



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Quest Software PacketTrap MSP with Avaya Aura® Communication Manager – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration procedures required to allow Quest Software PacketTrap MSP to collect call quality data from Avaya Aura® Communication Manager utilizing Avaya Call Detail Recording (CDR) and Real Time Control Protocol (RTCP).

The PacketTrap MSP collects, stores and processes these call records to provide usage analysis, latency, and packet drop.

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 a compliance-tested CDR and RTCP solution comprised of Avaya Aura® Communication Manager and Quest Software PacketTrap MSP

Quest Software PacketTrap MSP provides a cost-effective way to offer enterprise-class server, application, and network management to customers.

It provides management and monitoring capabilities to MSPs' to further manage their customer's devices and networks. This solution includes traffic analysis on any device, application, virtual infrastructure and VoIP monitoring as well as Professional Services Automation (PSA) integration. Quest Software PacketTrap MSP ensures complete visibility and access so that you are the first to know about bandwidth clogs, server and device failures, connectivity issues, and are able to perform routine network maintenance.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established using the intra switch environment.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN connection to the PacketTrap MSP server.

**Note: For the first phase Quest Software PacketTrap MSP software, Quest Software PacketTrap MSP only performs with one instance of Communication Manager for call QoS. Thus, these Application Notes only support one instance of Communication Manager. The next phase of Quest Software PacketTrap MSP software will include the multiple instances of Communication Manager.**

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing included basic call, transfer, and conference.

The serviceability testing focused on verifying the ability of Quest Software PacketTrap MSP to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to Quest Software PacketTrap MSP.

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.

### 2.2. Test Results

All test cases were executed and verified.

## 2.3. Support

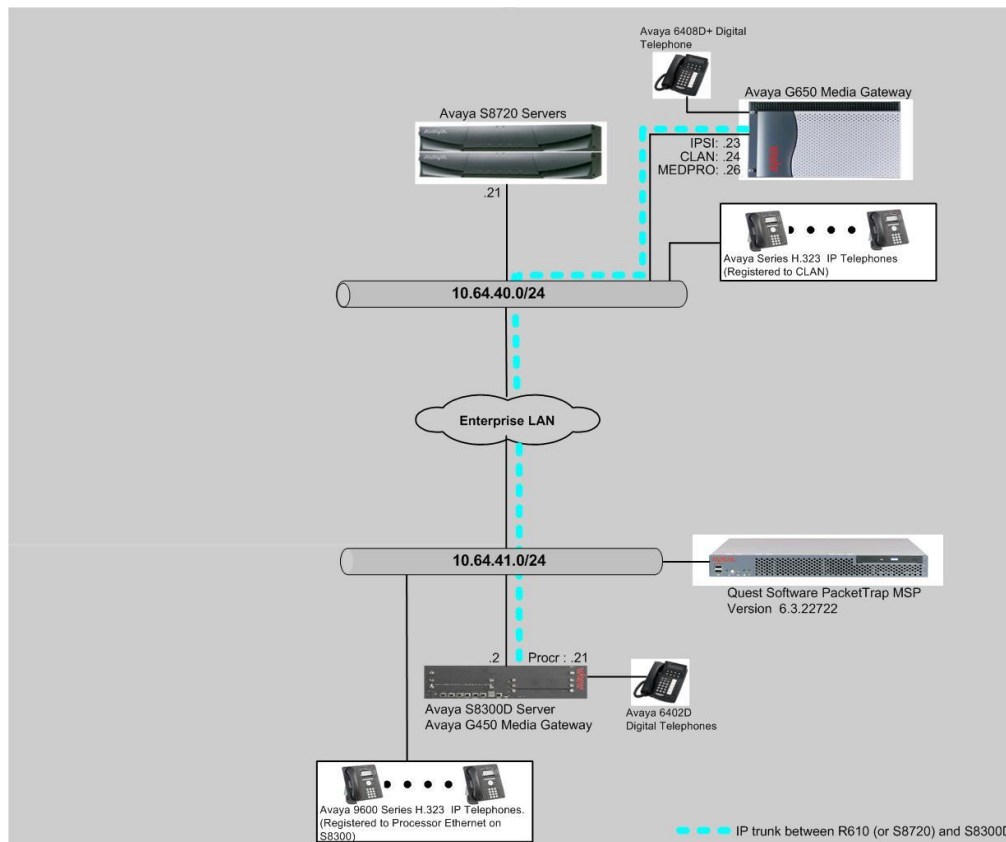
Technical support on Quest Software PacketTrap MSP can be obtained through the following:

- **Phone:** (800) 306-9329 Option 9 Ext. 17873  
(949) 754-8000  
(949) 754-8080
- **Email:** [nmsquestions@quest.com](mailto:nmsquestions@quest.com)

## 3. Reference Configuration

**Figure 1** provides the test configuration used for the compliance test. The configuration consists of an Avaya Server running Avaya Aura® Communication Manager and Quest Software PacketTrap MSP. The solution described herein is also extensible to other Avaya Servers and Media Gateways.

