



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Zenitel IP Operating Room Master with Avaya IP Office - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Zenitel IP Operating Room (OR) Master to interoperate with Avaya IP Office R11.0. The Zenitel IP OR Master is an IP Intercom for clean rooms that supports voice transmission using the Session Initiation Protocol (SIP).

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 IP Operating Room Master Station to interoperate with Avaya IP Office.

The Zenitel IP Operating Room (OR) Master Station is an intercom station intended for use in operating theatres and clean rooms. The station front plate is totally flat and without any holes to minimize bacteria accumulation. Chemical resistant and anti-bacterial front surface for easy cleaning. Four dynamic navigation keys and four speed dial keys for quick access to system menus and directory entries. With a large backlit display and Vingtor-Stentofon audio technology the station allows users to read caller ID, listen and talk at a distance.

The IP OR Master Station is registered with IP Office as a 3rd party SIP user/extension.

Note: The Zenitel IP Operating Room Master Station may be referred to as 'IP OR Master Station' or 'IP OR Master intercom phone' or 'IP OR Master unit' or 'IP OR Master' throughout this document but they all refer to the same thing.

2. General Test Approach and Test Results

The general test approach was to place calls to and from the IP OR Master intercom phone and exercise basic telephone operations. For serviceability testing, failures such as 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 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 IP OR Master Station did not include use of any specific encryption features as requested by Zenitel.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing was to verify that:

- IP OR Master successfully registers with IP Office using the UDP protocol.
- IP OR Master successfully establishes audio calls with good quality RTP audio to Avaya H.323, SIP and digital endpoints registered to IP Office.
- IP OR Master successfully establishes audio calls with a simulated PSTN.
- IP OR Master successfully negotiates the appropriate audio codec.
- DTMF tones could be passed successfully to energize relay on IP OR Master and switch audio direction.
- IP OR Master successfully calls multiple destinations using a hunt group.
- IP OR Master 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 IP OR Master to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to the devices and denying service on IP Office.

2.2. Test Results

All test cases passed successfully with the following exception and issues noted.

1. Call Park has a different meaning on the IP OR Master functionality than that of the Call Park feature on IP Office. When the Call Park function is used on IP OR Master it places multiple calls put 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 IP OR Master can be obtained through the following:

- **Phone:** +47 4000 2700
- **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 the IP OR Master with IP Office. The configuration consists of IP Office Server Edition and IP500V2 Expansion. IP Office has connections to Avaya H.323 and SIP deskphones as well as SIP registrations with IP OR Master. A SIP trunk connects IP Office to a simulated PSTN.

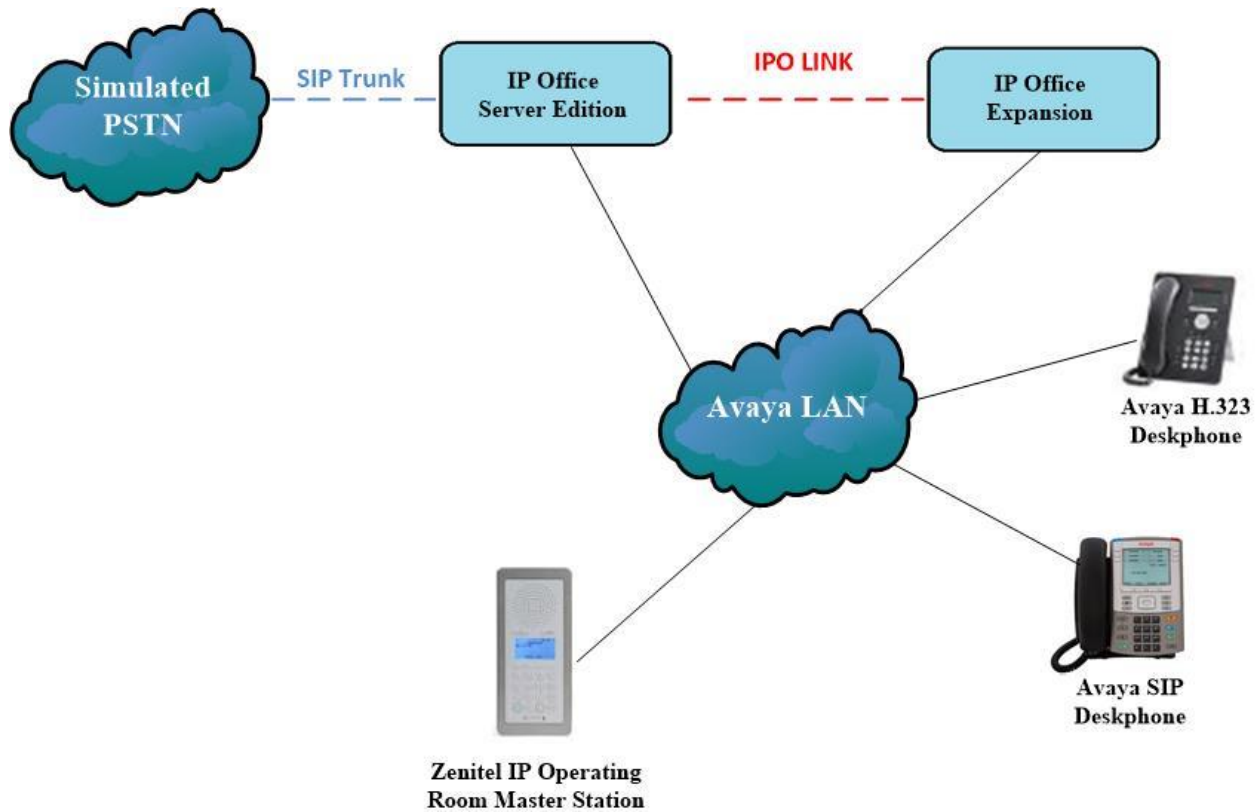


Figure 1: Avaya IP Office with Zenitel IP OR Master configuration

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 9408 Digital Deskphone	V 2.0
Zenitel IP Operating Room Master Station	02.10.3.0

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.

