



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

---

# **Application Notes for Configuring Panasonic KX-TGP600 Base Station with TPA65 and TPA68 DECT Wireless Desk Phones and Repeater KX-A406 with Avaya IP Office Server Edition Release 11.0 - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for provisioning the Panasonic KX-TGP600 Base Station with TPA65 and TPA68 DECT Wireless Desk Phones and Repeater KX-A406 to interoperate with Avaya IP Office Server Edition Release 11.0.

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 steps required to integrate Panasonic KX-TGP600 Base Station with KX-UDT131DECT Handset and Repeater KX-A406 with Avaya IP Office Server Edition.

The KX-TGP600 is a SIP Cordless phone, which consists of a base unit, a cordless handset TPA60 and wireless desk phones TPA65 and TPA68. The handset is the same as the KX-TPA60 or KX-UDT131/KX-UDT121 and the desk phone are the same as the KX-TPA65 and KX-TPA68. It can be expandable up to 8 cordless headsets and desk phones in total, therefore it can have 8 simultaneous calls if using Narrowband mode or 4 simultaneous calls if using Wideband mode.

In the compliance testing, Avaya IP Office Server Edition system consists of Avaya IP Office Primary Linux running on Virtualized Environment and a 500V2 Expansion.

# 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the TGP600 SIP cordless phone and Avaya SIP, H.323, and digital stations and exercising common telephony features, such as hold, transfer, and conference.

The serviceability testing focused on verifying that the TGP600 SIP Phone comes back into service after re-connecting the Ethernet connection or rebooting the PC on which the TGP600 SIP phone is running.

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 only (private network side). 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 Panasonic TGP600 SIP cordless phone did not include use of any specific encryption features as requested by Panasonic.

## **2.1. Interoperability Compliance Testing**

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP phones, H.323 phones, Digital phones and PSTN endpoints.

- Successful registration of the TGP600 SIP cordless phone with IP Office
- Calls between the TGP600 and its wireless desk phones and Avaya SIP, H.323, and digital stations.
- G.711 codec support.
- Caller ID display on Avaya and Panasonic headset or desk phone.
- Proper recognition of DTMF tones.
- Basic telephony features including Hold, Mute, Transfer, and Conference.
- Proper system recovery after a restart of the TGP600 SIP cordless phone and loss of IP connectivity.

## 2.2. Test Results

All test cases passed successfully.

## 2.3. Support

For technical support on the TGP600 SIP Cordless Phone and TPA65 and TPA68 DECT Wireless Desk Phones, contact Panasonic Support via phone, email, or website.

- Phone: +1 (800) 225-5329
- Web: <https://panasonic.net/cns/pcc/support/sipphone>

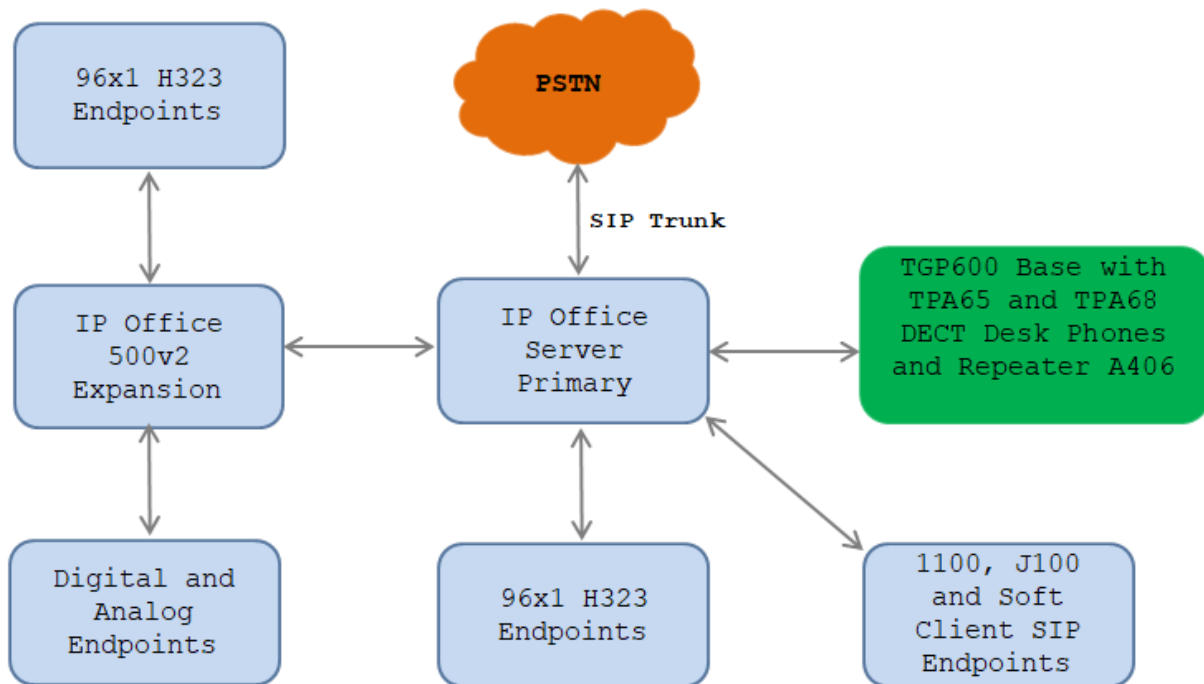
### 3. Reference Configuration

**Figure 1** illustrates the test configuration used for the DevConnect compliance testing.

The Avaya components used to create the simulated enterprise customer site includes:

- IP Office Server Edition running in Virtualized environment.
  - Avaya IP Office Voicemail Pro.
- Avaya IP Office 500 V2 as expansion systems.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- IP Office Primary has SIP trunk to PSTN.

Panasonic TGP600 SIP Cordless Phone registers to IP Office Primary as SIP endpoint.



**Figure 1: Avaya Interoperability Test Lab Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya IP Office Server Edition (Primary Server) <ul style="list-style-type: none"><li>Avaya IP Office Voicemail Pro</li></ul>	11.0.4.1.0 Build 11 11.0.4.1.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.0.4.1.0 Build 11
Avaya IP Office Manager	11.0.4.1.0 Build 11
Avaya 96x1 Series IP Deskphones (H.323)	6.8002
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.0.0.21
Avaya 1408 Digital Telephone	48.02
Analog Telephone	---
<b>Panasonic</b>	
Panasonic KX-TGP600 SIP Cordless Phone	IPL Version: SIP 2.10 Firmware Version: 10.008
Panasonic KX-TPA65 Wireless Desk Phone	Firmware Version: 03.04.001
Panasonic KX-TPA68 Wireless Desk Phone	Firmware Version: 02.00.005
Panasonic KX-A406 Repeater	---

**Note:** Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

## 5. Avaya IP Office Primary Server Configuration

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.

