Avaya Solution & Interoperability Test Lab

Application Notes for iNEMSOFT CLASSONE® Endpoint Manager with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

The Application Notes describe configuration required for iNEMSOFT CLASSONE® Endpoint Manager to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

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

iNEMSOFT CLASSONE® Endpoint Manager is an application used with Avaya Aura® infrastructure to manage Avaya endpoints.

iNEMSOFT CLASSONE® Endpoint Manager helps managing Avaya endpoints during switch upgrades, maintenance outages, disasters and system failures with the use of Avaya's System Management Service (SMS) interface and PUSH interfaces provided by Avaya endpoints.

2. General Test Approach and Test Results

The general test approach was to validate successful integration of CLASSONE® Endpoint Manager.

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

During Interoperability Compliance testing, the following feature tests were expected:

- Upgrading and downgrading firmware on Avaya H.323 and SIP endpoints
- Phone profile backup and restore.
- Checking Avaya endpoints status via CLASSONE® Endpoint Manager console.
- Failover of Avaya endpoints between two Avaya Aura® sites.
- Display the current Avaya Aura® site on the Avaya endpoints display.

2.2. Test Results

All tests were executed successfully with the following observation.

- Avaya J100 Series SIP phones do not support PUSH interface. Thus, the display of current Avaya Aura® site provided by CLASSONE® Endpoint Manager is not available for these phones.

2.3. Support

iNEMSOFT support for customers with current maintenance and support agreement may be obtained via the following means:
Phone: (214) 423-2815
E-mail: rtisupport@inemsoft.com

3. Reference Configuration

The following reference configuration shows primary and secondary sites. During compliance testing, Avaya endpoints were switched between both sites.

