Avaya Solution & Interoperability Test Lab

Application Notes for Mutare Voice Spam Filter with Avaya IP Office Server Edition and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Mutare Voice Spam Filter to interoperate with Avaya IP Office Server Edition and Avaya Session Border Controller for Enterprise. Mutare Voice Spam Filter is a call filtering solution.

In the compliance testing, Mutare Voice Spam Filter used SIP trunk with Avaya IP Office Server Edition and Avaya Session Border Controller for Enterprise to support spam call filtering.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required for Mutare Voice Spam Filter to interoperate with Avaya IP Office Server Edition and Avaya Session Border Controller for Enterprise (SBCE). Voice Spam Filter is a call filtering solution.

In the compliance testing, Voice Spam Filter used SIP trunk with IP Office Server Edition and SBCE to support spam call filtering. The IP Office Server Edition configuration consisted of two IP Office systems, a primary Linux server and an expansion IP500V2 that were connected via Small Community Network (SCN) trunk.

Voice Spam Filter can be deployed as a standalone solution or as a feature of the Mutare Voice solution. The compliance testing focused on Voice Spam Filter as a standalone call filtering solution.

Incoming calls to the Avaya SIP-enabled network are delivered by SBCE via SIP trunk to Voice Spam Filter for spam call filtering. Voice Spam Filter examines the SIP call signaling information to identify the caller ID, and checks the caller ID against enterprise whitelist, enterprise blacklist, as well as dynamic robocall list hosted on the Mutare external database in the cloud. Non-spam calls are released by Voice Spam Filter to IP Office, and spam calls can be configured to be dropped or redirected to resource destinations on IP Office. Released and redirected calls are accomplished by modifying the SIP INVITE request line and sent to IP Office as the next hop.

The Voice Spam Filter solution consisted of a Voice Screening Proxy server and a Voice Application Server. The Voice Screening Proxy was the server that interfaced with IP Office and SBCE via SIP trunk. The Voice Application Server checked the caller ID against the local enterprise whitelist and blacklist and interfaced with the Mutare cloud for check of caller ID against the dynamic robocall list on the external database.

The SIP trunks connection with IP Office can be with either the primary Linux server or the expansion IP500V2 system. The configuration shown in these Application Notes used the primary Linux server IP Office system for SIP trunk connectivity.

©2019 Avaya Inc. All Rights Reserved.

2. General Test Approach and Test Results

The feature test cases were performed manually. Inbound calls were made from different PSTN calling numbers that match to the enterprise whitelist, enterprise blacklist, dynamic robocall list on external database, along with different settings for spam call handling.

The serviceability test cases were performed manually such as disconnecting/reconnecting the Ethernet connection to Voice Spam Filter.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

For the testing associated with this Application Note, the interface between Avaya systems and Voice Spam Filter did not include use of any specific encryption features as requested by Mutare.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Voice Spam Filter:

- Proper handling of SIP exchanges including OPTIONS, G.711MU, G.729, codec negotiation, media shuffling, and session refresh.

- Proper handling of call scenarios including release, redirect, blacklist, whitelist, robocall list, not on any list, hold/resume, forwarding, transfer, conference, abandon, invalid number, do not disturb, busy, simultaneous calls, and across SCN scenarios.

The serviceability testing focused on verifying the ability of Voice Spam Filter to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Voice Screening Proxy, and of SBCE to activate alternate route to IP Office when Voice Screening Proxy did not respond within the specified interval.

©2019 Avaya Inc. All Rights Reserved.

2.2. Test Results

All test cases were executed, and the following were observations on Voice Spam Filter:

- By design, only SIP signaling packets flow through Voice Spam Filter and not RTP packets.

- By design, the first call for the day or the call after Voice Application Server has been idling for a while can take longer for Voice Spam Filter to process. In the compliance testing, the experienced delay was ~10 seconds from the time Voice Spam Filter received the INVITE to the time the message was released to IP Office.

- An updated opensips.cfg script dated 8/22/2019 is needed to replace the default version that came with Voice Screening Proxy version 2.4.5. The updated script included fixes for redirected calls and for Voice Screening Proxy to stay in the record route until end of call.

- For a call scenario where the SIP Service Provider sent a session interval deemed insufficient by IP Office with a 422 Session Interval Too Small being exchanged and therefore a subsequent re-INVITE, Voice Spam Filter reported two history entries for the scenario. This can be managed by ensuring the SIP Service Provider is not sending session intervals that are too small as part of initial planning.

2.3. Support

Technical support on Voice Spam Filter can be obtained through the following:

- **Phone:** +1 (855) 782-3890
- **Email:** help@mutare.com
- **Web :** http://www.mutare.com/support.asp

©2019 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The detailed administration of basic connectivity between IP Office and SBCE are not the focus of these Application Notes and will not be described.

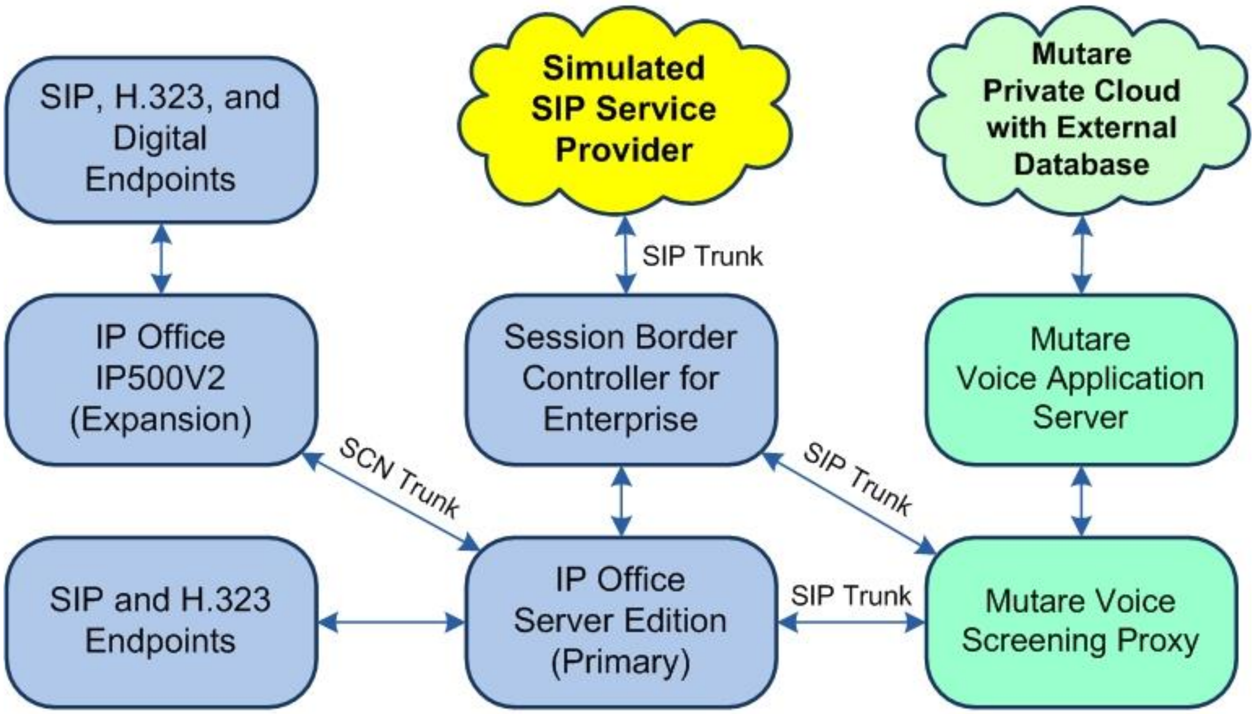


Figure 1: Compliance Testing Configuration

©2019 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition (Primary) in Virtual Environment	11.0.4.1.0
Avaya IP Office on IP500V2 (Expansion)	11.0.4.1.0
Avaya Session Border Controller for Enterprise in Virtual Environment	8.0 (8.0.0.0-19-16991)
Avaya 1120E IP Deskphone (SIP)	4.4.23.0
Avaya J129 IP Deskphone (SIP)	4.0.0.0.21
Avaya 1616-I IP Deskphone (H.323)	1.3120
Avaya 9611G IP Deskphone (H.323)	6.8202
Mutare Voice Screening Proxy on CentOS • opensips.cfg	2.4.5 7 8/22/2019
Mutare Voice Application Server on Windows Server 2016	1.9.0.0 Standard

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

©2019 Avaya Inc. All Rights Reserved.

5. Configure Avaya IP Office

This section provides the procedures for configuring the IP Office systems. The procedures include the following area:

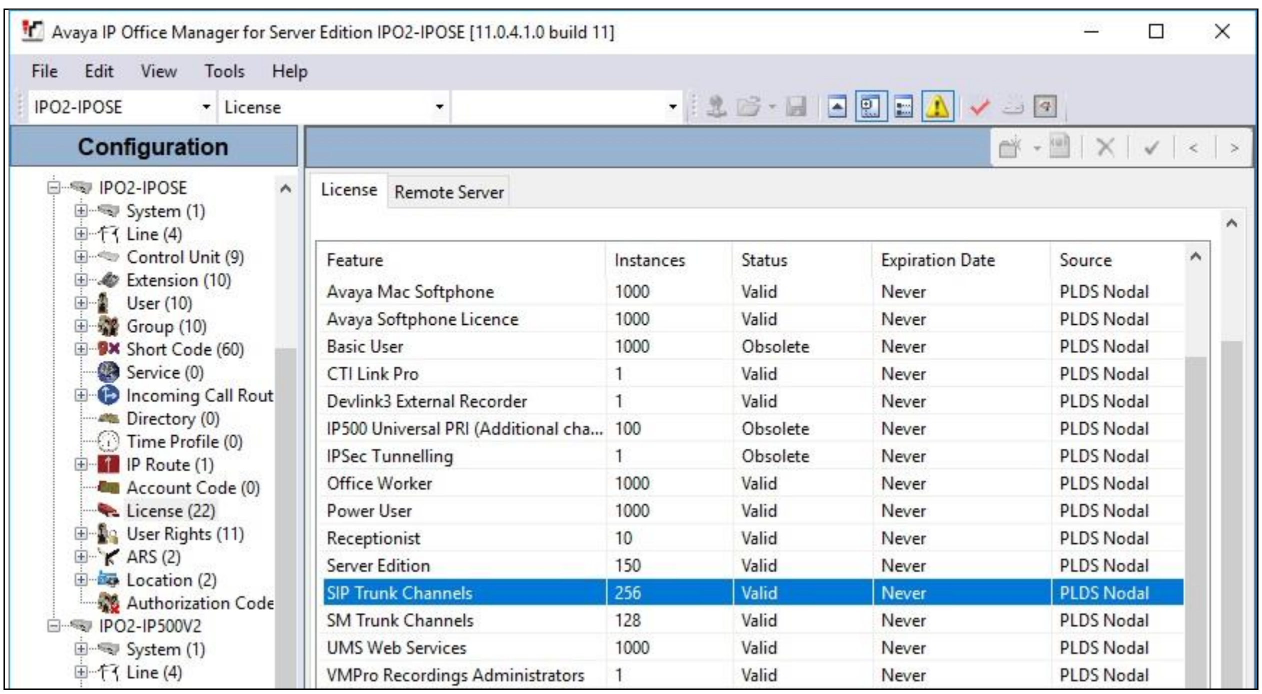
- Verify license
- Administer system
- Administer line
- Administer incoming call route

5.1. Verify License

From a PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Select the proper primary IP Office system, and log in using the appropriate credentials.

