



Application Notes for Enghouse Interactive Communications Center 10.1 with Avaya IP Office Server Edition 11 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 10.1 to interoperate with Avaya IP Office Server Edition 11. Enghouse Interactive Communications Center is a multi-channel and multi-contact solution that can handle voice, fax, web, and email contacts. The compliance testing focused on the voice integration with Avaya IP Office Server Edition using the TAPI and SIP user interfaces.

The Avaya IP Office Server Edition configuration consisted of two Avaya IP Office systems, a primary Linux server at the Main site and an expansion IP500V2 at the Remote site that were connected via Small Community Network trunks. In the compliance testing, two Enghouse Interactive Communications Center servers were deployed, a primary server at the Main site to interface with the primary IP Office system via TAPI and SIP user interfaces, and an expander server at the Remote site to interface with the expansion IP Office system via TAPI only.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center (EICC) 10.1 to interoperate with Avaya IP Office Server Edition 11. EICC is a multi-channel and multi-contact solution that can handle voice, fax, web, and email contacts. The compliance testing focused on the voice integration with IP Office Server Edition using the TAPI and SIP user interfaces.

The IP Office Server Edition configuration consisted of two IP Office systems, a primary Linux server at the Main site and an expansion IP500V2 at the Remote site that were connected via Small Community Network trunks. In the compliance testing, two EICC servers were deployed, a primary server at the Main site to interface with the primary IP Office system via TAPI and SIP user interfaces, and an expander server at the Remote site to interface with the expansion IP Office system via TAPI only.

The agents were configured as users on the two IP Office systems, with ACD functionality provided by EICC. Each EICC server used TAPI 2 in third party mode to monitor agent users on the local IP Office system and provided call control via the Enghouse Interactive TouchPoint client application. The status of agent users on the expansion IP Office system were relayed by the expander EICC server to the primary EICC server, for centralized tracking of agent availability.

All groups were required by EICC to be configured on the primary IP Office system, and were monitored by the primary EICC server. Upon being notified of an incoming group call via TAPI events, the primary EICC server used TAPI line redirect capability to redirect call to an available agent that can reside on either the Main or Remote site, and the answering agent's desktop was populated with call related information received via the TAPI interface. Call related actions such as answer and drop can be initiated via the TouchPoint client application, and were supported by EICC using TAPI line control capabilities. In addition, EICC used TAPI to support forwarding, message waiting indicator (MWI), and supervisor monitor and intrude features.

The SIP user interface was used by the primary EICC server to support voicemail, announcement, and basic call recording features. Voicemail and announcement calls were redirected to an available virtual SIP user to terminate to EICC, and recording was accomplished by intruding a virtual SIP user onto an active call to pick up the media for recording.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the EICC application, the application automatically registered virtual SIP users with the primary IP Office system, and established TAPI connection from each EICC server with the local IP Office system.

For the manual part of testing, incoming calls were made to the general routing groups configured on the primary IP Office system. EICC used the TAPI event messages to track agent states, and redirected calls to available agents. Manual call controls from the agent desktops were exercised to verify remaining features such as answering and transferring of calls.

Voicemail was tested by not answering personal calls at the agent, and having the call cover to EICC for proper leaving of voice message and activation of MWI. Manual call was made subsequently from agent to the voicemail group for retrieval of voice message and proper deactivation of MWI.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the EICC servers and clients.

The verification of tests included human checking of proper states at the agent desktops and agent telephone displays, and of reviewing the System Monitor logs from the two IP Office systems.

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 IP Office and EICC did not include use of any specific encryption features as requested by Enghouse Interactive.

2.1. Interoperability Compliance Testing

The compliance testing included feature and serviceability areas.

The feature testing focused on verifying the following on EICC:

- Virtual SIP user registrations, G.711 and G.729 codec, and inbound DTMF.
- Use of TAPI functions to monitor users and groups, redirect incoming calls, support call control and supervisor monitor and intrude via client desktops, and set call forwarding and MWI.
- Proper handling of call scenarios including incoming calls to different groups, screen pop, hold, reconnect, blind/attended transfer, attended conference, voicemail, announcement, call forwarding, MWI, supervisor monitor, supervisor intrude, non-ACD call, queuing, hot desking, outgoing call, outpulse of DTMF digits, multiple calls, multiple agents, long duration, park/unpark at destination agent, follow me, and recording of basic calls.

The feature testing call flows included calls within the primary IP Office at the Main site, calls within the expansion IP Office at the Remote site, as well as calls between the two IP Office systems.

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

2.2. Test Results

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

- By design, for a hold and reconnect call scenario, the basic call recording feature captured the audio up to the hold action.
- Only one EICC expander server is supported in the current version.
- For the attended conference scenarios, after one of the agent drops, the remaining agent's Active tab reflected the name of the dropped agent instead of the remaining PSTN party.
- Special character as part of a dial string is not supported by TouchPoint, and the workaround is to use the agent telephone for such dialing.

2.3. Support

Technical support on EICC can be obtained through the following:

- **Phone:** (800) 513-2810
- **Web:** www.enghouseinteractive.com
- **Email:** usa.support@enghouse.com

3. Reference Configuration

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

The devices used in the compliance testing are shown in the table below.

Device Type	Device Number/Extension
Main Site	
Agent Extensions	21031, 21034
Agent Users	21031, 21032
Supervisor Extension	21030
Supervisor User	21030
Remote Site	
Agent Extensions	22031, 22034
Agent Users	22031, 22032
Supervisor Extension	22030
Supervisor User	22030

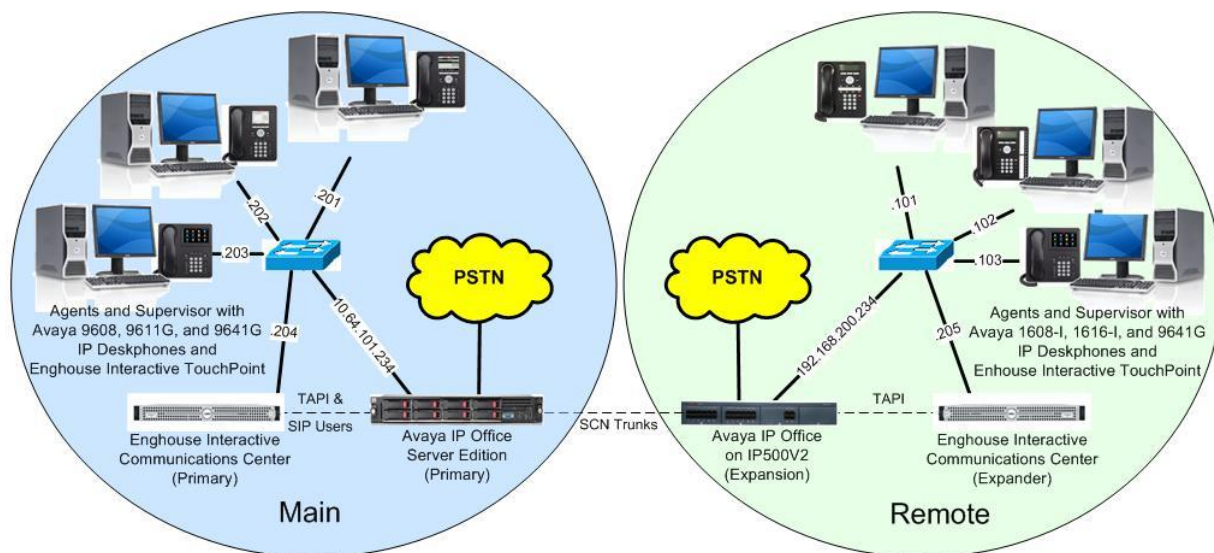


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Main Site	
Avaya IP Office Server Edition (Primary)	11.0.0.1.0
Avaya 9608, 9611G & 9641G IP Deskphone (H.323)	6.6604
Enghouse Interactive Communications Center on Windows Server 2012 R2 <ul style="list-style-type: none">CTI Application ServerSIP ServerAvaya IP Office TAPI2 Driver (tspi2w)	10.1.0.8600 Standard 10.1.0.8600 10.1.0.8600 1.0.0.44
Enghouse Interactive TouchPoint on Windows 10 Pro	10.1.0.8600
Remote Site	
Avaya IP Office on IP500V2 (Expansion)	11.0.0.1.0
Avaya 1608-I & 1616-I IP Deskphone (H.323)	1.3110
Avaya 9611G IP Deskphone (H.323)	6.6604
Enghouse Interactive Communications Center on Windows Server 2012 R2 <ul style="list-style-type: none">CTI Auxiliary ServicesAvaya IP Office TAPI2 Driver (tspi2w)	10.1.0.8600 Standard 10.1.0.8600 1.0.0.44
Enghouse Interactive TouchPoint on Windows 10 Pro	10.1.0.8600

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 configurations consisting of no more than two IP Office systems.

5. Configure Avaya IP Office

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

- Verify licenses
- Administer groups
- Administer agent extensions
- Administer agent users
- Assign agents users to monitor group
- Administer supervisors
- Administer SIP registrar
- Administer SIP extensions
- Administer SIP users
- Administer short code
- Administer system settings
- Administer NoUser source number
- Administer security settings

Note that all procedures above apply to the primary IP Office system, and only a subset of the procedures apply to the expansion IP Office system as listed below.

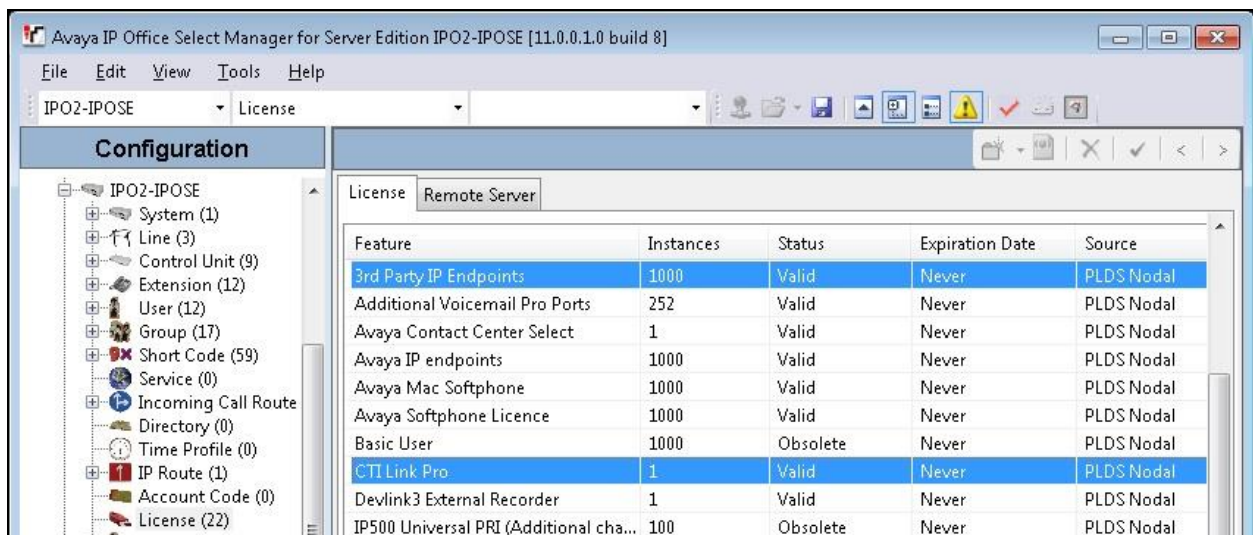
- Verify licenses
- Administer agent extensions
- Administer agent users
- Administer supervisors
- Administer system settings
- Administer NoUser source number
- Administer security settings

5.1. Verify Licenses

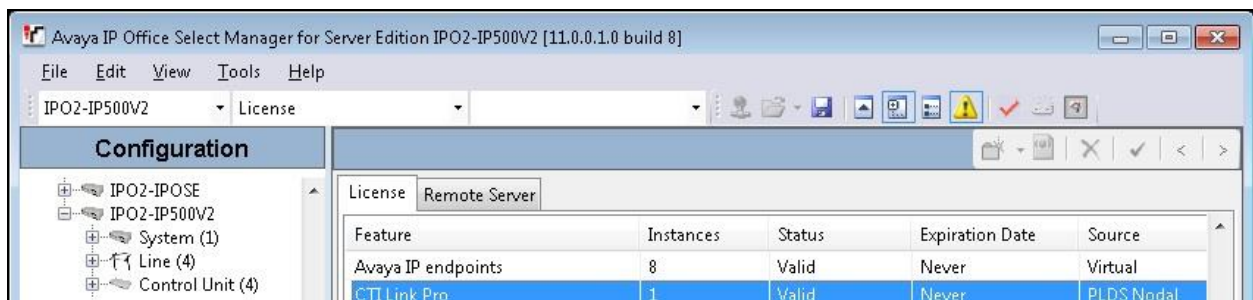
From a PC running the IP Office Manager application, select **Start → All Programs → IP Office → Manager** to launch the application. Select the primary IP Office system, and log in using the appropriate credentials.

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

From the configuration tree in the left pane, select the primary IP Office system, in this case **IPO2-IPOSE**, followed by **License** to display licenses in the right pane. Verify that there are licenses for **3rd Party IP Endpoints** and **CTI Link Pro**, with both license **Status** being “Valid”, as shown below.

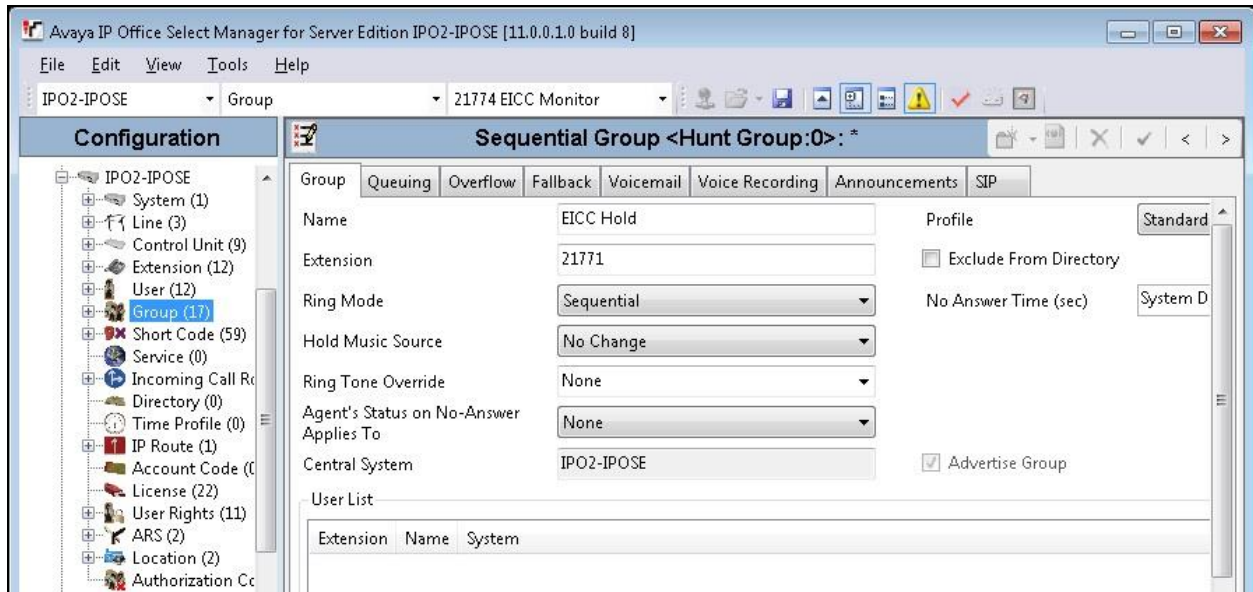


From the configuration tree in the left pane, select the expansion IP Office system, in this case **IPO2-IP500V2**, followed by **License** (not shown) to display licenses in the right pane. Verify that there is a **CTI Link Pro** license, and with the license **Status** being “Valid”, as shown below.

