



Avaya Solution & Interoperability Test Lab

Application Notes for Inline Pro Mentol Pro V5 with Avaya Aura® Communication Manager R8.0 and Avaya Aura® System Manager R8.0 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Inline Pro Mentol Pro to interoperate with Avaya Aura® Communication Manager and Avaya Aura® System Manager.

Mentol Pro provides real-time monitoring and management solutions for IP telephony networks. Mentol Pro provides visibility of Avaya and other vendor's IP telephony solutions from a single console and enables a reduction in complexity when managing complex IP telephony environments.

Mentol Pro integrates directly to Communication Manager using Secure Shell (SSH) or Telnet and uses Simple Network Management Protocol (SNMP) to query Communication Manager. At the same time, Mentol Pro processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager. A connection to System Manager gives the status of registered SIP users.

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 procedures for configuring Mentol Pro from Inline Pro to interoperate with Avaya Aura® Communication Manager R8.0 and Avaya Aura® System Manager R8.0.

Mentol Pro provides complete, end-to-end visibility across IP telephony network supporting complex multi-vendor environment. The solution collects data directly from Avaya Aura® Communication Manager and Avaya Aura® System Manager and gives a visual representation of actionable voice performance information that is required to resolve issues quickly. Centralized collection and storage of information allow to monitor PBX status (full details for gateways, port networks, boards, trunks & route patterns) and to overview call details and usage data.

Mentol Pro is a monitoring and reporting tool that supports proactive control of voice quality and call accounting of corporate telephony. It visualizes historical data on the voice traffic bandwidth, the processing of calls and the interconnection of network objects. The solution uses common metrics like MOS, delay, jitter and packet loss, which makes an analysis of the communication channels congestion and identification of efficient routing easier for users.

To prevent incidents, Mentol Pro sends messages with detailed information on the incident via e-mail, SMS and SNMP trap with the option of setting individual notification parameters.

Mentol Pro uses seven integration methods to monitor a Communication Manager system.

1. System Access Terminal (SAT) – Mentol Pro connects to Communication Manager to issue 'list', 'display' and 'status' commands to produce statistics for that Communication Manager.
2. Real Time Transport Control Protocol (RTCP) collection – Mentol Pro collects RTCP information sent by Avaya resources including Communication Manager boards, media gateways, media servers and IP deskphones.
3. Call Detail Recording (CDR) collection – Mentol Pro collects CDR information sent by Communication Manager.
4. Simple Network Management Protocol (SNMP) – These are SNMP traps from Communication Manager, sent to the Mentol Pro server to be processed.
5. Avaya Communication Manager SysLog – Sending out the Avaya System Log to the Mentol Pro server for processing.
6. Internet Control Message Protocol (ICMP) - connection between Communication Manager and Mentol Pro, to observe ping commands and basic IP connectivity.
7. System Manager HTTPS – Screen scraping of the SIP users to obtain the user registration information.

2. General Test Approach and Test Results

The general test approach was to use Mentol Pro web user interface to display the configurations of Communication Manager and verify against what is displayed on the SAT interface. The SAT interface is accessed by using Secure Shell (SSH) to Communication Manager running on VMware (used in this testing). Calls were placed between various Avaya endpoints and Mentol Pro was used to display the RTCP and CDR information collected. SNMP traps, ICMP, SysLog and information from System Manager HTTPS were also verified from the Mentol Pro web interface. Information on RTCP, CDR, SysLog, ICMP, HTTPS and SNMP are available using a program such as Wireshark and can be verified using that or other similar tools.

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.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of the SAT interface as a programmatic approach to integrate 3rd party applications. Avaya may make changes or enhancements to the SAT interface in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using this SAT interface. Using the SAT interface in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real time delays be inserted between each command execution.

Note: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Communication Manager Releases,

including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

For feature testing, Mentol Pro was used to view the configuration of Communication Manager via collected SAT data such as media gateways, media servers, Enterprise Survivable Server (ESS), Local Survivable Processor (LSP), trunk groups, route patterns, DS1 boards, IP network regions, stations, processor occupancy, alarm and error information.

For the collection of RTCP and CDR information, the endpoints included Avaya H.323, Digital and SIP users. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, outbound trunk calls, transfer and conference calls. This information displayed by Mentol Pro was verified in Wireshark.

For serviceability testing, LAN failures were applied to Mentol Pro and Communication Manager to simulate system unavailability. Reboots of Communication Manager and the G450 Media Gateway were also performed during serviceability testing.

2.2. Test Results

All test cases passed successfully, with the following observations noted.

1. The call direction was not reported as part of the RTCP data.
2. The G726 codec was not supported by Mentol Pro showing as part of the RTCP data.
3. There are some differences in the call records generated by SIP endpoints compared to analog, digital, and H.323 endpoints. As a result, in certain scenarios involving SIP endpoints (e.g., two-party call, transfer, conference or call forwarding), a CDR application may see more or less records, or records with condition codes/calling party other than expected. Avaya is investigating the differences and code changes may be made available in a future release pending the outcome of that investigation. During compliance testing, when a SIP phone is used to initiate a call to a phone that is forwarded to the PSTN the CDR record shows a call from the initial SIP phone to the PSTN and it is expected to show from the forwarded-to phone to the PSTN.

2.3. Support

For technical support on Mentol Pro, contact the Inline Pro at:

- Hotline: +7 (812) 603 40 63
- Email: support@inlinepro.ru

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Mentol Pro interoperability with Communication Manager and System Manager. The configuration consists of a Communication Manager system with an Avaya G450 Media Gateway. This system has Avaya H.323, SIP and Digital endpoints. A QSIG trunk connected to another Communication Manager served to simulate external calls. System Manager and Session Manager provided SIP support to the Avaya SIP endpoints. Mentol Pro was installed on a server running Microsoft Windows Server 2016. Both the Monitoring and Web Application software are installed on this server. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers, Media Gateways and IP telephones.

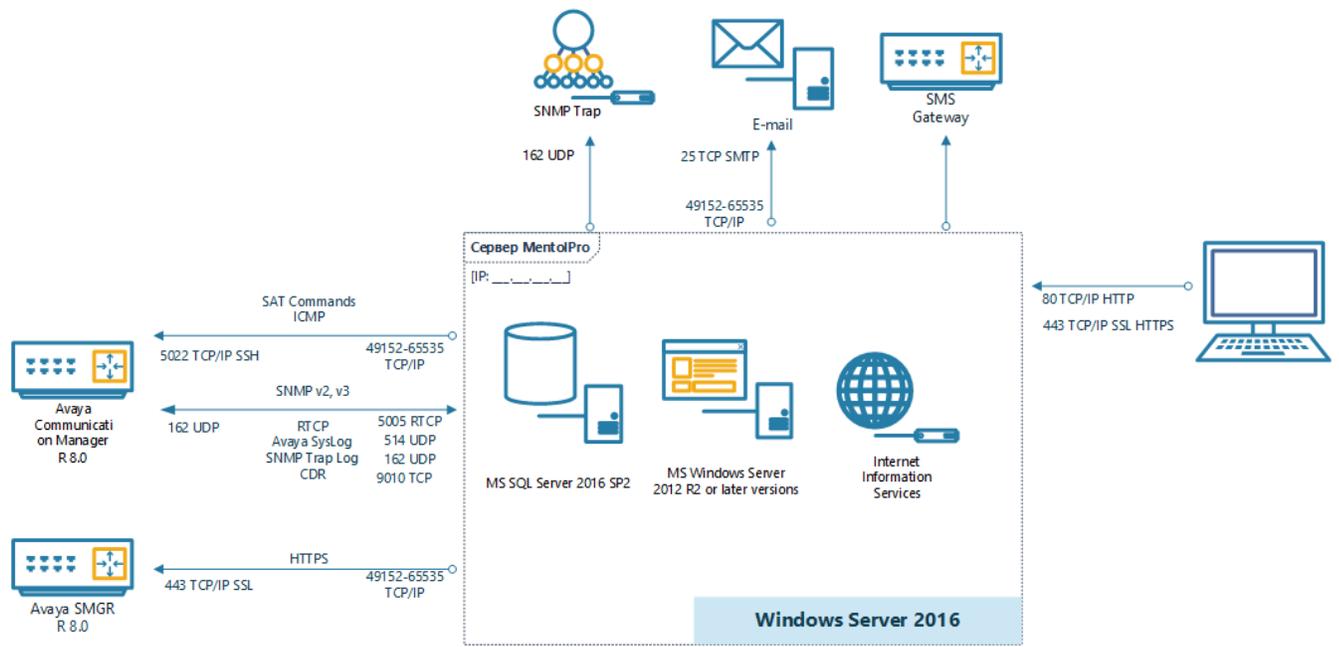


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Avaya Equipment / Software	Release / Version
Avaya Aura® System Manager running on a virtual server	System Manager 8.0.0.0 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.0.0.098090
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.0 Build No. – 8.0.0.0.800035
Avaya Aura® Communication Manager running on a virtual server	R8.0 R018x.01.0.822.0
Avaya G450 Media Gateway	37.39.0/1
Avaya 96x1 H.323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya 9408 Digital Deskphone	V2.0
Inline Pro Equipment / Software	Release / Version
Inline Pro Mentol Pro	Ver 5

5. Configure Avaya Aura® Communication Manager connections

This section describes the steps required to configure Communication Manager to interoperate with Mentol Pro. This includes creating a login account and a SAT User Profile for Mentol Pro to access Communication Manager and enabling SNMP, RTCP and CDR reporting. Access to the Communication Manager System Logs is also provided for Mentol Pro.

5.1. Configure SAT Connection

A user is defined to have access to certain SAT commands. A SAT user profile is configured on Communication Manager and a user is then associated with the user profile.

5.1.1. Configure SAT User Profile

A SAT user profile specifies which SAT forms may be accessed by the user assigned to the user profile and the type of access to each form. As Mentol Pro does not modify any system configuration, create a SAT user profile with limited permissions to assign to the Mentol Pro login account.

Enter the **add user-profile *n*** command, where *n* is the next unused profile number. Enter a descriptive name for **User Profile Name** and enable all categories by setting the **Enbl** field to **y**.