*Note: Avaya S8720 Servers and an Avaya G650 Media Gateway were included to simulate trunk calls.*



**Figure 1: Test configuration for Quest Software PacketTrap MSP**

## 4. Equipment and Software Validated

The following equipment and software/firmware were used for the test configuration provided.

Equipment		Software/Firmware
Avaya S8300 Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0.1
Avaya 9600 Series IP Telephones		
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6400D Series Digital Telephones		-
Quest Software PacketTrap MSP on Windows 2003 server		6.3.22722

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring CDR and RTCP Monitor Server in Avaya Aura® Communication Manager. These steps are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8300D Server. All steps are the same for the other Avaya Servers unless otherwise noted. Avaya Aura® Communication Manager will be configured to generate CDR records using TCP/IP to the IP address of the PC running the PacketTrap MSP. For the Avaya S8720 Server, the TCP/IP link originates at the IP address of the CLAN board. For the Avaya S8300 Server, the TCP/IP link originates at the IP address of the local media server (with node-name – “procr”).

## 5.1. Configure Avaya Call Detail Recording

Use the **change node-names ip** command to create a new node name, for example, **quest**. This node name is associated with the IP Address of the PC running the PacketTrap MSP application. Also, take note of the node name – **procr**. It will be used in the next step.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
default	0.0.0.0	
msgserver-ip	10.64.41.21	
procr	10.64.41.21	
procr6	::	
quest	10.64.41.249	

Use the **change ip-services** command to define the CDR link to use the TCP/IP. To define a primary CDR link, the following information should be provided:

- Service Type: **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- Local Node: **procr**
- Local Port: **0** [The Local Port is fixed to 0 because Avaya Aura® Communication Manager initiates the CDR link.]
- Remote Node: **quest** [The Remote Node is set to the node name previously defined.]
- Remote Port: **50004** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in the PacketTrap MSP.]

change ip-services					Page	1 of	4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				
CDR1		procr	0	quest	50004		

On **Page 3** of the ip-services form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to **n**. By disabling RSP, the solution will utilize the TCP/IP protocol.

Note: Although the TCP/IP was utilized, Avaya recommendation on a CDR solution is utilizing Reliable Session Protocol (RSP)

change ip-services					Page	3 of	4
SESSION LAYER TIMERS							
Service	Reliable	Packet Resp	Session Connect	SPDU	Connectivity		
Type	Protocol	Timer	Message Cntr	Cntr	Timer		
CDR1	n	30	3	3	60		
CDR2	y	30	3	3	60		

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

- CDR Date Format: **month/day**
- Primary Output Format: **unformatted**
- Primary Output Endpoint: **CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats?: n** [Allows CDR formats to use 6.x CDR formats. If the field is set to y, then CDR formats utilize the 3.x CDR formats.]
- **Intra-switch CDR?: y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH CDR form.]
- **Record Outgoing Calls Only?: n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting?: y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting?: y** [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]

change system-parameters cdr		Page 1 of 1
CDR SYSTEM PARAMETERS		
Node Number (Local PBX ID): 1	CDR Date Format: month/day	
Primary Output Format: unformatted	Primary Output Endpoint: CDR1	
Secondary Output Format: unformatted Secondary Output Endpoint: CDR2		
Use ISDN Layouts? n	Enable CDR Storage on Disk? y	
Use Enhanced Formats? n	Condition Code 'T' For Redirected Calls? n	
Use Legacy CDR Formats? n	Remove # From Called Number? n	
Modified Circuit ID Display? n	Intra-switch CDR? y	
Record Outgoing Calls Only? n	Outg Trk Call Splitting? y	
Suppress CDR for Ineffective Call Attempts? y	Outg Attd Call Record? n	
Disconnect Information in Place of FRL? n	Interworking Feat-flag? n	
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n		
Calls to Hunt Group - Record: group-ext		
Record Called Vector Directory Number Instead of Group or Member? n		
Record Agent ID on Incoming? y	Record Agent ID on Outgoing? y	
Inc Trk Call Splitting? y	Inc Attd Call Record? n	
Record Non-Call-Assoc TSC? n	Call Record Handling Option: warning	
Record Call-Assoc TSC? n	Digits to Record for Outgoing Calls: dialed	
Privacy - Digits to Hide: 0	CDR Account Code Length: 6	

