**Avaya Solution & Interoperability Test Lab**

# Application Notes for Resource Software International Shadow CMS Version 5.3.4.2 and Avaya Aura® Communication Manager Release 8.1.3 - Issue 1.1

## Abstract

These Application Notes describe the configuration steps required for Resource Software International (RSI) Shadow CMS Contact Center Reporting (CCR) to interoperate with Avaya Aura® Communication Manager.

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 CMS Contact Center Reporting (CCR) to interoperate with Avaya Aura® Communication Manager.

Resource Software International Shadow CMS Contact Center Reporting software utilizes Avaya Aura® Communication Manager Basic Call Management System (BCMS) data to provide Agent and Queue management reporting.

# 2. General Test Approach and Test Results

The general test approach was to configure the Avaya equipment and verify RSI Shadow CMS CCR interoperability as on a customer site. The interoperability compliance test included both feature and functionality testing.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the RSI Shadow 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 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 systems and the RSI Shadow CMS did not include use of any specific encryption features as requested by RSI.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack,

or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real-time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Avaya Product Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on the RSI Shadow CMS server:

- Monitor and display all hunt groups.
- Monitor and display all VDNs.
- Monitor and display historical agent summary, real-time agent status detail including: Ready, Not ready, After call work, etc.

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

## 2.2. Test Results

All test cases were verified and passed.

## 2.3. Support

For the technical support on the Resource Software International Shadow CMS, contact Resource Software International via phone, email and website below.

- **Phone**: (+1)905-576-4575
- **Email**: rsi@telecost.com
- **Address**: 40 King St. W., Suite 300, Oshawa, Ontario, L1H 14A
- **Website**: www.telecost.comEmail:rsi@telecost.com

# 3. Reference Configuration

**Figure 1** illustrates a sample configuration consisting of Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Media Server running in Virtual Environment. Avaya G450 Media Gateway registers to Communication Manager. The RSI Shadow CMS server was running in Windows 2016 server and connected to Communication Manager via SSH port 5022.

