Abstract

This document provides the configuration details and steps for connecting to and obtaining more information about your AvayaLive Collaboratory.
# Table of Contents

## Introduction
- 1.1. **Your Welcome Package**  
- 1.2. **Support**  
- 1.3. **Reference Configuration**  
- 1.4. **Lab Components**

## Configure OpenVPN Client
- 1.5. **Configure Microsoft Windows Client**  
- 1.6. **Configure MacOS Client**  
- 1.7. **Configure Linux Client**  
- 1.8. **Configure iPad Client**

## Getting More Information From Within Collaboratory
2. Introduction

This document provides the configuration details and steps for connecting to the AvayaLive Collaboratory. The intent of Collaboratory is to provide an environment where application developers can learn about Avaya Aura® Collaboration Environment and the services it provides, and develop applications using those services. While Collaboratory provides all the services available in Collaboration Environment, it does not allow application developers to test performance, scalability and the full gamut of redundancy capabilities of the Avaya Aura® infrastructure. OpenVPN is the client used to access the lab.
1.1. **Your Welcome Package**

Your welcome email from AvayaLive will point you to a customized Welcome Page from which you can download this document and a CustomerAccess.csv file giving you:

1. the OpenVPN username and password you need to connect into your Collaboratory. The steps to do this are described in Section 3 below.
2. The URL (of the form http://IPaddr:8400) you browse to once you are connected over the VPN. This page includes information and software you need for using and configuring your Collaboratory. It is described further in Section 4 below.

1.2. **Support**

If you have problems connecting to or using your Collaboratory, please:

1. Carefully re-read this document.
2. Open a support request at support.avaya.com, by
   a. Log in at [http://support.avaya.com](http://support.avaya.com).
   b. Click on Service Requests link at the top right center of the toolbar.
   c. Select “I need to fix my product” for issues with your lab environment
   d. Select “I need implementation assistance” for questions regarding API/SDK help.
   e. Enter your provided SoldTo
   f. Search for the product: AvayaLive Collaboratory. Your account will have AvayaLive Collaboratory associated with it based upon your approved purchase through the AvayaLive portal.
   g. Complete the rest of the request.

![Create a Service Request]

- [Find your Sold To](#)
- [Find your Serial Number](#)
- [Find your SEID](#)
We encourage you to refer to this document and ensure that you have correctly configured your systems for access to Collaboratory before submitting technical support tickets for connectivity issues.

1.3. **Reference Configuration**

Each lab is accessed through up to 10 individual SSL VPN tunnels. A tunnel must be established for each server, PC or telephone used in the lab. Once the tunnel is established, the subscriber will have access to various Avaya Aura® components in the lab through SSH or HTTP access. Additionally 10 more IPSec Tunnels are allowed for supporting H.323 using the Avaya 9600 Series Deskphones. It is assumed that the user is familiar with the Avaya Aura® infrastructure and Collaboration Environment’s role in the same. More detailed information about the Avaya Aura® infrastructure can be found in *Section Error! Reference source not found.*. The various servers in the lab are:

- **System Manager (SMGR)** – This server is the provisioning and configuration system for the lab. Subscribers will use it to configure and deploy applications they develop for Collaboration Environment. The majority of the configuration of the lab is already done for the user.
- **Collaboration Environment (CE-1, CE-2)** – Two instances are provided to support creation of Collaboration Environment clusters.
- **Session Manager (SM)** – This SIP proxy is responsible for SIP registrations and operates as a SIP proxy between various components.
- **Communication Manager (CM)** – Provides H.323, and SIP endpoints sequenced with CM.
- **Avaya Media Server (AMS)** – Shared instance for Collaboration Environment and CM.

There are also some shared (common) servers in the environment that are used by all of the Collaboratory labs hosted in the environment. This common equipment supports PSTN calling, email, and Scopia video services.
Collaboratory Stack

Figure 1: Collaboratory
1.4. **Lab Components**

Login information and IP addresses for Collaboratory access are located in the spreadsheet (CustomerAccess.csv) located on the website for your lab. The welcome email has the URL for your lab, where you can get everything you need during your time on Collaboratory.

