Avaya Solution & Interoperability Test Lab

Application Notes for Resource Software International Shadow Real-Time Dashboard 2.3 with Avaya IP Office Server Edition 9.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Resource Software International Shadow Real-Time Dashboard 2.3 to interoperate with Avaya IP Office Server Edition 9.1.

Resource Software International Shadow Real-Time Dashboard is a computer telephony solution that uses the TAPI and DevLink interfaces from Avaya IP Office to provide real-time monitoring of groups and agent activities.

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 Resource Software International Shadow Real-Time Dashboard servers used the TAPI and DevLink interfaces from the local Avaya IP Office system to monitor groups and users on the local system.

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 Resource Software International (RSI) Shadow Real-Time Dashboard (RTD) 2.3 to interoperate with Avaya IP Office Server Edition 9.1.

RSI Shadow RTD is a computer telephony solution that uses the TAPI 2 in third party mode and the DevLink interfaces from Avaya IP Office to provide real-time monitoring of groups and agent activities.

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 (SCN) trunks. In the compliance testing, two RSI Shadow RTD servers used the TAPI and DevLink interfaces from the local Avaya IP Office system to monitor groups and users on the local system.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon startup of the Shadow RTD application, the application automatically obtained a list of groups and users from the local IP Office system.

For the manual part of the testing, calls were placed manually to groups and agents. Shadow RTD used TAPI and DevLink event messages to monitor group and agent activities, and provided real-time status via a web interface. Manual call control from the agent telephones were exercised where applicable to verify updated status reporting for user actions such as answer and drop.

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

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Shadow RTD:

- Proper handling of real-time TAPI and DevLink event messages.

- Proper handling of call scenarios involving log in, log out, inbound, outbound, internal, external, group, personal, answer, drop, hold/reconnect, do not disturb, park/unpark, agent call forwarding, group call forwarding, queuing, abandoned call, voicemail, multiple calls, multiple agents, transfer, and conference.

- Proper handling of cross systems scenarios involving distributed hunt groups, PSTN, hot desking, transfer, conference, internal, call park, forwarding, follow me, overflow, fallback, and resiliency.

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 Shadow RTD to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Shadow RTD server.

2.2. Test Results

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

- When an agent unparked a call via the short code, the Device Status widget left behind an outstanding entry, which can only be cleared by restarting the application. The workaround is to unpark the call using the Call Park toggle button.

- The Agents on External Calls widget only reflected an agent call immediately after answered by agent. Any further call flow such as transfer and conference was ignored by design with the associated agent call entry removed from the widget.

- The Device Status widget showed an extra entry for conference scenarios when the conference-from agent used hot desking. The extra entry did end appropriately upon conclusion of the conference.

- By design, an internal call between an agent on primary and an agent on expansion was reflected on the Agents on External Calls widget for both Shadow RTD servers.

- A hunt group call that an expansion agent received via the primary PSTN was reported as a tandem hunt group call by the primary Shadow RTD server, and as a non-hunt group call by the expansion Shadow RTD server.

- A hunt group call that a primary agent receives via the expansion PSTN is reported as a regular hunt group call by the primary Shadow RTD server, and as a tandem non-hunt group call by the expansion Shadow RTD server.

- A distributed hunt group call that an expansion agent received via the expansion PSTN was reported as a tandem hunt group call by the primary RTD server, and as a tandem non-hunt group call by the expansion Shadow RTD server.

- When remote hot desking was used by an agent, the reporting of distributed hunt group calls answered by the agent differed in terms of regular hunt group versus tandem hunt group, and the agent call was not reflected in the Agents on External Calls widget.

2.3. Support

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

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

3. Reference Configuration

The IP Office Server Edition configuration used in compliance testing consisted of a primary Linux server at the Main site, and an expansion IP500V2 at the Remote site, with SCN trunks connectivity between the two systems. Each IP Office system has connectivity to the PSTN, for testing cross systems PSTN scenarios.

The detailed administration of IP Office resources is not the focus of these Application Notes and will not be described. As shown in **Figure 1** below, each site has a Shadow RTD server monitoring group and user activities from the local IP Office system. For calls that traverse multiple IP Office systems in a distributed hunt group configuration, the following results can be expected:

- All relevant real-time and historical hunt group statistics can be observed on the Shadow RTD server connected to the IP Office system configured with the specific hunt group.

- Extension device status can be observed on the Shadow RTD server connected to the IP Office system configured with the specific extension.

- For a distributed hunt group call where the answering party and the hunt group are configured on different systems, the historical hunt group widgets will indicate the call was handled by a tandem system.