Note: For compliance testing **User Profile 66** was created.

```
add user-profile 66                                     Page 1 of 41
                                                    USER PROFILE 66

User Profile Name: MentolPro

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

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

On **Page 2** of the **USER PROFILE** form, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the **Set All Permissions To** field. Submit the form to create the user profile.

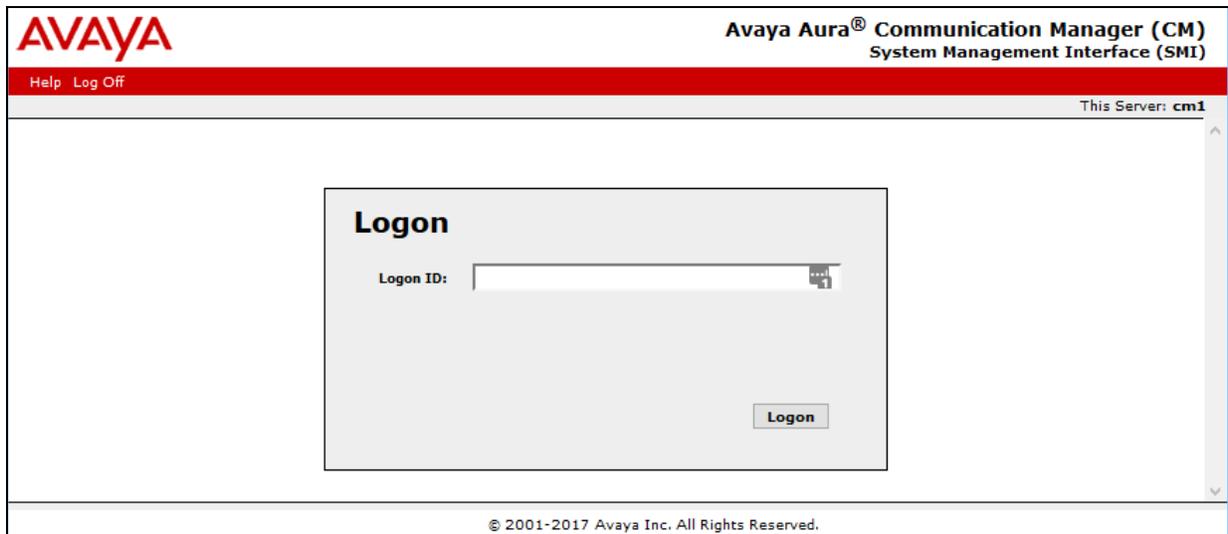
```