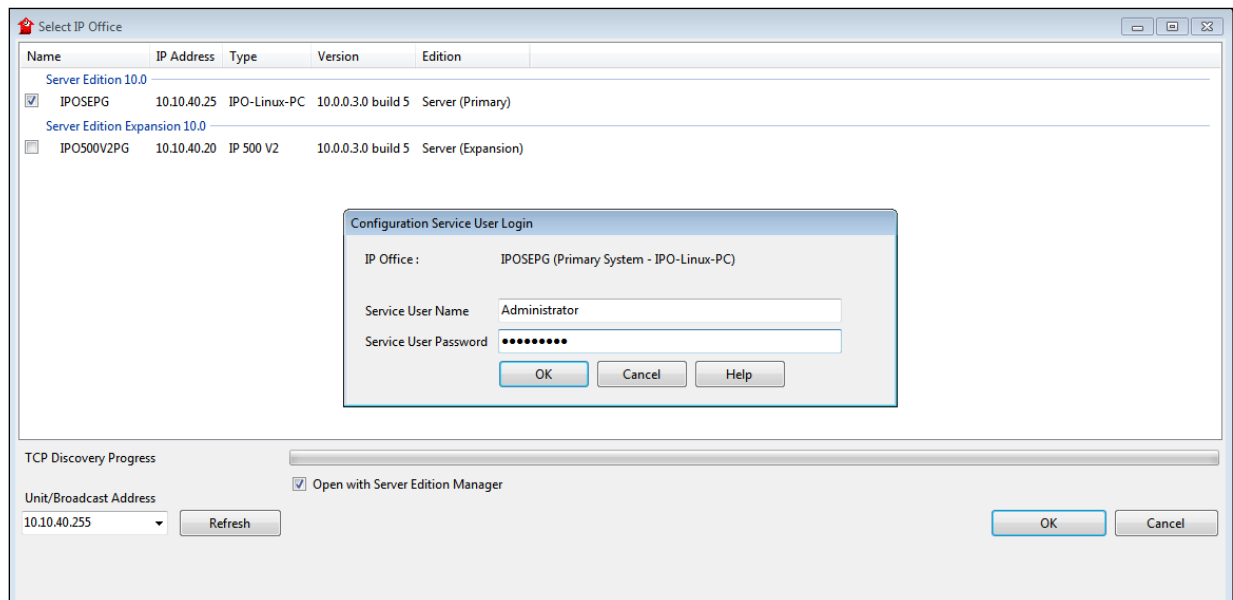
5. Avaya IP Office Configuration

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 IP OR Master 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 IP OR Master to 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 IP OR Master extensions 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.

Note: The Zenitel IP OR Master does not support TLS/SRTP and was configured using the system setting 'preferred' as this will allow for both secure and nonsecure connections.

5.2.1. LAN1 - LAN Settings configuration

For the IP OR Master 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.

The screenshot displays the IP Office configuration interface. On the left, a tree view shows the system hierarchy, with 'IPOSEPG' selected under 'System (1)'. The main panel on the right is titled 'IPOSEPG' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The configuration fields for LAN1 are as follows:

Field	Value
IP Address	10 . 10 . 40 . 25
IP Mask	255 . 255 . 255 . 0
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input checked="" type="radio"/> Disabled

An 'Advanced' button is located at the bottom right of the configuration area.

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**, **5060** and **5061** from the dropdown boxes, respectively. 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).

The screenshot shows the Avaya configuration interface for LAN1 VoIP settings. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. The left sidebar has tabs for LAN Settings, VoIP, and Network Topology. The main content area is divided into several sections:

- H323 Gatekeeper Enable**: ☒ H323 Gatekeeper Enable. Below it are ☐ Auto-create Extn, ☐ Auto-create User, and ☐ H323 Remote Extn Enable. H.323 Signalling over TLS is set to **Disabled** (dropdown), and Remote Call Signalling Port is **1720** (spinner).
- SIP Trunks Enable**: ☒ SIP Trunks Enable.
- SIP Registrar Enable**: ☒ SIP Registrar Enable. Below it are ☐ Auto-create Extn/User, ☐ SIP Remote Extn Enable, and Allowed SIP User Agents set to **Block blacklist only** (dropdown). SIP Domain Name is **devconnect.local** (text field). SIP Registrar FQDN is empty (text field).
- Layer 4 Protocol**: ☒ UDP, ☒ TCP, and ☒ TLS. UDP Port is **5060**, Remote UDP Port is **5060**. TCP Port is **5060**, Remote TCP Port is **5060**. TLS Port is **5061**, Remote TLS Port is **5061**.
- Challenge Expiry Time (secs)**: **7** (spinner).
- RTP**: Port Number Range (Minimum: **40750**, Maximum: **50750**) and Port Number Range (NAT) (Minimum: **40750**, Maximum: **50750**).

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.

