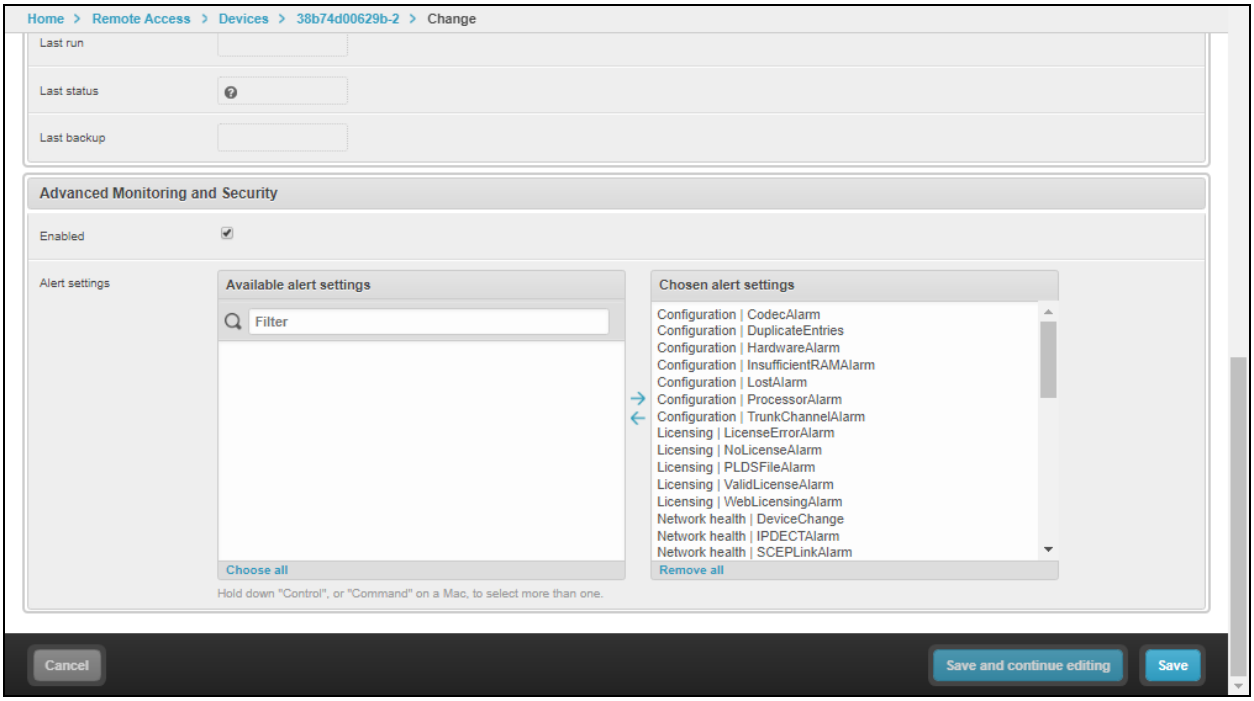
When the appropriate **Device** is opened, click on **Change** at the top.



Scroll down and enter the appropriate Credentials, this will be the **Username** and **Password** of the Web Services user created in **Section 5.3**.



Scroll down to the section called **Advanced Monitoring and Security**. Ensure **Enabled** is ticked. For compliance testing all **Available alert settings** were chosen as shown below. Click on **Save** at the bottom of the screen.

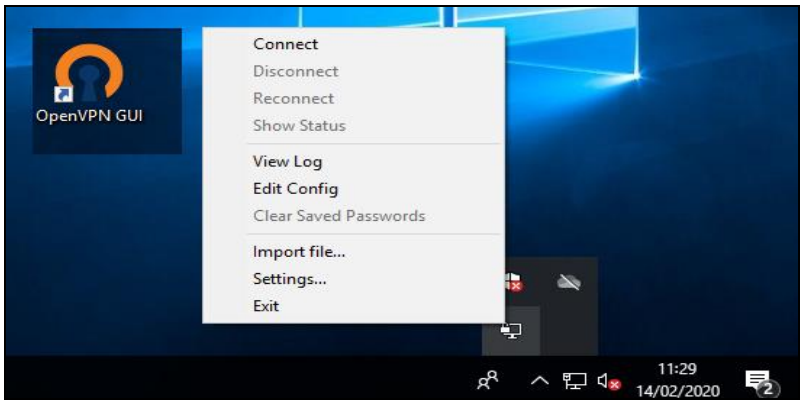


7. Verification Steps

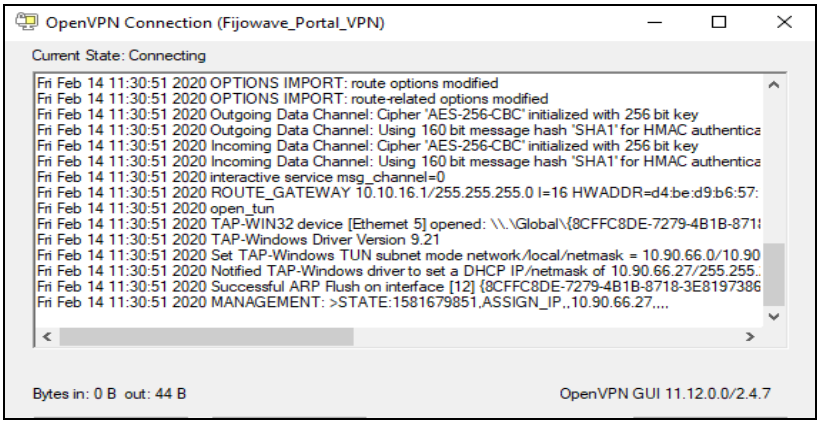
The following steps can be taken to ensure that connections between Fijowave Fijoport Remote Access and IP Office are up. The Fijowave Portal VPN is executed in order to setup the VPN connection. This connection can be verified, and the IP Office applications can be run.

7.1. Verify Fijowave Portal VPN

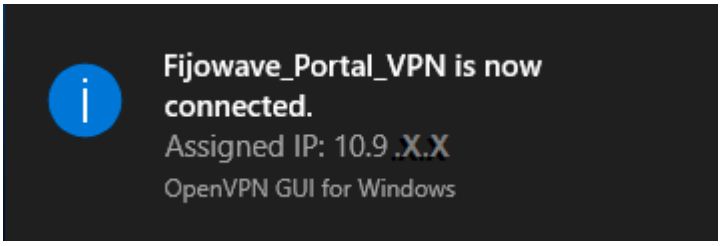
Start the VPN application by double-clicking on the shortcut. Once this is started it will appear in the system tray at the bottom right of the screen where is can be accessed and **Connect** is chosen.



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

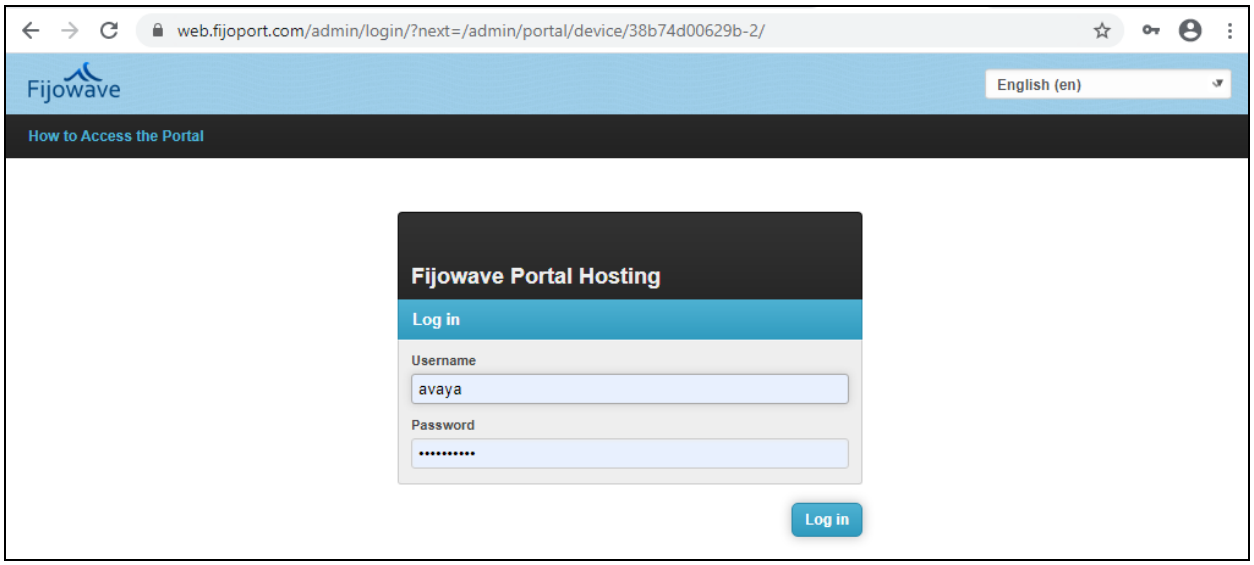


The following message verifies that the VPN is up and running and connected correctly.

