



Avaya Solution & Interoperability Test Lab

Application Notes for estos GmbH estos ECSTA with Avaya IP Office Server Edition – Issue 1.0

Abstract

These Application Notes describe the configuration steps necessary for provisioning estos ECSTA v6.0 to successfully interoperate with Avaya IP Office Server Edition R11.1.

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 necessary for provisioning estos GmbH estos ECSTA v6 to successfully interoperate with Avaya IP Office Server Edition R11.1. estos ECSTA for Avaya IP Office is middleware which integrates with Avaya IP Office using the Centralized CTI Web Services API to provide, call control, device control and call monitoring.

Note: Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as an expansion cabinet. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and user names. This allows calls between systems and support for a range of internal call features. A connection to IP Office 500 V2 as a standalone is possible with the use of an IP Office Application Server but this was not the focus of these Application Notes.

Centralized CTI Web Services API was introduced on IP Office Server Edition R11.0 and provides, along with other services, Telephony functionality. With previous versions of IP Office, a TAPI connection to each IP Office node was required in order to provide call control and device control. With the introduction of Centralized CTI Web Services API, a single third-party server is now the requirement which will provide telephony functionality for all IP Office nodes. Centralized CTI Web Services uses one-X® Portal, which is installed with IP Office Server edition by default, and this must be configured along with some security settings on IP Office, (see **Section 5**).

2. General Test Approach and Test Results

The test approach was to connect estos ECSTA to IP Office using the Web Services API to obtain information on all the IP Office devices and then use a phone application to make and receive calls on these devices. The estos ECSTA TAPI driver was installed on a Windows 10 64bit PC. On the same PC, the phone application EPhone.exe was installed and was used to monitor and control Avaya H.323, SIP IP and Digital telephones, using the Web Services API via the IP Office Primary server. Inbound and outbound calls to the PSTN were made using simulated PSTNs.

The IP Office Centralized CTI Web Services API Telephony functionality includes:

- Make/Answer/Disconnect a call.
- Place a call on hold and retrieve a held call.
- Swap Hold.
- Transfer a call (Supervised & Blind).
- Initiate a conference/Drop a conference participant/Disconnect a conference.
- Call Forwarding, (all, CFNA and Busy).
- Generate DTMF tones.
- Mute/Unmute.
- Do Not Disturb.

Note: A client was not used during compliance testing. Instead, a test harness called EPhone.exe provided by estos was used to demonstrate call control of the IP Office endpoints which included both IP and Digital phones.

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 IP Office and estos ECSTA did use a secure SSL link.

2.1. Interoperability Compliance Testing

The objective of Interoperability Compliance Testing is to provide assurance to the potential customers that the tested products operate as specified and can interoperate in an environment similar to the one that will be encountered at a customer's premises. The interoperability compliance testing focused ensuring that the connection between estos ECSTA and IP Office was successful and to do that the following tests were carried out using EPhone.exe.

- Answer incoming calls both from internal and external callers.
- Make calls to internal and external numbers.
- Hold/Unhold incoming and outgoing calls.
- Transfers (Blind/Supervised).
- Transfers to External/Mobile numbers.
- Set/Cancel Call Forwards.
- Serviceability testing, which focused on verifying the behaviour of estos ECSTA under different simulated LAN failures.

2.2. Test Results

Tests were performed to ensure full interoperability of IP Office with estos ECSTA. Performance and load testing is outside the scope of the compliance testing. All the test cases passed successfully.

2.3. Support

Information on estos and product support can be obtained through the following:

- Online: <https://support.estos.de/de>
- Phone: + 49 (8151) 36856-177

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an IP Office Server Edition Primary Server and IP500V2 Expansion. The estos ECSTA makes use of the Web Services API to provide telephony functions that allow for third party call control of all Avaya phones. A variety of Avaya deskphones were used to generate intra-switch calls (calls between phones on the same system), and outbound/inbound calls to/from the PSTN.

Note: Two simulated PSTN lines was used, consisting of a SIP trunk connection to Session Manager and an ISDN ETSI link to Communication Manager.

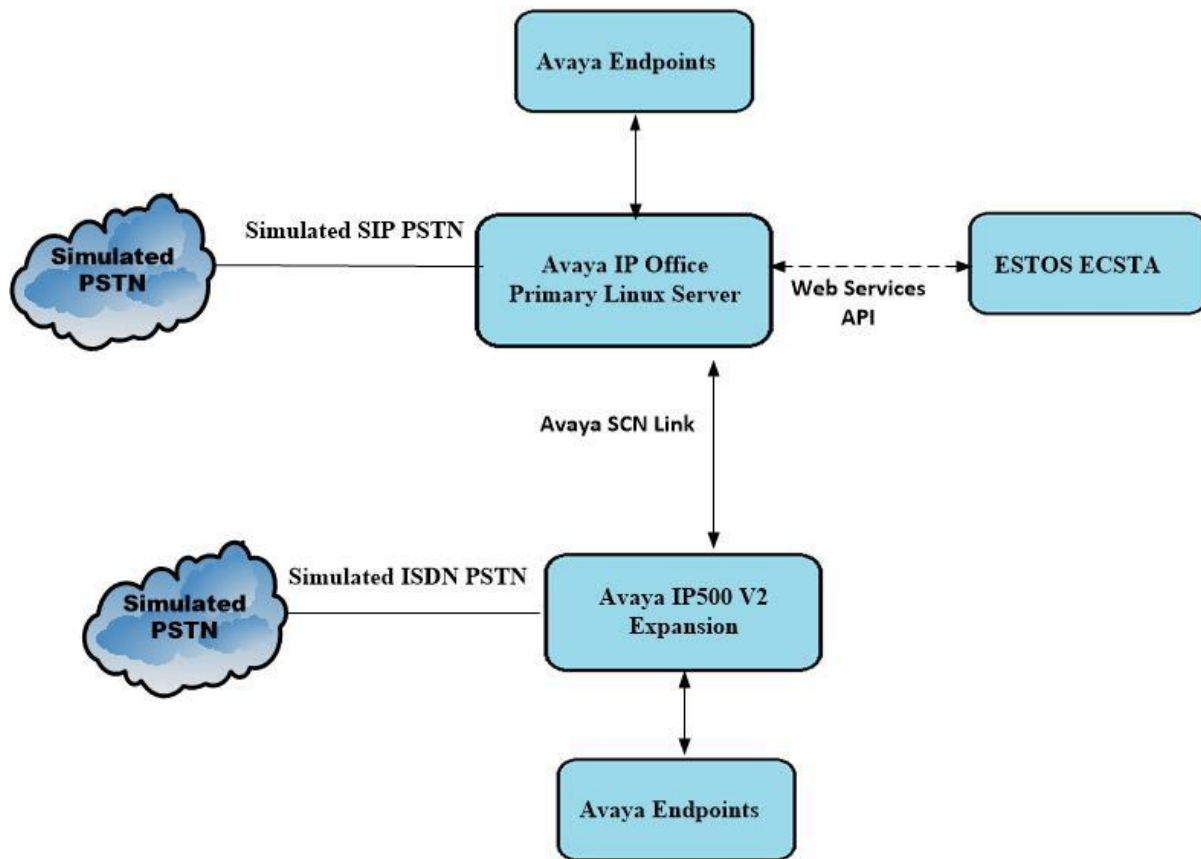


Figure 1: Avaya IP Office Server Edition and estos ECSTA reference configuration.

4. Equipment and Software Validated

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

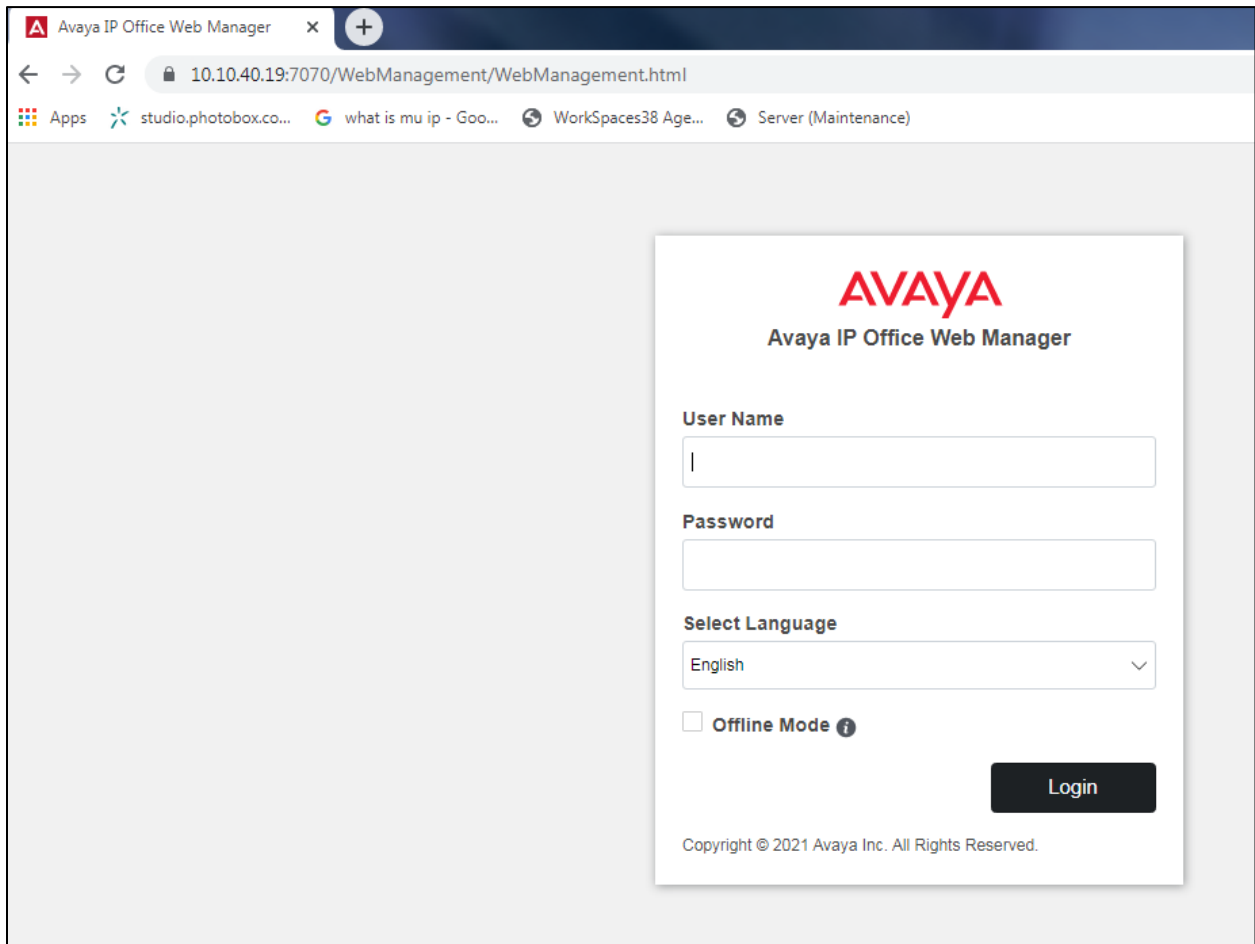
Equipment/Software	Release/Version
Avaya IP Office Server Edition running on a Virtual Platform	11.1.2.0.0 Build 239
Avaya IP Office 500 V2 Expansion	11.1.2.0.0 Build 239
Avaya J179 IP Phone (H.323)	6.8304
Avaya J159 IP Phone (SIP)	4.0.7.0.7
Avaya 9508 Digital	2.0
estos GmbH estos ECSTA	6.0.7.889