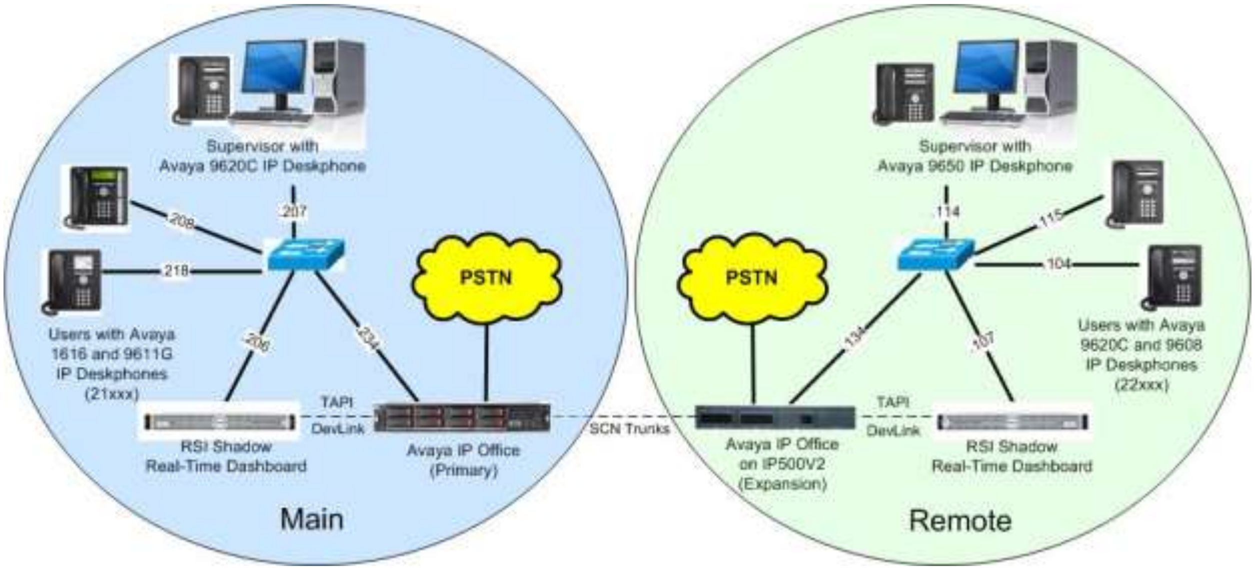


Figure 1: Compliance Testing Configuration

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)	9.1.400.137
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.6029
Avaya 9620C IP Deskphone (H.323)	3.230A
RSI Shadow Real-Time Dashboard on Windows 7 Enterprise • Avaya IP Office TAPI2 Driver (tspi2w_64.tsp) • Avaya DevLink (devlink.dll)	2.3.0.0 SP1 1.0.0.42 1.0.0.5
Remote Site	
Avaya IP Office on IP500 V2 (Expansion)	9.1.400.137
Avaya 9608 IP Deskphone (H.323)	6.6029
Avaya 9620C IP Deskphone (H.323)	3.230A
Avaya 9650 IP Deskphone (H.323)	3.230A
RSI Shadow Real-Time Dashboard on Windows 7 Enterprise • Avaya IP Office TAPI2 Driver (tspi2w_64.tsp) • Avaya DevLink (devlink.dll)	2.3.0.0 SP1 1.0.0.42 1.0.0.5

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 in all configurations.

5. Configure Avaya IP Office

This section provides the procedures for configuring an IP Office system. The procedures include the following area:

- Verify license

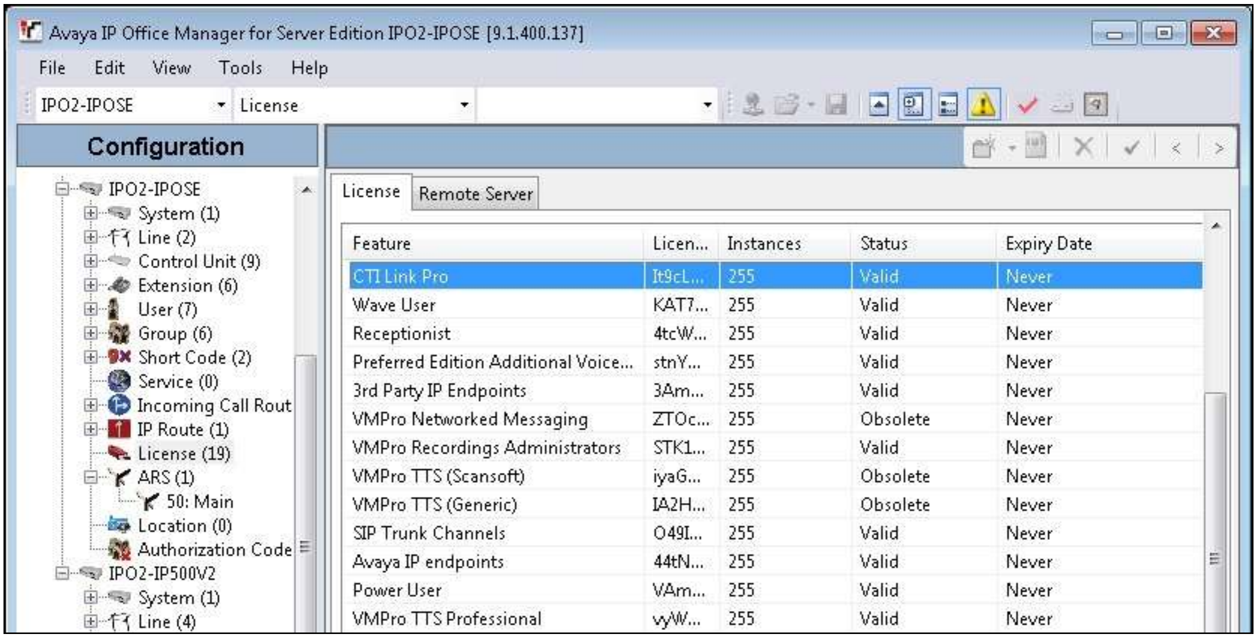
The screenshot in this section was captured from the primary IP Office on the Main site. The same procedure needs to be repeated for the expansion IP Office on the Remote site.

5.1. Verify License

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

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

The **Avaya IP Office Manager** screen is displayed. From the configuration tree in the left pane, select **License** under the applicable IP Office system to display a list of licenses in the right pane. Verify that there is a license for **CTI Link Pro** and that the **Status** is "Valid", as shown below.