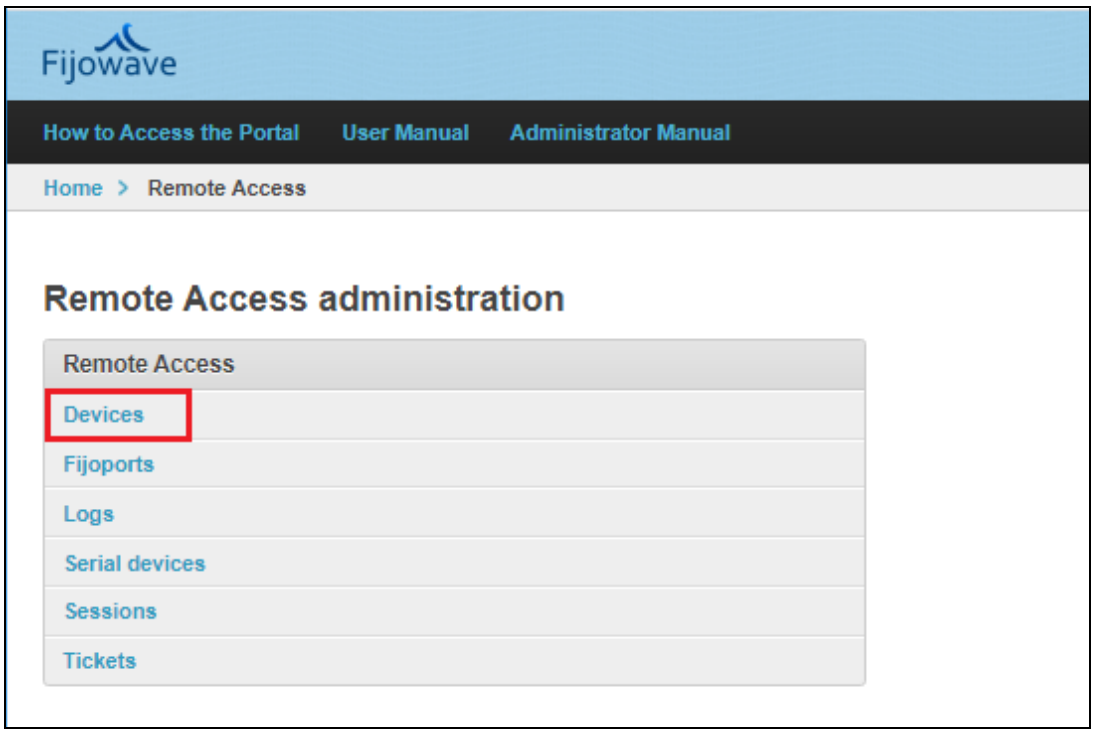


7.2. Verify Monitoring of IP Office

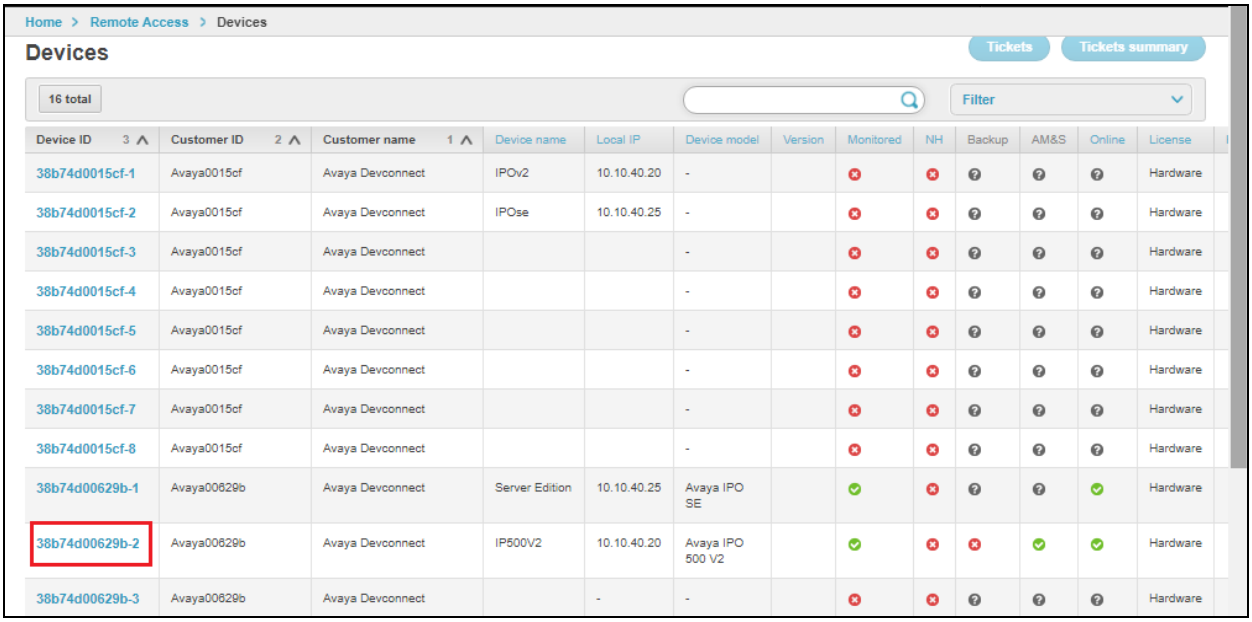
Open a URL to **web.fijoport.com** as shown below, enter the appropriate credentials and click on **Log in**.



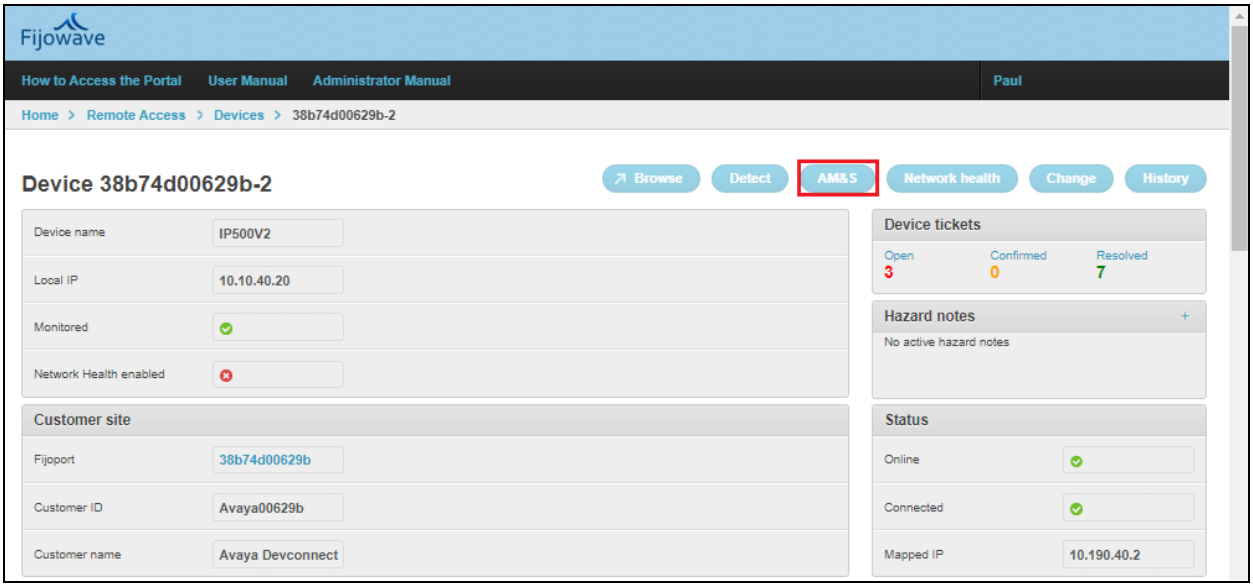
Click on **Devices**.



