



Avaya Solution & Interoperability Test Lab

Application Notes for Empirix OneSight with Avaya Aura® Suite - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Empirix OneSight with the Avaya Aura® Suite using SNMP. The Avaya Aura® products included Avaya Aura® Communication Manager, Avaya G450 Media Gateway, Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. Empirix OneSight is a monitoring solution that receives SNMP traps, collects performance data via SNMP polls, and displays the data on the Empirix OneSight real-time dashboard.

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 Empirix OneSight with the Avaya Aura® Suite using SNMP. The Avaya Aura® products included Avaya Aura® Communication Manager, Avaya G450 Media Gateway, Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. Empirix OneSight is a monitoring solution that receives SNMP traps, collects performance data via SNMP polls, and displays the data on the Empirix OneSight real-time dashboard. The following table specifies the SNMP versions supported between Empirix OneSight and the Avaya Aura® Suite for SNMP traps and polls.

Avaya Product	Data Type	SNMP Version(s)
Avaya Aura® Communication Manager	SNMP Trap	SNMPv1, v2c, v3
	SNMP Poll	SNMPv1, v2c, v3
Avaya G450 Media Gateway	SNMP Trap	SNMPv1, v2c
	SNMP Poll	SNMPv1, v2c
Avaya Aura® System Manager	SNMP Trap	SNMPv2c, v3
	SNMP Poll	SNMPv3
Avaya Aura® Session Manager	SNMP Trap	SNMPv2c, v3
	SNMP Poll	SNMPv3
Avaya Aura® Application Enablement Services	SNMP Trap	SNMPv2c, v3
	SNMP Poll	SNMPv1, v2c, v3

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying that Empirix OneSight could receive SNMP traps and poll for performance data from Avaya Aura® Suite and display the data on the OneSight dashboard.

The serviceability testing focused on verifying that OneSight came back into service after re-connecting the Ethernet connect or rebooting the OneSight 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 features and functionality:

- SNMP traps sent from Avaya Aura® Suite, including Communication Manager, G450 Media Gateway, System Manager, Session Manager, and AES.
- OneSight periodically polling for performance data using SNMP from Avaya Aura® Suite.
- Avaya Aura® Suite responding to SNMP polls.
- OneSight receiving SNMP traps and performance data and displaying them on the dashboard.
- Proper system recovery after rebooting and reconnecting the Ethernet cable to the OneSight server.

Note: Refer to **Section 1** for the SNMP versions covered between Empirix OneSight and the Avaya Aura® Suite.

2.2. Test Results

All test cases passed with the following observation(s) noted:

- In order for Empirix OneSight to process SNMPv1 traps, logging and debugging must be enabled as shown in **Section 9.1.1**. This may impact performance on OneSight. For additional information contact Empirix. This is not required for SNMPv2c and v3 traps.
- When viewing SNMP poll data in the OneSight dashboard, the following messages are displayed for string and IP address data:
 - “SNMP STRING types are not currently supported for historical data.”
 - “SNMP IP-ADDRESS types are not currently supported for historical data.”

2.3. Support

For technical support on Empirix OneSight, contact Empirix Support via phone, email, or website.

- **Phone:** +1 (978) 313-7002
- **Web:** <http://www.empirix.com/contact>
- **Email:** support@empirix.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Empirix OneSight with the Avaya Aura® Suite, including Communication Manager, G450 Media Gateway, System Manager, Session Manager, and AES. There were two OneSight servers in the test configuration. The main OneSight server was used for system configuration, viewing SNMP data, receiving SNMP traps from all Avaya Aura® products, except AES, and polling for SNMP data from all Avaya Aura® products. The second OneSight server served as the data collector for AES SNMP traps and forwarded those traps to the main OneSight server. This was required because AES needed a different community string for SNMPv1 and v2c traps than the other Avaya Aura® products. OneSight used SNMP to collect alarms and performance data from the Avaya Aura® Suite. Refer to the table in **Section 1** for the SNMP versions support between OneSight and the Avaya Aura® Suite. All of the servers were deployed in a virtualized environment.

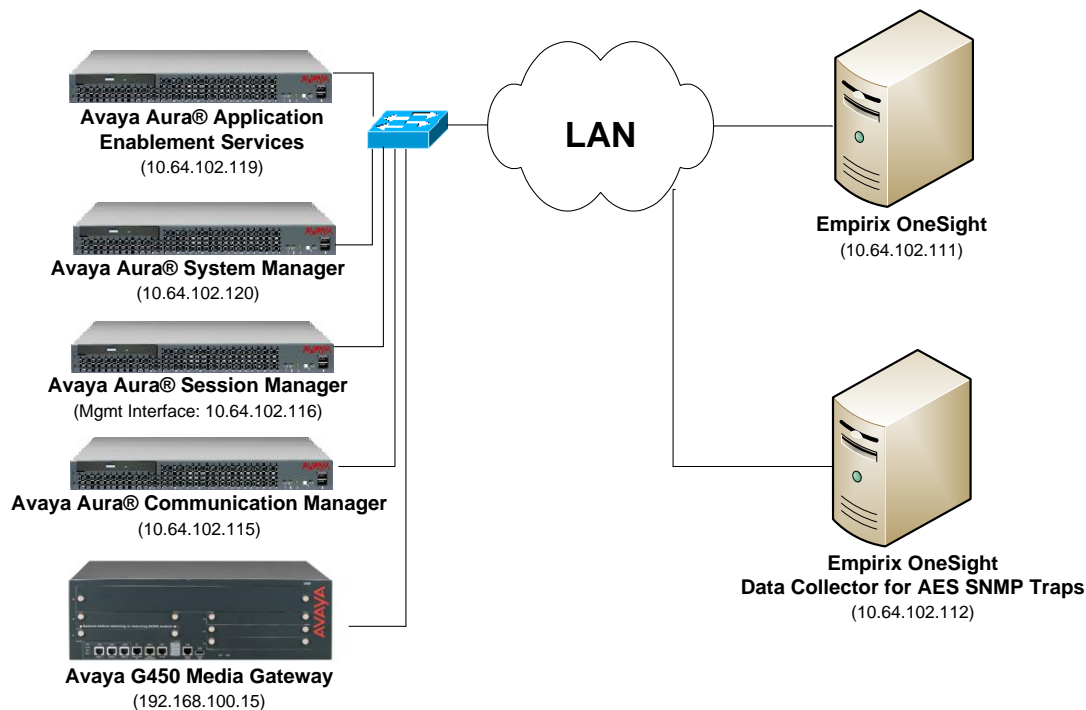


Figure 1: Empirix OneSight with Avaya Aura® Suite

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	7.1.1 FP1 (R017x.01.0.532.0 with Patch 23985)
Avaya G450 Media Gateway	38.20.1
Avaya Aura® System Manager	7.1.1.0 Build No. 7.1.0.0.1125193 Software Update Revision No. 7.1.1.0.046931 Feature Pack 1
Avaya Aura® Session Manager	7.1.1.0711008
Avaya Aura® Application Enablement Services	7.1 (7.1.0.0.0.17-0)
Empirix OneSight	9.6 SR0 (Build 76)

5. Configure Avaya Aura® Communication Manager

This section provides the procedure for configuring SNMP on Communication Manager. The procedure includes the following areas:

- Launch Maintenance Web Interface
- Administer SNMP Access
- Administer FP Traps
- Restart SNMP Agent

5.1. Launch Maintenance Web Interface

Access the Communication Manager web interface by using the URL <https://<ip-address>> in an Internet browser, where <ip-address> is the Communication Manager IP address. Log in using the appropriate credentials. In the subsequent webpage, select **Administration → Server (Maintenance)** from the top menu. The **Server Administration** webpage is displayed as shown in the following section.

5.2. Administer SNMP Access

To configure Communication Manager to respond to SNMP polls, navigate to **SNMP → Access**. The **Access** webpage is displayed as shown below. In the sample configuration below, SNMP polls using SNMPv1, v2c, and v3 are configured simultaneously for informational purposes. Note that only *one* SNMP version needs to be configured and only one SNMP version was tested at a time with OneSight.

For SNMPv1 or v2c, configure the following fields:

IP Address:	Set to the OneSight IP address (e.g., <i>10.64.102.111</i>).
Access:	Set to <i>read-only</i> .
Community Name:	Set to appropriate community string (e.g., <i>public</i>).

For SNMPv3, configure the following fields:

IP Address:	Set to the OneSight IP address (e.g., <i>10.64.102.111</i>).
User Name:	Specify a user name (e.g., <i>admincm</i>).
Authentication Protocol:	Set to <i>MD5</i> .
Authentication Password:	Set to a valid password to be used by OneSight.
Privacy Protocol:	Set to <i>DES</i> .
Privacy Password:	Set to a valid password to be used by OneSight.

Once completed, press the **Submit** button.

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

Help Log Off Administration

Administration / Server (Maintenance) This Server: devcon-cm

Access

The Access SMI page is used to configure SNMP access to CM.

Add SNMP Users / Communities

SNMP Version 1
 IP address: 10.64.102.111
 Access: read-only
 Community Name: public

SNMP Version 2c
 IP address: 10.64.102.111
 Access: read-only
 Community Name: public

SNMP Version 3
 Access: read-only
 User Name: admincm
 Authentication Protocol: MD5
 Authentication Password: admin123
 Minimum 8 characters. (for authentication and privacy)
 Privacy Protocol: DES
 Privacy Password: admin123
 Minimum 8 characters. (for privacy)

Submit Cancel Help

5.3. Administer FP Traps

To configure Communication Manager to send SNMP traps to OneSight, navigate to **SNMP → FP Traps**. The **FP Traps** webpage is displayed as shown below. In the sample configuration below, SNMP traps using SNMPv1, v2c, and v3 are configured simultaneously for informational purposes. Note that only *one* SNMP version needs to be configured and only one SNMP version was tested at a time with OneSight.

For SNMPv1 or v2c, configure the following fields:

IP Address: Set to the OneSight IP address (e.g., 10.64.102.111).
Port: Use the default port 162 for SNMP traps.
Notification: Set to *trap*.
Community Name: Set to appropriate community string (e.g., *public*).

For SNMPv3, configure the following fields:

IP Address: Set to the OneSight IP address (e.g., 10.64.102.111).
User Name: Specify a user name (e.g., *admincm*).
Authentication Protocol: Set to *MD5*.
Authentication Password: Set to a valid password to be used by OneSight.

Privacy Protocol: Set to *DES*.
Privacy Password: Set to a valid password to be used by OneSight.

Once completed, press the **Submit** button.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', and 'Administration'. Below this, a red banner reads 'Administration / Server (Maintenance)' and 'This Server: devcon-cm'. A left-hand menu lists various system management options, with 'FP Traps' selected under the 'Alarms' section. The main content area is titled 'FP Traps' and contains the text: 'The FP Traps page allows specification of the alarms to be sent as traps.' Below this, there is a section titled 'Add Trap Destination' which contains three configuration blocks for SNMP versions 1, 2c, and 3. Each block includes fields for IP address, Notification, Community Name, and Port. The SNMP Version 3 block also includes fields for User Name, Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password. The bottom of the page features a copyright notice: '© 2001-2017 Avaya Inc. All Rights Reserved.'

SNMP Version	IP address	Notification	Community Name	Port
SNMP Version 1	10.64.102.111	trap	public	162
SNMP Version 2c	10.64.102.111	trap	public	162
SNMP Version 3	10.64.102.111	trap	public	162

Additional fields for SNMP Version 3:

- User Name: admin
- Authentication Protocol: MD5
- Authentication Password: admin123 (Minimum 8 characters)
- Privacy Protocol: DES
- Privacy Password: admin123 (Minimum 8 characters)
- Engine ID: [local Engine ID]

5.4. Restart SNMP Agent

Select **SNMP** → **Agent Status** from the left pane to display the **Agent Status** webpage and restart the SNMP agent. Click the **Stop Master Agent** button followed by the **Start Master Agent** button.