add user-profile 66
USER PROFILE 66
Set Permissions For Category: To: Set All Permissions To:rm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
Name Cat Perm
aar analysis J rm
aar digit-conversion J rm
aar route-chosen J rm
abbreviated-dialing 7103-buttons C rm
abbreviated-dialing enhanced C rm
abbreviated-dialing group C rm
abbreviated-dialing personal C rm
abbreviated-dialing system C rm
aca-parameters P rm
access-endpoint P rm
adjunct-names A rm
administered-connection C rm
aesvcs cti-link A rm
aesvcs interface A rm
  
```

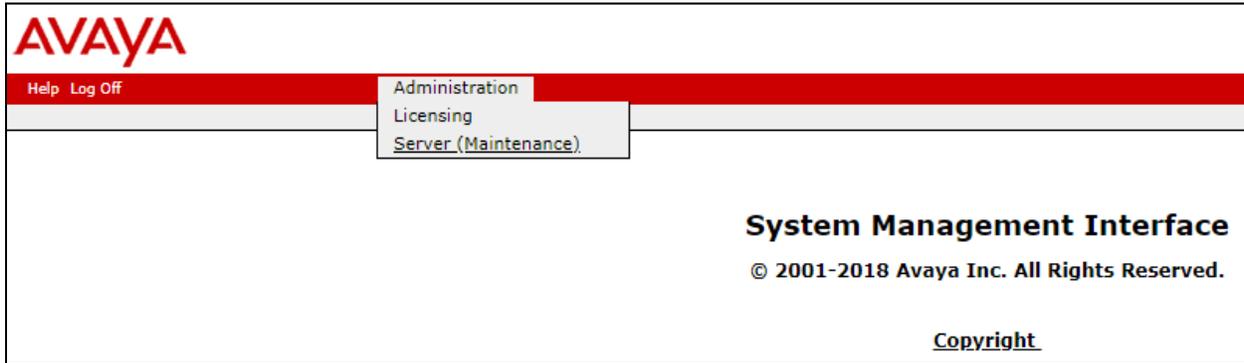
5.1.2. Configure Login Group

Create an Access-Profile Group on Communication Manager System Management Interface (SMI) to correspond to the SAT User Profile created in **Section 5.1.1**.

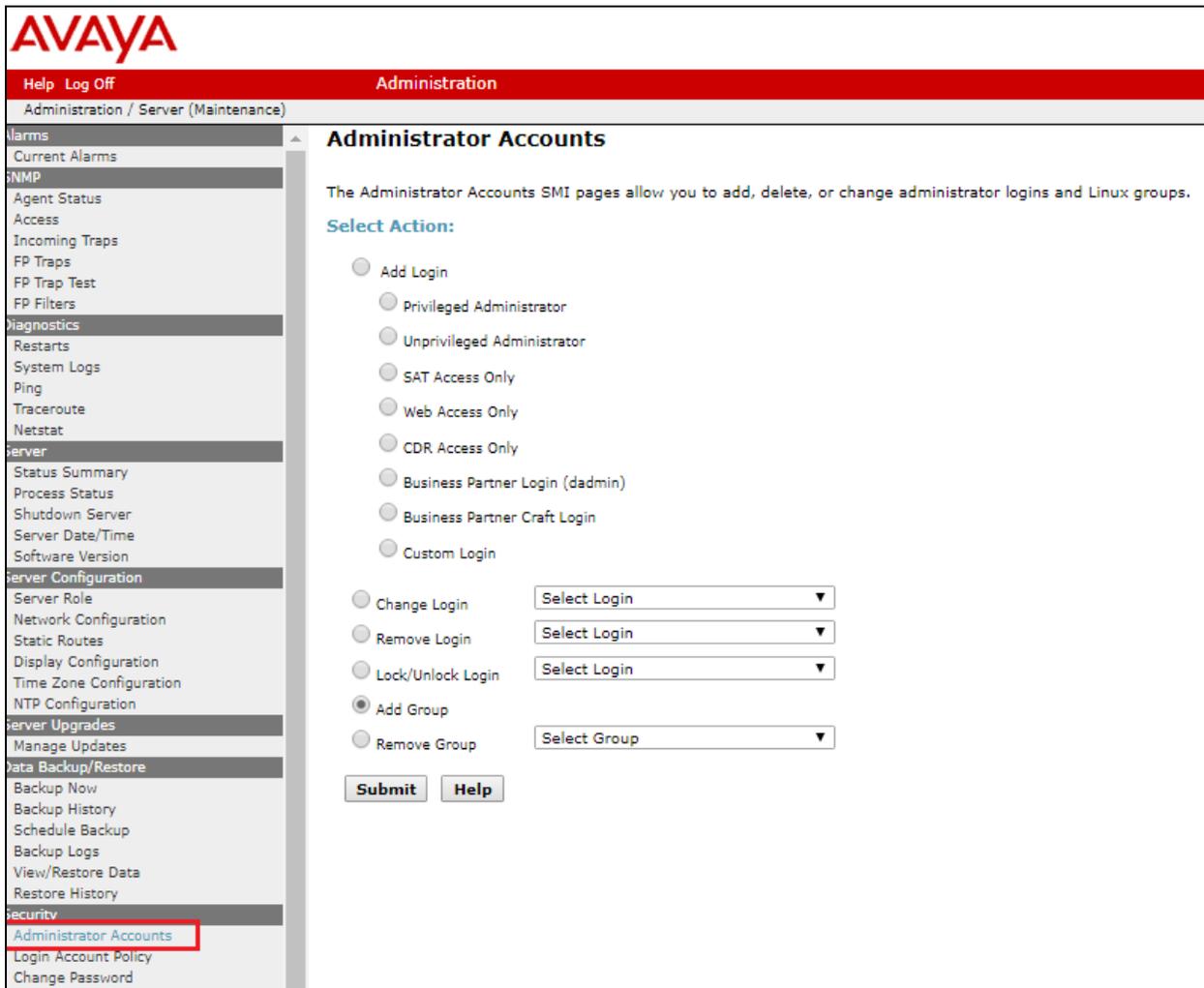
Using a web browser, enter *https://<IP address of Communication Manager>* to connect to the Communication Manager server being configured and log in using appropriate credentials



Once logged in, click on **Server (Maintenance)**.



Navigate to **Security** → **Administrator Accounts** in the left window and select **Add Group** in the main window. Click on **Submit** to add a new group.



Select the profile from the drop-down box to correspond with the user-profile created in that was created in **Section 5.1.1** and click on **Submit**.

Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile Linux group. (Mask).

Select Action:

Add a new access-profile group: prof66 ▼

Add a new non-access-profile group:

Group Name:

Group Number: (1000 to 60000)

Submit **Cancel** **Help**

5.1.3. Configure Login

Create a login account for Mentol Pro to access the Communication Manager SAT. Repeat this for each Communication Manager if there are more than one.

From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**.

Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

Add Login

Privileged Administrator

Unprivileged Administrator

SAT Access Only

Web Access Only

CDR Access Only

Business Partner Login (dadmin)

Business Partner Craft Login

Custom Login

Change Login ▼

Remove Login ▼

Lock/Unlock Login ▼

Add Group ▼

Remove Group ▼

Submit **Help**

For the field **Login name**, enter a login ID, this will be used by Mentol Pro to log into Communication Manager to issue the SAT commands. Configure the other parameters for the login as follows:

- **Primary group: users** [Limits the permissions of the login]
- **Additional groups (profile): prof66** [Select the access-profile group created in **Section 5.1.2**. Ignore the warnings as SAT access was selected.]
- **Enter password / Re-enter password** [Define the password]
- Click **Submit** to continue. [This completes the configuration of the login]

Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Manager System

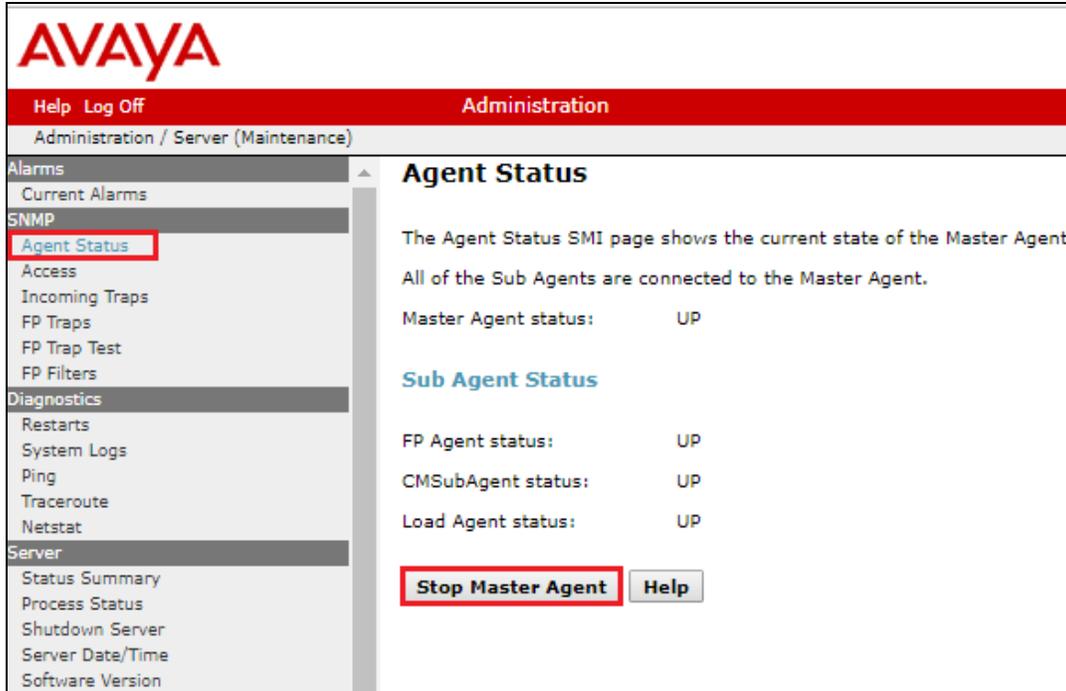
Login name	<input type="text" value="mentolpro"/>
Primary group	<input checked="" type="radio"/> users <input type="radio"/> susers
Additional groups (profile)	<input type="text" value="prof66"/>  You must assign a profile that has no web access if you want a login with SAT access only.
Linux shell	<input type="text" value="/opt/ecs/bin/autosat"/>  This shell setting does NOT disable the "go shell" SAT command for this user.
Home directory	<input type="text" value="/var/home/mentolpro"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/>
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Enter password	<input type="password" value="....."/>
Re-enter password	<input type="password" value="....."/>
Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes

5.2. Configure SNMP Connections

Two separate connections were made for SNMP and they were to Communication Manager and the G450 Media Gateway. The setup for both connections are shown here.

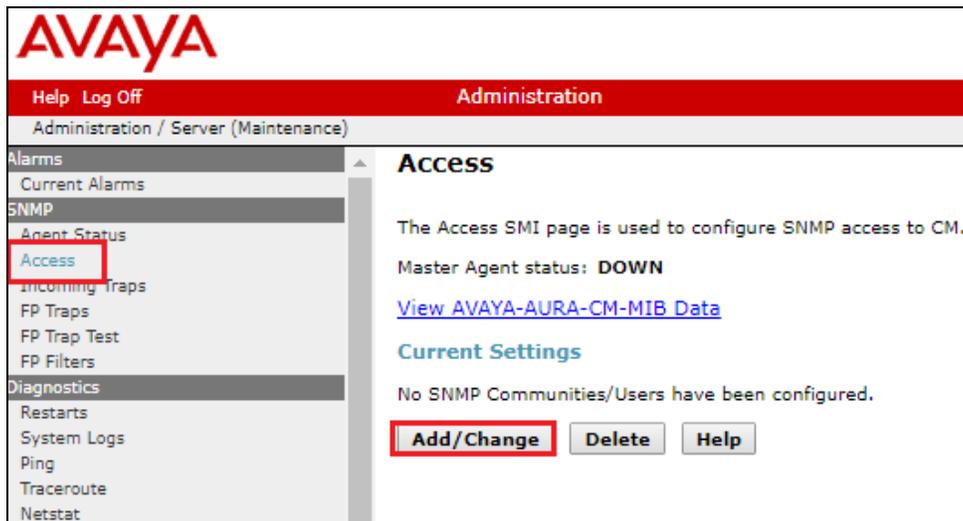
5.2.1. Configure SNMP on Avaya Aura® Communication Manager

Navigate to **SNMP** → **Agent Status** in the left window. Click **Stop the Master Agent** if the **Master Agent status** is **UP** to allow setup of SNMP Agent.



The screenshot shows the Avaya Administration console interface. The top navigation bar includes 'Help' and 'Log Off' on the left, and 'Administration' on the right. Below this is a breadcrumb trail: 'Administration / Server (Maintenance)'. A left-hand navigation menu is visible, with categories: 'Alarms', 'SNMP', 'Access', 'Incoming Traps', 'FP Traps', 'FP Trap Test', 'FP Filters', 'Diagnostics', and 'Server'. The 'SNMP' category is expanded, and 'Agent Status' is selected and highlighted with a red box. The main content area is titled 'Agent Status' and contains the following text: 'The Agent Status SMI page shows the current state of the Master Agent. All of the Sub Agents are connected to the Master Agent.' Below this, the status is listed: 'Master Agent status: UP'. Under the heading 'Sub Agent Status', the following are listed: 'FP Agent status: UP', 'CMSubAgent status: UP', and 'Load Agent status: UP'. At the bottom of the main content area, there are two buttons: 'Stop Master Agent' (highlighted with a red box) and 'Help'.

Navigate to **SNMP** → **Access** in the left window. Click in **Add/Change** in the main window.



The screenshot shows the Avaya Administration console interface. The top navigation bar includes 'Help' and 'Log Off' on the left, and 'Administration' on the right. Below this is a breadcrumb trail: 'Administration / Server (Maintenance)'. A left-hand navigation menu is visible, with categories: 'Alarms', 'SNMP', 'Access', 'Incoming Traps', 'FP Traps', 'FP Trap Test', 'FP Filters', 'Diagnostics', and 'Server'. The 'SNMP' category is expanded, and 'Access' is selected and highlighted with a red box. The main content area is titled 'Access' and contains the following text: 'The Access SMI page is used to configure SNMP access to CM. Master Agent status: DOWN'. Below this, there is a blue link: '[View AVAYA-AURA-CM-MIB Data](#)'. Under the heading 'Current Settings', the text reads: 'No SNMP Communities/Users have been configured.' At the bottom of the main content area, there are three buttons: 'Add/Change' (highlighted with a red box), 'Delete', and 'Help'.

To send FP traps to the Mentol Pro server, navigate to **SNMP → FP Traps** in the left window. From the main window, click on **Add/Change**.

AVAYA

Help Log Off Administration

Administration / Server (Maintenance)

Alarms

- Current Alarms

SNMP

- Agent Status
- Access
- Incoming Traps
- FP Traps**
- FP Trap Test
- FP Filters

Diagnostics

- Restarts
- System Logs
- Ping
- Traceroute
- Netstat

Server

- Status Summary
- Process Status

FP Traps

The FP Traps page allows specification of the alarms to be sent as traps.

Note:

- The FP Traps SMI page is for the administration of CM Fault Performance Traps only. Additionally, Fault Performance Traps should not be sent to SAL IP Addresses.

Master Agent status: **UP**

[View AVAYA-AURA-CM-ALARM-MIB Data](#)

Current Settings

No trap destinations have been configured.

Add/Change Delete Help

Under **SNMP Version 2c** enter the Mentol Pro server IP and select **trap** from the drop-down box, add a **Community Name** such as **mentolpro** as shown below. The **Port** should be left with the default value of **162**. Click on **Submit** at the bottom of the page once this is done.

FP Traps

The FP Traps page allows specification of the alarms to be sent as traps.

Add Trap Destination

SNMP Version 1

IP address: Port:

Notification: trap

Community Name:

SNMP Version 2c

IP address: Port:

Notification:

Community Name:

SNMP Version 3

IP address: Port:

Notification:

User Name:

Authentication Protocol:

Authentication Password: Minimum 8 characters. (for authentication and privacy)

Privacy Protocol:

Privacy Password: Minimum 8 characters. (for privacy)

Engine ID:

Submit **Cancel** **Help**

The following screen should then be displayed.

FP Traps

The FP Traps page allows specification of the alarms to be sent as traps.

- **Success: Requested FP trap destination successfully added.**
- **Administration successfully changed.**

Note:

- The FP Traps SMI page is for the administration of CM Fault Performance Traps only. Additionally, Fault Performance Traps should not be sent to SAL IP Addresses.

Master Agent status: **UP**

[View AVAYA-AURA-CM-ALARM-MIB Data](#)

Current Settings

IP address	Port	Notification	SNMP Version	Community / User Name	V3 Sec
<input type="checkbox"/> 10.10.40.120	162	trap	2c	mentolpro	

Navigate to **SNMP** → **Agent Status** in the left window and if the **Master Agent status** is **DOWN** as shown below, click on Start Master Agent. Note that this may already be started.



Help Log Off Administration

Administration / Server (Maintenance)

- Alarms
 - Current Alarms
- SNMP
 - Agent Status**
 - Access
 - Incoming Traps
 - FP Traps
 - FP Trap Test
 - FP Filters
- Diagnostics
 - Restarts
 - System Logs
 - Ping
 - Traceroute
 - Netstat
- Server
 - Status Summary
 - Process Status

Agent Status

The Agent Status SMI page shows the current state of the Master Sub Agents are NOT connected to the Master Agent.

Master Agent status: DOWN

Sub Agent Status

FP Agent status: UP
CMSubAgent status: UP
Load Agent status: UP

5.2.2. Configure SNMP on G450 Media Gateway

This section provides the procedures for configuring SNMP on the Avaya G450 Media Gateway. The procedures include the following areas:

- Administer community string
- Administer SNMP traps
- Commit configuration

Use the **snmp-server community** command below to set the desired community strings for read-only and read-write access, where **public** and **private** can be any desired community string. Note that the community strings are required to be set on the G450 Media Gateway, although not used by Mentol Pro.

```
G450-001 (super) # snmp-server community read-only public read-write private
```

Use the **snmp-server host** command shown below to enable SNMP traps and notifications to Mentol Pro, where **10.10.40.120** is the IP address of the Mentol Pro server, and **public** is the read-only community string from above.

```
G450-001 (super) # snmp-server host 10.10.40.120 traps v2c public udp-port 162 all
```

Use the **copy** command below to commit the current configuration.