**Note:** SSH:, WEB: etc. is *not part of the login credentials, rather they describe the connection methodology.*

The following components were used for the sample configuration provided:

- OpenVPN Client for Windows, Linux, Mac, and iOS
- Avaya Aura® System Manager
- Avaya Aura® Collaboration Environment
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Media Server
- Avaya one-X Communicator
- Avaya 9600 Series Deskphones

3. **Configure OpenVPN Client**

This section describes the configuration for the OpenVPN Client for various operating systems. Please be sure to use the section for the operating system you are using.

1.5. **Configure Microsoft Windows Client**

2. Select appropriate link to download the Windows Installer.
3. Install the OpenVPN client. Select all defaults. (If prompted to install tap driver for windows, accept and allow the driver to be installed.)
Welcome to the OpenVPN
2.3.4-1001 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 XP, or higher.
4. After the installation is complete, uncheck Show Readme, check Start OpenVPN GUI and click **Finish**. The OpenVPN GUI client will be loaded in the system tray.
5. When starting the OpenVPN client after the initial install **make sure to do so with the “Run as Administrator” option.**
6. Extract the lab.zip file in the C:\Program Files\OpenVPN\config directory. Not (Shown)
7. From the Sytem Tray right-click the OpenVPN GUI Icon and click Connect.
8. Enter Username and Password to gain access to Collaboratory.
9. From System tray verify OpenVPN GUI Icon is green and mouse over icon to verify configuration.

![OpenVPN GUI Icon](image)

10.

1.6. **Configure MacOS Client**

1. Create directory to store and extract zip file (lab#.zip) included in welcome email.
2. Go to [https://openvpn.net/index.php/access-server/download-openvpn-as-sw/357.html](https://openvpn.net/index.php/access-server/download-openvpn-as-sw/357.html) (Tunnelblick 3.3 stable was used in this example).
3. After downloading .dmg file double-click Tunnelblick.dmg file in the Downloads folder.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Modified</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnelblick_3.3.dmg</td>
<td>Jul 22, 2013 3:39 PM</td>
<td>8.6 MB</td>
</tr>
</tbody>
</table>
4. When the Tunnelblick window opens double-click the Tunnelblick icon. If prompted select **Open** to allow the installation to begin (not shown). If prompted enter the administrator’s credentials (not shown) and the installation should begin.

5. Once the installation is completed click the **Launch** button.
6. A “Welcome to Tunnelblick” window should be displayed. Click the **I have configuration files** button.

![Welcome to Tunnelblick Window]

7. From the “Which Type of Configuration Do You Have?” window, click **OpenVPN Configuration(s)**.

![Which Type of Configuration Do You Have?]
8. “An Empty Tunnelblick VPN Configuration Has Been Created” window should be displayed. Follow the instructions given in this window. Once completed, click **Done**.

![An Empty Tunnelblick VPN Configuration Has Been Created](image)

9. If prompted to ‘check ip address’, select your desired choice.
10. If prompted to ‘check for updates automatically’, select your desired choice.
11. When prompted to “Install Configuration For All Users”, select your desired choice. Then enter administrator’s credentials (not shown) to complete the installation.

![Install Configuration For All Users?](image)
12. Click **OK** to complete the installation.

![Tunnelblick VPN Configuration Installation](image)

13. In order to connect the VPN tunnel, click the Tunnelblick icon located at the top right of the screen (not shown). From the menu click the desired VPN.