Feature	Licen...	Instances	Status	Expiry Date
CTI Link Pro	It9cL...	255	Valid	Never
Wave User	KAT7...	255	Valid	Never
Receptionist	4tcW...	255	Valid	Never
Preferred Edition Additional Voice...	stnY...	255	Valid	Never
3rd Party IP Endpoints	3Am...	255	Valid	Never
VMPro Networked Messaging	ZTOc...	255	Obsolete	Never
VMPro Recordings Administrators	STK1...	255	Valid	Never
VMPro TTS (Scansoft)	iyaG...	255	Obsolete	Never
VMPro TTS (Generic)	IA2H...	255	Obsolete	Never
SIP Trunk Channels	O49I...	255	Valid	Never
Avaya IP endpoints	44tN...	255	Valid	Never
Power User	VAm...	255	Valid	Never
VMPro TTS Professional	vyW...	255	Valid	Never

6. Configure RSI Shadow Real-Time Dashboard

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

- Administer TAPI driver
- Administer console

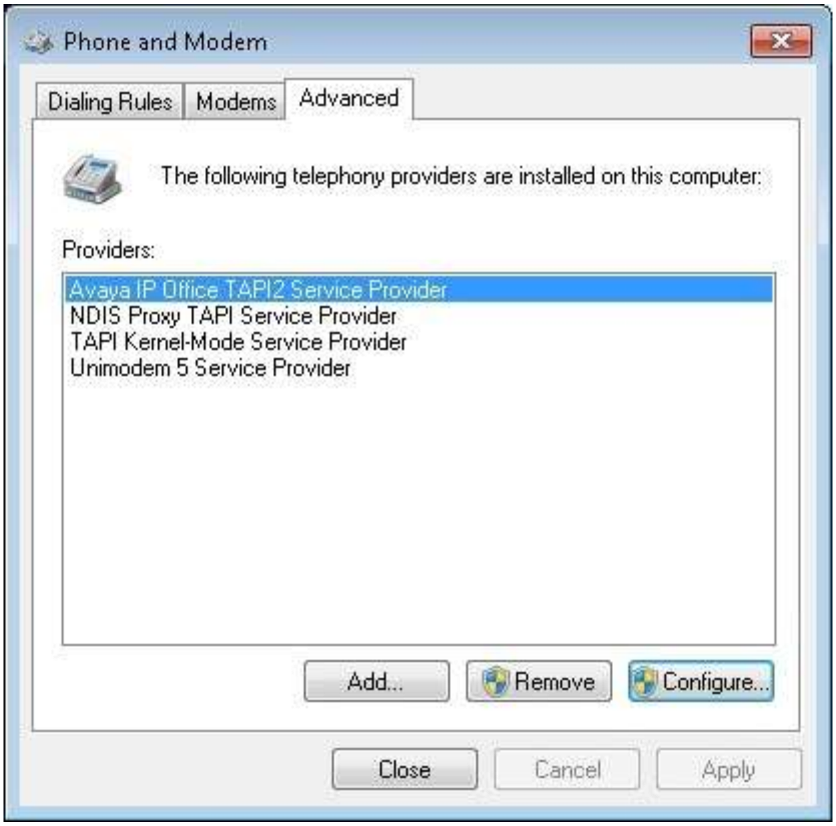
The configuration of Shadow RTD is typically performed by RSI Support Services. The procedural steps are presented in these Application Notes for informational purposes.

The screenshots in this section were captured from the Shadow RTD server connected to the primary IP Office on the Main site. The same procedures need to be repeated for the Shadow RTD server connected to the expansion IP Office on the Remote site.

6.1. Administer TAPI Driver

From the Shadow RTD server, select **Start → Control Panel → Phone and Modem**, to display the **Phone and Modem** screen below.

Select the **Advanced** tab, followed by **Avaya IP Office TAPI2 Service Provider**, and click **Configure**.



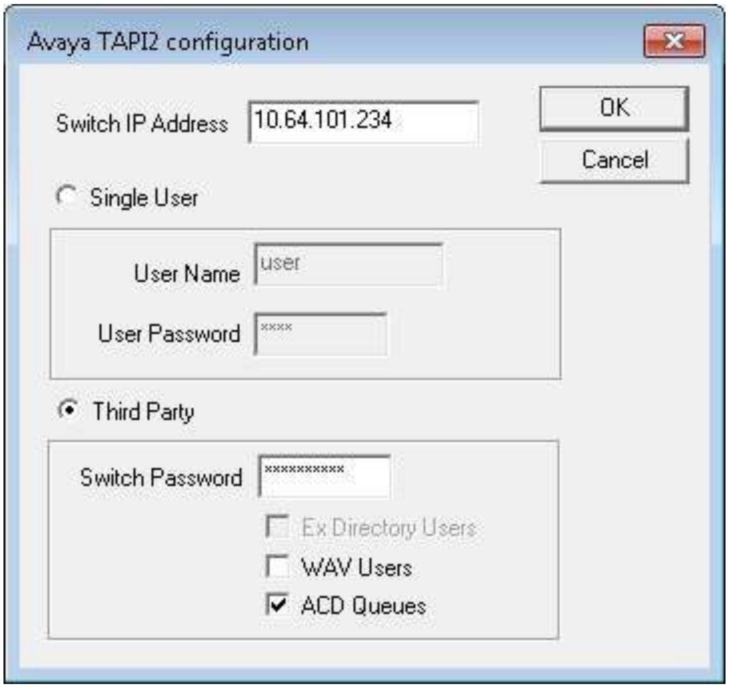
Phone and Modem

The following telephony providers are installed on this computer:

Providers:

Avaya IP Office TAPI2 Service Provider
NDIS Proxy TAPI Service Provider
TAPI Kernel-Mode Service Provider
Unimodem 5 Service Provider

The **Avaya TAPI2 configuration** screen is displayed**.** For **Switch IP Address**, enter the IP address of the local IP Office system. Select the radio button for **Third Party**, enter the local IP Office password for **Switch Password**, and check **ACD Queues**. Reboot the Shadow RTD server.



