Avaya Solution & Interoperability Test Lab

Application Notes for configuring Fijowave Fijoport Remote Access with the Avaya Aura® Platform– Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Fijowave's Fijoport Remote Access to access the Avaya Aura® Platform. The Avaya Aura® Platform is a list of Avaya products which can be found in **Section 4**, these being from the Avaya Aura® core telephony products.

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 allow a remote access connection to administer and maintain Avaya's core telephony products.

Fijoport Remote Access (Fijoport) is used as a remote access device with the Avaya Aura® Platform. 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.

Once the VPN tunnel between the Fijoport and Fijowave Portal server has been established, the various Avaya components configured on the Fijoport will have Mapped IP addresses associated with them, allowing access from any PC running the Open VPN client. For example, Avaya Aura® System Manager has a "lab IP address" of 10.10.40.10, this is obviously not accessible from the outside world and even with the Fijoport establishing a connection to the Fijowave Portal server, this same address is useless to anyone trying to establish a connection. However, the Fijoport solution maps a new virtual IP address. That new mapped IP is what is used by the user trying to access System Manager. This same concept is used for all Avaya applications that are to be accessed, and this may be using PuTTY or a Web Browser or an FTP program such as FileZilla.

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 the Avaya Aura® Platform. Remote access is provided to a PC from outside the Avaya DevConnect LAN, allowing the user on that PC administer and maintain the Avaya devices listed in **Section 4**. The PC uses OpenVPN and the Fijowave Portal to establish a connection to the Avaya DevConnect lab and using Mapped IP addresses provided by the Fijowave Portal a http session or a PuTTY session can be opened to the device in question as if the user was on the DevConnect LAN.

Some definitions used to describe the connection are as follows.

- VPN - Virtual Private Network
- RAS - Remote Access Session
- CSE - Customer Support Engineer
- SMS - Short Message Service

The solution test involved 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 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. The CSE logs onto the Operator interface via the Fijowave Portal VPN and instructs the Portal server to establish a remote access session

(RAS) to specified customer network equipment via the Fijoport box. The CSE runs applications locally on a 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, used by Fijowave to setup a secure tunnel to the Avaya network.

2.1. Interoperability Compliance Testing

The compliance testing includes the test scenarios shown below.

- Avaya Aura® System Manager R10.1
    - Open an SSH session using PuTTY to navigate and issue commands
    - Open a file sharing session using FileZilla, transfer a file back and over
    - Open a web browser session for configuration
- Avaya Aura® Session Manager R10.1
    - Open an SSH session using PuTTY to navigate and issue commands (traceSM)
    - Open a file sharing session using FileZilla, transfer a file back and over
- Avaya Aura® Communications Manager R10.1
    - Open an SSH session using PuTTY to navigate and issue commands
    - Open a web browser session for configuration
- Avaya Aura® Applications Enablement Services R10.1
    - Open an SSH session using PuTTY to navigate and issue commands
    - Open a web browser session for configuration
- Avaya Aura® Media Server R10.1
    - Open an SSH session using PuTTY to navigate and issue commands
    - Open a web browser session for configuration

- Avaya Aura® Contact Center R10.1
    - Open a web browser session for configuration
- Avaya Aura® Experience Portal R10.1
    - Open an SSH session using PuTTY to navigate and issue commands
    - Open a web browser session for configuration
- Avaya Messaging R10.1
    - Use the Messaging Client for configuration

2.2. Test Results

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

1. The Firewall where the Avaya devices are located will need to allow an outbound SSH connection take place over port 443.
2. The Browse button will need to be altered for most of the Avaya Web Browser connections as the default (http://<IPAddress>) is not valid for most of the Avaya applications that are accessible via web browser, see **Section 6.2**.
3. A connection from an Avaya Softphone is not possible as the Mapped IP address is still an address outside of the Enterprise and is thus deemed a public IP address and should be connected via Avaya Session Border Controller as a Remote Worker.

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 and establishes a secure connection with a Portal server appliance hosted by Fijowave. Authorized users can establish a connection to the various Avaya products 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.

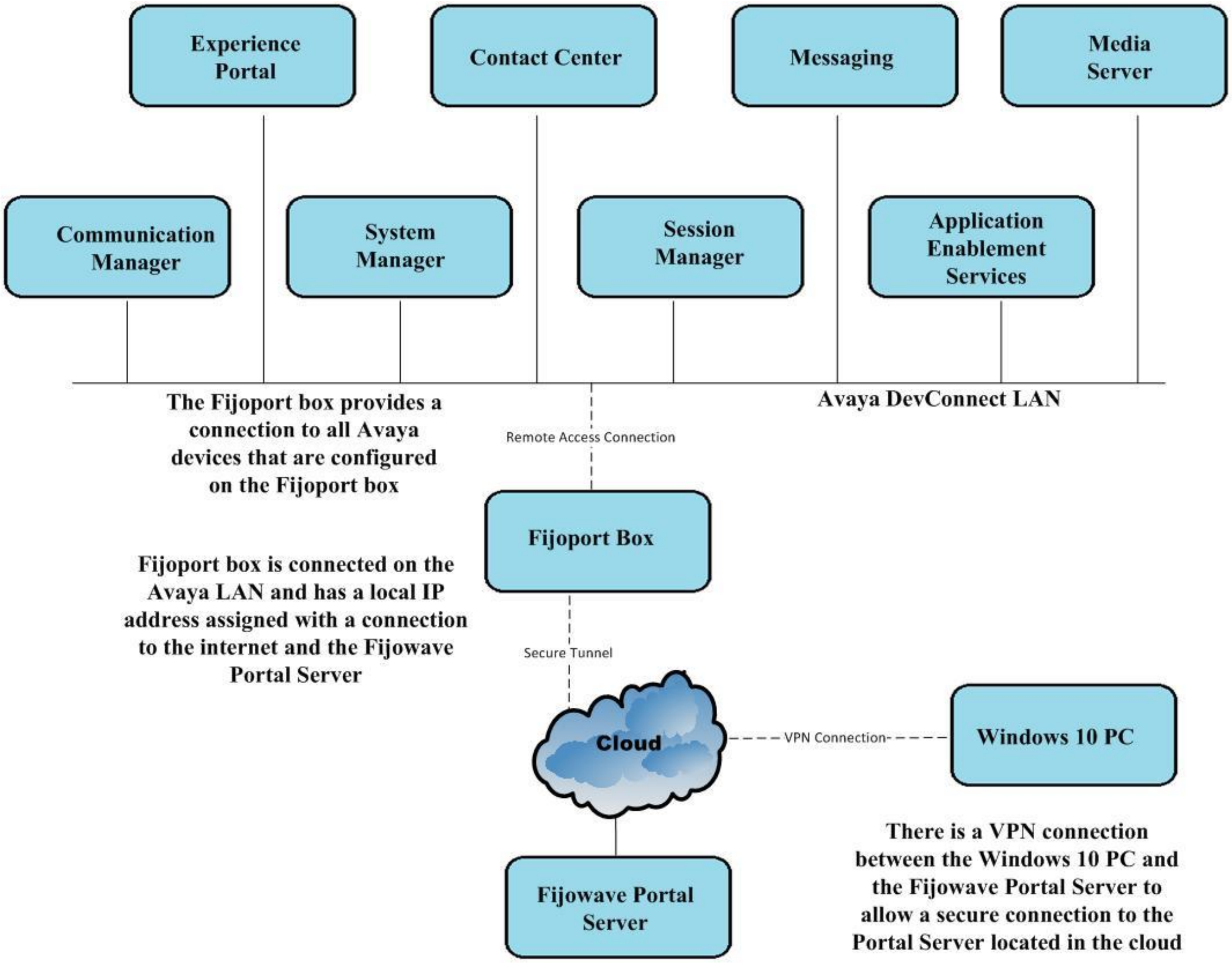

Experience Portal
Contact Center
Messaging
Media Server
Communication Manager
System Manager
Session Manager
Application Enablement Services
Avaya DevConnect LAN
The Fijoport box provides a connection to all Avaya devices that are configured on the Fijoport box
Remote Access Connection
Fijoport Box
Fijoport box is connected on the Avaya LAN and has a local IP address assigned with a connection to the internet and the Fijowave Portal Server
Secure Tunnel
Cloud
VPN Connection
Windows 10 PC
There is a VPN connection between the Windows 10 PC and the Fijowave Portal Server to allow a secure connection to the Portal Server located in the cloud
Fijowave Portal Server

Figure 1: Reference configuration of Fijowave Fijoport Remote Access with the Avaya Aura® Platform

4. Equipment and Software Validated

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

Equipment/Software	Release Version
Avaya Aura® System Manager running on a virtual server	10.1.0.0 Build No. – 10.1.0.0.537353 SW Update Revision No: 10.1.0.0.0614254
Avaya Aura® Session Manager running on a virtual server	10.1 Build No. – 10.1.0.0.1010019
Avaya Aura® Communication Manager running on a virtual server	10.1 Update ID 01.0.974.0-27293
Avaya Messaging running on MS Windows Server 2019	10.8.20.1502
Avaya Aura® Application Enablement Services	10.1.0.0.0.11-0
Avaya Aura® Media Server	8.0.2.184
Avaya Aura® Contact Center	7.1.2.0
Avaya Experience Portal	8.1.0.0.0337
Fijowave Fijoport Box	2.0
Fijowave Portal VPN	2.4
Fijowave Portal Server	3.8

5. Configure Avaya Aura® Platform

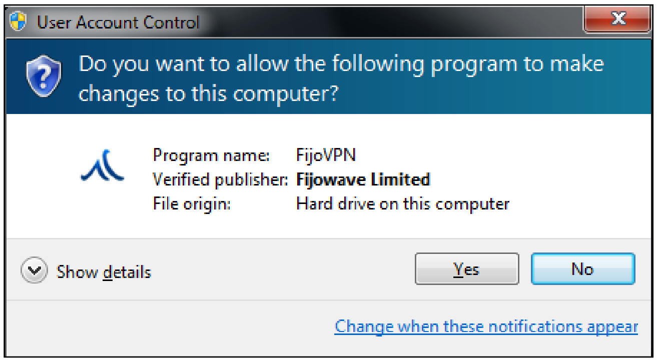
There was no specific configuration of any kind on any of the Avaya products involved in the compliance testing. All configurations took place on the Fijoport, the Open VPN Client and Fijowave Portal server.

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 Fijowave 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, FijowavePortalServer2.4.rar, browse to the Fijowave Portal VPN directory and run the installer FijoVPN-2.4.x-xxxx.exe (not shown). Click **Yes** if User Account Control asks permission to proceed.

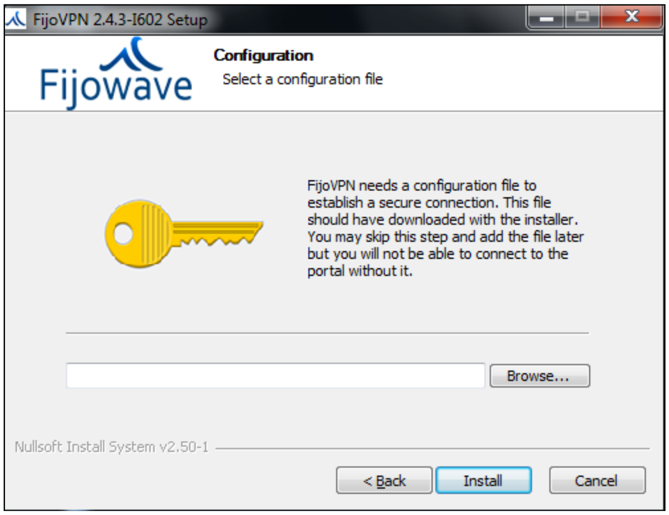


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: FijoVPN
Verified publisher: **Fijowave Limited**
File origin: Hard drive on this computer

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

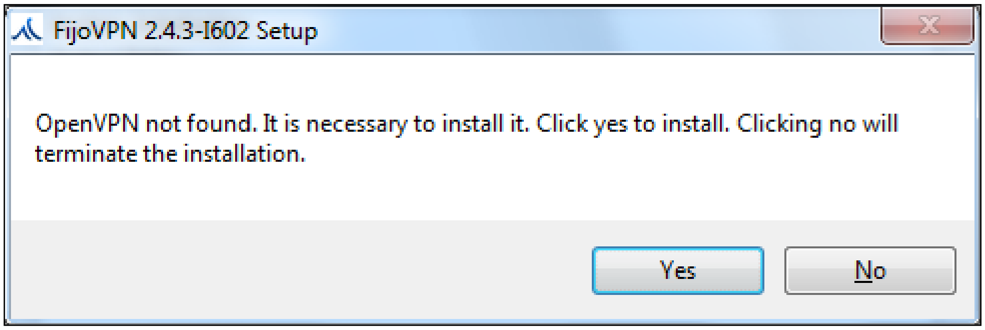


FijoVPN 2.4.3-I602 Setup

Configuration
Select a configuration file

FijoVPN needs a configuration file to establish a secure connection. This file should have downloaded with the installer. You may skip this step and add the file later but you will not be able to connect to the portal without it.