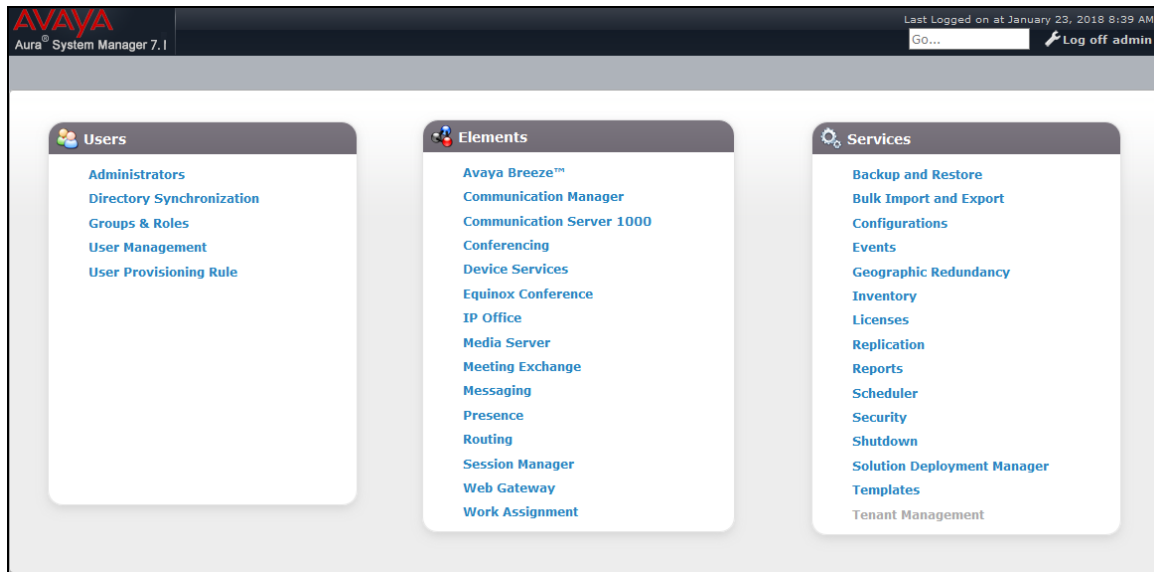
6. Configure Avaya G450 Media Gateway

This section covers the configuration of the G450 Media Gateway to enable SNMPv1 or v2c. Log into the G450 Media Gateway command line interface with the appropriate credentials using SSH (not shown). At the command prompt, enter the command shown below. In the **snmp-server host** command specify the OneSight IP address, specify **v1** or **v2c** in the command depending on the SNMP version desired, and **public** as the community name. The **show snmp** command may be used to view the SNMP configuration.

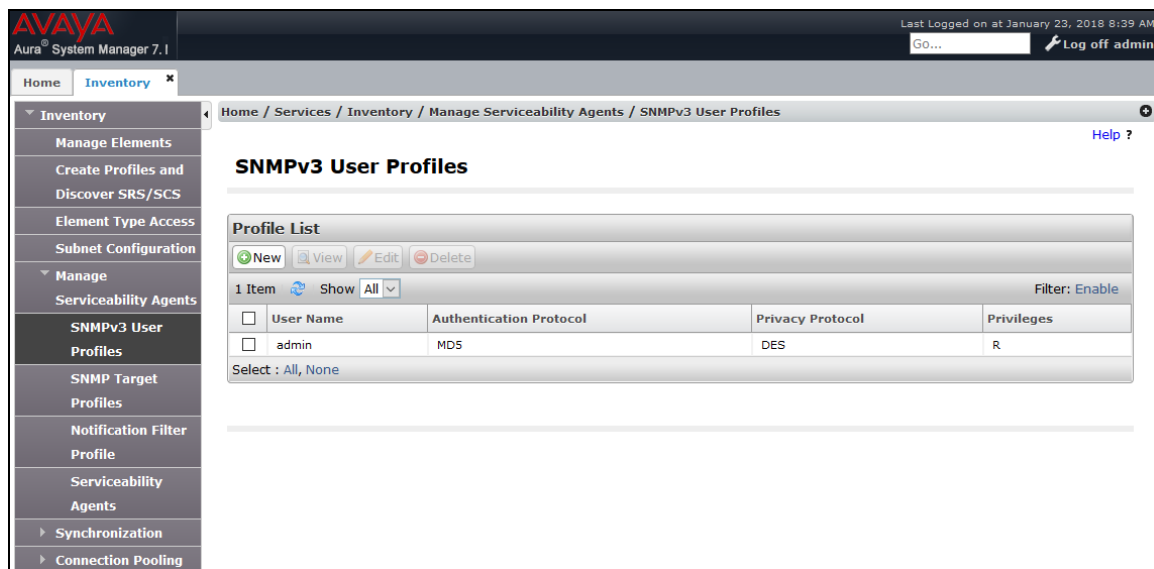
```
snmp-server host 10.64.102.111 traps v2c public
```

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

This section provides the procedure for enabling SNMP traps and 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**.



Configure the **User Details** for SNMPv3 polls for System Manager and Session Manager.

AVAYA
Aura® System Manager 7.1

Last Logged on at February 2, 2018 2:28 PM
GO... Log off admin

Home / Services / Inventory / Manage Serviceability Agents / SNMPv3 User Profiles

New User Profile

Commit Back

User Details

* User Name: admin

* Authentication Protocol: SHA

* Authentication Password:

* Confirm Authentication Password:

* Privacy Protocol: DES

* Privacy Password:

* Confirm Privacy Password:

* Privileges: None

* Required

Commit Back

Next, under **Manage Serviceability Agents** in the left pane, select **SNMP Target Profiles**. Click **New** to provide the configuration details for SNMP traps. In the **Target Details** tab, configure the following fields:

Name: Provide a name (e.g., *admin*).

IP Address: Set to the OneSight IP address (e.g., *10.64.102.111*).

Port: Specify port *162* for SNMP traps.

Notification Type: Set to *Trap*.

Protocol: Set to *v2c* or *v3*.

AVAYA
Aura® System Manager 7.1

Last Logged on at January 23, 2018 8:39 AM
GO... Log off admin

Home / Services / Inventory / Manage Serviceability Agents / SNMP Target Profiles

New Target Profile

Commit Back

Target Details * Attach/Detach User Profile

Target Details

* Name: admin

Description:

* IP Address: 10.64.102.111

* Port: 162

* Notification Type: Trap

* Protocol: V3

* Required

Commit Back

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

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar has a tree view with 'Inventory' expanded, and 'Serviceability Agents' selected. The main content area is titled 'Serviceability Agents' and shows a table of agents. The table has columns: Hostname, IP Address, System Name, System OID, and Status. Two agents are listed, both with checkboxes selected.

	Hostname	IP Address	System Name	System OID	Status
<input checked="" type="checkbox"/>	devcon-sm.avaya.com	10.64.102.116	devcon-sm.avaya.com		active
<input checked="" type="checkbox"/>	devcon-smgr.avaya.com	10.64.102.120	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	active

In the **Manage Profile** webpage, navigate to the **SNMP Target Profiles** tab and select the entry in the **Assignable Profiles** section. Click **Assign** to push the SNMP details to System Manager and Session Manager.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar has a tree view with 'Inventory' expanded, and 'Serviceability Agents' selected. The main content area is titled 'Manage Profile' and shows the 'SNMP Target Profiles' tab. The table 'Assignable Profiles' has one item selected.

	Name	Domain Type	IP Address	Port	SNMP Version
<input checked="" type="checkbox"/>	admin	UDP	10.64.102.111	162	V3

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.

Avaya Aura System Manager 7.1

Last Logged on at January 23, 2018 8:39 AM

Home / Services / Inventory / Manage Serviceability Agents / Serviceability Agents

Manage Profile [Commit] [Back]

Selected Agents | SNMP Target Profiles | **SNMPv3 User Profiles**

Assignable Profiles

Assign

1 Item

<input checked="" type="checkbox"/>	User Name	Authentication Protocol	Privacy Protocol	Privileges
<input checked="" type="checkbox"/>	admin	MD5	DES	R

Select : All, None

Removable Profiles

[Commit] [Back]

8. Configure Avaya Aura® Application Enablement Services

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

Navigate to **Utilities** → **SNMP** → **SNMP Agent** to enable SNMP polls. In the sample configuration below, SNMP polls using SNMPv1, v2c, and v3 are configured simultaneously for informational purposes. Note that only *one* SNMP version needs to be configured and only one SNMP version was tested at a time with OneSight. Click **Apply Changes**.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Jan 23 11:12:54 2018 from 192.168.100.226
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.0.0.17-0
Server Date and Time: Fri Jan 26 15:13:25 EST 2018
HA Status: Not Configured

Utilities | SNMP | SNMP AgentHome | 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

SNMP Agent

MIB II System Group Data:
Location: Unknown
Contact: Unknown

SNMP Protocol Access:
☒ Enable SNMP Version 1
Community Name: empirix
☒ Enable SNMP Version 2c
Community Name: empirix
☒ Enable SNMP Version 3
User
User Name: admin
Authentication Protocol: MD5
Authentication Password:
Privacy Protocol: DES
Privacy Password:
Authorized IP Addresses for SNMP Access*
☐ No Access
☒ Any IP Addresses
☐ Following IP Addresses
IP Address 1: 10.64.102.111
IP Address 2:
IP Address 3:
IP Address 4:
IP Address 5:

Apply Changes Cancel Changes

Next, navigate to **Utilities → SNMP → SNMP Trap Receivers** to enable SNMP traps. In the sample configuration below, SNMP v3 was configured. To use SNMPv2c, set the **SNMP Version** field to *v2c* and set the **Security Name** (i.e., community name) to a valid value. When testing SNMPv2c, the **Security Name** was set to *empirix* as seen in **Section 9.3.2**. The **Authentication Protocol** and **Privacy Protocol** fields do not apply when using SNMPv2c. Click **Apply Changes**.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Jan 23 11:12:54 2018 from 192.168.100.226
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.0.0.17-0
Server Date and Time: Fri Jan 26 15:15:15 EST 2018
HA Status: Not Configured

Utilities | SNMP | SNMP Trap ReceiversHome | 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

Edit SNMP Trap

☒ Enabled

Device: NMS

IP Address: 10.64.102.112

Port: 162

Notification Type: Trap

SNMP Version: 3

Security Name: admin

Authentication Protocol: MD5

Authentication Password: Confirm Password:

Privacy Protocol: DES

Authentication Password: Confirm Password:

Apply Changes Cancel Changes

9. Configure Empirix OneSight

This section provides the procedures for configuring OneSight. The procedures fall into the following areas:

- Modify `OSDC.properties` Files
- Launch OneSight Web Interface
- Configure SNMP Traps
- Configure SNMP Polls

Note: The Appendix provides a high-level overview for configuring SNMP metrics and monitor groups in OneSight. This is outside the scope of these Application Notes, but a brief description is provided for informational purpose. Refer to [7] for more details.

9.1. Modify `OSDC.properties` Files

There are six (6) `OSDC.properties` files that must be configured on the OneSight Server (10.64.102.111) for:

1. SNMP Traps for Communication Manager, System Manager, and Session Manager
2. SNMP Polls for Communication Manager
3. SNMP Polls for G450 Media Gateway
4. SNMP Polls for System Manager
5. SNMP Polls for Session Manager
6. SNMP Polls for AES

There is also one other `OSDC.properties` file that must be configured on the OneSight Data Collector Server (10.64.102.112) for AES SNMP traps. A separate OneSight data collector was required for AES because it uses a different community name than the other Avaya Aura® products.

9.1.1. Configure OSDC.properties File for SNMP Traps from Communication Manager, System Manager, and Session Manager

The `OSDC.properties` file used for SNMP traps from Communication Manager, System Manager, and Session Manager was stored in the

C:\Empirix\DataCollector\properties directory. This file was located in the OneSight server with IP address 10.64.102.111. The following sections provide the relevant configuration for these Application Notes.

In this file, the **Location** parameter was not set since the default location is used. The **Comm.ServerName** specifies the IP address of the OneSight server (e.g., *10.64.102.111*) that serves as the data collector for SNMP traps for all Avaya Aura® products, except AES. In the **SNMP.Agents** section, SNMP polls are disabled in this file since this file is used to configure SNMPv3 traps only. SNMPv1 and v2c traps are configured on OneSight via the web interface as shown in **Section 9.3.1**. In the **Agents.SNMPTrap** section, SNMP traps are enabled. In addition, this file specifies that SNMPv3 is enabled and the SNMPv3 credentials for Communication Manager (10.64.102.115), Session Manager (10.64.102.116), and System Manager (10.64.102.120).

