Avaya Solution & Interoperability Test Lab

Application Notes for Nectar for Avaya with Avaya Aura® Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Nectar for Avaya with Avaya Aura® Application Enablement Services. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It captures information about the DMCC and TSAPI services running on Avaya Aura® Application Enablement Services, such as link status, service state, licenses acquired and errors, number of active sessions, and messages sent, using SNMP polling. Nectar for Avaya also captures alarms using SNMP traps.

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 for Avaya with Avaya Aura® Application Enablement Services (AES). Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It captures information about the Device, Media, and Call Control (DMCC) and Telephony Service Application Programming Interface (TSAPI) services running on Avaya Aura® Application Enablement Services, such as link status, service state, licenses acquired and errors, number of active sessions, and messages sent, using Simple Network Management Protocol (SNMP) polling. Nectar for Avaya also captures alarms using SNMP traps.

The following table specifies the SNMP versions supported between Nectar and Avaya Aura® Application Enablement Services for SNMP traps and polls.

Avaya Product	Data Type	SNMP Version(s)
Avaya Aura® Application Enablement Services	SNMP Traps	SNMPv2c, v3
	SNMP Polling	SNMPv2c, v3

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 to capture information about AES DMCC and TSAPI services and alarms using SNMP. The data was displayed on the Nectar Remote Intelligence Gateway (RIG) client.

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

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 Nectar for Avaya used SNMPv3 for SNMP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following Nectar features and functionality.

- Collecting DMCC and TSAPI service data (i.e., service state, link state, license info, active sessions, and messages sent) from AES using SNMPv2c and v3 polling.
- Capturing SNMP traps for AES alarm conditions using SNMPv2c and v3 traps.
- Displaying the AES DMCC and TSAPI data and AES alarms in the RIG client.
- Verifying proper system recovery after a restart of Nectar and loss of IP network connectivity.

2.2. Test Results

All tests passed with the following observation:

- In AES 10.1.0.2, SNMPv3 trap receiver configuration is performed via the OAM web-based interface and also requires manually modifying the `/etc/snmp/snmpd.conf` configuration file. This is not required when configuring SNMPv2c traps. Refer to **Section 5.3.1**.
- When SNMPv3 traps is configured, AES also sends Inform Requests to the SNMP trap receiver.
- If AES is configured for SNMPv3 traps, but SNMPv2c traps are also being sent by AES, remove SNMPv2c traps by using the `configureNMS.sh` command as described in **Section 5.3.1**.

2.3. Support

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

Phone:	+1 (888) 811-8647 (US) +1 (631) 270-1077 (outside the US)
Website:	https://support.nectarcorp.com
Email:	support@nectarcorp.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Nectar for Avaya in an Avaya Aura® environment, including AES. Nectar captured data and alarms from AES using SNMP and displayed them on the RIG client.

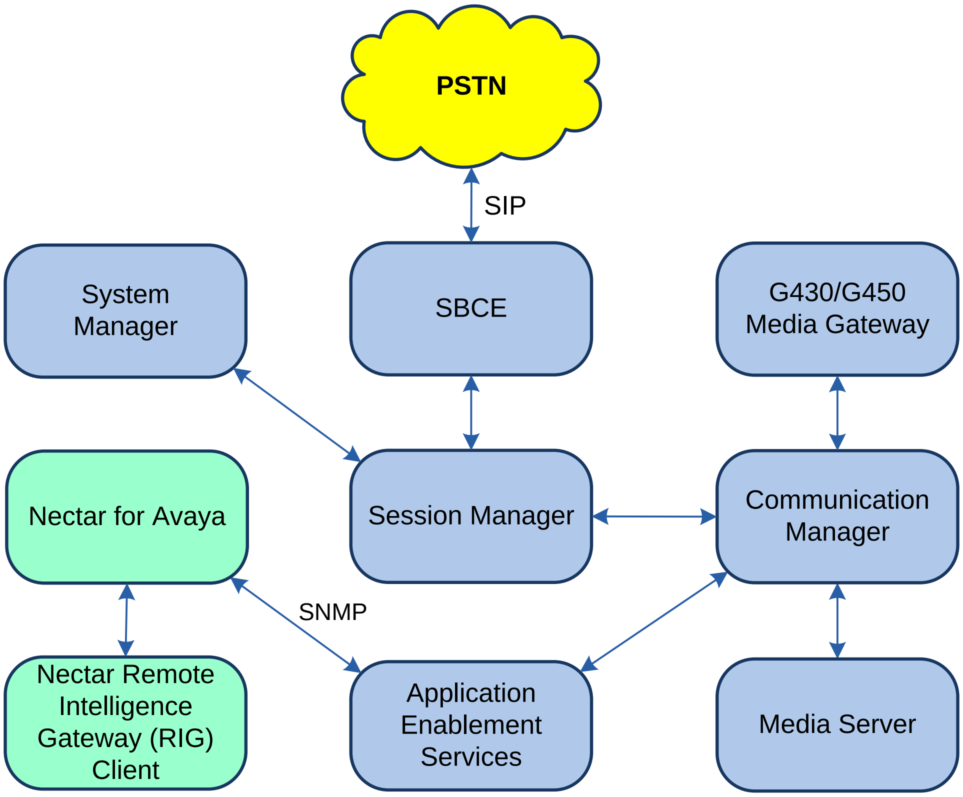


Figure 1: Nectar for Avaya with Avaya Aura® Application Enablement Services

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	10.1.0.1.0-SP1
Avaya G430 Media Gateway	FW 42.8.0 Vintage 1
Avaya G450 Media Gateway	FW 42.7.0 Vintage 3
Avaya Aura® Media Server	v.10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya Aura® Application Enablement Services	10.1.0.2.0.12-0
Nectar for Avaya	2022.1-21422
Nectar Remote Intelligence Gateway (RIG) Client	2022.1-20314

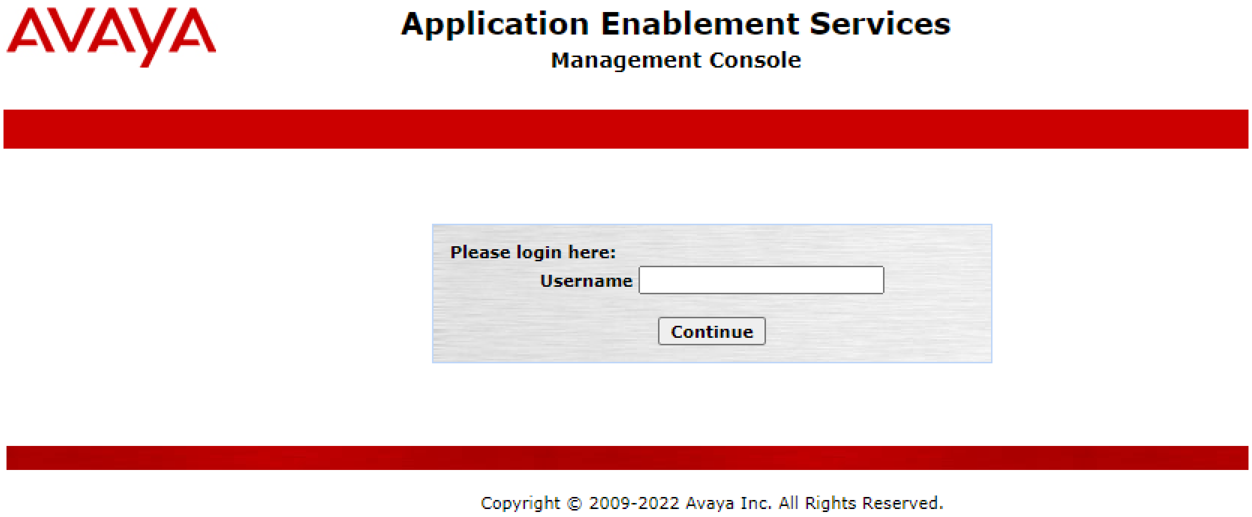
5. Configure Avaya Aura® Application Enablement Services

This section covers the configuration of SNMP traps and polling on AES using the OAM web-based interface. The procedure includes the following areas:

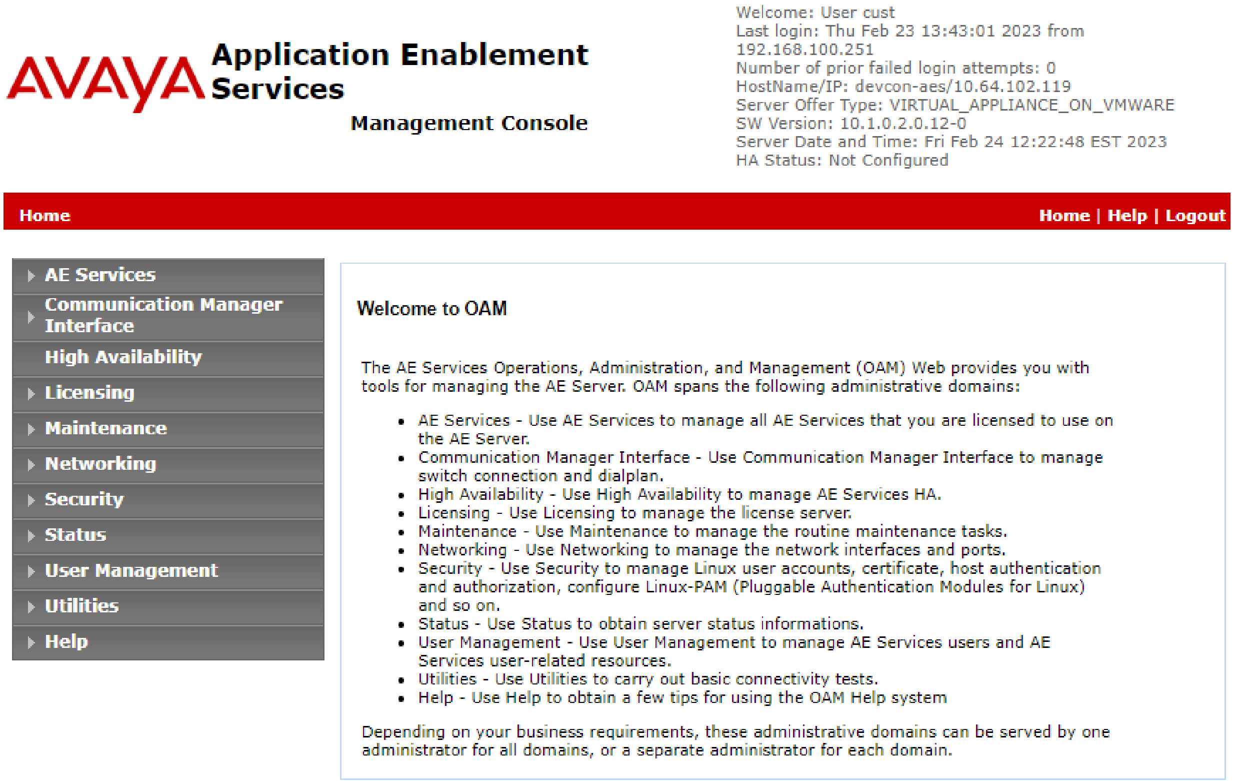
- Launch OAM Interface
- Administer SNMP Agent Settings
- Administer SNMP Trap Receiver Configuration

5.1. Launch OAM Interface

AES is configured via the OAM web interface. To access the web interface, enter **https://<*ip-addr*>** as the URL in a web browser, where <*ip-addr*> is the AES IP address. Log in using the appropriate credentials.


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Continue
Copyright © 2009-2022 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Thu Feb 23 13:43:01 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Fri Feb 24 12:22:48 EST 2023
HA Status: Not Configured

Welcome to OAM

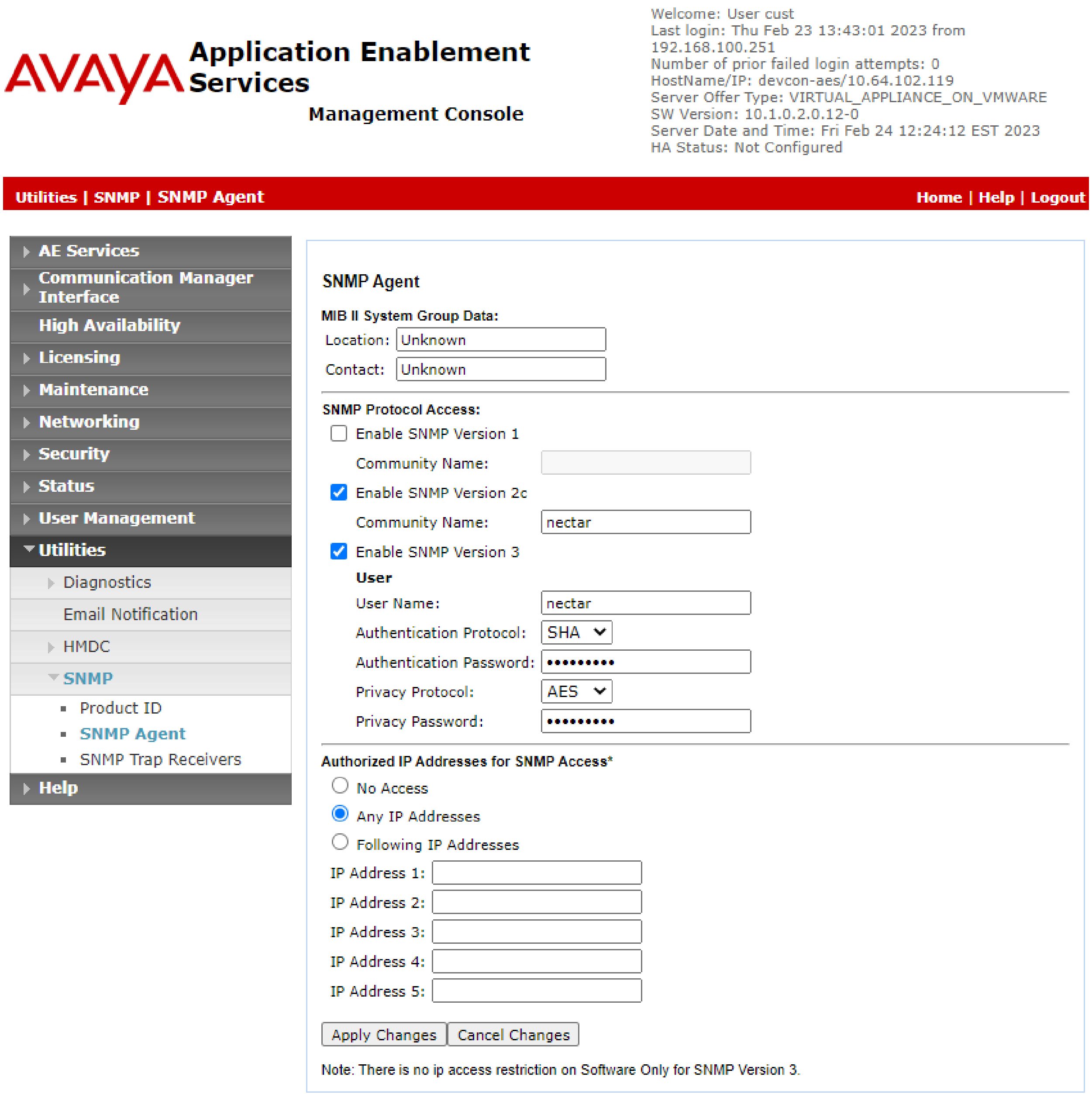
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

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

5.2. Administer SNMP Agent Settings

Navigate to **Utilities → SNMP → SNMP Agent** to enable SNMP polling. In the sample configuration below, SNMP polling using SNMPv2c and SNMPv3 are configured simultaneously for informational purposes. Note that only one SNMP version needs to be configured.