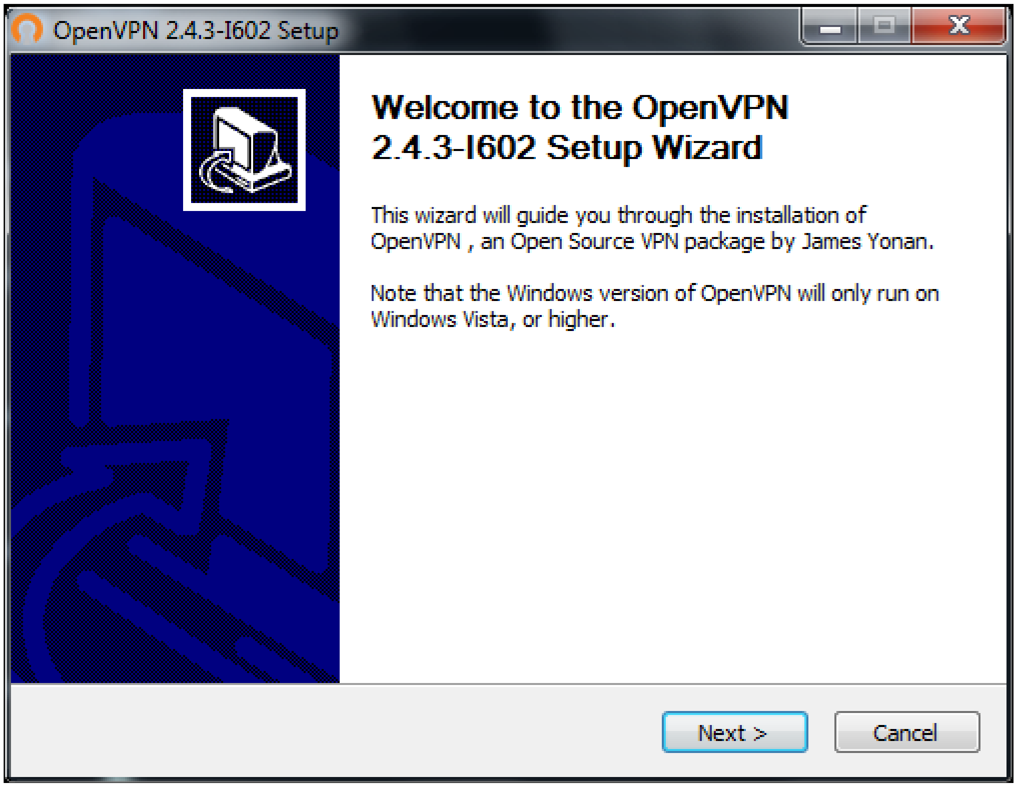
If OpenVPN is not already installed, then install it by clicking **Yes** and following the OpenVPN installation instructions.



FijoVPN 2.4.3-I602 Setup

OpenVPN not found. It is necessary to install it. Click yes to install. Clicking no will terminate the installation.

Click on **Next** to continue.



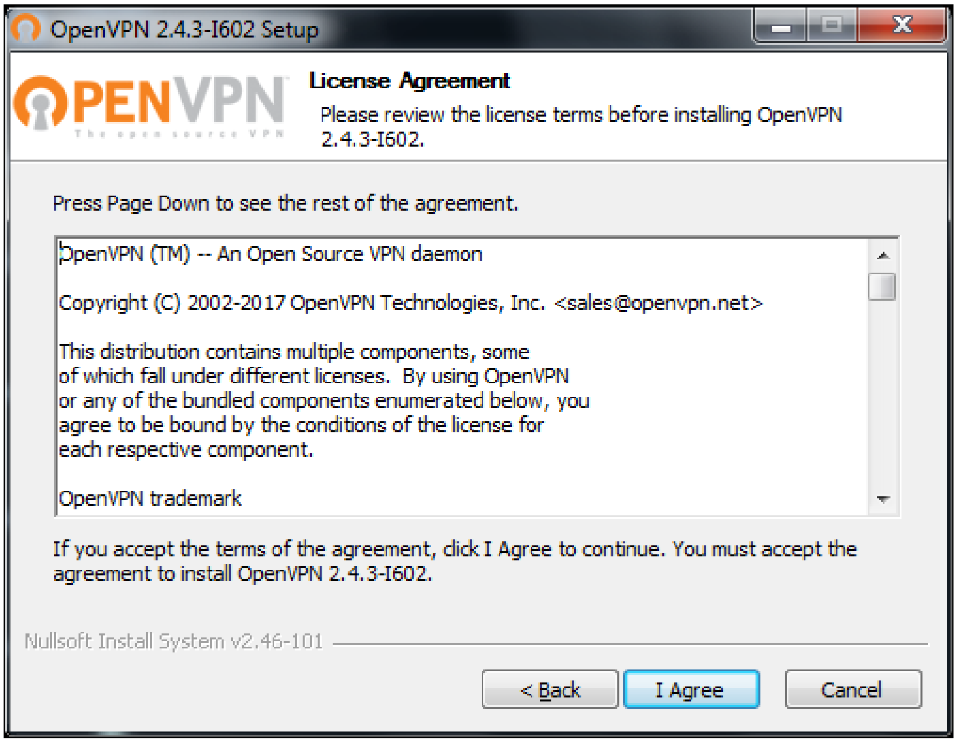
OpenVPN 2.4.3-I602 Setup

Welcome to the OpenVPN 2.4.3-I602 Setup Wizard

This wizard will guide you through the installation of OpenVPN , an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN will only run on Windows Vista, or higher.

Click on **I Agree** to continue.



OpenVPN 2.4.3-I602 Setup

License Agreement

Please review the license terms before installing OpenVPN 2.4.3-I602.

Press Page Down to see the rest of the agreement.

OpenVPN (TM) -- An Open Source VPN daemon

Copyright (C) 2002-2017 OpenVPN Technologies, Inc. <sales@openvpn.net>

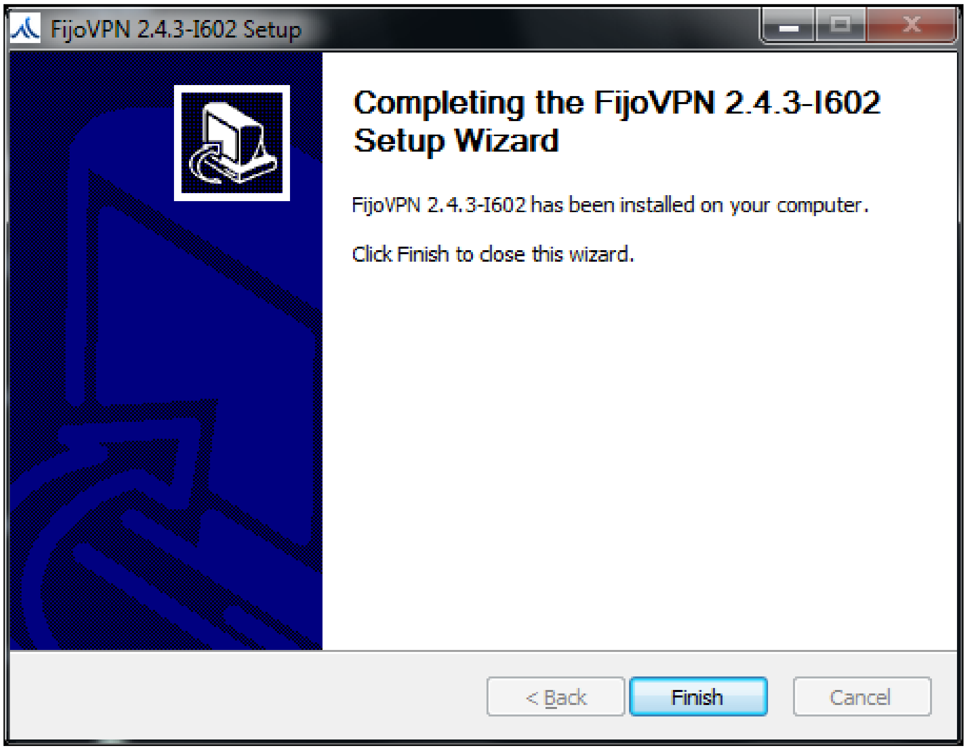
This distribution contains multiple components, some of which fall under different licenses. By using OpenVPN or any of the bundled components enumerated below, you agree to be bound by the conditions of the license for each respective component.

OpenVPN trademark

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.4.3-I602.

Nullsoft Install System v2.46-101

Close the installer by clicking **Finish**.



FijoVPN 2.4.3-I602 Setup

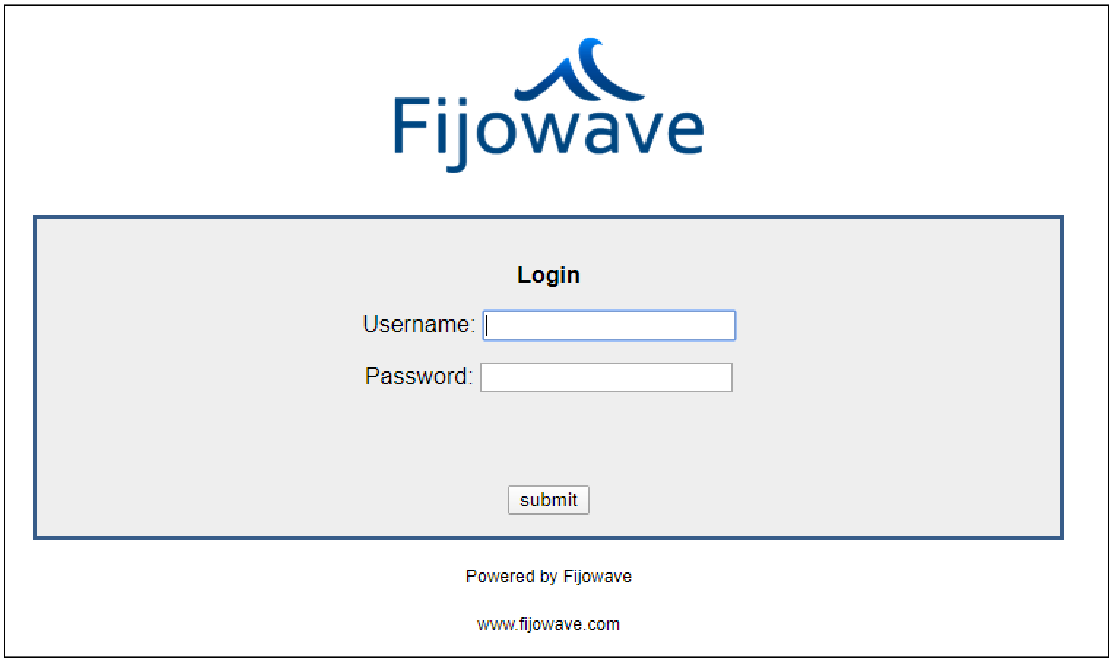
Completing the FijoVPN 2.4.3-I602 Setup Wizard

FijoVPN 2.4.3-I602 has been installed on your computer.

