User's Guide

SCOM

AudioCodes™ Management Pack

Version 1.0.5.65

audiocodes

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank.

> ## Notice
>
> Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.
>
> This document is subject to change without notice.
>
> Date Published: January-28-2018

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

LTRT	Description
30805	Initial document release for Version 1.05.45
30806	Updates for adding SNMPv3 users and new template for Skype for Business.
30807	Update of Version number to 1.0.5.51
30808	Updated to Version 1.0.5.65

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at https://online.audiocodes.com/documentation-feedback.

1   Introduction

This document describes how to install and use the AudioCodes SCOM Management Pack which manages AudioCodes gateways in the SCOM environment.

SCOM (System Center Operations Manager) enables customers to reduce the cost of data center management across server operating systems and hypervisors through a single, familiar and easy-to-use interface. Different views show state, health and performance information, as well as alerts generated according to availability, performance, configuration or an identified security situation. Operators can gain a rapid insight into the state of the IT environment, and the IT services running across different systems and workloads.

The purpose of the AudioCodes SCOM Management Pack is to allow the SCOM server to monitor AudioCodes gateways through SNMP. This includes Discovery, health states, alerts, performance counters and tasks.

> **Note:** The AudioCodes SCOM Management Pack runs only on SCOM 2012 and on SCOM 2012 R2. It is not *backward-compatible* to run on SCOM 2007.

This page is intentionally left blank.

2   AudioCodes Management Pack - Gateway Support

The following AudioCodes gateways are supported by the AudioCodes SCOM Management Pack:

- Mediant 4000 E-SBC
- Mediant 3000 Gateway and E-SBC
- Mediant 2600 E-SBC
- Mediant 2000 Media Gateway
- Mediant 1000 Media Gateway
- Mediant 1000B Gateway and E-SBC
- Mediant 1000B MSBR
- Mediant 800 MSBR
- Mediant 800B Gateway and E-SBC
- MediaPack Media Gateways MP-124 (FXS)
- MediaPack Media Gateways MP-118 (FXS and FXO)
- MediaPack Media Gateways MP-114 (FXS and FXO)
- MediaPack Media Gateways MP-112 (FXS)
- MediaPack 1288

This page is intentionally left blank.

3 Setting up the AudioCodes SCOM Management Pack

This chapter describes the following setup procedures:

■ Running the Setup Wizard. See below

■ Importing Management Pack. See Section 3.2 on page 22.

3.1 Running the Setup Wizard

This section describes how to setup the AudioCodes SCOM Management Pack environment on the SCOM server. Once you have completed this setup, you can import the AudioCodes Management Pack into the SCOM environment and manage AudioCodes devices.

> ⚠ **Note:** This step is only required if you have received the Management Pack in executable file format.

➢ **To setup the AudioCodes Management Pack:**

1. Run the AudioCodesSCOM.exe file; the AudioCodes SCOM Setup wizard is displayed:

Figure 3-1: AudioCodes Setup Wizard Welcome Screen
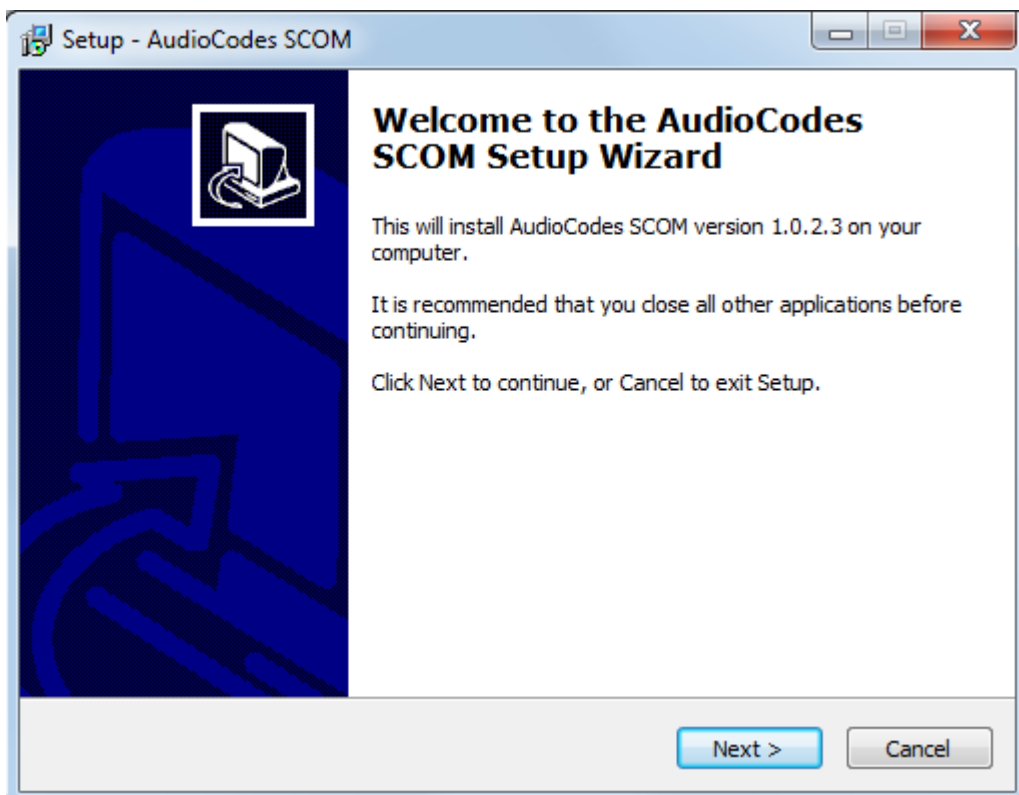
2. Click **Next**; the Select Destination Location screen is displayed:

Figure 3-2: Select Destination Location
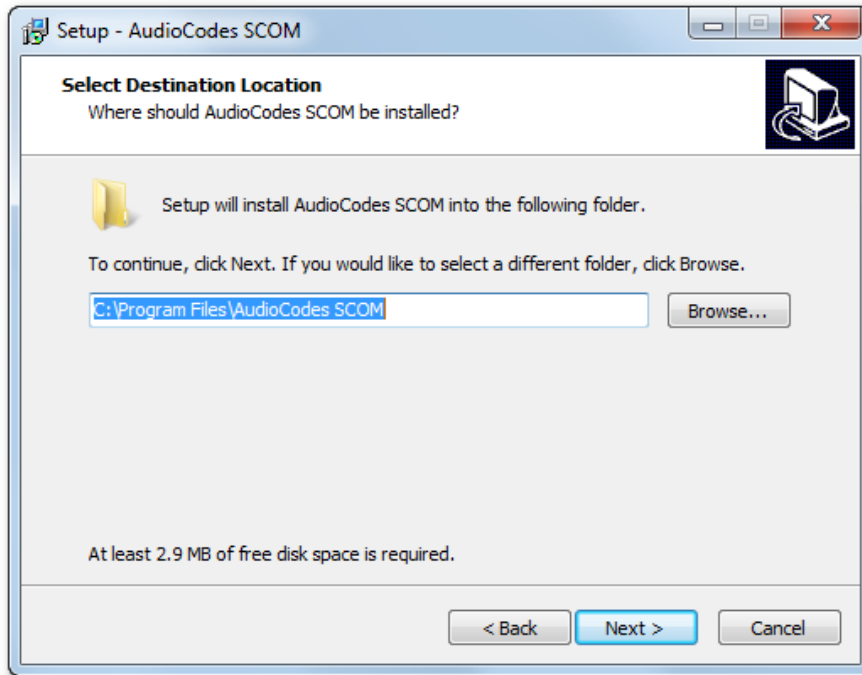
3. Choose the folder for installing the AudioCodes Management Pack, and then click **Next**; the **Ready to Install** screen is displayed:

Figure 3-3: Ready to Install
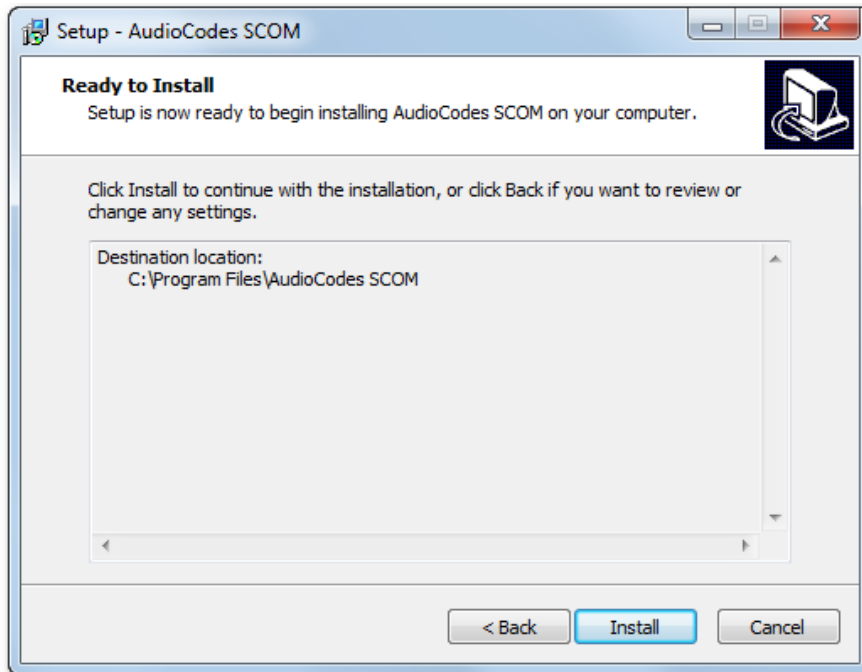
4. Verify the installation settings and then click **Install**; the Completion screen is displayed:

Figure 3-4: AudioCodes Setup Wizard Complete

5. Click **Finish** to exit the setup.

3.2 Importing Management Pack

This section describes how to import the AudioCodes Management Pack into the SCOM 2012 or 2012R2 environment. Once you import the Management Pack, you can manage AudioCodes gateways via the SNMP interface.

➢ **To import the AudioCodes Management Pack into the SCOM environment:**

1. Start the SCOM; the SCOM interface is displayed.

2. In the main SCOM window, click the **Administration** pane; the **Administration** pane is displayed:

Figure 3-5: Administration Pane
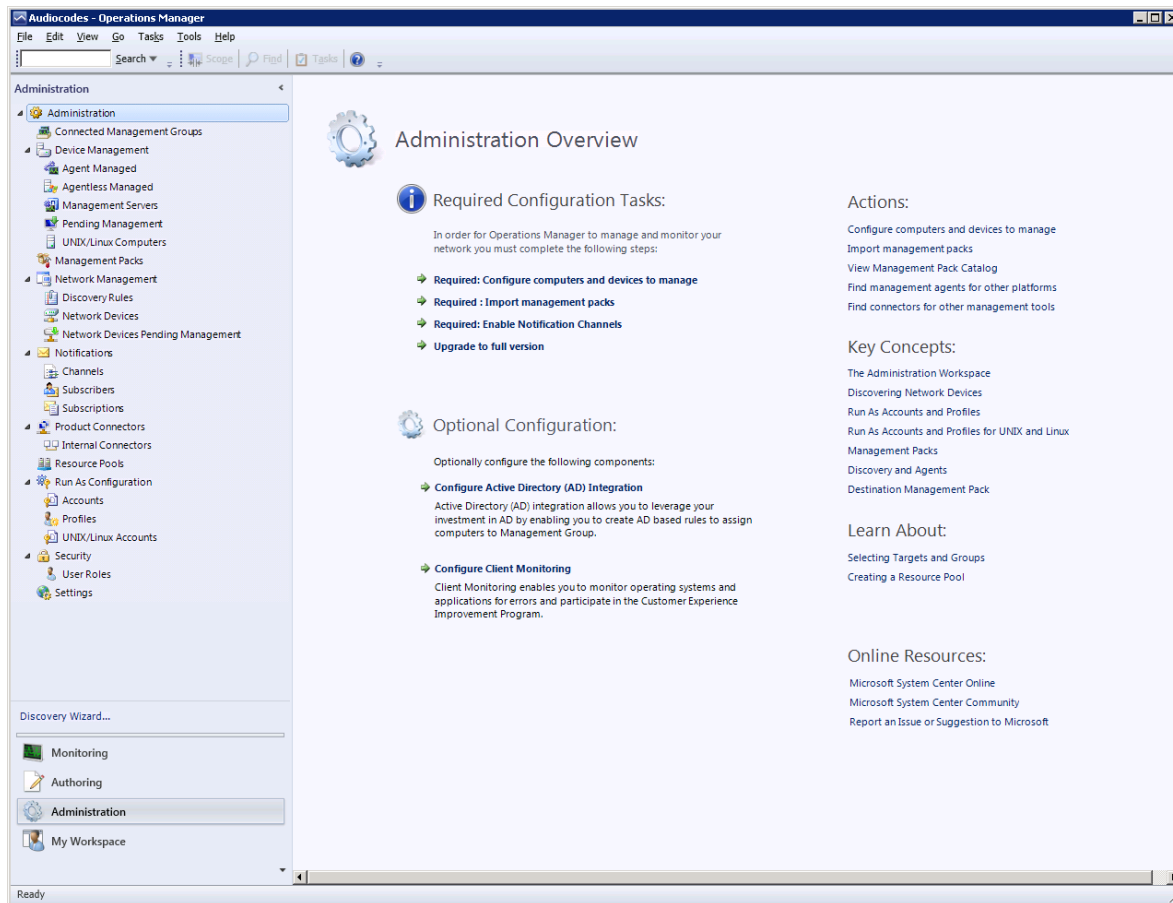
Figure 3-6: Import Management Packs Option
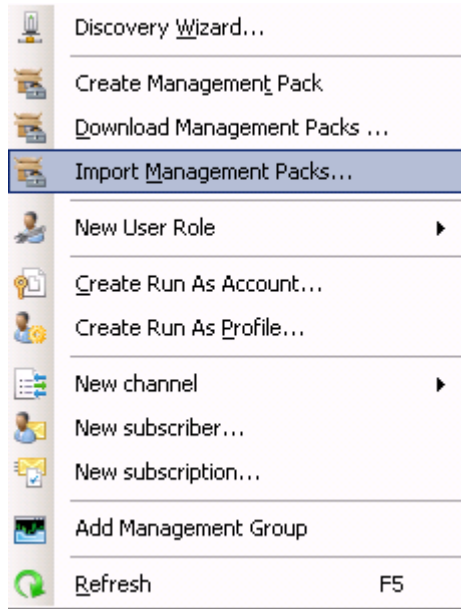
3.   In the Navigation tree, right-click **Management Packs**, and then from the pop-up menu, choose **Import Management Packs**; the Select Management Packs window is displayed:

Figure 3-7: Select Management Packs
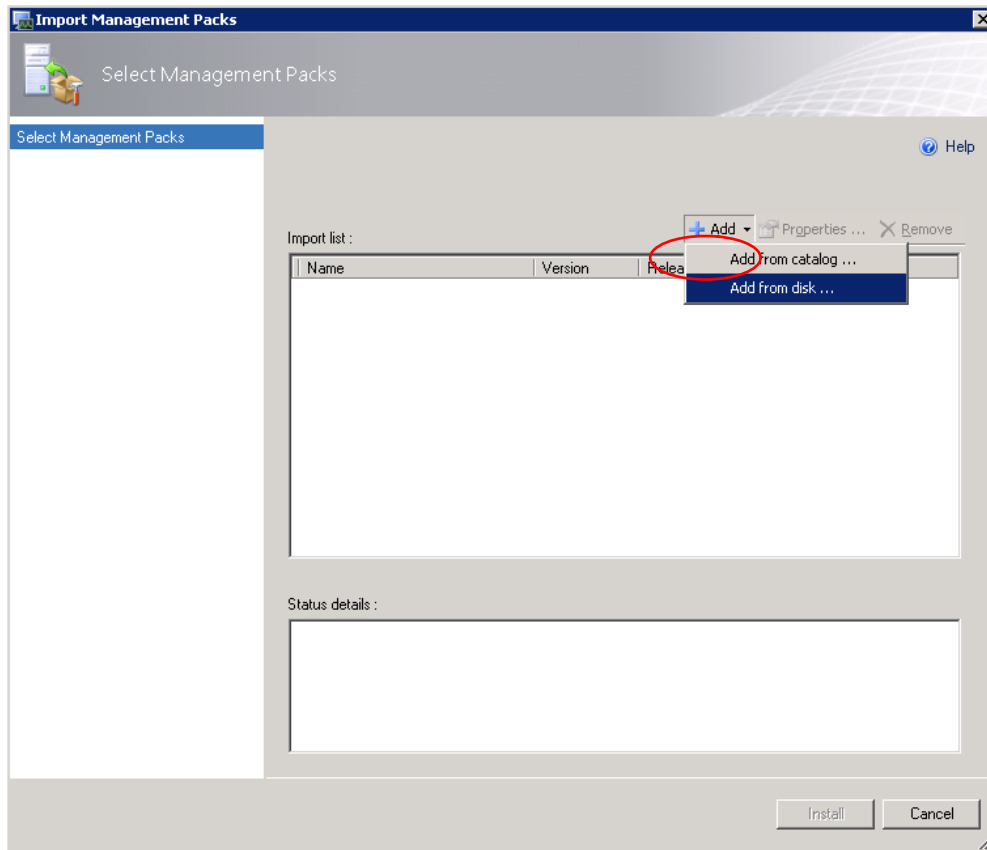
4. Click the **Add** button, and then choose **Add from disk**; the following dialog is displayed:

Figure 3-8: Online Catalog Connection
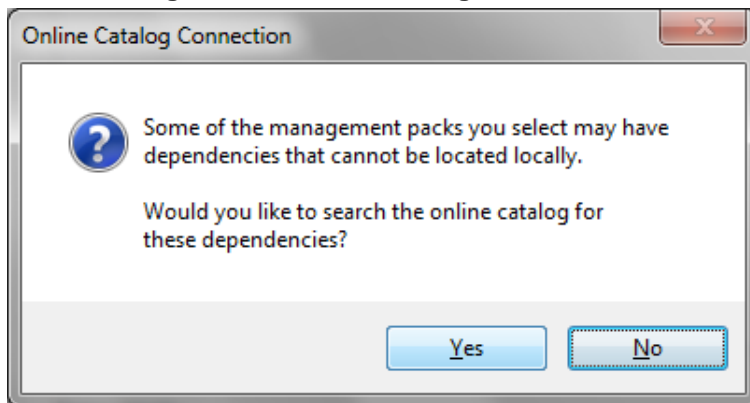
5. Click **No** to decline choosing Management Pack from a Catalog.

6. Locate the saved AudioCodes Management Pack (in XML format) on you disk (the location that you chose in Section 3 on page 19) and then click the **Open** button; the Select Management Packs window is displayed:

Figure 3-9: Select AudioCodes Management Packs
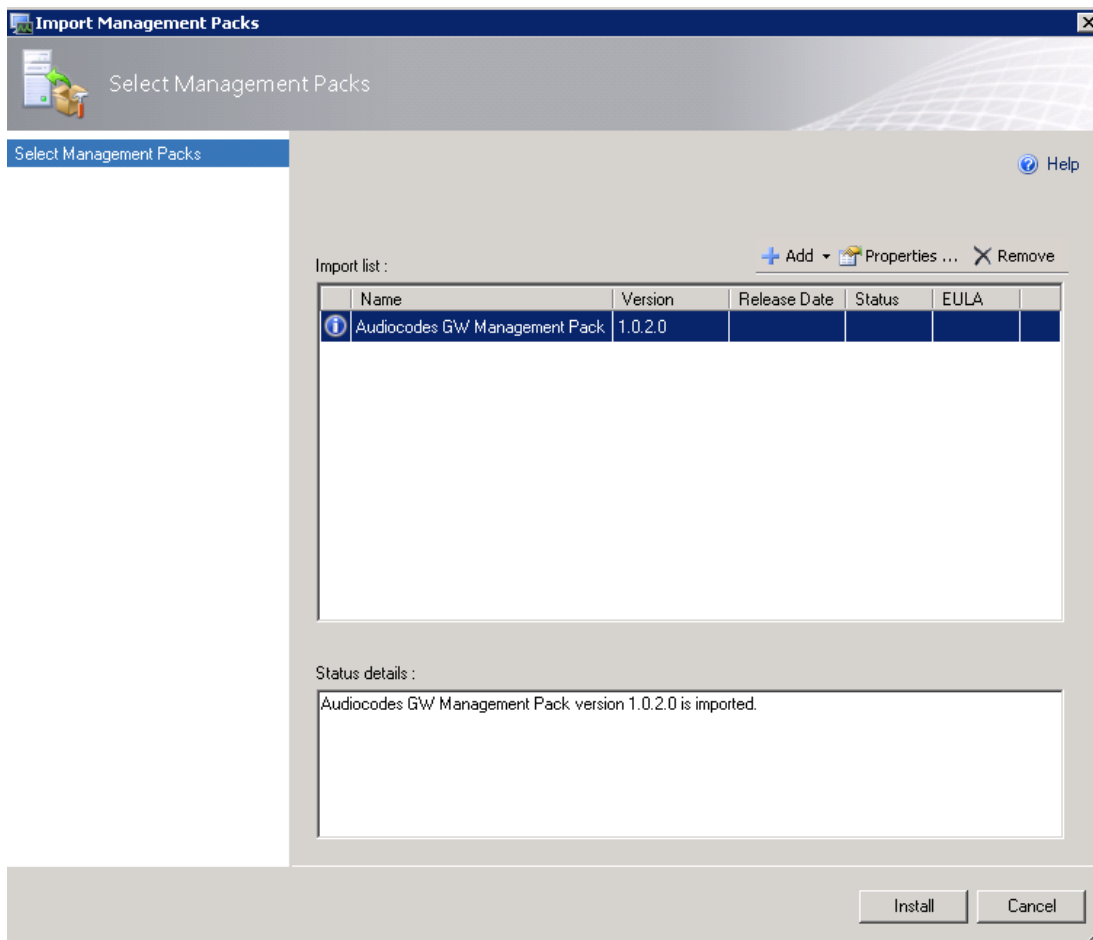
7. Select the AudioCodes GW Management Pack, and then click the **Install** button.
.

4   Discovering Gateway Devices

When Management Packs are installed you have to discover your AudioCodes gateways as Network Elements to enable SCOM to make a full discovery. You discover the gateways by using the Discovery Wizard to create a Discovery Rule.

> **Note:** You can create a single Discovery rule for each SCOM server.

4.1   Creating Discovery Rule

This section describes how to discover gateways as a network device.

