



Avaya Solution & Interoperability Test Lab

Application Notes for iNEMSOFT ONCENTS Endpoint Manager 6.1 with Avaya Aura® Communication Manager 8.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for iNEMSOFT ONCENTS Endpoint Manager 6.1 to interoperate with Avaya Aura® Communication Manager 8.1.3, Avaya Aura® Application Enablement Services 8.1.3, Avaya Aura® System Manager 8.1.3, Avaya Aura® Session Manager 8.1.3, 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 6.1 to interoperate with Avaya Aura® Communication Manager 8.1.3, Avaya Aura® Application Enablement Services 8.1.3, Avaya Aura® System Manager 8.1.3, Avaya Aura® Session Manager 8.1.3, and Avaya IP phones.

In the compliance testing, five 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.
- User Management Web Services (UMWS) with System Manager to obtain SIP user profile detail including name of associated Communication Manager.
- PUSH interface with Avaya IP phones to obtain subscription data including IP, MAC, model, and extension.
- SNMP interface with Avaya IP phones to obtain phone information including MAC, type, serial number, and sometimes the associated call server. Note that the call server setting isn't obtained by ONCENTS for all phone types and any needed MIB file for the phones are pre-taken care of and built into ONCENTS. The SNMP version used by ONCENTS is version 2c.

ONCENTS also serves as the file server for Avaya IP phones for necessary phone settings and upload/download of phone firmware. The file server integration does not utilize any Avaya published API and therefore is outside the scope of the compliance test.

The compliance testing used 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, EMWS, and UMWS. 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 UMWS to obtain Communication Manager name from the SIP user profile.
- Use of PUSH Subscribe to obtain phone IP address, MAC, model, and extension.
- Use of SNMP to obtain phone MAC, type, serial number, and associated call server where applicable.

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 on ONCENTS from the compliance testing.

- The current release of ONCENTS does not perform certificate validation for EMWS and UMWS connections.
- Usage of SNMP included obtainment of call server information from all IP phones used in the testing except J179 H.323. This has been addressed by iNEMSOFT but was not verified as part of the compliance test.

2.3. Support

Technical support on ONCENTS can be obtained through the following:

- **Phone:** (214) 423-2815
- **Email:** 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.