The **Avaya IP Office Manager for Server Edition IPO2-IPOSE** screen is displayed, where **IPO2-IPOSE** is the name of the primary IP Office system.

From the configuration tree in the left pane, select **License** under the IP Office system that will be used for SIP trunk connection with Voice Spam Filter, in this case "IPO2-IPOSE", and a list of licenses is displayed in the right pane. Verify that there is a license for **SIP Trunk Channels** and that the **Status** is "Valid", as shown below.

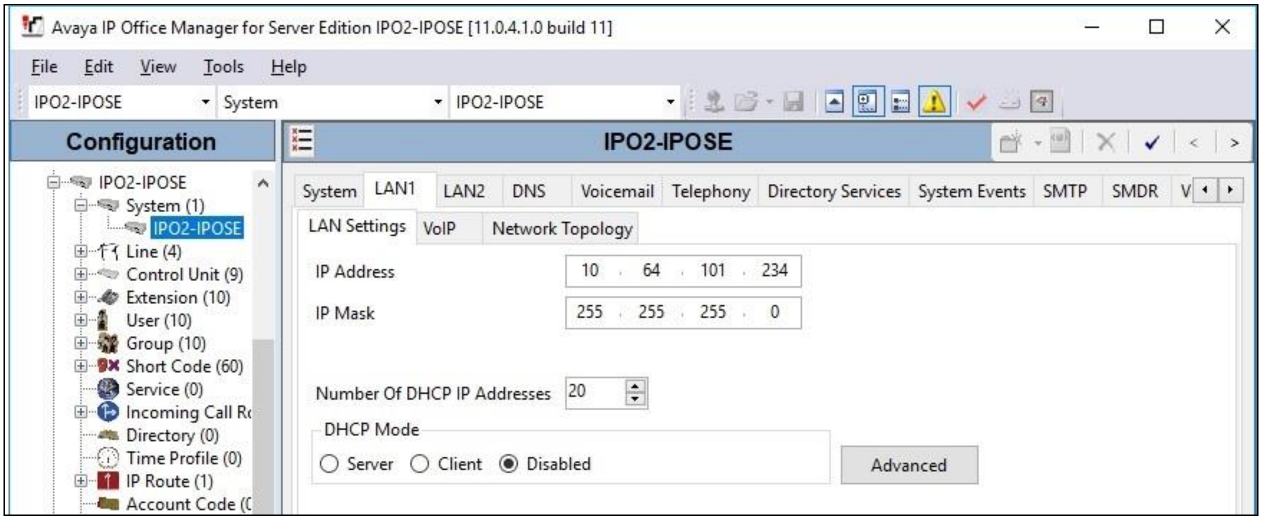


©2019 Avaya Inc. All Rights Reserved.

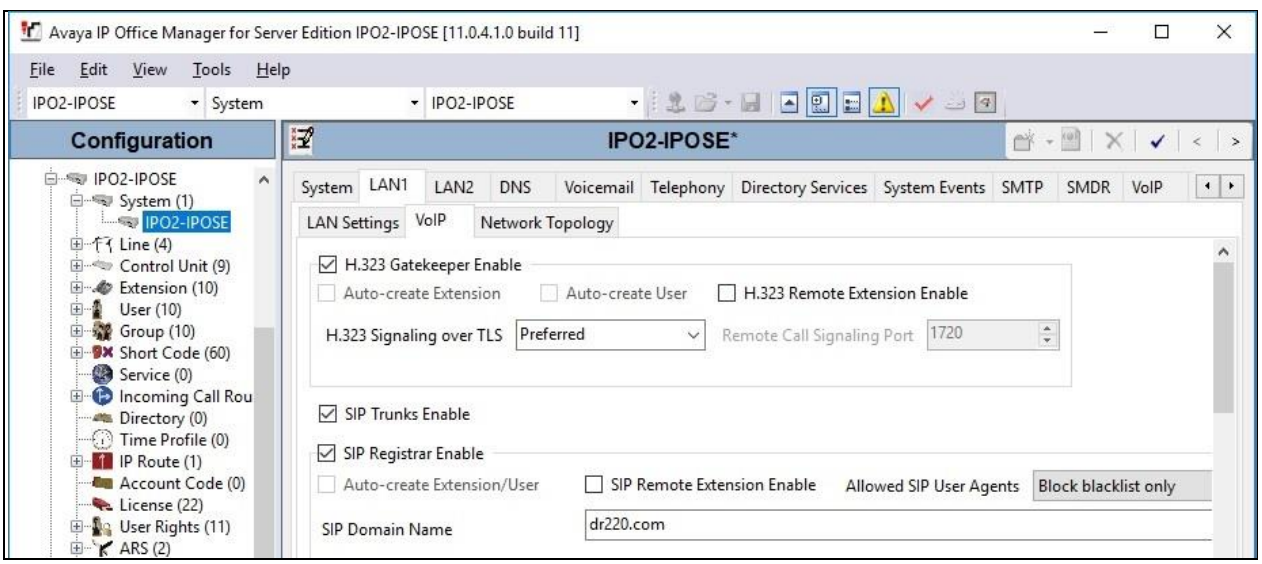
5.2. Administer System

From the configuration tree in the left pane, select **System** under the IP Office system used for SIP trunk connection with Voice Spam Filter, to display the system screen in the right pane.

Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right pane. Make a note of the **IP Address**, which will be used later to configure Voice Spam Filter. Note that IP Office can support SIP trunk on the LAN1 and/or LAN2 interfaces, and the compliance testing used the LAN1 interface.



Select the **VoIP** sub-tab. Make certain that **SIP Trunks Enable** is checked, as shown below. Retain the default values in the remaining fields.

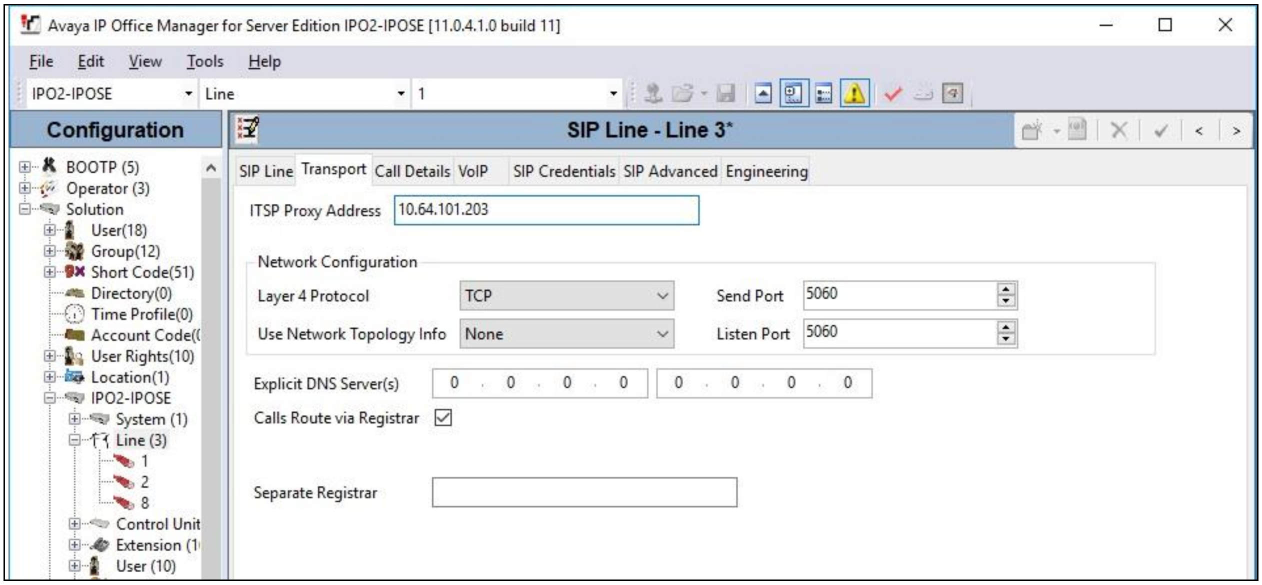


©2019 Avaya Inc. All Rights Reserved.

5.3. Administer Line

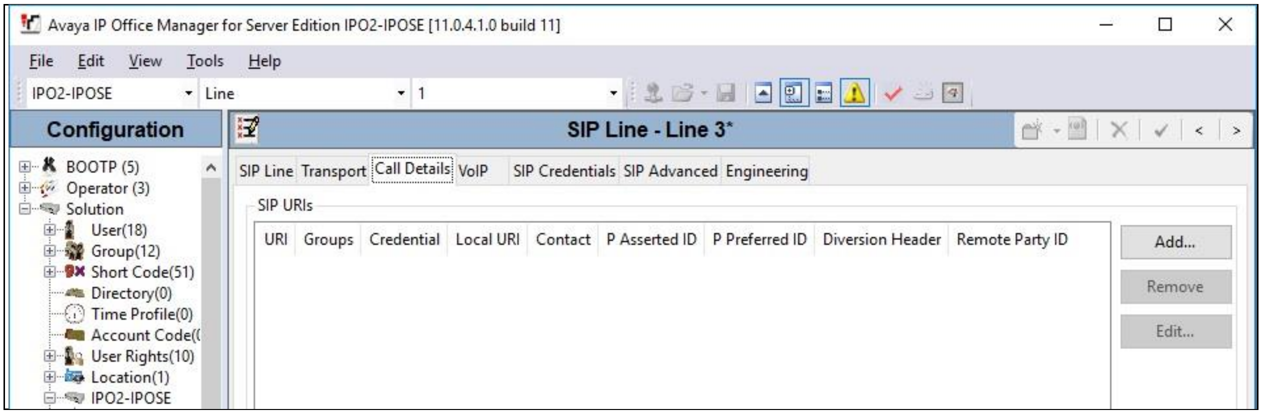
From the configuration tree in the left pane, right-click on **Line** under the IP Office system used for SIP trunk connection with Voice Spam Filter and select **New → SIP Line** from the pop-up list to add a new SIP line.

Select the **Transport** tab. For **ITSP Proxy Address**, enter the IP address of the Voice Screening Proxy server. Retain the defaults in the remaining fields. Note that Voice Spam Filter can support UDP and TCP, and the compliance testing used the TCP protocol.



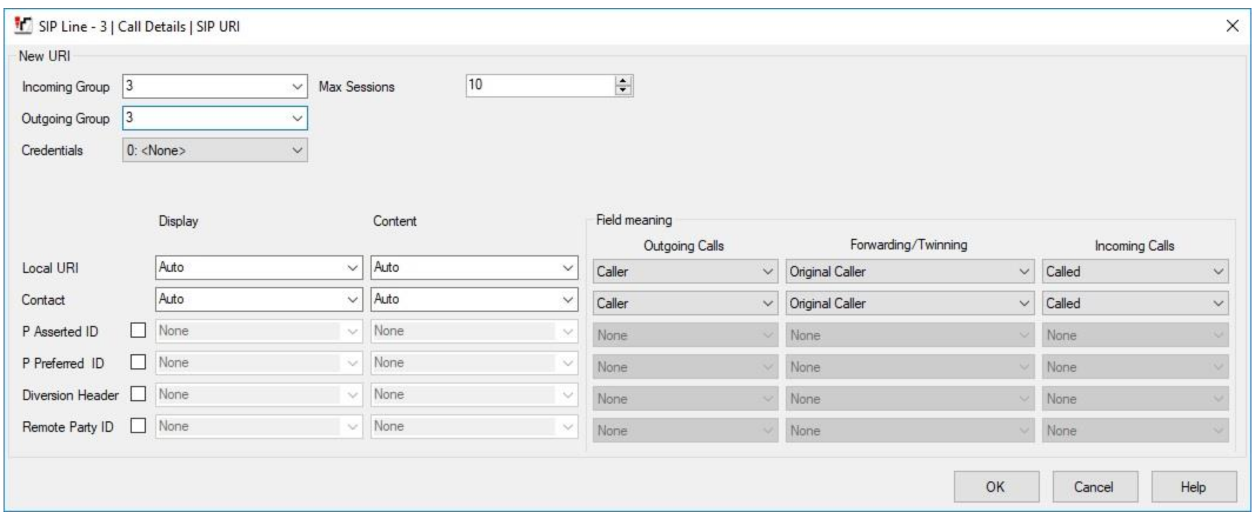
©2019 Avaya Inc. All Rights Reserved.