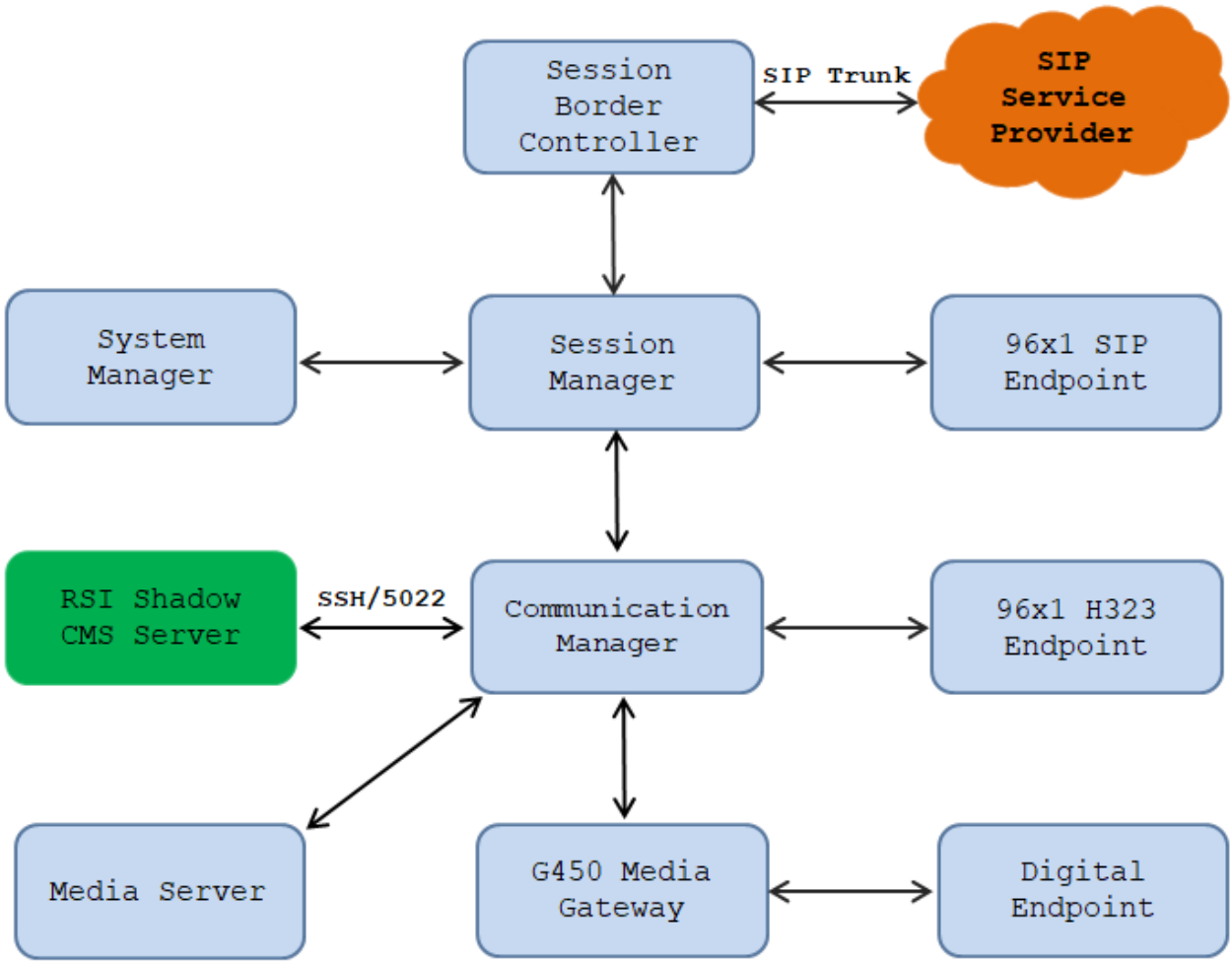



**Figure 1: Test Configuration Diagram**

# 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya Aura® Communication Manager running in a Virtual Environment | Release 8.1.3<br>R018x.01.0.890.0<br>CM 8.1.3.0.0.890.26568 |
| Avaya G450 Media Gateway | 41.20.0 |
| Avaya Aura® Media Server running in a Virtual Environment | 8.0 |
| Avaya Aura® Session Manager running in a Virtual Environment | Release 8.1.3<br>8.1.3.0.813014 |
| Avaya Aura® System Manager running in a Virtual Environment | Release 8.1.3<br>Build No. - 8.1.0.0.733078<br>Software Update Revision No:<br>8.1.3.0.1011784<br>Feature Pack 3 |
| Avaya Session Border Controller for Enterprise | Version 8.1.1.0 |
| Avaya 9611G IP Deskphone (SIP) | Release 7.1.9.0.8 |
| Avaya 9641G IP Deskphone (H.323) | Release 6.8304 |
| Avaya 9408 Digital Deskphone | Release 20 |
| Resource Software International Shadow CMS | Version 5.3.4.2 (64 Bit) |

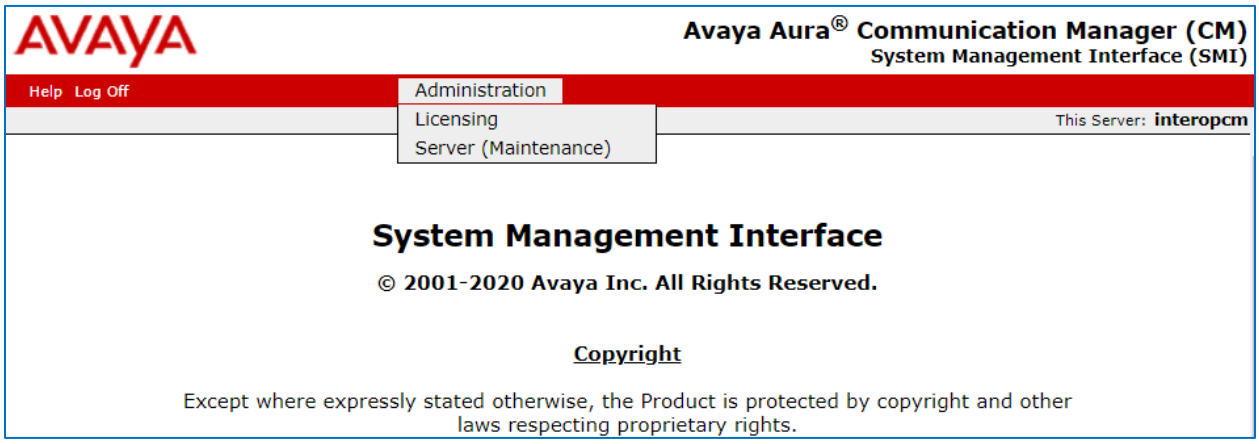
# 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

