



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Nectar for Avaya with Avaya Experience Portal 8.1 - Issue 1.0

### Abstract

These Application Notes describe the configuration steps required to integrate Nectar for Avaya with Avaya Experience Portal. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It captures Avaya Media Processing Platform (MPP) operational status, number of active calls, resource utilization (i.e., CPU/Memory/Data usage), application URLs, and alarms from Avaya Experience Portal using SNMP.

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 Experience Portal. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It captures Avaya Media Processing Platform (MPP) operational status, number of active calls, resource utilization (i.e., CPU/Memory/Data usage), application URLs, and alarms from Avaya Experience Portal using SNMP.

The following table specifies the SNMP versions supported between Nectar and Avaya Experience Portal for SNMP traps and polls.

Avaya Product	Data Type	SNMP Version(s)
Avaya Experience Portal	SNMP Traps	SNMPv2c, v3
	SNMP Polling	SNMPv1

# 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 Experience Portal resource utilization, call status, application status, 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 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.

For the testing associated with these Application Notes, the interface between Avaya systems and Nectar for Avaya used the security features provided by SNMPv3 for SNMP traps.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following Nectar features and functionality.

- Collecting MPP resource utilization data (i.e., CPU, memory, and data usage), operational status, number of active calls, and application URLs from Experience Portal using SNMP polling.
- Capturing SNMP traps for alarm conditions on Experience Portal, including MPP.
- Verifying proper system recovery after a restart of Nectar and loss of IP network connectivity.

## 2.2. Test Results

The compliance test passed with the following observations:

- Experience Portal does not support the GETBULK operation. Therefore, only SNMPv1 is supported for SNMP polling.
- Nectar for Avaya does not display SNMP traps when using SNMPv1. Use SNMPv2c or SNMPv3.
- The Dependency Trees on Nectar for Avaya do not support SNMP traps.

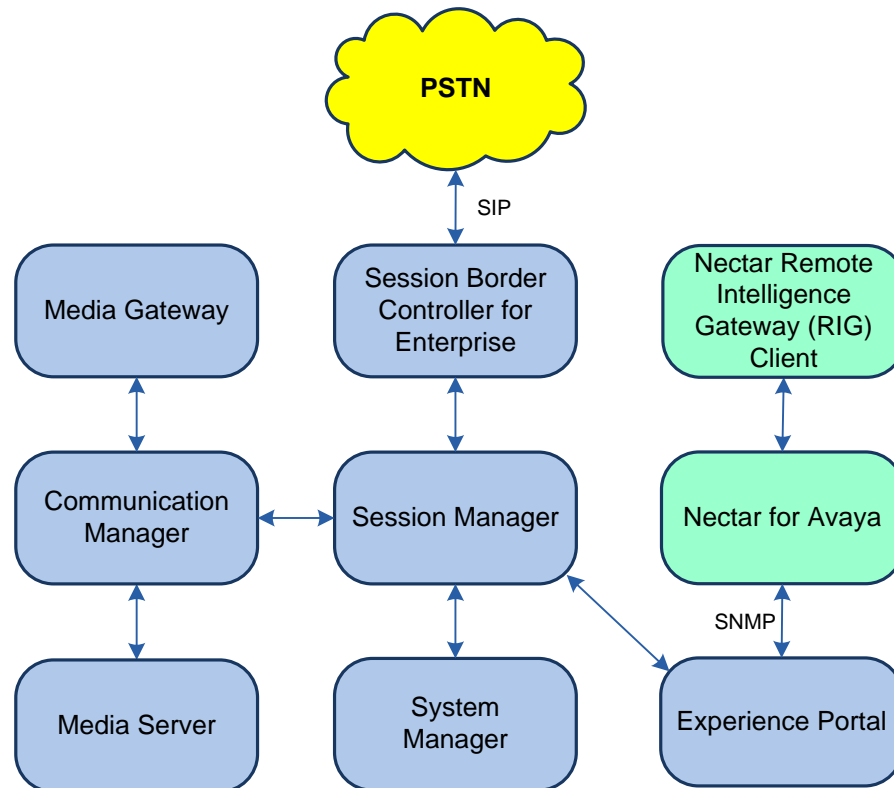
## 2.3. Support

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](mailto:support@nectarcorp.com)

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration consisting of Nectar with an Avaya SIP-based network, including Experience Portal. Nectar captured data and alarms from Experience Portal using SNMP. The RIG client was used to display resource utilization data, MPP operational status, active calls, and alarms.



**Figure 1: Nectar for Avaya 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	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 Experience Portal	8.1.1.0.0251
Nectar for Avaya	2022.1-21422
Nectar Remote Intelligence Gateway (RIG) Client	2022.1-20314

## 5. Configure Avaya Experience Portal

This section covers the configuration of Experience Portal using the Experience Portal Manager (EPM) web interface. The procedure includes the following areas:

- Launch Experience Portal Manager
- Administer SNMP Trap Configuration
- Administer SNMP Agent Settings

### 5.1. Launch Experience Portal Manager

Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://<ip-addr>** as the URL in a web browser, where **<ip-addr>** is the IP address of EPM. Log in using the appropriate credentials.