➢   **To discover the gateway as a Network Device:**

1.   In the Administration pane, right-click **Network Devices** ,and then in the pop-up menu, choose **Discovery Wizard**:

Figure 4-1: Open Discovery Wizard
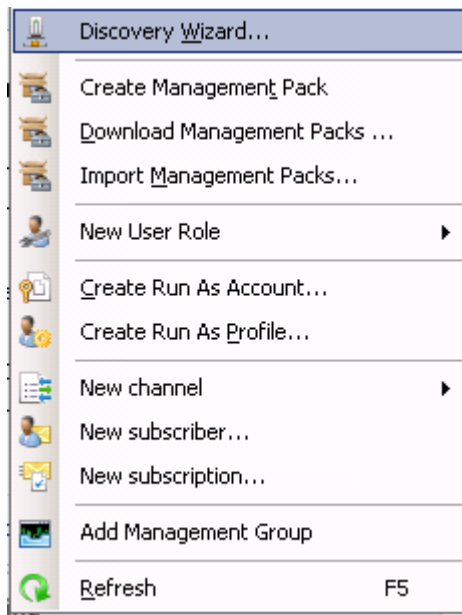
The Computer and Device Management Wizard is displayed:

Figure 4-2: Computer and Device Management Wizard
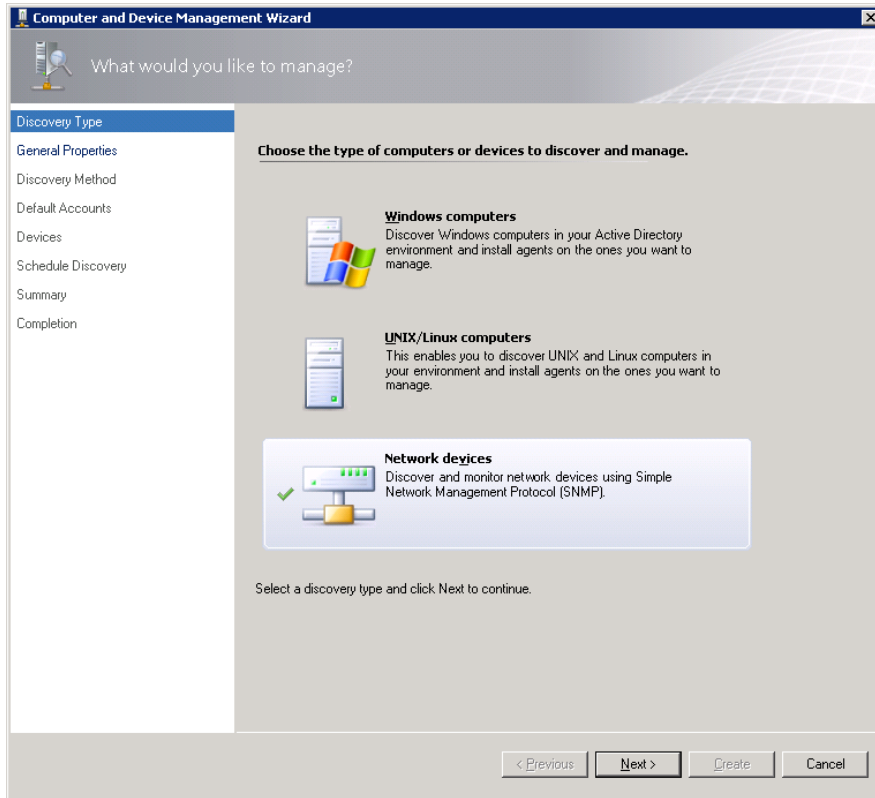
2. Select the **Network devices** option, and then click **Next**; the General Properties window is displayed:

Figure 4-3: General Properties

3. In the 'Name' field, enter a description of the Discovery Rule.

4. From the Available servers drop-down list, choose the SCOM server e.g., SCOM.iLync15.local, and then click **Next**; the Discovery Method window is displayed:

Figure 4-4: Discovery Method
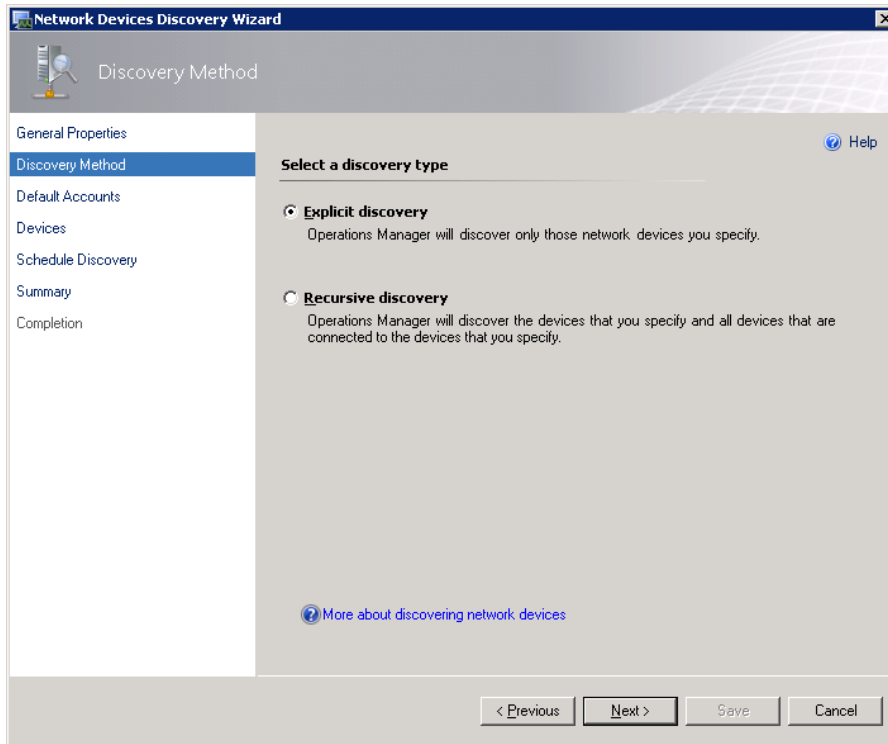
5. Select the appropriate actions, and then click **Next**; the Defaults Accounts page is displayed:

Figure 4-5: Default Accounts
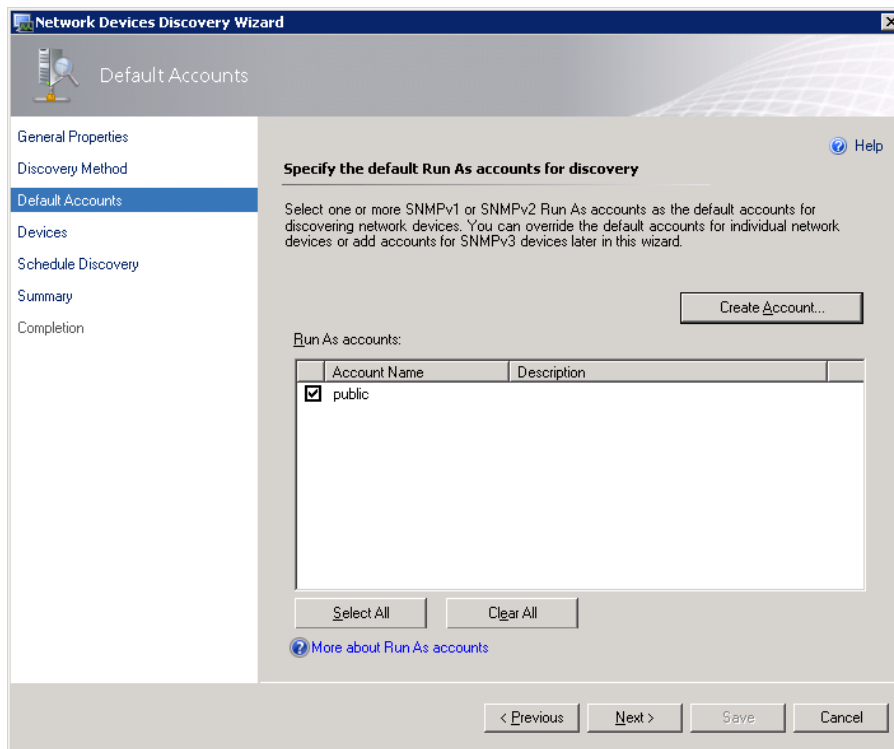
6. Choose the default SNMP SCOM account (this account is always-'public') or click **Create Account** button to create a new default account; a wizard opens. Enter a Display Name and Community String (use the same community string that is configured on the network device that you wish to discover), and then click **Create**.

7. **Click Next**; the Devices page is displayed with the new user details:

Figure 4-6: Devices
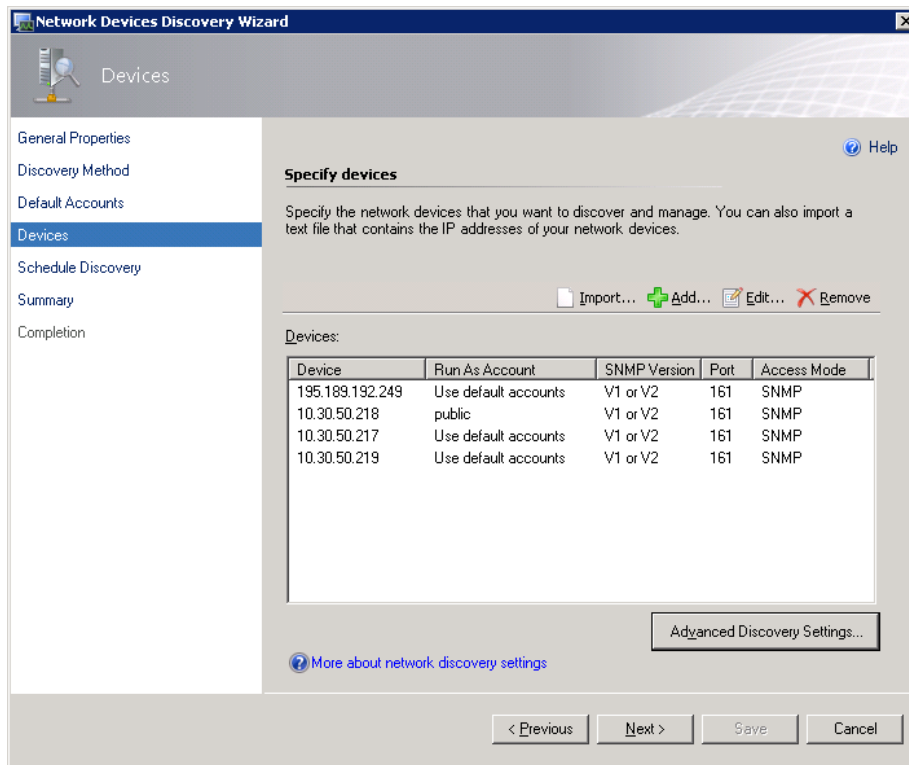
8. Click the [Add...] button to add the IP addresses of devices to be discovered (if you wish to add a device with SNMPv3, see Section 5 on page 37); the Add a Device dialog is displayed:

Figure 4-7: Add a Device
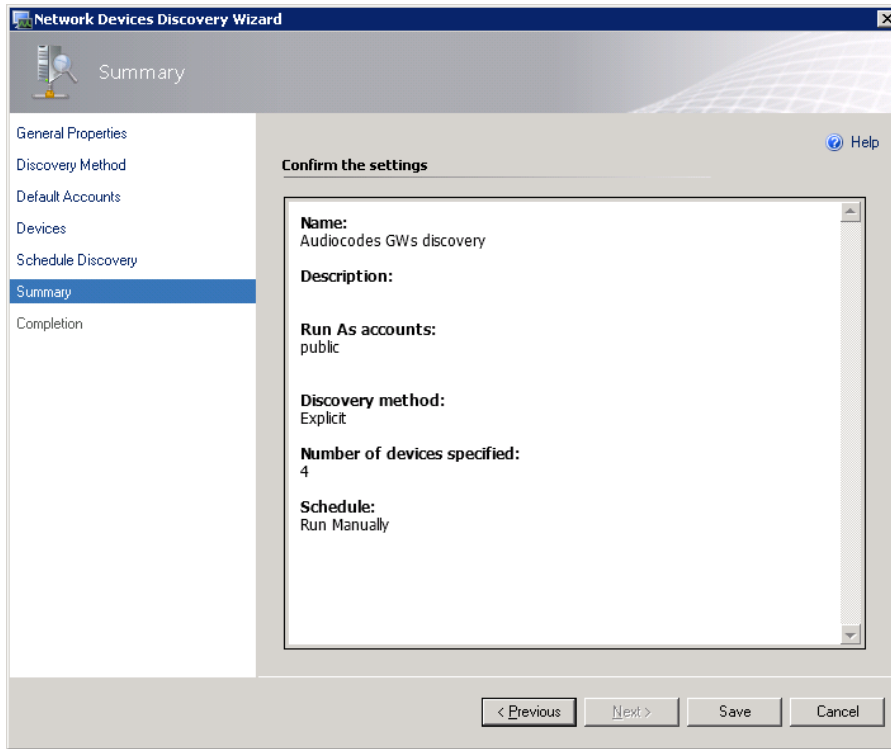
9. In the 'Name or IP address' field, enter the Enter the Name or IP address of the device.

10. From the Access mode field drop-down list, select **SNMP**.

11. Optional: From the 'SNMP V1 or V2 Run As Account' drop-down list, select a different already configured default account.

   • If you wish to configure a new SNMP V1 or V2 default account, then click the **Add SNMP V1 or V2 Run As Account** button; a wizard opens. Enter a Display Name and Community String (use the same community string that is configured on the network device that you wish to discover), and then click **Create**.

   Note that the same dialog opens as in the 'Default Accounts' step above.

12. Click **Next**; the Schedule Discovery screen is displayed:

Figure 4-8: Schedule Discovery
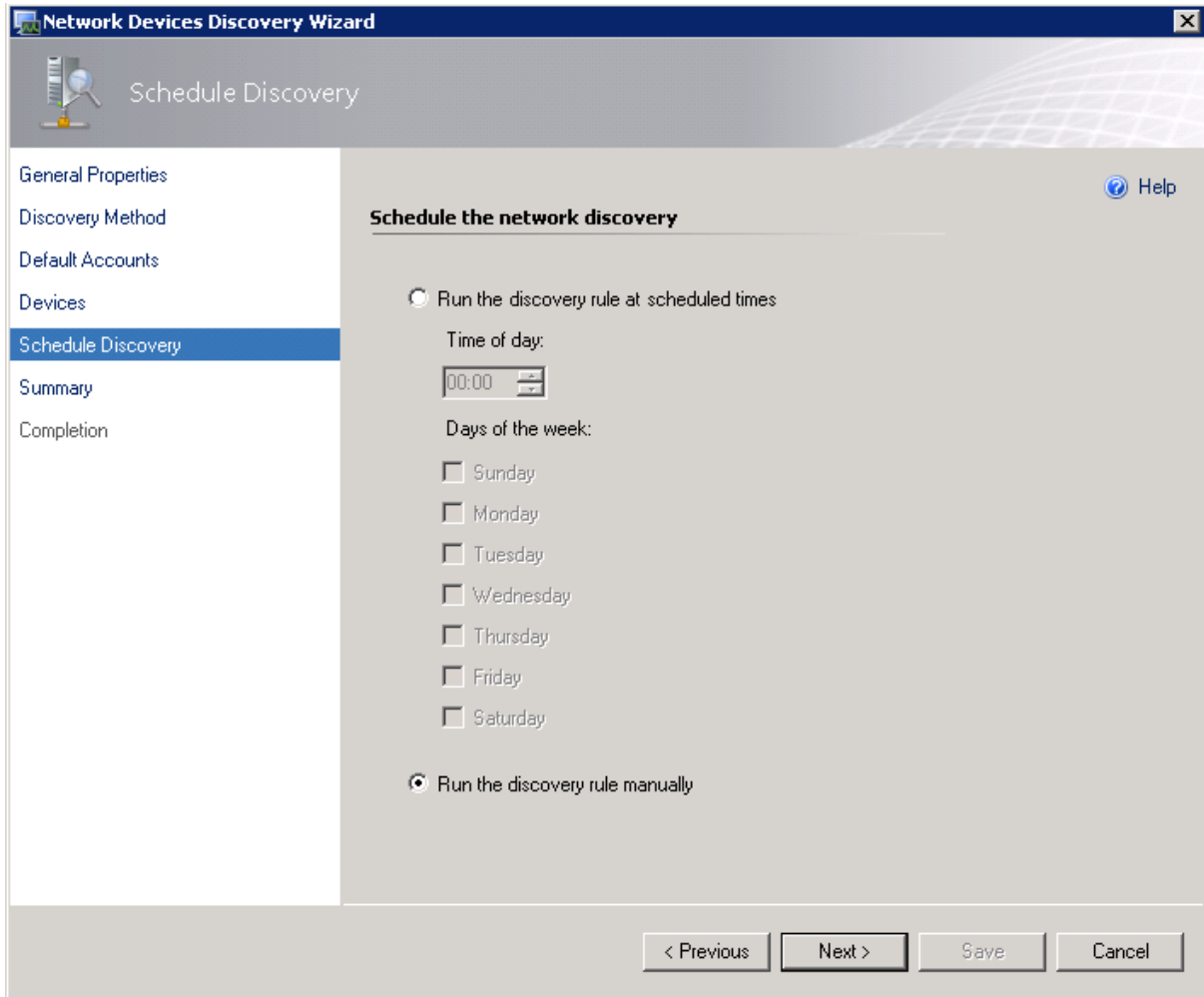
13. Select the **Run the discovery rule manually** option, and then click **Next**; the Summary page is displayed:

Figure 4-9: Summary

14. Review the settings, and then click **Save**.
15. Wait for the discovery rule to complete saving.

Figure 4-10: Discovery Saving Progress
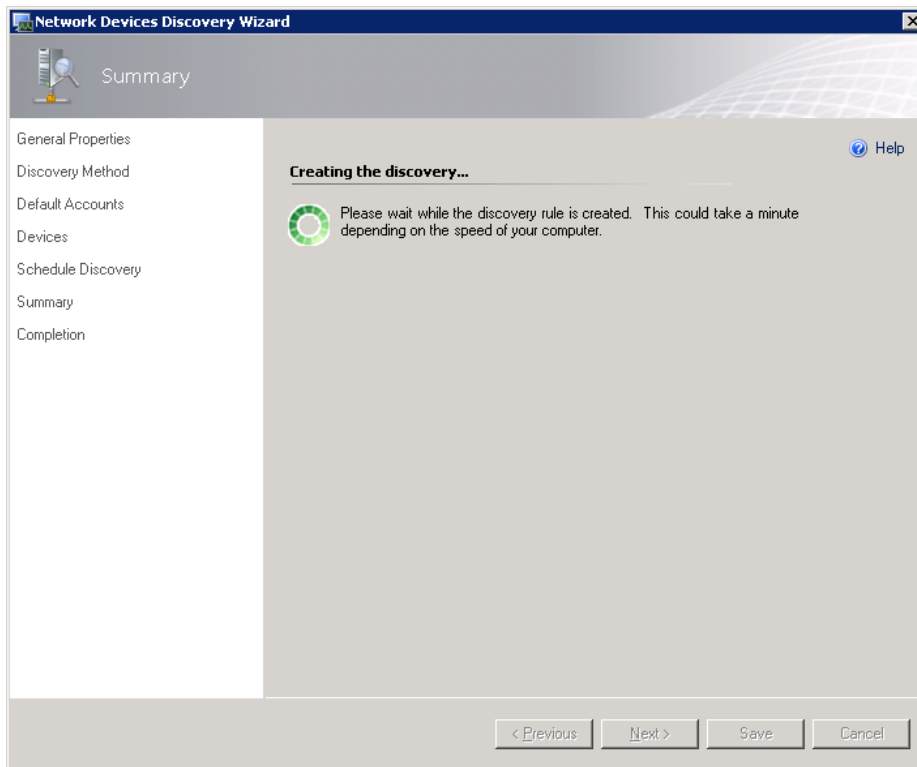
16. Click the **Close** button; a confirmation window is displayed:

Figure 4-11: Network Discovery Rule Confirmation
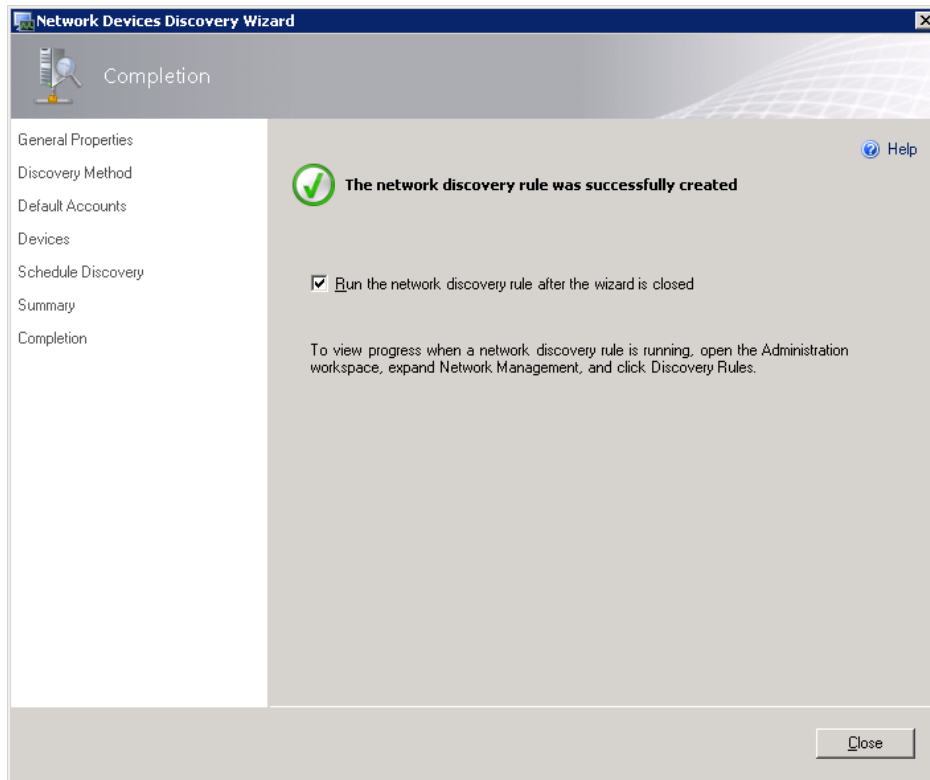
The newly created rule should appear in the 'Discovery Rules' pane. When the rule has been successfully created, it should have the status 'Idle'.

17. Wait for 5-8 minutes to allow the SCOM to make a full discovery.

Figure 4-12: Discovery Rules Confirmation
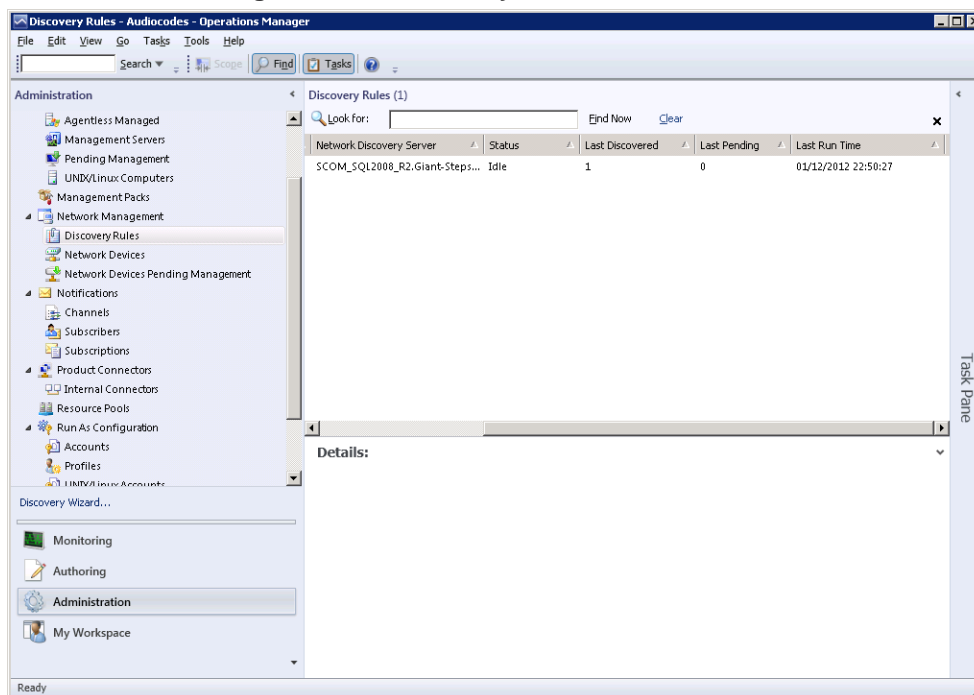
18. Click the **Administration** pane, and then in the Navigation tree, select **Network Devices**.

