DevConnect Program

Application Notes for Resource Software International Shadow Call Management System Version 5.4 with Avaya IP Office Server Edition Release 11.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Resource Software International Shadow Call Management System (Shadow CMS) to interoperate with Avaya IP Office Server Edition. Resource Software International (RSI) Shadow CMS is a call reporting application.

In the compliance testing, RSI Shadow CMS used the DevLink3 interface from Avaya IP Office to monitor agent users and provided real-time agent status and cradle to grave reporting.

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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required for RSI Shadow CMS to interoperate with Avaya IP Office Server Edition. Shadow CMS is a call reporting application.

The Avaya IP Office Server Edition configuration consisted of two Avaya IP Office systems, a Primary Linux server and an Expansion IP500V2 that were connected via Small Community Network (SCN) trunks. In the compliance testing, RSI Shadow CMS server used DevLink3 interface to connect to the Primary Linux Server and monitored groups and users on both the Primary and Expansion systems.

In the compliance testing, Shadow CMS used the DevLink3 interface from IP Office Server Edition to monitor agent users and provided real-time agent status and cradle to grave reporting.

The DevLink3 interface was used by Shadow CMS to obtain configured system resources from IP Office such as configured hunt groups and agent users, and to obtain real-time agent status and call events. The obtained information was used to produce real-time agent status and cradle to grave reporting, which were accessible via the Shadow CMS web interface.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Shadow CMS, the application automatically sends DevLink3 commands to obtain configured hunt groups, users and hunt group membership information from both the Primary and Expansion systems.

For the manual part of the testing, calls were made from the PSTN and from local users to the hunt groups and agent users on both the Primary and Expansion systems. Necessary user actions such as hold/reconnect were performed from the user telephones to generate events for the various call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the Shadow CMS server.

The verification focused on the cradle to grave reporting and real-time agent status reflection.

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 Server Edition and Shadow CMS did not include use of any specific encryption features as requested by RSI.

2.1. Interoperability Compliance Testing

The compliance testing included feature and serviceability areas.

The feature testing call flows included calls within the primary IP Office, calls within the Expansion IP Office, as well as calls between the two IP Office systems. The feature testing focused on verifying the following on Shadow CMS:

- Use of DevLink3 ReadFile commands to obtain hunt groups, users and hunt group membership information.

- Use of DevLink3 extension events to provide real-time reporting of user status for do-not-disturb and hunt group membership features.

- Use of DevLink3 call events to provide cradle to grave reporting for various call scenarios including internal, external, inbound, outbound, drop, hold/reconnect, blind/attended transfer, blind/attended conference, voicemail coverage, voicemail retrieval, hunt group, hunt group queuing, hot desking, park/unpark, forwarding, multiple users, multiple calls, long duration, overflow, fallback and mobile twinning.

The serviceability testing focused on verifying the ability of Shadow CMS to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to the Shadow CMS server.

2.2. Test Results

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

- User feature configuration changes on IP Office Manager cannot reflect in real-time on Shadow CMS due to nature of the interface. Devlink3 events are only generated for stations events happening directly on a phone due to user action. A workaround is to restart the Shadow CMS service to force a re-synchronization with IP Office or to wait for re-query of all devices during midnight rollover routine by Shadow CMS.

- User feature status changes via short codes may not always be reflected by Shadow CMS, and the recommendation is to always use the programmed buttons on the user telephones.

- Shadow CMS by design does not show inbound ringing events. It shows the status once the calls are connected.

- During transfer and conference calls, after the party that transferred the call or when the party that initiated the conference drops off, Shadow CMS grid still shows that the call is connected for these users.

- After a park/un-park call is completed, dashboard shows the name of the user that parked the call to "Park". The proper name is reflected if the user re-login or after the midnight rollover routine of Shadow CMS.

- Shadow CMS by design provides information on Do Not Disturb feature however it does not provide information on Call Forward, Follow Me, Overflow etc.

2.3. Support

Technical support on Shadow CMS can be obtained through the following:

- **Phone:** (800) 891-6014
- **Email:** support@telecost.com
- **Web:** www.telecost.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The IP Office Server Edition configuration used in compliance testing consisted of a Primary Linux Server and an Expansion IP500V2 system, with SCN trunks connectivity between the two systems. The IP Office Primary system has connectivity to the PSTN through Avaya Session Border Controller, for testing cross systems PSTN scenarios. Shadow CMS connects to the Primary system via DevLink3 however gets all the call events from both Primary and Expansion systems.

The detailed administration of general devices such as Voicemail Pro, hunt groups and agent users are assumed to be in place and are not covered in these Application Notes.

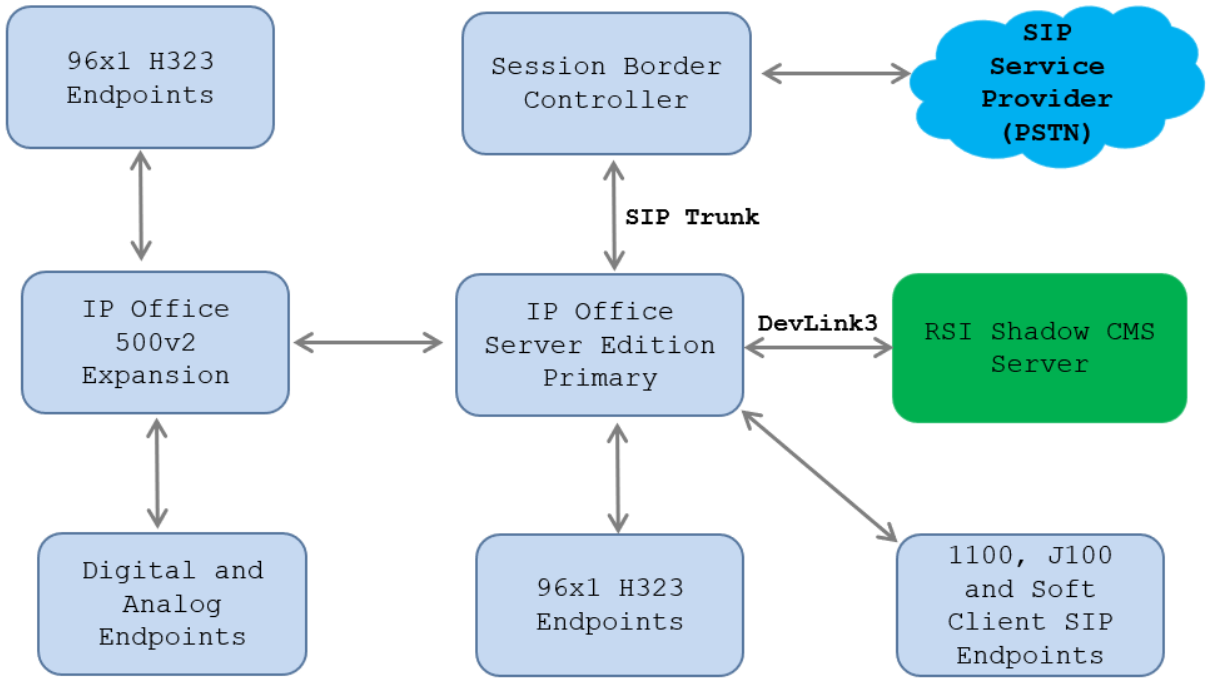


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition	11.1.3.0 Build 23
Avaya IP Office 500V2 Expansion	11.1.3.0 Build 23
Avaya IP Office Manager	11.1.3.0 Build 23
Avaya Session Border Controller	10.1.2.0-64-23285 HotFix-1
Avaya 96x1 Series IP Deskphone (H.323)	6.8.5.4.10
Avaya J100 IP Deskphones (J169, J179)	4.1.2.0.11
Avaya Workplace Client For Windows (SIP)	3.35.0.67
Avaya 9508 Digital Deskphone	1.0
Avaya Analog phone	-
RSI Shadow CMS Enterprise	5.4.2.5

