



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for iNEMSOFT ONCENTS Endpoint Manager 6.2 with Avaya Aura® Communication Manager 10.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for iNEMSOFT ONCENTS Endpoint Manager 6.2 to interoperate with Avaya Aura® Communication Manager 10.1, Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Session Manager 10.1, and Avaya IP phones.

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 iNEMSOFT ONCENTS Endpoint Manager 6.2 to interoperate with Avaya Aura® Communication Manager 10.1, Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Session Manager 10.1, and Avaya IP phones.

In the compliance testing, four Avaya interfaces were used by ONCENTS to manage Avaya IP phones as follows:

- System Management Services (SMS) with Application Enablement Services to obtain Communication Manager configuration information including software version, dial plan, stations, and list of registered H.323 stations. The SMS interface is also used by ONCENTS to change H.323 station extensions and reboot H.323 stations.
- Element Manager Web Services (EMWS) with Session Manager to obtain list of configured SIP users and their registration status including IP address, MAC, model, extension, and firmware version. The EMWS interface is also used by ONCENTS to reboot SIP users with Avaya IP phones.
- PUSH interface with Avaya IP phones to obtain subscription data including IP address, MAC, model, extension, and serial number.
- SNMP interface with Avaya IP phones to obtain phone information including MAC, model, extension, call server, and serial number. The SNMP version used by ONCENTS is version 2c.

ONCENTS also serves as the file server for Avaya IP phones for obtainment of necessary phone settings and firmware. The file server integration does not utilize any Avaya published API and therefore is outside the scope of the compliance test. In the testing, the Avaya IP phones used ONCENTS as the file server with HTTPS access to obtain the security certificate and pertinent settings file.

The compliance testing used the 96x1 IP Deskphones (H.323 and SIP) and J1xx IP Phones (H.323 and SIP).

## 2. General Test Approach and Test Results

The feature test cases were performed manually with specific actions performed from the ONCENTS web-based interface to initiate API message exchanges such as obtaining an updated list of registered H.323 endpoints.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to ONCENTS.

The verification of tests included use of ONCENTS web interface to verify action results and use of ONCENTS logs for proper message exchanges.

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 testing associated with these Application Notes, the interfaces between Avaya systems and ONCENTS include encrypted SMS and EMWS. The PUSH and SNMP interfaces with IP phones were non-encrypted as requested by ONCENTS.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on ONCENTS:

- Use of SMS to obtain Communication Manager software version, dial plan, stations, registered H.323 stations, change H.323 station extensions, and reboot of H.323 stations.
- Use of EMWS to obtain configured SIP users and registration status including IP address, MAC, model, extension, firmware version, and reboot of SIP user device.
- Use of PUSH Subscribe to obtain phone IP address, MAC, model, extension, and serial number.
- Use of SNMP to obtain phone MAC, model, extension, call server, and serial number.

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

## 2.2. Test Results

All test cases were executed and verified. The following were observations from the compliance testing.

- The current release of ONCENTS does not perform certificate validation for the EMWS connection.
- A new **PUSH\_MODE** parameter for the 46xxsettings file was introduced by Avaya in SIP firmware 7.1.12 and 4.0.8 and needs to be set for PUSH applications. The new parameter was manually added to ONCENTS in the compliance testing.
- A new validation on PUSH request content type was added by Avaya for SIP phones for security reasons but was missed in the release notes. For PUSH applications that use the content type of **text/xml** from the PUSH SDK, the new validation will fail with **306 Empty Post Content** returned in the response. ONCENTS 6.2.4 version contains support for the more appropriate content type of **application/x-www-form-urlencoded** and Avaya will issue release notes amendment to describe the new validation and needed change by PUSH applications.

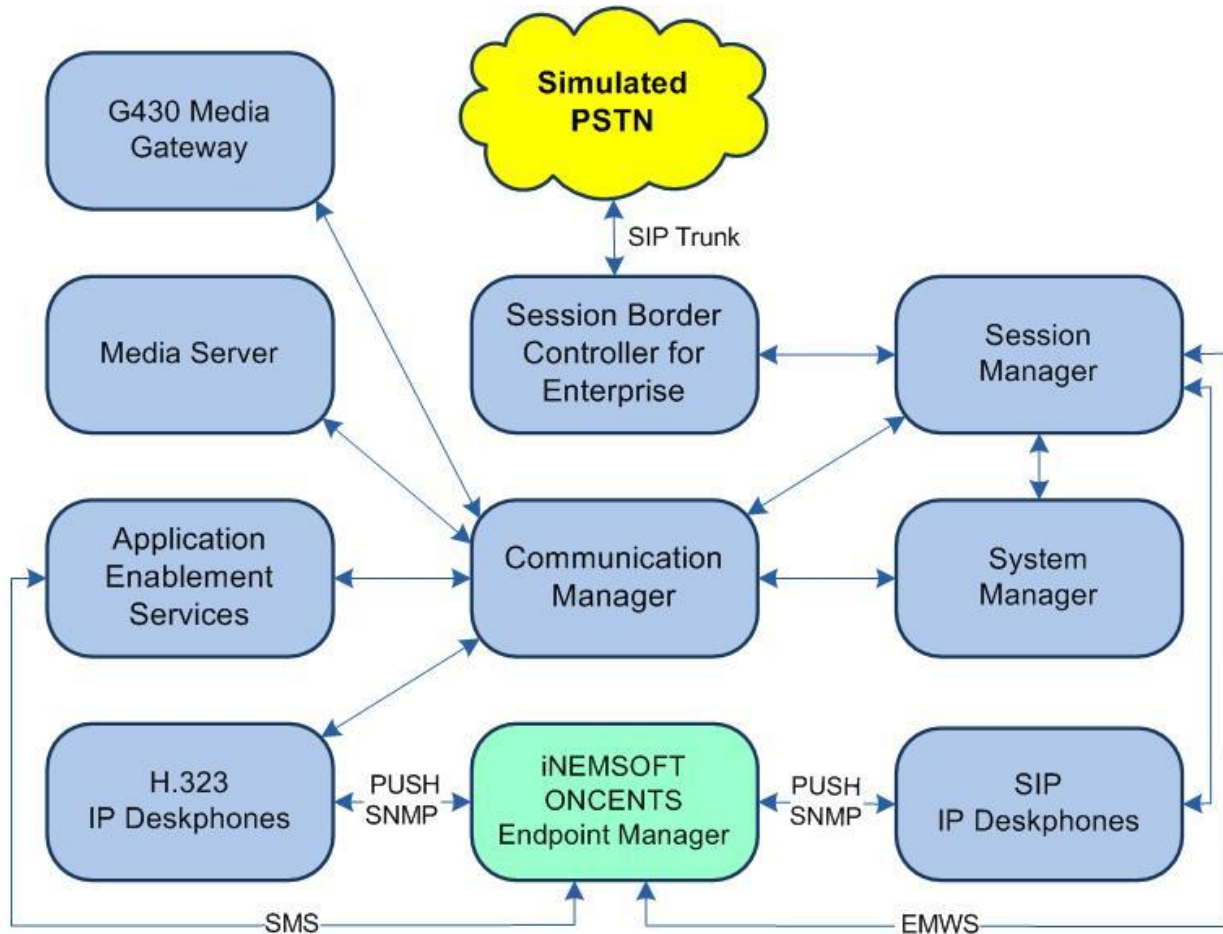
## 2.3. Support

Technical support on ONCENTS can be obtained through the following:

- **Phone:** (214) 423-2815
- **Email:** [emsupport@inemsoft.com](mailto:emsupport@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, Application Enablement Services, System Manager, and Session Manager are not the focus of these Application Notes and will not be described.