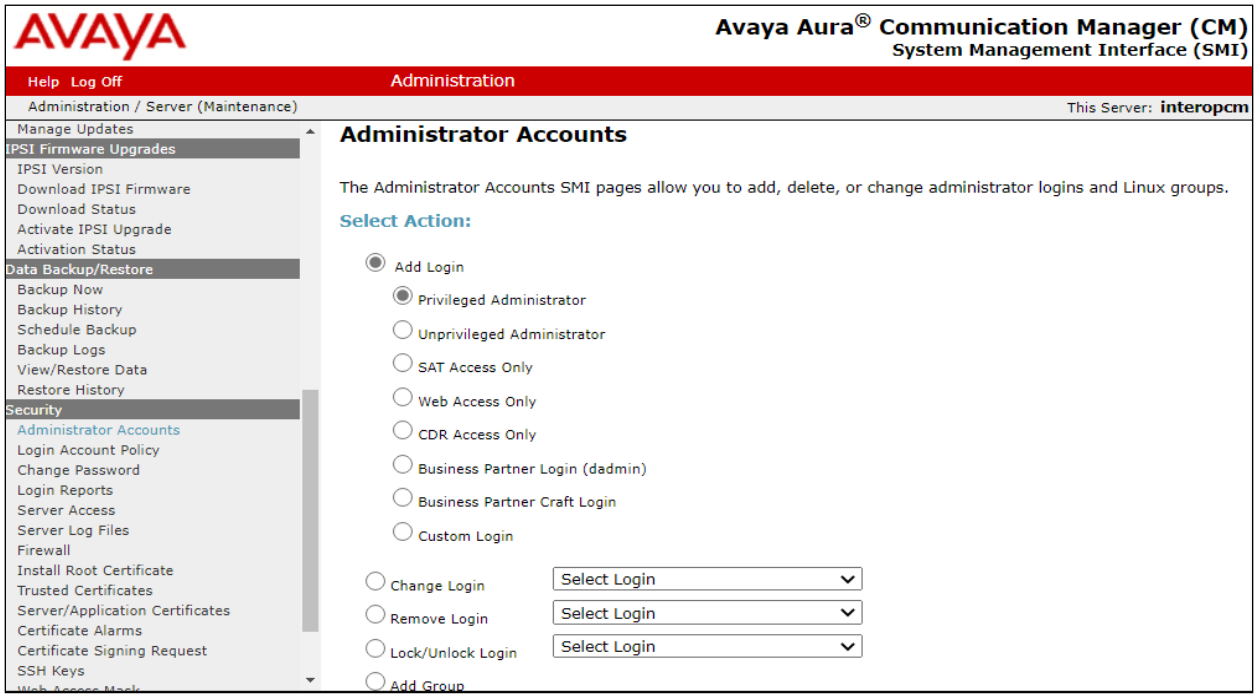
- Configure SAT User
- Configure SAT Access
- Configure System Parameters Features
- Configure Customer Options Parameters Features
- Configure Hunt Group
- Configure Vector
- Administer VDN
- Administer Agent Login ID

## 5.1. Configure SAT User

In order to add a SAT user on Communication Manager System Management Interface (SMI), use a web browser, enter https://<IP address of Communication Manager> to connect to the Communication Manager Server being configured and log in using appropriate credentials (not shown). Select **Administration → Server (Maintenance)**.



