



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring iNEMSOFT CLASSONE® iCAS IP Radio Gateway which were compliance tested with Avaya Aura® Session 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 contain instructions for iNEMSOFT CLASSONE® iCAS (iCAS) IP Radio Gateway with Avaya Aura® Session Manager (Session Manager) to successfully interoperate.

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

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 with Avaya Meeting Exchange
- Application Notes for iNEMSOFT CLASSONE® iCAS Dispatch Console with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services
- Application Notes for iNEMSOFT CLASSONE® Endpoint Manager with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services

These Application Notes assume that Communication Manager and Session Manager are already installed and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult references [1], [2], and [3].

2. General Test Approach and Test Results

The general test approach was to place calls to and from CLASSONE® iCAS IP Radio Gateway and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711MU)
- Inbound calls
- Outbound calls
- Call termination (origination/destination)
- Serviceability

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 these Application Notes, the interface between Avaya systems and iNEMSOFT did not utilize encryption capabilities.

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 calls and hold/resume and iCAS IP Radio Gateway interactions with Session Manager, Communication Manager, and Avaya SIP, H.323, and digital telephones 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

CLASSONE® iCAS support can be obtained via following means:

Phone: 214-423-2815

Web: www.inemsoft.com

Email: rtisupport@inemsoft.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and iNEMSOFT CLASSONE® iCAS IP Radio Gateway.