Note: SNMP logging and debugging were enabled. This is required for SNMPv1 traps; otherwise, SNMP traps would not be processed by OneSight.

```
# -----  
# Location  
# -----  
# Defaults to: <unspecified>  
#  
# The location name is used to designate a group of one or more Data Collectors. It  
# is a user friendly name used during configuration of Empirix Onesight. Monitors  
# assigned to a location are load balanced across all data collectors with that  
# location name.  
#  
# For VQ Probe, DO NOT MAKE CHANGE HERE - CHANGE ONLY VIA THE USER INTERFACE.  
#  
# Location = NOT_SET  
  
ooo  
  
#####  
#[Comm]  
#  
# Communication Options  
#  
# These options determine how the agent framework communicates  
# with the OneSight server.  
#  
#####  
  
# -----  
# Comm.ServerName  
# Comm.ServerPort  
# Comm.ConnectFrom  
# -----
```

```

# Defaults to: localhost
#
# Comm.Server specifies the name or IP address of Empirix Onesight server (required),
# the IP port on which the server is listening (optional), and the local IP address to
# be used for the outbound connection (optional).
#
# Port 5007 is the default server listen port. This value does not have to be
# specified unless the Empirix Onesight server configuration has been changed to a
# different port.
#
# If this machine has multiple IP addresses, you can control which IP address is used
# for the outbound connection to the Empirix Onesight server using the ConnectFrom
# property.
#
#
Comm.ServerName = 10.64.102.111

                                000

#####
#[Agents.SNMP]
#####
Agents.SNMP.Java.Library = com.wrq.wam.agents.SnmpMonitor.SnmpMonitor
Agents.SNMP.Status = disabled
Agents.SNMP.DebugMode = false
Agents.SNMP.LogDetail = false
#Agents.SNMP.MaxThreads = 50
#Agents.SNMP.SiblingLifetime = 180
#Agents.SNMP.TableCacheTimeout = 60
#Agents.SNMP.SecondaryTimeout = 60

#####
#[Agents.SNMPTrap]
#####
Agents.SNMPTrap.Java.Library = com.wrq.wam.agents.SnmpTrapMonitor.SnmpTrapMonitor
Agents.SNMPTrap.Status = enabled
Agents.SNMPTrap.DebugMode = true
Agents.SNMPTrap.LogDetail = true

# Agent Threadcount settings.
Agents.SNMPTrap.MaxThreadCount = 50
Agents.SNMPTrap.MaxTasksPerThread = 500

Agents.SNMPTrap.V3Enabled = true

Agents.SNMPTrap.V3EnabledDevices = 3

Agents.SNMPTrap.UserName.1 = admin
Agents.SNMPTrap.Password.1 = admin123
Agents.SNMPTrap.Protocol.1 = MD5
Agents.SNMPTrap.PrivPassword.1 = admin123
Agents.SNMPTrap.PrivProtocol.1 = DES
Agents.SNMPTrap.DeviceIP.1 = 10.64.102.115

Agents.SNMPTrap.UserName.2 = admin
Agents.SNMPTrap.Password.2 = admin123
Agents.SNMPTrap.Protocol.2 = MD5
Agents.SNMPTrap.PrivPassword.2 = admin123
Agents.SNMPTrap.PrivProtocol.2 = DES
Agents.SNMPTrap.DeviceIP.2 = 10.64.102.116

```

```
Agents.SNMPTrap.UserName.3 = admin
Agents.SNMPTrap.Password.3 = admin123
Agents.SNMPTrap.Protocol.3 = MD5
Agents.SNMPTrap.PrivPassword.3 = admin123
Agents.SNMPTrap.PrivProtocol.3 = DES
Agents.SNMPTrap.DeviceIP.3 = 10.64.102.120
```

9.1.2. Configure OSDC.properties File for SNMP Polls to Communication Manager

The OSDC.properties file used for Communication Manager SNMP polls was stored in the C:\Empirix\DataCollector (2)\properties directory. This file was located in the OneSight server with IP address 10.64.102.111. The following sections provide the relevant configuration for these Application Notes. Additional SNMP poll configuration is required as shown in **Section 9.4**.

```
Comm.ServerName = 10.64.102.111

                                ooo

Location = CM_SNMP_POLL

                                ooo

#####
#[Agents.SNMP]
#####
Agents.SNMP.Java.Library = com.wrq.wam.agents.SnmpMonitor.SnmpMonitor
Agents.SNMP.Status = enabled
Agents.SNMP.DebugMode = false
Agents.SNMP.LogDetail = false

#####
#[Agents.SNMPTrap]
#####
Agents.SNMPTrap.Java.Library = com.wrq.wam.agents.SnmpTrapMonitor.SnmpTrapMonitor
Agents.SNMPTrap.Status = disabled
Agents.SNMPTrap.DebugMode = false
Agents.SNMPTrap.LogDetail = false

# Agent Threadcount settings.
Agents.SNMPTrap.MaxThreadCount = 10
Agents.SNMPTrap.MaxTasksPerThread = 100

Agents.SNMPTrap.V3Enabled = false
```

9.1.3. Configure OSDC.properties File for SNMP Polls to G450 Media Gateway

The OSDC.properties file used for G450 Media Gateway SNMP polls was stored in the C:\Empirix\DataCollector (3)\properties directory. This file was located in the OneSight server with IP address 10.64.102.111. The file was configured similarly to the one shown in Section 9.1.2, except that the **Location** parameter was set to *MG_SNMP_POLL*. Additional SNMP poll configuration is required as shown in **Section 9.4**.

9.1.4. Configure OSDC.properties File for SNMP Polls to System Manager

The OSDC.properties file used for System Manager SNMP polls was stored in the C:\Empirix\DataCollector (4)\properties directory. This file was located in the OneSight server with IP address 10.64.102.111. The file was configured similarly to the one shown in Section 9.1.2, except that the **Location** parameter was set to *SYSMGR_SNMP_POLL*. Additional SNMP poll configuration is required as shown in **Section 9.4**.

9.1.5. Configure OSDC.properties File for SNMP Polls to Session Manager

The OSDC.properties file used for Session Manager SNMP polls was stored in the C:\Empirix\DataCollector (5)\properties directory. This file was located in the OneSight server with IP address 10.64.102.111. The file was configured similarly to the one shown in **Section 9.1.2**, except that the **Location** parameter was set to *SESSION_SNMP_POLL*. Additional SNMP poll configuration is required as shown in **Section 9.4**.

9.1.6. Configure OSDC.properties File for SNMP Polls to AES

The OSDC.properties file used for AES SNMP polls was stored in the C:\Empirix\DataCollector (6)\properties directory. This file was located in the OneSight server with IP address 10.64.102.111. The file was configured similarly to the one shown in Section 9.1.2, except that the **Location** parameter was set to *AES_SNMP_POLL*. Additional SNMP poll configuration is required as shown in **Section 9.4**.

9.1.7. Configure OSDC.properties File for SNMP Traps from AES

The OSDC.properties file used for AES SNMP traps was stored in the C:\Empirix\DataCollector (6)\properties directory. This file was located in the OneSight AES data collector server with IP address 10.64.102.112. The following sections provide the relevant configuration for these Application Notes. Note that AES SNMP traps were forwarded to the OneSight server with IP address 10.64.102.111. Additional SNMP poll configuration is required as shown in **Section 9.4**.

```
Comm.ServerName = 10.64.102.111

                                ooo

Location = DC_AES_TRAPS

                                ooo

#####
#[Agents.SNMP]
#####
Agents.SNMP.Java.Library = com.wrq.wam.agents.SnmpMonitor.SnmpMonitor
Agents.SNMP.Status = enabled
Agents.SNMP.DebugMode = false
Agents.SNMP.LogDetail = false

#####
#[Agents.SNMPTrap]
#####
Agents.SNMPTrap.Java.Library = com.wrq.wam.agents.SnmpTrapMonitor.SnmpTrapMonitor
Agents.SNMPTrap.Status = enabled
Agents.SNMPTrap.DebugMode = false
Agents.SNMPTrap.LogDetail = false

# Agent Threadcount settings.
Agents.SNMPTrap.MaxThreadCount = 10
Agents.SNMPTrap.MaxTasksPerThread = 100

Agents.SNMPTrap.V3Enabled = true

Agents.SNMPTrap.V3EnabledDevices = 1
#Below property number should be equal to the V3EnabledDevices number

Agents.SNMPTrap.UserName.1 = admin
Agents.SNMPTrap.Password.1 = admin123
Agents.SNMPTrap.Protocol.1 = MD5
Agents.SNMPTrap.PrivPassword.1 = admin123
Agents.SNMPTrap.PrivProtocol.1 = DES
Agents.SNMPTrap.DeviceIP.1 = 10.64.102.119

Agents.SNMPTrap.V3Enabled = false
```

9.1.8. Restart OneSight Service

After modifying the OSDC.properties files, restart the **OneSight** service under Windows Services.

9.2. Launch OneSight Web Interface

From a web browser, enter the URL <http://<hostname>:8080>, where <hostname> is the OneSight hostname or IP address. Log in with the appropriate credentials.



In the subsequent webpage, click **Configure** to display the **Configuration Quick Links** in the left pane as shown below.



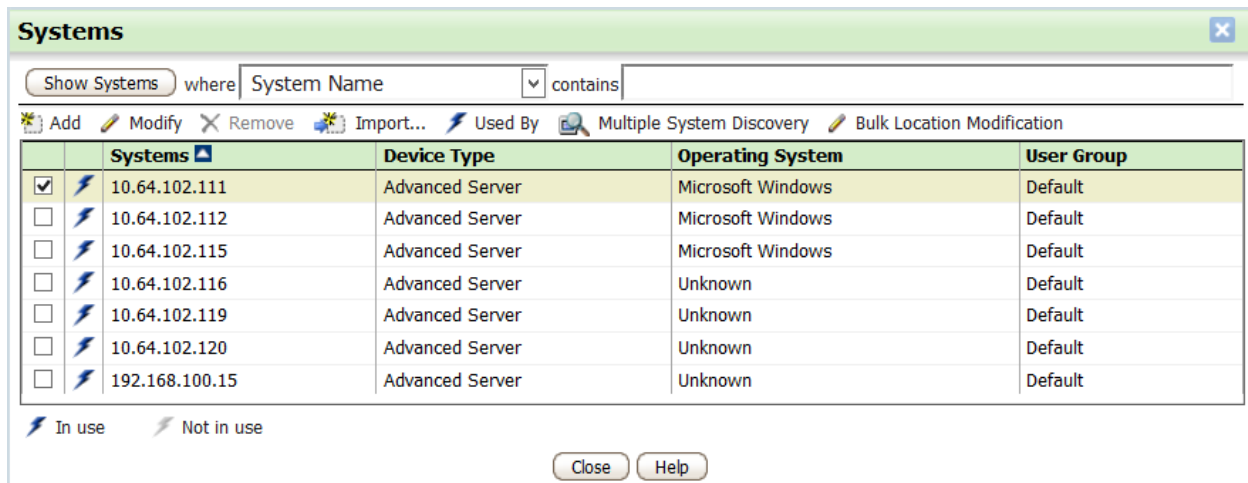
9.3. Configure SNMP Traps

This section covers the procedures for configuring SNMP traps for Avaya Aura® Suite. The configuration for AES SNMP traps has been separated into its own section since it differs from the configuration for all the other Avaya Aura® products.

9.3.1. Configure SNMP Traps for Communication Manager, G450 Media Gateway, System Manager, and Session Manager

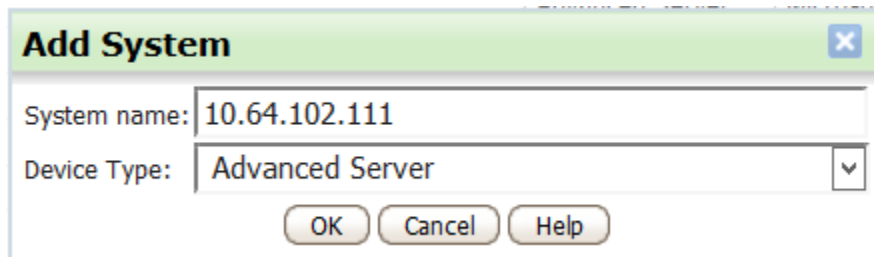
This section configures the OneSight data collector for SNMP traps from Communication Manager, G450 Media Gateway, System Manager, and Session Manager.

From the OneSight web interface, select **Systems** under **Configuration Quick Links** in the left pane. The **Systems** screen is displayed as shown below. Click **Add**.



	Systems	Device Type	Operating System	User Group
<input checked="" type="checkbox"/>	10.64.102.111	Advanced Server	Microsoft Windows	Default
<input type="checkbox"/>	10.64.102.112	Advanced Server	Microsoft Windows	Default
<input type="checkbox"/>	10.64.102.115	Advanced Server	Microsoft Windows	Default
<input type="checkbox"/>	10.64.102.116	Advanced Server	Unknown	Default
<input type="checkbox"/>	10.64.102.119	Advanced Server	Unknown	Default
<input type="checkbox"/>	10.64.102.120	Advanced Server	Unknown	Default
<input type="checkbox"/>	192.168.100.15	Advanced Server	Unknown	Default

In the **Add System** dialog box, enter a descriptive name for the **System name**. In this example, the OneSight IP address was used. Click **OK**.