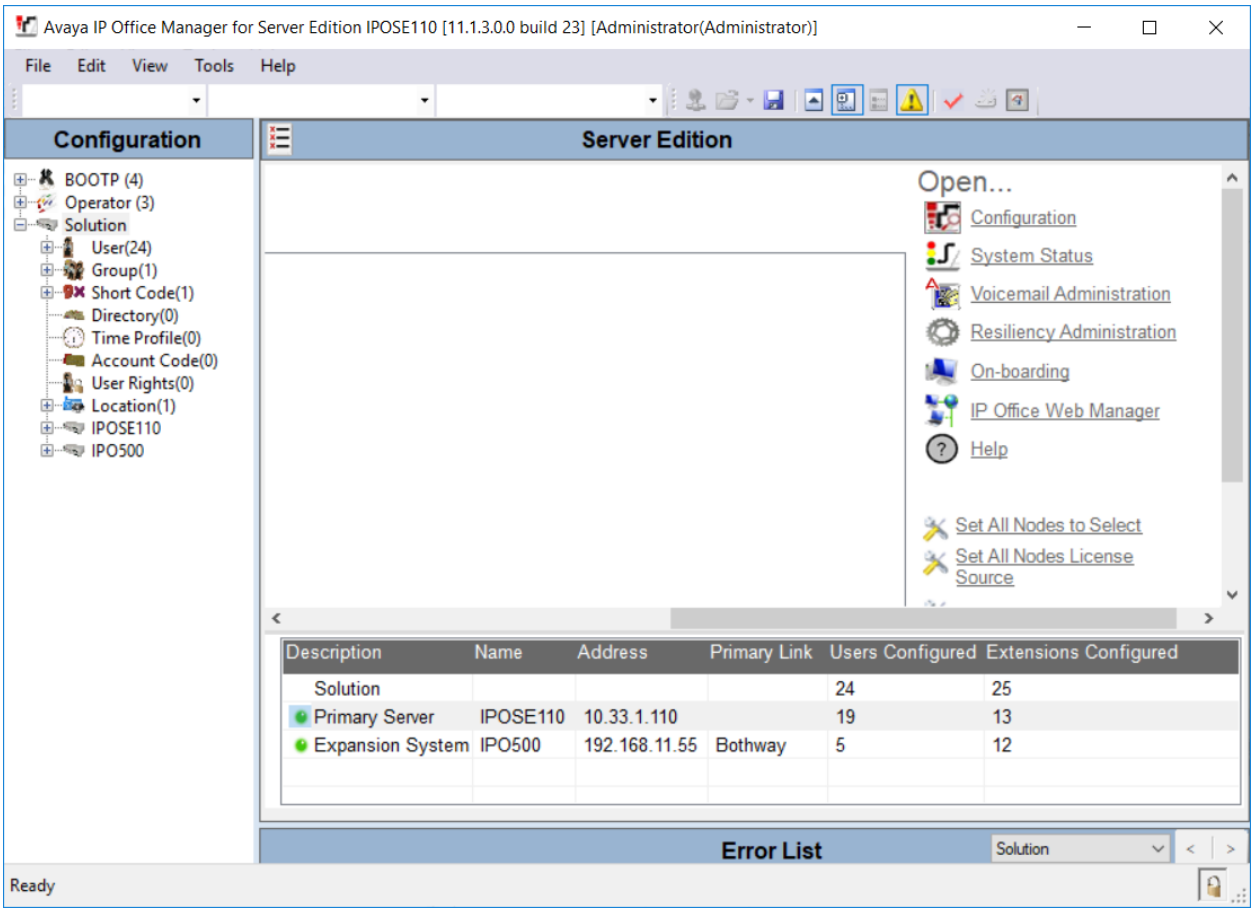
Note: *Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and when deployed with IP Office Server Edition in all configurations.*

5. Configure Avaya IP Office

This section provides the procedures for configuring IP Office Server Edition. The configuration shown here is only required to be carried out on the Primary system of Avaya IP Office Server Edition. The procedures include the following areas:

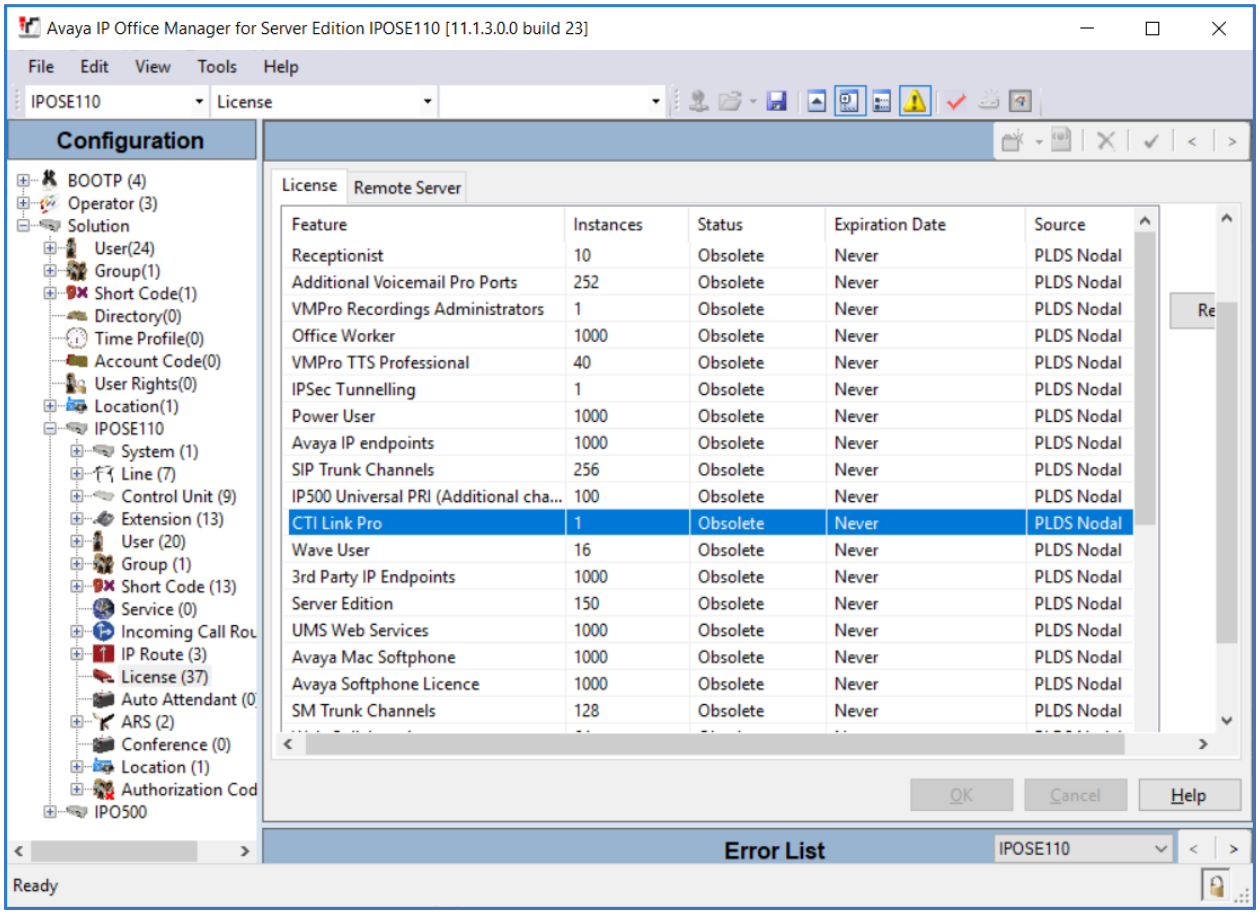
- Verify License
- Administer System Interfaces
- Administer Rights Groups
- Administer Service Users