If the Intra-switch CDR field is set to **y** on **Page 1** of the system-parameters cdr form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked. To simplify the process of adding multiple extensions in the Assigned Members field, the Intra-switch CDR by COS feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

change intra-switch-cdr				Page 1 of 3	
INTRA-SWITCH CDR					
Assigned Members:		4	of 5000	administered	
1: 72001	19:	37:	55:	73:	91:
2: 72002	20:	38:	56:	74:	92:
3: 72003	21:	39:	57:	75:	93:
4: 72007	22:	40:	58:	76:	94:
5:	23:	41:	59:	77:	95:

## 5.2. Configure RTCP Monitor Server

This section provides the procedures for configuring RTCP Monitor Server. Since the PacketTrap MSP utilizes RTCP packet to calculate and report the quality of the call stream, a RTCP Monitor Server needs to be created in Avaya Aura® Communication Manager. The following screen describes the setting of the RTCP Monitor Server. Enter the **change system-parameters ip-options** command to configure the RTCP Monitor Server. Provide the following information:

- **Server IPV4 Address** - IP address of the PacketTrap MSP server
- **IPV4 Server Port – 5005** [This port number must match with the PacketTrap MSP RTCP Listening Port. The default value for the Default Server Port field is 5005]
- **RTCP Report Period(secs) – 5** [The report period indicates Avaya Aura® Communication Manager forwards RTCP packet to the RTCP Monitor Server, which is the PacketTrap MSP server. The default value for the Default RTCP Report Period(secs) field is 5]

Default values may be used in the remaining fields.

```

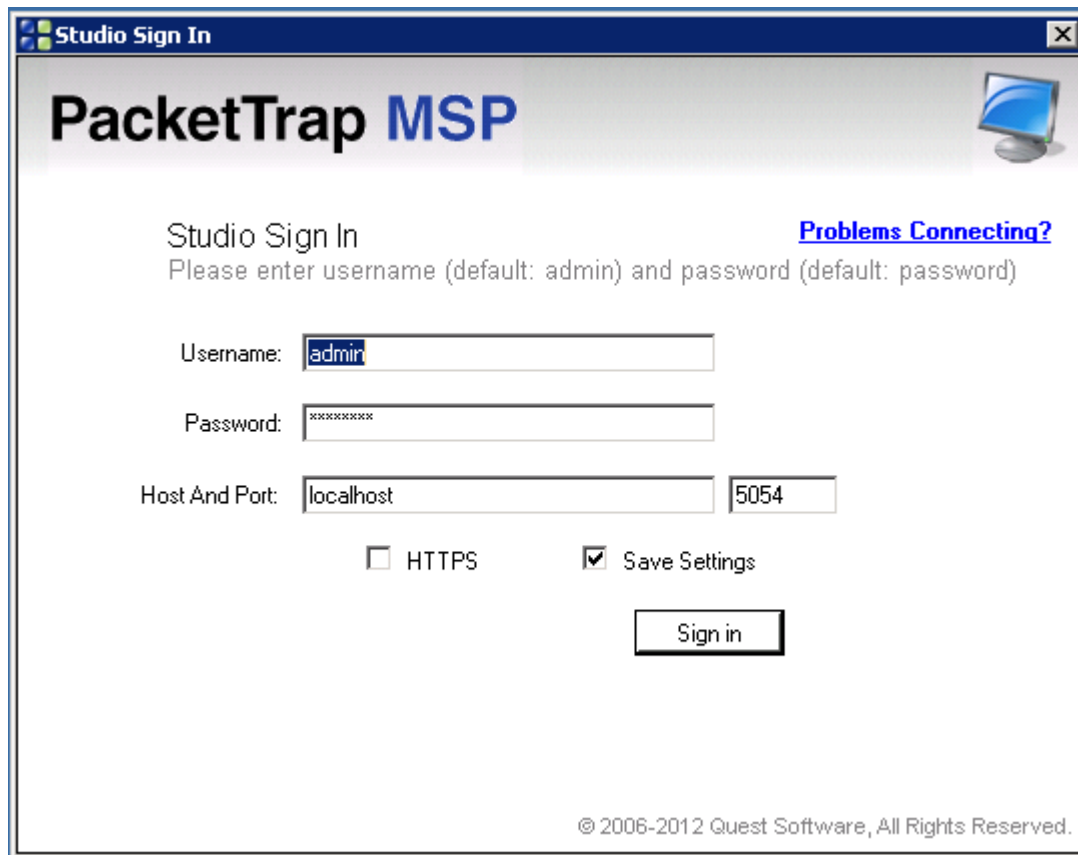
change ip-network-region 1                                     Page 2 of 20
                                IP NETWORK REGION

RTCP Reporting Enabled? y

RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? n
    Server IPV4 Address: 10.64.41.249
    IPV4 Server Port: 5005
    Server IPV6 Address:
    IPV6 Server Port: 5005
    RTCP Report Period(secs): 5
  