Welcome: User cust
Last login: Thu Feb 23 13:43:01 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Fri Feb 24 12:24:12 EST 2023
HA Status: Not Configured

SNMP Agent

MIB II System Group Data:

Location: Unknown

Contact: Unknown

SNMP Protocol Access:

□ Enable SNMP Version 1

Community Name:

☑ Enable SNMP Version 2c

Community Name: nectar

☑ Enable SNMP Version 3

User

User Name: nectar

Authentication Protocol: SHA

Authentication Password: •••••••••

Privacy Protocol: AES

Privacy Password: •••••••••

Authorized IP Addresses for SNMP Access*

○ No Access

● Any IP Addresses

○ Following IP Addresses

IP Address 1:

IP Address 2:

IP Address 3:

IP Address 4:

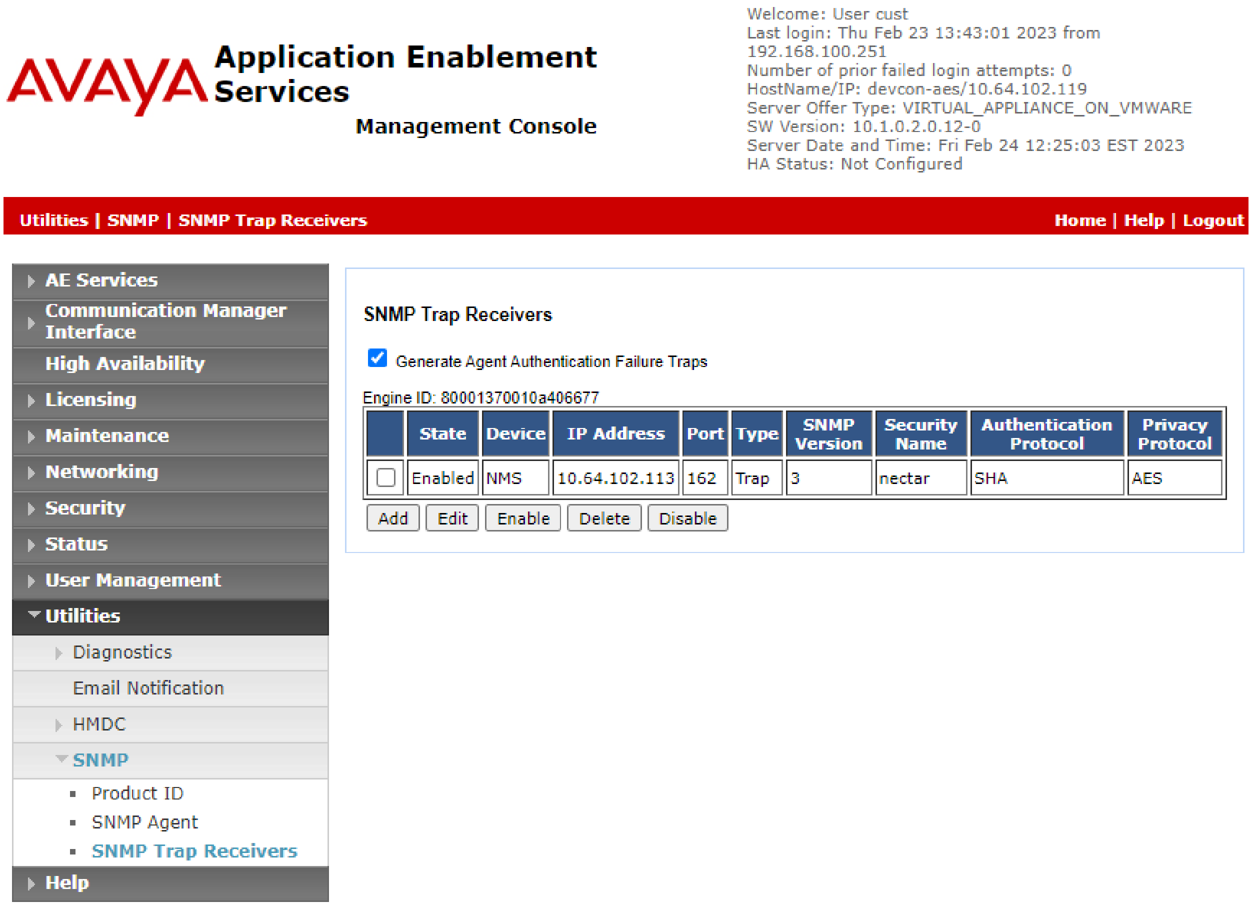
IP Address 5:

Apply Changes | Cancel Changes

Note: There is no ip access restriction on Software Only for SNMP Version 3.

5.3. SNMP Trap Receiver Configuration

This section covers SNMP trap receiver configuration on AES. On the OAM web interface, navigate to **Utilities → SNMP → SNMP Trap Receivers** to enable SNMP traps. In **SNMP Trap Receivers**, enable **Generate Agent Authentication Failure Traps** as shown below. Click **Add** to add an SNMP trap receiver.



Welcome: User cust
Last login: Thu Feb 23 13:43:01 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Fri Feb 24 12:25:03 EST 2023
HA Status: Not Configured

SNMP Trap Receivers

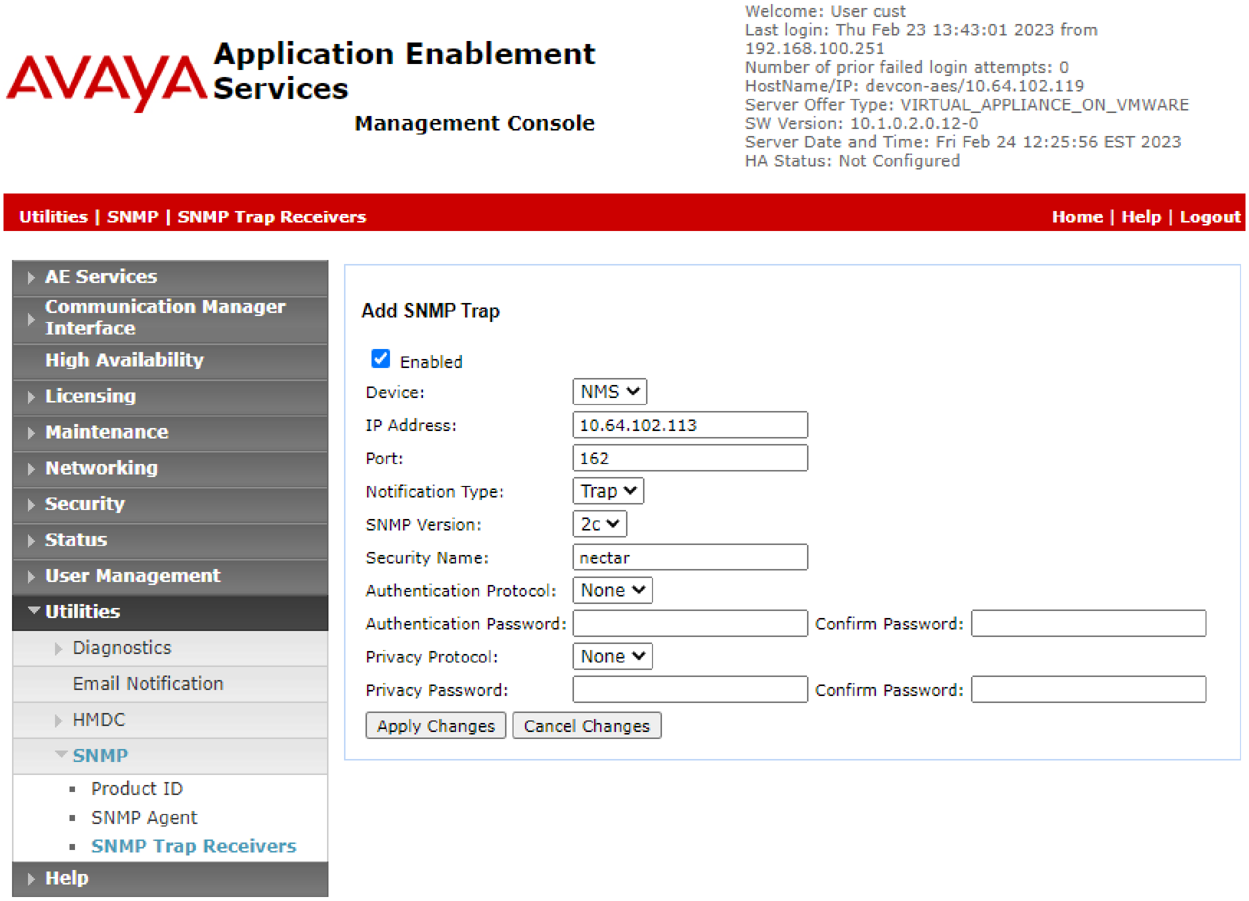
☑ Generate Agent Authentication Failure Traps

Engine ID: 80001370010a406677

	State	Device	IP Address	Port	Type	SNMP Version	Security Name	Authentication Protocol	Privacy Protocol
□	Enabled	NMS	10.64.102.113	162	Trap	3	nectar	SHA	AES

The **SNMP Trap** page is displayed. For SNMPv2c traps, configure the following fields:

Enabled:	Enable the SNMP trap receiver.
Device:	Set to *NMS*.
IP Address:	Set to Nectar IP address (e.g., *10.64.102.113*).
Port:	Set to default SNMP trap port *162*.
Notification Type:	Set to *Trap*.
SNMP Version:	Set to *v2c*.
Security Name:	Set to a valid community name (e.g., *nectar*).