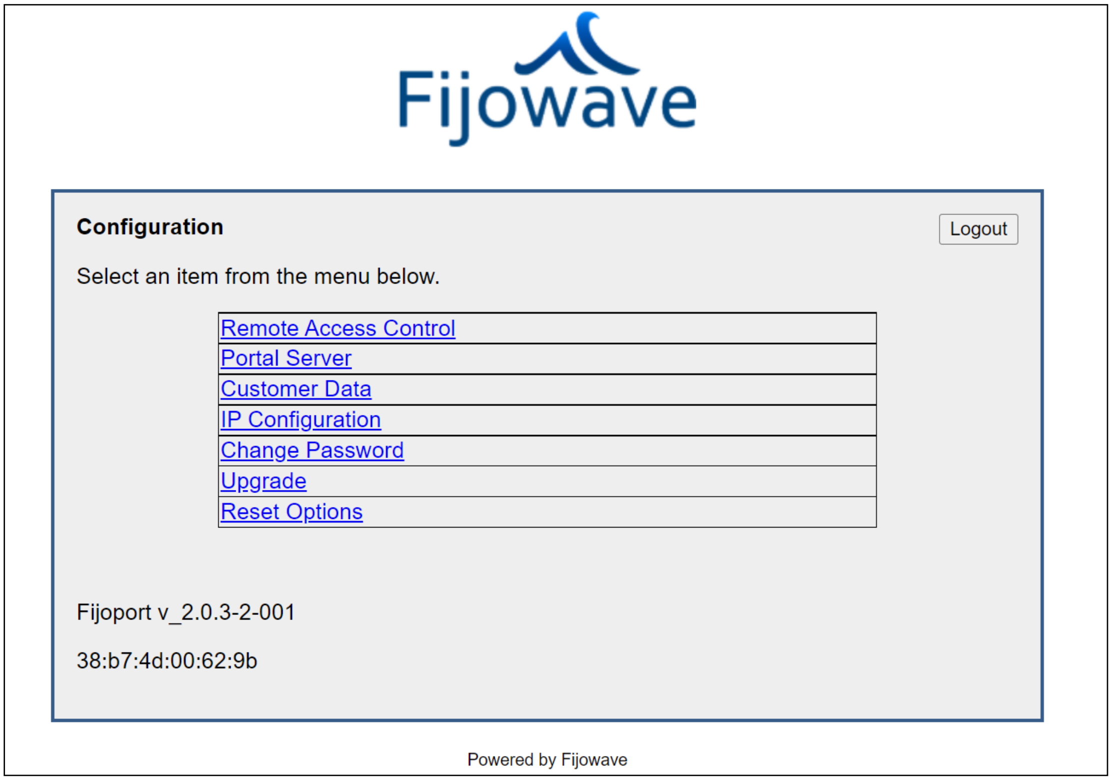
Click Finish to close this wizard.

6.2. Configure Fijowave Fijoport

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



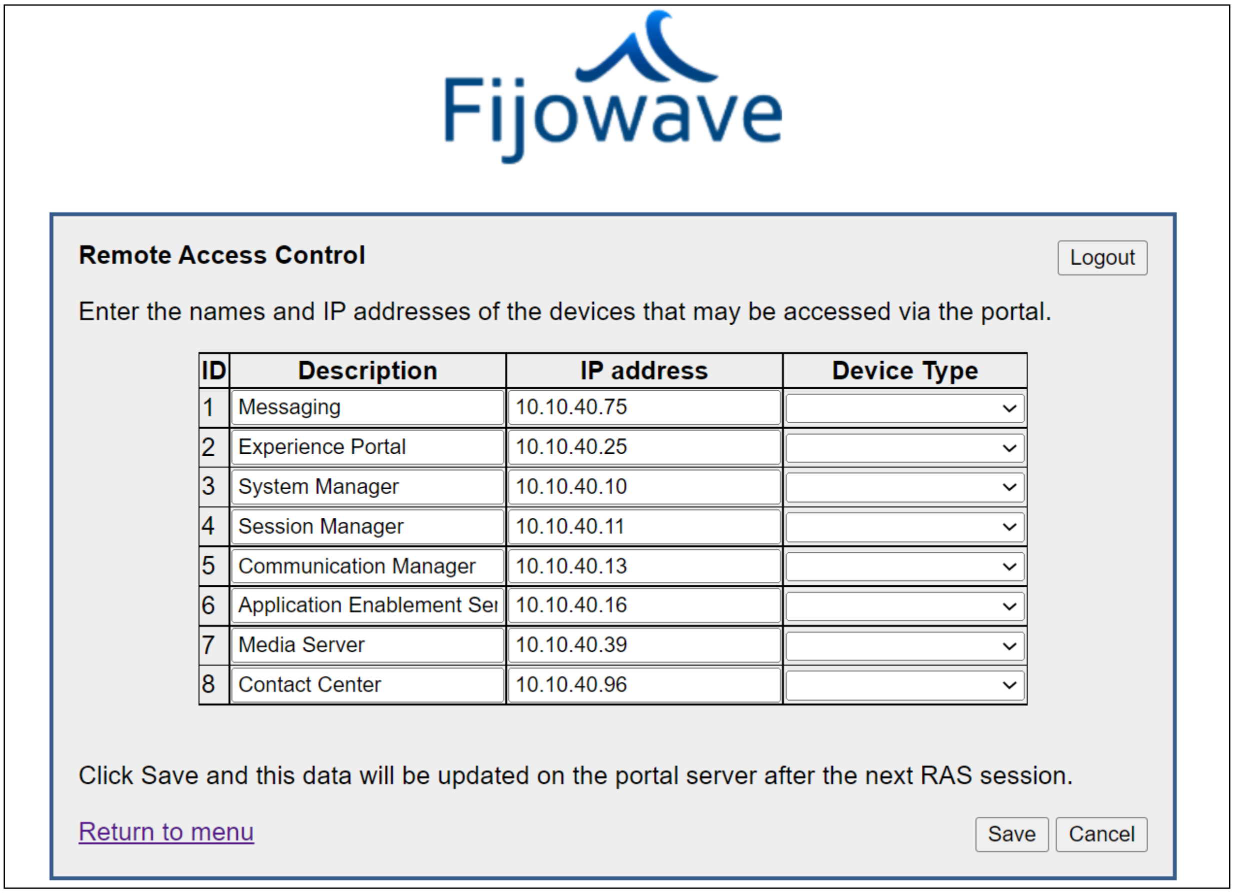
Click on the **Remote Access Control** link.



Fijoport v_2.0.3-2-001

38:b7:4d:00:62:9b

The Avaya products that are to be accessed remotely are all added here in this list. There are up to eight devices that can be added, with the devices that were accessed for compliance testing shown below.



Remote Access Control

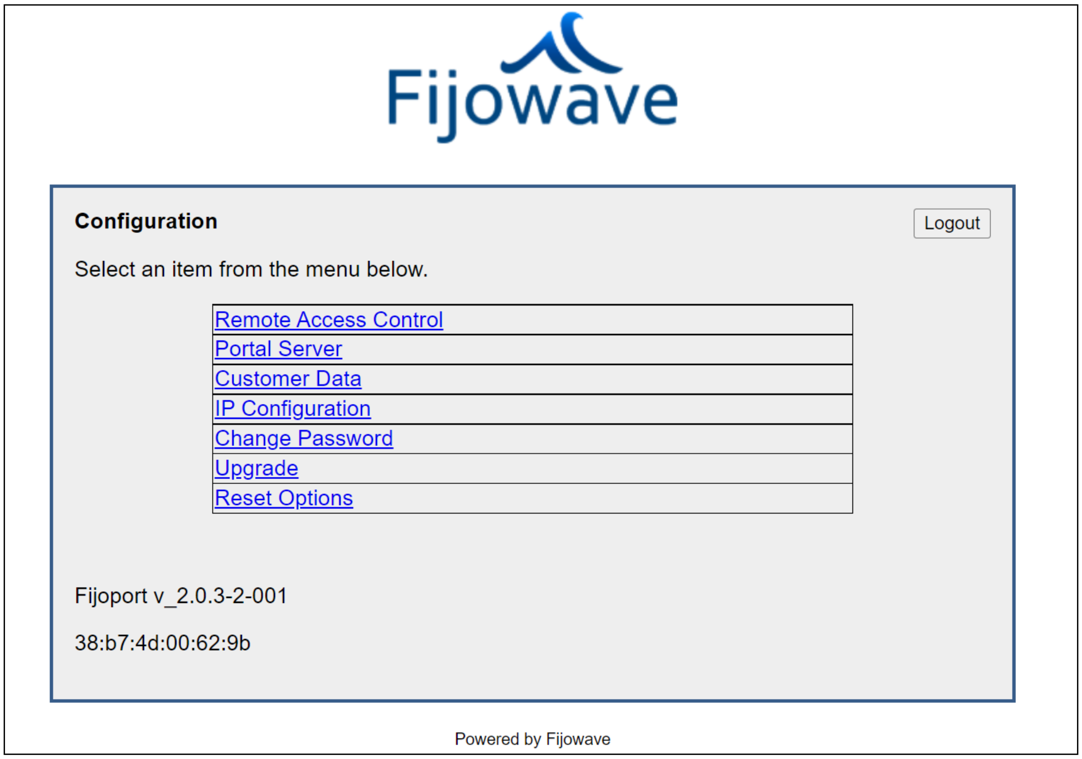
Enter the names and IP addresses of the devices that may be accessed via the portal.

ID	Description	IP address	Device Type
1	Messaging	10.10.40.75	
2	Experience Portal	10.10.40.25	
3	System Manager	10.10.40.10	
4	Session Manager	10.10.40.11	
5	Communication Manager	10.10.40.13	
6	Application Enablement Se	10.10.40.16	
7	Media Server	10.10.40.39	
8	Contact Center	10.10.40.96	

Click Save and this data will be updated on the portal server after the next RAS session.

Once the devices are all added, click on **Save** and then **Return to menu** to get back to the main menu.

Click on the **Portal Server** link.



Configuration

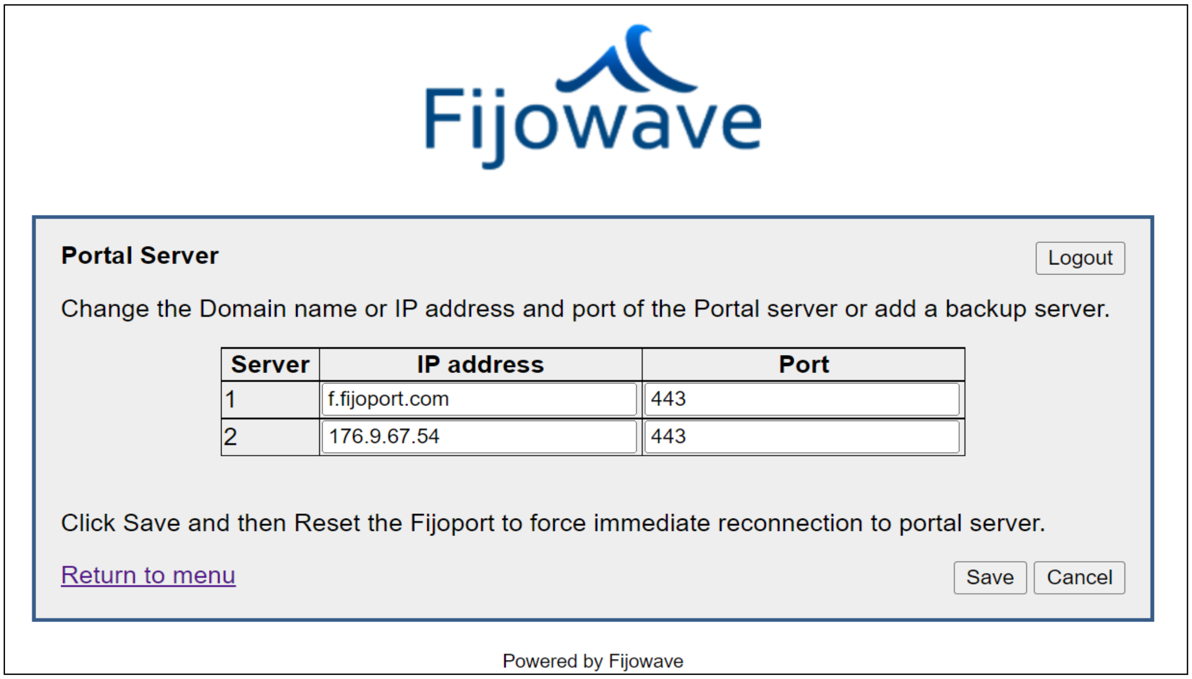
Select an item from the menu below.

Fijoport v_2.0.3-2-001

38:b7:4d:00:62:9b

Powered by Fijowave

The FQDN of the Fijowave Portal Server is added here. The **Port** will default to **443** if nothing is added. The **IP address** of the same Portal server was also added in case of any difficulties with the FQDN. Click on **Save** once the information is added.