Select IP Office

Name	IP Address	Type	Version	Edition
Server Edition 11.0				
<input checked="" type="checkbox"/> IPOSE110	10.33.1.110	IPO-Linux-PC	11.0.4.1.0 build 11	Server (Primary)

Configuration Service User Login

IP Office: IPOSE110 (Primary System - IPO-Linux-PC)

Service User Name: Administrator

Service User Password: .....

OK Cancel Help

TCP Discovery Progress

Unit/Broadcast Address: 10.33.1.110 Refresh

☒ Open with Server Edition Manager

OK Cancel

On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE110**, on the navigation pane will expand the menu on this server.

Description	Name	Address	Primary Link	Users Configured	Extensions Configured
Solution				35	41
Primary Server	IPOSE110	10.33.1.110		17	14
Expansion System	EXP110	192.168.199.55	Bothway	18	27

In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

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

## 5.1. Licensing

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

In the reference configuration, **IPOSE110** was used as the system name of the Primary Server and **EXP500** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

Navigate to **License** in the Navigation Pane. In the Details Pane, verify that the **License Status** for **3rd Party IP Endpoints** is **Valid** and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.

The screenshot shows the Avaya IP Office Configuration window. The left pane displays the navigation tree with the following structure:

- Configuration
  - BOOTP (2)
  - Operator (3)
  - Solution
    - User (35)
      - Group(1)
      - Short Code (46)
      - Directory(0)
      - Time Profile(0)
      - Account Code(0)
      - User Rights(11)
      - Location(2)
        - IPOSE110**
          - System (1)
            - IPOSE110
              - Line (5)
              - Control Unit (9)
              - Extension (14)
              - User (18)
              - Group (0)
              - Short Code (6)
              - Service (0)
              - Incoming Call Route (1)
              - IP Route (3)**
                - License (33)**
                - ARS (1)
                - Location (2)
                - Authorization Code (0)

The right pane shows the 'License' configuration for the 'Remote Server'.

License Mode: License Normal  
 Licensed Version: 11.0  
 PLDS Host ID: [Redacted]  
 PLDS File Status: Valid

Feature	Instances	Status	Expiration Date	Source
SIP Trunk Channels	512	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	10	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
<b>3rd Party IP Endpoints</b>	<b>384</b>	<b>Valid</b>	<b>Never</b>	<b>PLDS Nodal</b>
Essential Edition	10	Obsolete	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	10	Obsolete	Never	PLDS Nodal
Server Edition	5	Valid	Never	PLDS Nodal
UMS Web Services	100	Valid	Never	PLDS Nodal
Avaya Mac Softphone	100	Valid	Never	PLDS Nodal
SM Trunk Channels	512	Valid	Never	PLDS Nodal
Web Collaboration	64	Valid	Never	PLDS Nodal
Avaya Contact Center Select	10	Valid	Never	PLDS Nodal
Devlink3 External Recorder	10	Valid	Never	PLDS Nodal
Basic User	384	Obsolete	Never	PLDS Nodal

At the bottom of the window, there are buttons for 'OK', 'Cancel', and 'Help'. The status bar at the bottom left indicates 'Sent 100% of IPOSE110'.

## 5.2. System Settings

The LAN2 tab settings correspond to the IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side).

Note: In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN2 interface configuration is not directly relevant to the interface with the TGP600 SIP phone, and therefore is not described in these Application Notes.

## 5.3. System – LAN1 Tab

In the sample configuration, the LAN1 interface is used for the SIP Registrar for the SIP endpoint.

### 5.3.1. LAN1 - LAN Settings Tab

To view or configure the LAN1 IP address and subnet mask, select the **LAN1 → LAN Settings** tab, and enter the information as needed, according to the customer network requirements:

- **IP Address: 10.33.1.110** was used in the reference configuration, this is the public IP address assigned to IP Office.
- **IP Mask: 255.255.255.0** was used in the reference configuration.
- Other parameters on this screen are set to the defaults.

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy, with 'IPOSE110' selected. The main window is titled 'IPOSE110\*' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'IP Address' field is set to '10 . 33 . 1 . 110' and the 'IP Mask' field is set to '255 . 255 . 255 . 0', both fields are highlighted with a red rectangle. Below these, the 'Number Of DHCP IP Addresses' is set to '144'. The 'DHCP Mode' section has three radio buttons: 'Server', 'Client', and 'Disabled', with 'Disabled' being the selected option. An 'Advanced' button is located to the right of the DHCP Mode section. At the bottom of the window are 'OK', 'Cancel', and 'Help' buttons.