Note: Compliance Testing is applicable when the tested solution is deployed with IP Office Server Edition in any configuration. For a standalone IP500V2 configuration an additional Avaya IP Office Application Server is required and was not tested as part of this compliance testing.

5. Configure Avaya IP Office

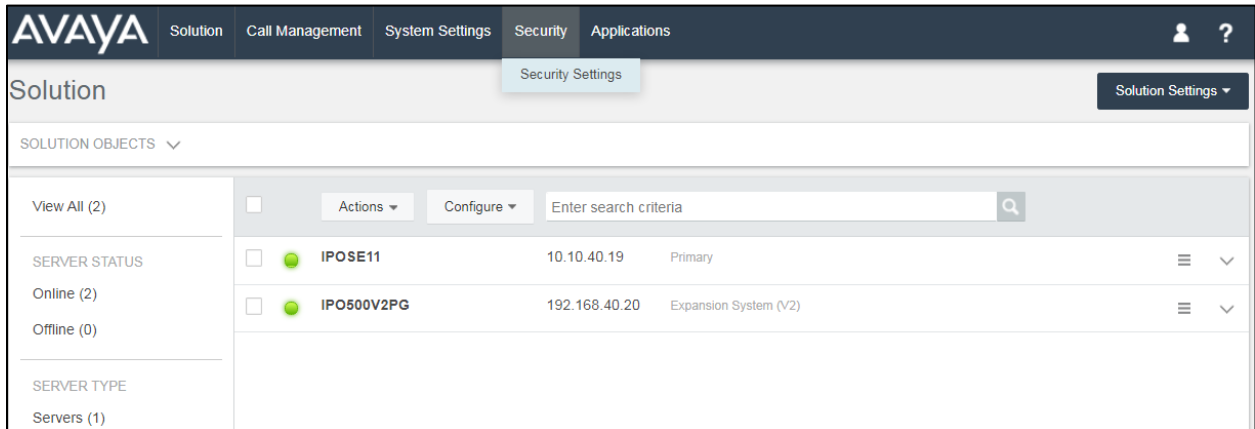
The configuration of IP Office can be carried out using the traditional IP Office Manager or the newer IP Office Web Manager. For this setup IP Office Web Manager was used to configure the connection to estos ECSTA. A new Rights Group and Service User were added specifically for the connection to estos ECSTA.

Open a URL to the IP Address of the IP Office Server Edition and enter the appropriate credentials, as shown below.

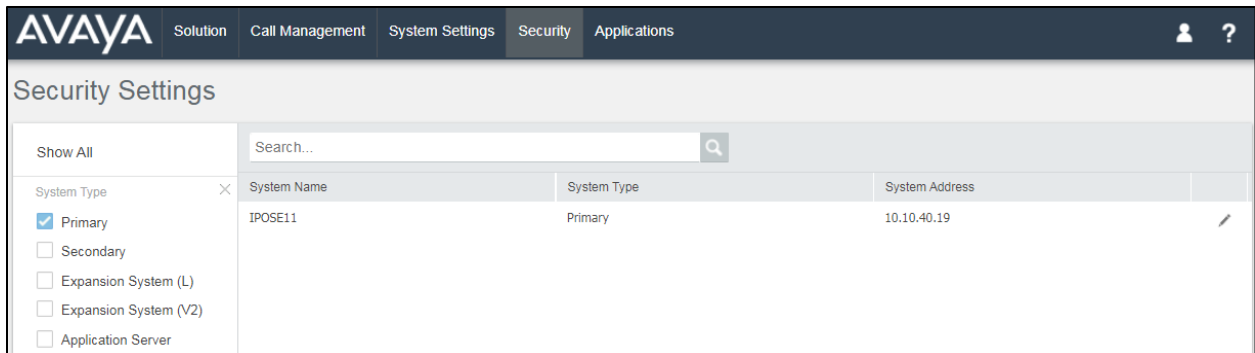


The image shows a browser window with the Avaya IP Office Web Manager login page. The browser's address bar shows the URL `10.10.40.19:7070/WebManagement/WebManagement.html`. The page features the Avaya logo and the text "Avaya IP Office Web Manager". Below this, there are three input fields: "User Name" (containing a single vertical bar), "Password", and "Select Language" (set to "English"). There is also an "Offline Mode" checkbox which is unchecked. A "Login" button is located at the bottom right of the form. At the very bottom of the page, the copyright notice "Copyright © 2021 Avaya Inc. All Rights Reserved." is visible.

From the top menu, navigate to **Security** → **Security Settings**.

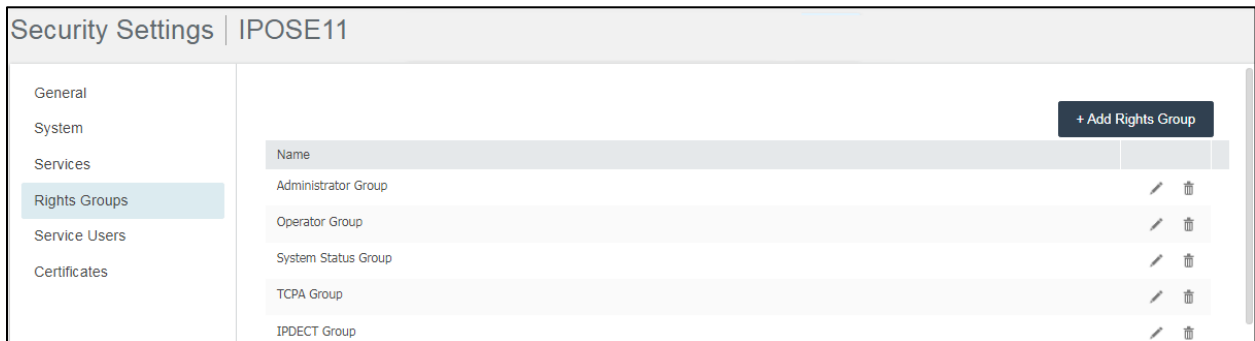


The **Primary** Server Edition was chosen.



5.1. Add a new Rights Group for estos ECSTA

Before the user is added, a new Right Groups needs to be configured for this user. Navigate to **Rights Groups** in the left window and click on **Add Rights Group** in the main window.



There are a number of tabs that can be configured, first enter a suitable **Name** in the **Group Details** tab.

The screenshot shows the 'Edit Rights Group' interface. At the top, there is a title 'Edit Rights Group' and a horizontal tab bar with the following tabs: 'Group Details', 'Configuration', 'Security Administrator', 'System Status', 'Telephony APIs', 'Web Services', 'External', and 'HTTP'. The 'Group Details' tab is currently selected. Below the tabs, there is a 'Name' label followed by a text input field containing the text 'estosWS'. At the bottom right of the interface, there are two buttons: 'Cancel' and 'Save'.

Navigate to **Telephony APIs** and ensure that all are selected, as shown below.

The screenshot shows the 'Edit Rights Group' interface with the 'Telephony APIs' tab selected. The 'IP Office Service Rights' section is visible, containing three items: 'Enhanced TSPI Access', 'DevLink3', and 'Location API'. Each item has a blue 'YES' button next to it, indicating that all these rights are selected. The 'Cancel' and 'Save' buttons are not visible in this view.

Under the **External** tab, ensure that **one-X CTI API** is ticked, as shown below. Click on **Save**.

Edit Rights Group

Group Details | Configuration | Security Administrator | System Status | Telephony APIs | Web Services | **External** | HTTP

IP Office Service Rights

Voicemail Pro Basic	Voicemail Pro Standard	Voicemail Pro Administrator	one-X Portal Administrator
<input type="checkbox"/> NO	<input type="checkbox"/> NO	<input type="checkbox"/> NO	<input type="checkbox"/> NO
one-X Portal Super User	Web Control Administrator	Web Control Security	WebRTC Gateway Administrator
<input type="checkbox"/> NO	<input type="checkbox"/> NO	<input type="checkbox"/> NO	<input type="checkbox"/> NO
Management API Read	Management API Write	Media Manager Administrator	Media Manager Standard
<input type="checkbox"/> NO	<input type="checkbox"/> NO	<input type="checkbox"/> NO	<input type="checkbox"/> NO
Reporter Administrator	one-x CTI API	Adjunct Server Connection	
<input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES	<input type="checkbox"/> NO	

Cancel Save

5.2. Add a Service User for estos ECSTA

Click on **Service Users** in the left window. Click on **Add Service Users** in the main window.

