DevConnect Program

Application Notes for iNEMSOFT CLASSONE iCAS IP Radio Gateway 3.6.1 with Avaya Aura® Session Manager 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for iNEMSOFT CLASSONE iCAS IP Radio Gateway 3.6.1 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the Avaya DevConnect Program.

1. Introduction

These Application Notes contain instructions for iNEMSOFT CLASSONE iCAS (iCAS) IP Radio Gateway with Avaya Aura® Session Manager (Session Manager) to successfully interoperate.

The iCAS solution is a system-of-systems, enabling operators to take control of their communications network and manage multiple transactions from many types of devices.

The iCAS solution enables operators to handle inbound calls, connect with radio dispatch, bridge various radio talk groups and frequencies with each other and with back-office voice systems, collaborate and manage field operations regardless of the type of voice-enabled device, while maintaining the highest level of business continuity and interoperability. iCAS as a solution integrates with several interfaces provided by Avaya products. However, this document only contains instructions for iCAS IP Radio Gateway with Session Manager. iCAS IP Radio Gateway registers to Session Manager as a SIP end point. Application notes related to other interfaces may be obtained via Avaya Support site.

- Application Notes for iNEMSOFT CLASSONE iCAS Dispatch Console with Avaya Aura® Session Manager and Avaya Aura® Communication Manager

2. General Test Approach and Test Results

The feature test cases were performed manually. At startup iCAS IP Radio Gateway registers with Session Manager as two SIP users via a non-encrypted connection.

Incoming VDN calls were placed to iCAS IP Radio Gateway server from internal stations and external callers and outbound calls were placed from iCAS IP Radio Gateway server linking parties using radio devices and end-users on traditional hard and softphones.

The main objectives were to verify the following:

- Registration
- Codecs (G.711MU)
- Inbound PSTN calls
- Internal calls
- Outbound calls
- Call termination (origination/destination)
- Serviceability
- IP Shuffling and Encryption were not tested

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.

For the testing associated with these Application Notes, the interface between Avaya systems and iCAS 6.0 did not include use of any specific encryption features as requested by iNemsoft.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on iCAS IP Radio Gateway. iCAS IP Radio Gateway operations such as inbound calls, outbound and iCAS IP Radio Gateway interactions with Session Manager and Avaya SIP, Avaya H.323 hardphones, and Avaya Agent for Desktop softphones were verified. The serviceability testing introduced failure scenarios to see if iCAS IP Radio Gateway can recover from failures.

2.2. Test Results

The test objectives were verified. For serviceability testing, iCAS IP Radio Gateway operated properly after recovering from failures such as cable disconnects, and resets of iCAS IP Radio Gateway and Session Manager. iCAS IP Radio Gateway successfully negotiated the codec that was used. The features tested worked as expected.

2.3. Support

Technical support on iCAS IP Radio Gateway can be obtained through the following:

- **Phone:** (214) 423-2815
- **Email :** rtisupport@inemsoft.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, iCAS IP Radio Gateway stations associated with the Station IDs shown in the table below.

Device Type	Extension
iCAS IP Radio Gateway Stations	66006, 66007 (SIP)