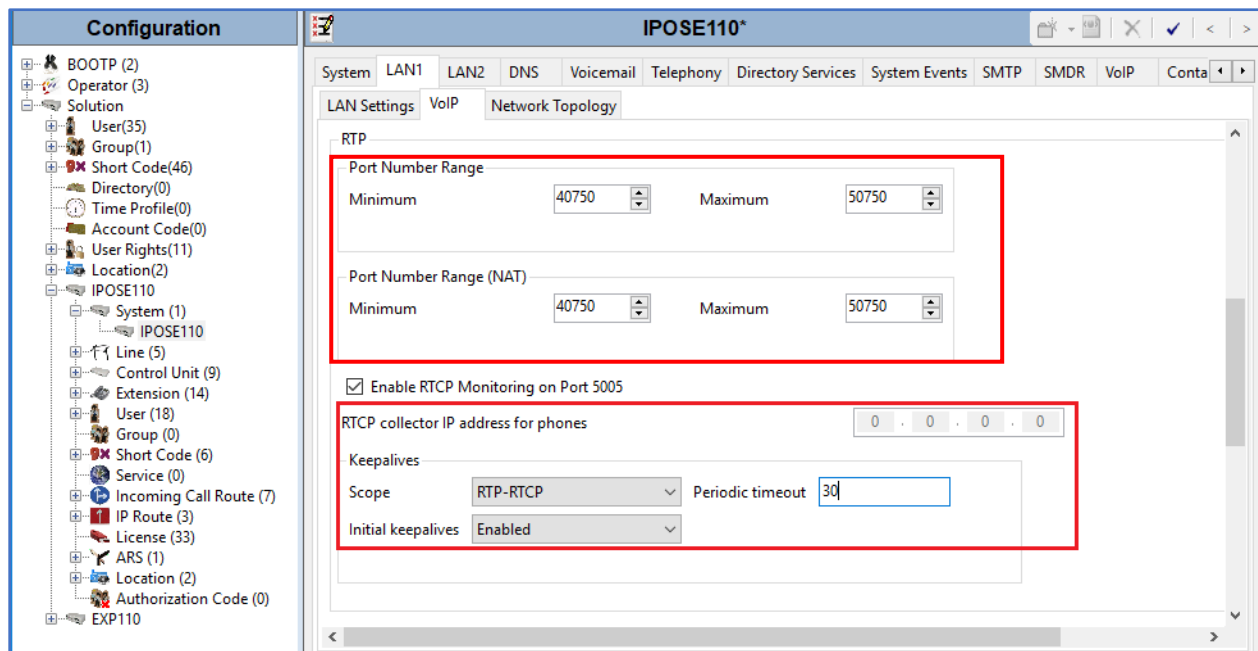
### 5.3.2. LAN1 VoIP Tab

- Select the **LAN1 → VoIP** tab in the Details Pane. Check the **SIP Registrar Enable** box to allow the configuration of SIP Registrar. Enter a SIP domain “**ipocc.com**” in the **SIP Domain Name** field and make sure all protocols are enabled and ports are configured in the **Layer 4 Protocol** section. In the compliance test, the TGP600 SIP phone registered to IPO using UDP protocol.

The screenshot displays the IPOSE110 configuration window. On the left, a tree view shows the configuration hierarchy, with 'IPOSE110' selected. The main pane has tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'VoIP', and 'Contact'. The 'VoIP' tab is active, showing 'LAN Settings' and 'Network Topology' sub-tabs. Under 'LAN Settings', the 'SIP Registrar Enable' checkbox is checked and highlighted with a red box. Below it, the 'SIP Domain Name' field is set to 'ipocc.com' and is also highlighted with a red box. The 'Layer 4 Protocol' section shows three protocols checked: UDP (port 5060), TCP (port 5060), and TLS (port 5061). These three rows are highlighted with a red box. The 'Challenge Expiration Time (sec)' is set to 22. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Scroll down the page:

- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN1. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. This is done to prevent possible issues with network firewalls closing idle RTP channels.
- Click **OK** to commit (not shown).



### 5.3.3. LAN1 - Network Topology Tab

On the **LAN1 Network Topology** tab in the Details pane, set the following:

- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to SIP endpoint and SIP trunk service on this LAN.
- Default values were used for all other parameters.
- Click the **OK** button (not shown).

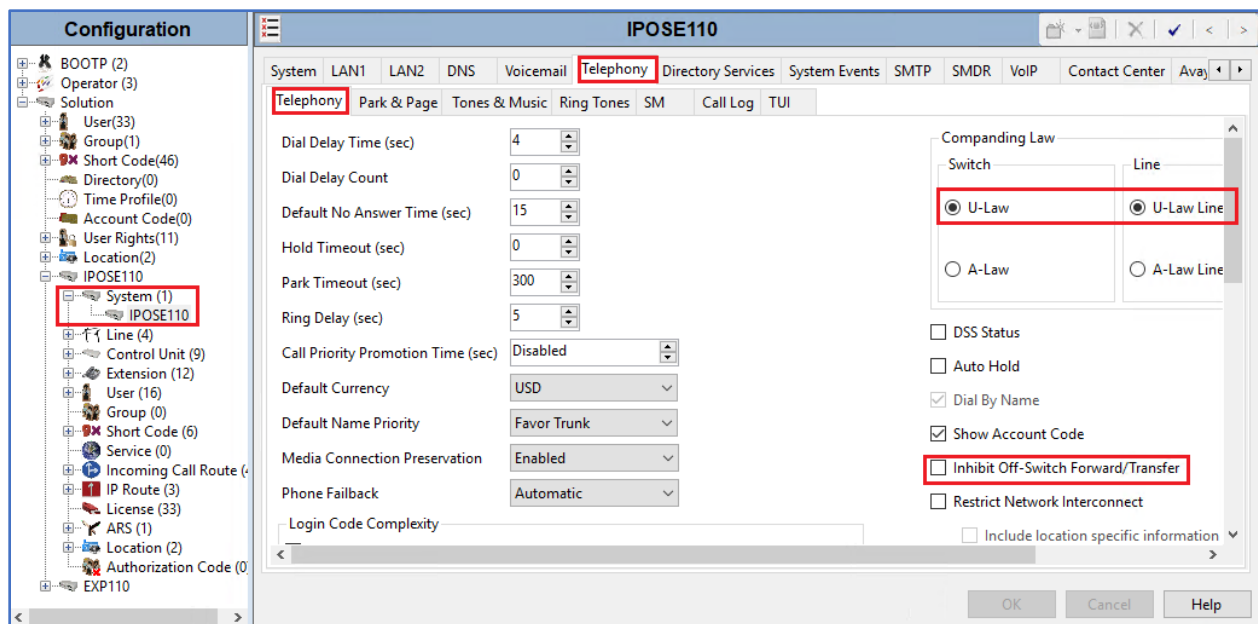
The screenshot shows the IPOSE110 configuration window with the 'Network Topology' tab selected. The 'Firewall/NAT Type' is set to 'Open Internet' and the 'Binding Refresh Time (sec)' is set to '60'. The 'STUN Server Address' is '0.0.0.0' and the 'STUN Port' is '3478'. The 'Public IP Address' is '0.0.0.0'. The 'Public Port' section shows 'UDP' set to '0', 'TCP' set to '0', and 'TLS' set to '0'. The 'Run STUN on startup' checkbox is unchecked. The 'Run STUN' and 'Cancel' buttons are visible. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Field	Value
STUN Server Address	0.0.0.0
STUN Port	3478
Firewall/NAT Type	Open Internet
Binding Refresh Time (sec)	60
Public IP Address	0 . 0 . 0 . 0
Public Port - UDP	0
Public Port - TCP	0
Public Port - TLS	0
Run STUN on startup	<input type="checkbox"/>

### 5.3.4. Telephony Tab

To access the System Telephony settings, navigate to the **Telephony** → **Telephony** tab in the **Details** pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location; **U-Law** was used for the compliance test.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).