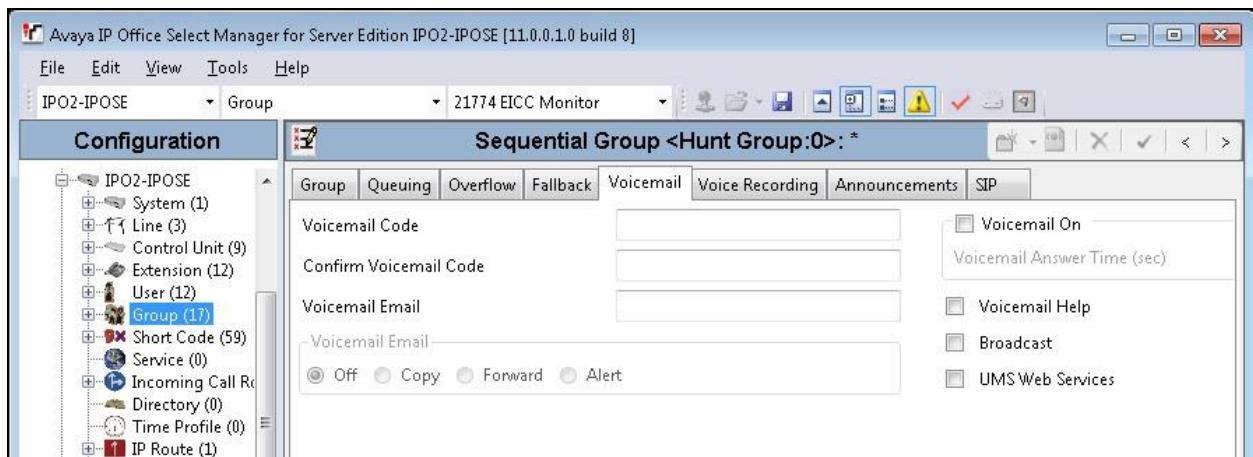


5.2. Administer Groups

From the configuration tree in the left pane, right-click on **Group** under the primary IP Office system and select **New** from the pop-up list to add a new group. For **Name** and **Extension**, enter desired values. Retain the default values for the remaining fields.



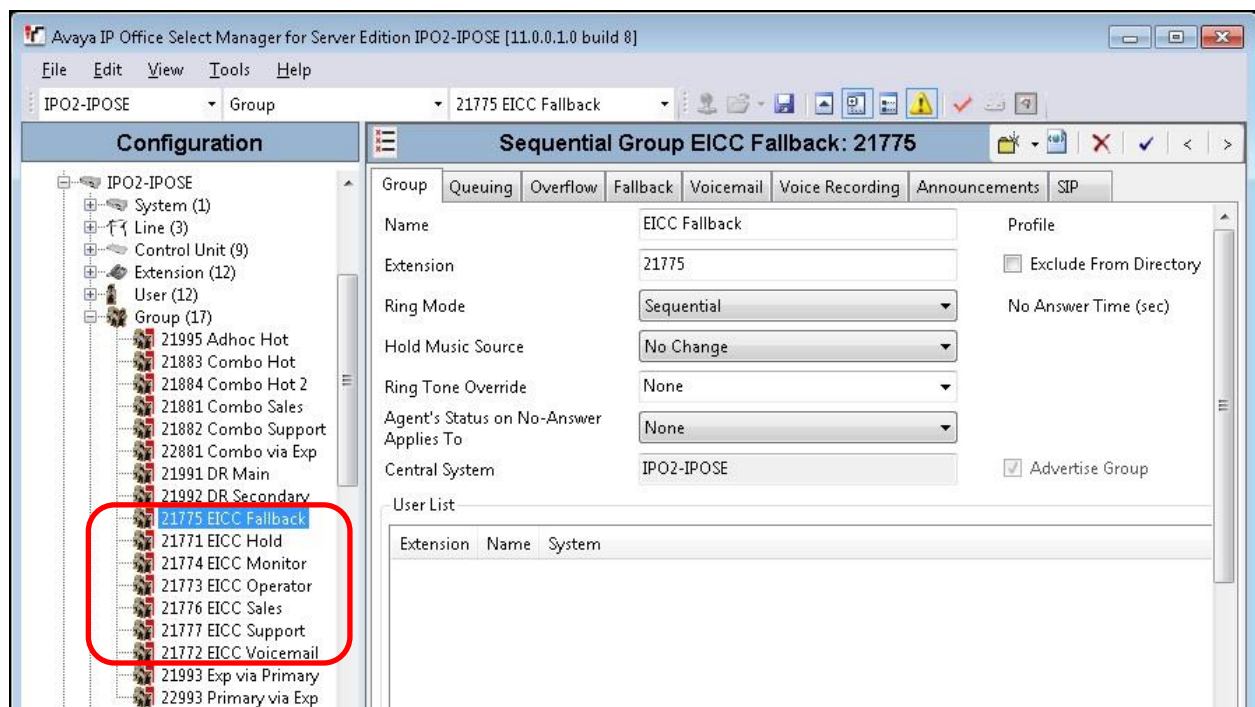
Select the **Voicemail** tab, and uncheck **Voicemail On** as shown below.



Repeat this section to create the groups shown below. These groups are used by EICC for routing and handling of incoming calls. Note that all groups are required by EICC to be configured on the primary IP Office system.

Extension	Name
21771	EICC Hold
21772	EICC Voicemail
21773	EICC Operator
21774	EICC Monitor
21775	EICC Fallback
21776	EICC Sales
21777	EICC Support

The created groups are shown in the left pane of the screen below.

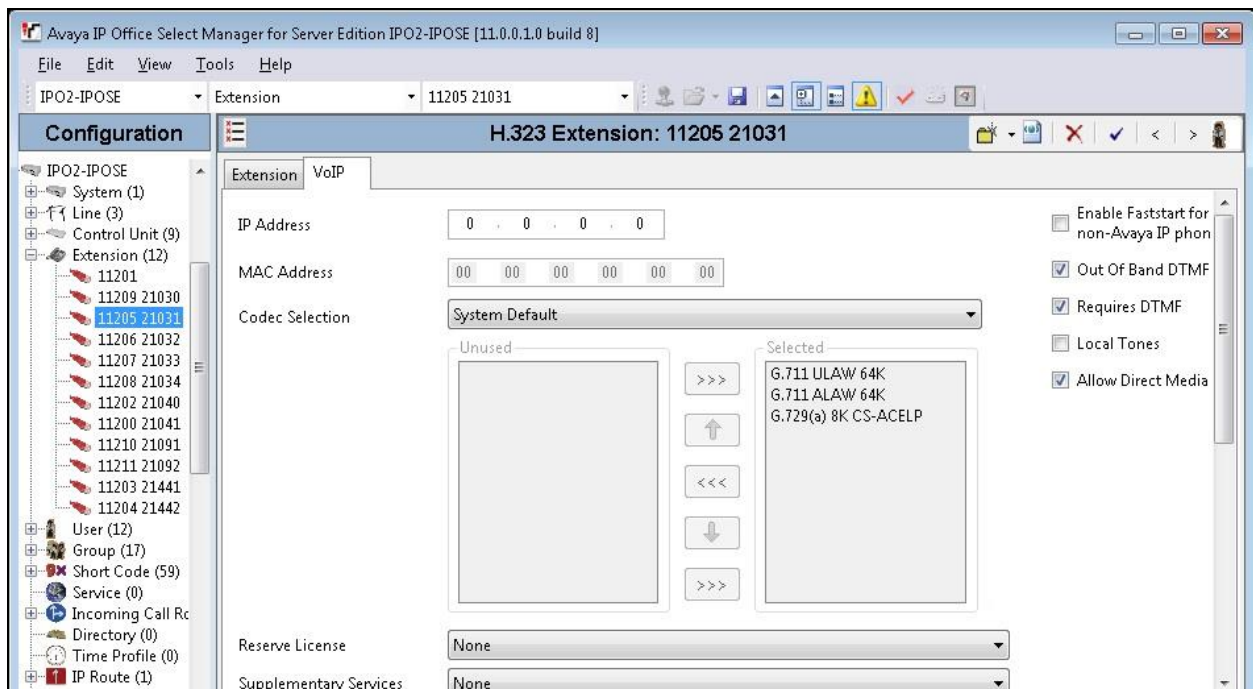


5.3. Administer Agent Extensions

From the configuration tree in the left pane, select the primary IP Office system, followed by the first H.323 extension on the system that will be used by agents and supervisors, in this case “21031”. Select the **VoIP** tab, and check **Requires DTMF** as shown below. Note that this parameter appears when the system parameter Ignore DTMF Mismatch for Phones is enabled.

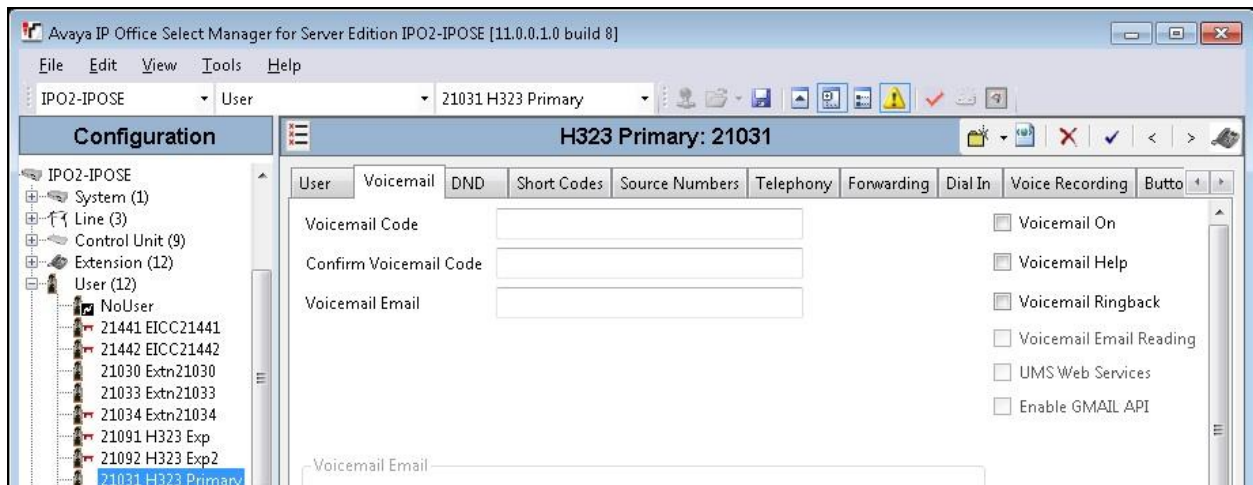
Repeat this section for all H.323 extensions on the Main site that will be used by agents and supervisors. In the compliance testing, three extensions on the Main site with extensions “21031”, “21034”, and “21030” were configured on the primary IP Office system.

Repeat this section for all H.323 extensions on the Remote site that will be used by agents and supervisors. In the compliance testing, three extensions on the Remote site with extensions “22031”, “22034”, and “22030” were configured on the expansion IP Office system (not shown).

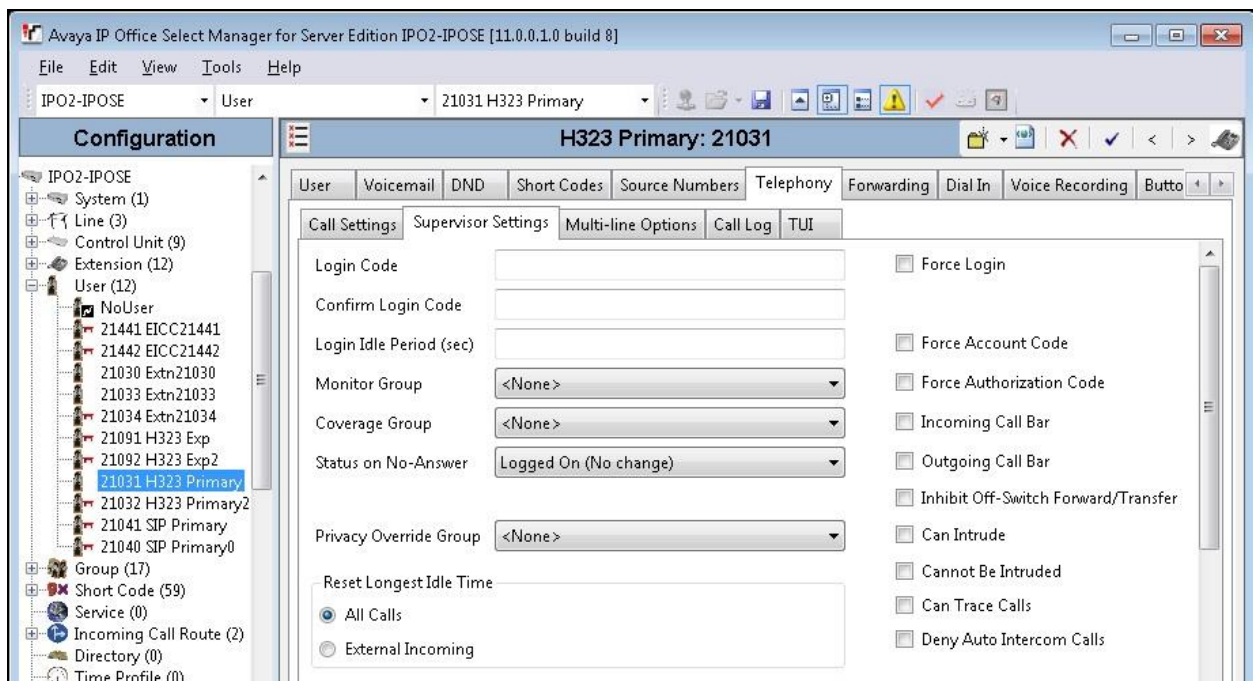


5.4. Administer Agent Users

From the configuration tree in the left pane, select the primary IP Office system, followed by the first user on the system that will be used by agents, in this case “21031”. Select the **Voicemail** tab, and uncheck **Voicemail On** as shown below.



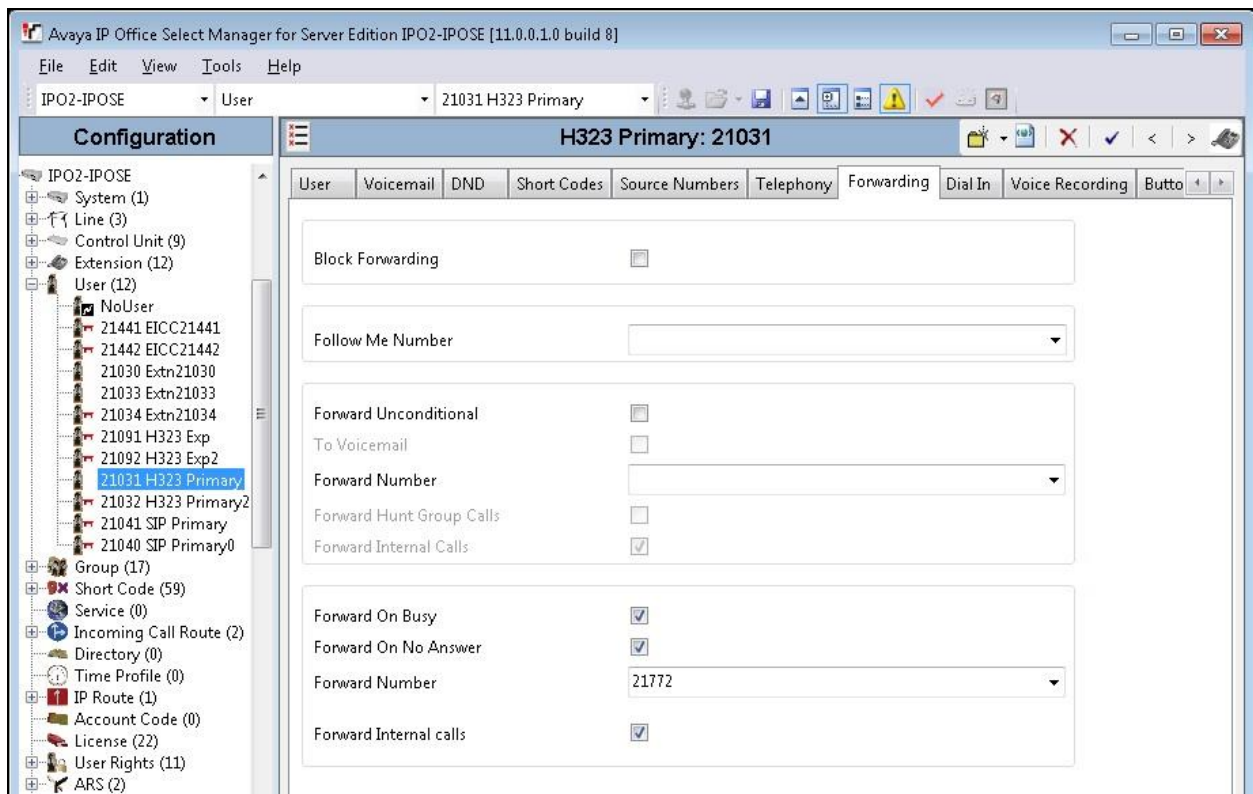
Select the **Telephony** tab, followed by the **Supervisor Settings** sub-tab. Uncheck **Cannot be Intruded**, and set **Can Intrude** to the desired setting.



Select the **Forwarding** tab. Check **Forward On Busy**, **Forward On No Answer**, and **Forward Internal calls**. For **Forward Number**, enter the EICC Voicemail group extension from **Section 5.2**.