Avaya TAPI2 configuration

Switch IP Address: 10.64.101.234

○ Single User

User Name: user

User Password: ****

● Third Party

Switch Password: ***********

□ Ex Directory Users

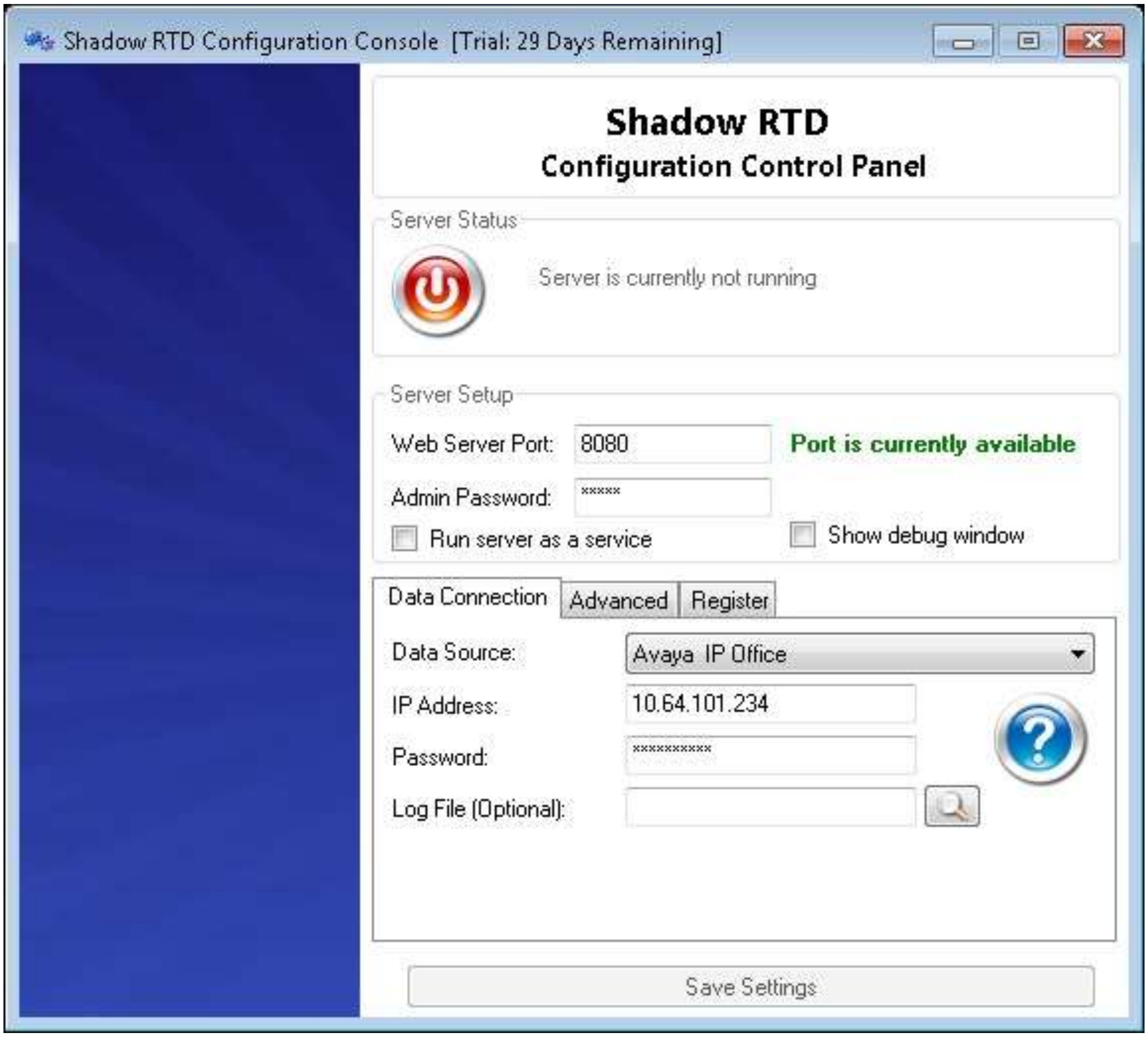
□ WAV Users

☑ ACD Queues

6.2. Administer Console

Select **Start → All Programs → RSI → Shadow RTD → Shadow RTD Console** to display the screen below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Web Server Port:** “8080”
- **Admin Password:** The Shadow RTD administrator credential.
- **Data Source:** “Avaya IP Office”
- **IP Address:** The IP address of the local IP Office system.
- **Password:** The pertinent credential for the local IP Office system.



Shadow RTD Configuration Console [Trial: 29 Days Remaining]

Shadow RTD
Configuration Control Panel

Server Status

Server is currently not running

Server Setup

Web Server Port: 8080 Port is currently available

Admin Password: *****

☐ Run server as a service ☐ Show debug window

Data Source: Avaya IP Office

IP Address: 10.64.101.234

Password: ***********

Log File (Optional):