Security Settings | IPOSE11

General | System | Services | Rights Groups | **Service Users** | Certificates

+ Add Service Users

Name	Access Rights		
Administrator	Administrator Group, Business Partner, System Status Group, TCPA Group	/	🗑️
EnhTcpservice	TCPA Group, TCPA Group	/	🗑️
IPDECTService	IPDECT Group, IPDECT Group	/	🗑️
BranchAdmin	SMGR Admin	/	🗑️
BusinessPartner	Business Partner	/	🗑️
Maintainer	Maintainer	/	🗑️
DirectoryService	Directory Group	/	🗑️
MCMAdmin	MCM Admin	/	🗑️
aurenzSDKuser	Management API Group	/	🗑️

Enter a suitable **Name** and **Password**. Ensure the **Account status** is **Enabled** and scroll down to add the **Rights Group** that was created previously in **Section 5.1**.

The screenshot shows a configuration form with the following sections:

- BASIC OPTIONS:** Name (estos), Password (masked), Account status (Enabled).
- ACCOUNT EXPIRY:** Account Expiration (NO).
- RIGHTS GROUPS:** A grid of 12 groups, each with a 'NO' toggle:
 - Adjunct Servers, Administrator Group, Backup Admin
 - Business Partner, Customer Admin, Directory Group
 - IPDECT Group, MCM Admin, Maint Admin
 - Maintainer, Management API Group, Operator Group

A red arrow on the right side of the form points downwards, indicating the scroll direction.

The **estosWS** Rights Group that was created in **Section 5.1** is selected here and **Save** is clicked to add the new user.

The screenshot shows a selection screen for rights groups. On the left, a sidebar lists 'Services', 'Rights Groups', 'Service Users', and 'Certificates'. The main area displays a grid of 18 groups, each with a toggle:

- Business Partner (NO), Customer Admin (NO), Directory Group (NO)
- IPDECT Group (NO), MCM Admin (NO), Maint Admin (NO)
- Maintainer (NO), Management API Group (NO), Operator Group (NO)
- SMGR Admin (NO), SNMPv3 Admin (NO), Security Admin (NO)
- System Admin (NO), System Status Group (NO), TCPA Group (NO)
- Upgrade Admin (NO), Zang Admin (NO), **estosWS (YES)**

At the bottom right, there are 'Cancel' and 'Save' buttons.

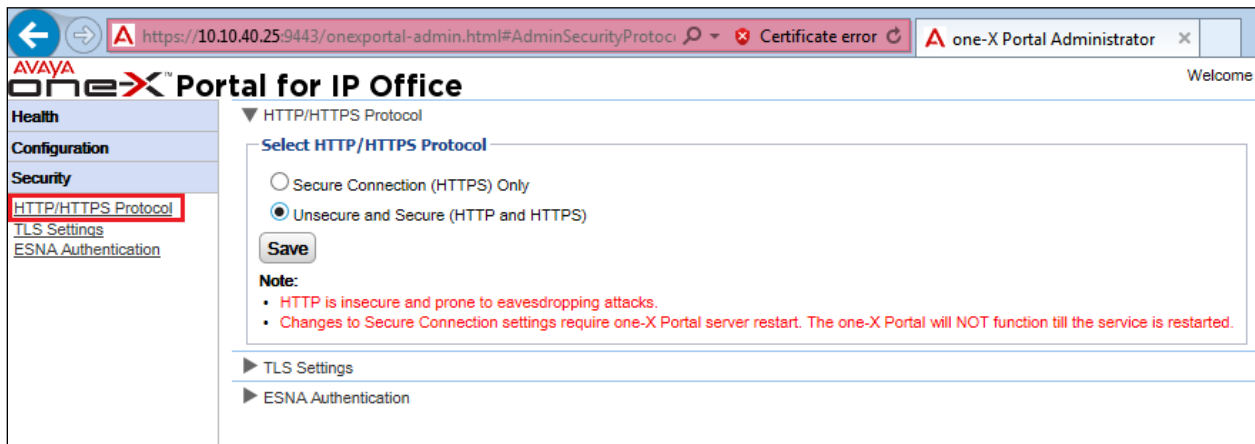
5.3. Configure Avaya one-X® Portal

For compliance testing the interface was using a secure link. However, if the interface is not using SSL the service must be allowed access to HTTP on port 8080. This is done on One-X® Portal Administrator under security.

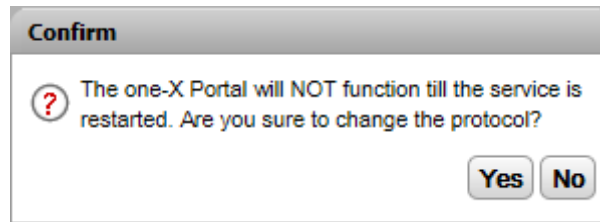
Open a web browser to the IP Office Server Edition on **https://<Server IP>:9443/onexportal-admin.html**. Enter the appropriate credentials and click on **Login**.



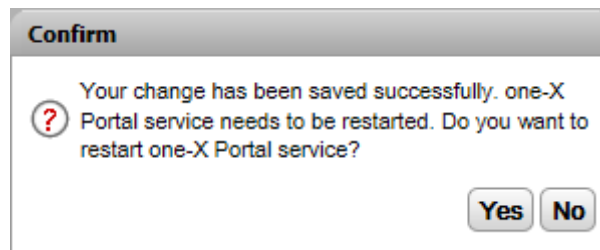
Click on **Security** in the left window and on **HTTP/HTTPS Protocol** and ensure that that **Unsecure and Secure (HTTP and HTTPS)** button is selected and click on **Save**.



Once Save is pressed above the following message is displayed, click on **Yes**.



Once Yes is pressed above the following message is displayed, click on **Yes** again. The One-X® Portal will now restart and will log out the user automatically and will be offline for 2-3 mins.



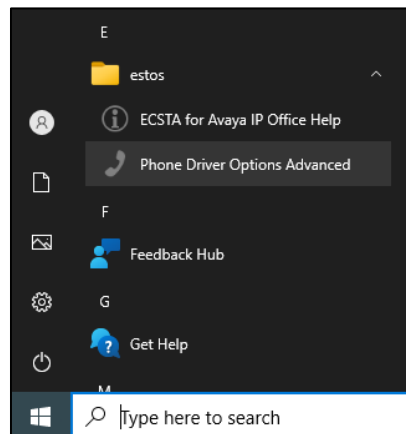
This concludes the setup on IP Office for CTI Web Services connections.

6. Configuration of estos ECSTA

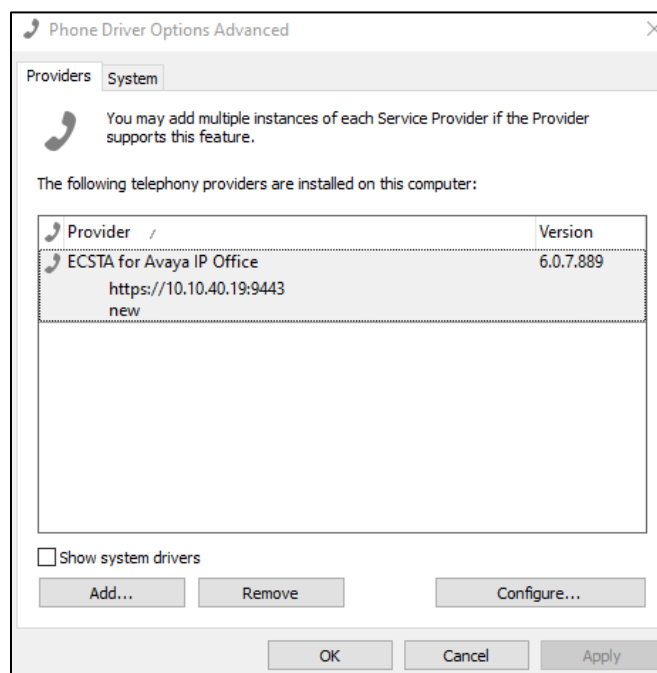
This section outlines the steps to configure the estos ECSTA to connect to IP Office. estos ECSTA can be installed on a server or desktop PC. Installation is carried out using software provide by estos. Installation instructions are outside the scope of this document but information on installation of estos ECSTA can be found in **Section 9** of this document.