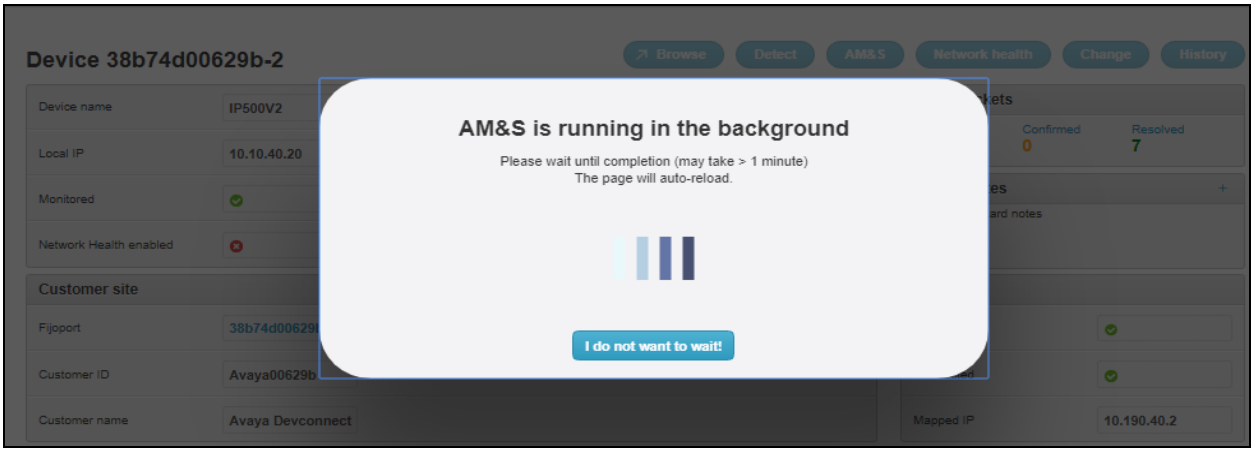
On sites where many Fijoports are in use, click on the **Device ID** to be accessed.



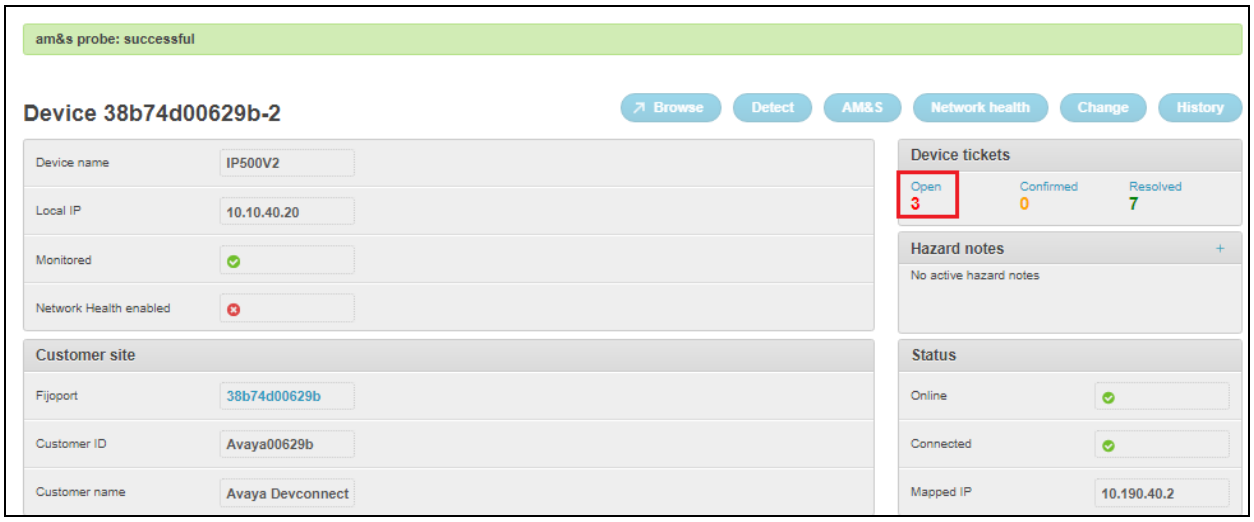
When the appropriate **Device** is opened, click on **AM&S** at the top. This will initiate a scan of any new alarms generated by the IP500 V2.



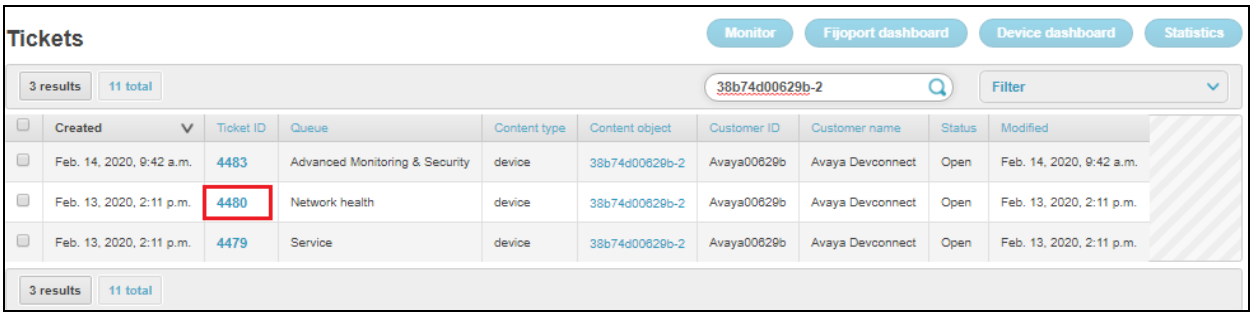
Something like the following should be displayed, showing that the data is being collected.