Repeat this section for all users on the Main site that will be used by agents. In the compliance testing, two users on the Main site “21031” and “21032” were configured on the primary IP Office system.

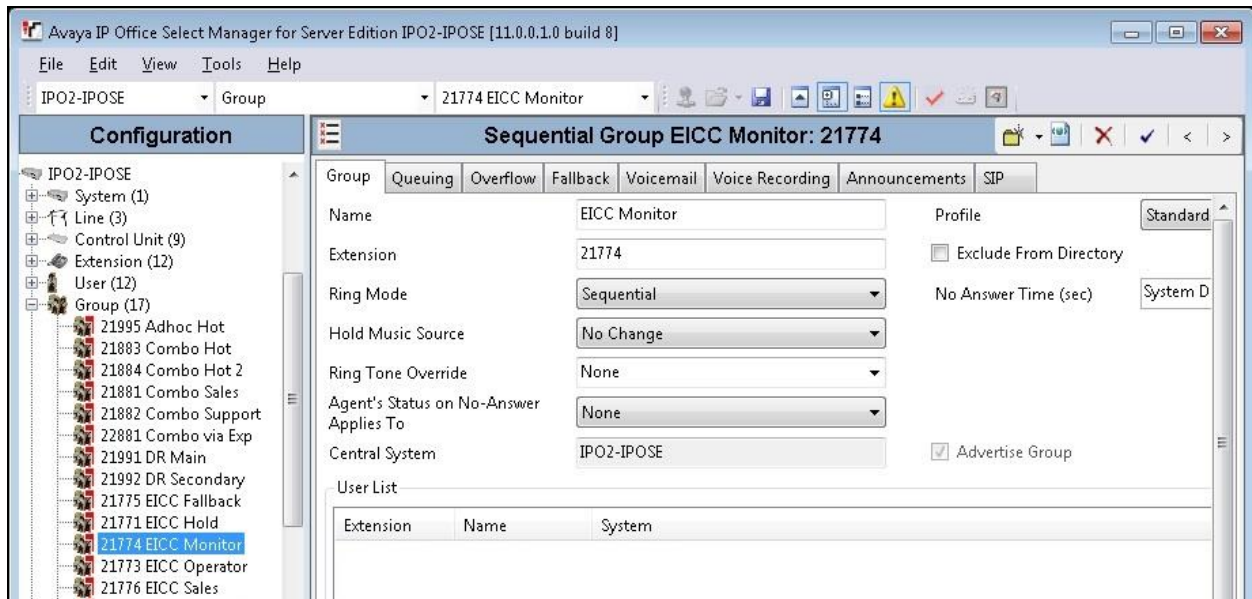
Repeat this section for all users on the Remote site that will be used by agents. In the compliance testing, two users on the Remote site “22031” and “22032” were configured on the expansion IP Office system (not shown).



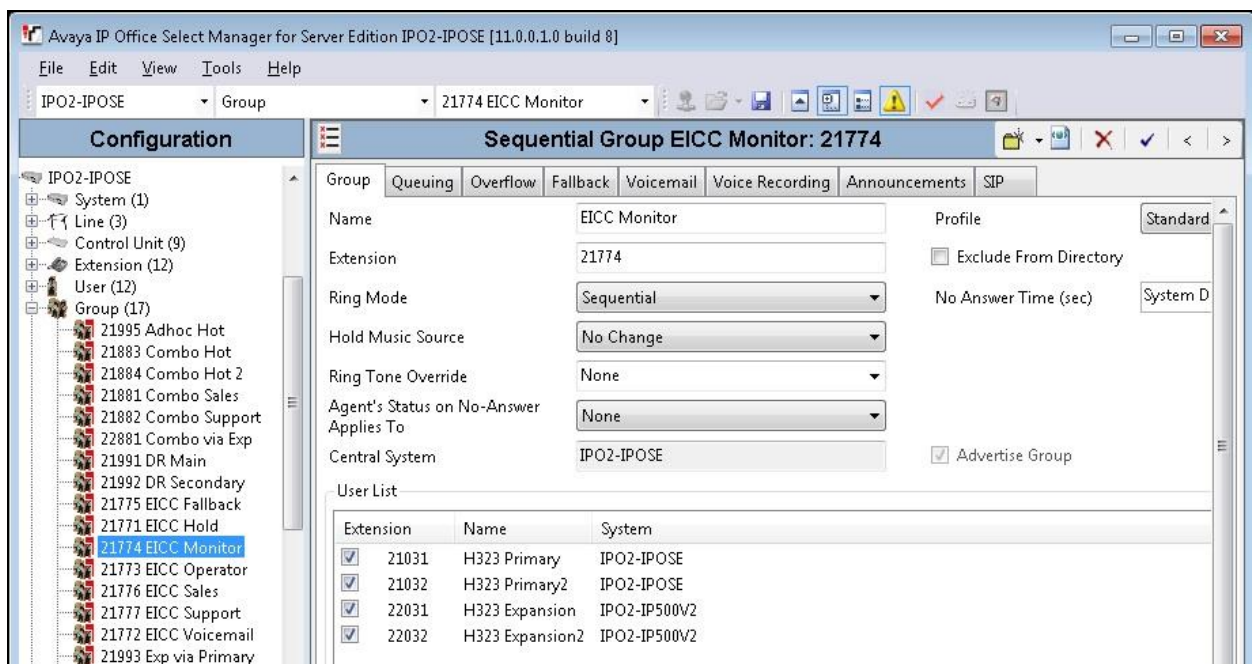
5.5. Assign Agent Users to Monitor Group

From the configuration tree in the left pane, select the EICC Monitor group under the primary IP Office system, in this case “21774”. Click on **Edit** (not shown) in the **User List** sub-section to add members.

In the next screen (not shown), select all agent users on both IP Office systems from **Section 5.4**.



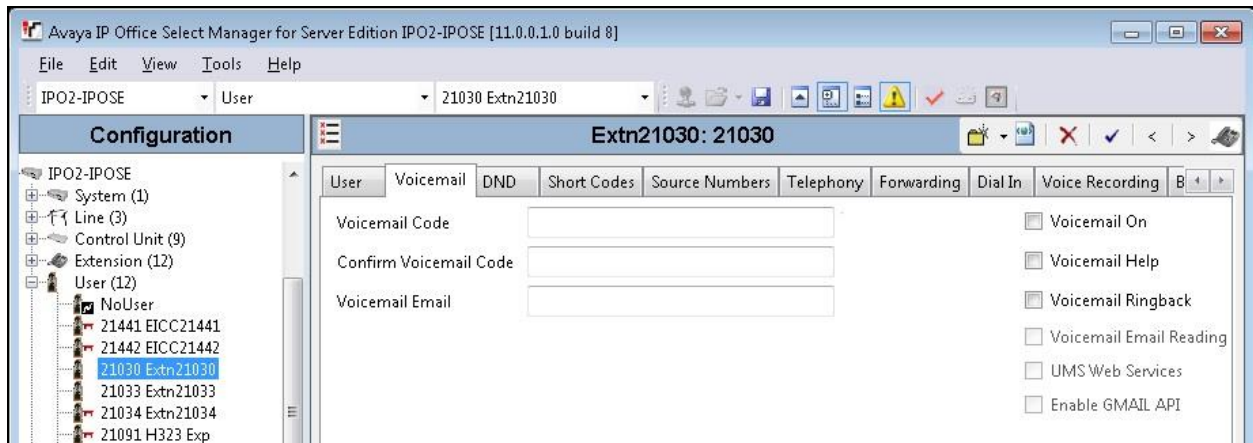
The resultant screen after the selection is shown below.



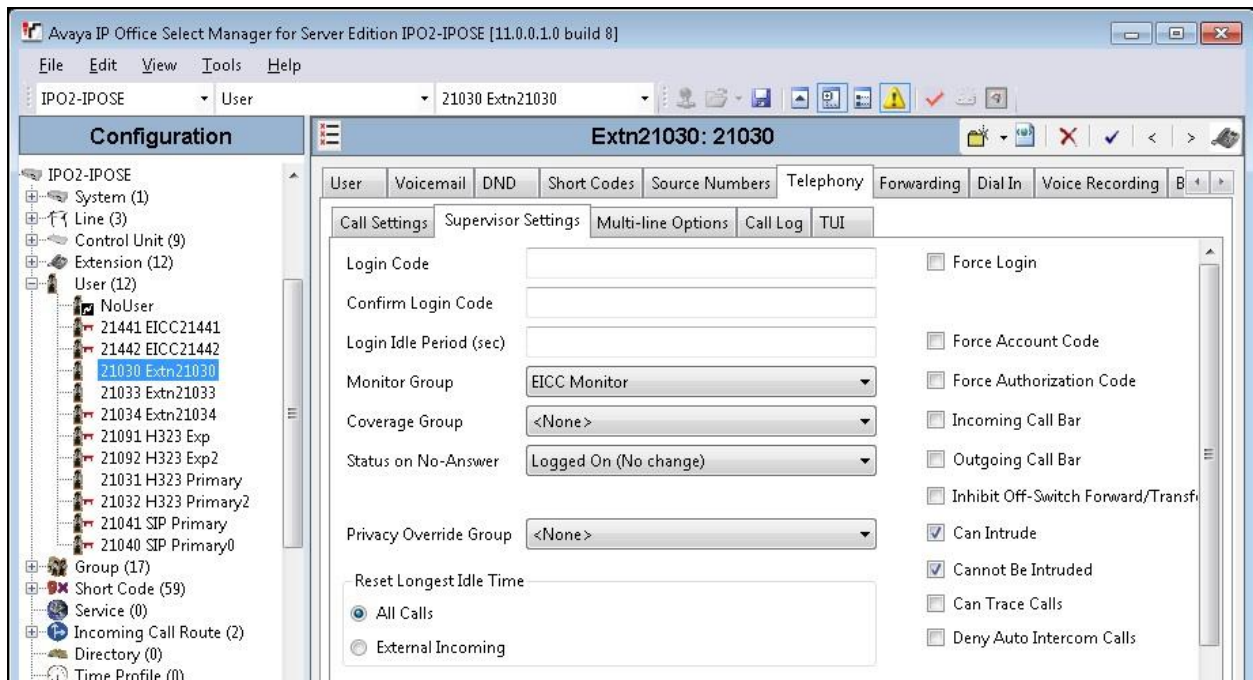
5.6. Administer Supervisors

From the configuration tree in the left pane, select the primary IP Office system, followed by the first user on the Main site that will be used as the supervisor, in this case “21030”.

Select the **Voicemail** tab, and uncheck **Voicemail On** as shown below.



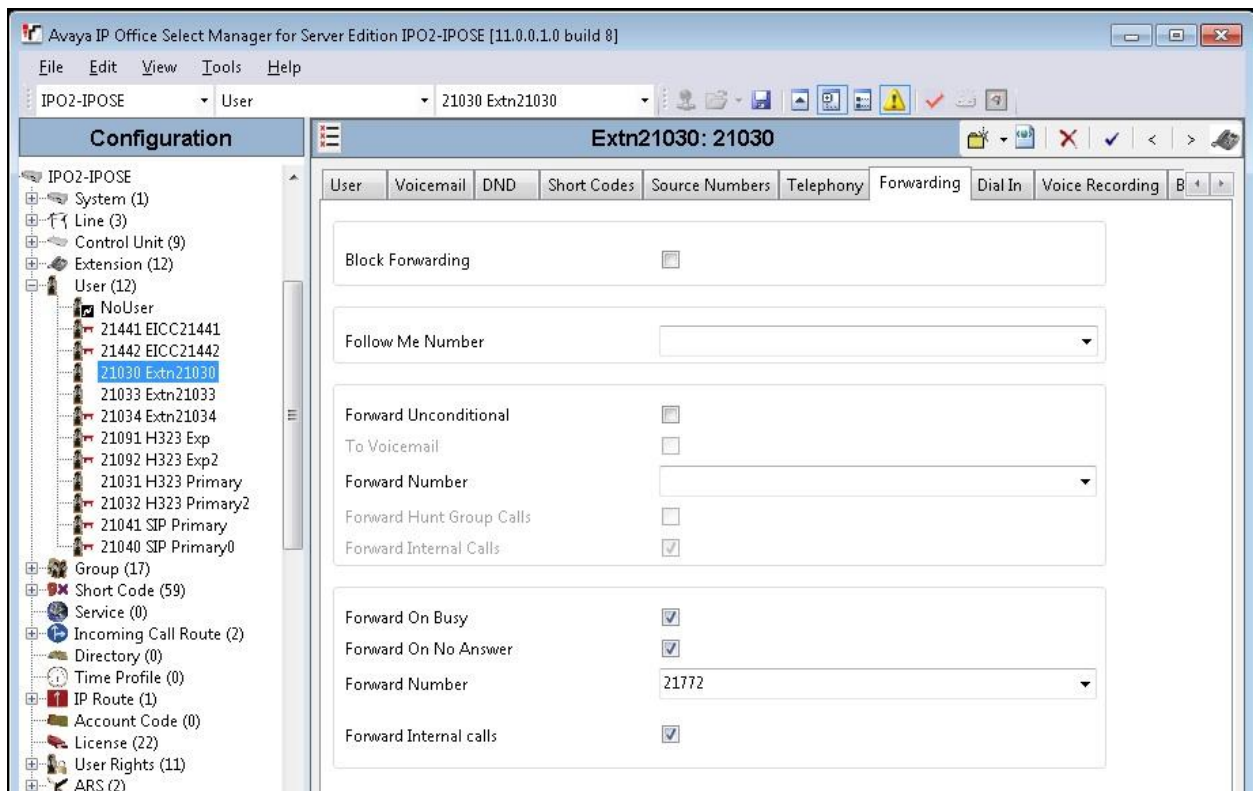
Select the **Telephony** tab, followed by the **Supervisor Settings** sub-tab. Check **Can Intrude**, and set **Cannot be Intruded** to the desired setting. For **Monitor Group**, select the EICC Monitor group from **Section 5.2**.



Select the **Forwarding** tab. Check **Forward On Busy**, **Forward On No Answer**, and **Forward Internal calls**. For **Forward Number**, enter the EICC Voicemail group extension from **Section 5.2**.

Repeat this section for all supervisors on the Main site. In the compliance testing, one supervisor on the Main site “21030” was configured on the primary IP Office system.

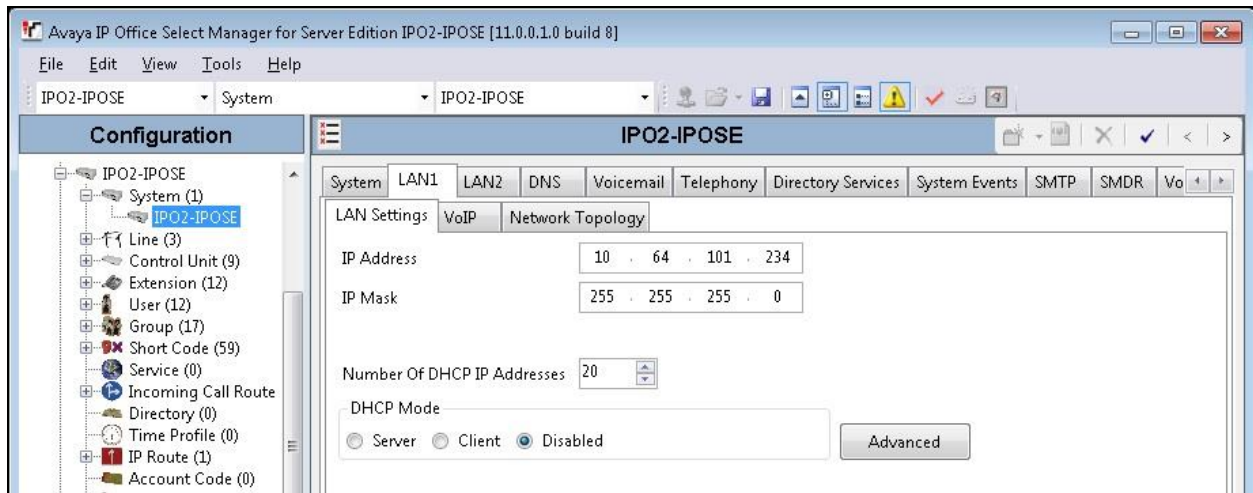
Repeat this section for all supervisors on the Remote site. In the compliance testing, one supervisor on the Remote site “22030” was configured on the expansion IP Office system (not shown).