From a PC running the IP Office Manager application, select **Start → Programs →IP Office → Manager** to launch the Manager application. Select the proper IP Office system, and log in using the appropriate credentials. The Avaya IP Office Manager for Server Edition screen is displayed as shown in the screen below.



5.1. Verify License

From the configuration tree in the left pane, select the Primary System which in this case is **IPOSE110** and then navigate to **License** to display a list of licenses in the right pane. Verify that there are valid licenses for **CTI Link Pro** as shown below.

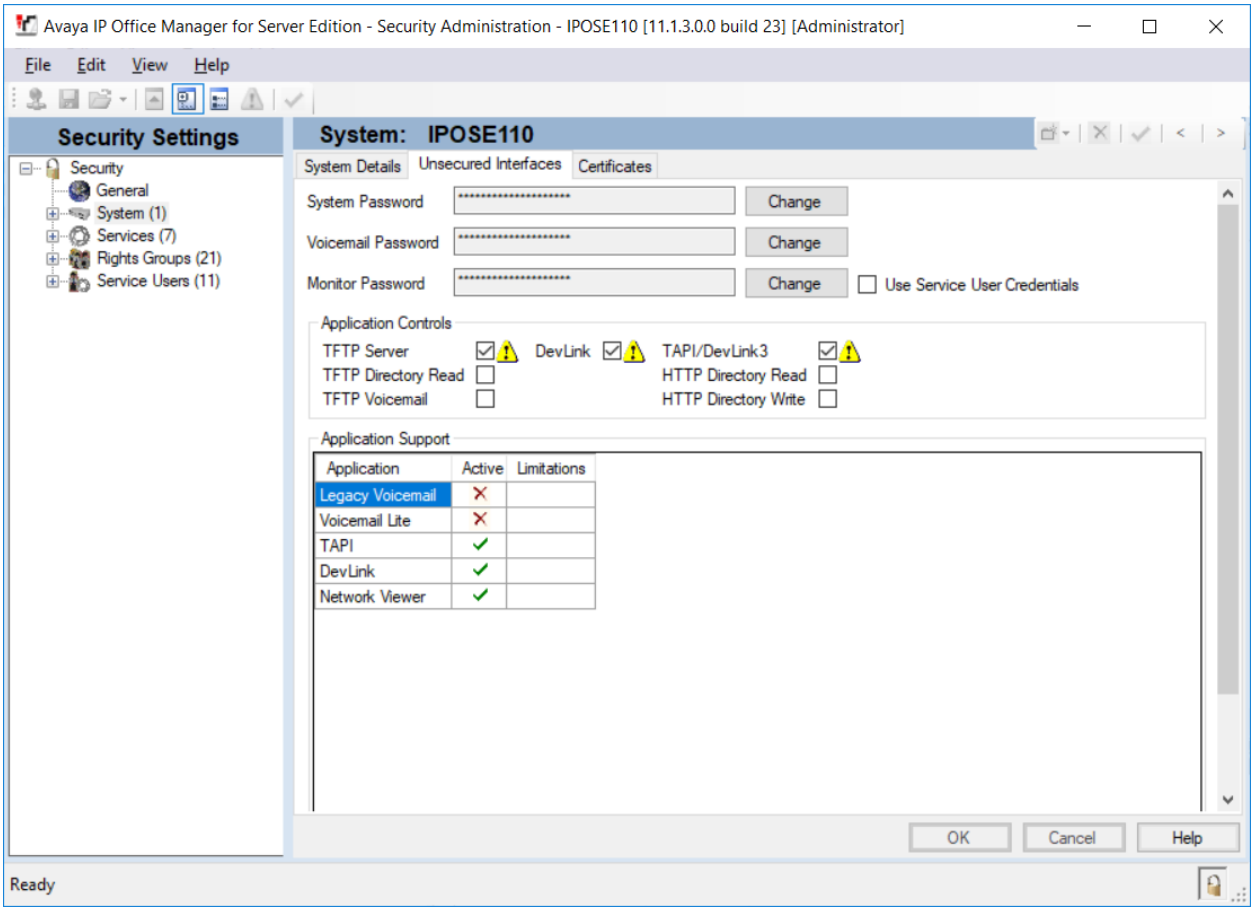


5.2. Administer System Interfaces

From the configuration tree in the left pane for the Primary System, select **File → Advanced → Security Settings** from the top menu.

The **Avaya IP Office Manager for Server Edition – Security Administration** screen is displayed. Select **Security → System** from the left pane, to display the **System** screen in the right pane.

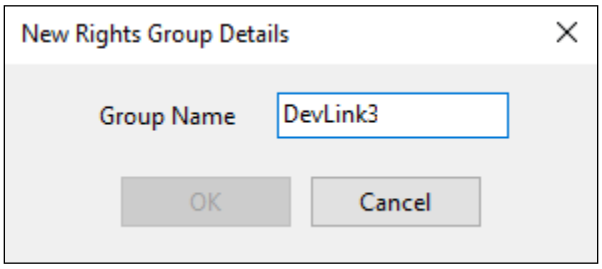
Select the **Unsecured Interfaces** tab, and make certain **TAPI/DevLink3** is checked, as shown below.