Figure 4-13: Network Devices
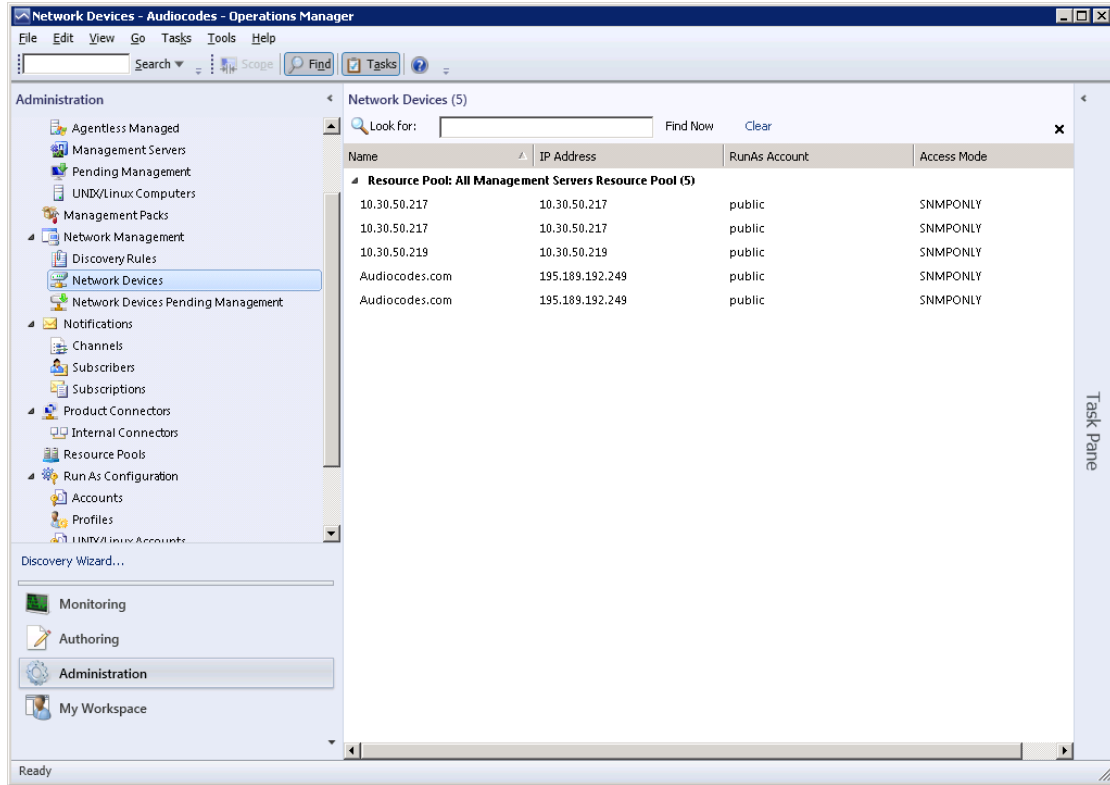
All discovered gateways are displayed in this window.

Note: Wait for five-eight minutes to allow the SCOM to make a full discovery.

4.2   Managing SCOM Accounts

SCOM accounts are managed in the Accounts screen.

➢ **To view currently defined SCOM user accounts:**

1. Open the Accounts page (**Administration** > **Run as Configuration** > **Accounts**); a screen similar to the following is displayed:

Accounts Page

- To view the account properties, select an account, and then in the Tasks pane, click the **Properties** button.

- To delete a user, select an account, and then in the Tasks pane, click the **Delete** button.

4.2.1   Adding Network Devices to Discovery Rule

This section describes how to add network devices to an existing Discovery Rule.

➢ **To add network devices to an existing discovery rule:**

1. In the Discovery Rules window, double-click the Discovery Rule; the Network Devices Discovery Wizard is displayed with the existing settings.

2. Run the wizard as described above in Section 4.1 on page 25.

This page is intentionally left blank.

5   Configuring SNMP

This section describes how to configure the SNMP connection between the managed AudioCodes devices and the SCOM.

The following topics are described:

- Adding SNMPv3 Users. See below.
- Disabling SNMP trap service. See Section 5.2 on page 50.
- Setting up the device to send SNMP traps. See Section 5.3 on page 51.

5.1   Adding SNMPv3 Users

This section describes how to add SNMPv3 users. You initially need to create the SNMPv3 on the device in the Web Interface, and then add the same user in the SCOM using the Discovery Wizard.

> **Note:** You must configure identical user credentials in the SCOM as you configure in the Web Interface.

5.1.1   Adding SNMP V3 Users in the Device Web Interface

The SNMP v3 Users page allows you to configure authentication and privacy for up to 10 SNMP v3 users.

➢ **To configure SNMP v3 users:**

1. In the device Web Interface, open the SNMP v3 Users page (**Configuration** tab > **System** menu > **Management** sub-menu > **SNMP** sub-menu > **SNMP V3 Users**).

2. Click **Add**; the following dialog box appears:

Figure 5-1: SNMP V3 Setting Page - Add Record Dialog Box

Figure 5-2: SCOM V3 User Added
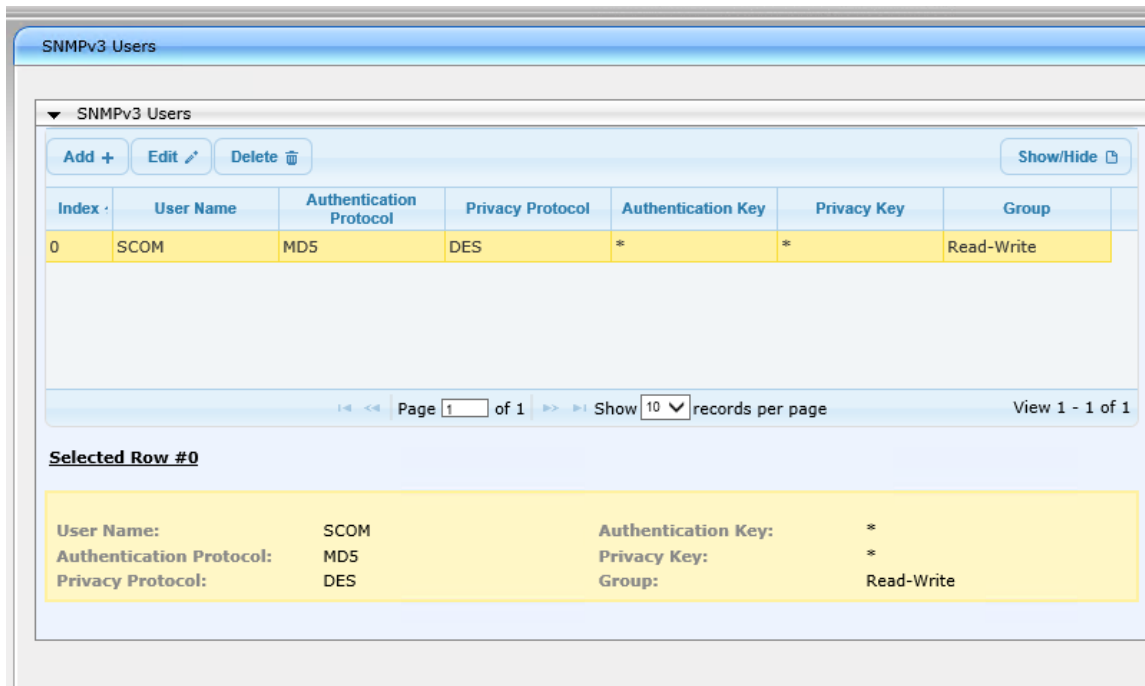
3. Configure the SNMP V3 Setting parameters according to the table below.

4. Click **Submit** to apply your settings.

5. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

Figure 5-3: Resetting the Device
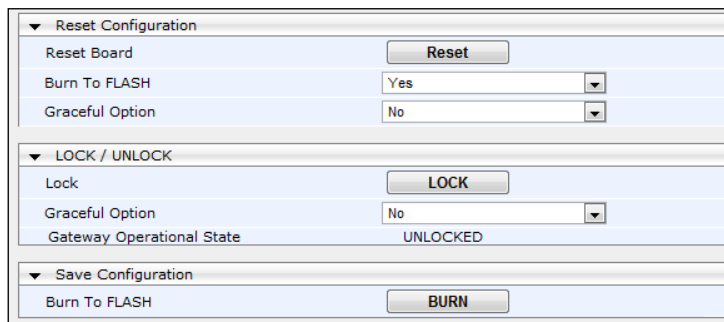
6. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).

7. Click the **Reset** button.

Table 5-1: SNMP V3 Users Parameters

Parameter	Description
Index **[SNMPUsers_Index]**	The table index. The valid range is 0 to 9.
User Name **[SNMPUsers_Username]**	Name of the SNMP v3 user. This name must be unique.
Authentication Protocol **[SNMPUsers_AuthProtocol]**	Authentication protocol of the SNMP v3 user. ▪ **[0]** None (default) ▪ **[1]** MD5 ▪ **[2]** SHA-1
Privacy Protocol **[SNMPUsers_PrivProtocol]**	Privacy protocol of the SNMP v3 user. ▪ **[0]** None (default) ▪ **[1]** DES ▪ **[2]** 3DES ▪ **[3]** AES-128 ▪ **[4]** AES-192 ▪ **[5]** AES-256
Authentication Key **[SNMPUsers_AuthKey]**	Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Privacy Key **[SNMPUsers_PrivKey]**	Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Group **[SNMPUsers_Group]**	The group with which the SNMP v3 user is associated. ▪ **[0]** Read-Only (default) ▪ **[1]** Read-Write ▪ **[2]** Trap **Note:** All groups can be used to send traps.

5.1.2 Adding SNMPv3 Accounts in SCOM

This section describes how to add SNMPv3 users in the SCOM.

➢ **To add SNMPv3 accounts:**

1. In the Administration pane, select **Run As Configuration** > **Accounts**, and then in the Actions pane, select **Create Run as Account**.

Figure 5-4: New SNMPv3 User
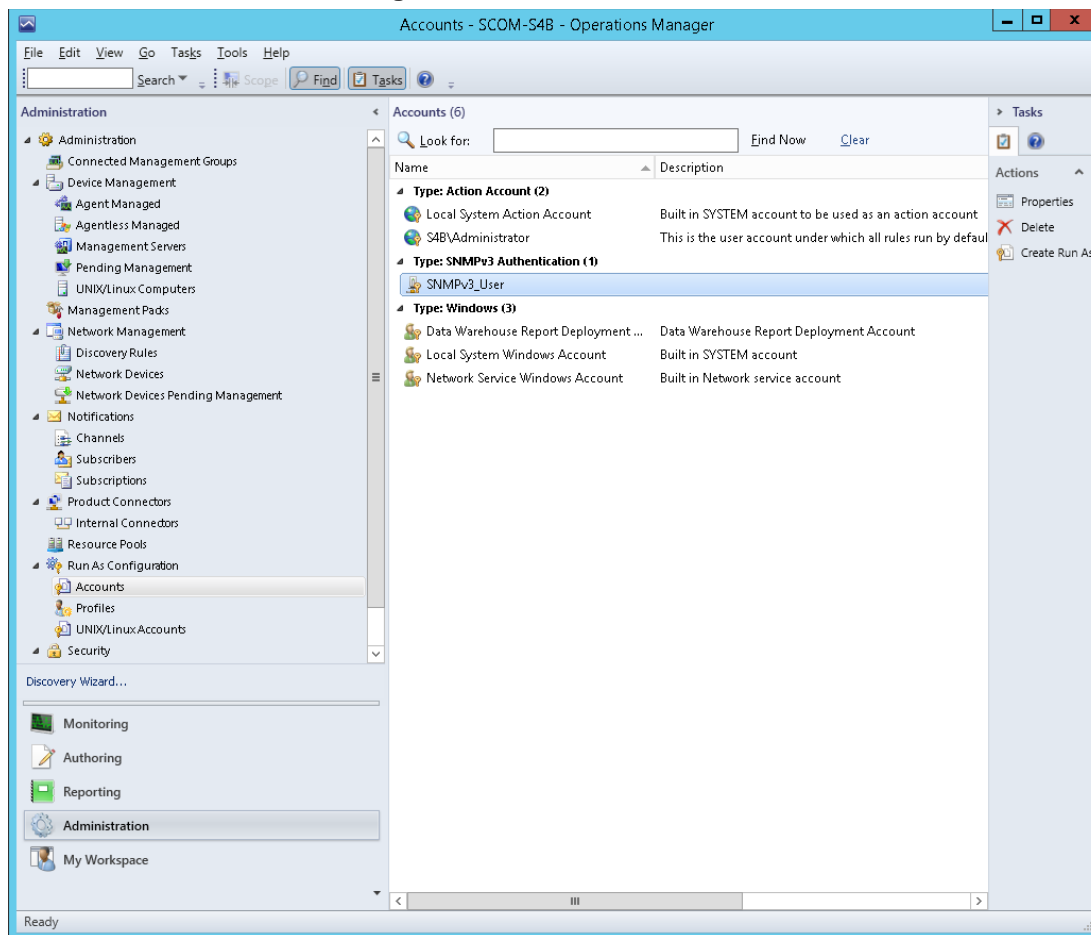
The Create Run as Account wizard is displayed:

Figure 5-5: Create Run as Account

2. From the "Run As account type" list box, select **SNMPv3 Account**.

3. Enter the desired display name and description.

Figure 5-6: Account Credentials
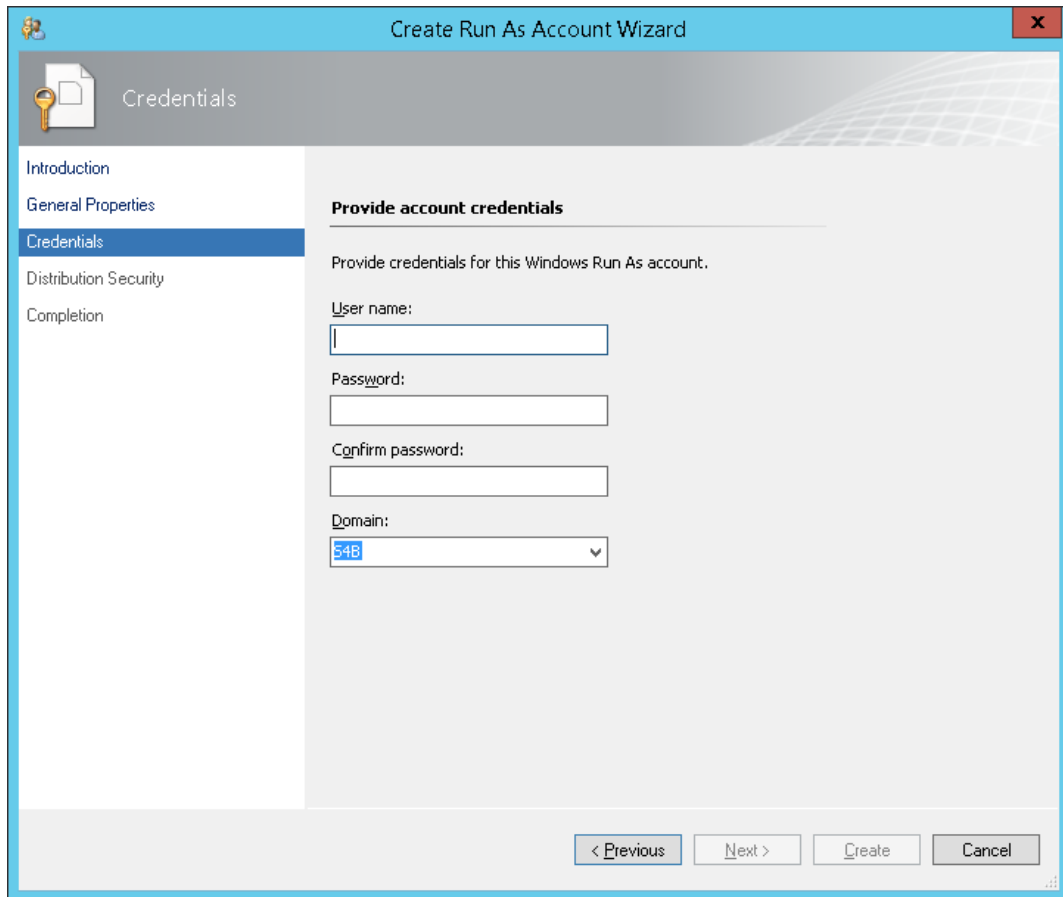
4. Create the new account using the same credentials that you configured in Section 4.1 on page 25 and in Section 5.1.1 on page 37.

5. Ensure that you set the Distribution Security to the **More Secure….** option.

Figure 5-7:SNMPv3 User-Distribution Security
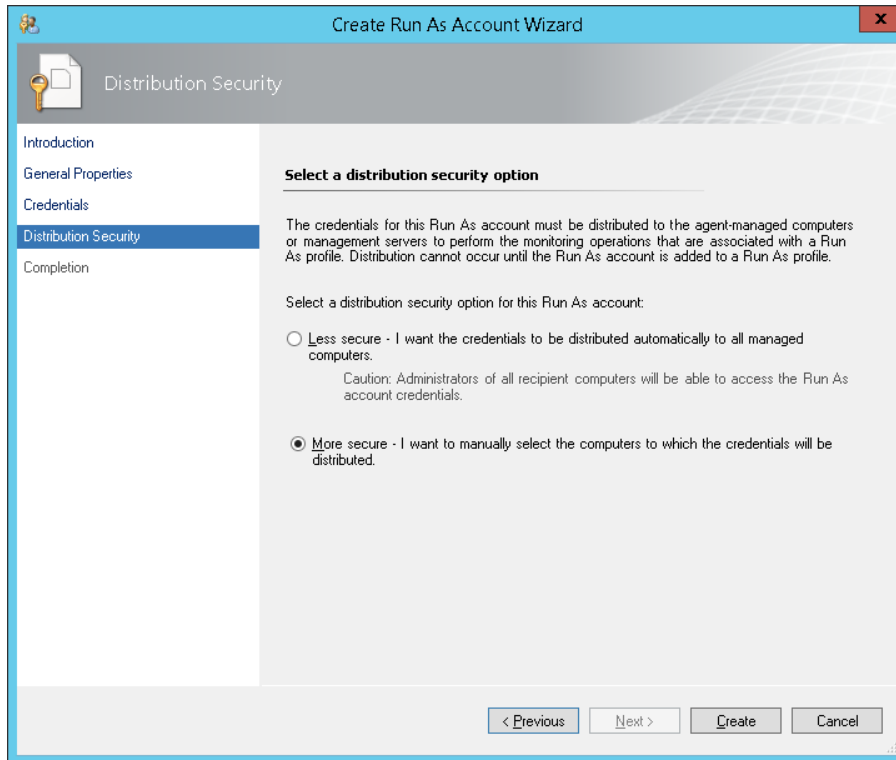
6.   At the end of the wizard process, click **Create** to create the new **SNMPv3_User** object.

Figure 5-8:SNMPv3 User-Wizard Completed Successfully
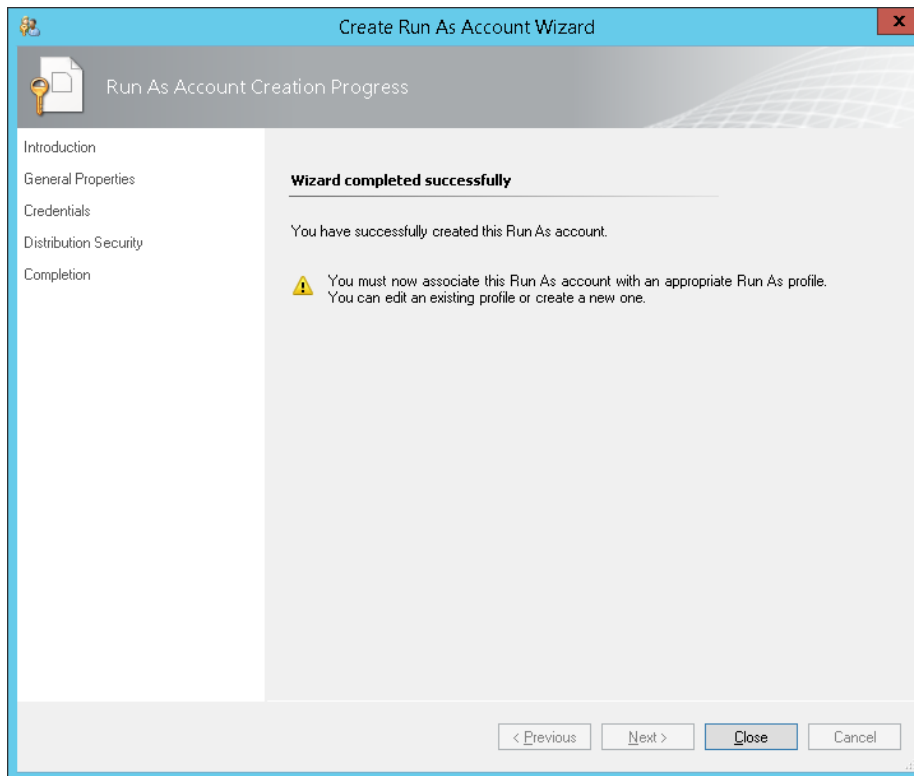
7. In the Administration pane, select **Run As Configuration** > **Profiles** and then select the profile that you wish to associate with the new SNMPv3 Run as account.