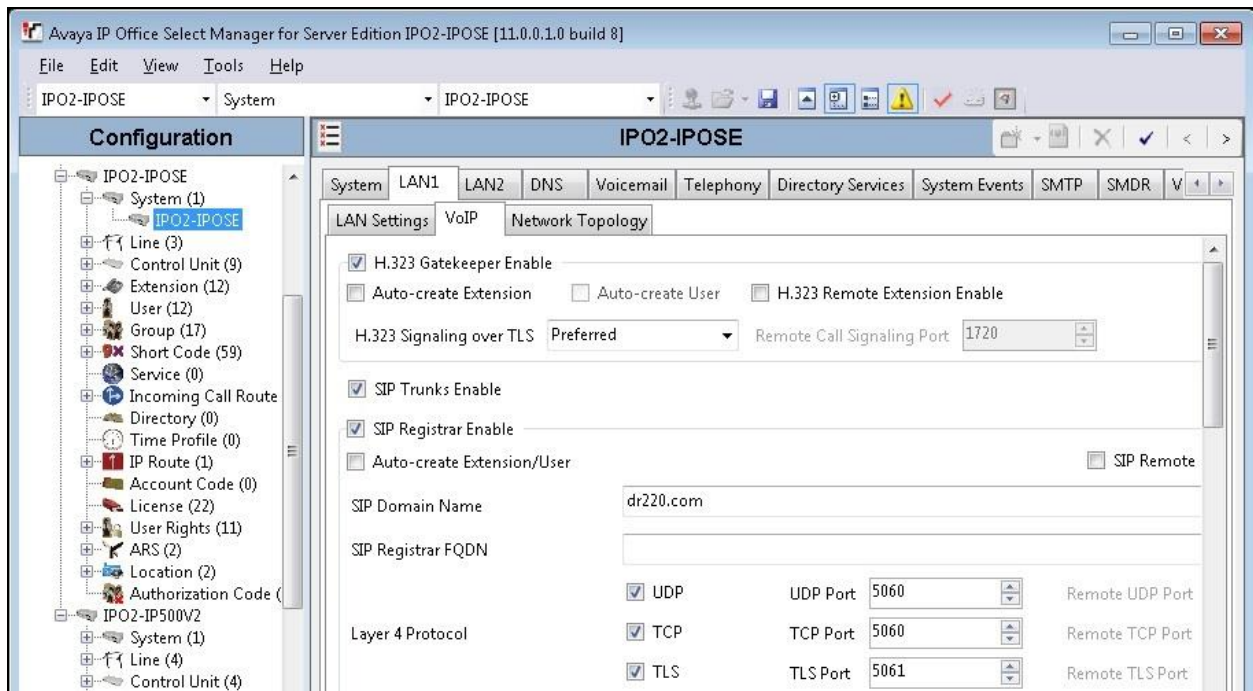
5.7. Administer SIP Registrar

From the configuration tree in the left pane, select **System** under the primary IP Office system to display the system screen in the right pane. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab.

Make a note of the **IP Address** field value, which will be used later to configure EICC. Note that IP Office can support SIP on the LAN1 and/or LAN2 interfaces, and the compliance testing used the LAN1 interface.

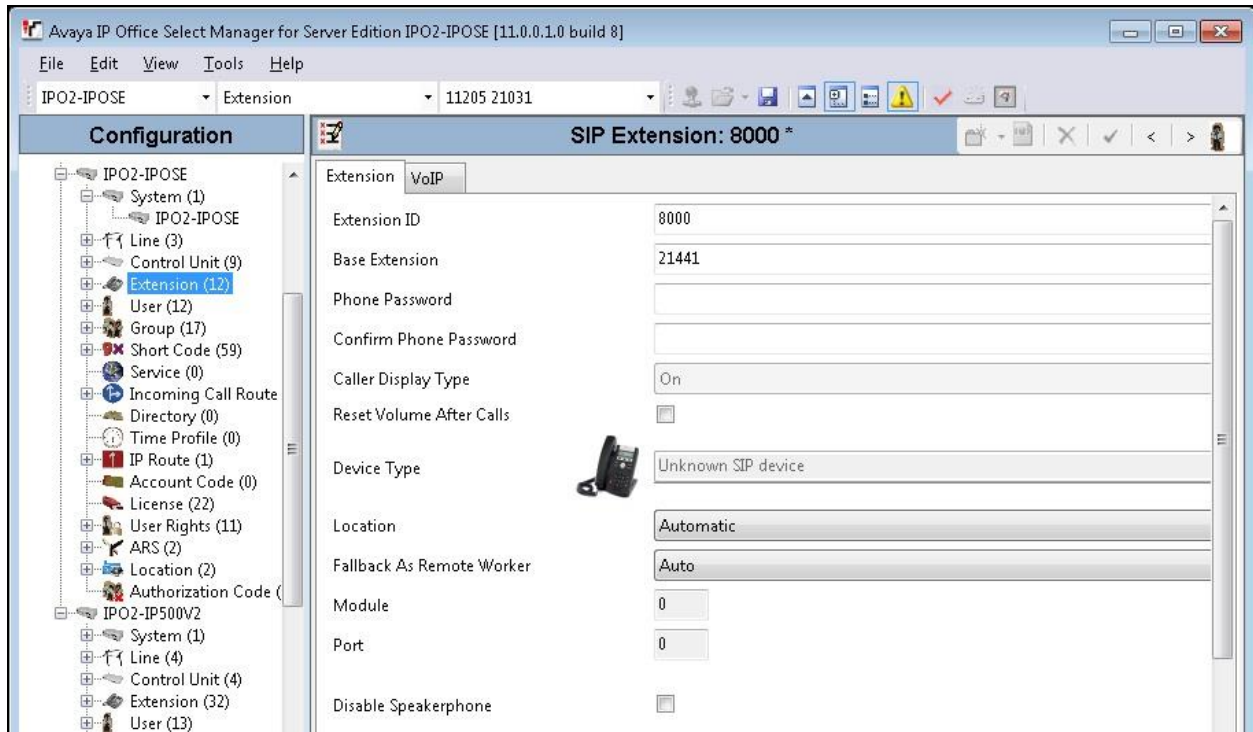


Select the **VoIP** sub-tab. Make certain that **SIP Registrar Enable** is checked, as shown below.



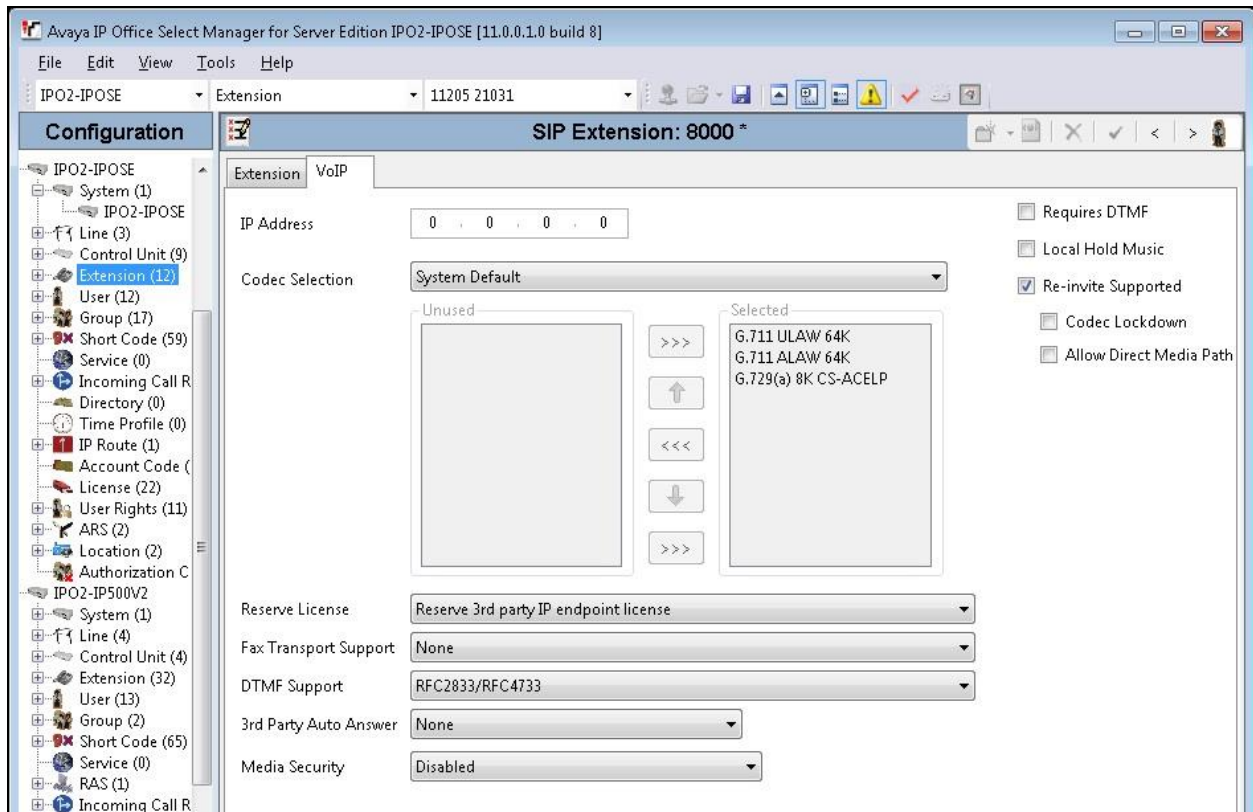
5.8. Administer SIP Extensions

From the configuration tree in the left pane, right-click on **Extension** under the primary IP Office system, and select **New → SIP Extension** from the pop-up list to add a new SIP extension. For **Base Extension**, enter an available extension number, in this case “21441”.



Select the **VoIP** tab, and uncheck **Allow Direct Media Path**. For **Reserve License**, select “Reserve 3rd party IP endpoint license”. For **Media Security**, select “Disabled”, as shown below.

Repeat this section to add the desired number of SIP extensions with consecutive extension numbers. In the compliance testing, two SIP extensions “21441” and “21442” were created.



5.9. Administer SIP Users

From the configuration tree in the left pane, right-click on **User** under the primary IP Office system, and select **New** from the pop-up list. For **Name** and **Full Name**, enter desired values. For **Extension**, enter the first SIP base extension from **Section 5.8**.

Avaya IP Office Select Manager for Server Edition IPO2-IPOSE [11.0.0.1.0 build 8]

File Edit View Tools Help

IPO2-IPOSE User 21030 Extn21030

Configuration

User (12)

User Voicemail DND Short Codes Source Numbers Telephony Forwarding Dial In Voice Recording But

Name EICC21441

Password

Confirm Password

Unique Identity

Conference PIN

Confirm Audio Conference PIN

Account Status Enabled

Full Name EICC SIP Port 1

Extension 21441

Email Address

Locale

Priority 5

System Phone Rights None

Profile Basic User

- ☐ Receptionist
- ☐ Enable Softphone
- ☐ Enable one-X Portal Services
- ☐ Enable one-X TeleCommuter
- ☐ Enable Remote Worker

Select the **Voicemail** tab, and uncheck **Voicemail On** as shown below.

Avaya IP Office Select Manager for Server Edition IPO2-IPOSE [11.0.0.1.0 build 8]

File Edit View Tools Help

IPO2-IPOSE User 21030 Extn21030

Configuration

User (12)

Voicemail DND Short Codes Source Numbers Telephony Forwarding Dial In Voice Recording But

Voicemail Code

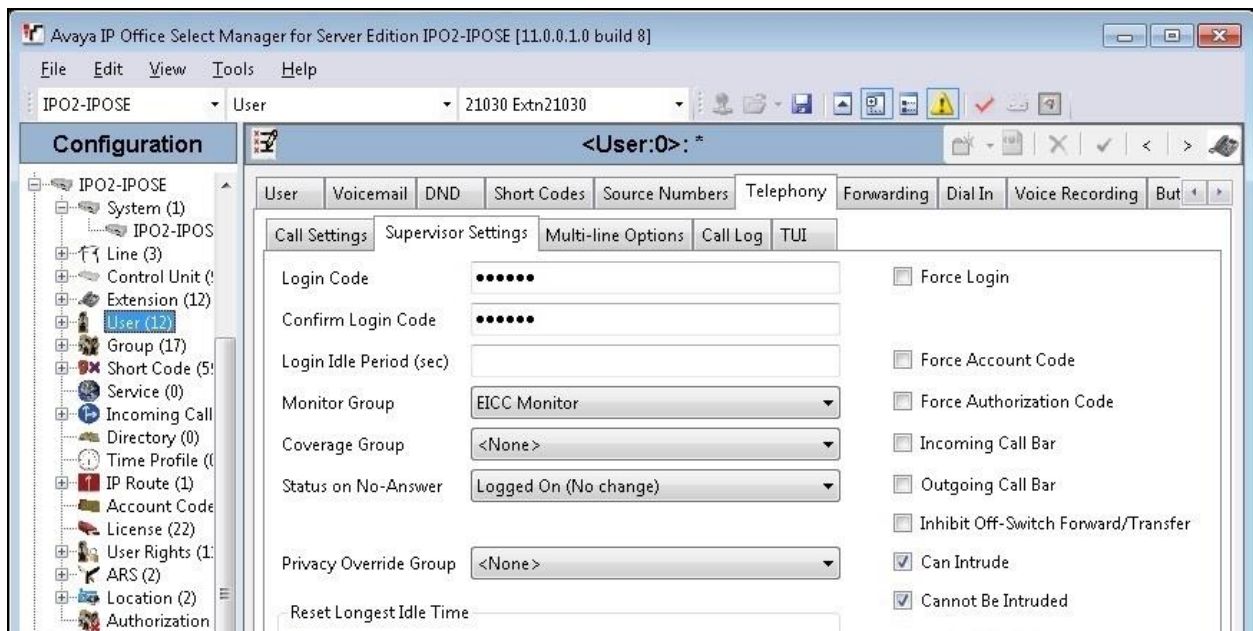
Confirm Voicemail Code

Voicemail Email

- ☐ Voicemail On
- ☐ Voicemail Help
- ☐ Voicemail Ringback

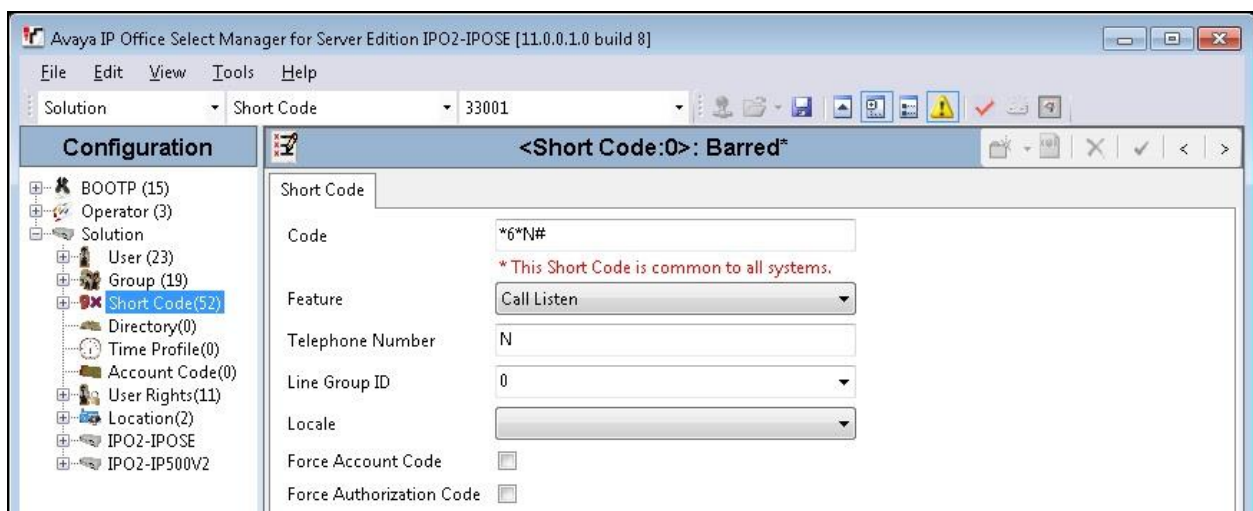
Select the **Telephony** tab, followed by the **Supervisor Settings** sub-tab. Enter desired password for **Login Code** and **Confirm Login Code**. Check **Can Intrude** and **Cannot be Intruded**. For **Monitor Group**, select the EICC Monitor group from **Section 5.2**.

Repeat this section to add a new user for each SIP extension from **Section 5.8**, using the same password for all SIP users as required by EICC. In the compliance testing, two SIP users “21441” and “21442” were created.



5.10. Administer Short Code

From the configuration tree in the left pane, right-click on **Solution → Short Code** and select **New** from the pop-up list to add a new common short code for Call Listen. Configure the fields exactly as shown below. This fixed short code value will be used by EICC to intrude virtual SIP users onto active calls for basic call recording.