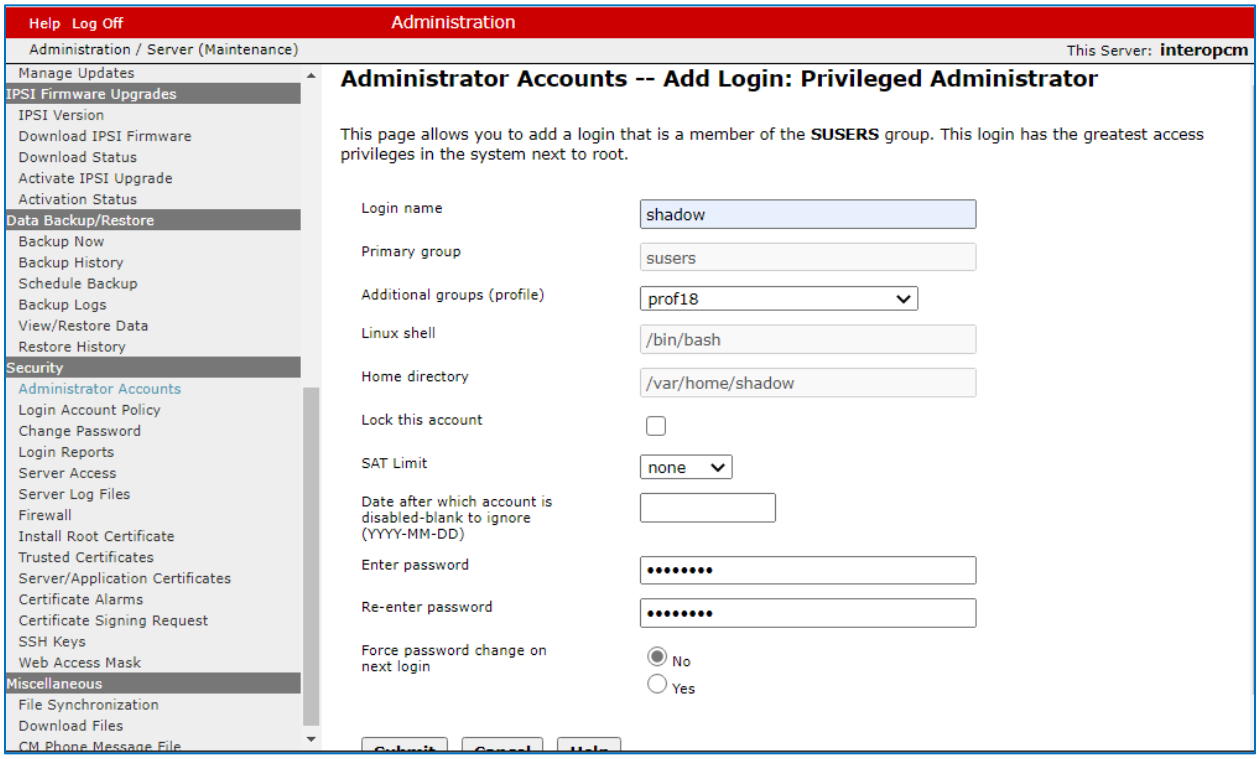

From **Administration** menu, navigates to **Security → Administrator Accounts**. The **Administrator Account** page displays in the right side. Select **Privileged Administrator** radio option under the **Add Login** section and select **Submit** button (not shown).



The **Add Login: Privileged Administrator** page displays, enter the parameters for the following fields.

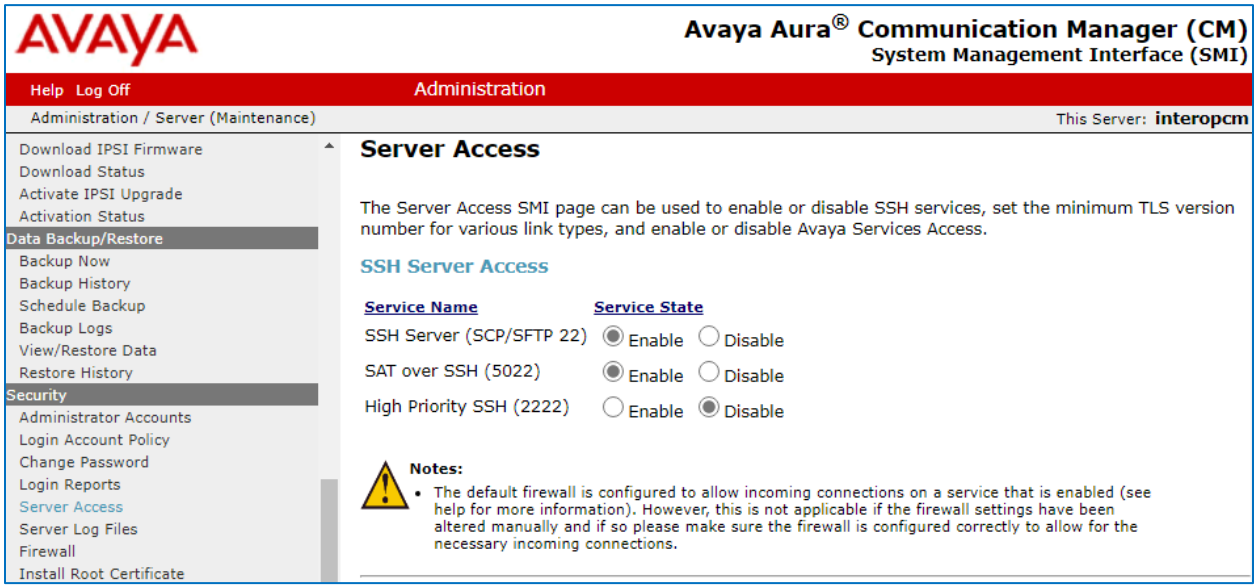
- **Login name**: enter a login name, e.g. shadow.
- **Enter password**: enter a password for the login above.
- **Re-enter password**: re-enter the password above.
- **Force password change on next login**: select "No".