Figure 5-9: Run as Profile
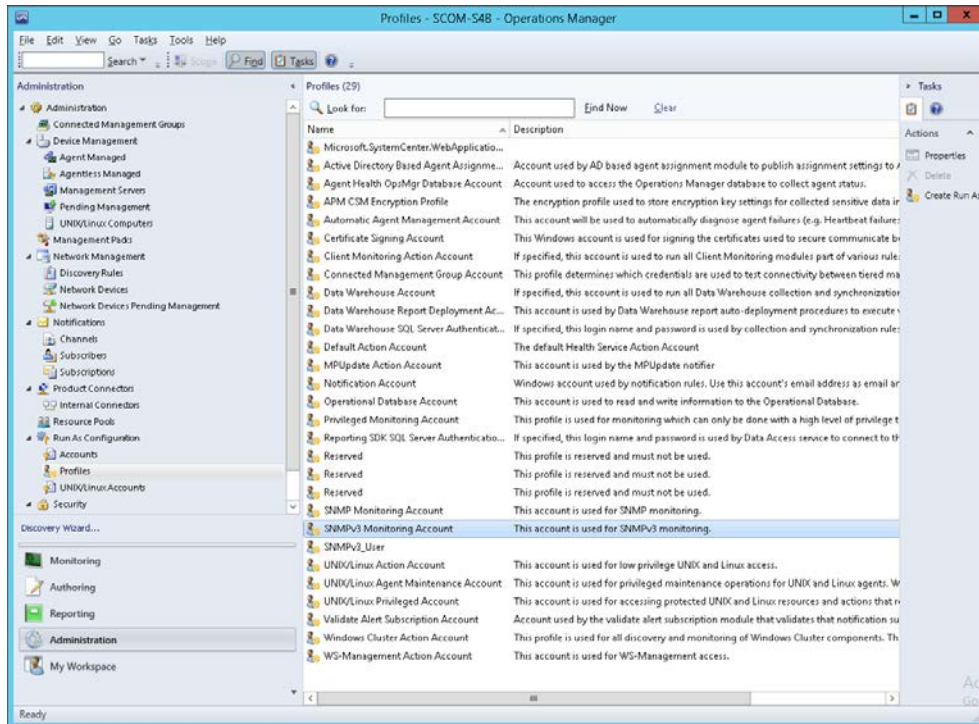
8. Right-click the SNMPv3 profile ("SNMPv3 Monitoring Account" in the above example) and select **Properties**. The Profile wizard opens:

Figure 5-10: Profile Wizard
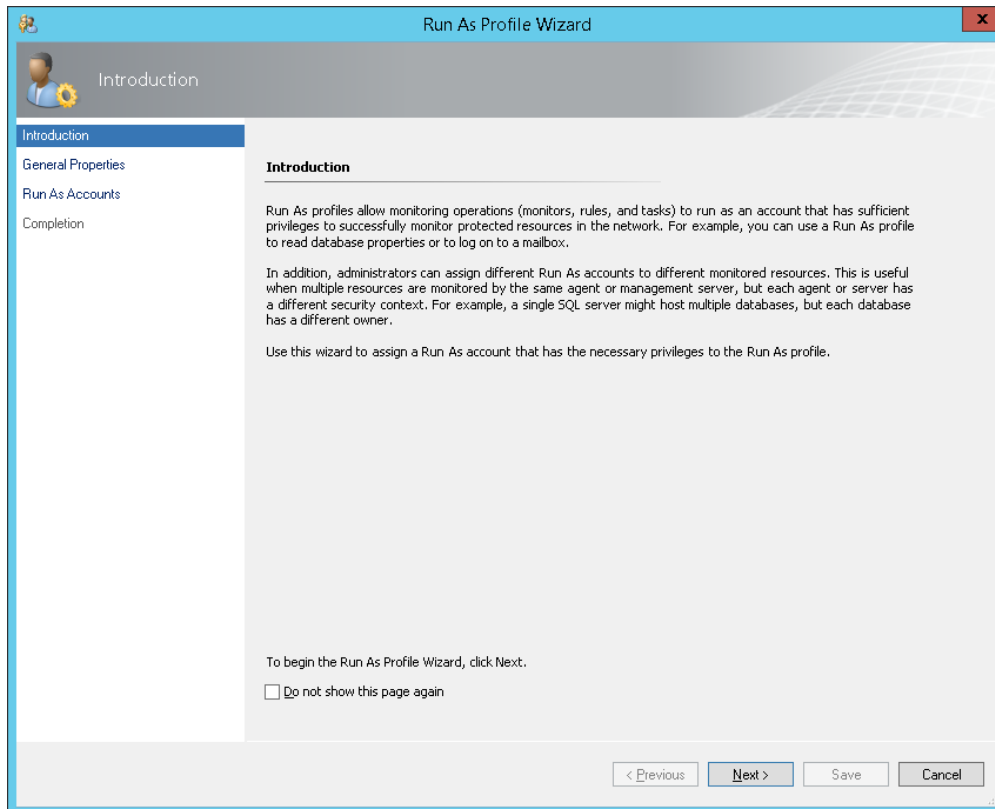
9. In the **General Properties** tab, enter the relevant properties and then in the **Run As Accounts** tab, select the SNMPv3 account that you just added:

Figure 5-11: Select Run As Account
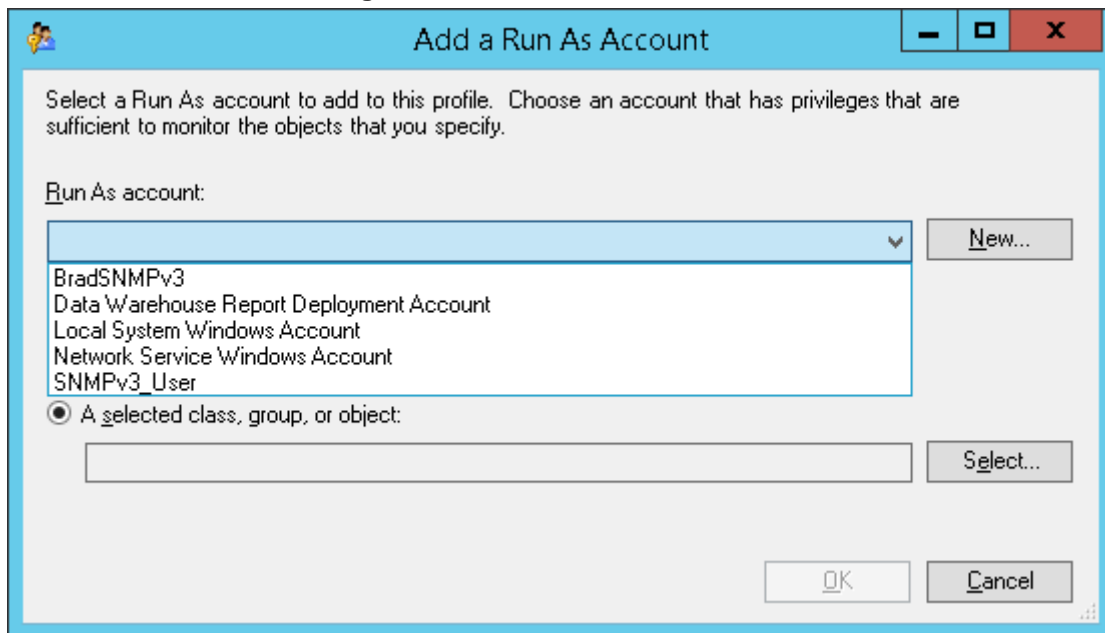
10. Click **Save** to save the new account.

11. In the Administration pane, click **Network Management** > **Network Devices** and select **Discovery Wizard**.

12. Run the Discovery Wizard to discover Network Devices.

13. Add the device using the new SNMPv3 user account:

Figure 5-12: Add a Device
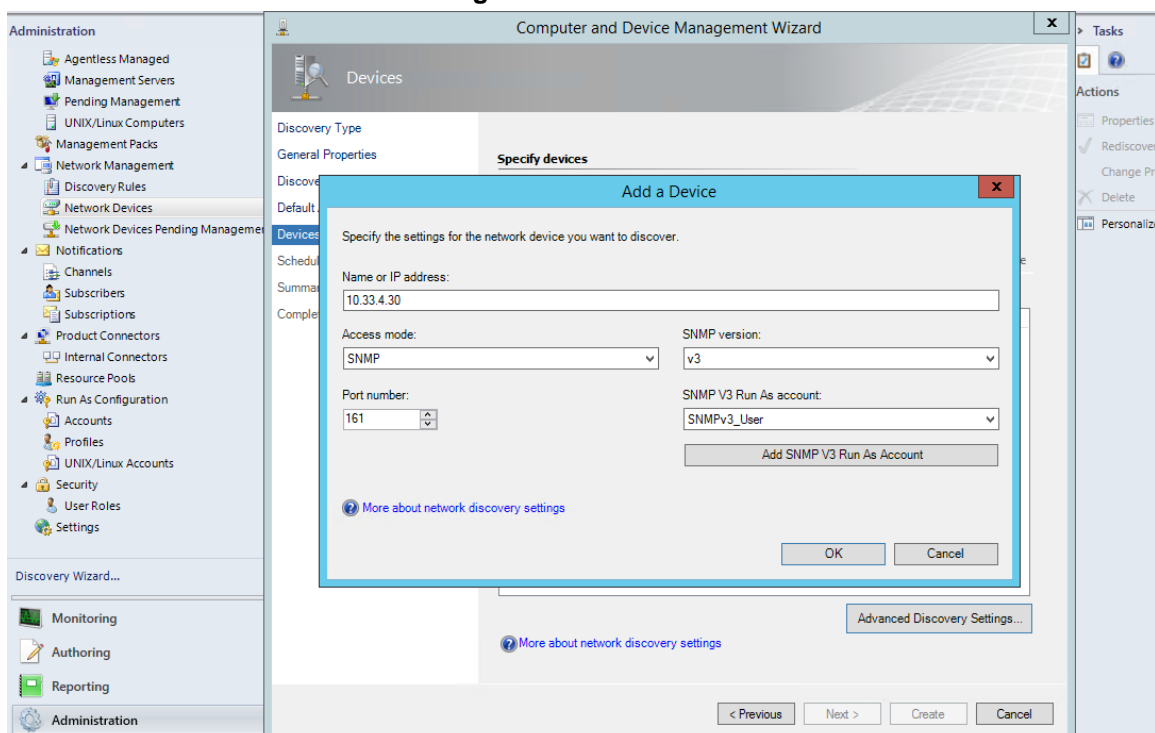
14. Click **Create** to add the device.

Note: This step it will take 1 hour to 24 hours to discover all the devices with SNMPv3.

The Devices page is displayed with the details of the new SNMPv3 account:

Figure 5-13: Devices Page
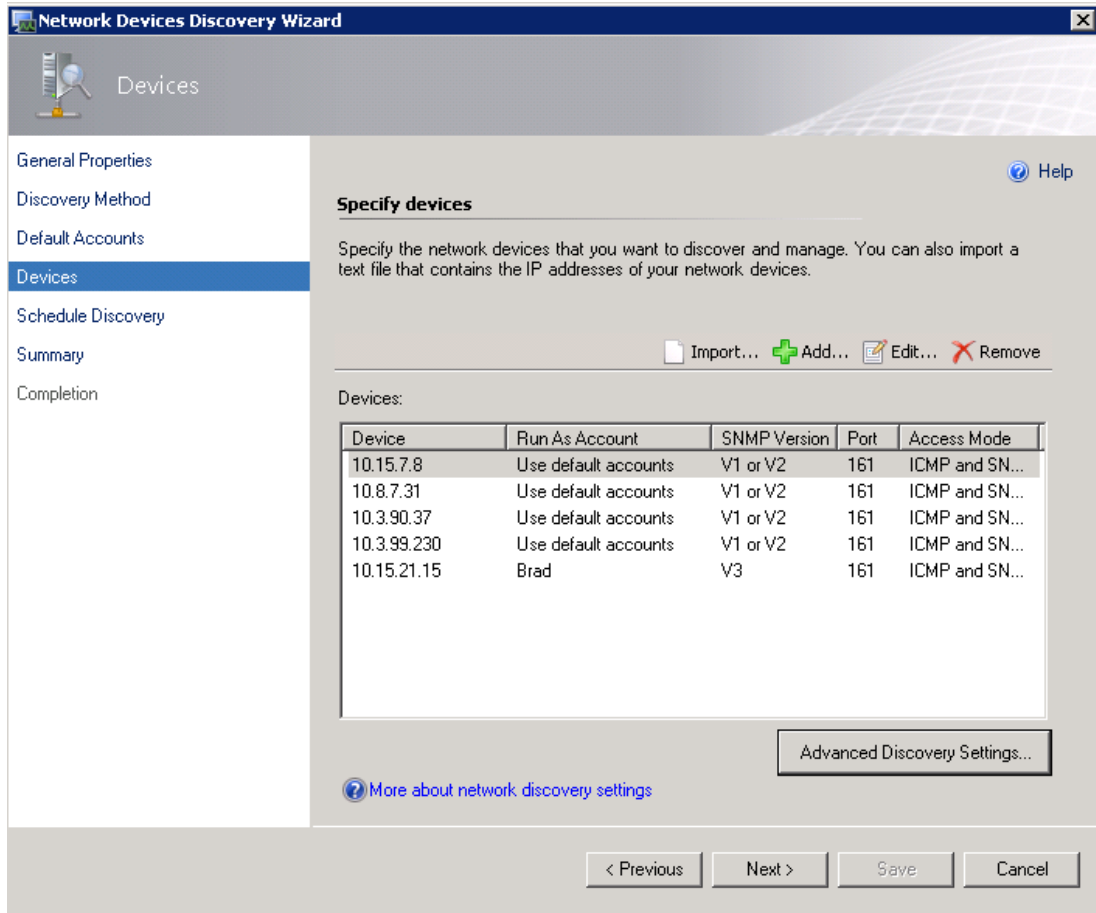
15. Click **OK**; the Schedule Discovery screen is displayed:

Figure 5-14: Schedule Discovery
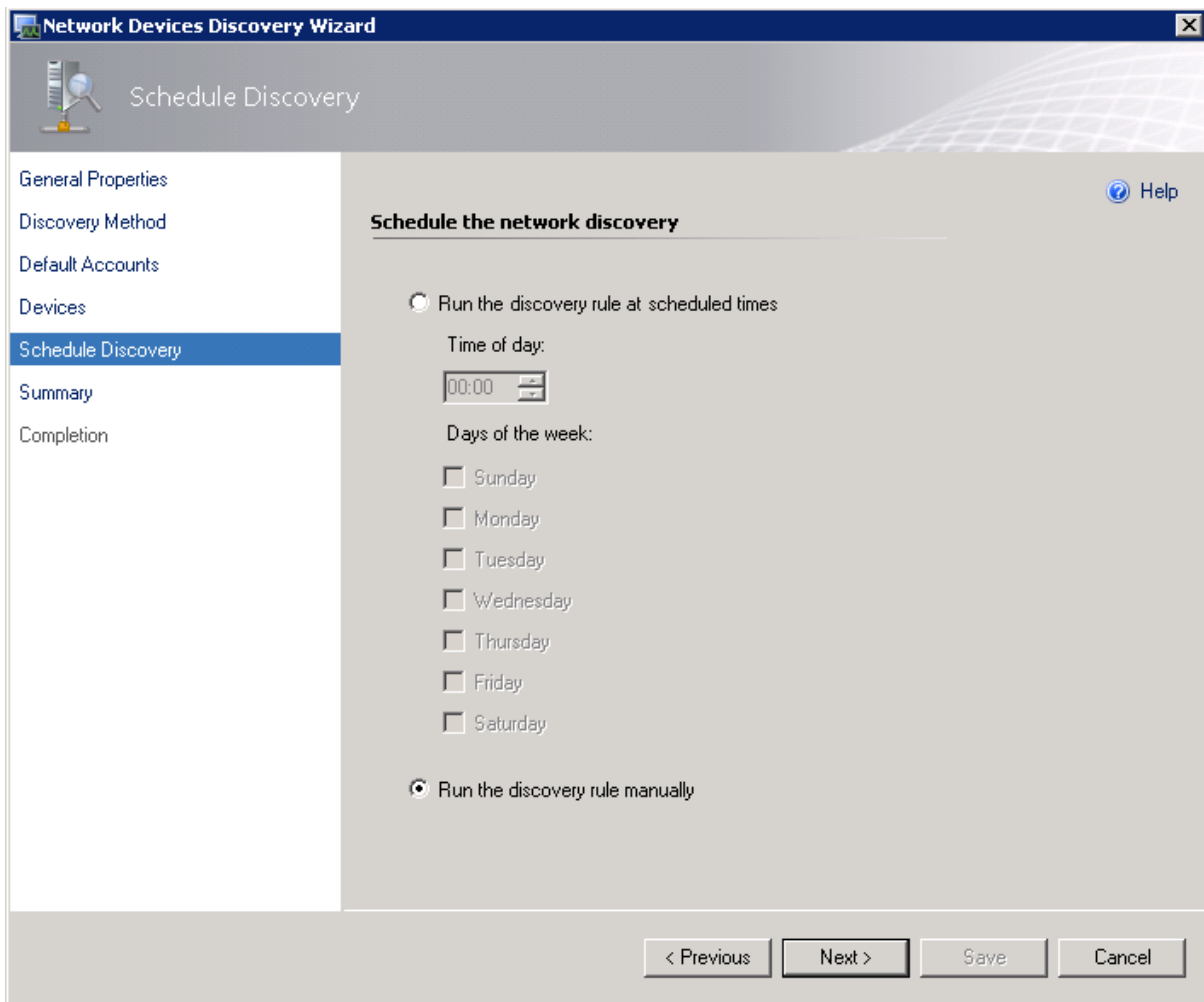
16. Select the **Run the discovery rule manually** option, and then click **Next**; the Summary page is displayed:

Figure 5-15: Summary

17. Review the settings, and then click **Save**.

The following message may be displayed:

Figure 5-16: Warning
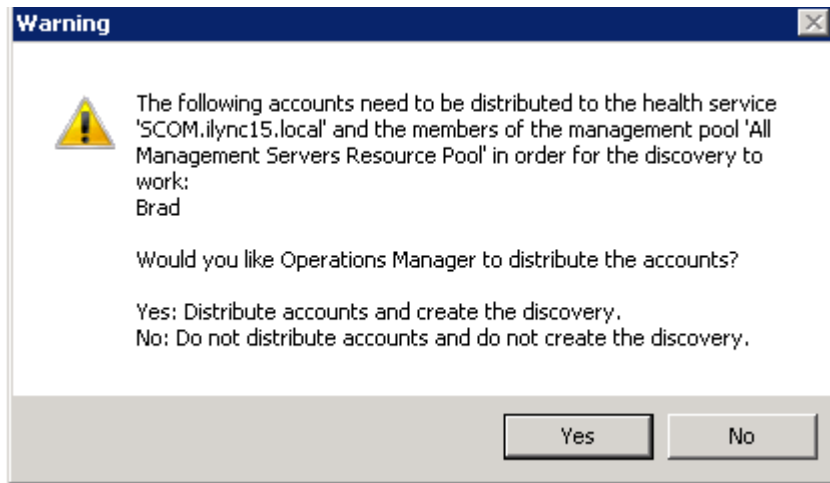
18. Click **Yes** to confirm.
19. Wait for the discovery rule to complete saving.

Figure 5-17: Discovery Saving Progress
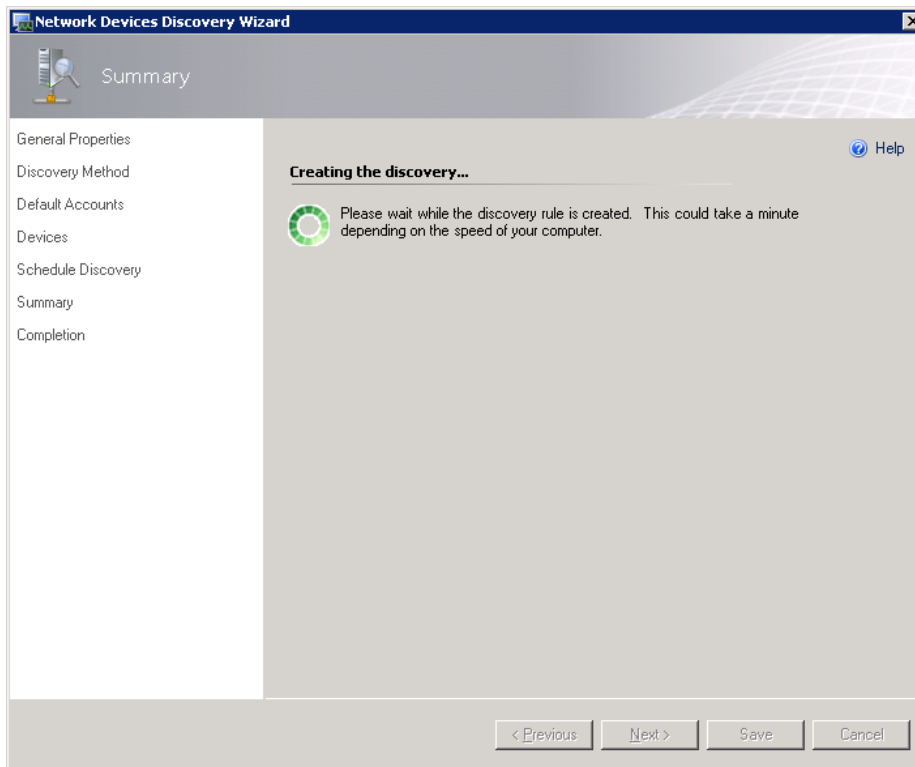
20. Click the **Close** button; a confirmation window is displayed:

Figure 5-18: Network Discovery Rule Confirmation
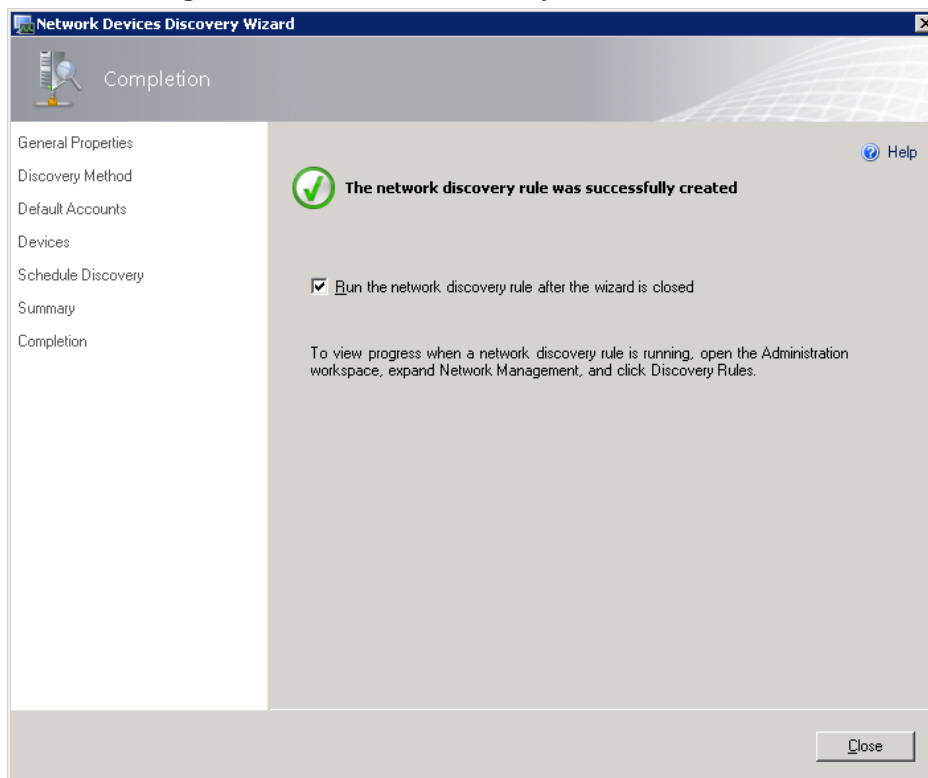
21. Wait for the SCOM to make a full discovery.

5.2 Disabling SNMP Trap Service

In order to view traps from the monitored AudioCodes devices, you must disable the SNMP Trap service.