5.3. Administer Rights Groups

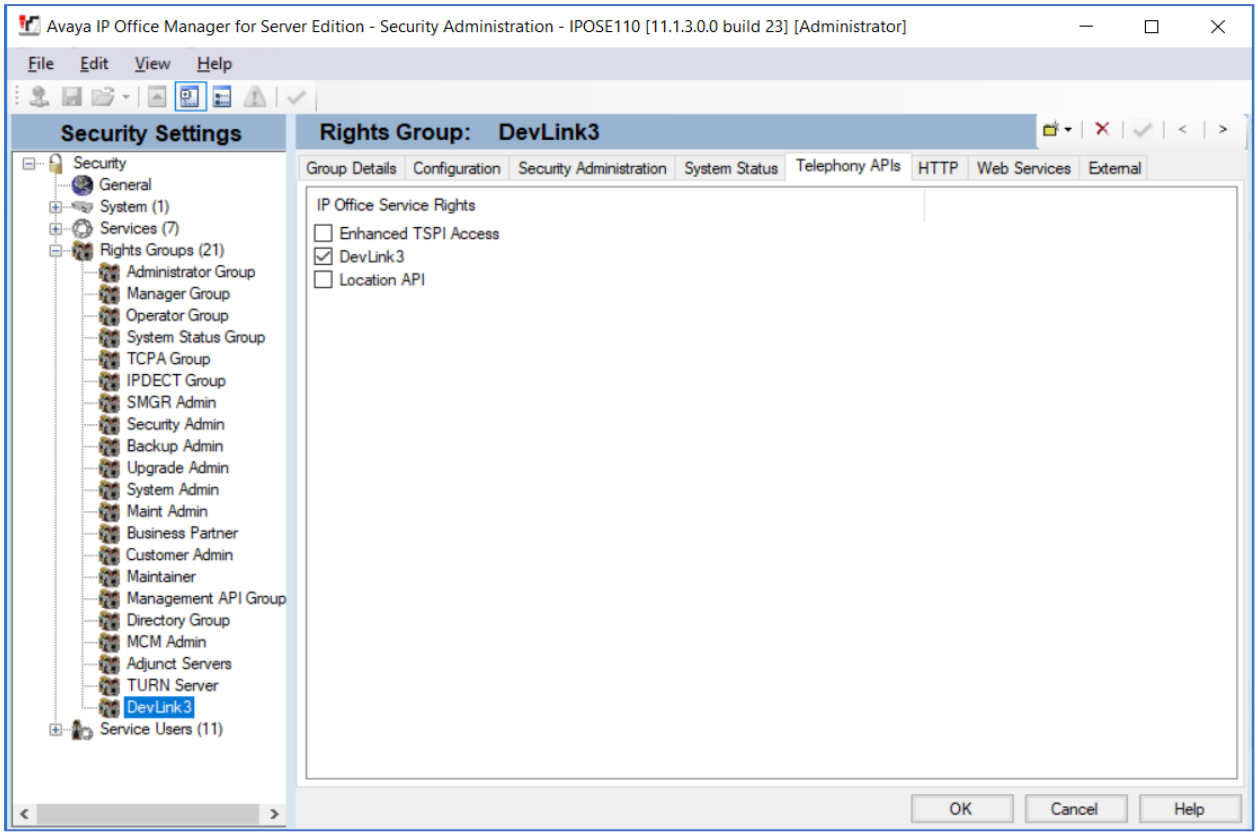
From the **Avaya IP Office Manager – Security Administration** screen shown in **Section 5.2**, select and right-click on **Rights Groups** in the left pane, followed by **New** from the pop-up list to add a new rights group.

The **New Rights Group Details** dialog box is displayed. For **Group Name**, enter a descriptive name, as shown below.



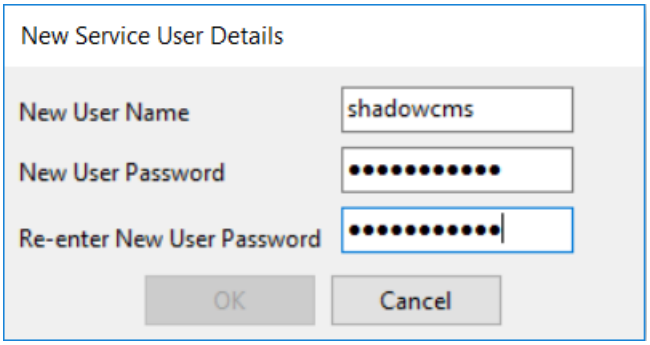
The **Avaya IP Office Manager for Server Edition – Security Administration** screen is updated, with **Rights Group: DevLink3** shown in the right pane, where **DevLink3** is the name of the newly added rights group.

Select the **Telephony APIs** tab in the right pane, and check **DevLink3**, as shown below.

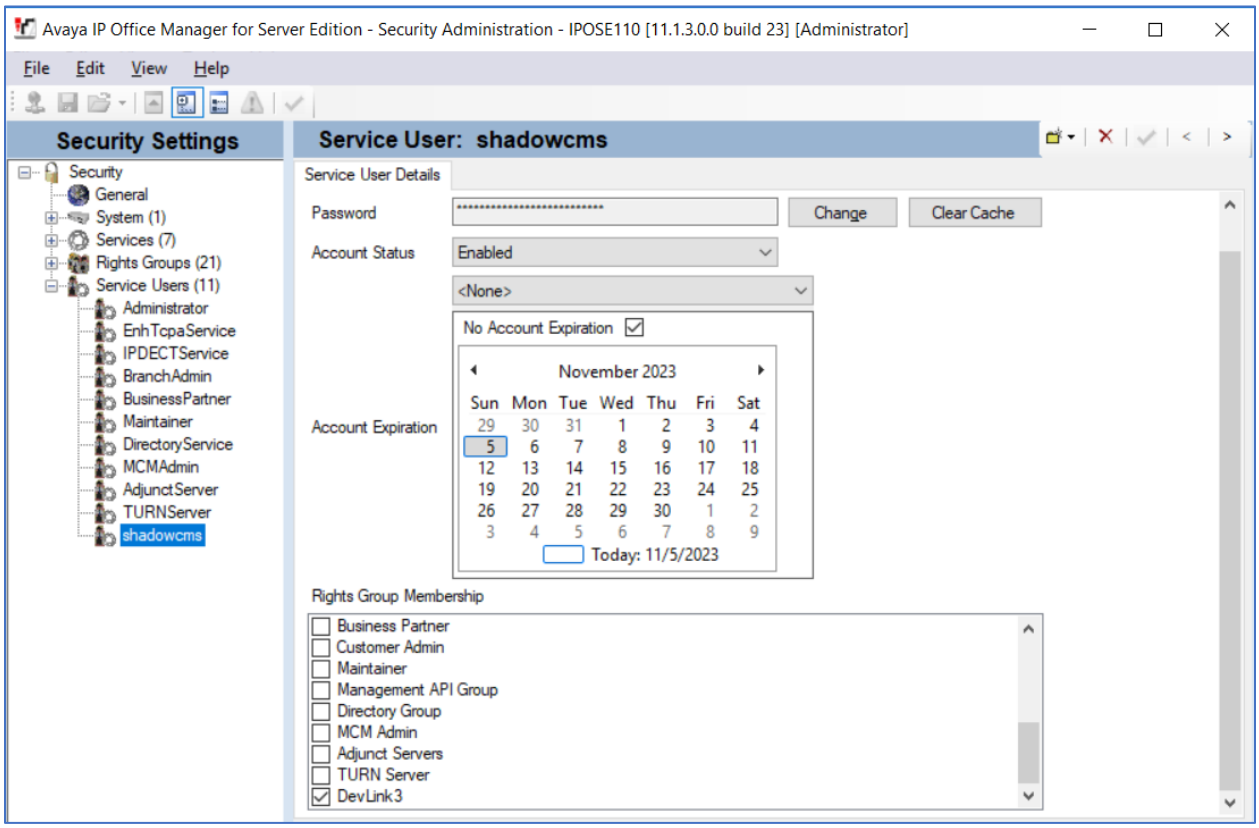


5.4. Administer Service Users

From the **Avaya IP Office Manager – Security Administration** screen shown in **Section 5.2**, select and right-click on **Service Users** in the left pane, followed by **New** from the pop-up list to add a new service user. The **New Service User Details** dialog box is displayed. Enter desired name and password, as shown below.