6.1. estos ECSTA configuration for IP Office

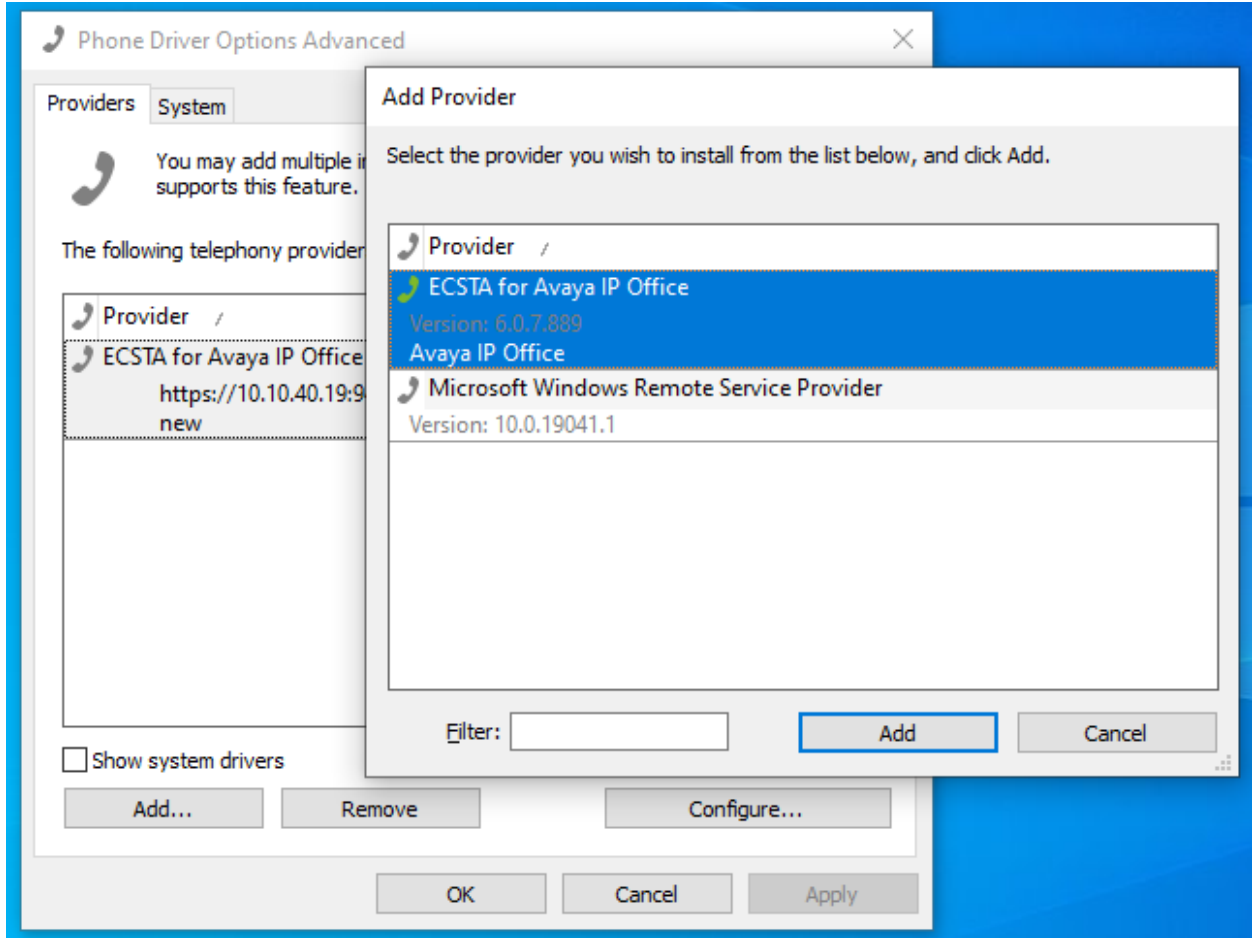
The **Phone Driver Options Advanced** can be located as shown below.



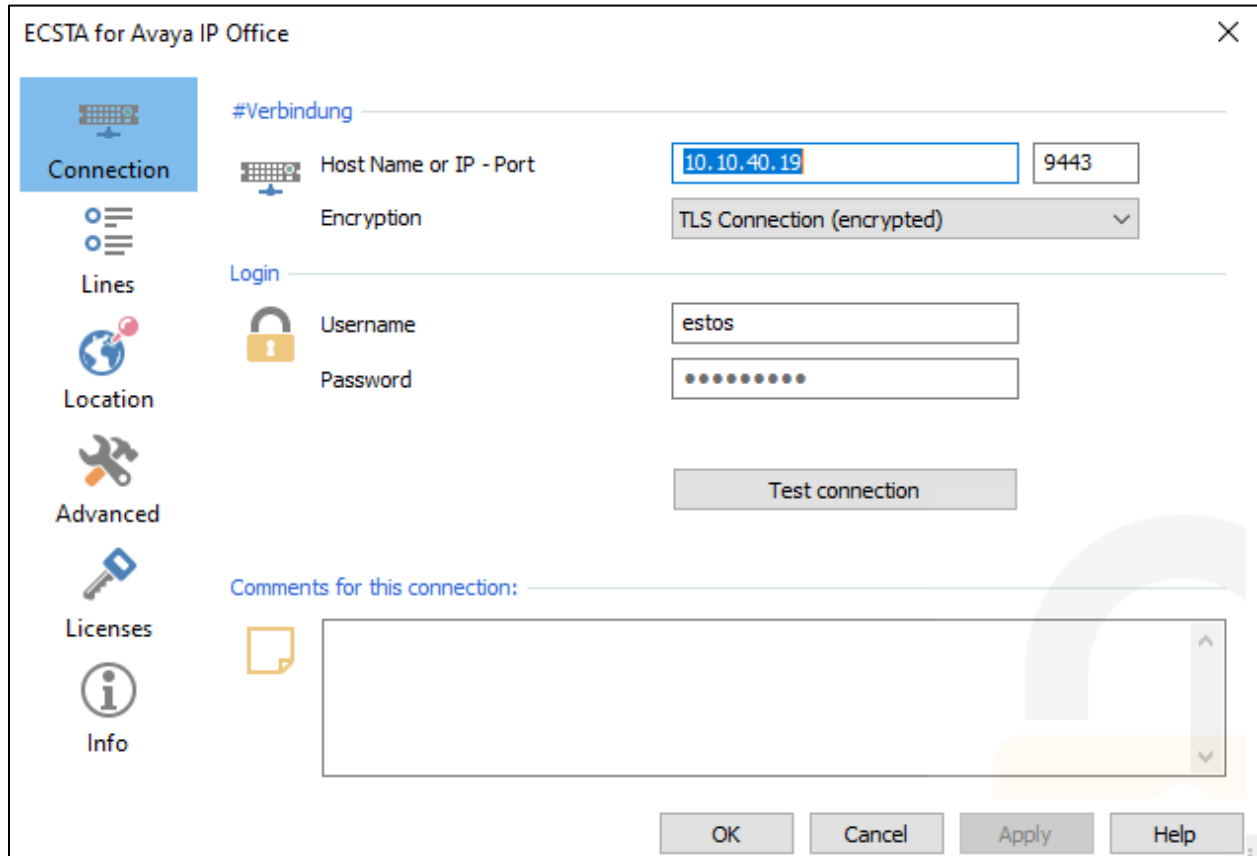
The **ECTSA for Avaya IP Office** driver is installed as part of the installation by the estos engineers. The existing driver can be configured by clicking on **Configure** at the bottom right of the screen. If a new driver was to be added for a second IP Office node, then click on **Add**.



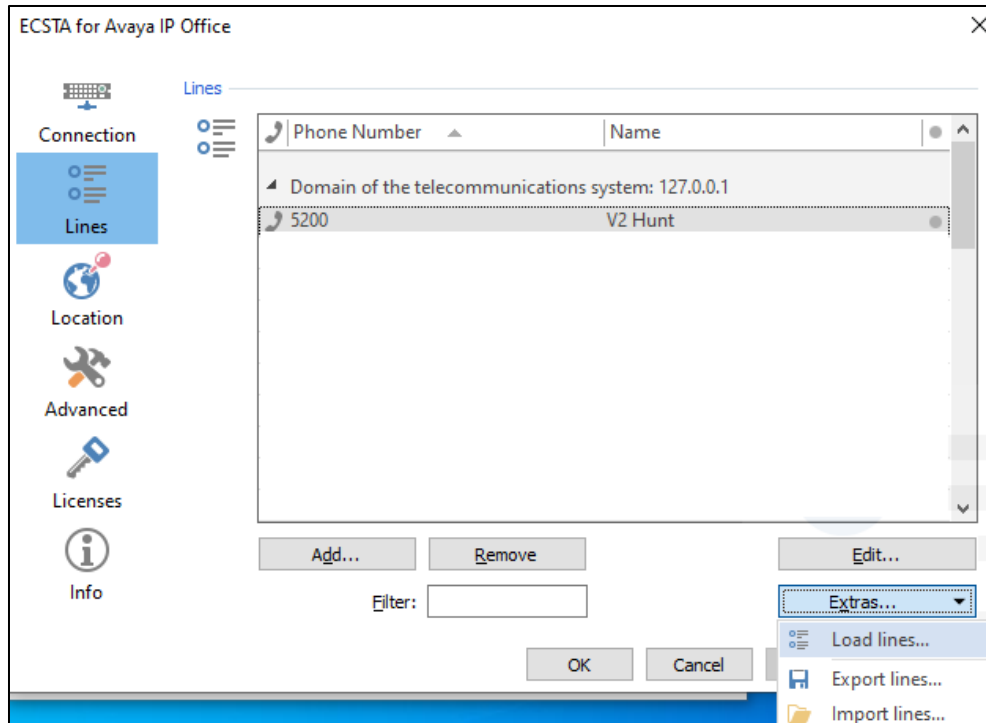
Clicking on **Add** will open a new window where an additional Driver or **Provider** can be added.



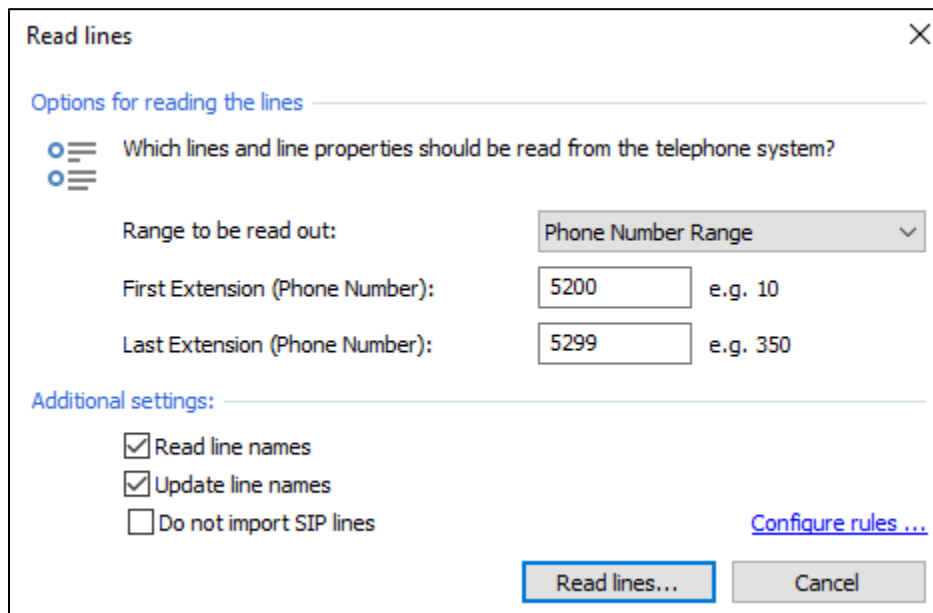
Pressing **Configure**, from the screen at the bottom of **Page 14**, opens the window below where the IP address of the Server Edition is added for **Host Name or IP - Port**, and **Port 9443** is used for the encrypted connection. **Encryption** is therefore set to **TLS Connection (encrypted)** as shown below. The **Username** and **Password** is set to that configured in **Section 5.2**. The Test connection button can be used, to verify, whether the configured parameters are correct so that a connection can be established between ECSTA TAPI driver and Avaya IP Office.