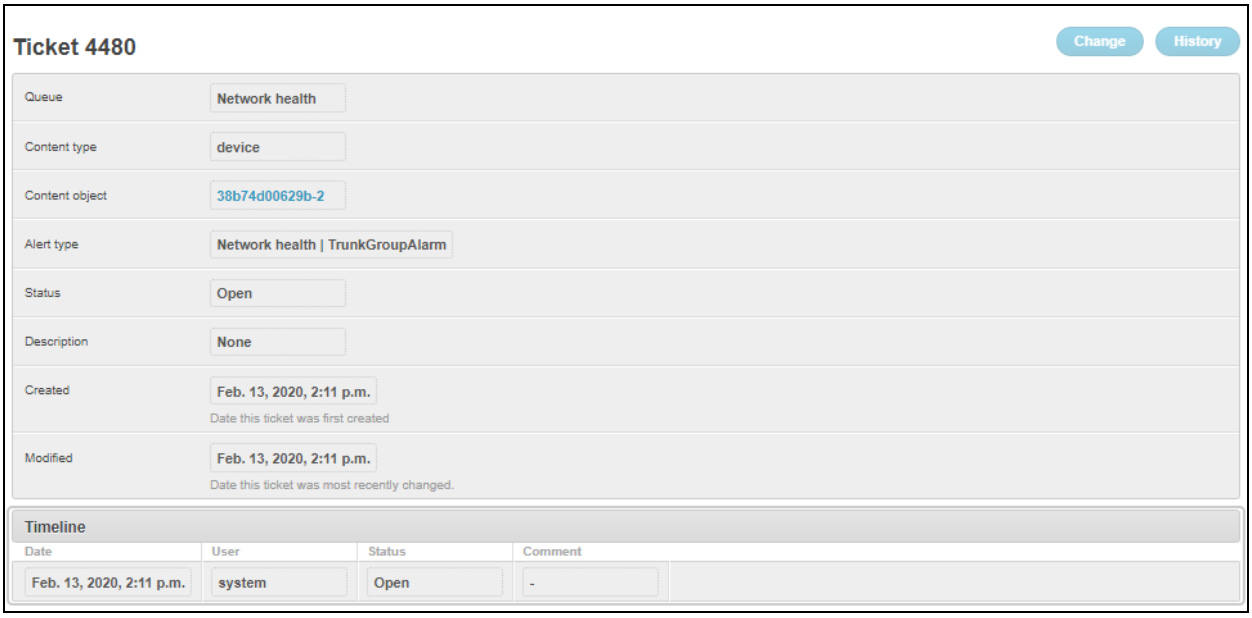
The message at the top of the screen shows that the am&s probe was successful. There are **3** tickets that have been opened showing that three new alarms are present. Clicking on **Open**, highlighted below will open a new window and display these three tickets.



These three tickets are shown below, the middle ticket **4480** was chosen, clicking on this will open the ticket as shown on the next page.

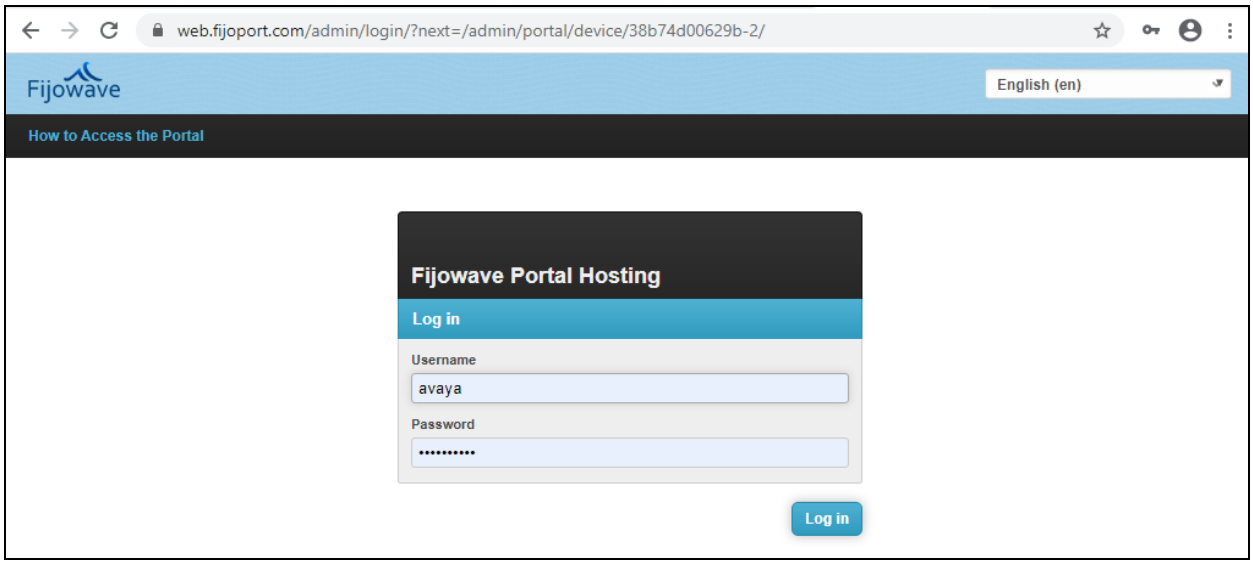


The ticket information shows that a **TrunkGroupAlarm** was created. There are no more details shown until the user logs into the IP Office in question to investigate the problem. This is shown in **Section 7.4**.

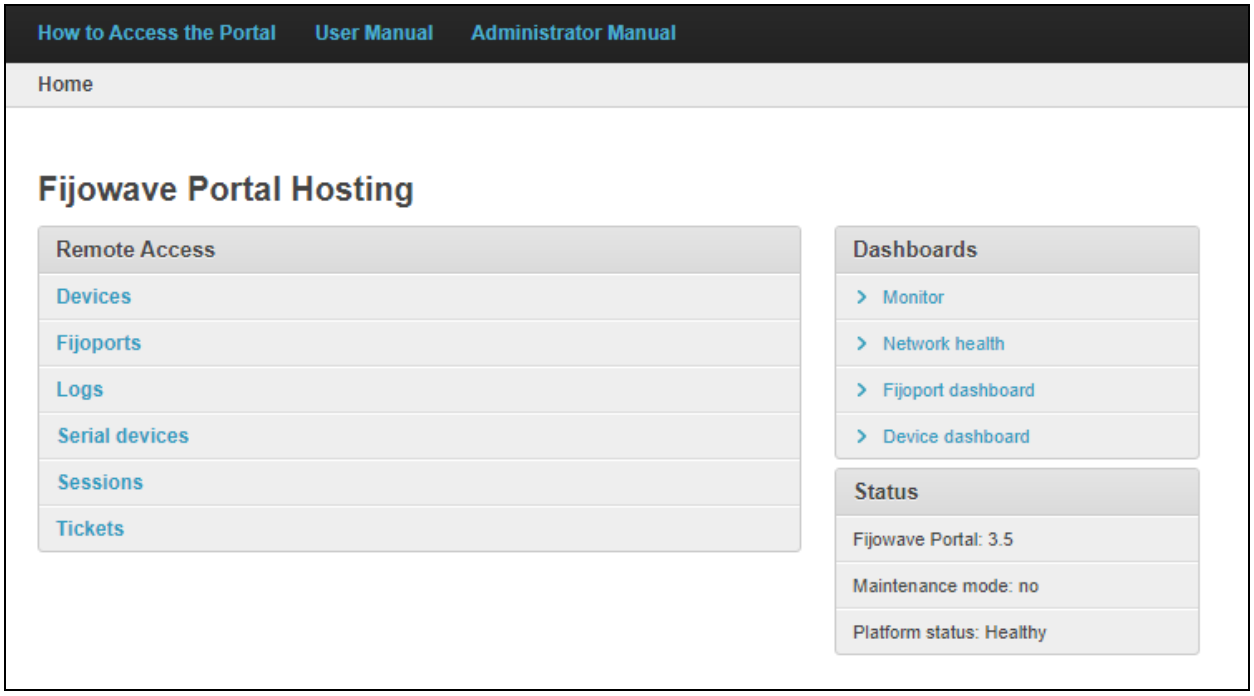


7.3. Verify connection to Fijoport

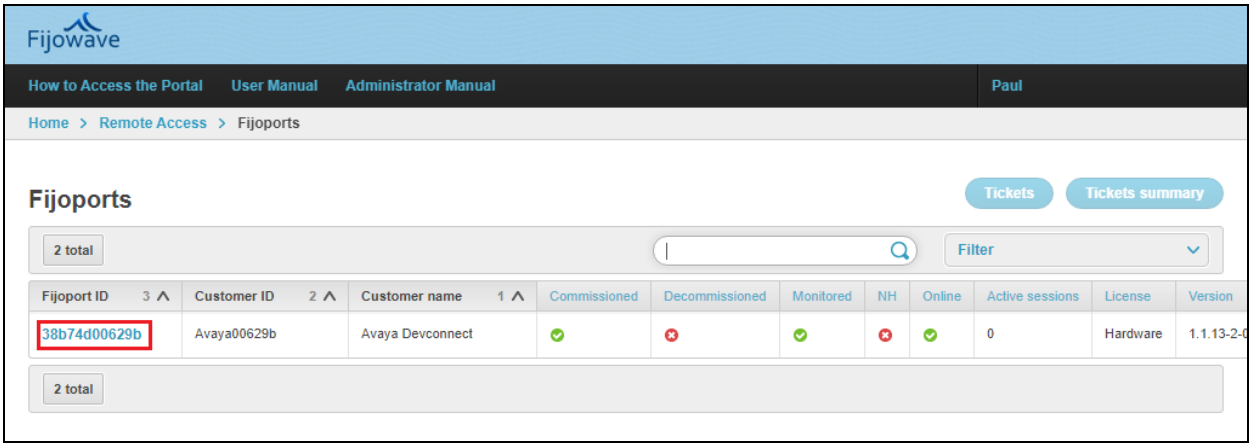
Open a URL to **web.fijoport.com** as shown below, enter the appropriate credentials and click on **Log in**.



