



Application Notes for Resource Software International Shadow Call Management System with Avaya IP Office Server Edition – 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 DevConnect Program at the Avaya Solution and Interoperability Test Lab.

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.
- Set A uses hot desking and logs into Set B as Set A. When Set A logs out of Set B, Set B logs in automatically with its own extension however the dashboard of Shadow CMS is not aware of this since there is no event sent to it from IP Office Manager. To send an event, Set B can re-login or will show the correct status after the midnight rollover routine of Shadow CMS.
- 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. The grid clears when the call ends.
- 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. RSI is aware of this issue and is investigating.
- 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. Each IP Office system has connectivity to the PSTN, 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.

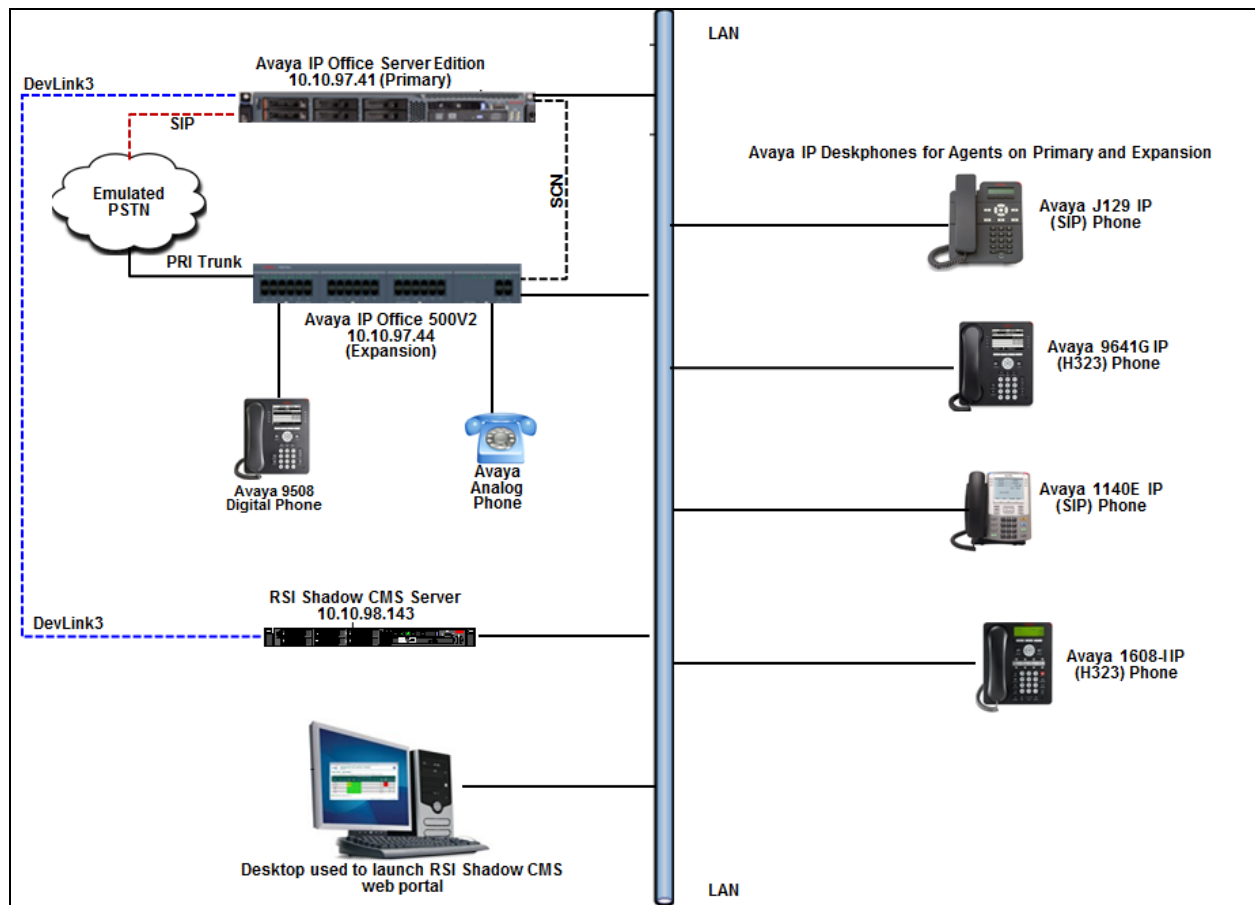


Figure 1: Compliance Testing Configuration

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 on Primary Linux server	11.0.0.0.0 build 849
Avaya IP Office 500 V2 Expansion	11.0.0.0.0 build 849
Avaya IP Deskphones: - 1140E (SIP) - J129 (SIP) -9641G (H.323) -1608-L (H.323)	4.4.23 2.0.0.0.45 6.6506 1.3110
Avaya 9508 Digital Phone	0.60
Resource Software International Shadow CMS on Windows 2008 R2 Standard SP1	5.2.0.0

