



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers– Issue 1.0**

### **Abstract**

These Application Notes describe the procedures necessary to configure Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers. The SIP endpoints used as Remote Workers included Avaya Flare® Experience for Windows and Avaya one-X® Mobile Preferred for IP Office.

Testing was performed to verify SIP registration and basic functionalities in audio calls for the remote endpoints. Calls were placed to and from the Remote Workers residing outside of the enterprise, across the public internet, to various Avaya endpoints located at the enterprise.

These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning steps described in this document. Testing of additional supported Remote Worker SIP endpoints, not listed under these Application Notes, is outside the scope of this document.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

# 1. Introduction

These Application Notes describe the procedures necessary to configure Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE) to support Remote Workers.

A Remote Worker is a SIP endpoint that resides in the untrusted network, registered to IP Office at the enterprise via the Avaya SBCE. Remote Workers offer the same functionality as any other endpoint at the enterprise. The SIP endpoints used as Remote Workers in the reference configuration included Avaya Flare® Experience for Windows and Avaya one-X® Mobile Preferred for IP Office on Apple and Android.

In the sample configuration, the IP Office system consisted of an Avaya IP Office Server Edition solution, which included a Primary Server running the Avaya IP Office Server Edition Linux software, and an IP Office Expansion System (V2), on an IP500V2 chassis.

Testing was performed to verify SIP registration of the Remote Workers located outside the enterprise to the Avaya IP Office Primary Server, via the Avaya SBCE. Audio calls were placed to and from the Remote Workers to various Avaya IP Office endpoints located at the enterprise to verify basic functionality.

The Avaya Session Border Controller for Enterprise (Avaya SBCE) functioned as the enterprise edge device providing protection against any external SIP-based attacks. For privacy over the public internet, the public side of the Avaya SBCE facing the remote workers should be configured to use the recommended values of TLS for signaling and SRTP for media encryption, as long as they are supported by the endpoints.

## 2. General Test Approach and Test Results

A simulated enterprise site containing the Avaya IP Office Server Edition Solution and the Avaya SBCE was installed at the Avaya Solution and Interoperability Lab. A separate location in the Lab containing the Remote Workers was configured to connect via the public network to the Avaya SBCE at the simulated enterprise site.

The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

## 2.1. Test Coverage

To verify Remote Worker basic functionality, the following areas were tested:

- Remote Worker endpoints registrations to the Avaya IP Office Server Edition Primary Server.
- Inbound audio calls to Remote Workers from different types of Avaya endpoints located at the enterprise. The Remote Workers clients used were Avaya Flare® Experience for Windows and Avaya one-X® Mobile Preferred for IP Office.
- Outbound audio calls from Remote Workers to various Avaya endpoint types located at the enterprise. The Remote Workers clients used were using Avaya Flare® Experience for Windows and Avaya one-X® Mobile Preferred for IP Office.
- Basic call handling features, such as hold, transfer and call forward.
- Call coverage to IP Office Voicemail Pro and Message Waiting Indicator (MWI) activation/deactivation.
- Voicemail navigation and DTMF transmission using RFC 2833.

## 2.2. Test Results

Basic Remote Worker functionality was successfully verified with the following observations and limitations.

- **SRTP media in Avaya Flare® Experience for Windows** – Avaya Flare® Experience for Windows Release 1.1.4.23 supports SRTP media encryption for audio calls only. Enabling Video in the softphone **Settings/Video** tab effectively changes the media encryption in the client from SRTP to RTP for all calls. During the test, Video was left disabled on the Avaya Flare® Remote Workers clients, and SRTP encryption was used for audio calls.
- **SRTP media in Avaya IP Office 9.0** – Avaya IP Office release 9.0 does not support direct SRTP connections on its interfaces. The Avaya SBCE was used to convert the SRTP media encryption used for the external connections to the Avaya Flare® Experience for Windows users, to RTP media in the internal enterprise network to the IP Office.

## 2.3. Support

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.

### 3. Reference Configuration

Figure 1 illustrates the sample configuration used to test the Remote Workers functionality.

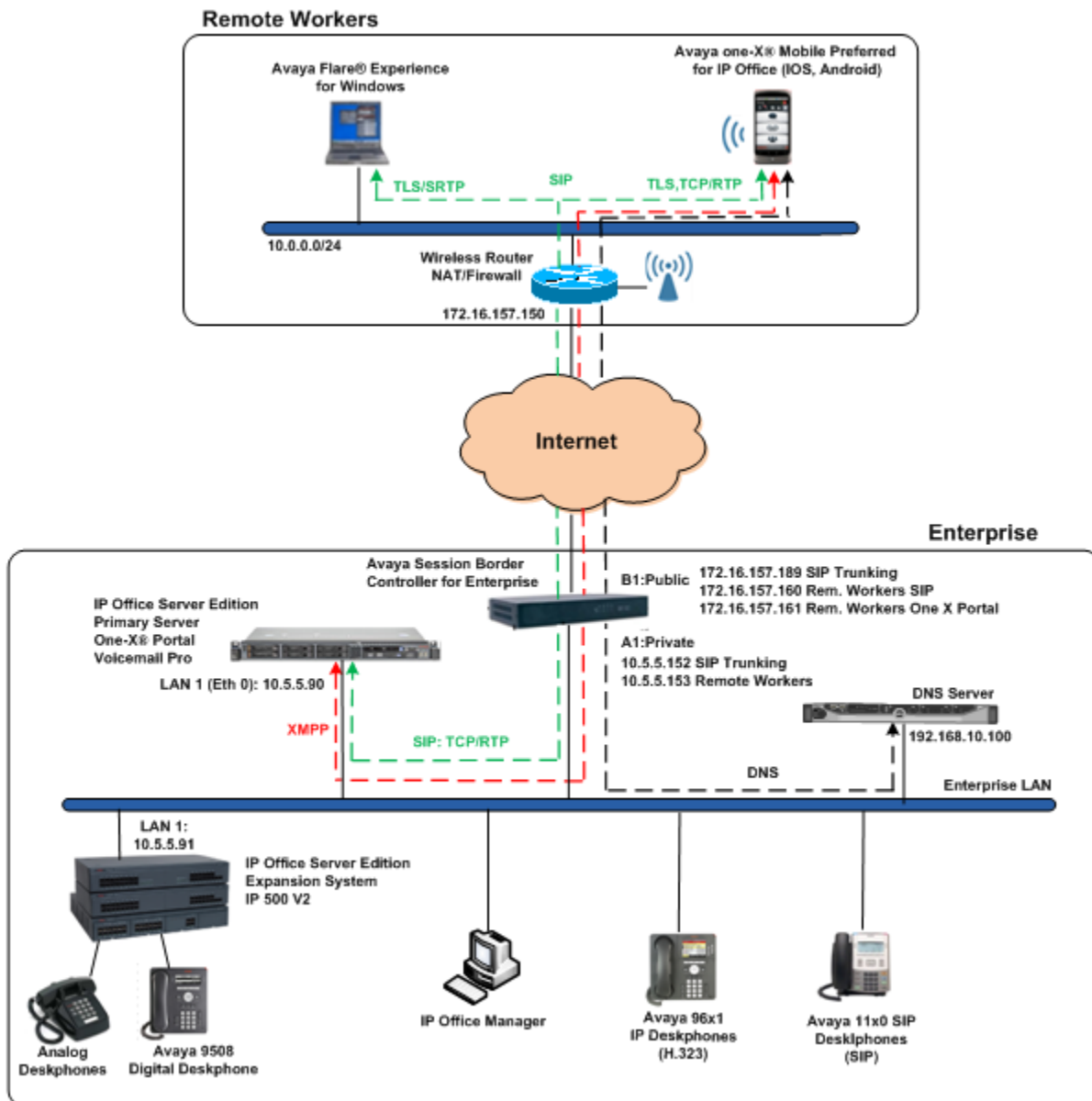


Figure 1: Test Configuration

Note that for security purposes, all public IP addresses shown throughout these Application Notes have been edited so the actual values are not revealed.

The main components used to create the simulated Enterprise and Remote Workers sites used during the test included:

- Avaya IP Office 9.0 Server Edition solution.
- Avaya Session Border Controller for Enterprise 6.3.
- Various endpoints including Avaya 96x1 IP telephones (H.323), Avaya 1140E SIP telephones, Avaya 9508D Digital Telephones and analog telephones at the enterprise site.
- Avaya Flare® Experience for Windows and Avaya one-X® Mobile Preferred for IP Office (for IOS and Android) at the Remote Workers site.
- DNS Server.

The Avaya IP Office Server Edition solution at the enterprise site comprises the following main components:

- IP Office Server Edition Primary server.
- IP Office Server Edition Expansion System (V2)

The IP Office Server Edition Primary server consists of a HP Proliant DL360 server. The Primary server provides the IP Office Server Edition software, Avaya one-X® Portal and Avaya Voicemail Pro. The server is the only component required to support IP endpoints and SIP trunking. The LAN1 port of the Primary Server (Eth0) is connected to the enterprise LAN. The LAN2 port (Eth1) was not used during the compliance test.

The optional Expansion System (V2) is used for the support of digital, analog and additional IP stations at the enterprise. It consists of an Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module). The LAN1 port of the Avaya IP Office IP500V2 is connected to the enterprise LAN. LAN2 was not used.

Located at the edge of the enterprise, the Avaya SBCE has two physical interfaces. Interface B1 was used to connect to the public network, while interface A1 was used to connect to the private enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flows through the Avaya SBCE, in this way protecting the enterprise against any SIP-based attacks. The Avaya SBCE also performs network address translation at both the IP and SIP layers.

Avaya Flare® Experience for Windows and Avaya one-X® Mobile Preferred for IP Office (for IOS and Android) are used in the sample configuration as Remote Workers. The Remote Workers Wi-Fi and Internet access is provided by a wireless Router/NAT/Firewall located at the Remote Worker site. The router also provides DHCP service to the local SIP endpoints.

The Avaya one-X® Mobile Preferred VoIP clients used during the test required the Fully Qualified Domain Name (FQDN) of the Avaya one-X® Portal server (or the router fronting it) to be entered on the Server ID field of the client settings screen. On a real customer deployment, this FQDN should be resolvable over the public Internet. For testing purposes, and since a private FQDN was used in the lab environment, the router at the Remote Workers site was configured to use one of the external IP addresses of the Avaya SBCE (172.16.157.161) as its

DNS server. The Avaya SBCE relayed DNS traffic to an internal DNS server (192.168.10.100) at the enterprise. This internal DNS server was configured to provide the proper external IP address information based on the type of service requested by the Avaya one-X® Mobile client.

The table below summarizes the encryption capabilities, at the time of writing these Application Notes, of the VoIP clients supported as Remote Workers with Avaya IP Office release 9.0 and Avaya SBCE 6.3,. Note that Avaya Flare® Experience for iPad was not part of the reference configuration and it was not tested.

	TLS	SRTP Audio	SRTP Video
Flare Experience for IP Office R1.1.4 (Windows version)	Yes	Yes	No
Flare Experience for IP Office R1.1.2 (iPad version)	Yes	Yes	No
one-X Mobile Preferred VoIP client for Android	Yes	No	No
one-X Mobile Preferred VoIP client for iOS	No	No	No

**Table 1: Supported clients and capabilities**

In the reference configuration, the following transport protocols were used between the Avaya SBCE and the Remote Workers over the simulated public network:

- Avaya Flare® Experience for Windows: TLS/SRTP
- Avaya one-X® Mobile Preferred for IP Office (Android): TLS/RTP
- Avaya one-X® Mobile Preferred for IP Office (IOS): TCP/RTP

The transport protocol used between the Avaya SBCE and the IP Office Primary Server across the private enterprise network was TCP/RTP.

**Note:** The intent behind these Application Notes is to simply illustrate a sample configuration and provide a general guide in the provisioning steps that are required in order to support Remote Workers on an Avaya IP Office solution and the Avaya SBCE. The settings presented here are based on the reference configuration are not intended to be prescriptive. Remote Worker integration with SIP Trunking was not part of the reference configuration. Interoperability Compliance Testing of Remote Worker endpoints with SIP Trunking should be performed separately with each Service Provider. Testing of additional supported Remote Worker SIP endpoints, not listed under **Section 4** in this document, is outside the scope of these Application Notes.

## 4. Equipment and Software Validated

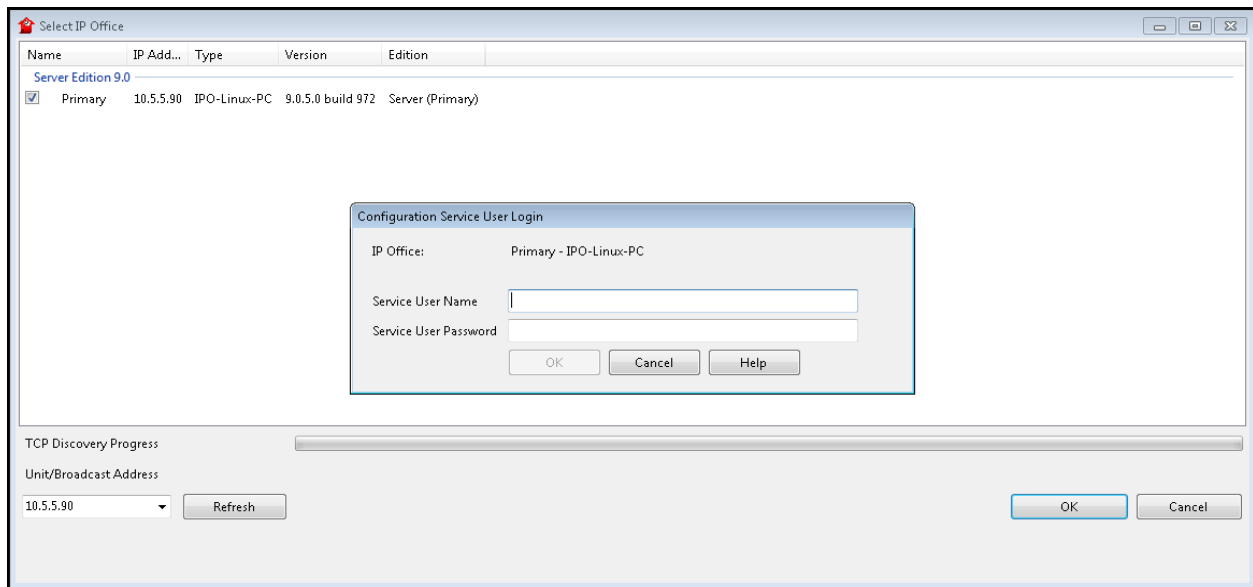
The following Avaya equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya IP Office Server Edition Primary server: <ul style="list-style-type: none"><li>• IP Office Server Edition</li><li>• Avaya one-X® Portal</li><li>• Voicemail Pro</li></ul>	9.0.5.0 Build 972 9.0.5.0. Build 5 9.0.5.0. Build 4
Avaya IP Office Server Edition Expansion System (V2): <ul style="list-style-type: none"><li>• Avaya IP 500 V2</li><li>• Avaya IP Office Digital Expansion Module DCPx16</li></ul>	9.0.500.972 9.0.500.972
Avaya IP Office Manager	9.0.5.0.Build 972
Avaya Session Border Controller for Enterprise	6.3.000-19-4338
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.2
Avaya 1140E IP Telephone (SIP)	04.04.14.00
Avaya Digital Phone 9508	0.55
Avaya one-X® Mobile Preferred for IP Office (Android)	1.9.0.9900 (Android 4.4.2)
Avaya one-X® Mobile Preferred for IP Office (IOS)	8.1.2. 599 (IOS 8.1.2)
Avaya Flare® Experience for IP Office (Windows)	1.1.4.23

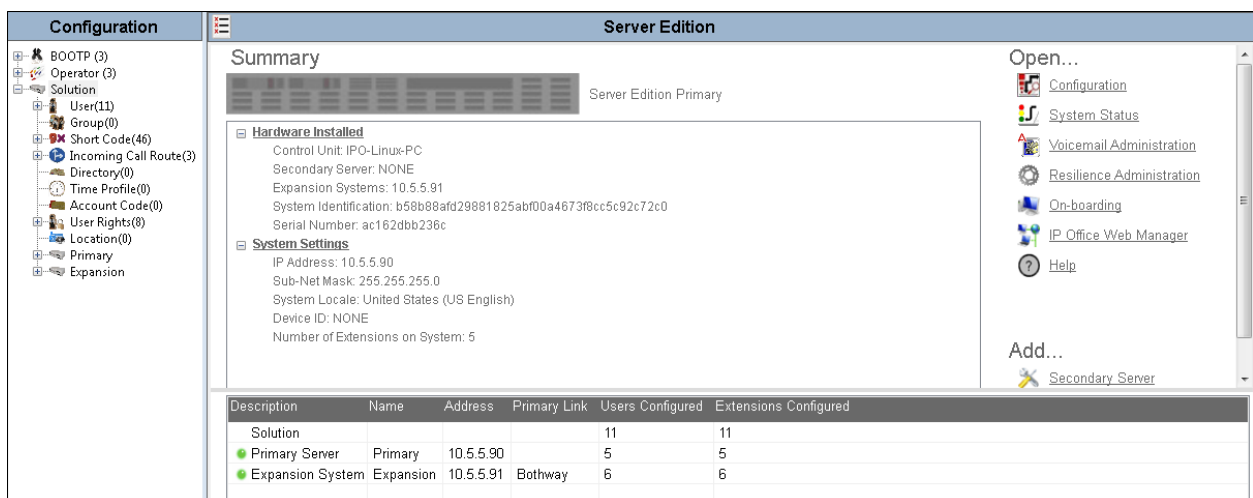
**Table 2: Hardware and Software Components Tested.**

## 5. Configure IP Office

This section describes the Avaya IP Office configuration necessary to support Remote Workers. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running IP Office Manager, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. This screen includes the system inventory of the Primary and Expansion systems in the solution. In the reference configuration the Remote Workers users registered to the Primary server, hence all the configuration steps shown were performed on the Primary server. Clicking the “plus” sign next to **Primary** on the left navigation pane will expand the menu on this server.