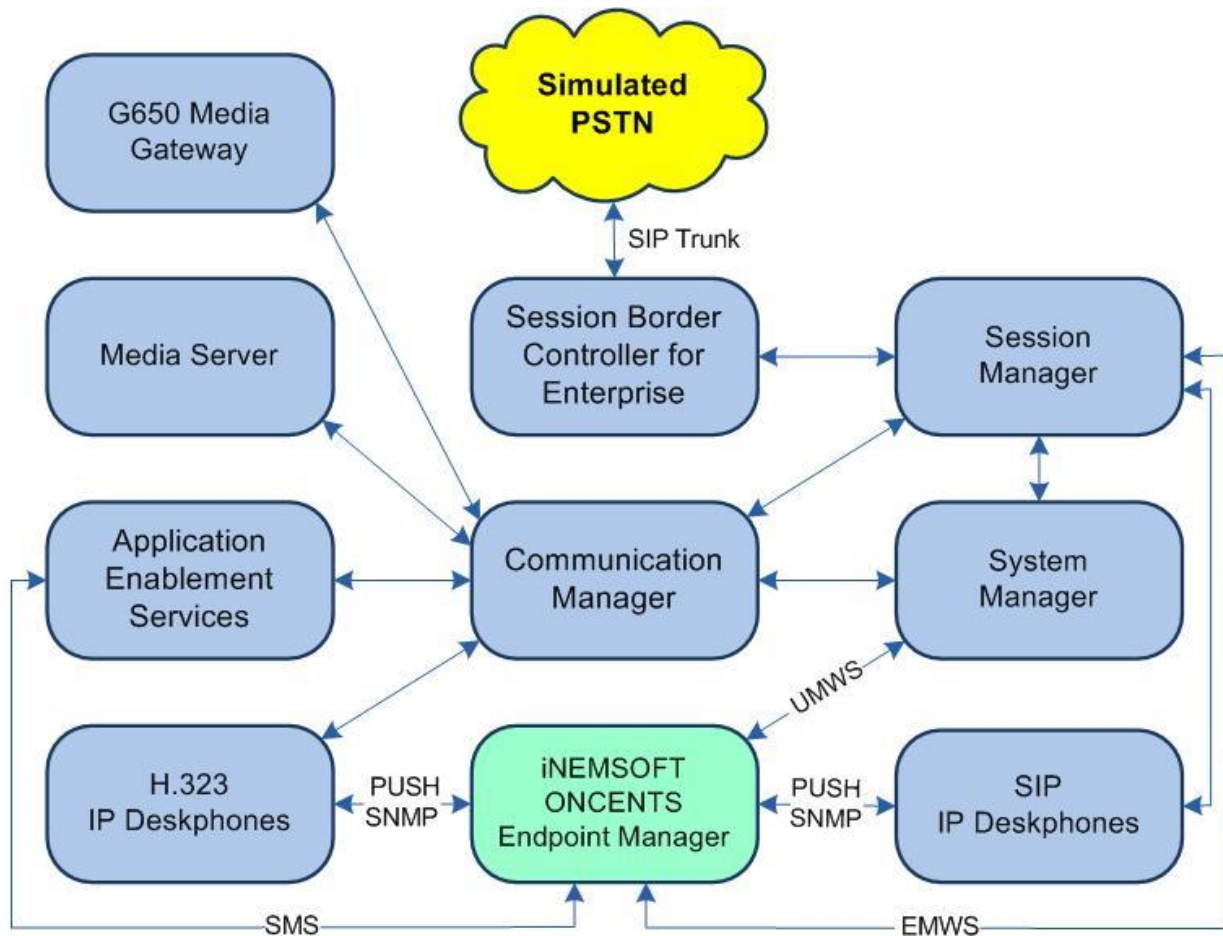


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

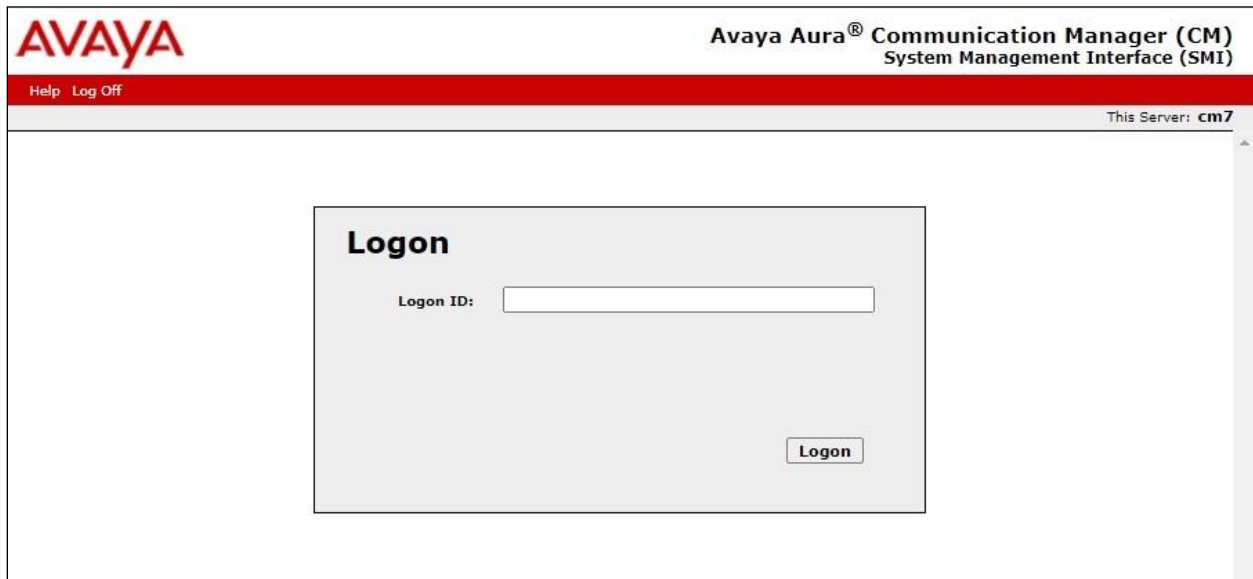
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3 (8.1.3.0.0.25-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya 9611G & J179 IP Deskphone (H.323)	6.8502
Avaya 9641G IP Deskphone (SIP)	7.1.11.0.8
Avaya J169 IP Deskphone (SIP)	4.0.7.1.5
iNEMSOFT ONCENTS on CentOS Linux	6.1.0 8.2.2004

5. Configure Avaya Aura® Communication Manager

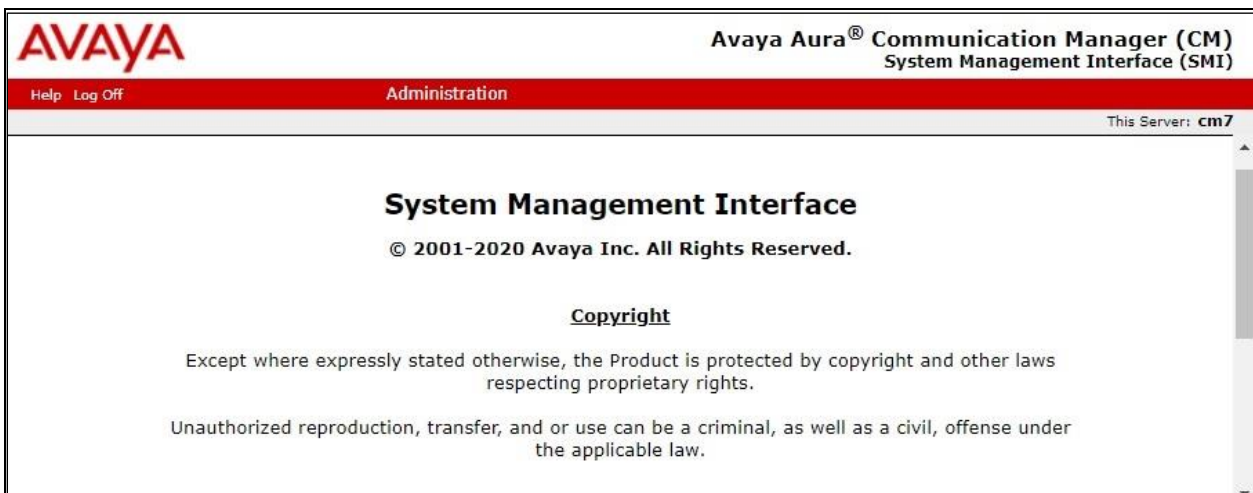
This section provides the procedure for configuring Communication Manager. The procedure involves adding an administrative user to be used by ONCENTS for SMS integration.

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 header includes the Avaya logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and navigation links "Help" and "Log Off". A status bar indicates "This Server: cm7". The main content area features a "Logon" box with a "Logon ID:" label, a text input field, and a "Logon" button.