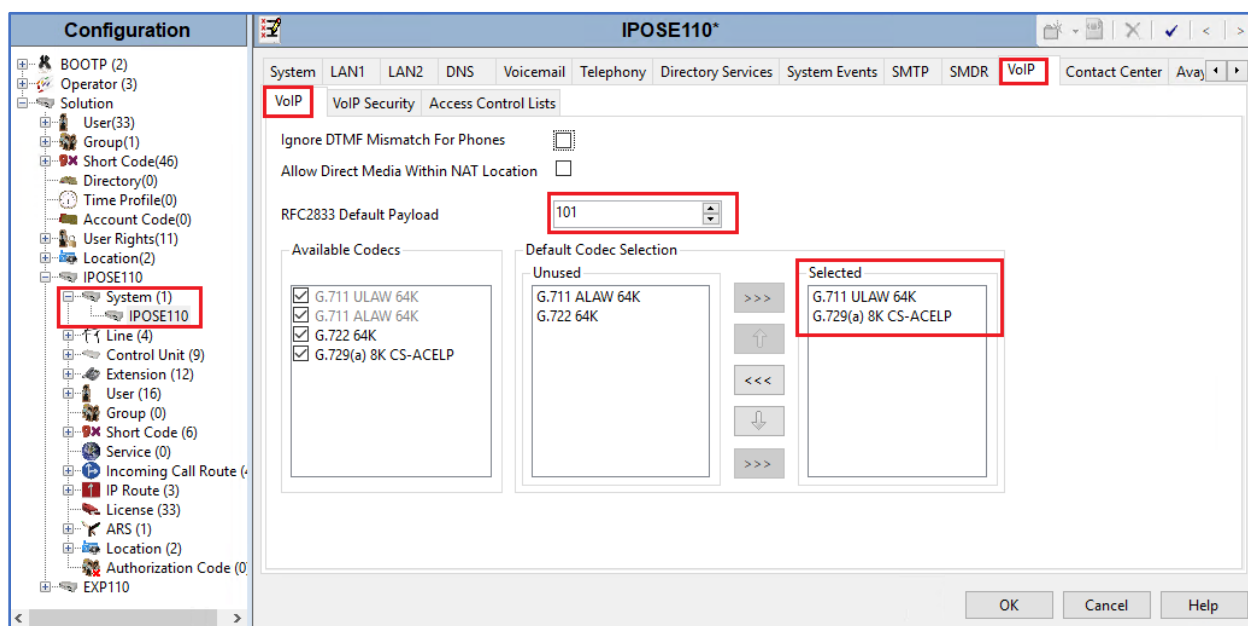
### 5.3.5. VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

#### 5.3.5.1 VoIP - VoIP Tab

Select the **VoIP** → **VoIP** tab, configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).



**Note:** The codec selections defined under this section (VoIP – VoIP Tab) are the codecs selected for the IP phones/extensions.

### 5.3.5.2 VoIP – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

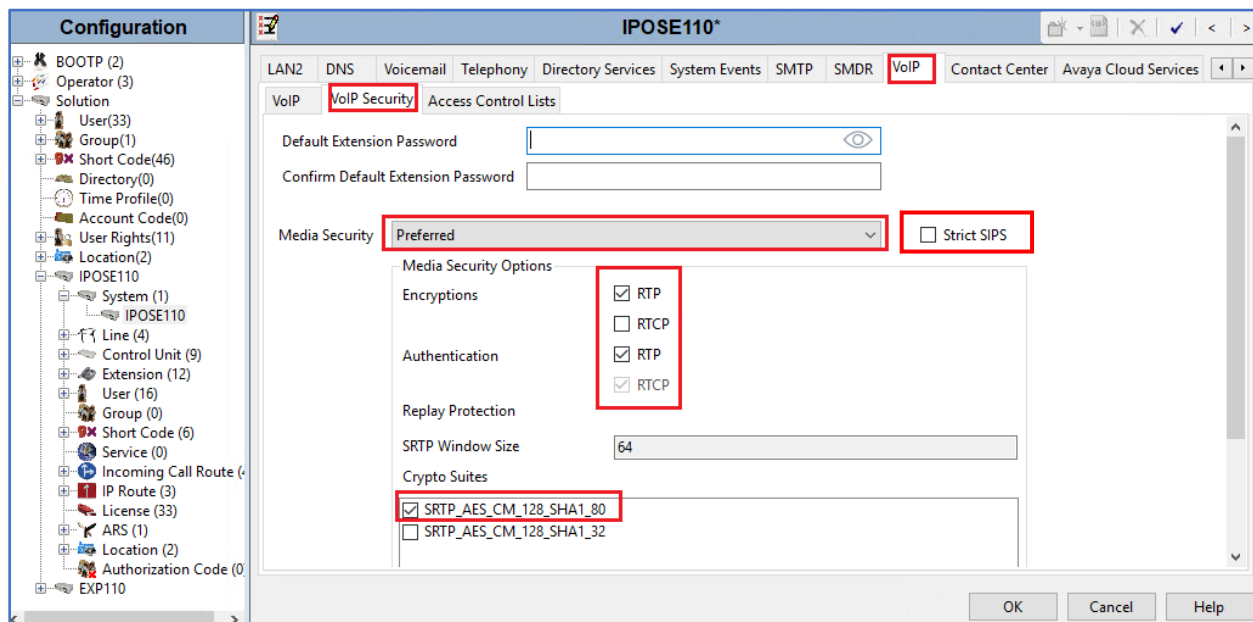
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

When enabling SRTP on the system, the recommended setting is **Preferred**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established.

To configure the use of SRTP, select the **VoIP → VoIP Security** tab on the Details pane.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Verify **Strict SIPS** is not checked.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP\_AES\_CM\_128\_SHA1\_80**.
- Click **OK** to commit (not shown).



## 5.4. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to communicate with endpoints.

Navigate to **IP Route**, right-click on **IP Route** and select **New**. The values used during the compliance test are shown below:

- Set the **IP Address** and **IP Mask** to **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP address of the gateway/router used to route calls to the network, e.g., **10.33.1.1**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