Add System

System name: 10.64.102.111

Device Type: Advanced Server

OK Cancel Help

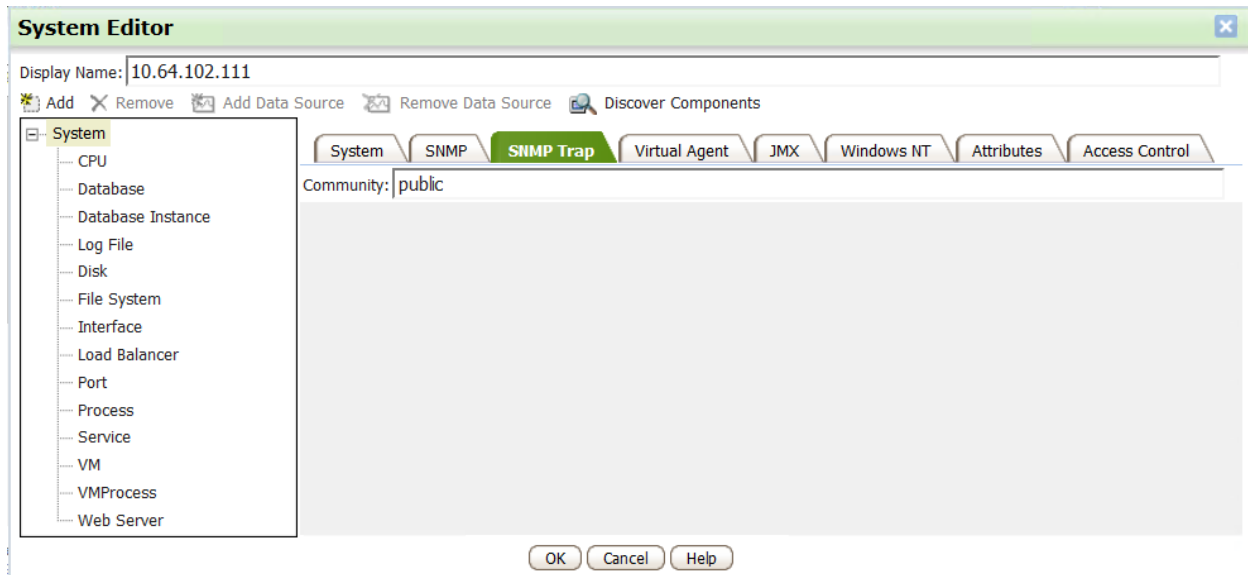
In the **System Editor** window, enter the OneSight IP address in the **DNS Name**, **IP Address**, **Alias**, **NetBIOS Name** fields. Set the **Location** field to *<Default Location>*. This uses the `OSDC.properties` file configured in **Section 9.1.1**, where the **Location** parameter was not set indicating the default location as configured here.

The screenshot shows the **System Editor** window. At the top, the **Display Name** is set to `10.64.102.111`. Below this is a toolbar with icons for **Add**, **Remove**, **Add Data Source**, **Remove Data Source**, and **Discover Components**. On the left is a tree view showing a hierarchy of system components: **System** (selected), **CPU**, **Database**, **Database Instance**, **Log File**, **Disk**, **File System**, **Interface**, **Load Balancer**, **Port**, **Process**, **Service**, **VM**, **VMProcess**, and **Web Server**. The main area on the right has several tabs: **System** (active), **SNMP**, **SNMP Trap**, **Virtual Agent**, **JMX**, **Windows NT**, **Attributes**, and **Access Control**. The **System** tab contains the following fields: **Device Type** (Advanced Server), **DNS Name** (10.64.102.111), **IP address** (10.64.102.111), **Alias** (10.64.102.111), **NetBIOS Name** (10.64.102.111), **Operating System** (Microsoft Windows), **Location** (<Default Location>), **On Failure** (Include Traceroute in alert), **When in Warning State Respond by** (<doing nothing>), **When in Critical State Respond by** (<doing nothing>), and **When returning to Good State Respond by** (<doing nothing>). At the bottom, there is a note: "Use additional Properties tabs to configure access to the data sources that OneSight metrics use to monitor this system." and buttons for **OK**, **Cancel**, and **Help**.

Skip the configuration of the **SNMP** tab, because **SNMP** polls use a different **Location** and the `OSDC.properties` files specified in **Sections 9.1.2** to **9.1.6**. The **SNMP** tab is not used in here.

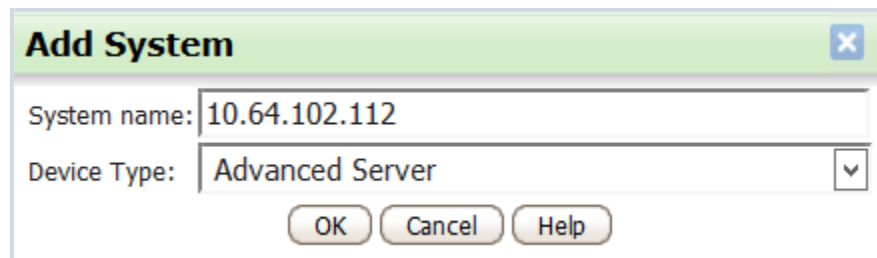
Select the **SNMP Trap** tab and set the **Community** field to *public*. The **Community** field should match the community string configured in Avaya Aura®, except for AES, which has a different community name. AES SNMP trap configuration is described in **Section 9.3.2**. Click **OK**.

Note: For SNMPv1, refer to the observation in **Section 2.2**.



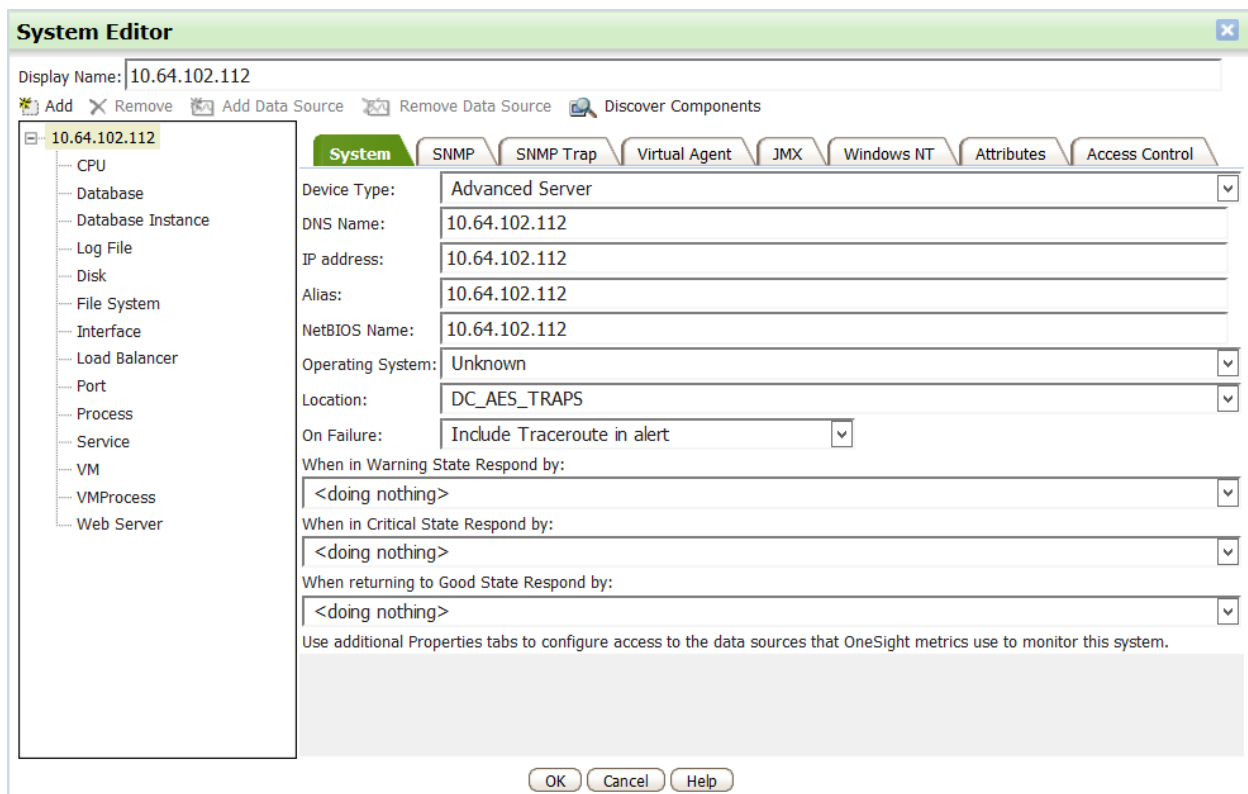
9.3.2. Configure SNMP Traps for AES

From the **Systems** screen, click **Add**. In the **Add System** dialog box, enter a descriptive name for the **System name**. In this example, the OneSight AES data collector IP address was used. Click **OK**.



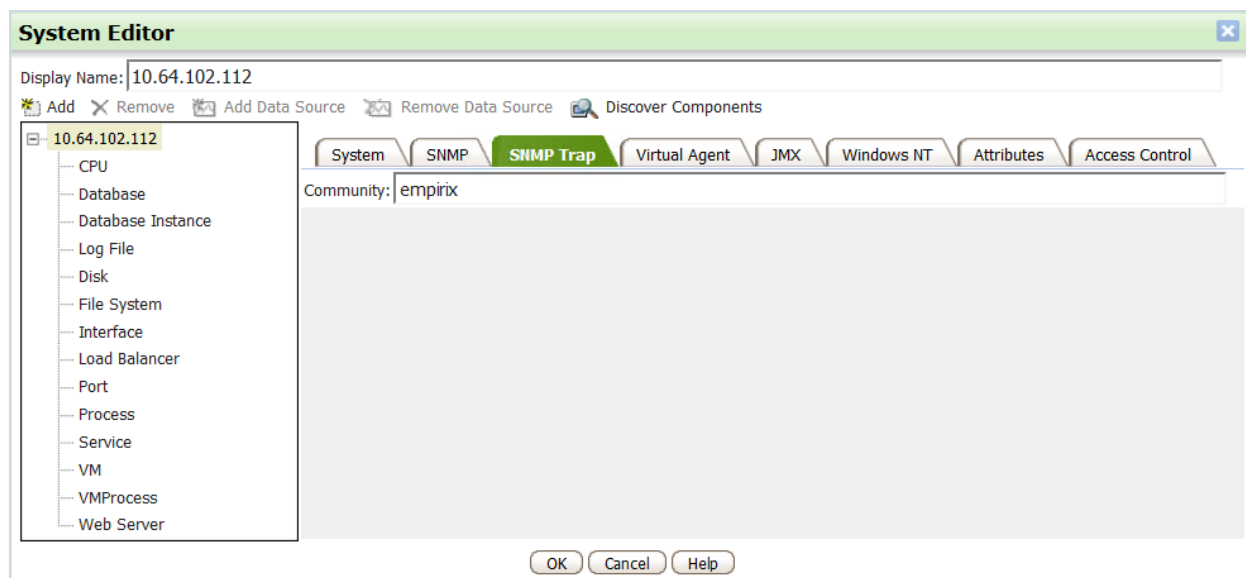
The **Add System** dialog box is shown. It has a title bar with a close button. The **System name** field contains the text "10.64.102.112". The **Device Type** dropdown menu is set to "Advanced Server". At the bottom are three buttons: **OK**, **Cancel**, and **Help**.

In the **System Editor** window, enter the OneSight AES data collector IP address in the **DNS Name**, **IP Address**, **Alias**, **NetBIOS Name** fields. Set the **Location** field to **DC_AES_TRAPS**. This uses the `OSDC.properties` file configured in **Section 9.1.1**, where the **Location** parameter was set to the same value.



The **System Editor** window is shown. The **Display Name** field at the top contains "10.64.102.112". Below it are buttons for **Add**, **Remove**, **Add Data Source**, **Remove Data Source**, and **Discover Components**. On the left is a tree view showing a hierarchy of system components, with "10.64.102.112" selected. The main area has tabs for **System**, **SNMP**, **SNMP Trap**, **Virtual Agent**, **JMX**, **Windows NT**, **Attributes**, and **Access Control**. The **System** tab is active, showing fields for **Device Type** (Advanced Server), **DNS Name** (10.64.102.112), **IP address** (10.64.102.112), **Alias** (10.64.102.112), **NetBIOS Name** (10.64.102.112), **Operating System** (Unknown), **Location** (DC_AES_TRAPS), **On Failure** (Include Traceroute in alert), and three response fields for warning, critical, and return to good states, all set to "<doing nothing>". At the bottom is a note: "Use additional Properties tabs to configure access to the data sources that OneSight metrics use to monitor this system." and three buttons: **OK**, **Cancel**, and **Help**.

Select the **SNMP Trap** tab and set the **Community** field to *empirix*. The **Community** field should match the community string configured in AES as configured in **Section 8**. Click **OK**.

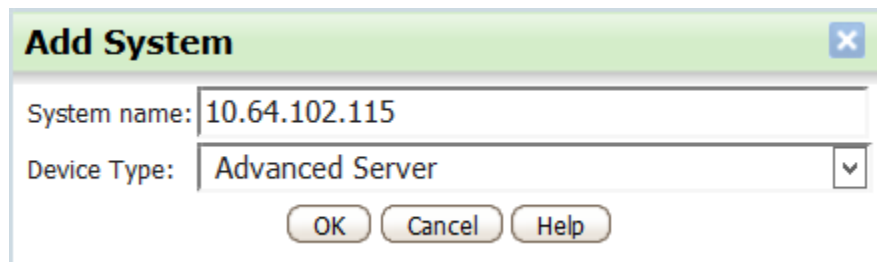


9.4. Configure SNMP Polls

This section covers the SNMP poll configuration for the Avaya Aura® Suite. In OneSight, one **System** should be added for each Avaya Aura® product as summarized in the table below. This configuration is performed in the OneSight server with IP address 10.64.102.111.

