Avaya Solution & Interoperability Test Lab

Application Notes for Nectar Foundation with Avaya Aura® System Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Nectar Foundation with Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar Foundation is a proactive health and performance monitor that provides enterprise customers and service providers with a comprehensive view of unified communications environments for monitoring, allowing service interruptions to be diagnosed and solved quicker. Nectar Foundation automatically captures Avaya Aura® System Manager and Avaya Aura® Session Manager inventory and provides resource utilization information using Avaya Aura® Routing Web Service, Avaya Aura® Session Manager Element Manager Web Service, and SNMP Polling.

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

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

1. Introduction

These Application Notes describe the configuration steps required to integrate Nectar Foundation with Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar Foundation is a proactive health and performance monitor that provides enterprise customers and service providers with a comprehensive view of unified communications environments for monitoring, allowing service interruptions to be diagnosed and solved quicker. Nectar Foundation automatically captures Avaya Aura® System Manager and Avaya Aura® Session Manager inventory and provides resource utilization information using Avaya Aura® Routing Web Service, Avaya Aura® Session Manager Element Manager Web Service, and SNMP Polling.

The Routing Web Service and Element Manager Web Service are RESTful Web Services that are part of the Avaya Aura® System Manager Web Services. The Routing Web Service provides programmatic access to Routing administration data available from the **System Manager → Routing** GUI. Nectar Foundation collected the following Routing data from System Manager:

- Locations
- SIP Entities
- Entity Links

The Session Manager Element Manager Web Service provides programmatic access to Session Manager Dashboard and User Registration status data. Nectar Foundation collected the following data from Session Manager:

- Session Manager Status
- Session Manager Instances
- User Registrations

Nectar Foundation captured the following resource utilization data from System Manager and Session Manager using SNMPv3 polls.

- CPU Utilization
- Linux Physical Memory Utilization

The frequency of data polling is configurable via Nectar Foundation or may be performed on demand.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on the ability of Nectar Foundation to capture System Manager and Session Manager inventory data from the Routing Web Service and the Element Manager Web Service. In addition, SNMPv3 polling was used to capture the resource utilization data. The data was displayed on the Nectar Remote Intelligence Gateway (RIG) client.

The serviceability testing focused on verifying that the Nectar Foundation came back into service after re-connecting the Ethernet cable (i.e., restoring network connectivity) and rebooting the Foundation server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following Foundation features and functionality. Alarms/alerts, system inventory, resource utilization and status, and call quality metrics were displayed on the RIG client.

- Collecting System Manager Inventory (e.g., Locations, SIP Entities, and Entity Links) using the Routing Web Service and displaying the inventory on the RIG client.
- Collecting Session Manager Inventory (e.g., Session Manager Status, Session Manager Instances, and User Registrations) using the Element Manager Web Service and displaying the inventory on the RIG client.
- Verifying configuration changes made to the relevant data via the System Manager Web interface were updated on RIG client.
- Verifying status changes made to Session Manager and SIP users were updated on RIG client.
- Verifying resource utilization (e.g., CPU Utilization and Linux Physical Memory Utilization) captured from System Manager and Session Manager via SNMPv3 polling.
- Tracking the registration status of existing and new Avaya SIP Deskphones.
- Verifying proper system recovery after a restart of the Foundation server and loss of IP network connectivity.

2.2. Test Results

The compliance test passed with the following observations:

- Initially, the Session Manager Inventory data displays zeros in the RIG client when it is first started, click or select the inventory item again to display the actual data.

- The Session Manager Element Manager Web Service API returns incorrect field values for SIP Monitoring and CDR in the Session Manager administration. These field values are returned as *false* even when they are enabled.

- Currently, Nectar Foundation doesn't support receiving SNMP traps from System Manager or Session Manager.

2.3. Support

For technical support and information on Nectar Foundation, contact Nectar Support at:

Phone:	1-888-811-8647
Website:	http://nectarcorp.com/support
Email:	support@nectarcorp.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Nectar Foundation with an Avaya SIP-based network, including Avaya Aura® System Manager and Avaya Aura® Session Manager. Nectar Foundation captured data from System Manager and Session Manager using System Manager Web Services and SNMP Polling. The Nectar RIG client was used to display system inventory and resource utilization data.

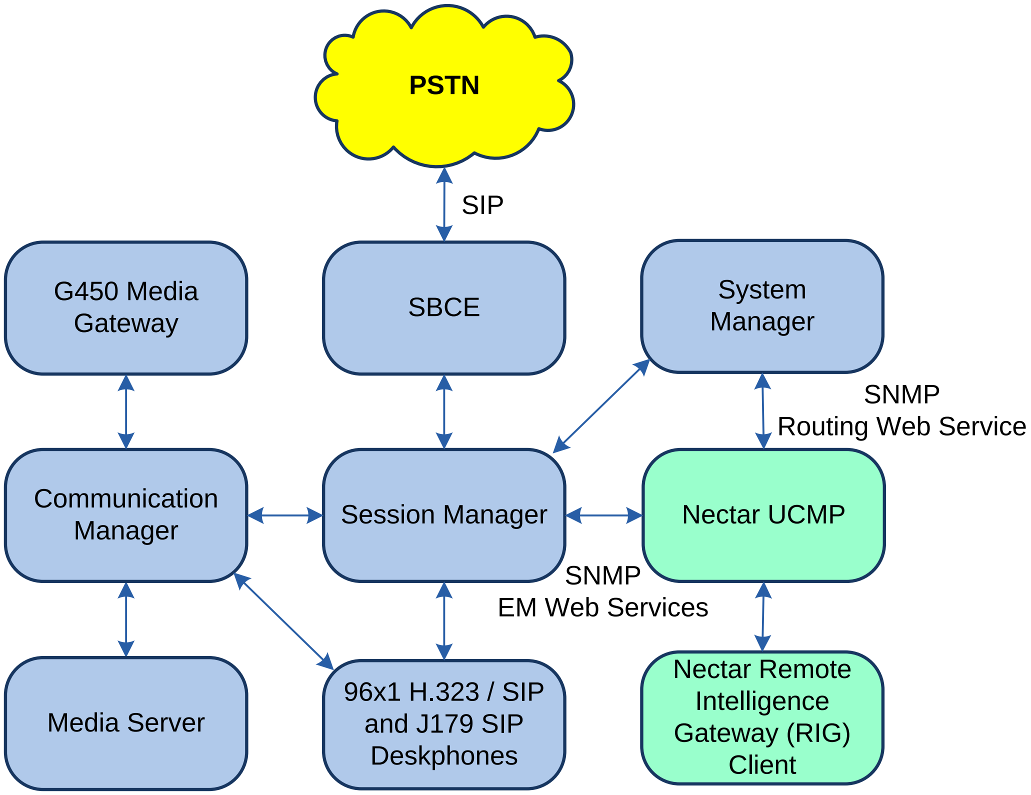


Figure 1: Nectar Foundation with Avaya SIP-based Network

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.2.0.0-FP2
Avaya G450 Media Gateway	FW 41.24.0
Avaya Aura® Media Server	v.8.0.2.93
Avaya Aura® System Manager	8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.2.0.0611167 Feature Pack 2
Avaya Aura® Session Manager	8.1.2.0.812039
Avaya Session Border Controller for Enterprise	8.1.0.0-14-18490
Avaya 96x1 Series IP Deskphones	6.8304 (H.323) 7.1.9.0.8 (SIP)
Avaya J179 SIP Deskphone	4.0.5.0.10
Nectar Foundation	8.3.0.2-09317
Nectar Remote Intelligence Gateway (RIG) Client	8.3.0.2-09317

5. Configure Avaya Aura® System Manager and Avaya Aura® Session Manager

This section provides the procedure for providing access to System Manager Web Services and enabling SNMP polling on System Manager and Session Manager. The procedures include the following areas:

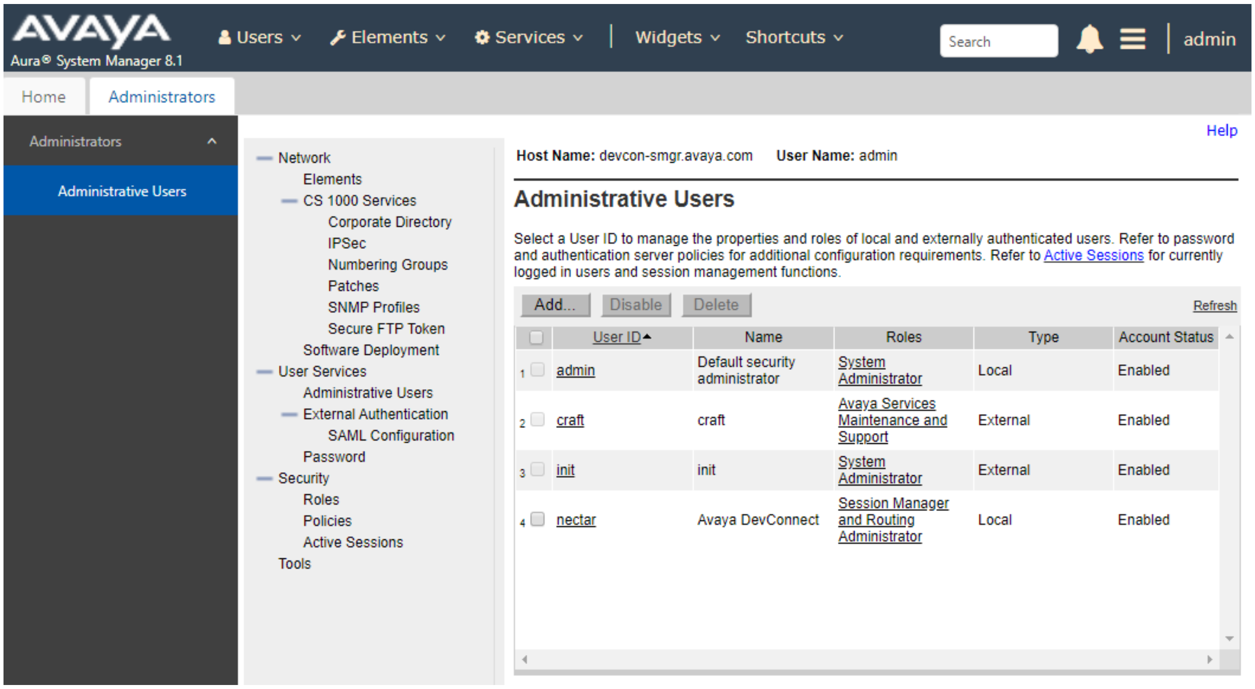
- Add New Administrator for Nectar Foundation Access
- Verify System Manager Web Services
- Enable SNMP Polling

Configuration was performed by accessing the browser-based GUI of System Manager using the URL https://<*ip-address*>, where <*ip-address*> is the System Manager IP address, and logging in using the appropriate credentials.

5.1. Add New Administrator for Nectar Foundation Access

A user account is required by Foundation to retrieve SIP trunk and user registration information using System Manager Web Services.

From the main webpage, navigate to **Users → Administrators**. In the **Administrative Users** web page shown below, click **Add**.



Host Name: devcon-smgr.avaya.com **User Name:** admin

Administrative Users

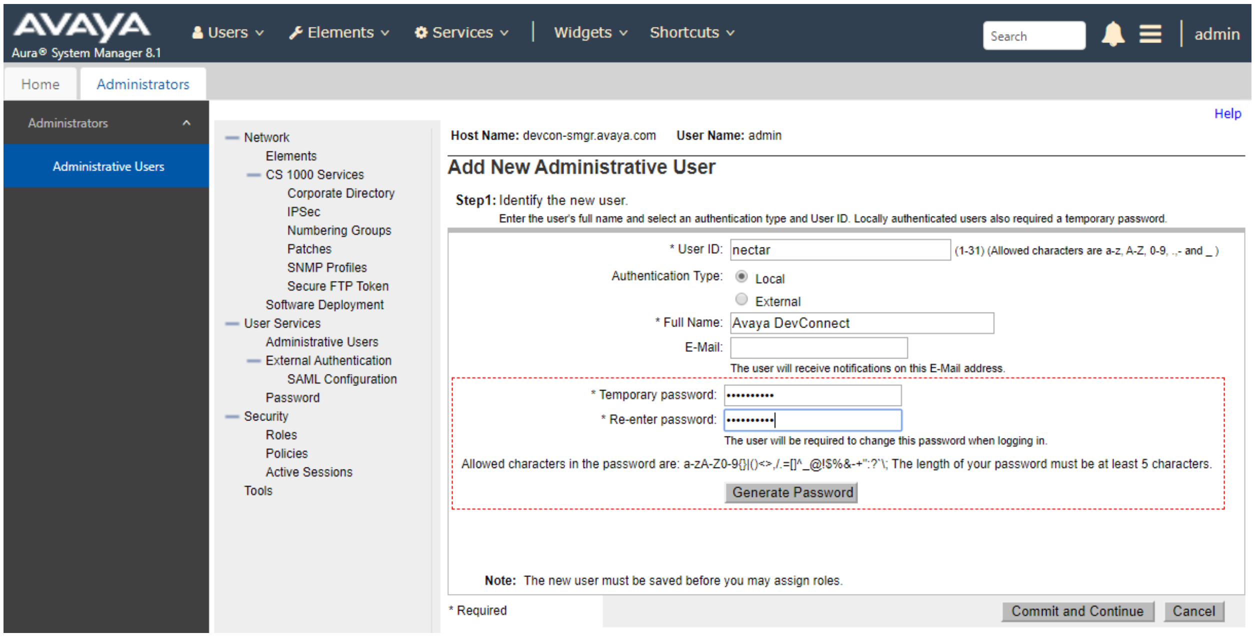
Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to Active Sessions for currently logged in users and session management functions.

	□	User ID▲	Name	Roles	Type	Account Status
1	□	admin	Default security administrator	System Administrator	Local	Enabled
2	□	craft	craft	Avaya Services Maintenance and Support	External	Enabled
3	□	init	init	System Administrator	External	Enabled
4	□	nectar	Avaya DevConnect	Session Manager and Routing Administrator	Local	Enabled

In the **Add New Administrative User** web page, configure the following parameters:

- **User:** Provide a descriptive name (e.g., *nectar*).
- **Authentication Type:** Select **Local** radio button.
- **Full Name:** Provide full name (e.g., *Avaya DevConnect*).
- **Temporary Password:** Provide account password.
- **Re-enter Password:** Re-enter the password.

After completing the form, click **Commit and Continue**.



Host Name: devcon-smgr.avaya.com **User Name:** admin

Add New Administrative User

Step1: Identify the new user.

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

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

Authentication Type: ● Local ○ External

* Full Name: Avaya DevConnect

E-Mail:

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

* Temporary password: ••••••••••

* Re-enter password: ••••••••••

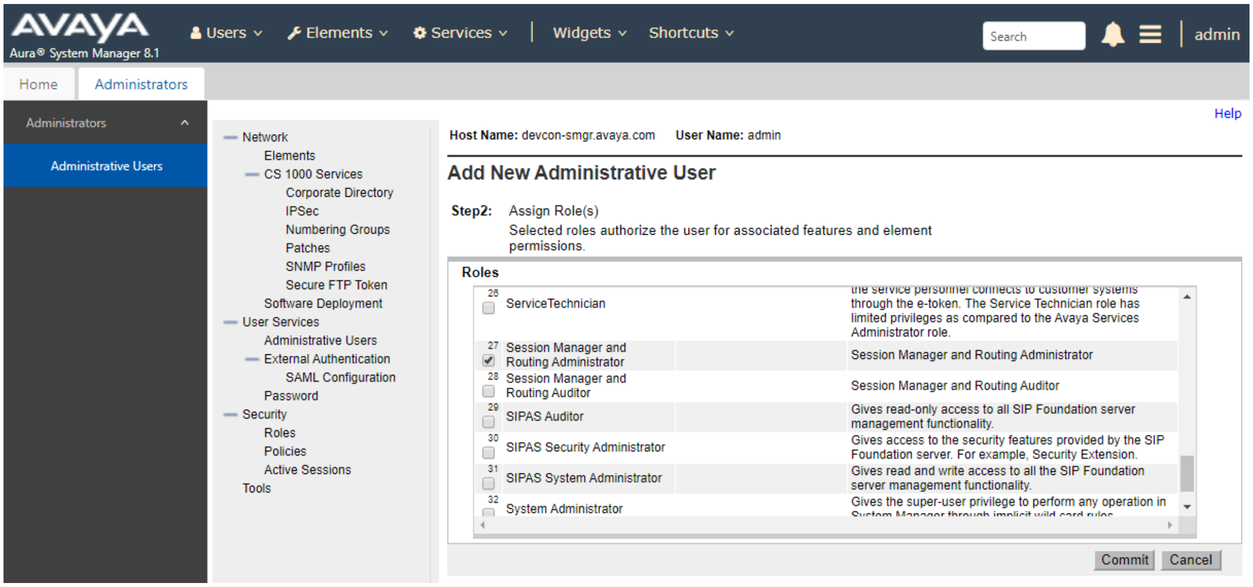
The user will be required to change this password when logging in.

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

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

* Required

On the next web page, assign the role to the administrative user. Scroll down and select **Session Manager and Routing Administrator**. Click **Commit**.



Host Name: devcon-smgr.avaya.com **User Name:** admin

Add New Administrative User

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

Roles

26	□ ServiceTechnician	the service personnel connects to customer systems through the e-token. The Service Technician role has limited privileges as compared to the Avaya Services Administrator role.
27	☑ Session Manager and Routing Administrator	Session Manager and Routing Administrator
28	□ Session Manager and Routing Auditor	Session Manager and Routing Auditor
29	□ SIPAS Auditor	Gives read-only access to all SIP Foundation server management functionality.
30	□ SIPAS Security Administrator	Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.
31	□ SIPAS System Administrator	Gives read and write access to all the SIP Foundation server management functionality.
32	□ System Administrator	Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Commit Cancel

Log out of the System Manager web interface. Log back into the System Manager web interface using the administrative user created above. During the first login attempt, the user must change the password using the **Change Password** link under the login prompt (not shown).

5.2. Verify System Manager Web Services

No additional configuration is required to enable the Routing Web Service or Element Manager Web Service. However, the steps in the following sections can be performed to verify that System Manager Web Services are running and that data can be retrieved using the Routing Web Service and Element Manager Web Service.

5.2.1. Verify System Manager Web Services is Running

To verify System Manager Web Services is running, perform the following steps:

- Log into System Manager using SSH.
- At the Linux prompt, enter the following command: `wget --no-check-certificate https://SMGR-IP/ws/grservice/getgrstate/test`, where `SMGR-IP` is the System Manager IP address.
- A similar output to the one below should be displayed indicating that the HTTP request was successful.

```
--2020-05-04 11:31:35--  https://10.64.102.120/ws/grservice/getgrstate/test
Connecting to 10.64.102.120:443... connected.
WARNING: cannot verify 10.64.102.120's certificate, issued by ‘/CN=System Manager
CA/OU=MGMT/O=AVAYA’:
  Self-signed certificate encountered.
    WARNING: certificate common name ‘devcon-smgr.avaya.com’ doesn't match requested
host name ‘10.64.102.120’.
HTTP request sent, awaiting response... 200 OK
Length: 698 [application/octet-stream]
Saving to: ‘test.4’

100%[============================================>] 698         --.-K/s   in 0s

2020-05-04 11:31:35 (72.3 MB/s) - ‘test.4’ saved [698/698]
```

5.2.2. Test Routing Web Service

Verify that data can be accessed from the System Manager Routing Web Service by requesting for SIP entity data using a web browser. Enter the following URL in the web browser: https://SMGR-IP/NRP/admin/sipentities, where SMGR-IP is the System Manager IP address. Enter the appropriate login credentials, from **Section 5.1**, when prompted. System Manager should respond with a list of SIP entities in the web browser.

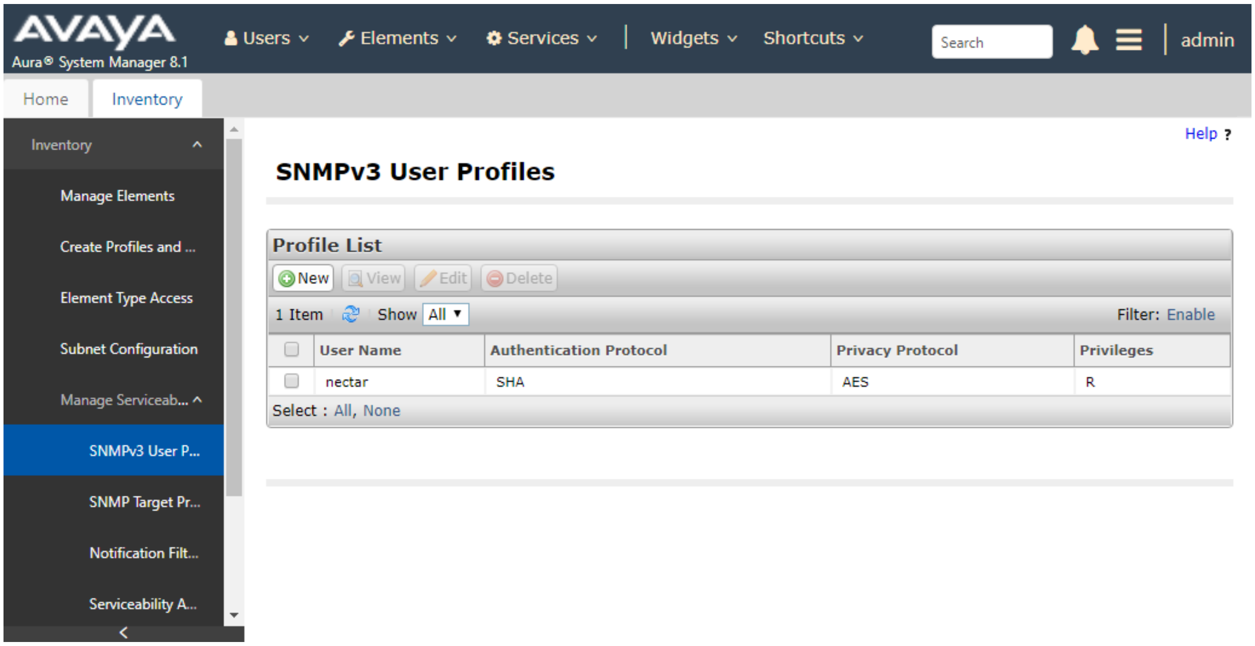
5.2.3. Test Element Manager Web Service

Verify that data can be accessed from the Session Manager Element Manager Web Service by requesting for Session Manager status using a web browser. Enter the following URL in the web browser: https://SMGR-IP/ASM/ws/asmstatuses, where SMGR-IP is the System Manager IP address. Enter the appropriate login credentials, from **Section 5.1**, when prompted. System Manager should respond with the Session Manager status in the web browser.

5.3. Configure SNMP

This section provides the procedure for enabling SNMP polls on System Manager and Session Manager. Configuration was performed by accessing the browser-based GUI of System Manager using the URL https://<*ip-address*>, where <*ip-address*> is the System Manager IP address. Log in using the appropriate credentials.

From the main webpage above, navigate to **Services** → **Inventory**. In the subsequent webpage, select **SNMPv3 User Profiles** under **Manage Serviceability Agents** in the left pane to display the webpage below. Click **New**.