Portal Server

Change the Domain name or IP address and port of the Portal server or add a backup server.

Server	IP address	Port
1	f.fijoport.com	443
2	176.9.67.54	443

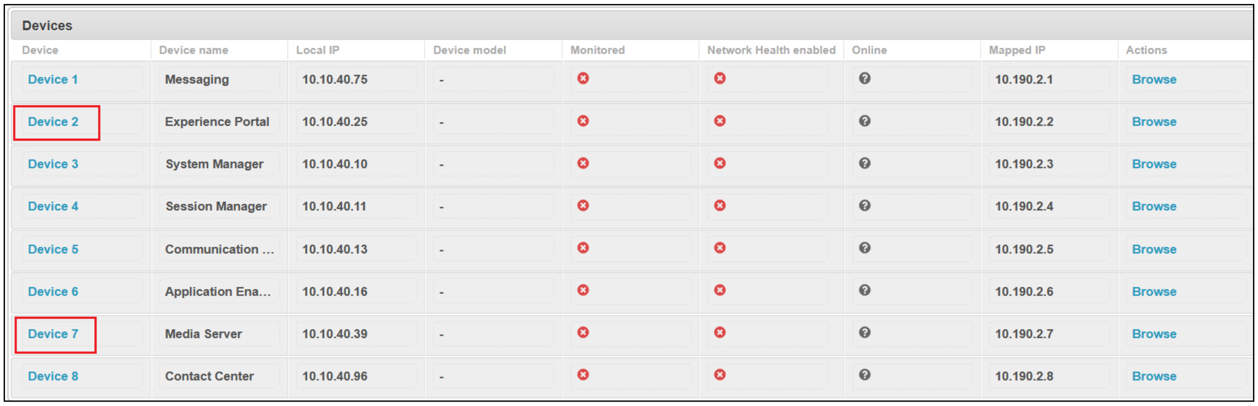
Click Save and then Reset the Fijoport to force immediate reconnection to portal server.

Powered by Fijowave

6.3. Configure URL on Fijowave Portal Server

Follow the steps in **Section 7** (verification) to connect to the Fijowave Portal Server. This section is referenced in **Section 7.2** which will lead back to this point to allow the continuation of the URL configuration.

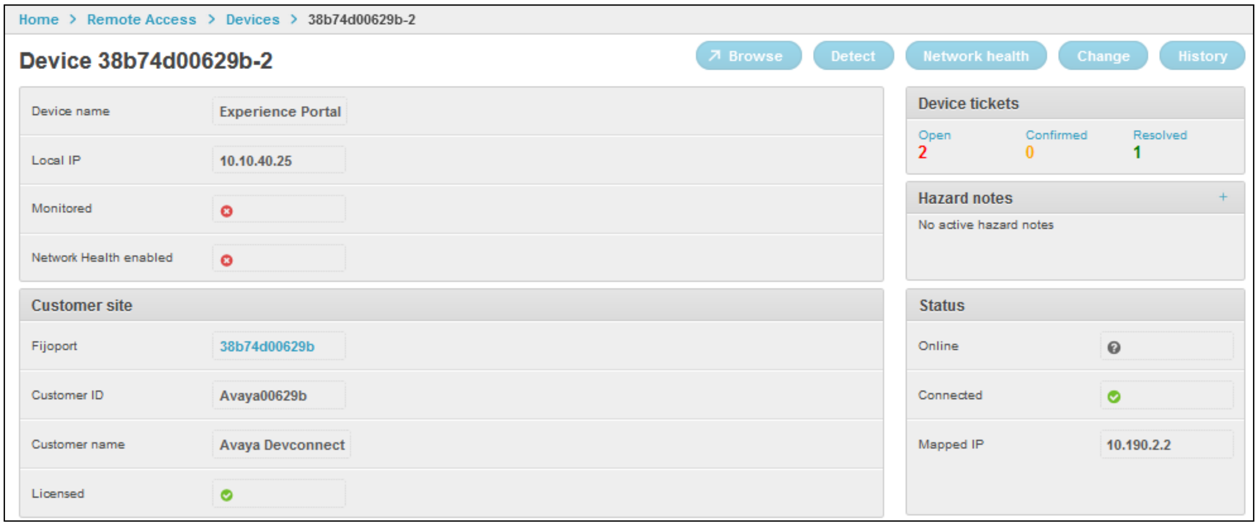
The **Devices** are shown below, to change what URL the **Browse** button will invoke, click on the Device in question. The following examples will show changes made to both **Experience Portal** and **Media Server**.



Devices

Device	Device name	Local IP	Device model	Monitored	Network Health enabled	Online	Mapped IP	Actions
Device 1	Messaging	10.10.40.75	-	✗	✗	?	10.190.2.1	Browse
Device 2	Experience Portal	10.10.40.25	-	✗	✗	?	10.190.2.2	Browse
Device 3	System Manager	10.10.40.10	-	✗	✗	?	10.190.2.3	Browse
Device 4	Session Manager	10.10.40.11	-	✗	✗	?	10.190.2.4	Browse
Device 5	Communication ...	10.10.40.13	-	✗	✗	?	10.190.2.5	Browse
Device 6	Application Ena...	10.10.40.16	-	✗	✗	?	10.190.2.6	Browse
Device 7	Media Server	10.10.40.39	-	✗	✗	?	10.190.2.7	Browse
Device 8	Contact Center	10.10.40.96	-	✗	✗	?	10.190.2.8	Browse

Clicking on **Device 2** above opens the page below. Click on **Change** at the top right of the page.



Device 38b74d00629b-2

Device name	Experience Portal
Local IP	10.10.40.25
Monitored	✗
Network Health enabled	✗

Customer site

Fijoport	38b74d00629b
Customer ID	Avaya00629b
Customer name	Avaya Devconnect
Licensed	✓

Device tickets

Open	Confirmed	Resolved
2	0	1

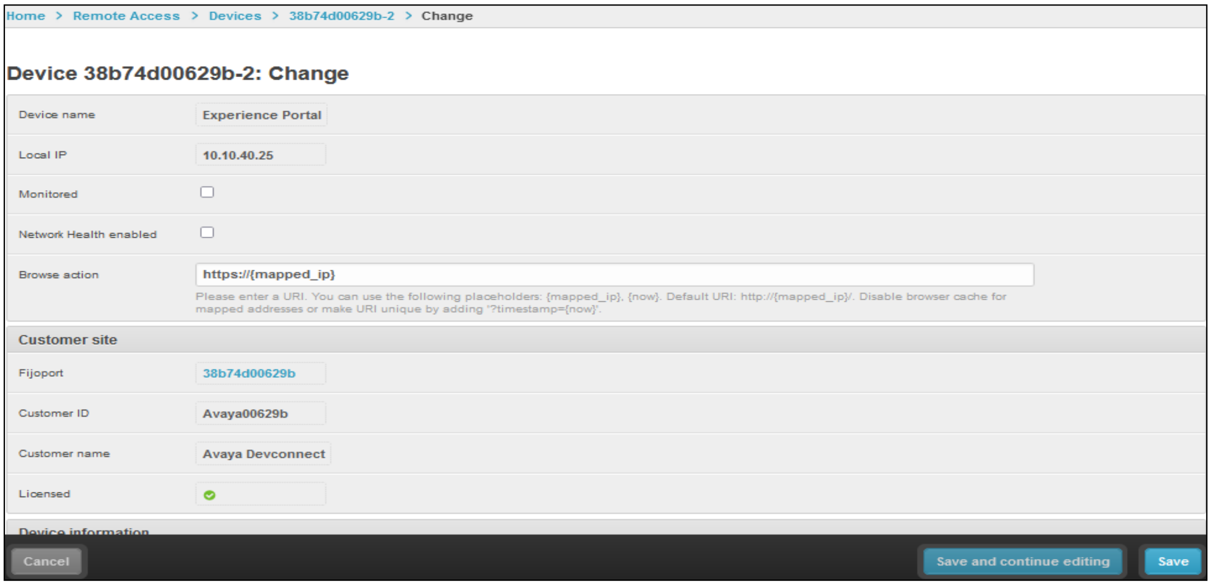
Hazard notes +

No active hazard notes

Status

Online	?
Connected	✓
Mapped IP	10.190.2.2

The **Browse action** field is changed to **https://{mapped_ip}**. This will ensure that the mapped IP address is opened but using https instead of http. Click on **Save** at the bottom right of the screen.

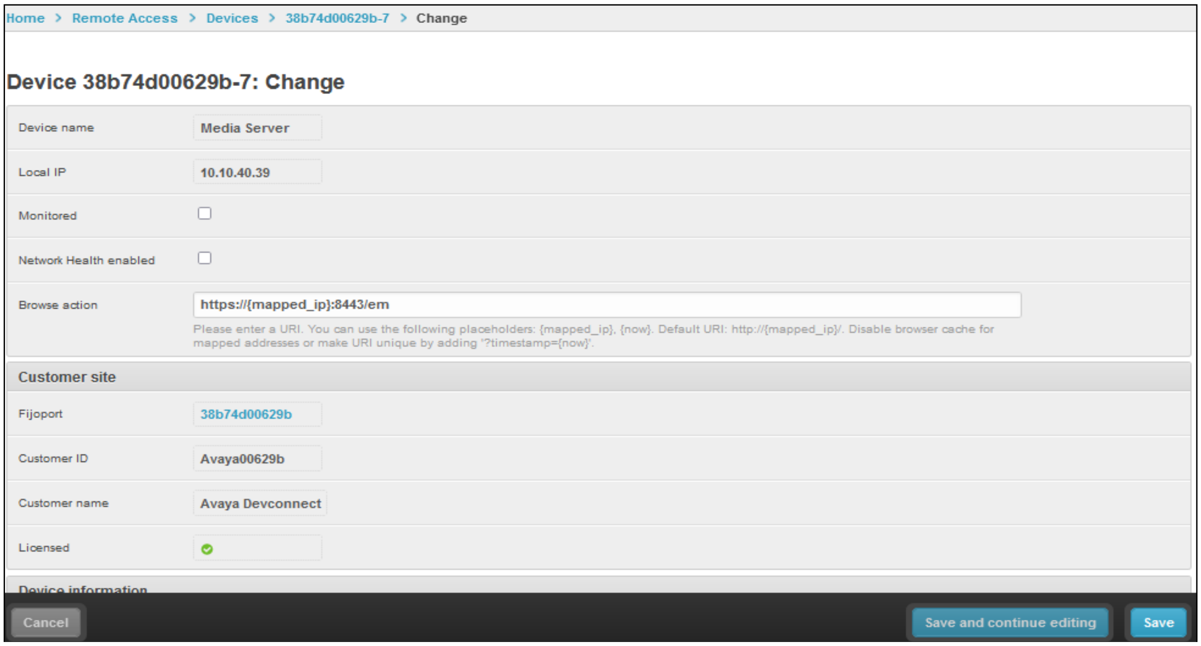


Home > Remote Access > Devices > 38b74d00629b-2 > Change

Device 38b74d00629b-2: Change

Device name	Experience Portal
Local IP	10.10.40.25
Monitored	□
Network Health enabled	□
Browse action	https://{mapped_ip} Please enter a URI. You can use the following placeholders: {mapped_ip}, {now}. Default URI: http://{mapped_ip}/. Disable browser cache for mapped addresses or make URI unique by adding '?timestamp={now}'.
Customer site	
Fijoport	38b74d00629b
Customer ID	Avaya00629b
Customer name	Avaya Devconnect
Licensed	✓

The example below shows similar changes being made for **Device 7** (Media Server). On this occasion the **Browse action** is more defined, that being **https://{mapped_ip}:8443/em**. This will ensure that once **Browse** button is pressed it will no longer go to the default http://{mapped_ip} but to the URL defined in the screen shot below, which is required to go to the login page of Media Server. Again, click on **Save** at the bottom right of the screen once this is complete.