The screenshot shows the VoIP configuration interface with the following settings:

- System** tab selected, **VoIP** sub-tab selected.
- Ignore DTMF Mismatch For Phones**: ☒
- Allow Direct Media Within NAT Location**: ☐
- RFC2833 Default Payload**: 101
- Available Codecs**:
 - ☒ G.711 ULAW 64K
 - ☒ G.711 ALAW 64K
 - ☒ G.722 64K
 - ☒ G.729(a) 8K CS-ACELP
- Default Codec Selection**:
 - Unused**: (Empty)
 - Selected**:
 - G.711 ALAW 64K
 - G.729(a) 8K CS-ACELP
 - G.711 ULAW 64K
 - G.722 64K

5.2.4. VoIP – VoIP Security configuration

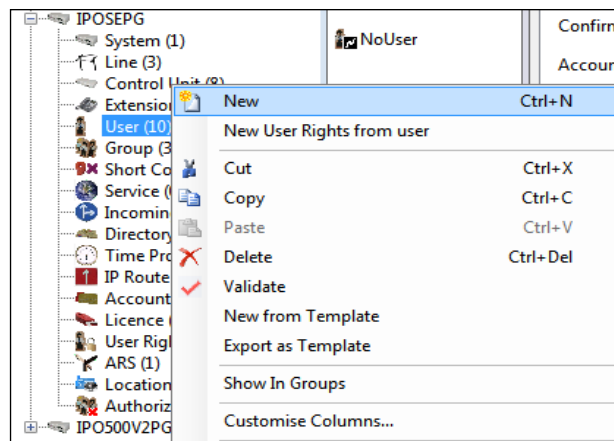
Media Security was set to **Preferred** with **RTP Encryption** and **RTP Authentication** ticked. RTCP was not encrypted for compliance testing and for simplicity during testing only one **Crypto** was chosen that being **SRTP_AES_CM_128_SHA1_80**.

The screenshot shows the VoIP Security configuration interface with the following settings:

- System** tab selected, **VoIP Security** sub-tab selected.
- Default Extension Password**: (Empty)
- Confirm Default Extension Password**: (Empty)
- Media Security**: Preferred
- Strict SIPS**: ☐
- Media Security Options**:
 - Encryptions**:
 - ☒ RTP
 - ☐ RTCP
 - Authentication**:
 - ☒ RTP
 - ☒ RTCP
 - Replay Protection**: (Empty)
 - SRTP Window Size**: 64
 - Crypto Suites**:
 - ☒ SRTP_AES_CM_128_SHA1_80
 - ☐ SRTP_AES_CM_128_SHA1_32

5.3. Create a SIP User/Extension for the IP OR Master Station

The IP OR Master 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 IP OR Master user. Note the password will be required again in **Section 6.1**.

5184: 5184*							
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In
Name	5184						
Password	••••						
Confirm Password	••••						
Unique Identity							
Audio Conference PIN							
Confirm Audio Conference PIN							
Account Status	Enabled ▼						
Full Name	Zenitel DoorPhone						
Extension	5184						
Email Address							
Locale	▼						
Priority	5 ▼						
System Phone Rights	None ▼						
Profile	Basic 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.

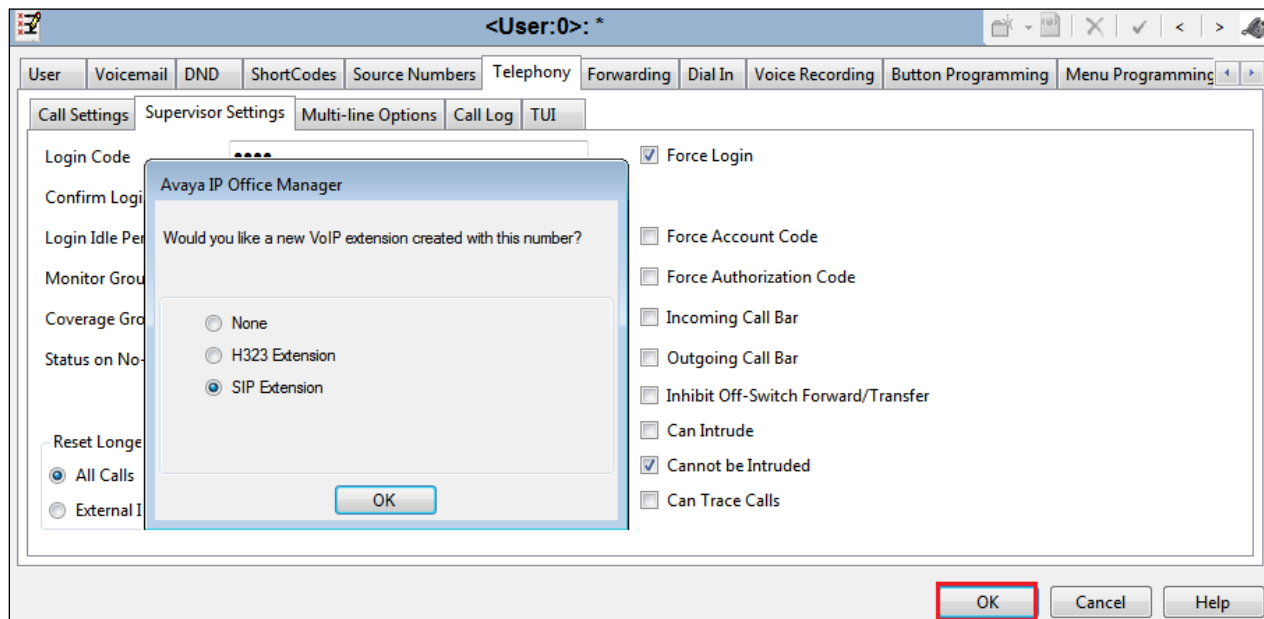
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Voicemail Code	<input type="text"/>							<input type="checkbox"/> Voicemail On	
Confirm Voicemail Code	<input type="text"/>							<input type="checkbox"/> Voicemail Help	
Voicemail Email	<input type="text"/>							<input type="checkbox"/> Voicemail Ringback	
								<input type="checkbox"/> Voicemail Email Reading	
								<input type="checkbox"/> UMS Web Services	
								<input type="checkbox"/> Enable GMAIL API	
Voicemail Email <input checked="" type="radio"/> Off <input type="radio"/> Copy <input type="radio"/> Forward <input type="radio"/> Alert									
DTMF Breakout Reception / Breakout (DTMF 0) <input type="text" value="System Default ()"/>									
Breakout (DTMF 2) <input type="text" value="System Default ()"/>									
Breakout (DTMF 3) <input type="text" value="System Default ()"/>									

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 user as stated in **Section 6.1**.