```

## 6. Configure Quest Software PacketTrap MSP for Avaya Aura® Communication Manager

This section describes the configuration of Quest Software PacketTrap MSP. From a PC running the PacketTrap MSP application, double click the Foglight Studio NMS icon to launch the PacketTrap MSP application. Provide credentials and click the **Sign in** tab.



The screenshot shows the 'Studio Sign In' window for PacketTrap MSP. The window has a title bar with 'Studio Sign In' and a close button. The main area has a header with 'PacketTrap MSP' and a computer icon. Below the header, it says 'Studio Sign In' and 'Please enter username (default: admin) and password (default: password)'. There is a link for 'Problems Connecting?'. The form includes fields for 'Username' (containing 'admin'), 'Password' (masked with 'xxxxxxx'), and 'Host And Port' (containing 'localhost' and '5054'). There are checkboxes for 'HTTPS' (unchecked) and 'Save Settings' (checked). A 'Sign in' button is at the bottom. The footer says '© 2006-2012 Quest Software, All Rights Reserved.'

Studio Sign In

**PacketTrap MSP**

Studio Sign In [Problems Connecting?](#)

Please enter username (default: admin) and password (default: password)

Username:

Password:

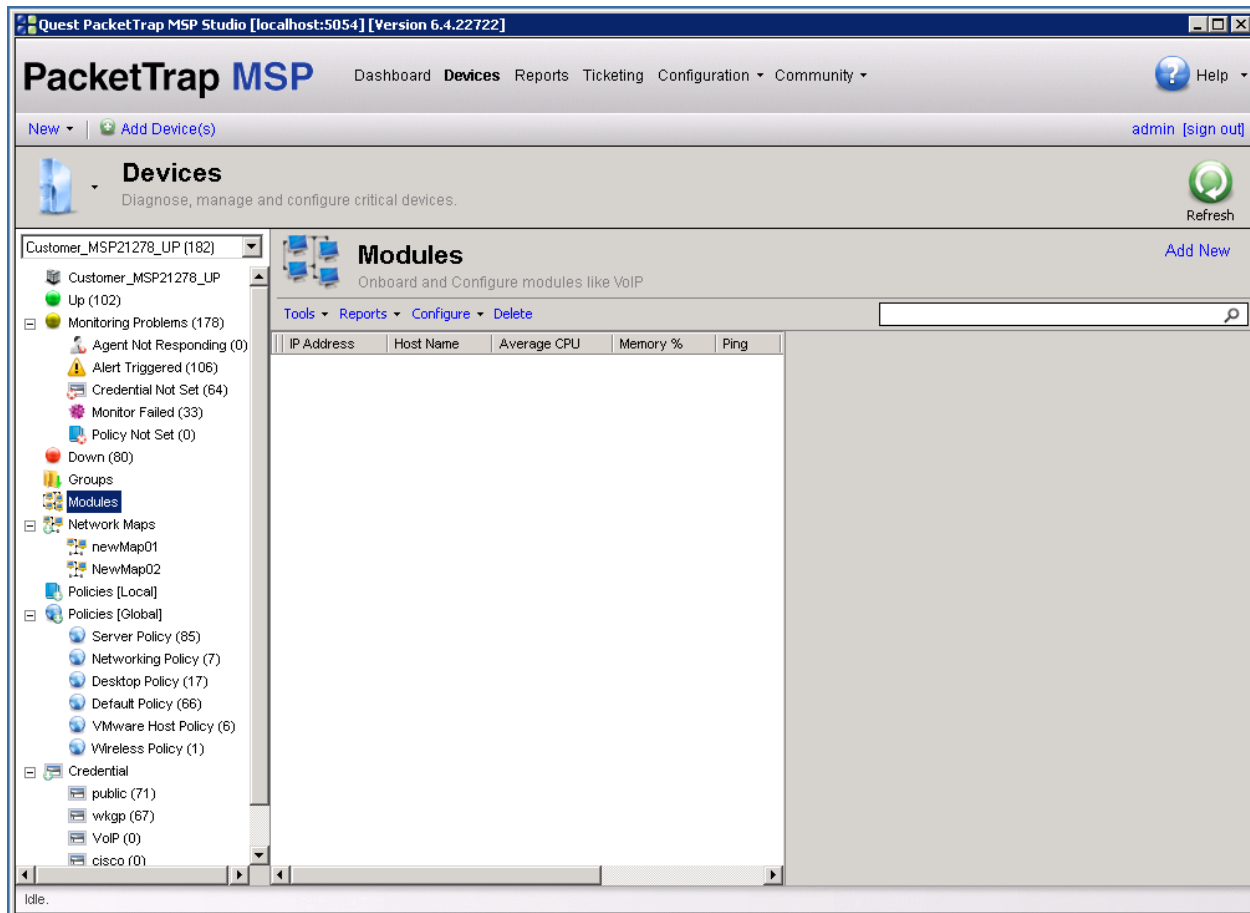
Host And Port:

☐ HTTPS ☒ Save Settings

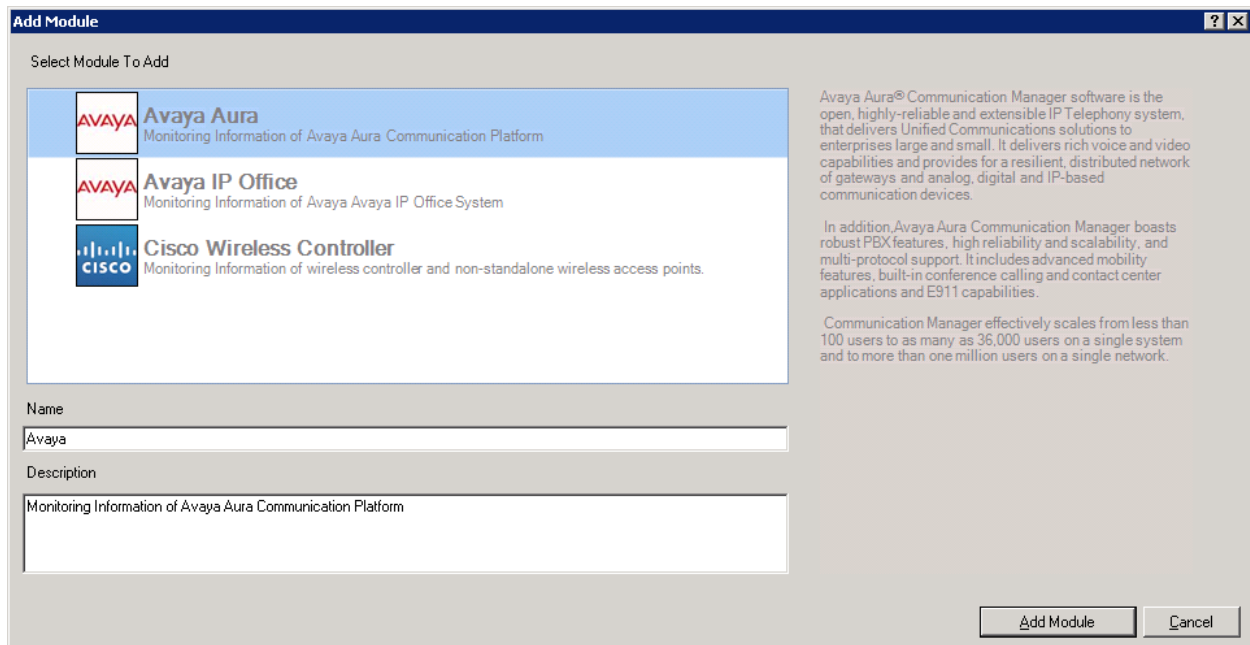
© 2006-2012 Quest Software, All Rights Reserved.