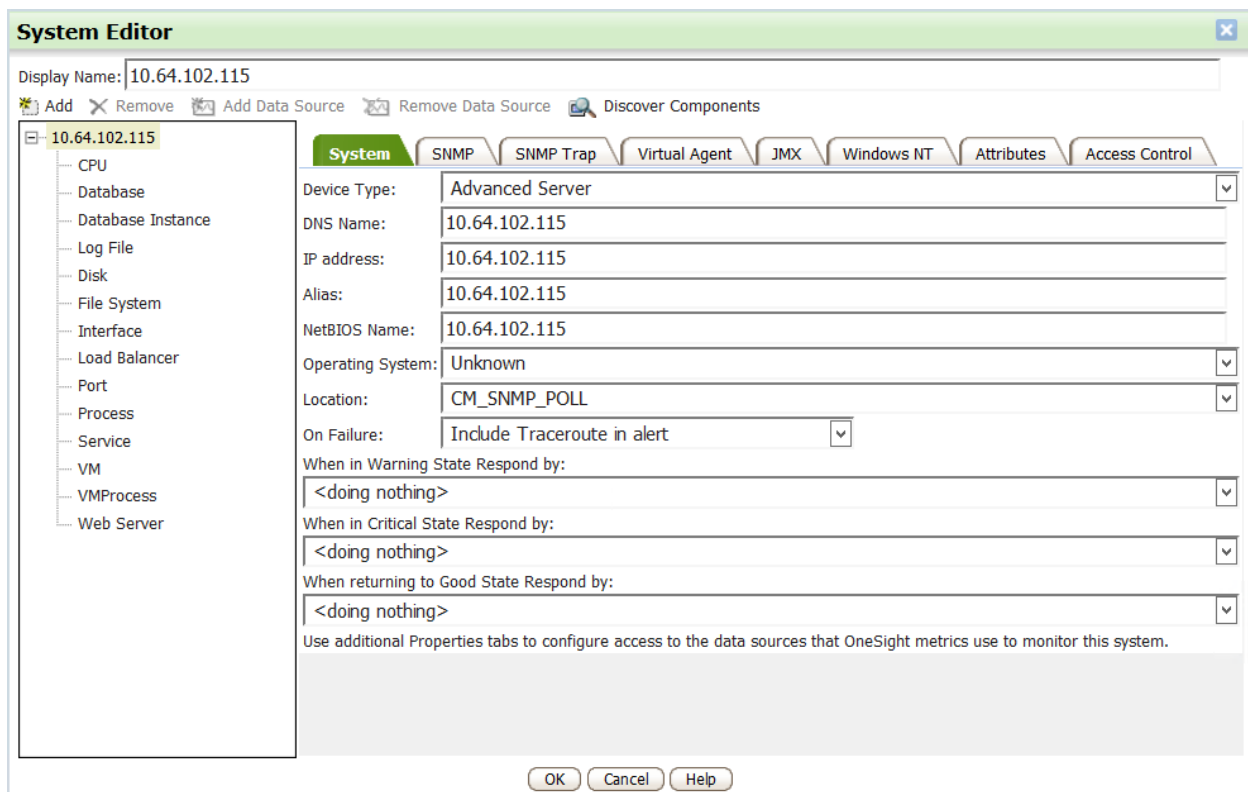
Avaya Aura® Product	IP Address	Location	OSDC Properties
Communication Manager	10.64.102.115	CM_SNMP_POLL	See Section 9.1.2
G450 Media Gateway	192.168.100.15	MG_SNMP_POLL	See Section 9.1.3
System Manager	10.64.102.120	SYSMGR_SNMP_POLL	See Section 9.1.4
Session Manager	10.64.102.116	SESSION_SNMP_POLL	See Section 9.1.5
AES	10.64.102.119	AES_SNMP_POLL	See Section 9.1.6

From the **Systems** screen, click **Add**. In the **Add System** dialog box, enter a descriptive name for the **System name**. This example illustrates the configuration for Communication Manager SNMP polls. In this example, the Communication Manager IP address was used. Click **OK**.



The **Add System** dialog box is shown. It has a title bar with a close button. Inside, there are two input fields: "System name:" with the value "10.64.102.115" and "Device Type:" with a dropdown menu showing "Advanced Server". At the bottom, there are three buttons: "OK", "Cancel", and "Help".

In the **System Editor** window, enter the Communication Manager IP address in the **DNS Name**, **IP Address**, **Alias**, **NetBIOS Name** fields. Set the **Location** field to *CM_SNMP_POLL*. This uses the `OSDC.properties` file configured in **Section 9.1.1**, where the **Location** parameter was to the same value.



The **System Editor** window is shown. It has a title bar with a close button. Below the title bar is a "Display Name:" field with the value "10.64.102.115". Below that is a toolbar with icons for "Add", "Remove", "Add Data Source", "Remove Data Source", and "Discover Components". On the left is a tree view showing a hierarchy of system components: "10.64.102.115" (selected), "CPU", "Database", "Database Instance", "Log File", "Disk", "File System", "Interface", "Load Balancer", "Port", "Process", "Service", "VM", "VMProcess", and "Web Server". On the right is a tabbed interface with tabs for "System", "SNMP", "SNMP Trap", "Virtual Agent", "JMX", "Windows NT", "Attributes", and "Access Control". The "System" tab is active. It contains several fields: "Device Type:" (Advanced Server), "DNS Name:" (10.64.102.115), "IP address:" (10.64.102.115), "Alias:" (10.64.102.115), "NetBIOS Name:" (10.64.102.115), "Operating System:" (Unknown), "Location:" (CM_SNMP_POLL), "On Failure:" (Include Traceroute in alert), "When in Warning State Respond by:" (<doing nothing>), "When in Critical State Respond by:" (<doing nothing>), and "When returning to Good State Respond by:" (<doing nothing>). At the bottom, there is a note: "Use additional Properties tabs to configure access to the data sources that OneSight metrics use to monitor this system." and three buttons: "OK", "Cancel", and "Help".

Select the **SNMP** tab and ensure that the fields match the configuration in **Section 5.2**, which describes the SNMP poll configuration for Communication Manager. Set the **Version** field to the appropriate SNMP version. Click **OK**.

The screenshot shows the 'System Editor' window with the 'Display Name' set to '10.64.102.115'. The left sidebar lists various system components, with 'System' selected. The main panel has tabs for 'System', 'SNMP', 'SNMP Trap', 'Virtual Agent', 'JMX', 'Windows NT', 'Attributes', and 'Access Control'. The 'SNMP' tab is active, displaying the following configuration fields:

- Community: public
- Timeout seconds: 15
- Timeout retries: 1
- Port: 161
- Version: Snmp_Version3 (dropdown menu)
- AuthMode: Auth/Priv (dropdown menu)
- User name: admincm
- Password: (masked with dots)
- AuthType: MD5 (dropdown menu)
- Privacy Mode: DES (dropdown menu)
- Privacy Password: (masked with dots)
- Context Name: (empty field)

At the bottom of the window are 'OK', 'Cancel', and 'Help' buttons.

Repeat the configuration in this section for the other Avaya Aura® products making the following adjustments:

- Use the appropriate IP address for each Avaya Aura® product.
- Select the appropriate **Location** for each Avaya Aura® product. Refer to the table at the beginning of this section or check the **Location** parameter in the `OSDC.properties` file.
- In the SNMP tab, configure the appropriate credentials for the appropriate SNMP version.

10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Empirix OneSight and Avaya Aura® Suite.

1. Generate SNMP traps from Avaya Aura® Suite and verify that the SNMP traps are received and displayed in the OneSight dashboard on the web interface. Navigate to Status → General to display the webpage below. In this example, an SNMP Trap for an ISDN link down event is displayed.

Group by: Monitor Group ▼

Communication Mgr


Shows name contains [Apply](#)

- CM_SNMP_GET_PROFILE (10.64.102.115) - Last measured value: 0
- ▲ Communication_Manager_7_Traps_Profile (10.64.102.111)
- Current alert: Trap Received:**
Enterprise: .iso.org.dod.internet.private.enterprises.avaya.mibs.avCommMgrMibs.avCmAlarmMib
Trap Event Name: avCmAlmServCmgWarning
...
- LIST MEASUREMENT - DEV CONNECT (10.64.102.115) - Last measured value: Waiting

Media Gateway

Shows name contains [Apply](#)

- From the OneSight dashboard, verify that SNMP Poll data is collected and displayed. The following example shows SNMP data from the G450 Media Gateway.

<div>  <div> Status Reports Configure </div> </div>			
Media Gateway			
<div> <div>Sample All Selected</div> <div>Show Report</div> </div>			
Shows All name contains <input type="text"/> <div>Apply</div>			
Monitor		Last Measured Value	
<input checked="" type="checkbox"/>	▲ Avaya_G700_Media_Gateway_Traps_Profile (10.64.102.111)	Trap Received	
<input checked="" type="checkbox"/>	● MediaGateway_SNMP_GET_PROFILE (192.168.100.15)	3	
Metric		Value	Last Measured
<input checked="" type="checkbox"/>	● cmgActiveClockSource for 192.168.100.15	3	12:04:56 PM America/New_York
<input checked="" type="checkbox"/>	● cmgActiveControllerInetAddressType for 192.168.100.15	1	12:01:59 PM America/New_York
<input checked="" type="checkbox"/>	● cmgClockSourceControl for 192.168.100.15	1	12:01:03 PM America/New_York
<input checked="" type="checkbox"/>	● cmgClockSwitching for 192.168.100.15	1	12:00:19 PM America/New_York
<input checked="" type="checkbox"/>	● cmgCurrent802Vlan for 192.168.100.15	1	12:06:13 PM America/New_York
<input checked="" type="checkbox"/>	● cmgDynCacLastUpdate for 192.168.100.15	0	12:05:09 PM America/New_York
<input checked="" type="checkbox"/>	● cmgDynCacRBBL for 192.168.100.15	-1	12:05:47 PM America/New_York
<input checked="" type="checkbox"/>	● cmgDynCacStatus for 192.168.100.15	2	12:05:37 PM America/New_York
<input checked="" type="checkbox"/>	● cmgGatewayNumber for 192.168.100.15	2	12:04:41 PM America/New_York
<input checked="" type="checkbox"/>	● cmgH248LinkErrorCode for 192.168.100.15	0	12:07:54 PM America/New_York
<input checked="" type="checkbox"/>	● cmgH248LinkStatus for 192.168.100.15	1	12:05:32 PM America/New_York

11. Conclusion

These Application Notes described the configuration steps required to integrate Empirix OneSight with the Avaya Aura® Suite using SNMP. The Avaya Aura® products included Avaya Aura® Communication Manager, Avaya G450 Media Gateway, Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. Empirix OneSight was able to receive SNMP traps and poll for performance data from Avaya Aura® Suite and display the data on the OneSight dashboard. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

12. References

This section references the Avaya and Empirix documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Avaya Aura® Communication Manager SNMP Administration and Reference Guide*, Release 7.1, Issue 1, May 2017.
- [2] *Administering Avaya G450 Branch Gateway*, Release 7.1.2, Issue 2, December 2017.
- [3] *Avaya Aura® System Manager 7.1 SNMP Whitepaper*, Issue 1.0, 28th April 2017.
- [4] *Administering Avaya Aura® System Manager 7.1.2*, Issue 10, January 2018.
- [5] *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 3, December 2017.
- [6] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.1.2, Issue 4, December 2017.
- [7] *Empirix OneSight Administrator Guide*, Release 9.5.1, September 2017, Revision A.

13. APPENDIX: Configuring Metrics, Profiles, Monitors, and Monitor Groups on Empirix OneSight

This section provides a high-level overview for how to load SNMP MIBs to Empirix OneSight. This is outside the scope of these Application Notes, but a summary is provided for informational purposes.

13.1. Add Metrics

From the OneSight web interface, select **Metrics** under **Configuration Quick Links**. The metrics are derived from the SNMP MIB files, including Avaya enterprise and standard MIBs. Click **Add**.

Global Metrics

Show metrics with name containing

Add Clone Modify Remove Used By Import Metric

Name	Default	Type	Status
avCmAlmAcPowerMajor	Default	SNMP Trap	Advanced
avCmAlmAcPowerMinor	Default	SNMP Trap	Advanced
avCmAlmAcPowerWarning	Default	SNMP Trap	Advanced
avCmAlmAdjIpMajor	Default	SNMP Trap	Advanced
avCmAlmAdjIpMinor	Default	SNMP Trap	Advanced
avCmAlmAdjIpWarning	Default	SNMP Trap	Advanced
avCmAlmAdjustAlarmIndex	Default	SNMP	Advanced
avCmAlmAdjustAlarmType	Default	SNMP	Advanced
avCmAlmAdjustMajorOffBrd	Default	SNMP	Advanced
avCmAlmAdjustMajorOnBrd	Default	SNMP	Advanced
avCmAlmAdjustMinorOffBrd	Default	SNMP	Advanced
avCmAlmAdjustMinorOnBrd	Default	SNMP	Advanced
avCmAlmAdjustOperation	Default	SNMP	Advanced
avCmAlmAdjustServMajor	Default	SNMP	Advanced
avCmAlmAdjustServMinor	Default	SNMP	Advanced
avCmAlmAdjustServWarning	Default	SNMP	Advanced
avCmAlmAdjustStatus	Default	SNMP	Advanced
avCmAlmAdjustWarningOffBrd	Default	SNMP	Advanced
avCmAlmAdjustWarningOnBrd	Default	SNMP	Advanced

Description: AES: authenticationFailure

In use Not in use

The Metric Editor is displayed. Provide a **Metric Name** and select the appropriate **System**, which is OneSight data collector, which is *10.64.102.111* in this case. Select the **Data Sources** tab.