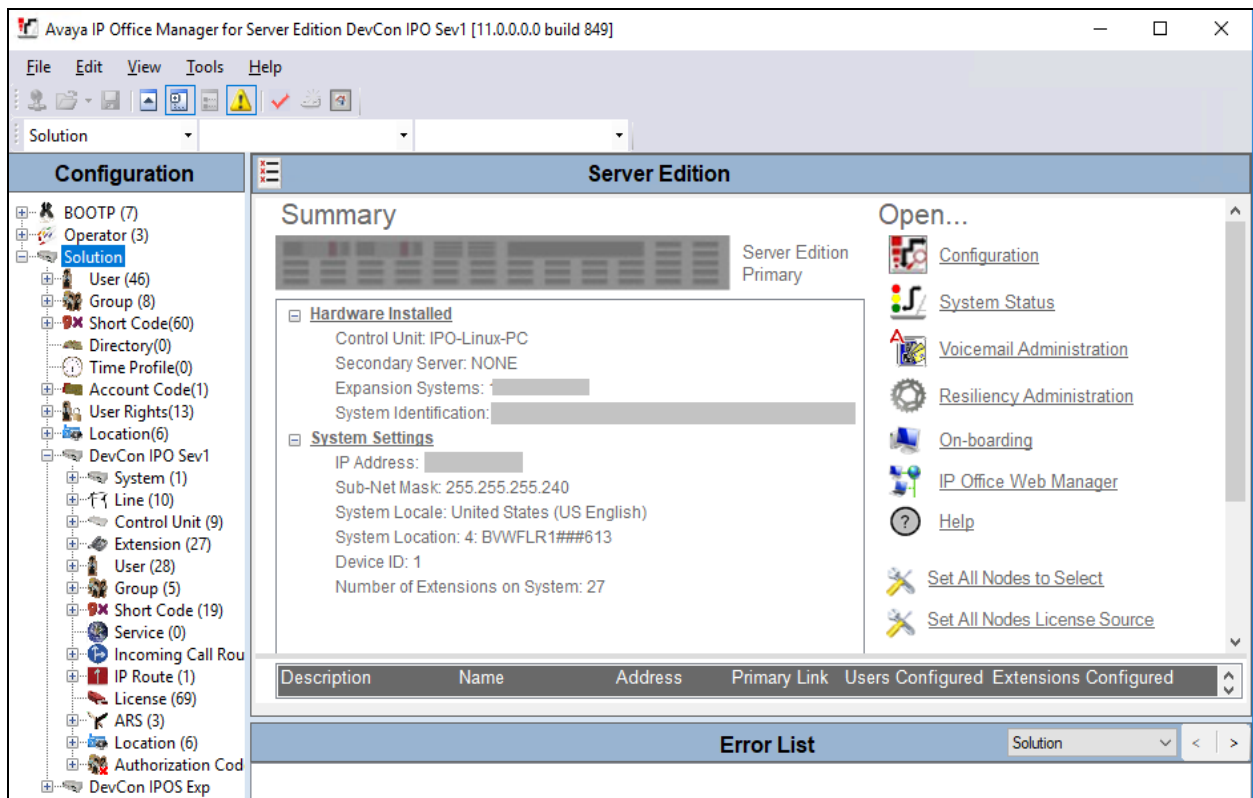
Note: *Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and when deployed with IP Office Server Edition in all configurations.*

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:

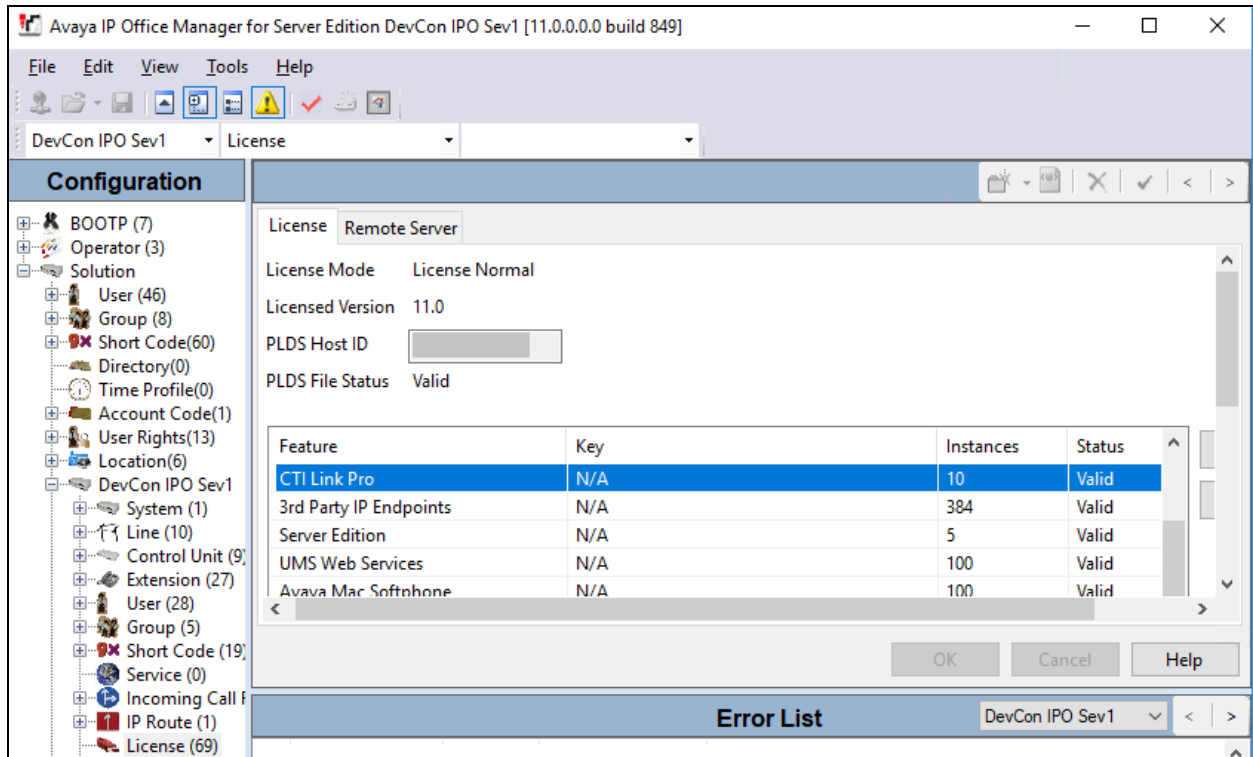
- Verify license
- Administer system interfaces
- Administer rights groups
- Administer service users

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 **DevCon IPO Sev1** 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.