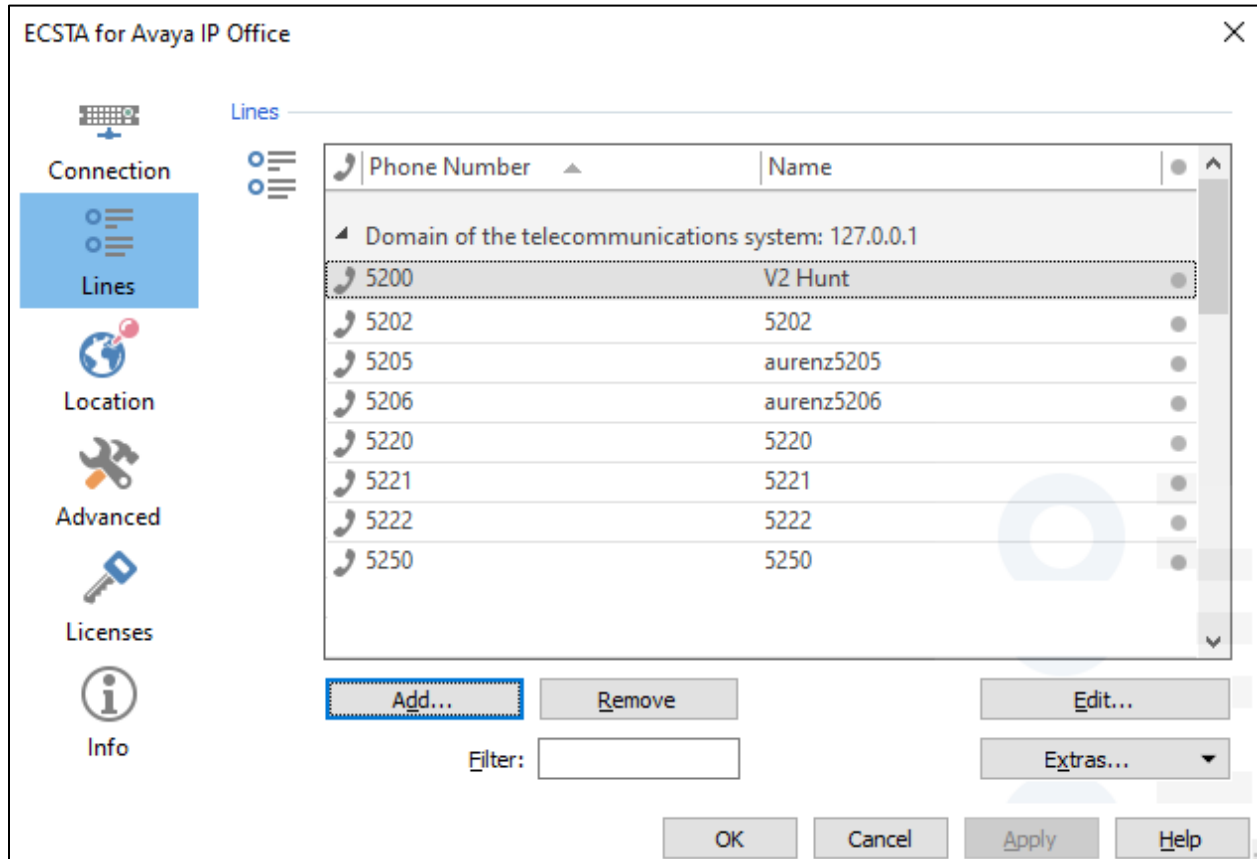
Clicking on **Lines** in the left window, allows the addition of the IP Office extensions, or Lines as they are called in reference to TAPI. The extensions that are to be monitored by ECSTA will be added here. A whole range of lines can be added by selecting **Extras** and **Load Lines** as shown below, or one Line can be added by clicking on **Add**.



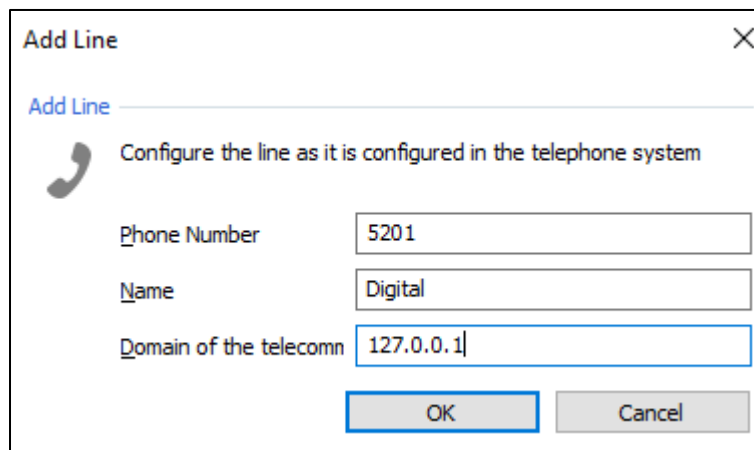
For compliance testing, a range of lines were added as shown below. Fill in the appropriate details and click on **Read lines**.



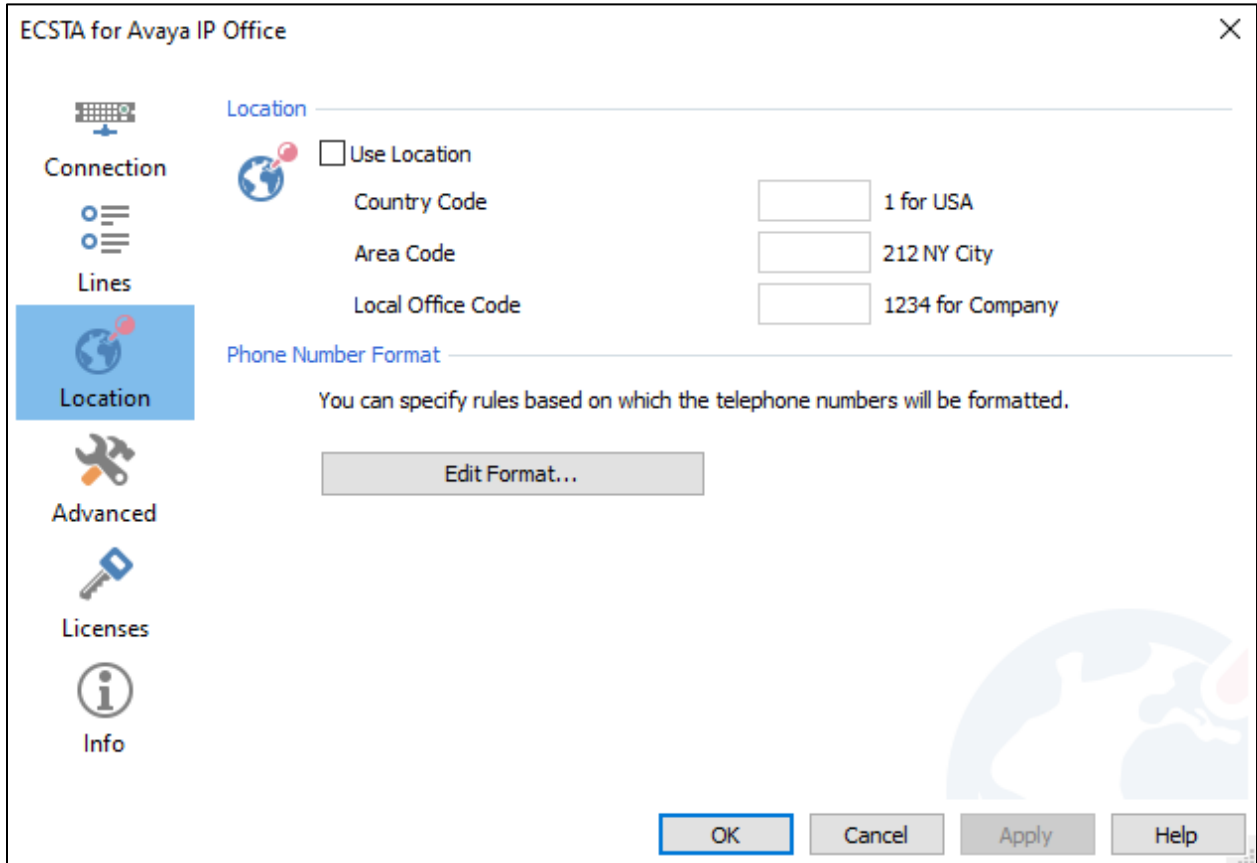
To add an individual line, click on **Add** as shown below.