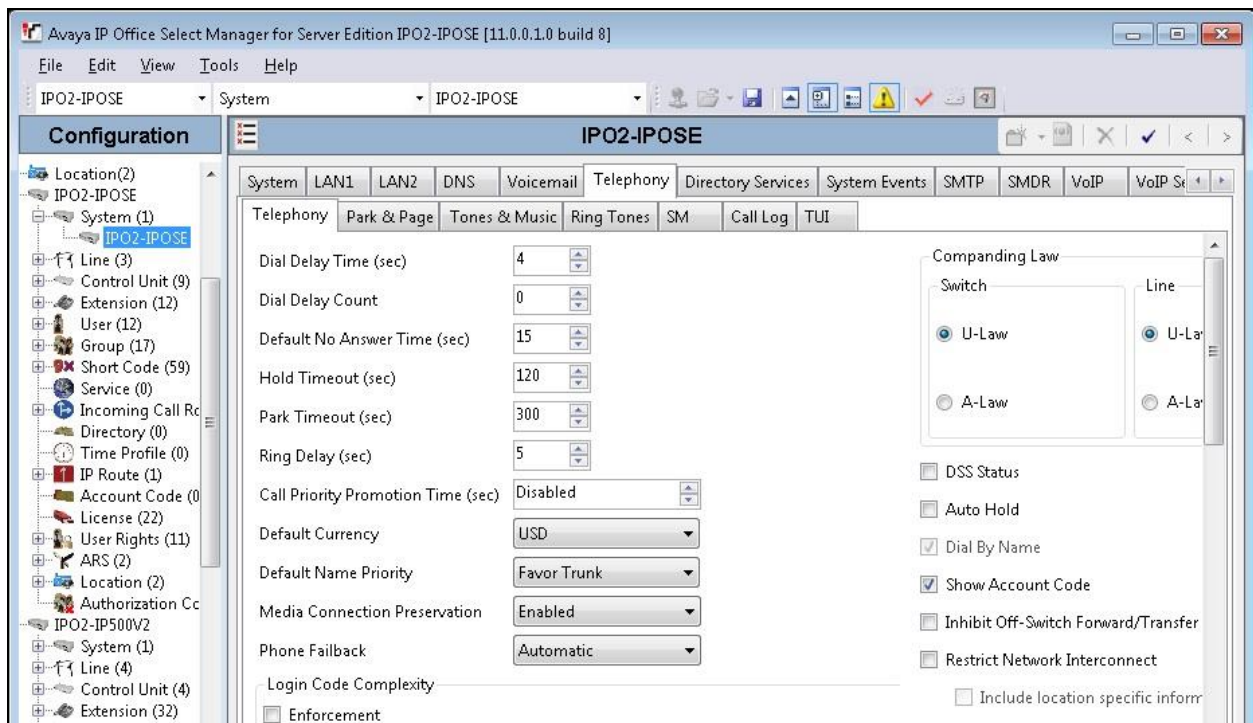


5.11. Administer System Settings

From the configuration tree in the left pane, select **System** under the primary IP Office system to display the system screen in the right pane. Select the **Telephony** tab, followed by the **Telephony** sub-tab in the right pane.

Uncheck **Inhibit Off-Switch Forward/Transfer** to allow call forwarding and transfer with EICC over SIP trunks.

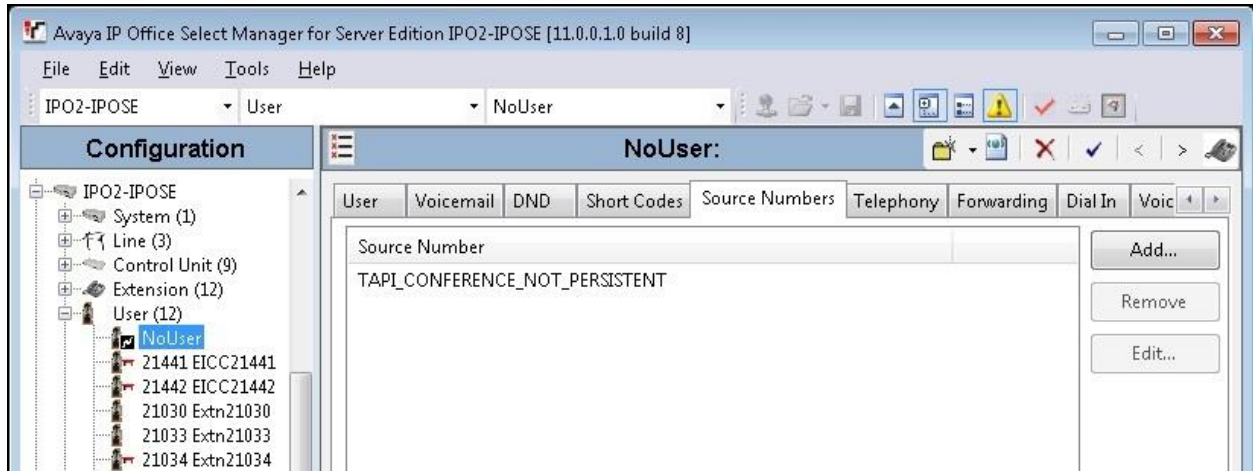
Repeat this section to uncheck **Inhibit Off-Switch Forward/Transfer** on the expansion IP Office system (not shown).



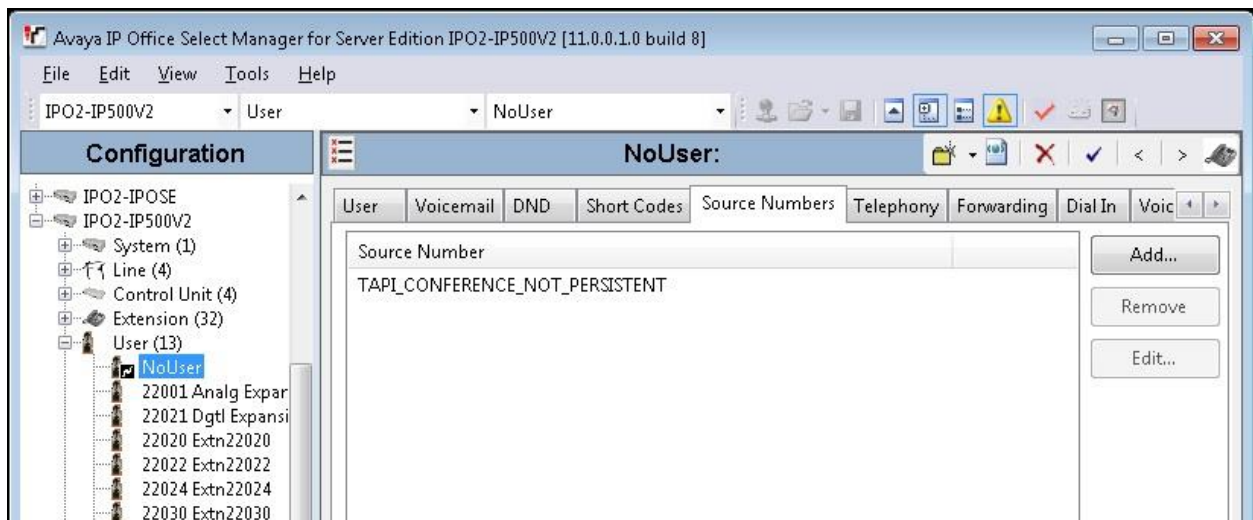
5.12. Administer NoUser Source Number

From the configuration tree in the left pane, select the primary IP Office system, followed by **User → NoUser**. Select the **Source Numbers** tab, and add the source number “TAPI_CONFERENCE_NOT_PERSISTENT” as shown below.

This source number setting enables a conference to be ended when the last remaining internal user exits the conference, and the setting applies to all users on the local IP Office system.



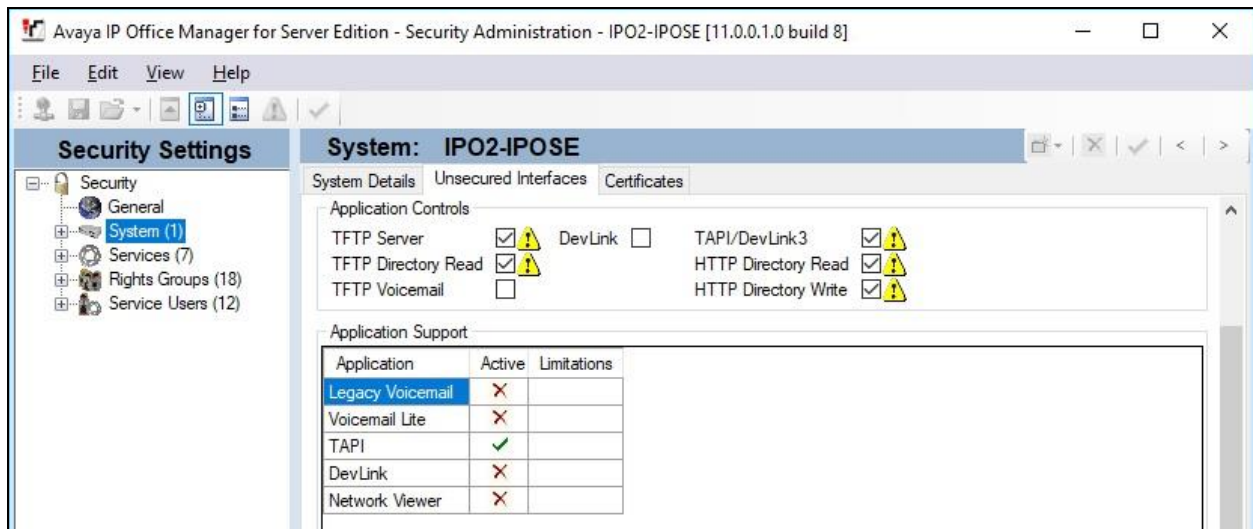
Repeat this section to add the same source number setting to **NoUser** on the expansion IP Office system.



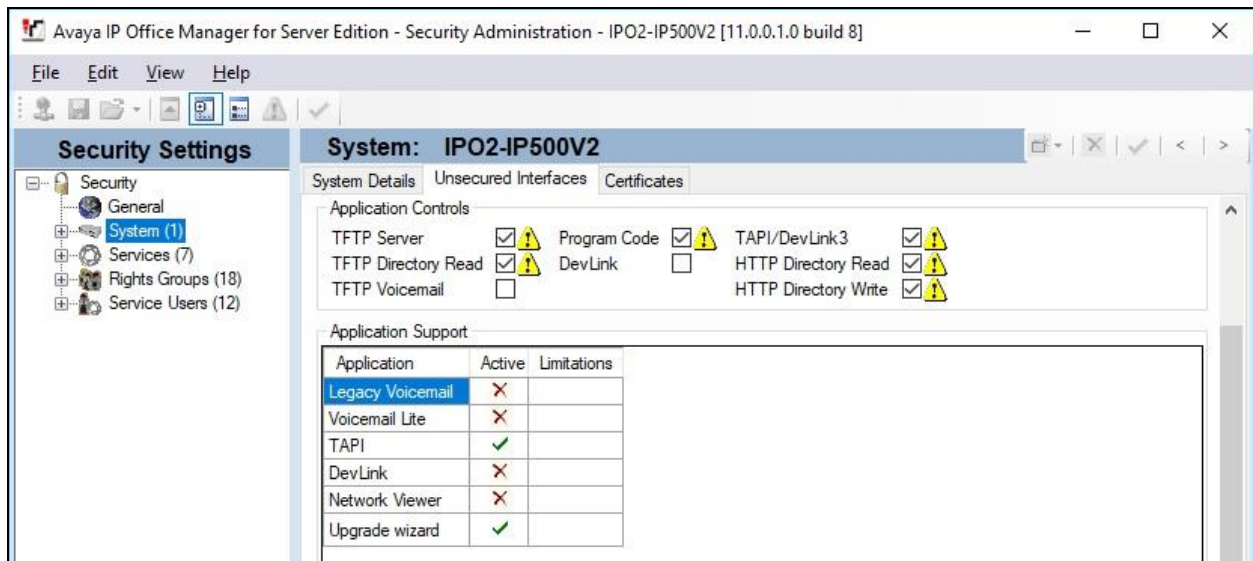
5.13. Administer Security Settings

From the configuration tree in the left pane, select the primary IP Office system, in this case **IPO2-IPOSE** (not shown), followed by **File → Advanced → Security Settings** from the top menu.

The **Avaya IP Office Manager for Server Edition – Security Administration - IPO2-IPOSE** screen is displayed, where **IPO2-IPOSE** is the name of the selected IP Office system. Select **Security → System** to display the **System** screen in the right pane. Select the **Unsecured Interfaces** tab, and check **TAPI/DevLink3** as shown below.



Repeat this section to enable **TAPI/DevLink3** on the expansion IP Office system.



6. Configure Enghouse Interactive Communications Center

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

- Administer TAPI driver
- Administer phone system type
- Administer phone system data
- Verify license
- Administer lines
- Administer queues
- Administer agent login class
- Administer agents and supervisors
- Administer mailboxes
- Administer SIP

Note that all procedures above applies to the primary EICC server, and only the administer TAPI driver procedure applies to the expander EICC server.

The configuration of EICC is typically performed by Enghouse Interactive installation technicians or third party resellers. The procedural steps are presented in these Application Notes for informational purposes.

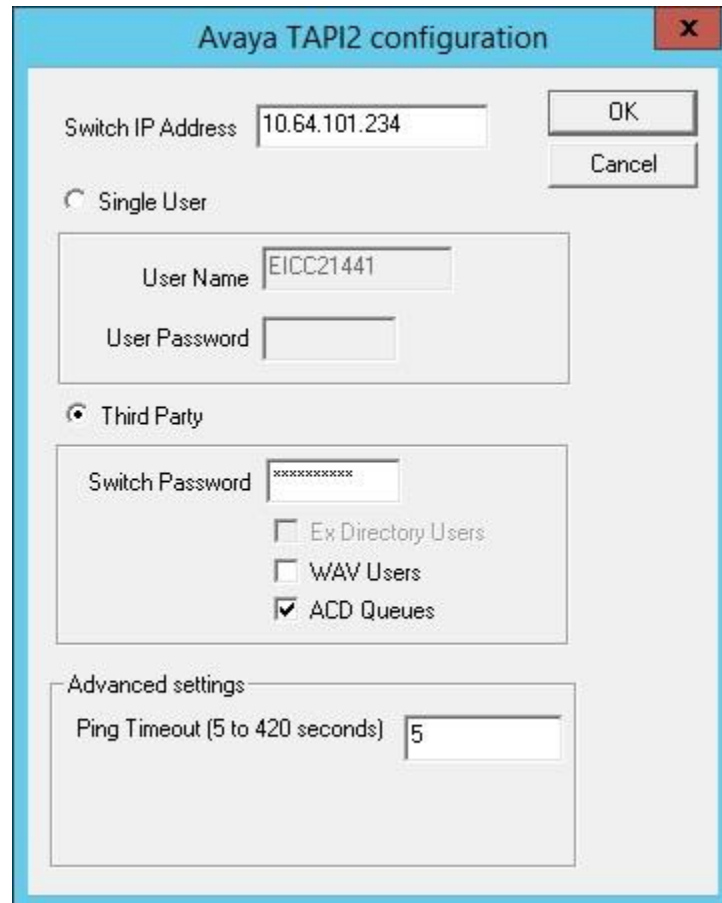
6.1. Administer TAPI Driver

From the primary EICC server, select **Start → Control Panel → Phone and Modem**, to display the **Phone and Modem** screen. Select the **Advanced** tab, followed by **Avaya IP Office TAPI2 Service Provider**, as shown below. Click **Configure**.



The **Avaya TAPI2 configuration** screen is displayed. For **Switch IP Address**, enter the IP address of the primary IP Office system, in this case “10.64.101.234”. Select the radio button for **Third Party**, and enter the applicable IP Office system password into the **Switch Password** field. Check **ACD Queues** as shown below. Reboot the primary EICC server.

Repeat this section to administer TAPI driver on the expander EICC server, and use the IP address and credentials for the expansion IP Office system (not shown).