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

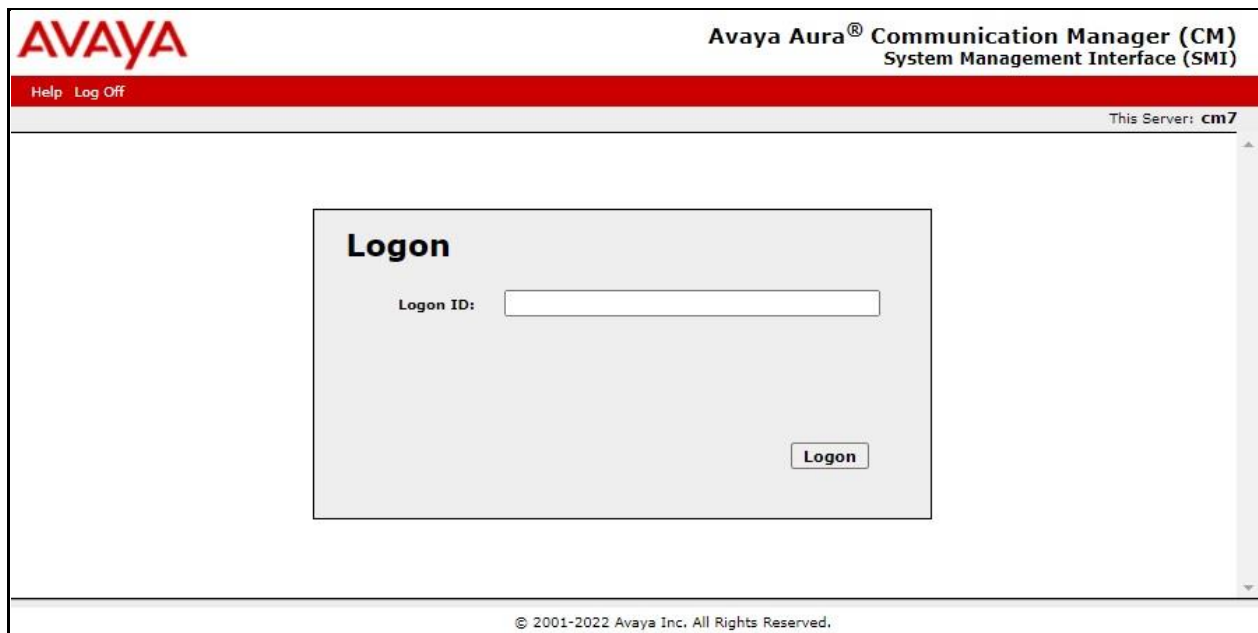
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	10.1 (10.1.0.1.0.974.27372)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1.0.77
Avaya Aura® Application Enablement Services in Virtual Environment	10.1 (10.1.0.1.0.7-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.0.1 (10.1.0.1.1010105)
Avaya Aura® System Manager in Virtual Environment	10.1.0.1 (10.1.0.1.0614394)
Avaya 9611G & J179 IP Deskphone (H.323)	6.8532
Avaya 9641G IP Deskphone (SIP)	7.1.15
Avaya J169 IP Deskphone (SIP)	4.0.13.0.6
iNEMSOFT ONCENTS on CentOS Linux	6.2.4 8

## 5. Configure Avaya Aura® Communication Manager

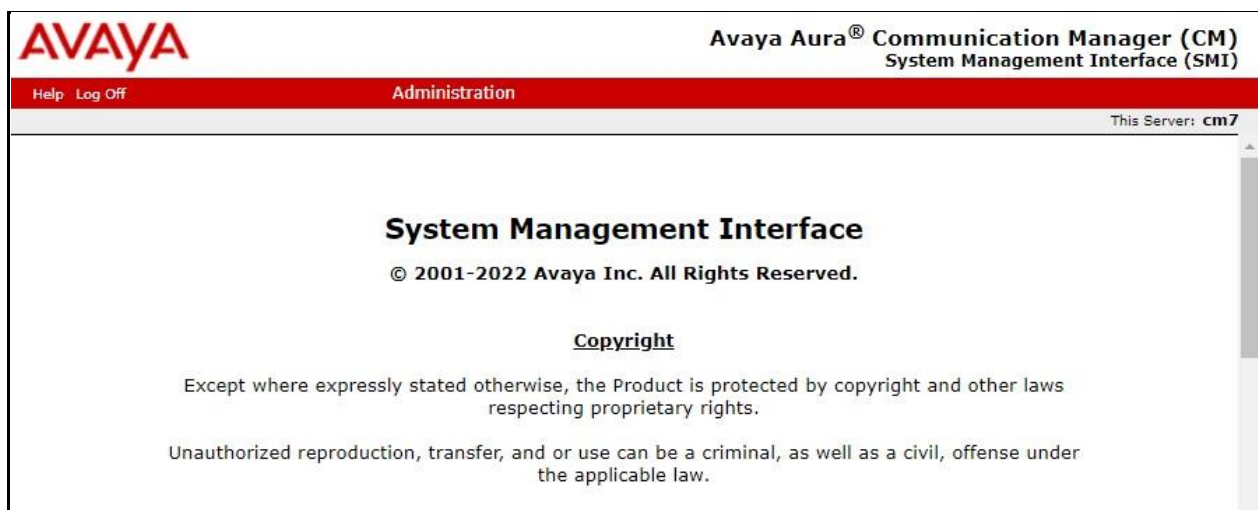
This section provides the procedure for configuring Communication Manager. The procedure involves adding an administrative user to be used by ONCENTS for SMS integration.

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



The screenshot shows the Avaya Aura® Communication Manager (CM) System Management Interface (SMI) login page. The top header features the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header is a red navigation bar with "Help" and "Log Off" links on the left, and "This Server: cm7" on the right. The main content area is a light gray box titled "Logon" containing a "Logon ID:" label, a text input field, and a "Logon" button. The footer displays the copyright notice "© 2001-2022 Avaya Inc. All Rights Reserved."

The **System Management Interface** screen is displayed next. Select **Administration → Server (Maintenance)** from the top menu.