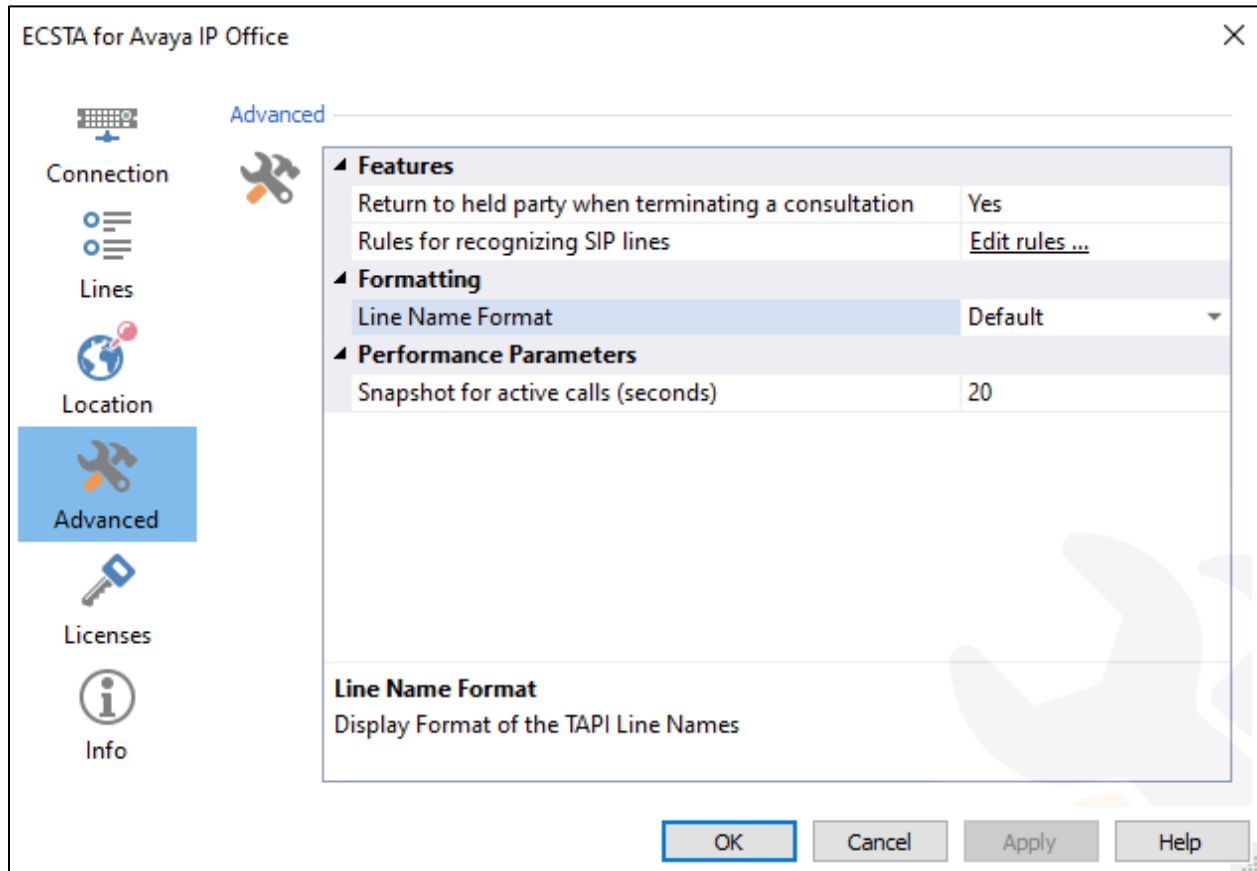
The **Phone Number** will be the extension number of the IP Office extension in question. The **Name** can be anything but may be useful to keep this the same as the extension number. **Domain of the telecom** was set to **127.0.0.1**, because One-X® Portal and IP Office were running on the same host. This could have been 10.10.40.19 also, as this was the IP address of the IP Office hosting one-X® Portal. ECSTA already has a link to 10.10.40.19 configured and so 127.0.0.1 was used.



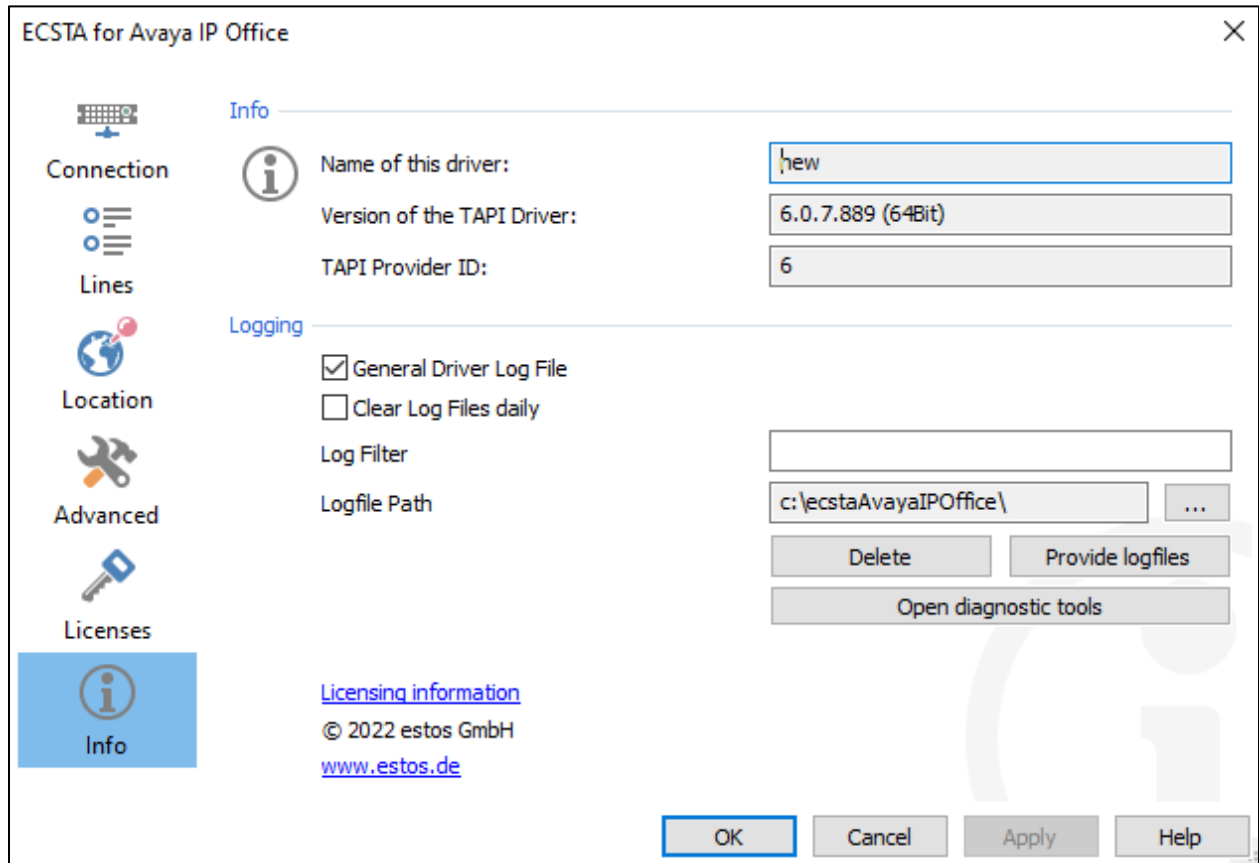
Clicking on **Location** in the left window, shows the settings that can be set for the Location information. There were no specific settings set for compliance testing.



Clicking on **Advanced** in the left window, opens the settings as shown below. Again, these were left as **Default** for compliance testing but can be changed depending on the setup required.



Clicking on **Info**, shows the location of the log files and the ECSTA **TAPI Driver** version. Clicking on **OK** at the bottom of the screen should exit the setup and save the changes.

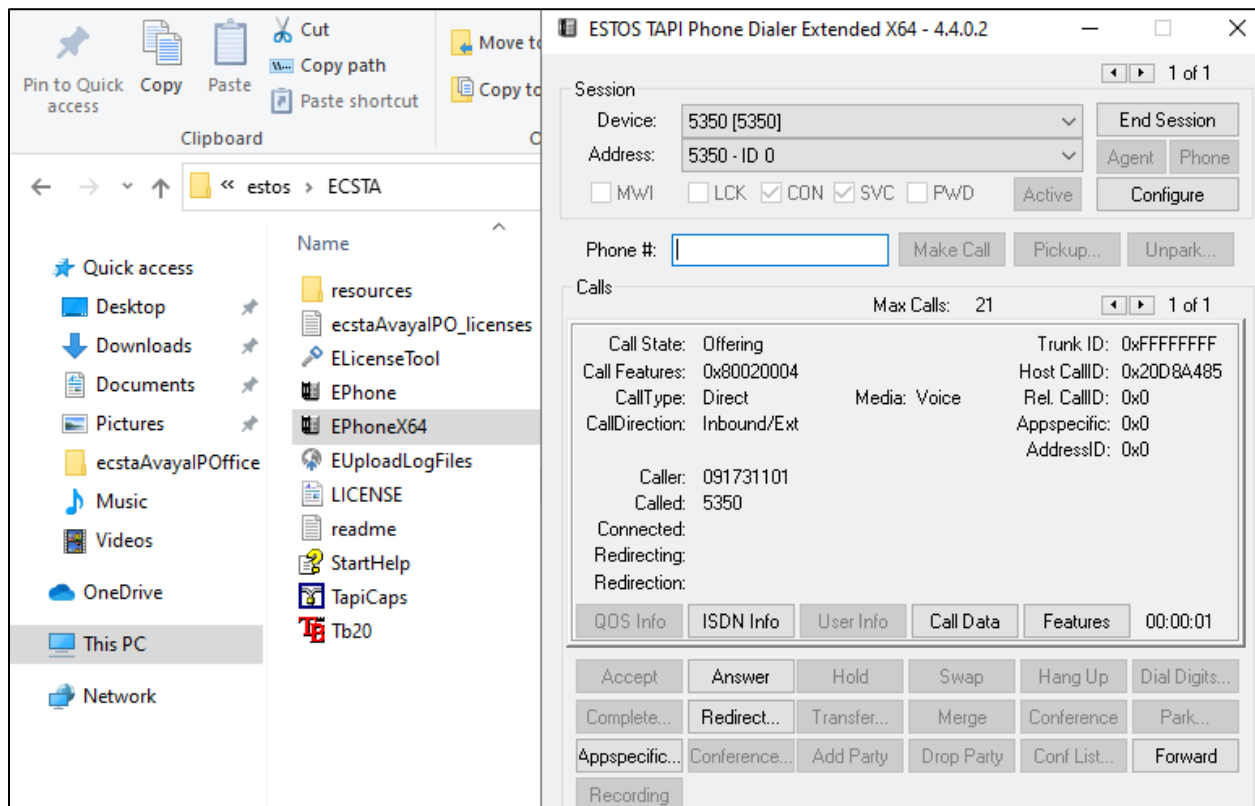


7. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and estos solution. To verify the solution, calls are made/received using the estos EPhone TAPI phone application.