The image shows the login page of the Avaya Experience Portal 8.1.1. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Avaya Experience Portal 8.1.1 (ExperiencePortal)". The main area is white and contains a "User Name:" label followed by a text input field. Below the input field is a black "Submit" button. At the bottom left, there is a link labeled "Change Password".

The main page of the EPM web interface is displayed as shown below.

**Avaya Experience Portal Manager**

Welcome, epadmin  
Last logged in today at 11:32:11 AM EDT

**Avaya Experience Portal 8.1.1 (ExperiencePortal)**

Expand All | Collapse All

- ▼ **User Management**
  - Roles
  - Users
  - Login Options
- ▼ **Real-time Monitoring**
  - System Monitor
  - Active Calls
  - Port Distribution
- ▼ **System Maintenance**
  - Audit Log Viewer
  - Trace Viewer
  - Log Viewer
  - Alarm Manager
- ▼ **System Management**
  - Application Server
  - EPM Manager
  - MPP Manager
  - Software Upgrade
  - System Backup
- ▼ **System Configuration**
  - Applications
  - EPM Servers
  - MPP Servers
  - SNMP
  - Speech Servers
  - VoIP Connections
  - Zones
- ▼ **Security**
  - Certificates
  - Licensing
- ▼ **Reports**
  - Standard
  - Custom
  - Scheduled
- ▼ **Multi-Media Configuration**
  - Email
  - HTML
  - SMS

You are here: Home

## Avaya Experience Portal Manager

Avaya Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

### Installed Components

**Media Processing Platform**  
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

**Email Service**  
Email Service is an Experience Portal feature which provides e-mail capabilities.

**HTML Service**  
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.

**SMS Service**  
SMS Service is an Experience Portal feature which provides SMS capabilities.

### Legal Notice

AVAYA GLOBAL SOFTWARE LICENSE TERMS  
REVISED: June 1st, 2020

THESE GLOBAL SOFTWARE LICENSE TERMS ("SOFTWARE LICENSE TERMS") GOVERN THE USE OF PROPRIETARY SOFTWARE AND THIRD- PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, THE END USER, ON BEHALF OF THEMSELF AND THE ENTITY FOR WHOM THEY ARE DOING SO (HEREINAFTER REFERRED TO AS "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN END USER AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF THE END USER IS ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THE END USER REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE LICENSE

## 5.2. Administer SNMP Trap Configuration

This section covers SNMP trap configuration on Experience Portal. On the EPM web interface, navigate to **System Configuration** → **SNMP** to display the following page.

The screenshot shows the Avaya Experience Portal 8.1.1 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, a welcome message for 'epadmin', and a 'Last logged in today at 11:32:11 AM EDT' timestamp. The main navigation menu on the left lists various system configuration options, including User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The 'System Configuration' menu item is expanded, showing a list of sub-items including Applications, EPM Servers, MPP Servers, SNMP, Speech Servers, VoIP Connections, Zones, Certificates, Licensing, Standard, Custom, Scheduled, Email, HTML, and SMS.

The main content area displays the 'SNMP' configuration page. The breadcrumb trail indicates the path: **Home** > **System Configuration** > **SNMP**. The page title is 'SNMP'. The description states: 'This page displays the destination servers to which Experience Portal sends Simple Network Management Protocol (SNMP) notifications when certain alarms occur.'

The 'SNMP Traps' section contains a table with the following columns: Host Address, Enable, Device, Transport Protocol, Port, Type, SNMP Version, Security Name, Authentication Protocol, and Privacy Protocol. The table contains one row with the following data: Host Address: 10.64.102.113, Enable: Yes, Device: NMS, Transport Protocol: UDP, Port: 162, Type: Trap, SNMP Version: 3, Security Name: nectar, Authentication Protocol: SHA, Privacy Protocol: AES128. Below the table are buttons for 'Add', 'Delete', and 'Test'.

At the bottom of the page, there are three buttons: 'SNMP Agent Settings', 'SNMP Device Notification Settings', and 'Help'.



Click **Add** to create an SNMP notification destination server as shown below.

Configure the following fields:

- **Enable:** Set to *Yes* to enable this SNMP trap destination.
- **Device:** Set to *NMS*.
- **Transport Protocol:** Set to *UDP*.
- **Host Address:** Set to the 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* or *3*, depending on the SNMP version desired.
- **Security Name:** Specify security name, such as *nectar*. This must match the **Community** on Nectar for SNMPv3.

The following fields apply to SNMPv3 only and must match the SNMP configuration on 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.