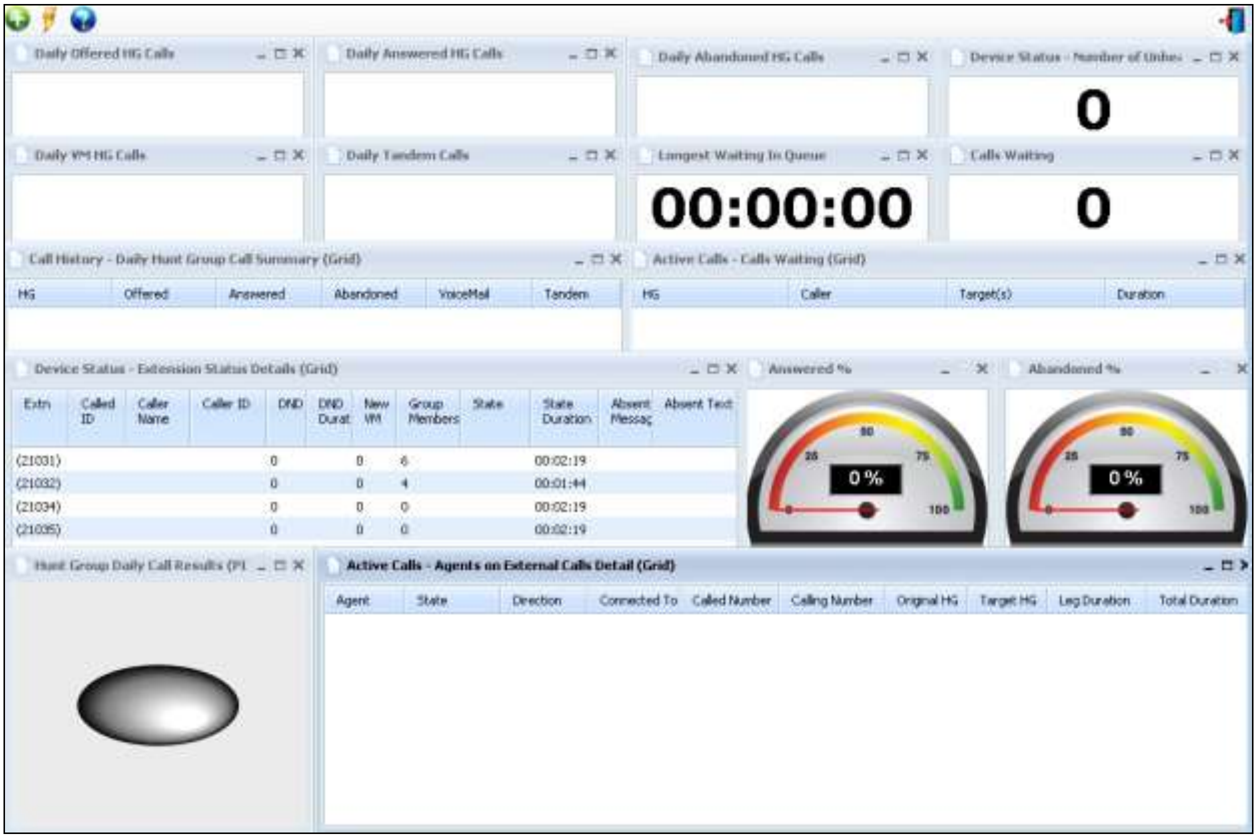
7. Verification Steps

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

7.1. Verify Main Site

Access the Shadow RTD web interface by using the URL "http://ip-address:port" in an Internet browser window, where "ip-address" is the IP address of the Shadow RTD server in the Main site, and "port" is the relevant web server port from **Section 6.2**. The **Login** screen is displayed (not shown). Log in using the appropriate credentials.

In the next screen, all configured widgets will be stacked up against the upper left corner. Rearrange the widgets as desired. In the compliance testing, all applicable widgets were enabled and used, as shown below.



Daily Offered HG Calls

Daily Answered HG Calls

Daily Abandoned HG Calls

Device Status - Number of Unbe

0

Daily VM HG Calls

Daily Tandem Calls

Longest Waiting In Queue

00:00:00

Calls Waiting

0

Call History - Daily Hunt Group Call Summary (Grid)

HG	Offered	Answered	Abandoned	VoiceMail	Tandem

Active Calls - Calls Waiting (Grid)

HG	Caller	Target(s)	Duration

Device Status - Extension Status Details (Grid)

Extn	Called ID	Caller Name	Caller ID	DND	DND Durat	New VM	Group Members	State	State Duration	Absent Messag	Absent Text
(21031)				0		0	6		00:02:19		
(21032)				0		0	4		00:01:44		
(21034)				0		0	0		00:02:19		
(21035)				0		0	0		00:02:19		

Answered %

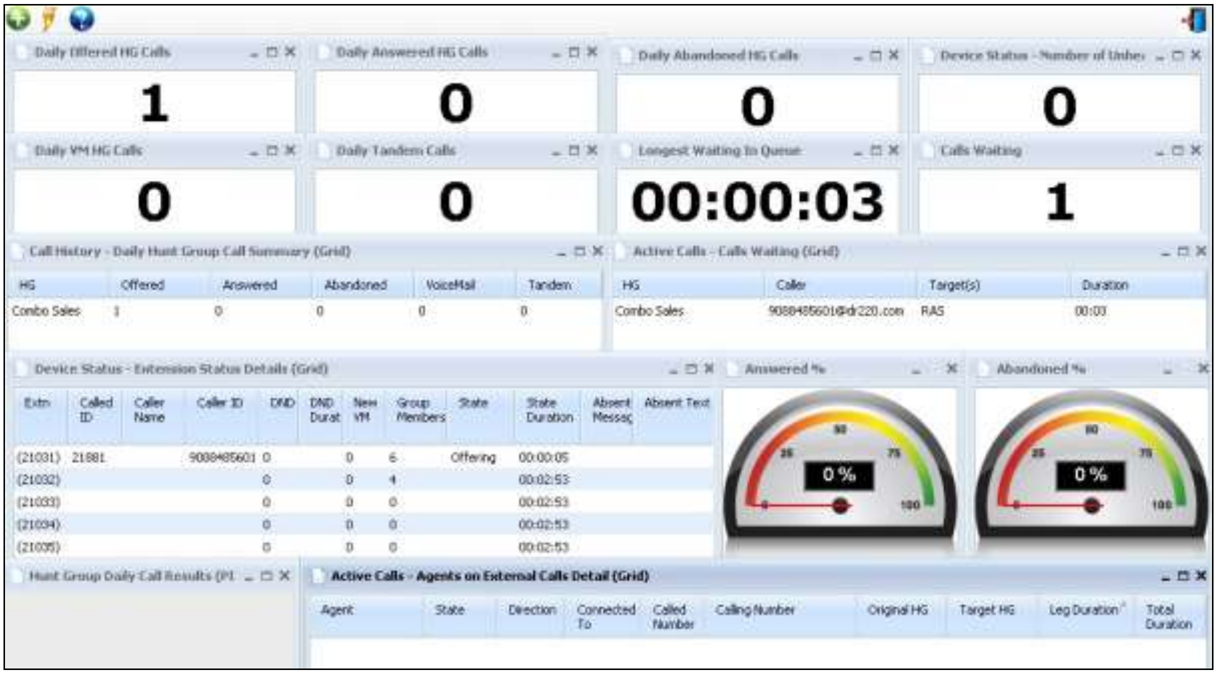
Abandoned %

Hunt Group Daily Call Results (Pi

Active Calls - Agents on External Calls Detail (Grid)

Agent	State	Direction	Connected To	Called Number	Calling Number	Original HG	Target HG	Leg Duration	Total Duration

Place a call from the PSTN to a distributed hunt group with answering agent on the Main site. Verify that the relevant widgets are updated appropriately.



