Avaya Solution & Interoperability Test Lab

Application Notes for Zenitel Turbine with Avaya IP Office using Session Initiation Protocol and Transport Layer Security - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Zenitel Turbine IP Intercom Station Series to interoperate with Avaya IP Office R11.0. The Zenitel Turbine is an IP Intercom that supports voice transmission using the Session Initiation Protocol (SIP) and Transport Layer Security (TLS).

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.

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 Zenitel Turbine IP Intercom Stations to interoperate with Avaya IP Office connecting with Session Initiation Protocol (SIP) and Transport Layer Security (TLS) to enable Secure Real-time Transport Protocol (SRTP) between the Zenitel Turbine IP Intercom Stations and the Avaya IP Office endpoints.

The Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as the secondary expansion cabinet. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and user names. This allows calls between systems and support for a range of internal call features.

The Zenitel Turbine IP Intercom Stations (Turbine Stations) are designed for intelligent communications as part of the Zenitel Intelligent Communication suite: SIP phones. Intelligent Communication is required for enterprise business intelligence and for critical communications. According to Zenitel, intelligence is defined three ways:

- Intelligibility: to hear, be heard and be understood in any situation or environment.
- Interoperability: to fully embed voice and audio within the mission critical processes of a business.
- IT Mandate: the fulfillment of the key performance measure of IT in provisioning mission critical technology including: High availability (.99999% uptime), maintainability (easy to provision and maintain) and cyber defensibility (full certification of compliance with standards needed to protect mission critical devices).

The Turbine Stations are made for tough environments at entrance and egress points to office buildings and gate and warehouse doors where clear communication is an issue. Also, in sectors like Building Security and Public Safety Oil & Gas, Heavy Industry, Transportation and even Marine.

All intercom stations in the Zenitel's Turbine series utilize the latest technology and some of the features include: HD voice quality, Open Duplex, Active Noise Cancellation, MEMS microphone, a 10W Class D amplifier and our unique speaker grille design.

In the compliance testing, each Zenitel Turbine IP Intercom Station was set up as a SIP user on Avaya IP Office and underwent testing of various call scenarios with other Avaya telephones and Zenitel Turbine IP Intercom Stations.

The following models in the Zenitel Turbine family were tested: TCIS-3, TCIS-6, TMIS-1, TFIE-1, ECPIR-3P. Other models in the Turbine family are not covered by this compliance test.

Note: The Zenitel Turbine phones may be referred to as Zentitel Turbine, Turbine Stations, Zenitel Turbine IP Intercom Station, Turbine Intercom, Turbine or Zenitel Turbine IP Intercoms throughout this document, but they all refer to the same phones that were tested.

2. General Test Approach and Test Results

The general test approach was to place calls to and from the Turbine Intercom phones and exercise basic telephone operations. For serviceability testing, failures such as LAN cable pulls, and hardware resets were performed.

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's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/Smartphone to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for Smartphone interfaces, different manufacturers utilize different Smartphone/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and the Zenitel Turbine IP Intercoms utilized enabled capabilities of TLS and SRTP.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. TCIS-3, TCIS-6, TMIS-1, TFIE-1 and ECPIR-3P models were tested. The feature testing was to verify that:

- Turbine successfully registers with IP Office using the TLS protocol.
- Turbine successfully establishes audio calls with good quality SRTP audio to Avaya H.323, SIP and digital endpoints registered to IP Office.
- Turbine successfully establishes audio calls with a simulated PSTN.
- Turbine IP successfully negotiates the appropriate audio codec.
- DTMF tones could be passed successfully to energize relay on Turbine unit and switch audio direction.
- Turbine successfully calls multiple Avaya destinations in a hunt group.
- Turbine successfully calls a variety of endpoints in its call list.
- Correct handling of forwarded calls, cover paths and hunt groups.

The serviceability testing focused on verifying the ability of Turbine to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to the devices and denying service on IP Office.

Note: Compliance testing was carried out with the Turbine phones set to use TLS/SRTP. Testing was also carried out with Turbine phones set to use TCP/RTP and these Application Notes are labelled, *Application Notes for Zenitel Turbine with Avaya IP Office using Session Initiation Protocol and Transmission Control Protocol*.

2.2. Test Results

All test cases passed successfully with the following observations noted.

1. For SRTP to work properly, each Zenitel extension configured on IP Office must be set to “Enforced” VoIP Security on the VoIP tab. This is to overcome an issue with SDP negotiation as the Zenitel SIP phones do not support RFC 5939 (Capability Negotiation).
2. Call Park has a different meaning on the Turbine functionality than that of the Call Park feature on IP Office. When the Call Park function is used on Turbine it places multiple calls on hold. For every Direct Access Key (DAK) key with Call Park configured, there can be only one active or resumed call.

2.3. Support

Technical support on Zenitel Turbine can be obtained through the following:

- **Phone:** +1 816 231 7200 (Americas) +47 4000 2700 (Global)
- **Email:** cs@zenitel.com
- **Web:** https://www.zenitel.com/customer-service

3. Reference Configuration

Figure 1 illustrates a test configuration that was used to compliance test the interoperability of Turbine with IP Office. The configuration consists of IP Office Server Edition and IP500V2 Expansion. IP Office has connections to Avaya Digital, H.323 and SIP deskphones as well as SIP registrations with Turbine. A SIP trunk connects IP Office to a simulated PSTN.

Note: The Zenitel Turbine phones register to the IP Office Server Edition.

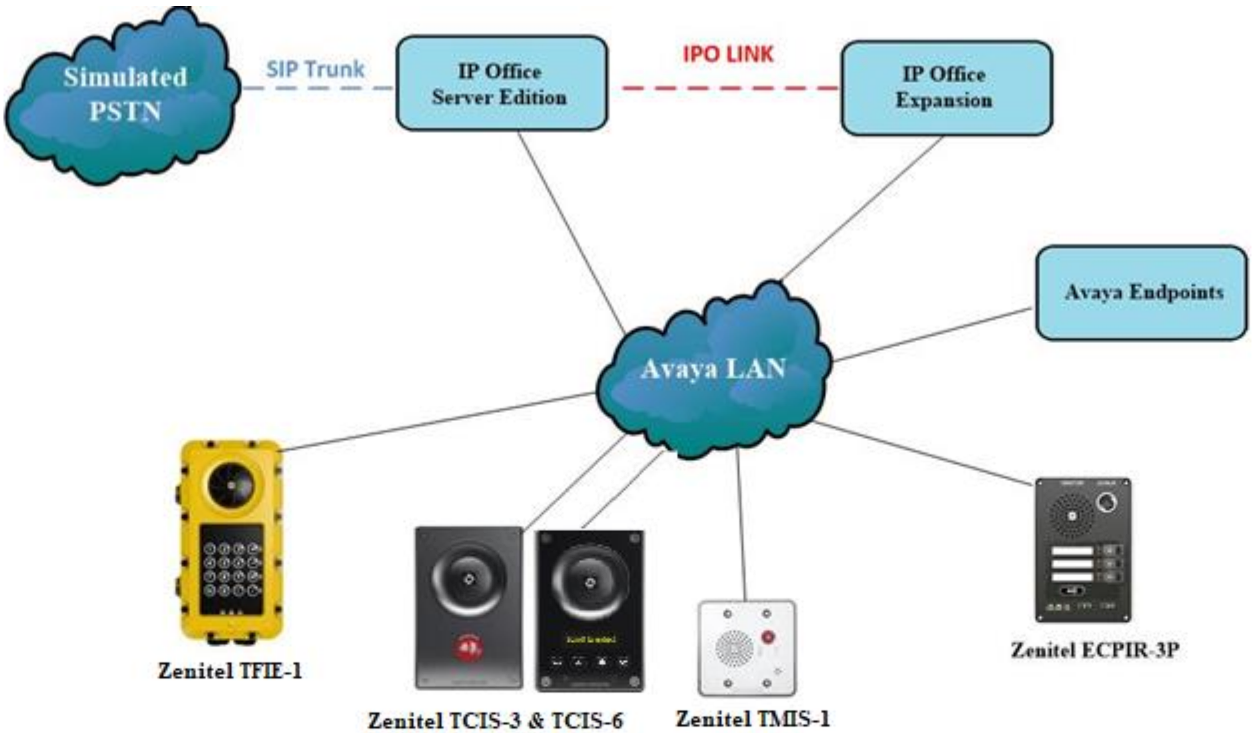


Figure 1: Avaya IP Office with Zenitel Turbine configuration

4. Equipment and Software Validated

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

Equipment/Software	Version/Release
Avaya IP Office Server Edition running on a virtual platform	R11.0.4.1.0 Build 11
Avaya IP Office IP500 V2	R11.0.4.1.0 Build 11
Avaya IP Office Manager	R11.0.4.1.0 Build 11
Avaya 96x1 Deskphone	H.323 Release 6.4014U
Avaya 1140e Deskphone	SIP R04.04.33.00
Avaya J129 SIP Deskphone	SIP R3.0.0.0.20
Avaya 9508 Digital Deskphone	R0.6
Avaya Equinox for Windows	V3.6.0.153.36
Zenitel Turbine IP Intercom - TCIS-3 - TCIS-6 - TMIS-1 - TFIE-1 - ECPIR-3P	5.0.3.0