**AVAYA** Welcome, epadmin  
Last logged in today at 11:35:57 AM EDT

**Avaya Experience Portal 8.1.1 (ExperiencePortal)** Home Help Logoff

Expand All | Collapse All

**▼ User Management**  
Roles  
Users  
Login Options

**▼ Real-time Monitoring**  
System Monitor  
Active Calls  
Port Distribution

**▼ System Maintenance**  
Audit Log Viewer  
Trace Viewer  
Log Viewer  
Alarm Manager

**▼ System Management**  
Application Server  
EPM Manager  
MPP Manager  
Software Upgrade  
System Backup

**▼ System Configuration**  
Applications  
EPM Servers  
MPP Servers  
SNMP  
Speech Servers  
VoIP Connections  
Zones

**▼ Security**  
Certificates  
Licensing

**▼ Reports**  
Standard  
Custom  
Scheduled

**▼ Multi-Media Configuration**  
Email  
HTML  
SMS

You are here: [Home](#) > [System Configuration](#) > [SNMP](#) > Add SNMP Trap Configuration

### Add SNMP Trap Configuration

Use this page to add a new SNMP notification destination server.

Enable: ☒ Yes ☐ No

Device:

Transport Protocol:

Host Address:

Port:

Notification Type:

SNMP Version:

Security Name:

Authentication Protocol:

Authentication Password:

Privacy Protocol:

Privacy Password:

**Save** **Cancel** **Help**

### 5.3. Administer SNMP Agent Settings

This section covers SNMP agent settings for polling on Experience Portal. On the EPM web interface, navigate to **System Configuration** → **SNMP** and click on **SNMP Agent Settings** (not shown). **Enable SNMP Version 1** and specify a **Security Name**, such as *nectar*. **Under Authorized for SNMP Access**, select **Allow All IP Addresses** or specify an IP address. Select **UDP** for the **Transport Protocol** and the **Default Port Number of UDP:161** as shown below.

**AVAYA** Welcome, epadmin  
Last logged in today at 11:32:11 AM EDT

**Avaya Experience Portal 8.1.1 (ExperiencePortal)** Home ? Help Logoff

Expand All | Collapse All

- ▼ **User Management**
  - Roles
  - Users
  - Login Options
- ▼ **Real-time Monitoring**
  - System Monitor
  - Active Calls
  - Port Distribution
- ▼ **System Maintenance**
  - Audit Log Viewer
  - Trace Viewer
  - Log Viewer
  - Alarm Manager
- ▼ **System Management**
  - Application Server
  - EPM Manager
  - MPP Manager
  - Software Upgrade
  - System Backup
- ▼ **System Configuration**
  - Applications
  - EPM Servers
  - MPP Servers
  - SNMP
  - Speech Servers
  - VoIP Connections
  - Zones
- ▼ **Security**
  - Certificates
  - Licensing
- ▼ **Reports**
  - Standard
  - Custom
  - Scheduled
- ▼ **Multi-Media Configuration**
  - Email
  - HTML
  - SMS

You are here: [Home](#) > [System Configuration](#) > [SNMP](#) > **SNMP Agent Settings**

### SNMP Agent Settings

Use this page to configure the Simple Network Management Protocol (SNMP) agent in Experience Portal so that third-party network management software can query Experience Portal status.

**SNMP Version 1**

☒ Enable SNMP Version 1

Security Name:

**SNMP Version 2c**

☐ Enable SNMP Version 2c

Security Name:

**SNMP Version 3**

☐ Enable SNMP Version 3

Security Name:

Authentication Protocol:

Authentication Password:

Privacy Protocol:

Privacy Password:

**Authorized for SNMP Access**

☒ Allow All IP Addresses

☐ Allow Only the Following:

IP Address/Hostname 1:

IP Address/Hostname 2:

IP Address/Hostname 3:

IP Address/Hostname 4:

IP Address/Hostname 5:

**Transport Protocol**

Transport Protocol:

**Port Number**

☒ Default Port Number (UDP:161)

☐ Custom Port Number:

**Save Apply Cancel Help**

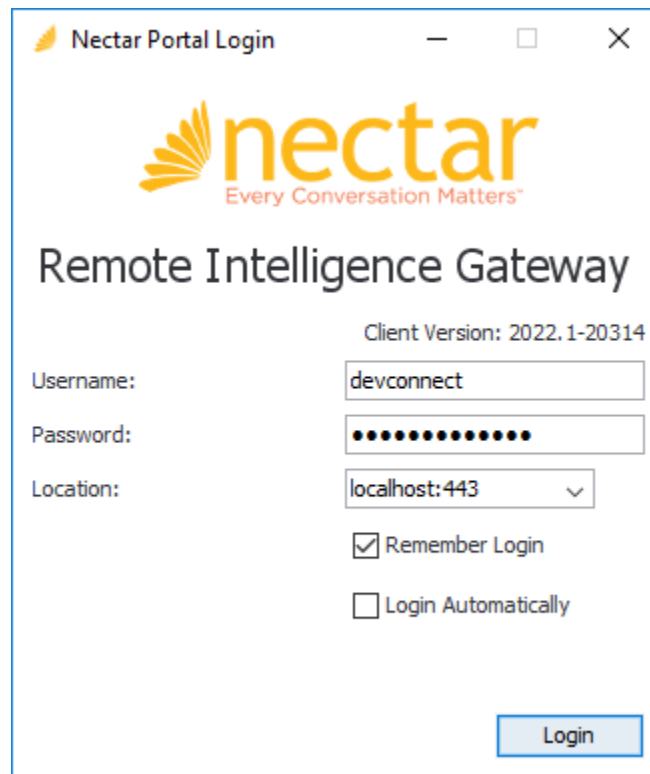
## 6. Configure Nectar for Avaya

This section covers the Nectar SNMP configuration for Experience Portal. The configuration was performed via the **RIG client**. The procedure covers the following areas:

- Launch the RIG Client
- Configure SNMP Polling Access
- Configure Interfaces
- 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**.

A screenshot of the Nectar Portal Login window. The window title is "Nectar Portal Login". It features the Nectar logo with the tagline "Every Conversation Matters™". Below the logo, it says "Remote Intelligence Gateway". The client version is "2022.1-20314". There are three input fields: "Username:" with the value "devconnect", "Password:" with masked characters, and "Location:" with the value "localhost:443" and a dropdown arrow. There are two checkboxes: "Remember Login" (checked) and "Login Automatically" (unchecked). A "Login" button is at the bottom right.

Nectar Portal Login

nectar  
Every Conversation Matters™

Remote Intelligence Gateway

Client Version: 2022.1-20314

Username: devconnect

Password: ●●●●●●●●●●

Location: localhost:443 ▼

☒ Remember Login

☐ Login Automatically

Login

## 6.2. Configure SNMP Polling Access

Navigate to **Modules** → **Avaya** → **Avaya Experience Portal** (not shown) and right-mouse click on the screen and select **Add** from the pop-up menu as shown below to add an entry for Experience Portal.

The screenshot shows the Nectar RIG interface. The top bar includes the Nectar logo and the text "Nectar RIG: localhost:443". Below this is a navigation bar with icons for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. A status bar shows "Primary: 2022.1-21422", "RTD: 3 ms", and "Users: 0". The main section is titled "Avaya Experience Portal:" and contains a "Management Servers" table. A right-click context menu is open over the table, showing options: Add..., Remove, Add to Selected Cluster, Remove Cluster, Enable, Disable, View, and Copy to Clipboard.

Ms Index	Cluster Index	Name	Description	Enable	Status	Ip	Role	Version
0	0	AEP				10.64.102.110	primary	8.1.1.0.0251

1 row

The **Add Management Server** dialog box is displayed as shown below. Configure the SNMP polling parameters, as described below, to match the settings in Experience Portal covered in **Section 5.3**.

- **Name:** Provide a descriptive name (e.g., *AEP*).
- **IP:** Provide the Experience Portal IP address (e.g., *10.64.102.110*).
- **SNMP Version:** Specify SNMPv1 for SNMP polling.
- **Port:** Specify port *161* for SNMP polling.
- **Community:** Specify the community name (e.g., *nectar*) as configured in Experience Portal in **Section 5.3**.

Click **Add** to submit the form.

The screenshot shows the 'Add Management Server' dialog box. The fields are filled as follows:

- Name:** AEP
- Description:** (empty)
- IP:** 10.64.102.110
- SNMP Version:** V1 (selected)
- Port:** 161
- Community:** nectar
- Authentication:** None (selected)
- User ID:** (empty)
- Password:** (empty)
- Privacy Protocol:** None
- Privacy Password:** (empty)

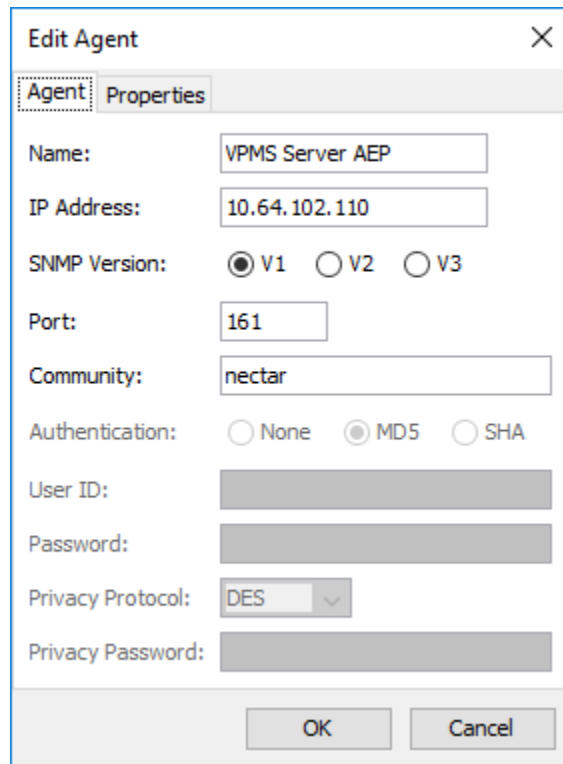
Buttons: Cancel, Add

Next, navigate to **Health** → **Elements** and then select **Agents** to display the window below. Right-mouse click on **VPMS Server AEP** and select **Edit** from the pop-up menu as shown below.

