



Avaya Solution & Interoperability Test Lab

Application Notes for Virsae Service Management for Unified communications with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Virsae Service Management for Unified Communications to interoperate with Avaya Aura® Communication Manager.

Virsae Service Management provides real-time monitoring and management solutions for IP telephony networks. Virsae Service Management 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.

Virsae Service Management 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, Virsae Service Management processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Virsae Service Management for Unified Communications (herein after referred to as VSM) with Avaya Aura® Communication Manager. VSM is a cloud-based service management platform that brings visibility, service transparency and cost savings to Unified Communications environments over the short, medium and long term.

The VSM product uses five integration methods to monitor a Communication Manager system.

- System Access Terminal (SAT) - The VSM uses a pool of Telnet/SSH connections to the SAT using the IP address of Communication Manager. By default, the solution establishes one Linux Shell connection and four concurrent SAT connections to each Communication Manager system and uses the connections to execute SAT commands. Communication Manager name and IP address is collected using the Linux shell command.
- Real Time Transport Control Protocol (RTCP) collection - VSM collects RTCP information sent by Avaya resources including IP Media Processor (MEDPRO) boards, media gateways, media servers and IP Deskphones.
- Call Detail Recording (CDR) collection - VSM collects CDR information sent by Communication Manager.
- Simple Network Management Protocol (SNMP) –VSM uses SNMP to capture the alarms.
- SFTP – VSM uses SFTP to collect the backup files from Communication Manager.

2. General Test Approach and Test Results

The general test approach was to use VSM web user interface (dashboard) and historical reporting 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 VSM dashboard and historical reporting was used to display the RTCP and CDR information collected. SNMP collection of alarms were also verified. VSM also collects the Syslog and backup files from Communication Manager and uses the Syslog file to parse the change logs.

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 the testing associated with these Application Notes, the interface between Avaya systems and VSM utilized capabilities of SSH as requested by Virsae.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations

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 the SAT interface as a programmatic approach to integration of 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 PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

For feature testing, VSM dashboard was used to view the configurations of Communication Manager via collected SAT data such as port networks, cabinets, media gateways, media servers, trunk groups, route patterns, DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. VSM dashboard was also used to view the Communication Manager name and IP address.

For the collection of RTCP and CDR information, the endpoints included Avaya H323, SIP, Equinox for Windows, digital and analog endpoints. The types of calls made included intra-switch calls, inbound/outbound trunk calls using both SIP and ISDN PRI trunks, transfer and conference calls. A backup schedule was configured for collecting Communication Manager backups and different logging levels were setup to collect Syslogs. The change logs were collected by parsing the Syslogs collected by VSM.

For serviceability testing, reboots were applied to VSM and removal of ethernet connection to VSM was also implemented.

2.2. Test Results

All test cases passed successfully with the following observations.

- A total of only five sessions with same credentials can be established with Communication Manager.
- If user encounters an issue where Communication Manager stops logging to command history, refer to PSN# PSN020269u for workaround.

2.3. Support

For technical support on Virsae Service Management, contact the Virsae Support Team at:

- Tel: +1 800 248 7080 (Americas)
+44 0808 234 2729 (UK and Europe)
+64 9 477 0696 (Asia Pacific)
- Email: support@virsae.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify VSM interoperability with Communication Manager. The configuration consists of a Communication Manager system with an Avaya G450 Media Gateway. The system has Avaya H323, SIP, Equinox for Windows, digital and analog endpoints configured for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. VSM was installed on a server running Microsoft Windows Server 2012 R2 with Service Pack 1. Architecturally the VSM Service relies on an appliance being placed on a corporate LAN and being configured to connect to a Unified Communication platform as well as the Microsoft Azure cloud via the internet. The VSM appliance acts as a collector and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service. A PC/Laptop is used to access the Virsae portal to manage VSM services, add additional users and view reporting data on the equipment being managed.

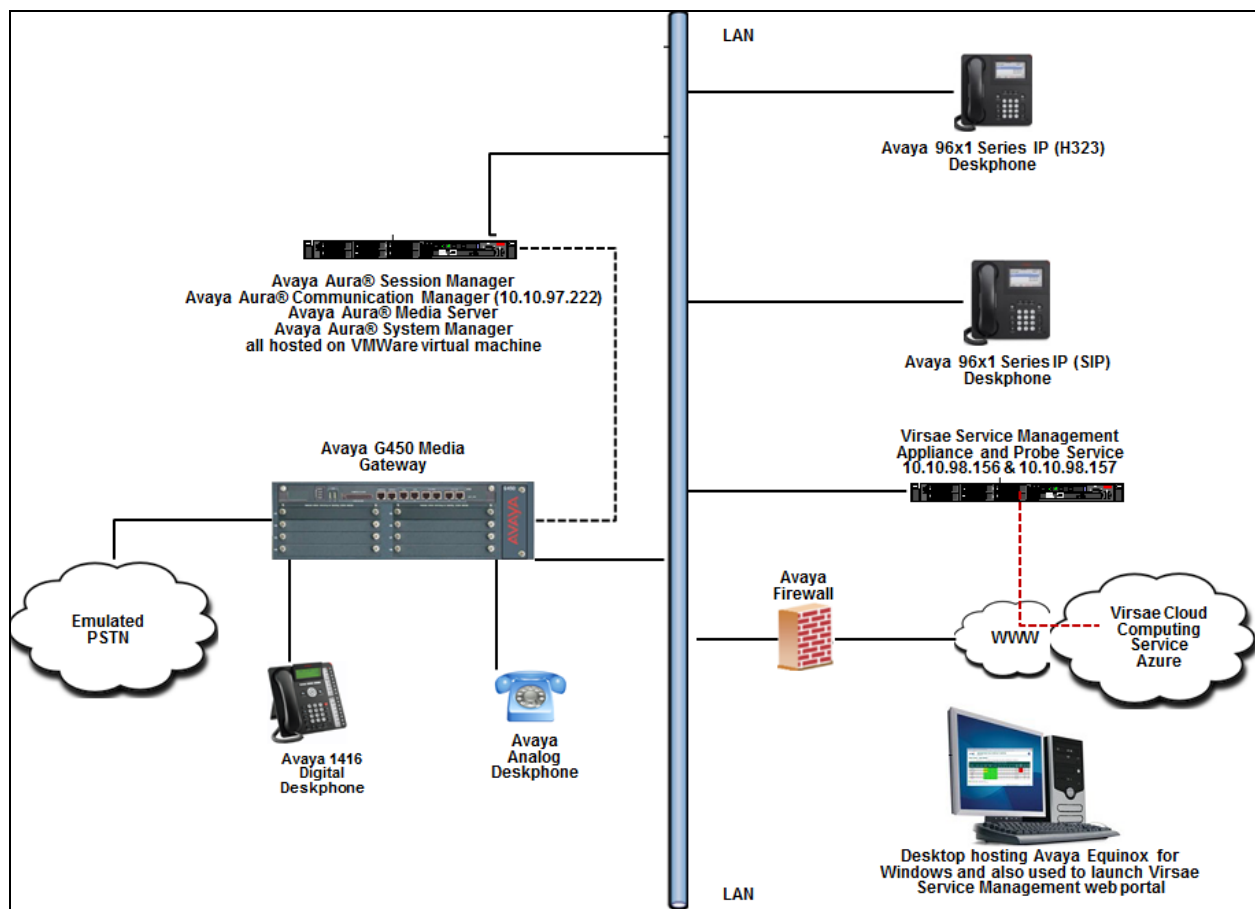


Figure 1: Test Configuration

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 running on virtual server	08.0.0.0.822
Avaya Aura® Media Server running on virtual server	8.0.0.117
Avaya G450 Media Gateway	40.10.0/1
Avaya Aura® System Manager running on virtual server	8.0.0.0.931077
Avaya Aura® Session Manager running on virtual server	8.0.0.0.800035
Avaya IP Deskphones - 9641GS (H.323) - 9611G (SIP)	6.6604 7.1.3.0.8
Avaya Equinox for Windows	3.4.0.152.46-ACW- INTEGRATIONNEXUS1
Avaya 1416 Digital Deskphone	15
Avaya 500 Analog Deskphone	N/A
VSM running on Windows 2012 R2 SP1	89.0.2.185