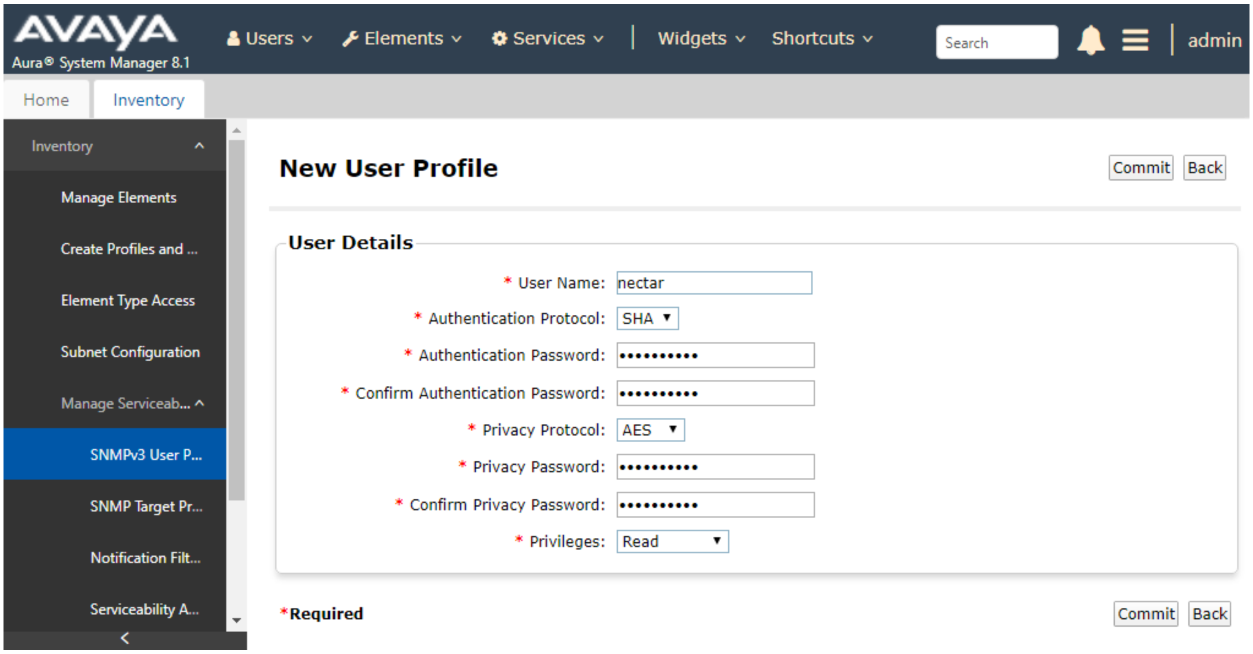


SNMPv3 User Profiles

Profile List

	User Name	Authentication Protocol	Privacy Protocol	Privileges
□	nectar	SHA	AES	R

Configure the **User Details** for SNMPv3 polls to be used for System Manager and Session Manager. Nectar Foundation requires that the SNMPv3 credentials match for System Manager and Session Manager. The following user profile will be used by System Manager and Session Manager.



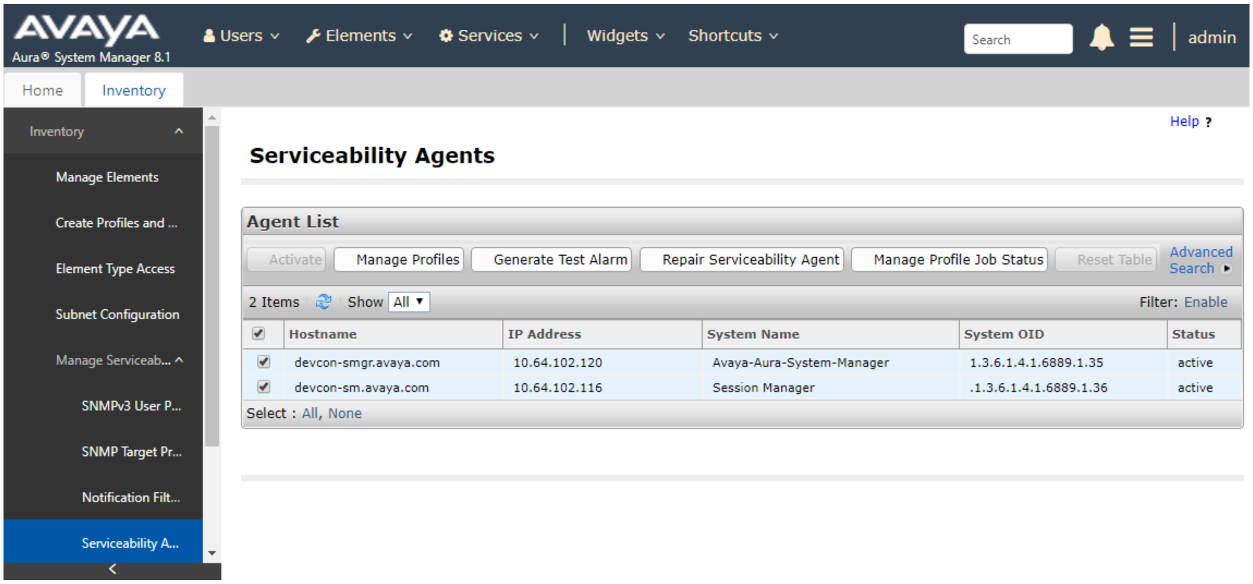
New User Profile

User Details

* User Name:	nectar
* Authentication Protocol:	SHA
* Authentication Password:	••••••••••
* Confirm Authentication Password:	••••••••••
* Privacy Protocol:	AES
* Privacy Password:	••••••••••
* Confirm Privacy Password:	••••••••••
* Privileges:	Read

*Required

Finally, under **Manage Serviceability Agents** in the left pane, select **Serviceability Agents**. Select the serviceability agents, which should include System Manager and Session Manager, by selecting both checkboxes as shown below. This step selects the serviceability agents to which the SNMP user profile configured above will be attached. Click on **Manage Profiles**.



Serviceability Agents

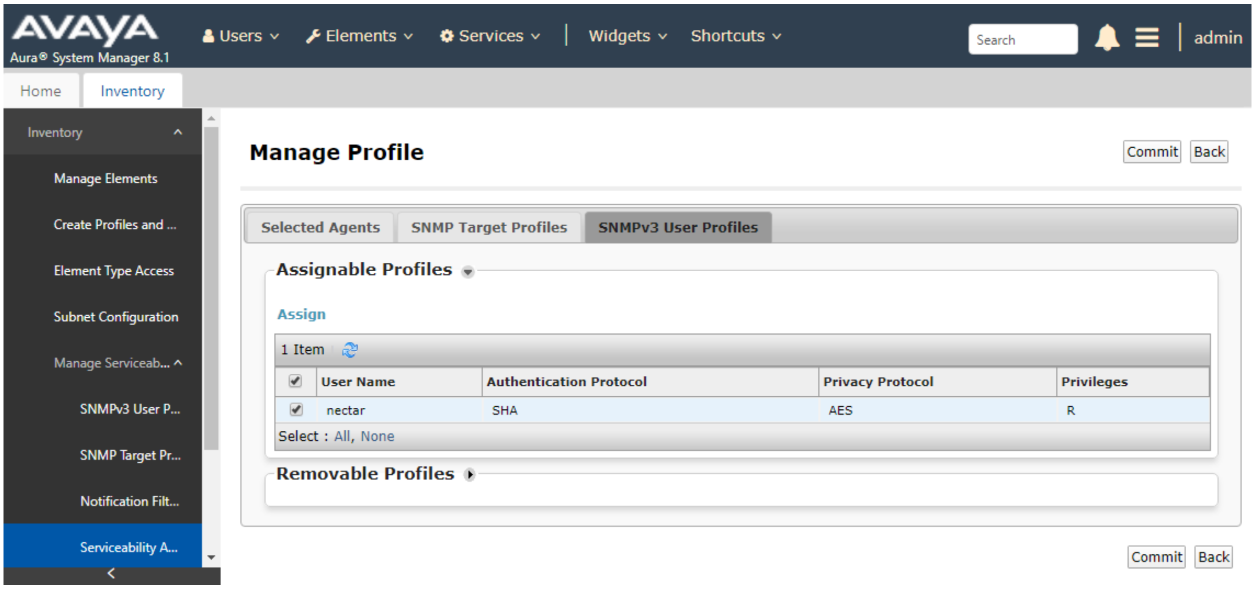
Agent List

2 Items Show All

☑	Hostname	IP Address	System Name	System OID	Status
☑	devcon-smgr.avaya.com	10.64.102.120	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active
☑	devcon-sm.avaya.com	10.64.102.116	Session Manager	.1.3.6.1.4.1.6889.1.36	active

Select : All, None

In the **SNMPv3 User Profiles** tab, select the entry in the **Assignable Profiles** section and click **Assign** to push the SNMP details to System Manager and Session Manager. Click **Commit** to submit the changes.