Home > Remote Access > Devices > 38b74d00629b-7 > Change

Device 38b74d00629b-7: Change

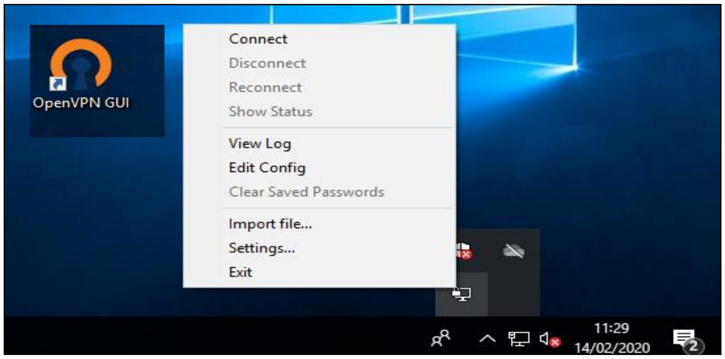
Device name	Media Server
Local IP	10.10.40.39
Monitored	□
Network Health enabled	□
Browse action	https://{mapped_ip}:8443/em Please enter a URI. You can use the following placeholders: {mapped_ip}, {now}. Default URI: http://{mapped_ip}/. Disable browser cache for mapped addresses or make URI unique by adding '?timestamp={now}'.
Customer site	
Fijoport	38b74d00629b
Customer ID	Avaya00629b
Customer name	Avaya Devconnect
Licensed	✓

7. Verification Steps

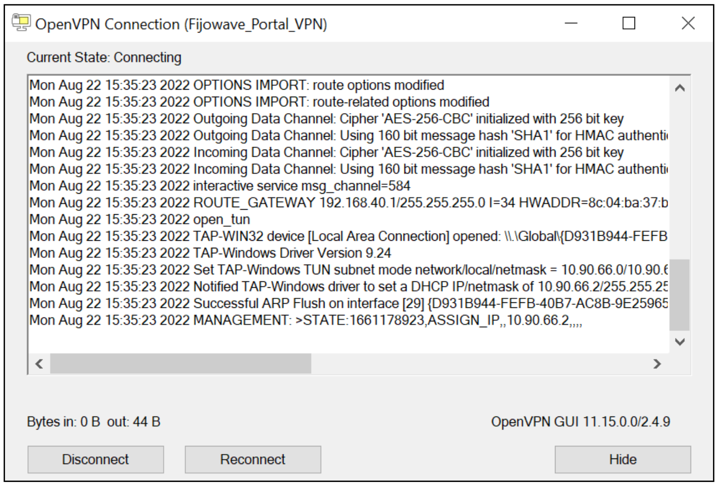
The following steps can be taken to ensure that remote access to the Avaya Aura® Platform of products is setup correctly.

7.1. Verify Fijowave Portal VPN

From a PC outside of the Avaya LAN, start the VPN application by double-clicking on the shortcut. Once the VPN 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. This may also appear on the system tray by default.



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



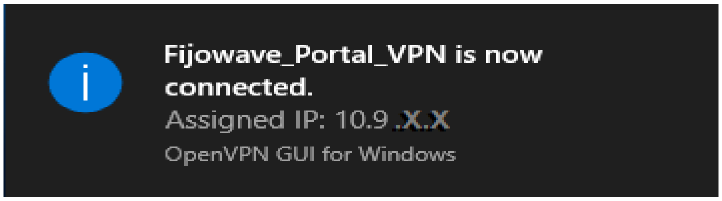
Current State: Connecting

```
Mon Aug 22 15:35:23 2022 OPTIONS IMPORT: route options modified
Mon Aug 22 15:35:23 2022 OPTIONS IMPORT: route-related options modified
Mon Aug 22 15:35:23 2022 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
Mon Aug 22 15:35:23 2022 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authenti
Mon Aug 22 15:35:23 2022 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
Mon Aug 22 15:35:23 2022 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authenti
Mon Aug 22 15:35:23 2022 interactive service msg_channel=584
Mon Aug 22 15:35:23 2022 ROUTE_GATEWAY 192.168.40.1/255.255.255.0 I=34 HWADDR=8c:04:ba:37:b
Mon Aug 22 15:35:23 2022 open_tun
Mon Aug 22 15:35:23 2022 TAP-WIN32 device [Local Area Connection] opened: \\.\Global\{D931B944-FEFB
Mon Aug 22 15:35:23 2022 TAP-Windows Driver Version 9.24
Mon Aug 22 15:35:23 2022 Set TAP-Windows TUN subnet mode network/local/netmask = 10.90.66.0/10.90.6
Mon Aug 22 15:35:23 2022 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.90.66.2/255.255.25
Mon Aug 22 15:35:23 2022 Successful ARP Flush on interface [29] {D931B944-FEFB-40B7-AC8B-9E25965
Mon Aug 22 15:35:23 2022 MANAGEMENT: >STATE:1661178923,ASSIGN_IP,,10.90.66.2,,,,
```

Bytes in: 0 B out: 44 B

OpenVPN GUI 11.15.0.0/2.4.9

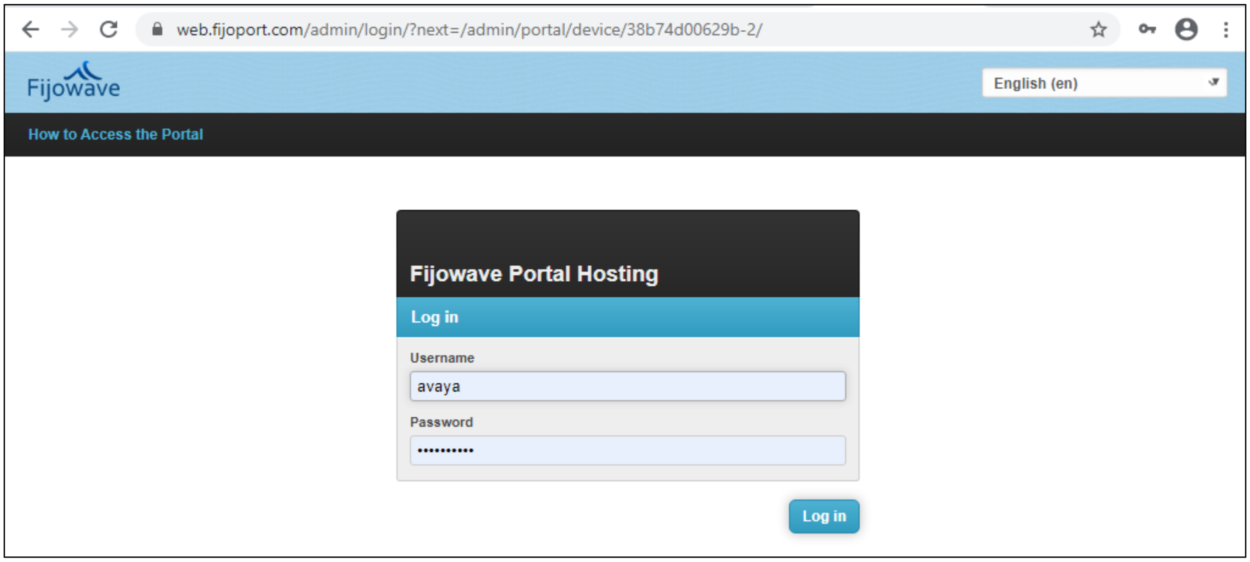
The following message verifies that the VPN is up and running and connected correctly.



Fijowave_Portal_VPN is now connected.
Assigned IP: 10.9 .X.X
OpenVPN GUI for Windows

7.2. Verify connection to Fijoport

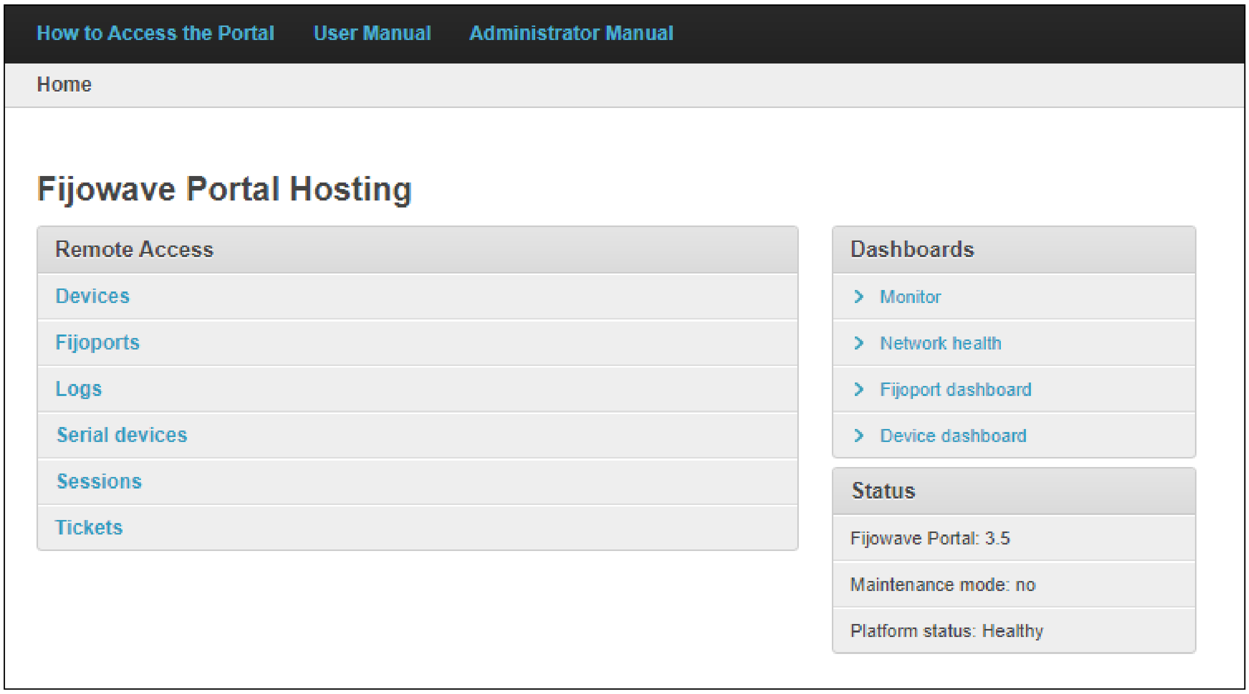
Open a URL to **web.fijoport.com** as shown below, enter the appropriate credentials and click on **Log in**.



Username: avaya

Password: ••••••••••

Click on **Fijoports**.