Note: 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**.**

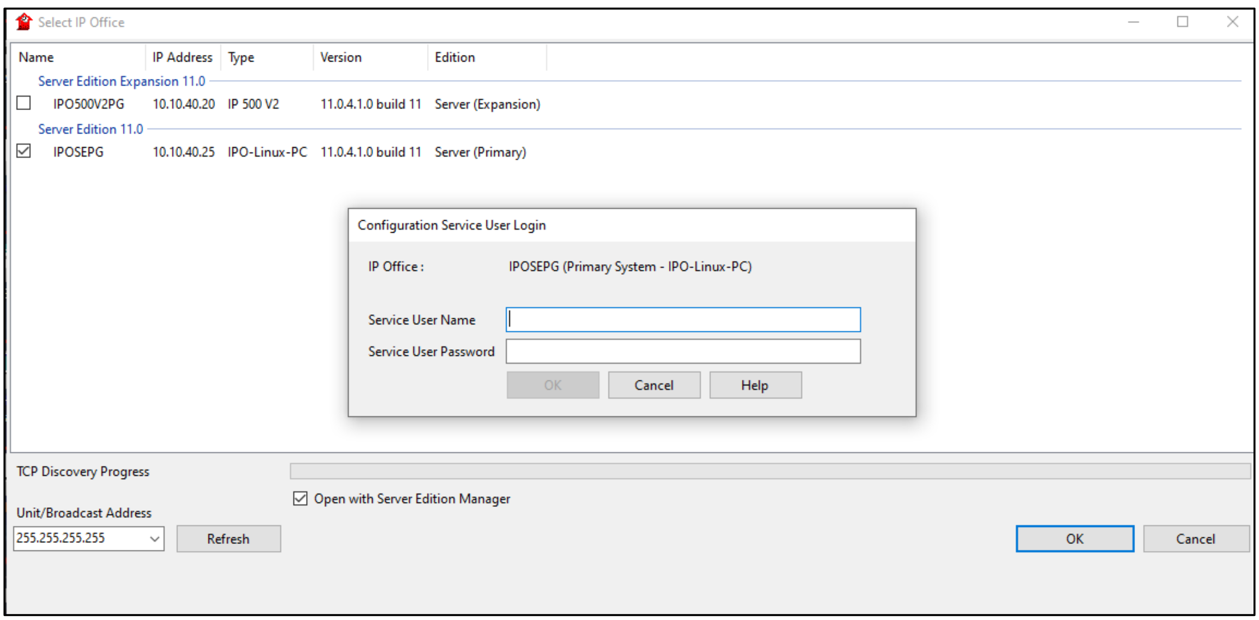
5. Avaya IP Office Configuration

Configuration and verification operations on the Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of the Avaya IP Office for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Launch Avaya IP Office Manager
- System Configuration
- Create a SIP User/Extension for the Turbine Intercom
- Configure SIP Extension
- Save Configuration

5.1. Launch Avaya IP Office Manager

From the IP Office Manager PC, click **Start → Programs → IP Office → Manager** to launch the Manager application (not shown). Select the required Server Edition as shown below and enter the appropriate credentials. Click on the **OK** button.



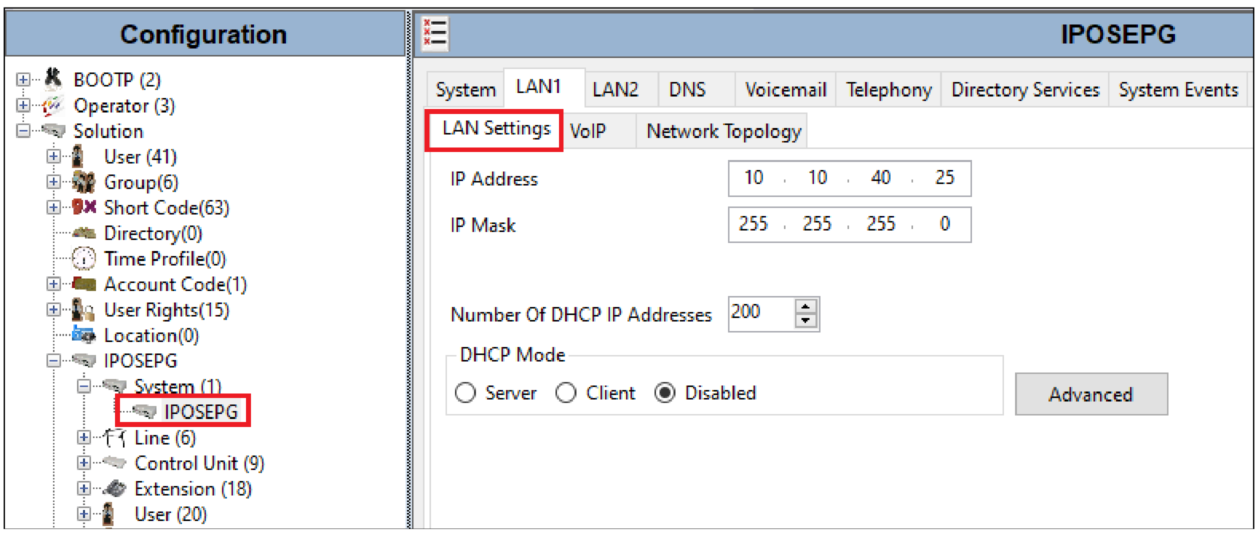
5.2. System Configuration

The IP Office system must be setup in the correct way to allow the Zenitel Turbine phones interoperate correctly. The LAN settings and VoIP security are the primary focus. Any settings that are changes on the Server Edition do not necessarily need to be mirrored on the expansion server as the Zenitel Turbine phones are registered on the Server Edition only.

Note: For compliance testing VoIP security was set as preferred as this allows for both RTP and STRP to be used. If the phones are set to use TLS and SRTP then this is what will be used as security is preferred.

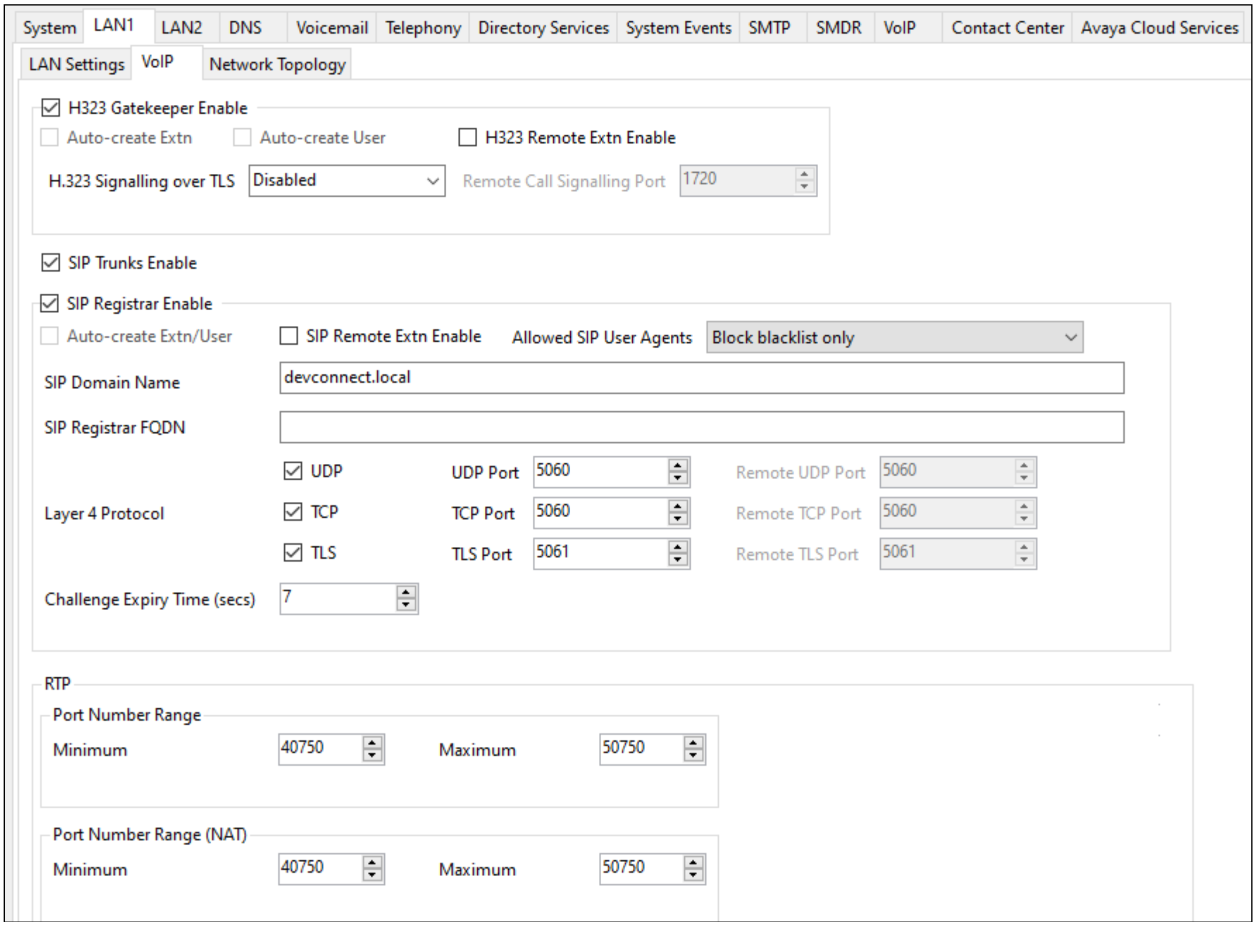
5.2.1. LAN1 - LAN Settings configuration

For the Turbine handsets to communicate with the IP Office **DHCP MODE** must be disabled. To disable DHCP, select **IPOSEPG → System (1)** then on the **LAN1** tab followed by the **LAN Settings** tab click on the **Disabled** radio button in the **DHCP Mode** section. Click the **OK** button (not shown) to save.



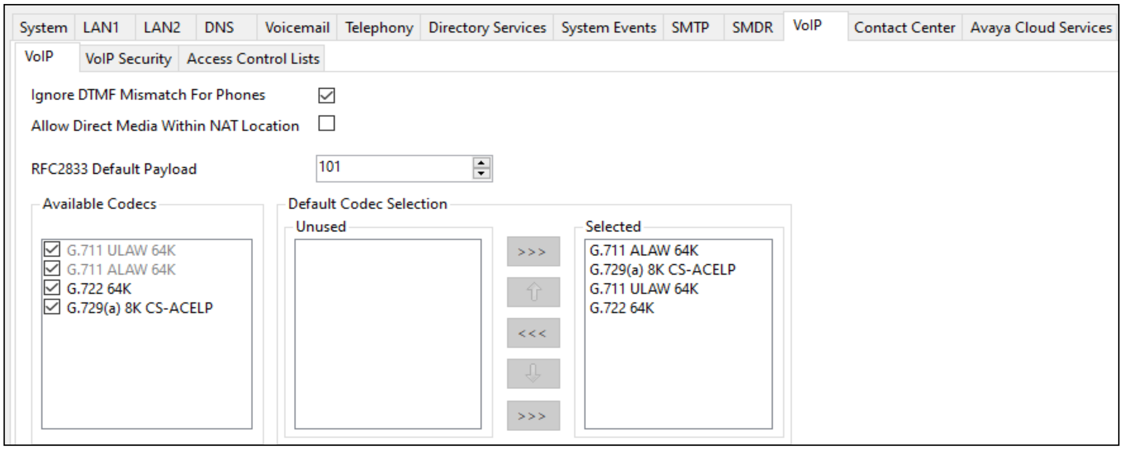
5.2.2. LAN1 - VoIP configuration

Select the **VoIP** tab and in the **Layer 4 Protocol** section check the **UDP**, **TCP** and **TLS** check boxes and select **Port 5060** and **5061** from the dropdown boxes. The other settings can be left as default or as shown below. Click on **OK** at the bottom of the screen to continue (not shown).