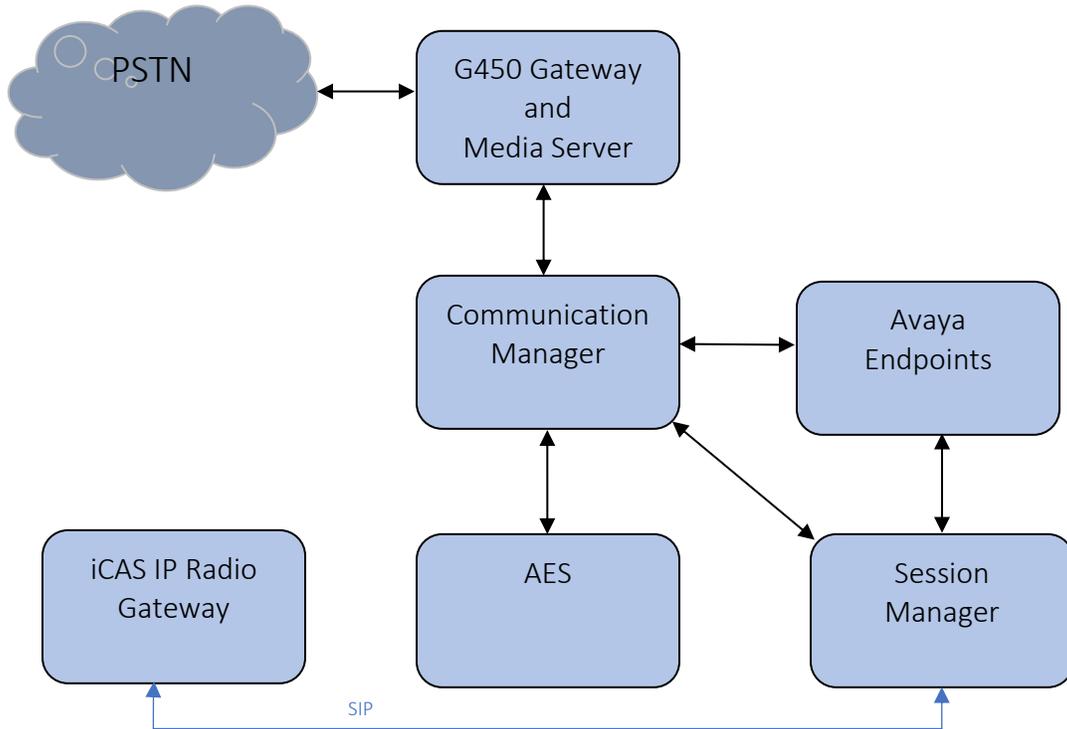


Figure 1: Test Configuration of CLASSONE® iCAS IP Radio Gateway by iNEMSOFT

4. Equipment and Software Validated

The following equipment and software were used for the test configuration. With the exception of Avaya G450 Gateway, all other Avaya products were deployed on a Virtualization Environment.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.0.1.1.890.25517
Avaya G450 Media Gateway	FW 40.19.1
Avaya Aura® Media Server	8.0.1.121
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya Aura® System Manager	8.1.0.0.733078
Avaya 9600 Series IP Deskphones	6.8.2 (H.323) 7.1.6.1 (SIP)
Avaya J100 Series IP Phones	6.8.2 (H.323) 4.0.2.1 (SIP)
iNEMSOFT CLASSONE® iCAS Radio Gateway	3.4

5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager web console and is then downloaded into Session Manager. Log on to System Manager via a web browser.



Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

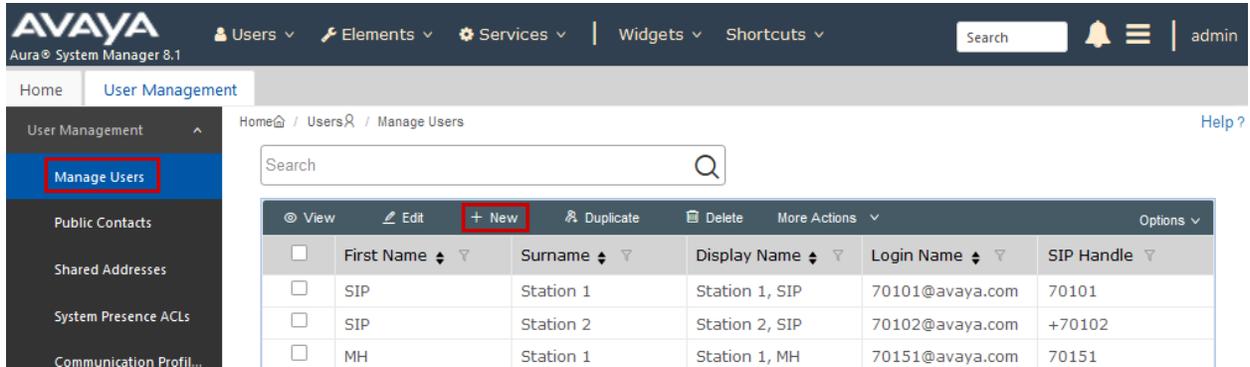
System Manager Dashboard is displayed.

5.1. Configure SIP Users

During the compliance test, no special users were created for this solution. However, the steps to configure a user are included.

Add a new SIP user for each iCAS IP Radio Gateway. During compliance testing SIP Users 70111, 70112, 70113 and 70114 were created for iCAS IP Radio Gateway.

To add new SIP users, Navigate to **Users → User Management → Manage Users**. Click **New**.



The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile icon labeled 'admin' are also present. The main content area is titled 'User Management' and 'Manage Users'. A sidebar on the left contains navigation options, with 'Manage Users' highlighted in blue and a red box around it. The main area features a search bar and a table of users. The table has columns for 'First Name', 'Surname', 'Display Name', 'Login Name', and 'SIP Handle'. The '+ New' button in the table's action bar is highlighted with a red box.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	Station 1	Station 1, SIP	70101@avaya.com	70101
<input type="checkbox"/>	SIP	Station 2	Station 2, SIP	70102@avaya.com	+70102
<input type="checkbox"/>	MH	Station 1	Station 1, MH	70151@avaya.com	70151

Configure the **Identity** tab as follows:

- **Last Name** – Enter last name of user.
- **First Name** – Enter first name of user.
- **Login Name** – Enter extension number@sip domain name.