AVAYA Application Enablement Services
Management Console
Welcome: User cust
Last login: Thu Feb 23 13:43:01 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Fri Feb 24 12:25:56 EST 2023
HA Status: Not Configured
Utilities | SNMP | SNMP Trap Receivers
Home | Help | Logout
AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Diagnostics
Email Notification
HMDC
SNMP
Product ID
SNMP Agent
SNMP Trap Receivers
Help
Apply Changes
Cancel Changes

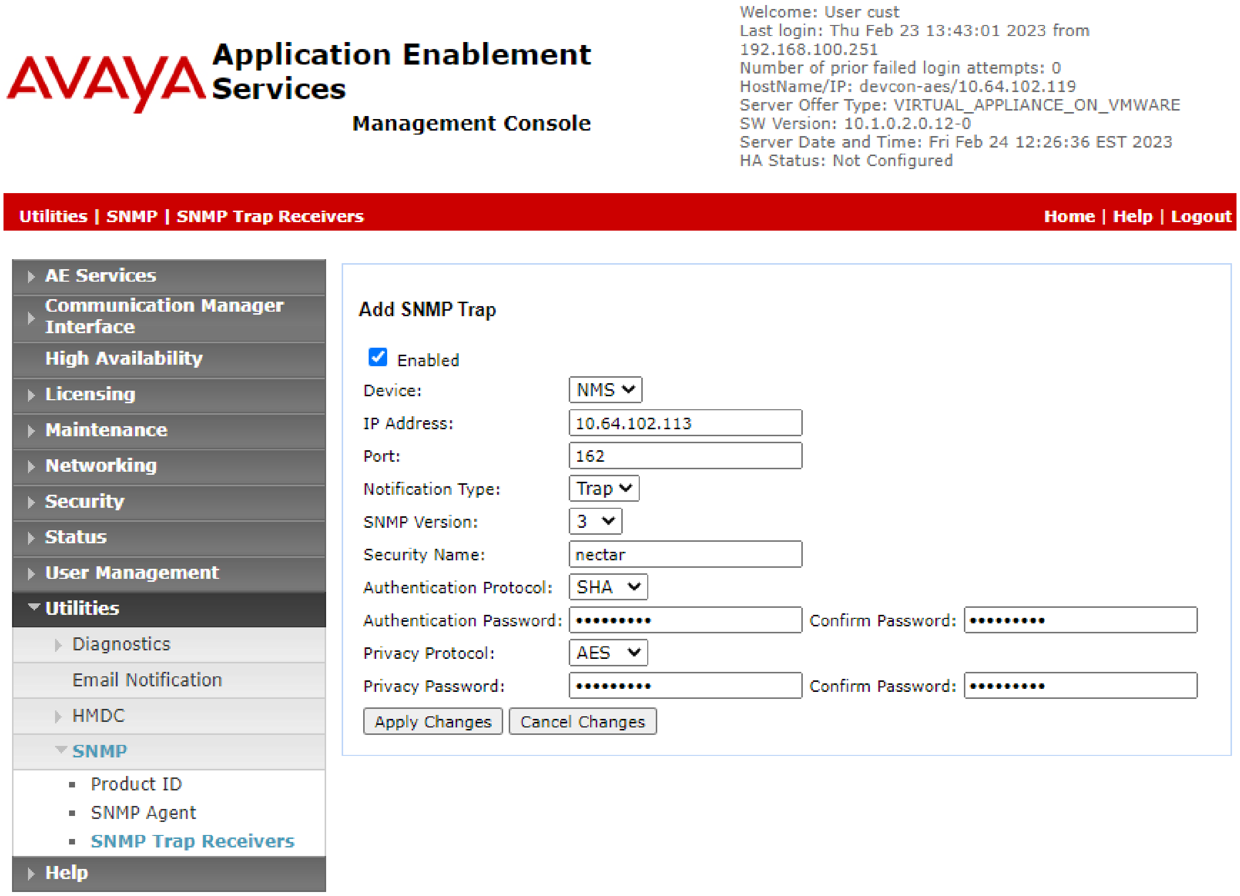
Add SNMP Trap

☑ Enabled

Device:	NMS		
IP Address:	10.64.102.113		
Port:	162		
Notification Type:	Trap		
SNMP Version:	2c		
Security Name:	nectar		
Authentication Protocol:	None		
Authentication Password:		Confirm Password:	
Privacy Protocol:	None		
Privacy Password:		Confirm Password:	

For SNMPv3 traps, configure the following fields in addition to the ones specified above for SNMPv2c traps. The following fields apply to SNMPv3 only and must match the SNMP configuration on Nectar configured in **Section 6.3**.

- **Security Name:** Specify a valid security name (e.g., *nectar*).
  Authentication Protocol: Select the authentication protocol, such as *SHA*.
- **Authentication Password:** Specify an authentication password.
- **Privacy Protocol:** Select the privacy protocol, such as *AES128*.
- **Privacy Password:** Specify a privacy password.



Welcome: User cust
Last login: Thu Feb 23 13:43:01 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Fri Feb 24 12:26:36 EST 2023
HA Status: Not Configured

Add SNMP Trap

☑ Enabled

Device:	NMS		
IP Address:	10.64.102.113		
Port:	162		
Notification Type:	Trap		
SNMP Version:	3		
Security Name:	nectar		
Authentication Protocol:	SHA		
Authentication Password:	•••••••••	Confirm Password:	•••••••••
Privacy Protocol:	AES		
Privacy Password:	•••••••••	Confirm Password:	•••••••••

Apply Changes | Cancel Changes

5.3.1. Configure /etc/snmpd/snmpd.conf File

After configuring SNMP traps as described in **Section 5.3**, verify that the `/etc/snmp/snmpd.conf` file on AES is correct. Root access is required to perform the following operations.

For SNMPv2c traps, the `snmpd.conf` file should contain the following entries in **USM configuration entries** section. No manual changes should be required for SNMPv2c.

```
# USM configuration entries
trap2sink 10.64.102.113 162
authtrapenable 1
```

For SNMPv3 traps, the `snmpd.conf` file should contain the following entries in **USM configuration entries** section. The **trapsess** command should be added manually to the file with the SNMPv3 credentials configured in **Section 5.3** as shown below.

```
# USM configuration entries
trapsess -u nectar -a SHA -A nectar123 -x AES -X nectar123 10.64.102.113 162
authtrapenable 1
```

If SNMPv3 traps is configured, but SNMPv2c traps are also being sent by AES, run the **/opt/spirit/scripts/configureNMS.sh -l** command to view the SNMP trap versions configured on AES as shown below. If SNMPv2c traps are also listed, remove SNMPv2c traps with the **configureNMS.sh** command.

```
[root@devcon-aes snmp]# /opt/spirit/scripts/configureNMS.sh -l
10.64.102.113 162 nectar trap v2
10.64.102.113 162 nectar inform v3
10.64.102.113 162 nectar trap v3
[root@devcon-aes snmp]# /opt/spirit/scripts/configureNMS.sh -r -v v2 10.64.102.113 162
v2 trap destination(10.64.102.113) removed
```

If changes were made manually to the `snmpd.conf` file or an SNMP trap version was removed via the `configureNMS.sh` command, restart the following services.

```
[root@devcon-aes snmp]# /usr/bin/systemctl restart snmpd.service
[root@devcon-aes snmp]# /usr/bin/systemctl restart aesvcsSpiritAgent.service
```

