Avaya Solution & Interoperability Test Lab

Application Notes for Nectar Unified Communications Management Platform (UCMP) with Avaya IP Office Server Edition - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Nectar Unified Communications Management Platform (UCMP) with Avaya IP Office Server Edition. Nectar UCMP is a proactive health and performance monitor that provides enterprise customers and service providers with a comprehensive view of unified communications environments for monitoring allowing service interruptions to be diagnosed and solved quicker. Nectar UCMP automatically captures Avaya IP Office system inventory, captures and reports alarms/alerts, provides resource utilization information, and delivers real-time RTCP call quality data. Nectar UCMP monitors Avaya IP Office using SNMP traps and polling, RTCP collection, and Service Monitoring Web Services.

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 Unified Communications Management Platform (UCMP) with Avaya IP Office Server Edition. Nectar UCMP is a proactive health and performance monitor that provides enterprise customers and service providers with a comprehensive view of unified communications environments for monitoring allowing service interruptions to be diagnosed and solved quicker. Nectar UCMP automatically captures Avaya IP Office system inventory, captures and reports alarms/alerts, provides resource utilization information, and delivers real-time RTCP call quality data. Nectar UCMP monitors Avaya IP Office using SNMP traps and polling, RTCP collection, and Service Monitoring Web Services.

The Avaya IP Office Server Edition configuration consisted of two Avaya IP Office systems, a primary Linux server and an expansion IP Office 500 V2 that were connected via a Small Community Network (SCN) trunk. In the compliance test, Nectar UCMP monitored each IP Office system.

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 UCMP to monitor Avaya IP Office using SNMP traps and polling, RTCP collection, and Service Monitoring Web Services, and provide resource utilization, system inventory, call quality data, performance alerts in the Nectar Remote Intelligence Gateway (RIG) client.

SNMP traps were generated on IP Office and sent to UCMP. UCMP either displayed these SNMP traps or converted them to alarm/alert conditions and displayed them in the Events log.

SNMP polling and Service Monitoring Web Services were used by UCMP to capture IP Office system inventory. In addition, Service Monitoring Web Services was used to collect resource utilization and status data from IP Office.

RTCP collection was used by UCMP to provide call quality metrics. The general approach was to place calls between Avaya H.323, SIP, and digital phones and injecting errors using a network impairment tool to simulate network delay and packet loss conditions on the LAN.

The serviceability testing focused on verifying that the Nectar UCMP came back into service after re-connecting the Ethernet cable (i.e., restoring network connectivity) and rebooting the UCMP server. This included tracking the Service Monitoring Web Services API connection status.

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 UCMP features and functionality. Alarms/alerts, system inventory, resource utilization and status, and call quality metrics were displayed on the RIG client.

- Collecting and displaying IP Office system inventory (e.g., expansion modules, extensions, internal modules, licenses, system resources, trunks, and voicemail).
- Verifying inventory updates after making changes on IP Office, such as adding/removing extensions.
- Verifying resource utilization and status information (e.g., CPU usage, memory usage, IP office uptime, voicemail status, and conference/data/VCM/RTP channels) as calls were made.
- Capturing SNMP traps and providing performance alerts for system interruptions, such as loss of trunk service.
- Tracking the registration status of Avaya H.323, SIP, and digital deskphones via Extension Monitoring.
- Generating alarm conditions and verifying that the Nectar Dependency Trees were correctly updated.
- Capturing RTCP data and providing call quality metrics.
- Verifying proper system recovery after a restart of the UCMP server and loss of IP network connectivity.

Note: A separate IP Office Voicemail Pro server was not monitored by UCMP, because the integrated voicemail system in IP Office Server Edition was used instead.

2.2. Test Results

The compliance test passed with the following observations:

- In the **Dashboard** of the RIG client, gauges for SM Trunks and SIP Trunks may be errantly displayed when monitoring those licenses. This has been corrected in UCMP 8.2.

- In the **Real-Time QoS** window of the RIG client, there is no call path information for Avaya J129 SIP Deskphones, because they don't provide call path information to UCMP during call setup. In addition, the endpoint name may be displayed as *unknown*, intermittently. However, the SIP extension is correctly displayed to allow mapping to the appropriate endpoint/user.

- In the UCMP inventory report of the RIG client, the admin state for SCN trunks and the status for Centralized Voicemail are displayed as *Undefined (0)*.

- Alarms and SCN Peers sections are displayed in the UCMP inventory report, but the content will be available in a future release.

2.3. Support

For technical support and information on Nectar UCMP, contact UC Support and Technical Assistance at:

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

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Nectar UCMP with Avaya IP Office Server Edition and an Avaya IP Office 500 V2 Expansion System. Nectar UCMP monitored each IP Office system using SNMP, RTCP, and Service Monitoring Web Services. The Nectar RIG client was used to display alarm/alert conditions, system inventory, resource utilization and status, and call quality metrics.

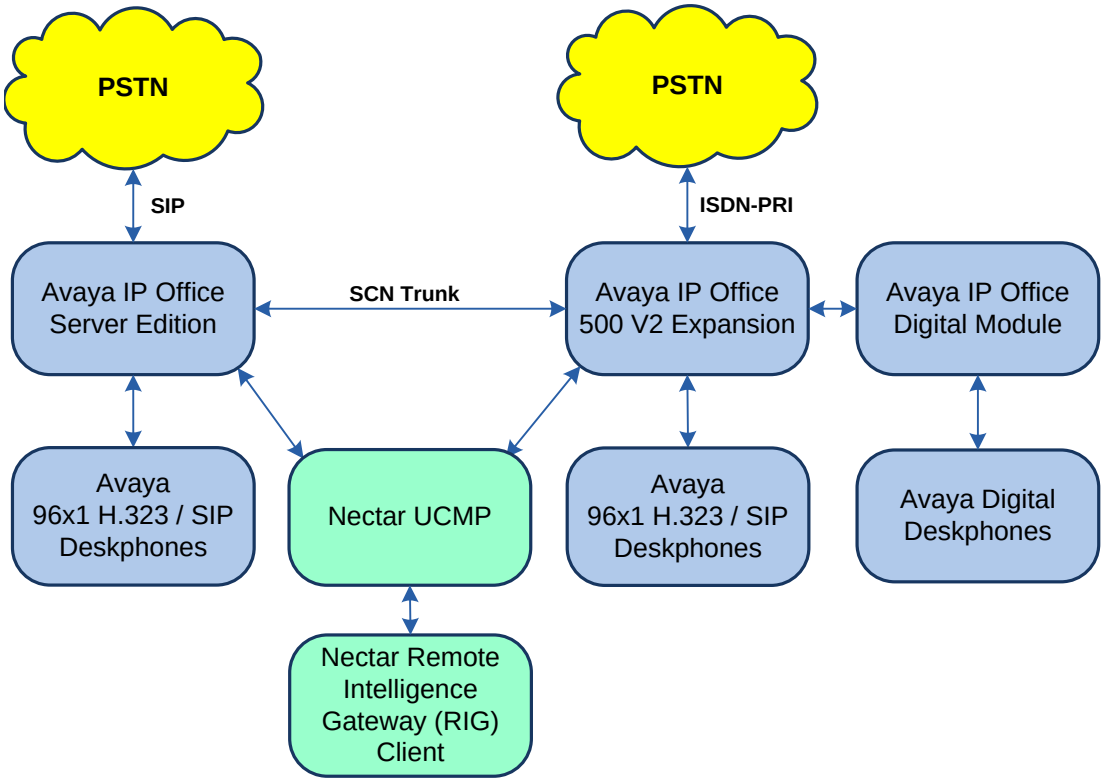


Figure 1: Nectar UCMP with Avaya IP Office Server Edition and Avaya IP Office 500 V2 Expansion

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition	11.0.4.0.0 build 74 and 11.0.4.0.47 build 1 (Critical Patch)
Avaya IP Office 500 V2 Expansion System	11.0.4.0.0 build 74 and 11.0.4.0.47 build 1 (Critical Patch)
Avaya IP Office Digital Module	11.0.4.0.0 build 74
Avaya 96x1 Series IP Deskphones	6.8002 (H.323)
Avaya J129 Deskphone	4.0.0.0.21 (21)
Avaya 1120E IP Deskphone	SIP 1120e.04.04.26.00
Avaya 1220 IP Deskphone	SIP 12x0.04.04.26.00
Avaya 9508 Digital Deskphones	0.60
Nectar Unified Communications Management Platform (UCMP)	8.1.0.2-26112
Nectar Remote Intelligence Gateway (RIG) Client	8.1.0.2-26022

Note: These Application Notes are applicable when the solution is deployed with IP Office Server Edition in all configurations and with a standalone IP Office 500 V2.

5. Configure Avaya IP Office Server Edition

This section provides the procedures to configure Avaya IP Office Server Edition for monitoring and management by UCMP. The procedures include the following areas:

- Configure Service Monitoring Web Services
- Configure SNMP
- Configure RTCP

Note: This section covers the configuration of Avaya IP Office Server Edition, but the configuration is the same for the Avaya IP Office 500 V2 Expansion System.

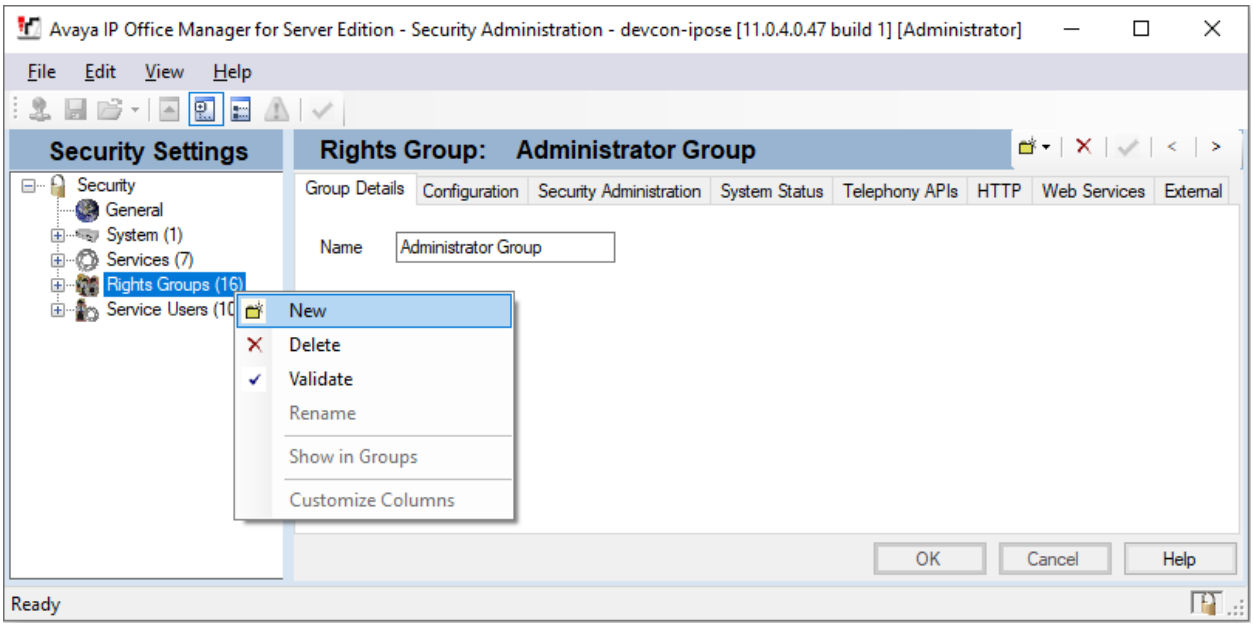
5.1. Configure Service Monitoring Web Services

A Service User must be configured to provide UCMP access to the API. A specific Rights Group and User with minimum permissions (just this API) should be created for use by UCMP.