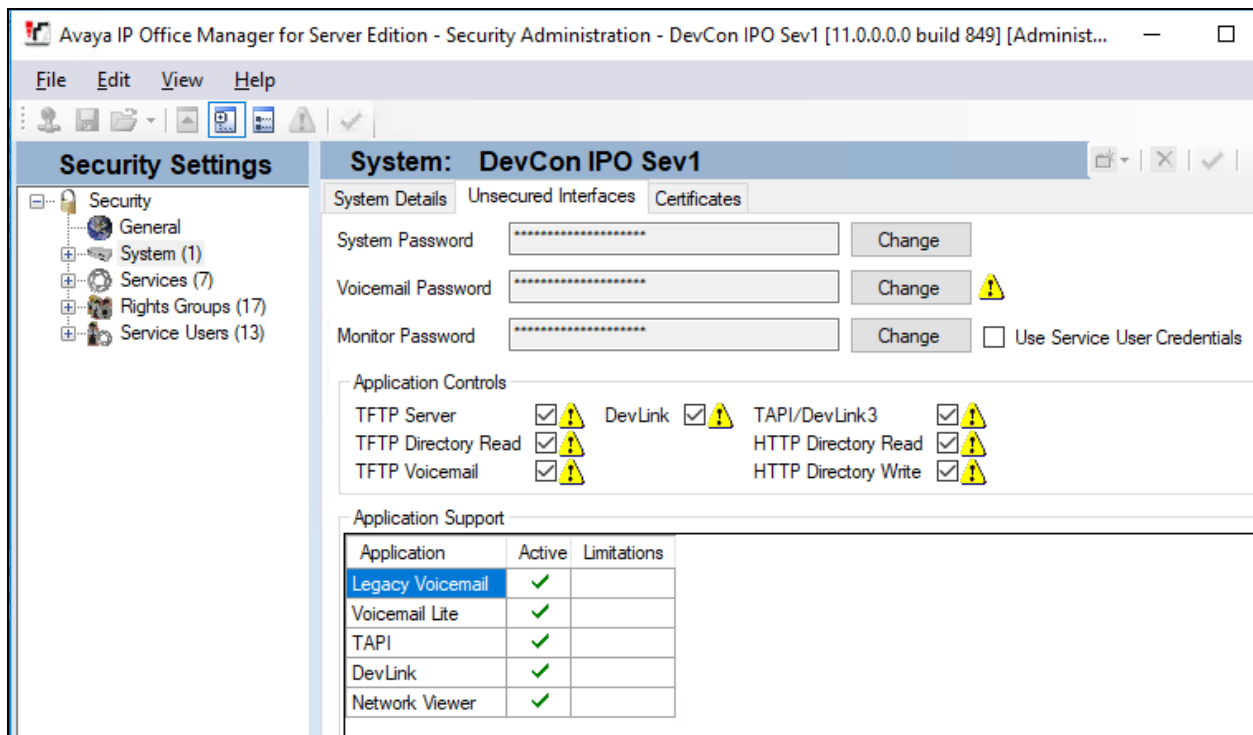


5.2. Administer System Interfaces

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.

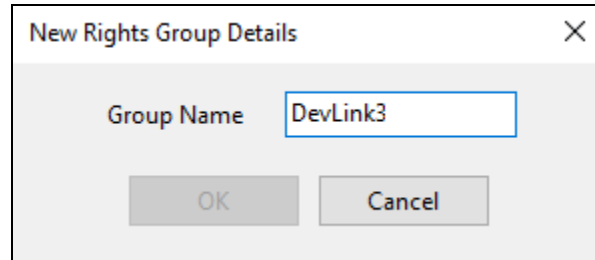
Select the **Unsecured Interfaces** tab, and make certain **TAPI/DevLink3** is checked, as shown below.