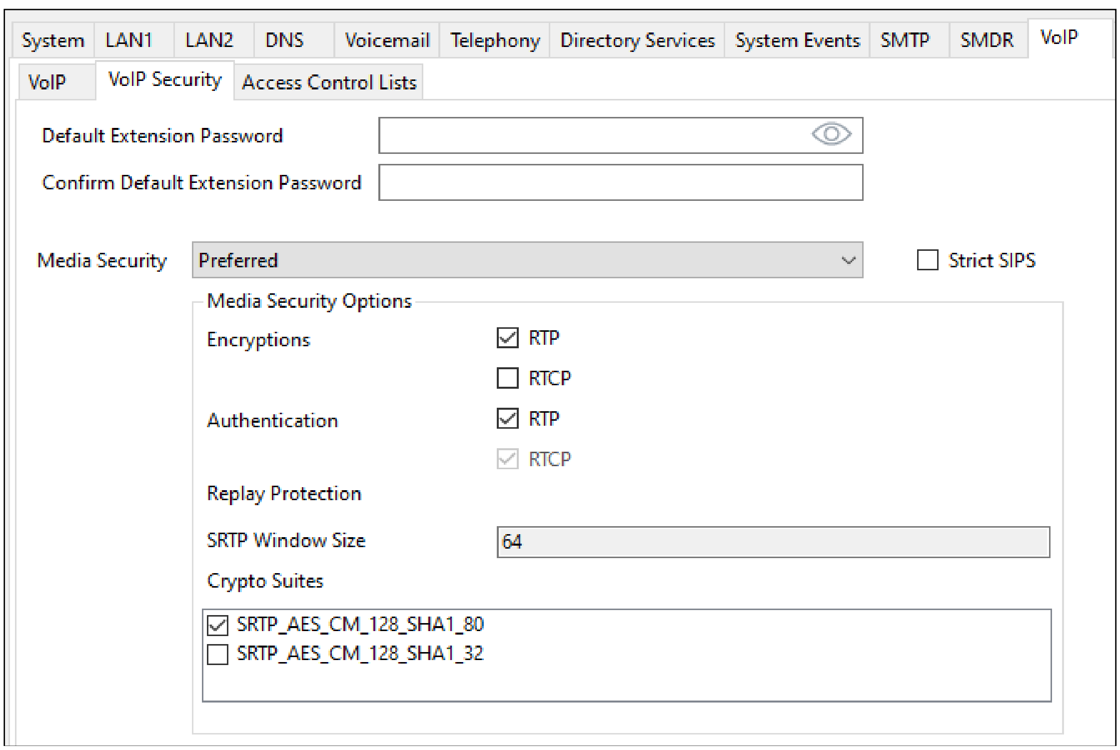
5.2.3. VoIP – Codec configuration

Select the **VoIP** tab along the top set of tabs and **VoIP** on the secondary tabs as shown below. The choice of Codec's is presented and can be chosen. The example below shows all available Codecs selected and an **RFC 2833 Default Payload** set to **101**. These can be changed depending on the needs of the site, for compliance testing everything was selected.



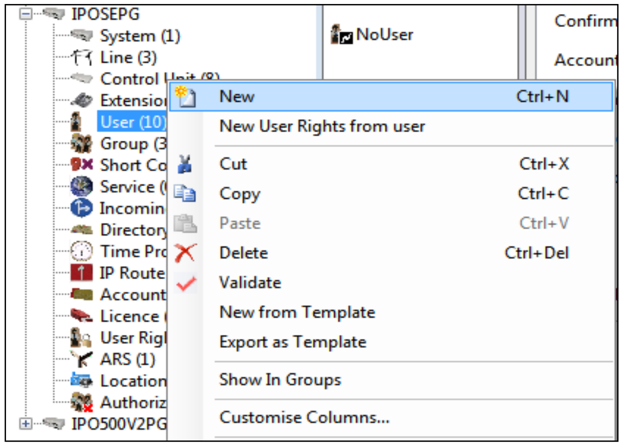
5.2.4. VoIP – VoIP Security configuration

Select the **VoIP Security** secondary tab. **Media Security** was set to **Preferred** with **RTP Encryption** and **RTP Authentication** ticked. RTCP was not encrypted for compliance testing and for simplicity during testing only one **Crypto** was chosen that being **SRTP_AES_CM_128_SHA1_80**.

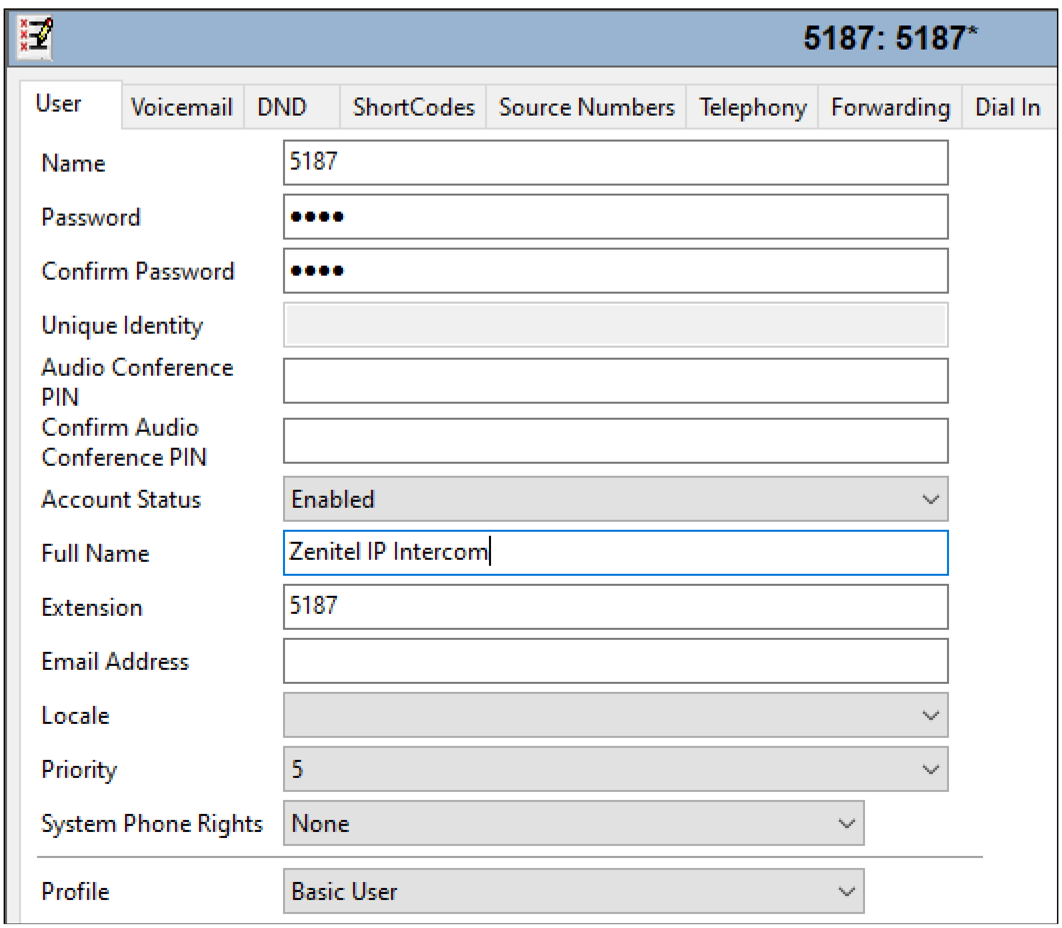


5.3. Create a SIP User/Extension for the Turbine Intercom

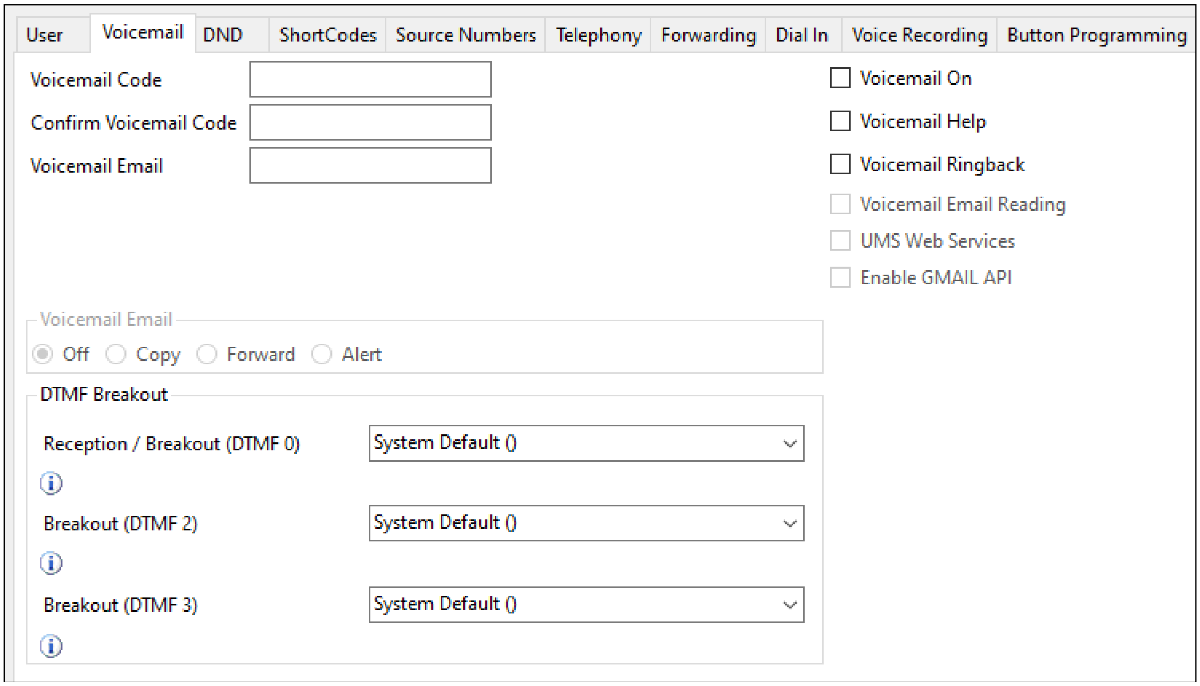
The Turbine phones are configured as SIP Extensions on IP Office. From the left window, right click on **User** and select **New**.