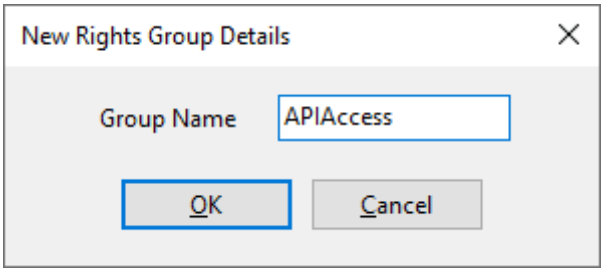
Note: This interface doesn't require a license on IP Office to enable its operation.

5.1.1. Create a Rights Group

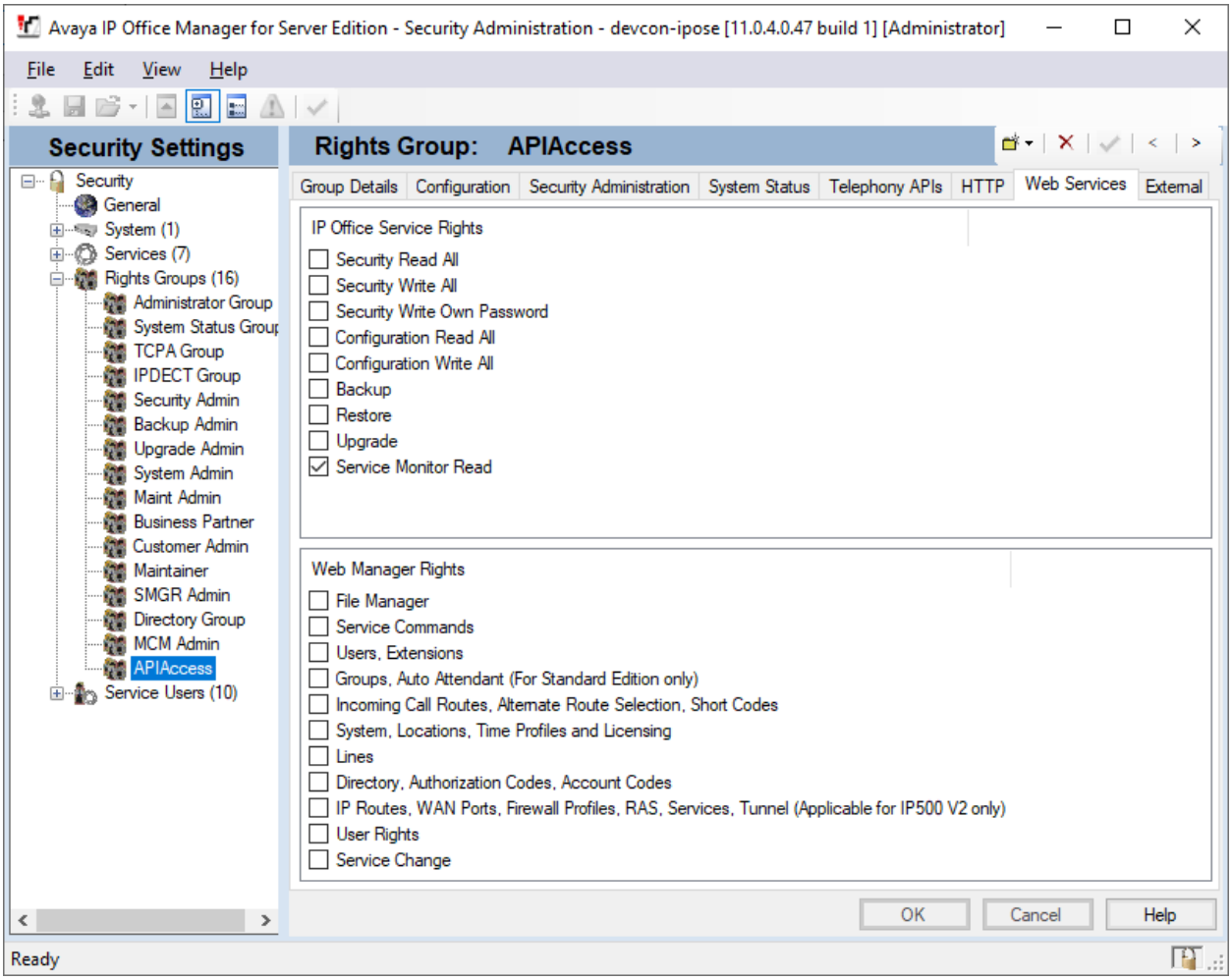
From IP Office Manager, navigate to **File → Advanced → Security Settings** to display the Security Settings as shown below. In **Security Settings**, right-click on **Rights Groups** and select **New** to create a new Rights Group.



In the **New Rights Group Details** dialog box, create a new Rights Group called *APIAccess*.

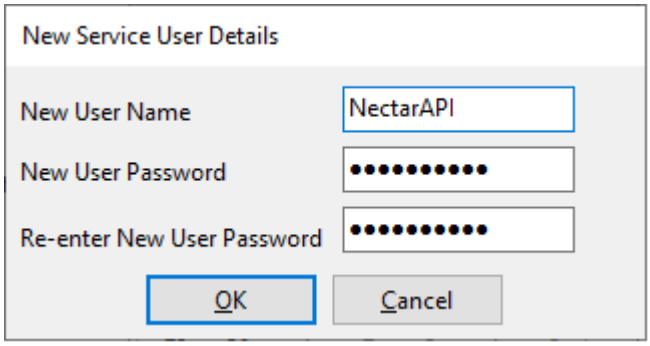


Click on the newly created *APIAccess* Rights Group. Select the **Web Services** tab and enable *Service Monitor Read* as shown below.

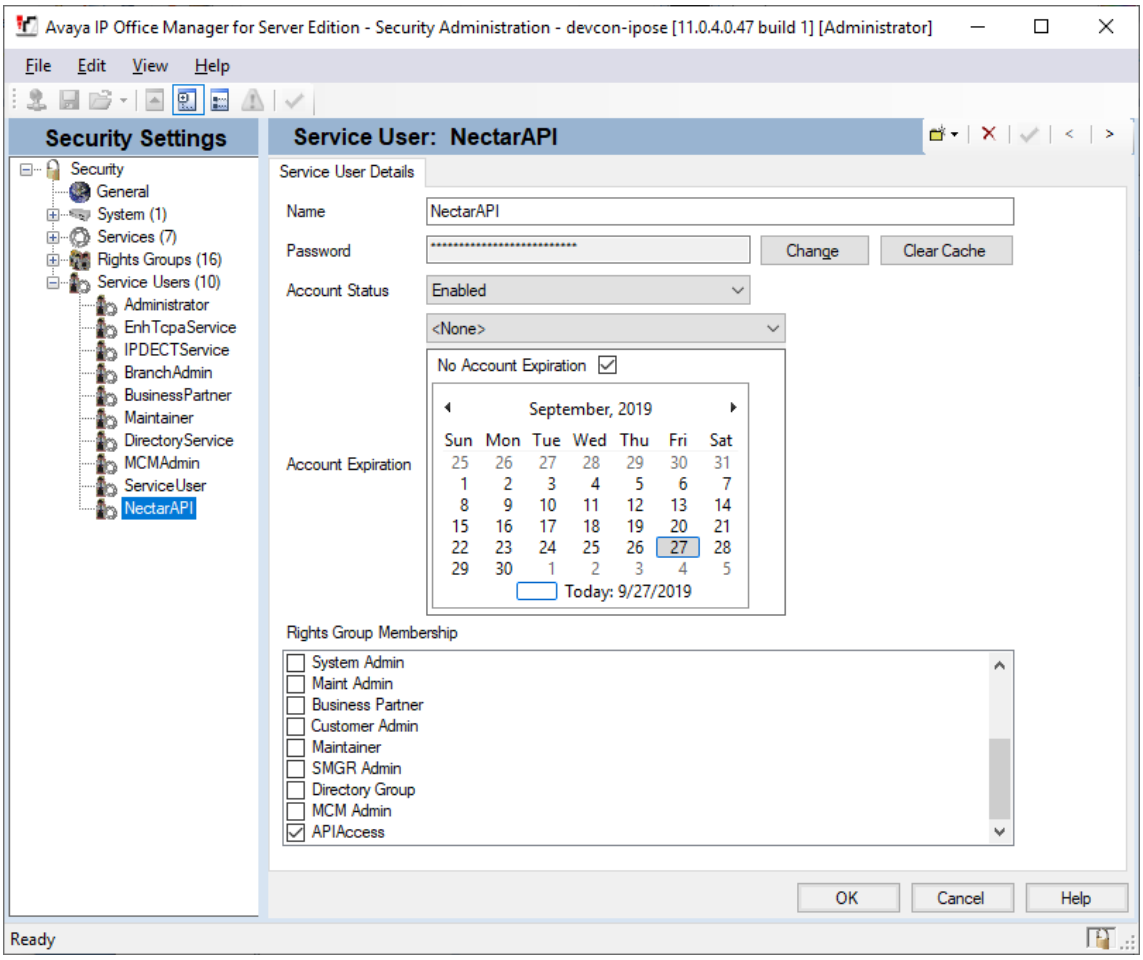


5.1.2. Create a Service User

In **Security Settings**, right-click on **Service Users** and select **New** to create a new Service User called *NectarAPI*. Enter a password for this account as shown below.