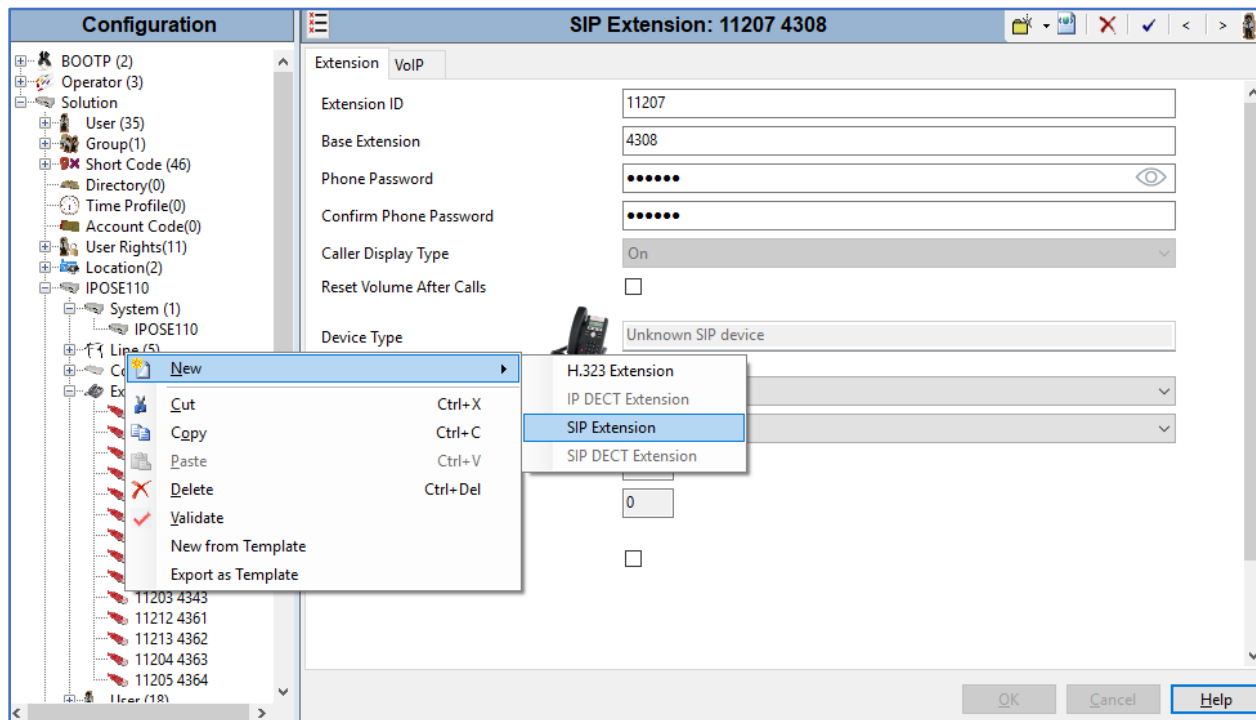
The screenshot shows a software configuration window titled "0.0.0.0\*". On the left is a "Configuration" tree with a hierarchical structure. The "IPOSE110" node under "System (1)" is highlighted with a red box. The main area on the right is titled "IP Route" and contains the following fields:

- IP Address:** 0 . 0 . 0 . 0
- IP Mask:** 0 . 0 . 0 . 0
- Gateway IP Address:** 10 . 33 . 1 . 1
- Destination:** LAN1 (selected from a dropdown menu)
- Metric:** 0 (in a text input field)

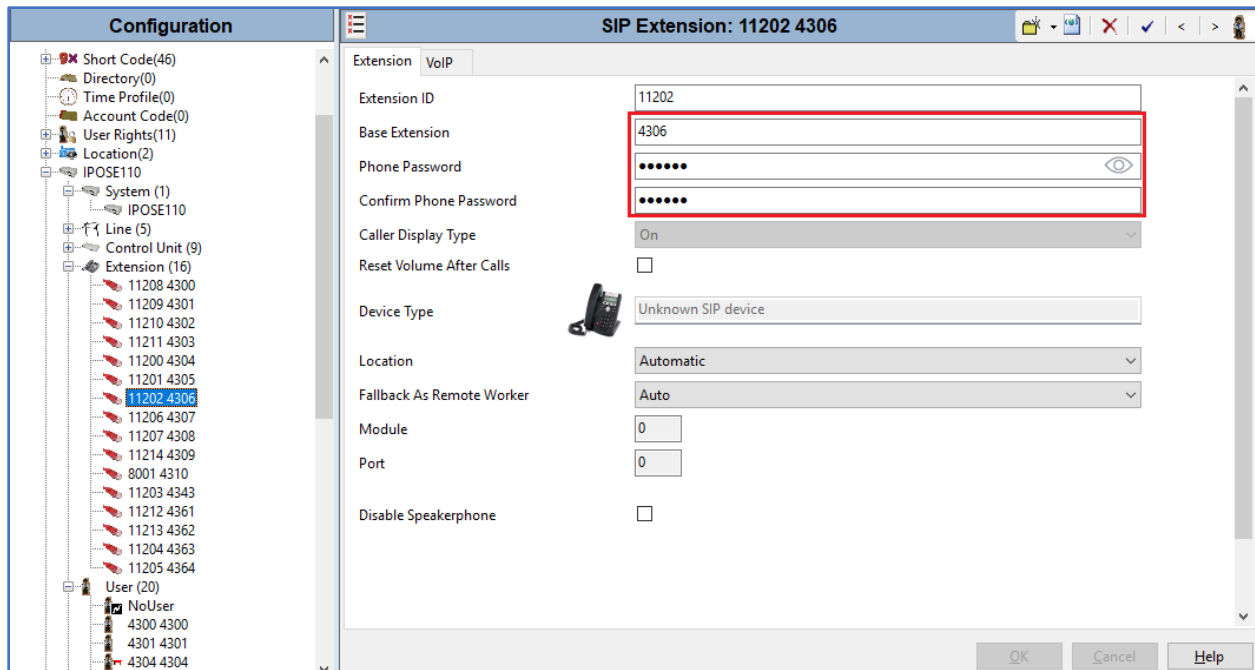
A red rectangle highlights the IP Address, IP Mask, Gateway IP Address, Destination, and Metric fields. At the bottom right of the window are three buttons: "OK", "Cancel", and "Help".