User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording
Call Settings Supervisor Settings Multi-line Options Call Log TUI								
Login Code	<input type="text" value="••••"/>							<input type="checkbox"/> Force Login
Confirm Login Code	<input type="text" value="••••"/>							
Login Idle Period (secs)	<input type="text"/>							<input type="checkbox"/> Force Account Code
Monitor Group	<input type="text" value="<None>"/>							<input type="checkbox"/> Force Authorization Code
Coverage Group	<input type="text" value="<None>"/>							<input type="checkbox"/> Incoming Call Bar
Status on No-Answer	<input type="text" value="Logged On (No change)"/>							<input type="checkbox"/> Outgoing Call Bar
								<input type="checkbox"/> Inhibit Off-Switch Forward/Transfer
Privacy Override Group	<input type="text" value="<None>"/>							<input type="checkbox"/> Can Intrude
Reset Longest Idle Time <input checked="" type="radio"/> All Calls <input type="radio"/> External Incoming								<input checked="" type="checkbox"/> Cannot be Intruded
								<input type="checkbox"/> Can Trace Calls
								<input type="checkbox"/> Deny Auto Intercom Calls

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.

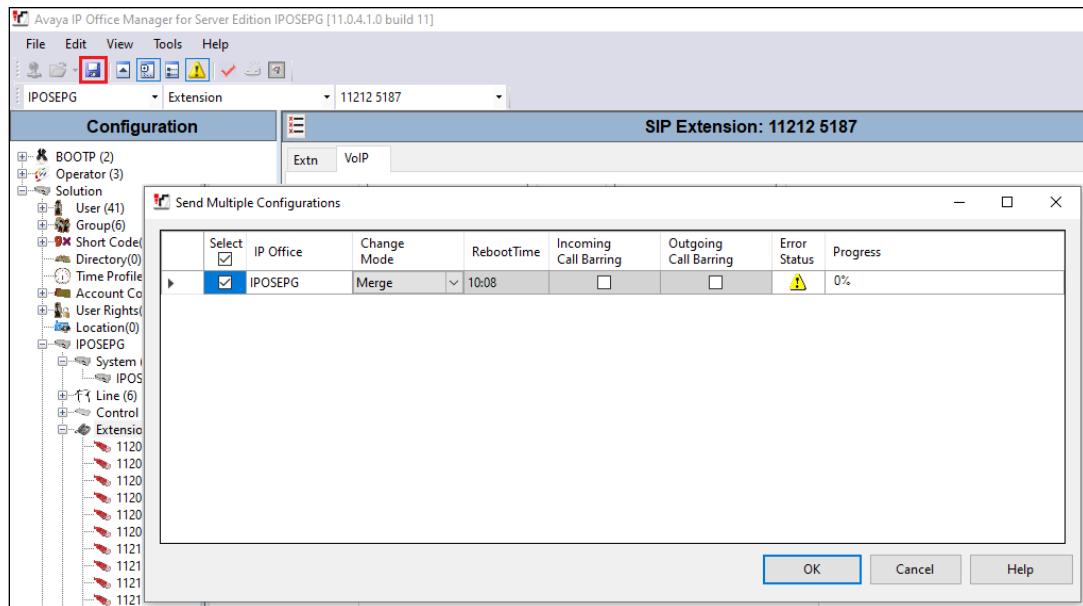
Media Security is set to **Same As System** for all IP OR Master extensions that are configured. This will allow for both secure and nonsecure media connections and will allow the IP OR Master to use UDP and RTP for the call and call setup. The **Advanced Media Security Options** were left the **Same As System** as well.

The screenshot displays the configuration interface for a SIP extension. On the left, a tree view under 'Configuration' shows the hierarchy: BOOTP (2), Operator (3), Solution, User (41), Group (6), Short Code (63), Directory (0), Time Profile (0), Account Code (1), User Rights (15), Location (0), IPOSEPG, System (1), IPOSEPG, Line (6), Control Unit (9), and Extension (18). The 'Extension (18)' list includes numbers from 11202 5120 to 11207 5183, with 11208 5184 highlighted in blue. The main panel is titled 'SIP Extension: 11208 5184' and has two tabs: 'Extn' and 'VoIP'. The 'VoIP' tab is active, showing various settings. The 'IP Address' field is set to '0 . 0 . 0 . 0'. The 'Codec Selection' section features a dropdown menu set to 'System Default', with 'Unused' and 'Selected' lists. The 'Selected' list contains: G.711 ALAW 64K, G.729(a) 8K CS-ACELP, G.711 ULAW 64K, and G.722 64K. To the right of the codec lists are checkboxes for 'Requires DTMF', 'Local Hold Music', 'Re-invite Supported', 'Codec Lockdown', and 'Allow Direct Media Path' (which is checked). Below these are dropdown menus for 'Reserve Licence' (None), 'Fax Transport Support' (None), 'DTMF Support' (RFC2833/RFC4733), and '3rd Party Auto Answer' (None). The 'Media Security' dropdown is set to 'Same as System (Preferred)'. At the bottom, the 'Advanced Media Security Options' section has a checkbox for 'Same As System' which is checked.