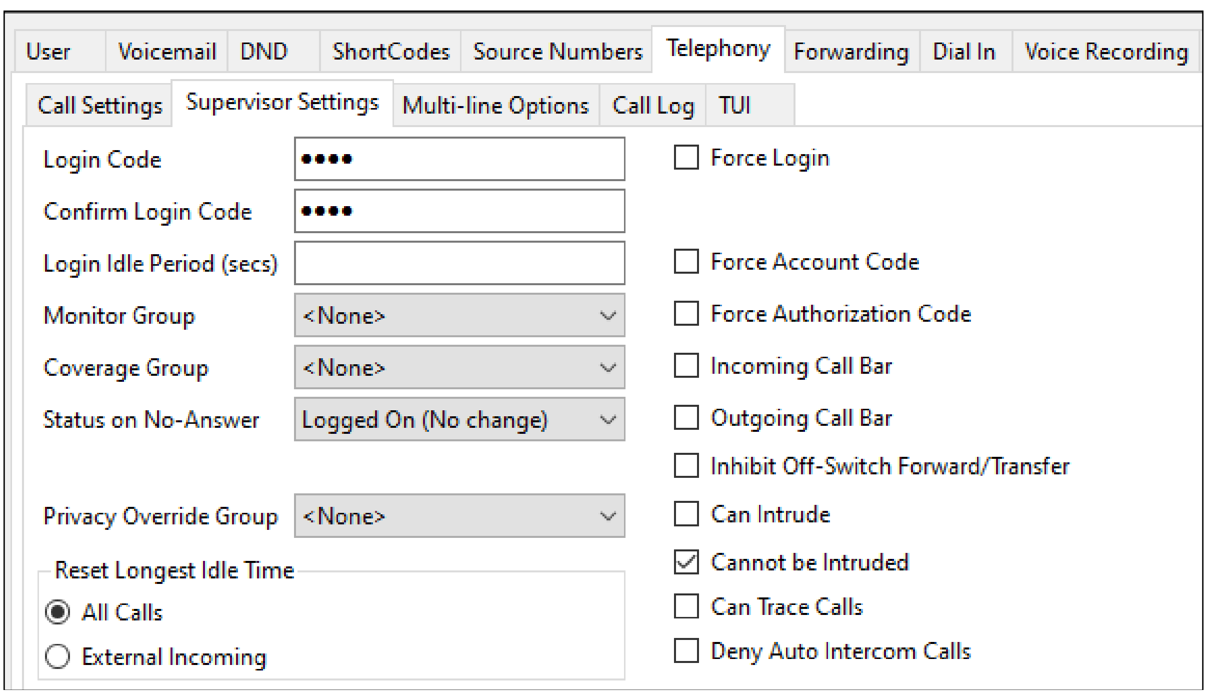
From the **User** tab, enter the appropriate details for this Turbine phone user.



Select the **Voicemail** tab and ensure that there is no tick in the box opposite **Voicemail On** as these phones do not required voicemail.

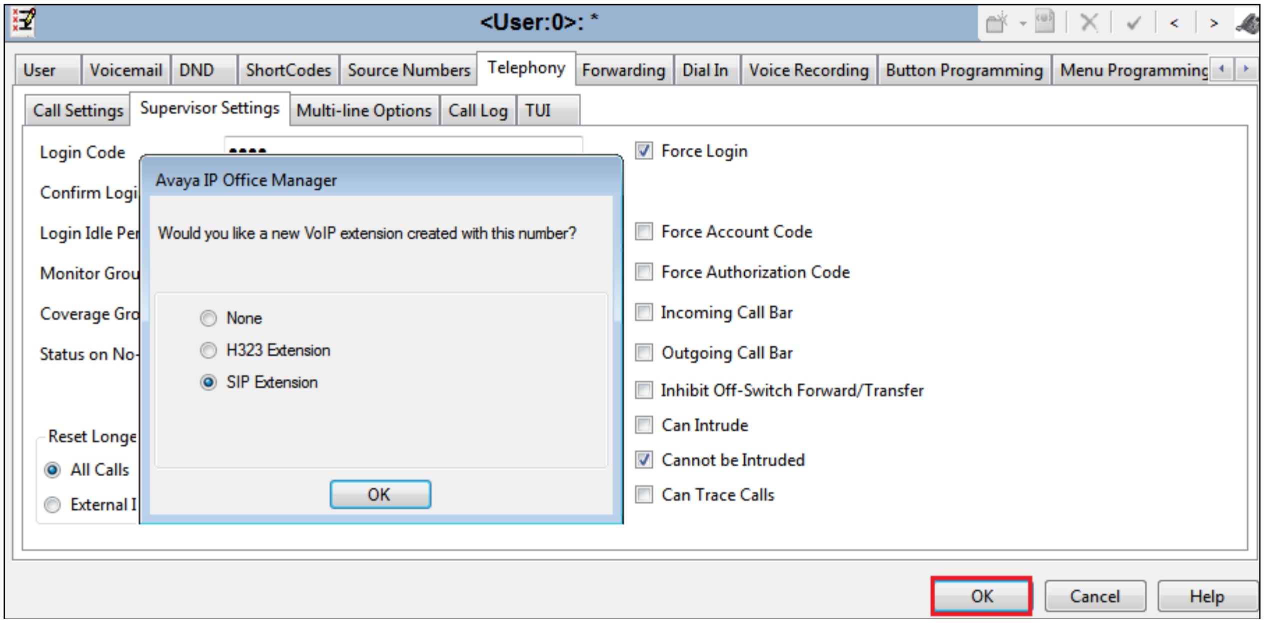


Select the **Telephony** tab and within that tab select the **Supervisor Settings** tab. The user **Login Code** is added here this will be the same as the password added on the previous page and will be used as stated in **Section 6.1**.



Once **OK** is clicked at the bottom of the screen on the previous page, a new window should appear asking to create a new extension. Select **SIP Extension** as is shown below.

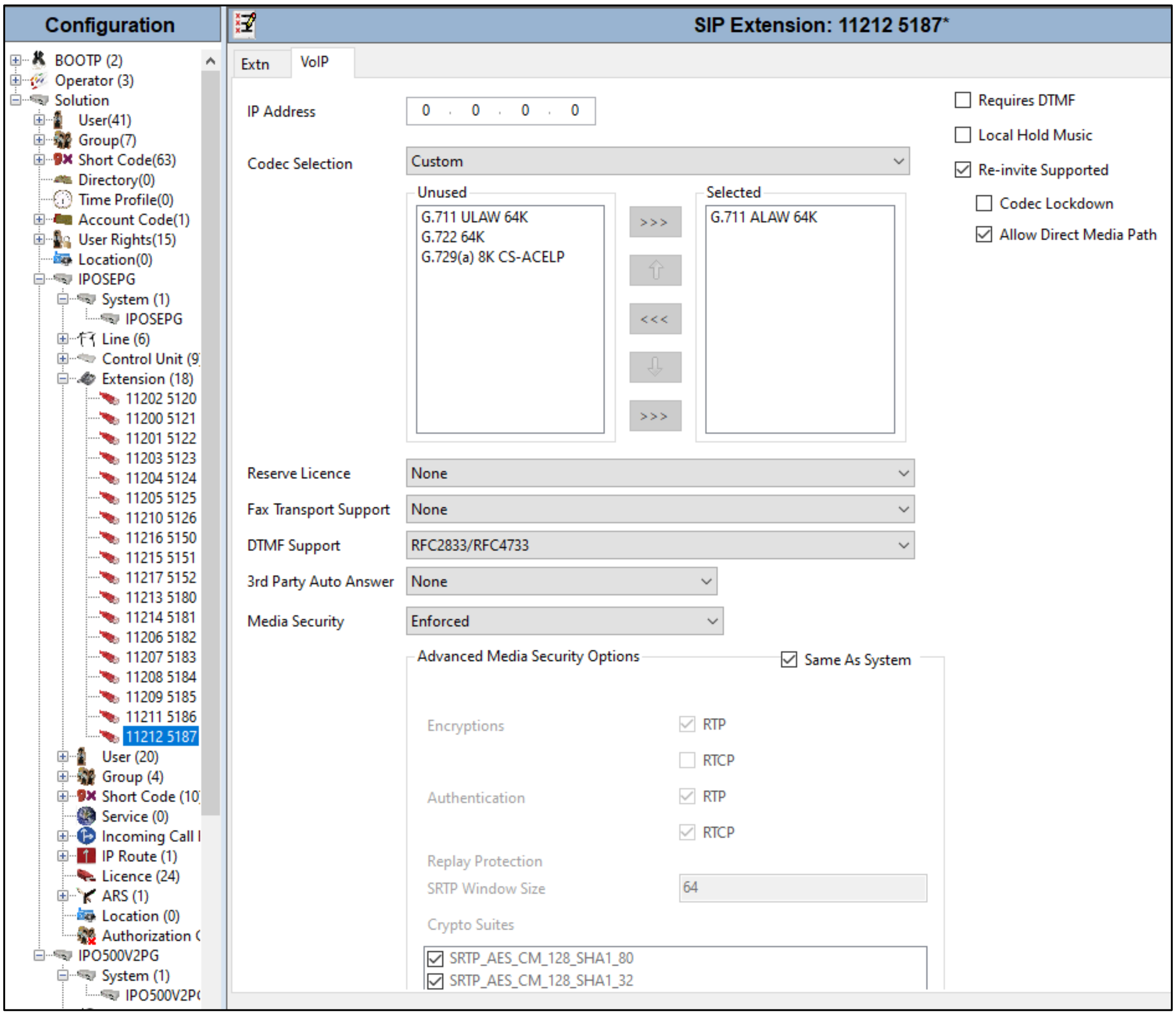
Note: If the system is not setup to auto-create extensions then a new extension can be added by right-clicking on **Extension** on the left window and selecting **New**, (not shown).