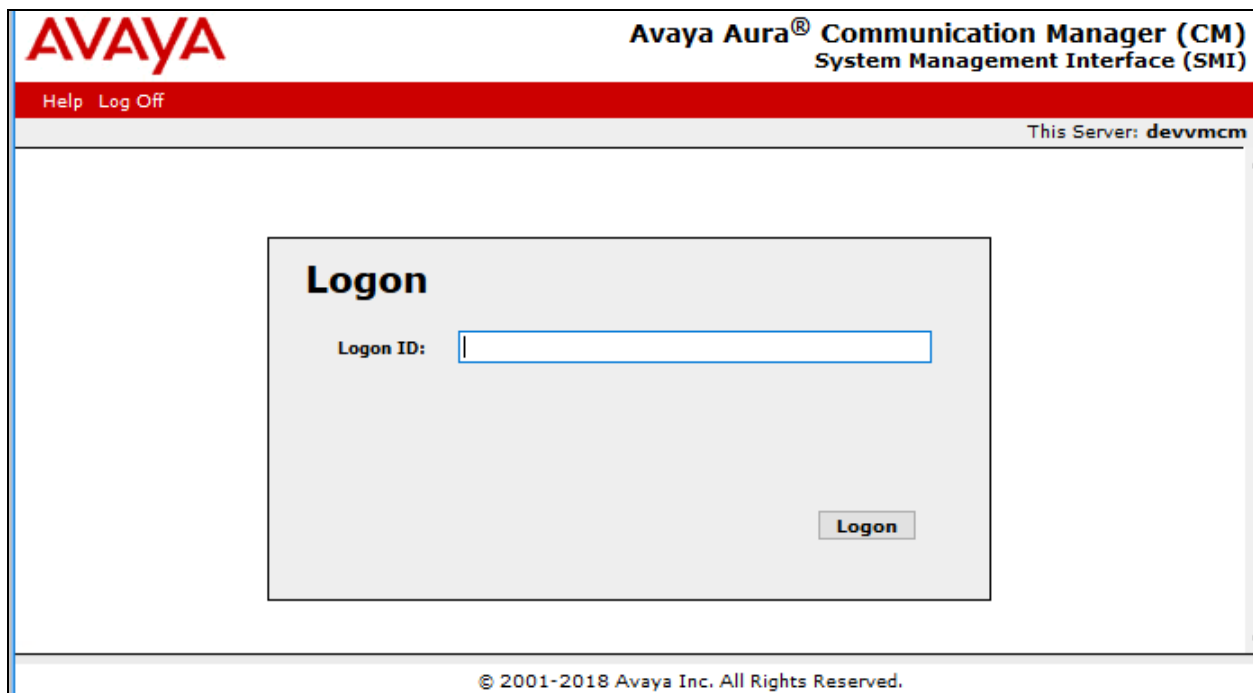
5. Configure Avaya Aura® Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with VSM. This includes creating a login account and a SAT User Profile for VSM to access Communication Manager and enabling SNMP, RTCP and CDR reporting.

5.1. Configure Login Group

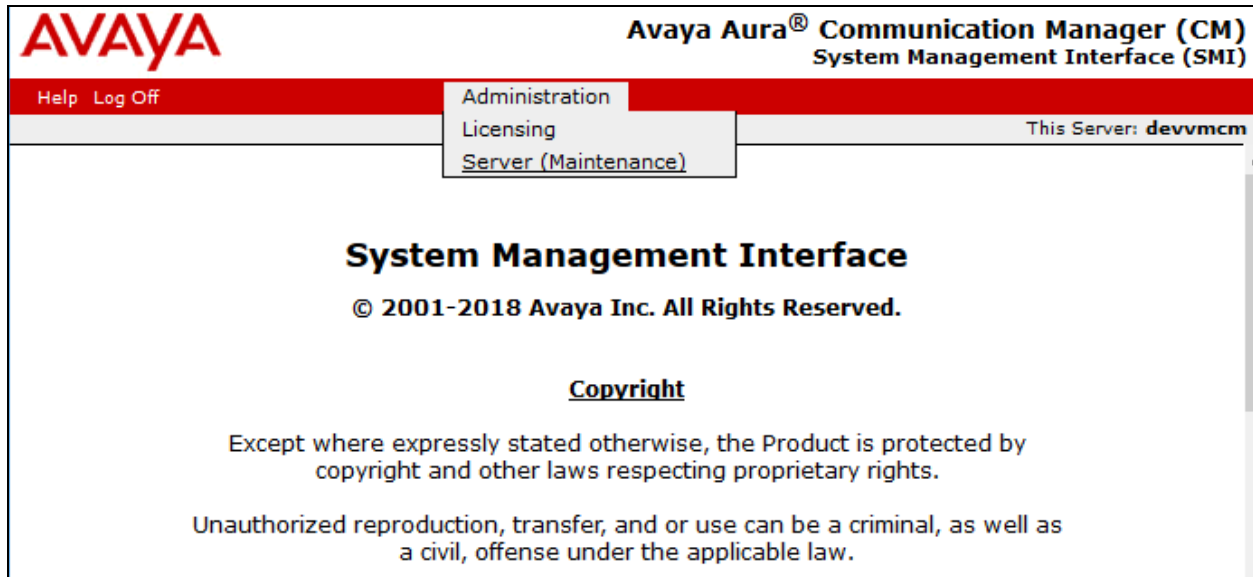
Create an Privileged Administrator account on Communication Manager System Management Interface (SMI) so that the VSM Probe can access Communication Manager with Super User rights. This can be achieved by creating a new user within Communication Manager with user profile 18.

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.



The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) login page. The page has a red header bar with the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header, there is a red bar with "Help" and "Log Off" links. On the right side of the page, it says "This Server: devvmcm". The main content area is a light gray box with the title "Logon". Inside this box, there is a label "Logon ID:" followed by a text input field. Below the input field is a "Logon" button. At the bottom of the page, there is a copyright notice: "© 2001-2018 Avaya Inc. All Rights Reserved."


Click **Administration** → **Server (Maintenance)**. This will open the **Server Administration Interface** that will allow the user to complete the configuration process.



Create a login account for VSM to access the Communication Manager SAT. Repeat this for each Communication Manager. From the navigation panel on the left side, navigate to **Security** → **Administrator Accounts**. Select **Add Login** and **Privileged Administrator** to create a new login account with privileged rights. Click **Submit**.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top header includes the Avaya logo and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)". Below the header, a red navigation bar contains "Help Log Off" and "Administration". The main content area is titled "Administrator Accounts" and includes a description: "The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups." Under the heading "Select Action:", there are several radio button options: "Add Login" (selected), "Privileged Administrator" (selected), "Unprivileged Administrator", "SAT Access Only", "Web Access Only", "CDR Access Only", "Business Partner Login (dadmin)", "Business Partner Craft Login", and "Custom Login". Below these are three sets of radio buttons for "Change Login", "Remove Login", and "Lock/Unlock Login", each with a "Select Login" dropdown menu. At the bottom, there are radio buttons for "Add Group" and "Remove Group", with a "Select Group" dropdown menu. The left sidebar contains a navigation menu with categories like "Server Date/Time", "Software Version", "Server Configuration", "Server Upgrades", "IPSI Firmware Upgrades", "Data Backup/Restore", and "Security". The "Security" category is expanded, showing "Administrator Accounts" as the selected option. At the bottom of the main content area, there are "Submit" and "Help" buttons.

For the field **Login name**, enter the login. In this configuration, the login **Virsa** is created along with the password for this user. Retain default values for all other fields. Click **Submit** to continue.



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

[Help](#) [Log Off](#)

Administration

Administration / Server (Maintenance)
This Server: devvmcm

Static Routes
Display Configuration
Time Zone Configuration
NTP Configuration
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
Miscellaneous
File Synchronization
Download Files

Administrator Accounts -- Add Login: Privileged Administrator

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

Login name

Virsa

Primary group

susers

Additional groups (profile)

prof18

Linux shell

/bin/bash

Home directory

/var/home/Virsa

Lock this account

☐

SAT Limit

none

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

Enter password

.....

Re-enter password

.....

Force password change on next login

☒ No
☐ Yes

Submit

Cancel

Help

5.2. Configure SNMP

SNMP is used to capture alarms raised by Avaya Communication Manager. To make changes to SNMP configuration the Master Agent must first be stopped by clicking the ‘Stop Agent’ button.

Access the Communication Manager System Management Interface as in **Section 5.1**. Click on **SNMP → Agent Status**. Click **Stop the Master Agent** if the **Master Agent status** is **UP** to allow setup of SNMP Agent.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The interface has a red header bar with the Avaya logo and the title 'Avaya Aura® Communication Manager (CM) System Management Interface (SMI)'. Below the header, there is a navigation menu on the left and a main content area on the right. The navigation menu includes sections like Alarms, SNMP, Diagnostics, Server, and Server Configuration. The 'SNMP' section is expanded, showing 'Agent Status' as the selected option. The main content area displays the 'Agent Status' page, which includes a description of the page's purpose, a status summary for the Master Agent and Sub Agents, and buttons for 'Stop Master Agent' and 'Help'.