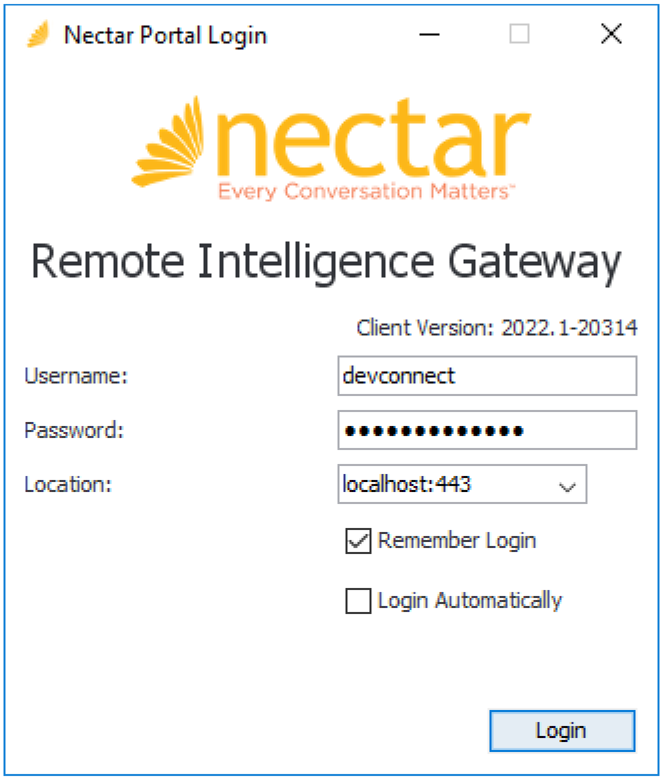
6. Configure Nectar for Avaya

This section covers the Nectar SNMP configuration for AES. The configuration was performed via the **RIG Client**. The procedure covers the following areas:

- Launch the RIG Client
- Configure SNMP Polling Access
- Configure SNMP Traps

6.1. Launch the RIG Client

In an Internet browser, enter the Nectar 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: 2022.1-20314

Username: devconnect

Password: ••••••••••••••

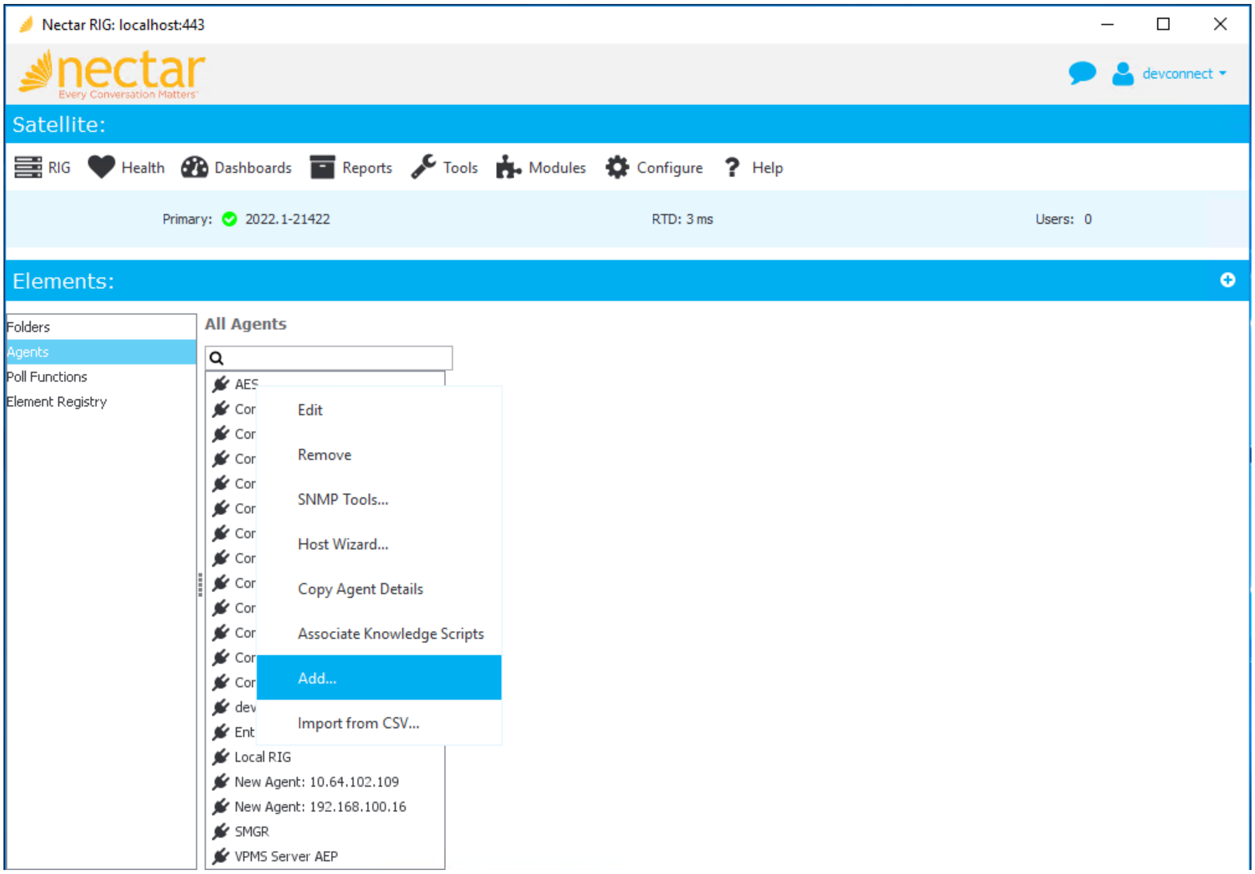
Location: localhost:443

☑ Remember Login

□ Login Automatically

6.2. Configure SNMP Polling Access

Navigate to **Health → Elements → Agents** and right-click in the **All Agents** section (i.e., middle pane) and select **Add** from the pop-up menu as shown below to add an entry for AES.

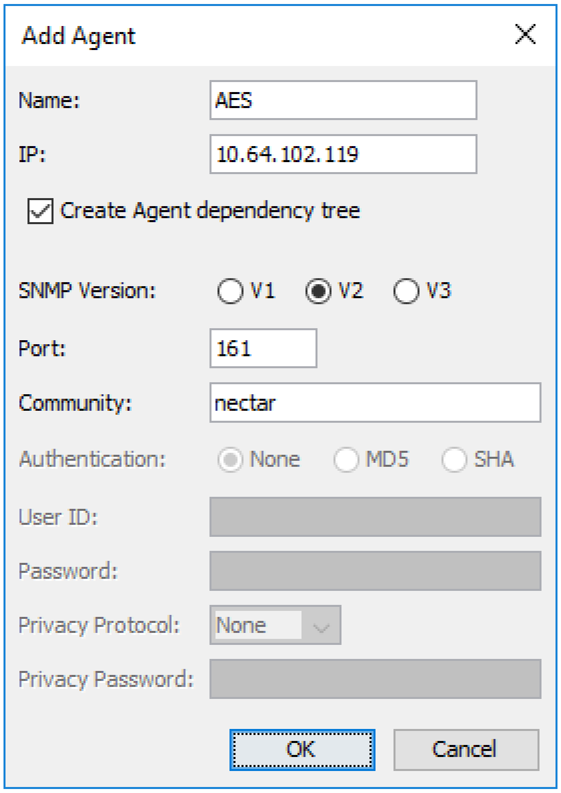


The **Add Agent** dialog box is displayed as shown below. This configuration allows the SNMPv2c or SNMPv3 polling to AES.

To conifgure SNMPv2c polling, configure the following fields:

- **Name:** Provide a descriptive name (e.g., *AES*).
- **IP:** Provide the AES IP address (e.g., *10.64.102.119*).
- **SNMP Version:** Specify SNMPv2c for SNMP polling.
- **Port:** Specify port *161* for SNMP polling.
- **Community:** Specify the community name (e.g., *nectar*) as configured in AES in **Section 5.2**.

Click **OK** to submit the form.