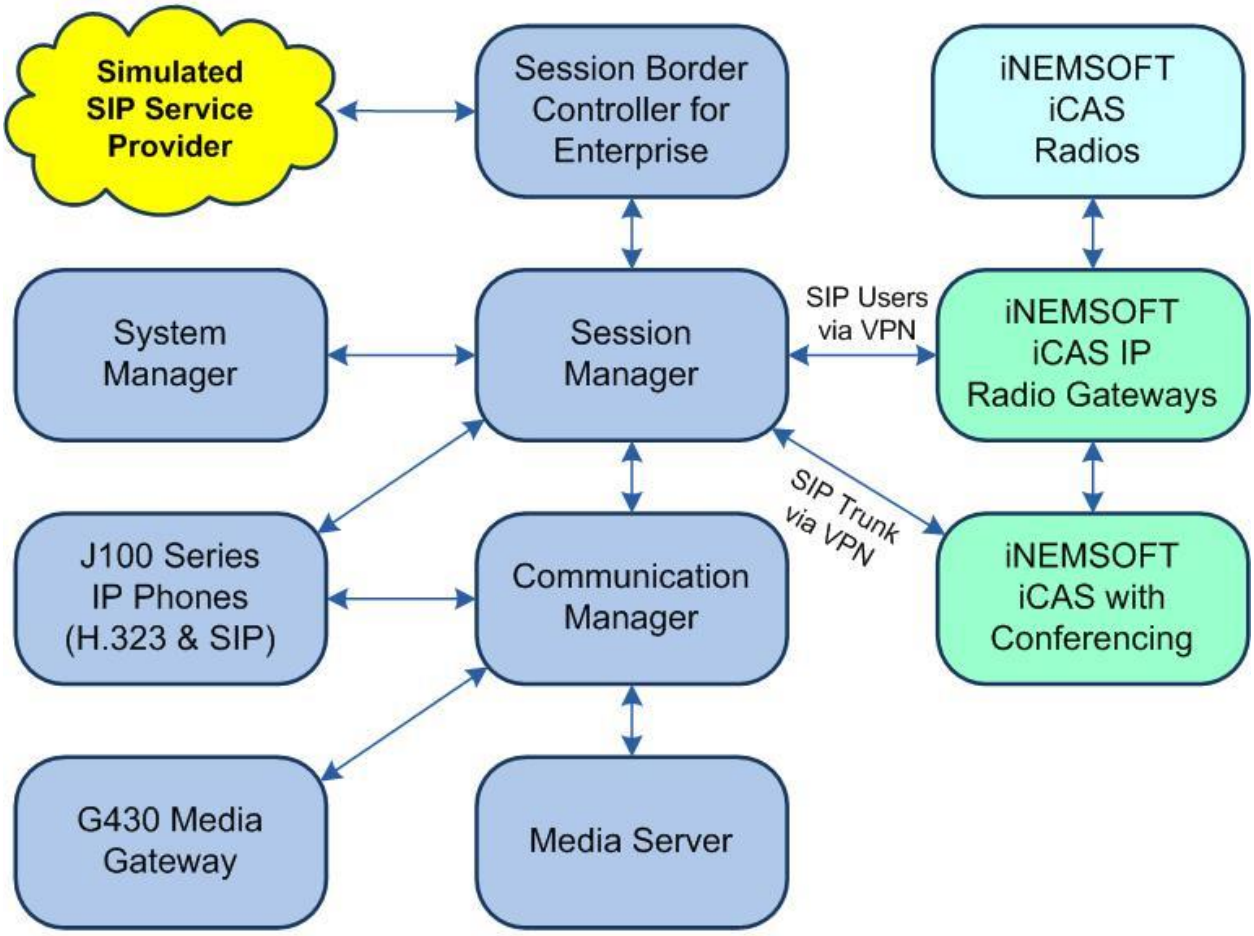


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	10.1.2 (10.1.2.0.0.974.27783)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1 (10.1.0.125)
Avaya Aura® Application Enablement Services in Virtual Environment	10.1.2 (10.1.2.0.0.12-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.2 (10.1.2.0.101.2016)
Avaya Aura® System Manager in Virtual Environment	10.1.2 (10.1.2.0.0715476)
Avaya Session Border Controller for Enterprise in Virtual Environment	10.1 (10.1.0.0-32-21432)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G IP Desk phone (H.323)	6.8.5.3.2
Avaya J169 IP Desk phone (SIP)	4.0.13.0.6
Avaya J179 IP Desk phone (H.323)	6.8.5.3.2
iNEMSOFT CLASSONE iCAS IP Radio Gateway	3.6.1