## 5.6. Administer SIP Extension

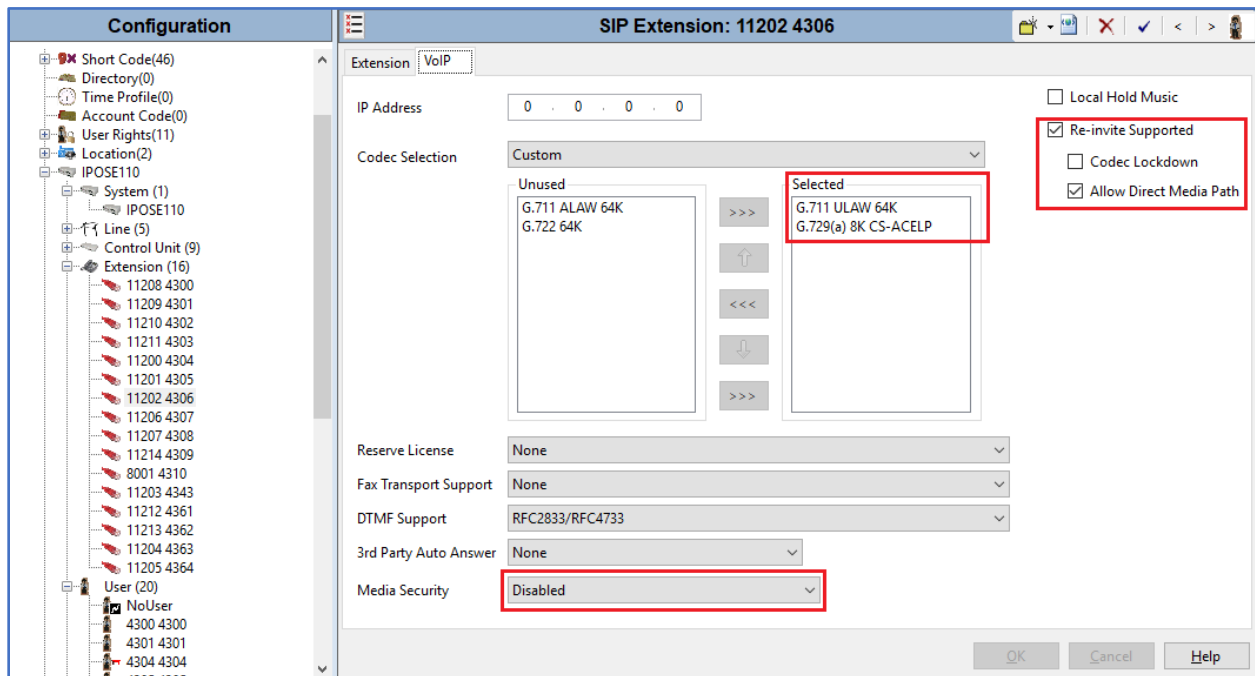
An extension needs to be created for every endpoint that registers to IPO. To create a new extension, from the left navigate pane, right click on **Extension** → **New** → **SIP Extension**.



The screen below shows the pre-created extension **4306** that was used for the compliance test. Note that the password is set in the **Phone Password** field is later used for the TGP600 SIP phone regerting to IPO.



The screen below shows the **VoIP** tab of the extension 4306, make sure the **Media Security** is set to **Disabled** to avoid audio issue since the TGP600 SIP phone did not use secure media SRTP for the testing. **Re-invite Supported** and **Allow Direct Media Path** checkbox are checked to support direct media between endpoints as possible.



## 5.7. Administer SIP User

A user can be newly added as new or edit by selecting **User** in the left pane. The screen below shows the user 4306 that was created for the testing. The extension **4306** is entered in the **Extension** field. The name is entered in the **Full Name** field will be displayed on the other endpoint when the call is established.

Configuration window for user 4306: 4306. The left pane shows the Configuration tree with 'User (20)' expanded, listing various users including 4306. The right pane shows the 'User' tab with fields for Name (4306), Password, Confirm Password, Unique Identity, Conference PIN, Confirm Audio, Conference PIN, Account Status (Enabled), Full Name (SIP 4306), Extension (4306), Email Address, Locale, Priority (5), System Phone Rights (None), ACCS Agent Type (None), and Profile (Basic User). The 'Full Name' and 'Extension' fields are highlighted with a red box.

In the **Voicemail** tab, make sure the **Voicemail On** checkbox is checked and enter a code for the **Voicemail code** field.

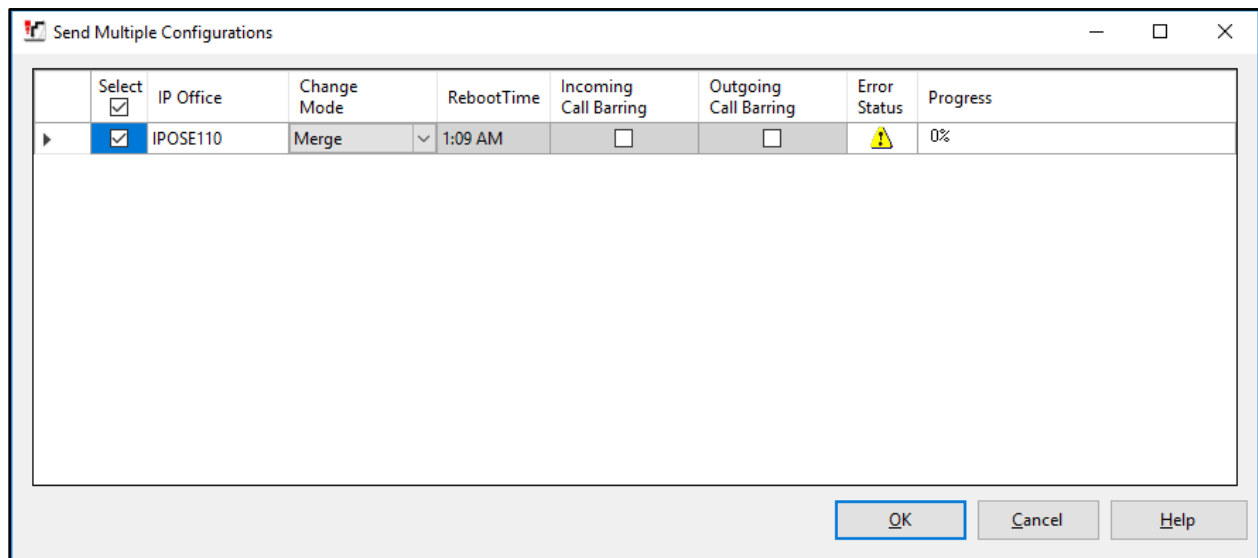
Configuration window for user 4306: 4306, showing the 'Voicemail' tab. The left pane shows the Configuration tree with 'User (20)' expanded, listing various users including 4306. The right pane shows the 'Voicemail' tab with fields for Voicemail Code, Confirm Voicemail Code, and Voicemail Email. The 'Voicemail Code' and 'Confirm Voicemail Code' fields are highlighted with a red box. The 'Voicemail On' checkbox is checked. The 'DTMF Breakout' section shows 'Reception/Breakout (DTMF 0)', 'Breakout (DTMF 2)', and 'Breakout (DTMF 3)' all set to 'System Default ()'. The 'Voicemail Email' section shows 'Off' selected. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