The appearance of the IP Office Manager can be customized using the View menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration.

Standard feature configurations that are not directly related to the interfacing with the Remote Workers are assumed to be already in place, and they are not part of these Application Notes.

## 5.1. Licensing

The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

Navigate to **Solution → Primary → License** on the left Navigation pane. Verify that there is a valid **Power User** license with sufficient instances for the amount of Remote Workers to be supported.

**Configuration**

- BOOTP (3)
- Operator (3)
- Solution
  - User(11)
    - Group(0)
  - Short Code(46)
  - Incoming Call Route(3)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(8)
  - Location(0)
  - Primary
    - System (1)
    - Line (4)
    - Control Unit (5)
    - Extension (5)
    - User (6)
      - Group (0)
      - Short Code (3)
    - Service (0)
    - IP Route (1)
    - License (16)**
    - ARS (1)
    - Location (0)
  - Expansion

License Remote Server

License Mode License Normal  
PLDS Host ID 662719

Feature	License Key	Instances	Status	Expiry Date	Source
Wave User	ydhVt58XgfCnS6QC7ctcqhsc3bFI...	255	Valid	Never	ADI Nodal
Receptionist	ZXnBG4dptv_CtMBuCXckc87LD...	255	Valid	Never	ADI Nodal
Preferred Edition Additional Voice...	sXOOdzLYXddnyMzM7eorBbr...	255	Valid	Never	ADI Nodal
3rd Party IP Endpoints	vt0DwMg_vGEuXMBBCBRevgoiO...	255	Valid	Never	ADI Nodal
SIP Trunk Channels	N4zj15vQAvhHqm7RUXgLRsr...	255	Valid	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	DhztLtmcvA80nSRg6qu@gx8Vd...	255	Valid	Never	ADI Nodal
UMS Web Services	4xyTt49RXdEc0MWKWNyoyRqrL...	255	Valid	Never	ADI Nodal
Avaya IP endpoints	Z4@sKDorXsGOB@8kRpxbcEqs...	255	Valid	Never	ADI Nodal
<b>Power User</b>	<b>tAQGdgb_vjG1N@bQ54ck5dZLL...</b>	<b>255</b>	<b>Valid</b>	<b>Never</b>	<b>ADI Nodal</b>
Office Worker	nXzerDoPtU8Khmy1W5ut5Zd9...	255	Valid	Never	ADI Nodal
VMP Pro TTS Professional	4yD2LzhovGLHKE2WCecwc97Vc...	255	Valid	Never	ADI Nodal
Server Edition	0XQdsvh6tspc4Mnr5XerH0icrg9...	255	Valid	Never	ADI Nodal
Server Edition Upgrade 255	@XtOLbyQtSFHnEZRCle_1oicSh...	1	Valid	Never	ADI Nodal
CTI Link Pro	tX9L1DoLtvrcOEw9gexgrG7VEkx...	255	Valid	Never	ADI Nodal
Server Edition Upgrade 10 255	chacILGYMXCSd_DUYQM9whAi...	10	Valid	Never	ADI Nodal
Preferred Edition Additional Voice...	Virtual Additional Voicemail Pro ...	22	Valid	Never	Virtual

## 5.2. LAN Settings

In the sample configuration, the LAN1 port was used to connect the IP Office to the enterprise network. Navigate to **Solution → Primary → System (1)** in the left Navigation pane and select the **LAN1 → LAN Settings** tab in the Details pane. Set the **IP Address** and **IP Mask** fields to the IP address and subnet mask assigned to the Avaya IP Office LAN1 port. All other parameters should be set according to customer requirements.

The screenshot shows the Avaya IP Office Configuration interface. On the left is a navigation tree with categories like BOOTP, Operator, Solution, User, Group, Short Code, Incoming Call Route, Directory, Time Profile, Account Code, User Rights, Location, Primary, System, and Line. The 'Primary' system is selected. The main pane shows the 'Primary' configuration for the 'LAN1' interface. The 'LAN Settings' tab is active, displaying fields for IP Address (10.5.5.90), IP Mask (255.255.255.0), Number Of DHCP IP Addresses (1), and DHCP Mode (Disabled). An 'Advanced' button is located at the bottom right of the LAN Settings section.

On the **VoIP** tab in the Details pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones with the H.323 protocol. The **SIP Trunks Enable** box must be checked if SIP trunks are to be configured on this interface. Check the **SIP Registrar Enable** box to allow the registration of the SIP Remote Workers users, as well as the Avaya 1140E SIP Telephones present in the enterprise network in the sample configuration. On the **Domain Name** field, the local SIP registrar domain name *sil.miami.avaya.com* was used. On the **Layer 4 Protocol** section, the default **UDP** and **TCP** protocols and ports were used. **TLS** was enabled, for the correct provisioning of the one-X® Mobile Android clients via one-X Portal. Defaults were used in the reference configuration for the rest of the **LAN1** settings.

The screenshot shows the 'VoIP' configuration tab for the 'Primary' system. It contains several sections: H323 settings (H323 Gatekeeper Enable, Auto-create Extn, Auto-create User, H323 Remote Extn Enable), SIP settings (SIP Trunks Enable, SIP Registrar Enable, Auto-create Extn/User, SIP Remote Extn Enable), Domain Name (sil.miami.avaya.com), Layer 4 Protocol (UDP, TCP, TLS with ports 5060, 5060, 5061 and Remote ports), Challenge Expiry Time (10 secs), and RTP settings (Port Number Range for Minimum and Maximum). The 'H323 Gatekeeper Enable', 'SIP Trunks Enable', and 'SIP Registrar Enable' checkboxes are checked.

### 5.3. Users

Navigate to **Solution → Primary → Users** in the left Navigation pane. Right click on **Users** and select **New** (not shown) to configure the Remote Workers users.

Enter the **Name**, **Password** and **Extension** number. Under **Profile**, select **Power User**. For the Avaya Flare® Experience for Windows Remote Worker user, check the box under **Enable Softphone**. Select the **Enable one-X Portal Services** check box only if the extension is to be granted access to the Avaya one-X® Portal user page. Select **Enable Flare**. The screen below shows the **User** tab for one of the Avaya Flare® Experience for Windows Remote Workers, “Flare SIP 4006” in the reference configuration.

**Configuration**

- BOOTP (3)
- Operator (3)
- Solution
  - User(11)
    - Group(0)
    - Short Code(46)
    - Incoming Call Route(3)
    - Directory(0)
    - Time Profile(0)
    - Account Code(0)
    - User Rights(8)
    - Location(0)
    - Primary
      - System (1)
      - Line (4)
      - Control Unit (5)
      - Extension (5)
      - User (6)
        - NoUser
        - 4001 Ext4001
        - 4006 Flare SIP 4006
        - 4002 SIP4002
        - 4010 SIP4010
        - 4005 Soft H323 4005
      - Group (0)
      - Short Code (3)
      - Service (0)
      - IP Route (1)
      - License (16)
      - ARS (1)
      - Location (0)
      - Expansion

**Flare SIP 4006: 4006**

User | Voicemail | DND | Short Codes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming

Name: Flare SIP 4006

Password: ••••

Confirm Password: ••••

Account Status: Enabled

Full Name:

Extension: 4006

Email Address:

Locale:

Priority: 5

System Phone Rights: None

ACCS Agent Type: None

Profile: Power User

☐ Receptionist

☒ Enable Softphone

☒ Enable one-X Portal Services

☐ Enable one-X TeleCommuter

☐ Enable Remote Worker

☒ Enable Flare

☐ Enable Mobile VoIP Client

Navigate to the user **Telephony → Supervisor Settings** tab. Enter the **Login Code** used by the endpoint to register. The same code used in the **Password** field was entered. Click **OK** (not shown) to save your changes.

**Flare SIP 4006: 4006**

User | Voicemail | DND | Short Codes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Prog

Call Settings | Supervisor Settings | Multi-line Options | Call Log | TUI

Login Code: ••••

Login Idle Period (secs):

Monitor Group: <None>

☐ Force Login

☐ Force Account Code

Repeat the previous steps to configure the **Name**, **Password**, **Extension** number, **Profile** and **Login Code** for the Avaya one-X® Mobile Preferred for IP Office users.

On the **User** tab, check the box under **Enable Softphone**. Select the **Enable one-X Portal Services** check box only if the extension is to be granted access to the Avaya one-X Portal user page. Select **Enable Mobile VoIP Client**.

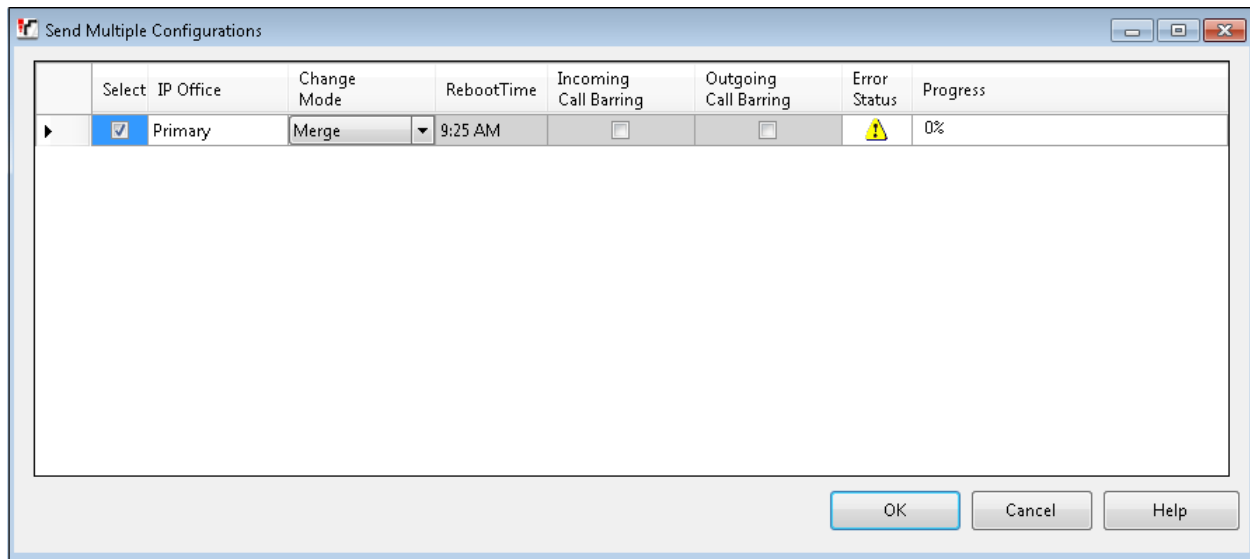
The screen below shows the **User** tab for one of the Avaya one-X® Mobile Preferred for IP Office Remote Workers, “SIP4002” in the reference configuration.

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under the 'Configuration' header, showing a hierarchy from 'BOOTP (3)' down to 'Expansion'. The 'User (6)' item is selected, and '4002 SIP4002' is highlighted. The main panel on the right is titled 'SIP4002: 4002' and contains the 'User' configuration tab. This tab includes fields for Name, Password, Confirm Password, Account Status, Full Name, Extension, Email Address, Locale, Priority, System Phone Rights, ACCS Agent Type, and Profile. Below these fields are several checkboxes for enabling various services: Receptionist, Enable Softphone, Enable one-X Portal Services, Enable one-X TeleCommuter, Enable Remote Worker, Enable Flare, and Enable Mobile VoIP Client. The 'Enable Mobile VoIP Client' checkbox is checked.

SIP4002: 4002	
User	Voicemail   DND   Short Codes   Source Numbers   Telephony   Forwarding   Dial In   Voice Recording   Button Programming
Name	SIP4002
Password	••••
Confirm Password	••••
Account Status	Enabled
Full Name	
Extension	4002
Email Address	
Locale	
Priority	5
System Phone Rights	None
ACCS Agent Type	None
Profile	Power User
<input type="checkbox"/> Receptionist <input checked="" type="checkbox"/> Enable Softphone <input checked="" type="checkbox"/> Enable one-X Portal Services <input type="checkbox"/> Enable one-X TeleCommuter <input type="checkbox"/> Enable Remote Worker <input type="checkbox"/> Enable Flare <input checked="" type="checkbox"/> Enable Mobile VoIP Client	

## 5.4. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top left of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed, showing details for those systems where the system configuration has been changed and needs to be sent back to the system. **Reboot** or **Merge** is shown under the **Change Mode** column, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.



## 6. Configure Avaya one-X® Portal for IP Office

The Avaya one-X® Mobile Preferred clients communicate with Avaya one-X® Portal to determine the feature and extension configuration. In the lab environment used to verify the remote workers functionality, an IP Office Server Edition was used, where Avaya one-X® Portal runs as a service on the Primary server. In other configurations, Avaya one-X® Portal may run on a separate server as part of the Avaya Application Server.

It is assumed that the installation and initial configuration of Avaya one-X® Portal has been completed and it is not discussed in this document. For more information consult the Avaya one-X® Portal documentation in the **References** section.

### 6.1. Avaya one-X® Portal Log in

The Avaya one-X® Portal configuration is accomplished by pointing a browser to the URL “<http://<server name>:<server port>/onexportal-admin.html>”, where <server name> is the name or the IP address of the one-X Portal server, and <server port> is the port number selected during one-X Portal for IP Office software installation (the default is 8080). The one-X Portal for IP Office login menu appears. Click on **Administrator Login** at the top of the screen. Enter the appropriate credentials and click on **Login**.



The screenshot shows the Avaya one-X Portal for IP Office login interface. At the top, there are two tabs: "Administrator Login" and "AFA Login". The main header features the "AVAYA one-X" logo and the text "Portal for IP Office". Below the header, there are input fields for "User name" and "Password". A "Language" dropdown menu is set to "English". There is a checkbox for "Remember me on this computer" and a "Login to phone" link. A "Login" button is located at the bottom right. At the bottom, there is a "Change Password" link and a copyright notice: "© 2014 Avaya Inc. All Rights Reserved."

The following screen is presented:

ID	Component Name	Status	Reported At	Additional Info	Page
34	CSTA-Provider-1-10.5.5.90	Available	Jan 16, 2014 4:39:50 PM	Provider OK	1
33	CSTA-Provider-1-Master	Available	Jan 16, 2014 4:39:50 PM	Master Available	2
3	DSML-Provider-1-10.5.5.90	Available	Jan 6, 2015 3:59:33 PM	Global resynchroniz	
1	DSML-Provider-1-ldap://ldap-server	Available	Jan 11, 2014 5:48:19 PM		

## 6.2. Configure XMPP Domain

Use this procedure to configure or change the XMPP Domain Name of Avaya one-X® Portal. The XMPP Domain Name, entered as a Fully Qualified Domain Name (FQDN), is entered by the Avaya one-X® Mobile Preferred clients in the Server ID field of the client settings screen in order to register with the IP Office, later in **Section 10**.