Section	Item
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
	Shutdown Server
	Server Date/Time
	Software Version
Server Configuration	Server Role
	Network Configuration

Agent Status

The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

All of the Sub Agents are connected to the Master Agent.

Master Agent status: UP

Sub Agent Status

FP Agent status: UP

CMSubAgent status: UP

Load Agent status: UP

Stop Master Agent **Help**

To allow VSM to use SNMP to collect configuration and status information from Communication Manager, navigate to **SNMP → FP Traps** in the left pane. Click **Add/Change** button as shown below.

The screenshot displays the Avaya Aura Communication Manager System Management Interface. The left-hand navigation pane is expanded to show the 'FP Traps' option under the 'SNMP' category. The main content area is titled 'FP Traps' and includes a description: 'The FP Traps page allows specification of the traps to be sent as traps.' A yellow warning icon is present next to a 'Note' section, which states: 'The FP Traps SMI page is for the administration of CM Fault Performance only. It is not for INADS. INADS traps are configured using the "almenable" and the "almsnmpconf" CLI command. Additional Fault Performance Traps should not be sent to SAL IP Addresses.' Below the note, the 'Master Agent status' is shown as 'UP'. A link 'View AVAYA-AURA-CM-ALARM-MIB Data' is provided. Under the 'Current Settings' section, there is a table with four columns: 'IP address', 'Port', 'Notification', and 'SNMP Version'. The 'SNMP Version' column contains a dropdown menu with 'v2c' selected. At the bottom of the page, there are three buttons: 'Add/Change', 'Delete', and 'Help'.

Configure the **SNMP Version 2c** section. Set the **IP address** to the VSM probe and **Notification** as **trap** from the drop-down menu. During compliance testing, **Community Name** field was set to **public**. Retain the default **Port** value and click **Submit** button.

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

Help Log Off Administration

Administration / Server (Maintenance) This Server: devvmcm

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:

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:

Lastly, the SNMP agent must be started. Navigate to **SNMP → Agent Status** as shown in the beginning of this Section. If the **Master Agent status** is **DOWN**, then click the **Start Master Agent** button (not shown). If the **Master Agent status** is **UP**, then the agent must be stopped and restarted.

Communication Manager also needs to be configured to send INADS alarm information to VSM via SNMP. This is done via the shell command “almsnmpconf”. To use this command, log into the Communication Manager server Linux prompt. Execute the command:

```
almsnmpconf [-d IP] [-c community];
```

where IP is the VSM Probe IP and community string used during compliance testing was **public**.

Check that the INAD SNMP alarms are enabled by executing the following command:

```
almenable
```

If the output is as below:

```
SNMP Alarm Origination:      n
```

then execute the command `almenable -s y` to enable it.

Note: For customers with duplicated servers, this needs to be done on each server individually.

To complete the SNMP configuration in Communication Manager, the VSM probe server must be added to the IP Node names table as shown below.

From the SAT prompt, enter the command **change node-names ip** and add an entry for the VSM probe IP address as shown below.

change node-names ip		Page	1 of	2
		IP NODE NAMES		
Name	IP Address			
virsaesnmp	10.10.98.157			

The name created above will be used in the IP Options page as shown below by entering the command **change system-parameters ip-options** and configure the following in **Page 3**.

- **Download Flag?:** y; note that when set to yes as shown, then these settings will be downloaded to the phone and will overwrite any 46xxxSettings.txt file settings.
- **Community String:** public.
- **SOURCE ADDRESSES:** The node-name IP configured above.

This configuration allows VSM to request information via SNMP.

change system-parameters ip-options		Page	3 of	4
IP-OPTIONS SYSTEM PARAMETERS				
SNMP PARAMETERS				
Download Flag? y				
Community String: public				
SOURCE ADDRESSES				
1.	virsaesnmp	4.		
2.		5.		
3.		6.		
SERVICES DIAL PAD PARAMETERS		ALTERNATIVE NETWORK ADDRESS TYPES		
Download Flag? n		ANAT Enabled? n		
Password: *				
MUSIC/ANNOUNCEMENTS IP-CODEC PREFERENCES				
Prefer use of G.711 by Music Sources? n				
Prefer use of G.711 by Announcement Sources? n				
Prefer use of G.711 by IP Endpoints Listening to Music? n				
Prefer use of G.711 by IP Endpoints Listening to Announcements? n				

5.3. Configure External Syslog Server

The following changes are required to define the VSM Probe as an external destination for Communication Manager Syslog. Access the Communication Manager System Management Interface as in **Section 5.1**. Navigate to **Security → Server Log Files** and configure the following.

- Under **Control File Synchronization of Syslog Configuration** check the box for **When the Submit button is clicked, send syslog configuration to all LSP and ESS servers.**
- Under **Control Logging to an External Syslog Server**, select the radio button for **Enable logging to the following syslog server.**
- Enter the VSM Probe IP address for **server name** field.
- Check all the boxes under **Select Which Logs are to be Sent to the Above Server.**

Click on the **Submit** button to complete this configuration.

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

Help Log Off Administration This Server: devvmcm

Administration / Server (Maintenance)

Ping
Traceroute
Netstat

Server
Status Summary
Process Status
Shutdown Server
Server Date/Time
Software Version

Server Configuration
Server Role
Network Configuration
Static Routes
Display Configuration
Time Zone Configuration
NTP Configuration

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

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**

At the SAT terminal enter the command **change logging-levels** as shown below. On **Page 1** set the following values.

- **Enable Command Logging?:** **y**
- **Log Data Values:** **both**
- All Action Values (with the exception of **Display, Monitor** and **Status**) to **'y'**

```
change logging-levels                                     Page 1 of 2

                                LOGGING LEVELS

Enable Command Logging? y
Log Data Values: both

When enabled, log commands associated with the following actions:

      add? y          export? y          refresh? y
      busyout? y      get? n             release? y
campon-busyout? y    go? y             remove? y
      cancel? y      import? y          reset? y
      change? y      list? y           save? y
      clear? y       mark? y           set? y
      disable? y     monitor? n         status? n
      display? n     netstat? y         test? y
      duplicate? y   notify? y          traceroute? y
      enable? y      ping? y           upload? y
      erase? y       recycle? y
```

On **Page 2** set the **Log PMS/AD Transactions** field to **'y'**.

```
change logging-levels                                     Page 2 of 2

                                LOGGING LEVELS

Log All Submission Failures: y
Log PMS/AD Transactions: y
Log IP Registrations and events: y
Log CTA/PSA/TTI Transactions: y
```

5.4. Configure Off-Site Backups

The following changes are required to define the VSM Probe as a destination for Communication Manager Backups. These Backup files will be sent from the VSM Probe to the Virsae Cloud Computing Service. Access the Communication Manager System Management Interface as in **Section 5.1**. Navigate to **Data Backup/Restore → Schedule Backup** and configure the following.

- Select the radio button for **Specify Data Sets** and check all the boxes below
- Select the radio button for **Network Device**
- **Method:** Select **sftp** from the drop-down menu
- **User Name and Password:** Configure a username and password
- **Host Name:** IP Address of the VSM Probe
- **Directory:** Configure a directory path
- Schedule the **Day of Week** and **Start Time**

Retain default values for all other fields and click on the **Add New Schedule** button.

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

Help Log Off Administration This Server: devvmcm

Administration / Server (Maintenance)

ping
Traceroute
Netstat

Server
Status Summary
Process Status
Shutdown Server
Server Date/Time
Software Version

Server Configuration
Server Role
Network Configuration
Static Routes
Display Configuration
Time Zone Configuration
NTP Configuration

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

Add New Schedule

Data Sets

☒ Specify Data Sets

☒ Server and System Files

☒ Security File

☒ Avaya Call Processing (ACP) Translations

☐ Save ACP translations prior to backup

☒ Do NOT save ACP translations prior to backup

☐ Full Backup

Note: A CM "save trans" is not executed by the Full Backup procedure.

Backup Method

☒ Network Device

Method: **sftp**

User Name: **virsae**

Password: *********

Host Name: **10.10.98.157**

Directory: **/**

Encryption

☐ Encrypt backup using pass phrase

Day of Week

☒ Sunday

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

Start Time

01 10

Backups are scheduled once per week on each of the days selected. All backups begin at the same time.

Add New Schedule **Help**

5.5. Configure CDR Link

The following changes are required to define the VSM Probe as a CDR destination.