Right mouse click **Modules** from the left pane of the screen, and select **Add New**.



Select **Avaya Aura** from the list of available modules, and select the **Add Module** tab.



The **Add Module** dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled "Select Module To Add". On the left, there is a list of three modules: **Avaya Aura** (Monitoring Information of Avaya Aura Communication Platform), **Avaya IP Office** (Monitoring Information of Avaya IP Office System), and **Cisco Wireless Controller** (Monitoring Information of wireless controller and non-standalone wireless access points). The **Avaya Aura** module is selected. On the right, there is descriptive text about Avaya Aura Communication Manager software. Below the list, there are two text boxes: "Name" (containing "Avaya") and "Description" (containing "Monitoring Information of Avaya Aura Communication Platform"). At the bottom right, there are two buttons: "Add Module" and "Cancel".

**Add Module**

Select Module To Add

**Avaya Aura**  
Monitoring Information of Avaya Aura Communication Platform

**Avaya IP Office**  
Monitoring Information of Avaya IP Office System

**Cisco Wireless Controller**  
Monitoring Information of wireless controller and non-standalone wireless access points.

Avaya Aura® Communication Manager software is the open, highly-reliable and extensible IP Telephony system, that delivers Unified Communications solutions to enterprises large and small. It delivers rich voice and video capabilities and provides for a resilient, distributed network of gateways and analog, digital and IP-based communication devices.

In addition, Avaya Aura Communication Manager boasts robust PBX features, high reliability and scalability, and multi-protocol support. It includes advanced mobility features, built-in conference calling and contact center applications and E911 capabilities.

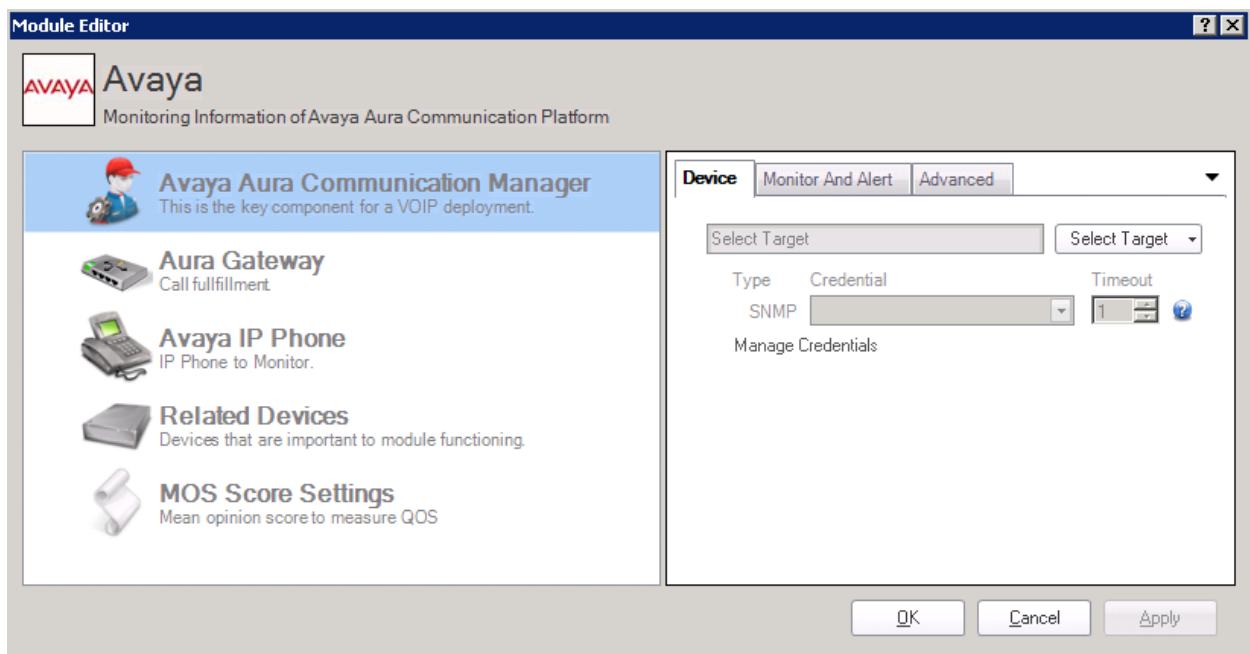
Communication Manager effectively scales from less than 100 users to as many as 36,000 users on a single system and to more than one million users on a single network.