5.4. Configure SIP Extension

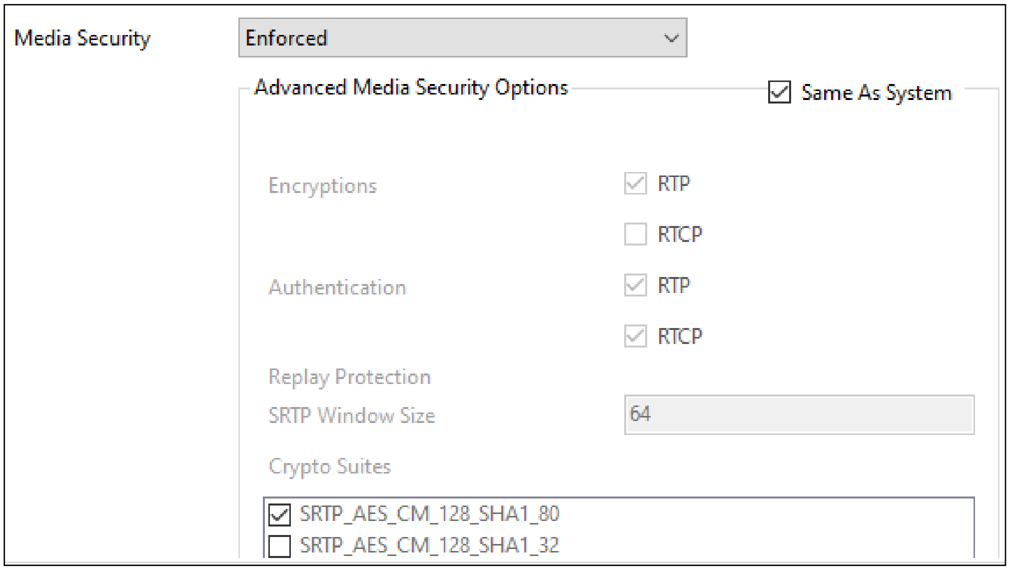
Expand **Extension** in the left window and select the required extension number. In the main window under **VoIP** tab, **Allow Direct Media Path** can be checked or unchecked as shown below. Other settings such as **DTMF Support** and **Codec Selection** are possible to change here if required by Zenitel.

Note: Compliance Testing was carried out with Allow Direct Media Path checked and with the other settings as shown below.



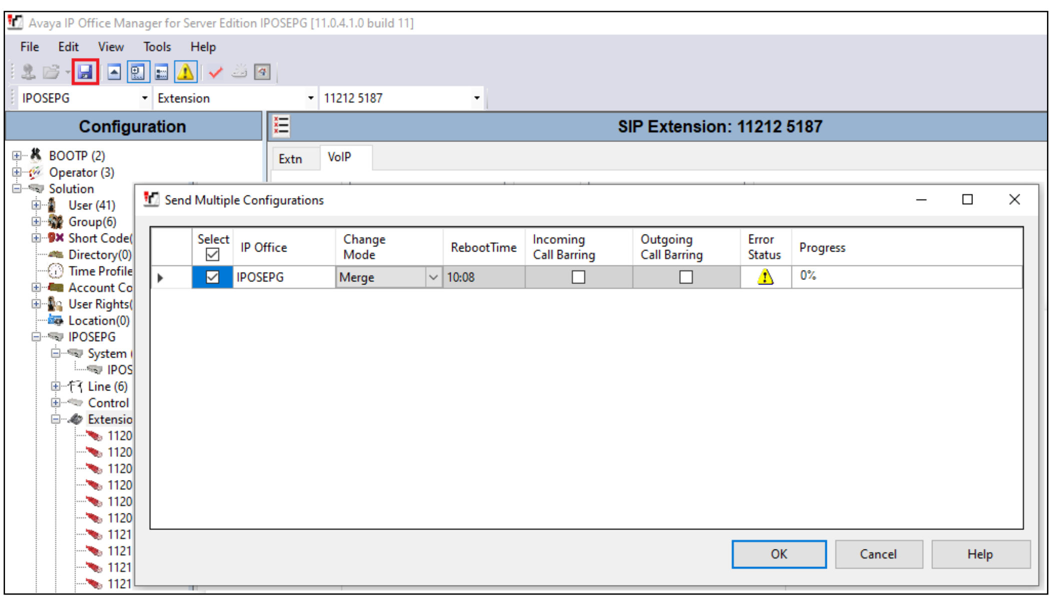
A closer look at the **Media Security** section is displayed on the following page.

Media Security is set to **Enforced** for all the Turbine extensions that are configured. This is due to the issue explained in **Section 2.2** [For SRTP to work properly, each Zenitel extension configured on IP Office must be set to "Enforced" VoIP Security. This is to overcome an issue with SDP negotiation as the Zenitel SIP phones do not support RFC 5939 (Capability Negotiation)]. With **Media Security** set to **Enforced** this will take out any negotiation requirement as the SRTP is now forced to be used. The **Advanced Media Security Options** were left the **Same As System** with the system **Crypto** being used.



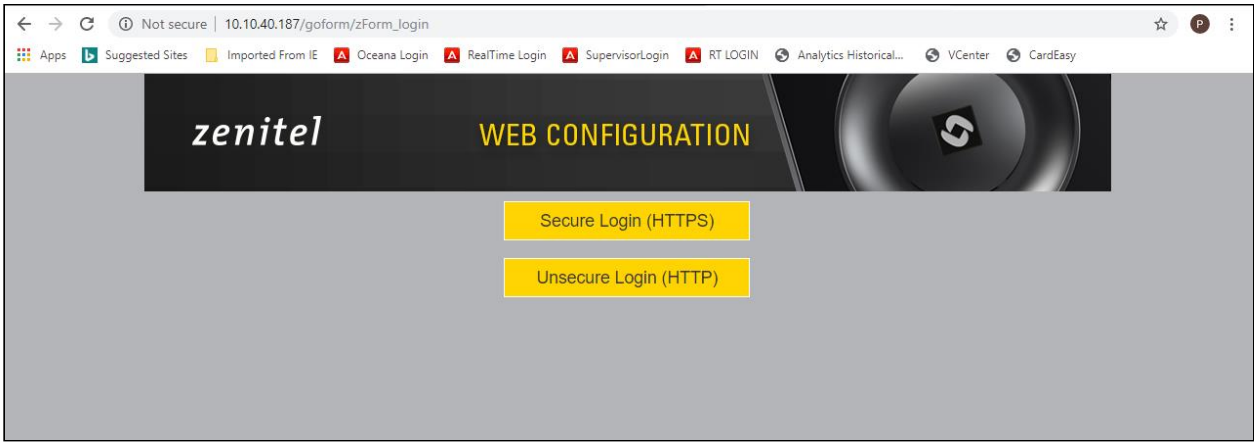
5.5. Save Configuration

Once all the configuration has been completed, click on the **Save** icon at the top left and then when the window opens select the IP Office by ticking the box and click **OK**.

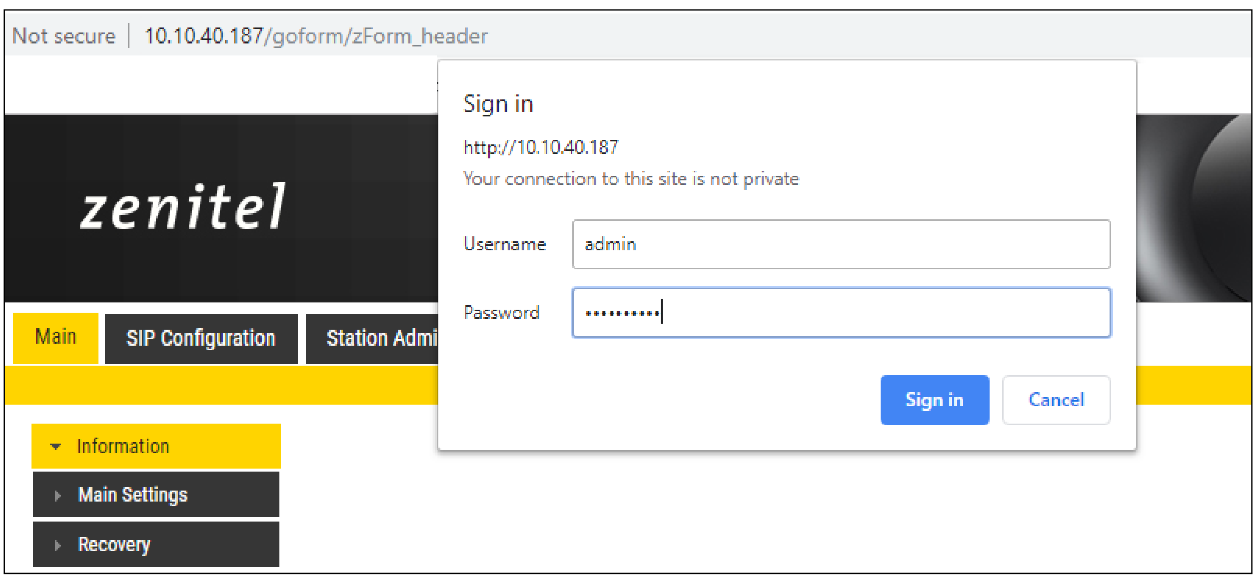


6. Configure Zenitel Turbine

The following steps detail the configuration for Turbine using the web interface. Access the Turbine web interface, enter **http://<ipaddress>** in an Internet browser window, where **<ipaddress>** is the IP address of Turbine. For compliance testing **Unsecure Login (HTTP)** was chosen.



Log in with the appropriate credentials.



