



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring TelStrat Engage 5.5 with Avaya IP Office 10.1 Using VoIP Recording – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for TelStrat Engage 5.5 to interoperate with Avaya IP Office 10.1 using VoIP recording. TelStrat Engage is a call recording solution.

In the compliance testing, TelStrat Engage used the TAPI interface from Avaya IP Office to monitor hunt group users on Avaya IP Office, and the port mirroring method to capture media associated with the monitored users for recording.

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.

# 1. Introduction

These Application Notes describe the configuration steps required for TelStrat Engage 5.5 to interoperate with Avaya IP Office 10.1 using VoIP recording. TelStrat Engage is a call recording solution.

In the compliance testing, TelStrat Engage used TAPI 2 in third party mode from Avaya IP Office to monitor hunt group users on Avaya IP Office. The port mirroring method was used to capture media from the Avaya IP Deskphones that were associated with the monitored users for call recordings.

# 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application established TAPI connectivity to IP Office for monitoring of extensions that can be used by the monitored users.

For the manual part of the testing, each call was handled manually on the agent with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Engage.

The verification of tests included use of Engage logs for proper message exchanges, and use of Engage web interface for proper logging and playback of calls.

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 this DevConnect Application Note 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 Telstrat Engage did not include use of any specific encryption features as requested by Telstrat.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Engage:

- Handling of TAPI events.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, hunt group, personal, hot desking, non-hot desking, hold/reconnect, transfer, conference, multiple calls, multiple agents, long duration, G.711, G.729, call park, forwarding, music on hold, mute/unmute, media shuffling and non-shuffling.

The serviceability testing focused on verifying the ability of Engage to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Engage.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Engage from the compliance testing.

- In the attended conference scenarios, the first recording for the conference-from user included silence for the period that the conference-from user was conversing with the conference-to user, and the second recording for the conference-from user contained the conversation with the conference-to user.
- In the unattended conference scenarios, two recording entries were produced for the conference-from user. One of the recording entries contained zero length, and the other contained all conversations involving the conference-from user.

## 2.3. Support

Technical support on Engage can be obtained through the following:

- **Phone:** (972) 633-4548
- **Email:** [support@telstrat.com](mailto:support@telstrat.com)

### 3. Reference Configuration

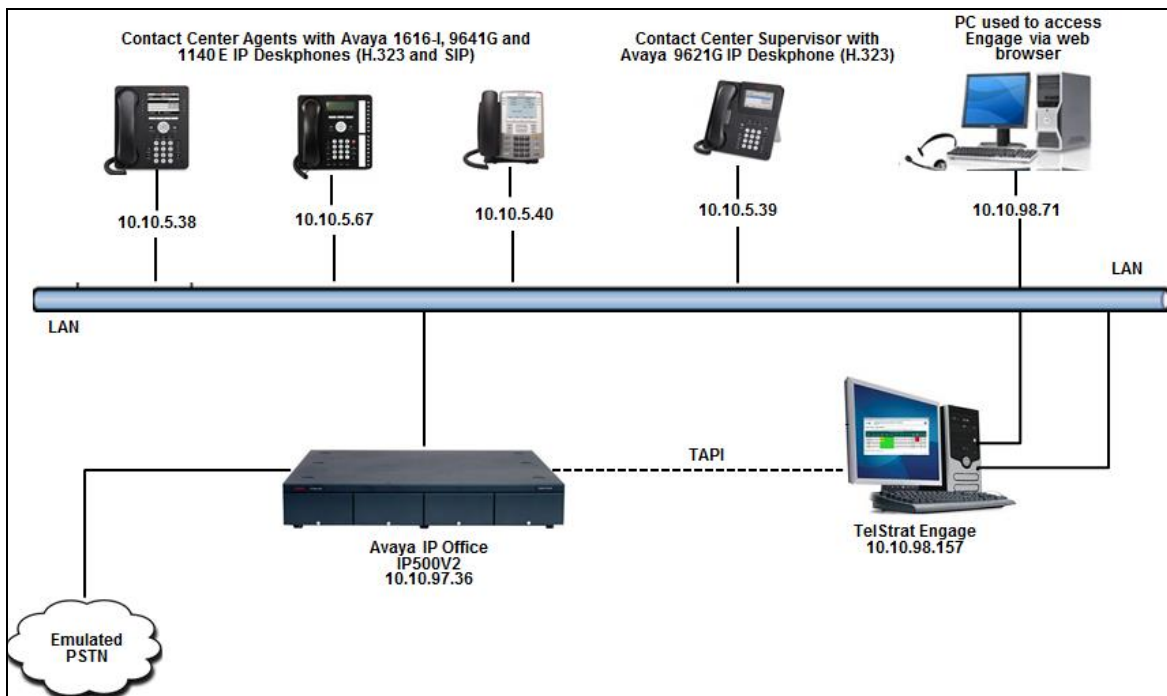
The configuration used for the compliance testing is shown in **Figure 1**.