Metric Editor

Metric Name:

General | Data Sources | Attributes | Access Control

Description:

Sample for Each:

Group:

System:

Report Category:

Translation Type:

Unit Measure:

Sample Every:

In the **Data Sources** tab, click the **List Mibs** button to populate the **Mib File** field with a list of MIB files to choose from. The list options for this field are derived from the Avaya and standard SNMP MIBs located in the C:\mibs directory. Select the appropriate MIB file. For **Trap Type**, provide the SNMP metric name from the MIB file selected. Provide a **Description** (optional). Click **OK**.

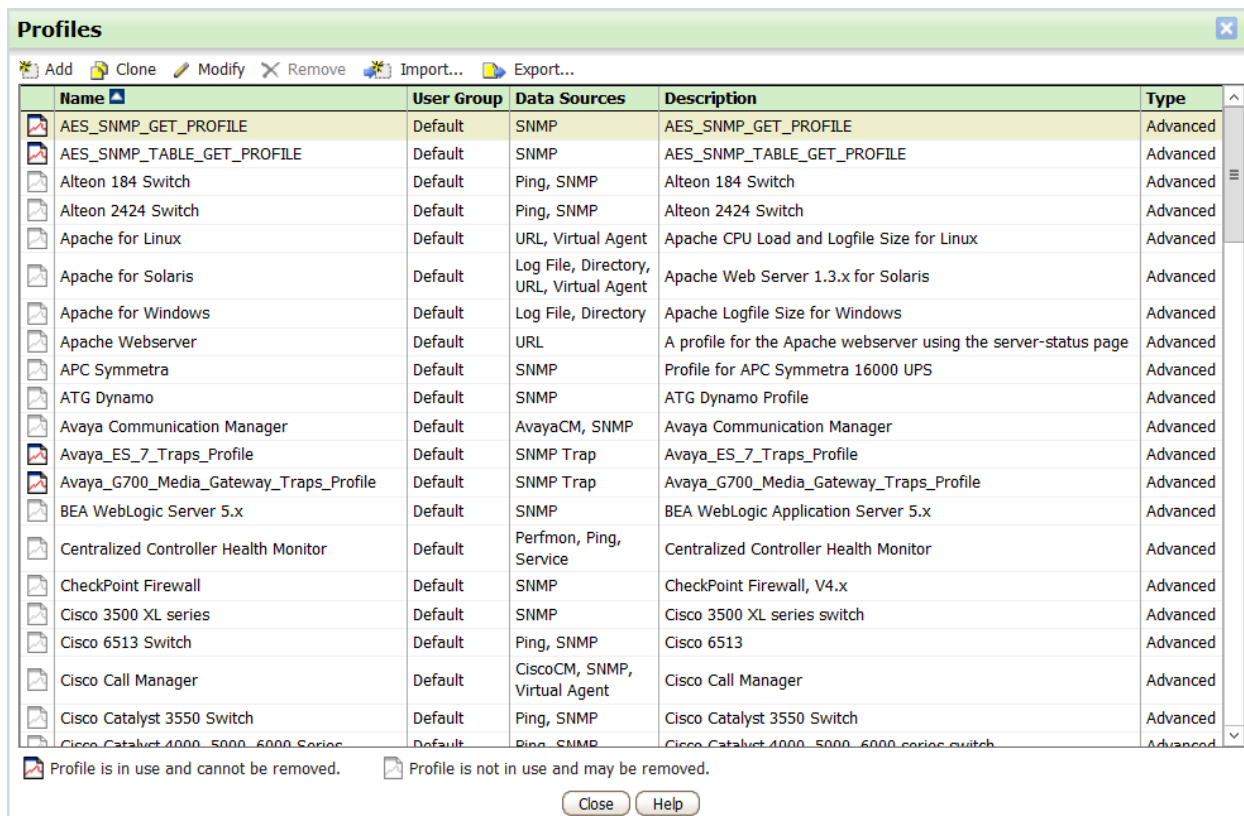
Repeat this step for each SNMP trap metric to add to OneSight. To add SNMP poll data, select **SNMP** from the left pane instead and follow similar steps.

The screenshot shows the **Metric Editor** window with the **Data Sources** tab selected. The **Metric Name** is **avCmAlmAlarmTest**. The left pane lists various data sources, with **SNMP Trap** selected. The right pane shows the **SNMP Trap Data Source** configuration. The **Mib File** is set to **AVAYA-AURA-CMALARM-MIB.mib**. The **Trap Type** is **avCmAlmAlarmTest**. The **Description** is **A test alarm has been issued by Communication**. The **Name Format** is **FullName**. The **Alert Level** is **1**. The **Hold Duration (in min)** is empty. The **OK**, **Cancel**, **Test**, and **Help** buttons are at the bottom.

Field	Value
Metric Name	avCmAlmAlarmTest
Mib File	AVAYA-AURA-CMALARM-MIB.mib
OID Version	
Enterprise	<Other>
Trap Type	<Other> avCmAlmAlarmTest
Description	<Other> A test alarm has been issued by Communication
Name Format	FullName
Reset Trap	<Other>
Alert Level	1
Hold Duration (in min)	

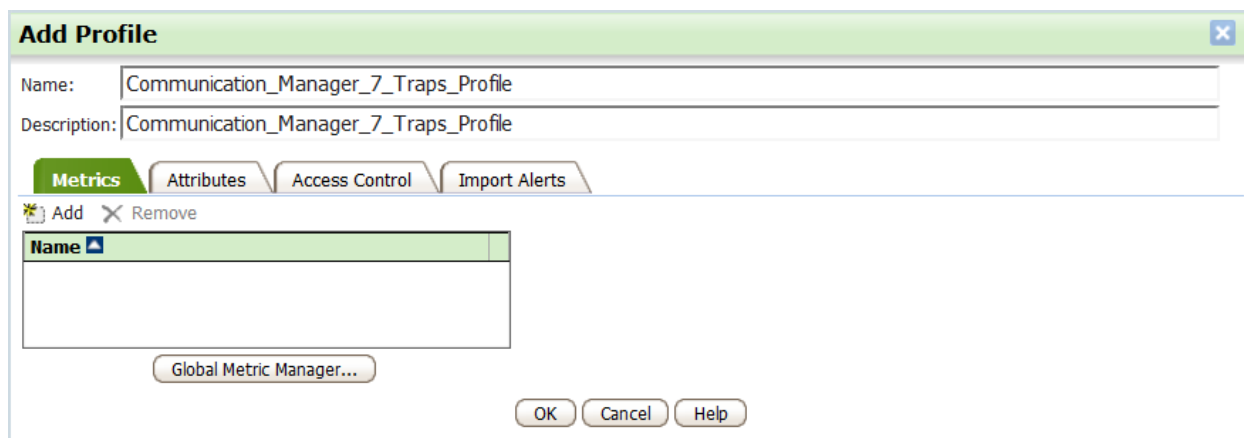
13.2. Add Profiles

From the OneSight web interface, select **Profiles** under **Configuration Quick Links**. Click **Add**.



Name	User Group	Data Sources	Description	Type
AES_SNMP_GET_PROFILE	Default	SNMP	AES_SNMP_GET_PROFILE	Advanced
AES_SNMP_TABLE_GET_PROFILE	Default	SNMP	AES_SNMP_TABLE_GET_PROFILE	Advanced
Alteon 184 Switch	Default	Ping, SNMP	Alteon 184 Switch	Advanced
Alteon 2424 Switch	Default	Ping, SNMP	Alteon 2424 Switch	Advanced
Apache for Linux	Default	URL, Virtual Agent	Apache CPU Load and Logfile Size for Linux	Advanced
Apache for Solaris	Default	Log File, Directory, URL, Virtual Agent	Apache Web Server 1.3.x for Solaris	Advanced
Apache for Windows	Default	Log File, Directory	Apache Logfile Size for Windows	Advanced
Apache Webserver	Default	URL	A profile for the Apache webserver using the server-status page	Advanced
APC Symmetra	Default	SNMP	Profile for APC Symmetra 16000 UPS	Advanced
ATG Dynamo	Default	SNMP	ATG Dynamo Profile	Advanced
Avaya Communication Manager	Default	AvayaCM, SNMP	Avaya Communication Manager	Advanced
Avaya_ES_7_Traps_Profile	Default	SNMP Trap	Avaya_ES_7_Traps_Profile	Advanced
Avaya_G700_Media_Gateway_Traps_Profile	Default	SNMP Trap	Avaya_G700_Media_Gateway_Traps_Profile	Advanced
BEA WebLogic Server 5.x	Default	SNMP	BEA WebLogic Application Server 5.x	Advanced
Centralized Controller Health Monitor	Default	Perfmon, Ping, Service	Centralized Controller Health Monitor	Advanced
CheckPoint Firewall	Default	SNMP	CheckPoint Firewall, V4.x	Advanced
Cisco 3500 XL series	Default	SNMP	Cisco 3500 XL series switch	Advanced
Cisco 6513 Switch	Default	Ping, SNMP	Cisco 6513	Advanced
Cisco Call Manager	Default	CiscoCM, SNMP, Virtual Agent	Cisco Call Manager	Advanced
Cisco Catalyst 3550 Switch	Default	Ping, SNMP	Cisco Catalyst 3550 Switch	Advanced
Cisco Catalyst 4000_5000_6000 Series	Default	Ping, SNMP	Cisco Catalyst 4000_5000_6000 series switch	Advanced

In **Add Profile**, provide a descriptive **Name** and **Description**. Click **Add** in the **Metrics** tab. Click **OK**.



Add Profile

Name: Communication_Manager_7_Traps_Profile

Description: Communication_Manager_7_Traps_Profile

Metrics | Attributes | Access Control | Import Alerts

Add Remove

Name

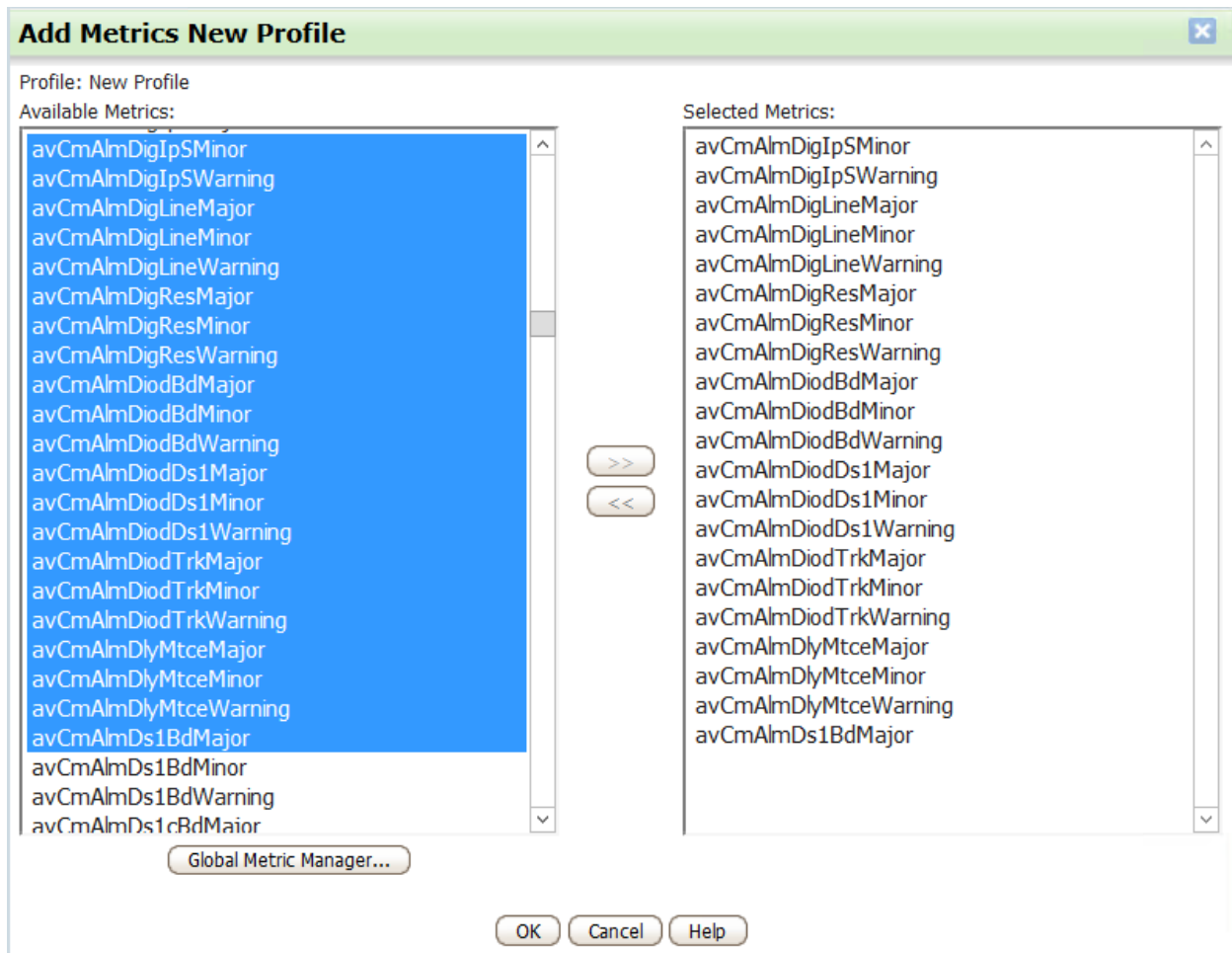
Global Metric Manager...