➢ **To disable SNMP Trap services**

1. **Click** > **Start** > **Administrative Tools** > **Services**.
2. Ensure that the service **SNMP Trap** is disabled.
3. Restart the service **System Center Management**.

5.3 Setting up the Device to Send SNMP Traps

In order for the device to automatically send SNMP traps to the SCOM server, you must configure the IP address of the SCOM server as a Trap Destination.

➢ **To send SNMPv3 traps to the SCOM:**

1. Open the SNMP Community String page (**SNMP** > **Community String**).

Figure 5-19: SNMP Community String

2. Ensure that the parameter 'Disable SNMP' is set to default **No**.
3. Click **Submit** to apply the changes.
4. Open the SNMP Trap Destinations screen (**SNMP** > **SNMP Trap Destinations**).

Figure 5-20: SNMP Trap Destinations

5. In the IP Address field, type the IP address of the SCOM server to which you wish to send traps.
6. From the Trap User drop-down list, select the SNMP Trap User that you defined in either Section 5.1.1 on page 37 or in Section 4.1 on page 25.
7. Click **Submit** to apply the changes.
8. (Optional): In the SNMP Trusted Manager screen, type the IP address of the SCOM server to which you wish to send traps.

Figure 5-21: Trusted Manager IP Address

SNMP Trap Destinations Parameters Description

Parameter	Description
Web: SNMP Manager **[SNMPManagerIsUsed_x]**	Enables the SNMP Manager to receive traps and checks the validity of the configured destination (IP address and port number). ▪ **[0]** (check box cleared) = (Default) Disables SNMP Manager ▪ **[1]** (check box selected) = Enables SNMP Manager
Web: IP Address **[SNMPManagerTableIP_x]**	Defines the IP address (in dotted-decimal notation, e.g., 108.10.1.255) of the remote host used as the SNMP Manager. The device sends SNMP traps to this IP address.
Trap Port **[SNMPManagerTrapPort_x]**	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid value range is 100 to 4000. The default is 162.
Web: Trap User **[SNMPManagerTrapUser]**	Associates a trap user with the trap destination. This determines the trap format, authentication level, and encryption level. ▪ v2cParams (default) = SNMPv2 user community string ▪ SNMPv3 user configured in 'Configuring SNMP V3 Users' (see Section 4.1 on page 25)
Trap Enable **[SNMPManagerTrapSendingEnable_x]**	Activates the sending of traps to the SNMP Manager. ▪ **[0]** Disable ▪ **[1]** Enable (Default)

9. Click **Submit** to apply the changes.

10. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

Figure 5-22: Resetting the Device

11. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).

12. Click the **Reset** button.

This page is intentionally left blank.

6   Viewing Gateway Element States

This section describes the GW Elements States. The following topics are described in this section:

- GW Element State View. See Section 6.1 below.
- Modules - All Modules State View. See Section 6.2 on page 57.
- Modules - System Modules State View. See Section 6.3 on page 58.
- Modules – Fan Tray State View. See Section 6.4 on page 59.
- Modules – Power Supply State View. See Section 6.5 on page 60.
- Trunks/Ports – Digital Trunks State View. See Section 6.6 on page.
- Trunks/Ports – Ethernet Ports State View. See Section 6.7 on page 62.

6.1   GW State View

This section describes the GW State View.

➢ **To open the GW State View:**

- In the AudioCodes Gateway folder, select **GW State View**; a screen similar to the following is displayed:

Figure 6-1: GW State View
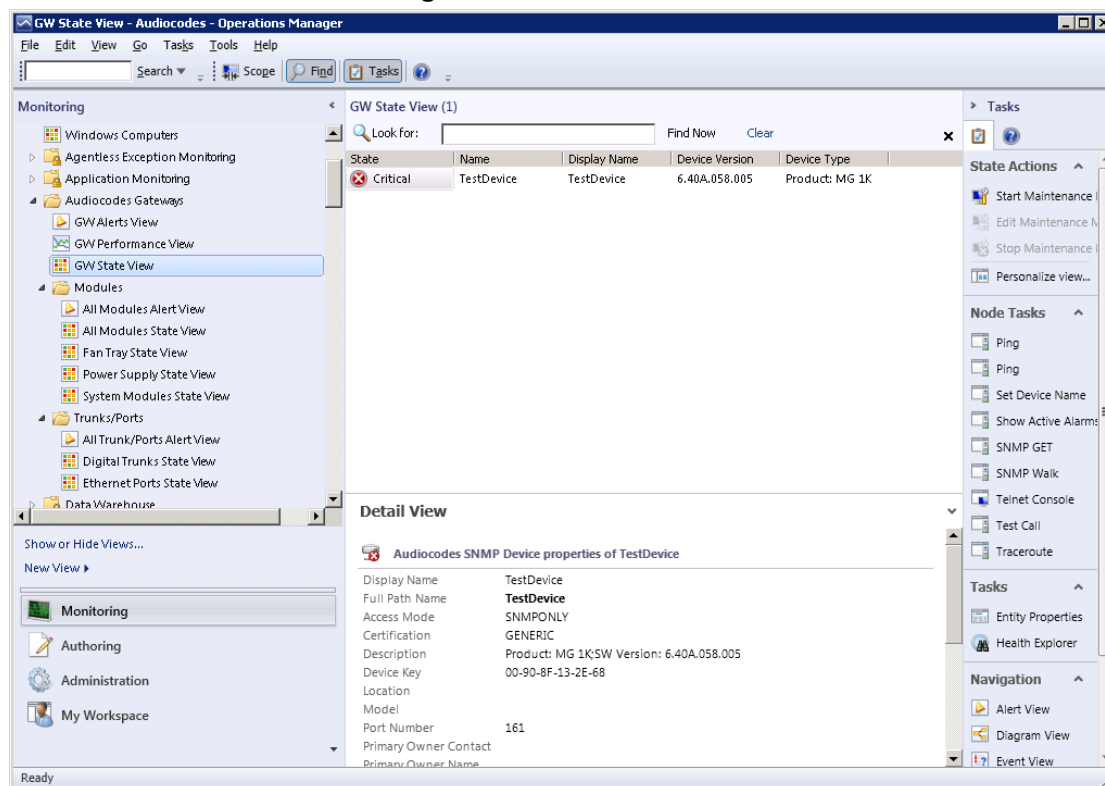
This screen is described as follows:

- The GW State View window contains all discovered gateways and their current health state.
- The Detail View pane at the bottom of the GW State View window contains the details of each selected gateway, including the Device address and description.GW State View contains several fields with specific information about the gateway, including 'State' and 'IP Address'.

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

- You can change the GW State View using the Personalize option – right-click any column name and select **Personalize View** or in the Tasks pane**,** select **Personalize View**; the Personalize View window is displayed:

Figure 6-2: Personalize View
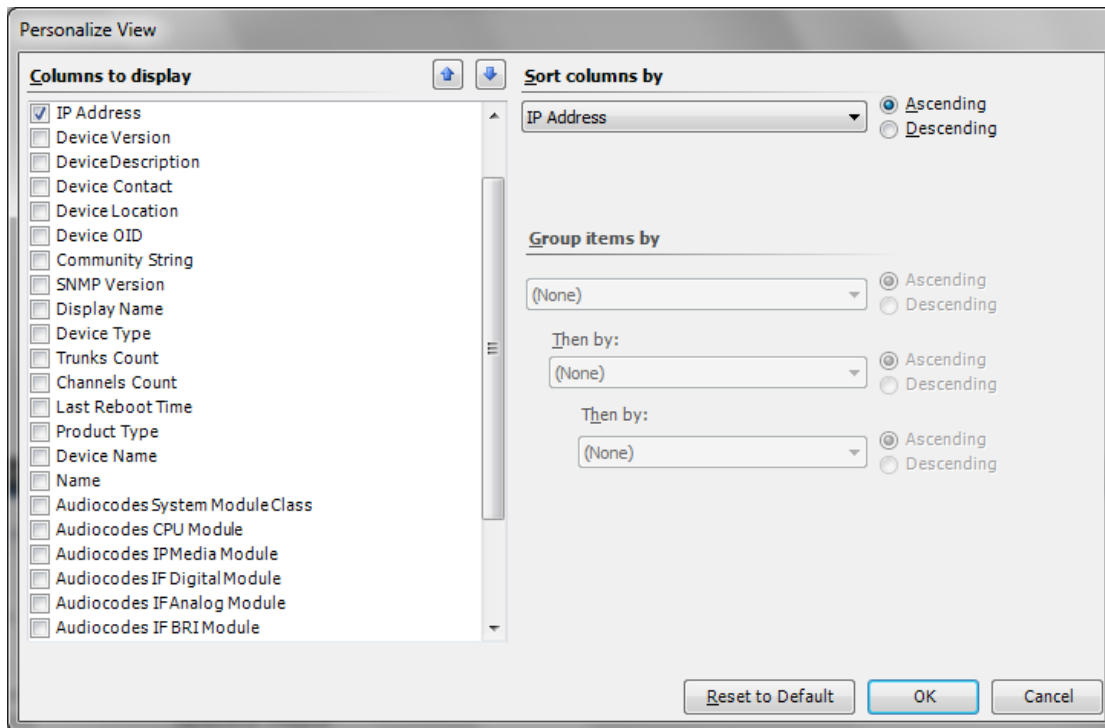
- In this window, you can select the fields you wish to view in the GW State View and sort the data inside the view.

- In addition, you can filter the data displayed in the view using the 'Look For' filter:

Figure 6-3: Look For Filter

6.2   Modules – All Modules State View

This section describes the All Modules State View.

➢ **To open the All Modules State View:**

■ In the AudioCodes Gateways folder, select **Modules** > **All Modules State View**; a screen similar to the following is displayed:

Figure 6-4: All Modules State View

This screen is described as follows:

- All Modules State View contains all modules of all discovered gateways as they are hosted on the real devices. The data represented in this view can be personalized as described in Section 6.1 on page 55.

- Select a module to load the Detail View pane at the bottom of the All Modules State View window.

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

> **Note:** Performance view is not supported at this monitoring level.

6.3 Modules – System Modules State View

This section describes the System Modules State View.

➢ **To open the System Modules State View:**

■ In the AudioCodes Gateways folder, select **Modules** > **System Modules State View**; a screen similar to the following is displayed:

Figure 6-5: System Modules State View
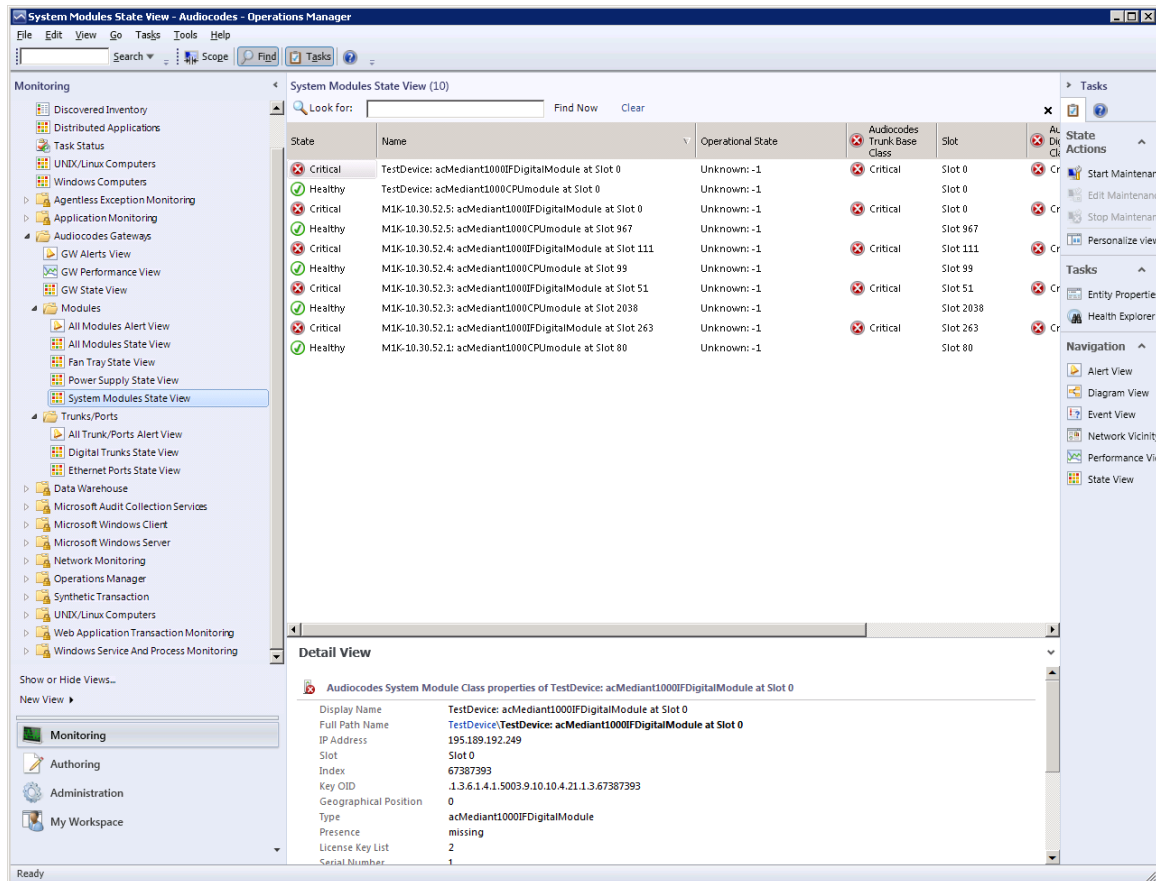
This screen is described as follows:

• System Modules State View contains all system modules of all discovered gateways as they are hosted on the real devices. The data displayed in this view can be personalized as described in Section 6.1 on page 55.

• Select a module to load the Detail View pane at the bottom of the System Modules State View window.

• Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

Note: Performance view is not supported at this monitoring level.

6.4   Modules – Fan Tray State View

This section describes the Fan Tray State View.

➢   **To open the Fan Tray State View:**

■   In the AudioCodes Gateways folder, select **Modules** > **Fan Tray State View**; a screen similar to the following is displayed:

Figure 6-6: Fan Tray State View
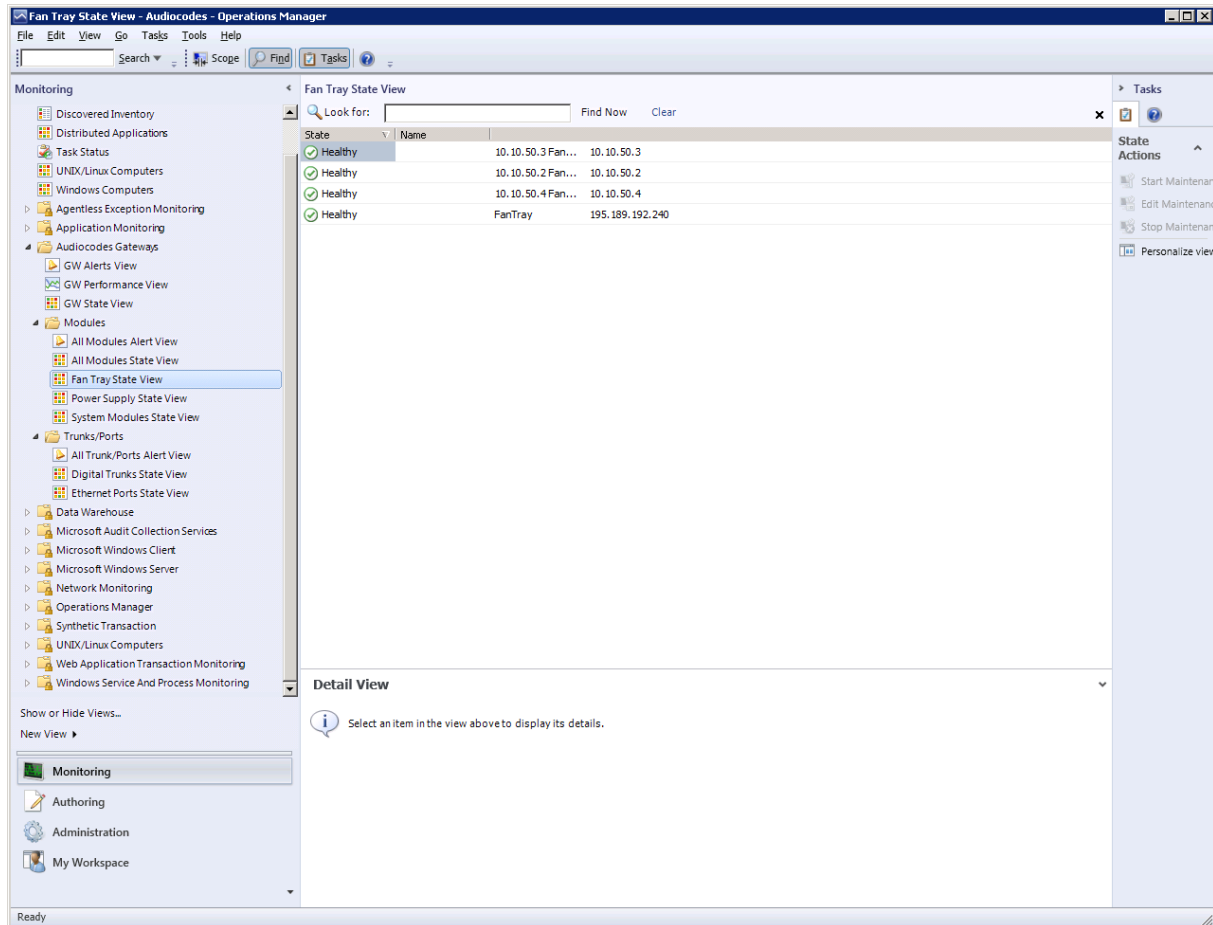
This screen is described as follows:

- Fan Tray State View contains all fan trays of all discovered GWs as they are hosted on the real devices. The data represented in the view can be personalized as described in Section 6.1 on page 55.

- Select a module to load the Detail View pane at the bottom of the Fan Tray State View window.

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

> **Note:** Performance view is not supported at this monitoring level.

6.5 Modules – Power Supply State View

This section describes the Power Supply State View.

➢ **To open the Power Supply State View:**

■ In the AudioCodes Gateways folder, select **Modules** > **Power Supply State View**; a screen similar to the following is displayed:

Figure 6-7: Power Supply State View
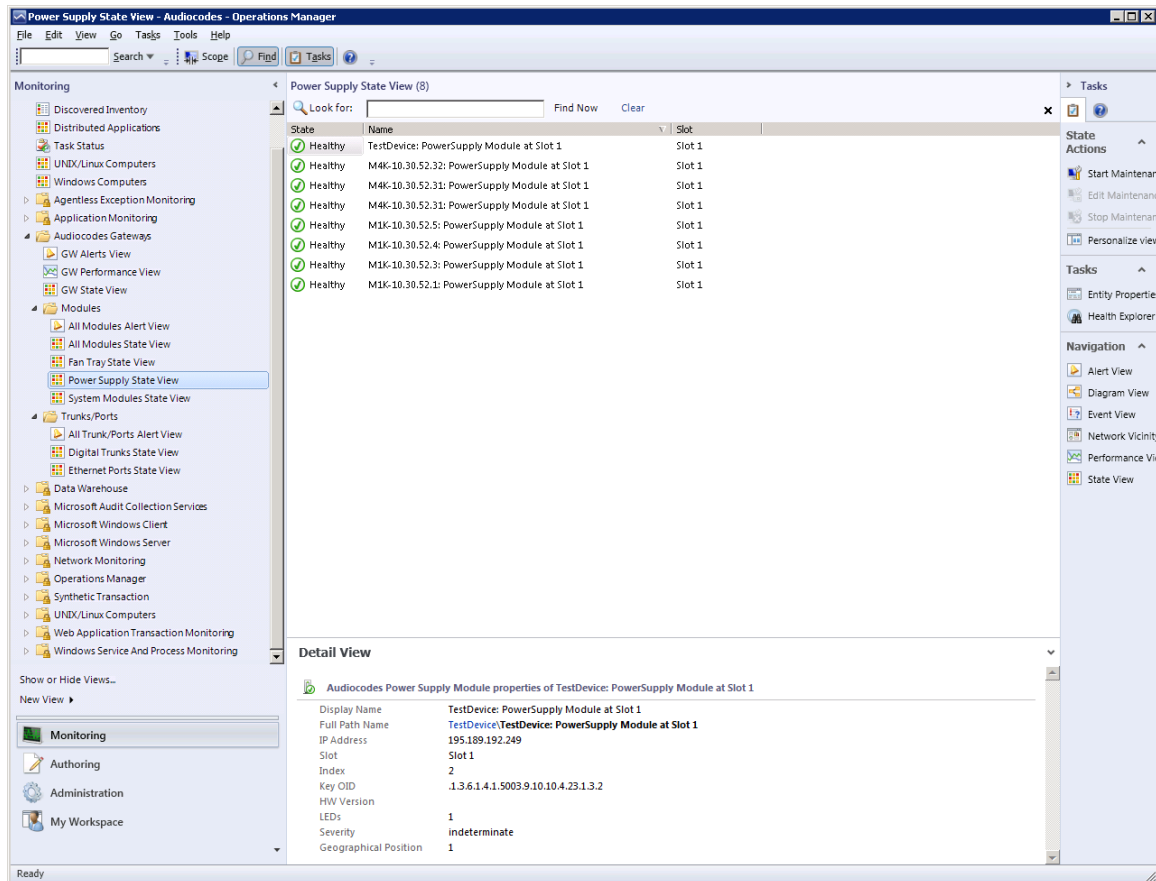
This screen is described as follows:

- Power Supply State View contains all power supply modules of all discovered GWs as they are hosted on the real devices. The data represented in the view can be personalized as described in Section 6.1 on page 55.

- Select a module to load the Detail View pane at the bottom of the Power Supply State View window.

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

⚠ **Note:** Performance view is not supported at this monitoring level.

6.6   Trunks/Ports – Digital Trunks State View

This section describes the Trunks/Ports – Digital Trunks State View.