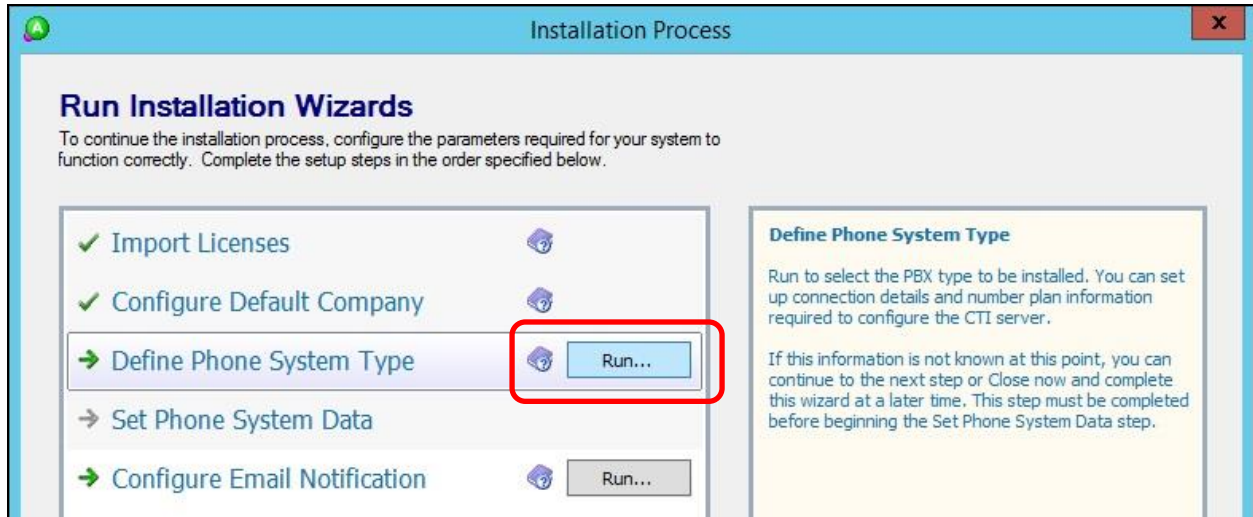


The image shows a screenshot of the 'Avaya TAPI2 configuration' dialog box. The title bar is blue with the text 'Avaya TAPI2 configuration' and a red close button. The dialog has a light gray background. At the top, there is a text field for 'Switch IP Address' containing '10.64.101.234', with 'OK' and 'Cancel' buttons to its right. Below this, there are two radio buttons: 'Single User' (unselected) and 'Third Party' (selected). Under 'Single User', there are text fields for 'User Name' (containing 'EICC21441') and 'User Password' (empty). Under 'Third Party', there is a text field for 'Switch Password' (containing masked characters), and three checkboxes: 'Ex Directory Users' (unchecked), 'WAV Users' (unchecked), and 'ACD Queues' (checked). At the bottom, there is a section titled 'Advanced settings' with a text field for 'Ping Timeout (5 to 420 seconds)' containing the value '5'.

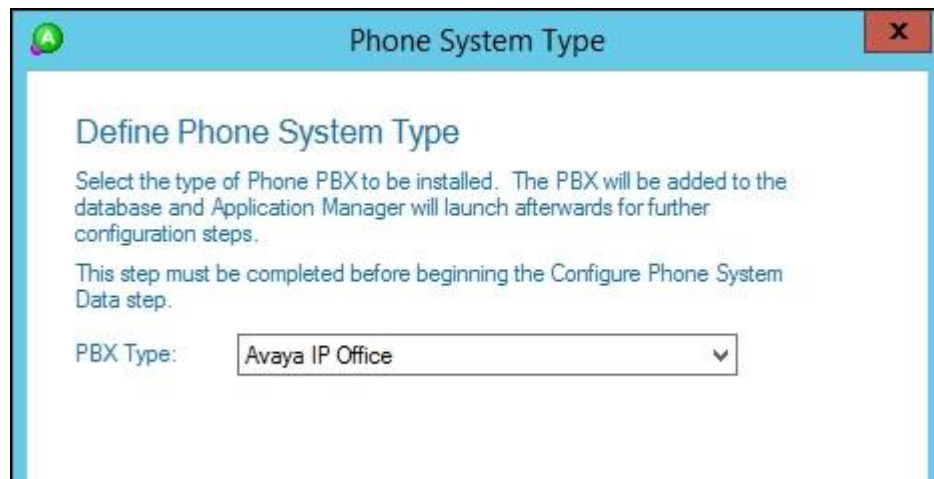
6.2. Administer Phone System Type

At the conclusion of EICC installation, the **Installation Process** screen will be displayed on the primary EICC server by the Installation Wizard. Follow [2] to import licenses and configure the default company.

The **Installation Process** screen shown below is displayed next. Click the **Run** button associated with **Define Phone System Type**.

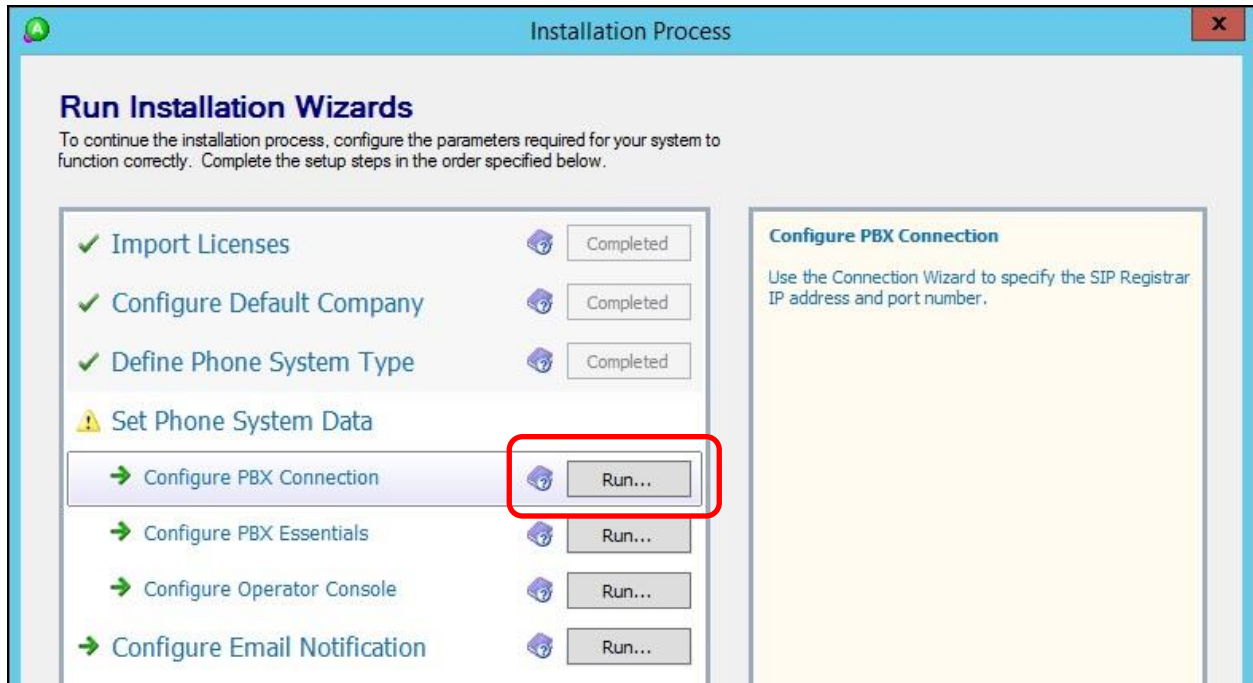


The **Phone System Type** screen is displayed next. For **PBX Type**, select “Avaya IP Office”.



6.3. Administer Phone System Data


The **Installation Process** screen below is displayed. Click the **Run** button associated with **Set Phone System Data** → **Configure PBX Connection** shown below.



The **Avaya IP Office PBX Setup Wizard** → **Configure PBX Connection** screen is displayed next. For **SIP Registrar IP Address**, enter the pertinent LAN IP address of the primary IP Office system from **Section 5.7**.



Continue with the Installation Wizard until the **Avaya IP Office PBX Setup Wizard → Create Park Queue** screen is displayed. For **Park Queue Number**, enter the extension of the EICC Hold group from **Section 5.2**.



The screenshot shows the 'Avaya IP Office PBX Setup Wizard' window with the title 'Create Park Queue'. The text explains that a Park queue is a Hunt Group for parked calls and is not normally dialed by users. A text box for 'Park Queue Number' contains the value '21771'.

Avaya IP Office PBX Setup Wizard

Create Park Queue

The Park queue is a Hunt Group for the management of parked calls.
This number is not normally dialed by users. It must be dialable by any dialogic voiceport installed in the system. This will appear as an entry in the General->System Queues section of this application.

Park Queue Number:

The **Avaya IP Office PBX Setup Wizard → Create Voice Messaging Queue** screen is displayed next. For **Voice Messaging Queue Number**, enter the extension of the EICC Voicemail group from **Section 5.2**.



The screenshot shows the 'Avaya IP Office PBX Setup Wizard' window with the title 'Create Voice Messaging Queue'. The text explains that a Voice Messaging Queue is a Hunt Group used as a Pilot Number for voicemail. A text box for 'Voice Messaging Queue Number' contains the value '21772'.

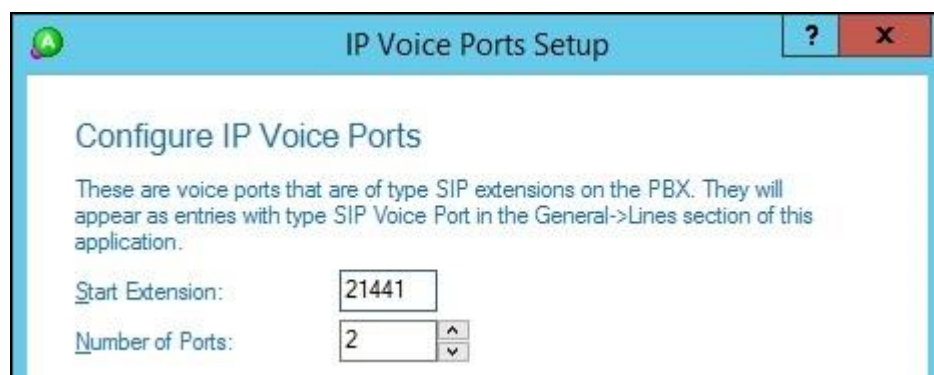
Avaya IP Office PBX Setup Wizard

Create Voice Messaging Queue

The Voice Messaging Queue is a Hunt Group used as the Pilot Number to dial Voicemail. When a user activates a Presence Profile the system will forward their phone to this number. The forward busy destination for users phones will need to be set manually or via the PBX Maintenance interface.
This number is dialed by all users, and is normally an easily remembered number. This will appear as an entry in the General->System Queues section of this application.

Voice Messaging Queue Number:

Continue with the Installation Wizard until the **IP Voice Ports Setup → Configure IP Voice Ports** screen is displayed. For **Start Extension**, enter the first SIP base extension from **Section 5.8**. For **Number of Ports**, select the total number of SIP extensions from **Section 5.8**.



The screenshot shows the 'IP Voice Ports Setup' window with the title 'Configure IP Voice Ports'. The text explains that these are SIP extensions on the PBX. A text box for 'Start Extension' contains '21441' and a spinner box for 'Number of Ports' is set to '2'.

IP Voice Ports Setup

Configure IP Voice Ports

These are voice ports that are of type SIP extensions on the PBX. They will appear as entries with type SIP Voice Port in the General->Lines section of this application.

Start Extension:

Number of Ports:

6.4. Verify License

The **Communications Center Administrator** screen is displayed upon completion of the Installation Wizard. Select **General** → **Licenses** from the left pane, to display **All Licenses** in the right pane. Verify that the following licenses are in place: **Avaya IP Office**, **CC SIP Ports**, **CT Control**, **TouchPoint**, and **UCUL (UC User License)**.

Communications Center Administrator - [Licenses]

File Edit Window Help

Language: English

Import/Register Licenses... Product Key: 92TV-DYUC-TZKZ-620S-PQA6

All Licenses

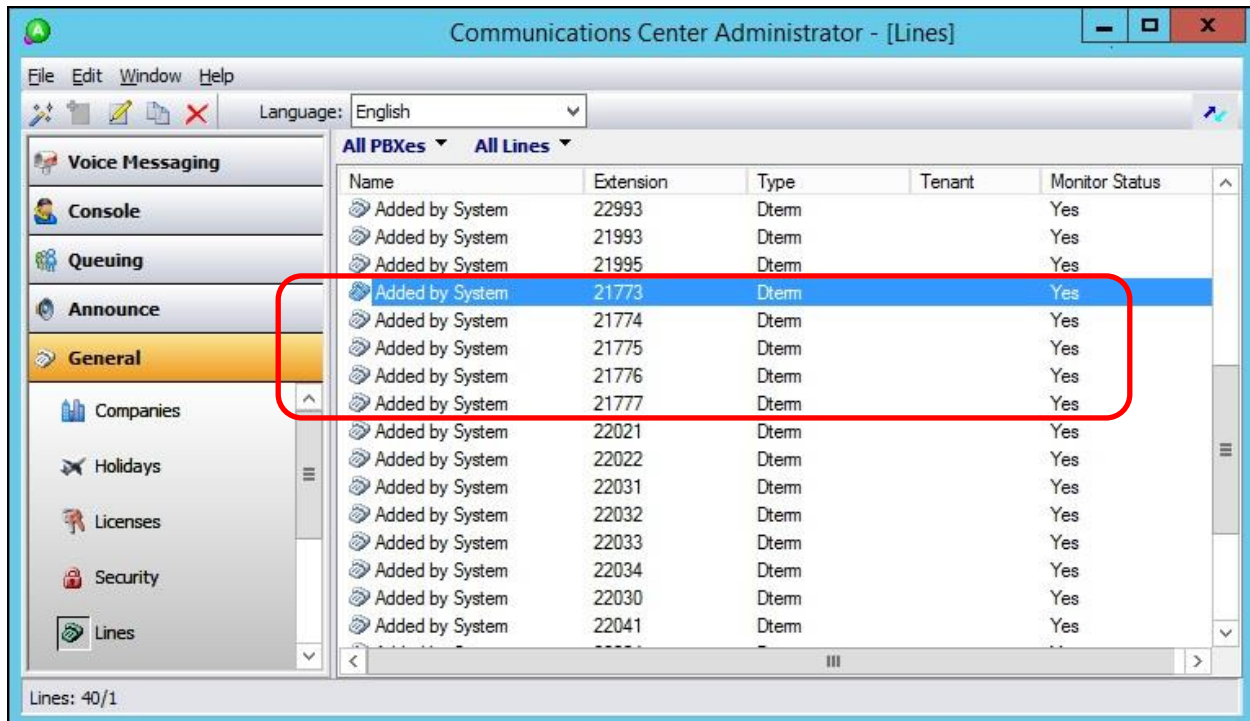
Description	Licenses	Units	Start Date	End Date
AdvancedChat	23	User		
Agent Desktop	23	User		
Announce	23	Port		
Autodial IVR	23	Port		
Avaya IP Office	1	units		
Callback	1	units		
CC SIP Ports	23	Port		
Community WFM Agent Adh...	23	units		
Community WFM Plugin	1	units		
CT Control	23	User		
Enhanced Routing Plugin	1	units		
Integration SDK Plug-in	23	User		
IVR	23	Port		
MediaExtraction	1	Site		
MM1 Chat Queuing	23	User		
MM1 Web Callback Queuing	23	User		
Multimedia ALL	23	User		
QMS Gateway	1	units		
Redundancy	1	units		
SalesforcePlugin	23	units		
SMS Gateway	1	units		
Snapshot	23	units		
Survey	1	units		
Teleopti WFM Agent Adhere...	1	units		
Teleopti WFM Plugin	1	units		
Third Party Email Plug-in	1	units		
TouchPoint	23	User		
TouchPoint Console	23	User		
TouchPoint UC User	23	User		
UCUL (UC User License)	23	User		
Unified Messaging for Excha...	23	User		
Web Browser Plug-in	23	units		
Work Force Scheduler	23	units		

Licenses: 33/1

6.5. Administer Lines

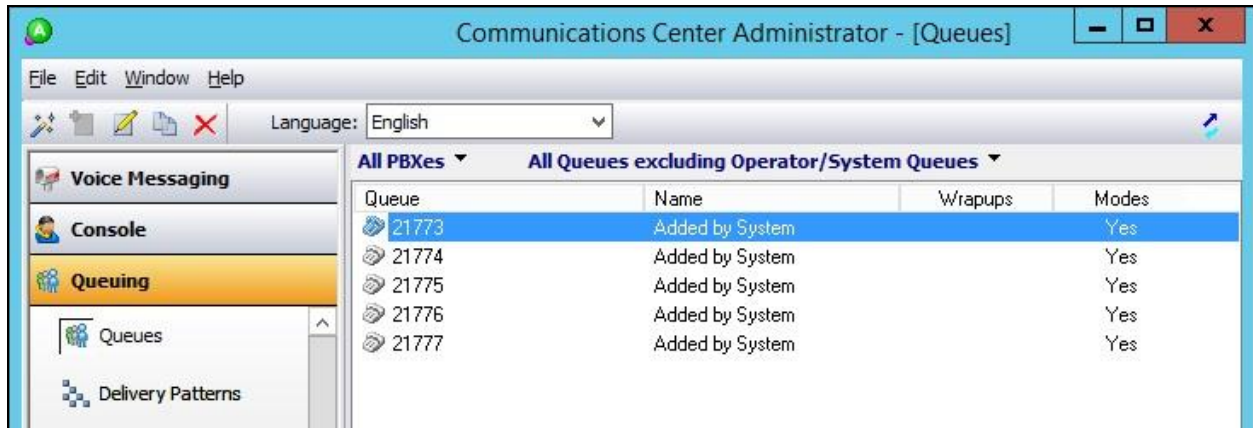
Select **General** → **Lines** from the left pane, to display all extensions obtained automatically from both IP Office systems. Locate the entries associated with a subset of the EICC groups from **Section 5.2**, in this case extensions “21773-21777”, right-click on the entries one at a time and select **Convert Into Queue**.