Configuration	SIP Extension: 11208 5184
Configuration	Extn VoIP
BOOTP (2)	IP Address: 0 . 0 . 0 . 0
Operator (3)	Codec Selection: System Default
Solution	Unused: [Empty]
User (41)	Selected: G.711 ALAW 64K, G.729(a) 8K CS-ACELP, G.711 ULAW 64K, G.722 64K
Group (6)	Requires DTMF: <input type="checkbox"/>
Short Code (63)	Local Hold Music: <input type="checkbox"/>
Directory (0)	Re-invite Supported: <input checked="" type="checkbox"/>
Time Profile (0)	Codec Lockdown: <input type="checkbox"/>
Account Code (1)	Allow Direct Media Path: <input checked="" type="checkbox"/>
User Rights (15)	Reserve Licence: None
Location (0)	Fax Transport Support: None
IPOSEPG	DTMF Support: RFC2833/RFC4733
System (1)	3rd Party Auto Answer: None
IPOSEPG	Media Security: Same as System (Preferred)
Line (6)	Advanced Media Security Options: <input checked="" type="checkbox"/> Same As System
Control Unit (9)	
Extension (18)	
11202 5120	
11200 5121	
11201 5122	
11203 5123	
11204 5124	
11205 5125	
11210 5126	
11216 5150	
11215 5151	
11217 5152	
11213 5180	
11214 5181	
11206 5182	
11207 5183	
11208 5184	

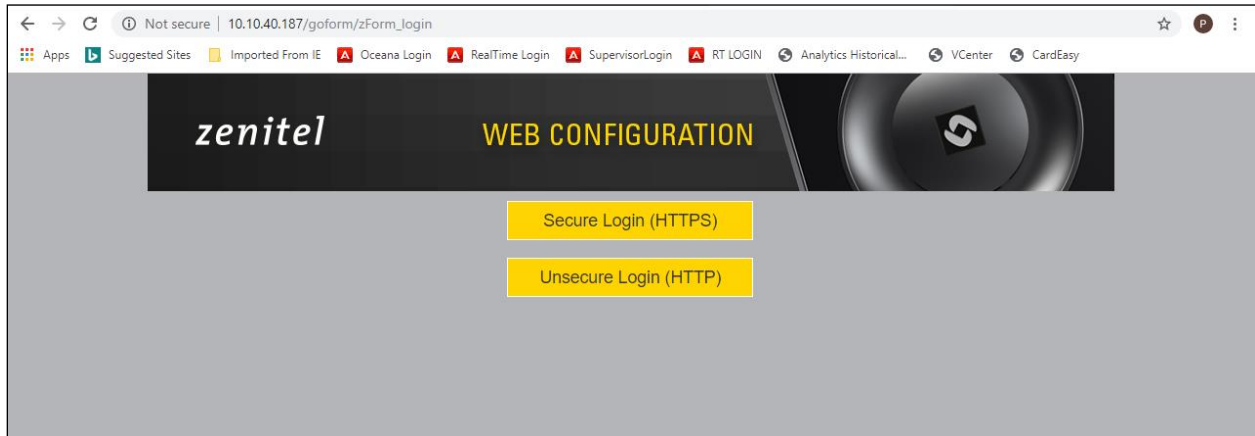
5.5. Save Configuration

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**.

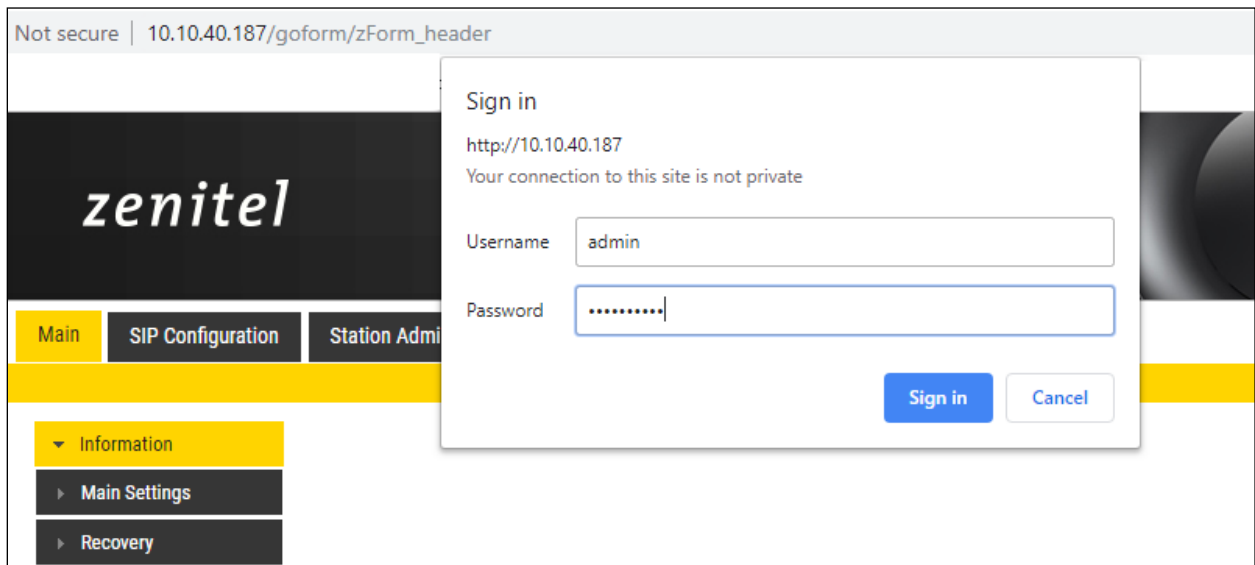


6. Configure Zenitel IP Operating Room Master

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



Log in with the appropriate credentials.