Daily Offered HG Calls: 1
Daily Answered HG Calls: 0
Daily Abandoned HG Calls: 0
Device Status - Number of Unhe: 0
Daily VM HG Calls: 0
Daily Tandem Calls: 0
Longest Waiting In Queue: 00:00:03
Calls Waiting: 1

Call History - Daily Hunt Group Call Summary (Grid)

HG	Offered	Answered	Abandoned	VoiceMail	Tandem
Combo Sales	1	0	0	0	0

Active Calls - Calls Waiting (Grid)

HG	Caller	Target(s)	Duration
Combo Sales	9088485601@dr220.com	RAS	00:03

Device Status - Extension Status Details (Grid)

Extn	Called ID	Caller Name	Caller ID	DND	DND Durat	New VM	Group Members	State	State Duration	Absent Messag	Absent Text
(21031)	21881		9088485601	0		0	6	Offering	00:00:05		
(21032)				0		0	4		00:02:53		
(21033)				0		0	0		00:02:53		
(21034)				0		0	0		00:02:53		
(21035)				0		0	0		00:02:53		

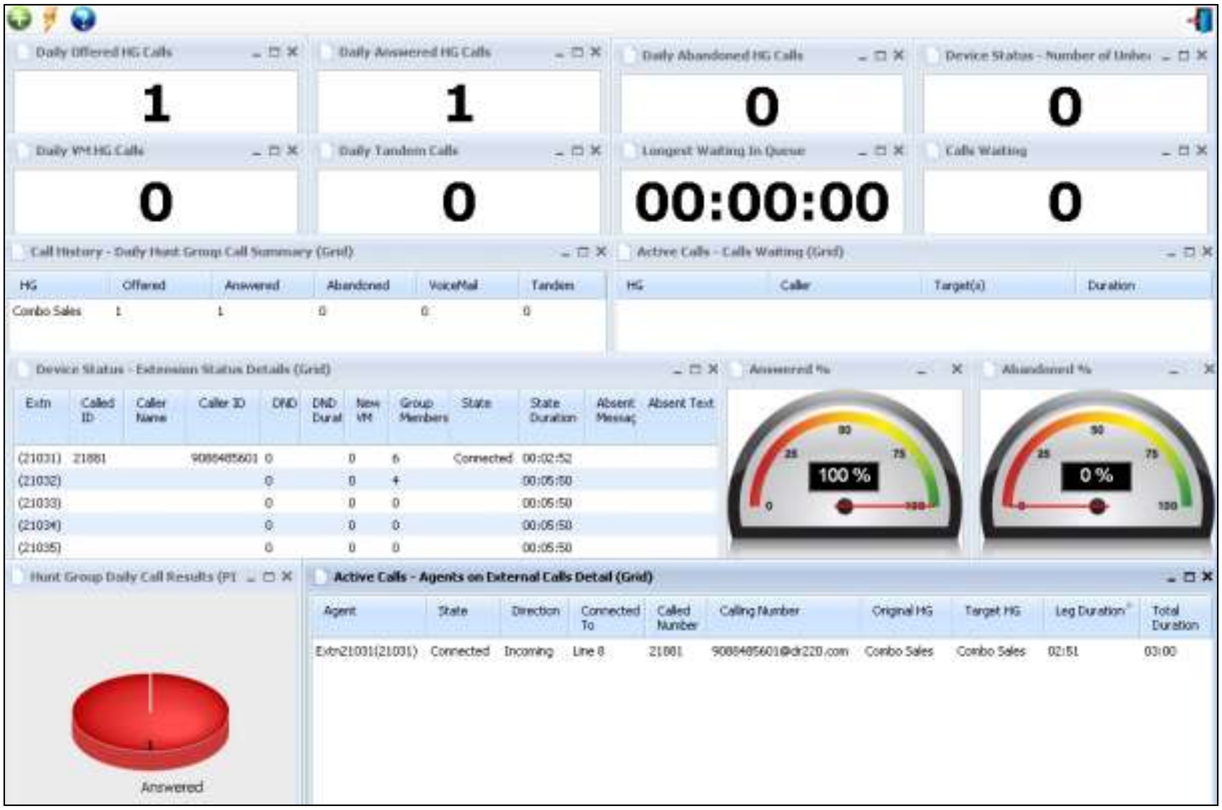
Answered %: 0 %
Abandoned %: 0 %

Hunt Group Daily Call Results (PI

Active Calls - Agents on External Calls Detail (Grid)

Agent	State	Direction	Connected To	Called Number	Calling Number	Original HG	Target HG	Leg Duration	Total Duration

Answer the call at the agent, and verify that the relevant widgets are updated appropriately.