Manage Profile

Assignable Profiles

☑	User Name	Authentication Protocol	Privacy Protocol	Privileges
☑	nectar	SHA	AES	R

Select : All, None

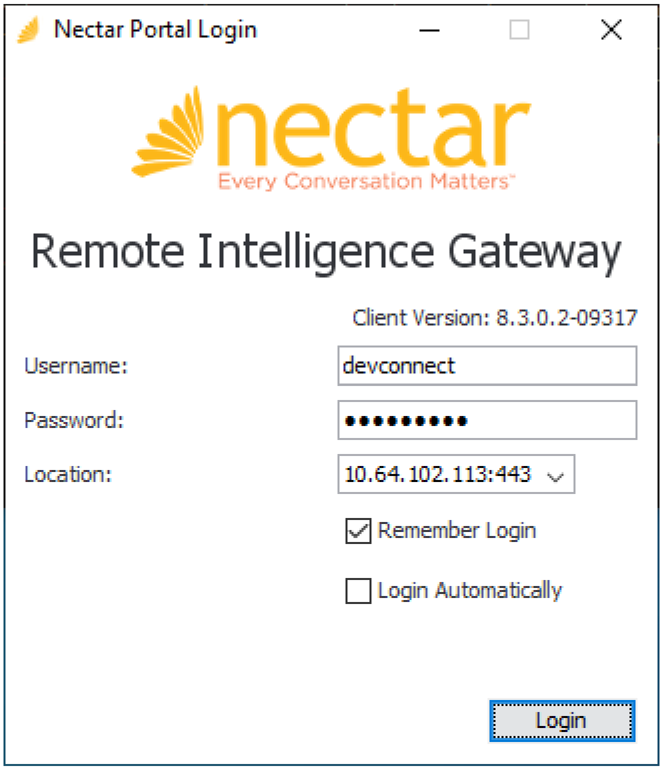
6. Configure Nectar Foundation

This section covers the Foundation configuration to collect Session Manager Inventory and resource utilization data from System Manager and Session Manager using SNMPv3 polling. The configuration was performed via the **RIG client**. The procedure covers the following areas:

- Launch the RIG Client
- Configure System Manager Web Services and SNMP Polling Access

6.1. Launch the RIG Client

In an Internet browser, enter the Foundation IP address in the URL field. The RIG client software is downloaded. Install and run the RIG client. In the **Nectar Portal Login** screen, enter the user credentials and click **Login**.



Client Version: 8.3.0.2-09317

Username: devconnect

Password: ●●●●●●●●●●

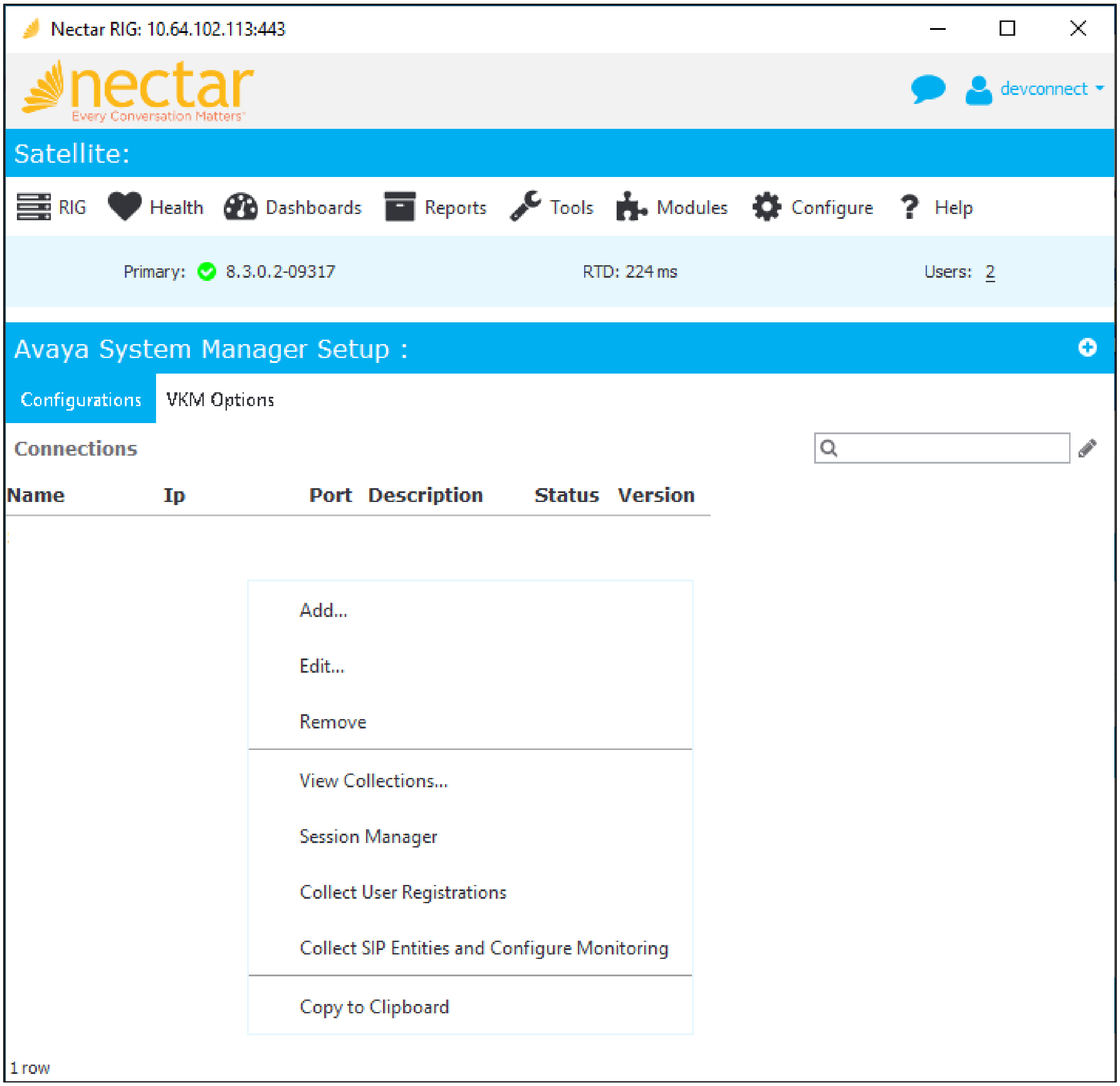
Location: 10.64.102.113:443

☑ Remember Login

□ Login Automatically

6.2. Configure System Manager Web Services and SNMP Polling Access

Navigate to **Modules → Avaya → System Manager** and right-mouse click on the screen and select **Add** from the pop-up menu shown below to add a System Manager and Session Manager connection.