```
G450-001 (super) # copy running startup-config
```

5.3. Configure RTCP Monitoring

To allow Mentol Pro to monitor the quality of H.323 IP calls, configure Communication Manager to send RTCP reporting to the IP address of the Mentol Pro server. This is done through the SAT interface, but for Avaya SIP endpoints this is done on the 46xxsettings file (see **Section 5.3.2**).

5.3.1. Setting RTCP for H.323 IP calls

Enter the **change system-parameters ip-options** command. In the **RTCP MONITOR SERVER** section, set **Server IPV4 Address** to the IP address of the Mentol Pro server. Set **IPV4 Server Port** to **5005** and **RTCP Report Period (secs)** to **5**.

```
change system-parameters ip-options                               Page 1 of 5
                        IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS
  Roundtrip Propagation Delay (ms)   High: 800       Low: 400
      Packet Loss (%)                High: 40        Low: 15
      Ping Test Interval (sec): 20
  Number of Pings Per Measurement Interval: 10
      Enable Voice/Network Stats? n

RTCP MONITOR SERVER
  Server IPV4 Address: 10.10.40.120   RTCP Report Period(secs): 5
      IPV4 Server Port: 5005
  Server IPV6 Address:
      IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
  Link Failure? y

                        H.323 IP ENDPOINT
H.248 MEDIA GATEWAY
  Link Loss Delay Timer (min): 5       Link Loss Delay Timer (min): 5
  Primary Search Time (sec): 75
  Recover Before LLDT Expiry? y       Periodic Registration Timer (min): 20
      Short/Prefixed Registration Allowed? n
```

Enter the **change ip-network-region *n*** command, where *n* is IP network region number to be monitored. On **Page 2**, set **RTCP Reporting to Monitor Server Enabled** to **y** and **Use Default Server Parameters** to **y**.

Note: Only one **RTCP MONITOR SERVER** can be configured per IP network region. Repeat this step for all IP network regions that are required to be monitored.

```
change ip-network-region 1                               Page 2 of 20
                                     IP NETWORK REGION

RTCP Reporting to Monitor Server Enabled? y

RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y

ALTERNATIVE NETWORK ADDRESS TYPES
  ANAT Enabled? n
```

5.3.2. Setting RTCP for SIP calls

For SIP deskphones, the RTCP settings are configured in the phone settings file.

From the appropriate HTTP server serving the SIP deskphones, locate the **46xxsettings.txt** file. Navigate to the **RTCP MONITORING** section. Set **RTCPMON** to the IP address of the Mentol Pro server. Set **RTCPMONPORT** to the same port number from **Section Error! Reference source not found.** Set **RTCPMONPERIOD** to the desired interval.

Manually reboot the SIP deskphones to obtain the updated settings.

```
##### RTCP MONITORING #####
##
## The RTCP monitor
## One RTCP monitor (VMM server) IP address in
## dotted-decimal format or DNS name format (0 to 15
## characters). Note that for H.323 telephones only this
## parameter may be changed via signaling from Avaya
## Communication Manager. For 96xx SIP models in Avaya
## environments, this parameter is set via the PPM server.
## This parameter is not supported on 16CC model phones.
## Note : This setting is applicable for 1603 SIP phones also.
## SET RTCPMON 192.168.0.10
##
## RTCPMONPORT sets the port used to send RTCP information
## to the IP address specified in the RTCPMON parameter.
## RTCPMONPORT is only supported on 46xx SIP telephones and
## 96xx telephones in non-Avaya environments. For 96xx SIP
## models in Avaya environments, this parameter is set via
## the PPM server. The default value is 5005.
## Note : This setting is applicable for 1603 SIP phones also.
## SET RTCPMONPORT "5005"
##
## RTCP Monitor Report Period
## Specifies the interval for sending out RTCP monitoring
## reports (5-30 seconds). Default is 5 seconds. This
## parameter applies only to 96xx SIP telephones.
## Note : This setting is applicable for 1603 SIP phones also.
## SET RTCPMONPERIOD 5
##
SET RTCPMON 10.10.40.120
SET RTCPMONPORT "5005"
SET RTCPMONPERIOD 5
```

5.4. Configure CDR Monitoring

To allow Mentol Pro monitor the CDR information, configure Communication Manager to send CDR information to the IP address of the Mentol Pro server.

Enter the **change node-names ip** command to add a new node name for the Mentol Pro server. In this configuration, the name **MentolPro** is added with the IP address specified as **10.10.40.120**. Note also the node name **procr** which is automatically added.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
Name          IP Address
AMS80vmpg    10.10.40.61
CLAN (Mentol) 10.10.10.10
G430         10.10.40.15
G450         10.10.40.14
LSPMentol    10.10.40.63
MentolPro   10.10.40.120
RDTT         10.10.40.240
SM80vmpg     10.10.40.58
aes80vmpg    10.10.40.56
default      0.0.0.0
procr       10.10.40.59
procr6       ::

( 12 of 12 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Enter the **change ip-services** command to define the CDR link. To define a primary CDR link, the following information should be provided:

- **Service Type: CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node: procr** [Communication Manager will use the processor-ethernet interface to send out the CDR. CLAN node could also be used.]
- **Local Port: 0** [The Local Port is set to 0 because Communication Manager initiates the CDR link.]
- **Remote Node: MentolPro** [The Remote Node is set to the node name previously defined.]
- **Remote Port: 9000** [The Remote Port may be set to a value between 5000 and 64500 inclusively. **9000** is the port number used by Mentol Pro.]

```
change ip-services Page 1 of 4
```

IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	n	procr	8765			
CDR1		procr	0	MentolPro	9000	
CDR2		procr	0	RDTT	9001	

On **Page 3** of the form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **n**.

```
change ip-services Page 3 of 4
```

SESSION LAYER TIMERS						
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	
CDR1	n	30	3	3	60	
CDR2	y	30	3	3	60	

Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test.

- **CDR Date Format: day/month**
- **Primary Output Format: customized**
- **Primary Output Endpoint: CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See **Reference [2]** for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats? n** [Specify the use of Communication Manager 3.x (“legacy”) formats in the CDR records produced by the system.]
- **Intra-switch CDR: y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form.]
- **Record Outgoing Calls Only? n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting? y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting? y** [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]

```

change system-parameters cdr                               Page 1 of 2
                                CDR SYSTEM PARAMETERS

Node Number (Local PBX ID):                               CDR Date Format: day/month
  Primary Output Format: customized   Primary Output Endpoint: CDR1
  Secondary Output Format: customized Secondary Output Endpoint: CDR2
    Use ISDN Layouts? y               Enable CDR Storage on Disk? y
    Use Enhanced Formats? n          Condition Code 'T' For Redirected Calls? n
  Use Legacy CDR Formats? n          Remove # From Called Number? y
Modified Circuit ID Display? n       Intra-switch CDR? y
    Record Outgoing Calls Only? n    Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? n          Outg Attd Call Record? n
    Disconnect Information in Place of FRL? n            Interworking Feat-flag? n
  Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n      Record Agent ID on Outgoing? y
  Inc Trk Call Splitting? y          Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n      Call Record Handling Option: warning
    Record Call-Assoc TSC? n        Digits to Record for Outgoing Calls: dialed
  Privacy - Digits to Hide: 0       CDR Account Code Length: 4
Remove '+' from SIP Numbers? y

```

On **Page 2**, the following are set specifically for Mentol Pro, these values were provided by Inline Pro before compliance testing.

```
change system-parameters cdr Page 2 of 2
                                CDR SYSTEM PARAMETERS

    Data Item - Length          Data Item - Length          Data Item - Length
1: date                        - 6      17: acct-code              - 15      33: -
2: space                       - 1      18: space                  - 1      34: -
3: time                        - 4      19: ppm                    - 5      35: -
4: space                       - 1      20: space                  - 1      36: -
5: sec-dur                     - 5      21: in-crt-id             - 3      37: -
6: space                       - 1      22: space                  - 1      38: -
7: cond-code                   - 1      23: out-crt-id            - 3      39: -
8: space                       - 1      24: space                  - 1      40: -
9: code-dial                   - 4      25: in-trk-code           - 4      41: -
10: space                      - 1      26: space                  - 1      42: -
11: code-used                  - 4      27: vdn                   - 7      43: -
12: space                      - 1      28: space                  - 1      44: -
13: dialed-num                 - 23     29: feat-flag              - 1      45: -
14: space                      - 1      30: return                 - 1      46: -
15: calling-num                - 15     31: line-feed              - 1      47: -
16: space                      - 1      32:                        -        48: -

                                Record length = 116
```

If the **Intra-switch CDR** field is set to **y** on **Page 1** of the CDR SYSTEM PARAMETERS form, then enter the **change intra-switch-cdr** command to define the extensions that will be subjected to intra-switch call detail recording. In the **Extension** column, enter the specific extensions whose usage will be tracked with the CDR records.

```
change intra-switch-cdr Page 1 of 3
                                INTRA-SWITCH CDR

    Assigned Members: 6 of 1000 administered
    Extension          Extension          Extension
2000
2001
2002
2050
2100
2101

Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other
members
```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Enter the **change trunk-group n** command, where **n** is the trunk group number, to verify that the **CDR Reports** field is set to **y**. Repeat for all trunk groups to be reported.

```

change trunk-group 1                                     Page 1 of 4
                                     TRUNK GROUP
Group Number: 1                                         Group Type: sip      CDR Reports: y
Group Name: SIPTRUNK                                   COR: 1              TN: 1             TAC:
*801
  Direction: two-way                                   Outgoing Display? n
  Dial Access? n                                       Night Service:
Queue Length: 0
Service Type: tie                                       Auth Code? n
                                                         Member Assignment Method: auto
                                                         Signaling Group: 1
                                                         Number of Members: 10

```

Enter **save translation** to save the changes made.