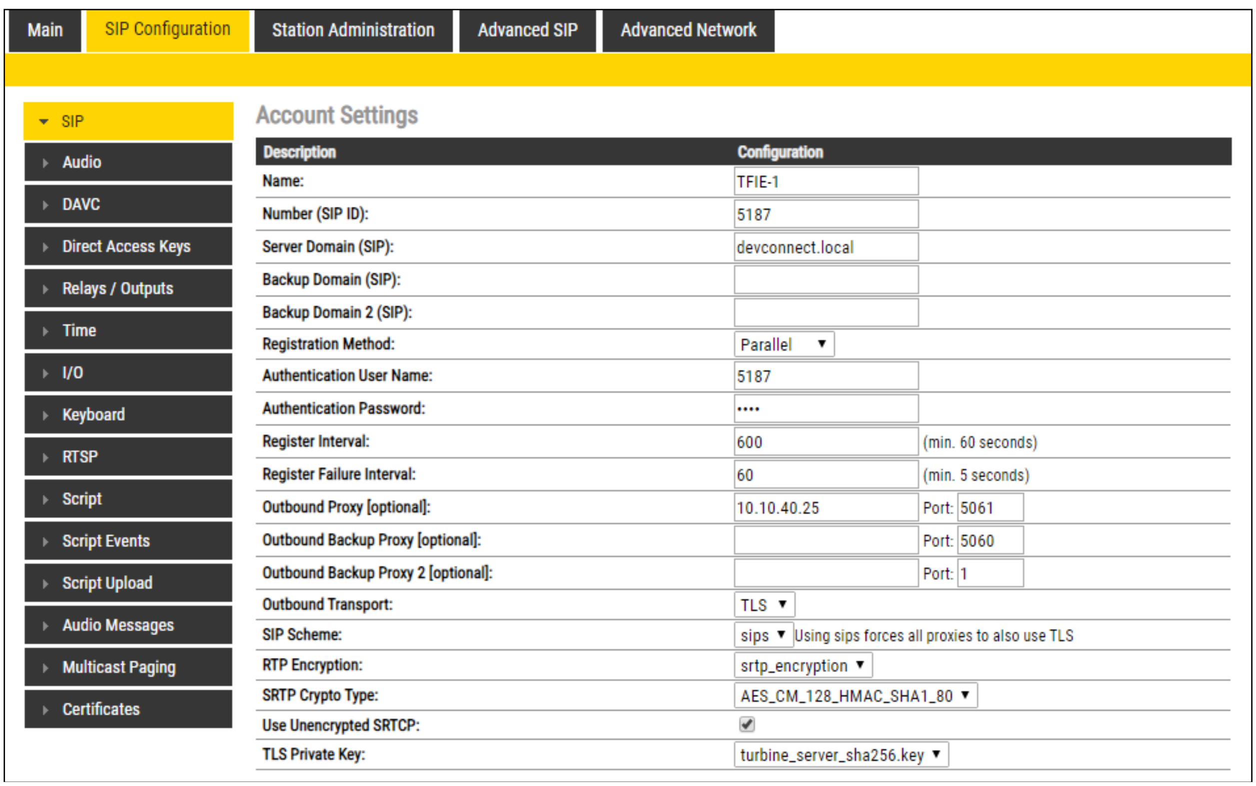
Upon logging in, information on that Turbine station is displayed. The following settings should be checked.

- SIP Configuration
- Direct Access Keys
- Certificates
- Audio

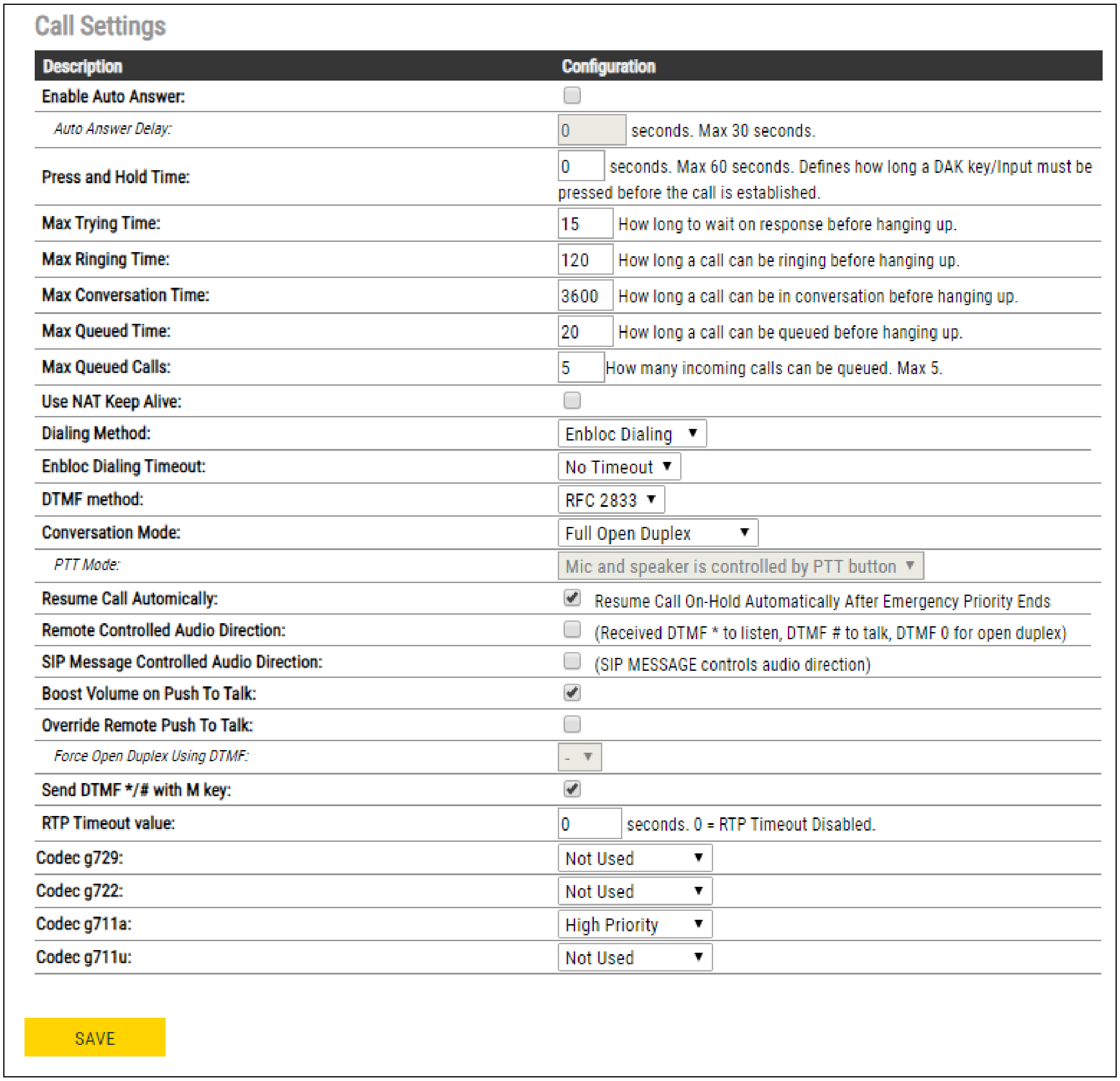
6.1. SIP Configuration

Click on **SIP Configuration → SIP** and configure the following in the **Account Settings** section:

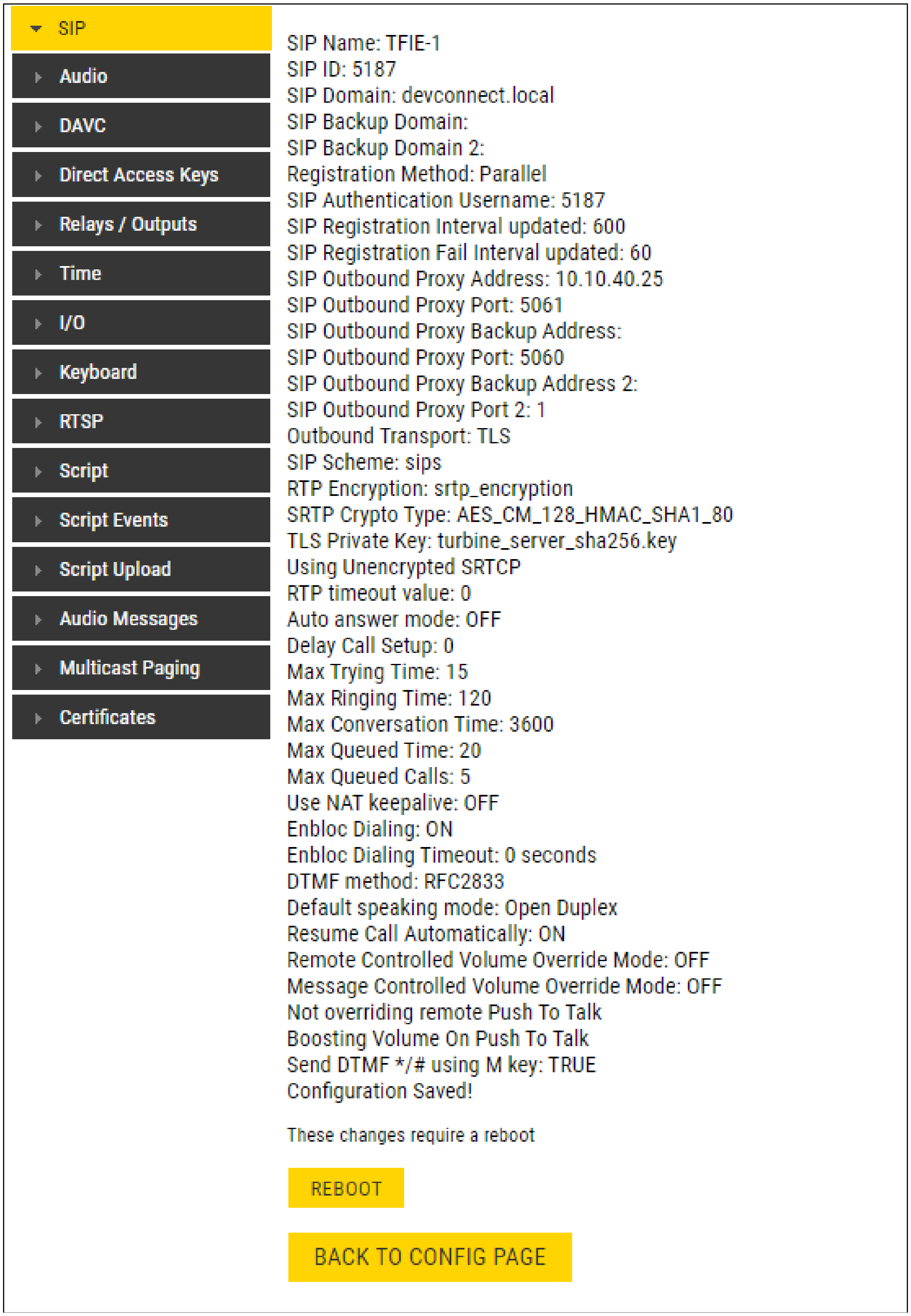
- **Name**: Enter the desired name.
- **Number (SIP ID)**: Enter a user extension administered from **Section 5.3**.
- **Server Domain (SIP)**: Enter the Domain of IP Office.
- **Authentication User Name**: Enter a user extension administered from **Section 5.3**.
- **Authentication Password**: Enter the **Login Code** from **Section 5.3**.
- **Outbound Proxy (optional)**: Enter the IP address of IP Office and **5061** as the **Port**.
- **Outbound Transport:** Set this to **TLS** to allow for secure transport and secure media SRTP.
- **SIP Scheme:** Set this to **sips**, again for secure communications.
- **RTP Encryption:** Set this to **srtp_encryption** as this will ensure the media is secure.
- **SRTP Crypto Type:** If SRTP is being used, an encryption method must be also set and **AES_CM_128_HMAC_SHA1_80** is being used on IP Office so this must be used here also to match that set in **Section 5.2.4**.
- **Use Unencrypted SRTCP:** This must match that configured on IP Office in **Section 5.2.4**, in this case it was left unencrypted so ticked.
- **TLS Private Key:** This is a private key that was installed with this system.