OK Cancel Help

In **Add Metrics New Profile**, select the metrics to include in the profile as shown below. Click the >> button to move the **Available Metrics** to the **Selected Metrics** section. The metrics were added in the previous section. Click **OK**.

Repeat these steps to add multiple profiles. As an example, profiles can be added for each Avaya Aura® product to group metrics on a per product basis.

Note: The MIBs can be grouped into various profiles as desired by the customer.



On the following screen, click **OK**.

Add Profile

Name: Communication_Manager_7_Traps_Profile

Description: Communication_Manager_7_Traps_Profile

Metrics | Attributes | Access Control | Import Alerts

Add Remove

name
avCmAlmDigIpSMajor
avCmAlmDigIpSMajorWarning
avCmAlmDigLineMajor
avCmAlmDigLineMinor
avCmAlmDigLineWarning
avCmAlmDigResMajor
avCmAlmDigResMinor
avCmAlmDigResWarning
avCmAlmDiodBdMajor
avCmAlmDiodBdMinor
avCmAlmDiodBdWarning
avCmAlmDiodDs1Major
avCmAlmDiodDs1Minor
avCmAlmDiodDs1Warning
avCmAlmDiodTrkMajor
avCmAlmDiodTrkMinor
avCmAlmDiodTrkWarning
avCmAlmDlyMtceMajor
avCmAlmDlyMtceMinor
avCmAlmDlyMtceWarning
avCmAlmDs1BdMajor

Alerts | SmartLinks

Measurement alerts, such as exceeded thresholds or unavailability, can have responses associated with them. A response can trigger an action plan, change a monitor's health, or in some cases, both. Use the list below to review or change configured alerts and responses for this monitor.

Add Clone Modify Remove Import Alert

Alert Description	Respond by	Respond by (Return to Good)
Sample Failure		
Acquisition Failure		
Default Trap		

Applies to Critical State
 Applies to Warning State

Global Metric Manager...

OK Cancel Help

13.3. Add Monitors

From the OneSight web interface, select **Monitors** under **Configuration Quick Links**. The following web page is displayed. Click **Add**.

Monitors

Show monitors where contains

Show

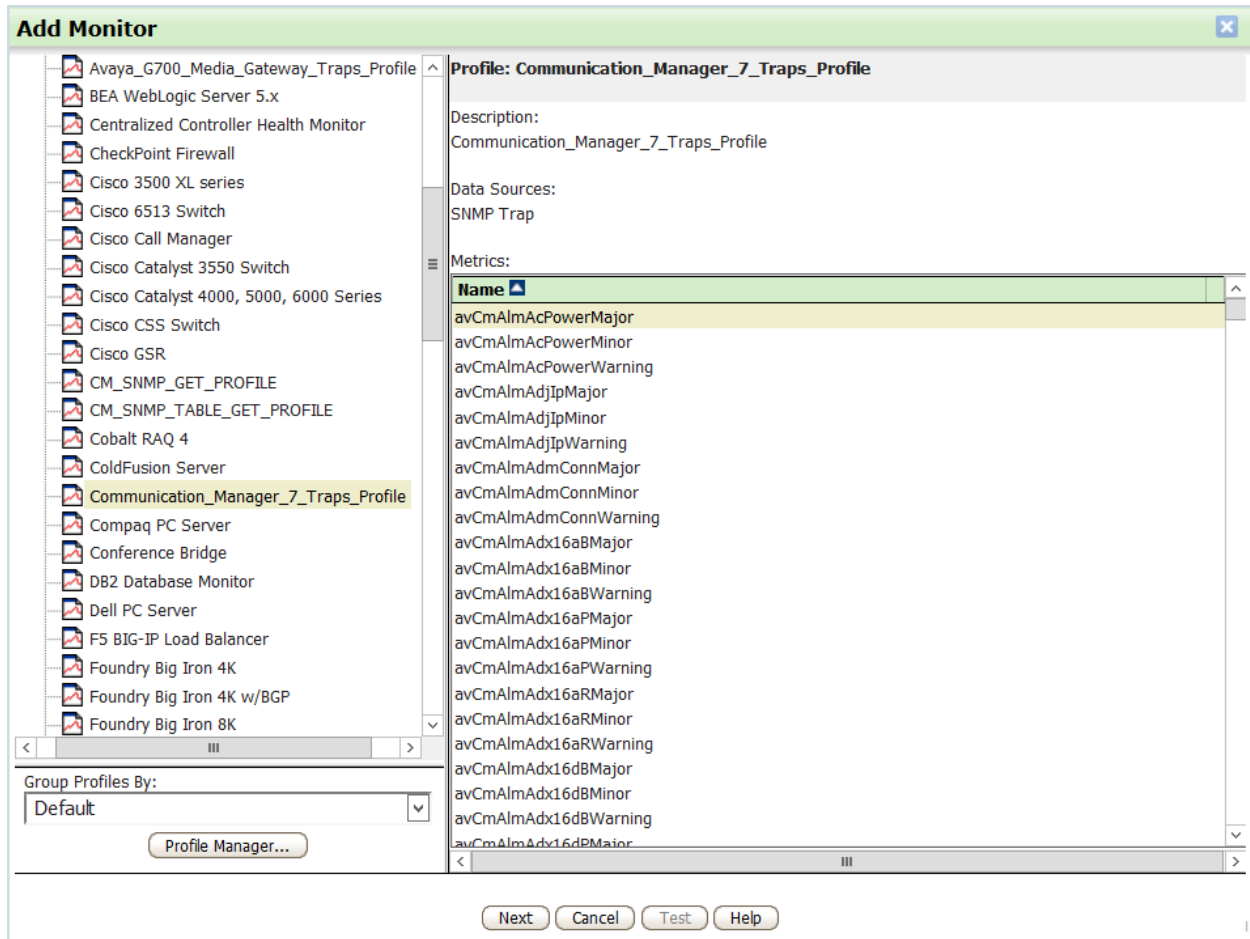
Add Clone Modify Remove Check All Uncheck All Bulk Modification

Enable	Name	User Group	Type
<input type="checkbox"/>	AES_SNMP_GET_PROFILE (10.64.102.119)	Default	System
<input type="checkbox"/>	AES_SNMP_TABLE_GET_PROFILE (10.64.102.119)	Default	System
<input checked="" type="checkbox"/>	Avaya_ES_7_Traps_Profile (10.64.102.112)	Default	System
<input checked="" type="checkbox"/>	Avaya_G700_Media_Gateway_Traps_Profile (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	CM_SNMP_GET_PROFILE (10.64.102.115)	Default	System
<input checked="" type="checkbox"/>	Communication_Manager_7_Traps_Profile (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	LIST MEASUREMENT - DEV CONNECT (10.64.102.115)	Default	System
<input checked="" type="checkbox"/>	MediaGateway_SNMP_GET_PROFILE (192.168.100.15)	Default	System
<input checked="" type="checkbox"/>	MediaGateway_SNMP_TABLE_GET_PROFILE (192.168.100.15)	Default	System
<input checked="" type="checkbox"/>	Session manager SNMP GET profile (10.64.102.116)	Default	System
<input checked="" type="checkbox"/>	Session manager table get profile (10.64.102.116)	Default	System
<input checked="" type="checkbox"/>	Session_Manager_7_CommonAlarm_Def_Profil (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	Session_Manager_7_SmELEM_Trap_Profile (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	Session_Manager_7_SmSecMod_Trap_Profile (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	Session_Manager_7_SmSIPAS_Trap_Profile (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	Session_Manager_7_SmThirdParty_Trap_Prof (10.64.102.111)	Default	System
<input checked="" type="checkbox"/>	SysMgr_SNMP_GET_PROFILE (10.64.102.120)	Default	System
<input checked="" type="checkbox"/>	SysMgr_SNMP_TABLE_GET_PROFILE (10.64.102.120)	Default	System
<input checked="" type="checkbox"/>	System Manager 7 Traps Profile (10.64.102.111)	Default	System

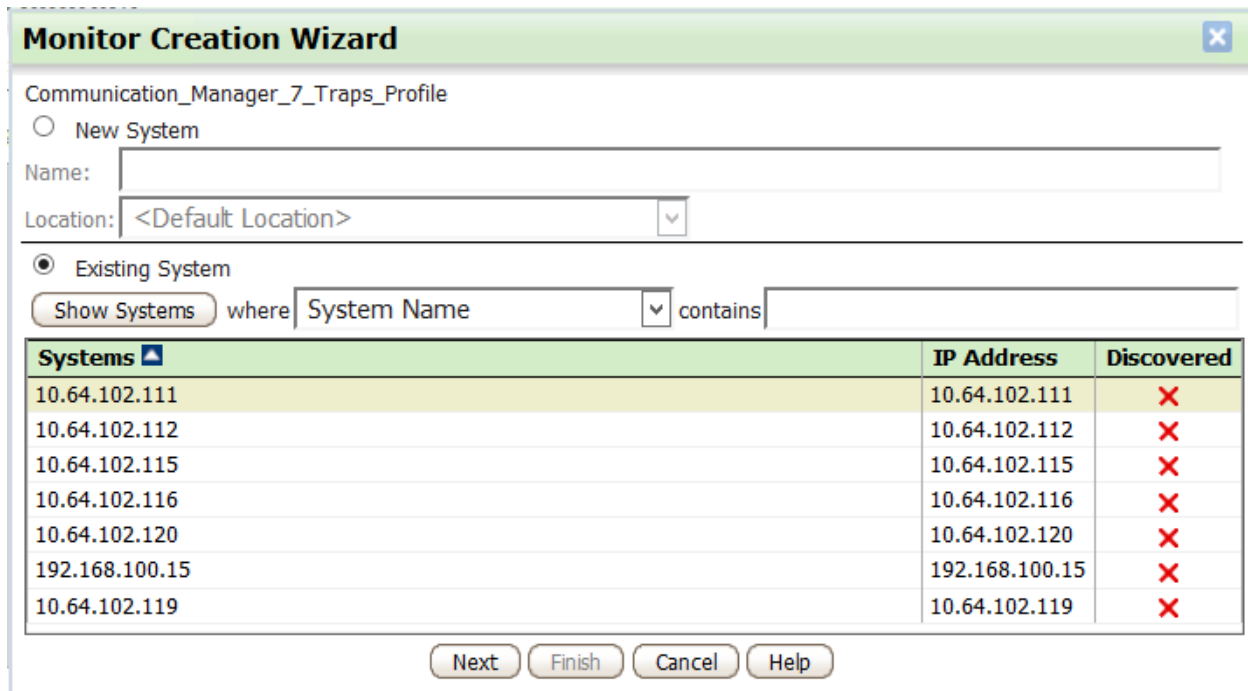
In use Not in use

Close Help

In **Add Monitor**, expand **Profiles** in left pane (not shown) and select the **Profile** as shown to add to the **Monitor**. Click **Next**.



Select the appropriate OneSight data collector under **Existing Systems**. These were added in **Section 9.3**. Click **Next**.



The image shows a 'Monitor Creation Wizard' window. At the top, the title bar says 'Monitor Creation Wizard'. Below the title bar, the text 'Communication_Manager_7_Traps_Profile' is displayed. There are two radio buttons: 'New System' (unselected) and 'Existing System' (selected). Below the radio buttons, there is a 'Name:' label followed by a text input field. Below that is a 'Location:' label followed by a dropdown menu showing '<Default Location>'. Under the 'Existing System' section, there is a 'Show Systems' button, followed by the text 'where', a 'System Name' dropdown menu, the text 'contains', and another text input field. Below this is a table with three columns: 'Systems', 'IP Address', and 'Discovered'. The table contains seven rows of data. The first row is highlighted in yellow. At the bottom of the window, there are four buttons: 'Next', 'Finish', 'Cancel', and 'Help'.