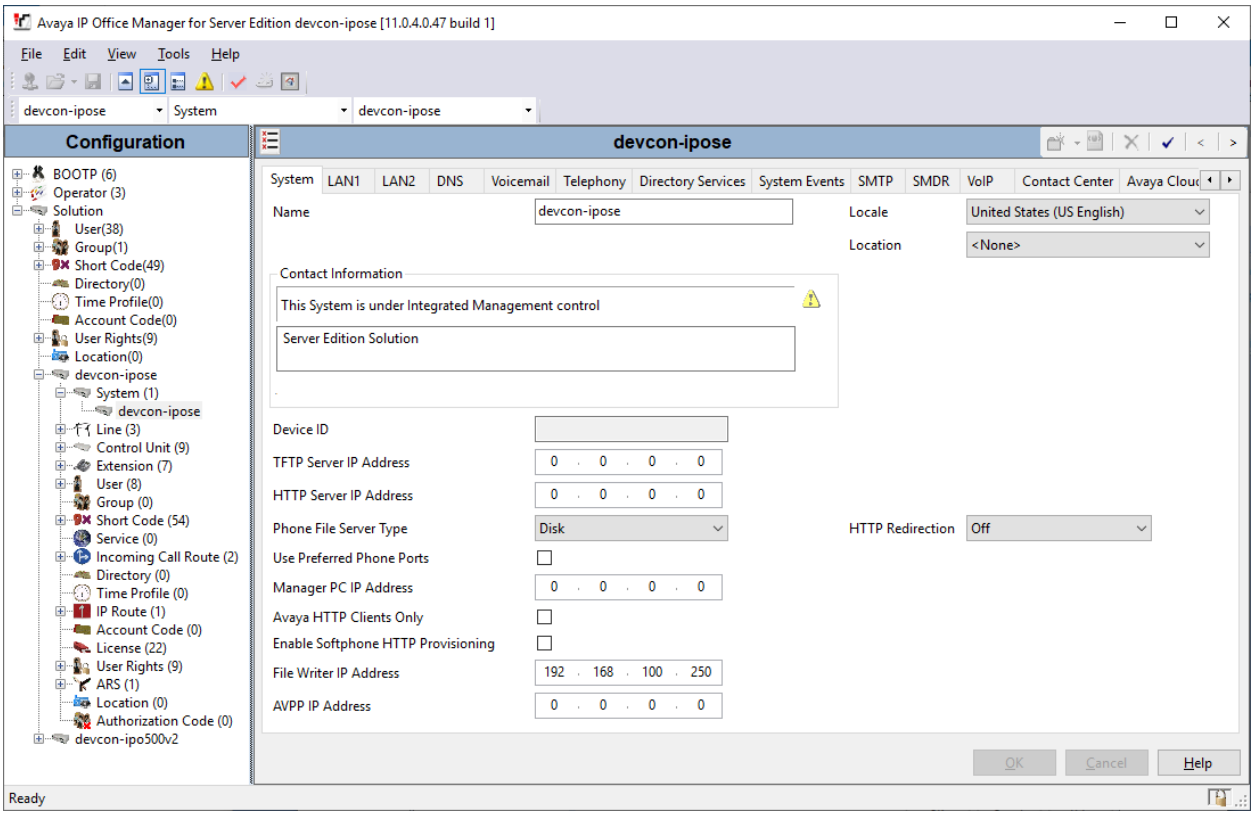
Click on the new created *NectarAPI* User. Confirm that **Account Status** is *Enabled*. In the **Rights Group Membership** section, select *APIAccess*. Click **OK** at the bottom of the screen to commit the changes. Save the **Security Settings** with the disk icon at the upper left.



5.1.3. HTTP/HTTPS Client Restriction

IP Office can be configured to only respond to HTTP/HTTPS requests from recognized Avaya devices. In order for UCMP to access the API, this setting must be disabled.

1. Navigate back to the configuration within IP Office Manager (**File → Configuration**).
2. Select **System** in the left pane followed by the **System** tab in right pane.
3. Uncheck or confirm the box for **Avaya HTTP Clients Only** is unchecked.



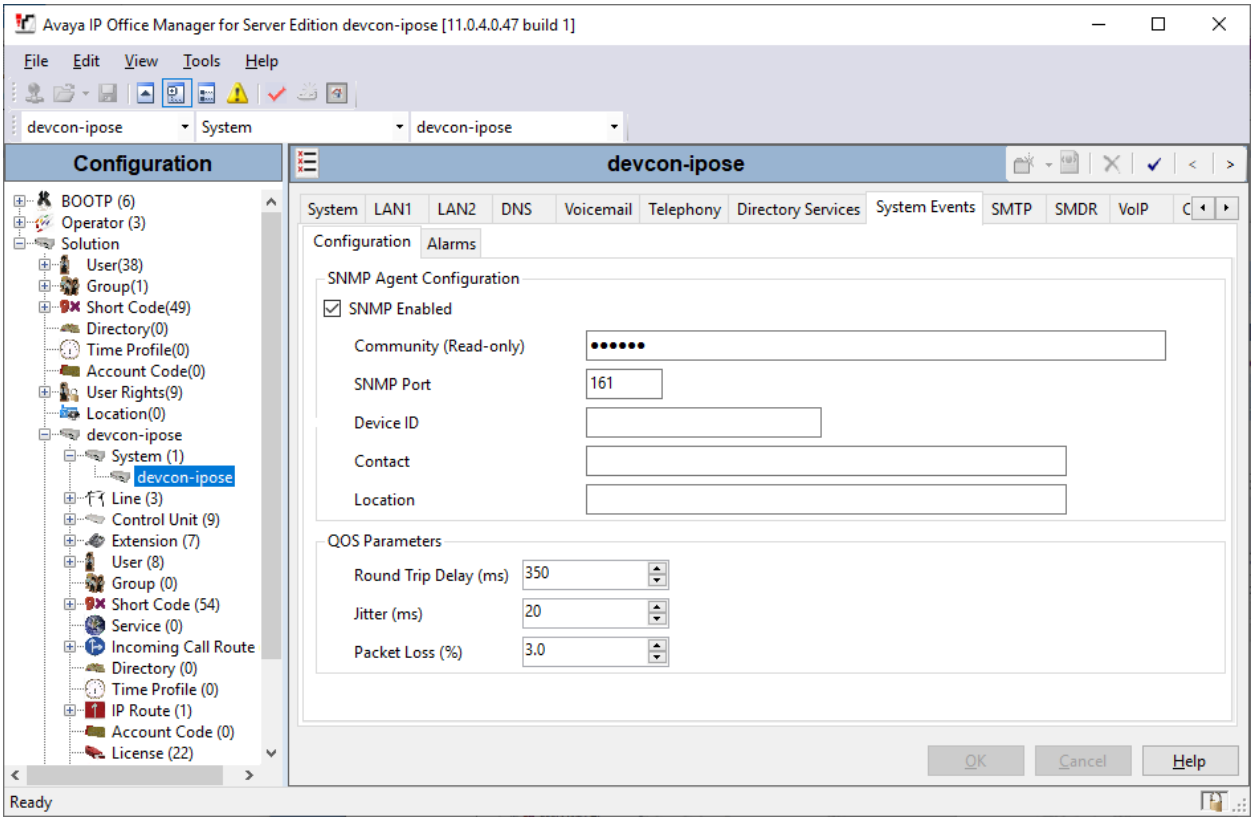
5.2. Configure SNMP

This section covers the configuration of SNMP polling and traps. In addition, the SNMP firewall setting is configured for IP Office 500 V2 Expansion System.

5.2.1. Configure SNMP Polling

To allow SNMP polling, specify the SNMP community string as follows:

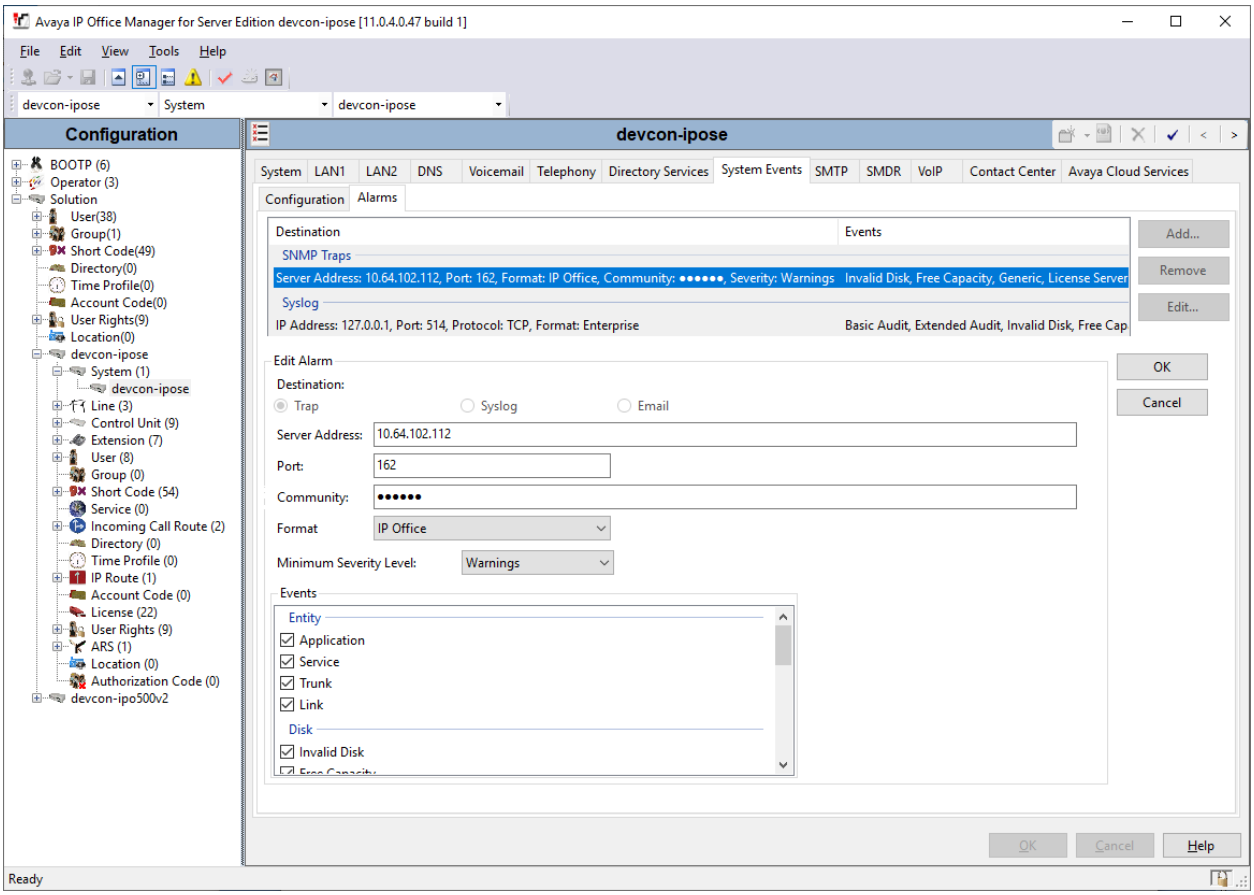
1. Select **System** in the left pane and then navigate to the **System Events → Configuration** tab.
2. Confirm that **SNMP Enabled** is checked.
3. Enter the **Community (Read-only)** string and confirm that **SNMP Port** is *161*.