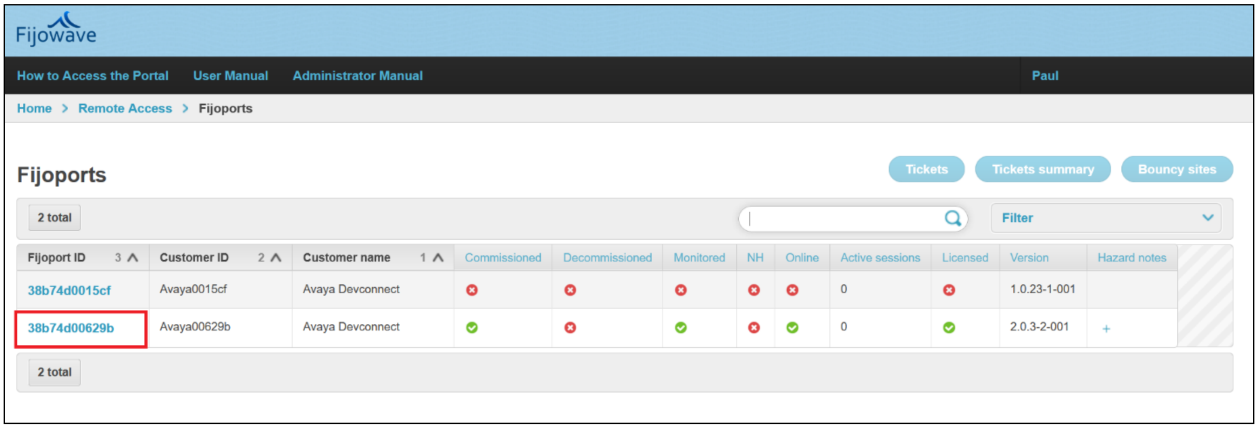


Fijowave Portal: 3.5

Maintenance mode: no

Platform status: Healthy

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



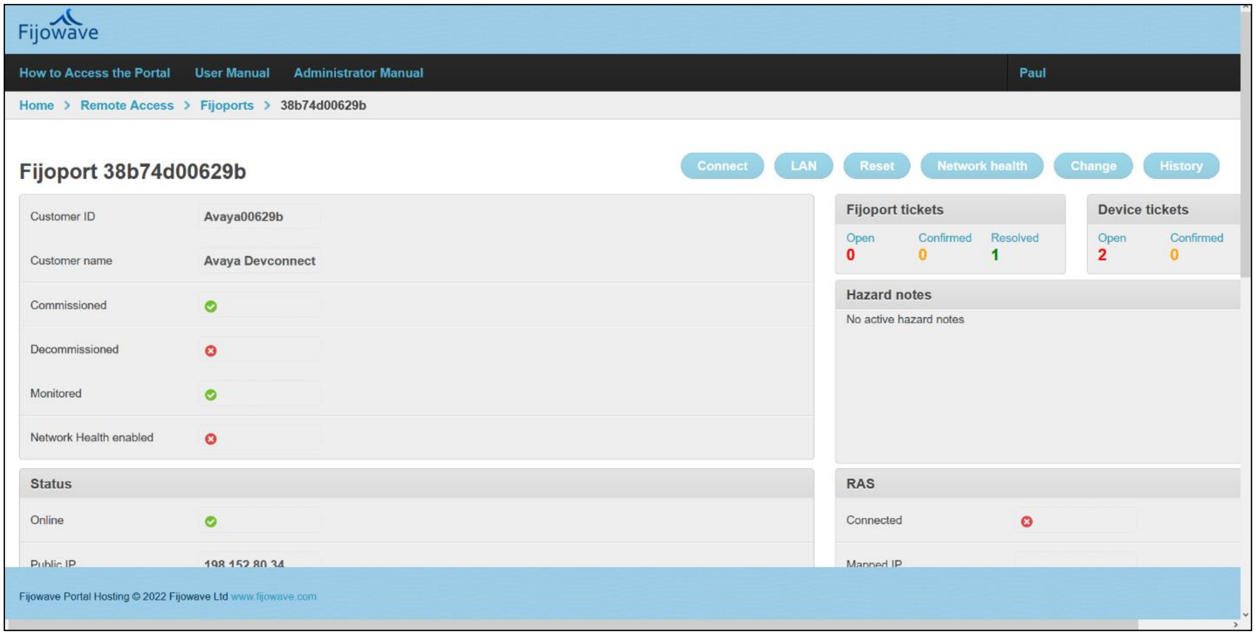
Fijoports

2 total

Fijoport ID 3 ∧	Customer ID 2 ∧	Customer name 1 ∧	Commissioned	Decommissioned	Monitored	NH	Online	Active sessions	Licensed	Version	Hazard notes
38b74d0015cf	Avaya0015cf	Avaya Devconnect	✗	✗	✗	✗	✗	0	✗	1.0.23-1-001	
38b74d00629b	Avaya00629b	Avaya Devconnect	✓	✗	✓	✗	✓	0	✓	2.0.3-2-001	+

2 total

Click on **Connect** at the top.



Fijoport 38b74d00629b

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

Fijoport tickets

Open	Confirmed	Resolved
0	0	1

Device tickets

Open	Confirmed
2	0

Hazard notes

No active hazard notes

Status

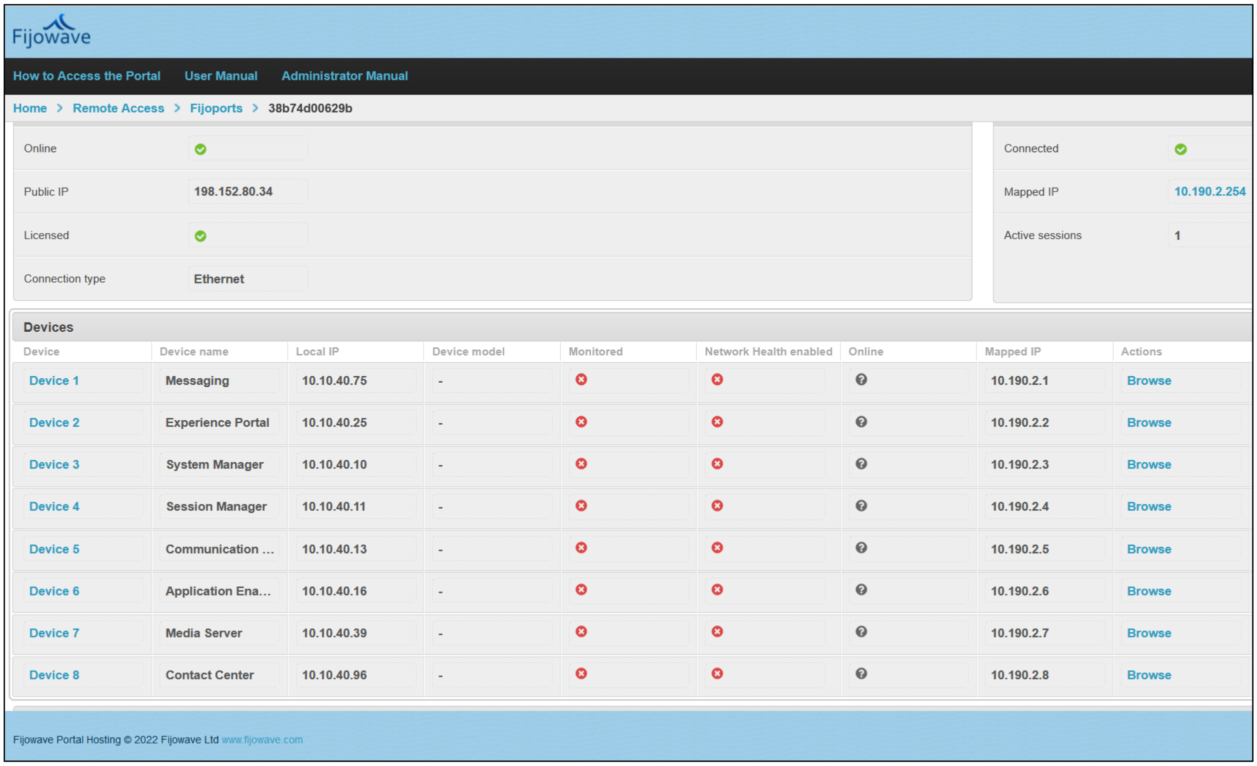
Online	✓
Public IP	198.152.80.34

RAS

Connected	✗
Mapped IP	

Fijowave Portal Hosting © 2022 Fijowave Ltd www.fijowave.com

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 Avaya devices.



Online	✓
Public IP	198.152.80.34
Licensed	✓
Connection type	Ethernet

Connected	✓
Mapped IP	10.190.2.254
Active sessions	1

Devices

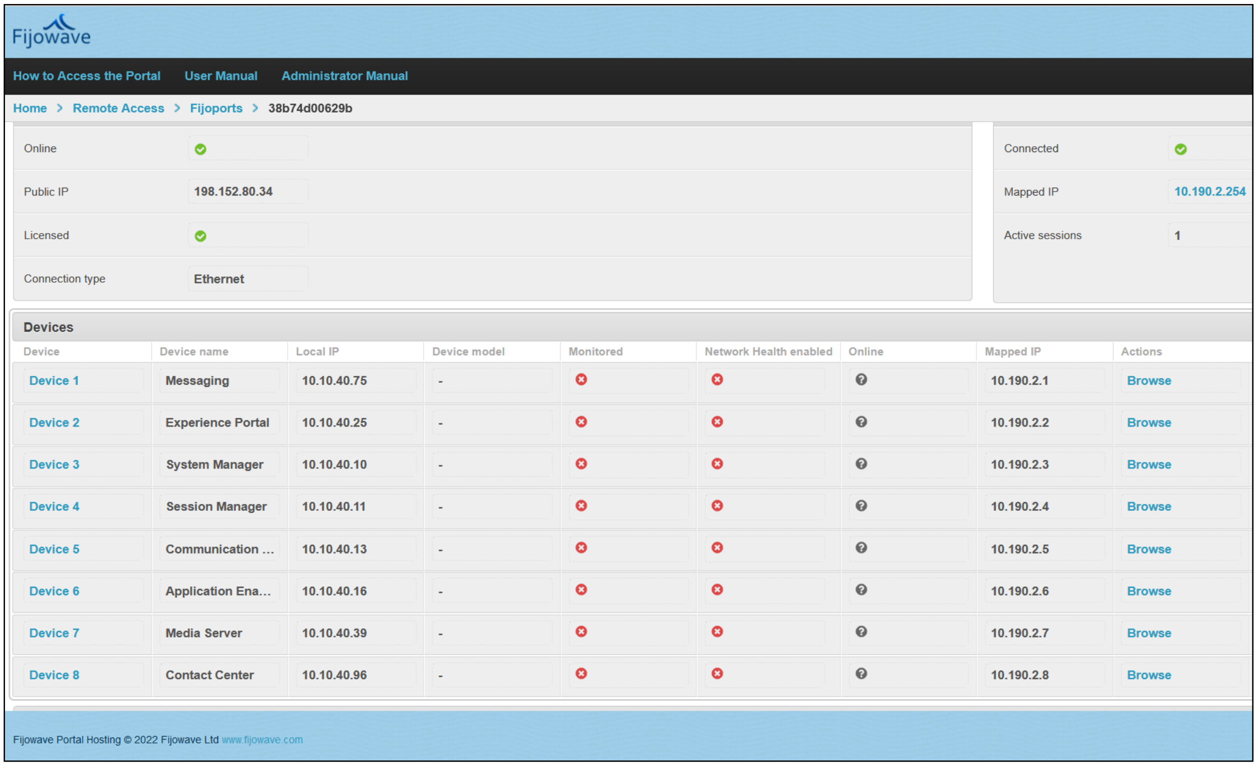
Device	Device name	Local IP	Device model	Monitored	Network Health enabled	Online	Mapped IP	Actions
Device 1	Messaging	10.10.40.75	-	✖	✖	?	10.190.2.1	Browse
Device 2	Experience Portal	10.10.40.25	-	✖	✖	?	10.190.2.2	Browse
Device 3	System Manager	10.10.40.10	-	✖	✖	?	10.190.2.3	Browse
Device 4	Session Manager	10.10.40.11	-	✖	✖	?	10.190.2.4	Browse
Device 5	Communication ...	10.10.40.13	-	✖	✖	?	10.190.2.5	Browse
Device 6	Application Ena...	10.10.40.16	-	✖	✖	?	10.190.2.6	Browse
Device 7	Media Server	10.10.40.39	-	✖	✖	?	10.190.2.7	Browse
Device 8	Contact Center	10.10.40.96	-	✖	✖	?	10.190.2.8	Browse

Fijowave Portal Hosting © 2022 Fijowave Ltd www.fijowave.com

There is some configuration required to allow the **Browse** button work correctly when pressed. The URL must be added manually for most of the devices shown above, this is because the Browse button is defaulted to open http://<MappedIP> and most of the devices will either require a https connection or for some cases https://<MappedIP>:Port/xxx. To ensure that the correct URL is therefore opened, please refer back to **Section 6.3**.

7.3. Verify Browse on Fijowave Portal server

With all the necessary **Browse** buttons configured as shown in **Section 6.3**, pick a device below and click on **Browse**.