The **Avaya IP Office Manager for Server Edition – Security Administration** screen is updated, with **Service User: shadowcms** shown in the right pane, where **shadowcms** is the name of the newly added service user from above. Scroll the **Rights Group Membership** in the bottom right pane as necessary and check the newly added rights groups from **Section 5.3**, in this case **DevLink3**.



6. Configure Resource Software International Shadow CMS

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

- Launch Web Interface
- Administer IP Office Connection

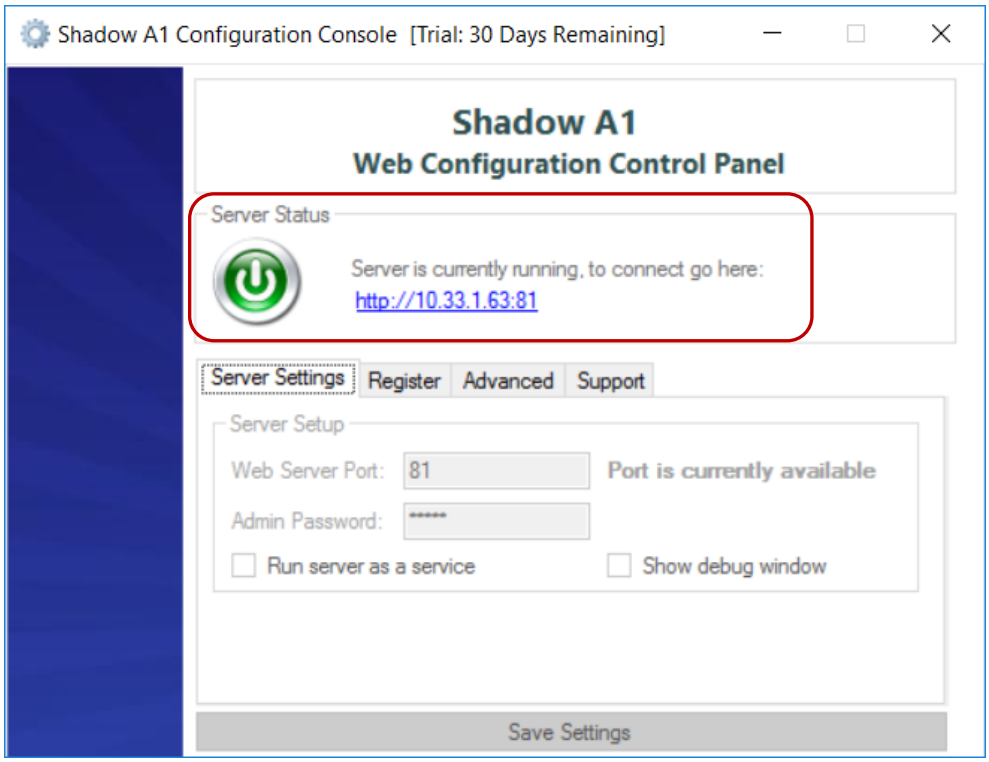
The configuration of Shadow CMS is typically performed by RSI Support Services. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch Web Interface

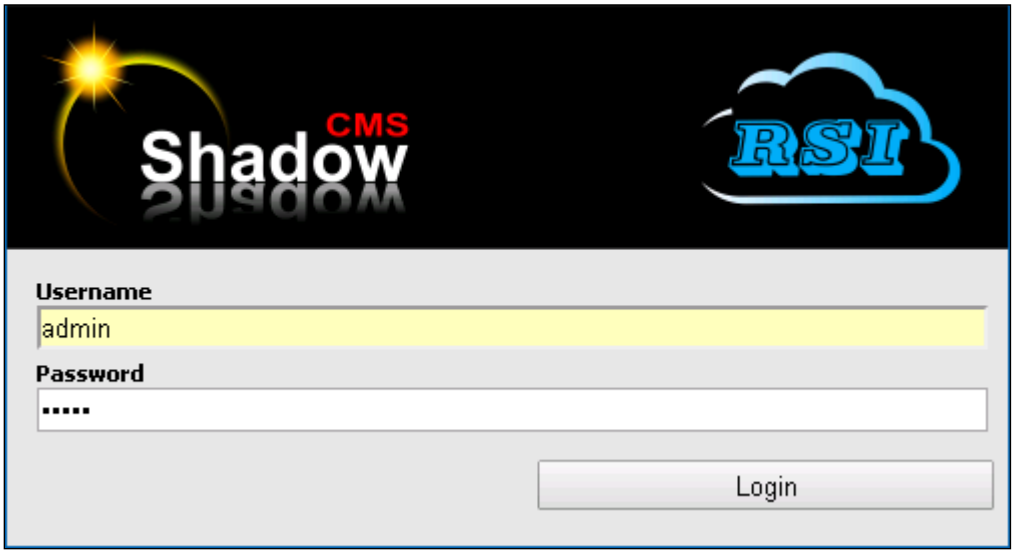
The Shadow CMS can be configured using the **Shadow CMS – Shadow Voice and Data Management** window. To access this window, from the server where Shadow CMS is installed, navigate to **Start → All Programs → RSI → Web CMS → Web CMS Configuration Console**.

The Web Configuration Control Panel window is shown below. Ensure that the **Server Status** button is **green**. If it is in red status, then click on the power button to start the server. Now click on the link that shows the IP Address of the server where Shadow CMS is installed.

Note that if the server status is green, then the **Shadow CMS – Shadow Voice and Data Management** can also be launched from another PC by typing the IP Address of the Shadow CMS server in a web browser.



Enter the **Username** and **Password** credentials and click the **Login** button.