5.2.2. Configure SNMP Traps

To enable SNMP traps, specify the SNMP trap destination as follows:

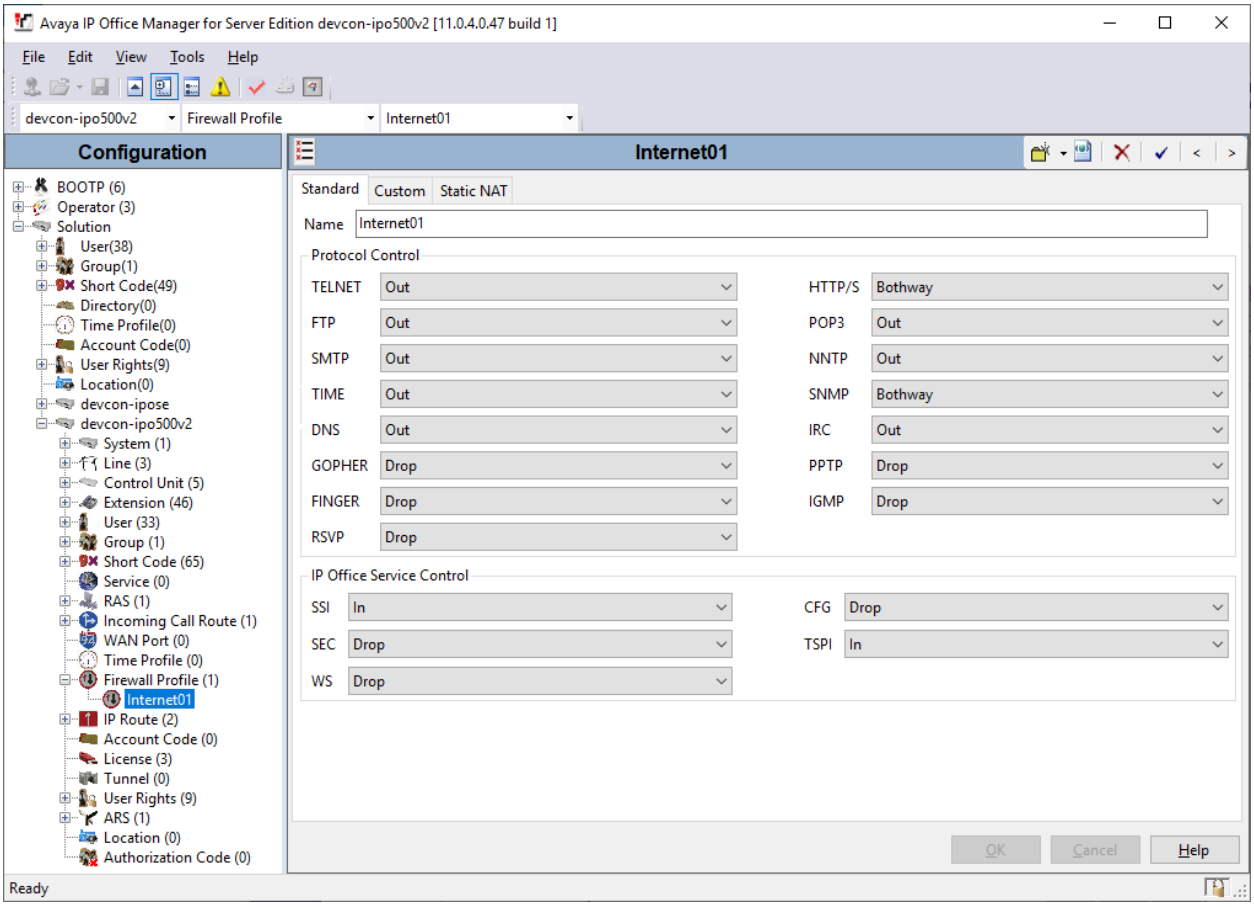
1. Navigate to **System Events** → A**larms** tab and click **Add**.
2. Select the **Trap** radio button.
3. Set **Server Address** to the IP address of the UCMP server (i.e., *10.64.102.112*).
4. Enter the SNMP **Community** (e.g., *NectarCMPr*).
5. Under **Events**, select all the check boxes (Note that the list extends off the screen).



5.2.3. Configure Firewall Settings (for IP Office 500 V2 Expansion only)

Configure the SNMP firewall setting as follows:

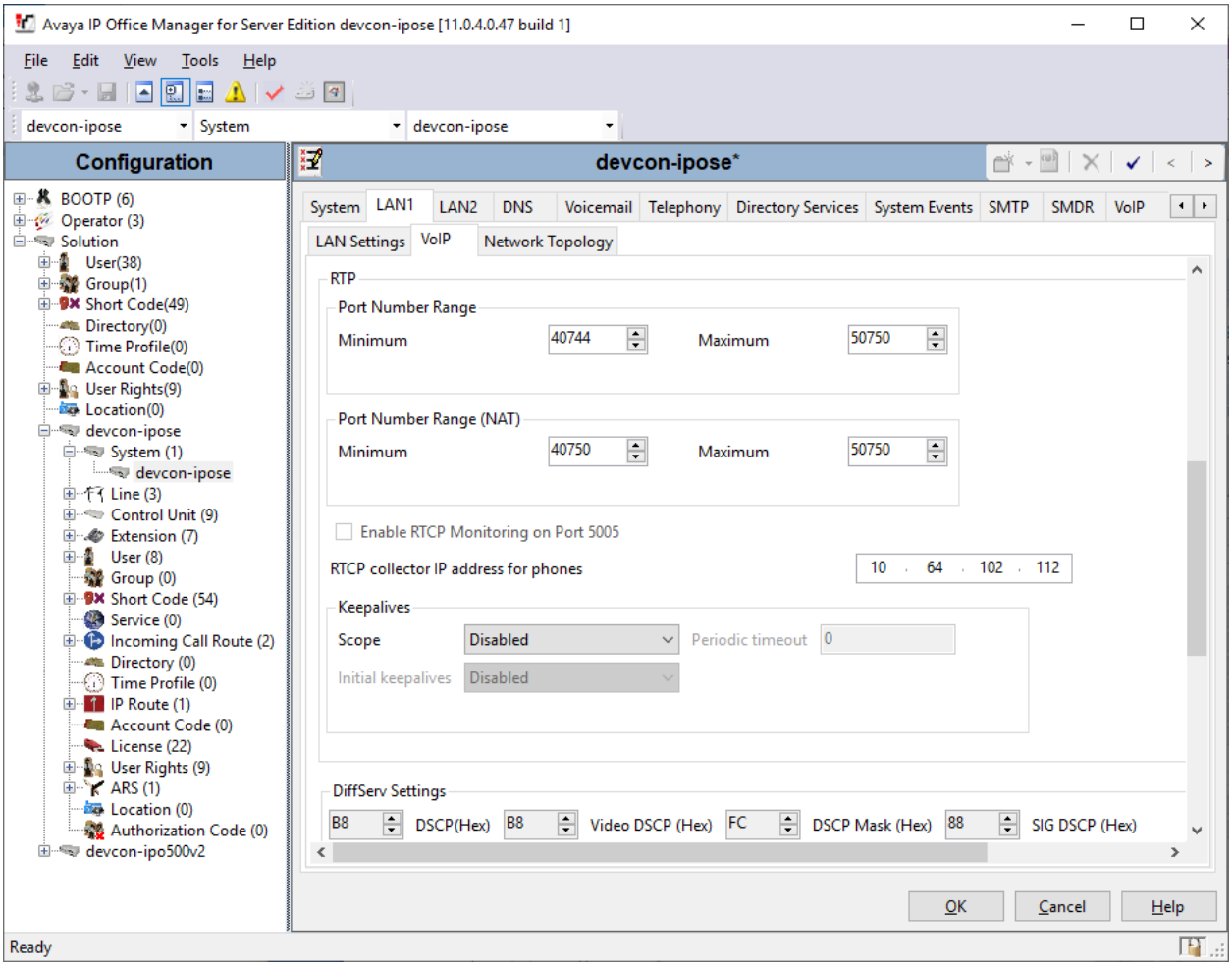
1. Select **Firewall Profile** in the left-hand pane.
2. In the **SNMP** field, select *Bothway* from the drop-down menu.



5.3. Configure RTCP

This section covers the configuration of RTCP for UCMP Real-Time QoS monitoring.

1. From IP Office Manager, select **System** in the left pane and then navigate to the **LAN1** tab, followed by **VoIP**.
2. Under RTP, set the **RTCP collector IP address for phones** field to the UCMP IP address.



6. Configure Nectar Unified Communications Management Platform (UCMP)

This section covers the configuration of UCMP to monitor and manage IP Office Server Edition. Refer to **[3]** for more information on configuring Nectar UCMP. The configuration was performed via the **RIG client**. The procedure covers the following areas:

- Launch the RIG Client
- Configure Service Monitoring Web Services
- Configure SNMP Polling
- Configure Real-Time Quality Monitoring
- Enable Phone Alarms
- Enable License Monitoring

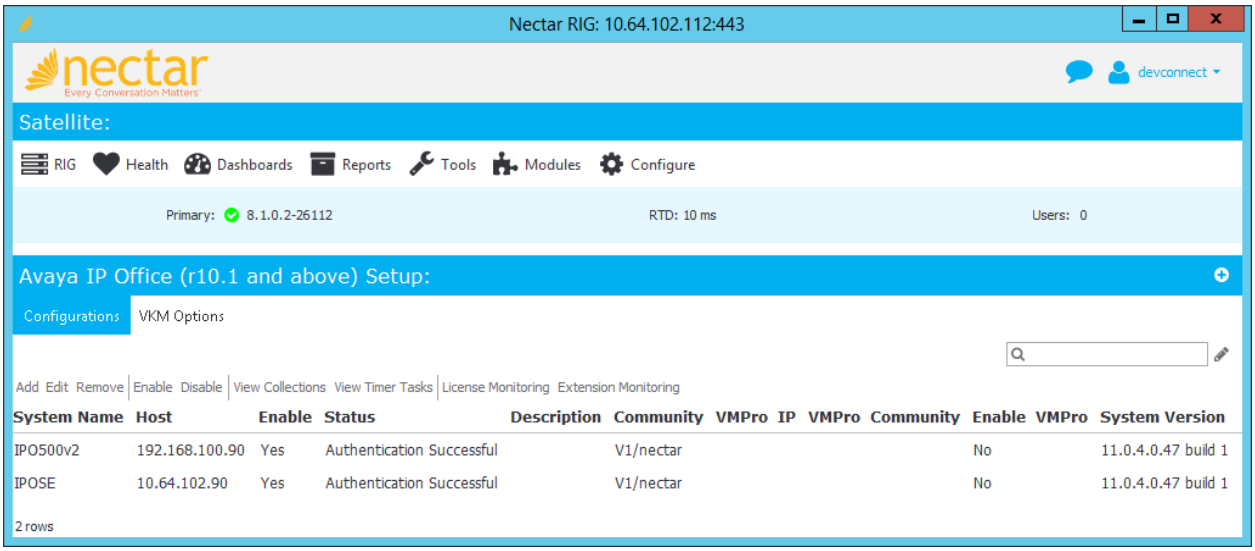
Note: This section covers the Nectar UCMP configuration for Avaya IP Office Server Edition, but the configuration is the same for the Avaya IP Office 500 V2 Expansion System. Also, note that a separate IP Office Voicemail Pro server was not monitored, because the integrated voicemail system in IP Office Server Edition was used.

6.1. Launch the RIG Client

In an Internet browser, enter the UCMP 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**.

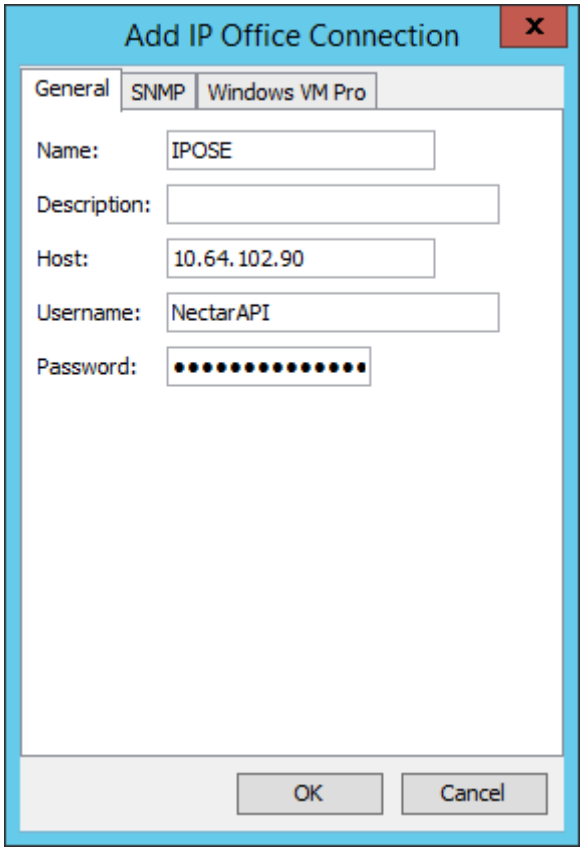
6.2. Configure Service Monitoring Web Services

Navigate to **Modules → Avaya → IP Office (r10.1 and above)** and click **Add** to add an IP Office connection.