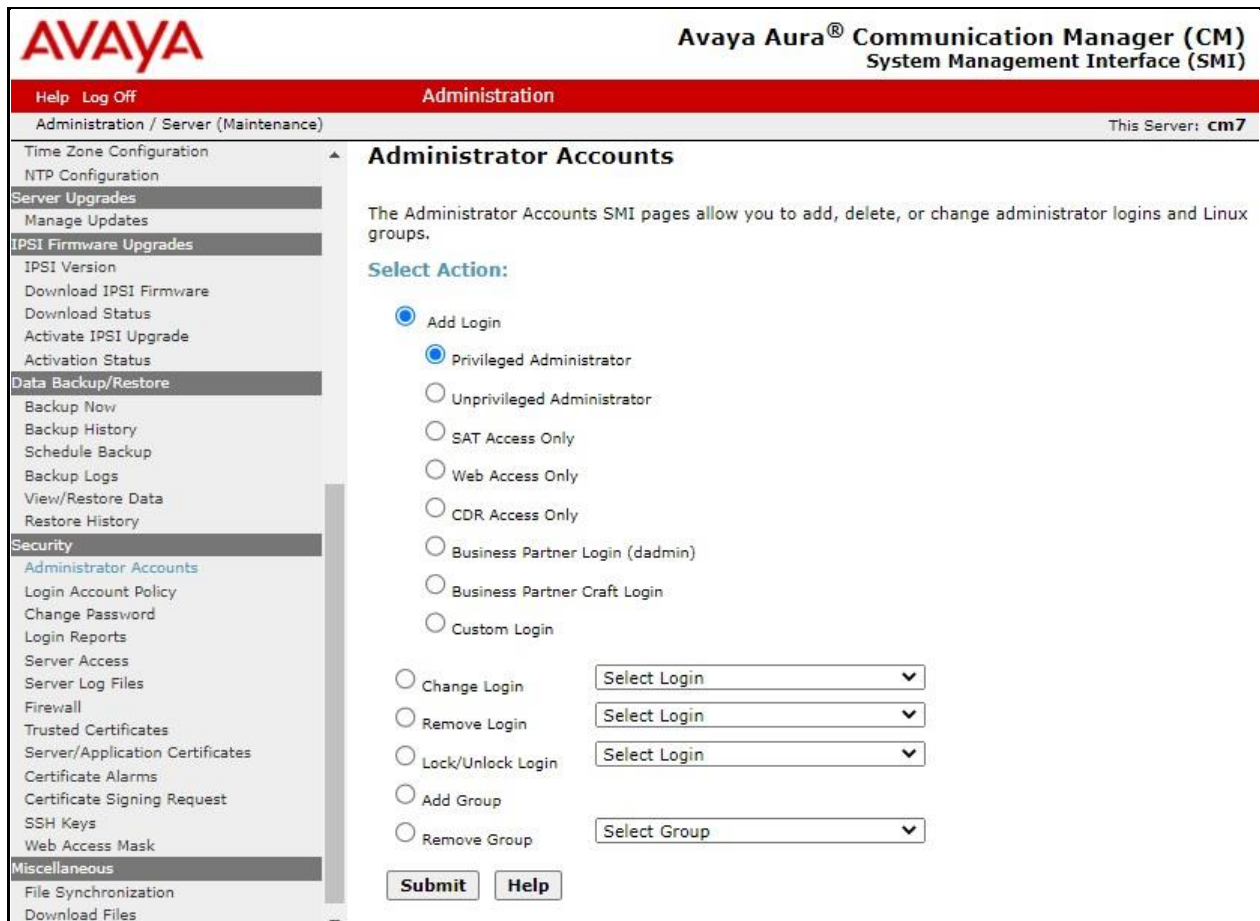


The screenshot shows the Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Administration screen. The top header features the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header is a red navigation bar with "Help" and "Log Off" links on the left, and "Administration" in the center. The right side of the bar shows "This Server: cm7". The main content area is titled "System Management Interface" and includes the copyright notice "© 2001-2022 Avaya Inc. All Rights Reserved." Below this is a section titled "Copyright" with the following text: "Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law."

The **Server Administration** screen is displayed. Scroll the left pane as necessary and select **Security → Administrator Accounts**.



The **Administrator Accounts** screen is displayed next. Select **Add Login** and **Privileged Administrator**, as shown below.





The **Administrator Accounts** screen is updated. Enter the desired credentials for **Login name**, **Enter password**, and **Re-enter password**. Retain the default values in the remaining fields.

Make a note of the account credentials, which will be used later to configure ONCENTS.

**AVAYA** Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: cm7

Administration / Server (Maintenance)

**Administrator Accounts -- Add Login: Privileged Administrator**

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name: inemsoft

Primary group: susers

Additional groups (profile): prof18

Linux shell: /bin/bash

Home directory: /var/home/inemsoft

Lock this account: ☐

SAT Limit: none

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Enter password: .....

Re-enter password: .....

Force password change on next login: ☐ Yes ☒ No

**Submit** **Cancel** **Help**

## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Administer ports
- Administer SMS properties
- Export CA certificate

### 6.1. Launch OAM Interface


Access the OAM web-based interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

 **Application Enablement Services**  
**Management Console**

Welcome: User  
Last login: Mon Oct 3 15:38:15 2022 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Mon Oct 17 09:29:50 EDT 2022  
HA Status: Not Configured

Home

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

## 6.2. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays user information: "Welcome: User", "Last login: Mon Oct 3 15:38:15 2022 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Mon Oct 17 09:30:22 EDT 2022", and "HA Status: Not Configured". The left navigation pane shows "Networking" selected, with sub-items: "AE Service IP (Local IP)", "Network Configure", "Ports", and "TCP/TLS Settings". The main content area is titled "Ports" and contains two sections: "CVLAN Ports" and "TSAPI Ports".

Section	Port Type	Port Number	Enabled	Disabled
CVLAN Ports	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	9998	<input checked="" type="radio"/>	<input type="radio"/>
DLG Port	TCP Port	5678		
TSAPI Ports	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		

Scroll down to the **SMS Proxy Ports** sub-section and configure **Proxy Port Min** and **Proxy Port Max** to the desired values.

Note that SMS can use up to 16 ports and the default values of **4101-4116** were used in the compliance testing as shown below.

The screenshot shows the "H.323 Ports" configuration page. It includes fields for "TCP Port Min" (20000), "TCP Port Max" (29999), "Local UDP Port Min" (20000), and "Local UDP Port Max" (29999). There is an "Enabled" radio button selected. Below these are "Server Media" settings: "RTP Local UDP Port Min\*" (30000) and "RTP Local UDP Port Max\*" (49999). A note states: "\* Note: The number of RTP ports needs to be double the number of extensions using server media." The "SMS Proxy Ports" section has "Proxy Port Min" (4101) and "Proxy Port Max" (4116). At the bottom are "Apply Changes" and "Restore Defaults" buttons.

### 6.3. Administer SMS Properties

Select **AE Services** → **SMS** → **SMS Properties** from the left pane, to display the **SMS Properties** screen in the right pane.

For **Default CM Host Address**, enter the IP address of Communication Manager, in this case **10.64.101.236**. Retain the default values for the remaining fields.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS" (selected), "TSAPI", and "TWS". Under "SMS", "SMS Properties" is selected. The right pane shows the "SMS Properties" configuration form with the following fields and values:

Field	Value
Default CM Host Address	10.64.101.236
Default CM Admin Port	5022
CM Connection Protocol	SSH
SMS Logging	NORMAL
SMS Log Destination	apache
CM Proxy Trace Logging	NONE
Max Sessions per CM	5
Proxy Shutdown Timer	1800 seconds
SAT Login Keepalive	180 seconds
CM Terminal Type	OSSIZ
Proxy Log Destination	/var/log/avaya/aes/ossicm.log

At the bottom of the form are three buttons: "Apply Changes", "Restore Defaults", and "Cancel".



## 6.4. Export CA Certificate

Select **Security** → **Certificate Management** → **CA Trusted Certificates** from the left pane, to display the **CA Trusted Certificates** screen. Select the pertinent CA certificate for secure connection with client applications, in this case **SystemManagerCA**, and click **Export**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Certificate Management' > 'CA Trusted Certificates'. The main content area displays a table of CA Trusted Certificates. The 'SystemManagerCA' certificate is selected.

CA Trusted Certificates

Alias	Status	Issued To	Issued By	Expiration Date
<input type="radio"/> serverCertDefault	valid	aes7-186238827-labUseOnly	aes7-186238827-labUseOnly	6/14/2023
<input type="radio"/> avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	8/14/2033
<input type="radio"/> avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	8/17/2027
<input checked="" type="radio"/> SystemManagerCA	valid	System Manager CA	System Manager CA	10/8/2028

The **Trusted Certificate Export** screen is displayed next. Copy everything in the text box, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** (not shown) lines.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Certificate Management' > 'CA Trusted Certificates'. The main content area displays the 'Trusted Certificate Export' screen. The 'SystemManagerCA' certificate is selected, and the 'Certificate PEM' is displayed in a text box.