Note that the EICC groups with extensions “21771-21772” were already configured as part of the Installation Wizard in **Section 6.3**.



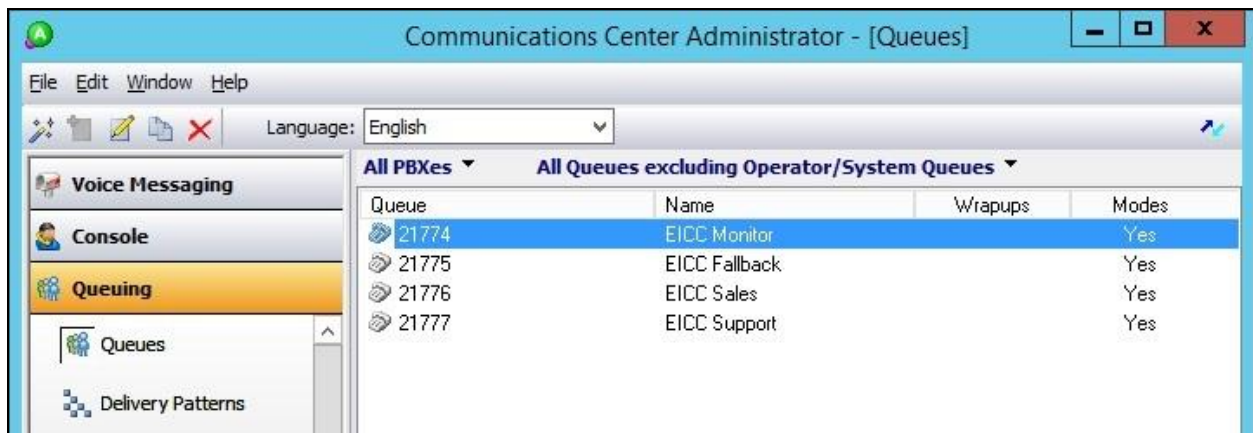
6.6. Administer Queues

Select **Queuing** → **Queues** from the left pane, to display a list of queues converted from **Section 6.5**. Right click on the entry associated with the EICC Operator group from **Section 5.2**, in this case extension “21773”, and select **Convert to Operator Queue**.



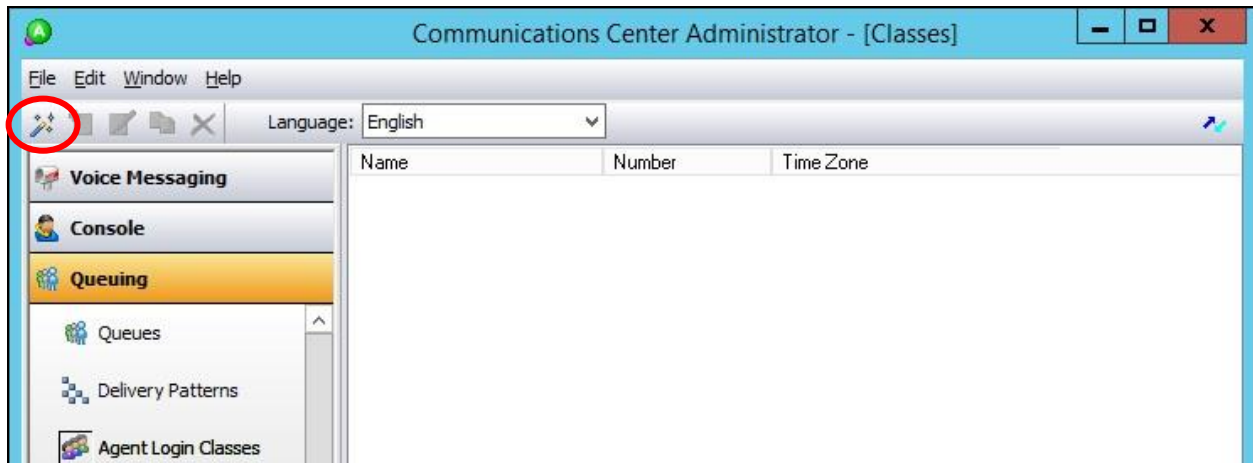
Right click on each remaining entry, and select **Edit** to modify the **Name** as desired. The queue name will be used in agent desktop screen pops.

In the compliance testing, the queues were modified to match corresponding group names from **Section 5.2**, as shown below.

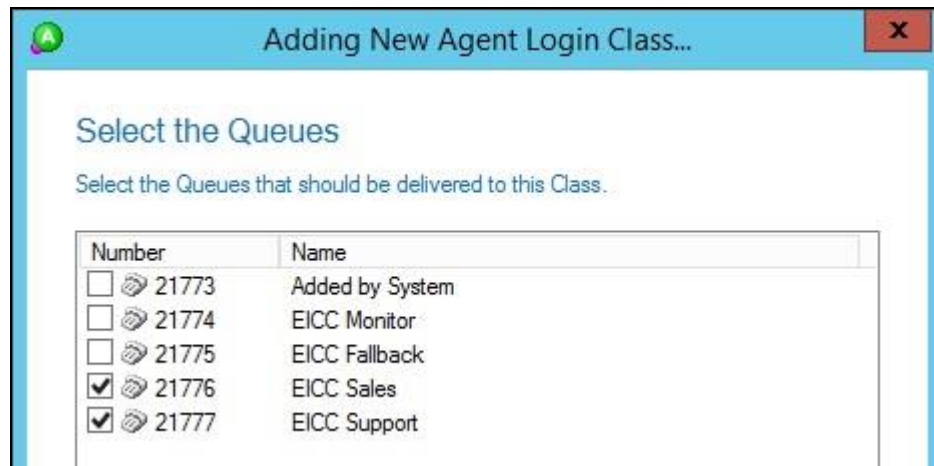


6.7. Administer Agent Login Class

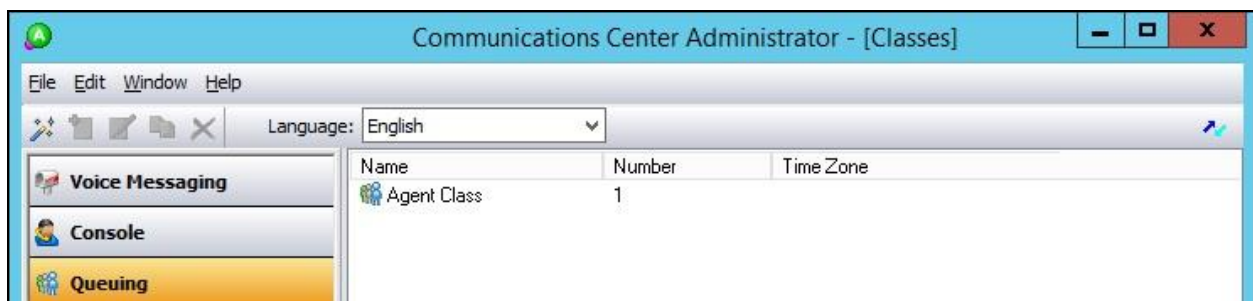
Select **Queuing** → **Agent login Classes** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



Follow the **Adding New Agent Login Class Wizard** in the subsequent screens to configure a new agent login class. In the **Select the Queues** screen, select the EICC Sales and EICC Support queues created from **Section 6.6**, as shown below.



In the compliance testing, one agent login class was created, as shown below.



6.8. Administer Agents and Supervisors

Select **Queuing** → **Agents** (not shown) from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



Follow the **Add Agent Wizard** in the subsequent screens to configure a corresponding entry for each agent and supervisor from **Section 5.4** and **Section 5.6** respectively. In the **Select Agent Login Class** screen, select the agent login class created from **Section 6.7**, as shown below.

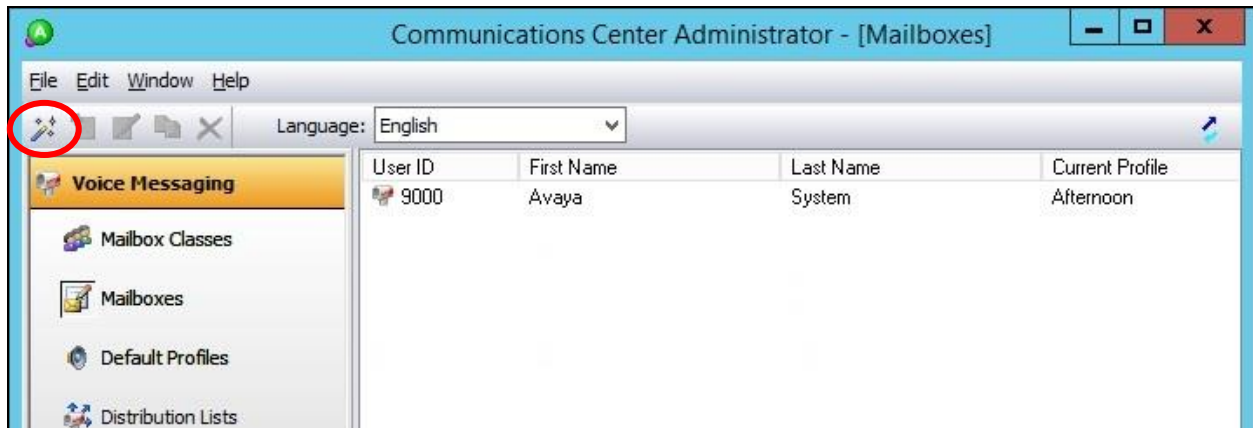


In the compliance testing, four agents and two supervisors were created as shown below.

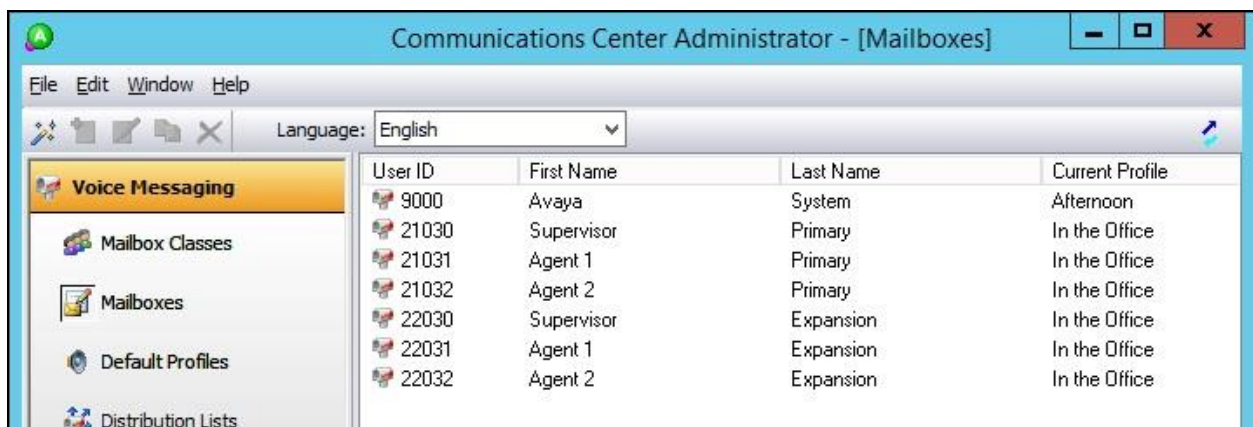


6.9. Administer Mailboxes

Select **Voice Messaging** → **Mailboxes** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



Follow the **Add Mailboxes Wizard** in the subsequent screens (not shown) to configure a corresponding mailbox for each agent and supervisor from **Section 6.8**. In the compliance testing, six mailboxes were created as shown below.

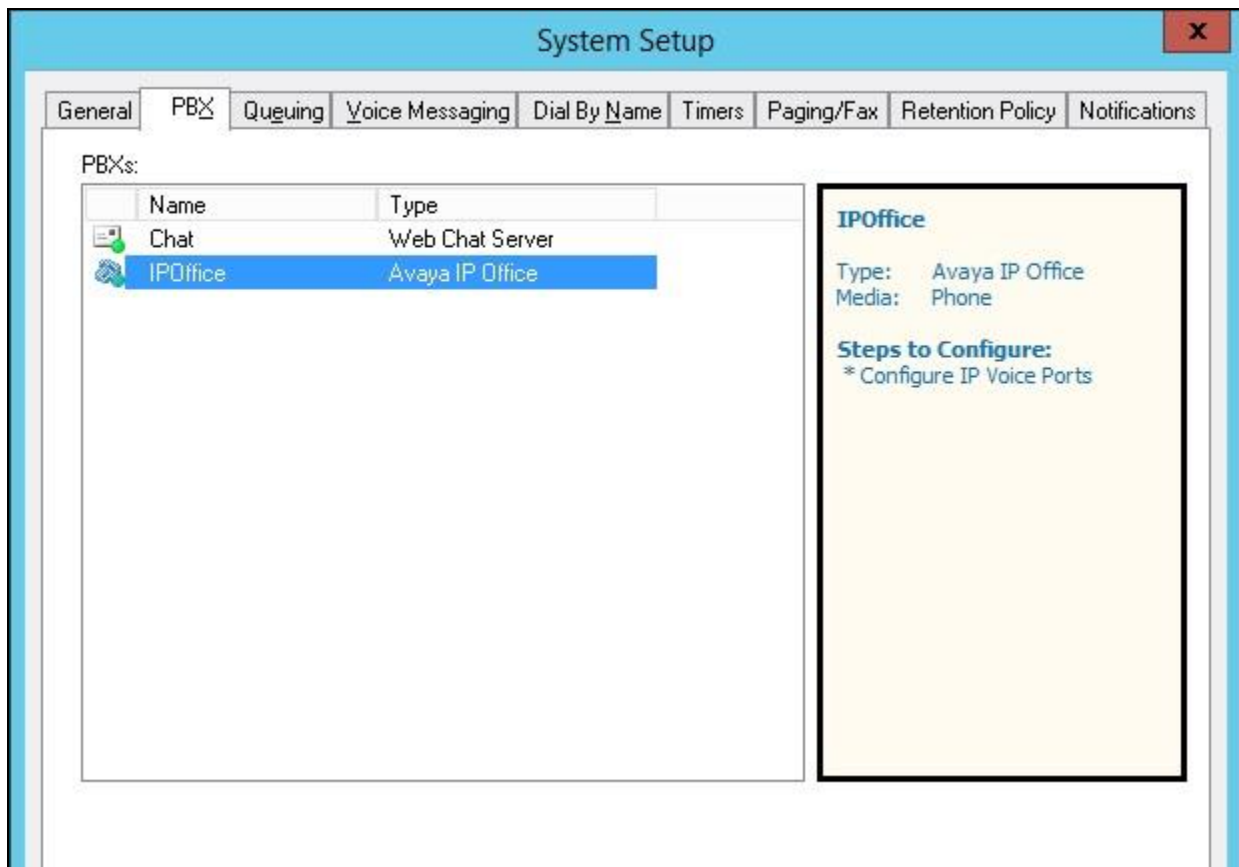


6.10. Administer SIP

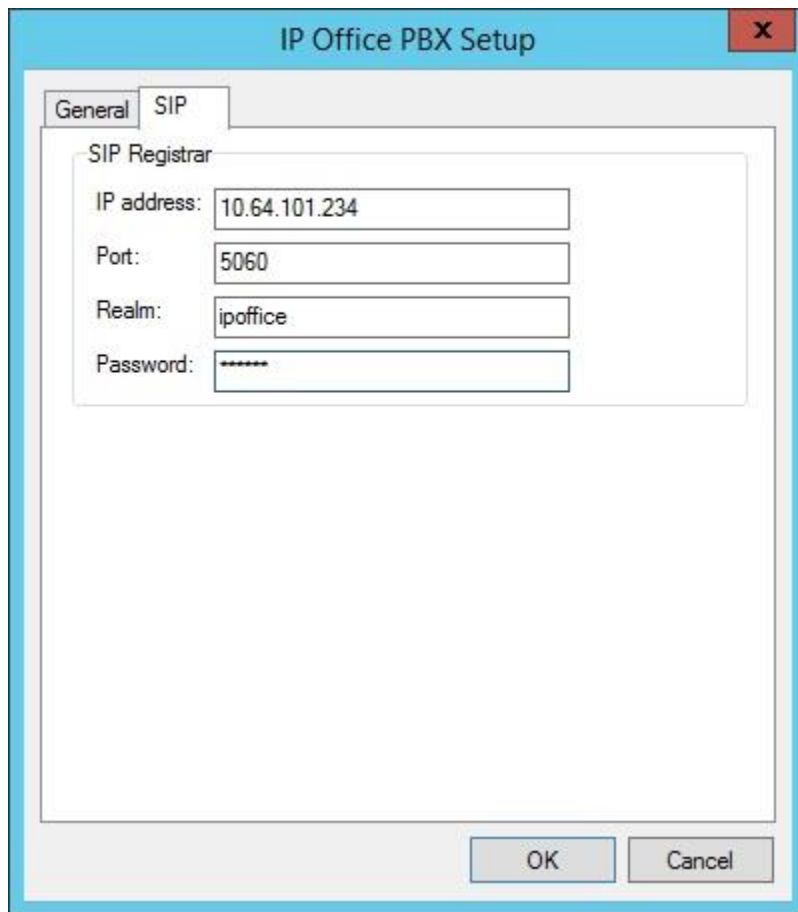
Select **File** → **System Setup** from the top menu, as shown below.