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

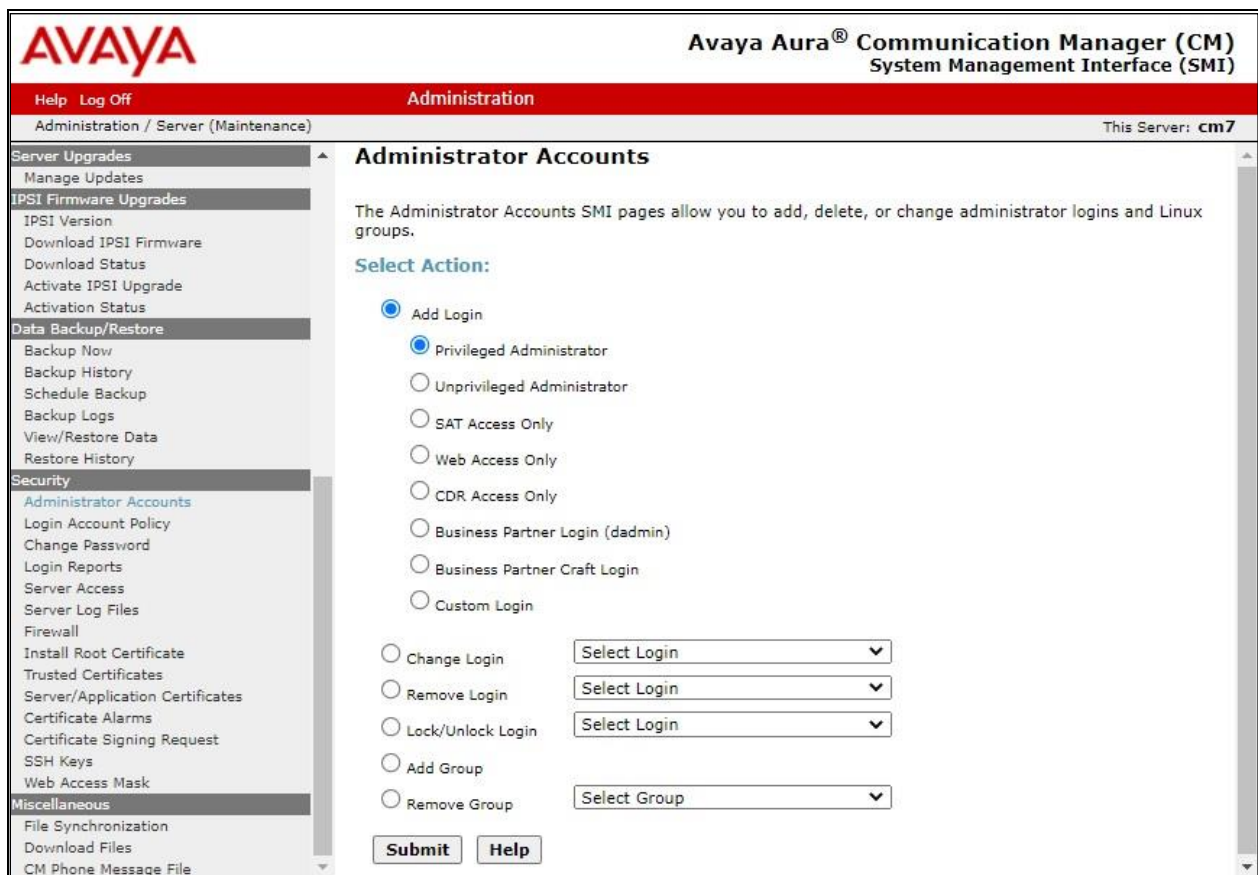


The screenshot shows the Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Administration screen. The header includes the Avaya logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and navigation links "Help" and "Log Off". A status bar indicates "This Server: cm7". The main content area features the title "System Management Interface", the copyright notice "© 2001-2020 Avaya Inc. All Rights Reserved.", and 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.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration page. The top navigation bar includes 'Help', 'Log Off', and 'Administration'. The breadcrumb trail is 'Administration / Server (Maintenance)'. The page title is 'Administrator Accounts -- Add Login: Privileged Administrator'. The left sidebar contains a tree view with categories: 'Server Upgrades' (Manage Updates), 'IPSI Firmware Upgrades' (IPSI Version, Download IPSI Firmware, Download Status, Activate IPSI Upgrade, Activation Status), 'Data Backup/Restore' (Backup Now, Backup History, Schedule Backup, Backup Logs, View/Restore Data, Restore History), 'Security' (Administrator Accounts, Login Account Policy, Change Password, Login Reports, Server Access, Server Log Files, Firewall, Install Root Certificate, Trusted Certificates, Server/Application Certificates, Certificate Alarms, Certificate Signing Request, SSH Keys, Web Access Mask), and 'Miscellaneous' (File Synchronization, Download Files). The main content area has a description: '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.' The form fields are: 'Login name' (inemsoft), 'Primary group' (susers), 'Additional groups (profile)' (prof18), 'Linux shell' (/bin/bash), 'Home directory' (/var/home/inemsoft), 'Lock this account' (checkbox), 'SAT Limit' (none), 'Date after which account is disabled-blank to ignore (YYYY-MM-DD)' (empty), 'Enter password' (masked with dots), 'Re-enter password' (masked with dots), and 'Force password change on next login' (radio buttons for No and Yes, with 'No' selected). At the bottom are 'Submit', 'Cancel', and 'Help' buttons.

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.			
Server Upgrades	Login name	inemsoft	
Manage Updates	Primary group	susers	
IPSI Firmware Upgrades	Additional groups (profile)	prof18	
IPSI Version	Linux shell	/bin/bash	
Download IPSI Firmware	Home directory	/var/home/inemsoft	
Download Status	Lock this account	<input type="checkbox"/>	
Activate IPSI Upgrade	SAT Limit	none	
Activation Status	Date after which account is disabled-blank to ignore (YYYY-MM-DD)		
Data Backup/Restore	Enter password	
Backup Now	Re-enter password	
Backup History	Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes	
Schedule Backup			
Backup Logs			
View/Restore Data			
Restore History			
Security			
Administrator Accounts			
Login Account Policy			
Change Password			
Login Reports			
Server Access			
Server Log Files			
Firewall			
Install Root Certificate			
Trusted Certificates			
Server/Application Certificates			
Certificate Alarms			
Certificate Signing Request			
SSH Keys			
Web Access Mask			
Miscellaneous			
File Synchronization			
Download Files			
	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. Below this bar is a central login box with a light gray background. Inside the box, the text "Please login here:" is followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 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 Jul 12 16:45:54 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Jul 13 08:52:12 EDT 2021
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. Scroll down to the **SMS Proxy Ports** 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 “4106-4116” were used in the compliance testing as shown below.

AVAYA Application Enablement Services
Management Console

Welcome: User
Last login: Mon Jul 12 16:45:54 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Jul 13 08:52:12 EDT 2021
HA Status: Not Configured

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager

▶ Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

Enabled Disabled

Enabled Disabled

Enabled Disabled

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

Server Media

RTP Local UDP Port Min*30000

RTP Local UDP Port Max*49999

* Note: The number of RTP ports needs to be double the number of extensions using server media.

SMS Proxy Ports

Proxy Port Min4101

Proxy Port Max4116

Apply Changes

Restore Defaults

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 and the text "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Mon Jul 12 16:45:54 2021 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: 8.1.3.0.0.25-0", "Server Date and Time: Tue Jul 13 08:52:12 EDT 2021", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "AE Services | SMS | SMS Properties" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services" (expanded), "CVLAN", "DLG", "DMCC", "SMS" (expanded), "SMS Properties" (selected), "TSAPI", "TWS", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", and "Security".

The right pane displays the "SMS Properties" configuration form. The fields and their values are as follows:

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 with columns: Alias, Status, Issued To, Issued By, and Expiration Date. The 'SystemManagerCA' certificate is selected and highlighted.