From the left hand side navigation menu, select **Configuration** → **IM/Presence**. Verify or enter the one-X Portal FQDN in the **XMPP Domain Name** field. In the reference configuration, *iposerver.sil.miami.avaya.com* was used. Click **Save**. The system displays another dialog box to restart Avaya one-X® Portal (not shown). Restart the server.

Providers

Users

CSV

Branding

IM/Presence Server

Server to Server Federation ☒

Disconnect on Idle ☐

Anyone can connect ☒

Port number

Idle timeout

MyBuddy username

XMPP Domain Name

**Save**

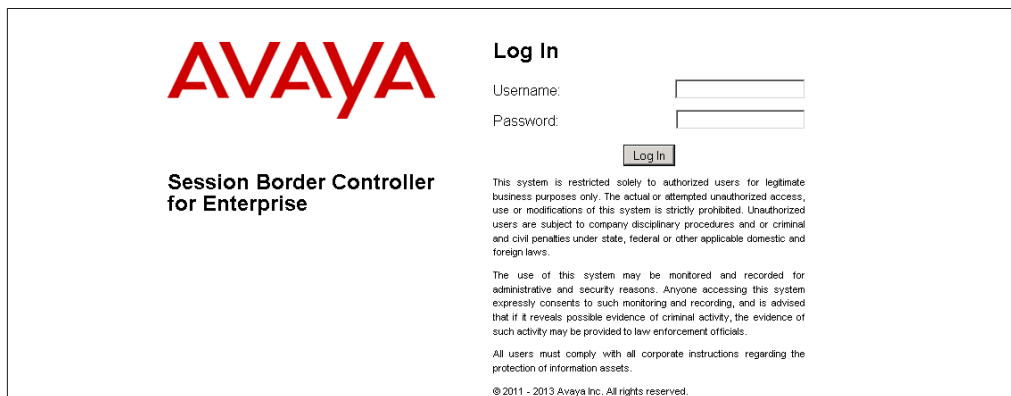
IM/Presence Exchange Service

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE to support the Remote Workers. It is assumed that the initial provisioning of the Avaya SBCE, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

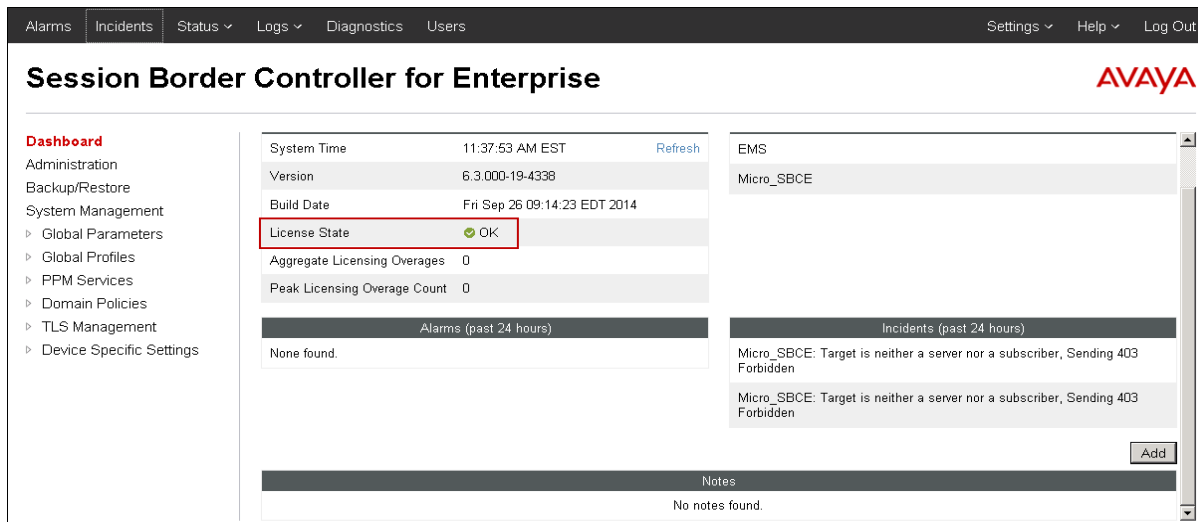
### 7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The login page features the Avaya logo on the left. To the right, under the heading "Log In", are fields for "Username:" and "Password:", followed by a "Log In" button. Below the login fields, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications 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." This is followed by a statement: "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." Below this is another statement: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. New in release 6.3 of the Avaya SBCE is the **License State** field. In the example below, the status **OK** indicates that a valid license is present.

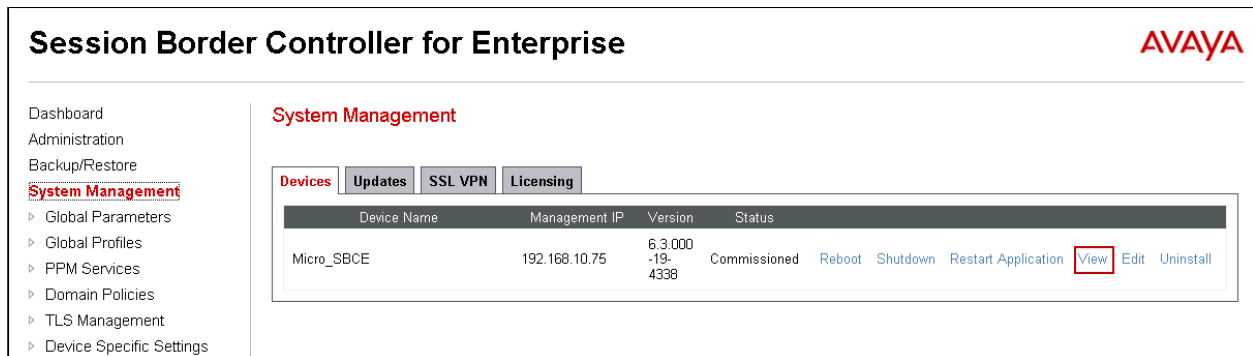


The dashboard has a top navigation bar with "Alarms", "Incidents", "Status", "Logs", "Diagnostics", and "Users". On the right of this bar are "Settings", "Help", and "Log Out". The main header reads "Session Border Controller for Enterprise" with the Avaya logo. A left sidebar lists menu items: "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "PPM Services", "Domain Policies", "TLS Management", and "Device Specific Settings". The main content area shows system information: "System Time" (11:37:53 AM EST), "Version" (6.3.000-19-4338), "Build Date" (Fri Sep 26 09:14:23 EDT 2014), "License State" (OK, highlighted with a red box), "Aggregate Licensing Overages" (0), and "Peak Licensing Overage Count" (0). Below this are sections for "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (listing two "Micro\_SBCE: Target is neither a server nor a subscriber, Sending 403 Forbidden" incidents), and "Notes" (No notes found).



## 7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **Micro\_SBCE** is shown. The management IP address that was configured during installation is shown here. Note that the management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



**Session Border Controller for Enterprise** AVAYA

**System Management**

Dashboard  
Administration  
Backup/Restore  
**System Management**  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
‣ TLS Management  
‣ Device Specific Settings

**Devices** Updates SSL VPN Licensing

Device Name	Management IP	Version	Status				
Micro_SBCE	192.168.10.75	6.3.000 -19- 4338	Commissioned	Reboot	Shutdown	Restart Application	<b>View</b> Edit Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, as shown on the screen on the next page, containing the current device configuration and network settings.

Note that the **A1** and **B1** interfaces correspond to the private and public interfaces for the Avaya SBCE. In the reference configuration, Remote Workers support was deployed on the same Avaya SBCE already provisioned for SIP trunking, but adding separate IP addresses. The highlighted **A1** and **B1** IP addresses are the ones relevant to these Application Notes. Other IP addresses assigned to these interfaces on the screen below are used to support SIP trunking and they are not discussed in this document. On the **License Allocation** area of the **System Information**, verify that there are sufficient **Standard** and **Advanced Sessions** to support the desired number of simultaneous Remote Workers sessions. The number of sessions and encryption features are primarily controlled by the license file installed.

System Information: Micro\_SBCE

**General Configuration**

Appliance Name	Micro_SBCE
Box Type	SIP
Deployment Mode	Proxy

**Device Configuration**

HA Mode	No
Two Bypass Mode	No

**License Allocation**

Standard Sessions	500
Requested: 500	
Advanced Sessions	100
Requested: 100	
Scopia Video Sessions	100
Requested: 100	
Encryption	<input checked="" type="checkbox"/>

**Network Configuration**

IP	Public IP	Netmask	Gateway	Interface
10.5.5.152	10.5.5.152	255.255.255.0	10.5.5.254	A1
10.5.5.153	10.5.5.153	255.255.255.0	10.5.5.254	A1
172.16.157.189	172.16.157.189	255.255.255.192	172.16.157.129	B1
172.16.157.160	172.16.157.160	255.255.255.192	172.16.157.129	B1
172.16.157.161	172.16.157.161	255.255.255.192	172.16.157.129	B1

**DNS Configuration**

Primary DNS	192.168.216.122
Secondary DNS	192.168.153.242
DNS Location	DMZ
DNS Client IP	172.16.157.189

**Management IP(s)**

IP	192.168.10.75
----	---------------

## 7.3. Network Management


Select **Network Management** under **Device Specific Settings** on the left-side menu to enter or to verify the network configuration parameters assigned to the Avaya SBCE interfaces.

Under **Devices** in the center pane, select the device being managed, **Micro\_SBCE** in the sample configuration. On the **Networks** tab, click **Add** or **Edit** to enter or to modify the network information as needed. Note that the **A1** and **B1** interfaces correspond to the private and public interfaces for the Avaya SBCE.

The following Avaya SBCE IP addresses and associated interfaces were used in the reference configuration:

- **A1: 10.5.5.152** – “Private” address previously configured for SIP trunking. This address is not relevant to the Remote Workers functionality and is not discussed in this document.
- **A1:10.5.5.153** – New “private” address added for Remote Workers access to the enterprise private network.
- **B1:172.16.157.189** – “Public” address previously configured for SIP trunking. This address is not relevant to the Remote Workers functionality and is not discussed in this document.
- **172.16.157.160** - New “public” address added for Remote Worker SIP traffic. Remote Worker SIP endpoints will use this “public” address to established connection to the IP Office through the Avaya SBCE for registration and telephony functions.
- **172.16.157.161** - New “public” address added for Remote Worker DNS and XMPP (one-X Portal) traffic. The Avaya SBCE relayed DNS traffic received from Avaya one-X® Mobile clients to an internal DNS server at the enterprise. This internal DNS server was configured to return the proper external IP address information based on the type of service requested by the Avaya one-X® Mobile client.

### Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ PPM Services

▸ Domain Policies

▸ TLS Management

▾ Device Specific Settings

Network Management

Network Management: Micro\_SBCE

Devices

Micro\_SBCE

Interfaces

Networks

Add

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	10.5.5.254	255.255.255.0	A1	10.5.5.152, 10.5.5.153	Edit Delete
Network_B1	172.16.157.129	255.255.255.192	B1	172.16.157.189, 172.16.157.160, 172.16.157.161	Edit Delete

## 7.4. Relay Services

IP Office Remote Worker best practices recommend that all traffic that is not SIP or media related (DNS, XMPP, etc.) should be forwarded directly from the endpoints to the required service through the enterprise firewall, and not through the Avaya SBCE. In the test environment, a firewall was not available between the simulated remote site and the IP Office location. The Relay Services feature of the Avaya SBCE was used to perform port forwarding capabilities normally done by the firewall.

Navigate to **Device Specific Settings** → **DMZ Services** → **Relay Services** and click **Add** to configure the application relays rules. The following screen shows the application relays needed in the sample configuration to allow all the necessary traffic to be routed to the appropriate internal servers.

The Application Relay named **DNS** was configured to relay DNS queries and responses on **UDP** port **53** between the Avaya one-X® Mobile Preferred VoIP clients and the enterprise DNS server. The **Remote IP:Port** was set to **192.168.10.100**, the IP address of the internal DNS server. The **Listen IP:Port** was set to the IP address and port of the Avaya SBCE's external IP address designated for application relay (**172.16.157.161**) . The **Connected IP** was set to the internal IP address of the Avaya SBCE used for Remote Workers (**10.5.5.153**).

The Application Relays named **OneXP1** and **OneXP2** were created to relay XMPP traffic on **TCP** ports **5222** and **8444** between the Avaya one-X® Mobile Preferred VoIP clients and Avaya one-X Portal. The **Remote IP:Port** was set in this case to the IP address of the internal Avaya one-X Portal server (**10.5.5.90**), which runs on the IP Office Primary server. Similarly, Application Relays **OneXP3** and **OneXP4** were created to relay XMPP traffic on **TCP** ports **8063** and **9443** between the Avaya Flare® Experience VoIP clients and Avaya one-X® Portal.

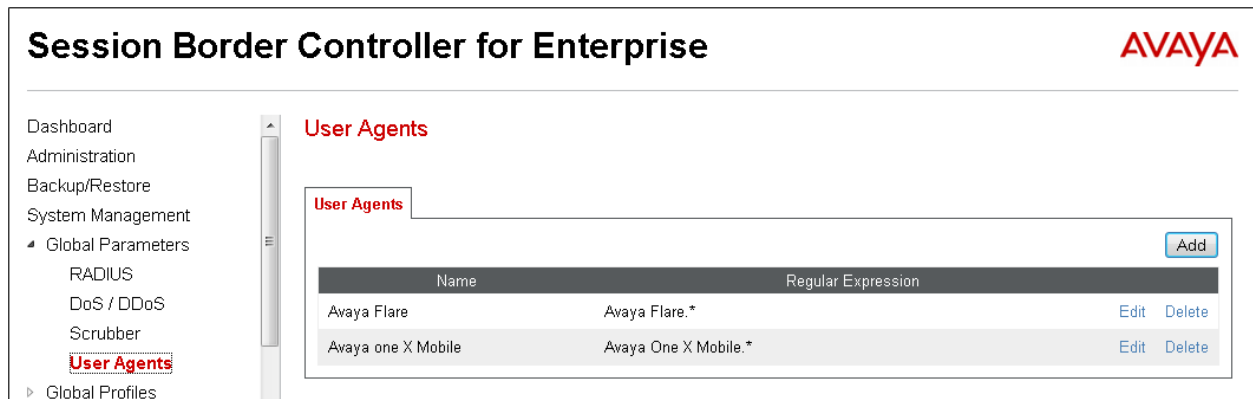
The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows a navigation menu with 'Relay Services' highlighted. The main content area is titled 'Relay Services: Micro\_SBCE' and contains a table of configured application relays. The table has columns for Name, Type, Remote Domain, Remote IP:Port, Remote Transport, Published Domain, Listen IP:Port, Listen Transport, and Connect IP. There are five rows of data, each with a 'View' link. An 'Add' button is located at the top right of the table.

Name	Type	Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP
OneXP1	XMPP	sil.miami.avaya.com	10.5.5.90:5222	TCP	sil.miami.avaya.com	172.16.157.161:5222	TCP	10.5.5.153 <a href="#">View</a>
DNS	LDAP	sil.miami.avaya.com	192.168.10.100:53	UDP	sil.miami.avaya.com	172.16.157.161:53	UDP	10.5.5.153 <a href="#">View</a>
OneXP2	XMPP	sil.miami.avaya.com	10.5.5.90:8444	TCP	sil.miami.avaya.com	172.16.157.161:8444	TCP	10.5.5.153 <a href="#">View</a>
OneXP3	XMPP	sil.miami.avaya.com	10.5.5.90:8063	TCP	sil.miami.avaya.com	172.16.157.161:8063	TCP	10.5.5.153 <a href="#">View</a>
OneXP4	XMPP	sil.miami.avaya.com	10.5.5.90:9443	TCP	sil.miami.avaya.com	172.16.157.161:9443	TCP	10.5.5.153 <a href="#">View</a>

## 7.5. User Agents

**User Agents** were created for the different endpoints tested. This allows for different policies to be applied based on the type of device being used. For example, Avaya Flare remote workers used SRTP for the media, while one-X® Mobile remote workers used RTP.