Name  
Avaya

Description  
Monitoring Information of Avaya Aura Communication Platform

**Add Module** **Cancel**

From the Module Editor page, click **Select Target** under the Device menu on the right pane, and select **Add a new device**.



The **Module Editor** dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled "Avaya" (Monitoring Information of Avaya Aura Communication Platform). On the left, there is a list of four modules: **Avaya Aura Communication Manager** (This is the key component for a VOIP deployment), **Aura Gateway** (Call fulfillment), **Avaya IP Phone** (IP Phone to Monitor), and **Related Devices** (Devices that are important to module functioning). The **Avaya Aura Communication Manager** module is selected. On the right, there is a "Device" tab with a dropdown menu. Below the dropdown, there is a "Select Target" button and a "Select Target" dropdown. Below that, there is a "Type" dropdown (set to "SNMP"), a "Credential" dropdown, and a "Timeout" dropdown (set to "1"). Below these, there is a "Manage Credentials" button. At the bottom right, there are three buttons: "OK", "Cancel", and "Apply".

**Module Editor**

**Avaya**  
Monitoring Information of Avaya Aura Communication Platform

**Avaya Aura Communication Manager**  
This is the key component for a VOIP deployment.

**Aura Gateway**  
Call fulfillment

**Avaya IP Phone**  
IP Phone to Monitor.

**Related Devices**  
Devices that are important to module functioning.

**MOS Score Settings**  
Mean opinion score to measure QOS

**Device** Monitor And Alert Advanced

Select Target Select Target

Type Credential Timeout

SNMP 1

Manage Credentials

**OK** **Cancel** **Apply**

From the Add Device Wizard page, enter the IP address of the S8300D and choose the SNMP community string and click **Next**.

**Add Device Avaya Aura Communication Manager - Avaya Aura in Default Site**

**Avaya Aura Communication Manager**  
This is the key component for a VOIP deployment.

**Target(s)**  
10.64.41.21

**Default Site Discovery Agent**  
WORKGROUP\WIN-SVR-2003 [Change](#)  
*Default agent is selected for site.*

☒ Exclude Existing Devices From Discovery  
☒ Ping [advanced](#)  
*Techniques to find prospective devices on the network to add to your device database*

**Credentials**

Type	Credential	Timeout
SNMP	public	10

[Manage Credentials](#)

< Back   Next   Cancel

Select **Finish**.

**Add Device Avaya Aura Communication Manager - Avaya Aura in Default Site**

**Avaya Aura Communication Manager**  
This is the key component for a VOIP deployment.

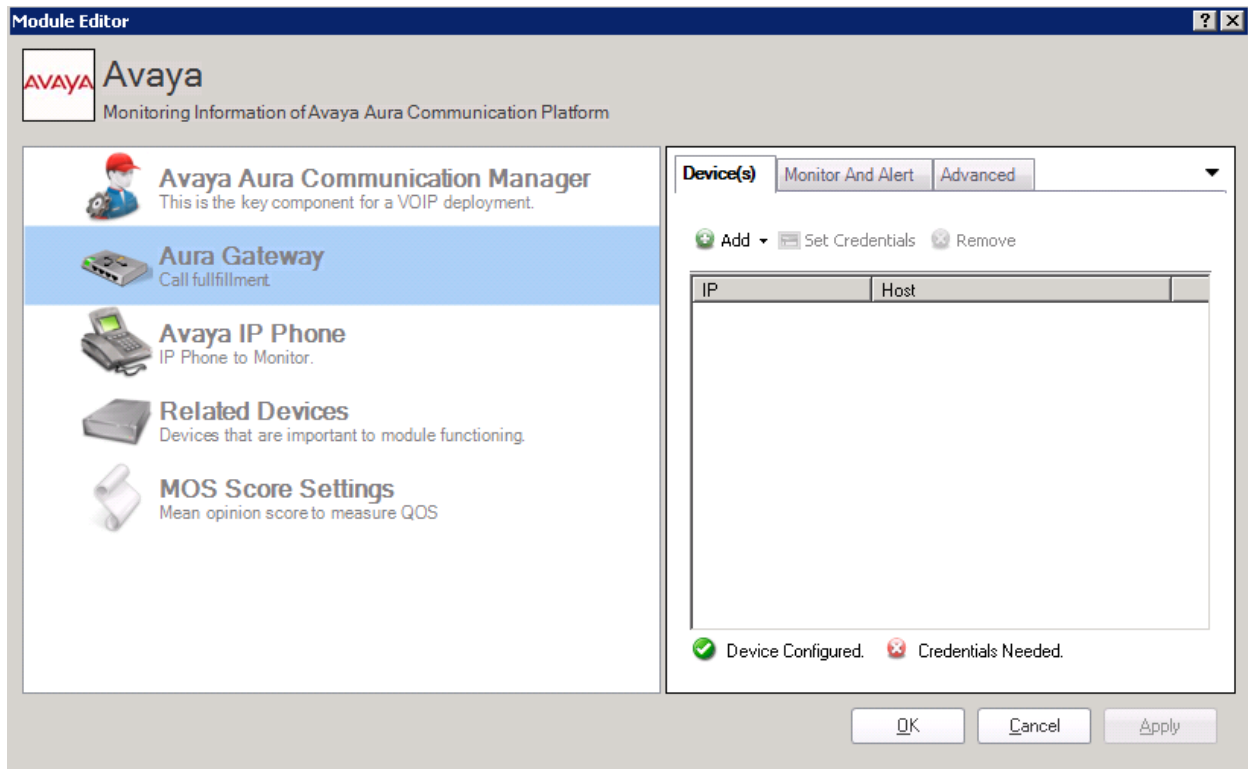
**Running Time:** 0 hours 0 mins 3 secs   [Refresh](#)   [Stop](#)