Use the **change ip-services** command to define the CDR link between Communication Manager and VSM Probe. To define a primary CDR link, provide the following information:

- **Service Type:** **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node:** **procr** [For the Communication Manager used during compliance testing, set the Local Node to the node name of the processor board.]
- **Local Port:** **0** [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node:** **virsaesnmp** [The Remote Node is set to the node name previously defined in **Section 5.2**.]
- **Remote Port:** **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in VSM Probe.]

change ip-services					Page	1 of	4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
CDR1	procr		0	virsaesnmp	9000		

On **Page 3** of the ip-services form, set 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		

Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track, and for the format of the CDR data. The example below shows the settings used during the compliance test. Configure the following information:

- **CDR Date Format:** **month/day**
- **Primary Output Format:** **unformatted**
- **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. Refer to the reference [2] in **Section 9** for additional details.

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

Node Number (Local PBX ID):                                     CDR Date Format: month/day
Primary Output Format: unformatted Primary Output Endpoint: CDR1
Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
Use ISDN Layouts? n                                           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? n
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? y Outg Attd Call Record? y
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
```

5.6. Configure RTCP Monitoring

To allow VSM to monitor the quality of H.323 IP calls, configure Communication Manager to send RTCP reporting to the IP address of the VSM probe. This is done through the SAT interface. For Avaya SIP endpoints, refer to the reference [9] in **Section 9**.

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

```
change system-parameters ip-options                                     Page 1 of 4
                               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: 10.10.98.157    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        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 the above 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
```

5.7. Configure Login for G450 Media Gateway

The VSM Probe requires access to the Media Gateways. This can be achieved by creating a new administrator on each Media Gateway or by providing the password for root access. To create a new username with admin access, login to G450 using root access and run the following command.