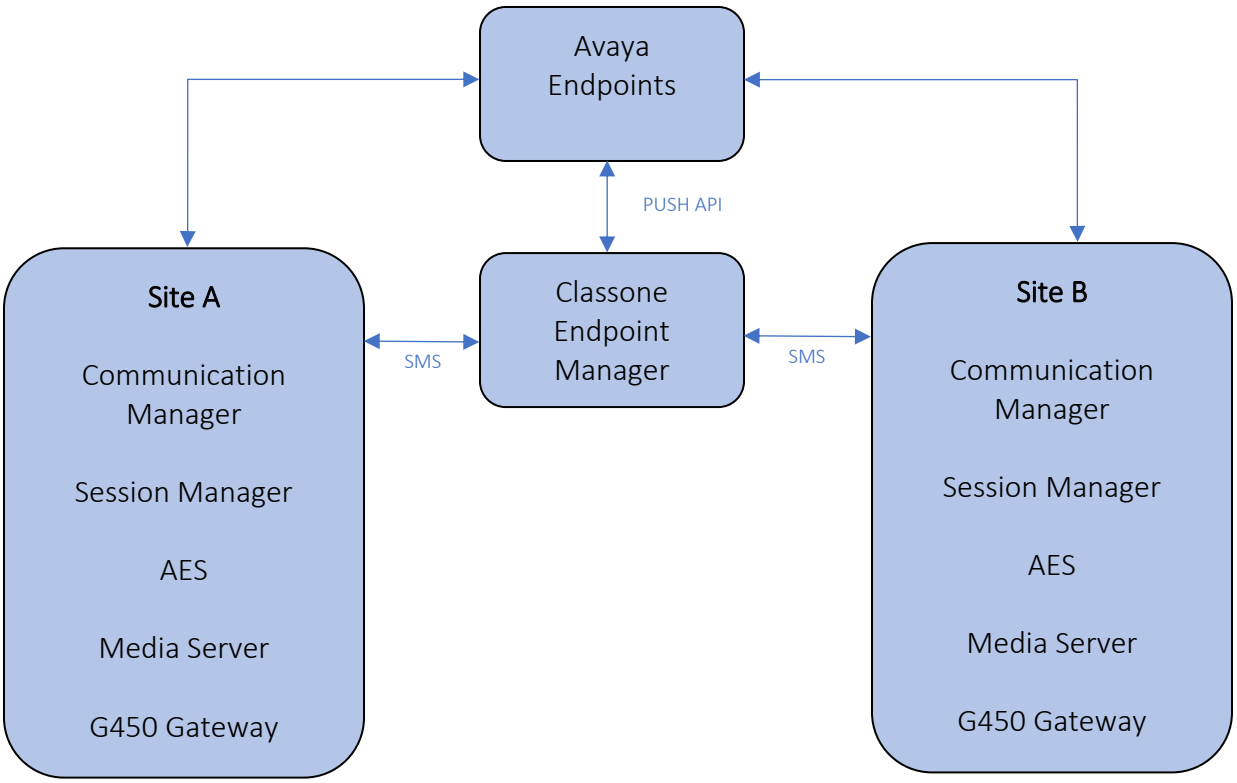


Figure 1: Reference Configuration

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	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 Aura® Application Enablement Services	8.1.0.0.0.9-1
Avaya 9600 Series IP Deskphones	6.6.5 (H.323) 6.8.2 (H.323) 7.1.6.1 (SIP) 7.1.6.0 (SIP)
Avaya J100 Series IP Phones	6.8.2 (H.323) 4.0.2.1 (SIP) 4.0.2.0 (SIP)
iNEMSOFT CLASSONE® Endpoint Manager	5.3

5. Configure Avaya Aura® Communication Manager

Communication Manager used an existing CTI link to AES. Configuration of this aspect is standard and not directly relevant to the interoperability of CLASSONE® Endpoint Manager. These application notes will not cover this aspect of the configuration.

5.1. Add System Management Service (SMS) User

CLASSONE® Endpoint Manager uses the AES SMS interface to query for administered stations.

A privileged user account was used during Compliance test; however, a local administrator can restrict the user account privileges. This involves creating a user profile via SAT, and then creating and assigning that user to the profile in the web admin pages.

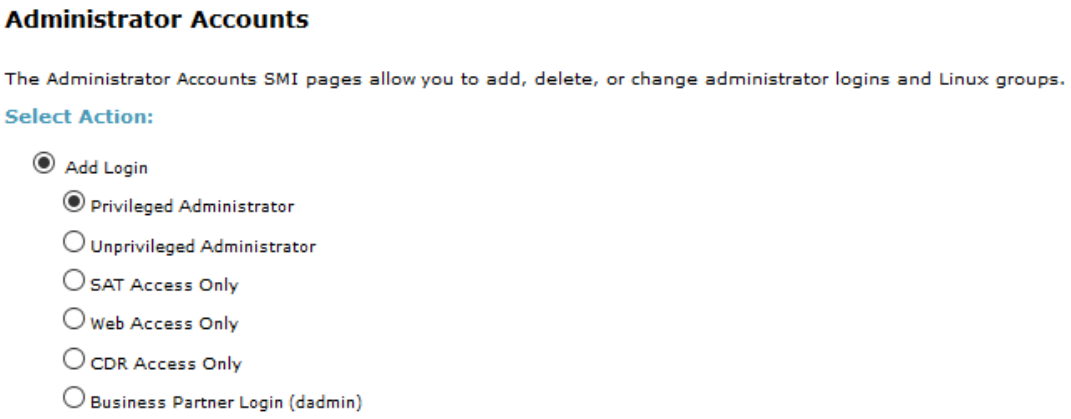
Use **add user-profile *next*** command to add a user profile for SMS user. On Page 1, set the following features to **y**:

- Call Center B
- Stations M

```
add user-profile next                                        Page   1 of
41
                              USER PROFILE 20

User Profile Name: iNEMSOFT SMS User

       This Profile is Disabled? n               Shell Access? n
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n           Extended Profile? n

             Name           Cat Enbl           Name                Cat Enbl
                    Adjuncts A   n            Routing and Dial Plan J   n
                Call Center B   y                         Security K   n
                   Features C   n                           Servers L   n
                   Hardware D   n                          Stations M   y
                 Hospitality E   n               System Parameters N   n
                          IP F   n                    Translations O   n
                 Maintenance G   n                        Trunking P   n
Measurements and Performance H   n                           Usage Q   n
               Remote Access I   n                     User Access R   n
```

Create a SMS user account on the Communication Manager **System Management Interface** web page, https://<communication-manager-ip-address>. Navigating to **Administration → Server (Maintenance)**