Systems	IP Address	Discovered
10.64.102.111	10.64.102.111	×
10.64.102.112	10.64.102.112	×
10.64.102.115	10.64.102.115	×
10.64.102.116	10.64.102.116	×
10.64.102.120	10.64.102.120	×
192.168.100.15	192.168.100.15	×
10.64.102.119	10.64.102.119	×

In the **Monitor Editor**, click **OK** to complete the process.

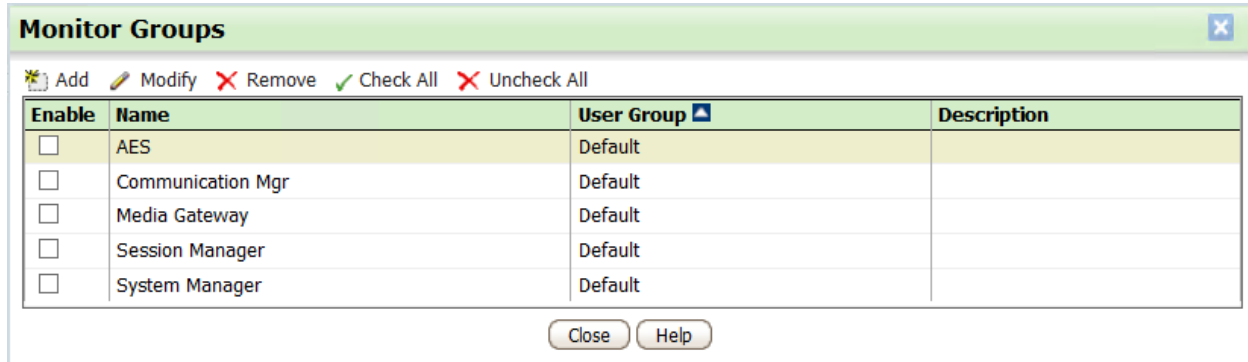
Note: Repeat these steps for each profile to monitor.

The screenshot shows the 'Monitor Editor' window with the 'Monitor' tab selected. The 'Monitor Name' field contains 'Communication_Manager_7_Traps_Profile (10.64.102.111)'. Below the tabs, the 'Profile' field shows 'Communication_Manager_7_Traps_Profile' and the 'Applied To System' field shows '10.64.102.111'. The main area is divided into two panes: 'Metrics' on the left and 'System Components' on the right. The 'Metrics' pane contains a list of 20 metrics, each preceded by a green checkmark. The 'System Components' pane is currently empty. At the bottom, there are buttons for 'Profile Editor...', 'System Editor...', 'OK', 'Cancel', 'Test', and 'Help'.

Metrics	System Components
✓ avCmAlmAcPowerMajor	
✓ avCmAlmAcPowerMinor	
✓ avCmAlmAcPowerWarning	
✓ avCmAlmAdjIpMajor	
✓ avCmAlmAdjIpMinor	
✓ avCmAlmAdjIpWarning	
✓ avCmAlmAdmConnMajor	
✓ avCmAlmAdmConnMinor	
✓ avCmAlmAdmConnWarning	
✓ avCmAlmAdx16aBMajor	
✓ avCmAlmAdx16aBMinor	
✓ avCmAlmAdx16aBWarning	
✓ avCmAlmAdx16aPMajor	
✓ avCmAlmAdx16aPMinor	
✓ avCmAlmAdx16aPWarning	
✓ avCmAlmAdx16aRMajor	
✓ avCmAlmAdx16aRMinor	
✓ avCmAlmAdx16aRWarning	
✓ avCmAlmAdx16dBMajor	
✓ avCmAlmAdx16dBMinor	

13.4. Monitor Groups

From the OneSight web interface, select **Monitor Groups** under **Configuration Quick Links**. Click **Add**.

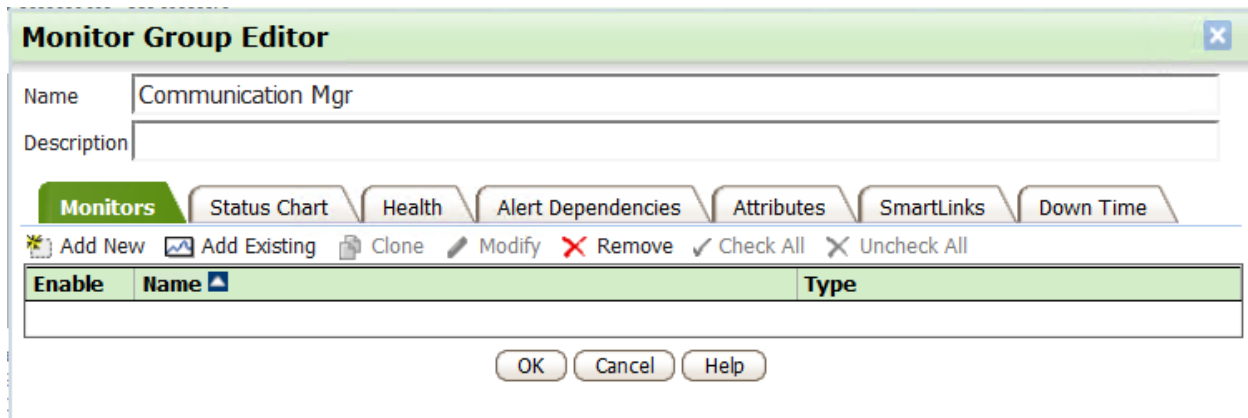


The **Monitor Groups** window displays a table of existing monitor groups. The table has four columns: **Enable**, **Name**, **User Group**, and **Description**. There are five rows of data, all with the **User Group** set to **Default**. The **Enable** column contains unchecked checkboxes for each row.

Enable	Name	User Group	Description
<input type="checkbox"/>	AES	Default	
<input type="checkbox"/>	Communication Mgr	Default	
<input type="checkbox"/>	Media Gateway	Default	
<input type="checkbox"/>	Session Manager	Default	
<input type="checkbox"/>	System Manager	Default	

Buttons: **Add**, **Modify**, **Remove**, **Check All**, **Uncheck All**, **Close**, **Help**.

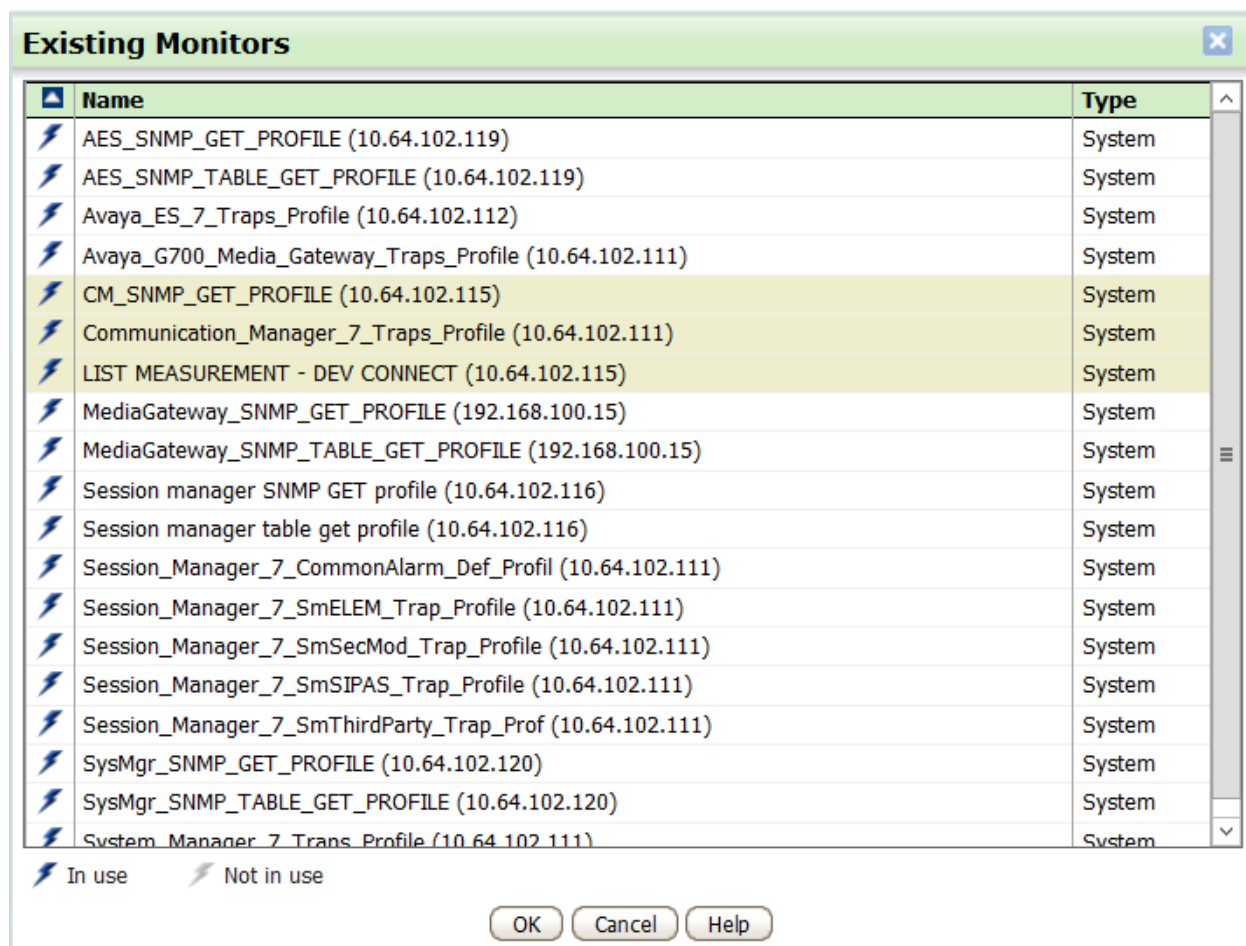
In the **Monitor Group Editor**, specify a **Name** and click on **Add Existing** since the monitors were configured in the previous section.



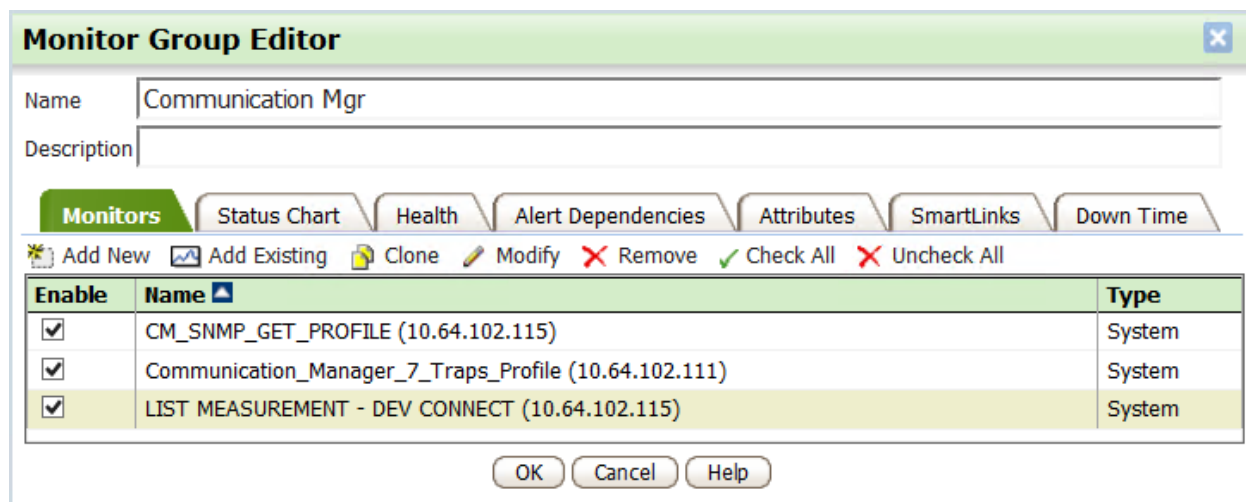
The **Monitor Group Editor** window shows the configuration for a new monitor group. The **Name** field is populated with "Communication Mgr". The **Description** field is empty. Below the fields are tabs for **Monitors**, **Status Chart**, **Health**, **Alert Dependencies**, **Attributes**, **SmartLinks**, and **Down Time**. The **Monitors** tab is selected. Below the tabs are buttons for **Add New**, **Add Existing**, **Clone**, **Modify**, **Remove**, **Check All**, and **Uncheck All**. Below these buttons is a table with three columns: **Enable**, **Name**, and **Type**. The table is currently empty.

Buttons: **OK**, **Cancel**, **Help**.

Select the monitors for this monitor group. In this example, the monitors corresponding to Communication SNMP traps and polls were selected. Click **OK**.



In the **Monitor Group Editor**, click **OK** to complete the process. Enable the **Monitor Groups**.



©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.