Trusted Certificate Export

Issued To: System Manager CA  
Issued By: System Manager CA  
Expiration Date: 10/8/2028

Certificate PEM:

```
-----BEGIN CERTIFICATE-----
NzCCA0gAwIBAgIILbHCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwwRU3lzdGVt
lmFnZXIgaQ0ExDTALBgNVBAsMBE1HTVQxZjAMBGA1UEAwwRU3lzdGVtIE1hbWFnZXIgaQ0ExDTALBgNVBAsM
TVQxZjAMBGA1UEAwwRU3lzdGVtIE1hbWFnZXIgaQ0ExDTALBgNVBAsMBE1HTVQxZjAMBGA1UEAwwRU3lzdGVt
kVLOePXG46TdUR7LjYz1NjkMBGp+vf/rLbyy8u+yO6YT9ZGzpjxYJwZgOKSjrgdkvzv2
I71UICM73wytBQwpzK12HQ00oS1ZAWjEwa/VuPQmbahGdC7UXO4DHMcnczhkWhEOJj4zkRM
T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
iXKM9PaCbcMN29D3RftjybrTqUSKfOUOSiNev7170KDMaC/pRXbc/6Wu03sykTUyCpB4Hx49
lh/c8vdSCYNmN07PPzNhesck0e7MZYwiDAQABO2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
MBaAFFojv41gJO2AZKk709pJBI14Gz7RMB0GA1UdDgQWBBrA17+C1CTtgMyp09PaSQZdeBs+
BgNVHQ8BAf8EBAMCAAYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFjXdeGUUxwOJM
wCz42v6QgmmRBBG2HJfmdPZZ23hKghApey8YyumsVg+A12qRNjb5tfox6p19XA9T8ttOHh
5/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
I6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvm3rW36vRkUBaIOs
-----
```