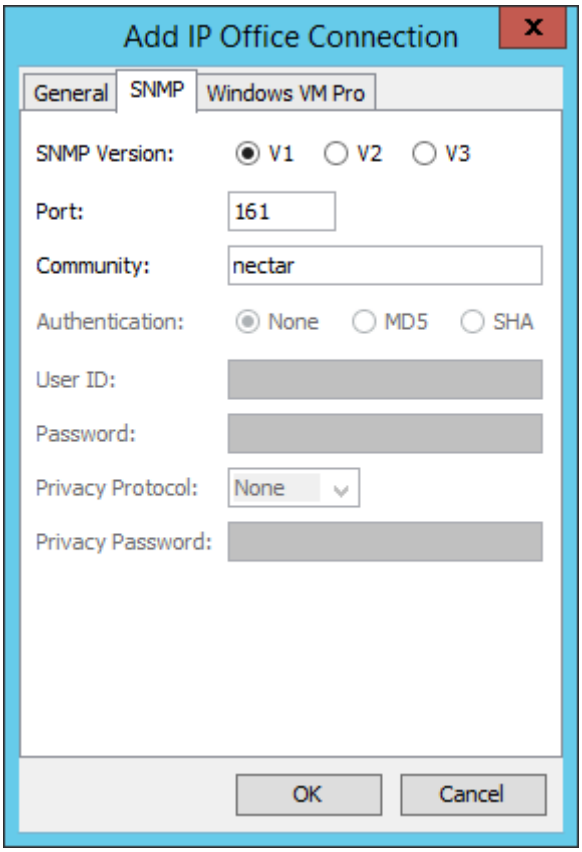
The **Add IP Office Connection** dialog window is displayed as shown below. Configure the following fields:

- **Name:** Enter the name of the IP Office system (e.g., *IPOSE*).
- **Host:** Enter the IP address of the IP Office system (e.g., *10.64.102.90*).
- **Username:** Enter the user name of the **Service User** (i.e., *NectarAPI*) configured in **Section 5.1.2**.
- **Password:** Enter the password of the **Service User** configured in **Section 5.1.2**.



6.3. Configure SNMP Polling

In the **SNMP** tab of the **Add IP Office Connection** dialog window, select the **SNMP Version** (e.g., *V1*), set the **Port** to *161*, and specify the **Community** string as configured in **Section 5.2.1**.

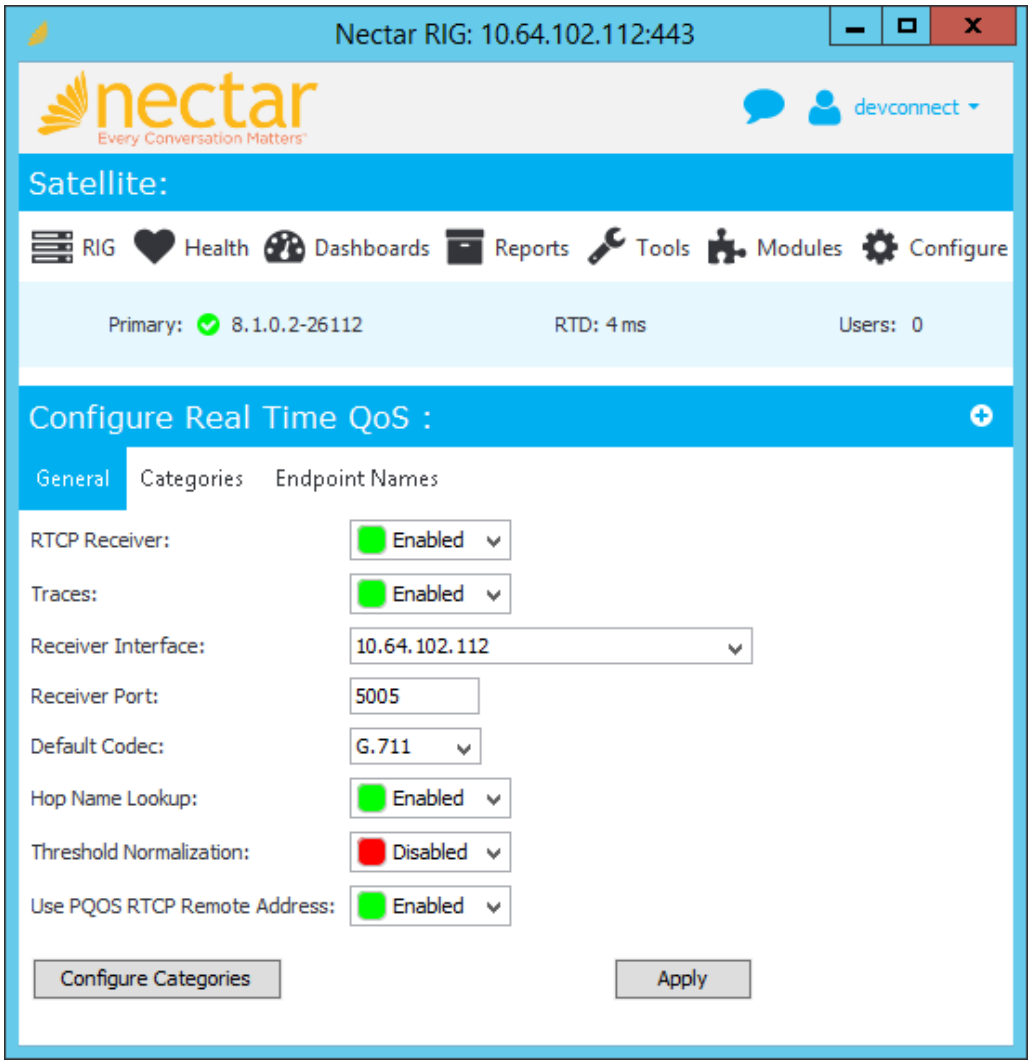


6.4. Configure Real-Time Quality Monitoring

Navigate to **Configure → Quality Management → Real Time QoS** and configure the following fields:

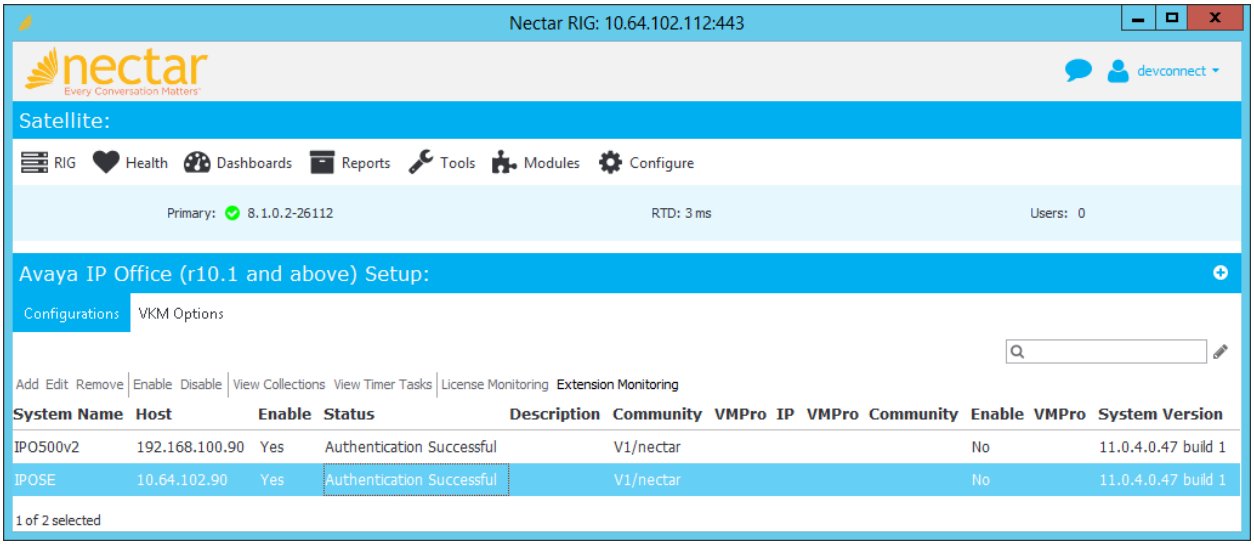
- **RTCP Receiver:** Set to *Enabled*.
- **Traces:** Set to *Enabled*.
- **Receiver Interface:** Set to the UCMP IP address (e.g., *10.64.102.112*).
- **Receiver Port:** Set to *5005*.
- **Default Codec:** Set to *G.711*.
- **Hop Name Lookup:** Set to *Enabled*.
- **Use PQOS RTCP Remote Address:** Set to *Enabled*.

Click **Apply** to start the **RTCP Receiver**.

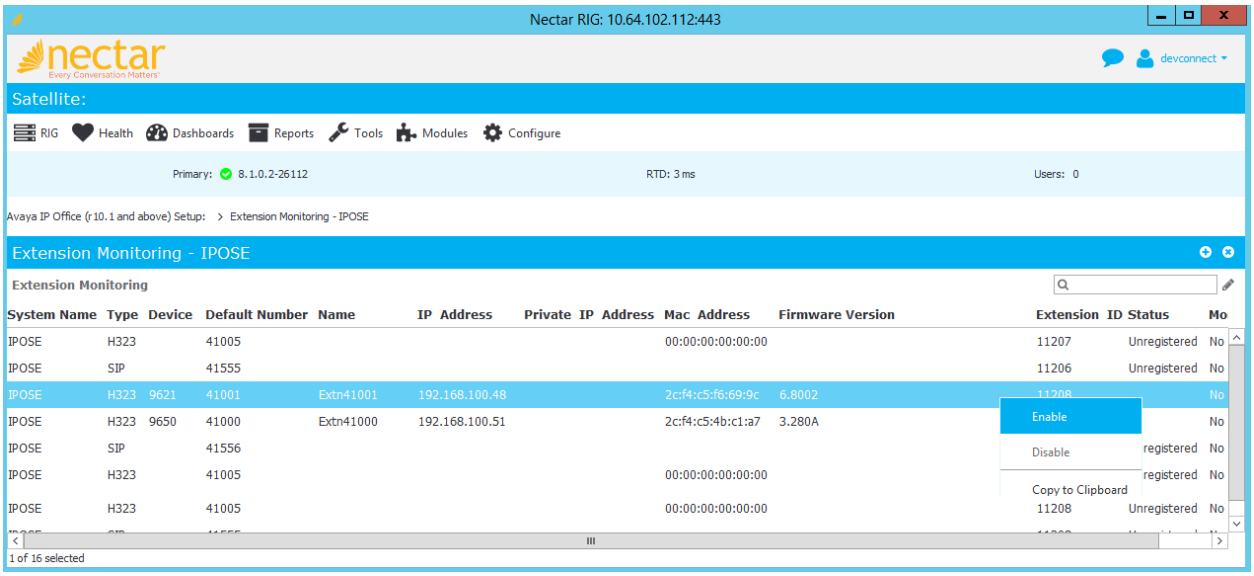


6.5. Enable Phone Alarms

To monitor the registration status of individual stations in the underlying **Dependency Tree**, navigate to **Modules → Avaya → IP Office (r10.1 and above)**. In the **Avaya IP Office (r10.1 and above) Setup** window shown below, select the desired system, and then click **Extension Monitoring**.