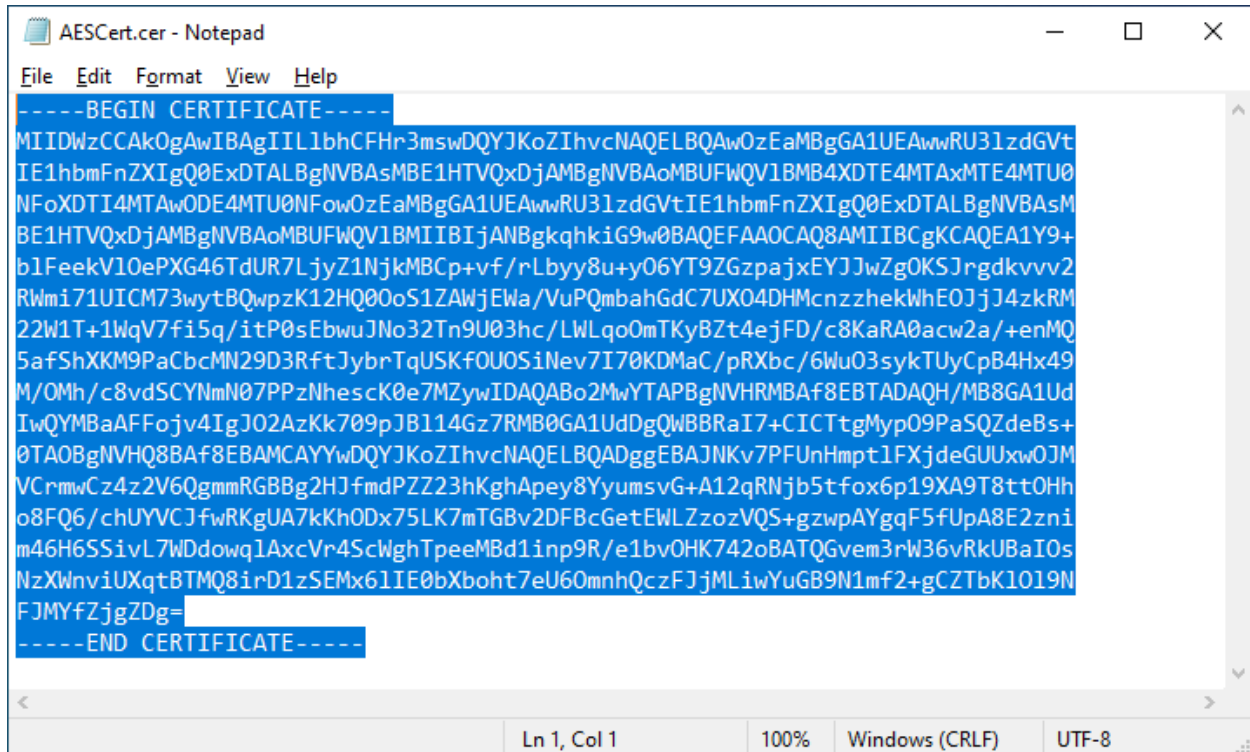
Alias	Status	Issued To	Issued By	Expiration Date
serverCertDefault	expired	aes7-081738682-labUseOnly	aes7-081738682-labUseOnly	Aug 5, 2020
avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027
SystemManagerCA	valid	System Manager CA	System Manager CA	Oct 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. It shows the 'Issued To' and 'Issued By' fields as 'System Manager CA' and the 'Expiration Date' as 'Oct 8, 2028'. Below this, the 'Certificate PEM' section displays a large text box containing the certificate data, starting with '-----BEGIN CERTIFICATE-----'.

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwRU3lzdG
IE1hbmFnZXIgaQ00ExDTALBgNVBAsMBE1HTVQxXDJAMBGNVBAoMBUFWQVIBMB4XDTE4MTAxMTE4
NFOxDTI4MTAwODE4MTU0NFOwOzEaMBGGA1UEAwRU3lzdGVtIE1hbmFnZXIgaQ00ExDTALBgNVB
BE1HTVQxXDJAMBGNVBAoMBUFWQVIBMB4XDTE4MTAxMTE4NFOxDTI4MTAwODE4MTU0NFOwOzEa
bFEEKVlOePQG46TdUR7LjYz1NjkMBGGA1UEAwRU3lzdGVtIE1hbmFnZXIgaQ00ExDTALBgNVB
22W1T+1WqV7f5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKFOUOSiNev7170KDMaC/pRXbc/6Wu03sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhesck0e7MZyWIDAQABo2MwYTAPEgNVHRMBAF8EBTADAQH/MB8G
IwQYMBAAFFojv4Igo2AZKk709pJBI14Gz7RMB0GA1UdDgQWBBrA17+C1CTtgMyp09PaSQZdeBs
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKy7PFUUnHmptlFXjdeGUUxwC
VCrmwCz42V6QgmmRBBg2HJfmdPZZ23hKghApey8YyumsVG+A12qRnj5f5fox6p19XA9T8t0f
```

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



```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIIL1bhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwwRU31zdGVt
IE1hbmFnZXIgaQ0ExDTALBgNVBAsMBE1HTVQxDjAMBGNVBAoMBUFWQV1BMB4XDTE4MTAxMTE4MTU0
NFOxDTI4MTAwODE4MTU0NFowOzEaMBGGA1UEAwwRU31zdGVtIE1hbmFnZXIgaQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBGNVBAoMBUFWQV1BMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
b1FeekV10ePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpaJxYJjwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0o0S1ZAWjEwa/VuPQmbahGdC7UX04DHMczzhekWhEOJjJ4zkRM
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6Wu03sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MzywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFojv4IgJO2AzKk709pJB114Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMyp09PaSQZdeBs+
0TA0BgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmpt1FXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRGGBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8tt0Hh
o8FQ6/chUYVCJfwRKgUA7kKh0Dx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7Wddowq1AxcVr4ScWghTpeeMBd1inp9R/e1bv0HK742oBATQGvem3rW36vRKUBaIOs
NzXWnviUXqtBTMQ8irD1zSEMx61IE0bXboht7eU60mnhQczFJjMLiwYuGB9N1mf2+gCZTbK1019N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

7. Configure Avaya Aura® System Manager

This section provides the procedures for configuring System Manager for EMWS integration with Session Manager and UMWS integration with System 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.