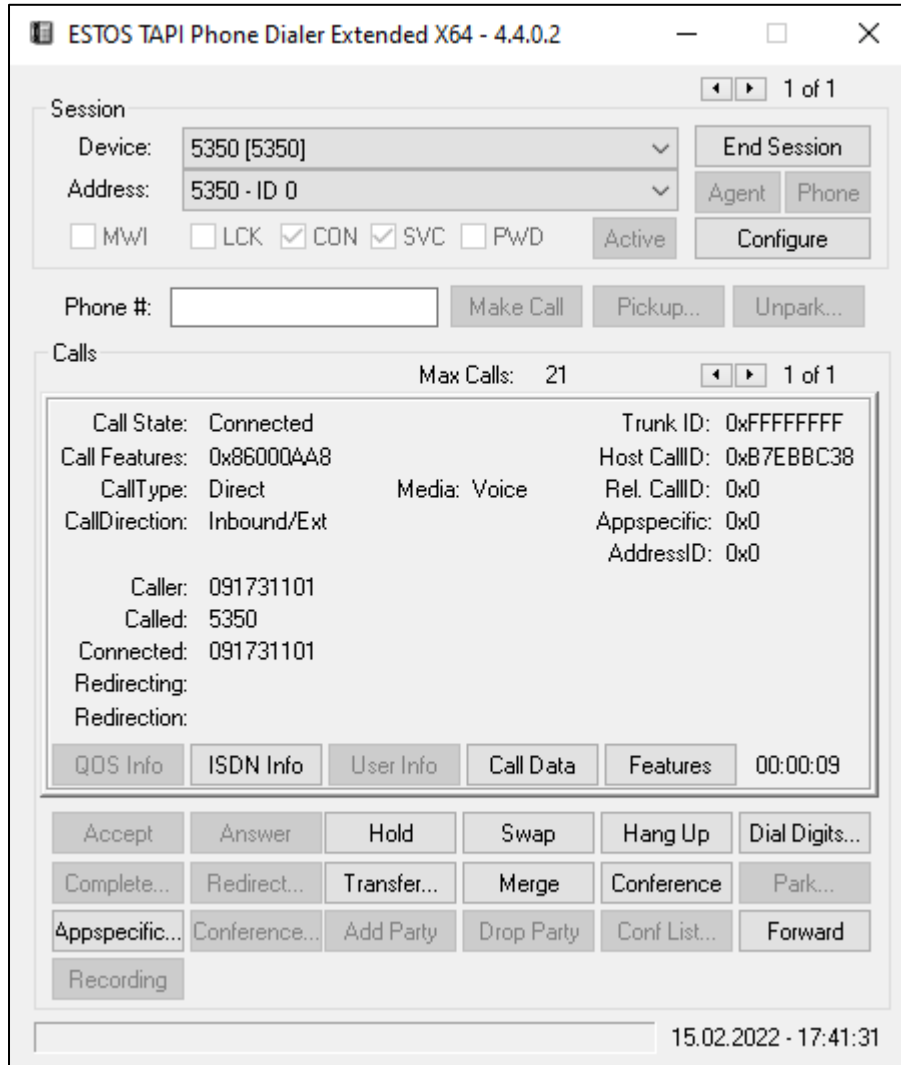
7.1. Verify the connection using estos EPhone.exe

The connection can be tested by opening the EPhone.exe or EPhoneX64.exe and using it to make and receive a call. That is the ultimate goal of compliance testing and once that can be achieved the setup is deemed successful. The EPhone.exe is typically located in the **estos/ECSTA** folder which would be under Program Files. Once the EPhone application is opened a **Device** is chosen, from a list of devices that appear, when the **Device** drop-down box is clicked (not shown). Extension **5350** was chosen below, which means that this device is now controlled by **estos TAPI Phone Dialer**. A call was made to this extension from **091731101** and the call can be answered by pressing the **Answer** button.



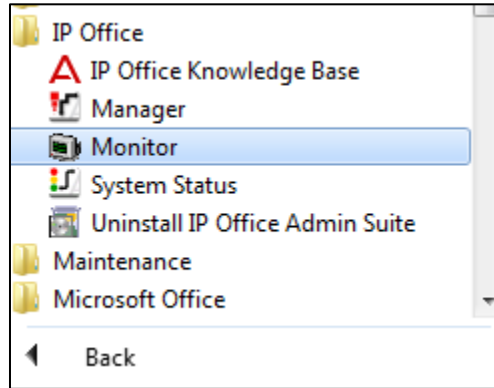
Once the call is answered, more telephony functions were enabled, such as **Hold**, **Transfer**, **Conference** and **Hang Up**.

Once these calls are successfully initiated using the TAPI Phone **Dialer** application, then there must be a successful connection between estos ECSTA TAPI driver and IP Office.

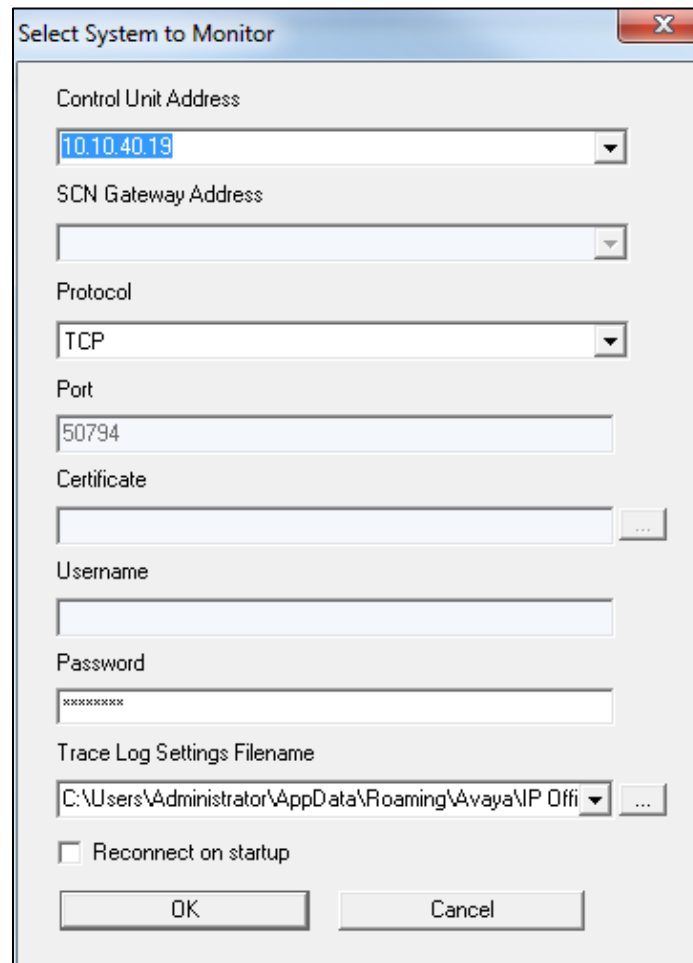


7.2. Verify connection from IP Office

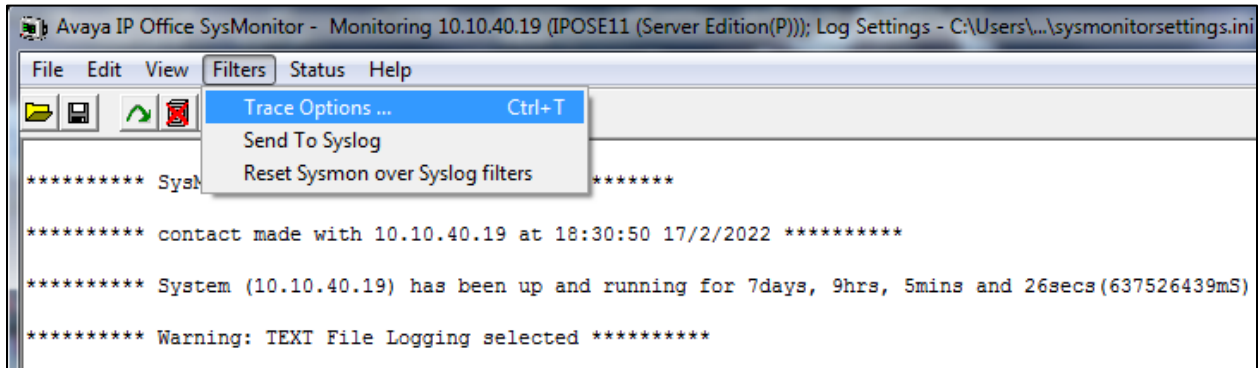
IP Office Monitor can be used to check on the TAPI messages on IP Office. Open IP Office Monitor.