User Profile | Edit | 70111@avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [dropdown]

* Last Name: IPRGW 1

* First Name: ClassOne

* Login Name: 70111@avaya.com

Last Name (Latin Translation): IPRGW 1

First Name (Latin Translation): ClassOne

Middle Name: Middle Name Of User

Select the **Communication Profile** tab followed by **Communication Profile Password** on the left pane and provide the following information:

- **Communication Profile Password** – Enter a numeric password
- **Confirm Password** – Repeat numeric password.

User Profile | Edit | 70111@avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile [toggle]

Avaya Breeze® Profile [toggle]

CM Endpoint Profile [toggle]

Presence Profile [toggle]

Comm-Profile Password

Comm-Profile Password: [password field]

* Re-enter Comm-Profile Password: [password field] [checkmark]

Generate Comm-Profile Password

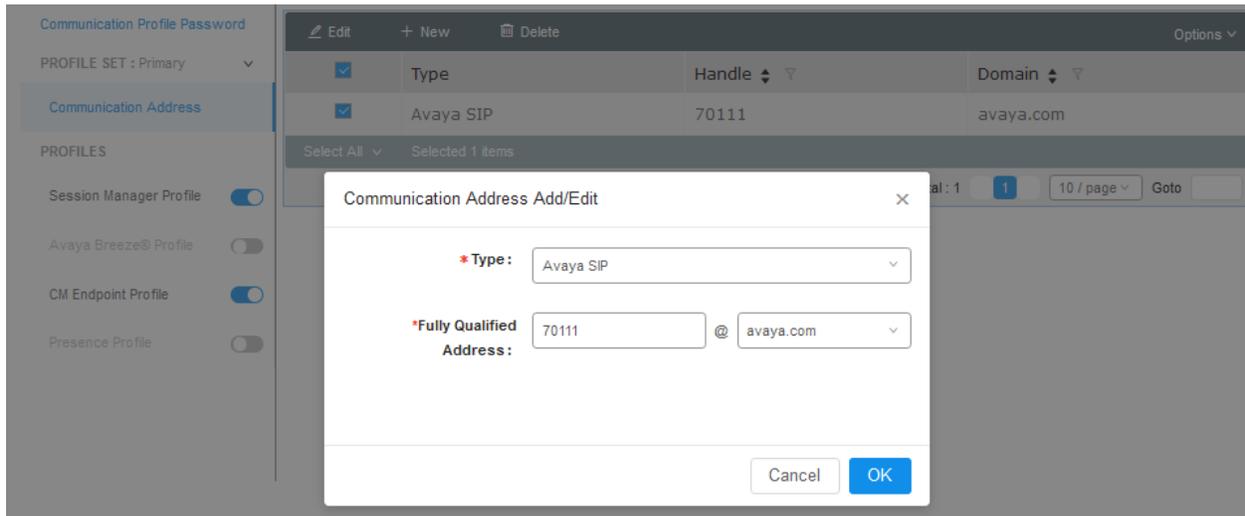
Cancel OK

Type	Handle	Domain
Avaya SIP	70111	avaya.com

On the left pane, select **Communication Address** followed by **New** to define a **Communication Address** for the new SIP user, and provide the following information.

- Type – Select Avaya SIP using drop-down menu.
- Fully Qualified Address – Enter same extension number and domain used for Login Name, created previously.

Click the **Add** button to save the Communication Address for the new SIP user.



On the left pane, enable **Session Manager Profile** and configure as follows:

- **Primary Session Manager** – Select one of the Session Managers.
- **Origination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
- **Home Location** – Select a predefined location.

The screenshot displays the configuration interface for SIP Registration. On the left, a sidebar shows the 'PROFILE SET : Primary' and a list of profiles: 'Session Manager Profile' (enabled), 'Avaya Breeze® Profile' (disabled), 'CM Endpoint Profile' (enabled), and 'Presence Profile' (disabled). The main configuration area is divided into several sections:

- SIP Registration:**
 - Primary Session Manager:** Input field contains 'sm81'.
 - Secondary Session Manager:** Input field contains 'Start typing...'.
 - Survivability Server:** Input field contains 'Start typing...'.
 - Max. Simultaneous Devices:** Dropdown menu set to '1'.
 - Block New Registration When Maximum Registrations Active?:** Unchecked checkbox.
- Application Sequences:**
 - Origination Sequence:** Dropdown menu set to 'cm81'.
 - Termination Sequence:** Dropdown menu set to 'cm81'.
- Emergency Calling Application Sequences:**
 - Emergency Calling Origination Sequence:** Dropdown menu set to 'Select'.
 - Emergency Calling Termination Sequence:** Dropdown menu set to 'Select'.
- Call Routing Settings:**
 - Home Location:** Dropdown menu set to 'DevConnect'.

On the left pane, enable **CM Endpoint Profile** and configure as follows:

- **System** – Select Managed Element defined in System Manager (not shown) for Communication Manager.
- **Use Existing Endpoints** - Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
- **Extension** - Enter same extension number used in this section.
- **Template** – Select template for type of SIP phone. During the compliance test, 9641SIP_DEFAULT_CM_8_1 was selected.

Select **Commit** once done.

The screenshot shows the configuration page for a CM Endpoint Profile. On the left, a sidebar lists profile categories: Communication Profile Password, PROFILE SET (Primary), Communication Address, PROFILES, Session Manager Profile (checked), Avaya Breeze Profile (unchecked), CM Endpoint Profile (checked), and Presence Profile (unchecked). The main configuration area includes the following fields and options:

- * System:** cm81
- * Profile Type:** Endpoint
- Use Existing Endpoints:**
- * Extension:** 70111
- Template:** 9641SIP_DEFAULT_CM_8_1
- * Set Type:** 9641SIP
- Security Code:** Enter Security Code
- Port:** IP
- Voice Mail Number:** (empty)
- Preferred Handle:** Select
- Calculate Route Pattern:**
- Sip Trunk:** aar
- SIP URI:** Select
- Enhanced Callr-Info Display for 1-line phones:**
- Delete on Unassign from User or on Delete User:**
- Override Endpoint Name and Localized Name:**
- Allow H.323 and SIP Endpoint Dual Registration:**

6. Configure iNEMSOFT CLASSONE® iCAS IP Radio Gateway

Installation and configuration of iCAS IP Radio Gateway is done by designated iNEMSOFT engineers. Hence, no configuration is provided in this document.

7. Verification Steps

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.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

The screenshot shows the 'User Registrations' page in the System Manager web interface. At the top, there are navigation buttons: View (dropdown), Default, Export, Force Unregister, AST Device Notifications, Reboot, Reload (dropdown), Failback, and As of 1:24 PM. Below this, it indicates '13 Items' and a 'Show All' dropdown. The main table has columns: Details, Address, First Name, Last Name, Actual Location, IP Address, Remote Office, Shared Control, and Simult. Devices. One row is visible with the following data: Details (checkbox), Hide (dropdown), 70111@avaya.com, ClassOne, IPRGW 1, DevConnect, 10.64.10.47, Remote Office (checkbox), Shared Control (checkbox), and Simult. Devices (1/1). Below the table, there is a 'User' details section with tabs for Registration, Device, Simultaneous, and History. The 'Registration' tab is active, showing a list of fields and their values: First Name (ClassOne), Last Name (IPRGW 1), Login Name (70111@avaya.com), Registration Address (70111@avaya.com), All Addresses (70111@avaya.com), Home Location (DevConnect), Actual Location (DevConnect), Primary SM (sm81), Secondary SM (---), Survivable SM (---), and Simultaneous Devices (1/1).

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

8. Conclusion

During compliance testing, iNEMSOFT CLASSONE® iCAS IP Radio Gateway successfully registered with Avaya Aura® Session Manager, placed and received calls to and from Avaya Endpoints.

9. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>

- [1] Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 4, November 2019.
- [2] Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 3, October 2019
- [3] Administering Avaya Aura® Session Manager, Release 8.1.1, Issue 2, October 2019

Documentation related to iCAS can be directly obtained from iNEMSOFT.

©2019 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.