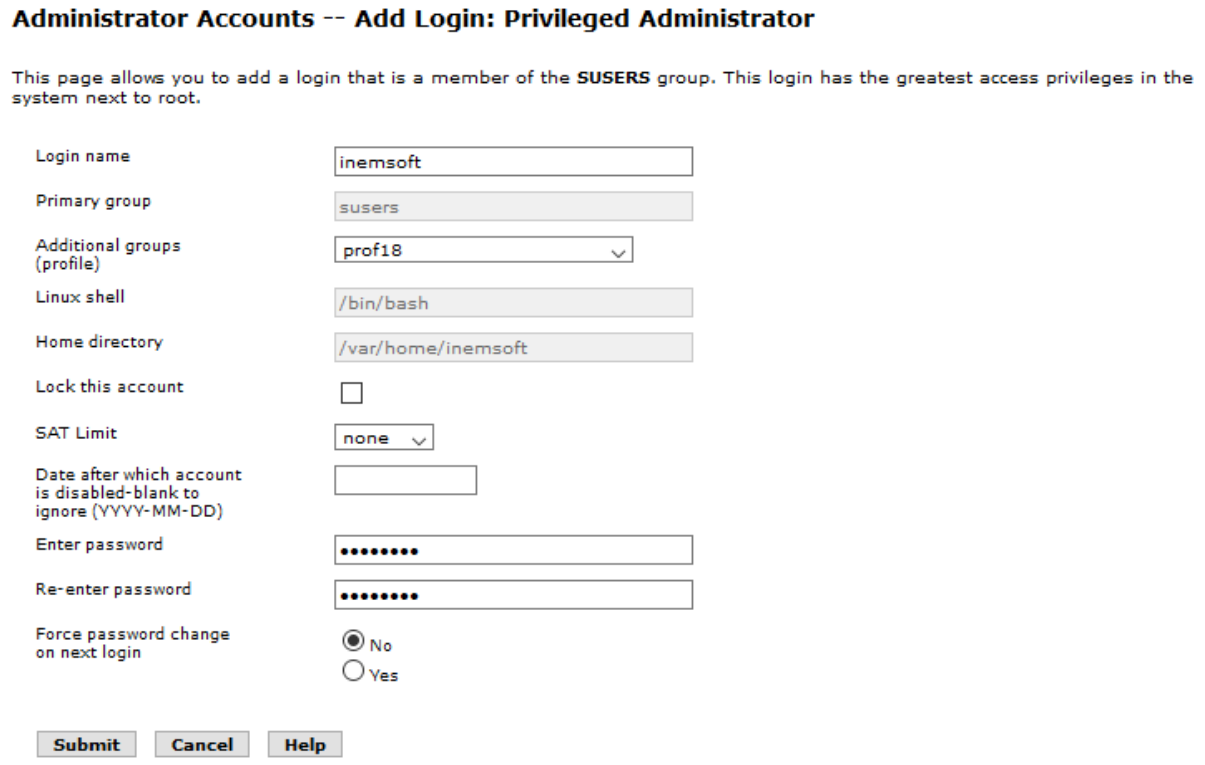
Select **Administrator Accounts** under **Security**, select **Add Login, Privileged Administrator** and **Submit**.



On the **Administrator Accounts – Add Login: Privileged Administrator** page:

- Type in a **Login Name**
- For **Additional Groups**, set it to the user-profile added above or leave default
- Type in a password in **Enter password or key** and **Re-enter password or key**

Once done, select **Submit.**



6. Configure Avaya Endpoints

If DHCP is used to retrieve configuration for Avaya IP Phones:

- Set HTTSRVR to CLASSONE® Endpoint Manager's IP Address from **Section 3**:
  - Option option-242 "HTTPSRVR="

If DHCP is not used, set the HTTP Server for the Avaya endpoints to the IP address of CLASSONE® Endpoint Manager.

7. Configure iNEMSOFT CLASSONE® Endpoint Manager

All Configuration related to CLASSONE® Endpoint Manager is performed by iNEMSOFT engineers, as such, is not provided in this document.

8. Verification Steps

Once the HTTP Server is changed on Avaya endpoints, reboot the phones and verify the configuration and/or firmware update is pulled from CLASSONE® Endpoint Manager. To verify that the configuration is getting updated from the correct HTTP Server; while the phone is booting up, verify on the phone screen, an HTTP request for 46xxsetting.txt to the newly configured HTTP Server, followed by a 200 OK response.

9. Conclusion

A set of feature and functional test cases were performed during Compliance testing. iNEMSOFT CLASSONE successfully demonstrated the ability to manage Avaya endpoints.

10. Additional References

[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
[4] CLASSONE® EM Web Admin User Guide

All documents related to Avaya products can be obtained via https://support.avaya.com.

All documents related to iNEMSOFT CLASSONE® can be obtained via emailing support@inemsoft.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.