Paste the copied content to a Notepad file and save with a desired file name and **.cer** as suffix, such as **AESCACert.cer** as shown below.

```
AESCA Cert.cer - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIIL1bhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwwRU31zdGVt
IE1hbmFnZXIqQ0ExDTALBgNVBAsMIBE1HTVQxXDJAMBGNVBAoMBUFWQV1BMB4XDTE4MTAxMTE4MTU0
NFoXDTE4MTAwODE4MTU0NFowOzEaMBGGA1UEAwwRU31zdGVtIE1hbmFnZXIqQ0ExDTALBgNVBAsM
BE1HTVQxXDJAMBGNVBAoMBUFWQV1BMBIIBIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
Y9+b1FeekV10ePXG46TduR7LjyZ1NjkmBCp+vf/rLbyy8u+y06YT9ZGzpaJxeyYJwZgOKSjrgdkv
v2RWmi71UICM73wyTBQwpzK12HQ00s1ZAWjEwa/VuPQmbahGdCUX04DHMczzhekWhE0JJ4zkrM
22W1T+1WqV7fi5q/itP0sEbWuJNo32Tn9U03hc/LWLqomTKyBzt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOU0S1Nev7I70KDMaC/prXbc/6Wu03sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhesck0e7MZYwIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBAAFFoJv4IgJ02AzKk709pJB114Gz7RMB0GA1UdDgQWBBrA17+CICttgMyp09PaSQZdeBs+
0TA0BgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmpt1FXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRBBG2HJfmdPZZ23hKghApey8YumsvG+A12qRnjB5tfox6p19XA9T8tt0Hh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpaYgqF5fUpA8E2zni
m46H6SSivL7WddowqlAxcVr4SclghTpeeMBd1inp9R/e1bv0HK742oBATQGvem3rW36vRkUBaIoS
NzXWnviUXqtBTMQ8irD1zSEMx61IE0bXboht7eU60mnhQczFJjMLiwYuGB9N1mf2+gCZTbK1019N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

## 7. Configure Avaya Aura® System Manager

This section provides the procedures for configuring System Manager for EMWS integration with Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer administrative users

### 7.1. 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.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

User ID:

Password:



## 7.2. Administer Administrative Users

Select **Users** → **Administrators** → **Administrative Users** from the top menu to display a list of existing administrative users (not shown). Select **Add** (not shown) from the right pane to add a new administrative user for ONCENTS to be used for EMWS integration.

The **Add New Administrative User** screen is displayed. Enter desired **User ID**, **Full Name**, **Temporary password**, and **Re-enter password** as shown below. For **Authentication Type**, select **Local**. Click **Commit and Continue**.

**AVAYA**  
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰

Home Administrators

Host Name: smgr7.dr220.com User Name: admin

### Add New Administrative User

**Step1:** Identify the new user.  
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

\* User ID:  (1-31) (Allowed characters are a-z, A-Z, 0-9, ., -, and \_)

Authentication Type: ☒ Local ☐ External

\* Full Name:

E-Mail:

The user will receive notifications on this E-Mail address.

\* Temporary password:

\* Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9[]()<>./:[]^\_@\$%&-+\*~?\'\\The length of your password must be at least 5 characters.

**Note:** The new user must be saved before you may assign roles.

\* Required

The screen below is displayed next for assigning role(s) to the new administrative user. Scroll the right pane as necessary to locate and check **34 System Administrator** as shown below.

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search [ ] [Bell Icon] [Menu Icon]

Home Administrators

Host Name: smgr7.dr220.com User Name: admin

### Add New Administrative User

**Step2:** Assign Role(s)  
Selected roles authorize the user for associated features and element permissions.

Roles	Description
<input type="checkbox"/> Routing Administrator	Session Manager and Routing Administrator
<input type="checkbox"/> Session Manager and Routing Auditor	Session Manager and Routing Auditor
<input type="checkbox"/> SIPAS Auditor	Gives read-only access to all SIP Foundation server management functionality.
<input type="checkbox"/> SIPAS Security Administrator	Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.
<input type="checkbox"/> SIPAS System Administrator	Gives read and write access to all the SIP Foundation server management functionality.
<input checked="" type="checkbox"/> <b>34 System Administrator</b>	Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.
<input type="checkbox"/> Tenant Administrator	A role for basic tenant administration functionality. It can be used as a template to build tenant specific roles.
<input type="checkbox"/> Template	
<input type="checkbox"/> TenantRestApi	TenantRestApi

[Commit] [Cancel]

Note that the new administrative user is required to change the temporary password upon initial log in, therefore log off as the existing user from the web interface and log back into System Manager using the new administrative user credentials created in this section.

The screen below is displayed upon successful log in. Enter desired password for **New Password** and **Confirm Password**. Click **Change**.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

You must change your temporary password to continue

New Password: [ ]

Confirm Password: [ ]

[Change] [Cancel] [Reset]

New passwords are limited to characters in the set **a-zA-Z0-9{}|()<>./,=-[]^\_@\$%&-+\"?:'\";** and must also meet the following policy requirement(s):

- Password length must be at least 5 characters.

## 8. Configure iNEMSOFT ONCENTS Endpoint Manager

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

- Prepare worksheet
- Query real-time data
- Manage H.323 endpoints
- Manage SIP endpoints

The configuration of ONCENTS is performed by the iNEMSOFT deployment group. The procedural steps are presented in these Application Notes for informational purposes.