Leave other fields at default and select **Submit** button (not shown) to complete.



## 5.2. Configure SAT Access

In order to enable the SAT access, navigate to **Security → Server Access**. The Server Access page displays in the right side, under **Service Name** select **Enable** in the row **SAT over SSH (5022)** and select **Submit** button to enable.




## 5.3. Configure System Parameter Feature

Use the "change system-parameters features" command to configure the following values for BCMS as highlighted below.

```
change system-parameters features                              Page  12 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
  AGENT AND CALL SELECTION
                          MIA Across Splits or Skills? n
                           ACW Agents Considered Idle? y
                    AUX Agents Considered Idle (MIA)? n
                      AUX Agent Remains in LOA Queue? n
                          Call Selection Measurement: current-wait-time
    Service Level Supervisor Call SelectionOverride? n
                                 Auto Reserve Agents: none
       Block Hang-up by Logged-in Auto-Answer Agents? n
  CALL MANAGEMENT SYSTEM
     REPORTING ADJUNCT RELEASE (determines protocol used by appl link)
                                      CMS (appl mis): R18.1/R19.0
                                   AAPC/IQ (appl ccr):

                                BCMS/VuStats LoginIDs? y
                    BCMS/VuStats Measurement Interval: hour
            BCMS/VuStats Abandon Call Timer (seconds):
                      Validate BCMS/VuStats Login IDs? n
                             Clear VuStats Shift Data: on-login
                  Remove Inactive BCMS/VuStats Agents? n
```

## 5.4. Configure Customer Options Feature

Use the command "display system-parameters customer-options" to verify the ACD, BMCS (Basic) and BCMS/VuStats Service Level are set to "Y", if they are not please contact Avaya sale representative to enable these features in the license.

```
display system-parameters customer-options                    Page   7 of  12
                          CALL CENTER OPTIONAL FEATURES

                           Call Center Release: 8.0

                                 ACD? y                        Reason Codes? y
                       BCMS (Basic)? y                Service Level Maximizer? n
          BCMS/VuStats Service Level? y              Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y      Service Observing (Remote/By FAC)? y
                  Business Advocate? n                Service Observing (VDNs)? y
                    Call Work Codes? y                             Timed ACW? y
       DTMF Feedback Signals For VRU? y                    Vectoring (Basic)? y
                  Dynamic Advocate? n                 Vectoring (Prompting)? y
        Expert Agent Selection (EAS)? y               Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y                Vectoring (3.0 Enhanced)? y
                  Forced ACD Calls? n      Vectoring (ANI/II-Digits Routing)? y
              Least Occupied Agent? y      Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                      Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y       Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                  Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

## 5.5. Configure Hunt Group

Use the command "add hunt-group <ext>" with "ext" is an available hunt group number. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.7**.

```
add hunt-group 1                                              Page   1 of   4
                                   HUNT GROUP

           Group Number: 1                                 ACD? y
             Group Name: Skill-1                         Queue? y
        Group Extension: 3320                           Vector? y
             Group Type: ucd-mia
                     TN: 1
                    COR: 1                       MM Early Answer? n
          Security Code:                   Local Agent Preference? n
 ISDN/SIP Caller Display:

            Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2** of the Hunt Group form, enable the **Skill** option and select "internal" in the **Measured** field.

```
add hunt-group 1                                              Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
                 Measured: internal
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

## 5.6. Configure Vector

Use the command "change vector n" while "n" is the vector number from 1-8000. The example of the vector 1 with the basic scripting is shown below. The vector 1 is used for the configuration of VDN in the next step.

```
change vector 1                                               Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Contact Center
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock?
n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing?
y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    10  secs hearing 1100     then silence
02 queue-to     skill 1    pri m
03 wait-time    5   secs hearing ringback
04 check        skill 1    pri m if expected-wait    < 30
05 announcement 1104
06 queue-to     skill 1    pri m
07 stop
```

## 5.7. Configure VDN

Use the "add vdn <ext>" command to add a VDN number. In the **Destination** field, enter **Vector Number** 1 as configured in **Section 5.6** above, the **Measured** field set to **Internal** and keep other fields at their default values.