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

- SIP Configuration
- Direct Access Keys
- Audio



The screenshot displays the Zenitel Web Configuration interface. The top navigation bar includes 'Main', 'SIP Configuration', 'Station Administration', 'Advanced SIP', and 'Advanced Network'. The left sidebar shows 'Information' expanded with 'Main Settings' and 'Recovery' options. The main content area is divided into two sections: 'INCA Information' and 'Status'.

INCA Information

Description	Information
IP Address:	10.10.40.222
Subnet Mask:	255.255.255.0
Default Gateway:	10.10.40.1
DNS Server 1:	10.10.40.1
DNS Server 2:	
Hardware Type:	8023
Hardware Version:	5
Software Version:	02.10.3.0
MAC Address:	00:13:cb:04:6e:c6

Status

Description	Status
Mode:	SIP
Name:	IPOSE
Number (SIP ID):	5184
Server Domain (SIP):	devconnect.local, Registered - Sun Jan 16 00:17:37 2000
Backup Domain (SIP):	
Backup Domain 2 (SIP):	
Outbound Proxy:	10.10.40.25

6.1. SIP Configuration

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

- **Display name:** Enter the desired name.
- **Directory Number (SIP ID):** Enter a user extension administered from **Section 5.3**.
- **Server Domain (SIP):** Enter the Domain of IP Office from **Section 5.2.2**.
- **Authentication User Name:** Enter a user extension administered from **Section 5.3**.
- **Authentication Password:** Enter the **Communication Profile Password** from **Section 5.3**.
- **Outbound Proxy (optional):** Enter the IP address of IP Office and **5060** as the **Port**.

Main	SIP Configuration	Station Administration	Advanced SIP	Advanced Network
Account Settings				
SIP		Configuration		
▶ Audio		Name: IPOSE		
▶ DAVC		Number (SIP ID): 5184		
▶ Direct Access Keys		Server Domain (SIP): devconnect.local		
▶ Relays / Outputs		Backup Domain (SIP):		
▶ Time		Backup Domain 2 (SIP):		
▶ RTSP		Registration Method: Parallel ▼		
▶ Multicast Paging		Authentication User Name: 5184		
▶ Language		Authentication Password: ****		
▶ Certificates		Register Interval: 600 (min. 60 seconds)		
		Register Failure Interval: 60 (min. 5 seconds)		
		Restart If Not Registered: Do Not Restart ▼		
		Outbound Proxy [optional]: 10.10.40.25 Port: 5060		
		Outbound Backup Proxy [optional]: Port: 5060		
		Outbound Backup Proxy 2 [optional]: Port: 5060		

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 G.711A being used in the example below.

Call Settings

Description	Configuration
Enable Auto Answer:	<input type="checkbox"/>
Auto Answer Delay:	0 seconds. Max 30 seconds.
Press and Hold Time:	0 seconds. Max 60 seconds. Defines how long a DAK key/Input must be pressed before the call is established.
Max Trying Time:	15 How long to wait on response before hanging up.
Max Ringing Time:	120 How long a call can be ringing before hanging up.
Max Conversation Time:	3600 How long a call can be in conversation before hanging up.
Max Queued Time:	20 How long a call can be queued before hanging up.
Max Queued Calls:	5 How many incoming calls can be queued. Max 5.
Use NAT Keep Alive:	<input type="checkbox"/>
Dialing Method:	Enbloc Dialing ▼
Enbloc Dialing Timeout:	No Timeout ▼
DTMF method:	RFC 2833 ▼
Conversation Mode:	Open Duplex ▼
Resume Call Automatically:	<input checked="" type="checkbox"/> Resume Call On-Hold Automatically After Emergency Priority Ends
Remote Controlled Audio Direction:	<input type="checkbox"/> (Received DTMF * to listen, DTMF # to talk, DTMF 0 for open duplex)
SIP Message Controlled Audio Direction:	<input type="checkbox"/> (SIP MESSAGE controls audio direction)
Send DTMF */# with M key:	<input checked="" type="checkbox"/>
Call LED off during ringing:	<input type="checkbox"/>
RTP Timeout value:	0 seconds. 0 = RTP Timeout Disabled.
Codec g729:	Not Used ▼
Codec g722:	Not Used ▼
Codec g711a:	High Priority ▼
Codec g711u:	Not Used ▼

SAVE

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.

▼ SIP	SIP Name: IPOSE
▶ Audio	SIP ID: 5184
▶ DAVC	SIP Domain: devconnect.local
▶ Direct Access Keys	SIP Backup Domain:
▶ Relays / Outputs	SIP Backup Domain 2:
▶ Time	Registration Method: Parallel
▶ RTSP	SIP Authentication Username: 5184
▶ Multicast Paging	SIP Registration Interval updated: 600
▶ Language	SIP Registration Fail Interval updated: 60
▶ Certificates	Restart On Not Registered: 0
	SIP Outbound Proxy Address: 10.10.40.25
	SIP Outbound Proxy Port: 5060
	SIP Outbound Proxy Backup Address:
	SIP Outbound Proxy Port: 5060
	SIP Outbound Proxy Backup Address 2:
	SIP Outbound Proxy Port 2: 5060
	Not using Unencrypted SRTP
	RTP timeout value: 0
	Auto answer mode: OFF
	Delay Call Setup: 0
	Max Trying Time: 15
	Max Ringing Time: 120
	Max Conversation Time: 3600
	Max Queued Time: 20
	Max Queued Calls: 5
	Use NAT keepalive: OFF
	Enbloc Dialing: ON
	Enbloc Dialing Timeout: 0 seconds
	DTMF method: RFC2833
	Default speaking mode: Full Open Duplex
	Resume Call Automatically: ON
	Remote Controlled Volume Override Mode: OFF
	Message Controlled Volume Override Mode: OFF
	Call LED off during ringing: FALSE
	Send DTMF */# using M key: TRUE
	Configuration Saved!
	These changes require a reboot
	REBOOT
	BACK TO CONFIG PAGE

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 IP OR Master. This phone has four buttons that can be assigned. The first button was assigned the Ringlist which contains the three numbers **5122**, **5250** and **5201** which will call these numbers in this order when pressed. Select **Button 1** to configure it. In the **Idle** field, select **Call To** from the drop down and enter the extension or **Ringlist** 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 such as **DTMF** as shown below.