```

save translation
                                     SAVE TRANSLATION
Command Completion Status                               Error Code
Success                                                0

```

5.5. Configure System Logs

Navigate to **Security** → **Server Log Files** in the left window and from the main window, select **enable logging to the following server**, enter the Mentol Pro server IP address as the **server name**. Tick all the boxes as shown below and click on **Submit**.

Note: If there are LSP and ESS servers in the setup ensure that the top tick box is also ticked.

AVAYA Avaya Aura®

Help Log Off Administration

Administration / Server (Maintenance)

Server Log Files

This page allows you to select logs to be sent to an external syslog server and to configure a command history command retention timeframe

Syslog Server

This section allows you to select logs to be sent to an external syslog server

Control File Synchronization of Syslog Configuration

When the **Submit** button is clicked, send syslog configuration to all LSP and ESS servers.

Control Logging to an External Syslog Server:

Disable logging to an external syslog server.
 Enable logging to the following syslog server.

Specify the Syslog Server to Receive Events:

server name

Select Which Logs Are to be Sent to the Above Server:

boot, cron, *.emerg logs
 security log
 kernel log
 command history log
 CM IP events log

Command History

This section allows you to configure a command history log retention timeframe

Specify the Number of Months to Retain Log

Number of months to store command history

Control Compression of Command History log

Enable compression

Submit **Help**

5.6. Configure Internet Control Message Protocol connection

There is no special configuration on Communication Manager for an Internet Control Message Protocol (ICMP) connection,

6. Configure Avaya Aura® System Manager Connection

Mentol Pro collects registered state data of SIP endpoint polling to the section “User Registration” of System Manager [Home / Elements / Session Manager / System Status / User Registrations]. Mentol Pro generates a data mapping that includes all the fields and then processes the fields for each device.

A System Manager user is setup and assigned a Role that has access to only the User Registrations page, therefore allowing Mentol Pro access to view what SIP users are registered and access to all information that page offers. To setup this user, log into System Manager as the Administrator and enter the password and click **Log On**.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

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

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

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

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

This system is restricted solely to authorized users for legitimate business 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.

All users must comply with all corporate instructions regarding the protection of information assets.

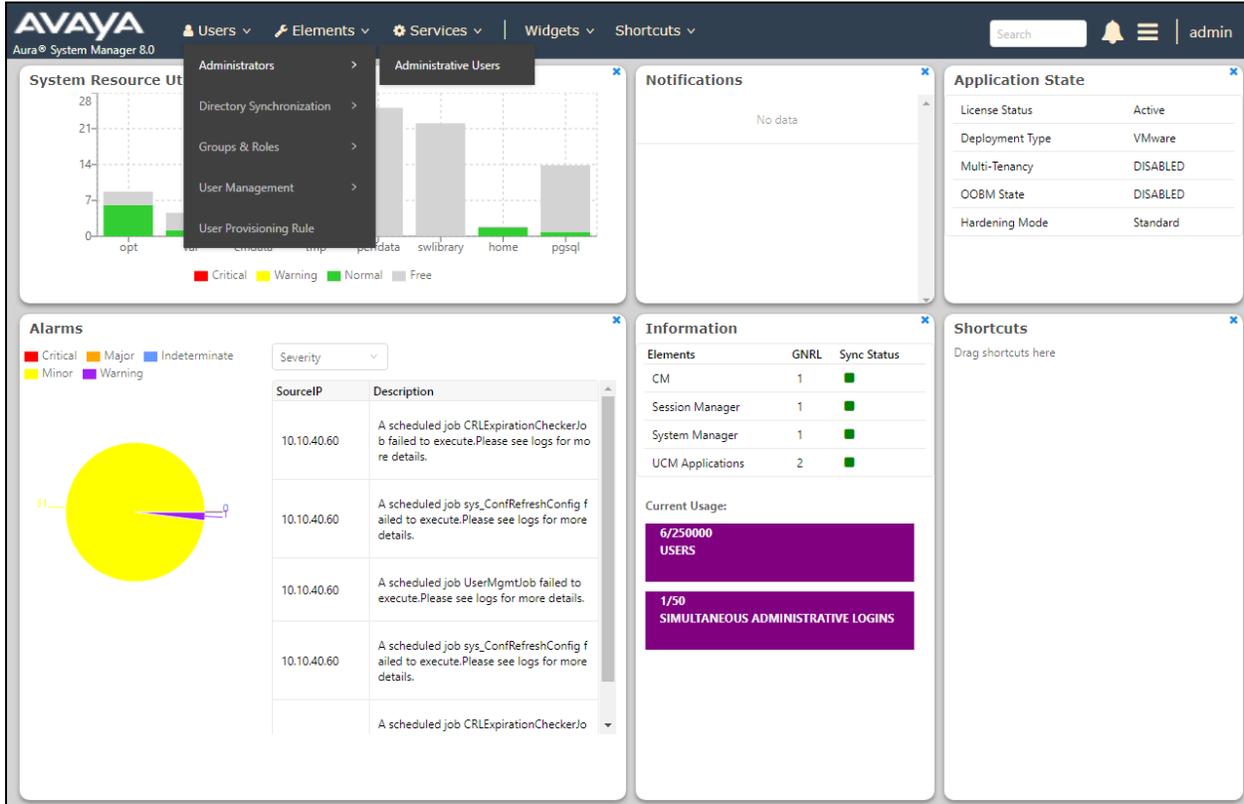
User ID:

Password:

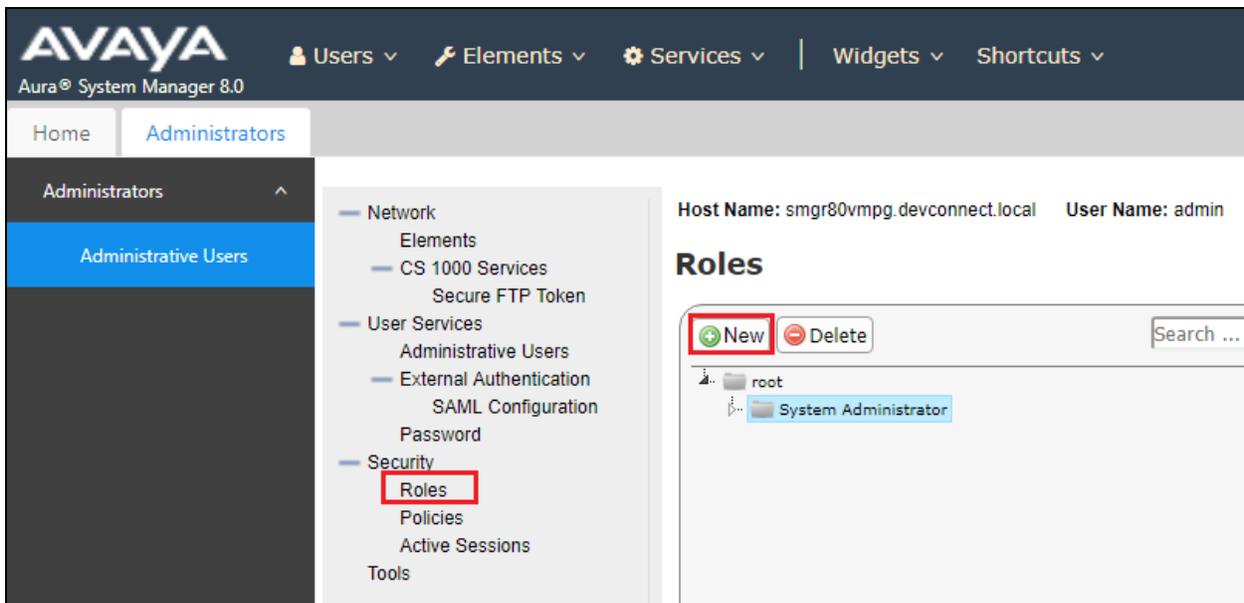
[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

Once logged in, navigate to **Users** → **Administrators** → **Administrative Users**.



Navigate to **Security** → **Roles** in the left window and click on **New** in the main window. Ensure that **System Administrator** is highlighted in the main window before you click on **New**.



Enter the appropriate name and description for the role. At the bottom of the screen, click on **Add Mapping** under the **Element Service Permissions** tab.

The screenshot shows the 'Role Details (MentolPro)' configuration page. At the top, it displays 'Host Name: smgr80vmpg.devconnect.local' and 'User Name: admin'. The page is divided into two main sections: 'Identification' and 'Element/Service Permissions'. The 'Identification' section contains fields for 'Parent Role Name' (System Administrator), 'Role Name' (MentolPro), and 'Description' (Used for check for SIP Registrations). Below these fields are 'Commit' and 'Cancel' buttons. The 'Element/Service Permissions' section is currently selected, showing 'Add Mapping...', 'Delete Mapping', and 'Copy All From...' buttons. Below these buttons is a table with columns for 'Name' and 'Permissions', which is currently empty.

For **Element or Resource Type**, select **Session Manager and Routing**. **Element or Resource Instance** should be selected as **All** and click on **Next** to continue.

The screenshot shows the 'Select Element and/or Network Service to Map to Role (MentolPro)' configuration page. It features three dropdown menus: 'Group Name' (--- No Group Selected ---), 'Element or Resource Type' (Session Manager and Routing), and 'Element or Resource Instance' (All). At the bottom of the page, there are 'Next' and 'Cancel' buttons.

The following screen will be displayed. Scroll down the screen to User Registrations.

Host Name: smgr80vmppg.devconnect.local User Name: admin

Permission Mapping (All elements of type: Session Manager and Routing for 'MentorPro')

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.
Template for permission set: Default Session Manager and Routing Permissions ▾

Role: MentorPro

Select / Unselect All

Session Manager and Routing:

Read/write access to all web pages under the Session Manager and Routing tabs Read-only access to all web pages under the Session Manager and Routing tabs

- ▶ Dashboard:
- ▶ Session Manager Administration:
- ▶ Communication Profile Editor:
- ▶ Local Host Name Resolution:
- ▶ Remote Access:
- ▶ SIP Firewall Configuration and Status:
- ▶ Device Settings Groups:
- ▶ Location Settings:
- ▶ Applications and Application Sequences:

Expand **User Registrations** and select **User Registrations Read-only**. Click on **Commit** at the bottom of the screen.

Permission Mapping (All elements of type: Session Manager and Routing for 'MentorPro')

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.
Template for permission set: Default Session Manager and Routing Permissions ▾

- ▶ Conference Factories:
- ▶ Implicit Users:
- ▶ NRS Proxy Users:
- ▶ SIP Entity Monitoring:
- ▶ Managed Bandwidth Usage:
- ▶ Security Module Status:
- ▶ Registration Summary:
- User Registrations:**
 - User Registrations Read-only User Registrations Read/Write
- ▶ Session Counts:
- ▶ User Data Storage:
- ▶ Maintenance Tests:
- ▶ SIP Tracer Configuration:
- ▶ SIP Trace Viewer:
- ▶ Call Routing Tests:

With the **Element/Service Permissions** set, click on **Commit** to save the new **Role**.

Role Details (MentolPro)

Identification

Parent Role Name: System Administrator

Role Name: (1-256) (Allowed characters are a-z, A-Z, 0-9, -, _ and space)

Description: Minimum 1 character

Commit **Cancel**

Element/Service Permissions **Assigned Users**

Add Mapping... **Delete Mapping** **Copy All From...**

<input type="checkbox"/>	Name	Permissions
1 <input type="checkbox"/>	All elements of type: Session Manager and Routing	User Registrations Read-only

A new User is now added from Mentol Pro to use. This new user will be assigned the Role created above with access to User Registrations only. Navigate to **User Services** → **Administrative Users** in the left window and click on **Add** in the main window.

Host Name: smgr80vmppg.devconnect.local User Name: admin [Help](#)

Administrative Users

Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to [Active Sessions](#) for currently logged in users and session management functions.

Add... **Disable** **Delete** [Refresh](#)

<input type="checkbox"/>	User ID ▲	Name	Roles	Type	Account Status
1 <input type="checkbox"/>	admin	Default security administrator	System Administrator	Local	Enabled
2 <input type="checkbox"/>	avaya_services_administrator	avaya_services_administrator	Avaya Services Administrator	External	Enabled
3 <input type="checkbox"/>	avaya_services_maintenance_and_support	avaya_services_maintenance_and_support	Avaya Services Maintenance and Support	External	Enabled
4 <input type="checkbox"/>	craft	craft	Avaya Services Maintenance and Support	External	Enabled
5 <input type="checkbox"/>	init	init	System Administrator	External	Enabled

Enter a suitable Full Name and Password, click on **Select Roles** to assign the new role to this user.

User Details (mentolpro)

Set user properties and assign predefined Roles.

User Status: Enabled Disabled

Full Name:

Authentication Type: Local External

Password Reset:

Password:

Re-enter password:

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

User ID:

E-Mail:

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

Roles

Role Name	Elements	Description

Scroll down until the newly created Role is found. Tick the box beside the role and click on **Commit** at the bottom of the screen.

User Roles (mentolpro)

Selected roles authorize the user for associated features and element permissions.

Roles

<input type="checkbox"/>	18 FIPS140-2 Crypto Officer	Gives read-write access to Security Link
<input type="checkbox"/>	19 MemberRegistrar	Member Registrar Role
<input checked="" type="checkbox"/>	20 MentolPro	Used for check for SIP Registrations
<input type="checkbox"/>	21 Messaging System Admin	Gives access to perform all activities related to Messaging or Mailbox. A user with this role cannot perform any tasks related to Communication Manager as a Modular Messaging administrator.
<input type="checkbox"/>	22 Patcher	Provides access to software maintenance functions such as update and maintenance.
<input type="checkbox"/>	23 Presence Admin	Gives read-write access to the Presence configuration.
<input type="checkbox"/>	24	Gives read-only access to logs, configuration information and

With the new role assigned to the new user, click on **Commit** to finish.

User Details (mentolpro)
Set user properties and assign predefined Roles.

User Status: Enabled Disabled

Full Name:

Authentication Type: Local External

Password Reset:

Password:

Re-enter password:

User ID:

E-Mail:

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.

Roles

Role Name	Elements	Description
MentolPro		Used for check for SIP Registrations

This new user can now log into System Manager and view the User Registrations, this will give information on the SIP users and allow Mentol Pro display this to the end user on their dashboard.

7. Configure Inline Pro Mentol Pro

The installation of Mentol Pro is performed by engineers from Inline Pro and involves a number of complex configurations. Therefore, the visual display of this setup is not possible. For information on the installation and configuration of Mentol Pro please contact Inline Pro from the information provided in **Section 2.3**.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Mentol Pro.

8.1. Verify Communication Manager

Verify that Mentol Pro has established a connection to the SAT by using the **status logins** command. The user **mentolpro** is shown below and can be seen as being logged in.