Navigate to **Global Parameters** → **User Agents** and click **Add** to configure the User Agents. The following screen shows the User Agents created in the reference configuration. The **Regular Expression** field is used to match the information contained on the User-Agent header arriving from the endpoint. The “.” in the expression is used to match any character string after the user agent name.



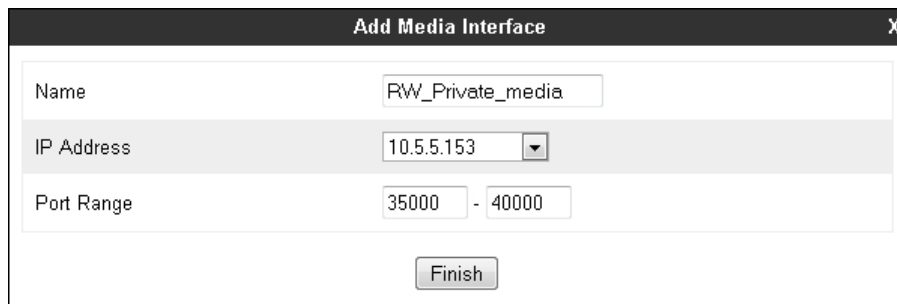
The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters (expanded), RADIUS, DoS / DDoS, Scrubber, **User Agents** (highlighted), and Global Profiles. The main content area is titled 'User Agents' and features a table with two columns: 'Name' and 'Regular Expression'. There are two entries in the table: 'Avaya Flare' with the regular expression 'Avaya Flare.\*' and 'Avaya one X Mobile' with the regular expression 'Avaya One X Mobile.\*'. Each entry has 'Edit' and 'Delete' links to its right. An 'Add' button is located in the top right corner of the table area.

Name	Regular Expression	
Avaya Flare	Avaya Flare.*	<a href="#">Edit</a> <a href="#">Delete</a>
Avaya one X Mobile	Avaya One X Mobile.*	<a href="#">Edit</a> <a href="#">Delete</a>

## 7.6. Media Interfaces

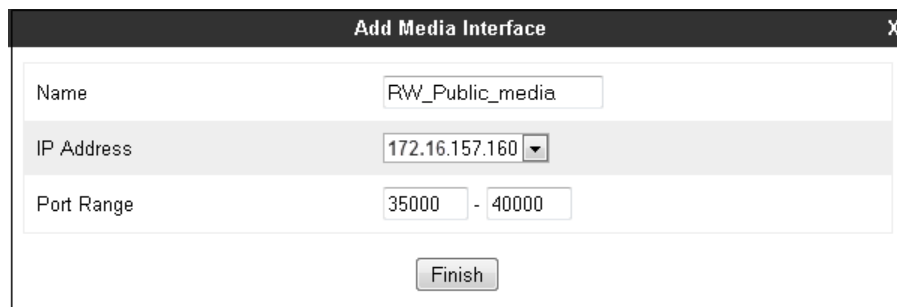
Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Micro\_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE used for Remote Workers from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. It contains three input fields: "Name" with the value "RW\_Private\_media", "IP Address" with a dropdown menu showing "10.5.5.153", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center.

A Media Interface facing the public network side was similarly created. The outside IP Address of the Avaya SBCE used for Remote Worker SIP traffic was selected from the drop-down menu. The **Port Range** was left at the default values. Click **Finish**.

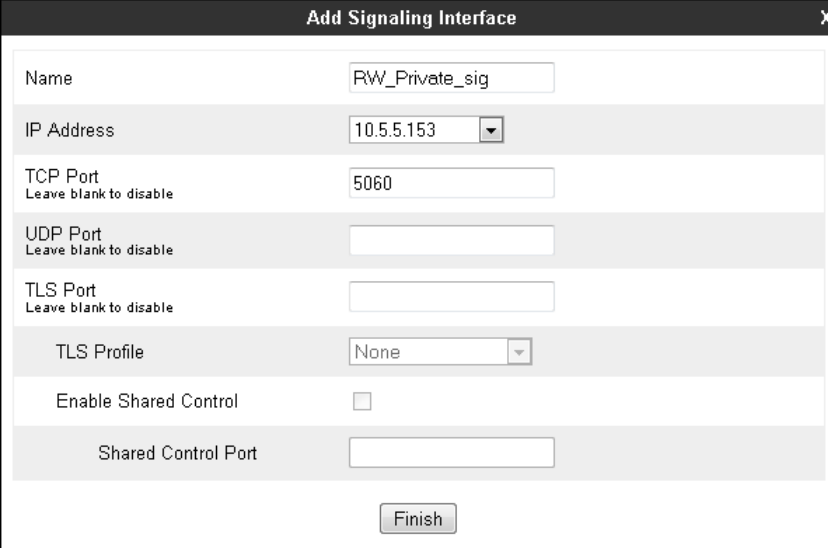


The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. It contains three input fields: "Name" with the value "RW\_Public\_media", "IP Address" with a dropdown menu showing "172.16.157.160", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center.

## 7.7. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Micro\_SBCE** device and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address of the Avaya SBCE used for Remote Workers from the **IP Address** drop-down menu. Enter **5060** for **TCP Port**, since TCP port 5060 was used to listen for Remote Worker signaling traffic from the IP Office in the sample configuration. Click **Finish**.



The screenshot shows a web-based configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are as follows:

Field Label	Value / Option
Name	RW_Private_sig
IP Address	10.5.5.153 (selected from dropdown)
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	(empty)
TLS Port <small>Leave blank to disable</small>	(empty)
TLS Profile	None (selected from dropdown)
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	(empty)

At the bottom center of the window is a button labeled "Finish".

A Signaling Interface facing the public network side was similarly created. The outside IP Address of the Avaya SBCE used for Remote Worker SIP traffic was selected from the drop-down menu. In the public network direction, both **TCP Port 5060** and **TLS Port 5061** were used. Select **AvayaSBCServer** from the **TLS Profile** drop down menu. Click **Finish**.

## 7.8. Server Interworking

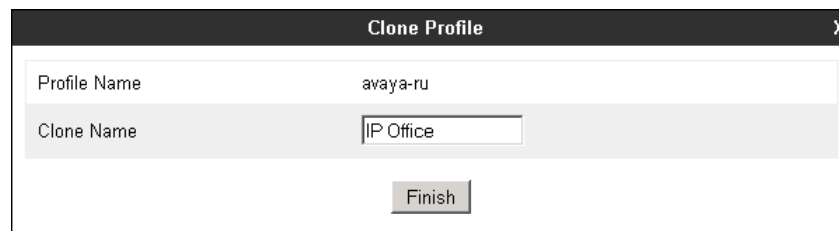
Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. In the reference configuration, a profile named **IP Office** was created by cloning the default **avaya-ru** interworking profile.

To configure the interworking profile for the IP Office, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select **avaya-ru** from the list of pre-defined profiles. Click **Clone**.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No

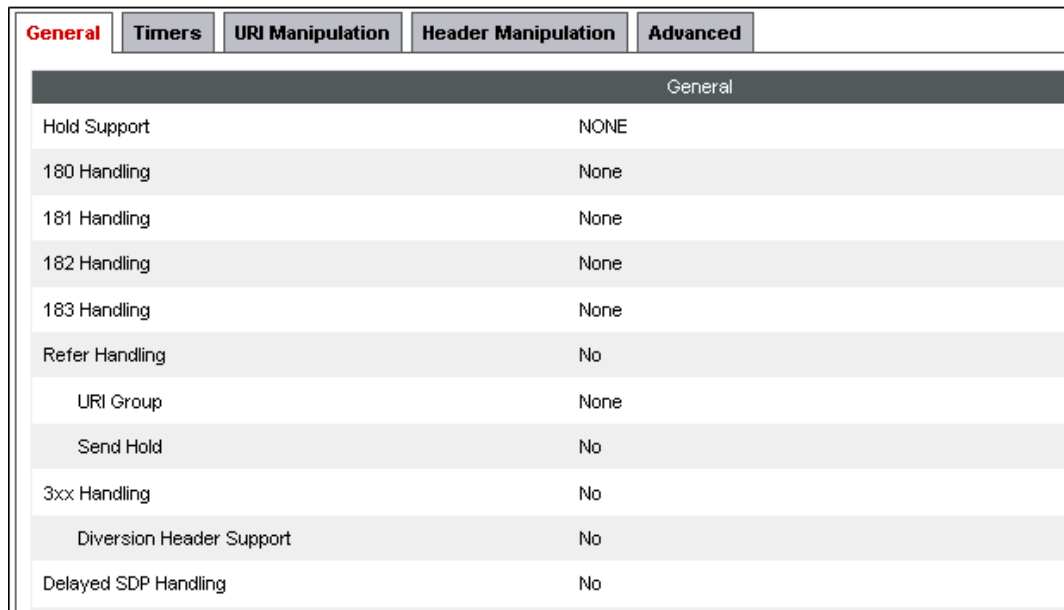


Enter a descriptive name for the cloned profile. Click **Finish**.



A dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two input fields: "Profile Name" with the value "avaya-ru" and "Clone Name" with the value "IP Office". Below the fields is a "Finish" button.

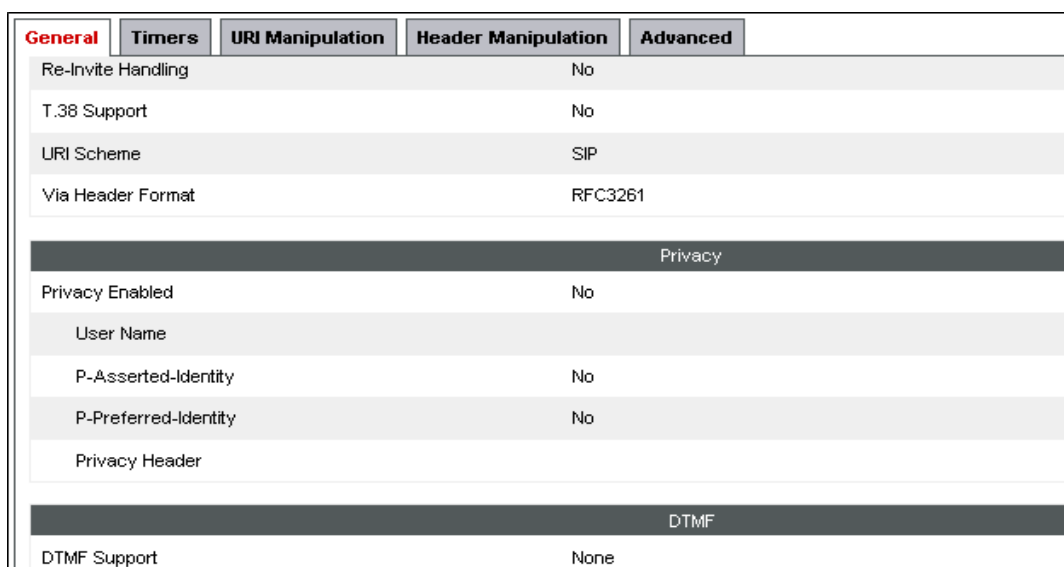
On the newly cloned *IP Office* interworking profile, verify the settings on the **General** tab:



A screenshot of the "General" tab in a configuration window. The tab is selected, and the settings are as follows:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No

Scroll down to the bottom of the tab:



A screenshot of the bottom portion of the "General" tab in a configuration window. The settings are as follows:

Privacy	
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

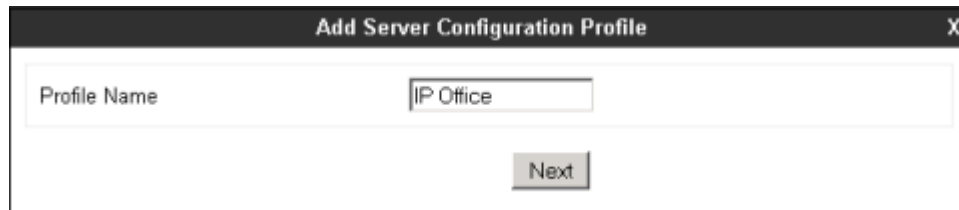
DTMF	
DTMF Support	None

The **Timers**, **URI Manipulation** and **Header Manipulation** tabs contain no entries.  
The **Advanced** tab settings are shown on the screen below:

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				No
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				Yes
OCS Extensions				No
AVAYA Extensions				Yes
NORTEL Extensions				No
Diversion Manipulation				No
Metaswitch Extensions				No
Reset on Talk Spurt				No
Reset SRTP Context on Session Refresh				No
Has Remote SBC				Yes
Route Response on Via Port				No
Cisco Extensions				No
				<a href="#">Edit</a>

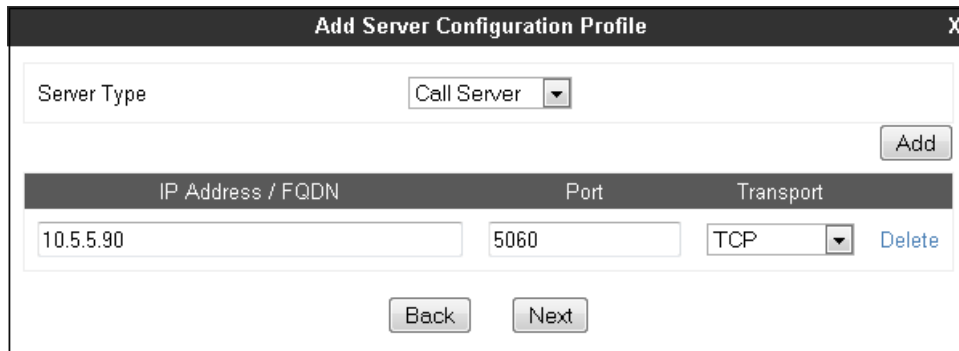
## 7.9. Server Configuration

From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



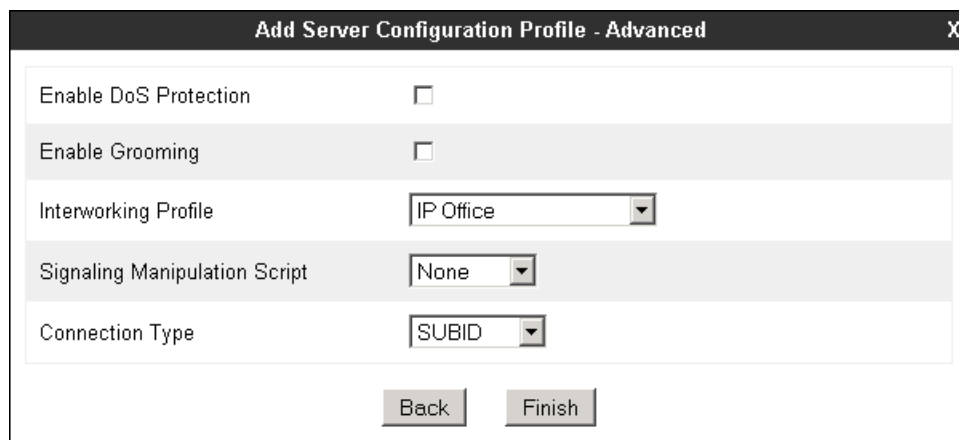
The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "IP Office". Below this field is a button labeled "Next".

On the **Add Server Configuration Profile** Tab select **Call Server** from the drop down menu for the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the IP Office LAN1, as defined in **Section 5.2**. Enter **5060** under **Port** and select **TCP** for **Transport**. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a "Server Type" dropdown menu set to "Call Server". To the right of this dropdown is an "Add" button. Below this is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The "IP Address / FQDN" field contains "10.5.5.90", the "Port" field contains "5060", and the "Transport" dropdown is set to "TCP". To the right of the "Transport" dropdown is a "Delete" link. At the bottom of the dialog are "Back" and "Next" buttons.

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select **IP Office** from the **Interworking Profile** drop down menu. Click **Finish**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced" with a close button (X) in the top right corner. Inside the dialog, there are several configuration options: "Enable DoS Protection" (checkbox), "Enable Grooming" (checkbox), "Interworking Profile" (dropdown menu set to "IP Office"), "Signaling Manipulation Script" (dropdown menu set to "None"), and "Connection Type" (dropdown menu set to "SUBID"). At the bottom of the dialog are "Back" and "Finish" buttons.