Daily Offered HG Calls: 1
Daily Answered HG Calls: 1
Daily Abandoned HG Calls: 0
Device Status - Number of Unhe: 0
Daily VM HG Calls: 0
Daily Tandem Calls: 0
Longest Waiting In Queue: 00:00:00
Calls Waiting: 0

Call History - Daily Hunt Group Call Summary (Grid)

HG	Offered	Answered	Abandoned	VoiceMail	Tandem
Combo Sales	1	1	0	0	0

Active Calls - Calls Waiting (Grid)

HG	Caller	Target(s)	Duration

Device Status - Extension Status Details (Grid)

Extn	Called ID	Caller Name	Caller ID	DND	DND Durat	New VM	Group Members	State	State Duration	Absent Messag	Absent Text
(21031)	21881		9088485601	0		0	6	Connected	00:02:52		
(21032)				0		0	4		00:05:50		
(21033)				0		0	0		00:05:50		
(21034)				0		0	0		00:05:50		
(21035)				0		0	0		00:05:50		

Answered %: 100 %
Abandoned %: 0 %

Hunt Group Daily Call Results (PI

Active Calls - Agents on External Calls Detail (Grid)

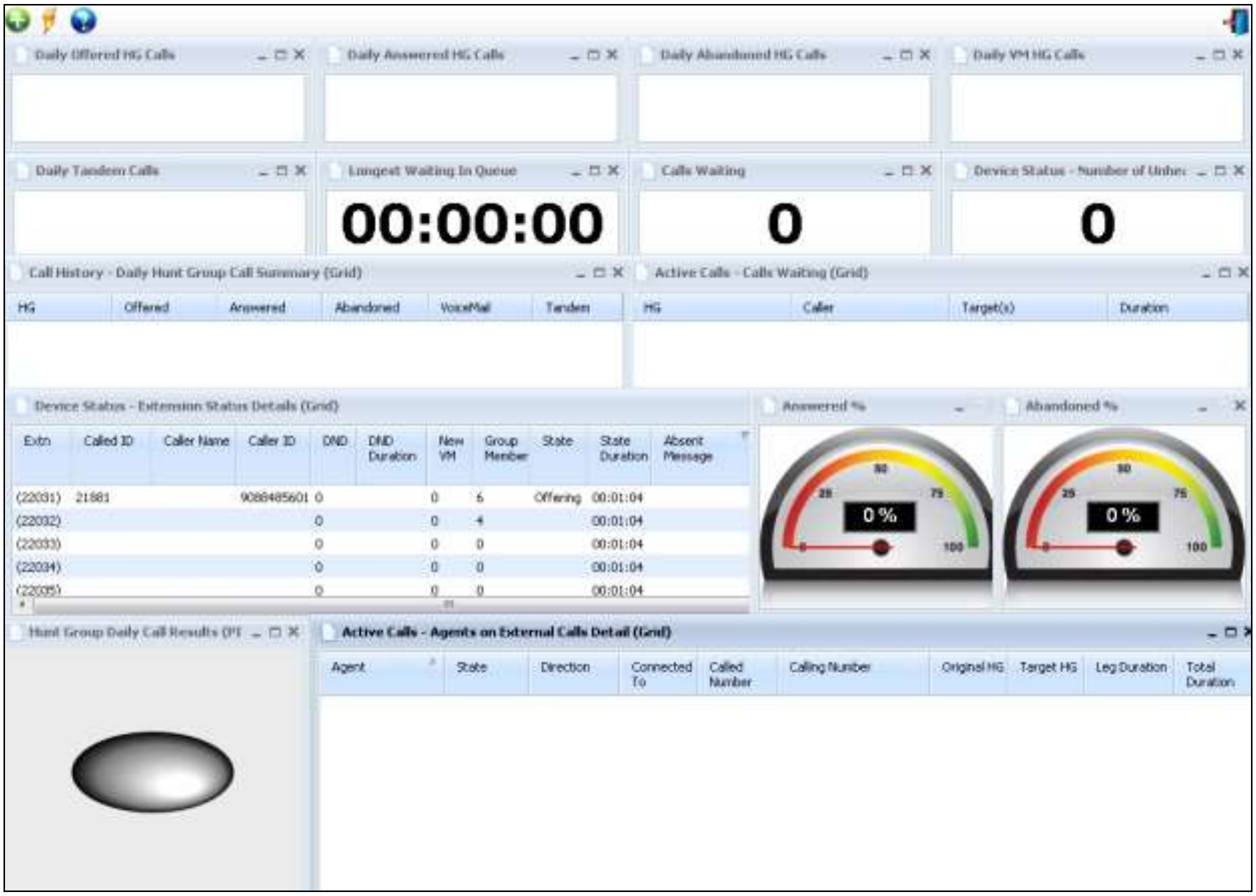
Agent	State	Direction	Connected To	Called Number	Calling Number	Original HG	Target HG	Leg Duration	Total Duration
Extn21031(21031)	Connected	Incoming	Line 8	21881	9088485601@dr220.com	Combo Sales	Combo Sales	02:51	03:00

7.2. Verify Remote Site

Access the Shadow RTD web interface by using the URL “http://ip-address:port” in an Internet browser window, where “ip-address” is the IP address of the Shadow RTD server in the Remote site, and “port” is the relevant web server port from **Section 6.2**. The **Login** screen is displayed (not shown). Log in using the appropriate credentials.

Place a call from the PSTN to a distributed hunt group with answering agent on the Remote site. Verify that the relevant widgets are updated appropriately.

Note that a distributed group call delivered to an agent on the expansion via the PSTN connection at the primary IP office system is reported by the Shadow RTD server at the Remote site as a non-hunt group call. In addition, the Shadow RTD server at the Main site increased the daily offered and tandem counts in the relevant widgets (not shown below).