➢ **To open the Trunks/Ports – Digital Trunks State View:**

■ In the AudioCodes Gateways folder, select **Trunk/Ports** > **Digital Trunks State View**; a screen similar to the following is displayed:

Figure 6-8: Digital Trunks State View
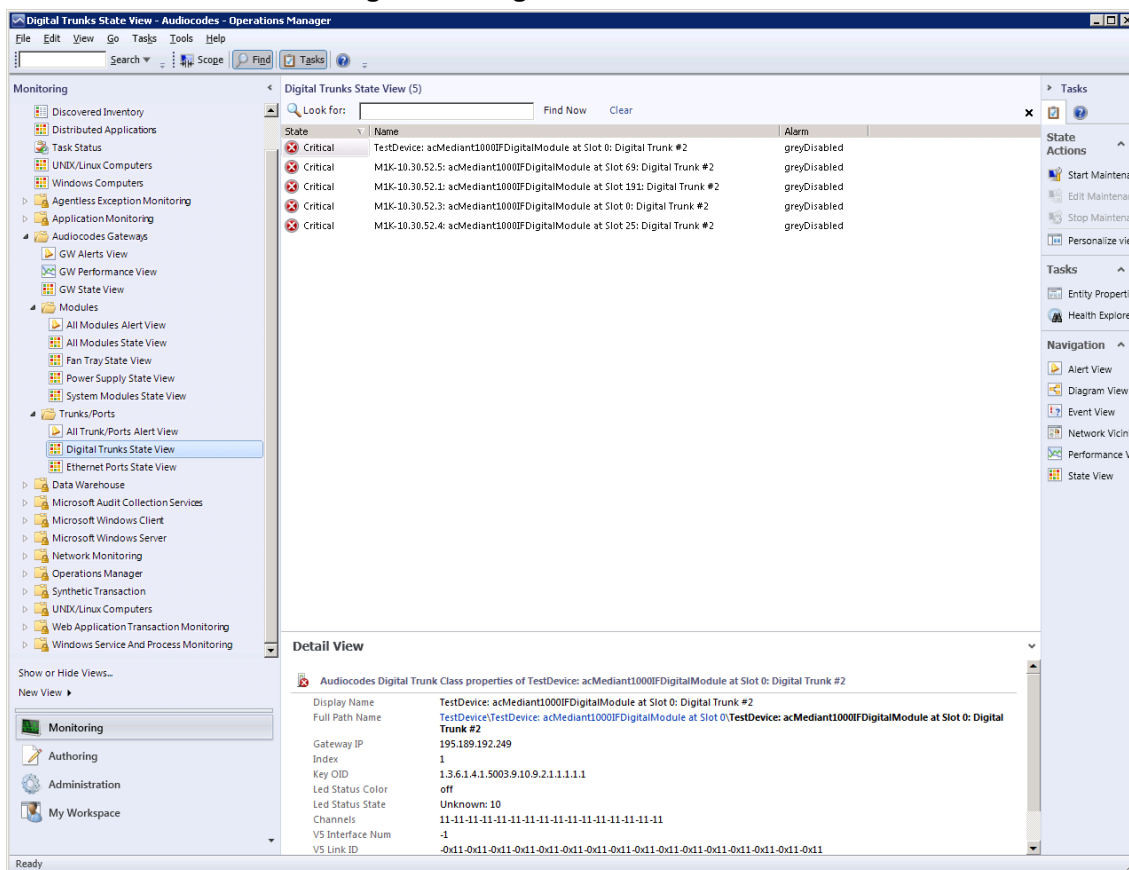
This screen is described as follows:

- Digital Trunks State View contains all digital trunks of all discovered gateways as they are hosted on the real devices. The data represented in the view can be personalized as described in Section 6.1 on page 55.

- Select a module to load the Detail View pane at the bottom of the Digital Trunks State View window.

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

6.7   Trunks/Ports – Ethernet Ports State View

This section describes the Trunks/Ports – Ethernet Ports State View.

➢ **To open the Trunks/Ports – Ethernet Ports State View:**

■ In the AudioCodes Gateways folder, select **Trunk/Ports** > **Ethernet Ports State View**; a screen similar to the following is displayed:

Figure 6-9: Ethernet Ports State View
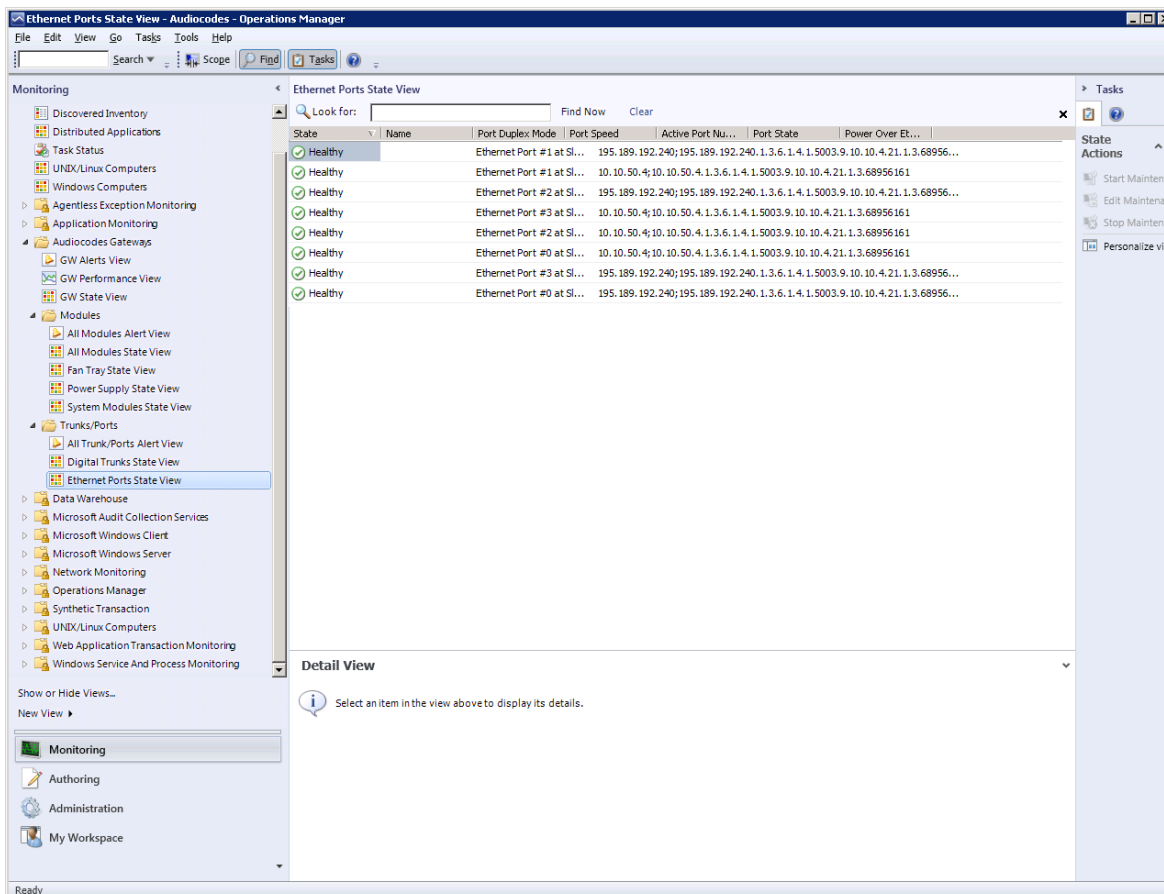
This screen is described as follows:

- Ethernet Ports State View contains all Ethernet ports of all discovered gateways as they are hosted on the real devices. The data displayed in this view can be personalized as described in Section 6.1 on page 55.

- Select a module to load the Detail View pane at the bottom of the Ethernet PortsState View window.

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

6.8   Diagram View

The Diagram View displays the Gateways' modules in a diagram view. Right-clicking the element in the diagram opens several additional options, such as opening element-related views and element-related properties.

➢ **To open the Diagram view:**

1. In the Monitoring pane, select **GW State View**, and then select the desired entry.

2. In the Tasks pane, under Navigation, select **Diagram View**; a screen similar to the following is displayed:

Figure 6-10: Diagram View
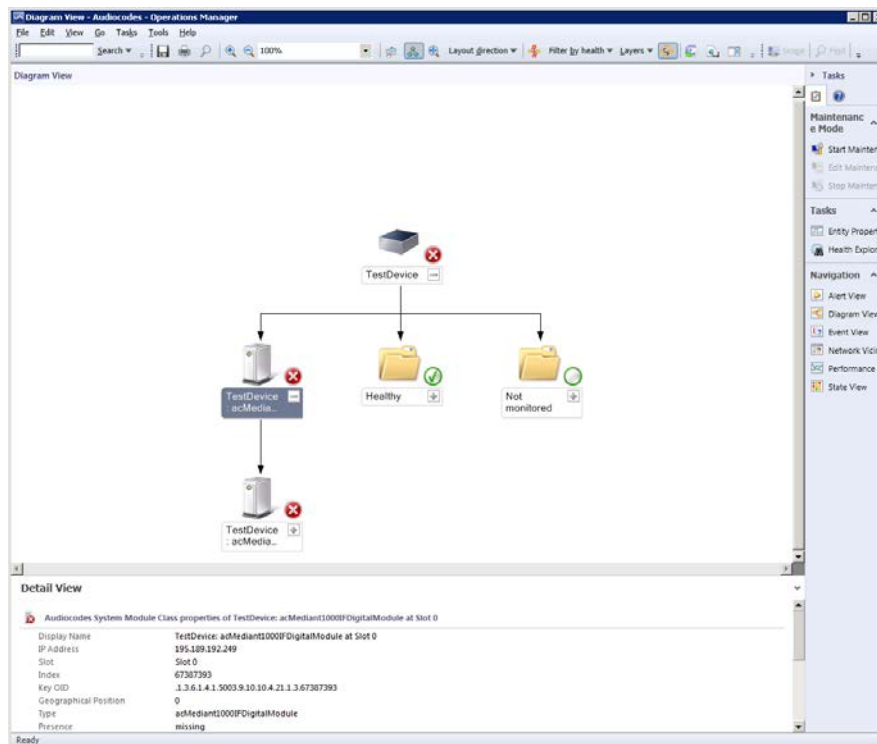
6.9 Running Tasks

This section describes how to perform various tasks.

6.9.1 Pinging AudioCodes Device

This task describes how to execute the ping operation on the device.

➢ **To execute the ping operation:**

1. Open the GW State View (see Section 6.1 on page 55) and select the required gateway.
2. Do one of the following:
   a. In the Node Tasks pane, left-click the **Ping** task.

Figure 6-11: Node Tasks Pane
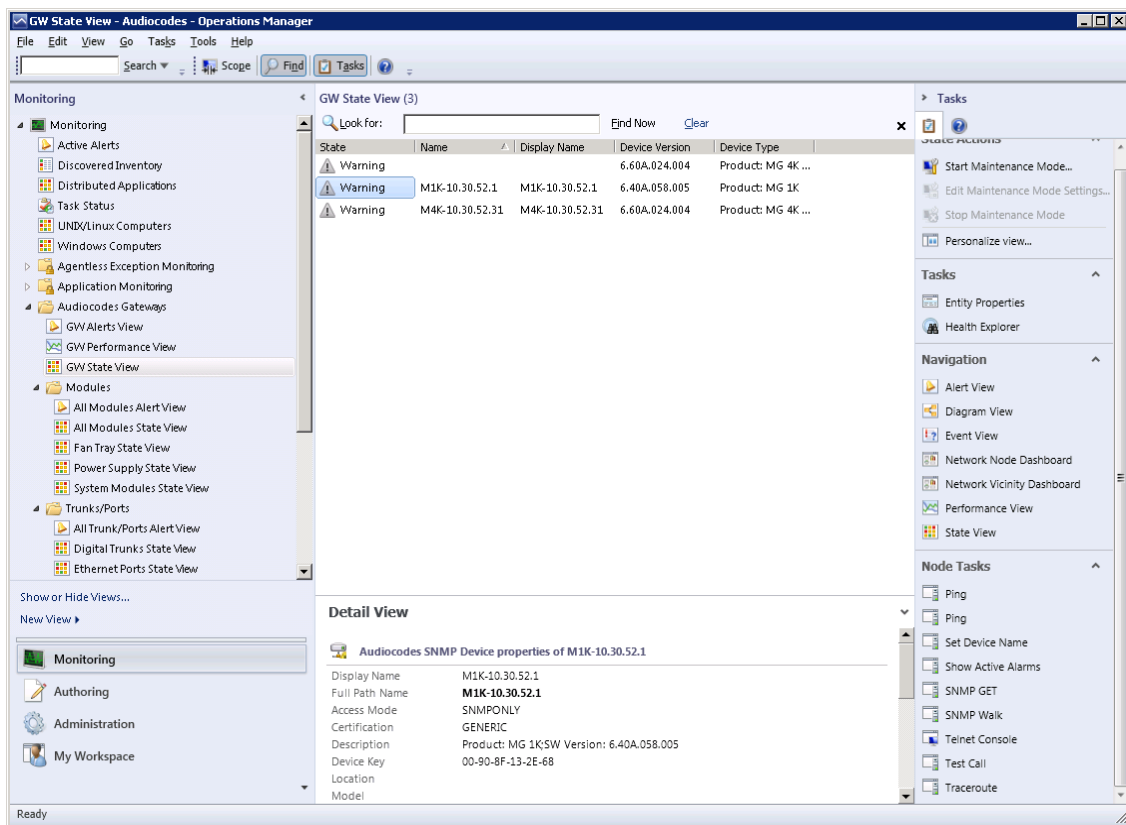
OR
   b. In the Main Menu, choose **Tasks** > **Node Tasks** > **Ping**.

Figure 6-12: Tasks Menu
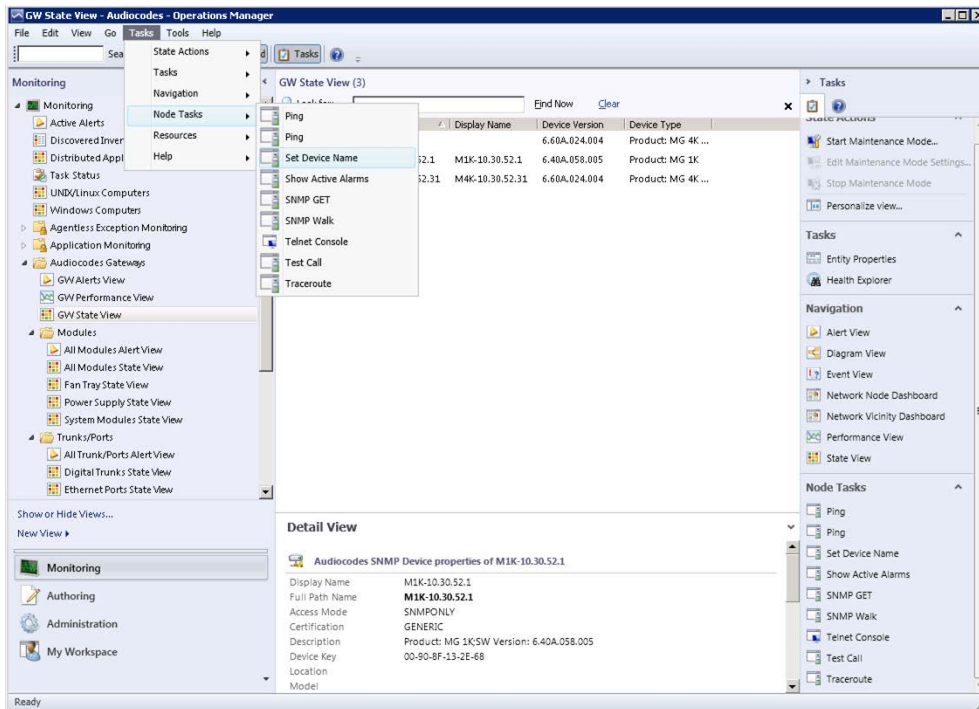
The Ping Run Task window is displayed:

Figure 6-13: Run Task-Ping
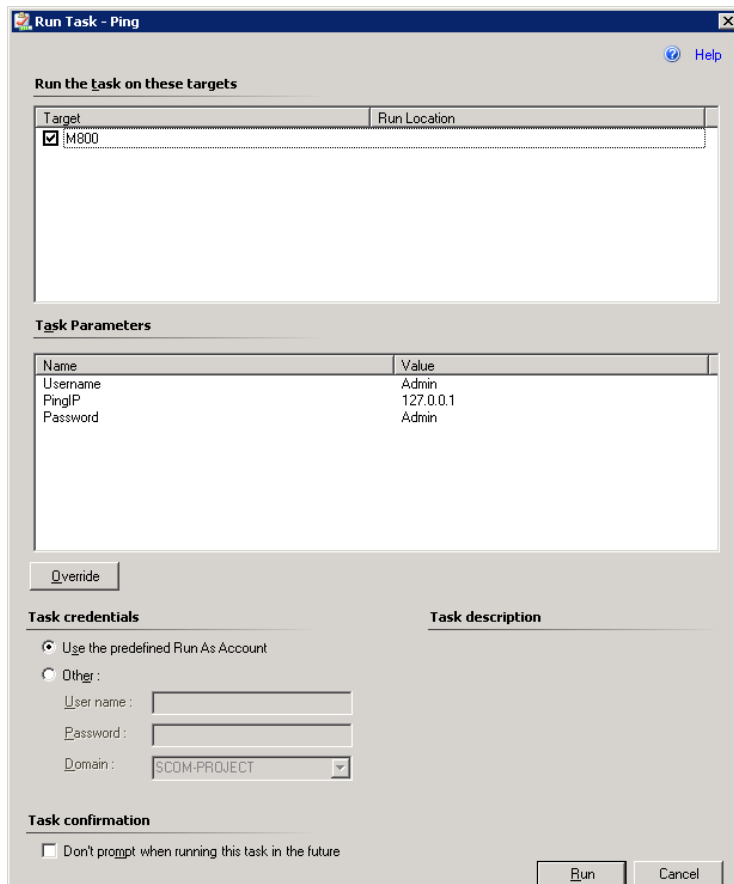
> ⚠️ **Note:** If you check the checkbox 'Don't prompt when running this task in the future' in the Task confirmation of the task configuration window (see Figure 6-13), the next time the Ping task is run immediately without the ability to change the task configuration.

4.   (Optional) Override the Username and/or Password for the Telnet connection:

   a.   In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.

   b.   Set the new values for Username and/or Password and Device Name.

   c.   Click the **Override** button.

5.   In the Run Task window, click the **Run** button; the Task Status – Ping window is displayed:

Figure 6-14: Task Status-Ping
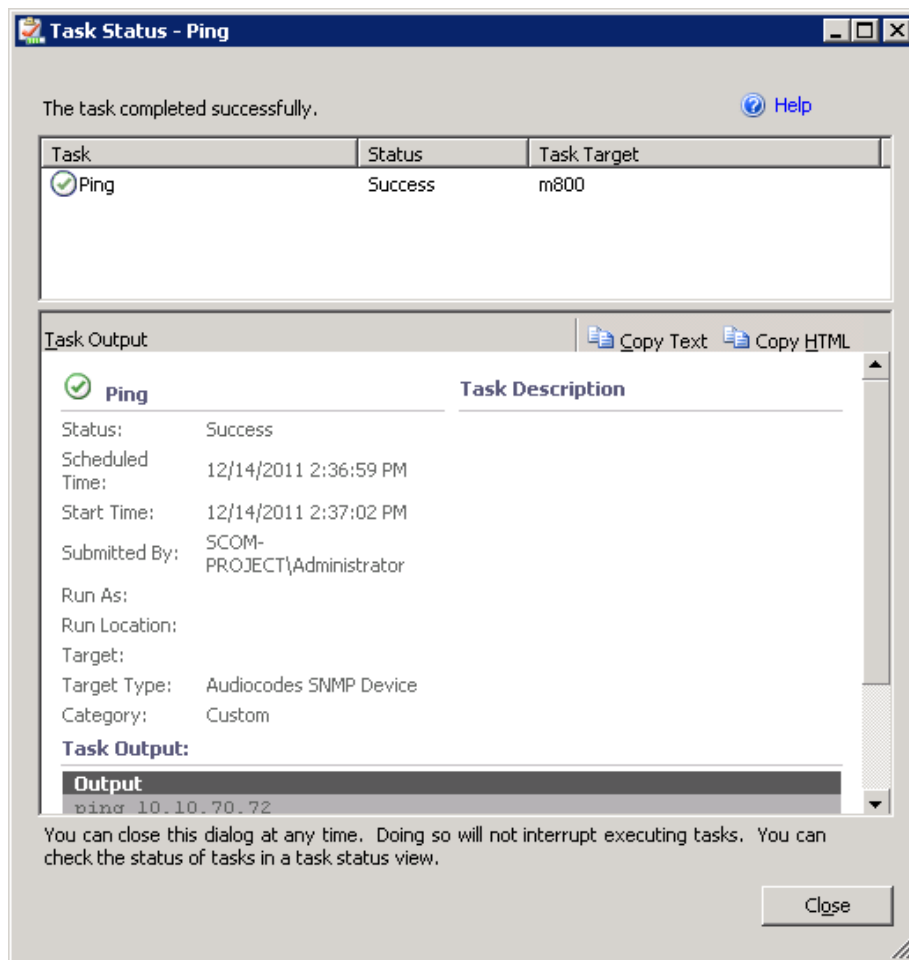
This window contains the Task execution status and output details.

6.9.2 Displaying Active Alarms

This task describes how to display the active alarms in the 'acActiveAlrmTable' table.

➢ **To display the list of active alarms:**

1. Open the GW State View (see Section 6.1 on page 55) and select the required gateway.

2. Do one of the following:

   a. In the Node Tasks pane, left-click the **Show Active Alarms** task.
   OR

   b. In the Main Menu, choose **Tasks** > **Node Tasks** > **Show Active Alarms**.

   The Show Active Alarms Run Task window is displayed:

Figure 6-15: Run Task-Show Active Alarms

> **Note:** If you check the checkbox 'Don't prompt when running this task in the future' in the Task confirmation of the task configuration window (see Section Figure 6-15), the next time the 'Show Active Alarms' task is run immediately without you being able to change the task configuration.

3. (Optional) Override the Username and/or Password for the Telnet connection:
   a. In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.
   b. Set the new values for Username and/or Password.
   c. Click the **Override** button.
4. In the Run Task window, click the **Run** button; the Task Status – Show Active Alarms window is displayed:

Figure 6-16: Task Status-Show Active Alarms
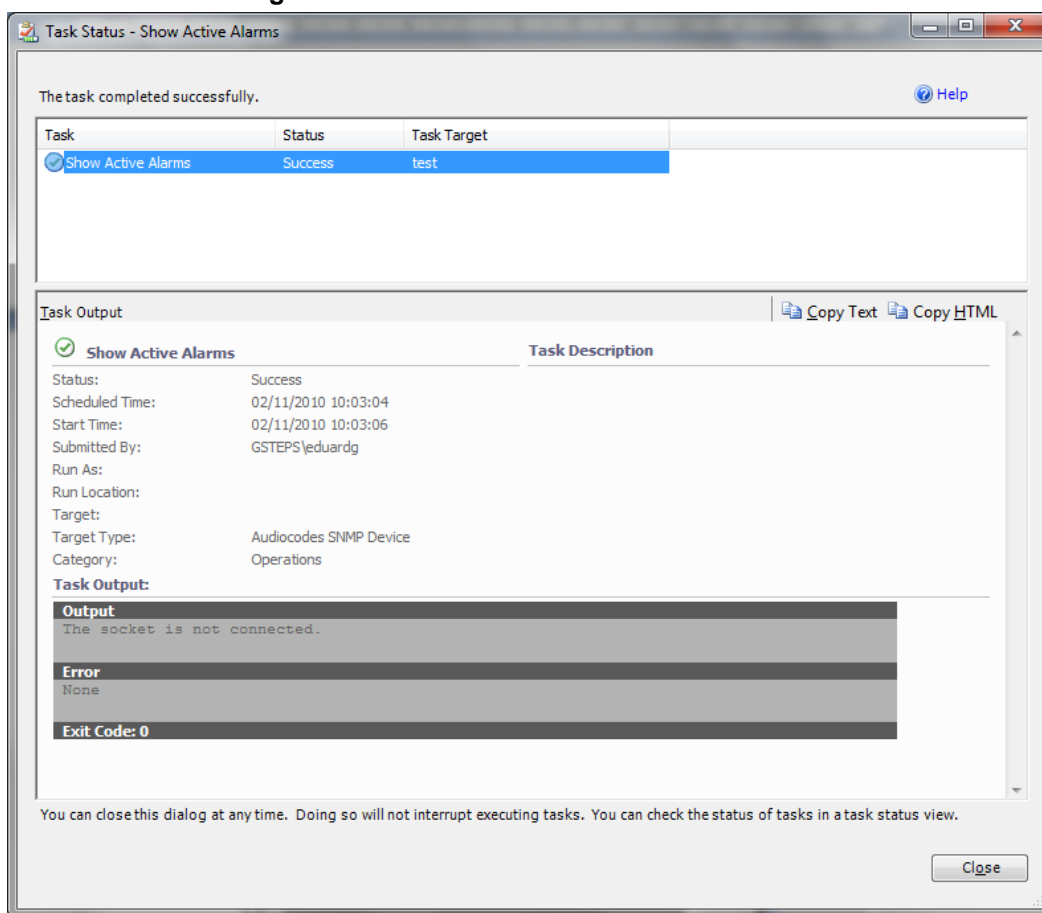
This window contains the Task execution status and output details.