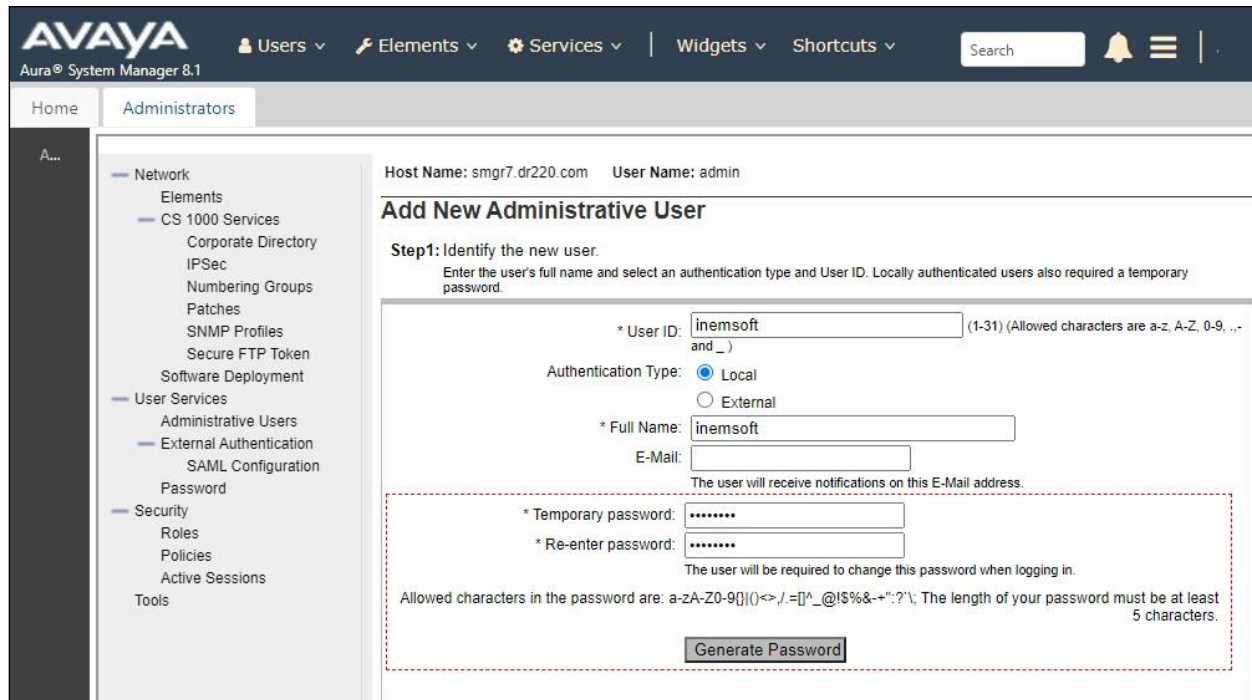
User ID:

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 and UMWS 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 8.1

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

Home Administrators

A...

- Network
 - Elements
- CS 1000 Services
 - Corporate Directory
 - IPSec
 - Numbering Groups
 - Patches
 - SNMP Profiles
 - Secure FTP Token
- Software Deployment
- User Services
 - Administrative Users
 - External Authentication
 - SAML Configuration
- Password
- Security
 - Roles
 - Policies
 - Active Sessions
- Tools

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.

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 **32 System Administrator** as shown below.

AVAYA Aura® System Manager 8.1

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

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"/> 27 Session Manager and Routing Administrator	Administrator role.
<input type="checkbox"/> 28 Session Manager and Routing Auditor	Session Manager and Routing Auditor
<input type="checkbox"/> 29 SIPAS Auditor	Gives read-only access to all SIP Foundation server management functionality.
<input type="checkbox"/> 30 SIPAS Security Administrator	Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.
<input type="checkbox"/> 31 SIPAS System Administrator	Gives read and write access to all the SIP Foundation server management functionality.
<input checked="" type="checkbox"/> 32 System Administrator	Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.
<input type="checkbox"/> 33 Tenant Administrator Template	A role for basic tenant administration functionality. It can be used as a template to build tenant specific roles.

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

You must change your temporary password to continue

New Password:

Confirm Password:

Change Cancel Reset

8. Configure iNEMSOFT ONCENTS Endpoint Manager

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

- Prepare worksheet
- Upload configuration file
- 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.

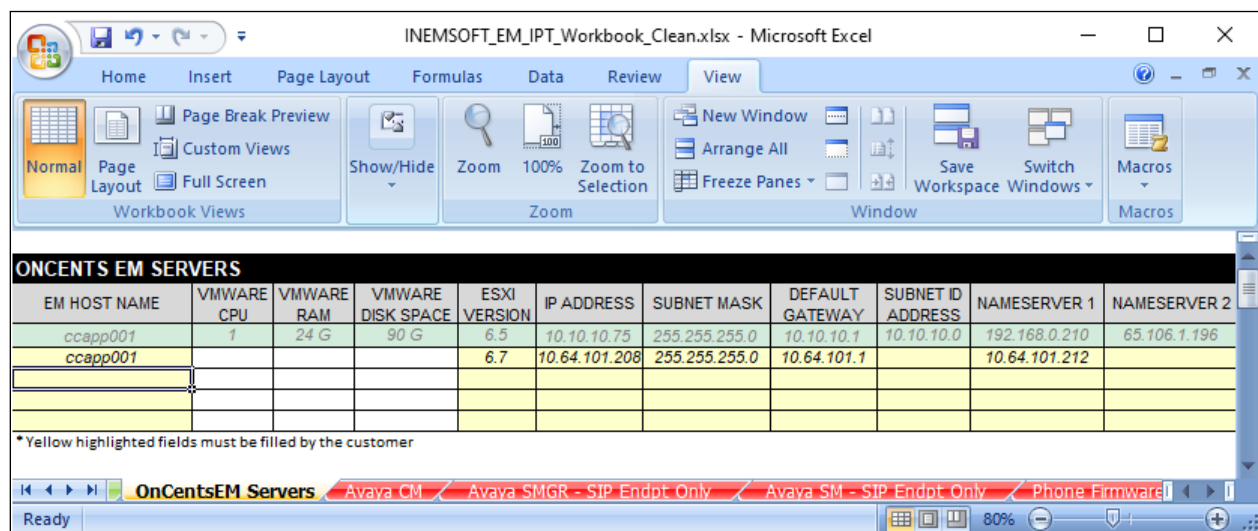
This section assumes that the CA certificate exported from Application Enablement Services in **Section 6.4** for SMS integration has been properly installed on ONCENTS, and that the SIP user profile query has been enabled on ONCENTS for customers with SIP endpoints.

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 parameters and values used in the compliance testing are described in the following section.

8.1.1. OnCentsEM Servers

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



EM HOST NAME	VMWARE CPU	VMWARE RAM	VMWARE DISK SPACE	ESXI VERSION	IP ADDRESS	SUBNET MASK	DEFAULT GATEWAY	SUBNET ID ADDRESS	NAMESERVER 1	NAMESERVER 2
ccapp001	1	24 G	90 G	6.5	10.10.10.75	255.255.255.0	10.10.10.1	10.10.10.0	192.168.0.210	65.106.1.196
ccapp001				6.7	10.64.101.208	255.255.255.0	10.64.101.1		10.64.101.212	

* Yellow highlighted fields must be filled by the customer

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

Parameter	Value	Description
EM Host Name	ccapp001	Desired host name for ONCENTS server
ESXI Version	6.7	The ESXI version where applicable
IP Address	10.64.101.208	IP address 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 **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 8.1.3	A desired name for Communication Manager
Version	8.1.3	Software version of Communication Manager
Street	350 Mount Kemble Ave	Pertinent street address
City	Morristown	Pertinent city
Zip Code	07960	Pertinent zip code
State	NJ	Pertinent state
SMS Login Username	inemsoft	Communication Manager user credential from Section 5
Secured	https	Use https for secured connection else http
Login Password	inemsoftcm	Communication Manager user credential from Section 5
Associated AES IP	10.64.101.239	IP address of Application Enablement Services

8.1.3. Avaya SMGR

Navigate to the **Avaya SMGR – SIP Endpt Only** 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
Login Username	inemsoft	System Manager user credential from Section 7.2
Login Password	iN3mLab%	System Manager user credential from Section 7.2

8.1.4. Avaya SM

Navigate to the **Avaya SM – SIP Endpt Only** 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	10.64.101.208	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

8.1.5. Bulk Phone Profile

Navigate to the **Bulk Phone Profile** tab (not shown). The parameter below was used in the compliance testing.