```
status logins

COMMUNICATION MANAGER LOGIN INFORMATION

Login      Profile  User's Address      Active Command      Session
mentolpr   66      10.10.40.120
*init      0       10.10.40.241      stat logins         3
```

Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.4** shows **up**.

```
status cdr-link

CDR LINK STATUS

Primary      Secondary
Link State: up      down
Number of Retries:    999
Date & Time: 2018/08/22 04:46:46    0000/00/00 00:00:00
Forward Seq. No: 0      0
Backward Seq. No: 0    0
CDR Buffer % Full: 0.00    0.05
Reason Code: OK      Maintenance busy
```

Wireshark can be used to check what data is being sent to Mentol Pro. From the Mentol Pro server open Wireshark and the filter can be changed to filter in such messages as RTCP, CDR and SNMP. The example below shows RTCP packets being received one containing the make and model of the phone making the call.

The screenshot shows the Wireshark interface with the following details:

- Filter:** rtcp
- Packet List:**

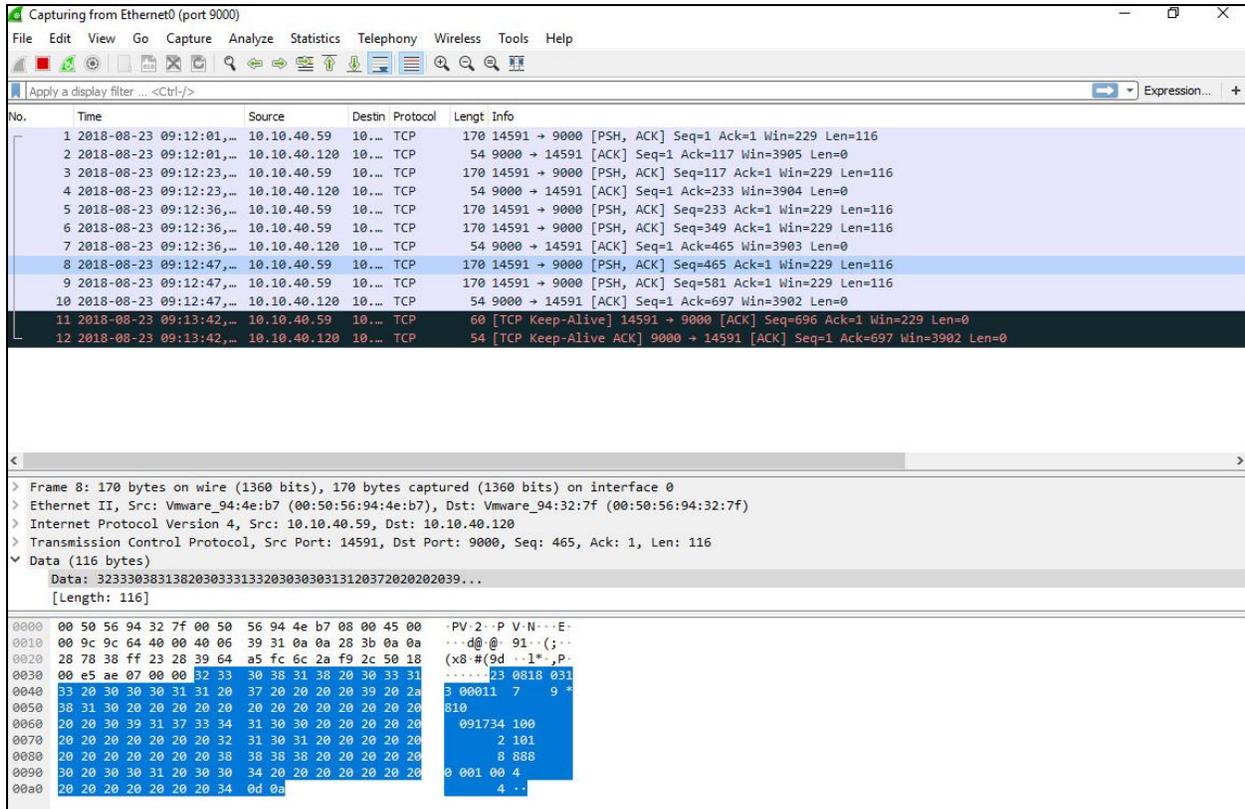
No.	Time	Source	Destin	Protocol	Length	Info
4394	2018-08-22 10:57:18,...	10.10.40.120	10...	ICMP	294	Destination unreachable (Port unreachable)
4409	2018-08-22 10:57:18,...	10.10.40.224	10...	RTCP	250	Sender Report Source description Application specific (-AV-) subtype=4Application specific (-AV-) subtyp
4410	2018-08-22 10:57:18,...	10.10.40.120	10...	ICMP	278	Destination unreachable (Port unreachable)
4674	2018-08-22 10:57:22,...	10.10.40.189	10...	RTCP	274	Sender Report Source description Application specific (-AV-) subtype=3Application specific (-AV-) subtyp
4675	2018-08-22 10:57:22,...	10.10.40.120	10...	ICMP	302	Destination unreachable (Port unreachable)
4888	2018-08-22 10:57:23,...	10.10.40.224	10...	RTCP	214	Sender Report Source description Application specific (-AV-) subtype=4Application specific (-AV-) subtyp
4889	2018-08-22 10:57:23,...	10.10.40.120	10...	ICMP	242	Destination unreachable (Port unreachable)
5340	2018-08-22 10:57:28,...	10.10.40.224	10...	RTCP	210	Sender Report Source description Application specific (-AV-) subtype=4Application specific (-AV-) subtyp
5341	2018-08-22 10:57:28,...	10.10.40.120	10...	ICMP	238	Destination unreachable (Port unreachable)
5392	2018-08-22 10:57:29,...	10.10.40.189	10...	RTCP	258	Sender Report Source description Application specific (-AV-) subtype=1Application specific (-AV-) subtyp
5393	2018-08-22 10:57:29,...	10.10.40.120	10...	ICMP	286	Destination unreachable (Port unreachable)
5718	2018-08-22 10:57:32,...	10.10.40.189	10...	RTCP	258	Sender Report Source description Application specific (-AV-) subtype=1Application specific (-AV-) subtyp
5719	2018-08-22 10:57:32,...	10.10.40.120	10...	ICMP	286	Destination unreachable (Port unreachable)
5783	2018-08-22 10:57:33,...	10.10.40.224	10...	RTCP	218	Sender Report Source description Application specific (-AV-) subtype=4Application specific (-AV-) subtyp
5784	2018-08-22 10:57:33,...	10.10.40.120	10...	ICMP	246	Destination unreachable (Port unreachable)
5873	2018-08-22 10:57:35,...	10.10.40.189	10...	RTCP	258	Sender Report Source description Application specific (-AV-) subtype=1Application specific (-AV-) subtyp
5874	2018-08-22 10:57:35,...	10.10.40.120	10...	ICMP	286	Destination unreachable (Port unreachable)
- Packet Details:**
 - 10... = Version: RFC 1889 Version (2)
 - ..0... = Padding: False
 - Subtype: 1
 - Packet type: Application specific (204)
 - Length: 4 (20 bytes)
 - Identifier: 0xcc74aa09 (3430197769)
 - Name (ASCII): -AV-
 - Application specific data: 00000273000107e0
 - Real-time Transport Control Protocol (Application specific)
 - 10... = Version: RFC 1889 Version (2)
 - ..0... = Padding: False
 - Subtype: 4
 - Packet type: Application specific (204)
 - Length: 14 (60 bytes)
- Packet Bytes:**