> SIP

> Audio

> DAVC

> Direct Access Keys

> Relays / Outputs

> Time

> RTSP

> Multicast Paging

> Language

> Certificates

Account Settings

	Function			
Button 1	Idle: Call To		Ringlist 1	
	Call: Answer/End Call	Filter Dir. No.	On Key Press	<input type="checkbox"/> Answer Group Call
Button 2	Idle: Call To	5201	No Ringlist	
	Call: Transfer Call	81000		
Button 3	Idle: Call To	5151	No Ringlist	
	Call: Send DTMF	DTMF 5	DTMF 0	
Button 4	Idle: Call To	5122	No Ringlist	
	Call: Hold Call	Filter Dir. No.		
Input 1	Idle: Call To		No Ringlist	
	Call: Do Nothing			
Input 2	Idle: Call To		No Ringlist	
	Call: Do Nothing			
Input 3	Idle: Call To		No Ringlist	
	Call: Do Nothing			

SAVE

Ringlist Settings

	Ringlist 1	With Previous	Ringlist 2	With Previous	Ringlist 3	With Previous
Value 1	5122	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>
Value 2	5250	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>
Value 3	5201	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>
Value 4		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>

6.3. Configure Audio

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

▶ SIP	Audio Settings	
▼ Audio	Description	Configuration
▶ DAVC	Speaker Volume:	3 ▼
▶ Direct Access Keys	Volume Override Level:	5 ▼ <small>Sets the volume during volume override. Volume and handset override happens during Emergency Group calls. ⓘ</small>
▶ Relays / Outputs	Microphone Sensitivity:	5 ▼ <small>Default value 5. 0 = very low sensitivity</small>
▶ Time	Volume Control Ch2:	0 <small>Line Out Gain Shouldn't be used with accessories Valid range: [-62..+24] dB</small>
▶ I/O	Audio Profile:	Normal ▼
▶ Keyboard	Noise Reduction Level:	0 ▼ <small>0 = disabled.</small>
▶ RTSP	Tone Volume:	0 ▼ <small>(-1)=disabled, 0=default, [1..4]=[-22..-1]dB</small>
▶ Script	Audio Out Source:	Voice Audio ▼ <small>Main Audio Out (Speaker) Sources</small>
▶ Script Events	Audio Input Source:	Normal Microphone ▼ <small>Audio source can be either line in or normal microphone</small>
▶ Script Upload	Line Out Source:	Audio Ch2 ▼ <small>Line out can play audio either from VoIP signal or direct from microphone</small>
▶ Audio Messages	Automatic Gain Control (AGC):	<input type="checkbox"/> <small>Automatic Gain Control. If speech level and environmental noise are very unstable it may be turned on.</small>
▶ Multicast Paging	Hardware AGC:	Disabled ▼ <small>Hardware Automatic Gain Control. Select Area Profile or Manual Control to enter own values. Doesn't work if AGC is enabled. Not recommend to use in Duplex Conversation Modes!</small>
▶ Certificates	Automatic Volume Control (AVC):	<input type="checkbox"/> <small>Volume depends on noise level</small>
	AVC Debug:	<input type="checkbox"/> <small>Shows current volume level on OLED display</small>
	AVC Advanced	<input type="checkbox"/> <small>Check to open advanced settings</small>

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

Main	SIP Configuration	Station Administration	Advanced SIP	Advanced Network
▶ Information	Commands			
▶ Main Settings	Description			
▼ Recovery	Action			
	Full reboot	REBOOT		
	Partial reboot	REBOOT		
	Factory reset	FACTORY RESET		
	Factory reset with DHCP	FACTORY RESET		
	Preferences			

7. Verification Steps

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

7.1. Verify Avaya IP Office SIP Endpoint Registration

Open the IP Office System Status application and click on **Extensions**. If the IP OR Master 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 **UDP**.

The screenshot displays the Avaya IP Office System Status application interface. The title bar indicates the system is running on IPOSEPG (10.10.40.25) and is an IP Office Linux PC 11.0.4.1.0 build 11. The main window has a menu bar with 'Help', 'Snapshot', 'LogOff', 'Exit', and 'About'. A left-hand navigation pane lists various system components: System, Alarms (9), Extensions (13), Trunks (6), Active Calls, Resources, Voicemail, IP Networking, and Locations. The 'Extensions (13)' section is expanded, and extension 5184 is selected. The main area shows the 'Extension Status' for 5184, listing various parameters and their values.