## 5.8. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

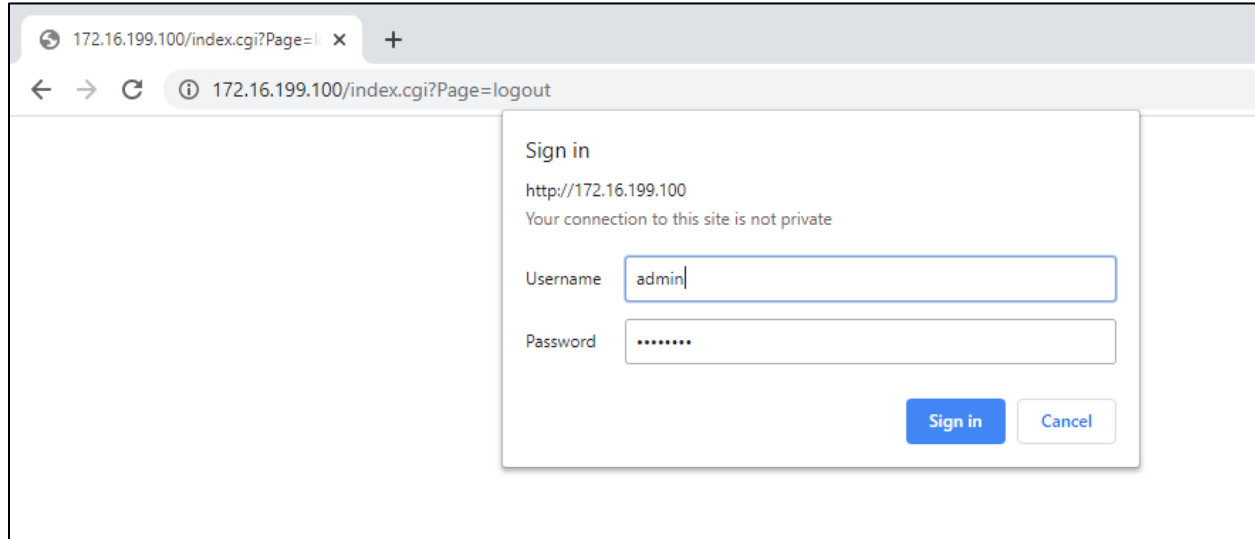
A screen similar to the one below will appear, with either **Merge** or **Reboot** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Reboot** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.



## 6. Configure Panasonic TGP600 SIP Phone

Launch a web browser and enter the IP address of TGP600 SIP phone. The Sign in window displays and enter the credentials, click on **Sign in** button to log in.



To configure the TGP600's lines, navigate to the **VoIP → SIP Settings → Line 2**. The **SIP Settings [Line 2]** window displays in the right window.

In the **Basic** section, configure the SIP parameters, including:

- **Phone Number:** enter the extension number as configured in **Section 5.6**.
- **Registrar Server Address:** enter the LAN1 IP address of IPO.
- **Registrar Server Port:** leave the default port 5060.
- **Proxy Server Address:** enter the LAN1 IP address of IPO.
- **Proxy Server Port:** enter the port 5060.
- **Outbound Proxy Server Address:** enter the LAN1 IP address of IPO.
- **Outbound Proxy Port:** enter the port 5060.
- **Service Domain:** enter the SIP domain *ipocc.com* as configured in **Section 5.3.2**.
- **Authentication ID:** enter the extension number as configured in **Section 5.6**.
- **Authentication Password:** enter the phone password as configured in **Section 5.6**.

Click on **Save** button (not shown) in the bottom of the window to save the changes.

**Panasonic**

KX-TGP600

Status Network System **VoIP** Telephone Maintenance

SIP Settings [Line 2]

Logout

Web Port Close

VoIP

SIP Settings

- Line 1
- Line 2
- Line 3
- Line 4
- Line 5
- Line 6
- Line 7
- Line 8

VoIP Settings

- Line 1
- Line 2
- Line 3
- Line 4
- Line 5
- Line 6

Basic	
Phone Number	4306
Registrar Server Address	
Registrar Server Port	5060 [1-65535]
Proxy Server Address	10.33.1.110
Proxy Server Port	5060 [1-65535]
Presence Server Address	
Presence Server Port	5060 [1-65535]
Outbound Proxy Server Address	10.33.1.110
Outbound Proxy Server Port	5060 [1-65535]
Service Domain	ipocc.com
Authentication ID	4306
Authentication Password	.....
Advanced	
SIP Packet QoS (DSCP)	0 [0-63]

In the **Advanced** section, leave all the fields at default values as shown in the screenshot below.

**Panasonic**  
KX-TGP600

Status Network System **VoIP** Telephone Maintenance

Logout  
Web Port Close

**VoIP**

**SIP Settings**

- Line 1
- Line 2
- Line 3
- Line 4
- Line 5
- Line 6
- Line 7
- Line 8

**VoIP Settings**

- Line 1
- Line 2
- Line 3
- Line 4
- Line 5
- Line 6

**Advanced**

SIP Packet QoS (DSCP)	0 [0-63]
Enable DNS SRV lookup	<input checked="" type="radio"/> Yes <input type="radio"/> No
SRV lookup Prefix for UDP	_sip._udp.
SRV lookup Prefix for TCP	_sip._tcp.
SRV lookup Prefix for TLS	_sips._tcp.
Local SIP Port	5060 [1024-49151]
SIP URI	
T1 Timer	500 milliseconds
T2 Timer	4 seconds
REGISTER Expires Timer	3600 seconds [1-4294967295]
Enable Session Timer (RFC 4028)	0 seconds [60-65535, 0: Disable]
Session Timer Method	<input checked="" type="radio"/> INVITE <input type="radio"/> UPDATE <input type="radio"/> INVITE/UPDATE
Enable 100rel (RFC 3262)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable SSAF (SIP Source Address Filter)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable c=0.0.0.0 Hold (RFC 2543)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Transport Protocol	<input checked="" type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TLS
TLS Mode	<input checked="" type="radio"/> SIPS <input type="radio"/> SIP-TLS

Navigate to the **VoIP → VoIP Settings → Line 2**. The **VoIP Settings [Line 2]** window displays in the right window. Leave all fields in the **Basic** and **Advanced** sections at default.

**Panasonic**  
KX-TGP600

Status | Network | System | **VoIP** | Telephone | Maintenance

Logout  
Web Port Close

**VoIP**

**SIP Settings**

- Line 1
- **Line 2**
- Line 3
- Line 4
- Line 5
- Line 6
- Line 7
- Line 8

**VoIP Settings**

- Line 1
- **Line 2**
- Line 3
- Line 4
- Line 5

**Basic**

PCMA	Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Priority	1 [1-255]
G.729A	Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Priority	1 [1-255]
PCMU	Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Priority	1 [1-255]
DTMF Type		<input checked="" type="radio"/> RFC2833 <input type="radio"/> Inband <input type="radio"/> SIP INFO

**Advanced**

RTP Packet QoS (DSCP)	0 [0-63]
RTCP Packet QoS (DSCP)	0 [0-63]
Enable RTCP	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable RTCP-XR	<input type="radio"/> Yes <input checked="" type="radio"/> No
RTCP&RTCP-XR Interval	5 seconds [5-65535]
SRTP Mode	RTP/SRTP
Enable Mixed SRTP&RTP by Conference	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Mixed SRTP&RTP by Transfer	<input type="radio"/> Yes <input checked="" type="radio"/> No

To configure the call features such as anonymous, call forward, and DND for Line 2, navigate to **Telephone → Call Control → Line 2**. The **Call Control [Line 2]** window displays in the right window.