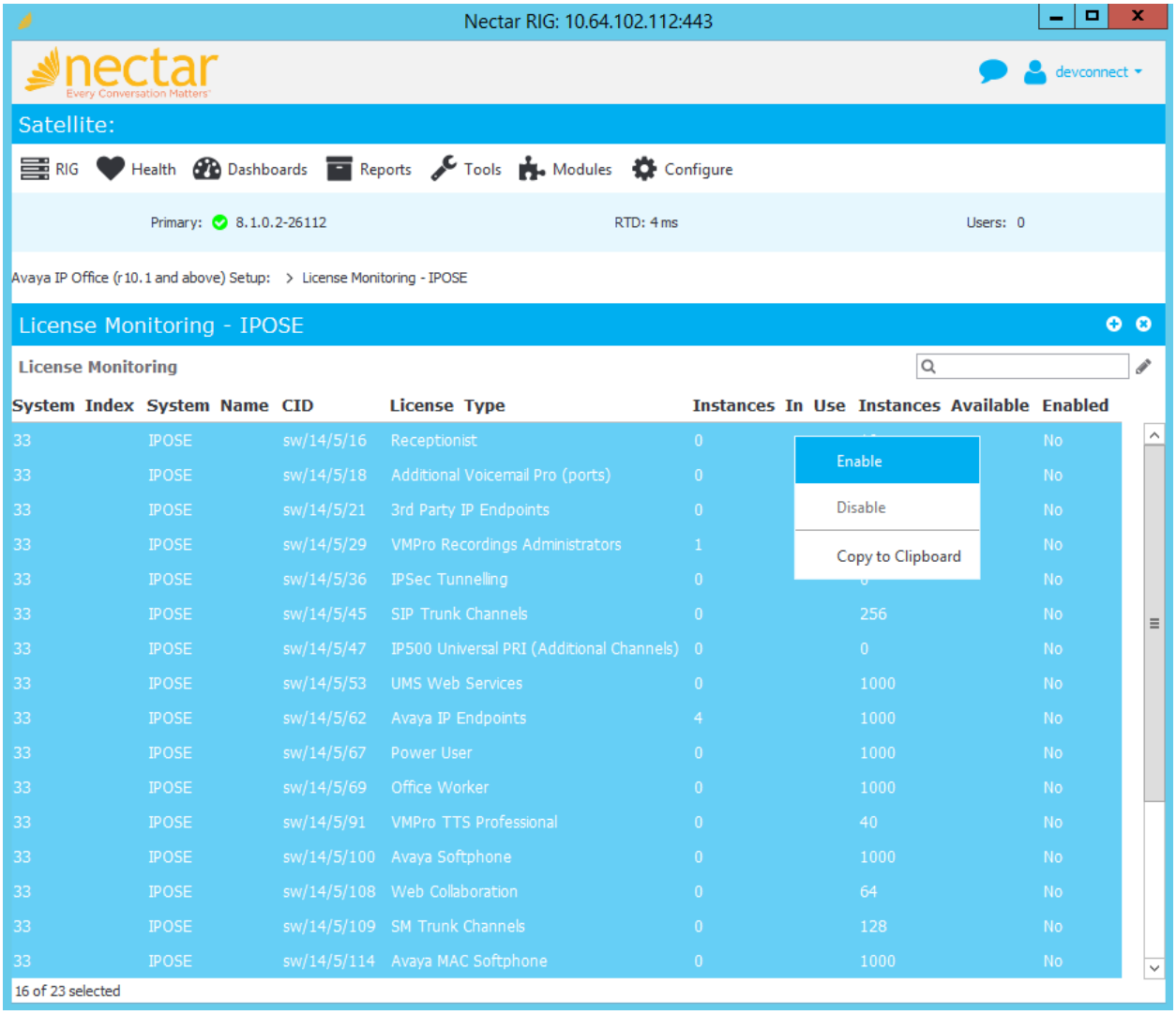


The **Extension Monitoring** window is displayed as shown below with a list of extensions. Right-click on the extension to monitor and select **Enable** as shown below.



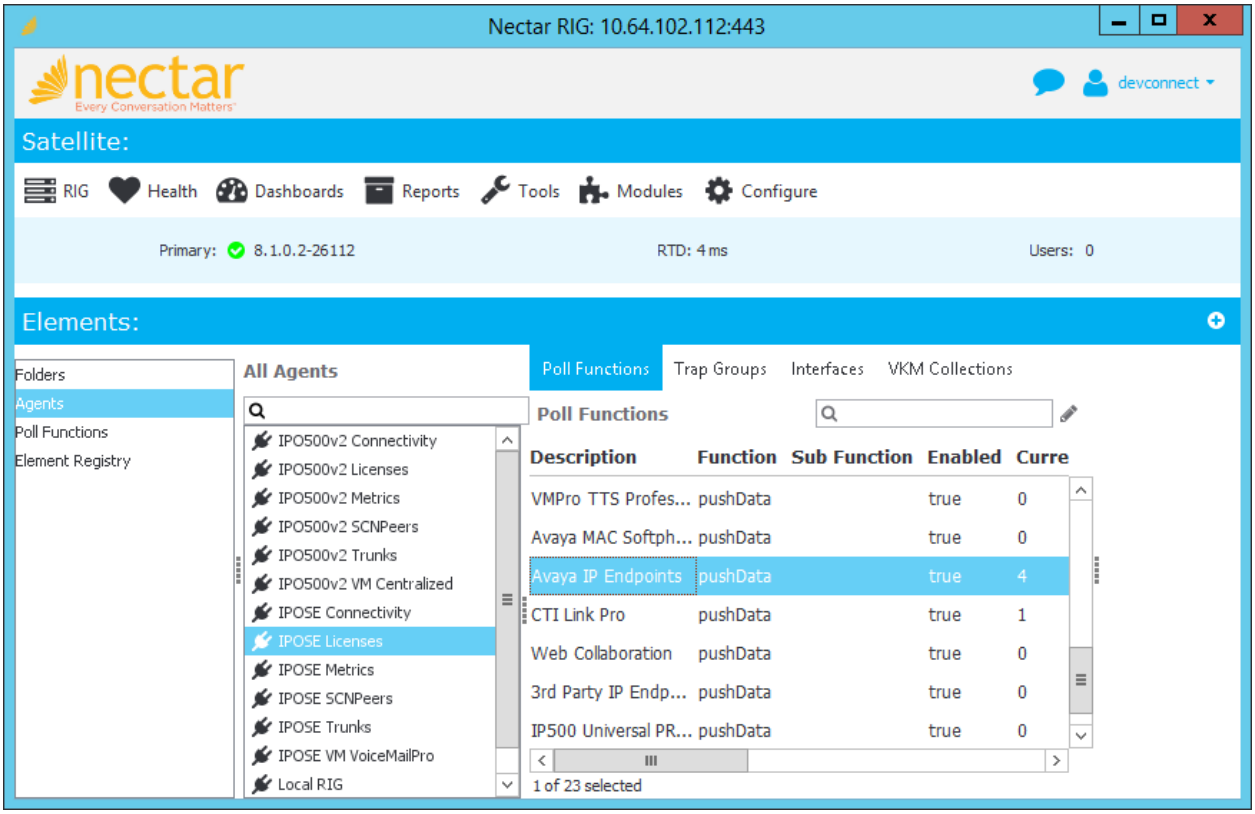
6.6. Enable License Monitoring

From the **Avaya IP Office (r10.1 and above) Setup** window, select the desired system and then click on **License Monitoring**. Select the license to monitor, then right-click and select **Enable** as shown below. In the following example, all licenses were monitored.

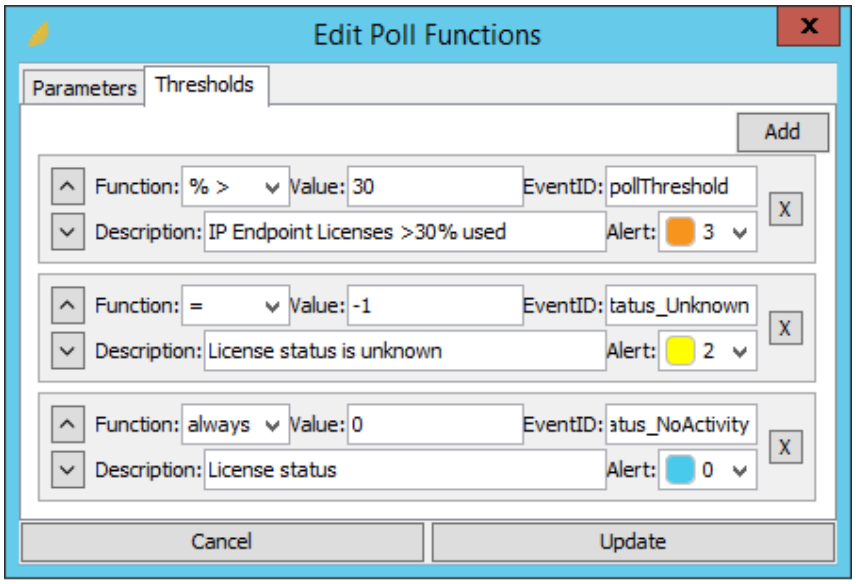


System Index	System Name	CID	License Type	Instances	In Use	Instances Available	Enabled
33	IPOSE	sw/14/5/16	Receptionist	0			No
33	IPOSE	sw/14/5/18	Additional Voicemail Pro (ports)	0			No
33	IPOSE	sw/14/5/21	3rd Party IP Endpoints	0			No
33	IPOSE	sw/14/5/29	VMPro Recordings Administrators	1			No
33	IPOSE	sw/14/5/36	IPSec Tunnelling	0			No
33	IPOSE	sw/14/5/45	SIP Trunk Channels	0		256	No
33	IPOSE	sw/14/5/47	IP500 Universal PRI (Additional Channels)	0		0	No
33	IPOSE	sw/14/5/53	UMS Web Services	0		1000	No
33	IPOSE	sw/14/5/62	Avaya IP Endpoints	4		1000	No
33	IPOSE	sw/14/5/67	Power User	0		1000	No
33	IPOSE	sw/14/5/69	Office Worker	0		1000	No
33	IPOSE	sw/14/5/91	VMPro TTS Professional	0		40	No
33	IPOSE	sw/14/5/100	Avaya Softphone	0		1000	No
33	IPOSE	sw/14/5/108	Web Collaboration	0		64	No
33	IPOSE	sw/14/5/109	SM Trunk Channels	0		128	No
33	IPOSE	sw/14/5/114	Avaya MAC Softphone	0		1000	No

Navigate to **Health → Elements → Agents → IPOSE Licenses** and then select a license (e.g., *Avaya IP Endpoints*) to highlight it for which a threshold is to be added or edited. Right-mouse click on the license and select **Edit**.