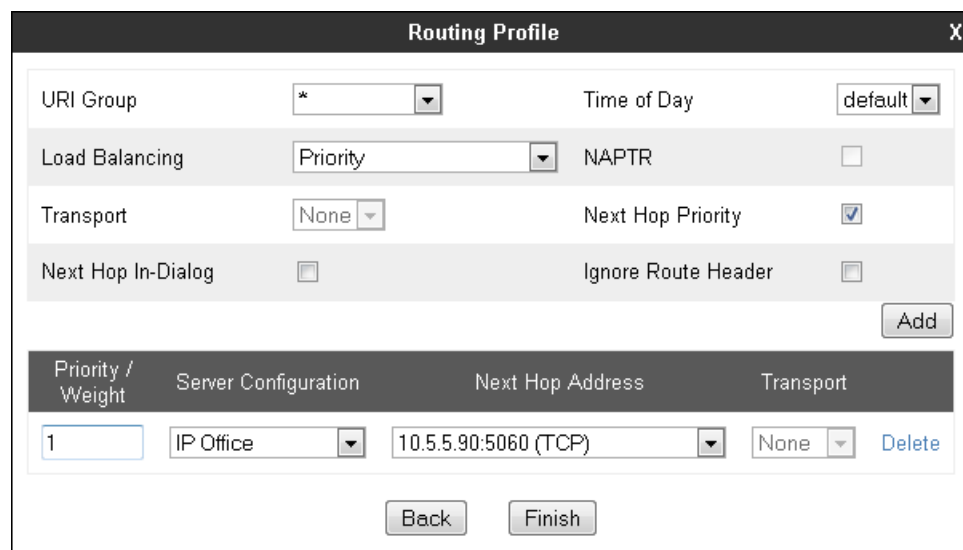
## 7.10. Routing

To create an inbound route to the IP Office, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The image shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "To IPO from RW". Below this field is a button labeled "Next".

On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Since only one next-hop is defined, enter **1** under **Priority/Weight**. Under **Server Configuration**, select **IP Office**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the IP Office Server Profile in **Section 7.9**. Defaults were used for all other parameters. Click **Finish**.



The image shows a "Routing Profile" dialog box with various configuration options and a table of next-hop addresses.

Configuration options:

- URI Group: \*
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐

Buttons: Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IP Office	10.5.5.90:5060 (TCP)	None	Delete

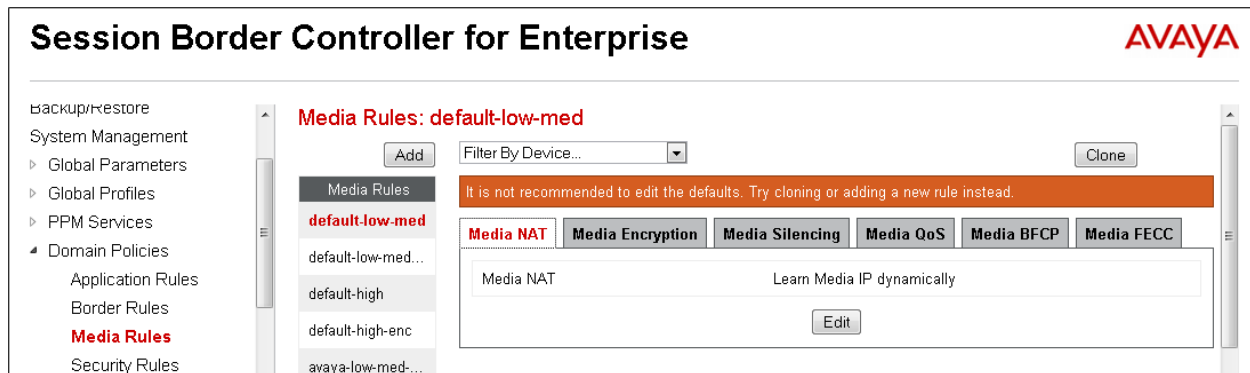
Buttons: Back, Finish

## 7.11. Media Rules

Media rules were created to specify the media encryption to be used with each type of Remote Worker endpoint. These rules will be later applied to the End Point Policy Groups and ultimately to the Subscriber and Server Flows, defined later in this document.

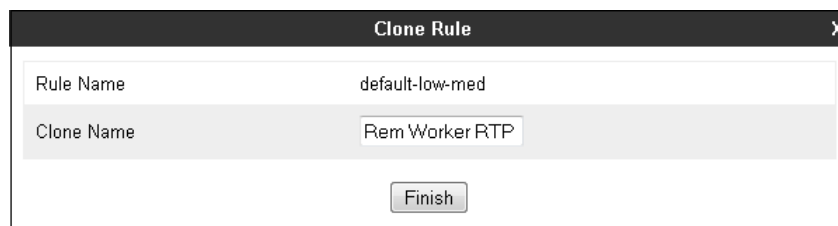
In the reference configuration, two new media rules were created, by cloning and then modifying the *default-low-med* rule.

From the **Domain Policies** menu on the left-hand navigation pane, select **Media Rules**. Select **default-low-med-enc** from the **Media Rules** list and click the **Clone** button.



### 7.11.1. Media Rule - RTP

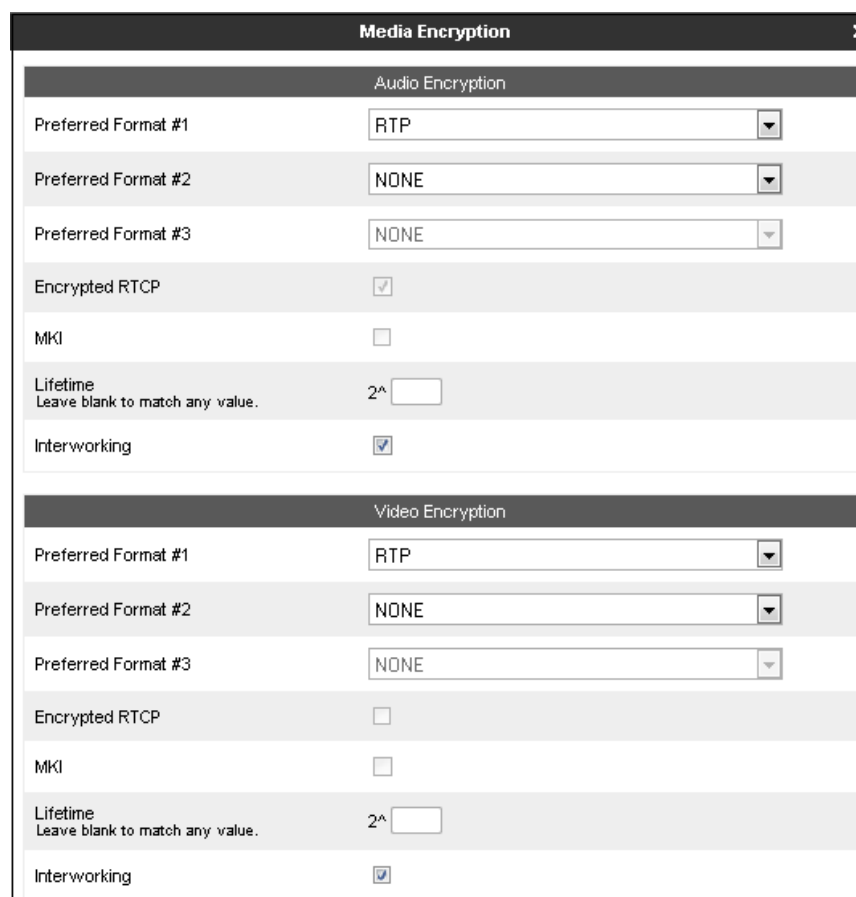
The first media rule used RTP for media encryption. Enter an appropriate **Clone Name**, similar to the screen below. Click **Finish**.



A dialog box titled "Clone Rule" with a close button (X) in the top right corner. It contains two input fields: "Rule Name" with the value "default-low-med" and "Clone Name" with the value "Rem Worker RTP". Below these fields is a "Finish" button.

Rule Name	default-low-med
Clone Name	Rem Worker RTP
<button>Finish</button>	

The screen below shows the **Media Encryption** tab of the cloned *Rem Worker RTP* rule. No modifications were made to the defaults on this or any other tab of this media rule.



A screenshot of the "Media Encryption" tab in a software interface. The tab is divided into two sections: "Audio Encryption" and "Video Encryption". Each section contains several settings: "Preferred Format #1", "Preferred Format #2", and "Preferred Format #3" (all dropdown menus); "Encrypted RTCP" (checkbox); "MkI" (checkbox); "Lifetime" (text input with a "2^" prefix and a note "Leave blank to match any value."); and "Interworking" (checkbox). The "Audio Encryption" section has "RTP" selected for Preferred Format #1, "NONE" for Preferred Format #2 and #3, "Encrypted RTCP" checked, "MkI" unchecked, "Lifetime" set to "2^", and "Interworking" checked. The "Video Encryption" section has "RTP" selected for Preferred Format #1, "NONE" for Preferred Format #2 and #3, "Encrypted RTCP" unchecked, "MkI" unchecked, "Lifetime" set to "2^", and "Interworking" checked.

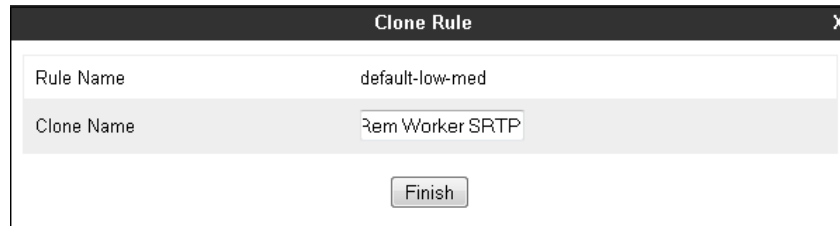
Audio Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input checked="" type="checkbox"/>
MkI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MkI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^
Interworking	<input checked="" type="checkbox"/>

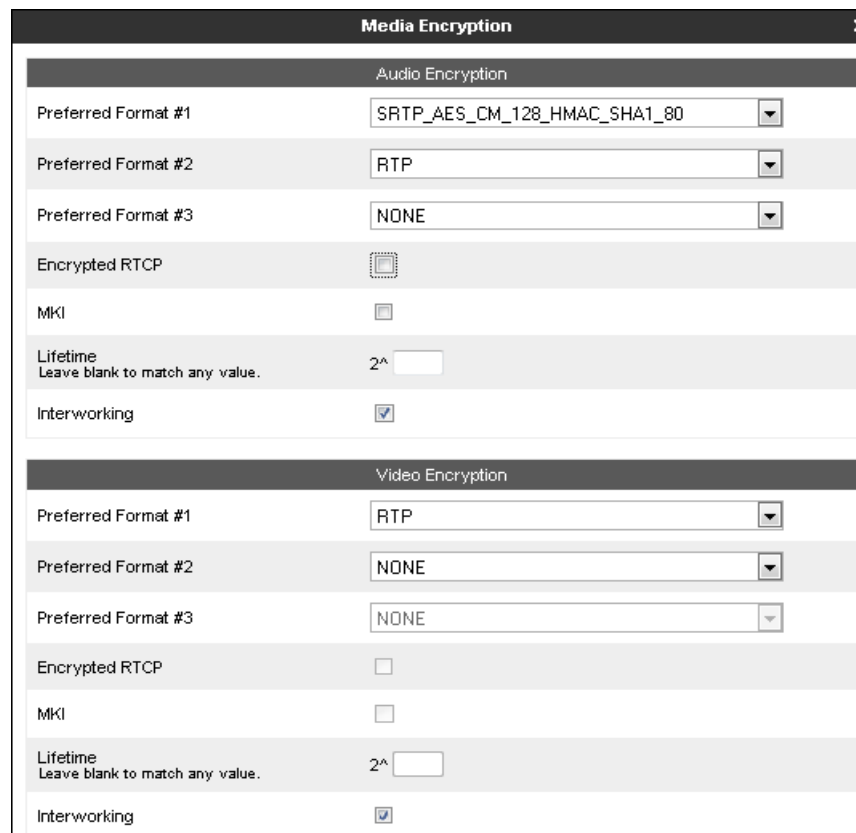
### 7.11.2. Media Rule - SRTP

The second media rule used SRTP as the preferred format for media encryption. Repeat the previous process to clone the *default-low-med rule*. Enter an appropriate **Clone Name**, similar to the screen below. Click **Finish**.



A dialog box titled "Clone Rule" with a close button (X) in the top right corner. It contains two input fields: "Rule Name" with the value "default-low-med" and "Clone Name" with the value "Rem Worker SRTP". Below these fields is a "Finish" button.

On the the **Media Encryption** tab of the new *Rem Worker SRTP* rule, click **Edit** (not shown). Under **Audio Encryption**, select *SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80* from the **Preferred Format #1** drop down menu. Select *RTP* under **Preferred Format #2**. Verify **Encrypted RTCP** is unchecked. Under **Video Encryption**, make sure to leave the **Preferred Format #1** as *RTP*, as shown.



A dialog box titled "Media Encryption" with a close button (X) in the top right corner. It is divided into two sections: "Audio Encryption" and "Video Encryption".

**Audio Encryption:**

- Preferred Format #1: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 (dropdown)
- Preferred Format #2: RTP (dropdown)
- Preferred Format #3: NONE (dropdown)
- Encrypted RTCP: ☐
- MKI: ☐
- Lifetime: 2^ (text input)
- Interworking: ☒

**Video Encryption:**

- Preferred Format #1: RTP (dropdown)
- Preferred Format #2: NONE (dropdown)
- Preferred Format #3: NONE (dropdown)
- Encrypted RTCP: ☐
- MKI: ☐
- Lifetime: 2^ (text input)
- Interworking: ☒

All other parameters were left at their default values. Click **Finish** (not shown) to save your changes.

## 7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE. In the reference configuration, three different End Point Policy Groups were created. These policy groups used default sets of rules already pre-defined in the configuration, with the exception of the new Media Rules defined in **Section 7.11**.

### 7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu. Select **Add**.

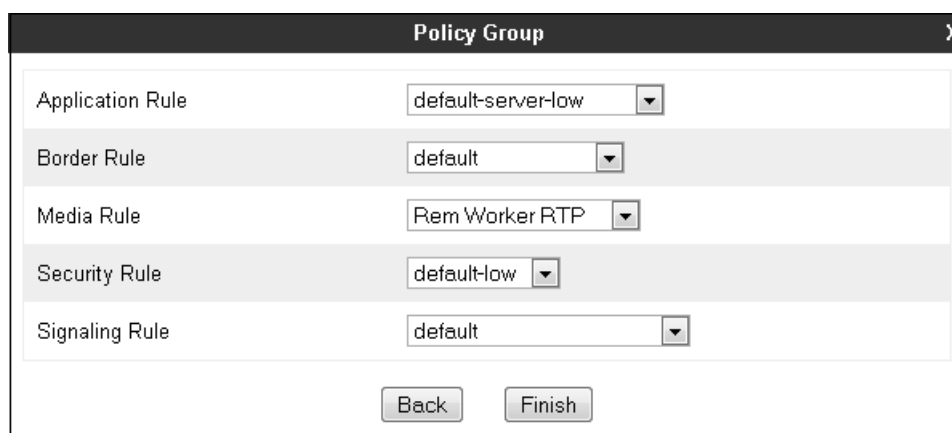
The screenshot shows the Avaya SBCE configuration interface. On the left is a sidebar menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, and Domain Policies. Under Domain Policies, 'End Point Policy Groups' is selected. The main area is titled 'Policy Groups: default-low' and contains an 'Add' button (highlighted with a red box), a 'Filter By Device...' dropdown, and a 'Clone' button. Below this is a list of existing policy groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, avaya-def-low-enc, avaya-def-high-sub..., and avaya-def-high-server. A table for configuring a new policy group is shown, with columns for Order, Application, Border, Media, Security, and Signaling. The table contains one row with the following values: Order 1, Application default, Border default, Media default-low-med, Security default-low, and Signaling default. An 'Edit' button is next to the row. A 'Summary' button is also visible.

Enter an appropriate name in the **Group Name** field. *Rem Worker Inside* was used. Click **Next**.