Select the **Call Details** tab, followed by **Add** in the **SIP URIs** sub-section.



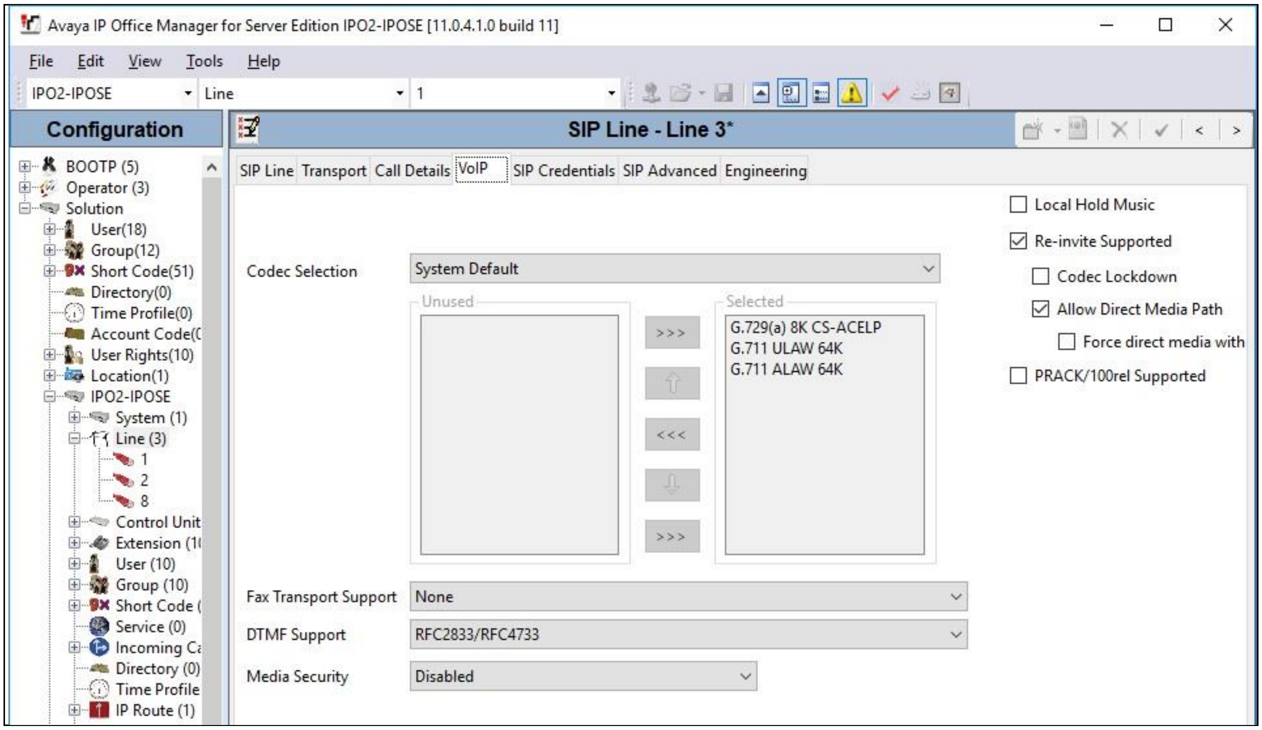
The screen below is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Incoming Group:** An available incoming group number.
- **Outgoing Group:** An available outgoing group number.
- **Max Sessions:** The maximum number of simultaneous calls.



©2019 Avaya Inc. All Rights Reserved.

Select the **VoIP** tab. Check **Re-invite Supported** and **Allow Direct Media Path**. Retain the default values in the remaining fields.

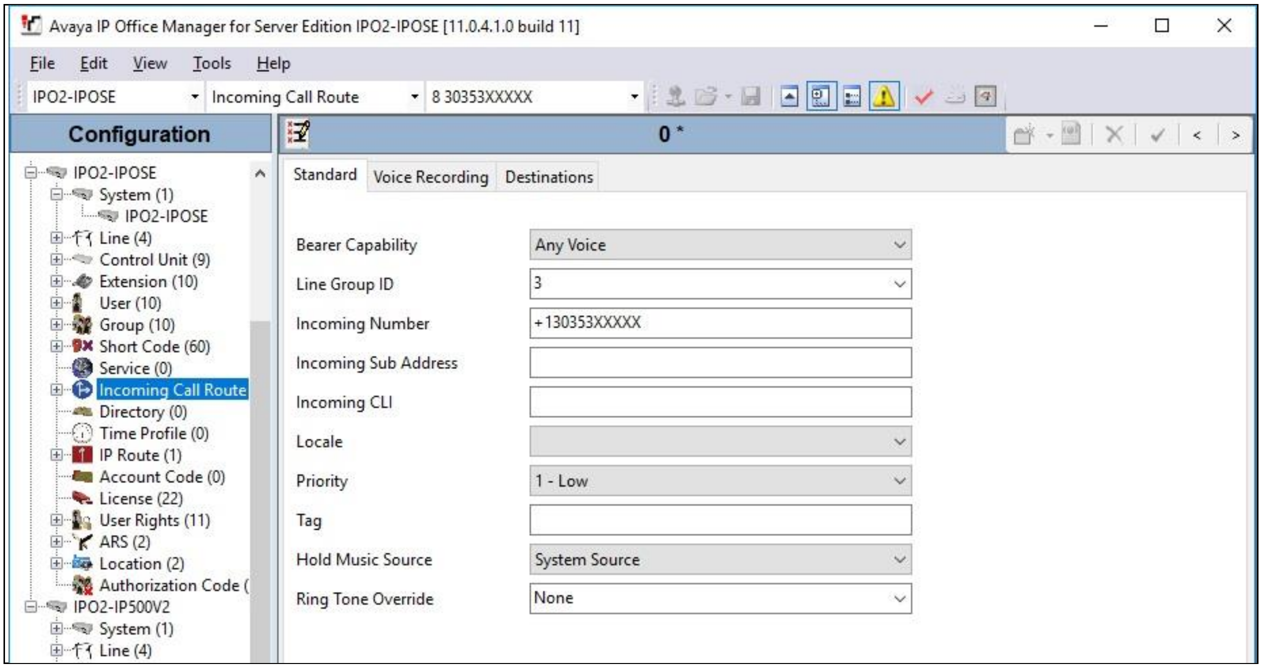


©2019 Avaya Inc. All Rights Reserved.

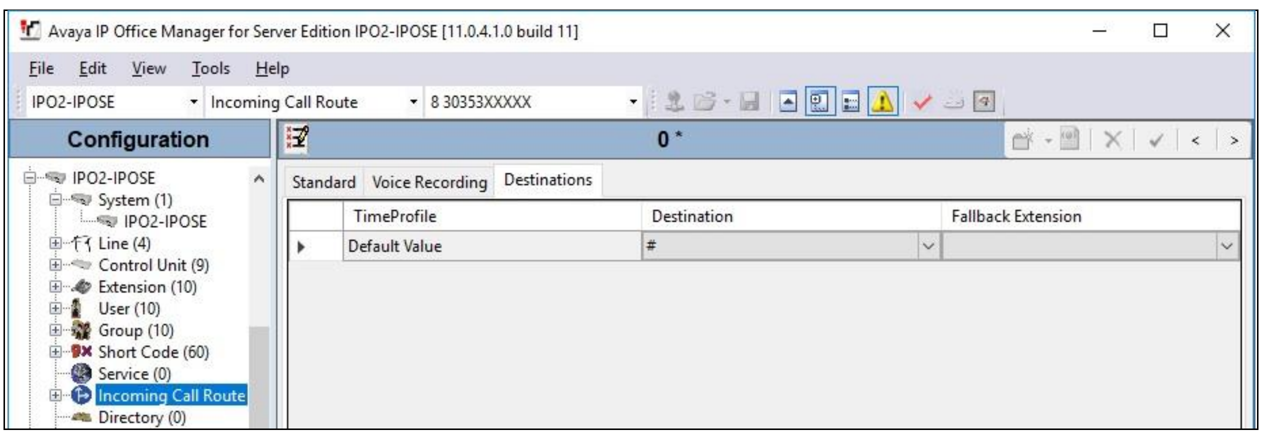
5.4. Administer Incoming Call Route

From the configuration tree in the left pane, right-click on **Incoming Call Route** under the IP Office system used for SIP trunk connection with Voice Spam Filter and select **New** from the pop-up list to add a new route for incoming calls from Voice Spam Filter.

For **Line Group ID**, select the incoming group number from **Section 5.3**, in this case "3". For **Incoming Number**, enter the pertinent E.164 pattern to match with, in this case "+130353XXXXX". Retain the default value in the remaining fields.



Select the **Destinations** tab. For **Destination**, enter "#" to match all "X" wildcards in the incoming number field from above.



©2019 Avaya Inc. All Rights Reserved.

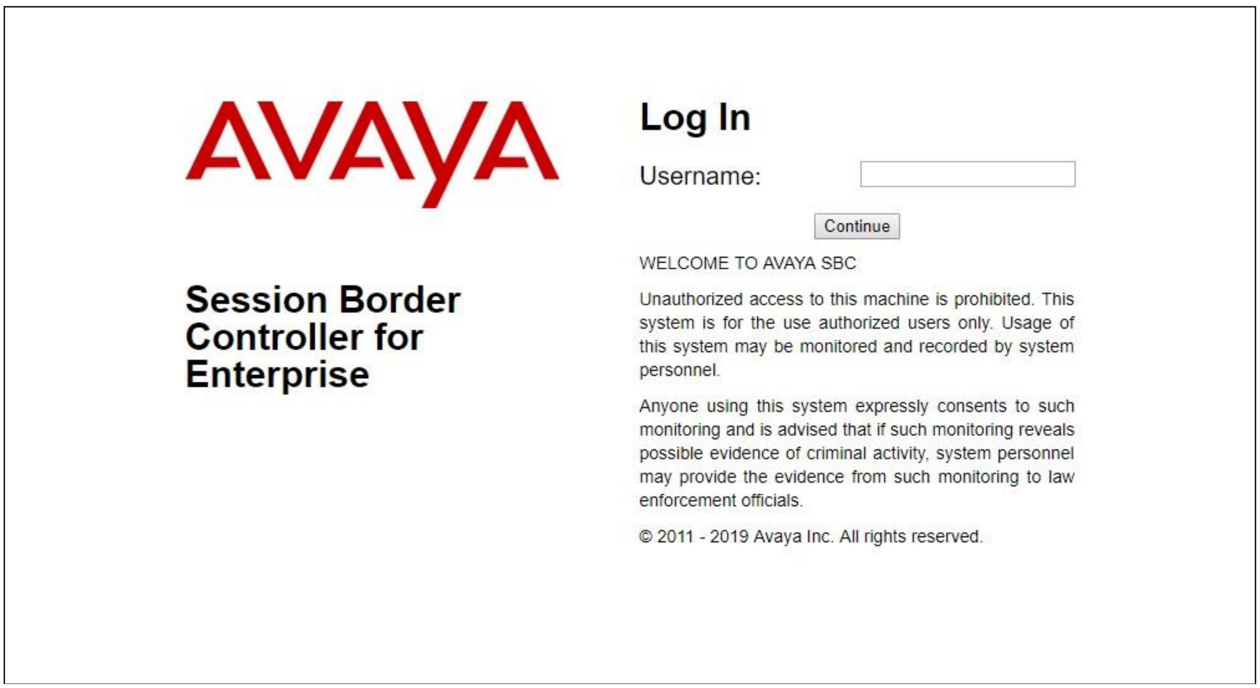
6. Configure Avaya Session Border Controller for Enterprise

This section provides the procedures for configuring SBCE. The procedures include the following areas:

- Launch web interface
- Administer SIP server profile
- Administer routing profile
- Administer interworking profile

6.1. Launch Web Interface

Access the SBCE web interface by using the URL "https://ip-address/sbc" in an Internet browser window, where "ip-address" is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.