In the **Call Settings** section, configure as required the **DTMF method** as **RFC 2833** or whatever is set on IP Office. Configure other options as required. Click **SAVE** when done and a screen will appear (shown on the next page) to confirm the setting. The **Codec** is also set here, with **g711a** being used in the example below.

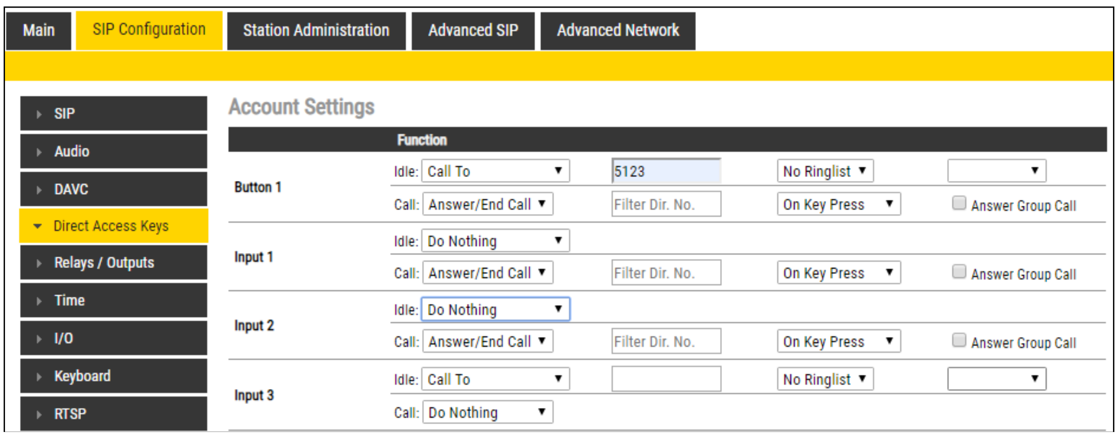


At this point the phone needs to be rebooted in order to save the SIP configuration, however this can be rebooted at a later stage should one wish to proceed with the configuration.



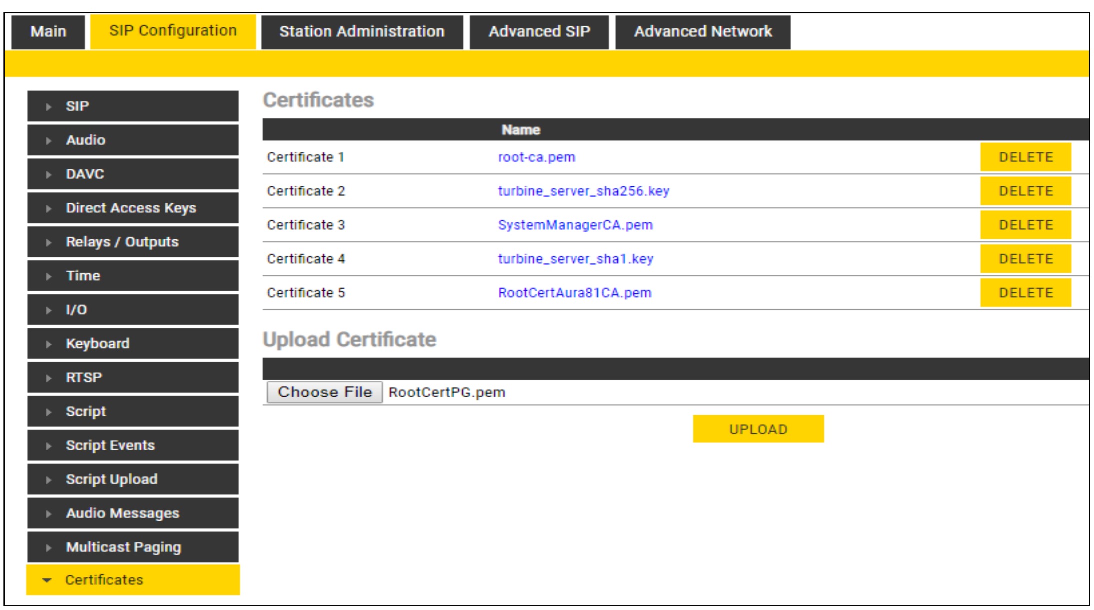
6.2. Configure Direct Access Keys

Click on the **Direct Access Keys** in the left window, this will bring up the functions as shown below where an extension to call can be assigned to the call button of the Turbine Intercom. This extension was an Avaya telephone, so when the button is pressed this telephone is called. Select **Button 1** to configure it. In the **Idle** field, select **Call To** from the drop down and enter the extension to be called when the button key is pushed. In the **Call** field, select **Answer/End Call** and **On Key Press**. This can be changed to use Hold or Transfer and other call features should they be required.



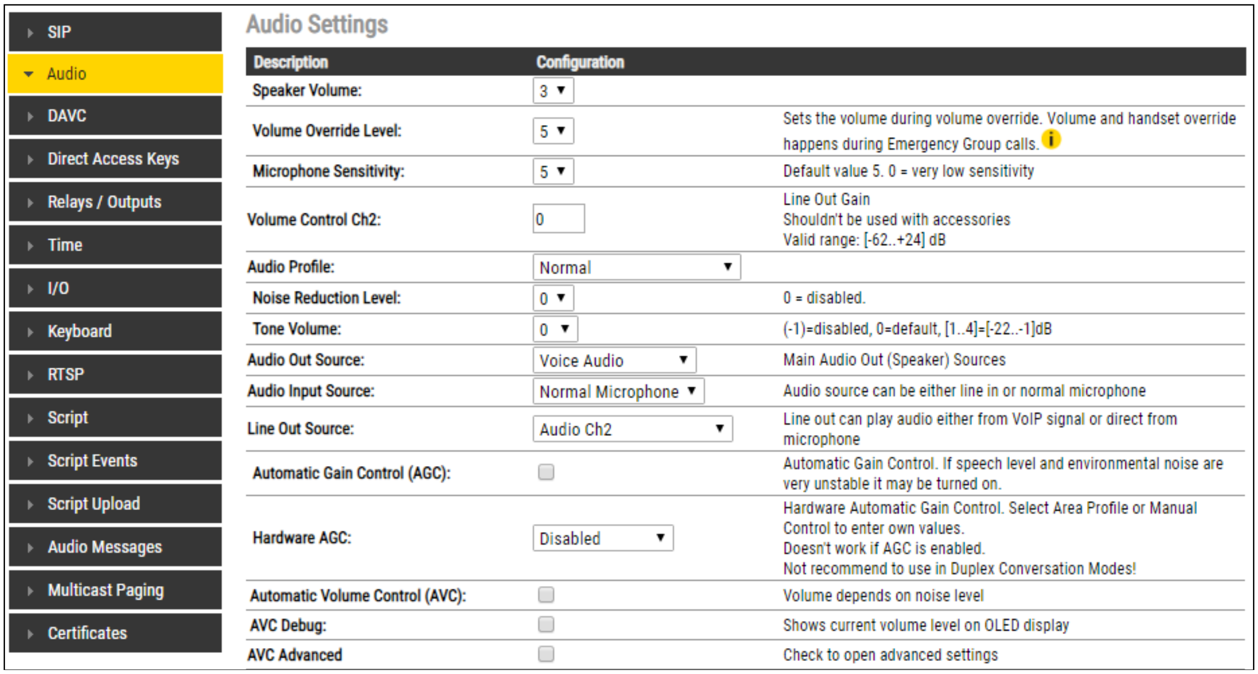
6.3. Configure Certificates

For TLS and SRTP to work the correct Root Certificate must be uploaded on to the Turbine IP Intercom. From the left-hand menu select **Certificates**. The Turbine certificates are listed. Click on **Choose File** and browse to the location of the root certificate .pem file. When selected click on the **Upload** button. This Root Certificate will be provided by the telecoms administrator as this may be a 3rd party certificate and not the default root certificate on IP Office.

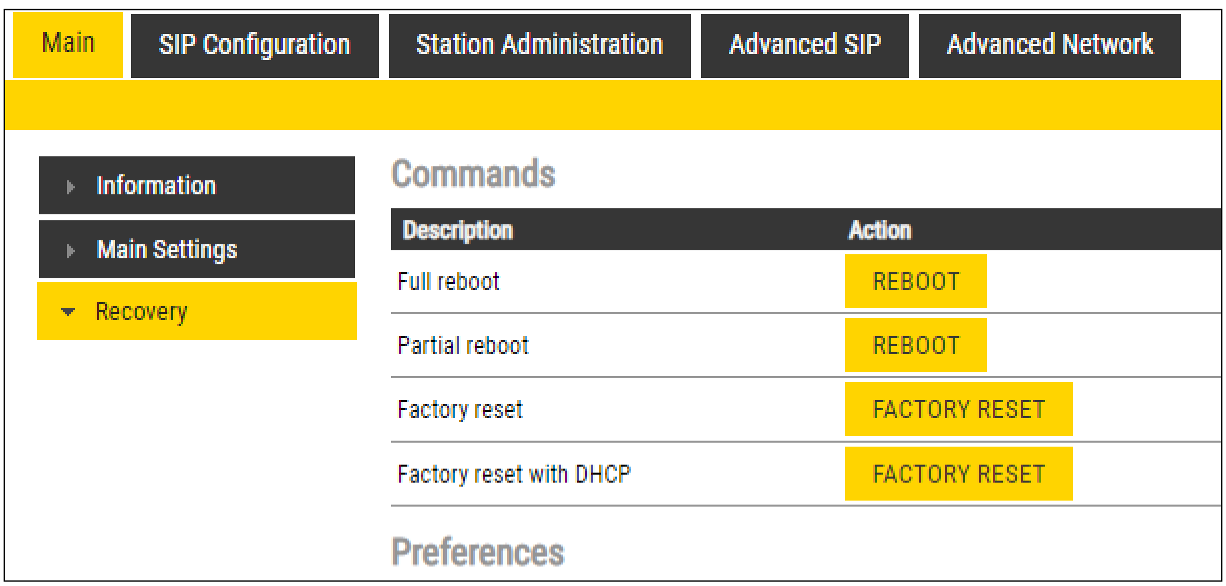


6.4. Configure Audio

Click on **Audio** in the left window, the volume of the speaker can be changed here.