```
username [choose a username] password [choose a password]  
accesstype admin
```

The above command will create a username with access type as admin.

6. Configure Virsae Service Management

This section describes the configuration of VSM required to interoperate with Communication Manager. Configuration of VSM to interoperate with Session and System Manager can be referred from [9] in **Section 9** and will not be detailed here.

This section provides a “snapshot” of VSM configuration used during compliance testing. Virsae creates the Business partner portal in the cloud environment and is beyond the scope of these Application Notes. The screen shots and partial configuration shown below, supplied by Virsae, are provided only for reference. These represent only an example of the configuration GUI of VSM, available through the web Portal. Contact Virsae for details on how to configure VSM. The configuration operations described in this section can be summarized as follows:

- Login to the Web Portal
- Configuring Avaya Aura® Communication Manager
- Configure Dashboard

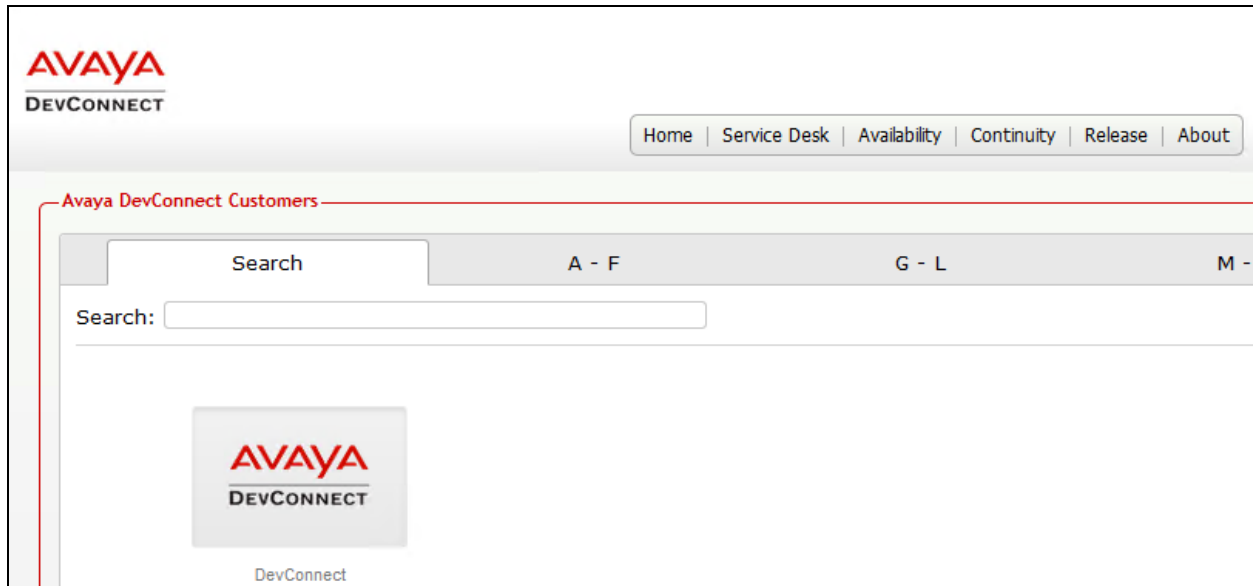
6.1. Login to the Web Portal

A portal for the business partner will be created by Virsae on the cloud and can be accessed by the business partner by typing the URL *<business partner name>.virsae.com* in a web browser. During compliance testing the URL used was *devconnect.virsae.com*. The Login screen is shown as below. Enter the **Email** and **Password** and click on the **Log In** button.

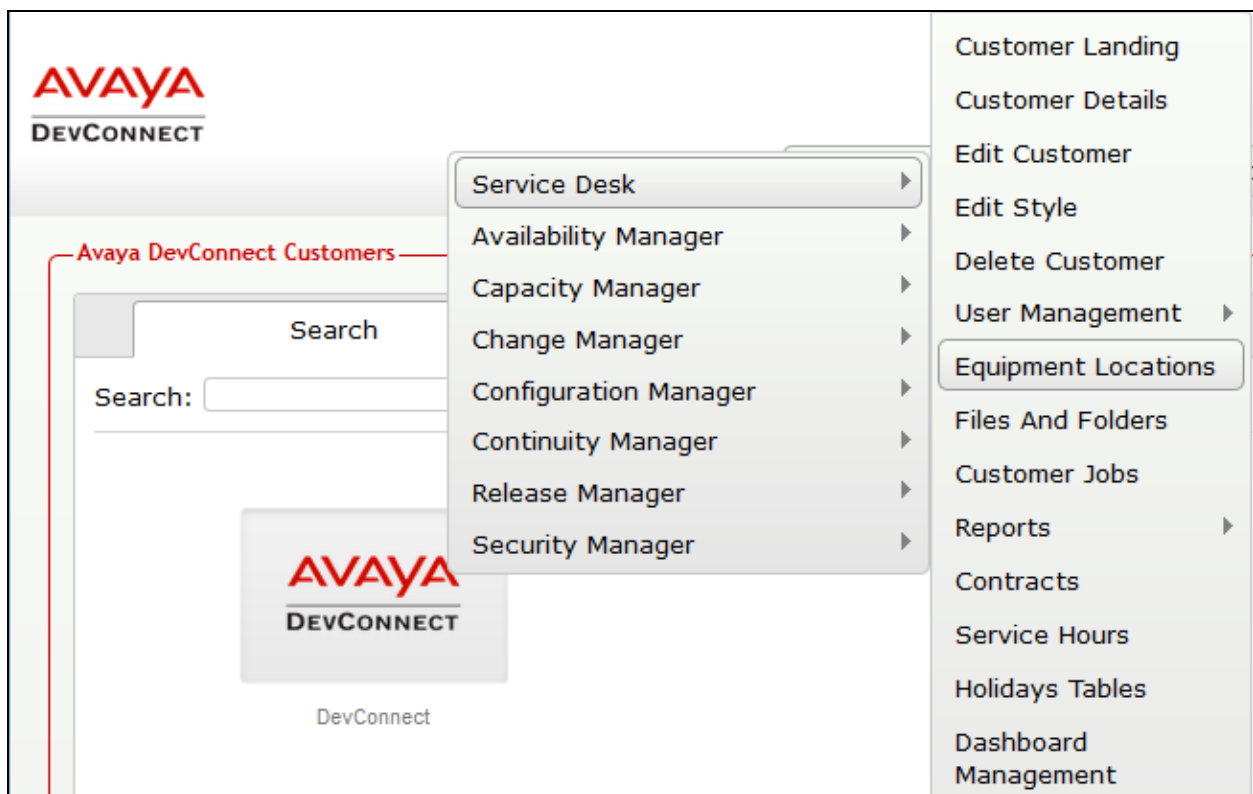


The screenshot shows a web login interface. At the top, the 'AVAYA' logo is displayed in red, with 'DEVCONNECT' in black text below it. Underneath the header, there are two text input fields: the first is labeled 'Email' and the second is labeled 'Password'. Below these fields is a grey 'Log In' button. At the bottom of the form, there is a blue hyperlink that reads 'Forgot your password?'.

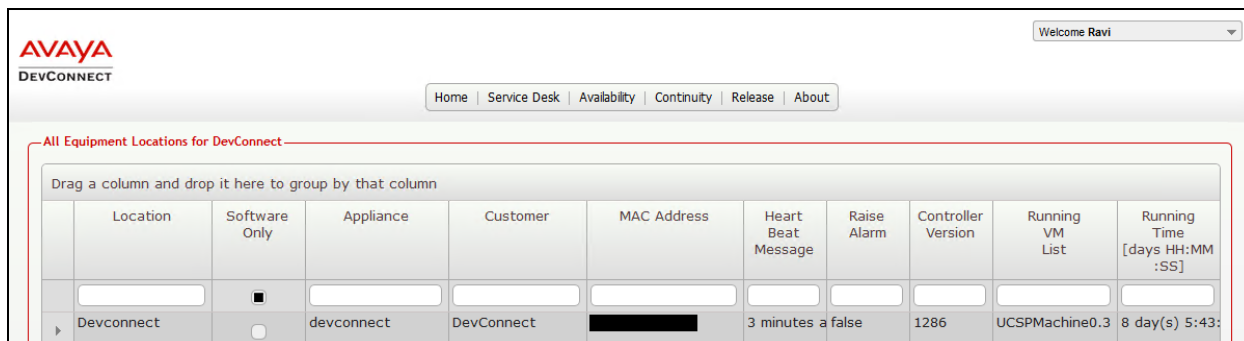
The customers belonging the business partner screen is shown. During compliance testing the customer created by Virsae is **Devconnect**.



Click on the customer icon and navigate to **Service Desk** → **Equipment Locations** as shown below.



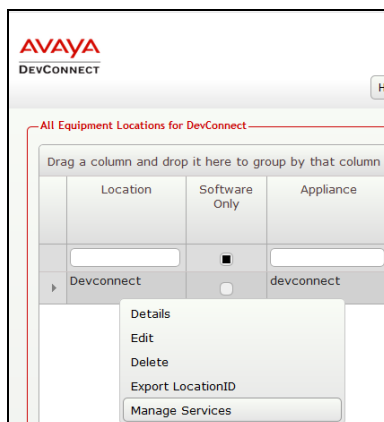
A **Location** called **Devconnect** is already configured as shown below.



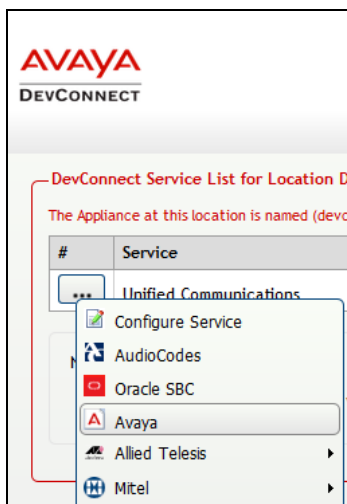
Location	Software Only	Appliance	Customer	MAC Address	Heart Beat Message	Raise Alarm	Controller Version	Running VM List	Running Time [days HH:MM:SS]