The detailed administration of IP Office resources is not the focus of these Application Notes and will not be described. In addition, the port mirroring of the layer 2 switch is also outside the scope of these Application Notes and will not be described.

The IP Office resources used in the compliance testing is shown in the table below. In the testing, Engage monitored all activities from three extensions that can be used by two users. User 28231 did not use hot desking, whereas user 28247 used hot desking and can login from either extension 28232 or 28233. During compliance testing the recording playback was played by using the web based interface to Engage.

The RTP stream from the Avaya IP Deskphones associated with all three extensions below were mirrored from the layer 2 switch and replicated over to Engage.

Contact Center Devices	Values
Hunt Groups	28000, 28001
Supervisor	28234
Extensions	28231, 28232, 28233
Users	28231, 28247



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office on IP500 V2	10.1 build 237
Avaya 1616 -I IP Deskphone (H.323)	1.350B
Avaya 9621G IP Deskphone (H.323)	6.6401
Avaya 9641G IP Deskphone (H.323)	6.6401
Avaya 1140E IP Deskphone (SIP)	04.04.26.0
TelStrat Engage on Windows Server 2012 <ul style="list-style-type: none"><li>• Avaya TAPI2</li></ul>	5.5.7.1 R2 Standard 3.2.34

*Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 only.*

## 5. Configure Avaya IP Office

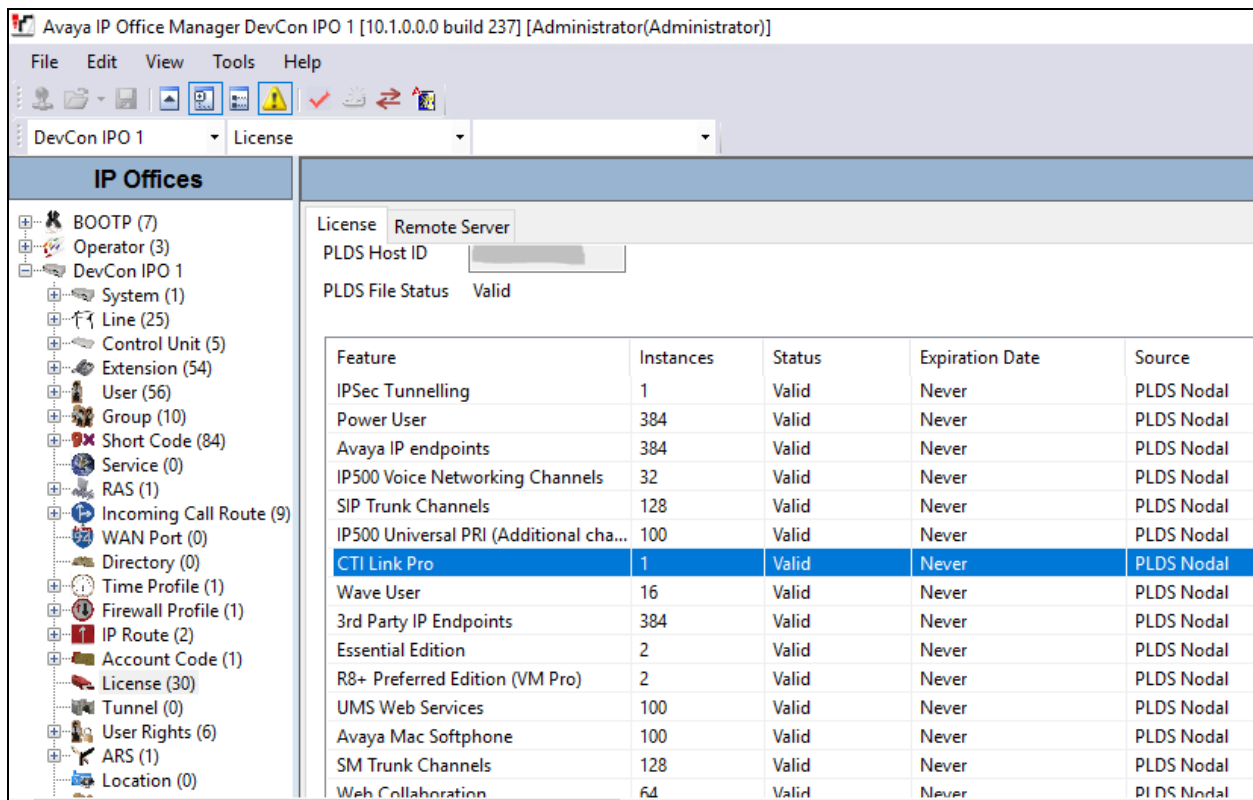
This section provides the procedures for configuring IP Office. The procedures include the following areas:

- Verify license
- Obtain telephone IP addresses

### 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 IP Office system, and log in using the appropriate credentials.

The **Avaya IP Office Manager** screen is displayed. From the configuration tree in the left pane, select **License** to display a list of licenses in the right pane. Verify that there is a license for **CTI Link Pro** and that the **Status** is “Valid”, as shown below.



Avaya IP Office Manager DevCon IPO 1 [10.1.0.0.0 build 237] [Administrator/Administrator]

File Edit View Tools Help

DevCon IPO 1 License

**IP Offices**

- BOOTP (7)
- Operator (3)
- DevCon IPO 1
  - System (1)
  - Line (25)
    - Control Unit (5)
    - Extension (54)
    - User (56)
    - Group (10)
    - Short Code (84)
    - Service (0)
    - RAS (1)
    - Incoming Call Route (9)
    - WAN Port (0)
    - Directory (0)
    - Time Profile (1)
    - Firewall Profile (1)
    - IP Route (2)
    - Account Code (1)
    - License (30)
    - Tunnel (0)
    - User Rights (6)
    - ARS (1)
    - Location (0)

License Remote Server

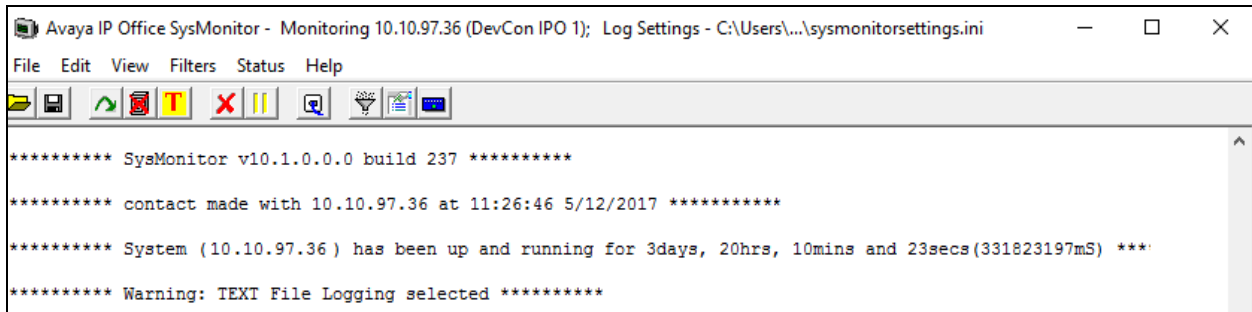
PLDS Host ID [REDACTED]

