



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Resource Software International Shadow Real-Time Dashboard 2.4 with Avaya IP Office Server Edition 10 – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for Resource Software International Shadow Real-Time Dashboard 2.4 to interoperate with Avaya IP Office Server Edition 10.

Resource Software International Shadow Real-Time Dashboard is a computer telephony solution that uses DevLink3 interfaces from Avaya IP Office to provide real-time monitoring of groups and agent activities.

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) 2.4 to interoperate with Avaya IP Office Server Edition 10.

RSI Shadow RTD is a computer telephony solution that uses the DevLink3 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 and an expansion IP500V2 that were connected via Small Community Network (SCN) trunks. In the compliance testing, RSI Shadow RTD server used DevLink3 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 IP Office system (primary and expansion) via DevLink3 connection.

For the manual part of the testing, calls were placed manually to groups and agents. Shadow RTD used DevLink3 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and the Shadow RTD did not utilize enabled capabilities of TLS or SRTP and did not include use of any specific encryption features as requested by Shadow RTD.

## **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 DevLink3 event messages.
- Proper handling of call scenarios involving log in, log out, inbound, outbound, internal, external, group, answer, drop, hold/reconnect, do not disturb, park/unpark, agent call forwarding, group call forwarding, queuing, abandoned call, voicemail, multiple calls, multiple agents, and transfer.
- Proper handling of cross systems scenarios involving distributed hunt groups, PSTN, hot desking, transfer, conference, internal, call park, forwarding, overflow, fallback.

The feature testing call flows included calls within the primary IP Office, calls within the expansion IP Office, as well as calls between the primary and expansion.

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.

- Shadow RTD does not 100% accurately display ringing or offering events in some call scenarios involving incoming calls to a distributed group which has agents in the primary and expansion systems, when using DevLink3 API.
- For call transfers and call parks, Shadow RTD will show the first leg and second leg of the call when using DevLink3 API.
- Shadow RTD does not support Blind and Attended Conference when using DevLink3 API.

## 2.3. Support

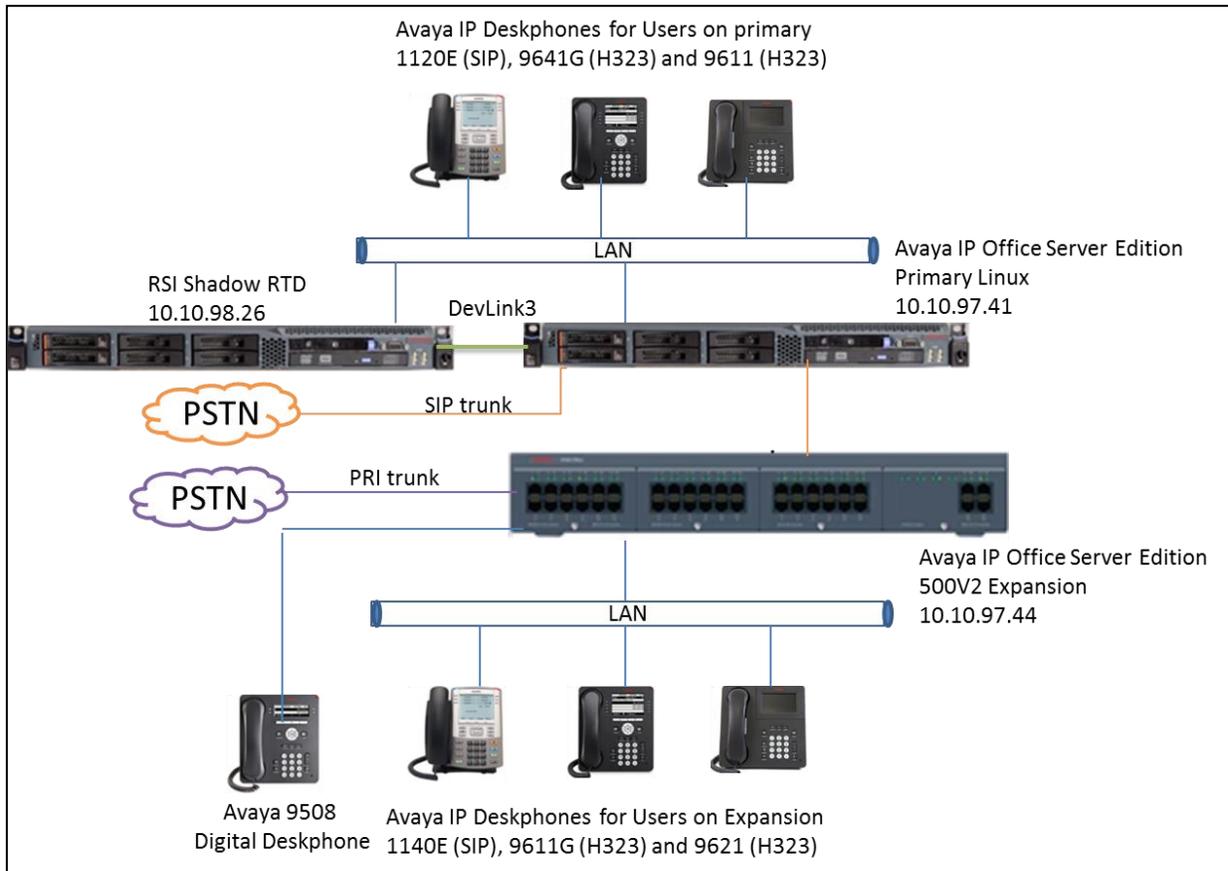
Technical support on Shadow RTD can be obtained through the following:

- **Phone:** (800) 891-6014
- **Email:** [support@telecost.com](mailto:support@telecost.com)
- **Web:** [www.telecost.com](http://www.telecost.com)

### 3. Reference Configuration

The IP Office Server Edition configuration used in compliance testing consisted of a primary Linux and an expansion IP500V2 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, Shadow RTD server monitoring group and user activities from the local IP Office 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
Avaya IP Office Server Edition (Primary)	10 SP3
Avaya 9508 IP Deskphone (H.323)	1.350B
Avaya 9611G, 9641G IP Deskphone (H.323)	6.6401
Avaya 9641G IP Deskphone (H.323)	3.230A
Avaya 1608-I IP Deskphone (H323)	ha1608ua1_390A.bin
Avaya 1120E, 1140E IP Deskphones (SIP)	4.4.23
RSI Shadow Real-Time Dashboard on Windows 2012 R2	2.4 SP1

*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

The document assumes that Avaya IP Office Server Edition has been installed and configured to work with an IP500V2 expansion. This section only describes the details on how to configure the IP Office to work with Shadow RTD application.

- CTI-Pro license.
- Administrative DevLink3.

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.

The screenshot displays the Avaya IP Office Manager for Server Edition application. The interface includes a menu bar (File, Edit, View, Tools, Help) and a toolbar. The main content area is titled 'Server Edition' and shows a 'Summary' for 'Server Edition Primary'. The summary is divided into two sections: 'Hardware Installed' and 'System Settings'. The 'Hardware Installed' section lists: Control Unit: IPO-Linux-PC, Secondary Server: NONE, Expansion Systems: 1 (10.97.44), System Identification: 858b6d69e18abf9f4755e57c276072a18ad0aa40, and Serial Number: ac162db2b1b8. The 'System Settings' section lists: IP Address: 10.97.41, Sub-Net Mask: 255.255.255.240, System Locale: United States (US English), System Location: 2: Belleville Primary, Device ID: 1, and Number of Extensions on System: 25. On the right side, there is an 'Open...' menu with options: Configuration, System Status, Voicemail Administration, Resiliency Administration, On-boarding, IP Office Web Manager, and Help. Below this is an 'Add...' menu with options: Set All Nodes to Select, Set All Nodes License Source, Secondary Server, and Expansion System. At the bottom, there is a table with the following data:

Description	Name	Address	Primary Link	Users Configured	Extensions Configured
Solution				46	63
Primary Server	DevCon IPO Sev1	10.97.41		27	25
Expansion System	DevCon IPOS Exp	10.97.44	Bothway	19	38

## 5.1. CTI Link Pro license

From the configuration tree in the left pane, navigate to **DevCon IPOS Sev1 → License** to display list of valid license. Verify CTI Link Pro license is 2 which means SCN option allowed on networks  $\leq 5$  nodes as shown below.