Click on **Fijoports**.

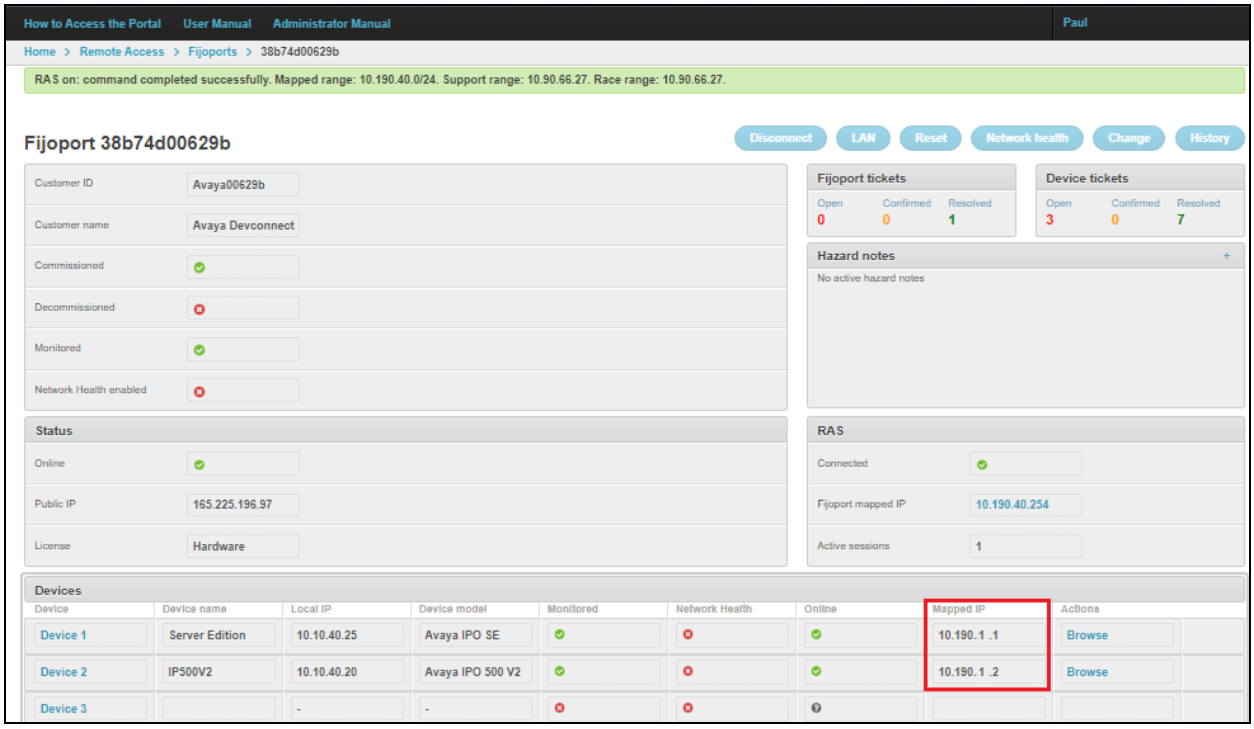


Click on the appropriate **Fijoport ID**. For compliance testing only one Fijoport was used, so there is only one choice displayed. On sites where many Fijoports are in use, click on the Fijoport ID to be accessed.



Click on **Connect** at the top.

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.



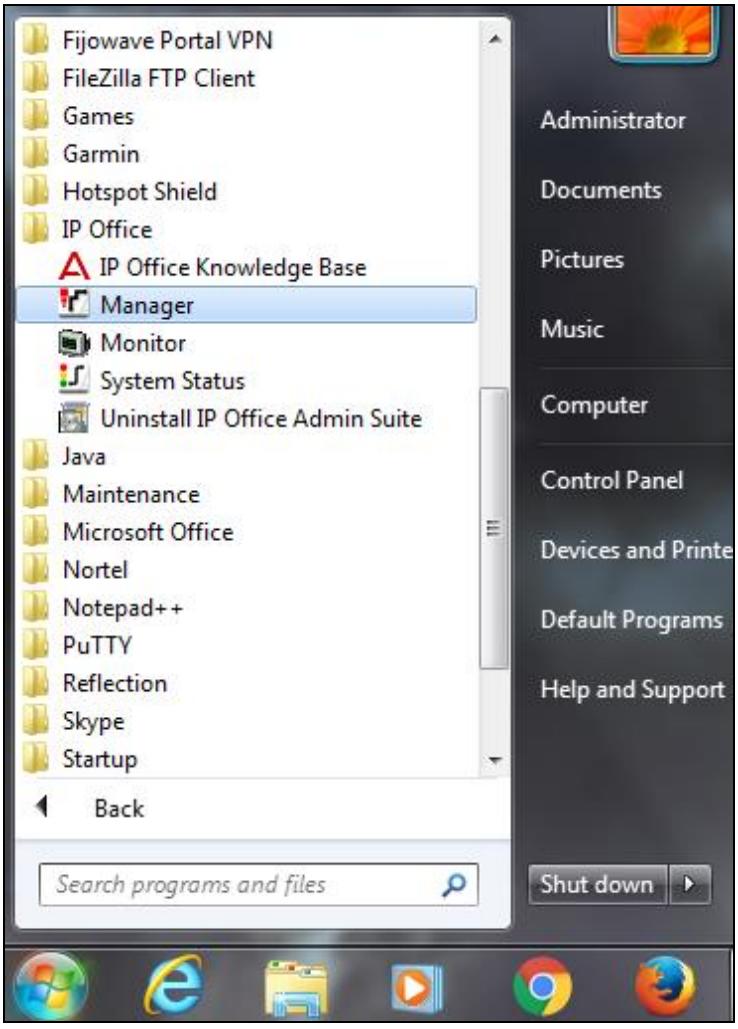
Using the **Mapped IP** from above the IP Office Manager and System Monitor can be used to access the IP office using these IP addresses to connect to each device, see **Section 7.4**.