This section assumes that the CA certificate exported from Application Enablement Services in **Section 6.4** for SMS integration has been properly installed on ONCENTS, and that the configuration file generated from the filled out worksheet in **Section 8.1** has been uploaded to the ONCENTS server.

### 8.1. Prepare Worksheet

Prior to deployment, customer needs to fill out a worksheet from iNEMSOFT with pertinent information for the Avaya products in the customer environment. The filled out worksheet is used to create a configuration file that gets uploaded by the iNEMSOFT deployment group.

The following sections describe the parameters and values that were filled out in the worksheet for the compliance testing.

### 8.1.1. OnCentsEM Servers

Open the worksheet and navigate to the **Must-OnCentsEM Servers** tab.

	VMWARE CPU	VMWARE RAM	VMWARE DISK SPACE	ESXI VERSION	IP ADDRESS (SM100)	HOST NAME	SUBNET MASK	DEFAULT GATEWAY	SUBNET ADDRESS	NAMESERVER 1
1										
2	ERS									
3										
4	1	24 G	170 G	6.5	10.64.101.208	ccapp001	255.255.255.0	10.64.101.1	10.64.101.0	10.64.101.212
5										
6	ds must be filled by the customer. Follow the example in Green row.									
7										
8										

The parameters and values below were used in the compliance testing.

Parameter	Value	Description
IP Address	10.64.101.208	IP address for ONCENTS server
Host Name	ccapp001	Desired host name for ONCENTS server
Subnet Mask	255.255.255.0	The applicable subnet mask for the network
Default Gateway	10.64.101.1	The applicable gateway for the network
Name Server 1	10.64.101.212	The applicable DNS server for the network
NTP Server 1	10.64.101.212	The applicable NTP server for the network
Domain Name	dr220.com	The applicable domain name for the network

### 8.1.2. Avaya CM

Navigate to the **Must-Avaya CM** tab shown in **Section 8.1.1**. The parameters and values below were used in the compliance testing.

Parameter	Value	Description
Procr IP Address	10.64.101.236	The procr IP address of Communication Manager
Name	CM 10.1	A desired name for Communication Manager
Version	10.1	Software version of Communication Manager
Street	350 Mount Kemble Ave	Pertinent street address
City	Morristown	Pertinent city
State	NJ	Pertinent state
SMS Login Username	inemsoft	Communication Manager user credential from <b>Section 5</b>
Login Password	inemsoftcm	Communication Manager user credential from <b>Section 5</b>
Associated AES IP	10.64.101.239	IP address of Application Enablement Services

### 8.1.3. Avaya SMGR

Navigate to the **MustAvaya SMGR** tab shown in **Section 8.1.1**. Note that this tab only applies to customers with SIP endpoints and the parameters and values below were used in the compliance testing.

Parameter	Value	Description
IP Address	10.64.101.235	IP address of System Manager
Domain	dr220.com	The applicable domain name for the network
Login Username	inemsoft	System Manager user credential from <b>Section 7.2</b>
Login Password	iN3mLab%	System Manager user credential from <b>Section 7.2</b>

### 8.1.4. Avaya SM

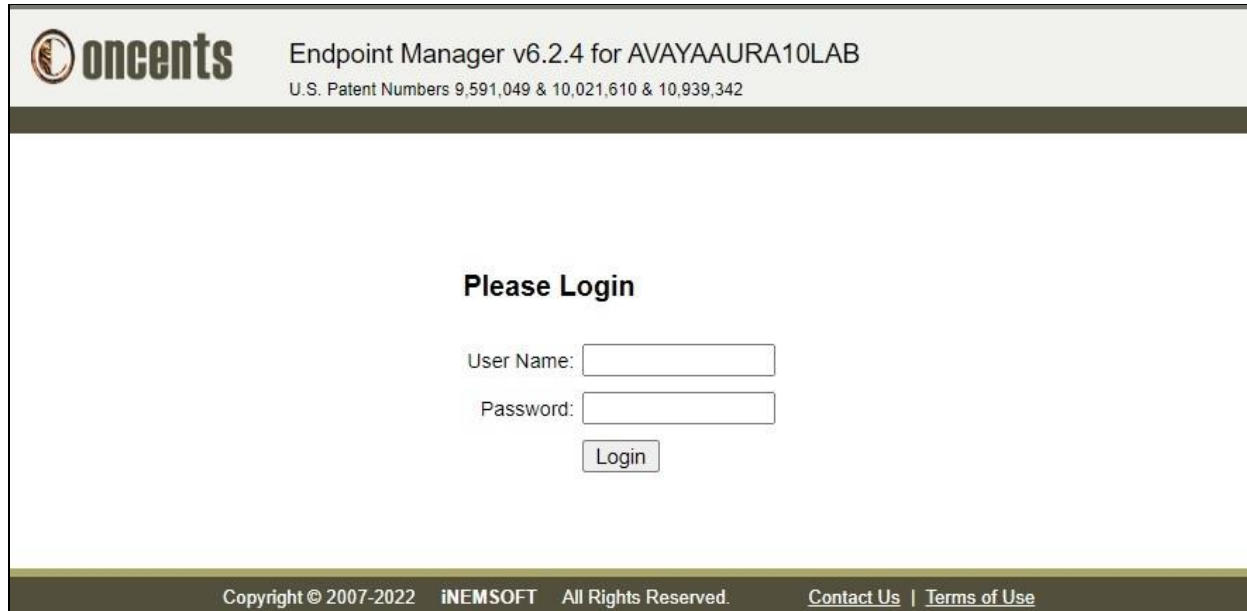
Navigate to the **Must-Avaya SM** tab shown in **Section 8.1.1**. Note that this tab only applies to customers with SIP endpoints and the parameters and values below were used in the compliance testing.

Parameter	Value	Description
Proxy IP Address	10.64.101.238	IP address of the Session Manager signaling interface
SIP Domain	dr220.com	The applicable domain name for the network
SIP Port	5061	The applicable port
Protocol	tls	The applicable protocol

## 8.2. Query Real-time Data

Access the ONCENTS web interface by using the URL **http://ip-address** in a browser window, where **ip-address** is the IP address of the ONCENTS server.

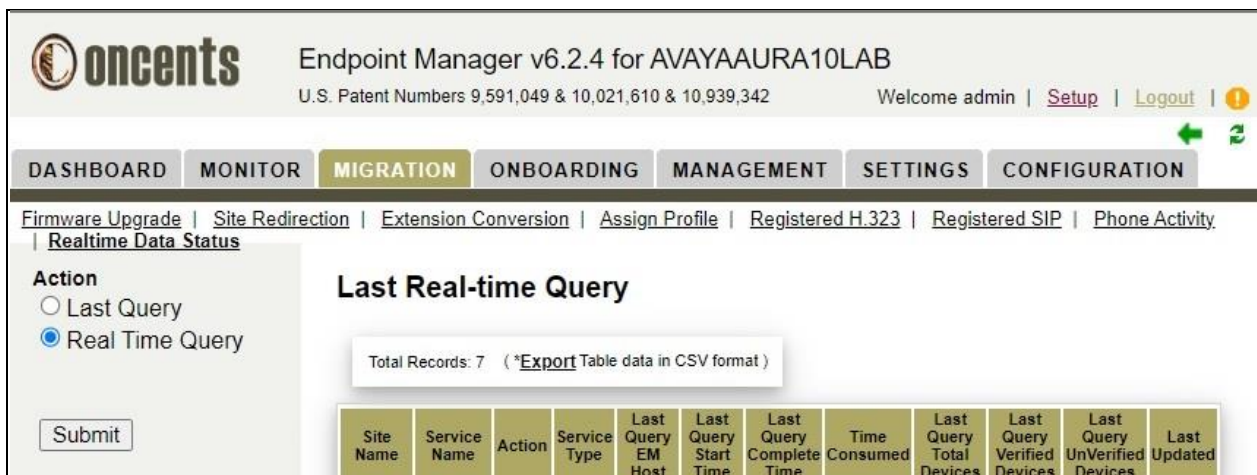
The **Please Login** screen below is displayed, where **AVAYAAURA10LAB** is the company name that was pre-configured as part of installation. Log in using the appropriate credentials.



The screenshot shows the ONCENTS web interface login page. The header includes the ONCENTS logo, the text 'Endpoint Manager v6.2.4 for AVAYAAURA10LAB', and 'U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342'. The main content area is titled 'Please Login' and contains a 'User Name:' input field, a 'Password:' input field, and a 'Login' button. The footer displays 'Copyright © 2007-2022 iNEMSOFT All Rights Reserved.' and links for 'Contact Us' and 'Terms of Use'.

In the subsequent screen, select **Setup → Device Admin** (not shown) from the upper right corner of screen, followed by **MIGRATION → Realtime Data Status** to display the **Last Real-time Query** screen.

Select **Real Time Query** in the left pane and click **Submit**.



The screenshot shows the 'Last Real-time Query' screen in the ONCENTS web interface. The header is identical to the login page. The navigation bar includes 'DASHBOARD', 'MONITOR', 'MIGRATION' (highlighted), 'ONBOARDING', 'MANAGEMENT', 'SETTINGS', and 'CONFIGURATION'. A breadcrumb trail shows 'Firmware Upgrade | Site Redirection | Extension Conversion | Assign Profile | Registered H.323 | Registered SIP | Phone Activity | Realtime Data Status'. The left sidebar has 'Action' with radio buttons for 'Last Query' and 'Real Time Query' (selected), and a 'Submit' button. The main content area is titled 'Last Real-time Query' and shows 'Total Records: 7 (\*Export Table data in CSV format)'. Below this is a table with 12 columns: Site Name, Service Name, Action, Service Type, Last Query EM Host, Last Query Start Time, Last Query Complete Time, Time Consumed, Last Query Total Devices, Last Query Verified Devices, Last Query UnVerified Devices, and Last Updated.