The screenshot shows the Nectar RIG interface at localhost:443. The top navigation bar includes links for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. Below this, a status bar shows 'Primary: 2022.1-21422', 'RTD: 3 ms', and 'Users: 0'. The main section is titled 'Elements:' and contains a sidebar with 'Folders' (Agents, Poll Functions, Element Registry) and a main area with tabs for 'All Agents', 'Poll Functions', 'Trap Groups', 'Interfaces', and 'VKM Collections'. The 'All Agents' tab is active, displaying a list of agents. A right-click context menu is open over the 'VPMS Server AEP' agent, showing 'Edit' and 'Remove' options.

Description	Function
Ping 10.64.102.110	ping
MPP Current State of MPP	AvayaVoicePortalM
MPP Active Calls on MPP	AvayaVoicePortalM
MPP CPU Usage of MPP	AvayaVoicePortalM
MPP Memory Usage of MPP	AvayaVoicePortalM
MPP Disk Usage of MPP	AvayaVoicePortalM
Web Server Check of 0:DevConnect Test Primary	CheckWebServer
Web Server Check of 0:REST Sample Primary	CheckWebServer
Web Server Check of 0:Test Application Primary	CheckWebServer
Web Server Check of 0:Test Application 2 Primary	CheckWebServer

Verify the **Edit Agent** configuration shown below matches the SNMP polling configuration shown above.



The 'Edit Agent' dialog box is shown with the 'Agent' tab selected. The configuration details are as follows:

Field	Value
Name:	VPMS Server AEP
IP Address:	10.64.102.110
SNMP Version:	<input checked="" type="radio"/> V1 <input type="radio"/> V2 <input type="radio"/> V3
Port:	161
Community:	nectar
Authentication:	<input type="radio"/> None <input checked="" type="radio"/> MD5 <input type="radio"/> SHA
User ID:	[Redacted]
Password:	[Redacted]
Privacy Protocol:	DES
Privacy Password:	[Redacted]

Buttons: OK, Cancel

## 6.3. Configure Interfaces

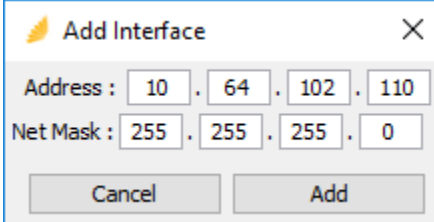
Nectar does not automatically discover the Experience Portal interface so it needs to be added. Navigate to **Health** → **Elements** and then select **Agents** (not shown) in the middle pane, and then select **Interfaces** in the right pane. Right-mouse click on the window and select **Add** from the pop-up menu as shown below.

The screenshot displays the Nectar RIG interface at localhost:443. The top navigation bar includes links for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. Below this, a status bar shows 'Primary: 2022.1-21422', 'RTD: 3 ms', and 'Users: 0'. The main content area is titled 'Elements:' and features a sidebar with 'Folders' (Agents, Poll Functions, Element Registry) and a central pane with tabs for 'All Agents', 'Poll Functions', 'Trap Groups', 'Interfaces', and 'VKM Collections'. The 'Interfaces' tab is active, showing a table with columns 'Ip' and 'Mask'. The table contains one row: '10.64.102.110' and '255.255.255.0'. To the right of the table is a context menu with options: 'Add...', 'Remove', 'Discover Interfaces', and 'Copy to Clipboard'. The 'Add...' button is highlighted in blue. The bottom of the interface shows a scroll bar and the text '1 row'.

Ip	Mask
10.64.102.110	255.255.255.0



In the **Add Interface** dialog box, enter the Experience Portal IP address (e.g., *10.64.102.110*) and click **Add**.