![No Active Connections](image)

14. Enter VPN credentials and click **OK**.

![Tunnelblick: Login Required](image)

15. Verify connection by mousing over the Tunnelblick icon at the top right of the screen.
1.7. **Configure Linux Client**

1. Verify OpenVPN version. This configuration was tested with OpenVpn 2.2.1.
2. Create directory to store zip file included in welcome email.

```
interop@utility:~$ mkdir -p celabvpn
```
3. Change directories to the newly created directory.
4. Unzip the file.
5. Start the OpenVPN client and log in using the VPN credentials.
6. The VPN client connection window must remain open. Use Ctrl-c to end the VPN session.
1.8. **Configure iPad Client**

1. Download **OpenVPN Connect** from the App Store.
2. Click **Install APP**.

3. Create a directory on the PC and copy the zip (lab#.zip) the file included in welcome email.
4. Unzip the file. This configuration was tested using WinZip14.5.
5. The extracted file should now be visible. Do not include the .zip file when adding the files to iTunes.
6. Connect the iPad to the PC for use with iTunes.
7. From iTunes, go to **Apps** then highlight the **OpenVPN** app. Click the **Add** button to upload the VPN files to the iPad.
8. Click the **Add** button, browse to the VPN files and select everything except the zip to upload to the iPad.
9. Click the **Sync** button to upload the files.
10. From the iPad select **OpenVPN** to start the session. One new OpenVPN profile should be available for import. Select the green plus sign to import the profile.
11. Provide the VPN credentials and select the **Connection** button to login.
12. Select **Yes** to allow the connection.
13. Status should now show connected.
4. Getting More Information from within Collaboratory

Once you browse to the In-Lab Information URL provided in the CustomerAccess.csv file you will see a page similar to the following. It contains links to:

1. The User and Configuration Guide for your Collaboratory.
2. A CustomerAccess.csv file which includes the links (IP addresses), logins and passwords assigned to each of your Collaboratory components.
3. Links to various telephone clients for you to test telephone calls within your Collaboratory.
4. Links to other administration guides and software that could prove useful while developing applications using your Collaboratory.

Collaboratory Lab001

Please read this message in its entirety, as it contains important technical information relating to your subscription to the AvayaLive Collaboratory, as well as how to obtain support for your Avaya Aura® Collaboration Environment application development activities.

Note: Your use of the AvayaLive Collaboratory is governed by the terms and conditions of Avaya’s Terms of Use for SaaS, and the related AvayaLive Collaboratory Service Description document. This material and can be found at www.avaya.com/Collaboratory, and has been communicated to you separately.

The following documents and links are attached for your reference:

- collaboratory_user_guide_3d000.pdf provides details on the required user-side setup and how to use the AvayaLive Collaboratory lab, including download and installation instructions for software components you may require.
- Customer Access credentials contains additional information needed for lab access (logins, passwords, IP addresses, URLs, etc), along with information about the Avaya Product and other servers in this lab environment available for your use.
- One-X Communicator 6.2.1 contains One-X Communicator download for Windows.
- Avaya one-X Communicator for Mac OS X 9.1 contains One-X Communicator download for MAC.
- Avaya IP Deskphone H.323 Release 6.3.1 is supported on the 9608, 9611G, 9621G and 9641G IP Deskphones only and when used with Avaya Aura® Communications Manager 5.2.1 and above, IP Office 7.0 latest SP and 8.0 or above. It will not load or operate on any other models.
- Avaya one-X® Deskphone H.323 Release 3.2.2 is supported on the 9620L, 9620C, 9630G, 9640, 9640G, 9650, 9650C and 9670G IP Deskphones only. It will not load or operate on any other models.
- Avaya 1600 Series IP Deskphone Software Release 4.3 Maintenance Release 4 software is supported on the 1603, 1603-I, 1603SW, 1603SW-I, 1608H, 1616H and 1618H IP Deskphones only. It will not load or operate on any other models.
- Configuration document Use MV_JPTel to setup a Windows server to load the latest H.323 phones firmware in order to support VPN connections.
- Java SDK 1.7 u67
- Eclipse IDE for Java EE Developers Juno or Kepler version recommended. Note: Kepler includes Maven
- Maven Download latest version
- CE SDK Download CE SDK from DevConnect Portal
©2014 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 this document is subject to change without notice. The configurations, technical data, and recommendations provided in this document 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 this document.