```
change vdn 3340                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3340                    Unicode Name? n
                                 Name*: Contact Center 1
                           Destination: Vector Number        1
                    Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: internal Report Adjunct Calls as ACD*? n
        Acceptable Service Level (sec): 20

        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

## 5.8. Configure Agent Login ID

To add an **Agent LoginID**, use the command "add agent-loginID <agent ID>" for each agent. In the compliance test, three agent login IDs 1000, 1001, and 1002 were created.

```
add agent-loginID 1001                                   Page   1 of   3
                                AGENT LOGINID

               Login ID: 1001                 Unicode Name? n   AAS? n
                   Name: Agent 1001                            AUDIX? n
                     TN: 1
                    COR: 1
          Coverage Path:                                LWC Reception: spe
          Security Code: 1234                 LWC Log External Calls? n
          Attribute:                         AUDIX Name for Messaging:

                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                           Password (enter again):
          MWI Served User Type:                            Auto Answer: station
 AUX Agent Remains in LOA Queue: system              MIA Across Skills: system
AUX Agent Considered Idle (MIA): system     ACW Agent Considered Idle: system
            Work Mode on Login: system     Aux Work Reason Code Type: system
```

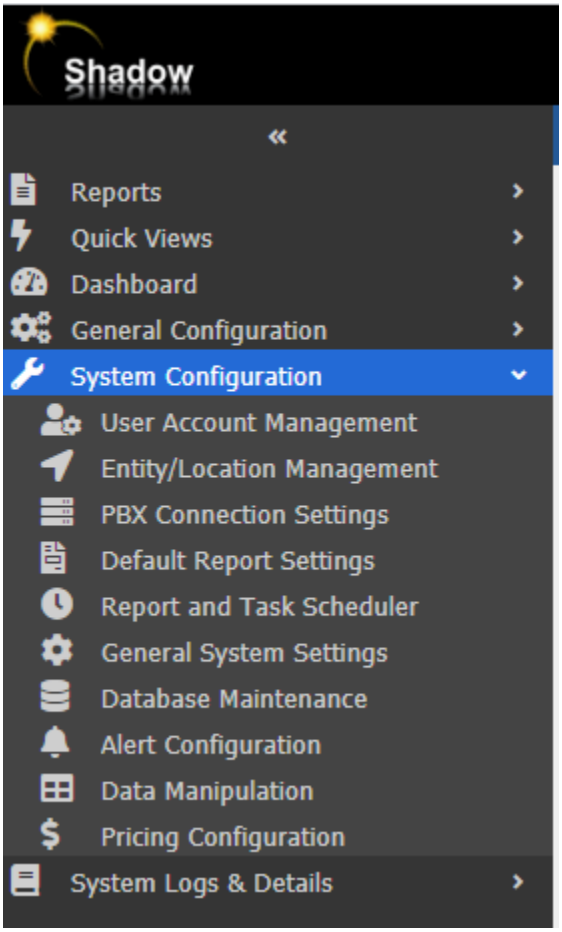
On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

```
add agent-loginID 1001                                    Page   2 of   3
                                  AGENT LOGINID
      Direct Agent Skill:                              Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL          SN   RL SL          SN   RL SL          SN   RL SL
 1: 1       1       16:                31:                46:
 2:                 17:                32:                47:
 3:                 18:                33:                48:
 4:                 19:                34:                49:
 5:                 20:                35:                50:
 6:                 21:                36:                51:
 7:                 22:                37:                52:
 8:                 23:                38:                53:
 9:                 24:                39:                54:
10:                 25:                40:                55:
11:                 26:                41:                56:
12:                 27:                42:                57:
13:                 28:                43:                58:
14:                 29:                44:                59:
15:                 30:                45:                60:
```

# 6. Configure RSI Shadow CMS

This section provides a brief configuration of RSI Shadow CMS server. For more details, please refer to the document reference in **Section 9**.