Add Agent

Name: AES

IP: 10.64.102.119

☑ Create Agent dependency tree

SNMP Version: ○ V1 ● V2 ○ V3

Port: 161

Community: nectar

Authentication: ● None ○ MD5 ○ SHA

User ID:

Password:

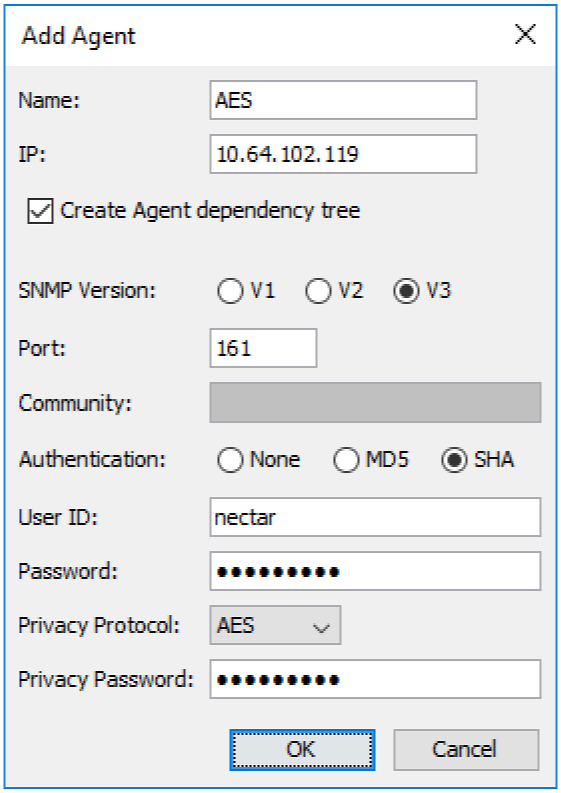
Privacy Protocol: None

Privacy Password:

To configure SNMPv3 polling, configure the following fields:

- **Name:** Provide a descriptive name (e.g., *AES*).
- **IP:** Provide the AES IP address (e.g., *10.64.102.119*).
- **SNMP Version:** Specify SNMPv3 for SNMP polling.
- **Port:** Specify port *161* for SNMP polling.
- **Authentication:** Specify *SHA* authentication.
- **User ID:** Specify the **User Name** (e.g., *nectar*) configured in **Section 5.2**.
- **Password:** Specify the **Authentication Password** configured in AES in **Section 5.2**.
- **Privacy Protocol:** Specify *AES* privacy protocol.
- **Privacy Password:** Specify the **Privacy Password** configured in AES in **Section 5.2**.
- **User ID:** Specify the **User Name** (e.g., *nectar*) configured in AES in **Section 5.2**.

Click **OK** to submit the form.



Add Agent

Name: AES

IP: 10.64.102.119

☑ Create Agent dependency tree

SNMP Version: ○ V1 ○ V2 ● V3

Port: 161

Community:

Authentication: ○ None ○ MD5 ● SHA

User ID: nectar

Password: •••••••••

Privacy Protocol: AES

Privacy Password: •••••••••

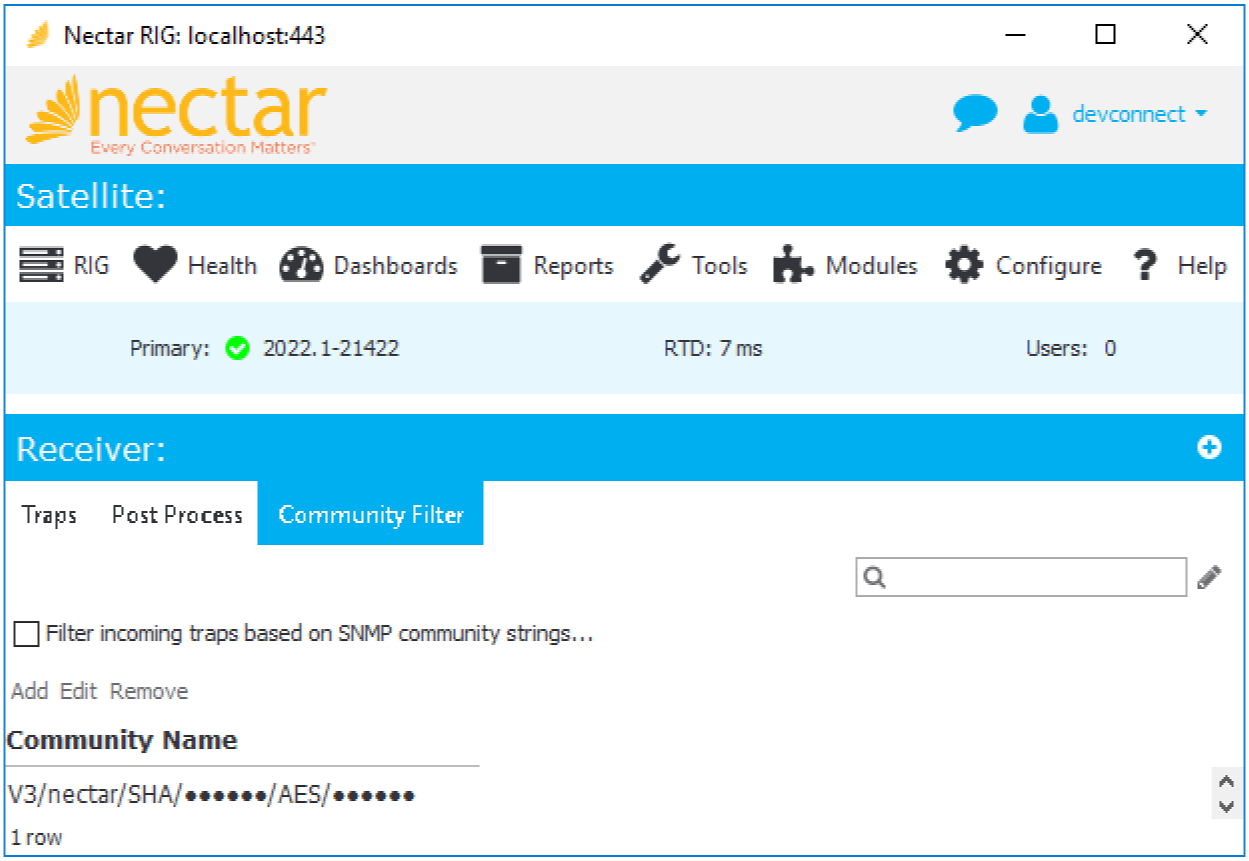
6.3. Configure SNMP Traps

Navigate to **Configure → Receiver** and select the **Community Filter** tab. The Community Filter serves two purposes:

- Filter SNMPv2c traps based on community name (optional).
- Configure credentials for SNMPv3 traps (required).

This section covers the configuration of credentials for SNMPv3 traps. Click **Add**.

Note: There is no additional configuration required to allow SNMPv2c traps.



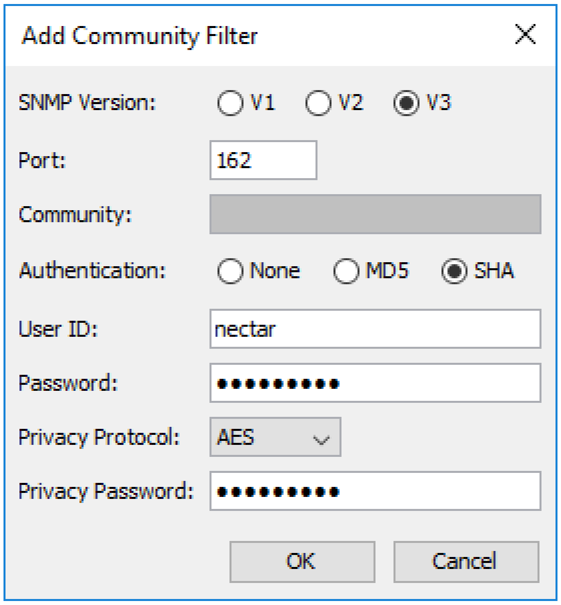
Primary: 2022.1-21422 RTD: 7 ms Users: 0

☐ Filter incoming traps based on SNMP community strings...

Community Name
V3/nectar/SHA/••••••/AES/••••••

1 row

In **Add Community Filter**, set the **SNMP Version** to *V3*, the **Port** to *162*, and specify the credentials as configured on AES. Click **OK**.