```

0000 00 50 56 94 32 7f 50 cd 22 b4 6c 1a 08 00 45 00  ·PV·2·P·"·1·...E·
0010 01 18 00 00 40 00 11 d4 8c 0a 0a 28 bd 0a 0a  ·...@·@·...(:·
0020 28 78 08 e9 13 8d 01 04 e6 56 81 c8 00 0c cc 74  (x·...·V·...t·
0030 aa 09 5b 7c ed 52 0c 76 10 00 88 7b 57 26 00 00  ·[·]·R·v·...{W&·
0040 02 73 00 01 87 e0 70 91 a6 57 00 00 00 00 00 00  ·s·...p·W·...·
0050 0e 57 00 00 00 00 e8 da 11 eb 00 01 98 55 81 ca  ·g·...·...U·...
0060 00 17 cc 74 aa 09 01 19 65 78 74 32 30 30 30 40  ·...t·...ext2000@·
0070 31 30 2e 31 30 2e 34 30 2e 31 38 39 3a 32 32 37  10.10.40 .189:227·
0080 38 04 04 32 30 30 06 33 41 76 61 79 61 20 49  8·:2000 3Avaya I·
0090 50 20 54 65 6c 65 70 68 6f 6e 65 20 28 53 39 36  P Teleph one (596·
00a0 30 38 5f 31 31 48 41 4c 42 52 36 5f 36 5f 36 5f  08 11HAL BR6 6 6·
00b0 30 34 5f 56 34 37 34 2e 74 61 72 28 00 00 81 cc  04 V474. tar)·...
00c0 00 04 cc 74 aa 09 2d 41 56 2d 00 00 02 73 00 01  ·...t·-A V·...s·
00d0 87 e0 84 cc 00 0e cc 74 aa 09 2d 41 56 2d 70 91  ·...t·-AV-p·...
00e0 a6 57 df b7 d0 00 00 00 02 73 00 01 87 e0 00 28  ·W·...·s·...·(·
00f0 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ·...·...·...·
0100 0a 0a 28 e0 13 8d 08 14 00 2e 00 00 00 00 85 cc  ·(·...·...·...·
0110 00 05 cc 74 aa 09 2d 41 56 2d 70 91 a6 57 80 00  ·...t·-A V-p·W·...

```

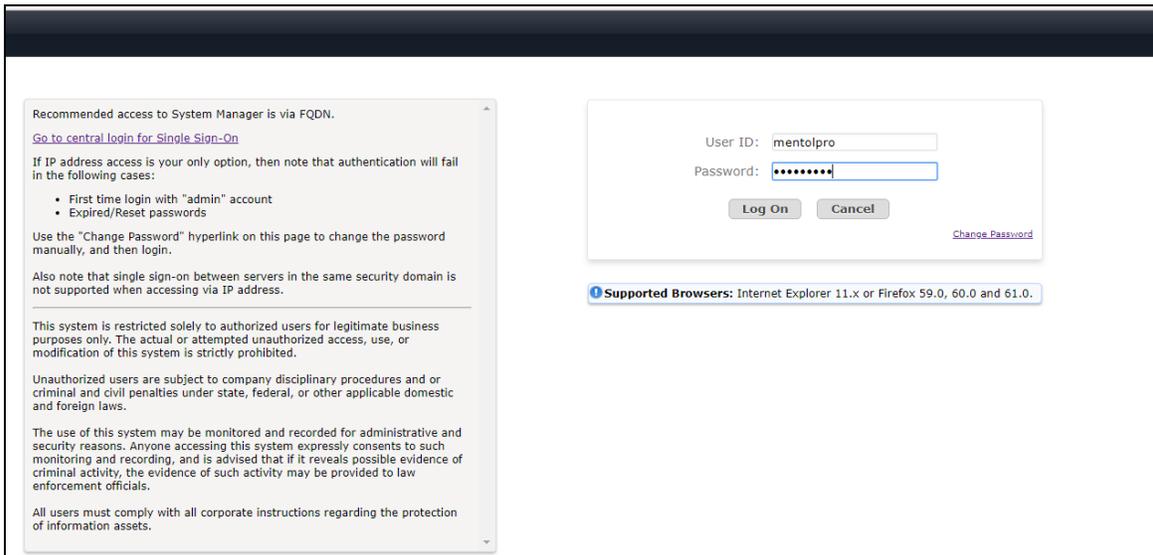
The following Wireshark collection filters on **port 9000** which is the port used to collect CDR information. Information on the caller is displayed in the highlighted section at the bottom of the screen.



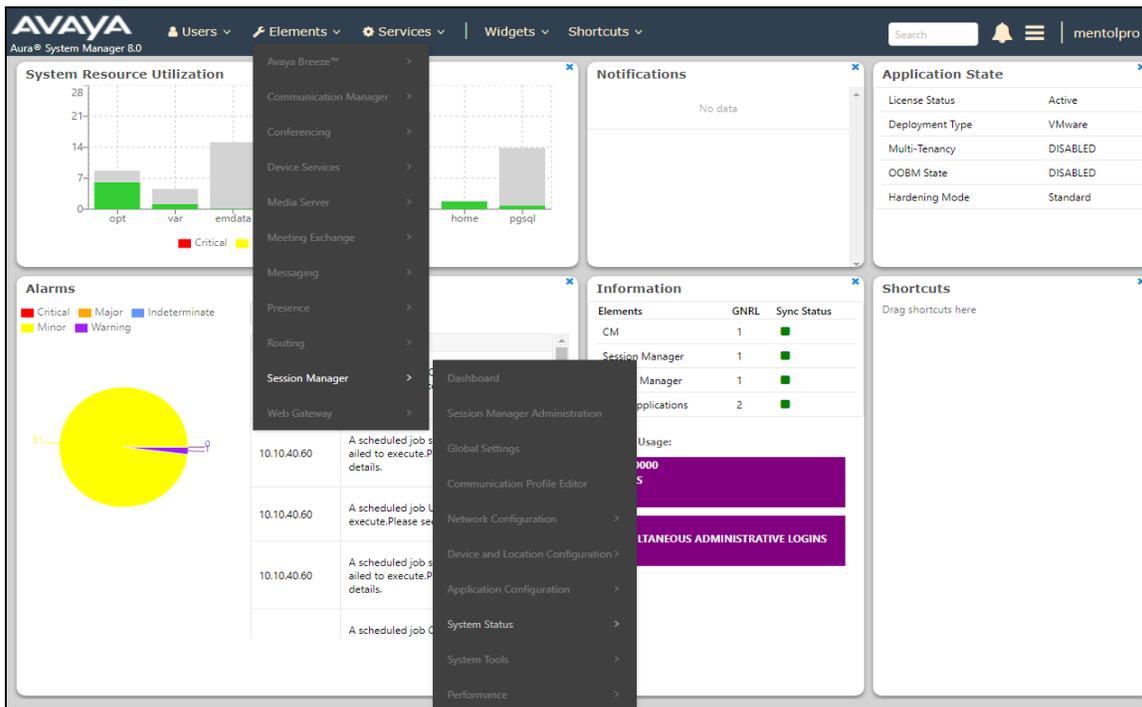
Note: Wireshark can be used to display SNMP, RTCP, CDR, any information that is sent to Mentol Pro can be displayed here and verified if required as long as the correct filter is applied to show the information required.

8.2. Verify System Manager User

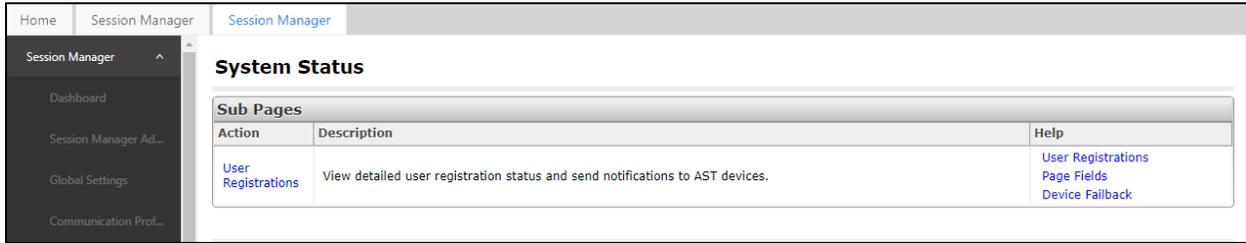
To verify that the connection is setup correctly to System Manager, log into System Manager using the user credentials created in **Section 6**. This user should have access to view the User Registrations page and this will verify that the connection to System Manager was setup correctly. Open the web page to the System Manager and enter the appropriate credentials.



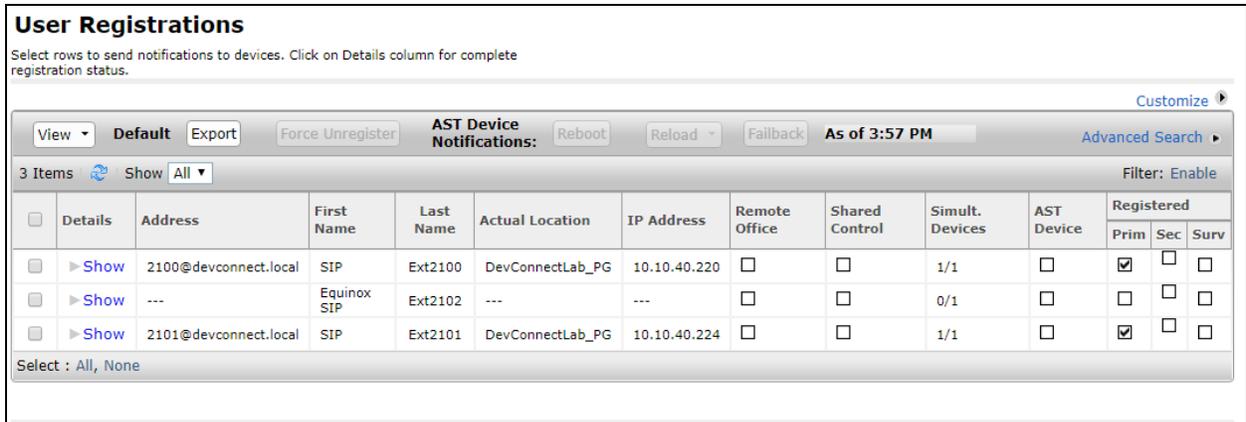
Under **Elements** the only selection available should be **Session Manager** and under Session Manager the only selection available should be **System Status**, click on **System Status**.