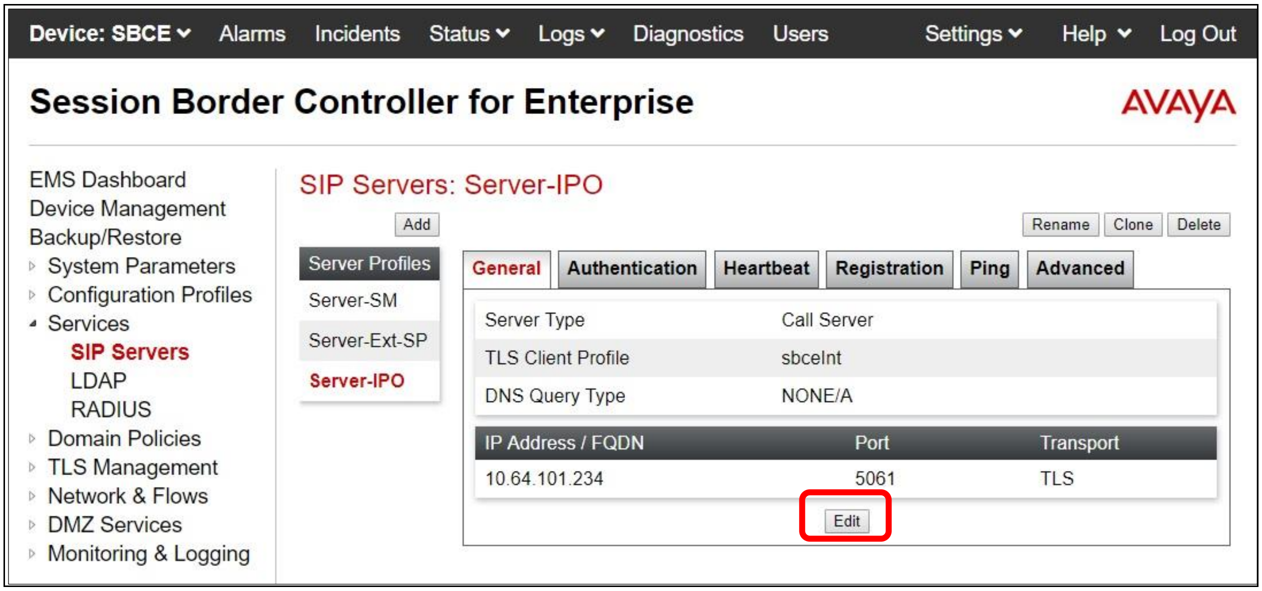


©2019 Avaya Inc. All Rights Reserved.

6.2. Administer SIP Server Profile

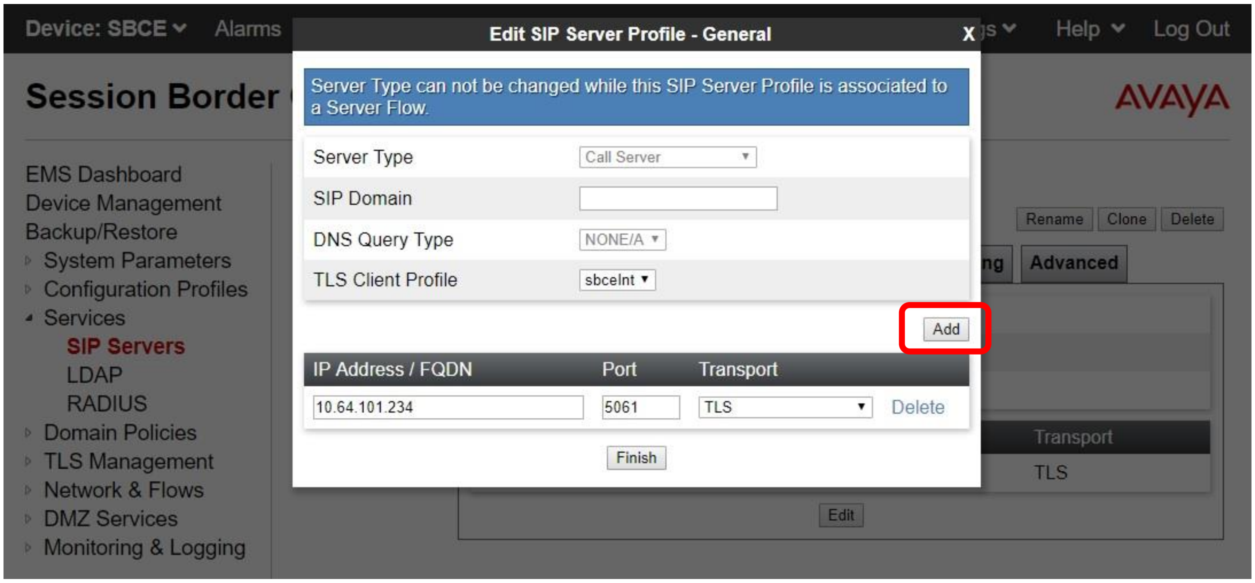
In the subsequent screen, select **Device → SBCE** from the left top menu, followed by **Backup/Restore → Services → SIP Servers** from the left pane to display the existing SIP server profiles.

Select the SIP server profile associated with IP Office, in this case "Server-IPO" as shown below. Click **Edit**.

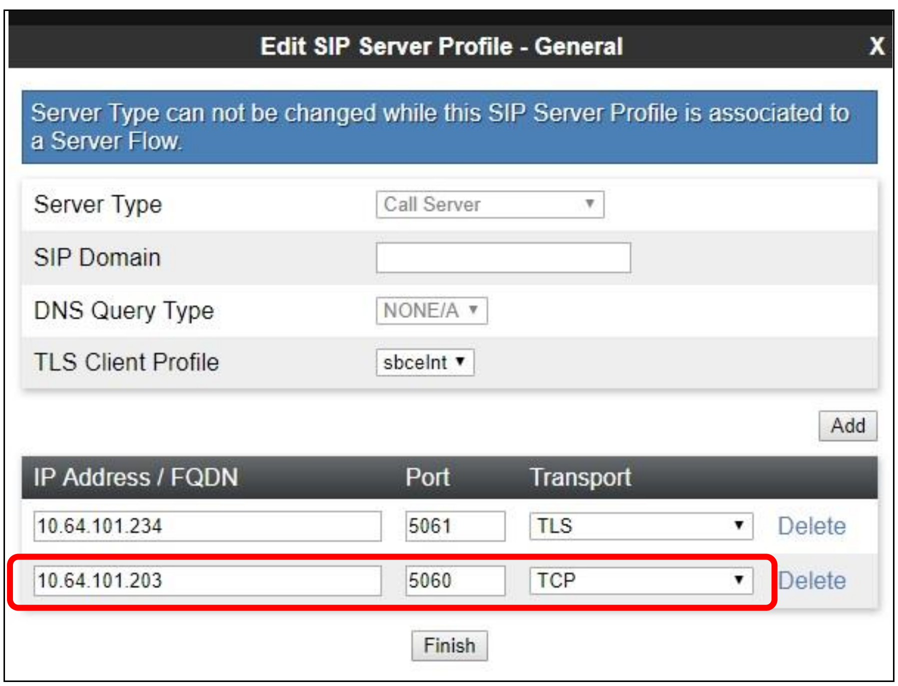


©2019 Avaya Inc. All Rights Reserved.

The **Edit SIP Server Profile – General** pop-up screen is displayed. Click **Add** to add an entry.



In the new entry, enter the IP address of the Voice Screening Proxy server for **IP Address / FQDN**. For **Port** and **Transport**, enter and select the values correspond to the Voice Spam Filter SIP line in **Section 5.3**.



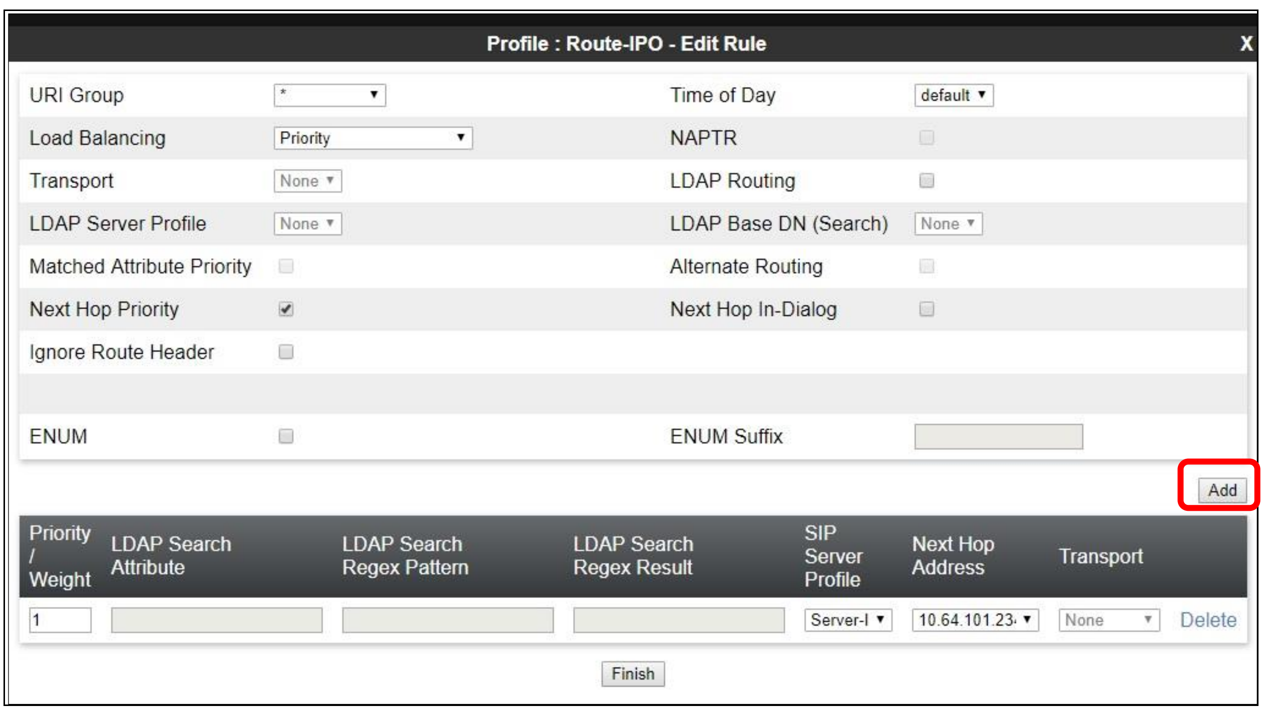
©2019 Avaya Inc. All Rights Reserved.