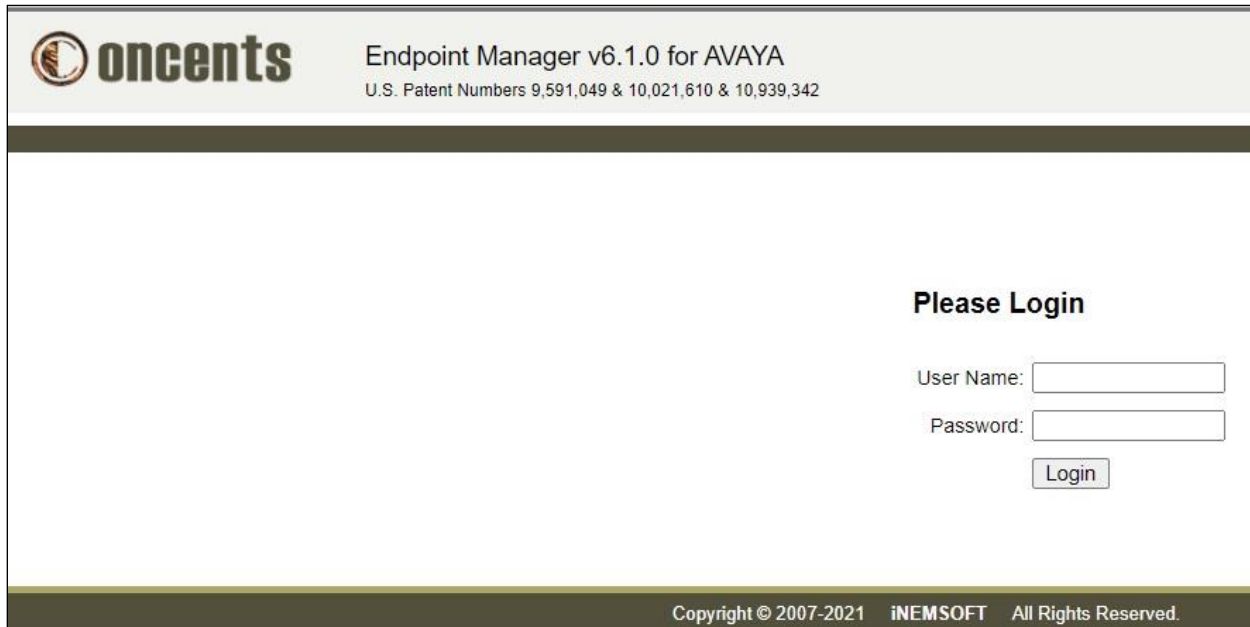
Parameter	Value	Description
Phone SNMP Query String	inemsoft	A desired community string

8.2. Upload Configuration File

A configuration file is created by iNEMSOFT based on the worksheet data from **Section 8.1** provided by the customer.

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 “AVAYA” 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. At the top left is the ONCENTS logo. To its right, the text reads "Endpoint Manager v6.1.0 for AVAYA" and "U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342". The main content area is titled "Please Login". Below this title are two input fields: "User Name:" and "Password:". Below the password field is a "Login" button. At the bottom of the page, a footer contains the text "Copyright © 2007-2021 iNEMSOFT All Rights Reserved."

In the subsequent screen, select **Setup → Host Admin** (not shown) from the upper right corner to display the **ClassOne® MidTier Web Administration** screen below.

Select **CONFIGURATION**.




The screenshot shows the ONCENTS web interface after selecting "CONFIGURATION". At the top left is the ONCENTS logo. To its right, the text reads "Endpoint Manager v6.1.0 for AVAYA" and "U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342". Below this is a navigation bar with four tabs: "OA&M", "UTILITIES", "CONFIGURATION", and "SNMP". The "CONFIGURATION" tab is selected. Below the navigation bar, on the left, is a sidebar with links: "OA&M", "Utilities", "Configuration", and "SNMP". The main content area is titled "ClassOne® MidTier Web Administration". Below this title is a bullet point: "• OA&M (Operations, Administration, and Maintenance)". Below the bullet point is the text: "Provides access to process control and operation information display of the ClassOne® Endpoint".

Select **Process**. For **Action Type**, select **Configure From File** to display the **Create Processes and Configurations From a File** screen.

Select **Choose File** and navigate to the zipped configuration file from iNEMSOFT as shown below. Click **Create Processes**.

After the configuration file is uploaded with processes created, manually log into the Linux shell of the ONCENTS server and restart the **classone** service.



oncents Endpoint Manager v6.1.0 for AVAYA
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

OA&M UTILITIES **CONFIGURATION** SNMP

Process | Web User | Access Control

Action Type:
Configure From File ▼

Submit

Create Processes and Configurations From a File

Please upload a liscened encrypted configuration zip file.

Choose File No file chosen
x EMConfigApplianceTest.zip

Password:

Create Processes

Copyright © 2007-2021 iNEMSOFT All Rights Reserved.

8.3. Manage H.323 Endpoints

Select **Setup** → **Device Admin** (not shown) from the upper right corner of screen, followed by **MIGRATION** → **Registered H.323** to display the **Registered H.323 Devices** screen.

Select the pertinent Communication Manager in the left pane, in this case “CM 8.1.3”, and check **Get Realtime Data** as shown below. Click **Submit**.

Endpoint Manager v6.1.0 for AVAYA
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

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

[Firmware Upgrade](#) | [Site Redirection](#) | [Extension Conversion](#) | **[Registered H.323](#)** | [Registered SIP](#) | [Phone Activity](#) |

CM:
CM 8.1.3
☒ Get Realtime Data
☐ Unmanaged Only
Submit

Registered H.323 Devices

- About**
Entry point to retrieve live registration data from CM for H.323 devices.

The screen is updated with a list of registered H.323 endpoints picked up from the SMS interface. 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).