Under **System Status** the only selection available is **User Registrations**, click on **User Registrations**.

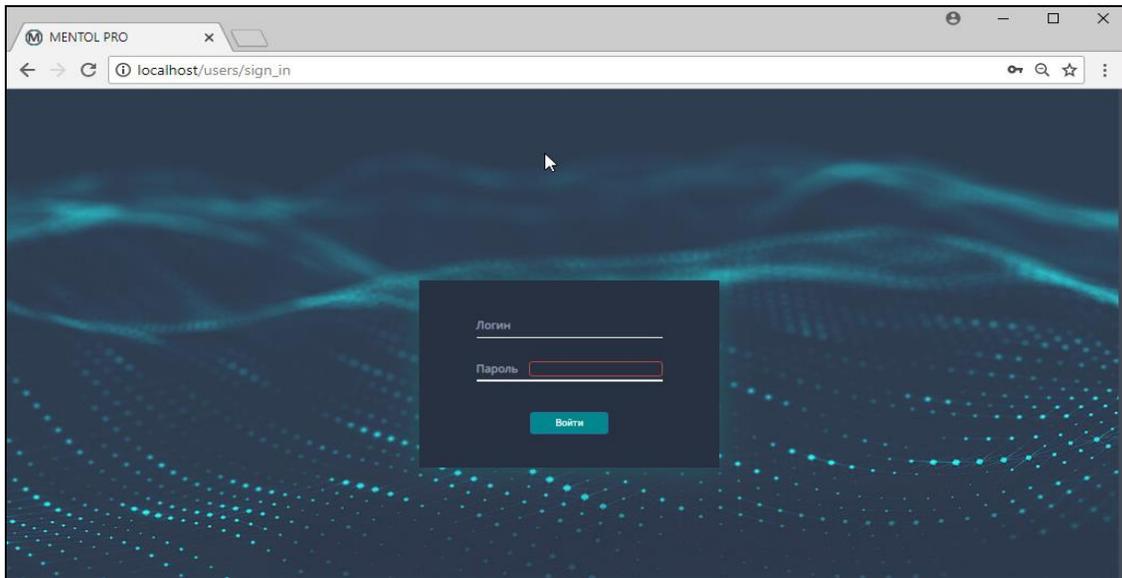


All the information on SIP users configured on System Manager is available to view here. This verifies that Mentol Pro has access to this information and that the connection to System Manager is setup successfully.

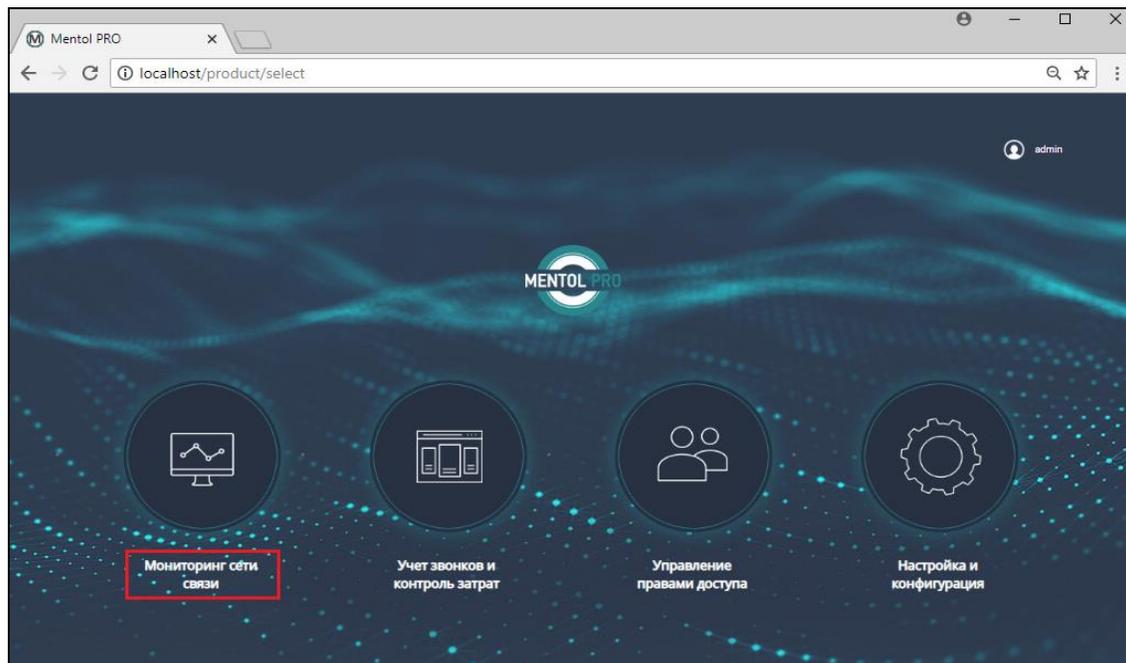


8.3. Verify Mentol Pro is Configured

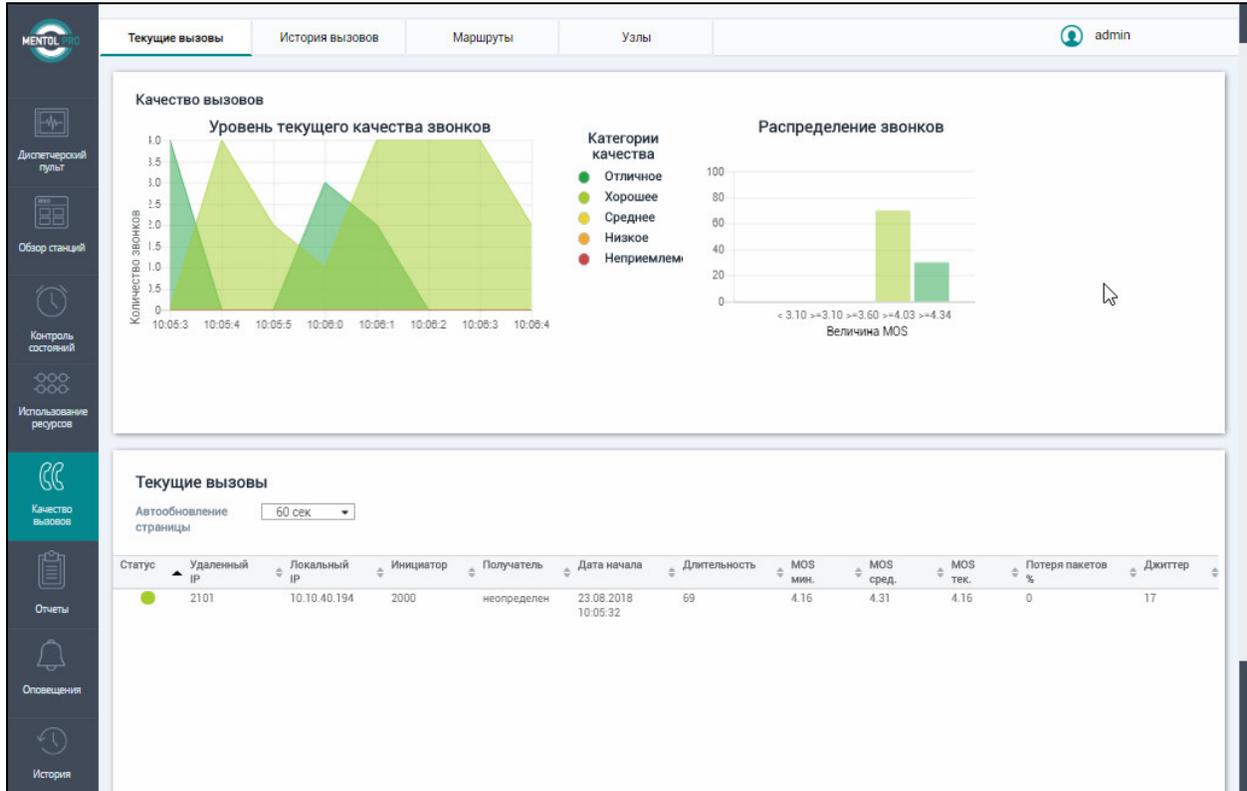
To verify that Mentol Pro is receiving and processing data from Communication Manager and System Manager open the Mentol Pro Dashboard and navigate through the various screens displaying this information. By accessing the web interface, information on calls and on Communication Manager should be visible. Open a http session to the Mentol Pro server, enter the appropriate credentials and click on the login button underneath.



Click on the Monitoring screen icon, highlighted below.



Information on a call shown below is provided using the RTCP connection to Communication Manager.



9. Conclusion

These Application Notes describe the procedures for configuring Inline Pro Mentol Pro to interoperate with Avaya Aura® Communication Manager R8.0 and Avaya Aura® System Manager R8.0. In the configuration described in these Application Notes, Mentol Pro established several connections with Communication Manager to view the configuration of Communication Manager. Mentol Pro also processed the RTCP information to monitor the quality of IP calls and collected CDR information sent by Communication Manager. Mentol Pro also obtained the Communication Manager name and IP address from the SNMP information. A connection to System Manager was established to view SIP user registrations. During compliance testing, all test cases were completed successfully.

10. Additional References

The following Avaya documentations can be obtained on the <http://support.avaya.com>.

- [1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0.1, 555-245-205, Issue 2, May 2016.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1, July 2018.
- [3] *Administering Avaya Aura® System Manager*, Release 8.0, Issue 3, September 2018.

Mentol Pro documentation are provided by contacting Inline Pro.

©2018 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.