The screenshot shows the Panasonic KX-TGP600 web interface. The top navigation bar includes tabs for Status, Network, System, VoIP, Telephone, and Maintenance. The 'Telephone' tab is selected. On the left sidebar, under 'Telephone', the 'Call Control' section is expanded, and 'Line 2' is selected. The main content area is titled 'Call Features' and contains a list of settings for the selected line.

Call Features	
Display Name	TPA68
Voice Mail Access Number	*17
Enable Anonymous Call	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Block Anonymous Call	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Do Not Disturb	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Call Waiting	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Call Forwarding Always	<input type="radio"/> Yes <input checked="" type="radio"/> No
Forwarding Number (Always)	
Enable Call Forwarding Busy	<input type="radio"/> Yes <input checked="" type="radio"/> No
Forwarding Number (Busy)	
Enable Call Forwarding No Answer	<input type="radio"/> Yes <input checked="" type="radio"/> No
Forwarding Number (No Answer)	
Ring Counts (No Answer)	3 counts [0, 2-20]
Enable Shared Call	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Key Synchronization	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Call Park Notification	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable Click to Call	<input type="radio"/> Yes <input checked="" type="radio"/> No

## 7. Verification Steps

This section provides verification steps that may be performed to verify that the solution is configured properly.

The following steps may be used to verify the configuration:

- Verify that TGP600 SIP phone can place calls to local extensions.
- Verify that TGP600 SIP phone can receive calls from local extensions.

### 7.1. IP Office System Status

The following steps can also be used to verify the configuration.

Use the IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.

The screenshot shows the Avaya IP Office System Status application window. The window has a title bar with the text "Avaya IP Office System Status" and standard window controls. Below the title bar is a blue header bar with the Avaya logo on the left and the text "IP Office System Status" on the right. Underneath the header bar is a menu bar with "Help", "Exit", and "About" options. The main content area is white and contains a "Logon" dialog box. The dialog box has a blue header with the word "Logon" and two tabs: "Online" (selected) and "Offline". The dialog contains several input fields: "Control Unit Address" with the value "10.33.1.110", "Proxy Server Address" with the value "<None>", "Services Base TCP Port" with the value "50804", "Local IP Address" with the value "Automatic", "User Name" with the value "Administrator", and a "Password" field. There are three checkboxes: "Auto reconnect" (checked), "Secure connection" (checked), and "Websocket connection" (unchecked). A "Logon" button is located at the bottom right of the dialog box.

Expand the **Extensions** from the left pane and select the extension 4306, the **Extension Status** window displays in the right pane, verify the **Current State** is **Idle**.

The screenshot shows the Avaya IP Office System Status application window. The title bar reads "Avaya IP Office System Status - IPOSE110 (10.33.1.110) - 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". On the left is a navigation pane with a tree view containing "System", "Alarms (36)", "Extensions (8)", "Trunks (5)", "Active Calls", "Resources", "Voicemail", "IP Networking", and "Locations". The "Extensions (8)" folder is expanded, and extension 4306 is selected. The right pane displays the "Extension Status" for extension 4306. Below the status details is a table showing call history.

**Extension Status**

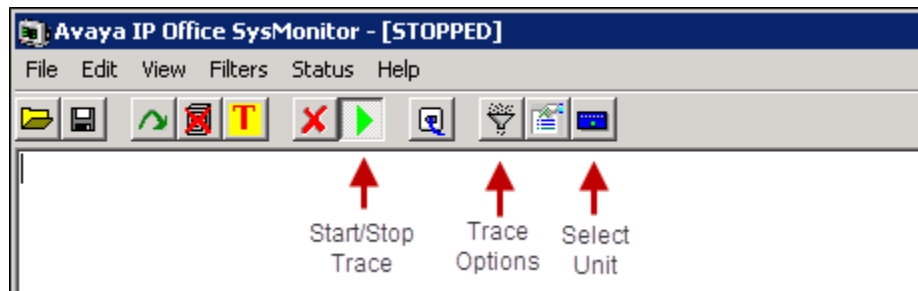
Extension Number: 4306  
 IP address: 172.16.199.100  
 Standard Location: None  
 Registrar: Primary  
 Telephone Type: Unknown SIP Device  
 User-Agent SIP header: Panasonic-KX-TGP600/10.008 (4c364e2d10e1)  
 Media Stream: RTP  
 Layer 4 Protocol: UDP  
 Current User Extension Number: 4306  
 Current User Name: 4306  
 Forwarding: Off  
 Twinning: Off  
 Do Not Disturb: Off  
 Message Waiting: On  
 Number of New Messages: 2  
 Phone Manager Type: None  
 SIP Device Features: REFER,UPDATE  
 License Reserved: No  
 Last Date and Time License Allocated: 30/12/2019 5:58:20 AM  
 Packet Loss Fraction: Connection Type:  
 Jitter: Codec:  
 Round Trip Delay: Remote Media Address:

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
	Idle	1 day 18:41:51			

At the bottom of the window, there is a status bar showing the time "12:40:11 AM" and the status "Online". Above the status bar are buttons for "Trace", "Trace All", "Pause", "Ping", "Call Details", "Print...", and "Save As...".

## 7.2. Monitor

The Avaya IP Office SysMonitor application can be used to monitor and troubleshoot signaling messaging on the SIP register. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



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





## 8. Conclusion

These Application Notes describe the configuration necessary for Panasonic TGP600 Base Station with TPA65 and TPA68 DECT Wireless Desk Phones and Repeater A406 with Avaya IP Office Server Edition Release 11.0. Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

## 9. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, is available at:

<http://support.avaya.com/>

- [1] *Deploying IP Office Platform Server Edition Solution*, Release 11.0, May 2018
- [2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, January 2019
- [3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, February 2019.
- [4] *Administering Avaya IP Office Platform with Manager, Release 11.0 FP4*, February 2019.
- [5] *Administering Avaya IP Office™ Platform with Web Manager, Release 11.0 FP4*, February 2019.
- [6] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows, Release 3.4.8*, November 2018
- [7] *Using Avaya Equinox for IP Office, Release 11.0 FP4*, February 2019

Additional Avaya IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

---

**©2020 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).