The screenshot shows a 'Policy Group' dialog box. It has a title bar with 'Policy Group' and a close button (X). Inside the dialog, there is a 'Group Name' label and a text input field containing the text 'Rem Worker Inside'. At the bottom right of the dialog is a 'Next' button.



In the **Policy Group** tab, under the **Application Rule** drop down menu, *default-server-low* was selected. Under **Media Rule**, the *Rem Worker RTP* media rule created in **Section 7.11** was selected. Default rules were used for all other fields as shown below. Click **Finish**.

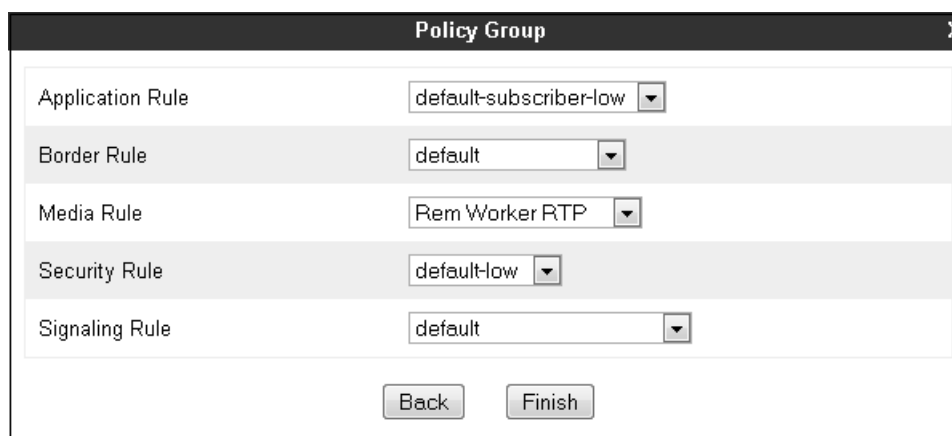


The screenshot shows a 'Policy Group' configuration window with a close button (X) in the top right corner. It contains five rows of configuration options, each with a label and a dropdown menu. The 'Application Rule' dropdown is set to 'default-server-low'. The 'Border Rule' dropdown is set to 'default'. The 'Media Rule' dropdown is set to 'Rem Worker RTP'. The 'Security Rule' dropdown is set to 'default-low'. The 'Signaling Rule' dropdown is set to 'default'. At the bottom of the window, there are two buttons: 'Back' and 'Finish'.

Rule Type	Selected Rule
Application Rule	default-server-low
Border Rule	default
Media Rule	Rem Worker RTP
Security Rule	default-low
Signaling Rule	default

### 7.12.2. End Point Policy Group – RTP

A second End Point Policy Group with the name *Rem Worker RTP* was created, repeating the steps described above. This policy group will be applied later to the Subscriber Flow corresponding to the one-X® Mobile users. Under the **Application Rule** drop down menu, *default-subscriber-low* was selected. Under **Media Rule**, the *Rem Worker RTP* media rule created in **Section 7.11** was selected. Default rules were used for all other fields as shown below. Click **Finish**.

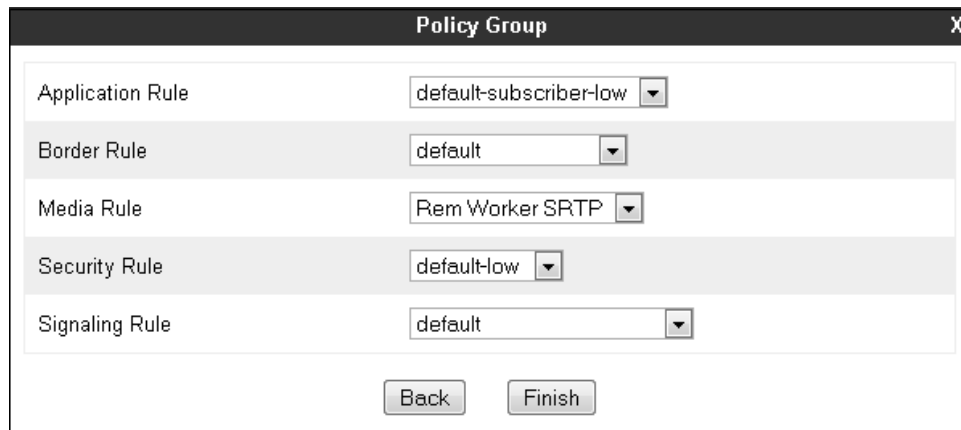


The screenshot shows a 'Policy Group' configuration window with a close button (X) in the top right corner. It contains five rows of configuration options, each with a label and a dropdown menu. The 'Application Rule' dropdown is set to 'default-subscriber-low'. The 'Border Rule' dropdown is set to 'default'. The 'Media Rule' dropdown is set to 'Rem Worker RTP'. The 'Security Rule' dropdown is set to 'default-low'. The 'Signaling Rule' dropdown is set to 'default'. At the bottom of the window, there are two buttons: 'Back' and 'Finish'.

Rule Type	Selected Rule
Application Rule	default-subscriber-low
Border Rule	default
Media Rule	Rem Worker RTP
Security Rule	default-low
Signaling Rule	default

### 7.12.3. End Point Policy Group - SRTP

A third End Point Policy Group with the name **Rem Worker SRTP** was created, repeating the steps described above. This policy group will be applied later to the Subscriber Flow corresponding to the Avaya Flare users. Under the **Application Rule** drop down menu, **default-subscriber-low** was selected. Under **Media Rule**, the **Rem Worker SRTP** media rule created in **Section 7.11** was selected. Default rules were used for all other fields as shown below. Click **Finish**.



The screenshot shows a window titled "Policy Group" with a close button (X) in the top right corner. The window contains five rows, each with a label on the left and a dropdown menu on the right. The rows are: "Application Rule" with "default-subscriber-low", "Border Rule" with "default", "Media Rule" with "Rem Worker SRTP", "Security Rule" with "default-low", and "Signaling Rule" with "default". At the bottom of the window are two buttons: "Back" and "Finish".

Rule Type	Selected Rule
Application Rule	default-subscriber-low
Border Rule	default
Media Rule	Rem Worker SRTP
Security Rule	default-low
Signaling Rule	default

Buttons: Back, Finish

## 7.13. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. Subscriber Flows are defined for each type of remote worker used. A Server Flow is configured for the IP Office. These flows combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

### 7.13.1. Subscriber Flow – Avaya one-X® Mobile users

Avaya one-X® Mobile remote workers clients used TCP or TLS for signaling and RTP for the media. See **Table 1** in **Section 3**. To create the call flow for the one-X® Mobile remote workers, from the **Device Specific** menu, select **End Point Flows** and select the **Subscriber Flows** tab. Click **Add** (not shown).

On the **Criteria** screen, enter an appropriate **Flow Name**. In the sample configuration *one X Mobile* was used. Under **User Agent**, select from the drop down menu the *Avaya one X Mobile* agent created in **Section 7.5**. Under **Signaling Interface**, select the signaling interface facing the remote endpoints, *RW\_Public\_sig*, created in **Section 7.7**. All other fields retained their default values. Click **Next**.

Criteria	
Flow Name	one X Mobile
URI Group	*
User Agent	Avaya one X Mobile
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	RW_Public_sig

Next

On the **Profile** screen, set the following:

- **Media Interface:** Select *RW\_Public\_media*. (Created in **Section 7.6**).
- **End Point Policy Group:** Select *Rem Workers RTP*. (Created in **Section 7.12.2**).
- **Roting Profile:** Select *To IPO from RW*. (Created in **Section 7.10**).
- **Phone Interworking Profile:** Select *Avaya-Ru* from the list of default profiles.
- **TLS Client Profile:** Select *Avaya SBCCClient*.
- Leave other fields at their default values.
- Click **Finish**.

Certain End Point Policy Groups are not available because there are no RADIUS servers configured. To use End Point Policy Groups containing Security Rules configured for authentication please add a RADIUS server.

Profile	
Source	<input checked="" type="radio"/> Subscriber <input type="radio"/> Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	RW_Public_media
End Point Policy Group	Rem Worker RTP
Routing Profile	To IPO from RW
Optional Settings	
Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	AvayaSBCCClient
File Transfer Profile	None
Signaling Manipulation Script	None
Presence Server Address Ex: domain.com, 192.168.0.101	
<div>BackFinish</div>	

### 7.13.2. Subscriber Flow – Avaya Flare users

Avaya Flare remote workers clients used TLS for signaling and SRTP for the media (or RTP if video is enabled). See **Table 1** in **Section 3**. To create the call flow for the Avaya Flare remote workers, from the **Device Specific** menu, select **End Point Flows**, then select the **Subscriber Flows** tab. Click **Add** (not shown).

The screen below shows the Subscriber Flow named *Flare tls-srtp* in the sample configuration. Note that **User Agent** is set to the *Avaya Flare* agent created in **Section 7.5**. The **End Point Policy Group** is set to *Rem Worker SRTP*, created in **Section 7.12.3**.

View Flow: Flare tls-srtp

Criteria

Flow Name	Flare tls-srtp
URI Group	*
User Agent	Avaya Flare
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	RW_Public_sig

Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	AvayaSBCClient
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Avaya Flare
Media Interface	RW_Public_media
End Point Policy Group	Rem Worker SRTP
Routing Profile	To IPO from RW
Presence Server Address	---

### 7.13.3. Server Flow – Avaya IP Office

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named ***IPO Serv from RW*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is uses the ***default*** profile. Click **Finish**.

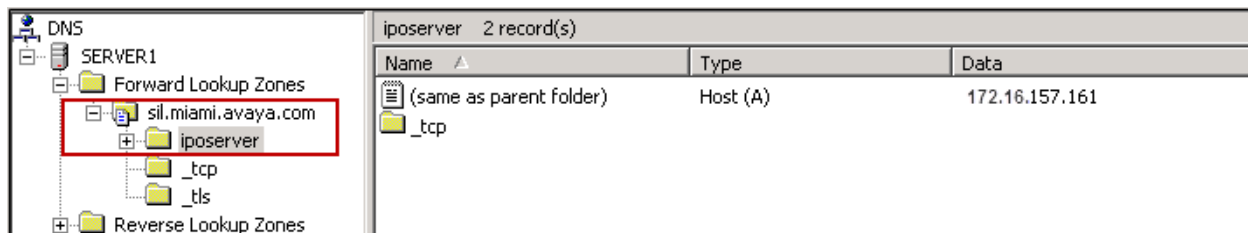
Edit Flow: IPO Serv from RW	
Flow Name	IPO Serv from RW
Server Configuration	IP Office
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	RW_Public_sig
Signaling Interface	RW_Private_sig
Media Interface	RW_Private_media
End Point Policy Group	Rem Worker RTP
Routing Profile	default
Topology Hiding Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None
<b>Finish</b>	

## 8. DNS Server Configuration

The Avaya one-X® Mobile Preferred VoIP clients used during the test required a Fully Qualified Domain Name (FQDN) to be entered on the Server ID field of the client settings screen. This FQDN should be reachable from the public Internet. For testing purposes, since a private FQDN was used in the lab environment, the router at the Remote Workers site was configured to use one of the external IP addresses of the Avaya SBCE (172.16.157.161) as its DNS server. The Avaya SBCE relayed DNS traffic to the internal DNS server (192.168.10.100) at the enterprise via the Relay Services configured in **Section 7.4**.

Detailed discussion of the DNS server configuration is beyond the scope of these Application Notes. The following screens are provided as an example illustrating the DNS settings used in the reference configuration to respond to the DNS queries from the one-X® Mobile Preferred clients.

The screen below shows the record for FQDN *iposerver.sil.miami.avaya.com*. A standard DNS query on this FQDN will return address **172.16.157.161**. This is the external Avaya SBCE address used for Remote Worker DNS and also XMPP (one-X Portal) traffic.

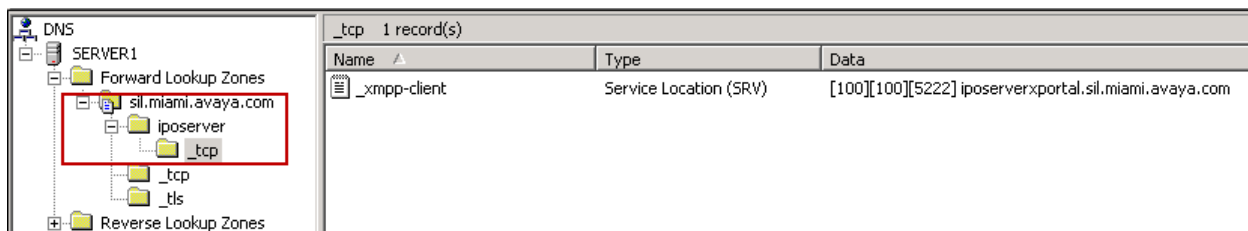


The screenshot shows the DNS configuration interface. On the left, a tree view under 'SERVER1' shows 'Forward Lookup Zones' expanded, with 'sil.miami.avaya.com' selected. Under this zone, 'iposerver' is highlighted with a red box. On the right, the 'iposerver' zone has 2 records. The first record is a Host (A) record with the name '(same as parent folder)' and the data '172.16.157.161'. The second record is a service record named '\_tcp'.

Name	Type	Data
(same as parent folder)	Host (A)	172.16.157.161
_tcp		

The internal DNS server was configured to provide the proper external IP address and port information based on the type of service requested by the one-X Mobile Preferred clients.

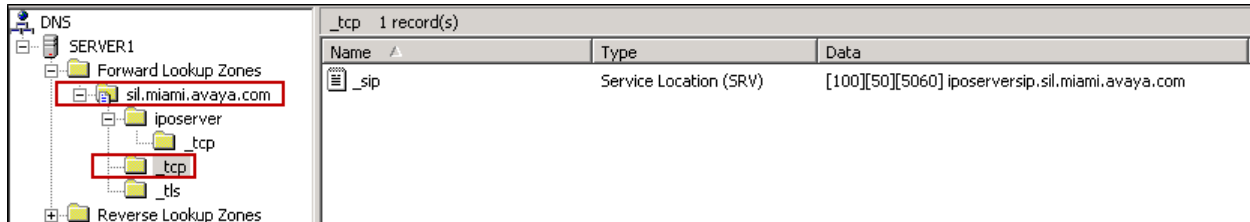
The screen below shows the XMPP Service Location record. A DNS service (SRV) query for XMPP returned *iposerverxportal.sil.miami.avaya.com* as the host offering the service on port **5222**. This host is later associated with IP address “172.16.157.161”, the external Avaya SBCE interface used for Remote Worker XMPP (one-X Portal) traffic. The Avaya SBCE relayed XMPP traffic received on this interface to the Avaya one-X® Portal server via Relay Services configured in **Section 7.4**.



The screenshot shows the DNS configuration interface. On the left, a tree view under 'SERVER1' shows 'Forward Lookup Zones' expanded, with 'sil.miami.avaya.com' selected. Under this zone, 'iposerver' is highlighted with a red box. On the right, the '\_tcp' zone has 1 record. The record is a Service Location (SRV) record with the name '\_xmpp-client' and the data '[100][100][5222] iposerverxportal.sil.miami.avaya.com'.

Name	Type	Data
_xmpp-client	Service Location (SRV)	[100][100][5222] iposerverxportal.sil.miami.avaya.com

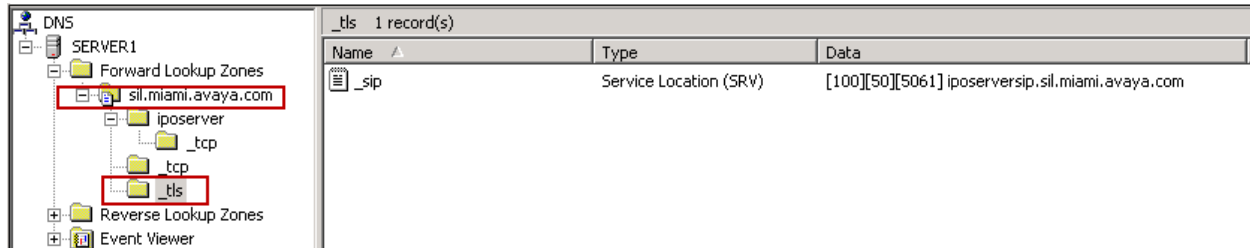
The screen below shows the SIP with TCP Service Location record. A DNS SRV query for SIP when using TCP returned *iposerversip.sil.miami.avaya.com* as the host offering the service on port **5060**. This host is later associated with IP address “172.16.157.160”, the external Avaya SBCE interface used for Remote Worker SIP and media traffic.