6.3. Administer Routing Profile

Select **Backup/Restore → Configuration Profiles → Routing** from the left pane to display the existing routing profiles.

Select the routing profile associated with IP Office, in this case "Route-IPO", as shown below. Click **Edit**.

The **Profile : Route-IPO – Edit Rule** pop-up screen is displayed. Click **Add** to add an entry.



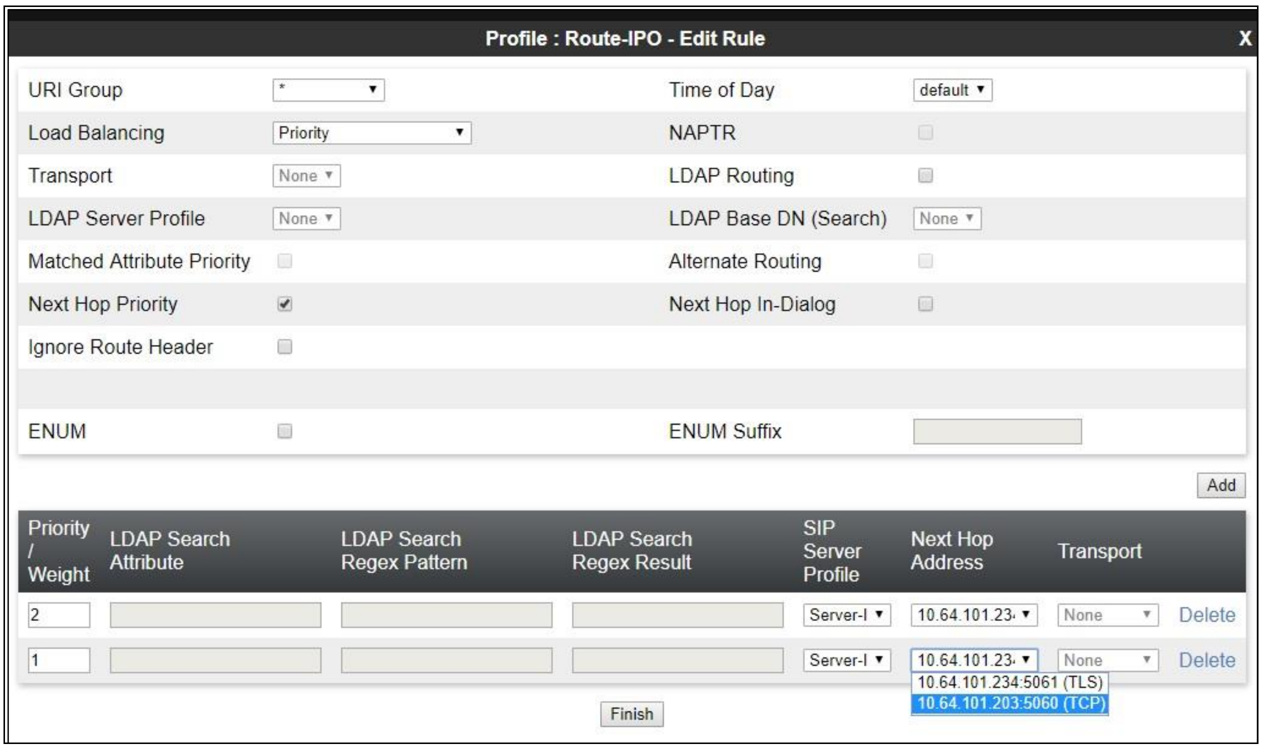
©2019 Avaya Inc. All Rights Reserved.

In the existing entry, update the **Priority / Weight** to a lesser priority, such as "2" as shown below.

In the new entry, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Priority / Weight:** The highest priority of "1".
- **SIP Server Profile:** The SIP server profile for IP Office, in this case "Server-IPO".
- **Next Hop Address:** Select the address entry associated with Voice Screening Proxy.

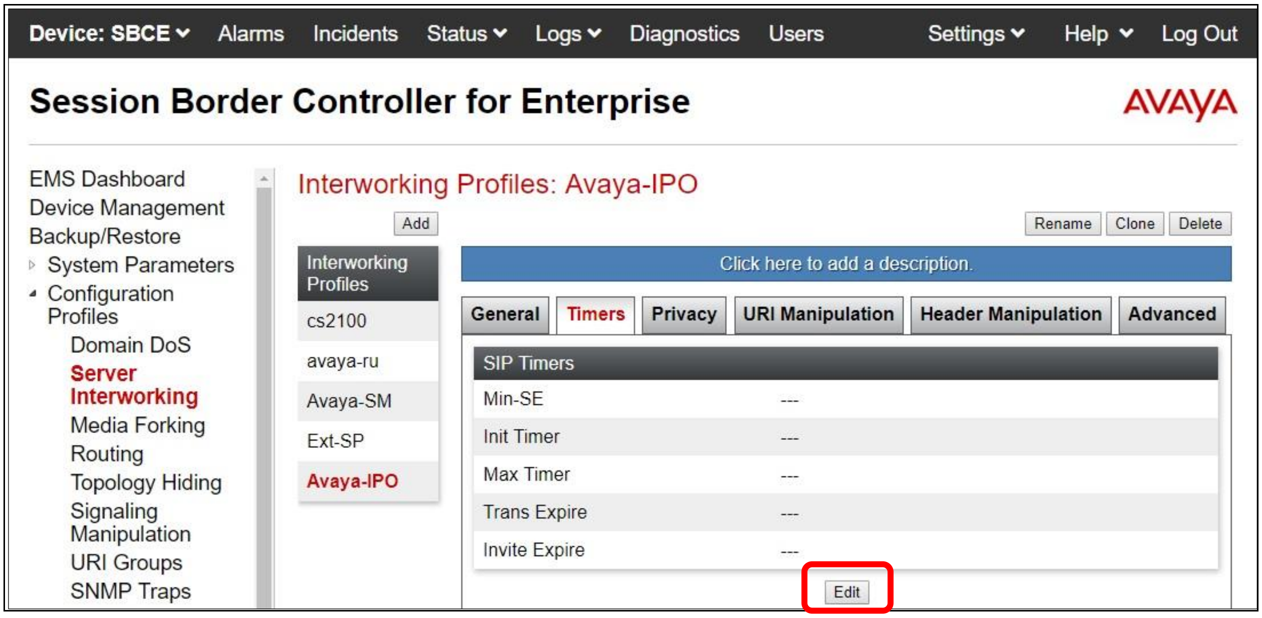
With this routing configuration, inbound calls to be routed from SBCE to IP Office will now route to Voice Screening Proxy as primary and will only route to IP Office as alternate when the Voice Screening Proxy is not available.



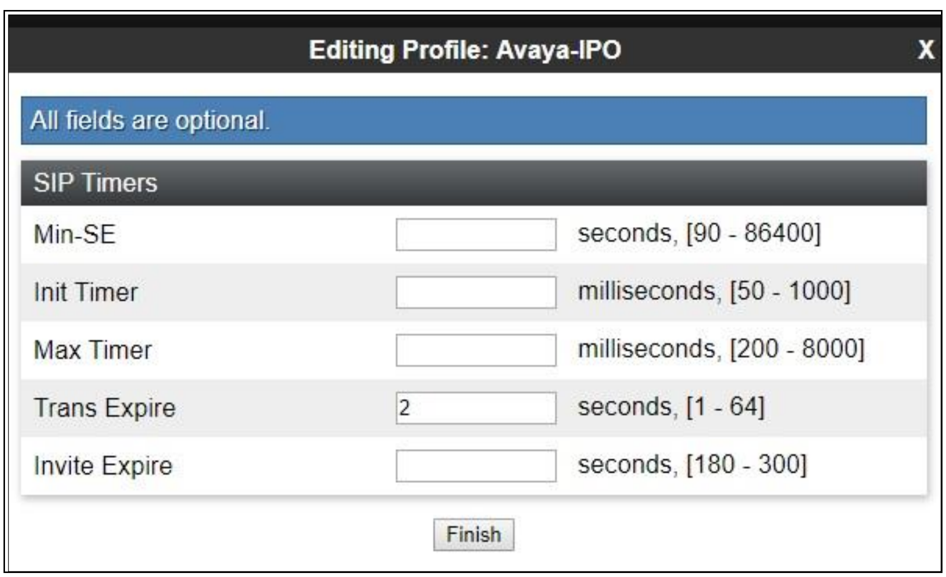
©2019 Avaya Inc. All Rights Reserved.

6.4. Administer Interworking Profile

Select **Backup/Restore → Configuration Profiles → Server Interworking** from the left pane to display the existing interworking profiles. Select the interworking profile associated with IP Office, in this case “Avaya-IPO”, as shown below. Select the **Timers** tab in the right pane and click **Edit**.



The **Editing Profile: Avaya-IPO** pop-up screen is displayed. For **Trans Expire**, enter an appropriate short duration. In the compliance testing, two seconds was used as the allotted time for SBCE to wait for a route response from Voice Screening Proxy as primary before routing to IP Office as alternate.



©2019 Avaya Inc. All Rights Reserved.