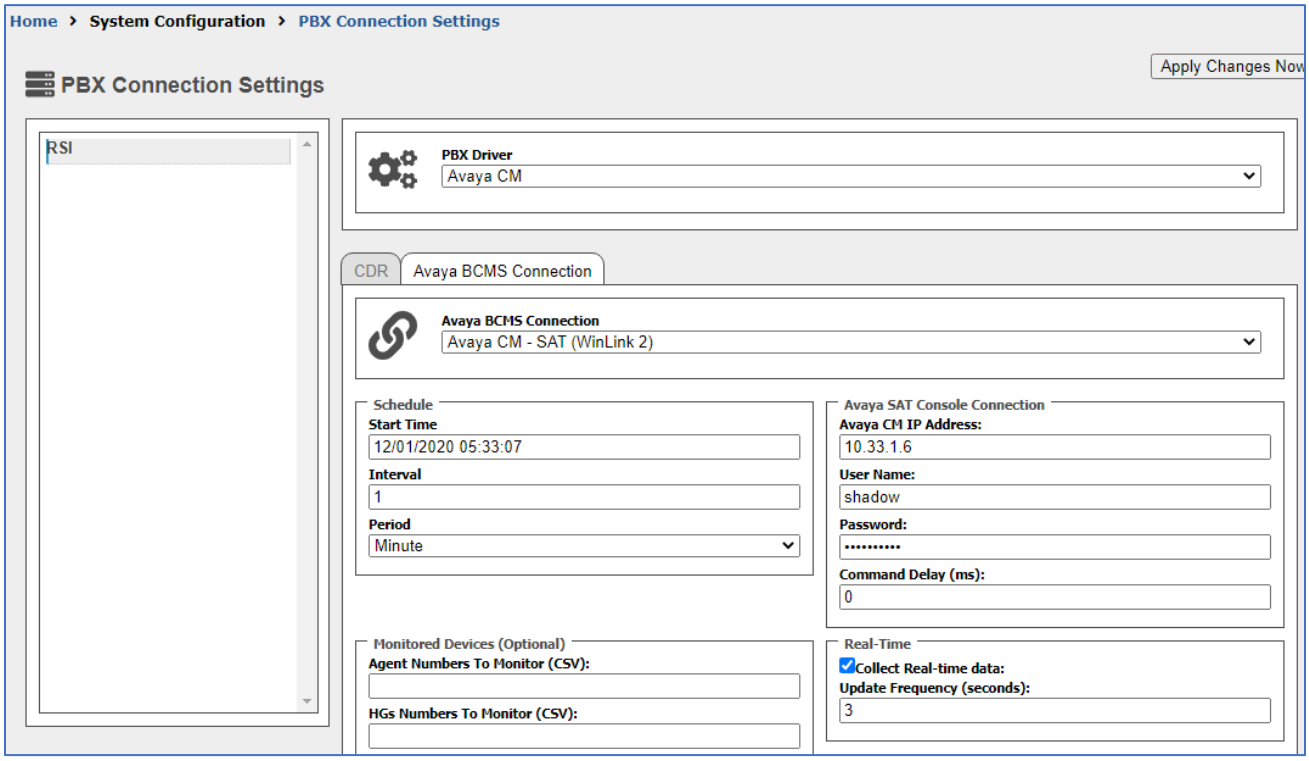
From the Shadow CMS server, start RSI Shadow CMS application and navigate to **System Configuration → PBX Connection Settings**.



The **PBX Connection Settings** displays in the right side, in the **PBX Driver** dropdown menu select “Avaya CM” in the list and select the **Avaya BCMS Connection** tab and provide the following values for the **Avaya BCMS Connection** settings:

- Avaya BCMS Connection = Avaya CM – SAT (Winlink 2).
- Avaya CM IP Address = IP address of Communication Manager.
- User Name = Name of SAT user created in **Section 5.1**.
- Password = Password of SAT user created in **Section 5.1**.

Leave all others values as default. Click Apply Changes Now. RSI Shadow CMS configuration is complete.



# 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and RSI Shadow CMS.

## 7.1. Verify Avaya Aura® Communication Manager

Use the command "**list agent-loginID**" to verify the status of agent.

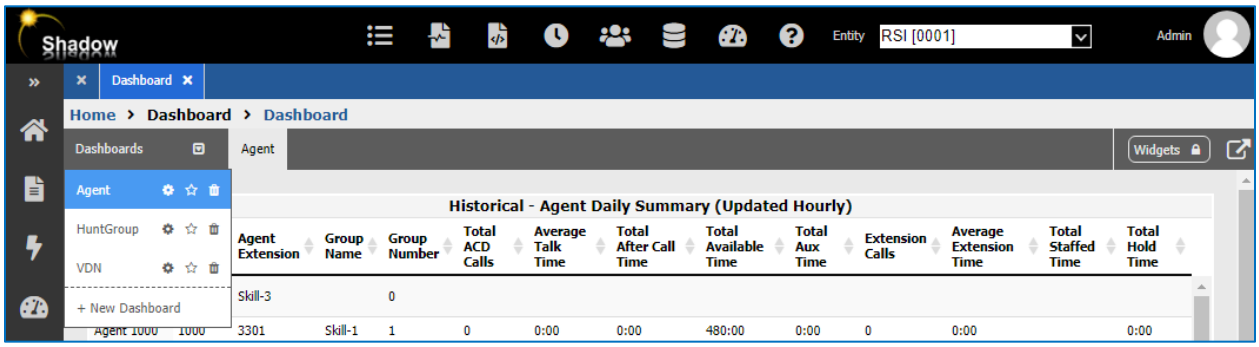
```
list agent-loginID
                                AGENT LOGINID
Login ID         Name             Extension      Dir Agt  AAS/AUD    COR AgPr SO
                Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

1000             Agent 1000      3301                                  1   lvl
                  1/01     /       /       /       /       /       /       /
1001             Agent 1001      3401                                  1   lvl
                  1/01     /       /       /       /       /       /       /
1002             Agent 1002      3403                                  1   lvl
```

Use the command "status logins" to show the list of SAT users currently log in Communication Manager, ther "shadow" user should be in the list.