PLDS File Status Valid

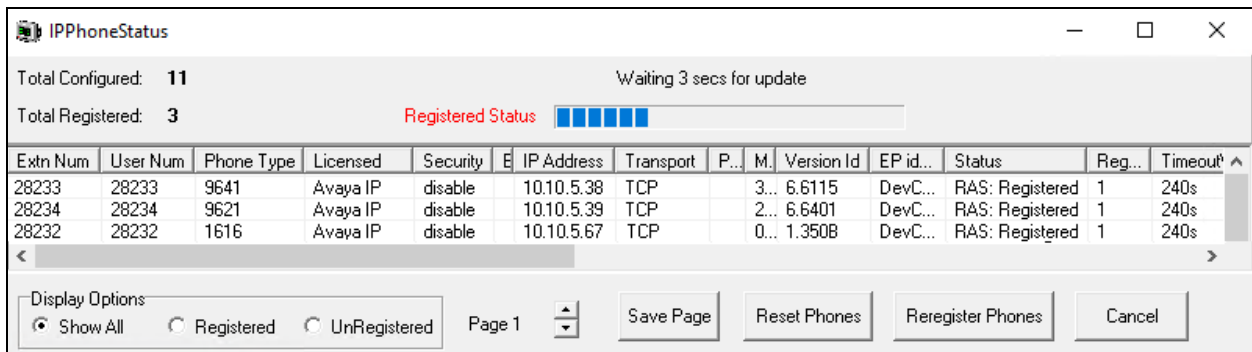
Feature	Instances	Status	Expiration Date	Source
IPSec Tunnelling	1	Valid	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Valid	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Valid	Never	PLDS Nodal
<b>CTI Link Pro</b>	<b>1</b>	<b>Valid</b>	<b>Never</b>	<b>PLDS Nodal</b>
Wave User	16	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Essential Edition	2	Valid	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	2	Valid	Never	PLDS Nodal
UMS Web Services	100	Valid	Never	PLDS Nodal
Avaya Mac Softphone	100	Valid	Never	PLDS Nodal
SM Trunk Channels	128	Valid	Never	PLDS Nodal
Web Collaboration	64	Valid	Never	PLDS Nodal

## 5.2. Obtain Telephone IP Address

From a PC running the IP Office Monitor application, select **Start** → **Programs** → **IP Office** → **Monitor** to launch the application. The **Avaya IP Office SysMonitor** screen is displayed, as shown below. Select **Status** → **H323 Phone Status** from the top menu.



The **IPPhoneStatus** screen is displayed. Make a note of the **IP Address** associated with each **Extn Num** that the users may be using from **Section 3**. Note that extension **28231** shown in **Section 3** is a SIP user and its IP address can be found similarly in the SysMonitor screen by navigating to **Status** → **SIP Phone Status** (not shown).



## 6. Configure TelStrat Engage

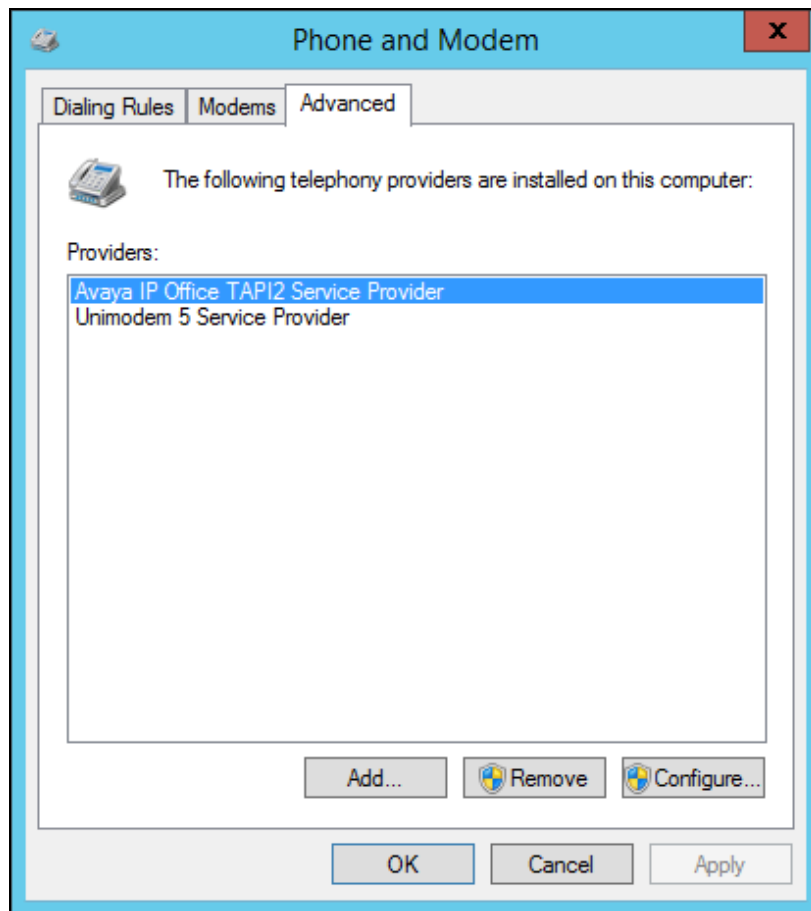
This section provides the procedures for configuring Engage. The procedures include the following areas:

- Administer TAPI driver
- Launch VoIP Engine Configuration
- Administer SPAN configuration
- Administer port mapping

The configuration of Engage is typically performed by TelStrat installation personnel or resellers. The procedural steps are presented in these Application Notes for informational purposes. The Avaya TAPI 2 driver is assumed to be pre-installed on the Engage server.