7.4. Verify Remote Access IP Office connections

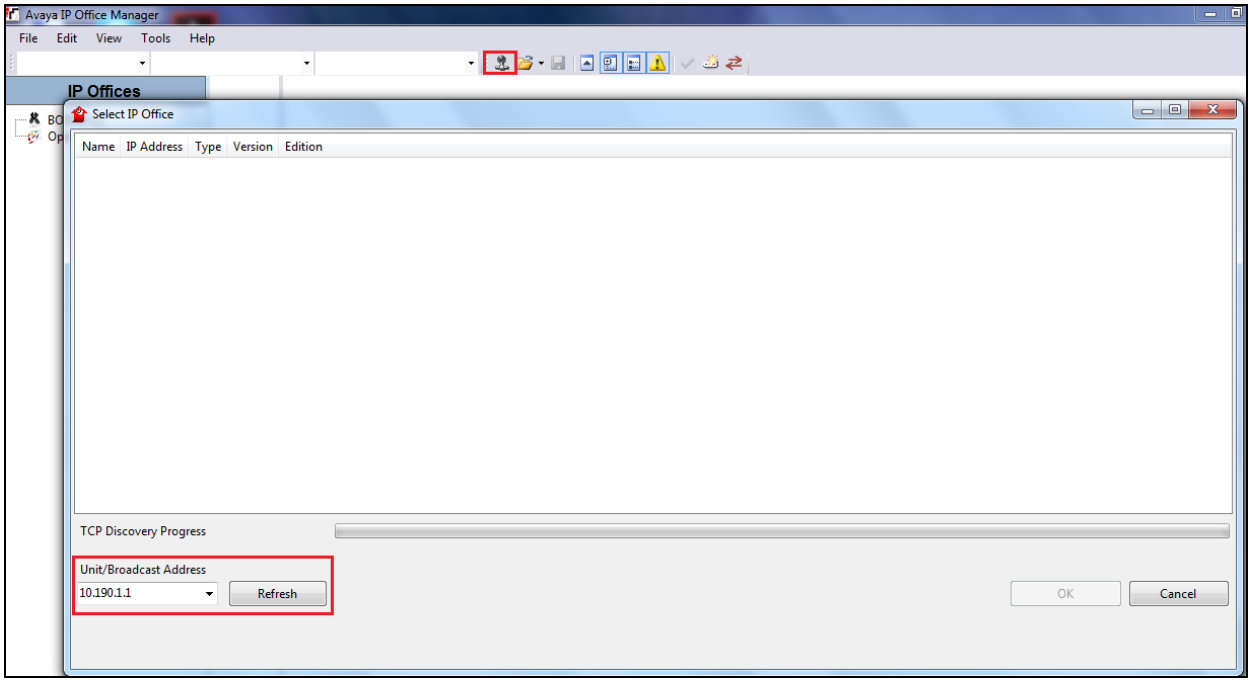
Once the secure tunnel is established to the IP Office, the IP Office clients can be used to connect to each of the Server Edition and the IP500 V2. To verify that Fijoport Remote Access is fully working, from the PC running the Fijowave Portal VPN, open the three IP Office applications, IP Office Manager,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

7.4.1. Verify IP Office Manager

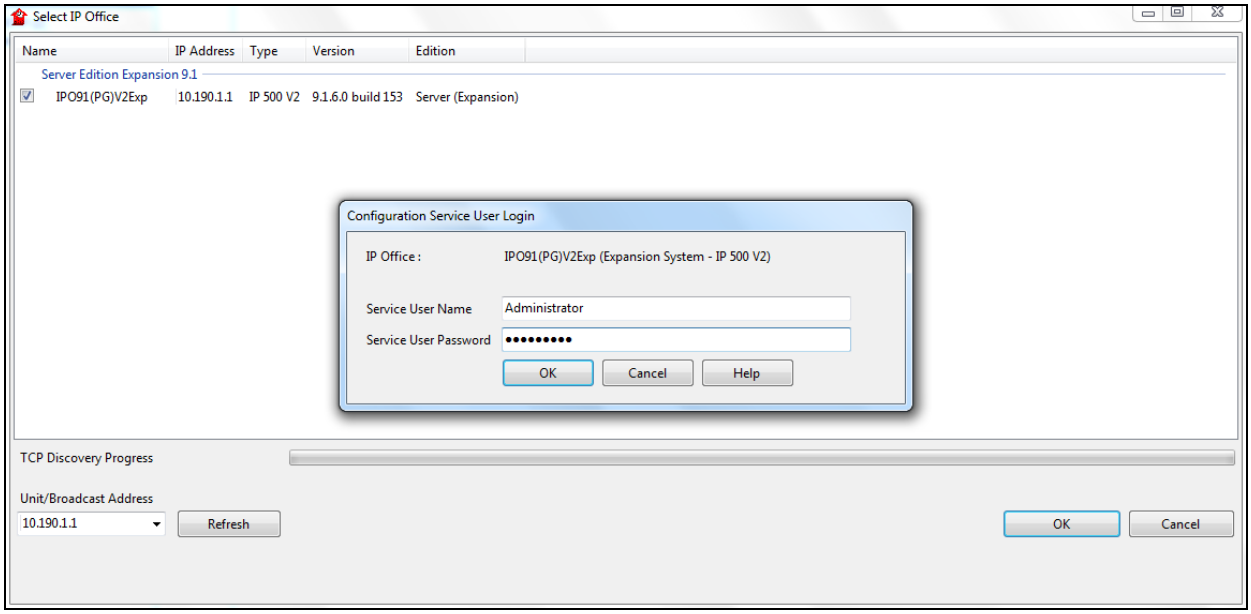
Open the IP Office Manager either from the desktop shortcut or from **Programs → IP Office** as shown below.



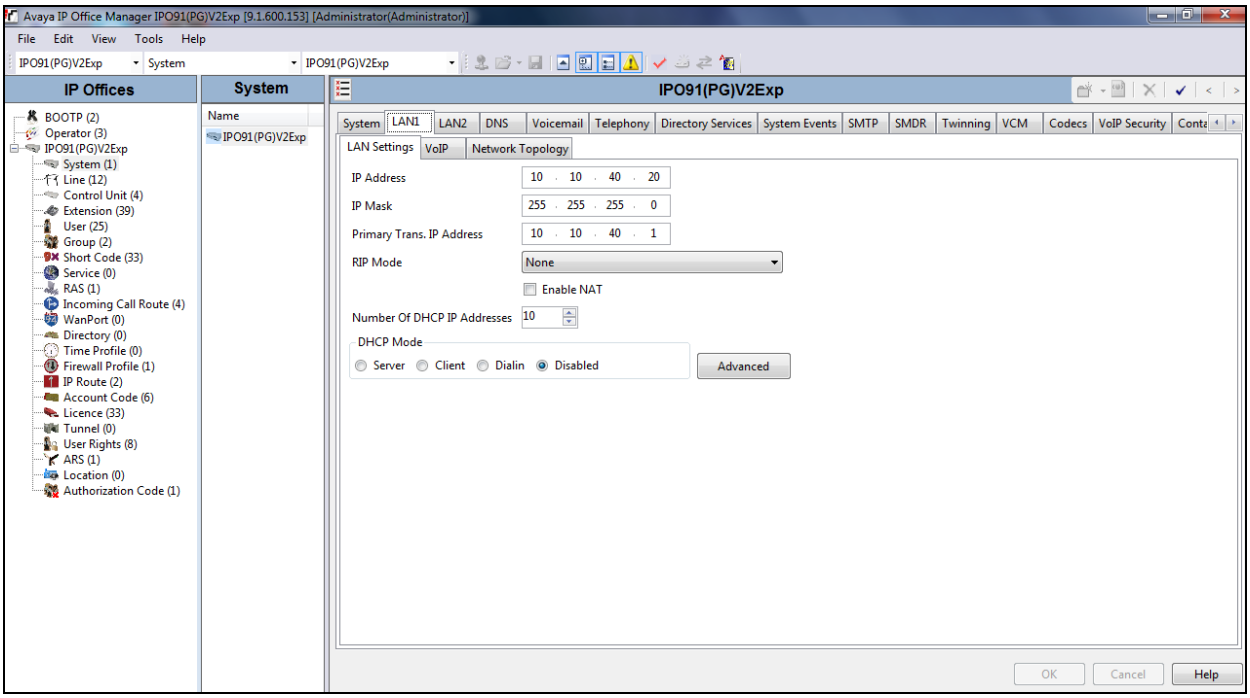
The **Unit Broadcast Address** will need to be set to that of the **Mapped IP** found in **Section 7.3**. The mapped IP address is entered, and **Refresh** is pressed and that should bring up the IP Office unit.



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.