The screenshot shows the DNS Manager interface. On the left, the tree view is expanded to 'Forward Lookup Zones' > 'sil.miami.avaya.com' > 'iposerver' > '\_tcp'. The main pane shows a single record for '\_sip' of type 'Service Location (SRV)' with the data '[100][50][5060] iposerversip.sil.miami.avaya.com'.

Name	Type	Data
_sip	Service Location (SRV)	[100][50][5060] iposerversip.sil.miami.avaya.com

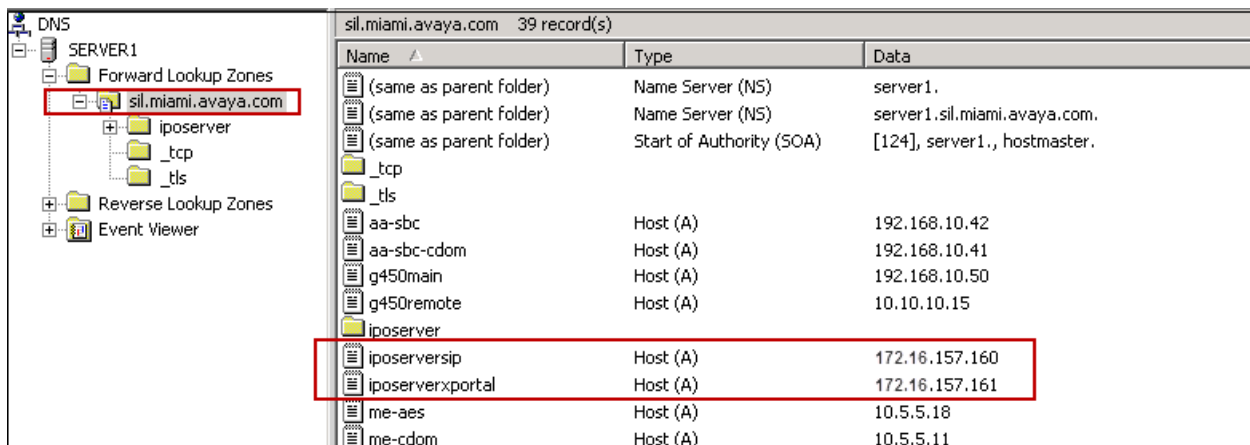
The Avaya one-X® Mobile Preferred for Android can be configured to use a secure connection using TLS. The screen below shows the Service Location record for SIP with TLS. In this case a DNS SRV query for SIP also returned *iposerversip.sil.miami.avaya.com* as the host offering the service, but on port **5061**.



The screenshot shows the DNS Manager interface. On the left, the tree view is expanded to 'Forward Lookup Zones' > 'sil.miami.avaya.com' > 'iposerver' > '\_tls'. The main pane shows a single record for '\_sip' of type 'Service Location (SRV)' with the data '[100][50][5061] iposerversip.sil.miami.avaya.com'.

Name	Type	Data
_sip	Service Location (SRV)	[100][50][5061] iposerversip.sil.miami.avaya.com

The following screen shows the Host records, associating the hosts offering the telephony (*iposerversip*) and one-X Portal (*iposerverxportal*) services in the *sil.miami.avaya.com* domain to the respective external interfaces of the Avaya SBCE.



The screenshot shows the DNS Manager interface. On the left, the tree view is expanded to 'Forward Lookup Zones' > 'sil.miami.avaya.com'. The main pane shows a list of 39 records. Two records are highlighted with a red box: 'iposerversip' and 'iposerverxportal', both of type 'Host (A)' with IP addresses 172.16.157.160 and 172.16.157.161 respectively.

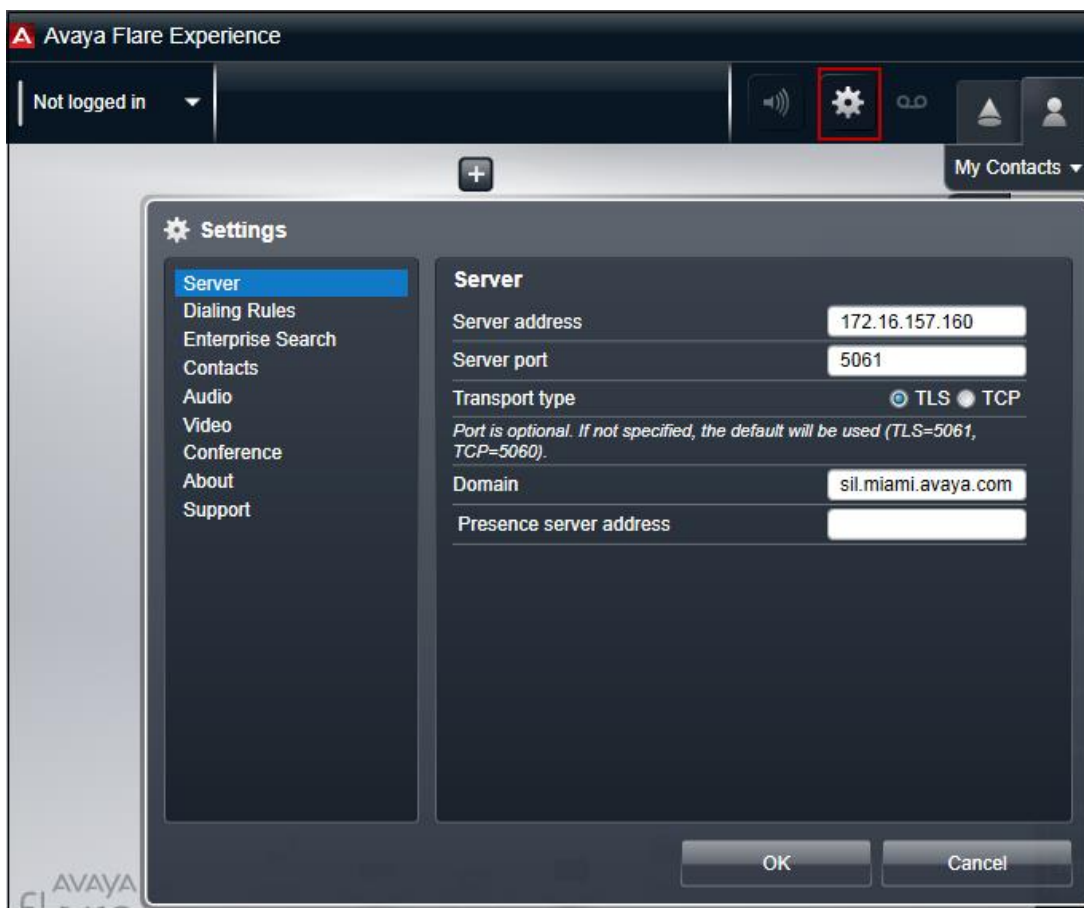
Name	Type	Data
(same as parent folder)	Name Server (NS)	server1.
(same as parent folder)	Name Server (NS)	server1.sil.miami.avaya.com.
(same as parent folder)	Start of Authority (SOA)	[124], server1., hostmaster.
_tcp		
_tls		
aa-sbc	Host (A)	192.168.10.42
aa-sbc-cdom	Host (A)	192.168.10.41
q450main	Host (A)	192.168.10.50
q450remote	Host (A)	10.10.10.15
iposerver		
iposerversip	Host (A)	172.16.157.160
iposerverxportal	Host (A)	172.16.157.161
me-aes	Host (A)	10.5.5.18
me-cdom	Host (A)	10.5.5.11



For a customer deployment, the one-X® Mobile Preferred clients may require to register to the IP Office as remote workers on the public network, and additionally to register to the IP Office locally on the private enterprise network. In this case Avaya recommends to use split DNS, where different sets of DNS information are provided depending on the source address of the DNS request. In the reference configuration, the remote workers resided solely in the untrusted network and subsequently split DNS was not necessary.

## 9. Avaya Flare® Experience for Windows Configuration

The following screen illustrates the Flare® Experience for IP Office client configuration. The **Server address** is the external IP address of the Avaya SBCE used for Remote Worker SIP and media traffic. The **Server port** is **5061** and the **Transport type** is set to **TLS**. The **Domain** was set to **sil.miami.avaya.com**, the domain configured in the IP Office LAN1 settings in **Section 5.2**.

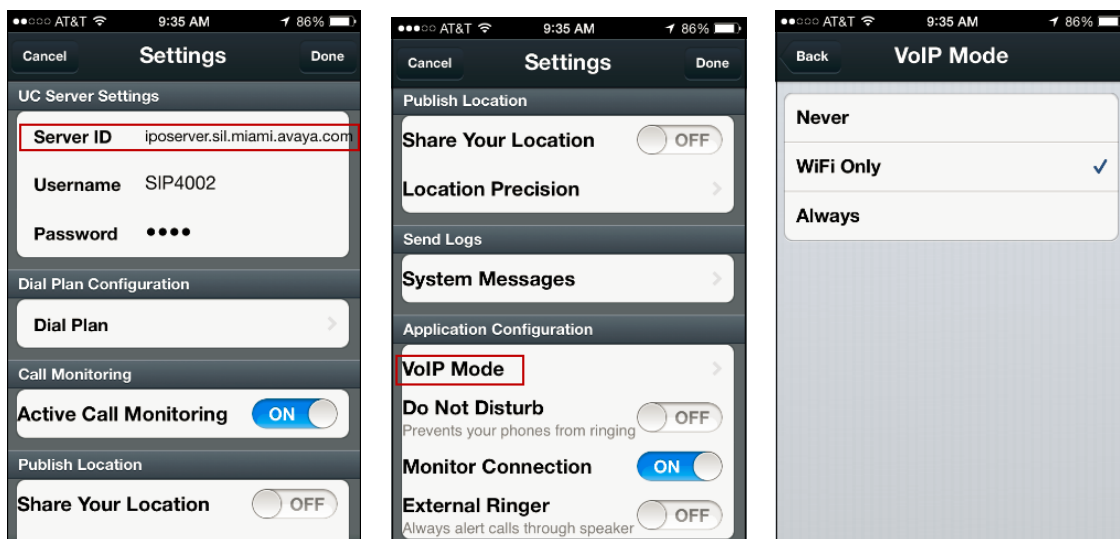


## 10. Avaya one-X® Mobile Preferred Client Configuration

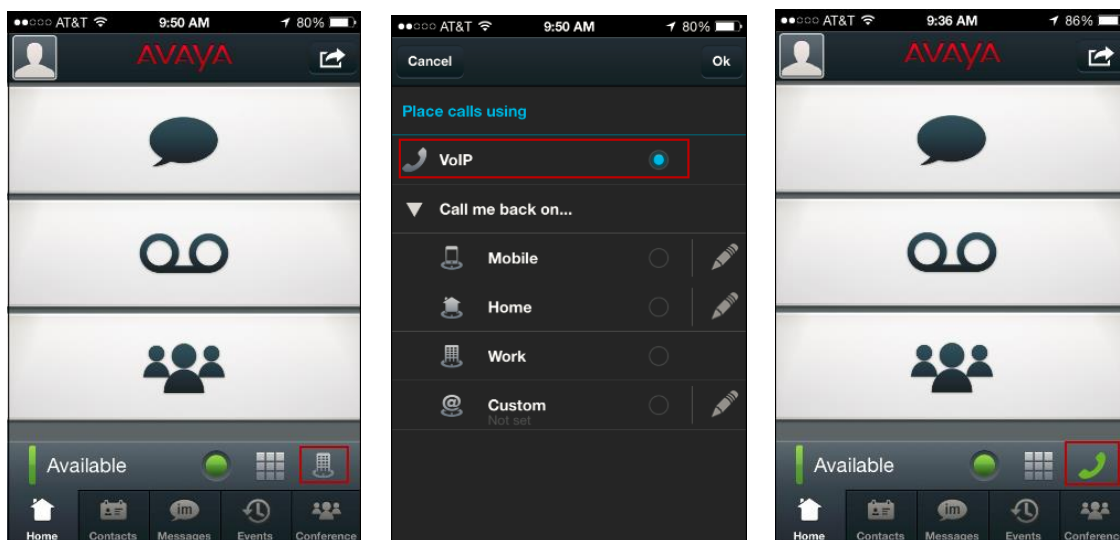
This section illustrates the administration settings on the Avaya one-X® Mobile Preferred for IP Office clients used in the reference configuration.

### 10.1. Avaya one-X® Mobile Preferred for iPhone

The following screen shows the settings used on the one-X® Mobile Preferred for IP Office clients, in the IOS version. Note that the **Server ID** was set to the FQDN of the XMPP Domain Name in the Avaya one-X® Portal server (**Section 6.2**). The **VoIP Mode** was set to operate on **WiFi Only** mode.

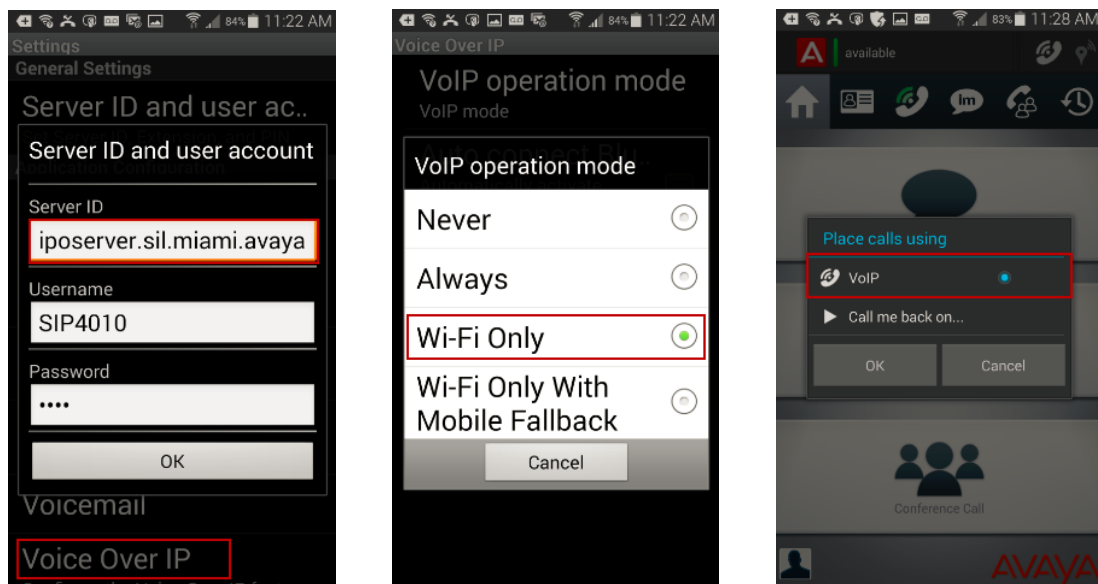


Click the **Call Facility** icon on the screen. Select **VoIP** to be able to make and receive calls from the client. At this point the phone sends a DNS SRV query for SIP to the DNS server, and once it gets the proper response, it will send a SIP registration to the IP Office via the Avaya SBCE. The green handset icon should pop up at the bottom of the screen.

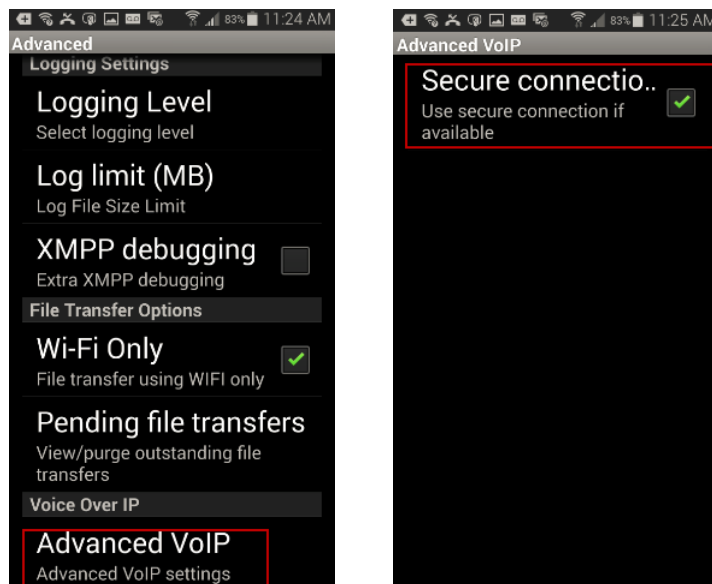


## 10.2. Avaya one-X® Mobile Preferred for Android

The one-X® Mobile Preferred for IP Office Android version was similarly configured:



Navigate to **Settings** → **Advanced** → **Advanced VoIP**. Select **Secure Connection** to allow for TLS communication to the Avaya SBCE.