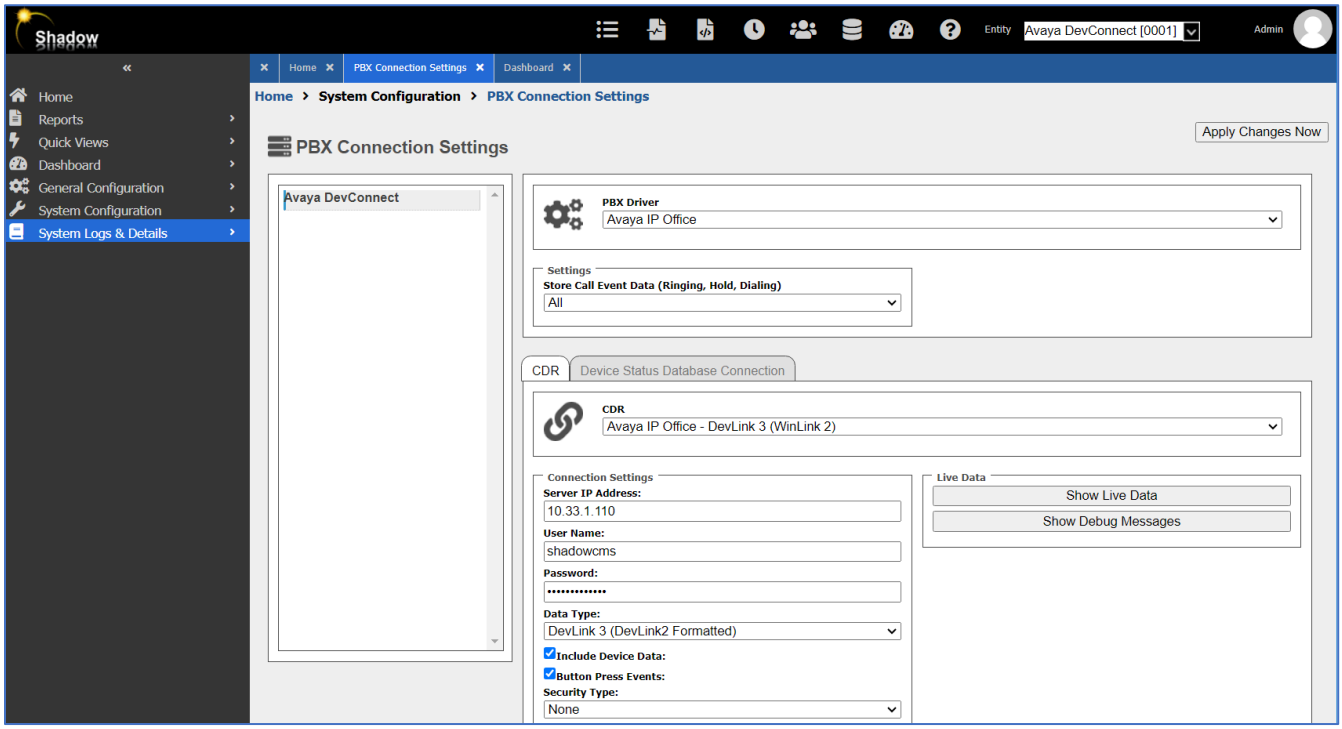


6.2. Administer IP Office Connection

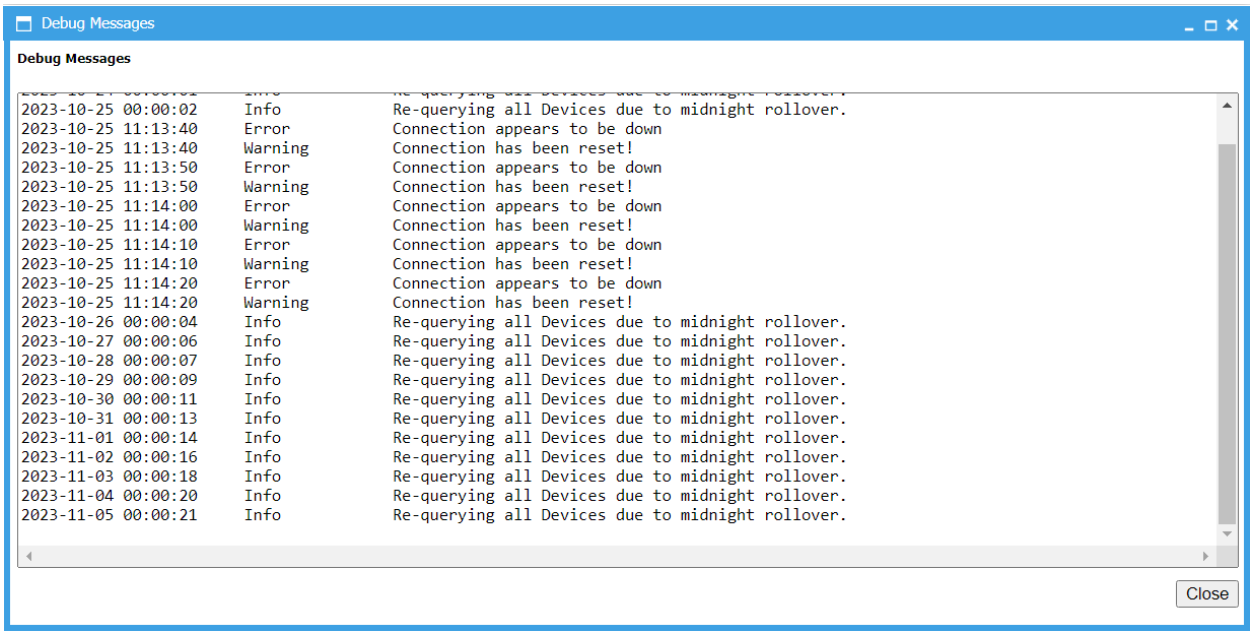
Once the proper credentials are entered from the previous section, the **Shadow CMS – Shadow Voice and Data Management** screen is seen as shown below. From this screen navigate to **System Configuration → PBX Connection Settings** and configure the following:

- **PBX Driver**: Select **Avaya IP Office** from the drop-down menu.
- **CDR**: Select **Avaya IP Office – DevLink 3 (WinLink 2)** from the drop-down menu.
- **Server IP Address**: Enter the IP address of IP Office Primary System.
- **User Name**: Enter the name configured in **Section 5.4**.
- **Password**: Enter the password configured for the above User Name in **Section 5.4**.
- **Data Type**: Select **DevLink 3 (DevLink2 Formatted)** from the drop-down menu.

Retain default values for all other fields and click the **Apply Changes Now** button.



From the above screen, click on the **Show Debug Messages** button and the **Debug Messages** screen is shown as seen below. If all the configuration from above is correct, user will see the successful connection messages to DevLink3 of Avaya IP Office.



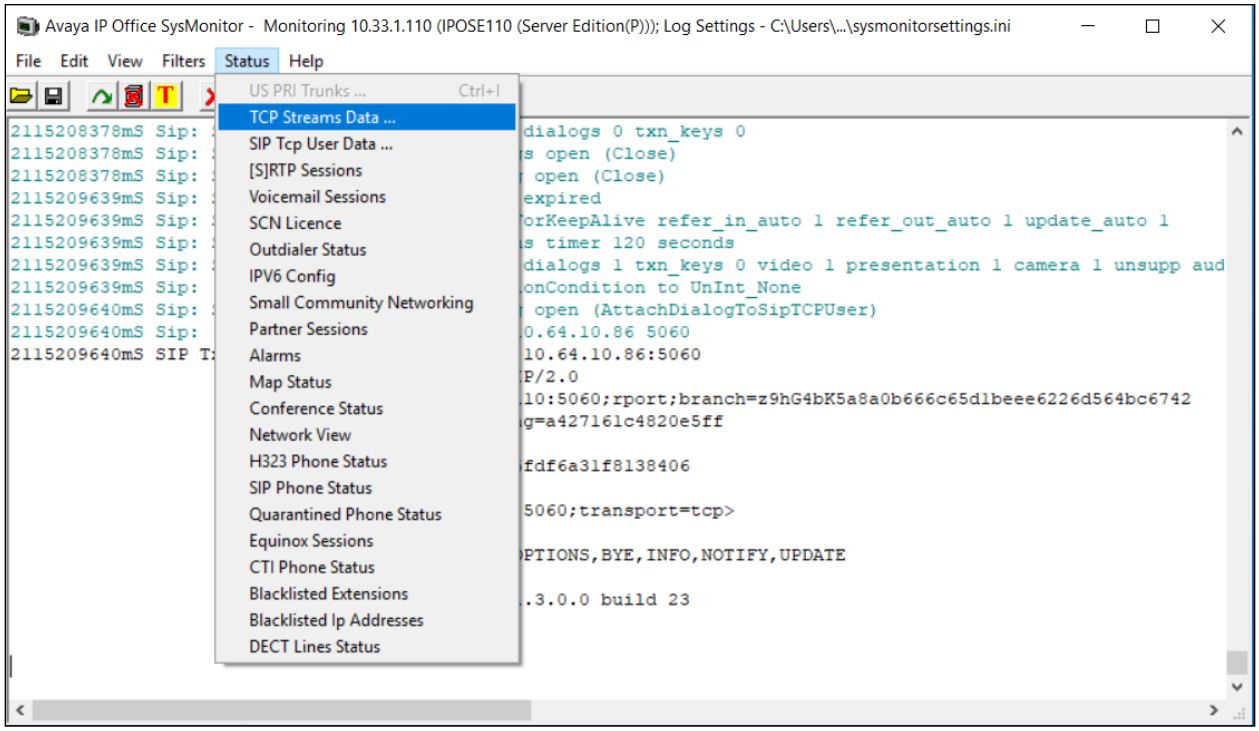
7. Verification Steps

This section provides tests that can be performed to verify proper configuration of IP Office and Shadow CMS.