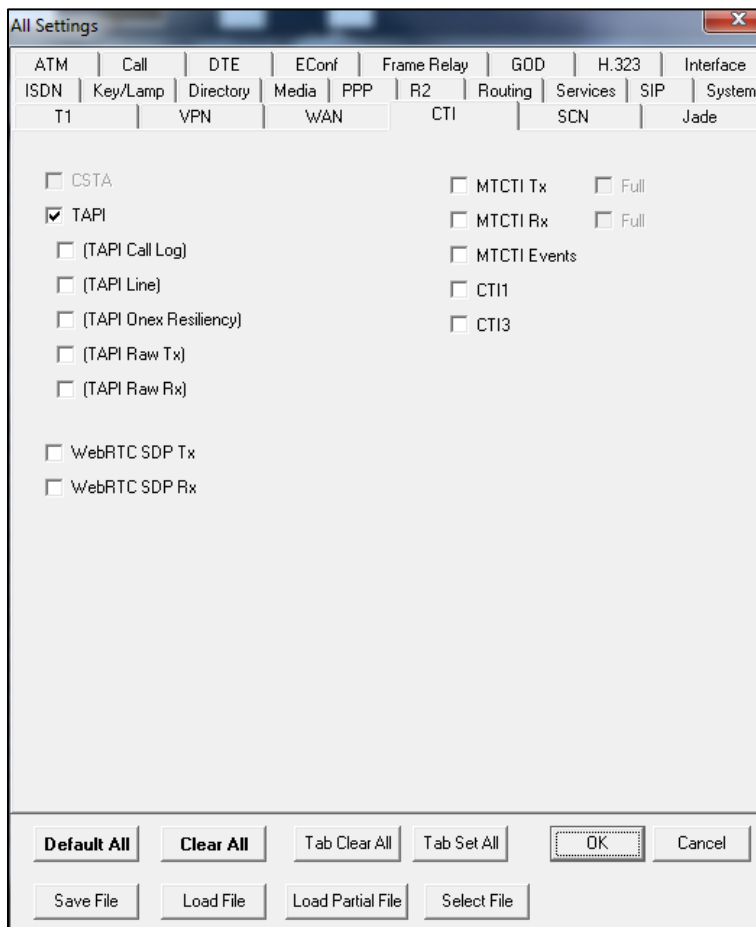
Select the IP Office (under **Control Unit Address**). Enter the appropriate credentials and click on **OK**.

A screenshot of the 'Select System to Monitor' dialog box. The dialog has a title bar with a close button. The fields are: Control Unit Address (dropdown menu with '10.10.40.19' selected), SCN Gateway Address (empty dropdown), Protocol (dropdown menu with 'TCP' selected), Port (text box with '50794'), Certificate (empty text box with a browse button), Username (empty text box), Password (password field with 'xxxxxxxx'), Trace Log Settings Filename (dropdown menu with 'C:\Users\Administrator\AppData\Roaming\Avaya\IP Offi' selected and a browse button), and a checkbox for 'Reconnect on startup' which is unchecked. At the bottom are 'OK' and 'Cancel' buttons.

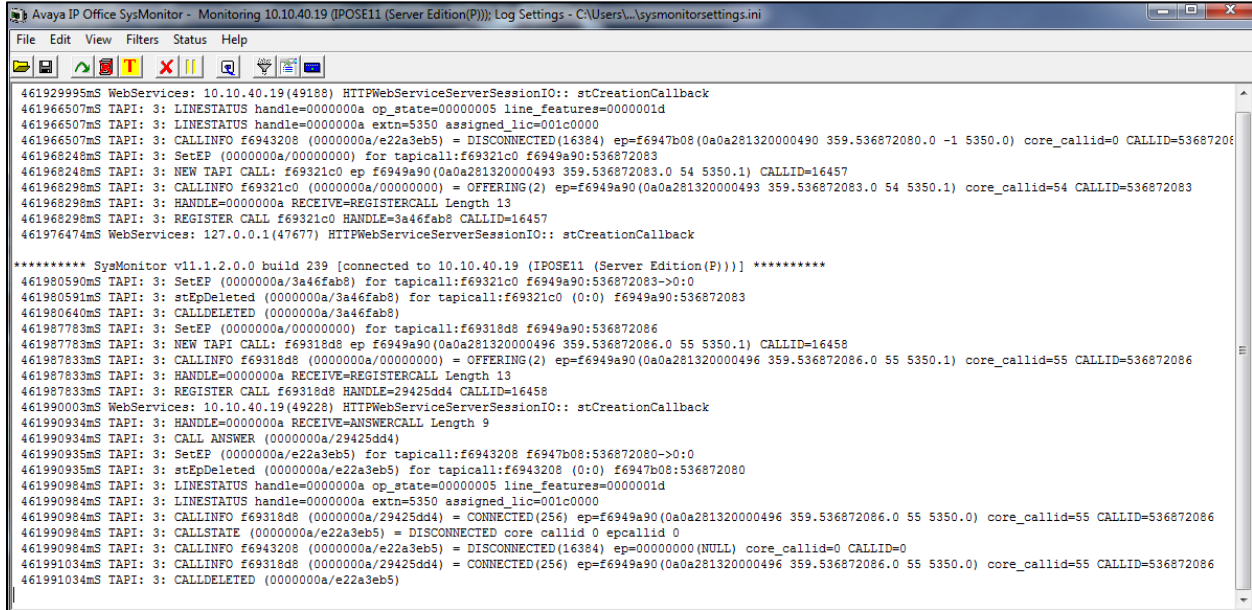
Click on **Trace Options**.



There are a number of traces that can be set, under CTI the following can be set for TAPI and CTI events. Clicking on **TAPI** below will show certain TAPI events, the type of events can be widened by selecting other boxes that may be relevant. Click on **OK** once everything has been selected appropriately.



When a call is made and answered, the trace should show the TAPI messages, something like what is shown below.



```
Avaya IP Office SysMonitor - Monitoring 10.10.40.19 (IPOSE11 (Server Edition(P))); Log Settings - C:\Users\...sysmonitorsettings.ini
File Edit View Filters Status Help
461929995ms WebServices: 10.10.40.19(49188) HTTPWebServiceServerSessionIO:: stCreationCallback
461966507ms TAPI: 3: LINESTATUS handle=0000000a op_state=00000005 line_features=0000001d
461966507ms TAPI: 3: LINESTATUS handle=0000000a extn=5350 assigned_lic=001c0000
461966507ms TAPI: 3: CALLINFO f6943208 (0000000a/e22a3eb5) = DISCONNECTED(16384) ep=f6947b08(0a0a281320000490 359.536872080.0 -1 5350.0) core_callid=0 CALLID=536872080
461968248ms TAPI: 3: SetEP (0000000a/00000000) for tapicall:f69321c0 f6949a90:536872083
461968248ms TAPI: 3: NEW TAPI CALL: f69321c0 ep f6949a90(0a0a281320000493 359.536872083.0 54 5350.1) CALLID=16457
461968298ms TAPI: 3: CALLINFO f69321c0 (0000000a/00000000) = OFFERING(2) ep=f6949a90(0a0a281320000493 359.536872083.0 54 5350.1) core_callid=54 CALLID=536872083
461968298ms TAPI: 3: HANDLE=0000000a RECEIVE=REGISTERCALL Length 13
461968298ms TAPI: 3: REGISTER CALL f69321c0 HANDLE=3a46fab8 CALLID=16457
461976474ms WebServices: 127.0.0.1(47677) HTTPWebServiceServerSessionIO:: stCreationCallback
***** SysMonitor v11.1.2.0.0 build 239 [connected to 10.10.40.19 (IPOSE11 (Server Edition(P)))] *****
461980590ms TAPI: 3: SetEP (0000000a/3a46fab8) for tapicall:f69321c0 f6949a90:536872083->0:0
461980591ms TAPI: 3: stEpDeleted (0000000a/3a46fab8) for tapicall:f69321c0 (0:0) f6949a90:536872083
461980640ms TAPI: 3: CALLDELETED (0000000a/3a46fab8)
461987783ms TAPI: 3: SetEP (0000000a/00000000) for tapicall:f69318d8 f6949a90:536872086
461987783ms TAPI: 3: NEW TAPI CALL: f69318d8 ep f6949a90(0a0a281320000496 359.536872086.0 55 5350.1) CALLID=16458
461987833ms TAPI: 3: CALLINFO f69318d8 (0000000a/00000000) = OFFERING(2) ep=f6949a90(0a0a281320000496 359.536872086.0 55 5350.1) core_callid=55 CALLID=536872086
461987833ms TAPI: 3: HANDLE=0000000a RECEIVE=REGISTERCALL Length 13
461987833ms TAPI: 3: REGISTER CALL f69318d8 HANDLE=29425dd4 CALLID=16458
461990003ms WebServices: 10.10.40.19(49228) HTTPWebServiceServerSessionIO:: stCreationCallback
461990934ms TAPI: 3: HANDLE=0000000a RECEIVE=ANSWERCALL Length 9
461990934ms TAPI: 3: CALL ANSWER (0000000a/29425dd4)
461990935ms TAPI: 3: SetEP (0000000a/e22a3eb5) for tapicall:f6943208 f6947b08:536872080->0:0
461990935ms TAPI: 3: stEpDeleted (0000000a/e22a3eb5) for tapicall:f6943208 (0:0) f6947b08:536872080
461990984ms TAPI: 3: LINESTATUS handle=0000000a op_state=00000005 line_features=0000001d
461990984ms TAPI: 3: LINESTATUS handle=0000000a extn=5350 assigned_lic=001c0000
461990984ms TAPI: 3: CALLINFO f69318d8 (0000000a/29425dd4) = CONNECTED(256) ep=f6949a90(0a0a281320000496 359.536872086.0 55 5350.0) core_callid=55 CALLID=536872086
461990984ms TAPI: 3: CALLSTATE (0000000a/e22a3eb5) = DISCONNECTED core callid 0 epcallid 0
461990984ms TAPI: 3: CALLINFO f6943208 (0000000a/e22a3eb5) = DISCONNECTED(16384) ep=00000000(NULL) core_callid=0 CALLID=0
461991034ms TAPI: 3: CALLINFO f69318d8 (0000000a/29425dd4) = CONNECTED(256) ep=f6949a90(0a0a281320000496 359.536872086.0 55 5350.0) core_callid=55 CALLID=536872086
461991034ms TAPI: 3: CALLDELETED (0000000a/e22a3eb5)
```

8. Conclusion

A full and comprehensive set of feature functional test cases were performed during compliance testing. Estos GmbH estos ECSTA v6.0 is considered compliant with Avaya IP Office R11.1. All test cases were passed.

9. Additional References

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.

Information on the installation and configuration of estos ECSTA can be found at <https://www.estos.com>.

[2] *estos ECSTA for Avaya IP Office*, Release 6.0.8.896.

©2022 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.