Site Name	Service Name	Action	Service Type	Last Query EM Host	Last Query Start Time	Last Query Complete Time	Time Consumed	Last Query Total Devices	Last Query Verified Devices	Last Query UnVerified Devices	Last Updated



The **System Wide Realtime Data Query Status** screen is displayed in the right pane. Click on **Start System Wide Realtime Data Query**.

Endpoint Manager v6.2.4 for AVAYAAURA10LAB  
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

Welcome admin | [Setup](#) | [Logout](#) |

**DASHBOARD** | **MONITOR** | **MIGRATION** | **ONBOARDING** | **MANAGEMENT** | **SETTINGS** | **CONFIGURATION**

[Firmware Upgrade](#) | [Site Redirection](#) | [Extension Conversion](#) | [Assign Profile](#) | [Registered H.323](#) | [Registered SIP](#) | [Phone Activity](#) | [Realtime Data Status](#)

**Action**  
☐ Last Query  
☒ Real Time Query

[Start System Wide Realtime Data Query](#) (May take prolonged time)

SIP Device Query Status	H.323 Device Query Status
Status: <b>NA</b> Start Time: NA Completed Time: NA	Status: <b>NA</b> Start Time: NA Completed Time: NA

[Submit](#)

Verify that the **Status** of **SIP Device Query Status** and **H.323 Device Query Status** are eventually updated to reflect **COMPLETED** as shown below, indicating successful SMS connection with Application Enablement Services and EMWS connection with Session Manager to pick up registered devices.

Endpoint Manager v6.2.4 for AVAYAAURA10LAB  
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

Welcome admin | [Setup](#) | [Logout](#) |

**DASHBOARD** | **MONITOR** | **MIGRATION** | **ONBOARDING** | **MANAGEMENT** | **SETTINGS** | **CONFIGURATION**

[Firmware Upgrade](#) | [Site Redirection](#) | [Extension Conversion](#) | [Assign Profile](#) | [Registered H.323](#) | [Registered SIP](#) | [Phone Activity](#) | [Realtime Data Status](#)

**Action**  
☐ Last Query  
☒ Real Time Query

[Start System Wide Realtime Data Query](#) (Cooling off for 5 minutes since last completion time)

SIP Device Query Status	H.323 Device Query Status
Status: <b>COMPLETED</b> Start Time: 2022-11-01 12:12:24 Completed Time: 2022-11-01 12:12:29 Avaya SMGR: 2 device, 2 verified. <a href="#">Start Query</a>	Status: <b>COMPLETED</b> Start Time: 2022-11-01 12:12:24 Completed Time: 2022-11-01 12:12:41 Avaya CM: 2 devices, 2 verified. <a href="#">Start Query</a>

[Submit](#)

### 8.3. Manage H.323 Endpoints

Select **Registered H.323** from the top to display the **H.323 Device Registration Data** screen.

A list of registered H.323 endpoints picked up from the SMS interface is displayed. Select the desired endpoints to manage as shown below. Set **Action Type** to **Add Device** and click **Submit** in the far right of the screen (not shown).

[Extension Conversion](#) | [Assign Profile](#) | **[Registered H.323](#)** | [Registered SIP](#) | [Phone Activity](#) | [Realtime Data Status](#)

### H.323 Device Registration Data

[View Messages](#)

OR

Search By Any Record Value

Range Segments: 1.2.0-255.0-255  
Wildcard Segments: 10.10.10.\*; 192.168.1.\*; 10.22.\*.\*  
CIDR Network Prefix Length: 10.10.0.0/16; 192.168.0.0/24

20 ▾ Per Page, Page 1 of 1  
Total Count: 3 (\* [Export](#) Table data in CSV format)

MAC Address	Extension	Display Name	IP Address	Model	Device Version (EM Version)	Serving Site	CM (CM IP)
<input checked="" type="checkbox"/> 70:38:EE:C9:D5:18*	65000	CM Supervisor	192.168.200.212	9611	6.8	AVAYA TEST	Avaya CM (10.64.101.236)
<input checked="" type="checkbox"/> C8:1F:EA:97:9B:B9*	65001	H323 Staff	192.168.200.179	9611	6.8	AVAYA TEST	Avaya CM (10.64.101.236)

[Check All](#) [Clear All](#)

Action Type:

Device Group (optional):

Device Profile (optional):

Model Profile (optional):

ERLocation (optional):



## 8.4. Manage SIP Endpoints

Select **Registered SIP** from the top to display the **SIP Device Registration Data** screen.

A list of registered SIP endpoints picked up from the EMWS interface is displayed. Select the desired endpoints to manage as shown below. Set **Action Type** to **Add Device** and click **Submit** in the far right of the screen (not shown).

[Extension Conversion](#) | [Assign Profile](#) | [Registered H.323](#) | **[Registered SIP](#)** | [Phone Activity](#) | [Realtime Data Status](#)

### SIP Device Registration Data

[View Messages](#)

OR

Search By Any Record Value

Range Segments: 1.2.0-255.0-255  
Wildcard Segments: 10.10.10.\* 192.168.1.\* 10.22.\*  
CIDR Network Prefix Length: 10.10.0.0/16;192.168.0.0/24

20 ▼ Per Page, Page 1 of 1  
Total Count: 2 (\*) [Export](#) Table data in Excel format)

MAC Address	Extension	Display Name	IP Address	SIP Login (Handle)	Device Version (EM Version)	Model	Serving Site (SIP Domain)	SM (System Name)
<input checked="" type="checkbox"/> <a href="#">B4:B0:17:84:06:18</a> *	66005	SIP 5, Avaya	192.168.200.144	66005@dr220.com (66005@dr220.com)	7.1.15.0.14 (96x1-IPT-SIP-R7_1_15_0-021022)	96x1	AVAYA TEST (dr220.com)	Avaya SM (DR-SM)
<input checked="" type="checkbox"/> <a href="#">C8:1F:EA:82:36:0A</a> *	66006	SIP 6, Avaya	192.168.200.169	66006@dr220.com (66006@dr220.com)	4.0.13.0.6 (J100-IPT-SIP-R4_0_13_0-071322)	J169	AVAYA TEST (dr220.com)	Avaya SM (DR-SM)

[Check All](#) [Clear All](#) Action Type:  ▼

Device Group (optional):  ▼

Device Profile (optional):  ▼

Model Profile (optional):  ▼

ERLocation (optional):  ▼

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, System Manager, and ONCENTS.

### 9.1. Verify SMS

Log into the System Access Terminal of Communication Manager. Use the **list registered-ip-stations** command to display a list of registered H.323 stations as shown below.