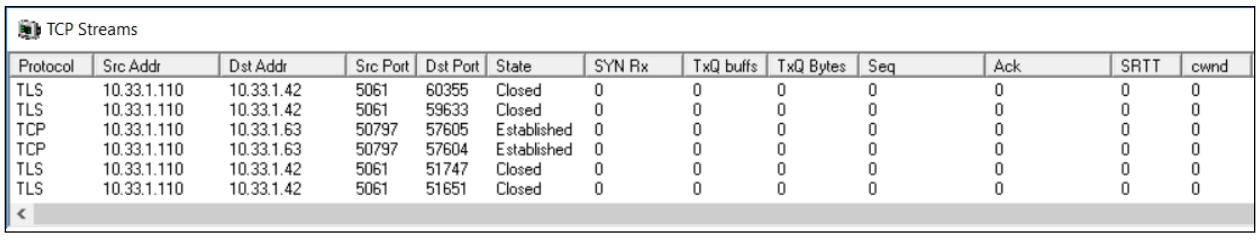
7.1. Verify Avaya IP Office

From a PC running the IP Office Monitor application, select **Start → All Programs → IP Office → Monitor** to launch the application, and connect to the IP Office Primary system.

The **Avaya IP Office SysMonitor** screen is displayed. Select **Status → TCP Stream Data** from the top menu.



The **TCP Streams** screen is displayed. Verify that there is an entry corresponding to the Shadow CMS server, with the IP address of the Shadow CMS server in the **Dst Addr** column. Also verify that the pertinent entry has the **State** as **Established**.



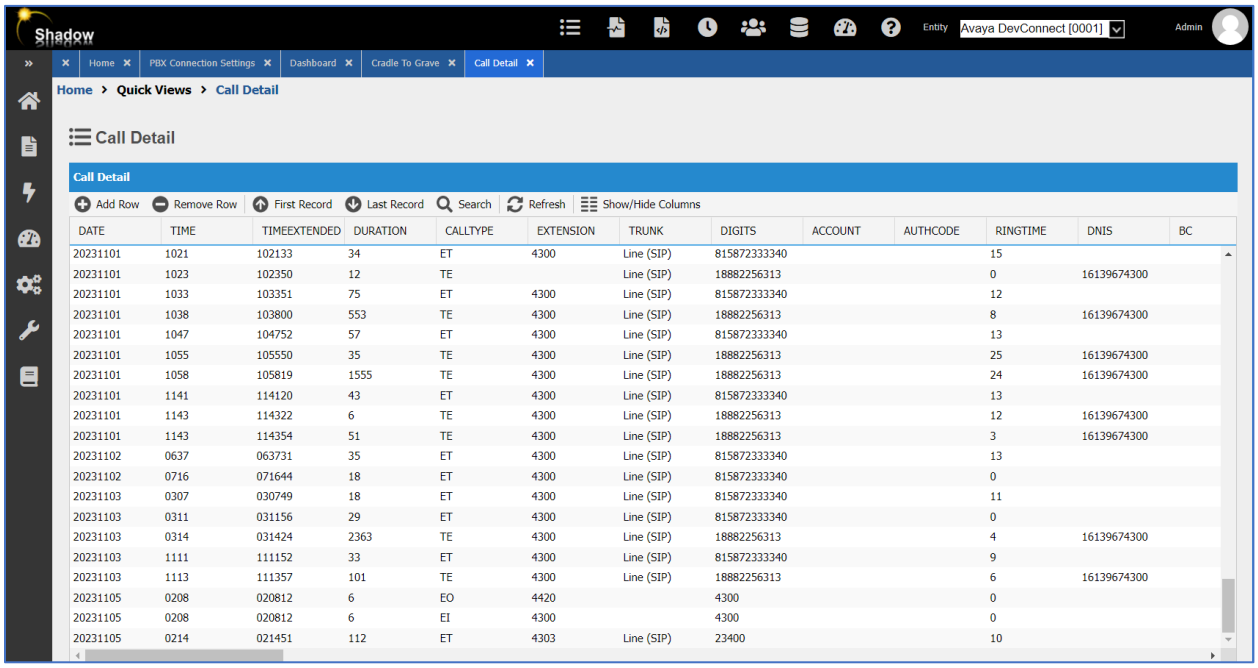
Protocol	Src Addr	Dst Addr	Src Port	Dst Port	State	SYN Rx	TxQ buffs	TxQ Bytes	Seq	Ack	SRTT	cwnd
TLS	10.33.1.110	10.33.1.42	5061	60355	Closed	0	0	0	0	0	0	0
TLS	10.33.1.110	10.33.1.42	5061	59633	Closed	0	0	0	0	0	0	0
TCP	10.33.1.110	10.33.1.63	50797	57605	Established	0	0	0	0	0	0	0
TCP	10.33.1.110	10.33.1.63	50797	57604	Established	0	0	0	0	0	0	0
TLS	10.33.1.110	10.33.1.42	5061	51747	Closed	0	0	0	0	0	0	0
TLS	10.33.1.110	10.33.1.42	5061	51651	Closed	0	0	0	0	0	0	0