The **System Setup** screen is displayed. Select the **PBX** tab, and double click on the IP Office entry shown below.



The **IP Office PBX Setup** screen is displayed. Select the **SIP** tab. For **Realm**, enter “ipoffice”. For **Password**, enter the common SIP user login code password from **Section 5.9**. Retain the default value in the remaining fields.



The screenshot shows a window titled "IP Office PBX Setup" with a close button (X) in the top right corner. Inside the window, there are two tabs: "General" and "SIP". The "SIP" tab is selected. Below the tabs, there is a section labeled "SIP Registrar" containing four input fields: "IP address:" with the value "10.64.101.234", "Port:" with the value "5060", "Realm:" with the value "ipoffice", and "Password:" with a masked value represented by six asterisks. At the bottom right of the window, there are two buttons: "OK" and "Cancel".

7. Verification Steps

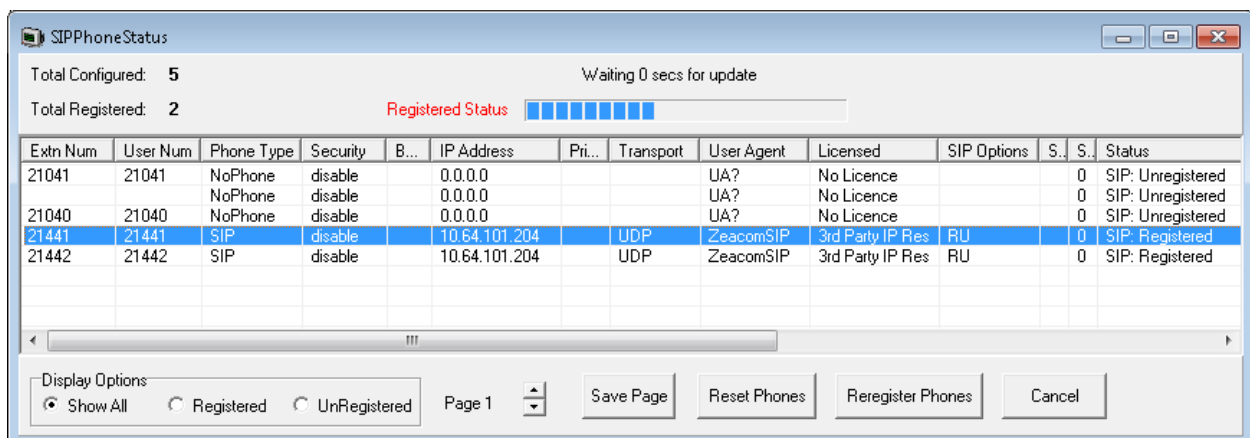
This section provides tests that can be performed to verify proper configuration of IP Office Server Edition and EICC.

7.1. Verify Main Site

From a PC running the IP Office Monitor application, select **Start → All Programs → IP Office → Monitor** to launch the application, and connect to the primary IP Office system. The **Avaya IP Office SysMonitor** screen is displayed. Select **Status → SIP Phone Status** from the top menu.



The **SIPPhoneStatus** screen is displayed. Verify that there is an entry for each SIP extension from **Section 5.8** and that the **Status** is “SIP: Registered“, as shown below.



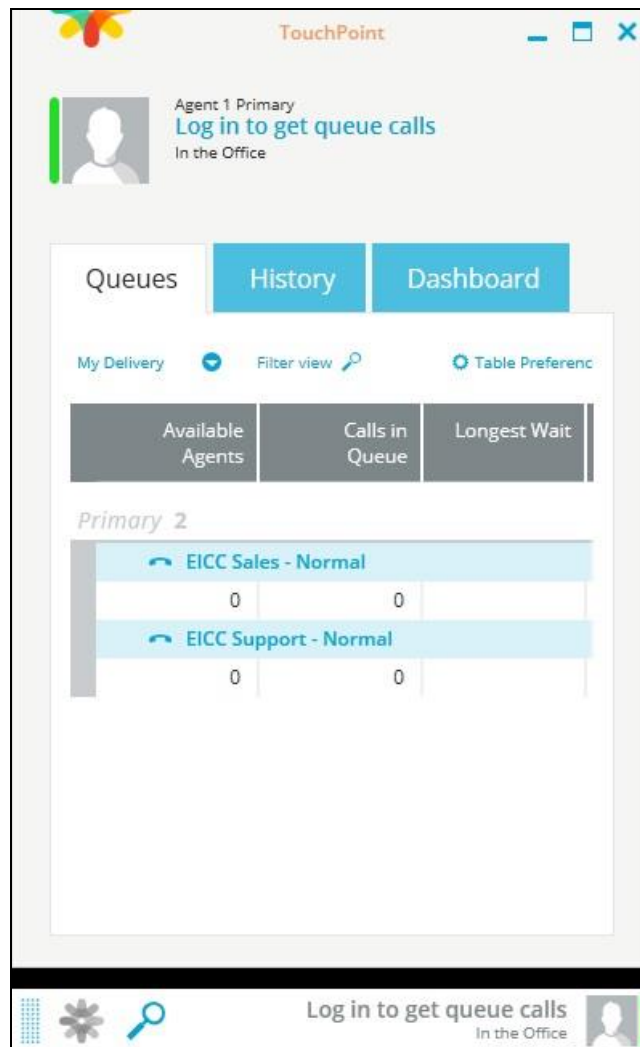
From the agent desktop, double-click on the **TouchPoint** shortcut icon shown below, which was created as part of TouchPoint installation.



The **Enghouse Interactive TouchPoint** login screen below is displayed. Enter the login name associated with an agent on the Main site from **Section 6.8**, and use the generic default PIN value from EICC. Retain the default value in the remaining fields.

A screenshot of the Enghouse Interactive TouchPoint login screen. At the top left is a large version of the colorful flower logo. Below it, the text "Enghouse Interactive TouchPoint" is displayed in a large, black, sans-serif font. In the top right corner, there is a small blue "X" icon. Below the title, there are two input fields. The first field contains the text "agent 1 primary". The second field contains four black dots, indicating a password. Below the password field is a checkbox with a blue checkmark inside, followed by the text "Remember me". At the bottom center, there is a blue rectangular button with the text "Open TouchPoint" in white. The entire screen is enclosed in a thin black border.

The **TouchPoint** screen is displayed, along with a Call Bar above the system tray, as shown below. Click on **Log in to get queue calls** toward the top of the screen.

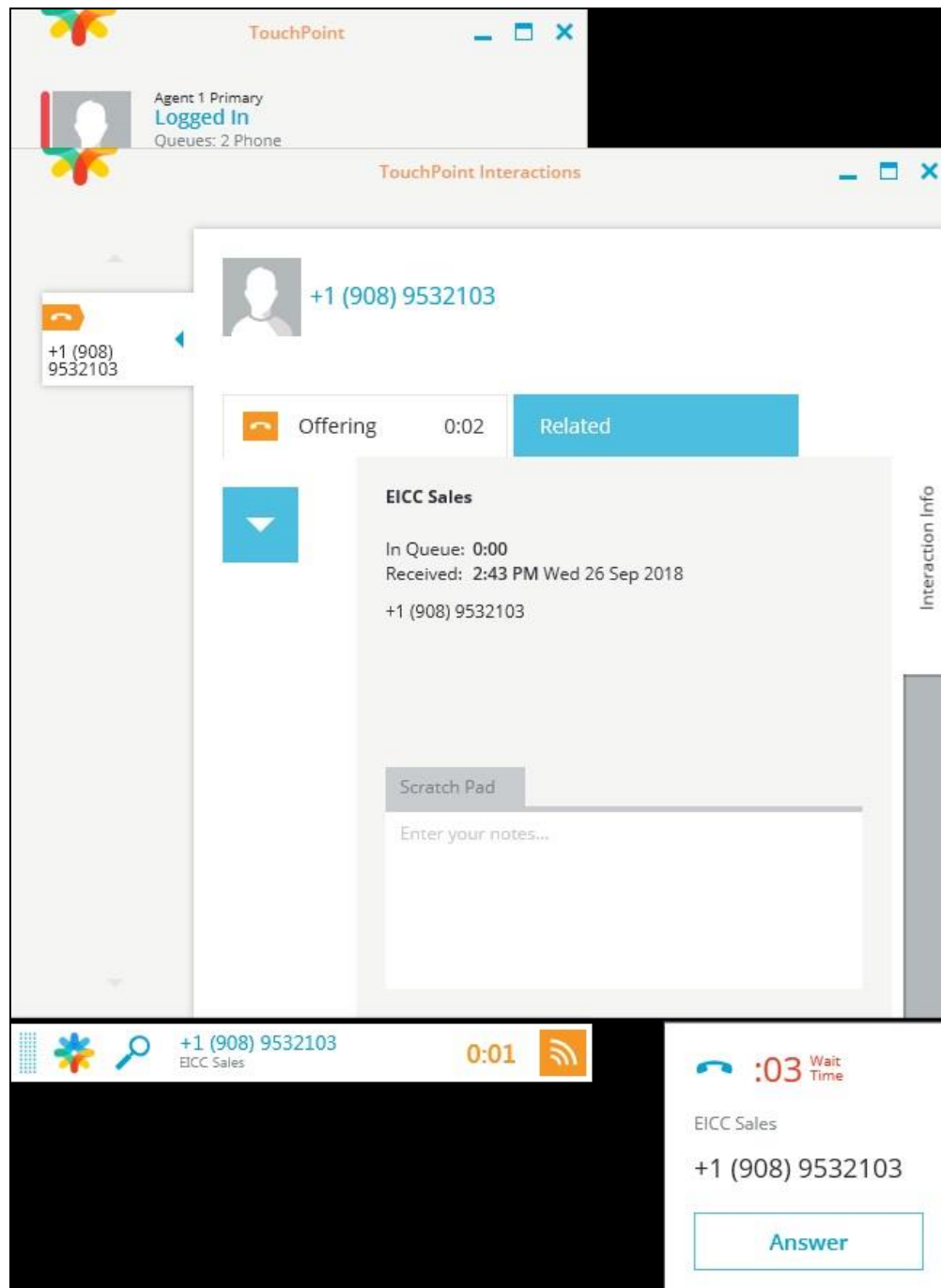


In the drop-down window, Select **Log in to Queues**, as shown below.



Make an incoming call from PSTN to the EICC Sales group, with available agent “21031” at the Main site. Verify that the agent desktop is populated with a **TouchPoint Interactions** screen with an **Offering** tab, along with a Pop-up Notification box, and that the Call Bar is updated to reflect the active call.

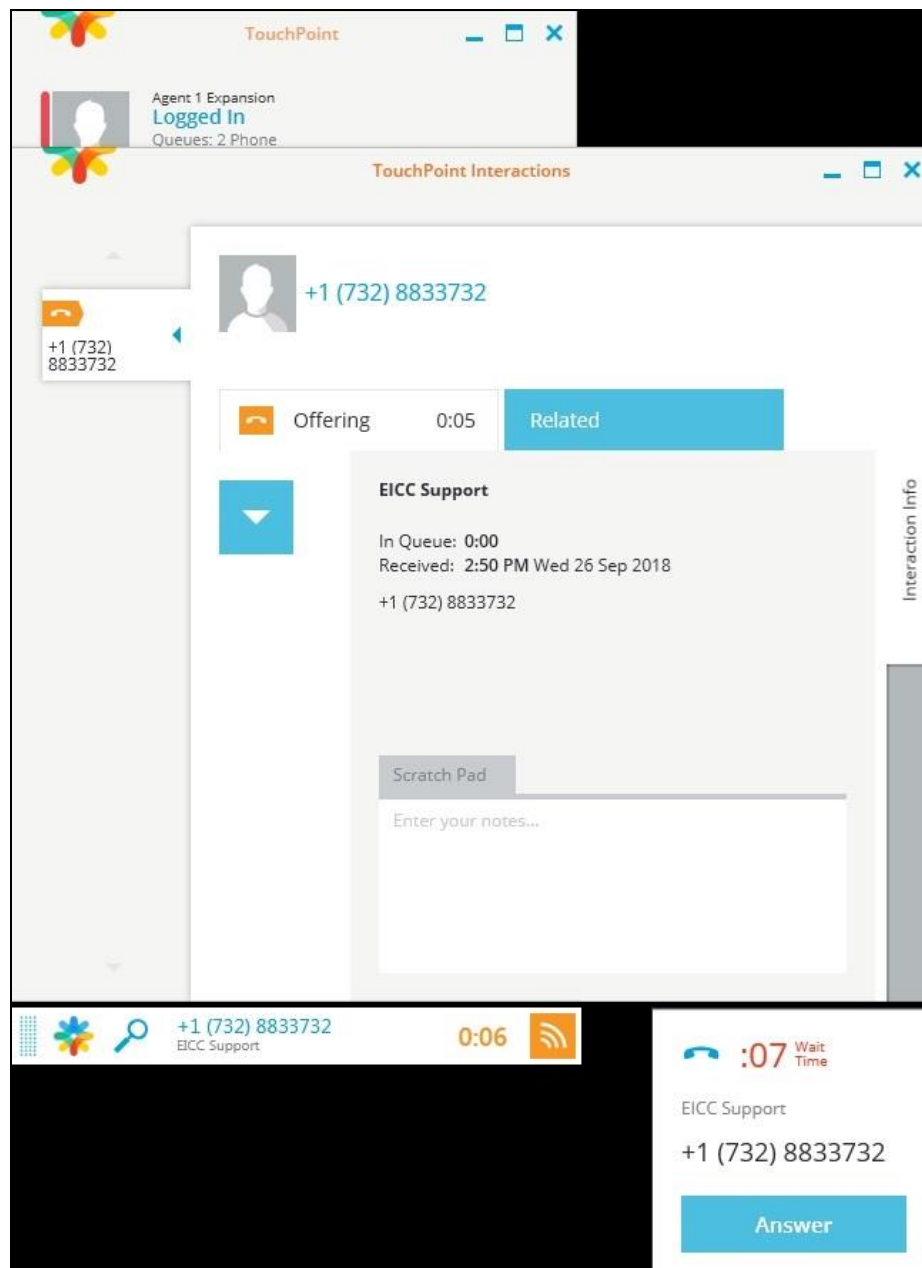
Click **Answer** from the Pop-up Notification box, and verify that the agent is connected to the PSTN caller with two-way talk paths.



7.2. Verify Remote Site

Repeat the procedures in **Section 7.1** to log in an agent on the Remote site into the queues. Make an incoming call from PSTN to the EICC Support group, with available agent “22031” at the Remote site. Verify that the agent desktop is populated with an **Interaction Info** screen with an **Offering** tab, along with a Pop-up Notification box, and that the Call Bar is updated to reflect the active call.

Click **Answer** in the Pop-up Notification box, and verify that the agent is connected to the PSTN caller with two-way talk paths.



8. Conclusion

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 10.1 to successfully interoperate with Avaya IP Office Server Edition 11 using the TAPI and SIP user interfaces. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

9. Additional References

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

1. *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, Issue 17a, August 2018, available at <http://support.avaya.com>.
2. *First-time Installation and Server Setup – IP Office*, July 2018, available at <https://partnerportal.enghouseinteractive.com/user/login>.
3. *IP Office PBX Programming Manual*, July 2018, available at <https://partnerportal.enghouseinteractive.com/user/login>.

©2018 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.