### 6.1. Administer TAPI Driver

From the Engage server, enter “phone and modem” anywhere on the desktop to locate **Phone and Modem**. Click on the pertinent entry from the result to launch the application. In the displayed **Phone and Modem** screen, select the **Advanced** tab. Select the **Avaya IP Office TAPI2 Service Provider** entry, and click **Configure**.





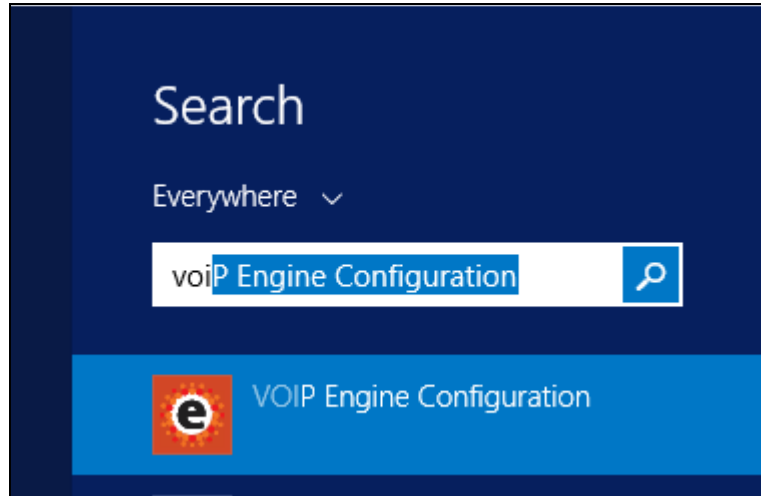
The **Avaya TAPI2 configuration** screen is displayed. For **Switch IP Address**, enter the IP address of IP Office. Select the radio button for **Third Party**, and enter the IP Office system password into the **Switch Password** field. Reboot the Engage server.

The screenshot shows a dialog box titled "Avaya TAPI2 configuration" with a close button (X) in the top right corner. The dialog contains the following fields and options:

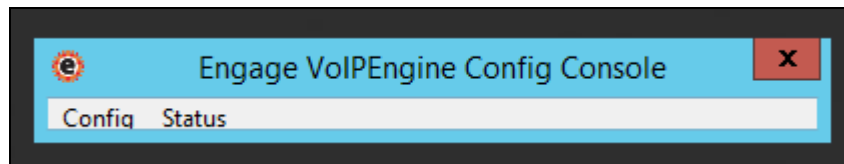
- Switch IP Address:** A text box containing "10.10.97.36".
- Buttons:** "OK" and "Cancel" buttons are located to the right of the IP address field.
- Radio Buttons:** "Single User" (unselected) and "Third Party" (selected).
- Single User Section:** A group box containing "User Name" and "User Password" text boxes.
- Third Party Section:** A group box containing a "Switch Password" text box (masked with asterisks), and three checkboxes: "Ex Directory Users", "WAV Users", and "ACD Queues" (all unselected).
- Advanced settings:** A group box containing a "Ping Timeout (5 to 420 seconds)" text box with the value "5".

## 6.2. Launch VoIP Engine Configuration

From the Engage server, enter “voip” anywhere on the desktop to locate **VOIP Engine Configuration**. Click on the pertinent entry from the result to launch the application.



The **Engage VoIP Engine Config Console** screen below is displayed. Click **Config**.



### 6.3. Administer SPAN Configuration

The **VoIP Configuration** screen is displayed. For **CTI Option**, select **Avaya IP Office** from the drop-down list. Click **More**.

The screenshot shows the 'VoIP Configuration' window. The 'CTI Option' dropdown menu is set to 'Avaya IP Office'. Other fields include 'IPD CC Address', 'IPD CC Port' (0), 'Observer Server', 'Observe Port' (0), 'Recording Board ID' (2300), 'User ID', and 'Password'. Under 'Calls To Record', 'All Trunk/Internal Calls' is selected. There are checkboxes for 'SoftPhone', 'IPDCC', and 'ACCS'. A 'More' button is highlighted with a red rectangular box. At the bottom, there is a 'Port Mapping' section with a table header: Recording Channel, Device ID, IP, DN, Record With.