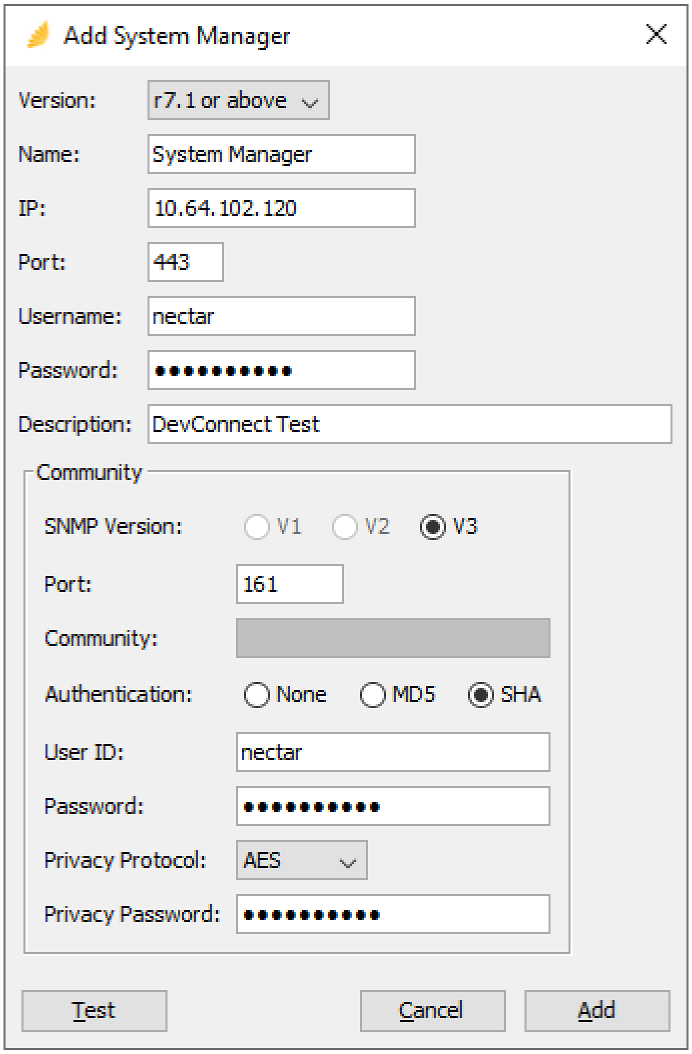


The **Add System Manager** dialog box is displayed as shown below. This configuration allows the System Manager Web Services access credentials and the SNMPv3 polling credentials for both System Manager and Session Manager to be specified.

Configure the following fields:

- **Version:** Select *r7.1 or above*.
- **Name:** Provide a descriptive name (e.g., *System Manager*).
- **Port:** Specify HTTPS port 443.
- **Username:** Specify the user name configured in **Section 5.1**.
- **Password:** Specify the password configured in **Section 5.1**.
- **Description:** Provide an optional description (e.g., *DevConnect Test*).

In the **Community** section, specify the SNMPv3 polling credentials from **Section 5.3**. Click **Test** to test the connection. Click **Add** to submit the form.



Version:	r7.1 or above
Name:	System Manager
IP:	10.64.102.120
Port:	443
Username:	nectar
Password:	●●●●●●●●●●●
Description:	DevConnect Test

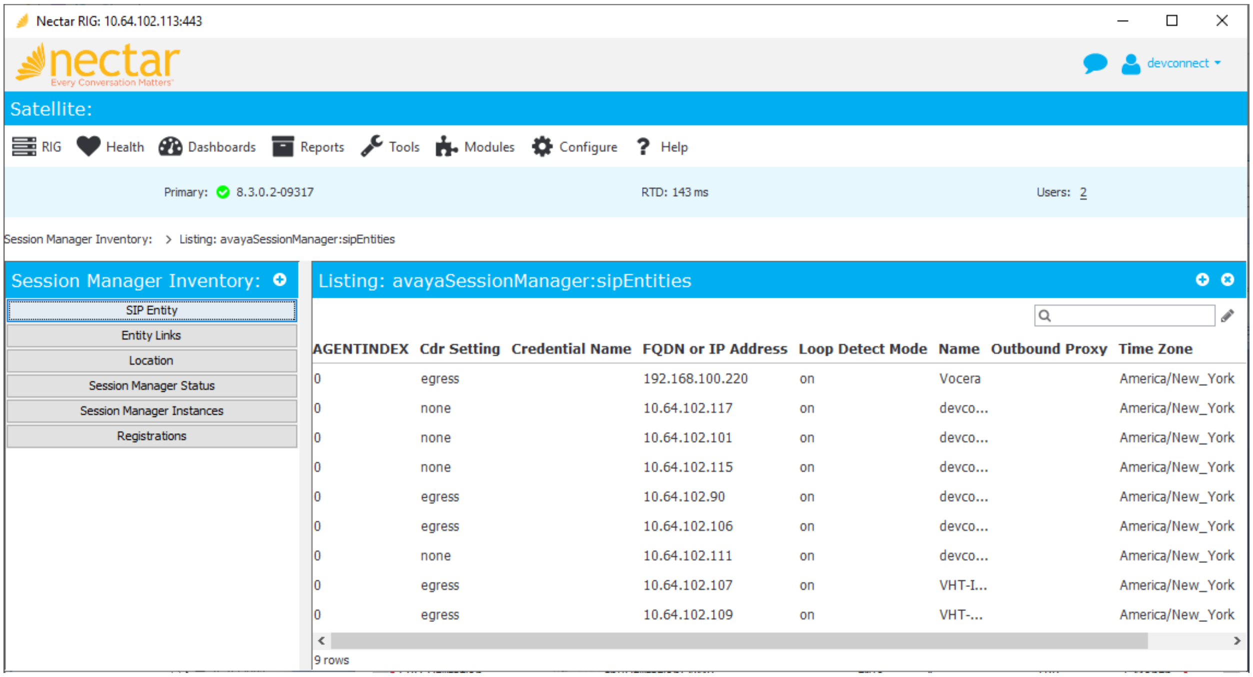
Community

SNMP Version:	○ V1 ○ V2 ● V3
Port:	161
Community:	
Authentication:	○ None ○ MD5 ● SHA
User ID:	nectar
Password:	●●●●●●●●●●●
Privacy Protocol:	AES
Privacy Password:	●●●●●●●●●●●

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Foundation with System Manager and Session Manager.

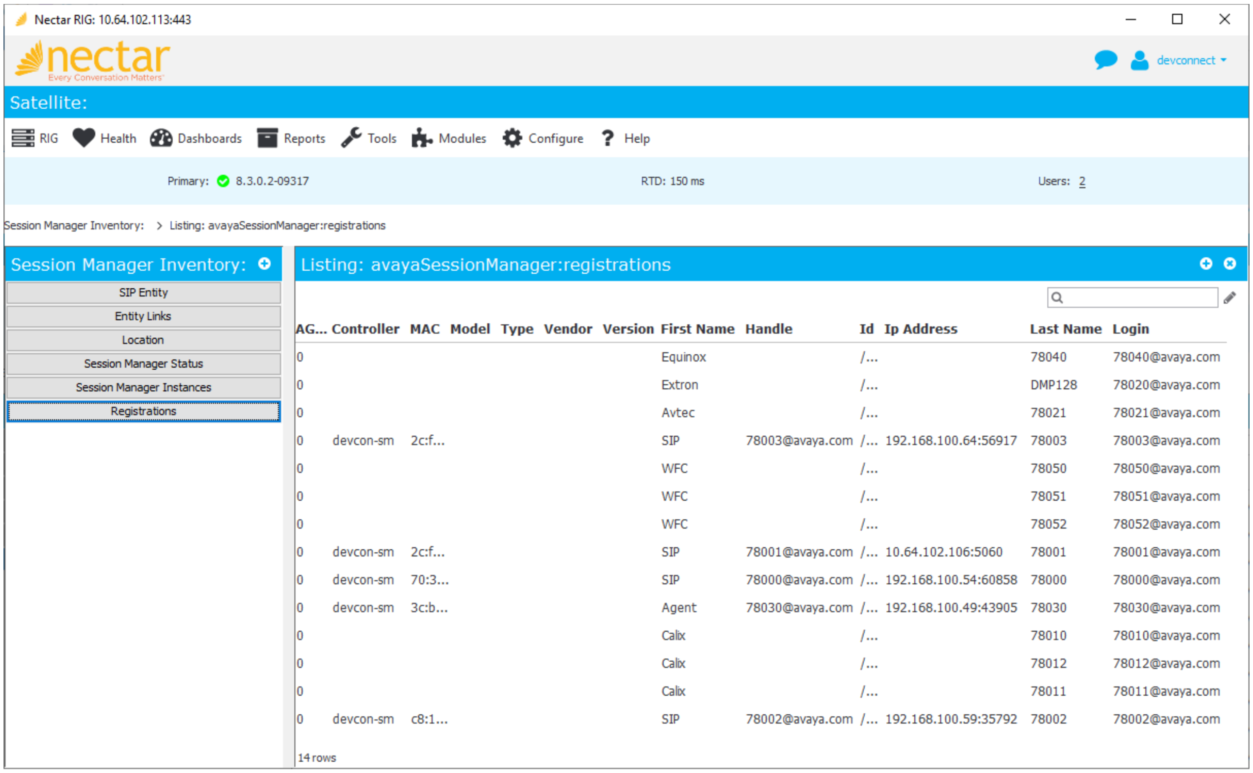
1. Navigate to **Reports → Inventory → Avaya → System Manager (r7.1 or above)** and select either **SIP Entity**, **Entity Links**, or **Location** to verify that Session Manager Inventory can be retrieved using the System Manager Routing Web Service. The following screen displays the list of SIP entities.