IP	DNS	Ping	SNMP	Role	Operating System	Vendor
10.64.41.21		1 ms	V2, V1 Responding		Unknown	Avaya Communication

Network Discovery Completed.

< Back   Finish   Cancel

Next chose the Gateway. Click on **Aura Gateway** and select **Add → Add New Device**.



From the Add Device Wizard page, enter the IP address of the G450 gateway and choose the SNMP community string and click **Next**.

**Add Device(s) Aura Gateway - Avaya Aura in Default Site**

**Aura Gateway**  
Call fulfillment

**Target(s)**  
10.64.41.2 [Bulk Entry](#)  
Accepted formats: IPv4: 10.0.0.1, IPv6: fe80:0000:0000:0000:020...

**Default Site Discovery Agent**  
WORKGROUPWIN-SVR-2003 [Change](#)  
Default agent is selected for site.

☒ Exclude Existing Devices From Discovery  
☒ Ping [advanced](#)  
Techniques to find prospective devices on the network to add to your device database

**Credentials**

Type	Credential	Timeout
SNMP	public	10

[Manage Credentials](#)

< Back   Next   Cancel

Select **Finish**.

All Responding (1)   **Running Time:** 0 hours 0 mins 0 secs   [Refresh](#)   [Stop](#)

IP	DNS	Ping	SNMP	Role	Operating System	Vendor
<input checked="" type="checkbox"/> 10.64.41.2		0 ms	V2, V1 Responding	Switch	Unknown	

Network Discovery Completed.   [Back](#)   [Finish](#)   [Cancel](#)

## 7. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of each Avaya Media Server, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that the PacketTrap MSP received the CDR record for the call. Compare the values of data fields in the CDR record with the expected values and verify that the values match.
- Place internal calls to and from various telephones, generate an appropriate RTCP Send Report in the PacketTrap MSP, and verify the report's accuracy.
- Using a network emulator, call latency and packet drop were injected in the network, and results from the network emulator, Avaya IP telephones, and the PacketTrap MSP were compared.

## 8. Conclusion

These Application Notes describe the procedures for configuring Quest Software PacketTrap MSP to collect call detail records and call quality data from Avaya Aura® Communication Manager. The PacketTrap MSP successfully passed all compliance testing.

## 9. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 6.0, Issue 8.0, June 2010, Document Number 555-245-205

[2] *Administering Avaya Aura™ Communication Manager*, Release 6.0 Issue 6.0, June 2010, Document Number 03-300509

The following PacketTrap MSP product documentation is available from Quest Software.

[3] PacketTrap MSP Product Page

<http://www.quest.com/foglight-network-management-system/>

[4] PacketTrap MSP Community

<http://communities.quest.com/community/nms>

[5] PacketTrap MSP Knowledgebase

<http://communities.quest.com/community/nms/knowledgebase>

---

**©2012 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).