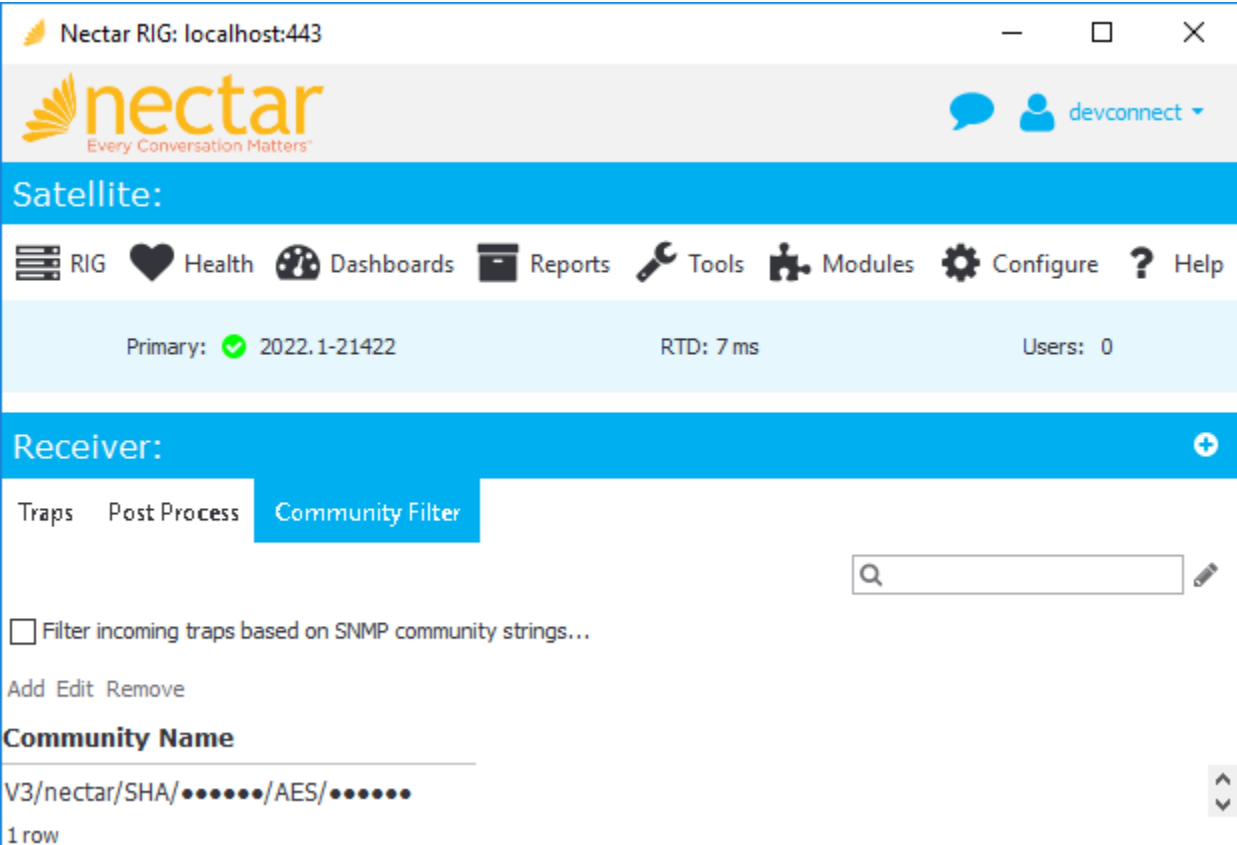
A dialog box titled "Add Interface" with a close button (X) in the top right corner. It contains two rows of input fields. The first row is labeled "Address :" and contains four input boxes with the values "10", "64", "102", and "110" separated by dots. The second row is labeled "Net Mask :" and contains four input boxes with the values "255", "255", "255", and "0" separated by dots. At the bottom, there are two buttons: "Cancel" and "Add".

## 6.4. Configure SNMP Traps

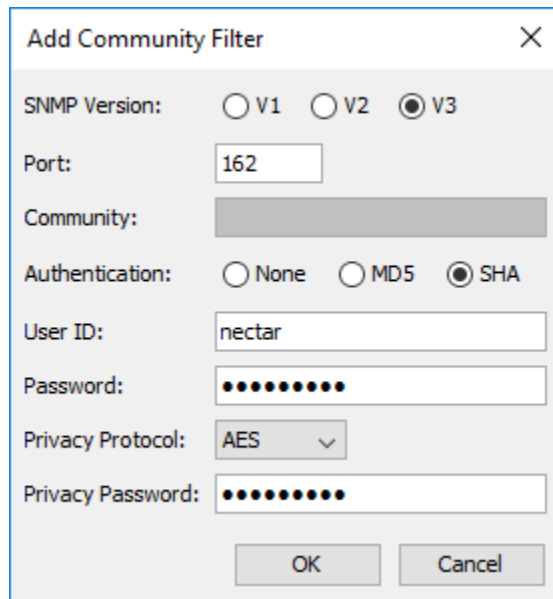
Navigate to **Configure** → **Receiver** and select the **Community Filter** tab. The Community Filter serves two purposes:

- 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**.

A screenshot of the Nectar RIG web interface. The top header shows the Nectar logo and the text "Nectar RIG: localhost:443". Below the header is a navigation bar with icons and labels for "RIG", "Health", "Dashboards", "Reports", "Tools", "Modules", "Configure", and "Help". A status bar below the navigation bar displays "Primary: 2022.1-21422", "RTD: 7 ms", and "Users: 0". The main content area is titled "Receiver:" and has a tabbed interface with "Traps", "Post Process", and "Community Filter" tabs. The "Community Filter" tab is active. It contains a search bar, a checkbox labeled "Filter incoming traps based on SNMP community strings...", and a table with the heading "Community Name". The table has one row with the value "V3/nectar/SHA/...../AES/.....".