7. Configure Mutare Voice Spam Filter

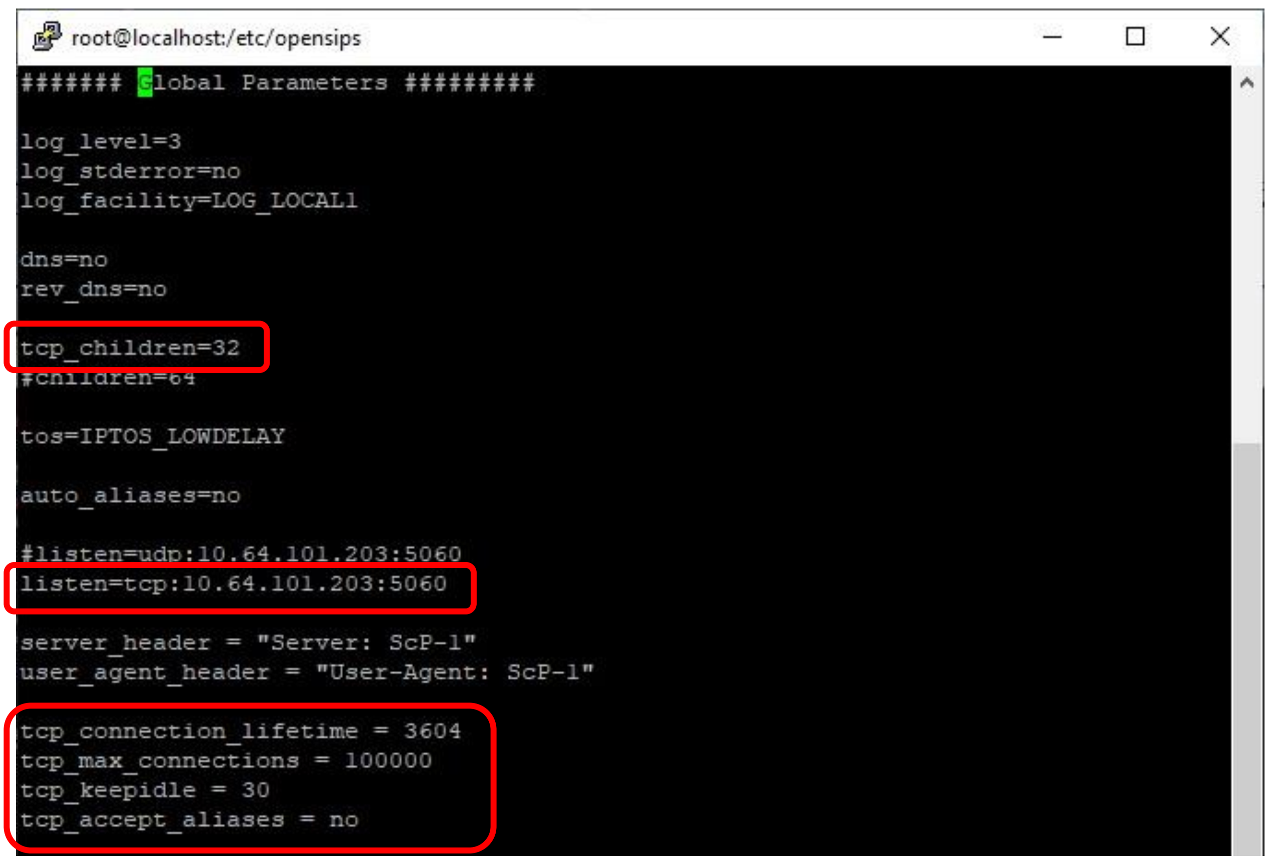
This section provides the procedures for configuring Voice Spam Filter. The procedures include the following areas:

- Administer opensips.cfg
- Administer SQL
- Administer control panel
- Administer rules manager

The configuration of Voice Spam Filter is typically performed by Mutare operations technician. The procedural steps are presented in these Application Notes for information purposes. This section assumes that values for API URL, Connect URL, appliance ID, account ID, and token have all been obtained from Voice Application Server and configured on Voice Screening Proxy.

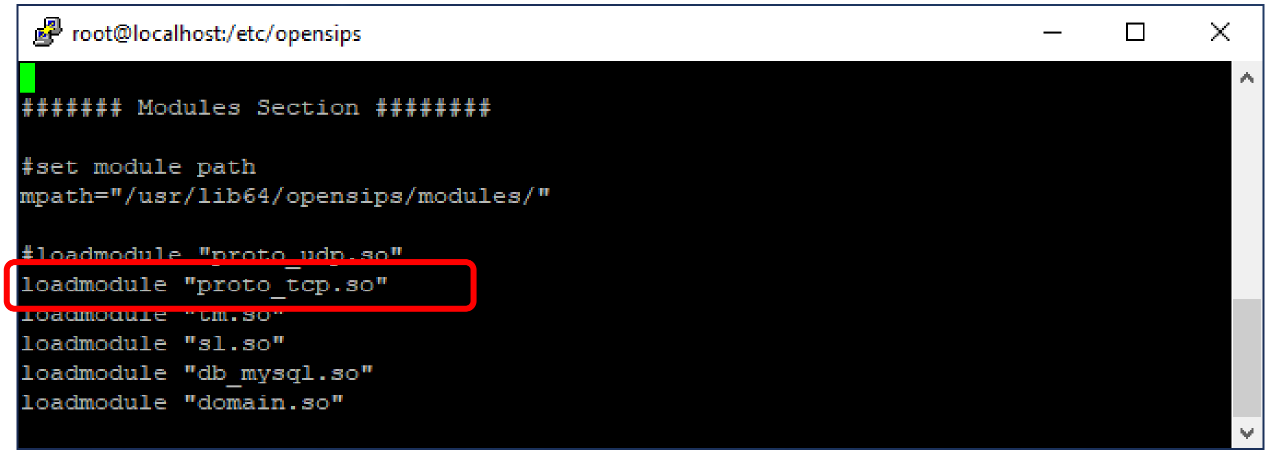
7.1. Administer opensips.cfg

Log in to the Linux shell of the Voice Screening Proxy server with super user credentials. Navigate to the **/etc/opensips** directory and edit the **opensips.cfg** file. Scroll down to the **Global Parameters** sub-section and uncomment out 6 TCP related parameters shown below. For the **listen** parameter, replace the default IP address with the IP address of the Voice Screening Proxy server.

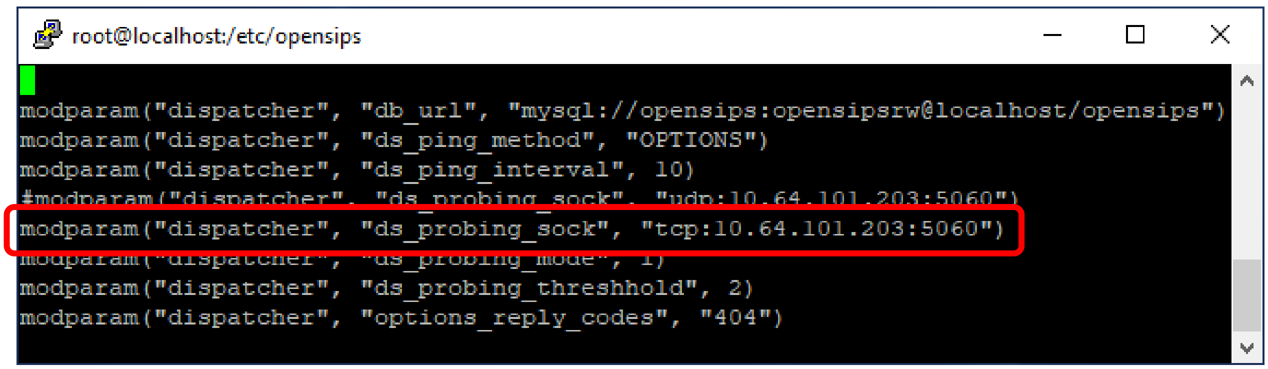


©2019 Avaya Inc. All Rights Reserved.

Scroll down to the **Modules Section** and uncomment out the TCP related module shown below.

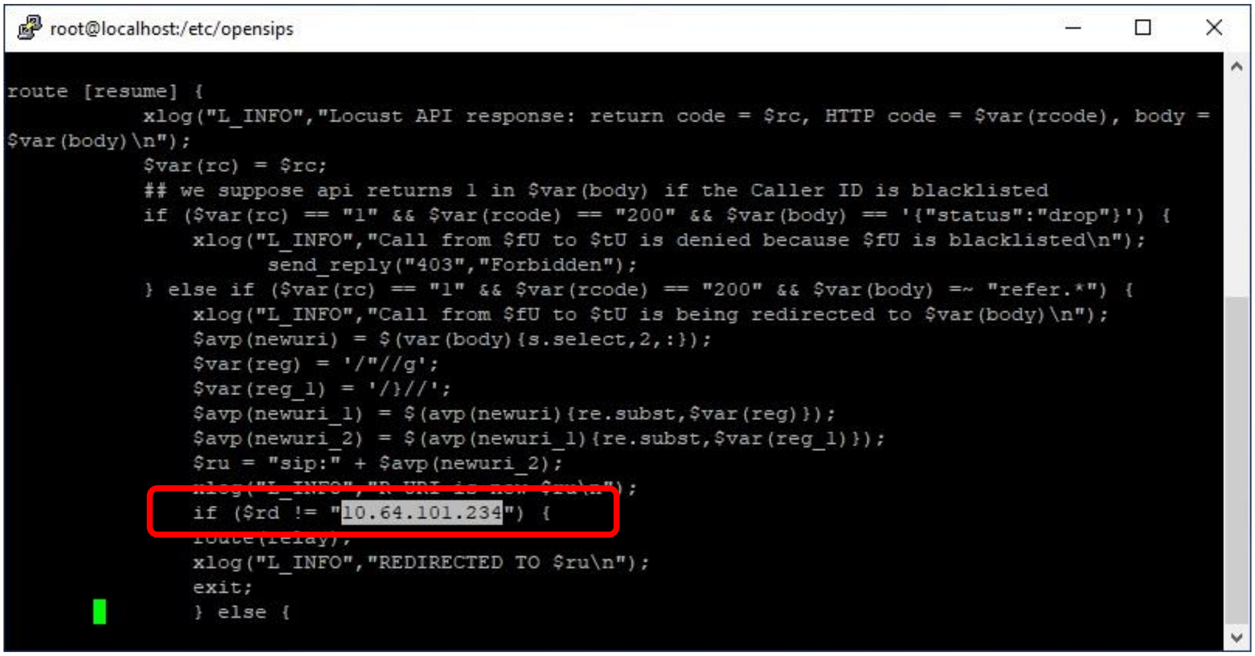


Scroll down to the section shown below, uncomment out the TCP related line and replace the default IP address with the IP address of Voice Screening Proxy as shown below.



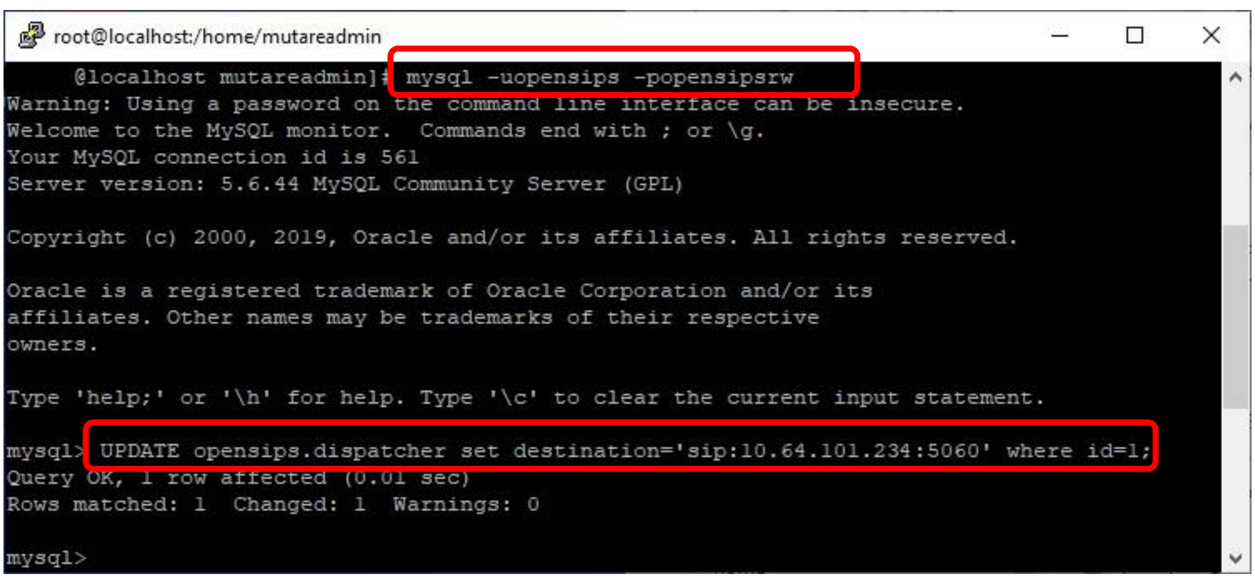
©2019 Avaya Inc. All Rights Reserved.