5.3. Administer Rights Groups

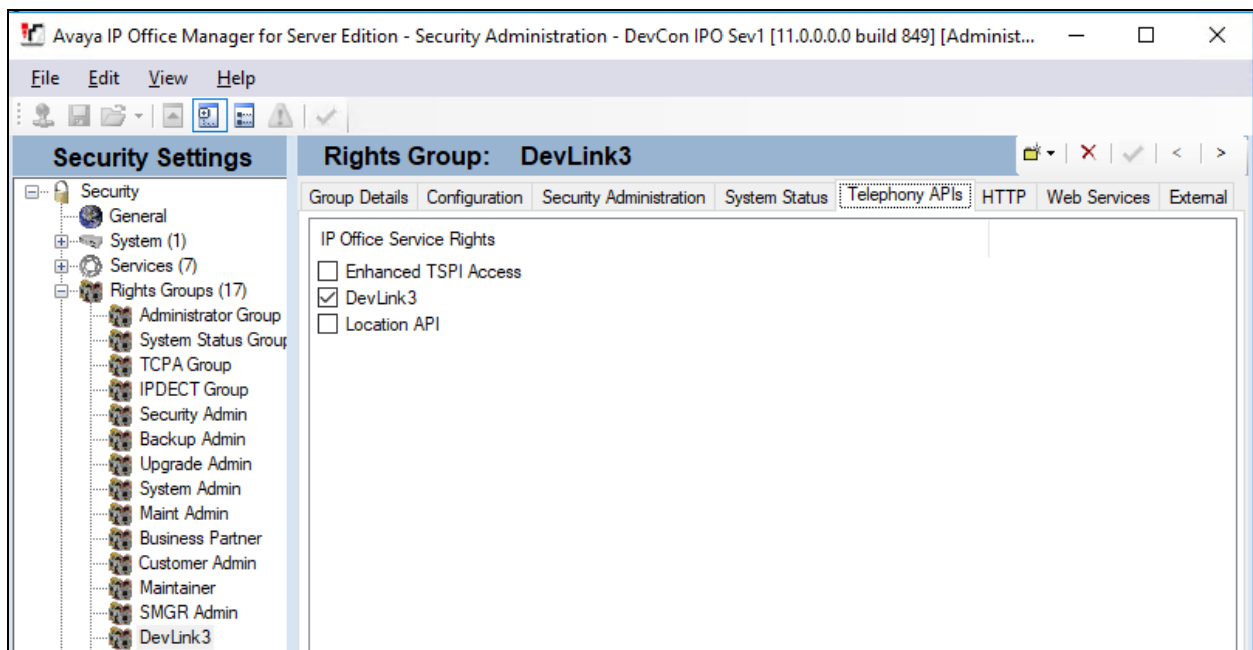
From the **Avaya IP Office Manager – Security Administration** screen shown in **Section 5.2**, select and right-click on **Rights Groups** in the left pane, followed by **New** from the pop-up list to add a new rights group.

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



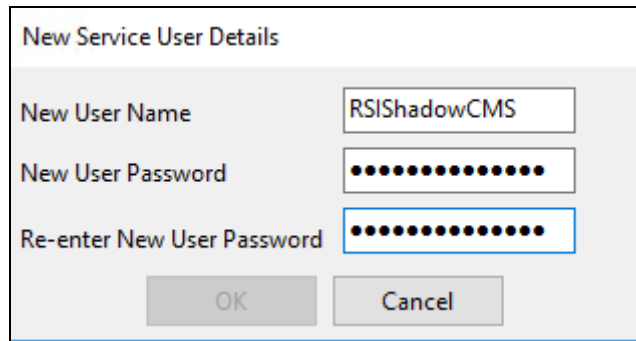
The **Avaya IP Office Manager for Server Edition – Security Administration** screen is updated, with **Rights Group: DevLink3** shown in the right pane, where **DevLink3** is the name of the newly added rights group.

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



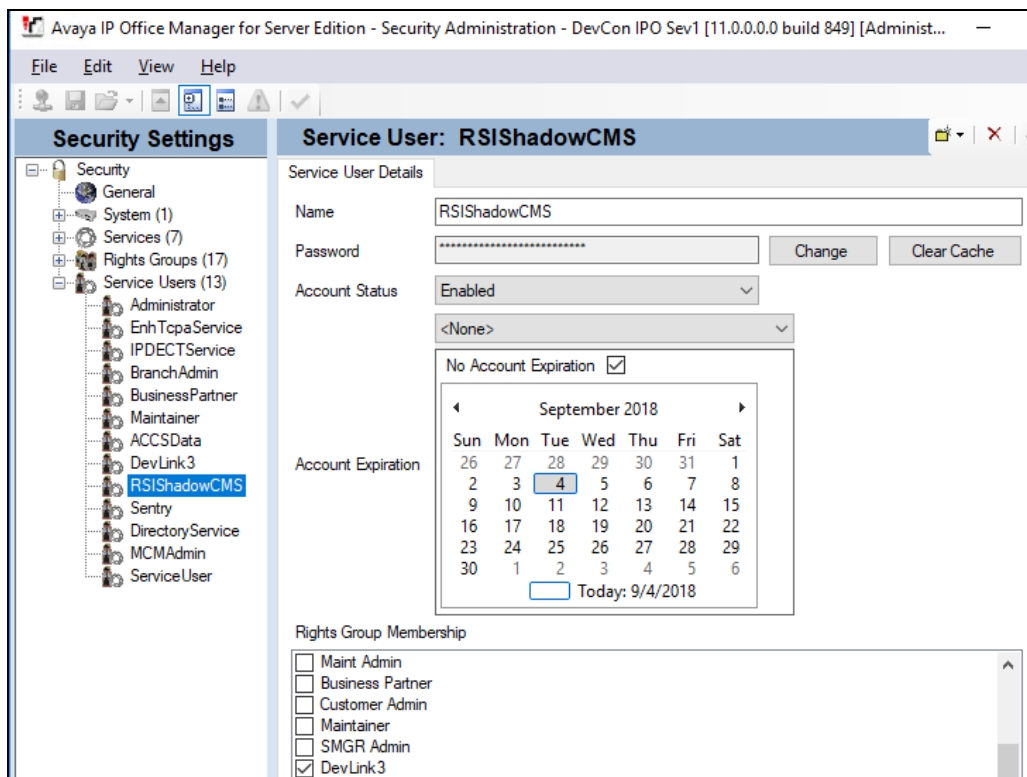
5.4. Administer Service Users

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 dialog box titled "New Service User Details" contains three input fields: "New User Name" with the text "RSIShadowCMS", "New User Password" with masked characters, and "Re-enter New User Password" also with masked characters. At the bottom are "OK" and "Cancel" buttons.