Call History - Daily Hunt Group Call Summary (Grid)

HG	Offered	Answered	Abandoned	VoiceMail	Tandem

Active Calls - Calls Waiting (Grid)

HG	Caller	Target(s)	Duration

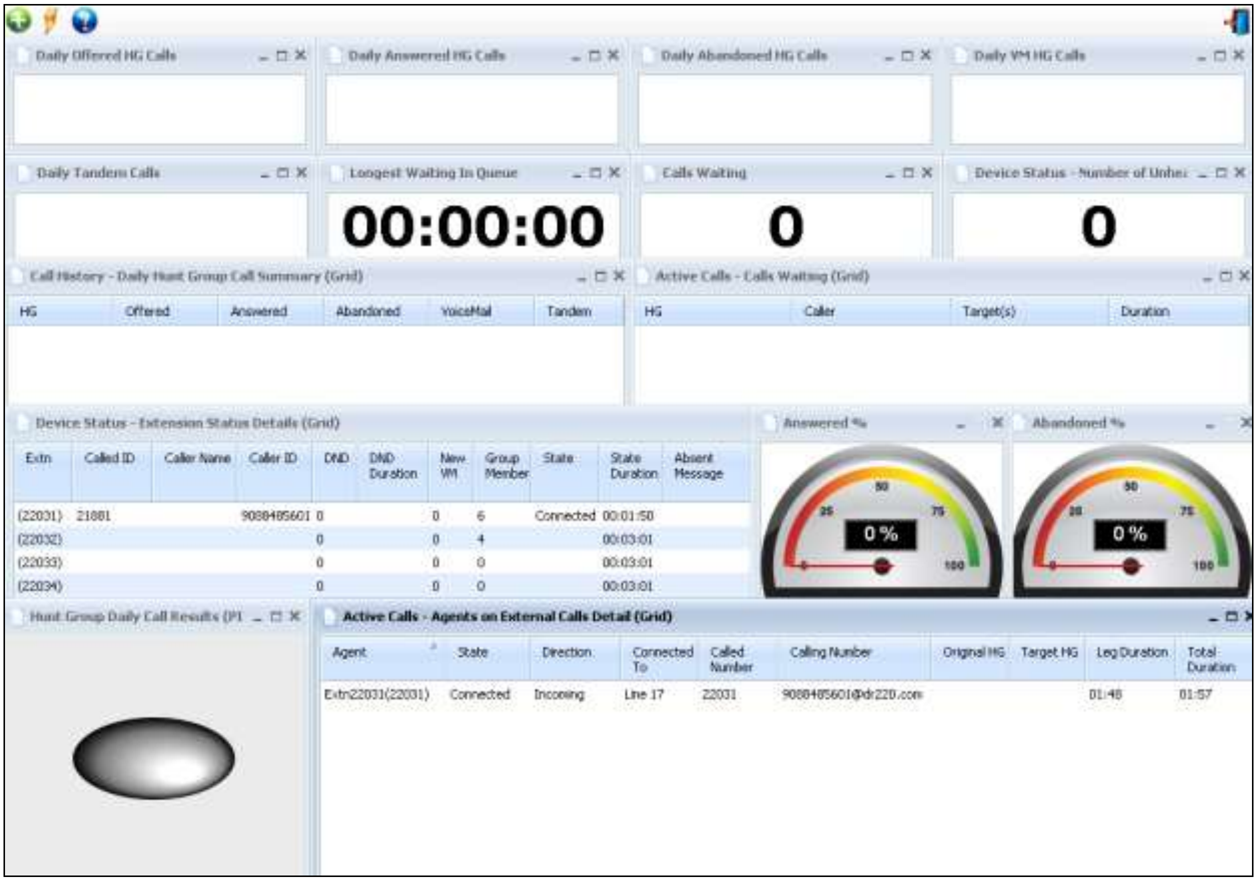
Device Status - Extension Status Details (Grid)

Extn	Called ID	Caller Name	Caller ID	DND	DND Duration	New VM	Group Member	State	State Duration	Absent Message
(22031)	21881		9088485601	0		0	6	Offering	00:01:04	
(22032)				0		0	4		00:01:04	
(22033)				0		0	0		00:01:04	
(22034)				0		0	0		00:01:04	
(22035)				0		0	0		00:01:04	

Active Calls - Agents on External Calls Detail (Grid)

Agent	State	Direction	Connected To	Called Number	Calling Number	Original HG	Target HG	Leg Duration	Total Duration

Answer the call at the agent, and verify that the relevant widgets are updated appropriately.



Daily Offered HG Calls

Daily Answered HG Calls

Daily Abandoned HG Calls

Daily VM HG Calls

Daily Tandem Calls

Longest Waiting In Queue

00:00:00

Calls Waiting

0

Device Status - Number of Unhe:

0

Call History - Daily Hunt Group Call Summary (Grid)

HG	Offered	Answered	Abandoned	VoiceMail	Tandem

Active Calls - Calls Waiting (Grid)

HG	Caller	Target(s)	Duration

Device Status - Extension Status Details (Grid)

Extn	Called ID	Caller Name	Caller ID	DND	DND Duration	New VM	Group Member	State	State Duration	Absent Message
(22031)	21881		9088485601	0		0	6	Connected	00:01:50	
(22032)				0		0	4		00:03:01	
(22033)				0		0	0		00:03:01	
(22034)				0		0	0		00:03:01	

Answered %

0 %

Abandoned %

0 %

Hunt Group Daily Call Results (Pi

Active Calls - Agents on External Calls Detail (Grid)

Agent	State	Direction	Connected To	Called Number	Calling Number	Original HG	Target HG	Leg Duration	Total Duration
Extn22031(22031)	Connected	Incoming	Line 17	22031	9088485601@dr220.com			01:48	01:57

8. Conclusion

These Application Notes describe the configuration steps required for RSI Shadow RTD 2.3 to successfully interoperate with Avaya IP Office Server Edition 9.1. 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 9.1.0, Issue 10.03, February 2015, available at http://support.avaya.com.

2. *Resource Software International Ltd. Shadow Real-Time Dashboard (RTD) Installation & Users Guide*, available from RSI Support.

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.