Scroll down to the **route [resume]** sub-section and replace the default IP address with the pertinent IP Office LAN IP address in the highlighted area shown below. This setting will use IP Office as the next hop.



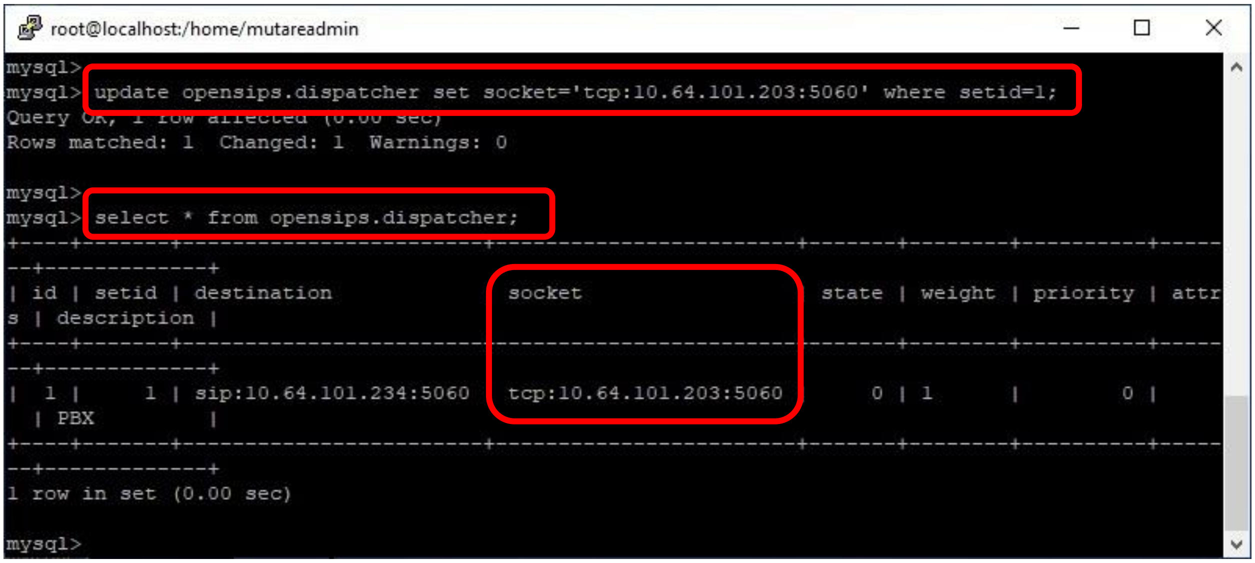
7.2. Administer SQL

From the command line, enter the two SQL commands shown below to update the next hop destination to the IP address of the pertinent IP Office LAN interface.



©2019 Avaya Inc. All Rights Reserved.

From the command line, enter the first SQL command below to set the TCP socket, and the second SQL command below to make certain the TCP socket has been set correctly.

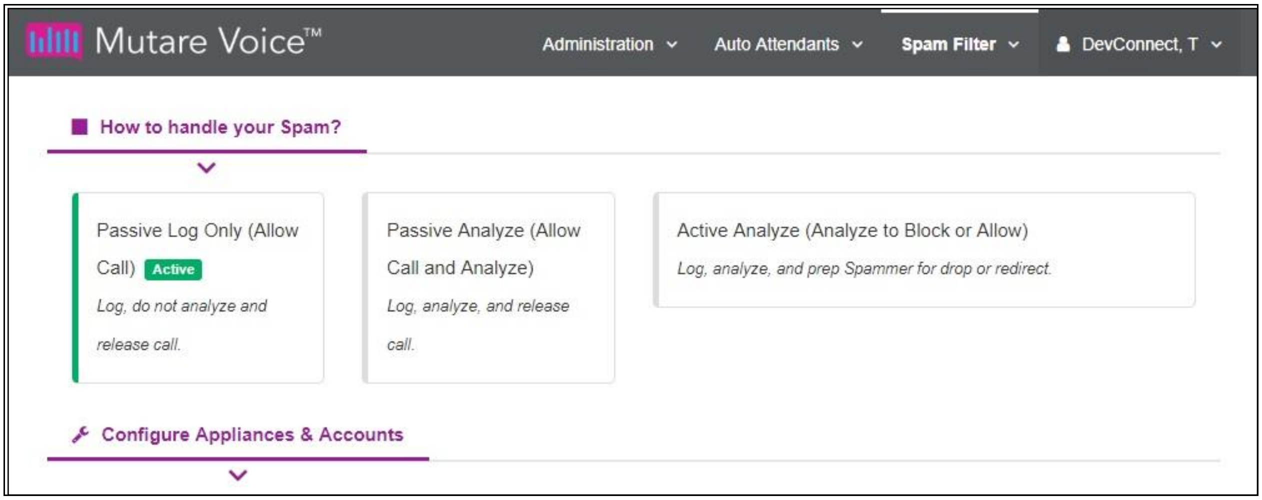


7.3. Administer Control Panel

Access the Voice Spam Filter web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Voice Application Server. The screen below is displayed. Log in using the appropriate credentials.

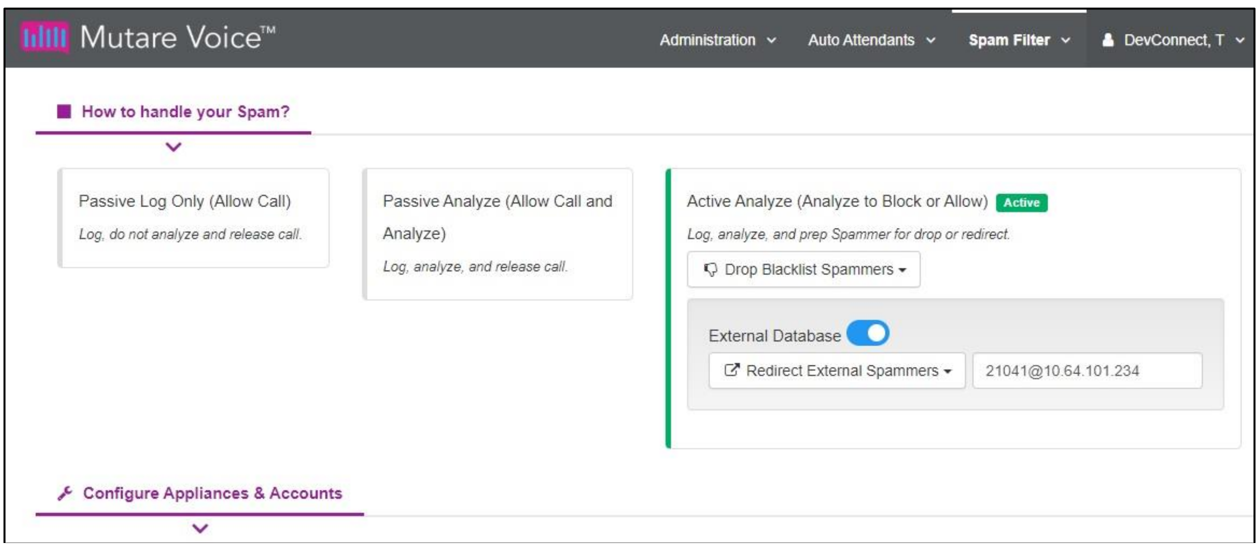
©2019 Avaya Inc. All Rights Reserved.

In the subsequent screen (not shown), select **Spam Filter → Control Panel** from the top menu to display the screen below.



Follow reference [3] to configure the desired action for handling of spam calls. The screenshot below shows a sample configuration with all calls to be analyzed, calls from calling parties on the enterprise blacklist to be dropped, and calls from calling parties on the robocall external database to be redirected.

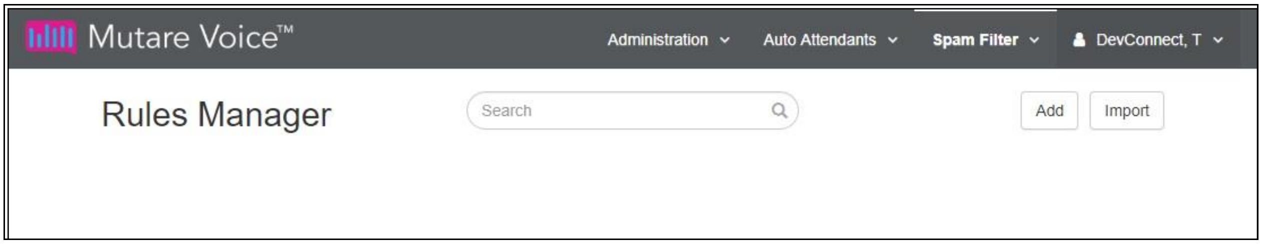
For redirected calls, enter "x@y" as destination where "x" is a desired resource extension and "y" is the IP address of the pertinent IP Office LAN interface. In the compliance testing, "21041" corresponded to a user extension on IP Office.



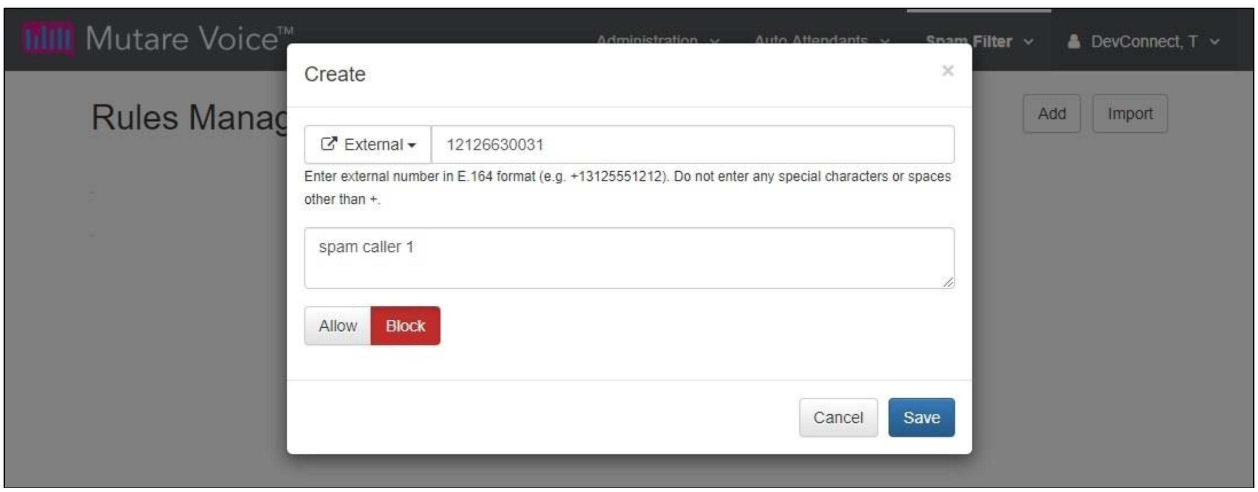
©2019 Avaya Inc. All Rights Reserved.

7.4. Administer Rules Manager

Select **Spam Filter → Rules Manager** from the top menu to display the **Rules Manager** screen below. Click **Import** to import a CSV file with existing numbers or **Add** to add individual numbers. In the compliance testing, **Add** was used.