Fijowave

How to Access the Portal User Manual Administrator Manual

Home > Remote Access > Fijoports > 38b74d00629b

Online	✓
Public IP	198.152.80.34
Licensed	✓
Connection type	Ethernet

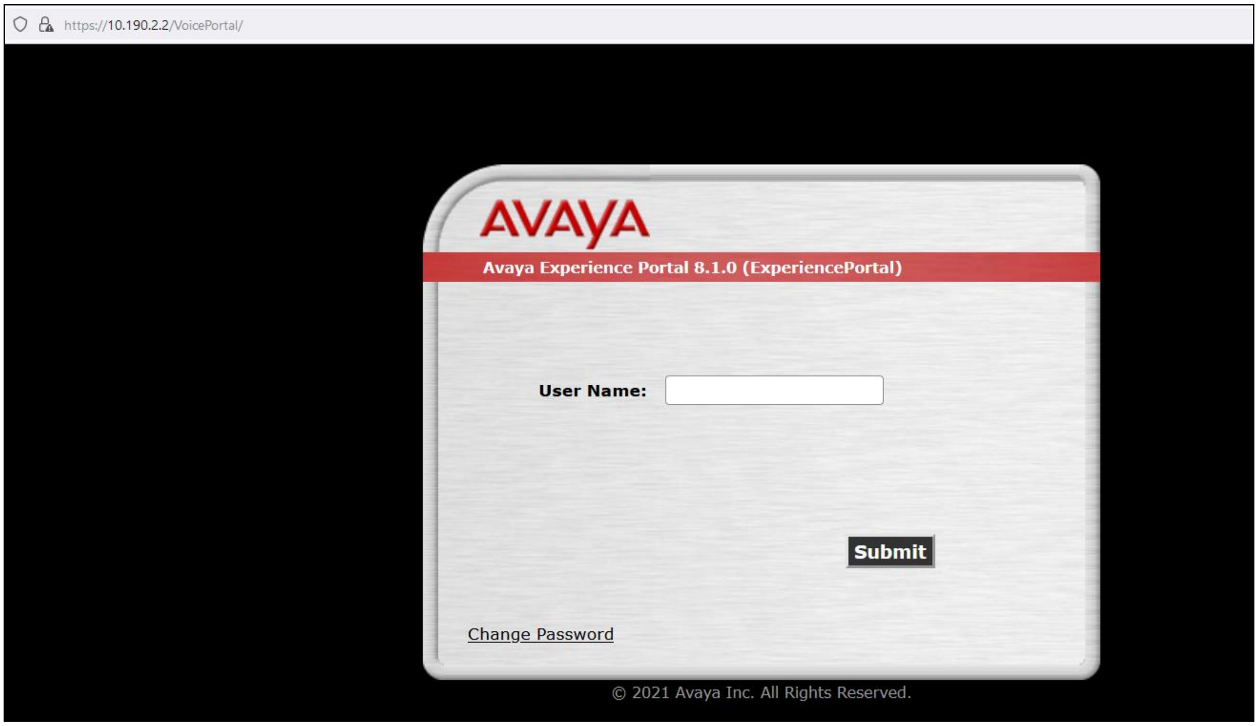
Connected	✓
Mapped IP	10.190.2.254
Active sessions	1

Devices

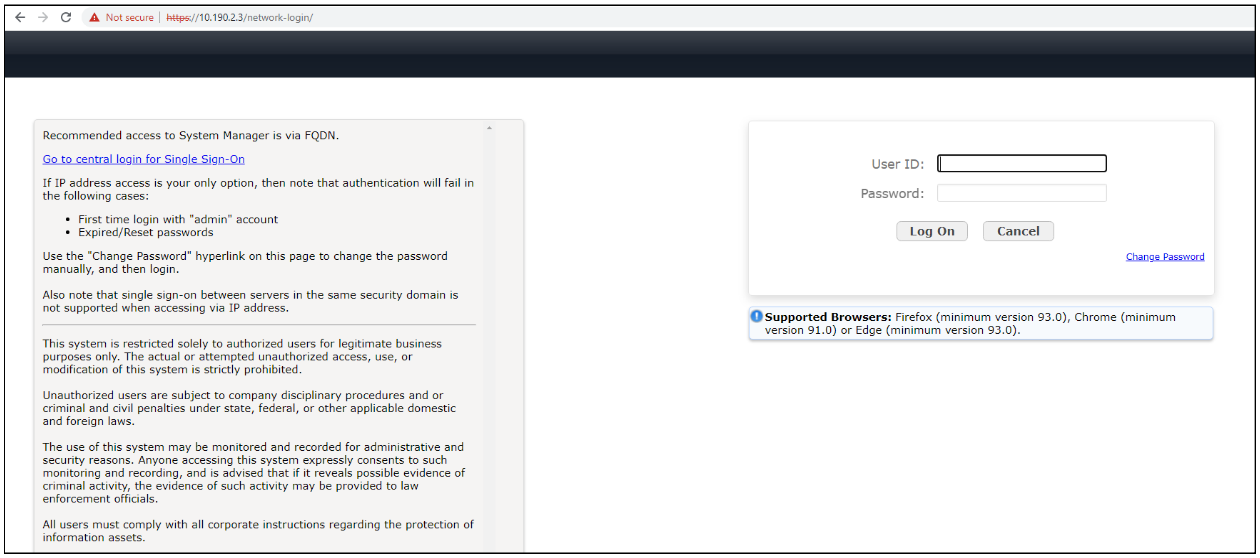
Device	Device name	Local IP	Device model	Monitored	Network Health enabled	Online	Mapped IP	Actions
Device 1	Messaging	10.10.40.75	-	✗	✗	?	10.190.2.1	Browse
Device 2	Experience Portal	10.10.40.25	-	✗	✗	?	10.190.2.2	Browse
Device 3	System Manager	10.10.40.10	-	✗	✗	?	10.190.2.3	Browse
Device 4	Session Manager	10.10.40.11	-	✗	✗	?	10.190.2.4	Browse
Device 5	Communication ...	10.10.40.13	-	✗	✗	?	10.190.2.5	Browse
Device 6	Application Ena...	10.10.40.16	-	✗	✗	?	10.190.2.6	Browse
Device 7	Media Server	10.10.40.39	-	✗	✗	?	10.190.2.7	Browse
Device 8	Contact Center	10.10.40.96	-	✗	✗	?	10.190.2.8	Browse

Fijowave Portal Hosting © 2022 Fijowave Ltd www.fijowave.com

The example below shows **Device 2** from the previous page was selected and **Browse** then opens a URL to Experience Portal, as shown below.


https://10.190.2.2/VoicePortal/
AVAYA
Avaya Experience Portal 8.1.0 (ExperiencePortal)
User Name:
Submit
Change Password
© 2021 Avaya Inc. All Rights Reserved.

Another example shows **Browse** being pressed on **Device 3**, which is System Manager and the login screen for System Manager is displayed.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

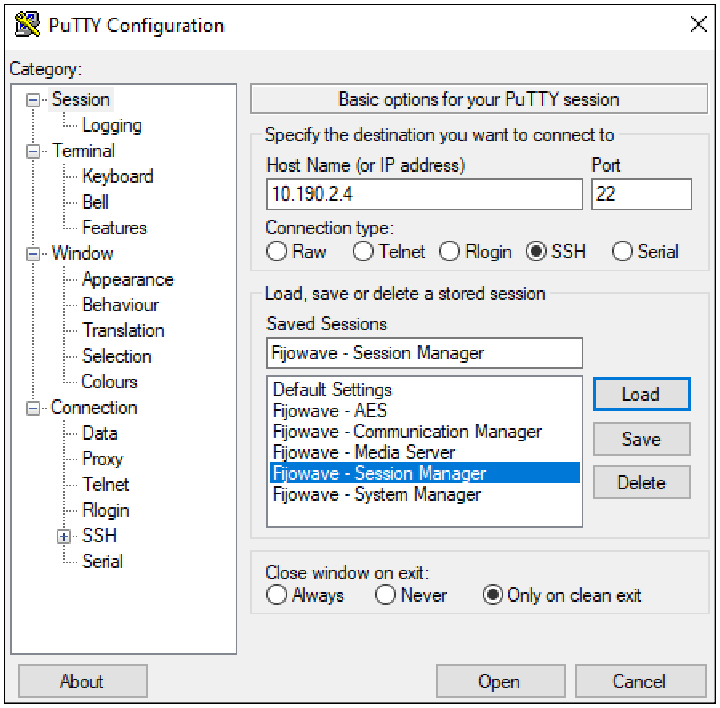
Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

7.4. Verify Secure Shell using PuTTY

The Mapped IP address is used in place of the System Manager or Session Manager IP address to allow access to the Linux commands using SSH and PuTTY.

Secure Shell (SSH) is a network protocol used to allow secure access to a UNIX terminal. The ssh command provides a secure encrypted connection between two hosts over an insecure network. This connection can also be used for terminal access, file transfers, and for tunneling other applications. PuTTY is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection. It can also connect to a serial port.

The example below shows a connection being made to Session Manager and starting “traceSM” which is commonly used to troubleshoot SIP connections. Open PuTTY (not shown) and enter the Mapped IP address for Session Manager from **Section 7.2**.



Specify the destination you want to connect to

Host Name (or IP address): 10.190.2.4

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

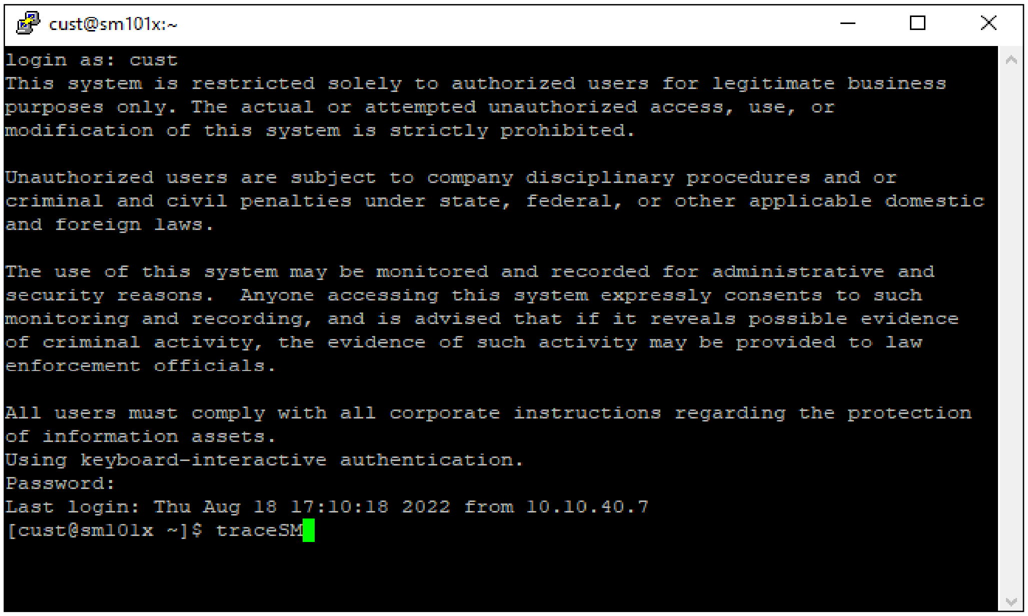
Load, save or delete a stored session

Saved Sessions: Fijowave - Session Manager

Default Settings
Fijowave - AES
Fijowave - Communication Manager
Fijowave - Media Server
Fijowave - Session Manager
Fijowave - System Manager

Close window on exit: ○ Always ○ Never ● Only on clean exit

Log in using whatever username/password is assigned to Session Manager. Run the **traceSM** command.



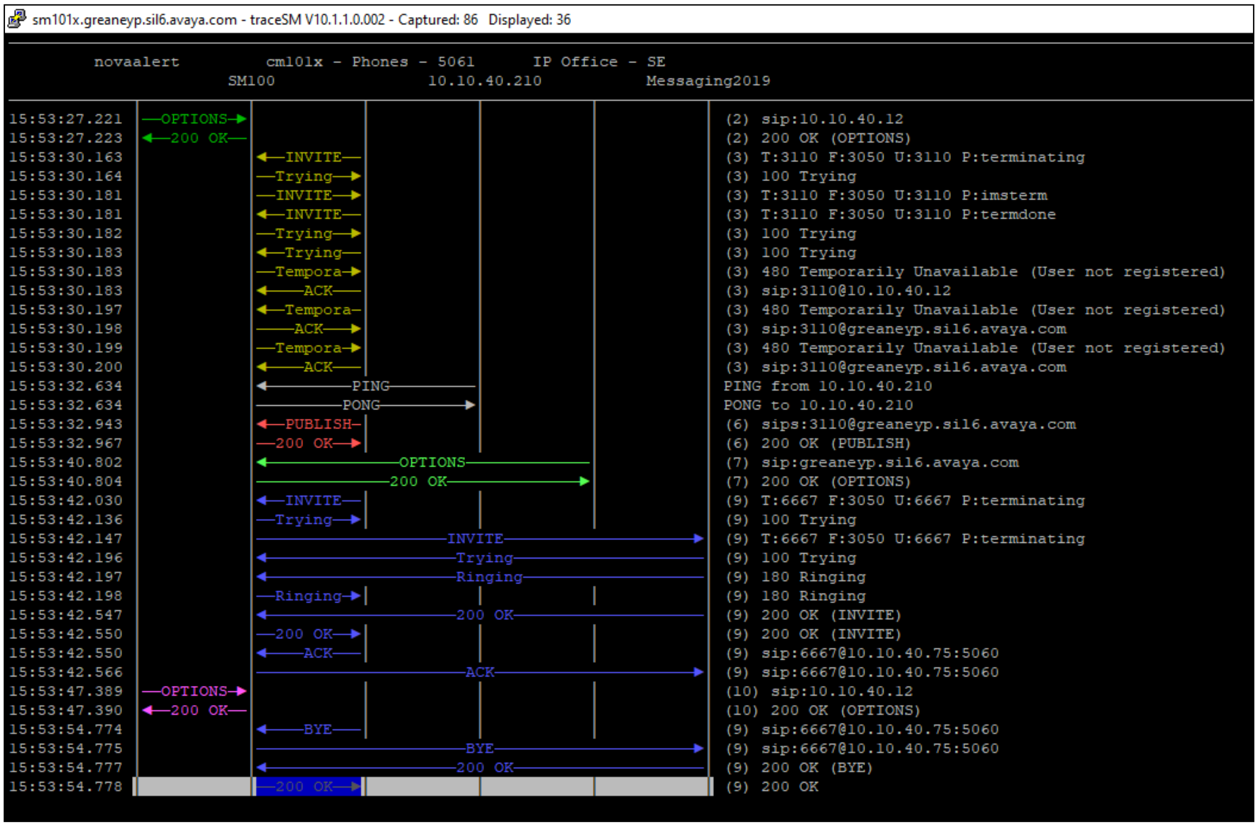
```
login as: cust
This system is restricted solely to authorized users for legitimate business
purposes only. The actual or attempted unauthorized access, use, or
modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or
criminal and civil penalties under state, federal, or other applicable domestic
and foreign laws.

The use of this system may be monitored and recorded for administrative and
security reasons.  Anyone accessing this system expressly consents to such
monitoring and recording, and is advised that if it reveals possible evidence
of criminal activity, the evidence of such activity may be provided to law
enforcement officials.

All users must comply with all corporate instructions regarding the protection
of information assets.
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 18 17:10:18 2022 from 10.10.40.7
[cust@sm101x ~]$ traceSM
```