Devconnect	<input type="checkbox"/>	devconnect	DevConnect		3 minutes	false	1286	UCSPMachine0.3	8 day(s) 5:43:

6.2. Configuring Avaya Aura® Communication Manager

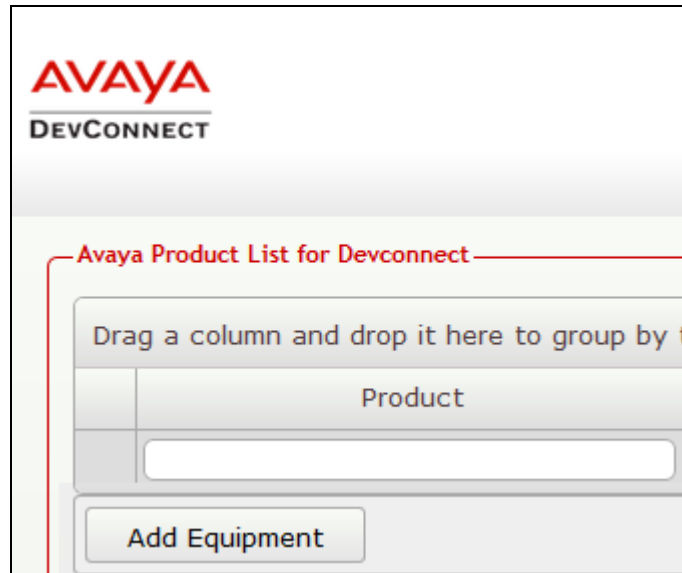
To add a Communication Manager to the Location created in **Section 6.1**, right click on the location **Devconnect** and select **Manage Services** as shown below.



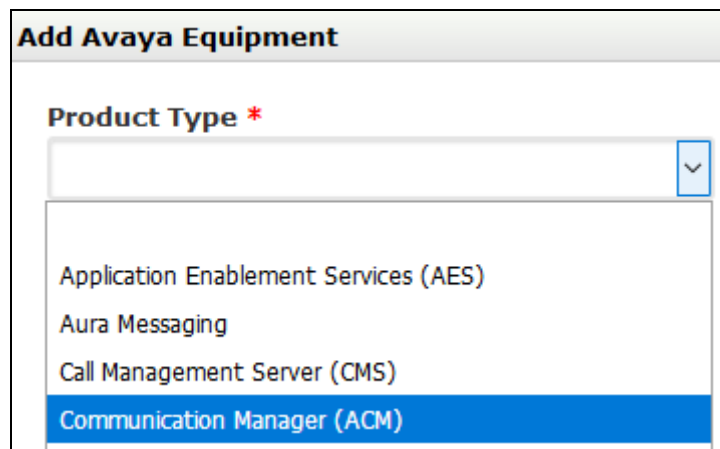
From the **Unified Communications Service**, select **Avaya**.



The product list for the configured location is shown as seen below. Click on the **Add Equipment** button.



From the **Add Avaya Equipment** window, select **Communication Manager (ACM)** from the **Product Type** drop-down menu.



In the **Configure Equipment** tab, configure the following values.

- **Equipment Name:** A descriptive name
- **Username:** The username configured in **Section 5.1**
- **Password:** The password configured in **Section 5.1**
- Check the **Use SSH** box
- **IP Address/Host Name:** IP address of Communication Manager
- **Default Site:** A descriptive site name
- **Command Set:** Select the version pertaining to the Communication Manager from the drop-down menu.
- **Default Username For Media Gateways:** As configured in **Section 5.7**
- **Default Password for Media Gateways:** As configured in **Section 5.7**
- **Monitored IP Network Regions:** During compliance testing region “1” was monitored
- Check the **Connect Directly To Media Gateways** box

Add Avaya Equipment

Product Type *
Communication Manager (ACM)

Configure Equipment | **Configure SNMP**

Equipment Name *
DevConnect ACM

Username *
Virsaer

Password *
••••••••

☒ **Use SSH**

Default Username For Media Gateways
virsaer

Default Password For Media Gateways
••••••••

IP Address/Host Name *
10.10.97.222

Default Site
Belleville

Command Set *
Version 7

Monitored IP Network Regions
1

☒ **Connect Directly To Media Gateways**

In the **Configure SNMP** tab, configure the following values.

- **SNMP Version:** Select **V2** from the drop-down menu
- **SNMP Community String:** Enter the value configured in **Section 5.2**

Click on the **Add** (not shown) button to complete the configuration.

Add Avaya Equipment

Product Type *
Communication Manager (ACM)

Configure Equipment | **Configure SNMP**

SNMP Version
V2

SNMP Community String *
public

The screen below shows the added Communication Manager equipment.

AVAYA
DEVCONNECT