6.9.3   Setting Device Display Name

This task describes how to change the device Display Name in the GW State View table.

➢ **To change the device Display Name:**

1. Open the GW State View (see Section 6.1 on page 55) and select the required gateway.
2. Do one of the following:
   a. In the Node Tasks pane, left-click the **Set Device Name** task.
       OR
   b. In the Main Menu, choose **Tasks** > **Node Tasks** > **Set Device Name**.
   The Set Device Name Run Task window is displayed:

Figure 6-17: Set Device Name

> **Note:** If you check the checkbox 'Don't prompt when running this task in the future' in the Task confirmation of the task configuration window (see Section Figure 6-15), the next time the 'Show Active Alarms' task is run immediately without you being able to change the task configuration.

3. (Optional) Override the DeviceName and/or CommunityString:

    a. In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.

    b. Set the new values for DeviceName and/or CommunityString.

    c. Click the **Override** button.

4. In the Run Task window, click the **Run** button; the Task Status – Set Device Name window is displayed:

Figure 6-18: Task Status-Set Device Name
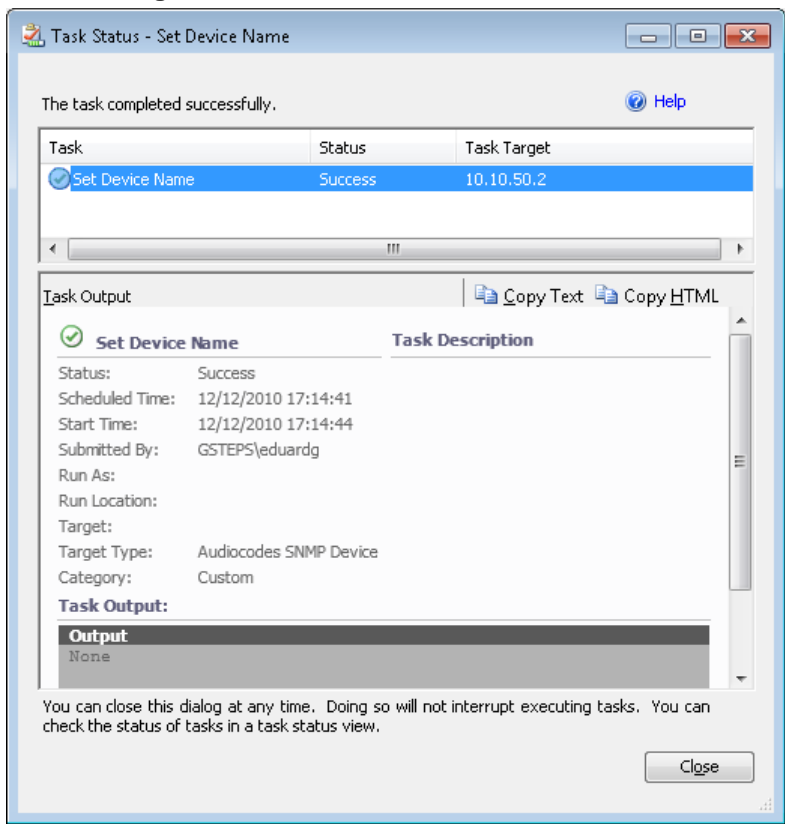
This window contains the Task execution status and output details.

6.9.4   Testing Call from Gateway

This task describes how to execute the test call from the gateway.

➢ **To test a call from the gateway:**

1. Open the GW State View (see Section 6.1 on page 55) and select the required gateway.

2. Do one of the following:

   a. In the Node Tasks pane, left-click the **Test Call** task.

   OR

   b. In the Main Menu, choose **Tasks** > **Node Tasks** > **Test Call**.

   The Test Call Run Task window is displayed:

Figure 6-19: Run Task – Test Call

> **Note:** If you check the checkbox "Don't prompt when running this task in the future" in Task confirmation of the task configuration window (see Figure 6-20 below), the next time you run the 'Test Call' task, it is run immediately without you being able to change the task configuration.

3. (Optional) Override the Username and/or Password for the Telnet connection:

a. In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.

b. Set the new values for the Username and/or Password.

c. Click the **Override** button.

> **Note:** Do not override the DTMFs and Destination PhoneNumber parameters.

4. In the Run Task window, click the **Run** button; the Task Status – Test Call window is displayed:

Figure 6-20: Task Status-Test Call
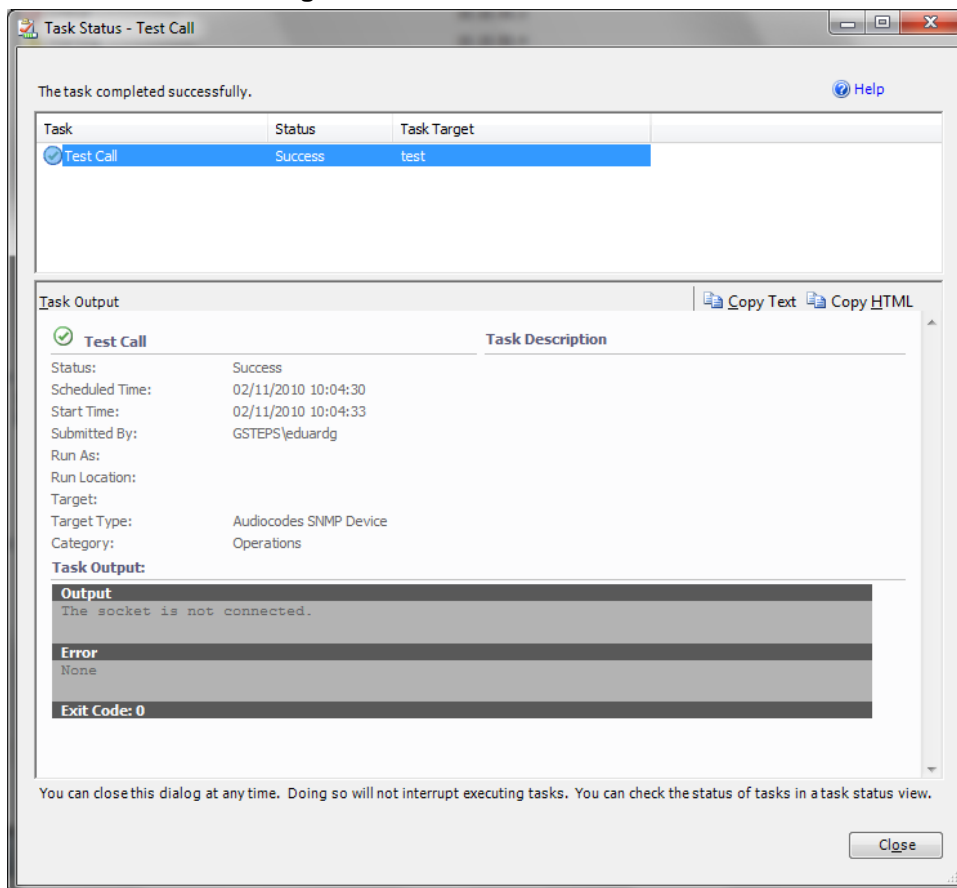
This window contains the Task execution status and output details.

7 Monitoring Gateway Element Health

Once a gateway is discovered, SCOM starts monitoring the gateway to determine its health state. Monitoring is performed for each discovered 'Gateway', 'Module' and 'Trunk' (together referred to as gateway elements).

7.1 Monitoring Types

The SCOM server collects data from the gateways using the following methods:

■ **Queries send from the SCOM to the gateway:**

- **Object-based monitoring** is the polling of a specific SNMP object value change i.e., the acSysModuleOperationalState module-related object is changed. For example, there is a power supply failure for a gateway power supply module.

- **Threshold-based monitoring** is an alert issued when a threshold defined for a performance counter is exceeded. This type of alert is applicable for gateways and trunks. Each performance counter has two types of thresholds 'High' and 'Low'. Each threshold type has two levels: 'Warning' and 'Critical'. Consequently, the final severity of threshold-based alert depends upon which level of threshold has been exceeded. Thresholds levels are described in Section 7.5 on page 82.

■ **Traps send from the gateway to the SCOM:**

- **Trap-based monitoring** is an alert issued as a result of a trap that was captured from an entire Gateway entity (Gateway, Module or Trunk).

> **Notes:**
> - Trap-based monitoring is not automatic. To enable this monitoring, you must configure the SCOM server as the trap destination. See Section 5.2 on page 50.
> - For a full list of all SNMP traps supported by the SCOM, see Appendix A on page 109.

7.2 Aggregated Health State

The final Health state of any entity is the aggregation of an entity-related alert and the Health states of its sub-elements (the Health state propagated from child element to the parent element).

Rollup Policy is used to determine this final health state of an entity. There are two types of Rollup policies used for the gateway health state definition:

■ **Best State** rollup policy defines the state of an entity as healthy in the event where at least one of its sub-elements is healthy, i.e. if a gateway contains several modules and at least one of the modules is healthy, then the overall state of the gateway is determined as 'Healthy'.

■ **Worst State** rollup policy defines the state of an entity according to the worst severity of any if its sub-elements, i.e. if a gateway contains several modules, where one of the modules is healthy, another module has the 'Warning' state and another is 'Critical', then the overall health state of the gateway is determined as 'Critical'.

> **Note:** Rollup Policy is not applicable for threshold-based alerts. For information on Configuring Threshold levels, see Section 7.7 on page 84.

7.2.1 Aggregated Health State-Gateway

The Aggregated health state of the gateway depends on the Fan Tray and Power Supply modules health together with the health states of all system modules residing on the gateway and is calculated according to the following rules:

■ **Worst state** Rollup policy - It is sufficient for the Fan Tray or Power Supply module to indicate 'Critical' for the corresponding gateway to indicate 'Critical'.

Dependence Rollup 'Worst State' policy is applicable for all corresponding Trunks/Ports residing on gateway modules.

■ **Best state** Rollup policy - It is sufficient for a single system module to indicate 'Healthy' for the corresponding gateway to indicate 'Healthy'.

Table 7-1: Health Indication

SNMP Object Health State	Indication
Green	The object is healthy.
Grey	The gateway exists in the list of network devices (**Administration** > **Network Devices**), it was successfully discovered at least once; however, is not responding to the monitors' requests.

7.3 SNMP-SCOM Object Severity Mapping

7.3.1 Gateway

The table below describes the translation of the gateway element health states to the corresponding SCOM health states.

Table 7-2: SNMP Gateway Objects Health State

SNMP Object Health State	SCOM Object Health State
noAlarm(0)	Healthy
intermediate(1)	Warning
minor(3)	Warning
major(4)	Critical
critical(5)	Critical

7.3.2 Module

The table below describes the translation of the module element health states to the corresponding SCOM health states.

Table 7-3:SNMP Gateway Modules Objects Health State

SNMP Object Module	SNMP Object Health State	SCOM Health State
acSysModuleOperationalState (System module)	enable(2)	Healthy
	disable(1)	Critical
acSysPowerSupplySeverity (Power Supply module)	Cleared(1)	Healthy
	Indeterminate(2)	Warning

SNMP Object Module	SNMP Object Health State	SCOM Health State
	minor(4)	Warning
	Major(5)	Critical
	Critical(6)	Critical

7.3.3   Digital Trunks

The table below describes the translation of the digital trunk element health state to the corresponding health state in the SCOM.

Table 7-4: Digital Trunk SNMP Polling

SNMP Object	SNMP Object Health State	SCOM Health State Indicator
acTrunkStatusAlarm	greenActive (1)	Healthy
	Other values	Critical

The monitor 'AudioCodes Digital Trunk Alarm' queries SNMP Object "Alarm" from table with OID 1.3.6.1.4.1.5003.9.10.9.2.1.1.1.1.

7.3.4   SNMP Traps

The table below describes the SNMP traps which cause the gateway module to indicate the Unhealthy state in the SCOM.

Table 7-5: Unhealthy State

Gateway Module	Trap	SCOM Unhealthy State
System modules	acHwFailureAlarm	Warning or Critical
Power Supply module	acPowerSupplyAlarm	Warning or Critical
Fan Tray module	acFanTrayAlarm	Warning or Critical
analog trunk module	acAnalogPortHighTemperature	Critical
	acAnalogPortSPIOutOfService	
Digital Trunk module	acTrunksAlarmNearEndLOS	Critical
	acTrunksAlarmNearEndLOF	
	acTrunksAlarmRcvAIS	
	acTrunksAlarmFarEndLOF	
Ethernet ports module	acBoardEthernetLinkAlarm	Critical

For more information on the traps described in the table below, see Appendix A on page 109.

7.4 Alert Monitoring

The SCOM Management Pack includes the following active alerts views:

- GW Alerts View. See Section 7.4.1 on page 76.
- All Modules Alerts View. See Section 7.4.2 on page 80.
- All Trunks/Ports Alerts View. See Section 7.4.3 on page 81.

7.4.1 GW Alerts View

GW Alerts View shows the entire gateway-related alerts (alerts related to the gateway and all hosted entities).

➢ **To view gateway alerts:**

1. Select the **Monitoring** pane, and then open the **AudioCodes Gateways** folder.
2. Select the **GW Alerts View**; a screen similar to the following is displayed:

Figure 7-1: GW Alerts View
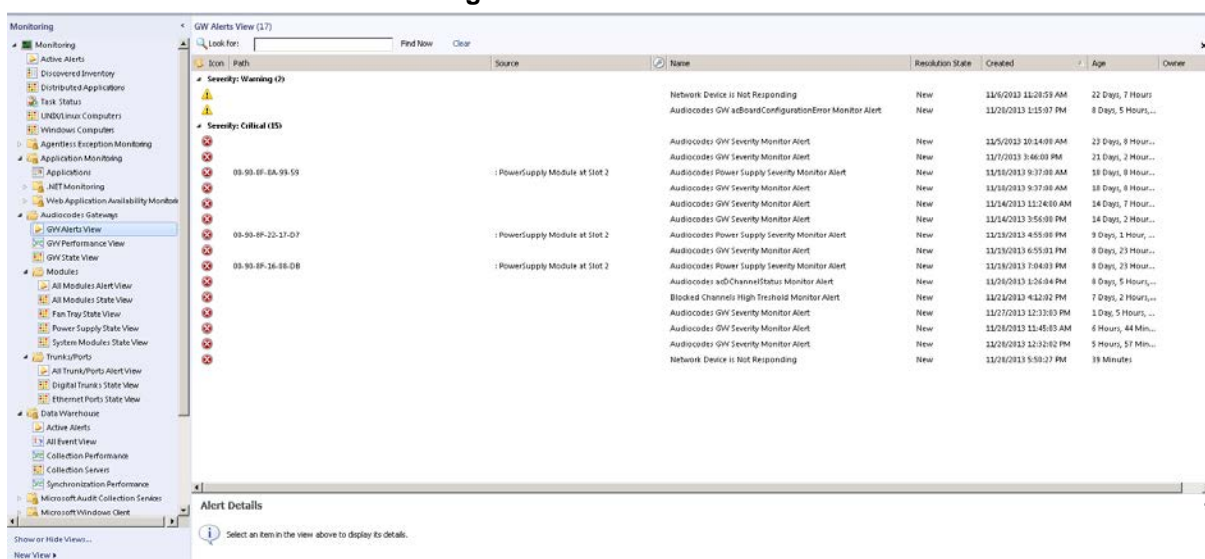
3. Select a specific Alert; the Alert Details are loaded:

Figure 7-2: Gateway Module Alert Details
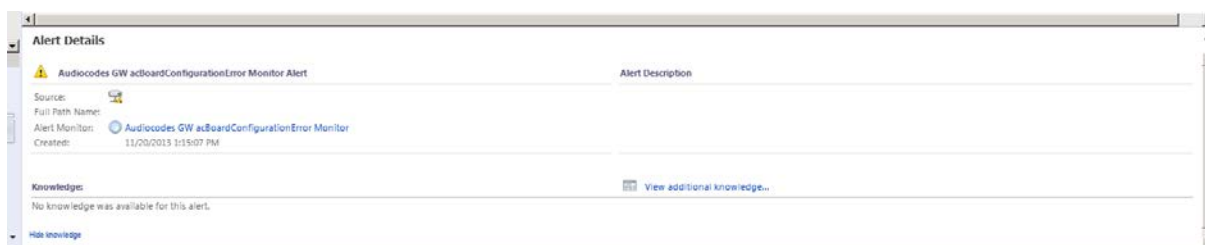
4. Click on the **View additional knowledge** Link to view additional information on the alert. The Alert Properties are displayed:

Figure 7-3: Alert Properties

Additional Information may be displayed in the Alert Description pane.

5. To view SNMP detailed information, select the **Alert Context** tab; the SNMP details for the alert are displayed:

Figure 7-4: Alert Properties-SNMP Information
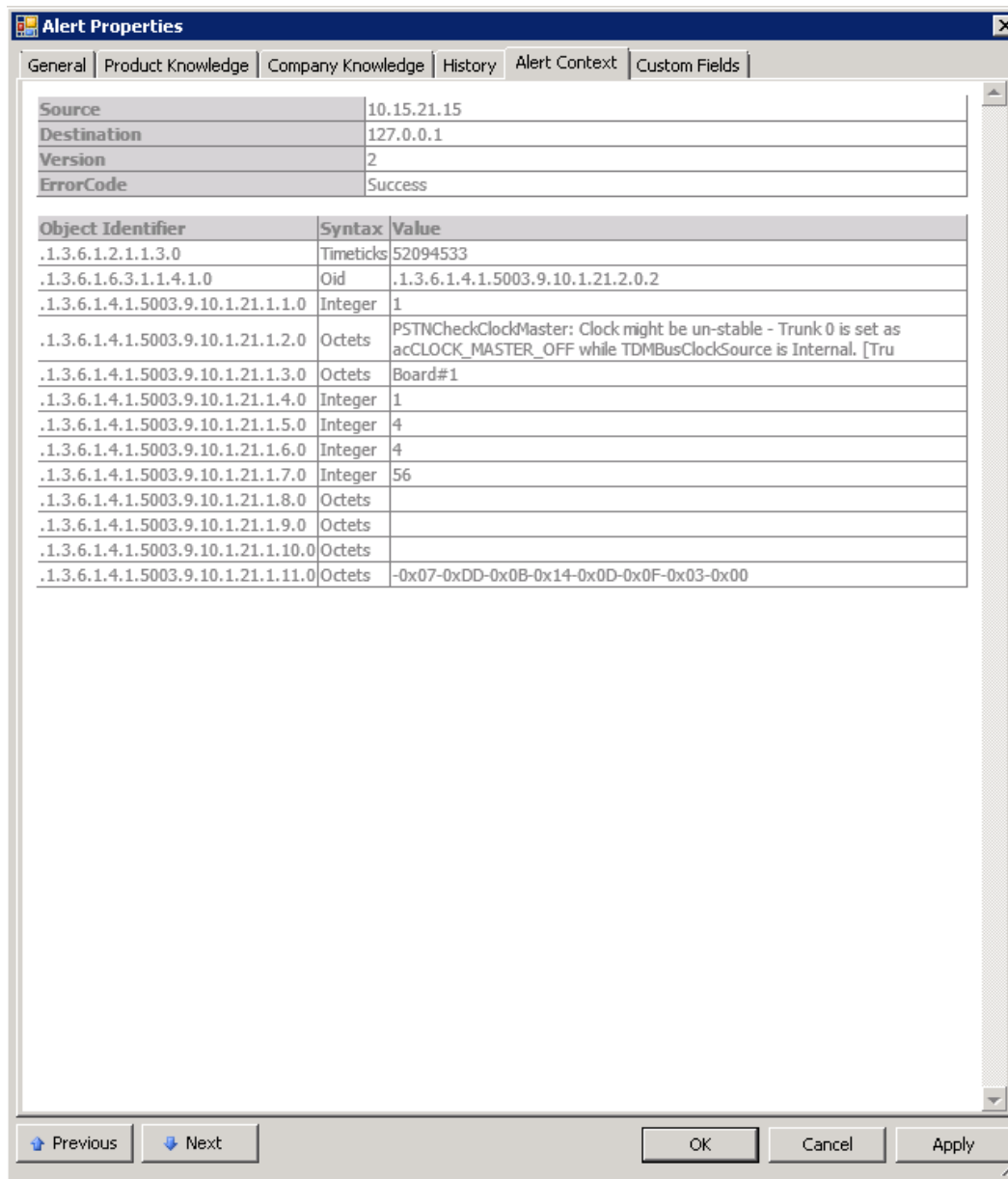
6. If you wish to configure the Alert Monitor, in the Alert Details screen, click the Alert Monitor, for example, click the **Audiocodes GW acBoardConfigurationError Monitor** link as shown in the figure below.

Figure 7-5: Gateway Monitor Alert Details
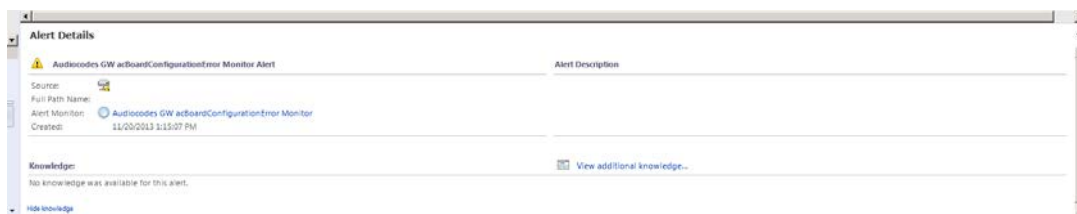
The gateway alert monitor properties are displayed:

Figure 7-6: Gateway Alert Monitor Properties

7. Select the **Overrides** tab to override the monitor. For more information, see Chapter 8 on page 91.

7.4.2   All Modules Alerts View

All Modules Alerts View shows the module-related alerts (alerts at the module level).