5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

5.1. Launch System Manager

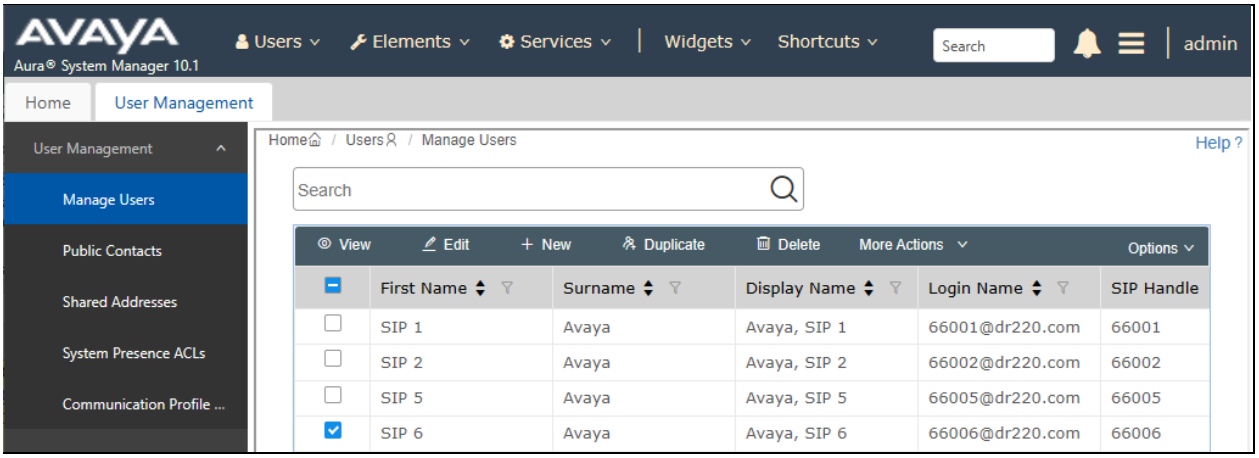
Access the System Manager web interface by using the URL "**https://ip-address**" in an Internet browser window, where "**ip-address**" is the IP address of System Manager. Log in using the appropriate credentials.

5.2. Administer Users

NOTE: To ensure that TSAPI can successfully monitor the SIP Endpoints, this step must be performed on all SIP Endpoints. It is not required for H.323 Endpoints.

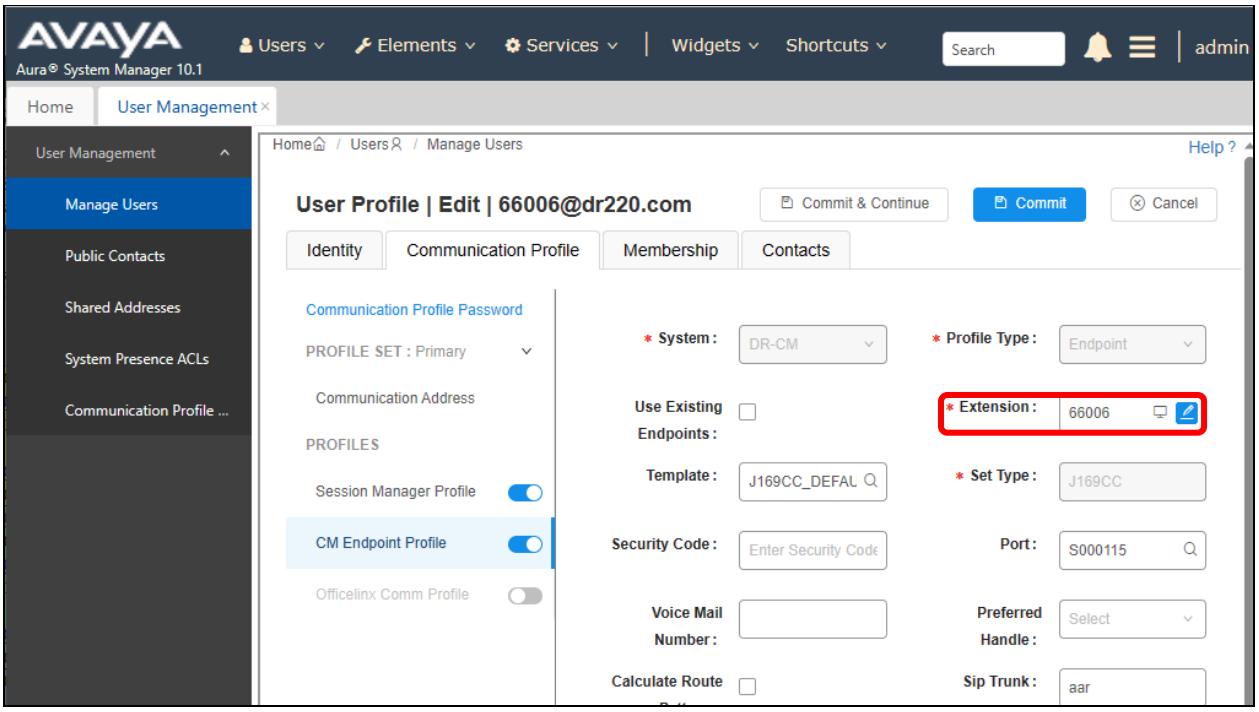
In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section** Error! Reference source not found., in this case "**66006**", and click **Edit**.