The **Avaya IP Office Advanced Configuration** screen is displayed next. Check **Mirroring By IP** to enable device mapping by IP addresses, and retain default values for all other fields.

The screenshot shows the 'Avaya IP Office Advanced Configuration' window. The 'Mirroring By IP' checkbox is checked. Under 'Ports', 'SIP Server IP Port' is 5060 and 'H.323 Server IP Port' is 0. Under 'Trace', 'SIP Trace' and 'H.323 Trace' are unchecked. At the bottom, 'Populate Agent Name' is unchecked. On the right, the 'Generic Value Mapping' section has 'Generic1' selected in the 'Target Fields' dropdown. Below it is a 'Mapped Source' section with 'CallData' listed.

## 6.4. Administer Port Mapping

The **VoIP Configuration** screen is displayed again. Right click in the empty screen and select **ADD**.

The screenshot shows the 'VoIP Configuration' window with the following fields and options:

- CTI Option:** Avaya IP Office (dropdown)
- Recording Board ID:** 2300
- IPO CC Address:** [Empty text box]
- IPO CC Port:** 0
- Observer Server:** [Empty text box]
- Observe Port:** 0
- User ID:** [Empty text box]
- Password:** [Empty text box]
- Calls To Record:**  All Trunk/Internal Calls,  All Trunk Calls,  Calls Selected By DN
- Buttons:** SoftPhone, More,  IPOCC,  ACCS

**Port Mapping Table:**

Recording Channel	Device ID	IP	DN	Record With
[Context Menu: ADD, Delete, Modify, Import file, Export File, Acquire via TAPI]				

**Footer:** No. of Log Files: 8, Config File Location, Other Parameters, OK, Cancel

The **Device And CommSrv Port Mapping** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Device ID:** One of the extensions from **Section 3**.
- **IP:** The IP address associated with the extension from **Section 5.2**.
- **DN:** "\*" as wild card to allow use of device by any user.
- **Recording Channel:** An available port.

Device And CommSrv Port Mapping

Device ID: 28232  SIP Phone

IP: 10.10.5.67

DN: \*

Recording Channel: 102

Calls To Record:  
 Trunk/Internal Calls  Trunk Calls

Recording Stream:  
 Mirroring

HotDesk DN

Add Cancel

Repeat this section to create a port mapping for each extension from **Section 3**.

In the compliance testing, three entries were created, as shown below.

The image shows a 'VoIP Configuration' dialog box for an 'Avaya IP Office'. It contains several configuration fields and a table for port mapping.

**Configuration Fields:**

- CTI Option: Avaya IP Office (dropdown)
- Recording Board ID: 2300 (text box)
- IPO CC Address: (empty text box)
- IPO CC Port: 0 (text box)
- Observer Server: (empty text box)
- Observe Port: 0 (text box)
- User ID: (empty text box)
- Password: (empty text box)

**Recording Options:**

- Calls To Record:  All Trunk/Internal Calls,  All Trunk Calls,  Calls Selected By DN
- Buttons: SoftPhone, More
- Checkboxes:  IPOCC,  ACCS

**Port Mapping Table:**

Recording Channel	Device ID	IP	DN	Record With
101	28231	10.10.5.40	*	Mirroring
102	28232	10.10.5.67	*	Mirroring
103	28233	10.10.5.38	*	Mirroring