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



The image shows a dialog box titled "Add Community Filter" with a close button (X) in the top right corner. The dialog contains the following fields and options:

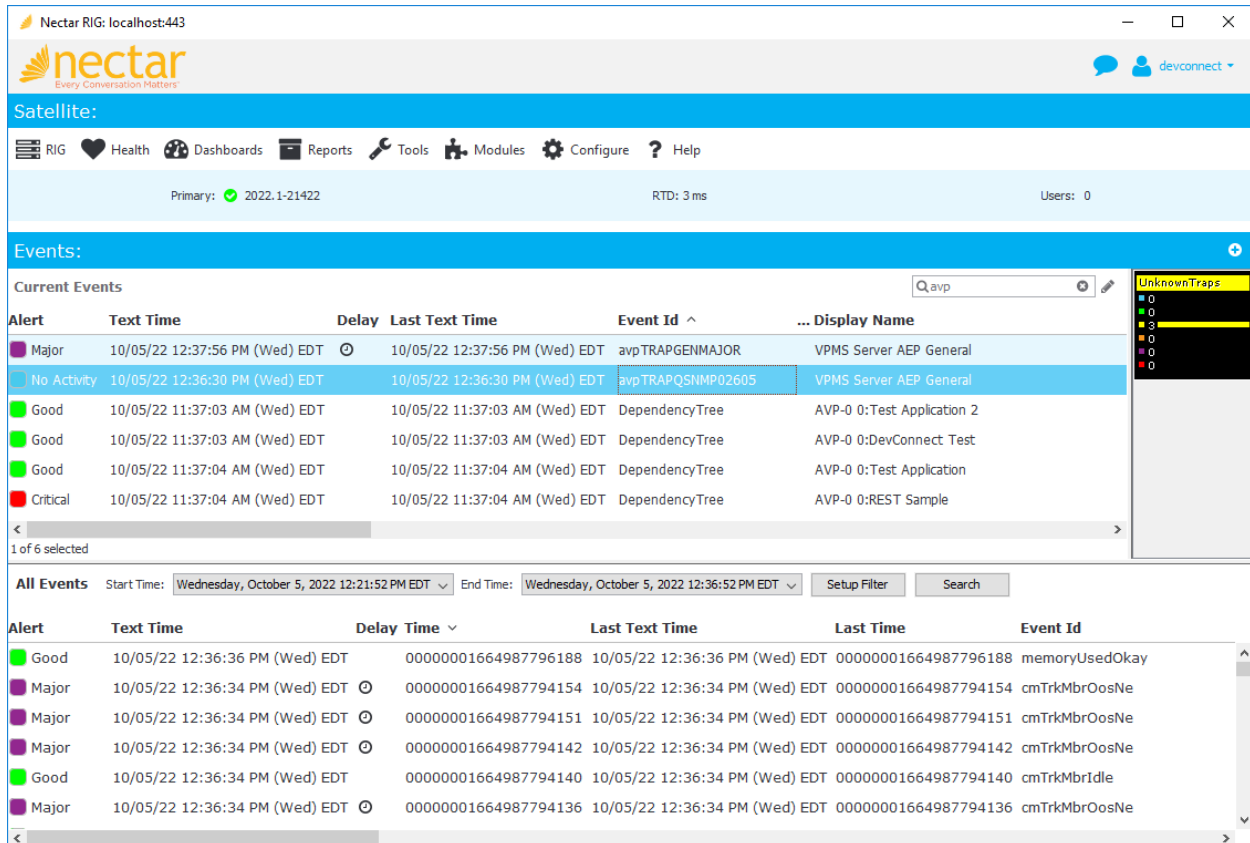
- SNMP Version:** Three radio buttons are present: ☐ V1, ☐ V2, and ☒ V3.
- Port:** A text input field containing the value "162".
- Community:** A text input field that is currently empty.
- Authentication:** Three radio buttons are present: ☐ None, ☐ MD5, and ☒ SHA.
- User ID:** A text input field containing the value "nectar".
- Password:** A text input field filled with ten black dots (••••••••••).
- Privacy Protocol:** A dropdown menu showing "AES" with a downward arrow.
- Privacy Password:** A text input field filled with ten black dots (••••••••••).

At the bottom of the dialog are two buttons: "OK" and "Cancel".

## 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Nectar with Experience Portal.

1. Generate alarm conditions on Experience Portal, such as an SNMP test alarm. Navigate to **Health → Events** to view SNMP traps and events as shown below.