Welcome

Home | Service Desk | Availability | Continuity | Release | About

Avaya Product List for Devconnect

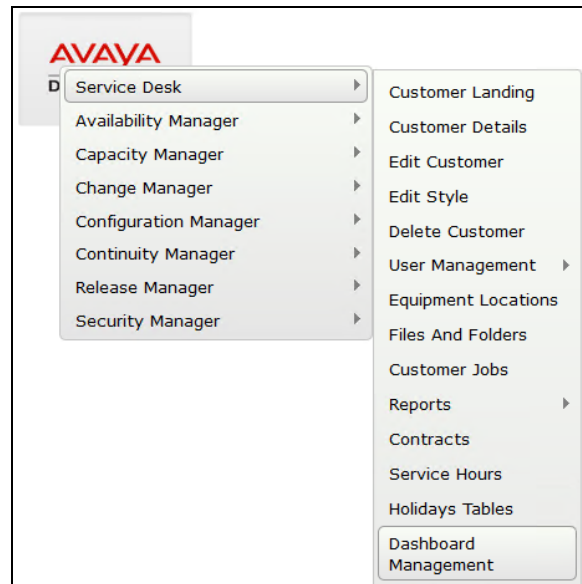
Drag a column and drop it here to group by that column

	Product	Name	IP Address/Host Name	User Name	Command Set
▶	Communication Manager (ACM)	Devconnect ACM	10.10.97.222	Virsae	Version 7

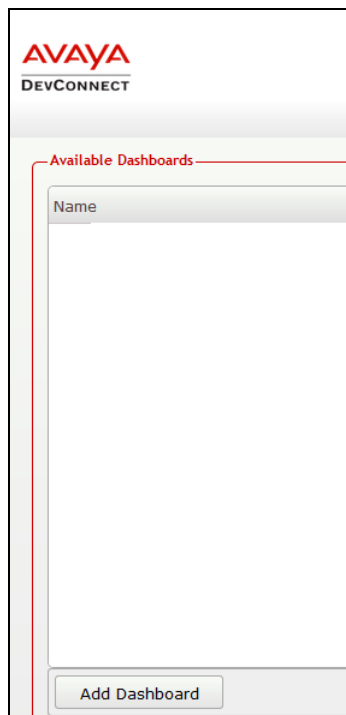
6.3. Configure Dashboard

This section shows the steps to configure Communication Manager on the dashboard.

From the customer icon, navigate to **Service Desk → Dashboard Management** as shown below.



From the **Available Dashboards** window, click on the **Add Dashboard** button.

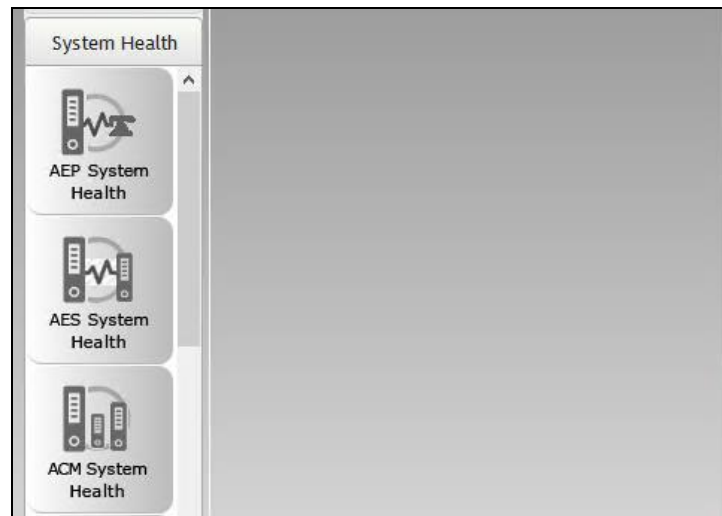


In the **Create Dashboard** window, type a descriptive name for **Name** and **Title** fields as shown below. Retain default values for all other fields. Click on **Layout** button and then click on **Submit** (not shown) button.

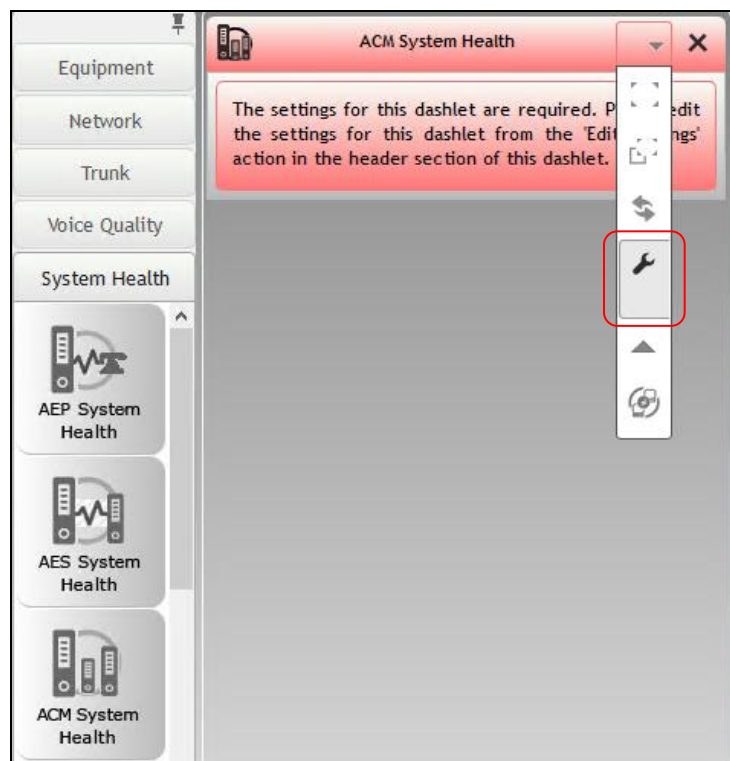
Screen below shows the above created Dashboard. Right click on it and select **Start**.

Name	Is Default	Active
DevConnect Dashboard	false	true

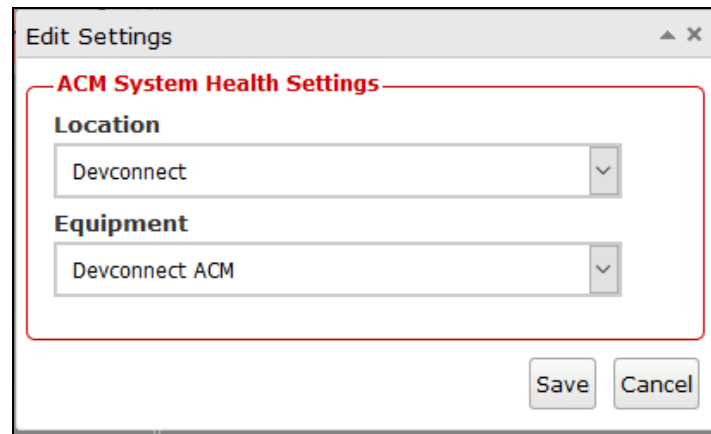
In the dashboard window shown below, click on **System Health** and drag the **ACM System Health** icon from the left to the right column.



From the drop-down menu for **ACM System Health** window, select the **Edit Settings** button as shown below.



In the **Edit Settings** window shown below, select the required **Location** and **Equipment** from the drop-down menu and click on the **Save** button.



Edit Settings

ACM System Health Settings

Location

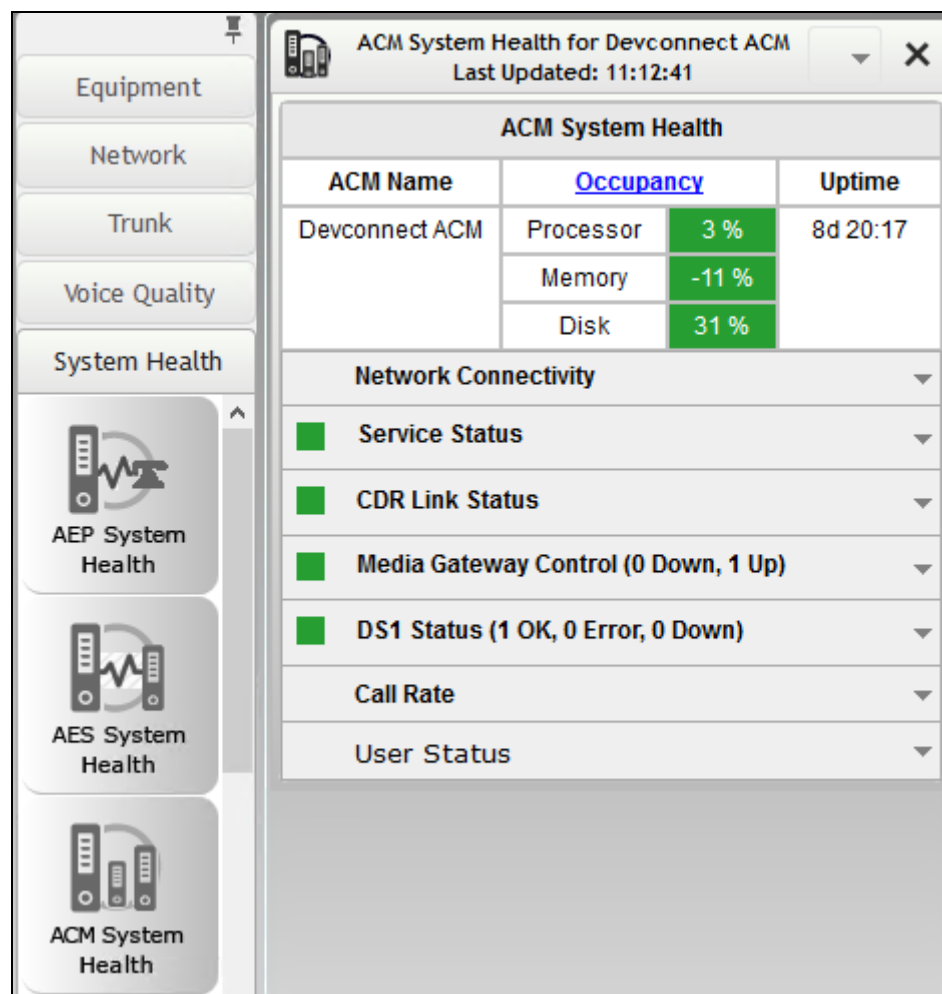
Devconnect

Equipment

Devconnect ACM

Save Cancel

The dashboard with the configured equipment is shown below. The above steps can be repeated to configure other equipment or/and dashboard parameters.



ACM System Health for Devconnect ACM
Last Updated: 11:12:41

ACM System Health			
ACM Name	Occupancy		Uptime
Devconnect ACM	Processor	3 %	8d 20:17
	Memory	-11 %	
	Disk	31 %	

Network Connectivity

- Service Status
- CDR Link Status
- Media Gateway Control (0 Down, 1 Up)
- DS1 Status (1 OK, 0 Error, 0 Down)
- Call Rate
- User Status

System Health

- AEP System Health
- AES System Health
- ACM System Health

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and VSM.

7.1. Verify Communication Manager

Verify that VSM has established concurrent connections to the Linux shell by using the **who -u** command.