**Footer:**

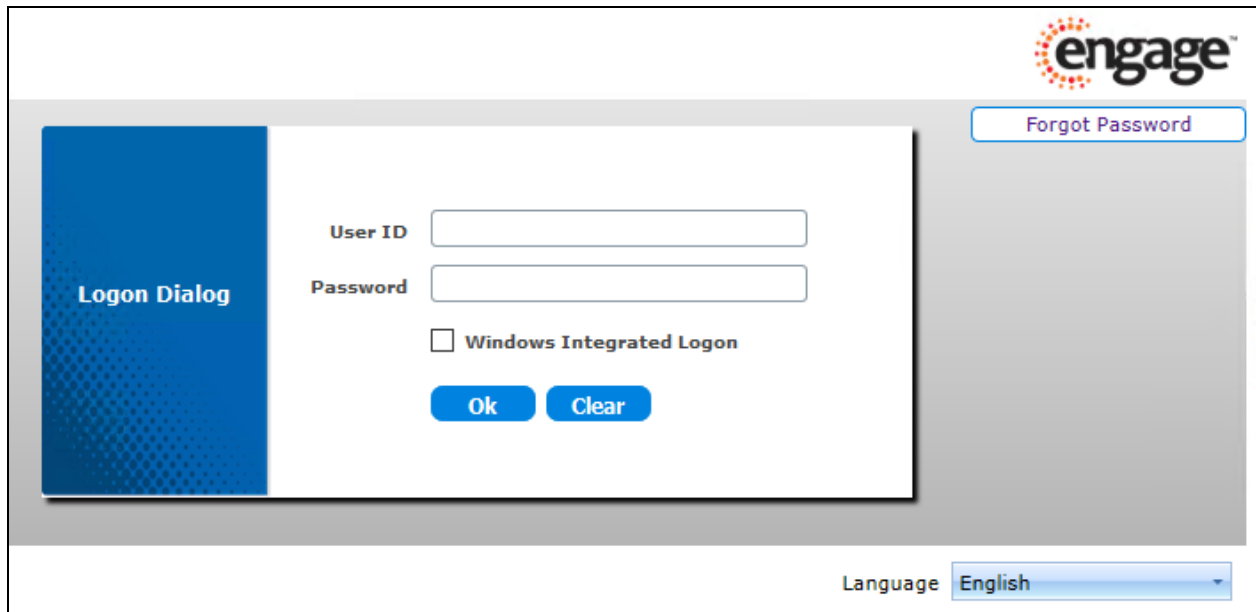
- No. of Log Files: 8 (text box)
- Buttons: Config File Location, Other Parameters, OK, Cancel

## 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of IP Office and Engage.

Log a user in to handle and complete a hunt group call. Access the Engage web-based interface by using the URL “http://ip-address/engage” in an Internet browser window, where “ip-address” is the IP address of the Engage server.

The **Logon Dialog** screen below is displayed. Log in using the appropriate credentials.



The screenshot displays the Engage web-based interface's logon dialog. The dialog box is titled "Logon Dialog" and features a blue header. Inside the dialog, there are two input fields: "User ID" and "Password". Below these fields is a checkbox labeled "Windows Integrated Logon". At the bottom of the dialog are two buttons: "Ok" and "Clear". The background of the interface shows the Engage logo in the top right corner, a "Forgot Password" link, and a language dropdown menu set to "English".

The screen is updated with a list of call recordings. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.

	Date	Start Time	End Time	Rec Duration	Hold Duration	Agent ID	Extension	CLID	Dialed Number	Direction
d Calls	11/29/2017	11:13:32 AM	11:13:47 AM	00:14		28233	28233	28233	962196756104	Out
	11/29/2017	11:12:59 AM	11:13:15 AM	00:15		28232	28232	56103	28232	In
	11/29/2017	11:05:07 AM	11:05:09 AM	00:02		28232	28232	28232	962196756103	Out

Double click on the entry and verify that the call recording can be played back.

The screenshot shows the application interface with the 'Playback Log' table. The entry for 11/29/2017 at 11:13:32 AM is highlighted. Below the table, a 'Media Player' window is open, displaying the audio waveform for the selected call. The call ID is 1711291113322300103. The media player shows the call started at 11:13:32 AM and ended at 11:13:47 AM. The playback progress is at 0:01 out of 0:14. The interface also shows 'Results: 149' and 'No of Records: 200'.



## 8. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage 5.5 to successfully interoperate with Avaya IP Office 10.1 using VoIP recording. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 9. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

1. *Administering Avaya IP Office™ Platform with Manager*, Release 10.1, June 2017.
2. *Deploying Avaya IP Office™ Platform IP500 V2*, 15-601042 Issue 32f - (20 July 2017).

Product documentation for Telstrat may be found at <http://esupport.telstrat.com>.

3. *Install – Setup Engage Server*, Release 5.5, Issue 1.1, December 2017.
4. *Recorder Administration Guide*, Release 5.5, Issue 1.0, December 2017.

---

**©2017 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](mailto:devconnect@avaya.com).