Extension Status	
Extension Number:	5184
IP address:	10.10.40.222
Standard Location:	None
Registrar:	Primary
Telephone Type:	Unknown SIP Device
User-Agent SIP header:	Zenitel IPSTATION v2.0
Media Stream:	Best Effort
Layer 4 Protocol:	UDP
Current User Extension Number:	5184
Current User Name:	5184
Forwarding:	Off
Twinning:	Off
Do Not Disturb:	Off
Message Waiting:	On
Phone Manager Type:	None
SIP Device Features:	REFER
License Reserved:	No
Last Date and Time License Allocated:	16/09/2019 13:18:05
DTMF Required:	No
Packet Loss Fraction:	
Jitter:	
Round Trip Delay:	
Connection Type:	
Codec:	
Remote Media Address:	

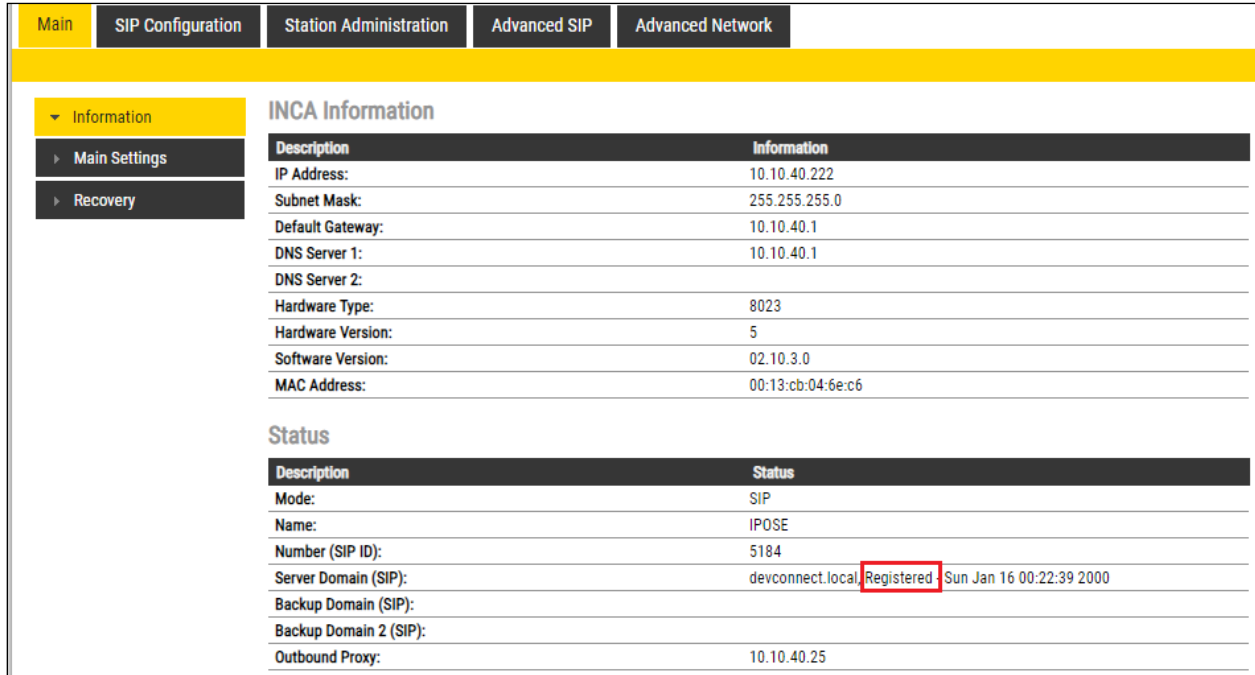
Click on an Active Call from the left window (not shown) the main window shown below shows the details of the active call. Note the **Media Stream** is **RTP** and the **Layer 4 Protocol** is **UDP**. The **Connection Type** is **Direct Media** as this was ticked in **Section 5.4**.

Call Details

Call Ref: 101	Call length: 00:00:15	
Originator		
Current State:	Connected	Time in State: 00:00:14
Currently at:	Extn 5184, 5184	
Receive Jitter:	0ms	
Receive Packet Loss Fraction:	0%	
Dialed Digits:	5122	
Codec:	G711 A	
Media Stream:	RTP	
Layer 4 Protocol:	UDP	
Destination		
Current State:	Connected	Time in State: 00:00:14
Currently at:	Extn 5122, 5122	
Receive Jitter:	0ms	
Receive Packet Loss Fraction:	0%	
Codec:	G711 A	
Media Stream:	RTP	
Layer 4 Protocol:	TLS	
Call target / Routing information		
Original Target:	Extn 5122	
Connection Type:	Direct Media	
Call Recording:	No	
Redirected to Twin:	No	
Routed across SCN trunk:	No	
Retargeting Count:	0	

7.2. Verify IP OR Master SIP Registration

From the IP OR Master 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.



The screenshot displays the IP OR Master web interface. At the top, there is a navigation bar with tabs: Main, SIP Configuration, Station Administration, Advanced SIP, and Advanced Network. The 'Main' tab is selected. On the left side, there is a sidebar menu with options: Information (selected), Main Settings, and Recovery. The main content area is titled 'INCA Information' and contains two tables. The first table, 'INCA Information', lists various system details. The second table, 'Status', shows the current state of the system, including the registration status, which is 'Registered' and highlighted with a red box.

Description	Information
IP Address:	10.10.40.222
Subnet Mask:	255.255.255.0
Default Gateway:	10.10.40.1
DNS Server 1:	10.10.40.1
DNS Server 2:	
Hardware Type:	8023
Hardware Version:	5
Software Version:	02.10.3.0
MAC Address:	00:13:cb:04:6e:c6

Description	Status
Mode:	SIP
Name:	IPOSE
Number (SIP ID):	5184
Server Domain (SIP):	devconnect.local Registered Sun Jan 16 00:22:39 2000
Backup Domain (SIP):	
Backup Domain 2 (SIP):	
Outbound Proxy:	10.10.40.25

7.3. Verify Successful Calls

Place a call to and from the IP OR Master. Verify 2-way audio is heard and validate call terminates successfully.

8. Conclusion

These Application Notes describe the configuration steps required for configuring Zenitel IP OR Master to interoperate with Avaya IP Office. All feature and serviceability tests were completed successfully with any 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 IP OR Master documentation can be found at <http://www.zenitel.com>

©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.