Nectar RIG: 10.64.102.113:443
nectar
Every Conversation Matters
devconnect
Satellite:
RIG
Health
Dashboards
Reports
Tools
Modules
Configure
Help
Primary: 8.3.0.2-09317
RTD: 143 ms
Users: 2
Session Manager Inventory: > Listing: avayaSessionManager:sipEntities
Session Manager Inventory:
SIP Entity
Entity Links
Location
Session Manager Status
Session Manager Instances
Registrations
Listing: avayaSessionManager:sipEntities

AGENTINDEX	Cdr Setting	Credential Name	FQDN or IP Address	Loop Detect Mode	Name	Outbound Proxy	Time Zone
0	egress		192.168.100.220	on	Vocera		America/New_York
0	none		10.64.102.117	on	devco...		America/New_York
0	none		10.64.102.101	on	devco...		America/New_York
0	none		10.64.102.115	on	devco...		America/New_York
0	egress		10.64.102.90	on	devco...		America/New_York
0	egress		10.64.102.106	on	devco...		America/New_York
0	none		10.64.102.111	on	devco...		America/New_York
0	egress		10.64.102.107	on	VHT-I...		America/New_York
0	egress		10.64.102.109	on	VHT-...		America/New_York

9 rows

2. Navigate to **Reports → Inventory → Avaya → System Manager (r7.1 or above)** and select either **Session Manager Status**, **Session Manager Instances**, or **Registrations** to verify that Session Manager Inventory can be retrieved using the Session Manager Element Manager Web Service. The following screen displays the user registrations.



Primary: 8.3.0.2-09317 RTD: 150 ms Users: 2

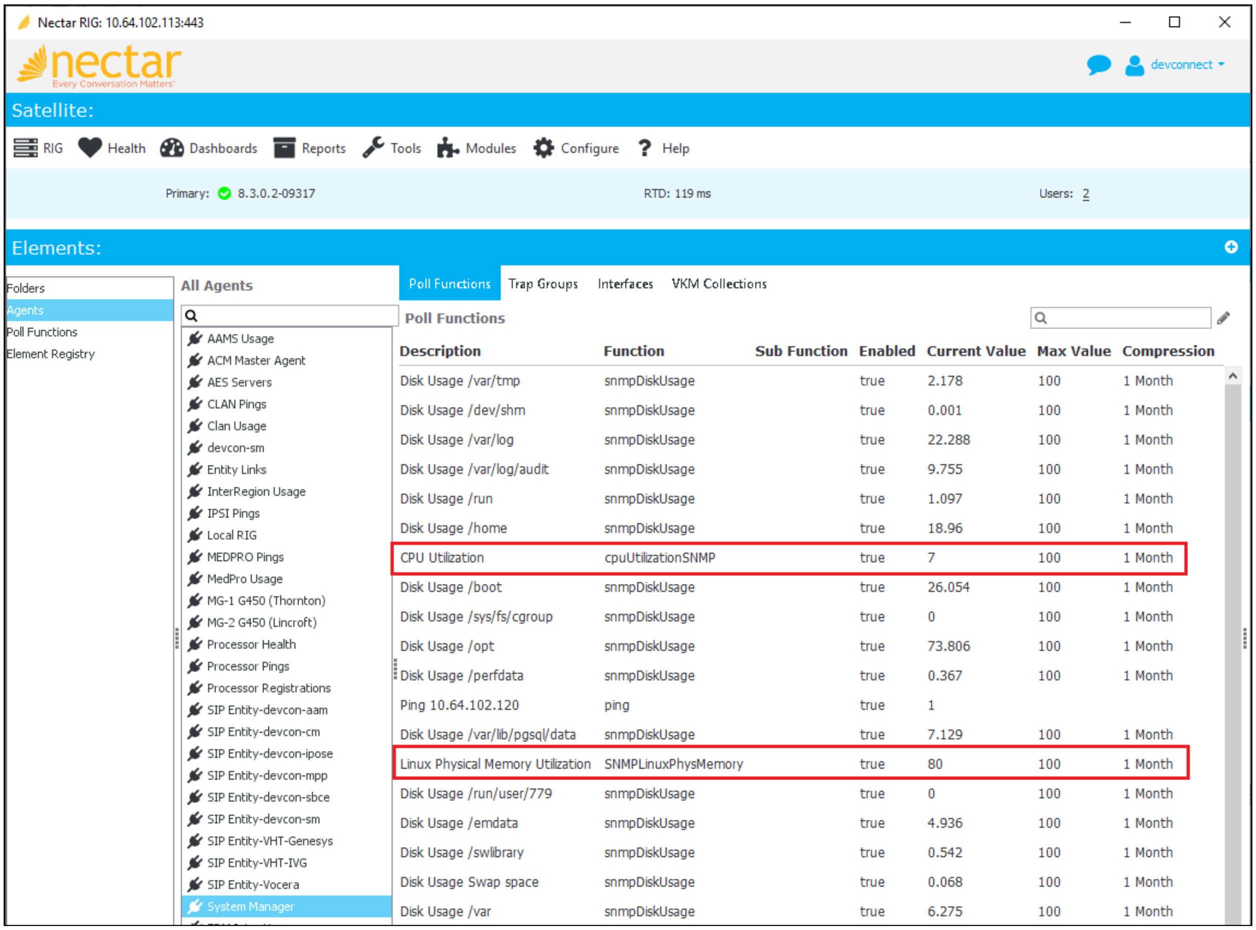
Session Manager Inventory: > Listing: avayaSessionManager:registrations

Listing: avayaSessionManager:registrations

AG...	Controller	MAC	Model	Type	Vendor	Version	First Name	Handle	Id	Ip Address	Last Name	Login
0							Equinox		/...		78040	78040@avaya.com
0							Extron		/...		DMP128	78020@avaya.com
0							Avtec		/...		78021	78021@avaya.com
0	devcon-sm	2c:f...					SIP	78003@avaya.com	/...	192.168.100.64:56917	78003	78003@avaya.com
0							WFC		/...		78050	78050@avaya.com
0							WFC		/...		78051	78051@avaya.com
0							WFC		/...		78052	78052@avaya.com
0	devcon-sm	2c:f...					SIP	78001@avaya.com	/...	10.64.102.106:5060	78001	78001@avaya.com
0	devcon-sm	70:3...					SIP	78000@avaya.com	/...	192.168.100.54:60858	78000	78000@avaya.com
0	devcon-sm	3c:b...					Agent	78030@avaya.com	/...	192.168.100.49:43905	78030	78030@avaya.com
0							Calix		/...		78010	78010@avaya.com
0							Calix		/...		78012	78012@avaya.com
0							Calix		/...		78011	78011@avaya.com
0	devcon-sm	c8:1...					SIP	78002@avaya.com	/...	192.168.100.59:35792	78002	78002@avaya.com