Add Community Filter

SNMP Version: ○ V1 ○ V2 ● V3

Port: 162

Community:

Authentication: ○ None ○ MD5 ● SHA

User ID: nectar

Password: ●●●●●●●●●

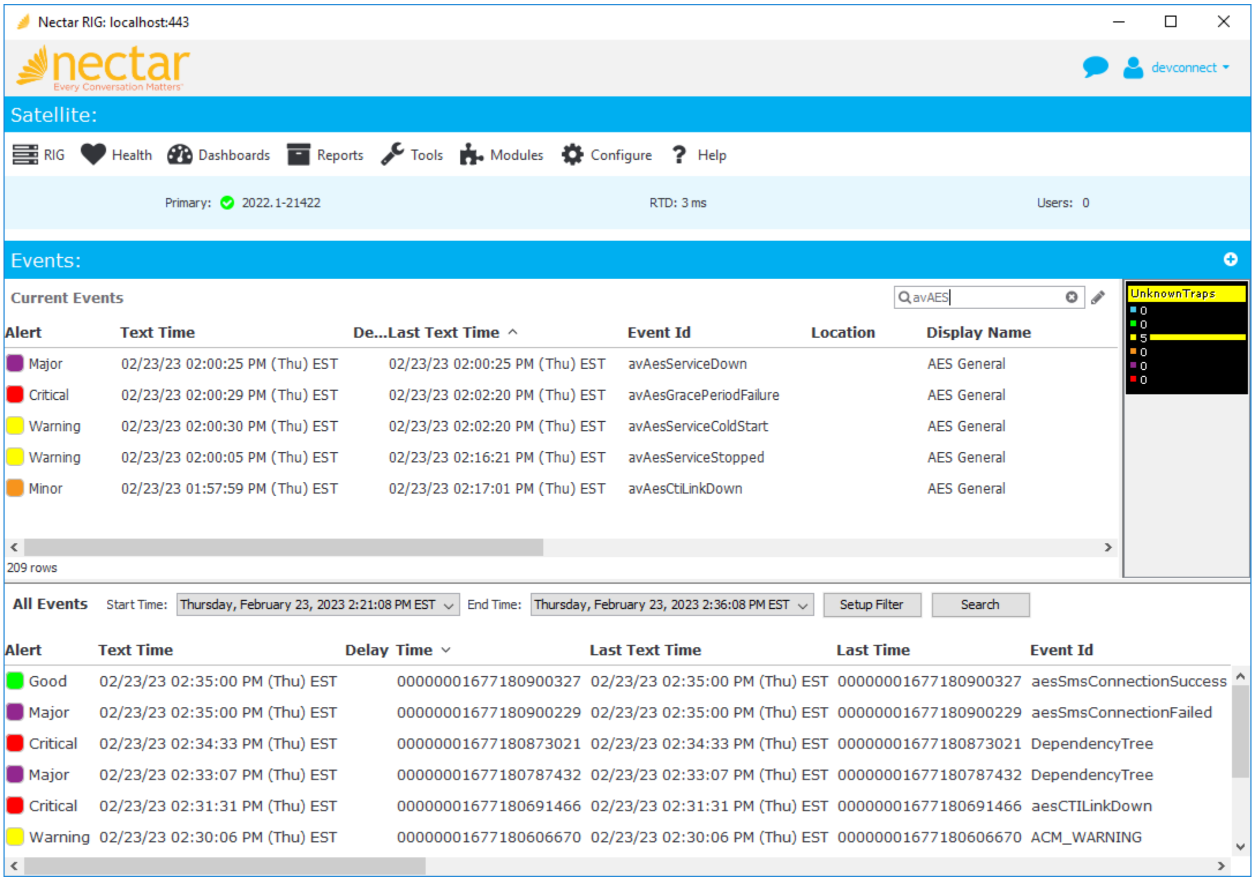
Privacy Protocol: AES

Privacy Password: ●●●●●●●●●

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Nectar for Avaya and AES.

1. Generate AE alarm conditions, such as a CTI link down condition. Navigate to **Health → Events** to view SNMP traps and events as shown below.



Primary: 2022.1-21422 RTD: 3 ms Users: 0

Events:

Current Events avAES

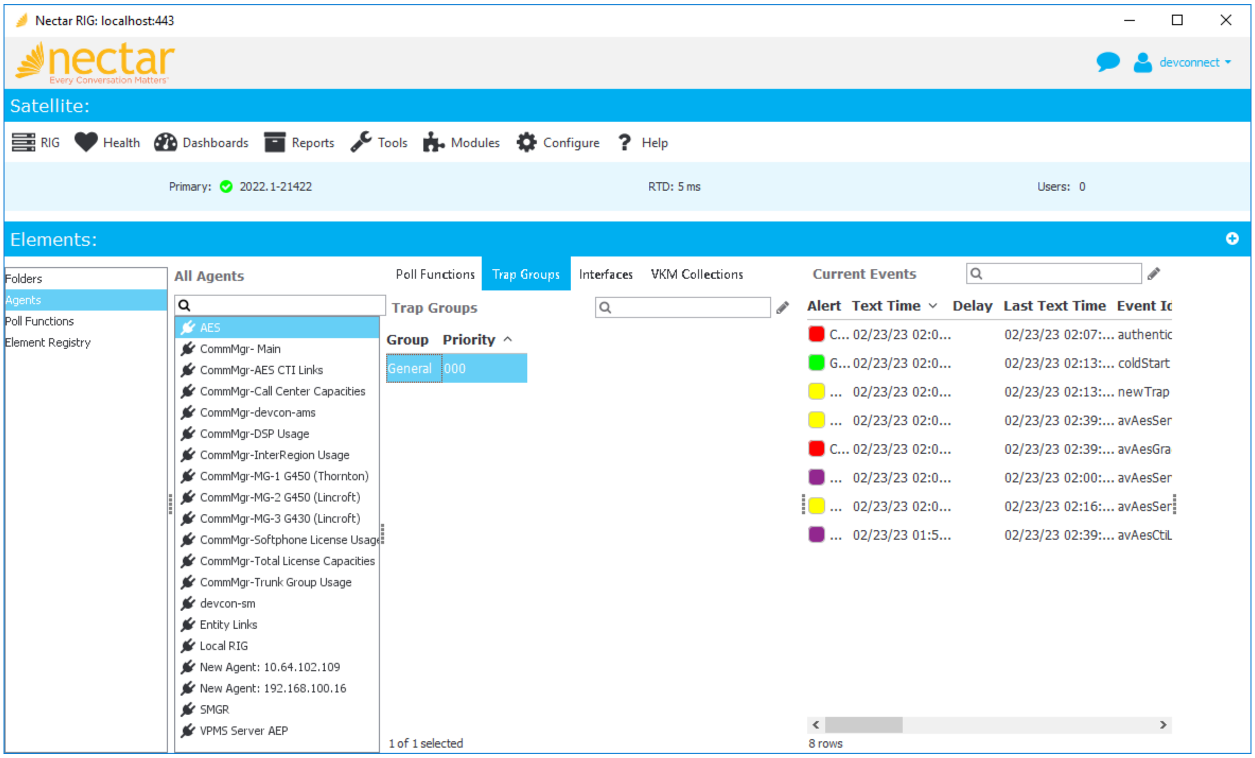
Alert	Text Time	De...Last Text Time	Event Id	Location	Display Name
🟪 Major	02/23/23 02:00:25 PM (Thu) EST	02/23/23 02:00:25 PM (Thu) EST	avAesServiceDown		AES General
🟥 Critical	02/23/23 02:00:29 PM (Thu) EST	02/23/23 02:02:20 PM (Thu) EST	avAesGracePeriodFailure		AES General
🟨 Warning	02/23/23 02:00:30 PM (Thu) EST	02/23/23 02:02:20 PM (Thu) EST	avAesServiceColdStart		AES General
🟨 Warning	02/23/23 02:00:05 PM (Thu) EST	02/23/23 02:16:21 PM (Thu) EST	avAesServiceStopped		AES General
🟧 Minor	02/23/23 01:57:59 PM (Thu) EST	02/23/23 02:17:01 PM (Thu) EST	avAesCtiLinkDown		AES General

209 rows

All Events Start Time: Thursday, February 23, 2023 2:21:08 PM EST End Time: Thursday, February 23, 2023 2:36:08 PM EST Setup Filter Search