The **Avaya IP Office Manager for Server Edition – Security Administration** screen is updated, with **Service User: RSIShadowCMS** shown in the right pane, where **RSIShadowCMS** 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**.



The screenshot shows the Avaya IP Office Manager for Server Edition - Security Administration interface. The left pane shows a tree view of Security Settings, with Service Users (13) expanded. The right pane shows the Service User Details for RSIShadowCMS. The Account Status is Enabled, and the Account Expiration is set to No Account Expiration. The Rights Group Membership section shows a list of groups, with DevLink3 checked.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 9/4/2018

Rights Group Membership

- ☐ Maint Admin
- ☐ Business Partner
- ☐ Customer Admin
- ☐ Maintainer
- ☐ SMGR Admin
- ☒ 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 Avaya IP Office connection

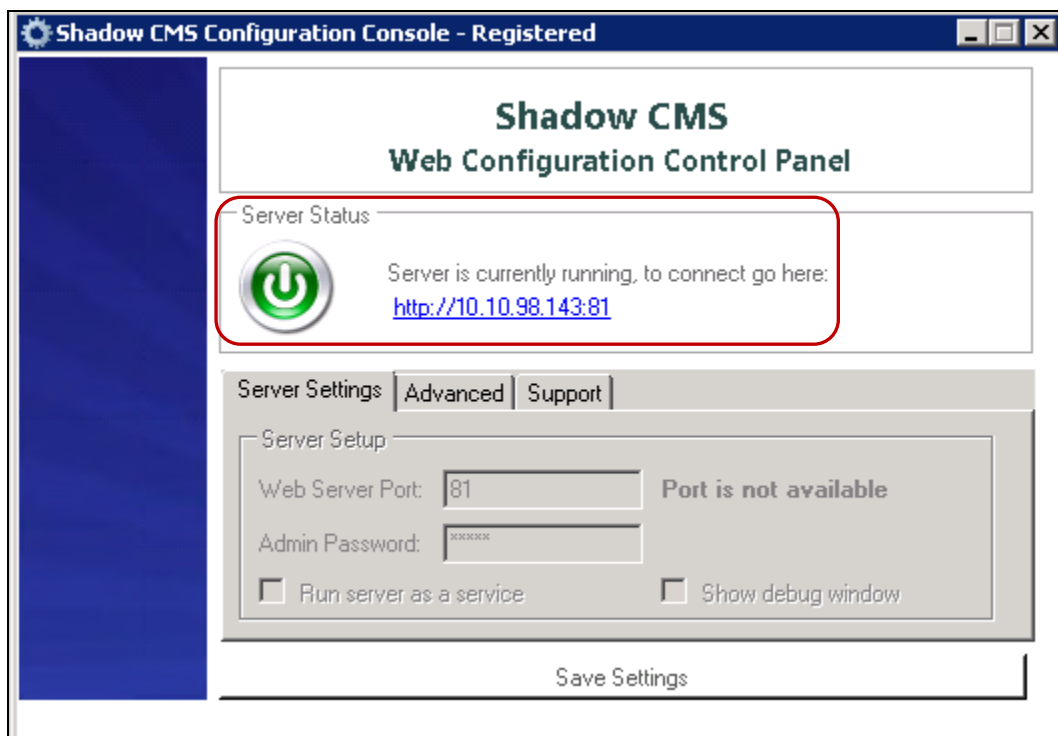
The configuration of Shadow CMS is typically performed by RSI Support Services. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch Web Interface

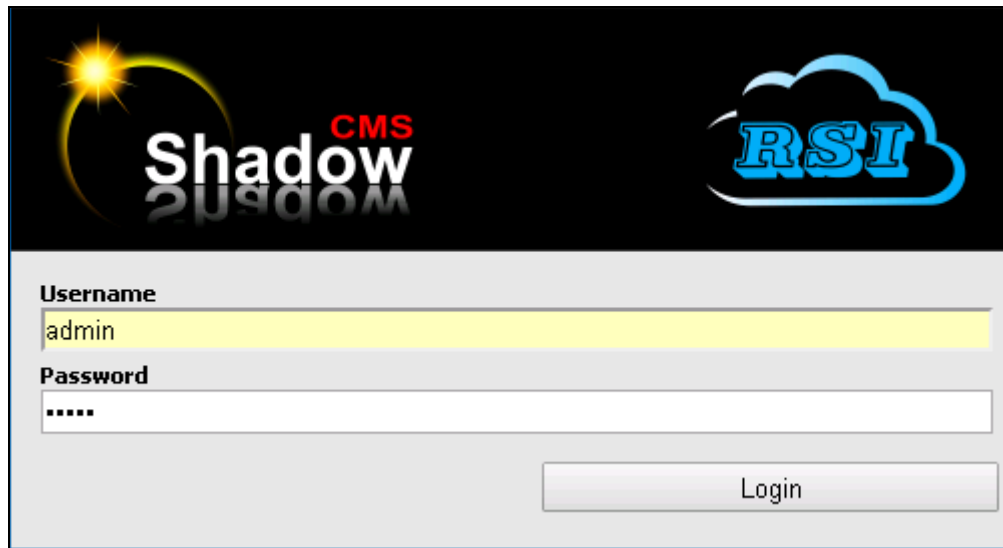
The Shadow CMS can be configured using the **Shadow CMS – Shadow Voice and Data Management** window. To access this window, from the server where Shadow CMS is installed, navigate to **Start → All Programs → RSI → Web CMS → Web CMS Configuration Console**.

The Web Configuration Control Panel window is seen as 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.