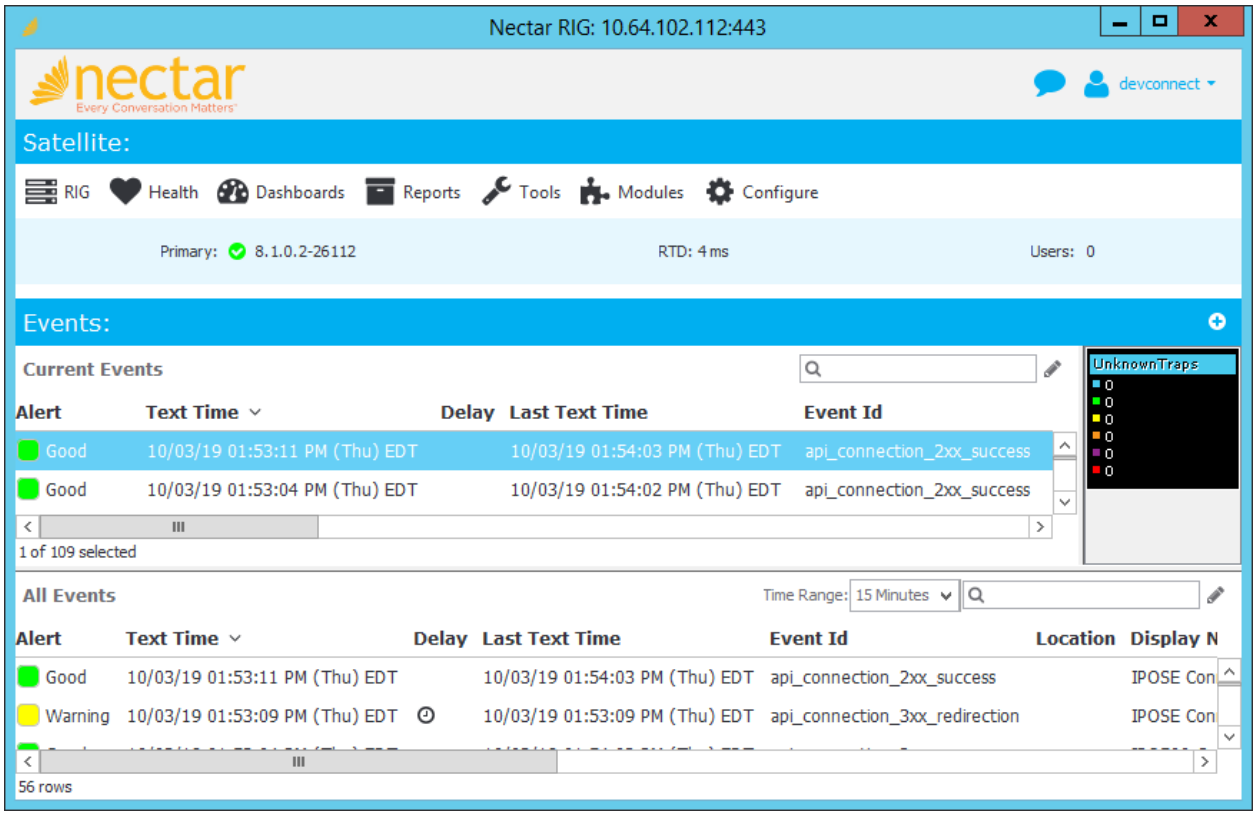
The **Edit Poll Functions** dialog window is displayed. Select the **Thresholds** tab, then click **Add** to add the desired threshold (see examples below). Click **Update** when done.



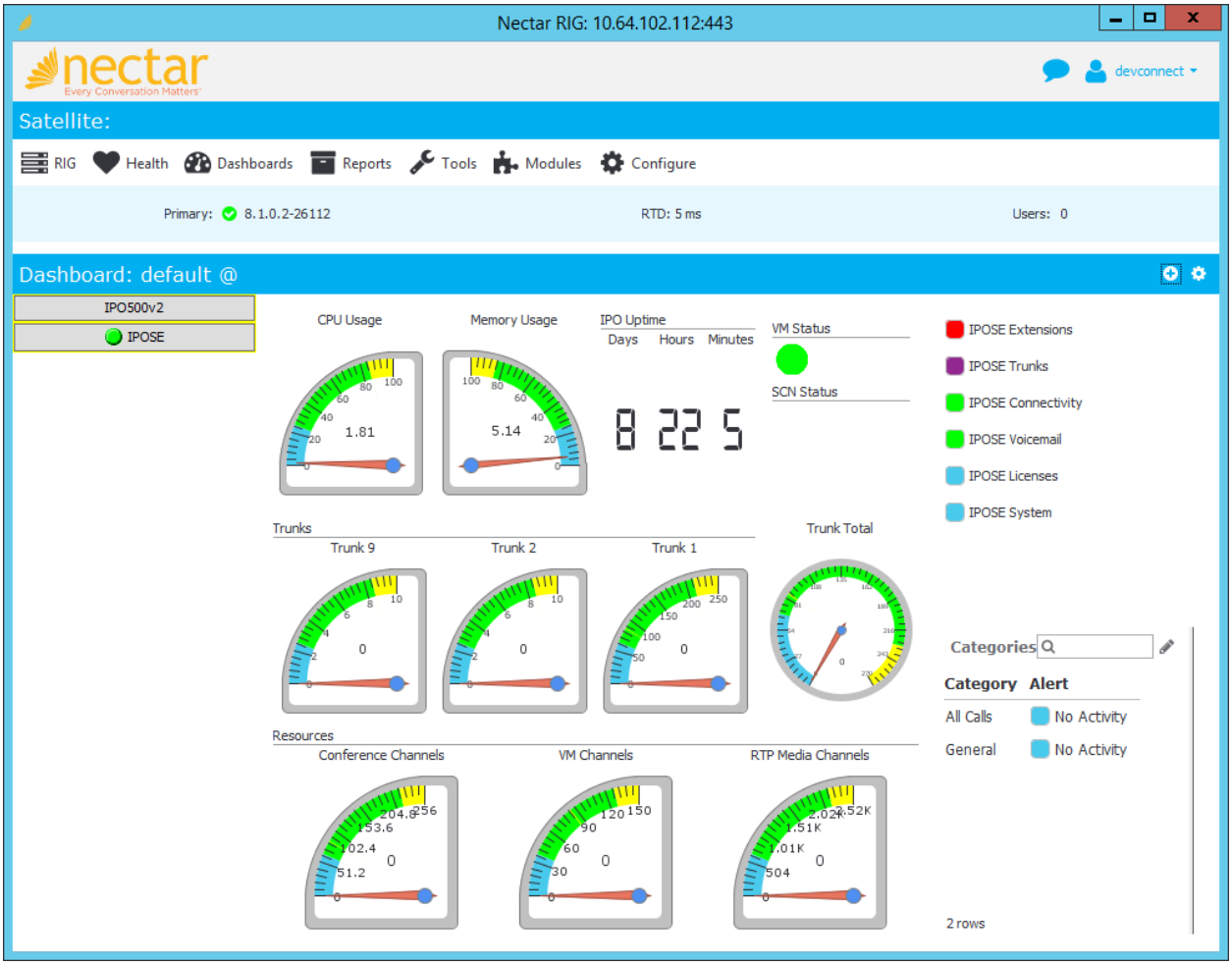
7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Nectar UCMP with Avaya IP Office Server Edition.

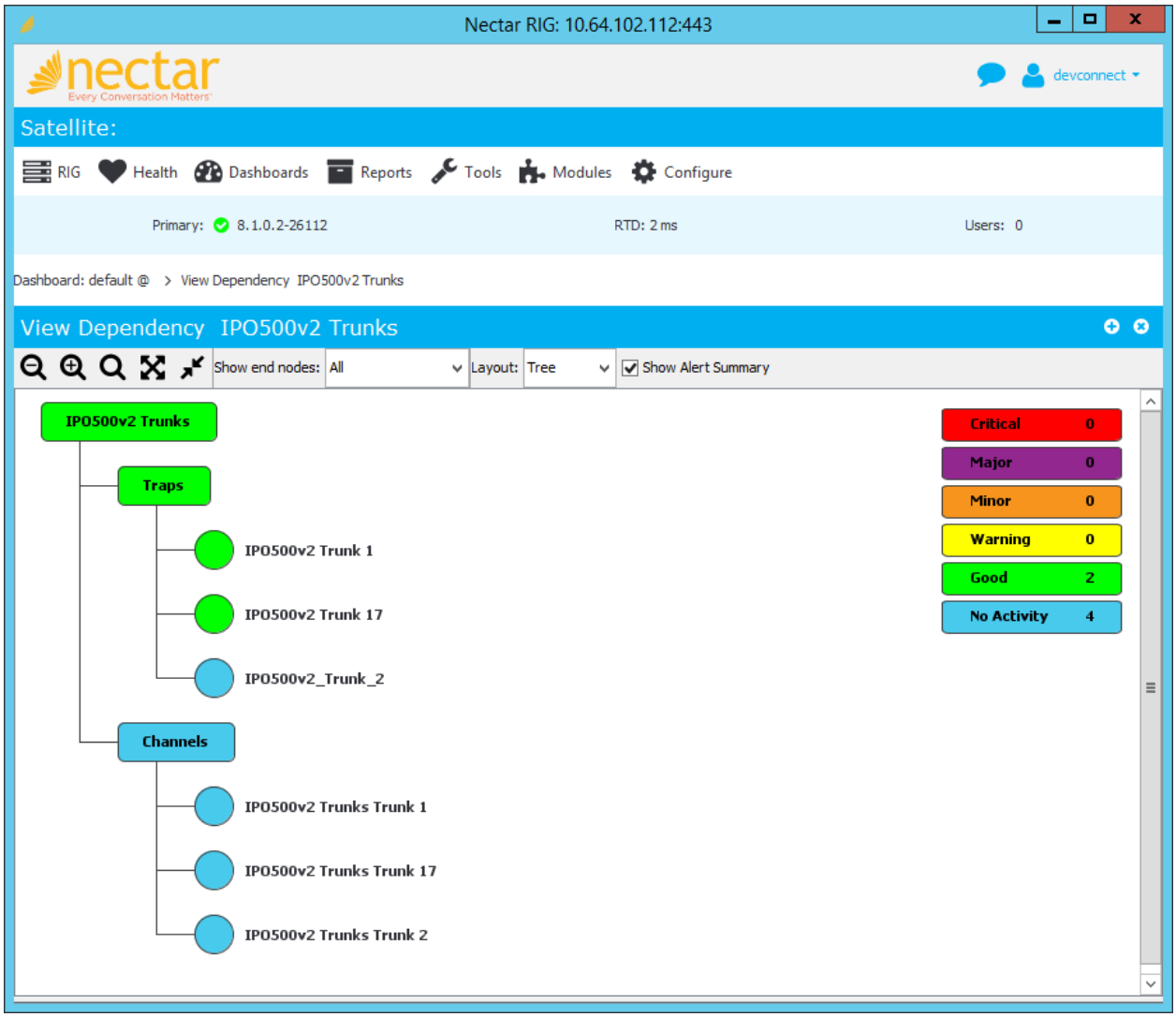
1. Navigate to **Health → Events** and verify that the Service Monitoring Web Services API connection is established as shown below.