```
list registered-ip-stations
```

```
REGISTERED IP STATIONS

Station Ext      Set Type/  Prod ID/   Station IP Address/
or Orig Port     Net Rgn   Release    Gatekeeper IP Address
Socket
65000            9611      IP_Phone   192.168.200.212
tls              1         6.8        10.64.101.236
65001            9611      IP_Phone   192.168.200.179
tls              1         6.8        10.64.101.236
```

From the ONCENTS web interface, follow the procedures in **Section 8.3** to display an updated list of registered H.323 endpoints. Verify that the number of entries match to the **list registered-ip-stations** command output above on Communication Manager. Note that a subset of the parameter value is obtained from the SMS interface.

Endpoint Manager v6.2.4 for AVAYAAURA10LAB

U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

MIGRATION

ONBOARDING

MANAGEMENT

SETTINGS

CONFIGURATION

[Extension Conversion](#) | [Assign Profile](#) | [Registered H.323](#) | [Registered SIP](#) | [Phone Activity](#) | [Realtime Data Status](#)

### H.323 Device Registration Data

[View Messages](#)

OR

Search By Any Record Value

Range Segments: 1.2.0-255.0-255  
Wildcard Segments: 10.10.10.\*; 192.168.1.\*; 10.22.\*.\*  
CIDR Network Prefix Length: 10.10.0.0/16; 192.168.0.0/24

20

 Per Page, Page 1 of 1

Total Count: 3 (\* [Export](#) Table data in CSV format)

MAC Address	Extension	Display Name	IP Address	Model	Device Version (EM Version)	Serving Site	CM (CM IP)
<input type="checkbox"/> 70:38:EE:C9:D5:18	65000	CM Supervisor	192.168.200.212	9611	6.8	AVAYA TEST	Avaya CM (10.64.101.236)
<input type="checkbox"/> C8:1F:EA:97:9B:B9	65001	H323 Staff	192.168.200.179	9611	6.8	AVAYA TEST	Avaya CM (10.64.101.236)

From the System Manager web interface from **Section 7.2**, select **Elements → Session Manager → System Status → User Registrations** from the top menu to display a list of SIP endpoints. Note the users that are registered with a check in the **Registered Prim** column.

Users

Elements

Services

Widgets

Shortcuts

Search

Aura® System Manager 10.1

Home

Session Manager

S...

User Registrations

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

View

Default

Export

Force Unregister

AST Device Notifications:

Reboot

Reload

Fallback

As of 3:23 PM

Advanced Search

8 Items

Show

All

Filter: Enable

	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered				
											Prim	Sec	3rd	4th	Surv
<input type="checkbox"/>	► Show	---	SIPRW 9	Avaya	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	66005@dr220.com	SIP 5	Avaya	DR-Loc	192.168.200.144	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	66006@dr220.com	SIP 6	Avaya	DR-Loc	192.168.200.169	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Follow the procedures in **Section 8.4** to display an updated list of registered SIP endpoints. Verify that the number of entries match to the registered entries from the **User Registrations** screen above. Note that a subset of the parameter value is obtained from the EMWS interface.

## SIP Device Registration Data

[View Messages](#)

OR

Search By Any Record Value

Range Segments: 1.2.0-255.0-255  
 Wildcard Segments: 10.10.10.\*; 192.168.1.\*; 10.22.\*.\*  
 CIDR Network Prefix Length: 10.10.0.0/16; 192.168.0.0/24

Per Page, Page 1 of 1  
 Total Count: 2 (\* [Export](#) Table data in Excel format)

MAC Address	Extension	Display Name	IP Address	SIP Login (Handle)	Device Version (EM Version)	Model	Serving Site (SIP Domain)	SM (System Name)
<input type="checkbox"/> <a href="#">B4:B0:17:84:06:18</a>	66005	SIP 5, Avaya	192.168.200.144	66005@dr220.com (66005@dr220.com)	7.1.15.0.14 (96x1-IPT-SIP-R7_1_15_0-021022)	96x1	AVAYA TEST (dr220.com)	Avaya SM (DR-SM)
<input type="checkbox"/> <a href="#">C8:1F:EA:82:36:0A</a>	66006	SIP 6, Avaya	192.168.200.169	66006@dr220.com (66006@dr220.com)	4.0.13.0.6 (J100-IPT-SIP-R4_0_13_0-071322)	J169	AVAYA TEST (dr220.com)	Avaya SM (DR-SM)

### 9.3. Verify PUSH

Select **MONITOR** from the top menu to display a list of monitored devices shown below. Scroll the screen to the right and click on the **Re-echo** option (not shown) associated with a desired entry, in this case the **SIP** device with IP address of **192.168.200.169**.

Endpoint Manager v6.2.4 for AVAYAAURA10LAB							
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342							
MIGRATION ONBOARDING MANAGEMENT SETTINGS CONFIGURATION							
EM Device - Extension [*]							
100 Per Page, Page 1 of 1							
Result Count: 4 Last Update: 2022-10-20 15:15:14 (* Export Table data in CSV format )							
MAC Address	Device Name	Extension	Display Name	SIP Login	Serial	IP Address (Private IP)	Model (HW Version)
<input type="checkbox"/> 70:38:EE:C9:D5:18		65000	CM Supervisor		12WZ123602DR	192.168.200.212 (192.168.200.212) (1)	9611GD01A
<input type="checkbox"/> C8:1F:EA:97:9B:B9		65001	H323 Staff		18WZ44600471	192.168.200.179 (192.168.200.179) (2)	J179D02A
<input type="checkbox"/> B4:B0:17:84:06:18		66005	SIP 5, Avaya	66005@dr220.com	10WZ50461481	192.168.200.144 (192.168.200.144) (0)	9641GD01A
<input type="checkbox"/> C8:1F:EA:82:36:0A		66006	SIP 6, Avaya	66006@dr220.com	18WZ125008L1	192.168.200.169 (192.168.200.169) (1)	J169D01A

Use Wireshark to capture packets in and out of the selected device. Verify that the packet capture shows a **POST /forms/push** packet from ONCENTS server with IP address **10.64.101.208** and **GET /subscribe** packets from the SIP device with IP address **192.168.200.169** as shown below.

wireshark-em-aura101-sip-j169-phn28-push-em624.pcapng							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
http							
No.	Time	Source	Destination	Protocol	Length	Info	
1452	10:12:34.389217	10.64.101.208	192.168.200.169	HTTP	223	POST /forms/push HTTP/1.1 (application/x-www-form-urlencoded)	
1455	10:12:34.479307	192.168.200.169	10.64.101.208	HTTP	355	HTTP/1.1 200 OK (text/html)	
1458	10:12:34.525444	192.168.200.169	10.64.101.208	HTTP	303	GET /subscribe1.do?action=resubscribe HTTP/1.1	
1464	10:12:34.584455	10.64.101.208	192.168.200.169	HTTP/XML	305	HTTP/1.1 200 OK	
1469	10:12:34.661034	192.168.200.169	10.64.101.208	HTTP	367	GET /subscribe1.do?MAC=c8%3A1f%3Aea%3A82%3A36%3A0a&Extn=66006&	
1471	10:12:34.736870	10.64.101.208	192.168.200.169	HTTP	438	HTTP/1.1 200 OK	
1518	10:12:37.115800	10.64.101.208	192.168.200.20	HTTP	427	HTTP/1.1 200 OK (text/html)	
1519	10:12:37.121982	192.168.200.20	10.64.101.208	HTTP	626	GET /images/ajax-loader.gif HTTP/1.1	
1525	10:12:37.187782	10.64.101.208	192.168.200.20	HTTP	665	HTTP/1.1 200 OK (GIF89a)	

Note that necessary phone settings for PUSH integration with ONCENTS are taken care of by ONCENTS as part of the file server capability, and the settings need to include PUSH parameters **PUSHCAP**, **PUSHPORT**, **PUSH\_MODE**, **SUBSCRIBELIST**, and **TPSLIST**. The screenshot below shows the values used for these parameters in the compliance testing.

PUSHCAP	22222
PUSHPORT	80
PUSH_MODE	0
SDPCAPNEG	1
SIG	2
SIPDOMAIN	dr220.com
SIPPROXYSRVR	"10.64.101.238"
SIP_CONTROLLER_LIST	10.64.101.238:5061;transport=tls
SIP_PORT_SECURE	5061
SNMPADD	10.64.101.208
SNMPSTRING	mystring
SSH_ALLOWED	0
STATIC	0
SUBSCRIBELIST	http://10.64.101.208/subscribe1.do
TLSSVR	"10.64.101.238"
TLSSVRID	1
TPSLIST	10.64.101.208

## 9.4. Verify SNMP

Select **MONITOR** from the top menu to display a list of monitored devices shown below. Scroll the screen to the right and click on the **Query** option (not shown) associated with a desired entry, in this case the **H.323** device with IP address of **192.168.200.179**.

Endpoint Manager v6.2.4 for AVAYAAURA10LAB  
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

MIGRATION ONBOARDING MANAGEMENT SETTINGS CONFIGURATION

EM Device - Extension [\*]

100 ▾ Per Page, Page 1 of 1  
Result Count: 4 Last Update: 2022-10-20 15:15:14 (\* Export Table data in CSV format )

MAC Address	Device Name	Extension	Display Name	SIP Login	Serial	IP Address (Private IP)	Model (HW Version)
<input type="checkbox"/> 70:38:EE:C9:D5:18		65000	CM Supervisor		12WZ123602DR	192.168.200.212 (192.168.200.212) (1)	9611GD01A
<input type="checkbox"/> C8:1F:EA:97:9B:B9		65001	H323 Staff		18WZ44600471	192.168.200.179 (192.168.200.179) (2)	J179D02A



Use Wireshark to capture packets in and out of the selected device. Verify that the packet capture shows **SNMP get-request** packets from ONCENTS server with IP address **10.64.101.208** and **SNMP get-response** packets from the H.323 device with IP address **192.168.200.179** as shown below.

The image shows a Wireshark packet capture window titled "wireshark-em-aura101-h323-j179-phn41-snmppcapng". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for packet capture and analysis. The packet list pane on the left shows a filter "snmp" and a list of 14 packets. The packet details pane on the right shows the selected packet (No. 231) with its structure: Ethernet II, Internet Protocol Version 4, and Simple Network Management Protocol (SNMP). The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
231	16:05:28.507386	10.64.101.208	192.168.200.179	SNMP	189	get-request 1.3.6.1.4.1.6889.2.69.5.1.72.0 1.3.6.1.4.1.6889.2.69.5.1.72.0
234	16:05:28.507386	192.168.200.179	10.64.101.208	SNMP	207	get-response 1.3.6.1.4.1.6889.2.69.5.1.72.0 1.3.6.1.4.1.6889.2.69.5.1.72.0
268	16:05:28.559612	10.64.101.208	192.168.200.179	SNMP	92	get-request 1.3.6.1.4.1.6889.2.69.5.1.74.0
273	16:05:28.563255	192.168.200.179	10.64.101.208	SNMP	100	get-response 1.3.6.1.4.1.6889.2.69.5.1.74.0
298	16:05:28.617228	10.64.101.208	192.168.200.179	SNMP	149	get-request 1.3.6.1.4.1.6889.2.69.5.6.4.0 1.3.6.1.4.1.6889.2.69.5.6.4.0
299	16:05:28.620931	192.168.200.179	10.64.101.208	SNMP	154	get-response 1.3.6.1.4.1.6889.2.69.5.6.4.0 1.3.6.1.4.1.6889.2.69.5.6.4.0
424	16:05:28.725342	10.64.101.208	192.168.200.179	SNMP	149	get-request 1.3.6.1.4.1.6889.2.69.5.6.1.0 1.3.6.1.4.1.6889.2.69.5.6.1.0
425	16:05:28.729206	192.168.200.179	10.64.101.208	SNMP	162	get-response 1.3.6.1.4.1.6889.2.69.5.6.1.0 1.3.6.1.4.1.6889.2.69.5.6.1.0
492	16:05:28.851073	10.64.101.208	192.168.200.179	SNMP	189	get-request 1.3.6.1.4.1.6889.2.69.5.1.79.0 1.3.6.1.4.1.6889.2.69.5.1.79.0
499	16:05:28.855138	192.168.200.179	10.64.101.208	SNMP	201	get-response 1.3.6.1.4.1.6889.2.69.5.1.79.0 1.3.6.1.4.1.6889.2.69.5.1.79.0
559	16:05:28.939177	10.64.101.208	192.168.200.179	SNMP	113	get-request 1.3.6.1.4.1.6889.2.69.5.1.129.0 1.3.6.1.4.1.6889.2.69.5.1.129.0
568	16:05:28.945419	192.168.200.179	10.64.101.208	SNMP	114	get-response 1.3.6.1.4.1.6889.2.69.5.1.129.0 1.3.6.1.4.1.6889.2.69.5.1.129.0

Note that necessary phone settings for SNMP integration with ONCENTS are taken care of by ONCENTS as part of the file server capability, and the settings need to include SNMP parameters **SNMPADD** and **SNMPSTRING**. The screenshot below shows the values used for these parameters in the compliance testing.

SIP_PORT_SECURE	5061
SNMPADD	10.64.101.208
SNMPSTRING	mystring
SSH_ALLOWED	0

## 10. Conclusion

These Application Notes describe the configuration steps required for iNEMSOFT ONCENTS Endpoint Manager 6.2 to interoperate with Avaya Aura® Communication Manager 10.1, Avaya Aura® Application Enablement Services 10.1, Avaya Aura® System Manager 10.1, Avaya Aura® Session Manager 10.1, and Avaya IP phones. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 5, September 2022, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 7, September 2022, available at <http://support.avaya.com>.
4. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 4, September 2022, available at <http://support.avaya.com>.
5. *iNEMSOFT oncents Endpoint Manager R6.2.4 User Guide*, October 2022, available upon request to [support@inemsoft.com](mailto:support@inemsoft.com).

---

**©2022 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).