The image shows a login interface for Shadow CMS. At the top, there is a black header bar. On the left side of the header is the 'Shadow CMS' logo, which includes a yellow sun-like icon and the text 'Shadow' in white with 'CMS' in red. On the right side of the header is the 'RSI' logo, which consists of the letters 'RSI' in blue inside a blue cloud shape. Below the header is a light gray rectangular area containing the login form. The form has two input fields: the first is labeled 'Username' and contains the text 'admin'; the second is labeled 'Password' and contains six dots. To the right of these fields is a 'Login' button.

Shadow CMS

RSI

Username

admin

Password

.....

Login

6.2. Administer Avaya IP Office Connection

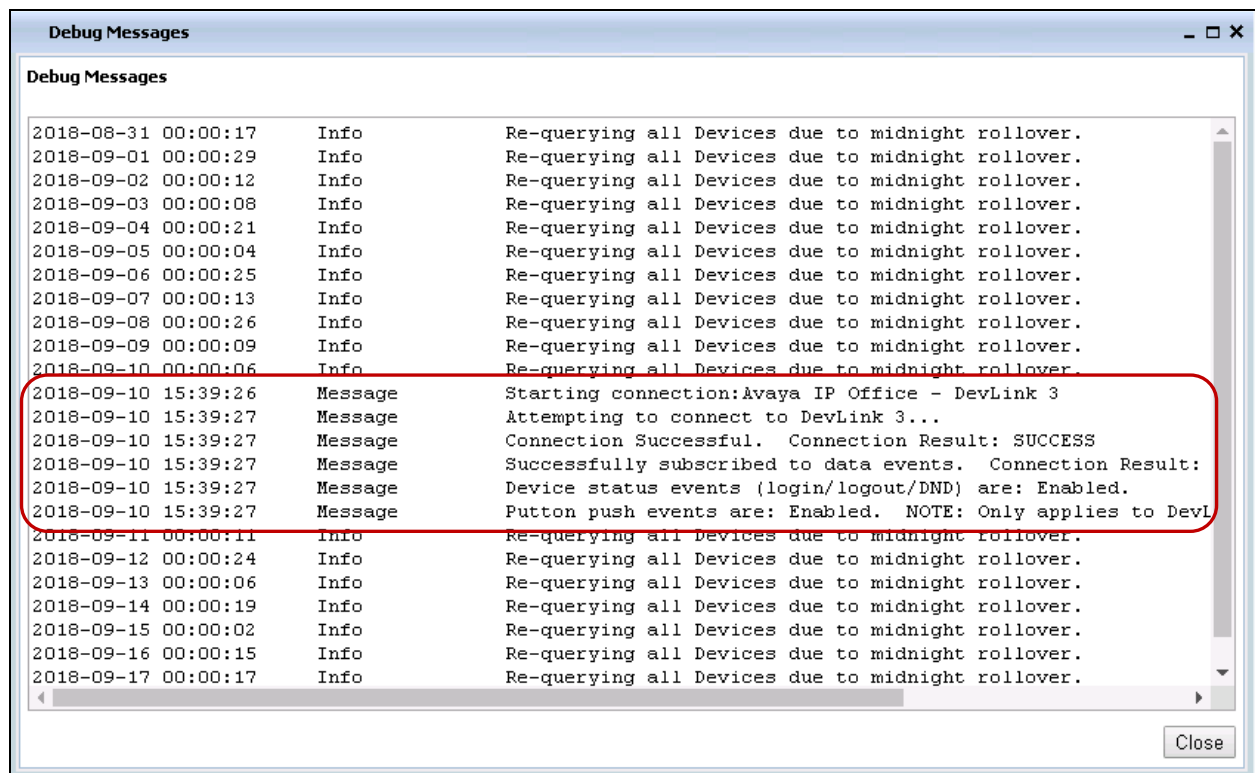
Once the proper credentials are entered from the previous section, the **Shadow CMS – Shadow Voice and Data Management** screen is seen as shown below. From this screen navigate to **System Configuration → PBX Connection Settings** and configure the following:

- **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.

The screenshot shows the Shadow CMS interface. At the top, the 'Shadow' logo is on the left, and 'Entity: RSI [0001]' and 'Admin' are on the right. Below the header is a navigation menu with options like 'Close', 'Call Detail', 'Cradle to Grave', 'Custom Report Builder', 'Report and Task Scheduler', 'Personnel Management', 'Database Maintenance', and 'Dashboard'. The main content area is titled 'PBX Connection Settings' and features an 'Apply Changes Now' button. On the left, a list of system configuration options is shown, with 'PBX Connection Settings' selected. The main configuration area includes a 'PBX Driver' dropdown set to 'Avaya IP Office', a 'CDR' dropdown set to 'Avaya IP Office - DevLink 3 (WinLink 2)', and a 'Connection Settings' section with fields for 'Server IP Address' (10.10.97.41), 'User Name' (RSIShadowCMS), 'Password' (masked), and 'Data Type' (DevLink 3 (DevLink2 Formatted)). There are also checkboxes for 'Include Device Data' and 'Button Press Events'. At the bottom, there are buttons for 'Show Live Data' and 'Show Debug Messages'.

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.