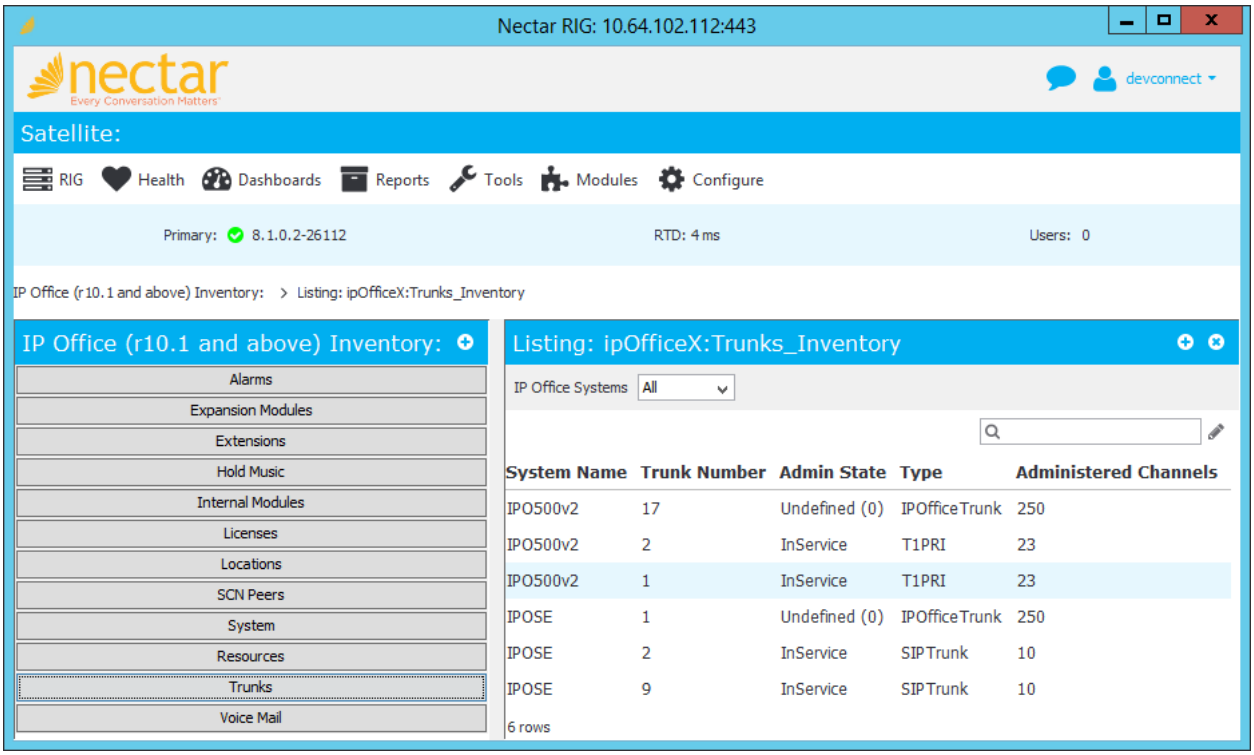
2. Navigate to **Dashboards → Dashboard** to verify that it was automatically created properly.



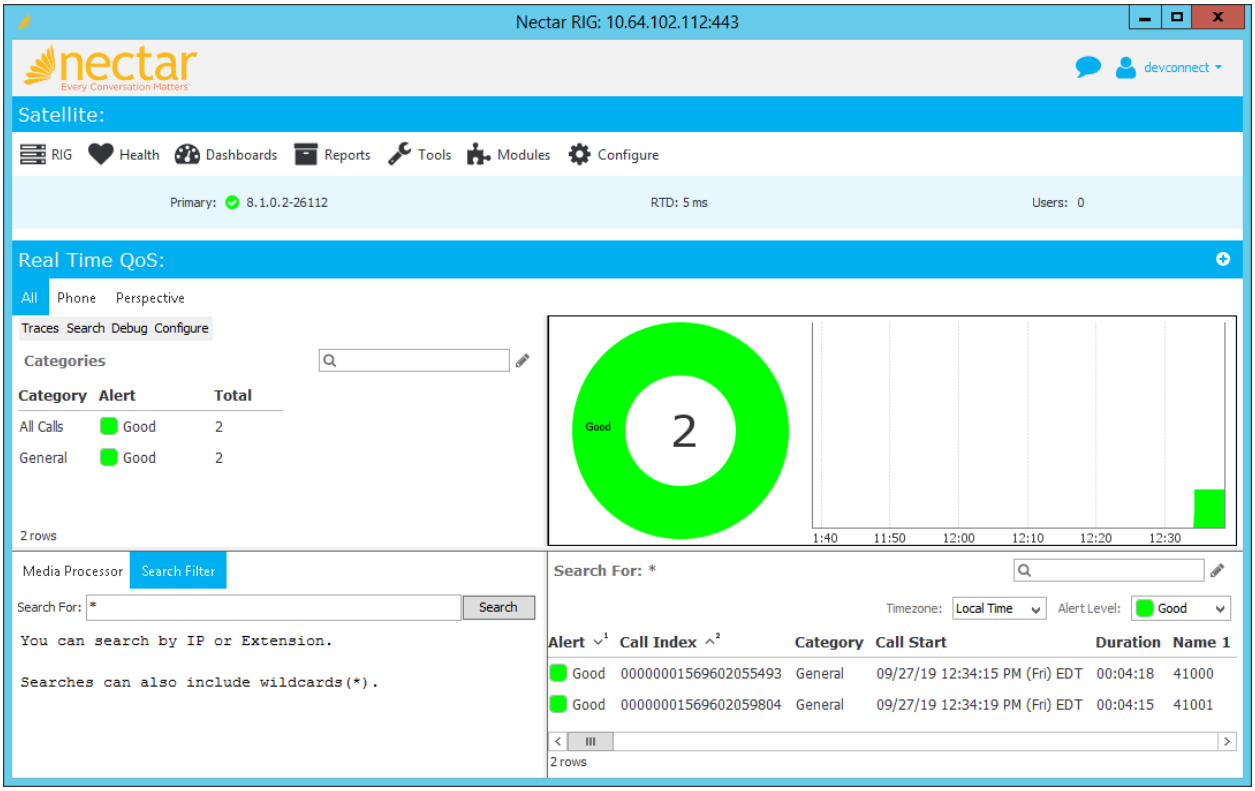
3. View the **Dependency Trees** and verify that the status conditions are correct. The **Trunks Dependency Tree** is shown below.



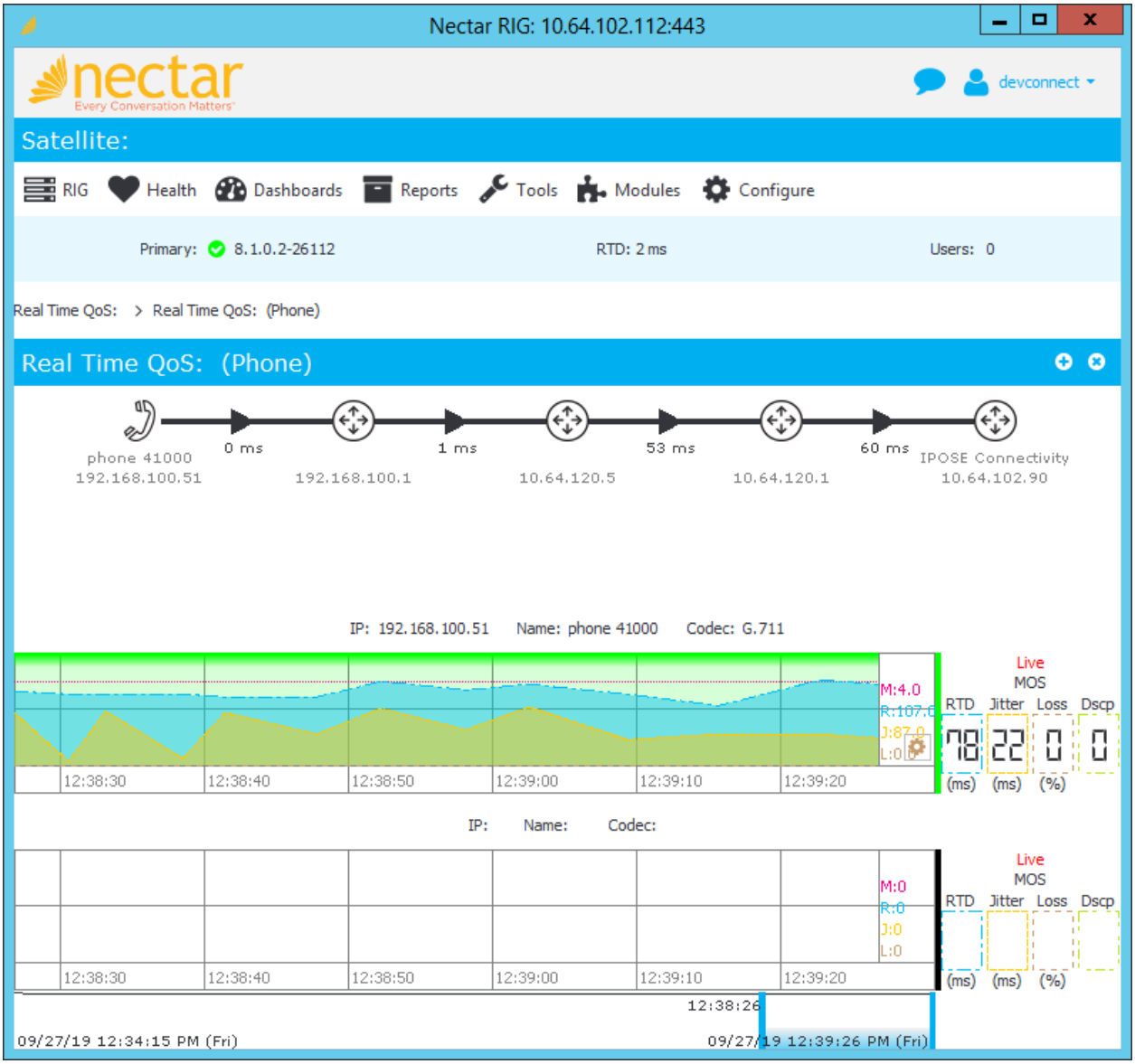
4. Navigate to **Reports → Inventory → Avaya IP Office (r10,1 and above)** to view the inventory information and verify that it is correct. The trunks inventory is shown below.



5. Establish a call between two Avaya IP Deskphones. Navigate to **Health → Quality Management → Real-Time QoS** to view the active calls. Double-click on one of the phones on the call to view the **Real-Time QoS metrics**.



The real-time QoS metrics and call path information for the phone are displayed as shown below.



8. Conclusion

These Application Notes described the configuration steps required to integrate Nectar Unified Communications Management Platform (UCMP) with Avaya IP Office Server Edition using SNMP traps and polling, RTCP, and Service Monitoring Web Services. The compliance test passed with observations noted in **Section 2.2.**

9. Additional References

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

[1] *Administering Avaya IP Office™ Platform Manager*, Release 11.0, February 2019, available at http://support.avaya.com.

[2] *Avaya IP Office Platform DevConnect support, Service Monitoring Web Services API*, 175418 Issue 1.02 (20-Jul-2017), available at http://devconnectprogram.com.

The following Nectar documentation is available from Nectar.

[3] *Nectar Deployment Guide: Avaya IP Office r10.1 and above*, Release 7.4, Version 1.1, January 2019.

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.