The following shows the traceSM running for Session Manager where the SIP traces can be examined.



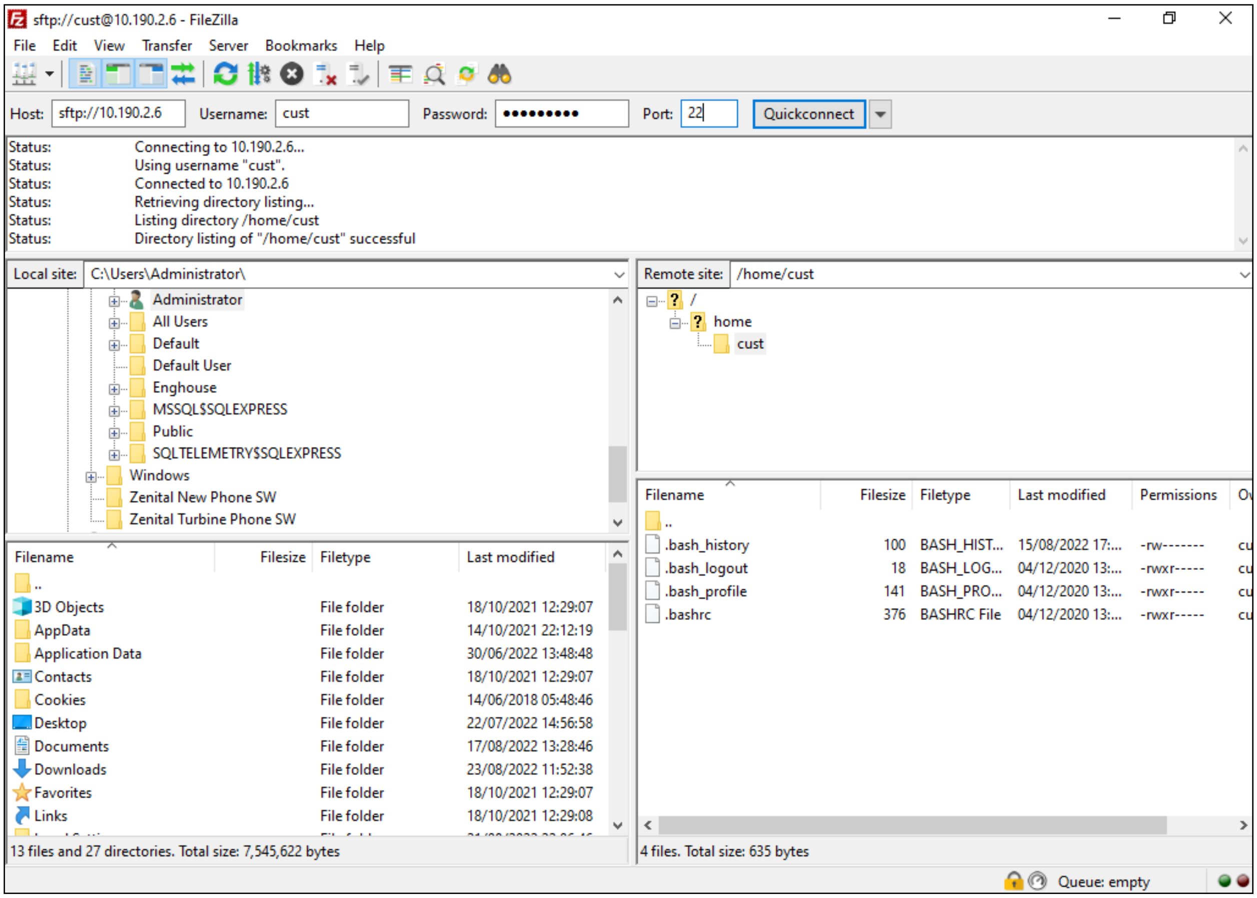
sm101x.greaneyp.sil6.avaya.com - traceSM V10.1.1.0.002 - Captured: 86   Displayed: 36

```
        novaalert          cm101x - Phones - 5061       IP Office - SE
                    SM100                 10.10.40.210            Messaging2019

15:53:27.221  --OPTIONS->                  (2) sip:10.10.40.12
15:53:27.223  <-200 OK--                   (2) 200 OK (OPTIONS)
15:53:30.163  <-INVITE--                   (3) T:3110 F:3050 U:3110 P:terminating
15:53:30.164  --Trying->                   (3) 100 Trying
15:53:30.181  --INVITE->                   (3) T:3110 F:3050 U:3110 P:imsterm
15:53:30.181  <-INVITE--                   (3) T:3110 F:3050 U:3110 P:termdone
15:53:30.182  --Trying->                   (3) 100 Trying
15:53:30.183  <-Trying--                   (3) 100 Trying
15:53:30.183  --Tempora->                  (3) 480 Temporarily Unavailable (User not registered)
15:53:30.183  <---ACK---                   (3) sip:3110@10.10.40.12
15:53:30.197  <-Tempora-                   (3) 480 Temporarily Unavailable (User not registered)
15:53:30.198  ----ACK-->                   (3) sip:3110@greaneyp.sil6.avaya.com
15:53:30.199  --Tempora->                  (3) 480 Temporarily Unavailable (User not registered)
15:53:30.200  <---ACK---                   (3) sip:3110@greaneyp.sil6.avaya.com
15:53:32.634  <-------PING--------         PING from 10.10.40.210
15:53:32.634  --------PONG------->         PONG to 10.10.40.210
15:53:32.943  <-PUBLISH-                   (6) sips:3110@greaneyp.sil6.avaya.com
15:53:32.967  --200 OK->                   (6) 200 OK (PUBLISH)
15:53:40.802  <-----------OPTIONS---------- (7) sip:greaneyp.sil6.avaya.com
15:53:40.804  -----------200 OK-----------> (7) 200 OK (OPTIONS)
15:53:42.030  <-INVITE--                   (9) T:6667 F:3050 U:6667 P:terminating
15:53:42.136  --Trying->                   (9) 100 Trying
15:53:42.147  ---------------INVITE--------------> (9) T:6667 F:3050 U:6667 P:terminating
15:53:42.196  <--------------Trying--------------- (9) 100 Trying
15:53:42.197  <--------------Ringing-------------- (9) 180 Ringing
15:53:42.198  --Ringing->                  (9) 180 Ringing
15:53:42.547  <--------------200 OK--------------- (9) 200 OK (INVITE)
15:53:42.550  --200 OK->                   (9) 200 OK (INVITE)
15:53:42.550  <---ACK---                   (9) sip:6667@10.10.40.75:5060
15:53:42.566  ----------------ACK--------------->  (9) sip:6667@10.10.40.75:5060
15:53:47.389  --OPTIONS->                  (10) sip:10.10.40.12
15:53:47.390  <-200 OK--                   (10) 200 OK (OPTIONS)
15:53:54.774  <---BYE---                   (9) sip:6667@10.10.40.75:5060
15:53:54.775  ----------------BYE--------------->  (9) sip:6667@10.10.40.75:5060
15:53:54.777  <--------------200 OK--------------- (9) 200 OK (BYE)
15:53:54.778  --200 OK->                   (9) 200 OK
```

7.5. Verify File Transfer Protocol

On occasion files will need to be taken from or placed onto the various Avaya devices. The example below shows an FTP session with Application Enablement Services. Please refer to **Section 7.2** for the list of mapped IP addresses and use the Mapped IP for Application Enablement Services as the **Host** address. Using the appropriate **Username/Password** combination, open the sftp session as shown below. This allows files to be transferred into the **home/cust** directory in this case.



Host: sftp://10.190.2.6 Username: cust Password: ••••••••• Port: 22

```
Status:         Connecting to 10.190.2.6...
Status:         Using username "cust".
Status:         Connected to 10.190.2.6
Status:         Retrieving directory listing...
Status:         Listing directory /home/cust
Status:         Directory listing of "/home/cust" successful
```

Local site: C:\Users\Administrator\

- Administrator
- All Users
- Default
- Default User
- Enghouse
- MSSQL$SQLEXPRESS
- Public
- SQLTELEMETRY$SQLEXPRESS
- Windows
- Zenital New Phone SW
- Zenital Turbine Phone SW

Filename	Filesize	Filetype	Last modified
..			
3D Objects		File folder	18/10/2021 12:29:07
AppData		File folder	14/10/2021 22:12:19
Application Data		File folder	30/06/2022 13:48:48
Contacts		File folder	18/10/2021 12:29:07
Cookies		File folder	14/06/2018 05:48:46
Desktop		File folder	22/07/2022 14:56:58
Documents		File folder	17/08/2022 13:28:46
Downloads		File folder	23/08/2022 11:52:38
Favorites		File folder	18/10/2021 12:29:07
Links		File folder	18/10/2021 12:29:08

13 files and 27 directories. Total size: 7,545,622 bytes

Remote site: /home/cust

- /
  - home
    - cust

Filename	Filesize	Filetype	Last modified	Permissions	Ow
..					
.bash_history	100	BASH_HIST...	15/08/2022 17:...	-rw-------	cu
.bash_logout	18	BASH_LOG...	04/12/2020 13:...	-rwxr-----	cu
.bash_profile	141	BASH_PRO...	04/12/2020 13:...	-rwxr-----	cu
.bashrc	376	BASHRC File	04/12/2020 13:...	-rwxr-----	cu

4 files. Total size: 635 bytes

The Mapped IP address for each device or Avaya product can be used to connect to it using whatever means necessary, the examples above were shown as these are typically used when configuring or troubleshooting these devices.

8. Conclusion

These Application Notes describe the configuration steps required for provisioning Fijowave's Fijoport Remote Access to interoperate with the Avaya Aura® Platform, a list of Avaya products that are listed in **Section 4**. It has been verified that the Fijoport solution allows a secure connection to the Avaya Aura® Platform allowing end users connect to the various Avaya Aura® products. 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 https://support.avaya.com.

[1] Avaya Messaging Server Configuration Guide. Release 11.0 .0.1609, Issue 17, 16 August 2022.

[2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022.

[3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022.

[4] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021.

[5] *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 4, April 2022.

[6] *Avaya Aura® Contact Center Server Administration*, Release 7.1, Issue 07.07, April 2022.

[7] *Implementing and Administering Avaya Aura® Media Server*, Release 10.1.x, Issue 2, July 2022.

[8] *Administering Avaya Experience Portal*, Release 8.1.1, Issue 2, February 2022.

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.