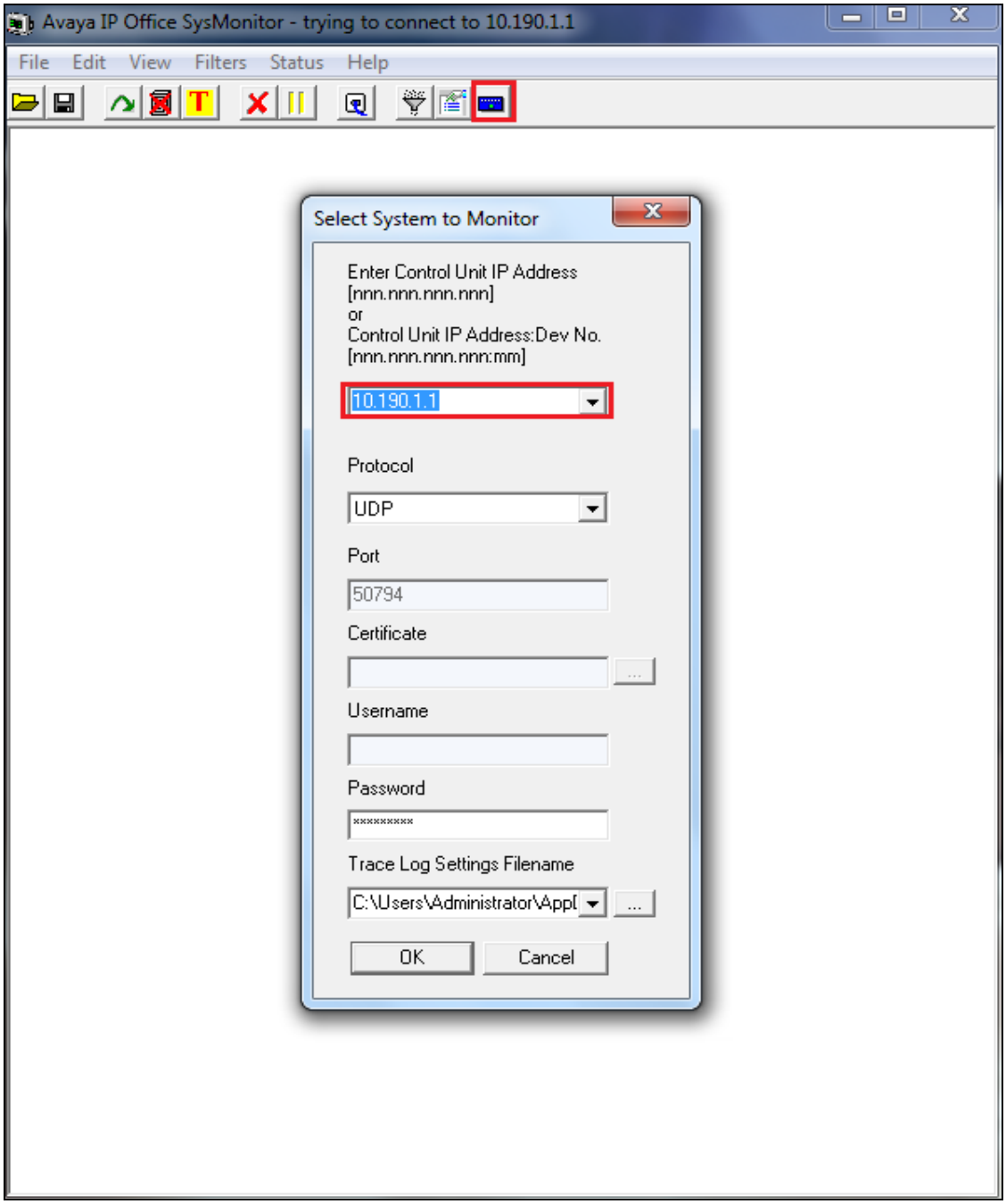
The IP Office Manager screen should be opened and should appear something like shown below where changed can be made and saved (not shown).



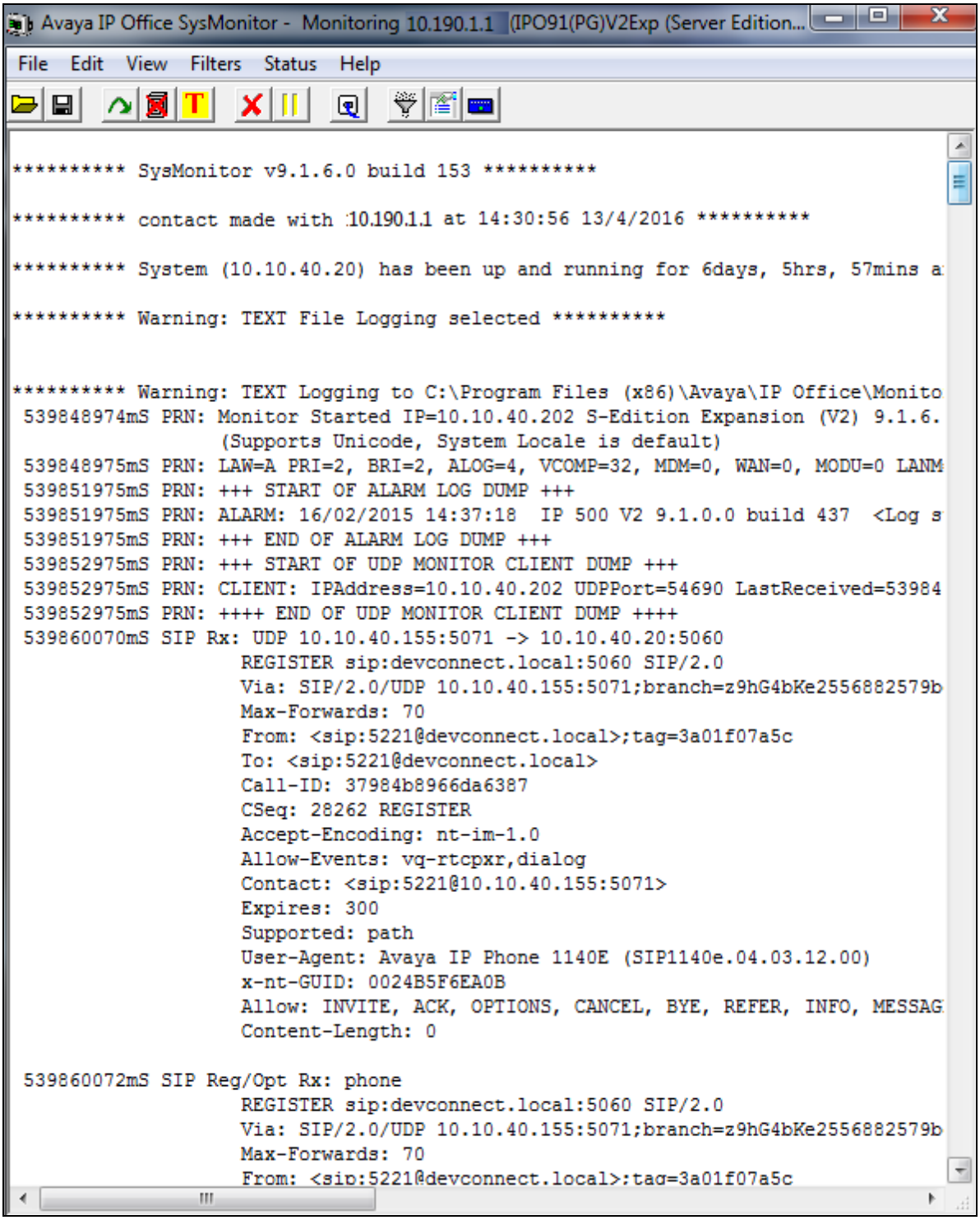
7.4.2. Verify IP Office Monitor

IP Office Monitor is accessed in the same was as IP Office Manager is from **Section 7.4.1**. 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 7.3**. Click on OK and the monitor should start correctly.