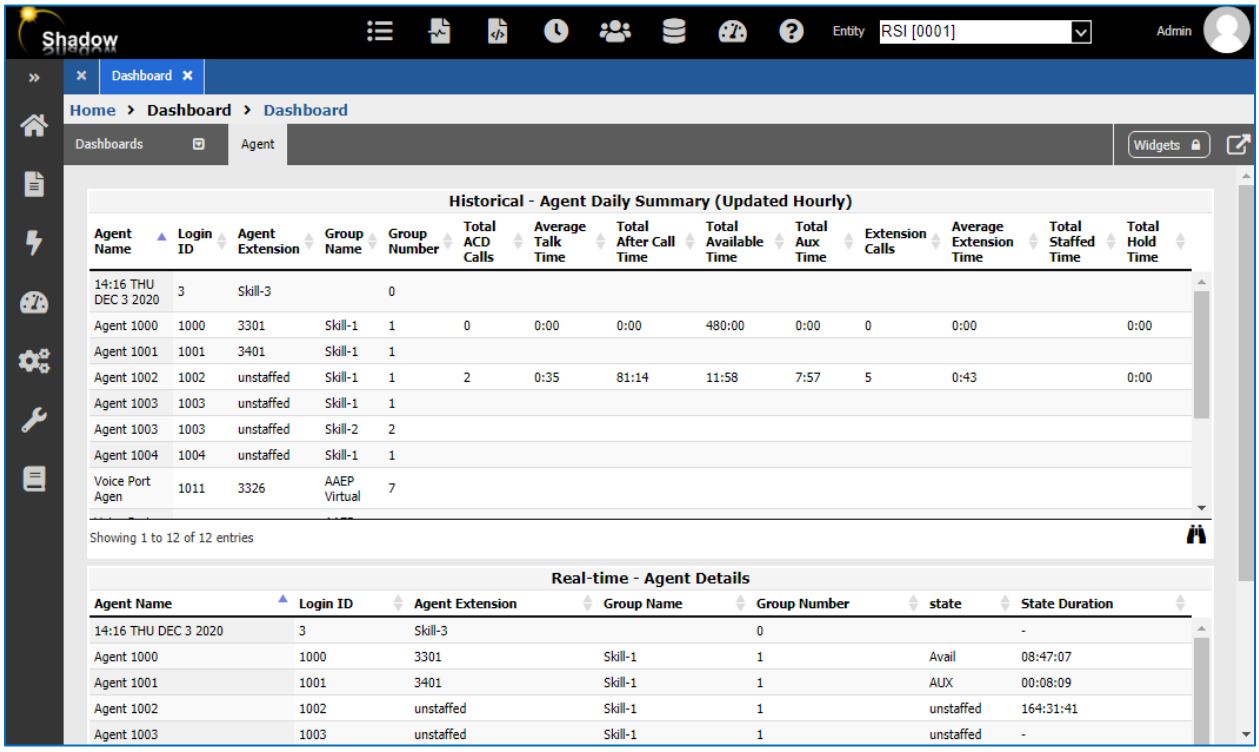
```
status logins

                    COMMUNICATION MANAGER LOGIN INFORMATION

Login      Profile   User's Address       Active Command               Session

 shadow       18                                                          3
                     10.33.100.52
*cust         18                        stat logins                       4
                     10.33.1.200
```

## 7.2. Verify Shadow CMS

Log in to the Shadow CMS web management interface, select **Dashboard** from the left menu (not shown). The **Dashboard** displays in the right side, select **Agent** in the list.




The **Agent** tab displays all configured agents in the Communication Manager and their status in the Real-time – Agent Details section



# 8. Conclusion

These Application Notes describe the configuration steps required for Resource Software International Shadow CMS to successfully interoperate with Avaya Aura® Communication Manager 8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

# 9. Additional References

This section references the product documentation that is relevant to these Application Notes. Documentation for Avaya products may be obtained via http://support.avaya.com


[1] Administering Avaya Aura® Communication Manager, Release 8.1, Document 03-300509, Issue 10, June 2020

[2] RSI Shadow CMS Startup Guide

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.