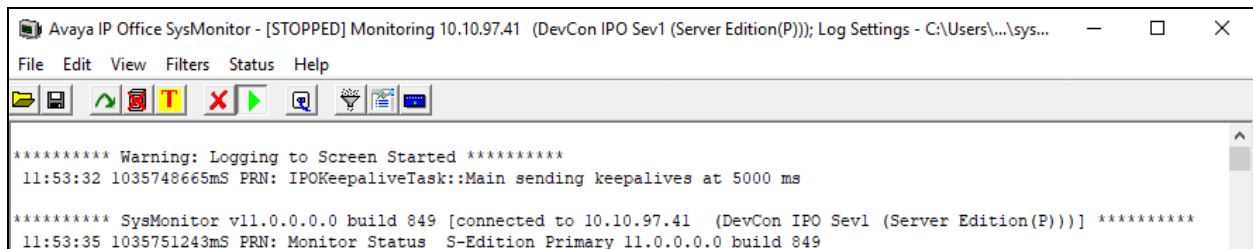
7. Verification Steps

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**.

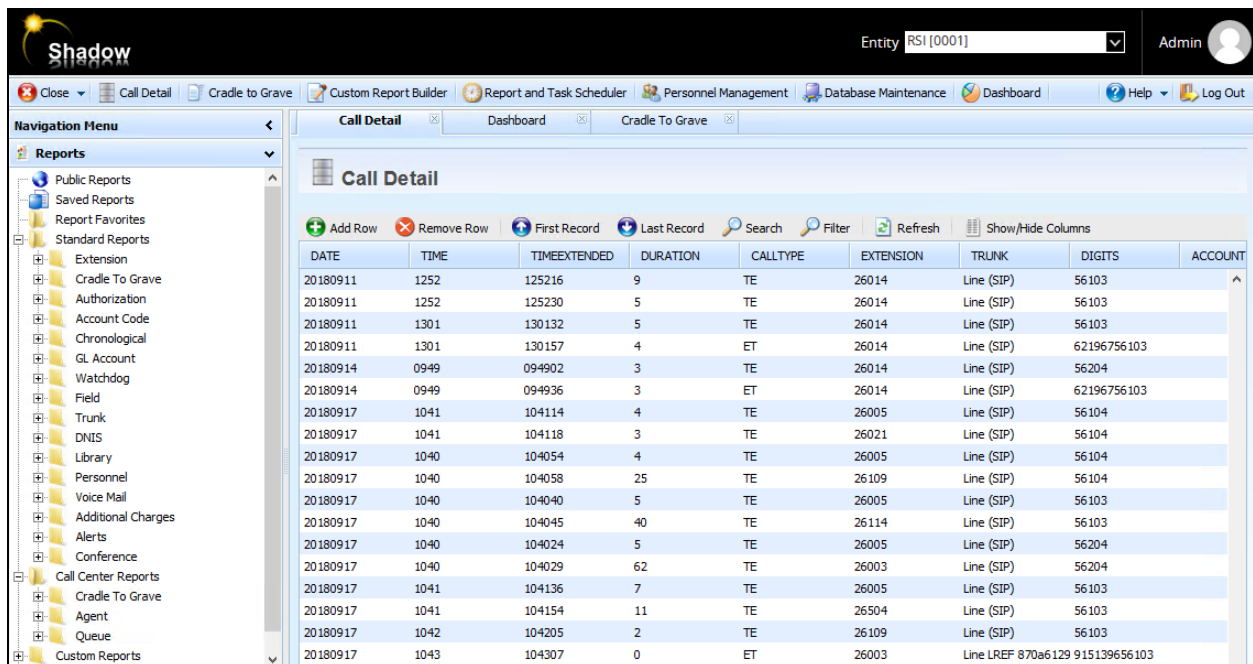
TCP Streams							
Protocol	Src Addr	Dst Addr	Src Port	Dst Port	State	SYN Rx	TxQ buffs ^
TCP	10.10.97.41	10.10.98.143	50797	49364	Established	0	0
TCP	10.10.97.41	10.10.98.143	50797	49272	Established	0	0
TCP	10.10.97.41	10.10.98.143	50797	49271	Established	0	0
TCP	10.10.97.41	10.10.98.143	50797	49270	Established	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.



The screenshot displays the Shadow CMS web interface. The top bar shows the Shadow logo, the entity 'RSI [0001]', and an 'Admin' user profile. The navigation menu on the left lists various report categories under 'Reports', including 'Public Reports', 'Saved Reports', 'Report Favorites', 'Standard Reports', 'Extension', 'Cradle To Grave', 'Authorization', 'Account Code', 'Chronological', 'GL Account', 'Watchdog', 'Field', 'Trunk', 'DNIS', 'Library', 'Personnel', 'Voice Mail', 'Additional Charges', 'Alerts', 'Conference', 'Call Center Reports', 'Cradle To Grave', 'Agent', 'Queue', and 'Custom Reports'. The main content area is titled 'Call Detail' and features a table of call records. The table has columns for DATE, TIME, TIMEEXTENDED, DURATION, CALLTYPE, EXTENSION, TRUNK, DIGITS, and ACCOUNT. The records show a list of calls with their respective details, including dates, times, durations, call types, extensions, trunks, and digits.