Alert	Text Time	Delay	Time	Last Text Time	Last Time	Event Id
🟩 Good	02/23/23 02:35:00 PM (Thu) EST		0000001677180900327	02/23/23 02:35:00 PM (Thu) EST	0000001677180900327	aesSmsConnectionSuccess
🟪 Major	02/23/23 02:35:00 PM (Thu) EST		0000001677180900229	02/23/23 02:35:00 PM (Thu) EST	0000001677180900229	aesSmsConnectionFailed
🟥 Critical	02/23/23 02:34:33 PM (Thu) EST		0000001677180873021	02/23/23 02:34:33 PM (Thu) EST	0000001677180873021	DependencyTree
🟪 Major	02/23/23 02:33:07 PM (Thu) EST		0000001677180787432	02/23/23 02:33:07 PM (Thu) EST	0000001677180787432	DependencyTree
🟥 Critical	02/23/23 02:31:31 PM (Thu) EST		0000001677180691466	02/23/23 02:31:31 PM (Thu) EST	0000001677180691466	aesCTILinkDown
🟨 Warning	02/23/23 02:30:06 PM (Thu) EST		0000001677180606670	02/23/23 02:30:06 PM (Thu) EST	0000001677180606670	ACM_WARNING

2. Alternatively, AES alarms may also be viewed by navigating to **Health → Elements → Agents**. Select *AES* under **All Agents** and then select the **Trap Groups** tab. In the **Trap Groups** tab, click on the **Group** as shown below. SNMP traps are displayed to the right.



Trap Groups

Group	Priority
General	000

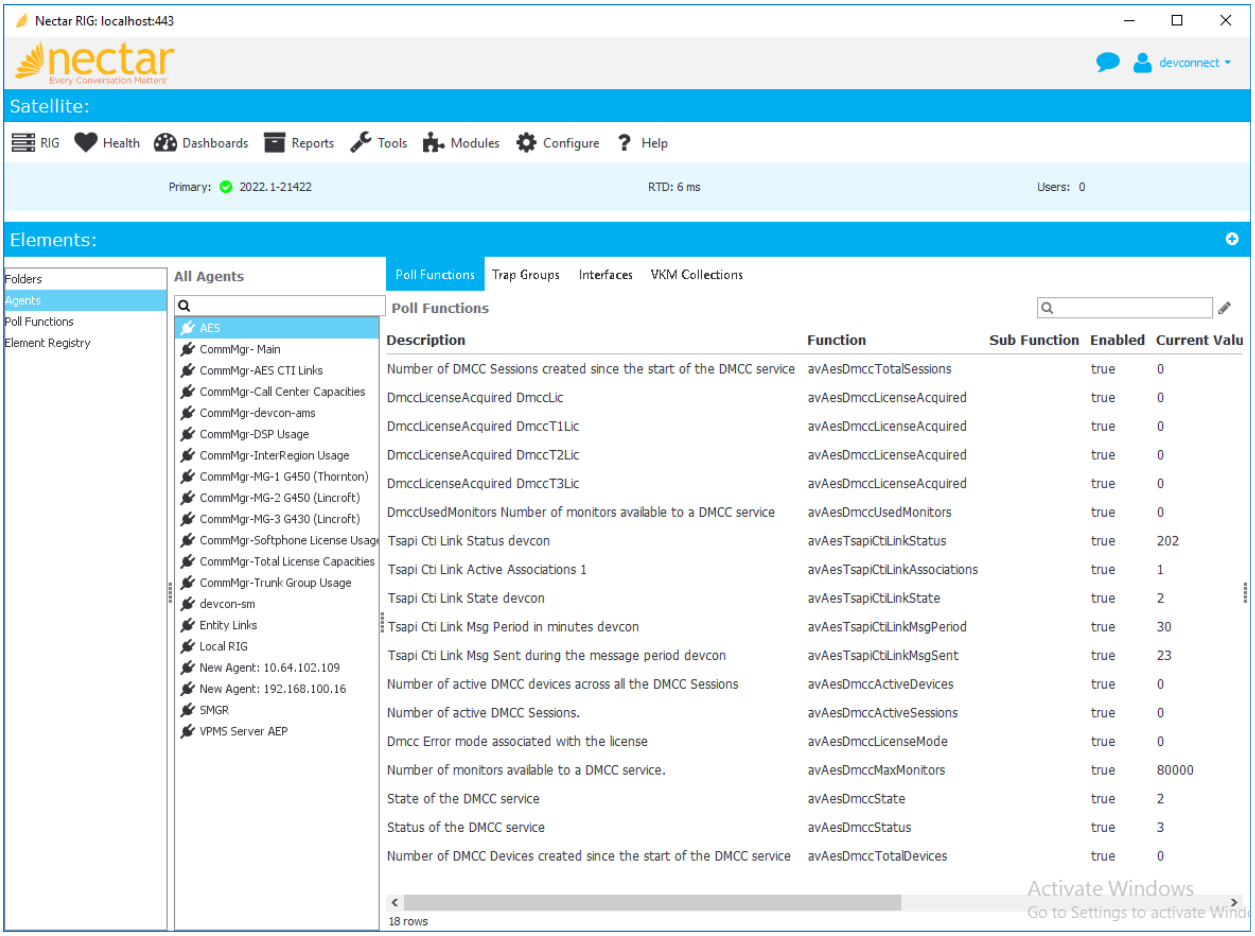
1 of 1 selected

Current Events

Alert	Text Time	Delay	Last Text Time	Event Ic
🟥 C...	02/23/23 02:0...		02/23/23 02:07:...	authentic
🟩 G...	02/23/23 02:0...		02/23/23 02:13:...	coldStart
🟨 ...	02/23/23 02:0...		02/23/23 02:13:...	newTrap
🟨 ...	02/23/23 02:0...		02/23/23 02:39:...	avAesSer
🟥 C...	02/23/23 02:0...		02/23/23 02:39:...	avAesGra
🟪 ...	02/23/23 02:0...		02/23/23 02:00:...	avAesSer
🟨 ...	02/23/23 02:0...		02/23/23 02:16:...	avAesSer
🟪 ...	02/23/23 01:5...		02/23/23 02:39:...	avAesCtiL

8 rows

3. Navigate to **Health → Elements → Agents** and then select *AES* under **All Agents** to view the SNMP polling data as shown below.



Primary: 2022.1-21422 RTD: 6 ms Users: 0

Poll Functions

Description	Function	Sub Function	Enabled	Current Valu
Number of DMCC Sessions created since the start of the DMCC service	avAesDmccTotalSessions		true	0
DmccLicenseAcquired DmccLic	avAesDmccLicenseAcquired		true	0
DmccLicenseAcquired DmccT1Lic	avAesDmccLicenseAcquired		true	0
DmccLicenseAcquired DmccT2Lic	avAesDmccLicenseAcquired		true	0
DmccLicenseAcquired DmccT3Lic	avAesDmccLicenseAcquired		true	0
DmccUsedMonitors Number of monitors available to a DMCC service	avAesDmccUsedMonitors		true	0
Tsapi Cti Link Status devcon	avAesTsapiCtiLinkStatus		true	202
Tsapi Cti Link Active Associations 1	avAesTsapiCtiLinkAssociations		true	1
Tsapi Cti Link State devcon	avAesTsapiCtiLinkState		true	2
Tsapi Cti Link Msg Period in minutes devcon	avAesTsapiCtiLinkMsgPeriod		true	30
Tsapi Cti Link Msg Sent during the message period devcon	avAesTsapiCtiLinkMsgSent		true	23
Number of active DMCC devices across all the DMCC Sessions	avAesDmccActiveDevices		true	0
Number of active DMCC Sessions.	avAesDmccActiveSessions		true	0
Dmcc Error mode associated with the license	avAesDmccLicenseMode		true	0
Number of monitors available to a DMCC service.	avAesDmccMaxMonitors		true	80000
State of the DMCC service	avAesDmccState		true	2
Status of the DMCC service	avAesDmccStatus		true	3
Number of DMCC Devices created since the start of the DMCC service	avAesDmccTotalDevices		true	0

18 rows

8. Conclusion

These Application Notes described the configuration steps required to integrate Nectar for Avaya with Avaya Aura® Application Enablement Services using SNMP. 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® Application Enablement Services*, Release 10.1.x, Issue 6, February 2023, available at http://support.avaya.com.

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.