## 11. System Verification

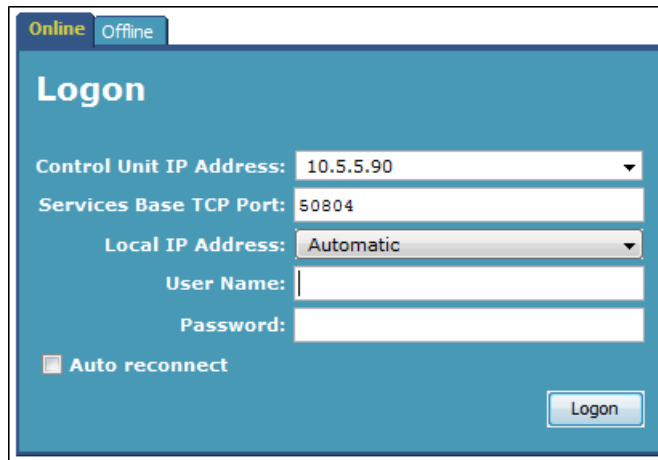
The following sections include steps that may be used to verify the functionality of the Remote Worker configuration covered on the previous sections.

### 11.1. Avaya IP Office

The Avaya IP Office System Status and Monitor applications are useful tools used for the verification and troubleshooting of the SIP connection of the Remote Workers to the IP Office.

#### 11.1.1. System Status

The Avaya IP Office System Status application can be used to verify the successful registration of the Remote Workers to the IP Office. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Under **Control Unit IP Address** select the IP address of the IP Office system under verification. Log in using the appropriate credentials.



The screenshot shows the 'Logon' window of the Avaya IP Office System Status application. At the top, there are two tabs: 'Online' (highlighted in yellow) and 'Offline'. The window has a blue header with the title 'Logon'. Below the header, there are several input fields and a checkbox. The 'Control Unit IP Address' field is a dropdown menu showing '10.5.5.90'. The 'Services Base TCP Port' field is a text box containing '50804'. The 'Local IP Address' field is a dropdown menu showing 'Automatic'. Below these are 'User Name' and 'Password' text boxes. At the bottom left, there is a checkbox labeled 'Auto reconnect'. At the bottom right, there is a 'Logon' button.

Select **Extensions** from the left pane. In the example, extensions **4002**, **4006** and **4010** are registered Remote Workers users. Note that the IP Address shown for these extensions, as seen from the IP Office, is **10.5.5.153**, which corresponds to the private interface of the Avaya SBCE used for Remote Workers.

**AVAYA** IP Office System Status

Help Snapshot LogOff Exit About

**Extension Summary**

You can get more information about an extension by double-clicking the Extension Number.

Extension Number	Current User Extension	Current User Name	Module/Slot/ IP Address	Port Number/ MAC Address	Telephone Type	Number of New Messages	Active Location
4001	4001	Ext4001	192.168.10.183	00-1B-4F-34-06-12	9620		None
4002	4002	\$1.SIP4002	10.5.5.153		Avaya One X Mobile	1	None
4006	4006	\$1.Flare SIP 4006	10.5.5.153		Avaya Flare	0	None
4010	4010	\$1.SIP4010	10.5.5.153		Avaya One X Mobile	0	None

Refresh Print...

1:03:56 PM Online

Additional status and call tracing information can be obtained by double-clicking the extension number of a particular extension:

**Extension Status**

Extension Number: 4006  
 IP address: 10.5.5.153  
 Active Location: None  
 Telephone Type: Avaya Flare  
 User Agent: Avaya Flare Engine/1.1.0 (Avaya 1.1.13; Windows NT 5.1)  
 Layer 4 Protocol: TCP  
 Current User Extension Number: 4006  
 Current User Name: \$1.Flare SIP 4006  
 Forwarding: Off  
 Twinning: Off  
 Do Not Disturb: Off  
 Message Waiting: Off  
 Number of New Messages: 0  
 Phone Manager Type: None  
 SIP Device Features: REFER,UPDATE  
 License Reserved: No  
 Last Date and Time License Allocated:  
 Packet Loss Fraction: Connection Type: VCM  
 Jitter: Codec: G711 Mu  
 Round Trip Delay: Remote Media Address: 10.5.5.91

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
11	Connected	00:00:33	4056	Outgoing	Line: 1 H.323 10.5.5.91 Channel: 1

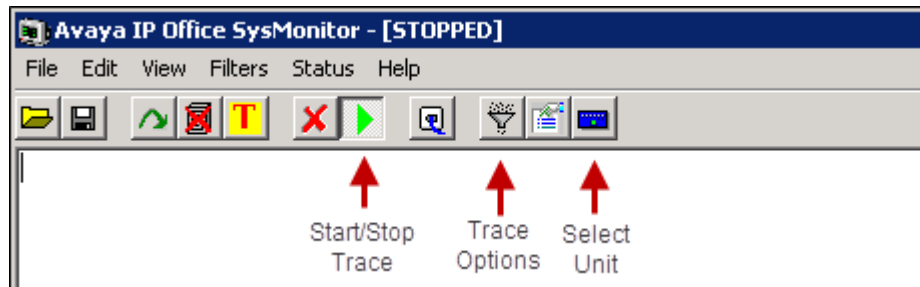
Trace Output:

1/8/15 5:40:14 PM-930ms Line = 1, Channel = 1, Line Ref = 1048, Q.931 Message = Setup, Call Ref = 11, Direction = From Switch, Calling Party Number = 4006, Called Pa  
 1/8/15 5:40:14 PM-949ms Line = 1, Channel = 1, Q.931 Message = CallProceeding, Call Ref = 11, Direction = To Switch

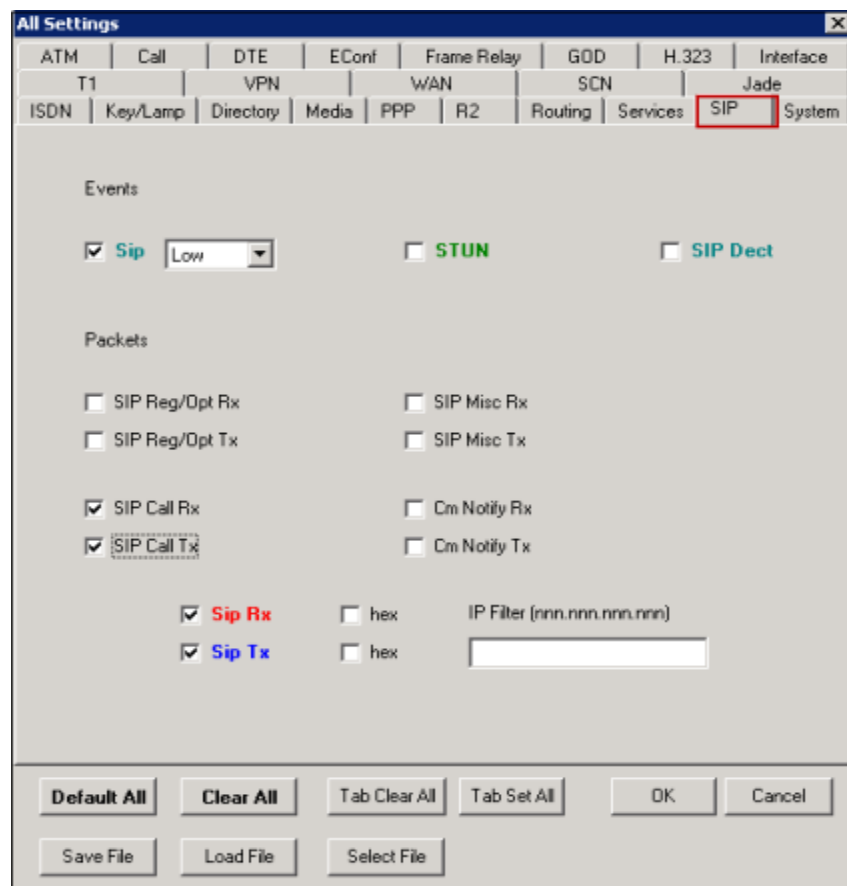
Trace Clear Pause Ping Back Call Details Print... Save As...

### 11.1.2. Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging from the Remote Workers. Launch the application from **Start → Programs → IP Office → Monitor** (not shown) on the PC where Avaya IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



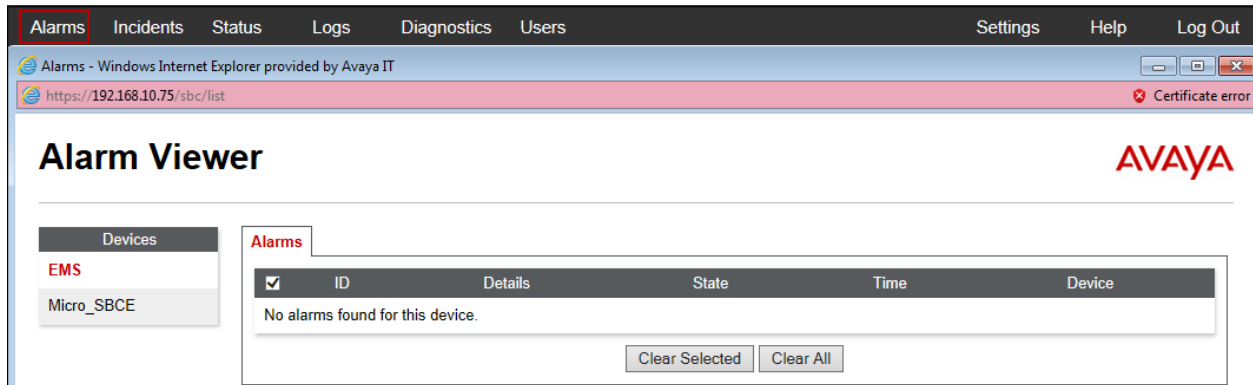
Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows the modification of the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.



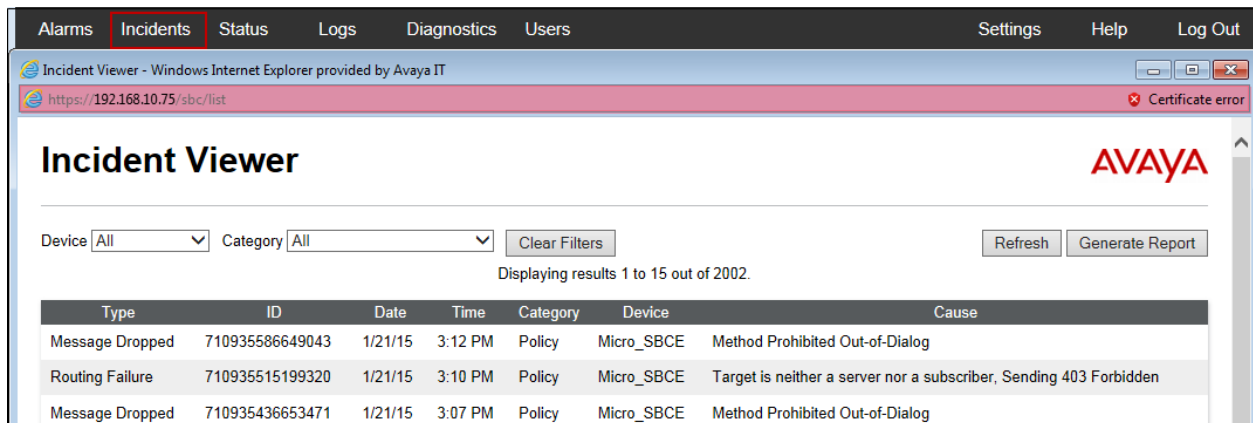
## 11.2. Avaya Session Border Controller for Enterprise

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

**Alarms:** Provides information about the health of the SBC.



**Incidents :** Provides detailed reports of anomalies, errors, policies violations, etc.



Under **Status** → **User Registrations**, a list of users registered via the Avaya SBCE and their current status is shown:

User Registrations - Avaya Session Border Controller for Enterprise - Windows Internet Explorer provided by Avaya IT

https://192.168.10.75/sbc/list

## User Registrations

Displaying entries 1 to 2 of 2.

AOR	SIP Instance	SBC Device	SM Address	Registration State	Last Reported Time	
4006@sil.miami.avaya.com	00ffa8d12f	Micro_SBCE	10.5.5.90 (PRIMARY)	REGISTERED	01/21/2015 15:25:17 EST	<a href="#">Details</a>
4010@sil.miami.avaya.com		Micro_SBCE	10.5.5.90 (PRIMARY)	REGISTERED	01/21/2015 14:25:24 EST	<a href="#">Details</a>

Additional information can be obtained clicking the **Details** link for a particular user:

View Registration Information : 4010@sil.miami.avaya.com

### User Information

AOR	4010@sil.miami.avaya.com
Controller Mode	No
Firmware	Avaya

### SIP Instance

User Agent	Avaya One X Mobile Android Generic 1.9.0.9989 motorola XT1028
------------	---

### Servers

SBC Device	Subscriber Flow	Server Flow	SM Address	SM Port	SM Transport	Endpoint Private IP	Endpoint Natted IP	Endpoint Transport	Registration State	Last Reported Time
Micro_SBCE	one X Mobile	IPO Serv from RW	10.5.5.90 (PRIMARY)	5060	TCP	10.0.0.6	172.16.157.150	TLS	REGISTERED	01/21/2015 14:25:24 EST



Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot shows the Avaya SBCE web interface. The left sidebar contains a navigation menu with options like TLS Management, Device Specific Settings, Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, Troubleshooting, Debugging, **Trace**, and DoS. The main content area is titled "Trace: Micro\_SBCE" and has three tabs: "Call Trace", "Packet Capture" (which is active), and "Captures". The "Packet Capture Configuration" section includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (\*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). There are "Start Capture" and "Clear" buttons at the bottom right of the configuration section.

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

The screenshot shows the "Captures" tab in the Avaya SBCE web interface. It features a "Refresh" button and a table with the following data:

File Name	File Size (bytes)	Last Modified	
<a href="#">test_20141201103347.pcap</a>	118,784	December 1, 2014 10:34:07 AM EST	<a href="#">Delete</a>

## 12. Conclusion

These Application Notes describe the procedures necessary to configure Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers, in the reference configuration shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2**.

## 13. Additional References

- [1] *Deploying IP Office Server Edition Solution*, Document 15-604134, November 2014  
<https://downloads.avaya.com/css/P8/documents/100175282>
- [2] *Avaya IP Office Manager Release 9.0.3*, Document 15-601011, May 2014  
<https://downloads.avaya.com/css/P8/documents/100174478>
- [3] *IP Office 9.0 Using System Status*, Document 15-601758, August 2013  
<https://downloads.avaya.com/css/P8/documents/100173994>
- [4] *Implementing one-X Portal for IP Office*, Document 15-601140, November 2014  
<https://downloads.avaya.com/css/P8/documents/100181228>
- [5] *Avaya IP Office 9.0.3. Administering one-X Portal for IP Office*, Document 15-601139, October 2014. <https://downloads.avaya.com/css/P8/documents/100175204>
- [6] *Administering Avaya one-X® Mobile for IP Office*, Release 9.0.3, May 2014.  
<https://downloads.avaya.com/css/P8/documents/100175092>
- [7] *Using Avaya one-X® Mobile Preferred for IP Office on Apple*, Release 9.0.3, May 2014  
<https://downloads.avaya.com/css/P8/documents/100175121>
- [8] *Using Avaya one-X® Mobile Preferred for IP Office on Android*, Release 9.0.3, May 2014  
<https://downloads.avaya.com/css/P8/documents/100175108>
- [9] *Avaya IP Office Knowledgebase*  
<http://marketingtools.avaya.com/knowledgebase>
- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, October 2014  
<https://downloads.avaya.com/css/P8/documents/101001325>

---

**©2015 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 Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)