EM Device - Registered H.323

[View Messages](#)

H.323 Device Registration Data

Search Value ... OR Search IP Range/Wildcard/CIDR ...
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 CSV format)

MAC Address	Extension	Display Name	IP Address	Model	Device Version (EM Version)	Serving Site	CM (CM IP)
<input checked="" type="checkbox"/> C8:1F:EA:97:9B:B9 *	65000	CM Supervisor	192.168.200.179	9611	6.8502	DevConnect	CM 8.1.3 (10.64.101.236)
<input checked="" type="checkbox"/> 70:38:EE:C9:D5:18 *	65001	CM Station 1	192.168.200.212	9611	6.8502	DevConnect	CM 8.1.3 (10.64.101.236)

[Check All](#) [Clear All](#)
Action Type: Add Device
Device Group (optional): Please
Device Profile (optional): Please
Model Profile (optional): Please

8.4. Manage SIP Endpoints

Select **MIGRATION** → **Registered SIP** to display the **Registered SIP Devices** screen.

Select the pertinent System Manager in the left pane, in this case “SMGR 8.1.3”, and check **Get Realtime Data** as shown below. Click **Submit**.

ONCENTS Endpoint Manager v6.1.0 for AVAYA
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

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

[Firmware Upgrade](#) | [Site Redirection](#) | [Extension Conversion](#) | [Registered H.323](#) | [Registered SIP](#) | [Phone Activity](#)

SMGR:
SMGR 8.1.3
☒ Get Realtime Data
☐ Unmanaged Only
Submit

Registered SIP Devices

- About**
Entry point to retrieve live registration data from SMGR for AST SIP devices.

The screen is updated with a list of registered SIP endpoints picked up from the EMWS interface. 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).

EM Device - Registered SIP

[View Messages](#)

SIP Device Registration Data

Search Value ... OR Search IP Range/Wildcard/CIDR ... **Q**

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"/> B4:B0:17:84:06:18 *	66002	SIP 2, Avaya	192.168.200.144	66002@dr220.com (66002@dr220.com)	7.1.11.0.8	96x1	(dr220.com)	(DR-SM)
<input checked="" type="checkbox"/> C8:1F:EA:82:36:0A *	66006	SIP 6, Avaya	192.168.200.163	66006@dr220.com (66006@dr220.com)	4.0.7.1.5	J169	(dr220.com)	(DR-SM)

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

Action Type: **Add Device**

Device Group (optional):
Device Profile (optional):
Model Profile (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  192.168.200.179
tls             1       6.8511    10.64.101.236
65001           9611    IP_Phone  192.168.200.212
tls             1       6.8502    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 endpoint. 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 v6.1.0 for AVAYA
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

MIGRATION

ONBOARDING

MANAGEMENT

SETTINGS

CONFIGURATION

tion | [Extension Conversion](#) | [Registered H.323](#) | [Registered SIP](#) | [Phone Activity](#) |

EM Device - Registered H.323

[View Messages](#)

H.323 Device Registration Data

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 CSV format)

MAC Address	Extension	Display Name	IP Address	Model	Device Version (EM Version)	Serving Site	CM (CM IP)
<input type="checkbox"/> C8:1F:EA:97:9B:B9	65000	CM Supervisor	192.168.200.179	9611	6.8511 (96x1-IPT-H323-R6_8_5_11-050321)	DevConnect	CM 8.1.3 (10.64.101.236)
<input type="checkbox"/> 70:38:EE:C9:D5:18	65001	CM Station 1	192.168.200.212	9611	6.8502 (96x1-IPT-H323-R6_8_5_02-110720)	DevConnect	CM 8.1.3 (10.64.101.236)

9.2. Verify EMWS

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.

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 12:49 PM Advanced Search

7 Items Show All Filter: Enable

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered
										Prim Sec Surv Visiting
Show	---	SIP 7	Avaya	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Show	66002@dr220.com	SIP 2	Avaya	DR-Loc	192.168.200.144	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC) <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Show	66006@dr220.com	SIP 6	Avaya	DR-Loc	192.168.200.163	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC) <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

Search Value ... OR Search IP Range/Wildcard/CIDR ... Q

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 type="checkbox"/> B4:B0:17:84:06:18	66002	SIP 2, Avaya	192.168.200.144	66002@dr220.com (66002@dr220.com)	7.1.11.0.8 (96x1-IPT-SIP-R7_1_11_0-092520)	96x1	(dr220.com)	(DR-SM)
<input type="checkbox"/> C8:1F:EA:82:36:0A	66006	SIP 6, Avaya	192.168.200.163	66006@dr220.com (66006@dr220.com)	4.0.7.1.5 (J100-IPT-SIP-R4_0_7_1-121020)	J169	(dr220.com)	(DR-SM)

9.3. Verify UMWS

From the **SIP Device Registration Data** screen in **Section 9.2**, scroll the screen to the right to locate the **CM (System Name)** column, which contains data obtained from the UMWS interface.

data in Excel format)

Extension	Display Name	IP Address	SIP Login (Handle)	Device Version (EM Version)	Model	Serving Site (SIP Domain)	SM (System Name)	CM (System Name)
66002	SIP 2, Avaya	192.168.200.144	66002@dr220.com (66002@dr220.com)	7.1.11.0.8 (96x1-IPT-SIP-R7_1_11_0-092520)	96x1	(dr220.com)	(DR-SM)	(DR-CM)
66006	SIP 6, Avaya	192.168.200.163	66006@dr220.com (66006@dr220.com)	4.0.7.1.5 (J100-IPT-SIP-R4_0_7_1-121020)	J169	(dr220.com)	(DR-SM)	(DR-CM)

9.4. Verify PUSH

From the ONCENTS screen shown in **Section 8.3**, 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.

Endpoint Manager v6.1.0 for AVAYA
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

DASHBOARD **MONITOR** MIGRATION ONBOARDING MANAGEMENT SETTINGS CONFIGURATION

Search By: MAC Address
MAC Address: *
Submit

EM Device - MAC Address [*]
100 Per Page, Page 1 of 1
Result Count: 5 Last Update: 07/22/2021 13:26:55 (* Export Table data in CSV format)

MAC Address	Device Name	Handle (Extension)	Display Name	SIP Login	Serial	IP Address (Private IP)	Model (HW Version)	FW Version (Signature)	Signal
<input type="checkbox"/> C8-1F-EA-97-9B-B9		65000	CM Supervisor		18WZ44600471	192.168.200.179 (192.168.200.179) (2)	J179D02A	96x1-IPT-H323-R6 8 5 11-050321 (6.8511)	H.323
<input type="checkbox"/> 70-38-EE-C9-D5-18		65001	CM Station 1		12WZ123602DR	192.168.200.212 (192.168.200.212)	9611GD01A	96x1-IPT-H323-R6 8 5 02-110720 (6.8502)	H.323
<input type="checkbox"/> B4-B0-17-84-06-18		66002	SIP 2, Avaya	66002@dr220.com	10WZ50461481	192.168.200.144 (192.168.200.144) (0)	9641	96x1-IPT-SIP-R7 1 11 0-092520 (7.1.11.0.8)	SIP
<input type="checkbox"/> C8-1F-EA-82-36-0A		66006	SIP 6, Avaya	66006@dr220.com	18WZ125008L1	192.168.200.163 (192.168.200.163)	J169	J100-IPT-SIP-R4 0 7 1-121020 (4.0.7.1.5)	SIP

Use Wireshark to capture packets in and out of the select device, in this case the J179 H.323 endpoint. Verify that the packet capture shows a subscription packet from the J179 H.323 endpoint with IP address **192.168.200.179** to the ONCENTS server with IP address **10.64.101.208**, as shown below.