DATE	TIME	TIMEEXTENDED	DURATION	CALLTYPE	EXTENSION	TRUNK	DIGITS	ACCOUNT
20180911	1252	125216	9	TE	26014	Line (SIP)	56103	
20180911	1252	125230	5	TE	26014	Line (SIP)	56103	
20180911	1301	130132	5	TE	26014	Line (SIP)	56103	
20180911	1301	130157	4	ET	26014	Line (SIP)	62196756103	
20180914	0949	094902	3	TE	26014	Line (SIP)	56204	
20180914	0949	094936	3	ET	26014	Line (SIP)	62196756103	
20180917	1041	104114	4	TE	26005	Line (SIP)	56104	
20180917	1041	104118	3	TE	26021	Line (SIP)	56104	
20180917	1040	104054	4	TE	26005	Line (SIP)	56104	
20180917	1040	104058	25	TE	26109	Line (SIP)	56104	
20180917	1040	104040	5	TE	26005	Line (SIP)	56103	
20180917	1040	104045	40	TE	26114	Line (SIP)	56103	
20180917	1040	104024	5	TE	26005	Line (SIP)	56204	
20180917	1040	104029	62	TE	26003	Line (SIP)	56204	
20180917	1041	104136	7	TE	26005	Line (SIP)	56103	
20180917	1041	104154	11	TE	26504	Line (SIP)	56103	
20180917	1042	104205	2	TE	26109	Line (SIP)	56103	
20180917	1043	104307	0	ET	26003	Line LREF 870a6129 915139656103		

Shadow

Entity RSI [0001] Admin

Close Call Detail Cradle to Grave Custom Report Builder Report and Task Scheduler Personnel Management Database Maintenance Dashboard Help Log Out

Navigation Menu

- Reports
 - Public Reports
 - Saved Reports
 - Report Favorites
 - Standard Reports
 - Call Center Reports
 - Custom Reports
 - Custom Report Builder
- Quick Views
- Dashboard

Call Detail Dashboard Cradle To Grave

Cradle to Grave

Calls

Expand All Collapse All Refresh Most Recent Calls Filter

Call Details	Extension	Number	Start Time	Duration
Internal	Pri_H323 26014 (26014) >> Exp_H323 26114 (26114)	26114	2018/09/17 10:43:29	00:00:04
Internal	Pri_H323 26014 (26014) >> Pri_H323 26003 (26003)	26003	2018/09/17 10:43:15	00:00:06
Outgoing	Pri_H323 26003 (26003)	915139656103	2018/09/17 10:43:07	00:00:00
Incoming	SaleExp (26504) >> 26109 (26109)	56103 (H323 56103)	2018/09/17 10:41:54	00:00:13
Incoming	Finance (26005)	56103 (H323 56103)	2018/09/17 10:41:36	00:00:07
Incoming	Finance (26005) >> Pri_SIP 26021 (26021)	56104 (OneOfFour)	2018/09/17 10:41:14	00:00:07
Incoming	Finance (26005) >> 26109 (26109)	56104 (OneOfFour)	2018/09/17 10:40:54	00:00:29
Incoming	Finance (26005) >> Exp_H323 26114 (26114)	56103 (H323 56103)	2018/09/17 10:40:40	00:00:45
Incoming	Finance (26005) >> Pri_H323 26003 (26003)	56204 (TwoOfFour)	2018/09/17 10:40:24	00:01:07
Outgoing	Pri_H323 26014 (26014)	62196756103	2018/09/14 09:49:36	00:00:03
Incoming	Pri_H323 26014 (26014)	56204 (TwoOfFour)	2018/09/14 09:49:02	00:00:03
Outgoing	Pri_H323 26014 (26014)	62196756103	2018/09/11 13:01:57	00:00:04
Incoming	Pri_H323 26014 (26014)	56103 (H323 56103)	2018/09/11 13:01:32	00:00:05
Incoming	Pri_H323 26014 (26014)	56103 (H323 56103)	2018/09/11 12:52:30	00:00:05
Incoming	Pri_H323 26014 (26014)	56103 (H323 56103)	2018/09/11 12:52:16	00:00:09
Outgoing	Pri_H323 26014 (26014)	62196756103	2018/09/11 12:49:50	00:00:04
Outgoing	Pri_H323 26014 (26014)	62196756103	2018/09/11 12:49:10	00:00:03
Outgoing	Pri_H323 26014 (26014)	62196756103	2018/09/11 12:47:49	00:00:05
Outgoing	Pri_H323 26014 (26014)	62196756103	2018/09/11 12:22:34	00:00:14

Shadow

Entity RSI [0001] Admin

Close Call Detail Cradle to Grave Custom Report Builder Report and Task Scheduler Personnel Management Database Maintenance Dashboard Help Log Out

Navigation Menu

- Reports
 - Public Reports
 - Saved Reports
 - Report Favorites
 - Standard Reports
 - Call Center Reports
 - Custom Reports
 - Custom Report Builder
- Quick Views
- Dashboard
- General Configuration
- System Configuration
- System Logs & Details

Call Detail Dashboard Cradle To Grave

Dashboards RealTime

Today - Queue: Percent Handled (Range)

83.33

Real-time - Device Status

All None Extension

Pri_H323 26003

1/1 Queues Logged In

Finance 26005

Real-time - Queue Status

Finance 26005

4/4 Agents 0 Calls Waiting - Longest Waiting

Result	Total	Pct	Avg Wait
Answered	4	80%	00:00:04
Abandoned	1	20%	00:00:07
Voice Mail	0	0%	-
Other	0	0%	-

5 Calls

SaleExp 26504

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 documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com>.

1. *IP Office™ Platform 11.0 Installing and Maintaining the IP Office Application Server*, 15-601011 Issue 13c - (Tuesday, May 22, 2018).
2. *IP Office™ Platform 11.0 Deploying IP Office Basic Edition*, 15-601042 Issue 33g - (Tuesday, May 22, 2018).
3. *Administering Avaya IP Office™ Platform with Manager*, Release 11.0 May 2018.
4. *IP Office™ Platform Description of Devlink3 API Introduced in Release 10.0*, Issue 1.0.

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

1. *Shadow CMS (Web) UserGuide.pdf*

©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.