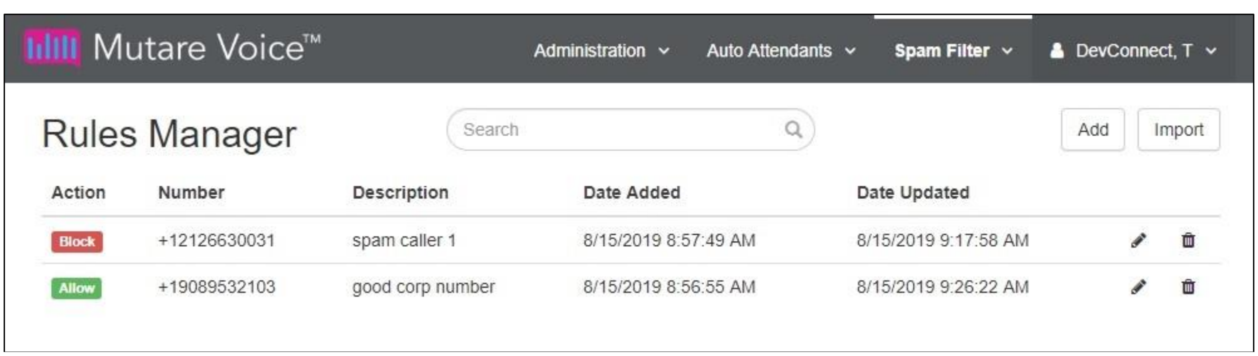


The **Create** pop-up box is displayed next. Enter a ten-digits calling number preceded with "1", a brief description, and select **Allow** for whitelist or **Block** for blacklist.



Repeat the procedures in this section to configure all calling numbers for the enterprise whitelist and blacklist.

In the compliance testing, two entries were created as shown below. Note that Voice Spam Filter automatically converted the numbers into E.164 format by adding the plus sign.



©2019 Avaya Inc. All Rights Reserved.

8. Verification Steps

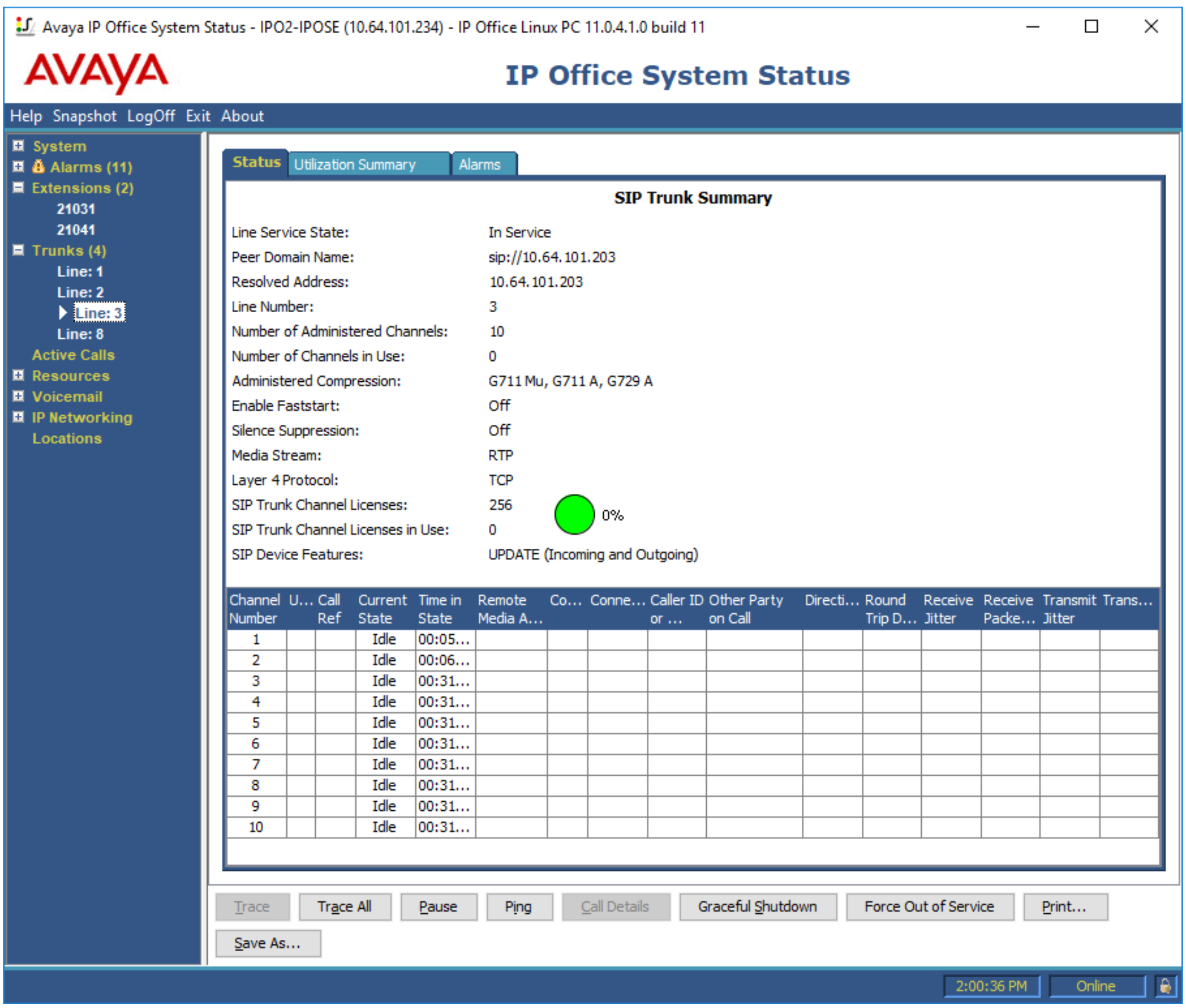
This section provides the tests that can be performed to verify proper configuration of IP Office, SBCE, and Voice Spam Filter.

8.1. Verify Avaya IP Office

From the **Avaya IP Office Manager for Server Edition IPO2-IPOSE** screen shown in **Section 5.1**, select **File → Advanced → System Status** to launch the System Status application, and log in using the appropriate credentials.

The **Avaya IP Office System Status – IPO2-IPOSE** screen is displayed. Expand **Trunks** in the left pane and select the SIP line from **Section 5.3**, in this case "3".

Verify that the **SIP Trunk Summary** screen shows all channels with **Current State** of "Idle", as shown below.

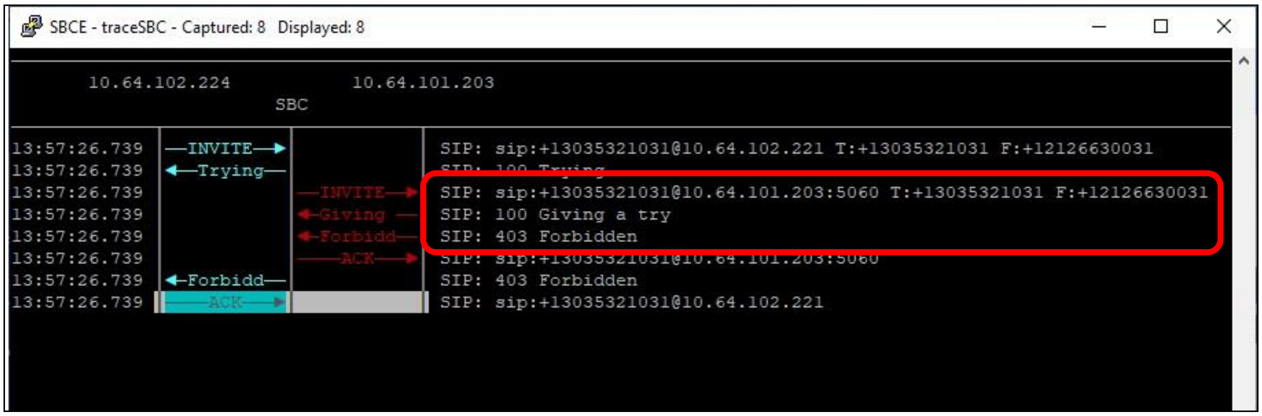


©2019 Avaya Inc. All Rights Reserved.

8.2. Verify Avaya Session Border Controller for Enterprise

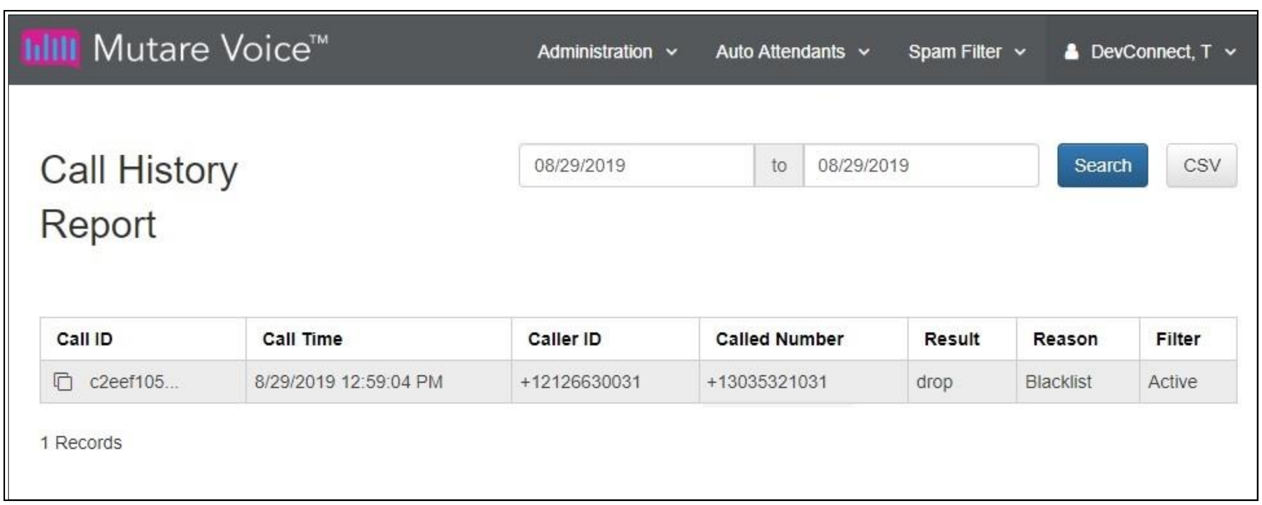
Log in to the Linux shell of the SBCE management interface with appropriate credentials and run the "tracesbc" command.

Make an inbound call from a PSTN caller with calling number on the enterprise blacklist from **Section 7.4**. Verify that the SBCE trace shows a **403 Forbidden** response from Voice Screening Proxy, and that the PSTN caller receives a call rejection treatment from the SIP Service Provider.



8.3. Verify Mutare Voice Spam Filter

From the Voice Spam Filter web interface, select **Spam Filter → Call History** from the top menu. Verify that there is an entry associated with the last call along with appropriate **Result** and **Reason** as shown below.



©2019 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps required for Mutare Voice Spam Filter to successfully interoperate with Avaya IP Office Server Edition and Avaya Session Border Controller for Enterprise. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, February 2019, available at http://support.avaya.com.

2. *Administering Avaya Session Border Controller for Enterprise*, Release 8.0.x, Issue 4, August 2019, available at http://support.avaya.com.

3. *Mutare Voice Admin Guide*, Version 1.9.0, June 26, 2019, available at https://mutare.com/knowledge/tech-docs.

©2019 Avaya Inc. All Rights Reserved.

©2019 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.