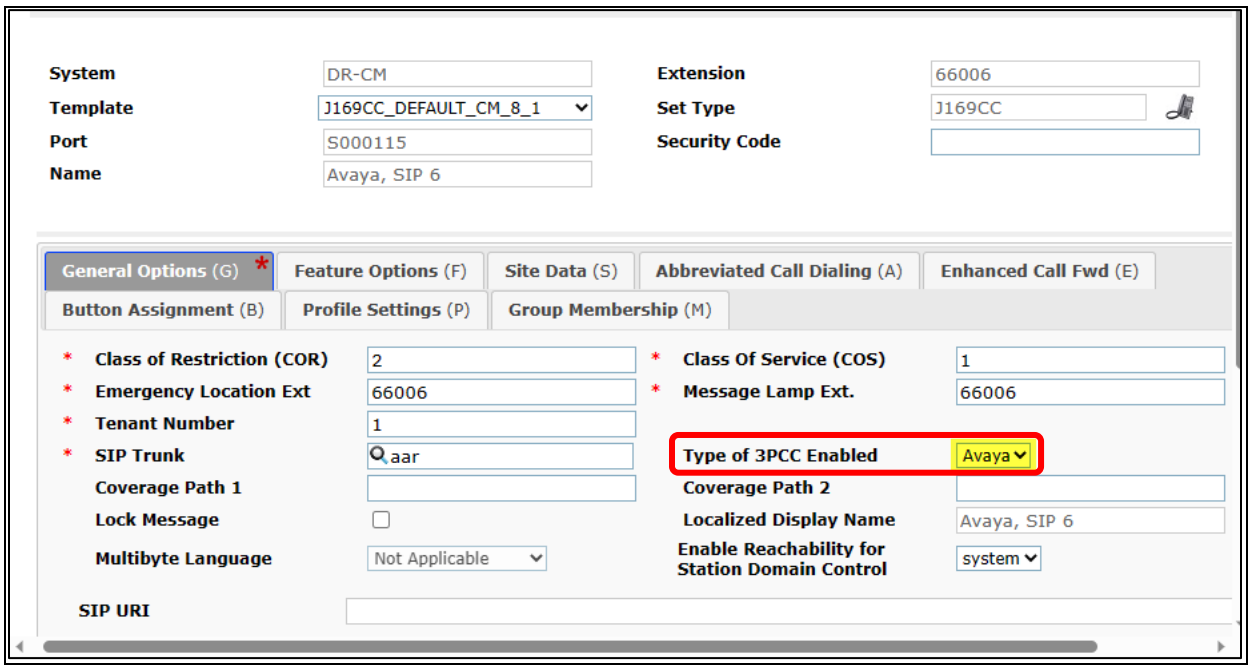
The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.



The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select "**Avaya**" as shown below.

Repeat this section for all SIP agent users from **Section** Error! Reference source not found.. In the compliance testing, one SIP agent extension **66006** was configured.



6. Configure iNEMSOFT ClassOne iCAS IP Radio Gateway

Configuration of iNEMSOFT CLASSONE iCAS IP Radio Gateway is done by designated iNEMSOFT engineers. Therefore, no configuration is provided in this document.