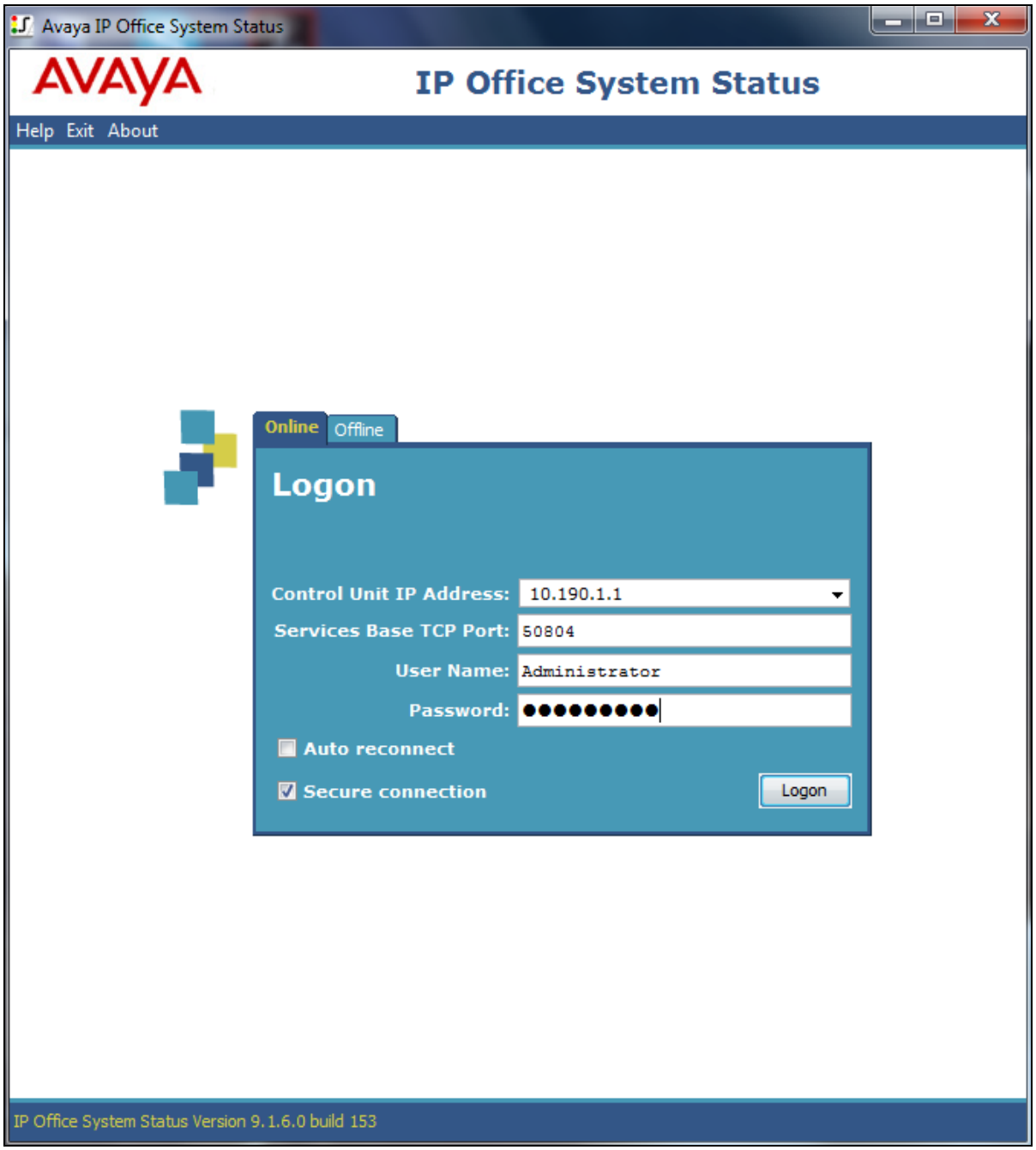
The monitor should now display information on IP Office correctly.



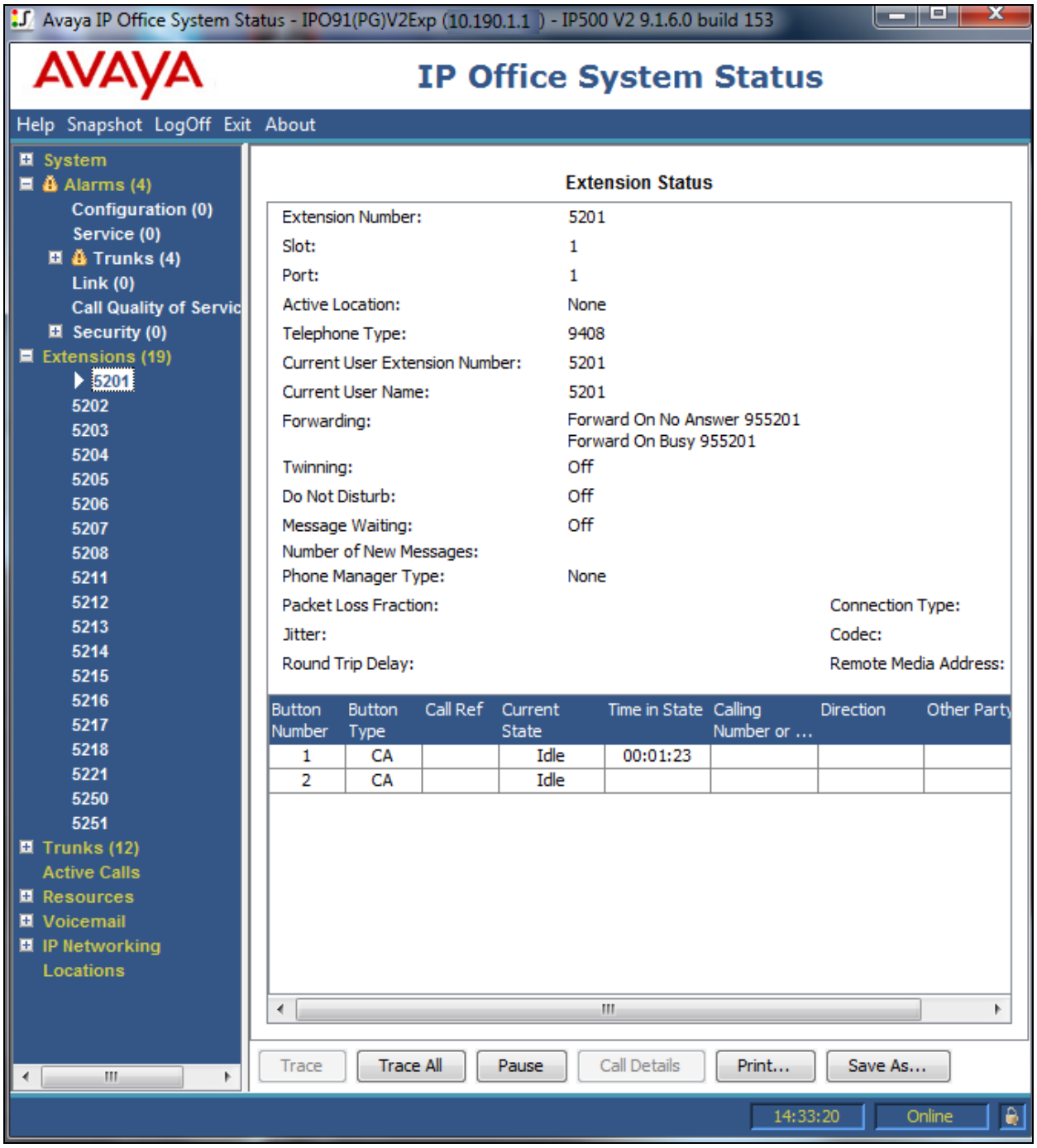
7.4.3. Verify IP Office System Status

IP Office System Status is accessed in the same was as IP Office Manager is from **Section 7.4.1**. 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 7.3**, enter the log in credentials and click on **Logon** and the monitor should start correctly.



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



8. Conclusion

These Application Notes describe the configuration steps required for provisioning Fijowave's Fijoport Advanced Monitoring to interoperate with Avaya IP Office IP500V2 standalone R11.0. It has been verified that the Fijoport solution allows both the monitoring of the IP Office IP500 V2 and a secure connection to IP Office to 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
- 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.