```
admin@devvmcm> who -u
Virsaes pts/0      2018-10-03 10:09 .          15265 (10.10.98.157)
Virsaes pts/1      2018-10-03 10:54 .          28812 (10.10.98.157)
Virsaes pts/2      2018-10-03 10:54 .          28443 (10.10.98.157)
Virsaes pts/3      2018-10-04 08:34 .           2746 (10.10.98.157)
Virsaes pts/4      2018-10-03 10:55 .          28912 (10.10.98.157)
admin pts/5      2018-10-03 16:44 17:06     25594 (10.10.98.71)
admin pts/6      2018-10-04 10:06 .           9835 (10.10.228.209)
```

Verify that VSM has established concurrent connections to the SAT by using the **status logins** command.

```
status logins

COMMUNICATION MANAGER LOGIN INFORMATION

Login      Profile  User's Address      Active Command      Session
-----
Virsaes    18      10.10.98.157
*admin     18      10.10.98.71         stat logins         3
```

Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.5** shows **up**.

```
status cdr-link

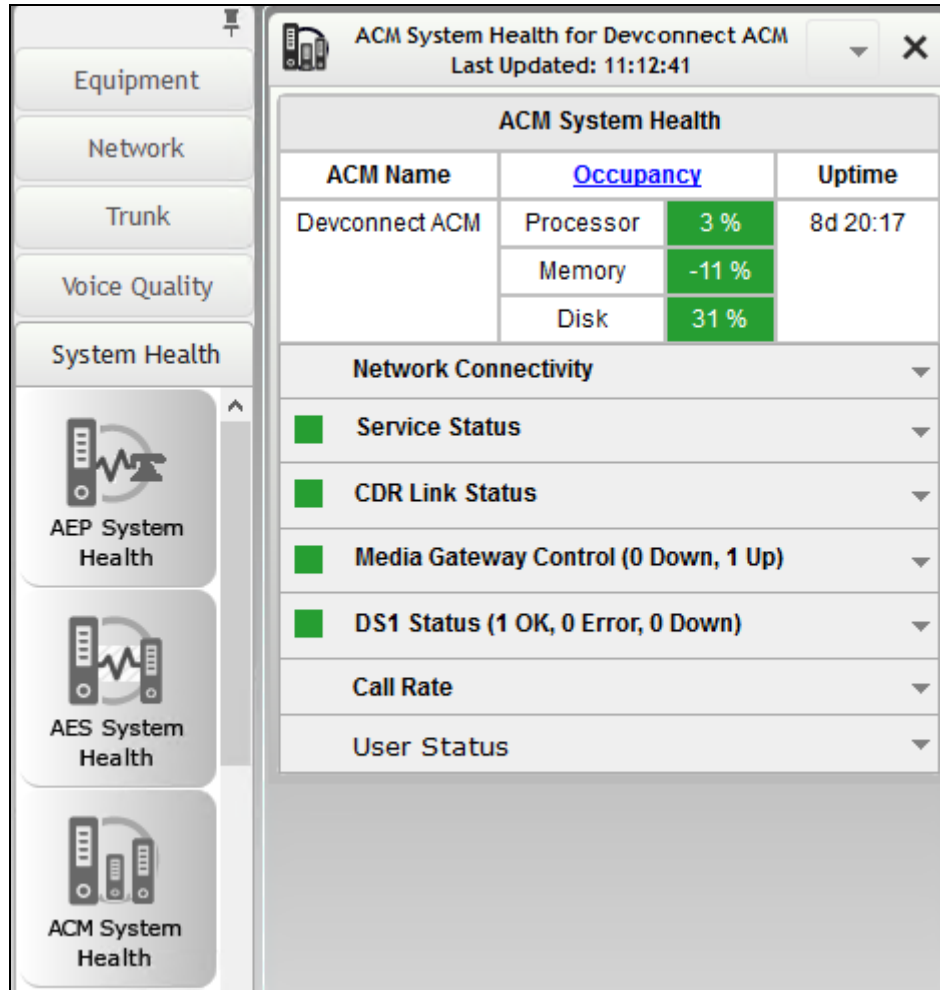
CDR LINK STATUS

Primary      Secondary
-----
Link State: up      down
Number of Retries:  999
Date & Time: 2018/10/03 16:43:12      0000/00/00 00:00:00
Forward Seq. No: 0      0
Backward Seq. No: 0      0
CDR Buffer % Full: 0.00      0.04
Reason Code: OK
```

7.2. Verify Virsae Service Management

This section provides the tests that can be performed to verify proper configuration of VSM. The following steps are done by accessing the VSM web portal for the Business partner.

After login to the web portal, navigate to **Service Desk → Dashboard Management** (not shown). Start the dashboard and the screen below shows the System Health of the already configured Communication Manager.



To view alarms using historical reporting, navigate to **Availability Manager → Manage Alarms** (not shown). A list of all unresolved alarms for all equipment is shown. Screen below shows the alarms by filtering for Communication Manager equipment.

AVAYA DEVCONNECT								
Home Service Desk Availability Continuity Release About								
Unresolved Alarms for DevConnect [Dates shown are 'Canada/Eastern' time zone]								
Alarm List Filter								
Drag a column and drop it here to group by that column								
Alarm	Description	Activate Date	Administered Id	Repeats	Equipment	Y	Vendor	Severity
					vconnect ACM			
LIC-ERR	The LIC-ERR MO works with the N...	2018-10-03 09:50:45	Unknown	2	Devconnect ...		Avaya	2
CDR Link Status Down	A call detail record link administere...	2018-10-01 07:02:25	Secondary	1043	Devconnect ...		Avaya	2
CUSTOMER ALARM TEST	Test alarm from customer equipme...	2018-09-28 15:42:20	devvmcm	0	Devconnect ...		Avaya	2
login	Login Authentication Failure trap h...	2018-09-28 11:35:40	devvmcm	1	Devconnect ...		Avaya	4
ISDN-SGR	ISDN-PR signalling group alarm An L...	2018-09-25 17:44:04	4	1	Devconnect ...		Avaya	2

To view voice quality using historical reporting, navigate to **Availability Manager → Voice Quality Management** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of voice quality for Communication Manager extensions. Real time voice quality can also be viewed in the dashboard.

AVAYA DEVCONNECT												
Home Service Desk Availability Continuity Release About												
Voice Calls for Customer DevConnect												
Voice Quality Management Filter												
Rule Sets: Voice Quality												
Expression (condition)												
<div> <div>ALL</div> <div> <div>Location equal Devconnect</div> <div>Date From greater than or equal 30 September 2018 12:00:00 AM</div> <div>Date To less than or equal 03 October 2018 05:00:00 PM</div> </div> </div>												
Go to page: 1 Show rows: 10 1-4 of 4												
Save Save All Apply												
Calls												
Name	Endpoint	IPNR	Mos Min	Mos M	Mos Avg	Stream Le...	IP Address	Port	DSCP	Call Time [Cana...	Source	
2 H323 56103	56103	1	4.4	4.4	4.4	0		2526	46	2018-10-03 16:4...	ext56103@...	:2...
0 OneOfFour	56104	1	4.4	4.4	4.4	4		6728	46	2018-10-03 16:4...	ext56104@...	:6...
2 H323 56103	56103	1	4.4	4.4	4.4	4		2526	46	2018-10-03 16:4...	ext56103@...	:2...
2 H323 56103	56103	1	4.4	4.4	4.4	3		2526	46	2018-10-03 16:4...	ext56103@...	:2...
2 H323 56103	56103	1	4.4	4.4	4.4	4		2526	46	2018-10-03 16:4...	ext56103@...	:2...
G450-for-VM (g450)	gwp	1	4.4	4.4	4.4	0			0	2018-10-03 16:4...	gwp@...	

To view CDR using historical reporting, navigate to **Service Desk** → **Call Details** (not shown). Create a rule set and apply the rule. Screen below shows a few examples of CDR for Communication Manager extensions.

AVAYA
DEVCONNECT

Home | Service Desk | Availability | Continuity | Release | About

Call Details for Customer DevConnect

Call Details Filter

Rule Sets: CDR

Expression (condition)

▼ ALL

Location equal Devconnect

Date From greater than or equal 30 September 2018 09:54:29 AM

Date To less than or equal 02 October 2018 05:00:00 PM

<< double-click to enter expression >>

Go to page: 1 Show rows: 10 1-5 of 5

Save Save All Apply

Call Details

Call Start Date-Time	Owner DN	Durati...	Dialed Number	Calling Number	Condition	A...	Ac...	A...	Auth...	I...	I...	C	Att	In...	No	Raw CDR Data
2018-10-02 16:22:12	56103	6	56103	4048511332	9					0	0...	0	#0	1	162000019	56103404851
2018-10-02 16:22:06	56104	12	56104	9078426003	9					0	0...	0	#0	1	162100029	56104907842
2018-10-02 11:44:41	56204	0	56204	9088426003	9					0	0...	0	#0	1	114300009	56204908842
2018-10-02 11:44:35	56204	6	56204	9078426003	9					0	0...	0	#0	1	114200019	56204907842
2018-10-02 11:38:11	56204	0	56204	4048511332	9					0	0...	0	#0	1	113600009	56204404851
2018-10-02 10:57:14	56103	6	56103	9078426003	9					0	0...	0	#0	1	105600019	56103907842

To view off-site backups, navigate to **Continuity Manager** → **Browse Backups** (not shown). Screen below shows a few examples of backups for Communication Manager.

AVAYA
DEVCONNECT

Home | Service Desk | Availability | Continuity | Release | About

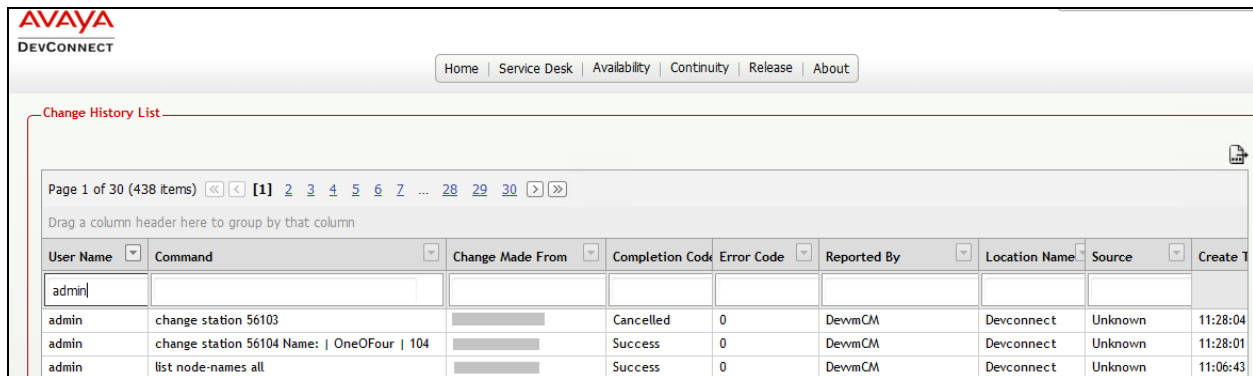
Files for Customer DevConnect

Page 1 of 32 (342 items) << < [1] 2 3 4 5 6 7 ... 30 31 32 > >>

Drag a column header here to group by that column

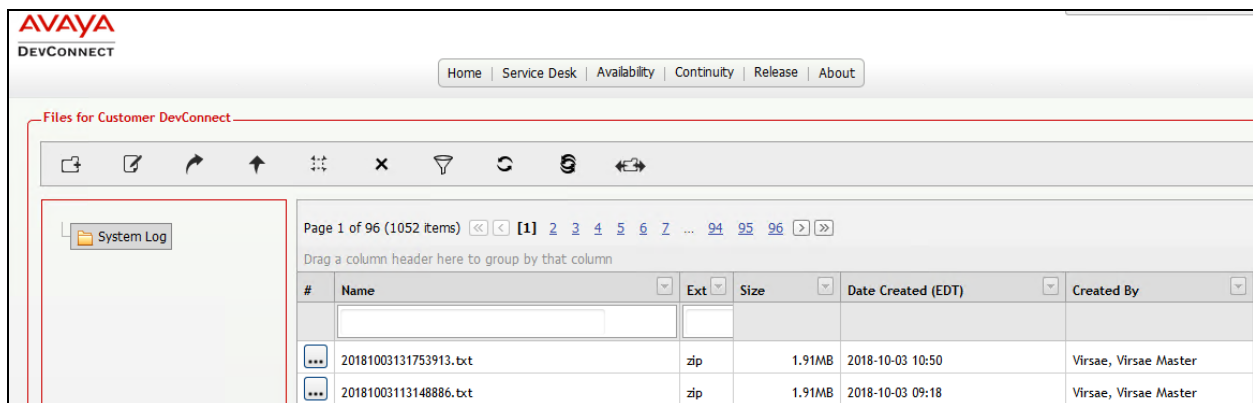
#	Name	Ext	Size	Date Created (EDT)	Created By
...	xln_devvmcm_121115_20181002.tar.gz	zip	717.08KB	2018-10-02 12:12	Virsae, Virsae Master
...	os_devvmcm_121001_20181002.tar.gz	zip	14.01KB	2018-10-02 12:11	Virsae, Virsae Master
...	security_devvmcm_121021_20181002.tar.gz	zip	1.35MB	2018-10-02 12:11	Virsae, Virsae Master

To view change history of Communication Manager, navigate to **Change Manager → View Change Logs** (not shown). Screen below shows a few examples of changes made by applying a filter on **User Name**.



User Name	Command	Change Made From	Completion Code	Error Code	Reported By	Location Name	Source	Create Time
admin	change station 56103		Cancelled	0	DevwmCM	Devconnect	Unknown	11:28:04
admin	change station 56104 Name: OneOfFour 104		Success	0	DevwmCM	Devconnect	Unknown	11:28:01
admin	list node-names all		Success	0	DevwmCM	Devconnect	Unknown	11:06:43

To view Syslog files, navigate to **Availability Manager → SysLog → Browse Syslog Files** (not shown). Screen below shows a few examples of Syslogs for Communication Manager.



#	Name	Ext	Size	Date Created (EDT)	Created By
...	20181003131753913.txt	zip	1.91MB	2018-10-03 10:50	Virsaee, Virsaee Master
...	20181003113148886.txt	zip	1.91MB	2018-10-03 09:18	Virsaee, Virsaee Master

8. Conclusion

These Application Notes describe the procedures for configuring the Virsaee Service Management to interoperate with Avaya Aura® Communication Manager. During compliance testing, all test cases were completed successfully with observations noted in **Section 2.2**.

9. Additional References

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

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Deploying Avaya Aura® Communication Manager in Virtual Appliance*, Release 8.0, Issue 3 September 2018.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0, Issue 1 July 2018.
3. *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1 July 2018.
4. *Avaya Aura® Communication Manager Screen Reference*, Release 8.0, Issue 2 August 2018.
5. *Deploying Avaya Aura® Session Manager in Virtual Appliance*, Release 8.0, Issue 2 September 2018.
6. *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2 August 2018.
7. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.0, Issue 2 September 2018.
8. *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0, Issue 4 September 2018.
9. *Application Notes for Virsae Service Management for Unified communications with Avaya Aura® Session Manager*, October 2018

Product documentation for Virsae products can be obtained directly from Virsae.

1. *Virsae Service Management - Implementation Guide*
2. *Virsae Service Management – Technical Requirements*

©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.