Feature	Key	Instances	Status	Expiration D
Receptionist	N/A	4	Valid	5/31/2017
Additional Voicemail Pro Ports	N/A	152	Valid	5/31/2017
VMPRO Recordings Administrators	N/A	1	Valid	5/31/2017
Office Worker	N/A	384	Valid	5/31/2017
Avaya Softphone Licence	N/A	100	Valid	5/31/2017
VMPRO TTS Professional	N/A	40	Valid	5/31/2017
Power User	N/A	384	Valid	5/31/2017
Avaya IP endpoints	N/A	384	Valid	5/31/2017
SIP Trunk Channels	N/A	128	Valid	5/31/2017
<b>CTI Link Pro</b>	<b>N/A</b>	<b>2</b>	<b>Valid</b>	<b>5/31/2017</b>
3rd Party IP Endpoints	N/A	384	Valid	5/31/2017
UMS Web Services	N/A	100	Valid	5/31/2017
Avaya Mac Softphone	N/A	100	Valid	5/31/2017
SM Trunk Channels	N/A	128	Valid	5/31/2017

## 5.2. Devlink3 Transport Options

This is configurable by navigating on the IP Office Manager to **File → Advanced Security Settings... → System → DevCon IPO Sev1**.

Availability of the DevLink3service is governed by the IP Office security setting: TAPI / DevLink 3 on the **Unsecured interfaces** tab in System Security as displayed in the below screen.

The screenshot shows the 'Security Settings' window for 'System: DevCon IPO Sev1'. The 'Unsecured Interfaces' tab is active. It displays fields for System Password, Voicemail Password, and Monitor Password, each with a 'Change' button. Below these are 'Application Controls' and 'Application Support' sections.

**Application Controls:**

TFTP Server	<input checked="" type="checkbox"/>	Program Code	<input type="checkbox"/>	TAPI/DevLink3	<input checked="" type="checkbox"/>
TFTP Directory Read	<input type="checkbox"/>	DevLink	<input checked="" type="checkbox"/>	HTTP Directory Read	<input checked="" type="checkbox"/>
TFTP Voicemail	<input checked="" type="checkbox"/>			HTTP Directory Write	<input checked="" type="checkbox"/>

**Application Support:**

Application	Active	Limitations
Legacy Voicemail	✓	
Voicemail Lite	✓	
Upgrade wizard	✗	
TAPI	✓	
one-X Portal Client	✓	
IP Office Directory Services	✓	
DevLink	✓	
IP DECT	#	Cannot view any Directory entries
Network Viewer	✓	

## 5.3. Administer Devlink3.

A combination of username and password is used to authenticate the application.

First, right click on **Right Groups → Add New right group** (not shown), configure a new **Rights Groups** and enable the checkbox **DevLink3** in the **Telephony APIs** tab as displayed below for new Rights Groups **DevLink3**.

The screenshot shows the 'Security Settings' window for 'Rights Group: DevLink3'. The 'Telephony APIs' tab is active. It displays the 'IP Office Service Rights' section with the following options:

- Enhanced TSPI Access
- DevLink3
- Location API

Configure a new Service User with username and password and assign it to the DevLink3 rights group by right click on **Service Users** → **Add New** (not shown), add new service user as show below:

Security Settings	Service Users (8)	Service User: DevLink3																																																																												
<ul style="list-style-type: none"> <li>Security           <ul style="list-style-type: none"> <li>General</li> <li>System (1)</li> <li>Services (7)</li> <li>Rights Groups (14)</li> <li>Service Users (8)</li> </ul> </li> </ul>	<table border="1"> <thead> <tr> <th>Service User Name</th> <th>Account Status</th> <th>Groups</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>Enabled</td> <td>Administrator Gro</td> </tr> <tr> <td>EnhTopaService</td> <td>Enabled</td> <td>TCPA Group;</td> </tr> <tr> <td>IPDECTService</td> <td>Disabled</td> <td>IPDECT Group;</td> </tr> <tr> <td>BranchAdmin</td> <td>Disabled</td> <td></td> </tr> <tr> <td>BusinessPartner</td> <td>Disabled</td> <td>Business Partner</td> </tr> <tr> <td>Maintainer</td> <td>Disabled</td> <td>Maintainer;</td> </tr> <tr> <td>ACCSDData</td> <td>Enabled</td> <td>Business Partner</td> </tr> <tr> <td>DevLink3</td> <td>Enabled</td> <td>DevLink3;</td> </tr> </tbody> </table>	Service User Name	Account Status	Groups	Administrator	Enabled	Administrator Gro	EnhTopaService	Enabled	TCPA Group;	IPDECTService	Disabled	IPDECT Group;	BranchAdmin	Disabled		BusinessPartner	Disabled	Business Partner	Maintainer	Disabled	Maintainer;	ACCSDData	Enabled	Business Partner	DevLink3	Enabled	DevLink3;	<div>Service User Details</div> <div>Name: DevLink3</div> <div>Password: <input type="password"/> <span>Change</span></div> <div>Account Status: Enabled</div> <div>&lt;None&gt;</div> <div> <input checked="" type="checkbox"/> No Account Expiration         <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <div style="text-align: center;">January 2017</div> <table border="1"> <thead> <tr> <th>Sun</th> <th>Mon</th> <th>Tue</th> <th>Wed</th> <th>Thu</th> <th>Fri</th> <th>Sat</th> </tr> </thead> <tbody> <tr> <td>25</td> <td>26</td> <td>27</td> <td>28</td> <td>29</td> <td>30</td> <td>31</td> </tr> <tr> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>7</td> </tr> <tr> <td>8</td> <td>9</td> <td>10</td> <td>11</td> <td>12</td> <td>13</td> <td>14</td> </tr> <tr> <td>15</td> <td>16</td> <td>17</td> <td>18</td> <td>19</td> <td>20</td> <td>21</td> </tr> <tr> <td>22</td> <td>23</td> <td>24</td> <td>25</td> <td>26</td> <td>27</td> <td>28</td> </tr> <tr> <td>29</td> <td>30</td> <td style="background-color: #e0e0e0;">31</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> </tr> </tbody> </table> <div style="text-align: center; margin-top: 5px;"> <input type="text"/> Today: 1/31/2017           </div> </div> </div> <div>Rights Group Membership</div> <ul style="list-style-type: none"> <li><input type="checkbox"/> Backup Admin</li> <li><input type="checkbox"/> Upgrade Admin</li> <li><input type="checkbox"/> System Admin</li> <li><input type="checkbox"/> Maint Admin</li> <li><input type="checkbox"/> Business Partner</li> <li><input type="checkbox"/> Customer Admin</li> <li><input type="checkbox"/> Maintainer</li> <li><input type="checkbox"/> SMGR Admin</li> <li><input checked="" type="checkbox"/> DevLink3</li> </ul>	Sun	Mon	Tue	Wed	Thu	Fri	Sat	25	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	31	1	2	3	4
Service User Name	Account Status	Groups																																																																												
Administrator	Enabled	Administrator Gro																																																																												
EnhTopaService	Enabled	TCPA Group;																																																																												
IPDECTService	Disabled	IPDECT Group;																																																																												
BranchAdmin	Disabled																																																																													
BusinessPartner	Disabled	Business Partner																																																																												
Maintainer	Disabled	Maintainer;																																																																												
ACCSDData	Enabled	Business Partner																																																																												
DevLink3	Enabled	DevLink3;																																																																												
Sun	Mon	Tue	Wed	Thu	Fri	Sat																																																																								
25	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	31	1	2	3	4																																																																								

## 6. Configure RSI Shadow Real-Time Dashboard

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

- 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.

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:** Any free TCP port on the system, example “8888”.
- **Admin Password:** Enter appropriated Shadow RTD administrator password.
- **Data Source:** Select “Avaya IP Office” from the drop down menu.
- **IP Address:** The IP address of the primary IP Office system.
- **Password:** The pertinent password for the DevLink3 account created in Section 5.3
- **Use DevLink3:** This option should be checked
- **DevLink3 UserName:** The pertinent username for the DevLink3 account created in Section 5.3

**Shadow RTD Configuration Console [Trial Expired - Live Connec...**

### Shadow RTD Configuration Control Panel

Server Status

Server is currently not running

Server Setup

Web Server Port:  **Port is currently available**

Admin Password:

Run server as a service  Show debug window

Data Connection **Advanced** Register

Data Source:

IP Address:

Password:

Log File (Optional):

Use DevLink3:

DevLink3 UserName:

**Save Settings**

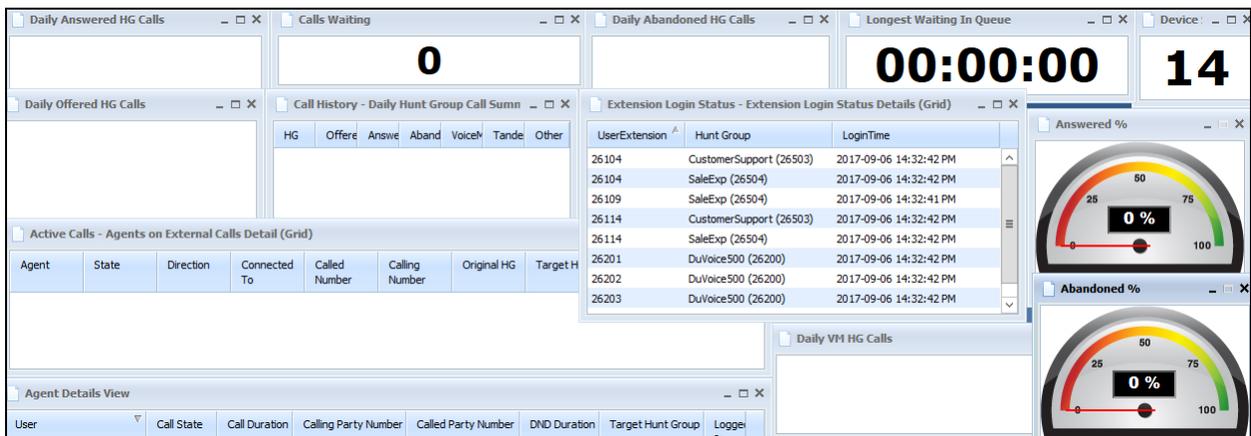
## 7. Verification Steps

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

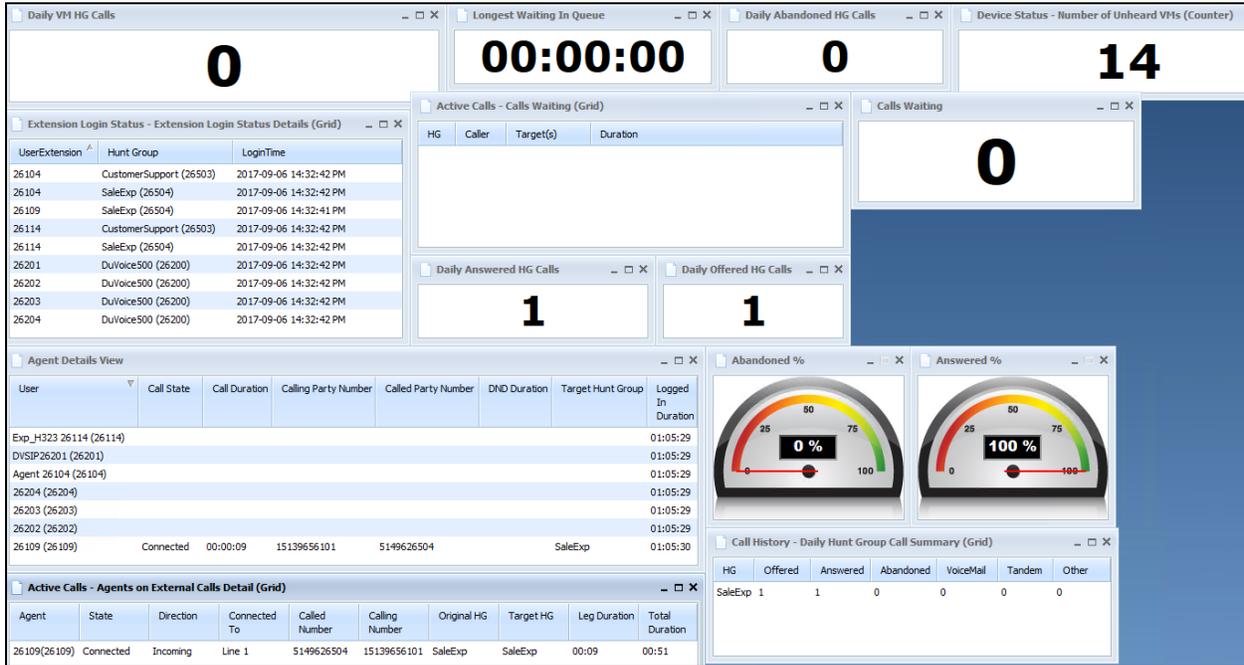
### 7.1. Verify RTD

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 0**. 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.



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.



## 8. Conclusion

These Application Notes describe the configuration steps required for RSI Shadow RTD 2.4 to successfully interoperate with Avaya IP Office Server Edition 10. 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 10, available at <http://support.avaya.com>.
2. *Resource Software International Ltd. Shadow Real-Time Dashboard (RTD) Installation & Users Guide*, available from RSI Support.

---

**©2017 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](mailto:devconnect@avaya.com).