Note that necessary phone settings for PUSH integration with ONCENTS were taken care of by ONCENTS as part of the file server capability.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.64.101.208

No.	Time	Source	Destination	Protocol	Length	Info
29	11:51:33.387324	10.64.101.208	192.168.200.179	TCP	66	80 → 58336 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
30	11:51:33.388179	192.168.200.179	10.64.101.208	TCP	60	58336 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
31	11:51:33.389520	192.168.200.179	10.64.101.208	HTTP	237	GET /subscribe1.do?action=resubscribe HTTP/1.1
32	11:51:33.440953	10.64.101.208	192.168.200.179	TCP	60	80 → 58336 [ACK] Seq=1 Ack=184 Win=30336 Len=0
33	11:51:33.445531	10.64.101.208	192.168.200.179	HTTP/XML	305	HTTP/1.1 200 OK
34	11:51:33.446287	192.168.200.179	10.64.101.208	TCP	60	58336 → 80 [ACK] Seq=184 Ack=252 Win=30272 Len=0
35	11:51:33.449100	192.168.200.179	10.64.101.208	TCP	60	58336 → 80 [FIN, ACK] Seq=184 Ack=252 Win=30272 ...

9.5. Verify SNMP

From the same **EM Device – MAC Address [*]** screen below, scroll the screen to the right and click on the **Query** option (not shown) associated with a desired entry.

ONCENTS Endpoint Manager v6.1.0 for AVAYA
U.S. Patent Numbers 9,591,049 & 10,021,610 & 10,939,342

DASHBOARD MONITOR MIGRATION ONBOARDING MANAGEMENT SETTINGS CONFIGURATION

Search By: MAC Address
MAC Address: *
Submit

EM Device - MAC Address [*]

100 Per Page, Page 1 of 1
Result Count: 5 Last Update: 07/22/2021 13:26:55 (* Export Table data in CSV format)

MAC Address	Device Name	Handle (Extension)	Display Name	SIP Login	Serial	IP Address (Private IP)	Model (HW Version)	FW Version (Signature)	Signal
<input type="checkbox"/> C8:1F:EA:97:9B:B9		65000	CM Supervisor		18WZ44600471	192.168.200.179 (192.168.200.179) (2)	J179D02A	96x1-IPT-H323-R6 8 5 11-050321 (6.8511)	H.323
<input type="checkbox"/> 70:38:EE:C9:D5:18		65001	CM Station 1		12WZ123602DR	192.168.200.212 (192.168.200.212) (1)	9611GD01A	96x1-IPT-H323-R6 8 5 02-110720 (6.8502)	H.323
<input type="checkbox"/> B4:B0:17:84:06:18		66002	SIP 2, Avaya	66002@dr220.com	10WZ50461481	192.168.200.144 (192.168.200.144) (0)	9641	96x1-IPT-SIP-R7 1 11 0-092520 (7.1.11.0.8)	SIP
<input type="checkbox"/> C8:1F:EA:82:36:0A		66006	SIP 6, Avaya	66006@dr220.com	18WZ125008L1	192.168.200.163 (192.168.200.163) (1)	J169	J100-IPT-SIP-R4 0 7 1-121020 (4.0.7.1.5)	SIP

Use Wireshark to capture packets in and out of the selected device, in this case J169 SIP endpoint from above. 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 J169 H.323 endpoint with IP address **192.168.200.163** as shown below.

Note that necessary phone settings for SNMP integration with ONCENTS were taken care of by ONCENTS as part of the file server capability.

wireshark-em-aura813-J169-sip-66006-query-snmp.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

snmp

No.	Time	Source	Destination	Protocol	Length	Info
93	12:53:04.121401	10.64.101.208	192.168.200.163	SNMP	189	get-request 1.3.6.1.4.1.6889.2.69.5.1.72.0 1.3
97	12:53:04.126947	192.168.200.163	10.64.101.208	SNMP	207	get-response 1.3.6.1.4.1.6889.2.69.5.1.72.0 1.
184	12:53:04.180696	10.64.101.208	192.168.200.163	SNMP	92	get-request 1.3.6.1.4.1.6889.2.69.5.1.74.0
189	12:53:04.182047	192.168.200.163	10.64.101.208	SNMP	92	get-response 1.3.6.1.4.1.6889.2.69.5.1.74.0
205	12:53:04.233696	10.64.101.208	192.168.200.163	SNMP	92	get-request 1.3.6.1.4.1.6889.2.69.6.1.52.0
216	12:53:04.237472	192.168.200.163	10.64.101.208	SNMP	100	get-response 1.3.6.1.4.1.6889.2.69.6.1.52.0
242	12:53:04.295181	10.64.101.208	192.168.200.163	SNMP	92	get-request 1.3.6.1.4.1.6889.2.69.6.7.23.0
277	12:53:04.309275	192.168.200.163	10.64.101.208	SNMP	105	get-response 1.3.6.1.4.1.6889.2.69.6.7.23.0

10. Conclusion

These Application Notes describe the configuration steps required for iNEMSOFT ONCENTS Endpoint Manager 6.1 to interoperate with Avaya Aura® Communication Manager 8.1.3, Avaya Aura® Application Enablement Services 8.1.3, Avaya Aura® System Manager 8.1.3, Avaya Aura® Session Manager 8.1.3, 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 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
4. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, February 2021, available at <http://support.avaya.com>.
5. *Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, Release 6.8.2, Issue 1, June 2019, available at <http://devconnectprogram.com>.
6. *Installing and Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.1.14, Issue 1, July 2021, available at <http://devconnectprogram.com>.
7. *Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, Release 6.8.2, Issue 1, June 2019, available at <http://devconnectprogram.com>.
8. *Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, Release 6.8.2, Issue 1, June 2019, available at <http://devconnectprogram.com>.
9. *oncents Endpoint Manager R6 User Guide*, June 2021, available upon request to support@inemsoft.com.

©2021 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.