14 rows

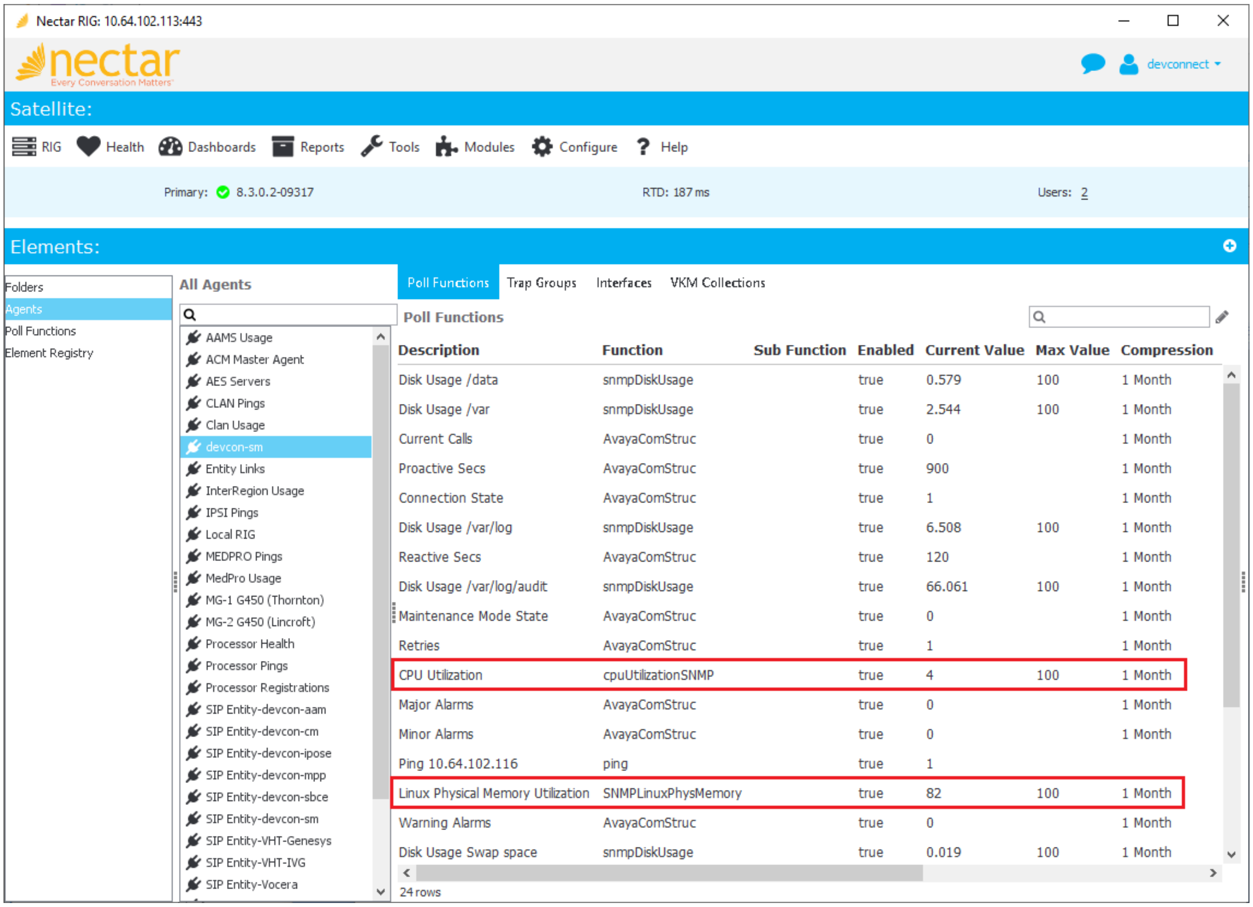
3. Navigate to **Health → Elements** and select **Agents** in the leftmost pane. In the **All Agents** pane, select the System Manager agent. In the **Poll Functions** tab, the *CPU Utilization* and *Linux Physical Memory Utilization*, derived from SNMPv3 polls, should be displayed.



Poll Functions

Description	Function	Sub Function	Enabled	Current Value	Max Value	Compression
Disk Usage /var/tmp	snmpDiskUsage		true	2.178	100	1 Month
Disk Usage /dev/shm	snmpDiskUsage		true	0.001	100	1 Month
Disk Usage /var/log	snmpDiskUsage		true	22.288	100	1 Month
Disk Usage /var/log/audit	snmpDiskUsage		true	9.755	100	1 Month
Disk Usage /run	snmpDiskUsage		true	1.097	100	1 Month
Disk Usage /home	snmpDiskUsage		true	18.96	100	1 Month
CPU Utilization	cpuUtilizationSNMP		true	7	100	1 Month
Disk Usage /boot	snmpDiskUsage		true	26.054	100	1 Month
Disk Usage /sys/fs/cgroup	snmpDiskUsage		true	0	100	1 Month
Disk Usage /opt	snmpDiskUsage		true	73.806	100	1 Month
Disk Usage /perfdata	snmpDiskUsage		true	0.367	100	1 Month
Ping 10.64.102.120	ping		true	1		
Disk Usage /var/lib/pgsql/data	snmpDiskUsage		true	7.129	100	1 Month
Linux Physical Memory Utilization	SNMPLinuxPhysMemory		true	80	100	1 Month
Disk Usage /run/user/779	snmpDiskUsage		true	0	100	1 Month
Disk Usage /emdata	snmpDiskUsage		true	4.936	100	1 Month
Disk Usage /swlibrary	snmpDiskUsage		true	0.542	100	1 Month
Disk Usage Swap space	snmpDiskUsage		true	0.068	100	1 Month
Disk Usage /var	snmpDiskUsage		true	6.275	100	1 Month

4. Navigate to **Health → Elements** and select **Agents** in the leftmost pane. In the **All Agents** pane, select the Session Manager agent. In the **Poll Functions** tab, the *CPU Utilization* and *Linux Physical Memory Utilization*, derived from SNMPv3 polls, should be displayed.



Description	Function	Sub Function	Enabled	Current Value	Max Value	Compression
Disk Usage /data	snmpDiskUsage		true	0.579	100	1 Month
Disk Usage /var	snmpDiskUsage		true	2.544	100	1 Month
Current Calls	AvayaComStruc		true	0		1 Month
Proactive Secs	AvayaComStruc		true	900		1 Month
Connection State	AvayaComStruc		true	1		1 Month
Disk Usage /var/log	snmpDiskUsage		true	6.508	100	1 Month
Reactive Secs	AvayaComStruc		true	120		1 Month
Disk Usage /var/log/audit	snmpDiskUsage		true	66.061	100	1 Month
Maintenance Mode State	AvayaComStruc		true	0		1 Month
Retries	AvayaComStruc		true	1		1 Month
CPU Utilization	cpuUtilizationSNMP		true	4	100	1 Month
Major Alarms	AvayaComStruc		true	0		1 Month
Minor Alarms	AvayaComStruc		true	0		1 Month
Ping 10.64.102.116	ping		true	1		
Linux Physical Memory Utilization	SNMPLinuxPhysMemory		true	82	100	1 Month
Warning Alarms	AvayaComStruc		true	0		1 Month
Disk Usage Swap space	snmpDiskUsage		true	0.019	100	1 Month

8. Conclusion

These Application Notes described the configuration steps required to integrate Nectar Foundation with Avaya Aura® System Manager and Avaya Aura® Session Manager using Avaya Aura® System Manager Web Services and SNMP polling. The compliance test passed with observations noted in **Section 2.2.**

9. Additional References

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

[1] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, April 2020, available at http://support.avaya.com.

[2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 3, March 2020, available at http://support.avaya.com.

[3] *Avaya Routing Web Service API Programming Reference*, Release 8.1, Issue 1, June 2019, available at http://support.avaya.com.

[4] *Avaya Aura® Session Manager Element Manager Web Service API Programming Reference*, Release 7.1.1, Issue 1.0, August 2017, available at http://support.avaya.com.

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.