If the phone was not rebooted earlier during the SIP configuration then click the **Main** tab and then click on **Recovery** as shown below. The telephone can be rebooted from this page.

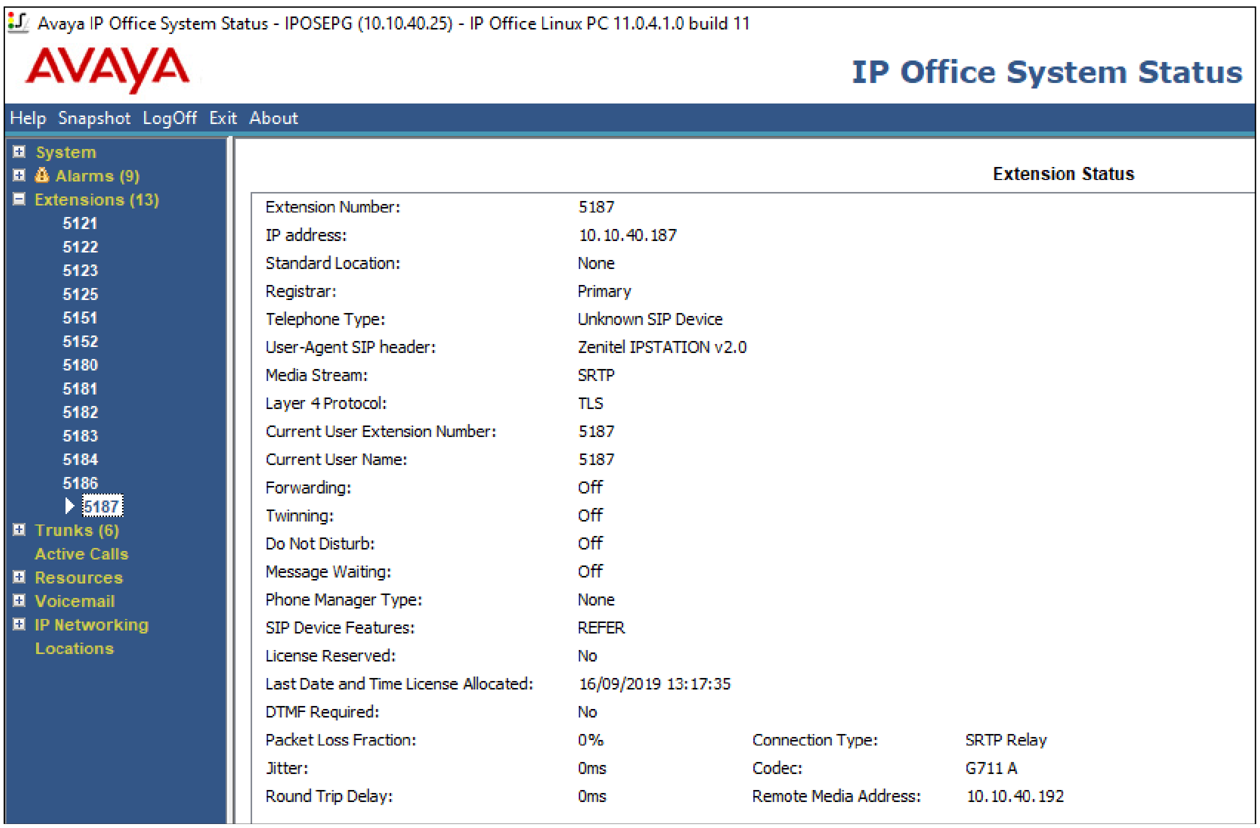


7. Verification Steps

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

7.1. Verify Avaya IP Office SIP Endpoint Registration

Open the IP Office System Status application and click on **Extensions**. If the Turbine extension is present in the list, it means it has registered correctly. Clicking on the extension will give further information on the connection as shown below. The **Layer 4 protocol** is shown to be **TLS** with **Media Stream** as **SRTP**.



Click on an Active Call from the left window (not shown) the main window shown below shows the details of the active call. Note the **Media Stream** is **SRTP** and the **Layer 4 Protocol** is **TLS**. The **Connection Type** here is shown as **SRTP Relay** meaning that the IP Office is being used to anchor the call.

Call Details

Call Ref: 100 Call length: 00:02:05

Originator

Current State:	Connected	Time in State:	00:02:02
Currently at:	Extn 5187, 5187		
Round Trip Delay:	0ms		
Receive Jitter:	2.4ms		
Receive Packet Loss Fraction:	0%		
Transmit Jitter:	0ms		
Transmit Packet Loss Fraction:	0%		
Dialed Digits:	5121		
Codec:	G711 A		
Media Stream:	SRTP		
Layer 4 Protocol:	TLS		

Destination

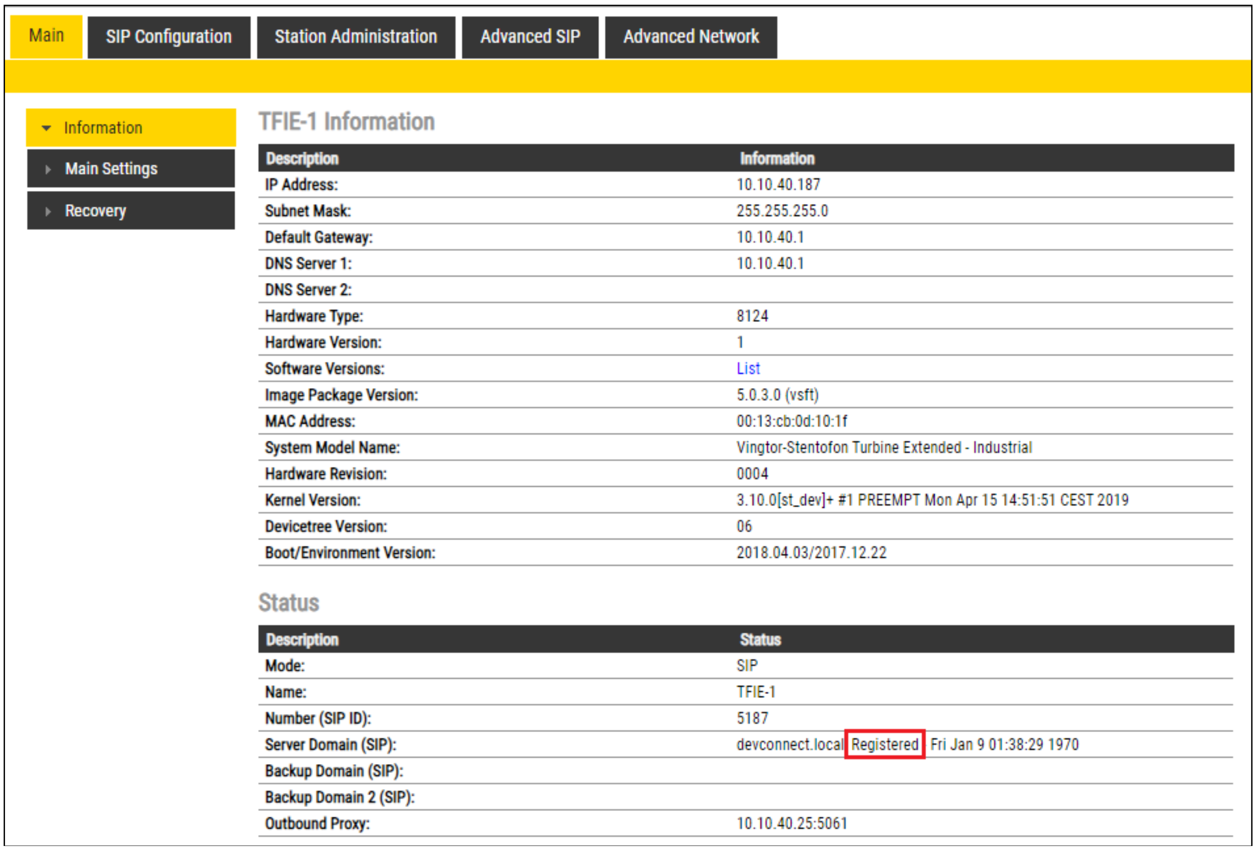
Current State:	Connected	Time in State:	00:02:02
Currently at:	Extn 5121, 5121		
Round Trip Delay:	6ms		
Receive Jitter:	0.1ms		
Receive Packet Loss Fraction:	0%		
Transmit Jitter:	10.6ms		
Transmit Packet Loss Fraction:	0%		
Codec:	G711 A		
Media Stream:	SRTP		
Layer 4 Protocol:	TLS		

Call target / Routing information

Original Target:	Extn 5121
Connection Type:	SRTP Relay
Call Recording:	No
Redirected to Twin:	No
Routed across SCN trunk:	No
Retargeting Count:	0

7.2. Verify Turbine SIP Registration

From the Turbine web interface, select **Information** from the left menu. Verify that the Registration state shows **Registered**. Place a call to another endpoint to verify basic call operation.



7.3. Verify Successful Calls

Place a call to and from the Turbine endpoint. Verify 2-way audio is heard and validate call terminates successfully.

8. Conclusion

These Application Notes describe the configuration steps required for configuring Zenitel Turbine to interoperate with Avaya IP Office using TLS. All feature and serviceability tests were completed successfully with all issues and observations outlined in **Section 2.2**.

9. Additional References

This section references the Avaya and Zenitel product documentation that are relevant to these Application Notes.

These documents form part of the Avaya official technical reference documentation suite. Further information may be obtained from *http://support.avaya.com* or from your Avaya representative.

[1] *Administering Avaya IP Office™ Platform with Manager*, Release 11.0 February 2019.

The Zenitel Turbine documentation can be found by contacting Zenitel at http://www.zenitel.com.

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.