7.2. Verify Resource Software International Shadow CMS

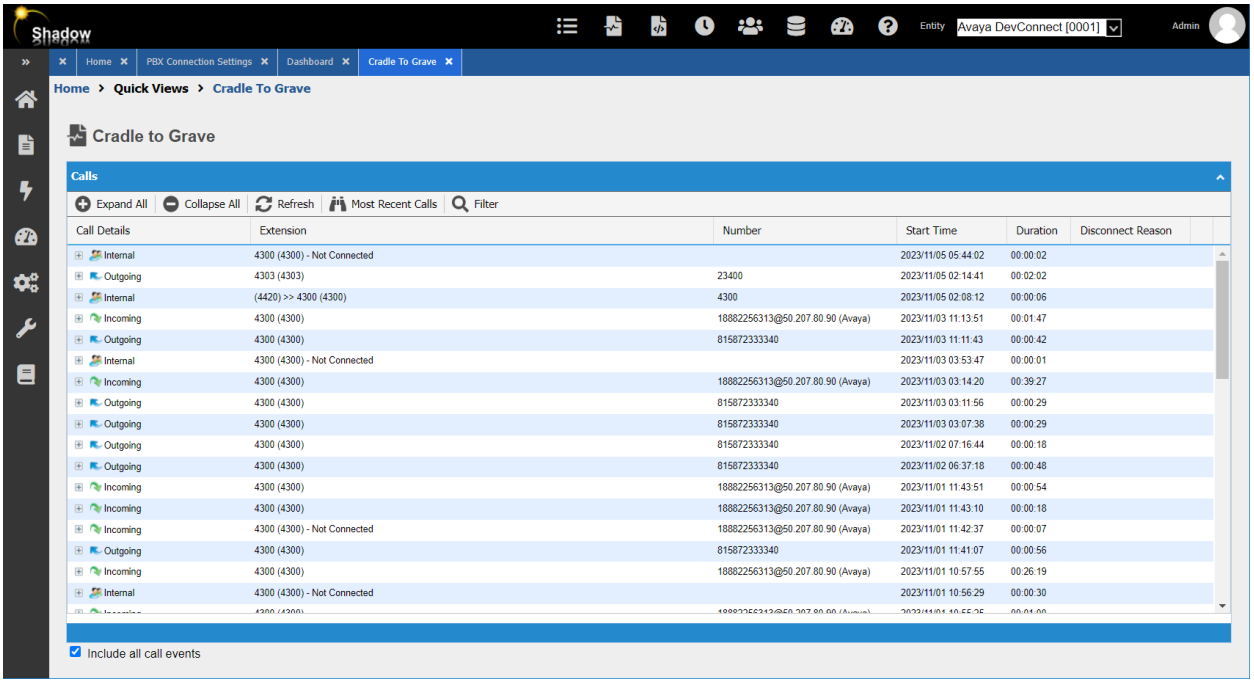
This section provides tests that can be performed to verify Shadow CMS Cradle To Grave, Call Detail and real-time Dashboard reporting.

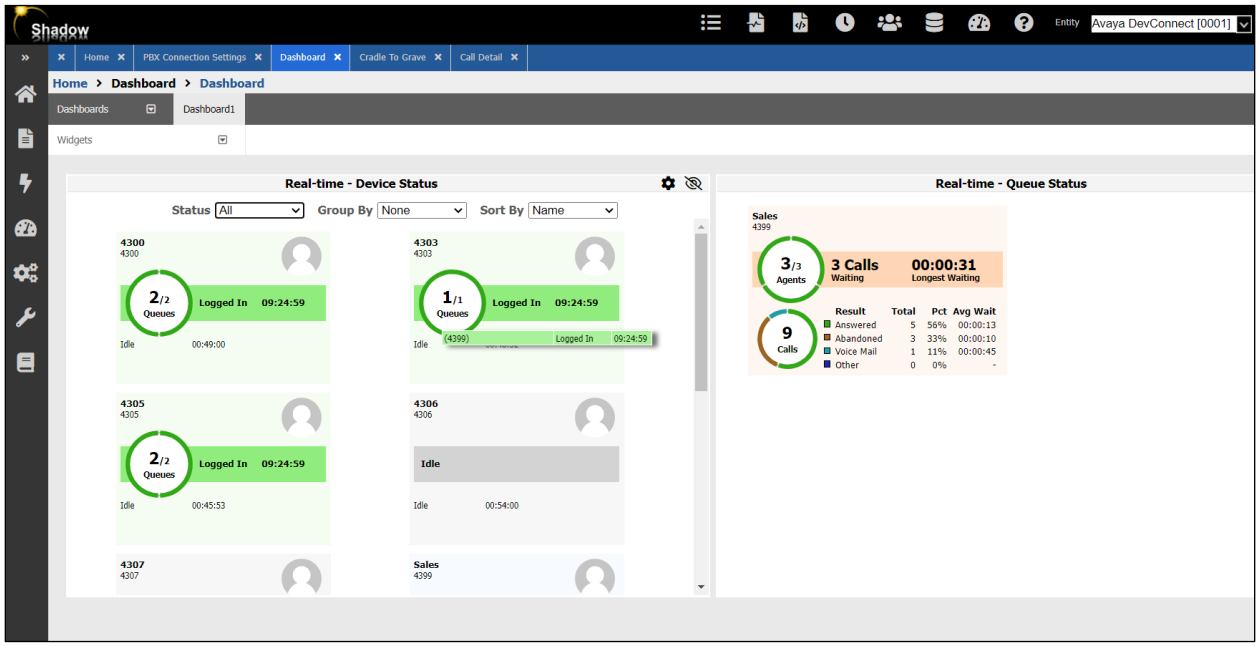
Place an incoming trunk call from PSTN to a hunt group with an available agent. Answer the call at the agent and perform a few actions such as hold/resume before ending the call.

Follow the procedures in **Section 6.1** to access the Shadow CMS web interface. From the tabs in top row, select the required functions. Example below shows screen shots of **Call Detail**, **Cradle To Grave** and **Dashboard** tabs.



DATE	TIME	TIMEEXTENDED	DURATION	CALLTYPE	EXTENSION	TRUNK	DIGITS	ACCOUNT	AUTHCODE	RINGTIME	DNIS	BC
20231101	1021	102133	34	ET	4300	Line (SIP)	815872333340			15		
20231101	1023	102350	12	TE		Line (SIP)	18882256313			0	16139674300	
20231101	1033	103351	75	ET	4300	Line (SIP)	815872333340			12		
20231101	1038	103800	553	TE	4300	Line (SIP)	18882256313			8	16139674300	
20231101	1047	104752	57	ET	4300	Line (SIP)	815872333340			13		
20231101	1055	105550	35	TE	4300	Line (SIP)	18882256313			25	16139674300	
20231101	1058	105819	1555	TE	4300	Line (SIP)	18882256313			24	16139674300	
20231101	1141	114120	43	ET	4300	Line (SIP)	815872333340			13		
20231101	1143	114322	6	TE	4300	Line (SIP)	18882256313			12	16139674300	
20231101	1143	114354	51	TE	4300	Line (SIP)	18882256313			3	16139674300	
20231102	0637	063731	35	ET	4300	Line (SIP)	815872333340			13		
20231102	0716	071644	18	ET	4300	Line (SIP)	815872333340			0		
20231103	0307	030749	18	ET	4300	Line (SIP)	815872333340			11		
20231103	0311	031156	29	ET	4300	Line (SIP)	815872333340			0		
20231103	0314	031424	2363	TE	4300	Line (SIP)	18882256313			4	16139674300	
20231103	1111	111152	33	ET	4300	Line (SIP)	815872333340			9		
20231103	1113	111357	101	TE	4300	Line (SIP)	18882256313			6	16139674300	
20231105	0208	020812	6	EO	4420		4300			0		
20231105	0208	020812	6	EI	4300		4300			0		
20231105	0214	021451	112	ET	4303	Line (SIP)	23400			10		





8. Conclusion

These Application Notes describe the configuration steps required for Resource Software International Shadow CMS to successfully interoperate with Avaya IP Office Server Edition using DevLink3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

9. Additional References

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

Product documentation for Avaya products may be found at *http://support.avaya.com*.

1. Deploying IP Office Essential Edition (IP500 V2) IP Office™ Platform 11.0, Issue 35h (Tuesday, May 18, 2021)
2. Deploying Avaya IP Office™ Server Edition Solution (English), Release 11.1 FP1, Issue 16, February 2021
3. Administering Avaya IP Office with Manager (English), Release 11.1.1, Issue 25, February 2021
4. Administering Avaya IP Office with Web Manager (English), Release 11.1.1, Issue 25, February 2021

Product Administration and User Guide documentation for RSI products can be obtained directly from RSI.

1. Shadow CMS (Web) UserGuide.pdf

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.