Nectar RIG: localhost:443

nectar  
Every Conversation Matters

Satellite:

RIG Health Dashboards Reports Tools Modules Configure ? Help

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

Events:

Current Events

Alert Text Time Delay Last Text Time Event Id ... Display Name

Major	10/05/22 12:37:56 PM (Wed) EDT		10/05/22 12:37:56 PM (Wed) EDT	avpTRAPGENMAJOR	VPMS Server AEP General
No Activity	10/05/22 12:36:30 PM (Wed) EDT		10/05/22 12:36:30 PM (Wed) EDT	avpTRAPQSNMP02605	VPMS Server AEP General
Good	10/05/22 11:37:03 AM (Wed) EDT		10/05/22 11:37:03 AM (Wed) EDT	DependencyTree	AVP-0 0:Test Application 2
Good	10/05/22 11:37:03 AM (Wed) EDT		10/05/22 11:37:03 AM (Wed) EDT	DependencyTree	AVP-0 0:DevConnect Test
Good	10/05/22 11:37:04 AM (Wed) EDT		10/05/22 11:37:04 AM (Wed) EDT	DependencyTree	AVP-0 0:Test Application
Critical	10/05/22 11:37:04 AM (Wed) EDT		10/05/22 11:37:04 AM (Wed) EDT	DependencyTree	AVP-0 0:REST Sample

1 of 6 selected

All Events Start Time: Wednesday, October 5, 2022 12:21:52 PM EDT End Time: Wednesday, October 5, 2022 12:36:52 PM EDT Setup Filter Search

Alert	Text Time	Delay Time	Last Text Time	Last Time	Event Id
Good	10/05/22 12:36:36 PM (Wed) EDT	00000001664987796188	10/05/22 12:36:36 PM (Wed) EDT	00000001664987796188	memoryUsedOkay
Major	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794154	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794154	cmTrkMbrOosNe
Major	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794151	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794151	cmTrkMbrOosNe
Major	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794142	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794142	cmTrkMbrOosNe
Good	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794140	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794140	cmTrkMbrIdle
Major	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794136	10/05/22 12:36:34 PM (Wed) EDT	00000001664987794136	cmTrkMbrOosNe

2. Navigate to **Health → Agents** and then select *VPMS Server AEP* under **All Agents** to view the data collected using SNMP polling, including MPP operational state, active calls, and resource utilization as shown below.

The screenshot shows the Nectar RIG interface for localhost:443. The top navigation bar includes links for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. The main content area is titled 'Elements:' and contains a sidebar with 'All Agents' and 'Poll Functions' tabs. The 'All Agents' tab is selected, showing a list of agents. The 'VPMS Server AEP' agent is highlighted. The 'Poll Functions' tab is also selected, displaying a table of monitoring functions.

Description	Function	Sub Function	Enabled	Current Value
Ping 10.64.102.110	ping		true	1
MPP Current State of MPP	AvayaVoicePortalMPPCurrentState		true	5
MPP Active Calls on MPP	AvayaVoicePortalMPPActiveCalls		true	0
MPP CPU Usage of MPP	AvayaVoicePortalMPPCPUUsage		true	1
MPP Memory Usage of MPP	AvayaVoicePortalMPPMemoryUsage		true	3
MPP Disk Usage of MPP	AvayaVoicePortalMPPDiskUsage		true	12
Web Server Check of 0:DevConnect Test Primary	CheckWebServer		true	200
Web Server Check of 0:REST Sample Primary	CheckWebServer		true	404
Web Server Check of 0:Test Application Primary	CheckWebServer		true	200
Web Server Check of 0:Test Application 2 Primary	CheckWebServer		true	200

3. Navigate to **Modules** → **Avaya** → **Experience Portal** and select Experience Portal. Right-mouse click on Experience Portal and hover over **View** to display more options. Select **Applications** to view application URLs or MPPs to view MPPs managed by Experience Portal. The windows below show how to navigate to the MPP list.

Nectar RIG: localhost:443

nectar  
Every Conversation Matters

devconnect

Satellite:

RIG Health Dashboards Reports Tools Modules Configure Help

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

Avaya Experience Portal:

Management Servers

Ms Index	Cluster Index	Name	Description	Enable	Status	Ip	Role	Version
0	0	AEP		true		10.64.102.110	primary	8.1.1.0.0251

1 of 1 selected

Context Menu Options:

- Add...
- Remove
- Add to Selected Cluster
- Remove Cluster
- Enable
- Disable
- View
- Copy to Clipboard
- VKM Options
- Applications
- MPPs
- Display

Nectar RIG: localhost:443

nectar

Every Conversation Matters

devconnect

Satellite:

RIG

Health

Dashboards

Reports

Tools

Modules

Configure

Help

Primary: 2022.1-21422

RTD: 5 ms

Users: 0

Avaya Experience Portal: > Experience Portal MPPs on

Avaya Experience Portal:

Management Servers

Q

Ms Index	Cluster Index	Name	Description	Enable	Status	Ip	Role	Version
0	0	AEP		true		10.64.102.110	primary	8.1.1.0.0251

1 of 1 selected

Experience Portal MPPs on

Q

Mpp Index	Name	Ip	Enable	Version	Mpp Oid Index	Cluster Index
0	MPP	10.64.102.111	true	8.1.1.0.0251	1	0

1 row

## 8. Conclusion

These Application Notes described the configuration steps required to integrate Nectar for Avaya with Avaya Experience Portal 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 Experience Portal*, Release 8.1.2, October 2022, available at <http://support.avaya.com>.

---

**©2022 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](mailto:devconnect@avaya.com).