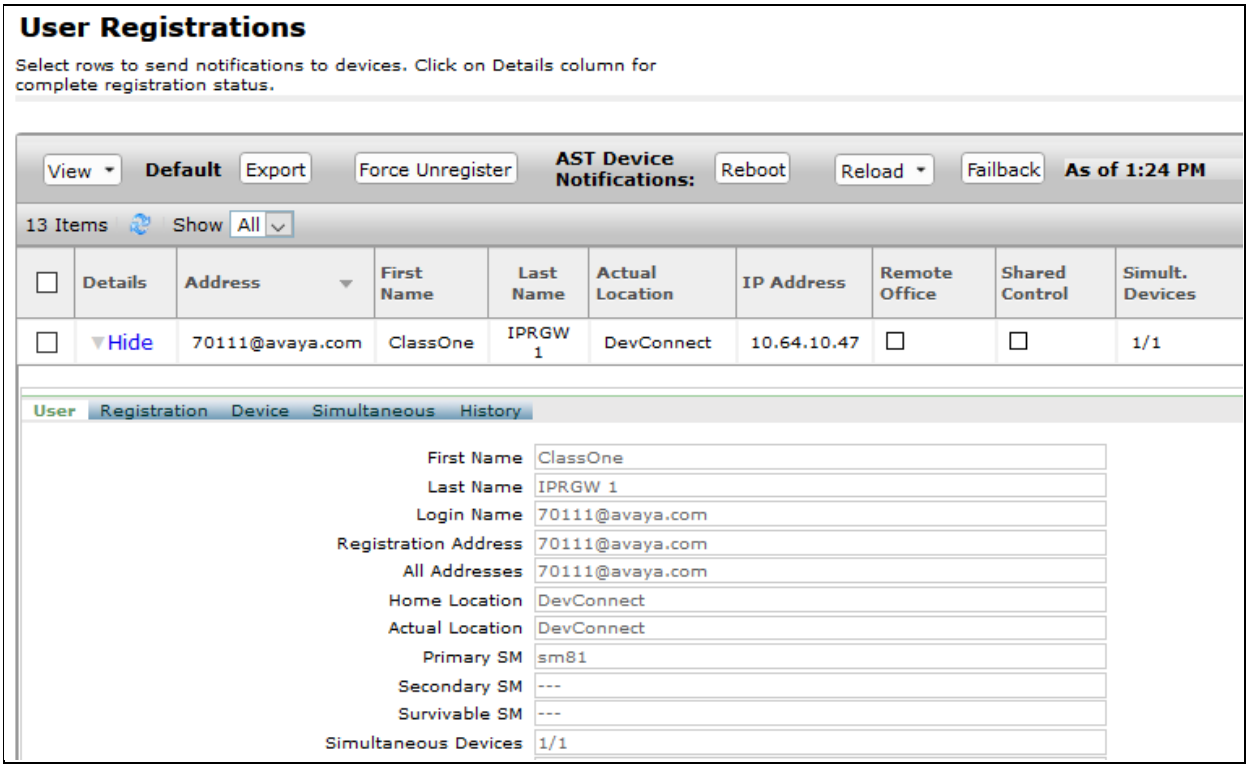
7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of iCAS IP Radio Gateway.

7.1. Verify iNEMSOFT ClassOne iCAS Radio Gateway

The following steps may be used to verify the configuration:

- Verify that iCAS IP Radio Gateway successfully registers with Session Manager server by following the **Session Manager → System Status → User Registrations** link on the System Manager Web Interface.



- Place calls to and from iCAS IP Radio Gateway and verify that the calls are successfully established with two-way talk path.

8. Conclusion

These Application Notes describe the configuration steps required for iNEMSOFT CLASSONE iCAS IP Radio Gateway 3.6.1 to successfully interoperate with Avaya Aura® Session Manger 10.1. All feature and serviceability test cases were completed with observations noted in **Section** Error! Reference source not found..

9. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 7, May 2023, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

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.