➢ **To view alerts for all modules:**

1. Select the **Monitoring** pane, and then open the **AudioCodes Gateways** folder.

2. Select the **All Modules Alerts View**; a screen similar to the following is displayed:

Figure 7-7: All Modules Alert View
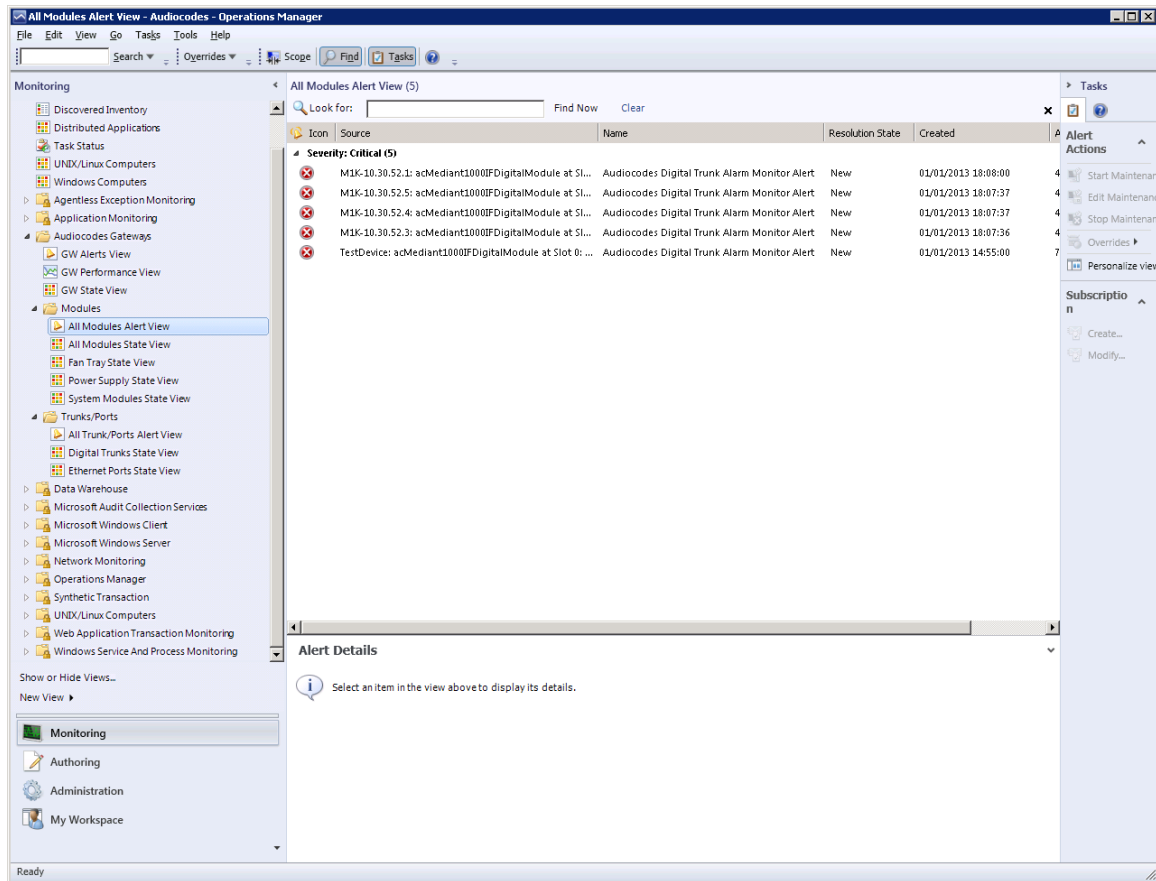
3. Select a specific Alert; the Alert Details are loaded.

Figure 7-8: Power Module Alert Details
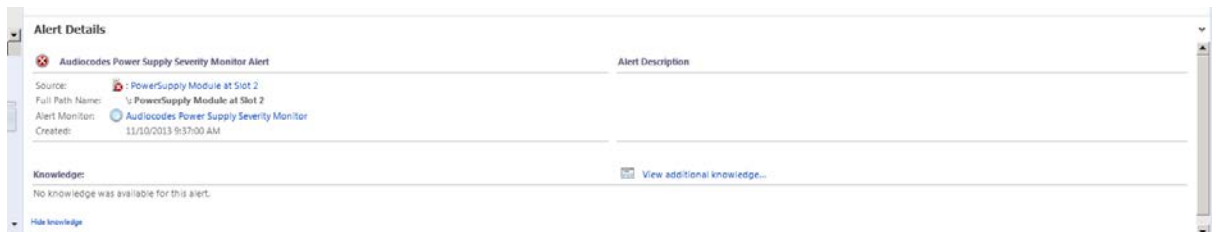
4. Click the **View additional knowledge** link to view additional details on the alert.

5. If you wish to configure the Alert Monitor, in the Alert Details screen, click the Alert Monitor, for example, click the **Audiocodes Power Supply Severity Monitor** link as shown in the figure above.

6. Select the **Overrides** tab to override the monitor. For more information, see Chapter 8 on page 91.

7.4.3   All Trunks/Ports Alerts View

All Trunks/Ports Alerts View shows the trunk/port-related alerts (alerts on trunk/port level).

➢ **To view alerts for all trunks/ports:**

1. Select the **Monitoring** pane, and then open the **AudioCodes Gateways** folder.

2. Select the **All Trunk/Ports View**; a screen similar to the following is displayed:

Figure 7-9: All Trunk/Ports View
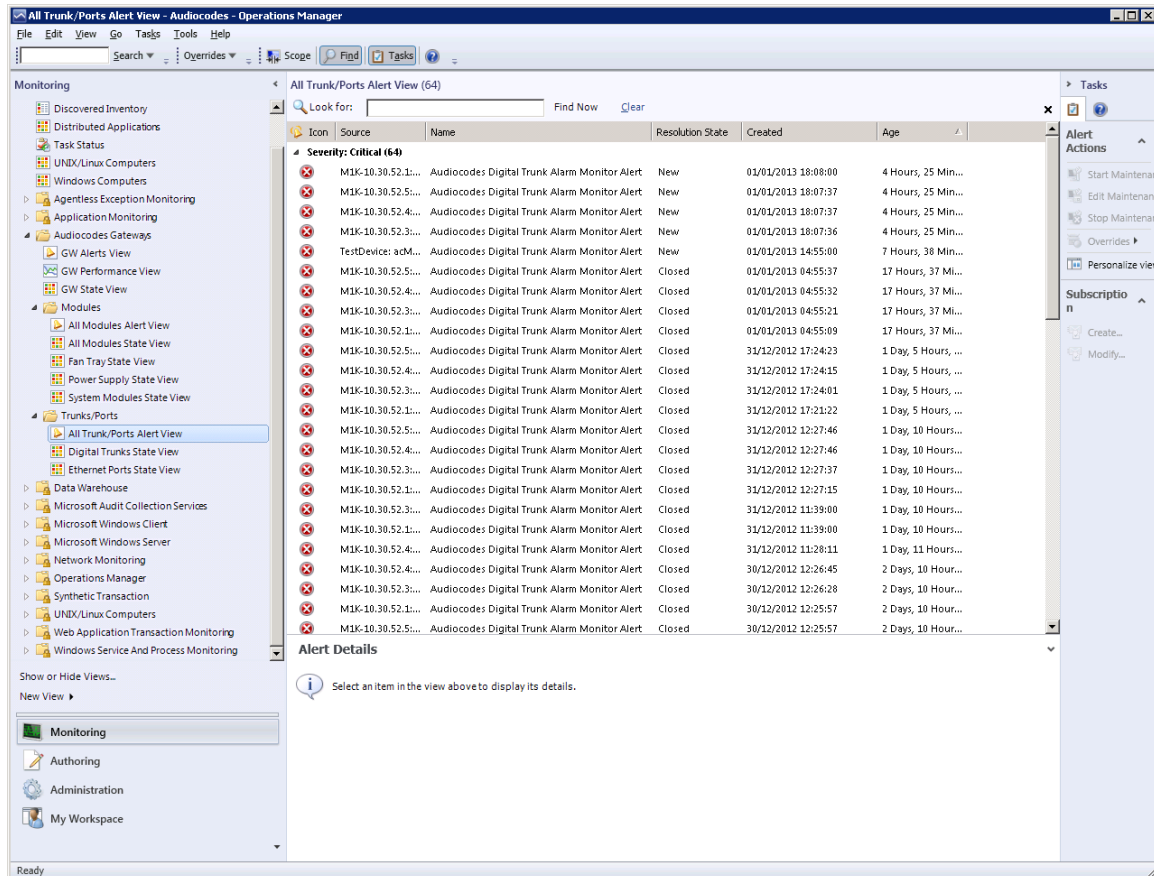
3. Select a specific Alert; the Alert Details are loaded.

Figure 7-10: All Trunk/Ports Alert Details
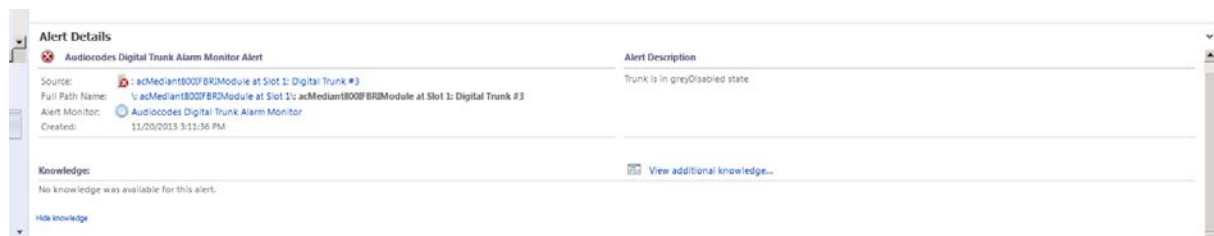
4. Click the **View additional knowledge** link to view additional details on the alert.

5. If you wish to configure the Alert Monitor, in the Alert Details screen, click the Alert Monitor, for example, click the **Audiocodes Digital Trunk Alarm Monitor** link as shown in the figure above.

6. Select the **Overrides** tab to override the monitor. For more information, see Chapter 8 on page 91.

7.5 Performance Monitoring

The AudioCodes device enables performance monitoring in the form of 'counters' for gateway and trunk modules. For example, for a gateway module, AudioCodes' Mediant 4000 device's 'Attempted Calls IP2Tel' counter polls the number of attempted IP to Tel calls during the last interval. For a trunk module, the AudioCodes Digital Trunk Available Channels counter polls the number of available in-service trunks for a specific trunk group. In the SCOM, the PM counter is represented by a rule (see Section 7.6 on page 83).

Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the server is reset, and then the counters are reset to zero.

Additionally, each counter rule is represented by a pair of threshold monitors (a high threshold monitor and a low threshold monitor). For example, the 'Attempted Calls IP2Tel' PM is represented in the SCOM by the 'AudioCodes Attempted Calls IP2Tel High Threshold Monitor'' and 'AudioCodes Attempted Calls IP2Tel Low Threshold Monitor'. For more information, see Section 7.7 on page 84.

For details on the performance monitoring counters that are supported by the AudioCodes Management Pack, see Section B on page 169.

7.5.1 Performance View

This section describes the performance view.

➢ **To open the Performance View,**

■ In the Monitoring pane, select **GW Performance View**.

Figure 7-11: GW Performance View
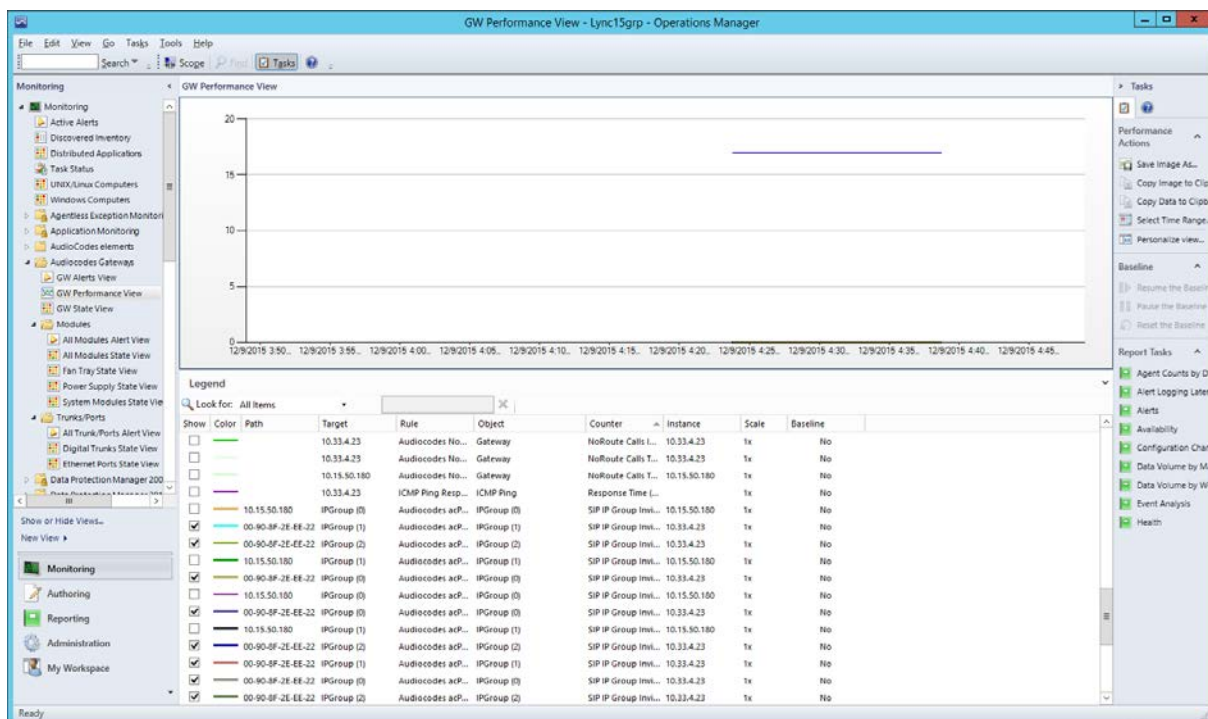
> **Note:**
>
> • The 'Object' field displays the IP Group index, on IP Group counters, and the SRD name on SRD counters.
> • IP Group name is not displayed in the SCOM.

- Right-clicking the graph opens the Personalize View and other options which allow you to customize the graph.

- The GW Performance View allows you to view gateway performance counters behavior. In the Legend window, you can select one or more counters to view them on the graph. Each counter on the graph has its own color. Using the 'Look for:' filter, you can limit the Legend to show only the counters on the graph (Items in the Chart) or only the counters which are not shown on the graph (Items not in the Chart) or specific counters (Items by text search). By default, all counters are available for selection in the Legend window (All Items).

- The GW Performance View provides updated information on most counters every 15 minutes. Counters for Channels provide updated information per minute. A graph can be refreshed manually (F5) or automatically.

7.6   Rules Monitoring

Rules are used in the SCOM for managing the AudioCodes SIP Performance Monitoring counters and for managing the Trunk Service Information.

Figure 7-12: Rules Monitoring

7.6.1   SIP Performance Monitoring Counters

SIP PM counters rules poll data from the AudioCodes devices by default every 15 minutes. The AudioCodes Management Pack includes a corresponding rule for each supported PM. For example, "Attempted Calls IP2Tel Counter Rules".

For a full list of PM counters supported by the SCOM, see Appendix B on page 169.

7.6.2   Trunk Service Information

Trunk Service counters (Trunk Performance Statistics) monitor the Channels states (channel in-service and channel out-of-service). The counters 'AudioCodes Digital Trunk Available Channels Counter Rule' and the 'AudioCodes Digital Trunk Blocked Channels Counter Rule' poll the trunk channel information.

7.7 Threshold Monitoring

This section describes how to configure the threshold values for the device PM counters. For each supported PM counter rule there is a pair of threshold monitors; a high level threshold monitor and a low level threshold monitor. For example, for the IP2Tel Counter rule there is the corresponding pair "AudioCodes Attempted Calls IP2Tel High Threshold Monitor" and "AudioCodes Attempted Calls IP2Tel Low Threshold Monitor".

You can set, based on your network environment, the low-level and high-level threshold integer values for these monitors. You can configure these integer values under the following circumstances:

■ When the monitor reaches its HighWarningLevel threshold

■ When the monitor reaches its HighCriticalLevel threshold

■ When the monitor reaches its LowWarningLevel threshold

■ When the monitor reaches its LowCriticalLevel threshold

An alarm is by default triggered when the High-Threshold value is exceeded or the Low-Threshold value is crossed. The alarm is cleared when the PMs value passes below the pre-defined High-Threshold or above the Low-Threshold value.

> **Note:** The log trap 'acPerformanceMonitoringThresholdCrossing' (non-alarm) (see Section A.2.6 on page 160) is sent each time a PM threshold is exceeded. The severity field is 'indeterminate' when crossing above the threshold and 'cleared' when it returns below the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

The following table describes the different alarm states when a threshold is crossed, and the different states when it is cleared:

Table 7-6: Alarm States

Alarm Initial State	Alarm Change State
Normal	Warning
Normal	Critical
Warning	Critical
Warning	Clear
Critical	Warning
Critical	Clear

The alarm that is raised depends on the counter value that is exceeded above the threshold or is crossed below the threshold.

For example, when the IP to Tel calls counter exceeds 50, an alarm is sent from the device. Alternatively, when the IP to Tel calls counter drops below 10, an alarm is sent from the device.

You can either set the threshold level for a specific object or for all objects of class: SNMP Network device.

> **Note:** See Section 7.3 on page 74 for the mapping between the SNMP severity levels and the SCOM severity levels.

➢ **To configure the threshold values:**

1. In the GW State View, right-click the gateway module that you wish to configure, and then choose **Open > Health Explorer for <GW IP>**; the Health Explorer is displayed:

Figure 7-13: Health Monitor-Initial View
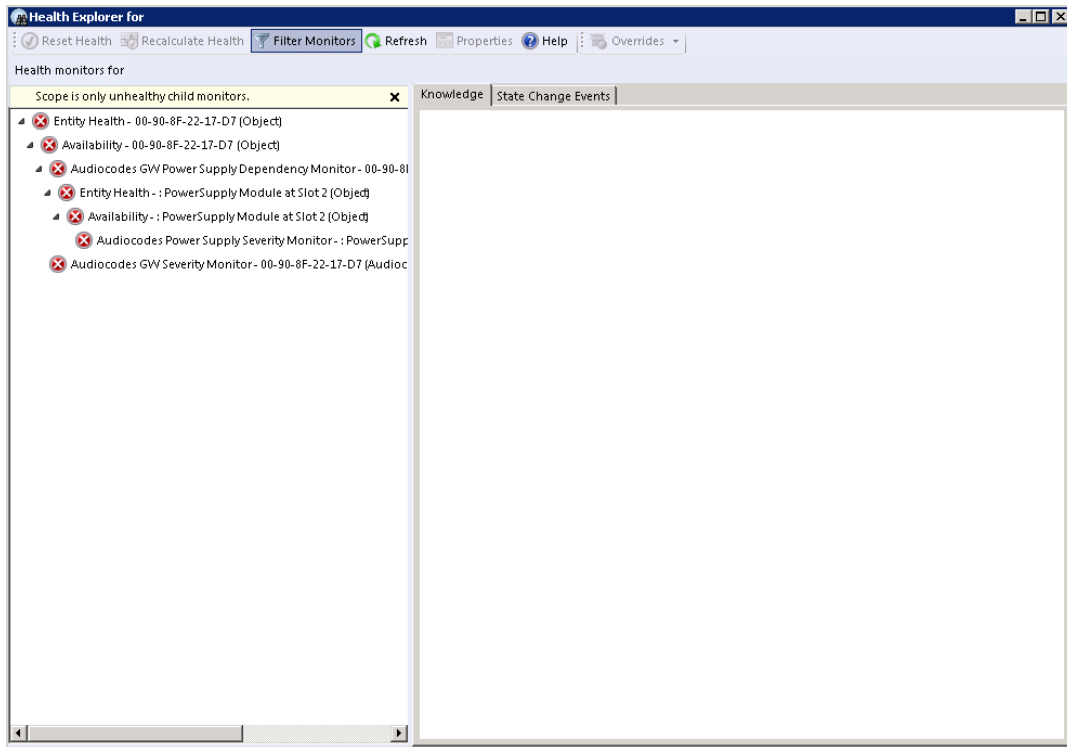
| ⚠ | **Note:** You can also configure thresholds for performance monitors in the Monitors window (**Authoring** > **Monitors**); however, this method is easier if you are currently in the Monitoring pane. |

2. Click the X adjacent to the message "Scope is only unhealthy child monitors"; the full list of monitors are displayed:

Figure 7-14: Health Monitor-Expanded View
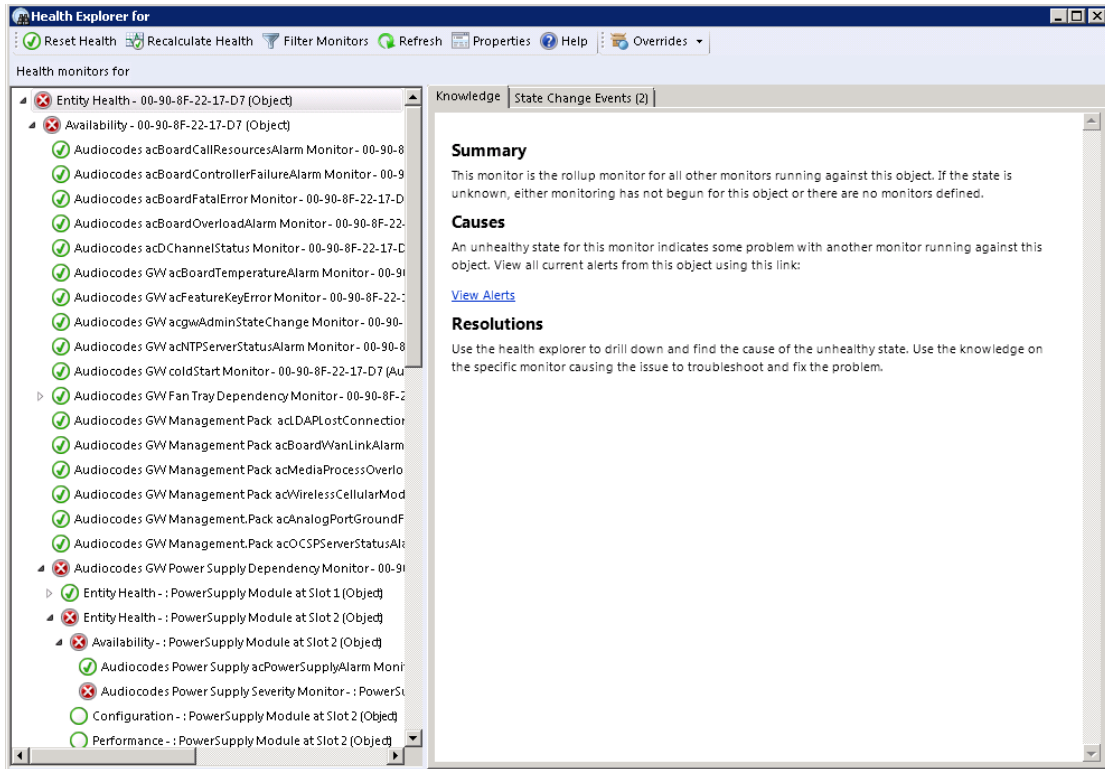
3. In the **Entity Health** tree, expand **Performance** node.

4. Select the required monitor right-click and choose **Monitor Properties**; the Threshold Monitor properties window for this monitor is displayed:

Figure 7-15: Threshold Monitor Properties
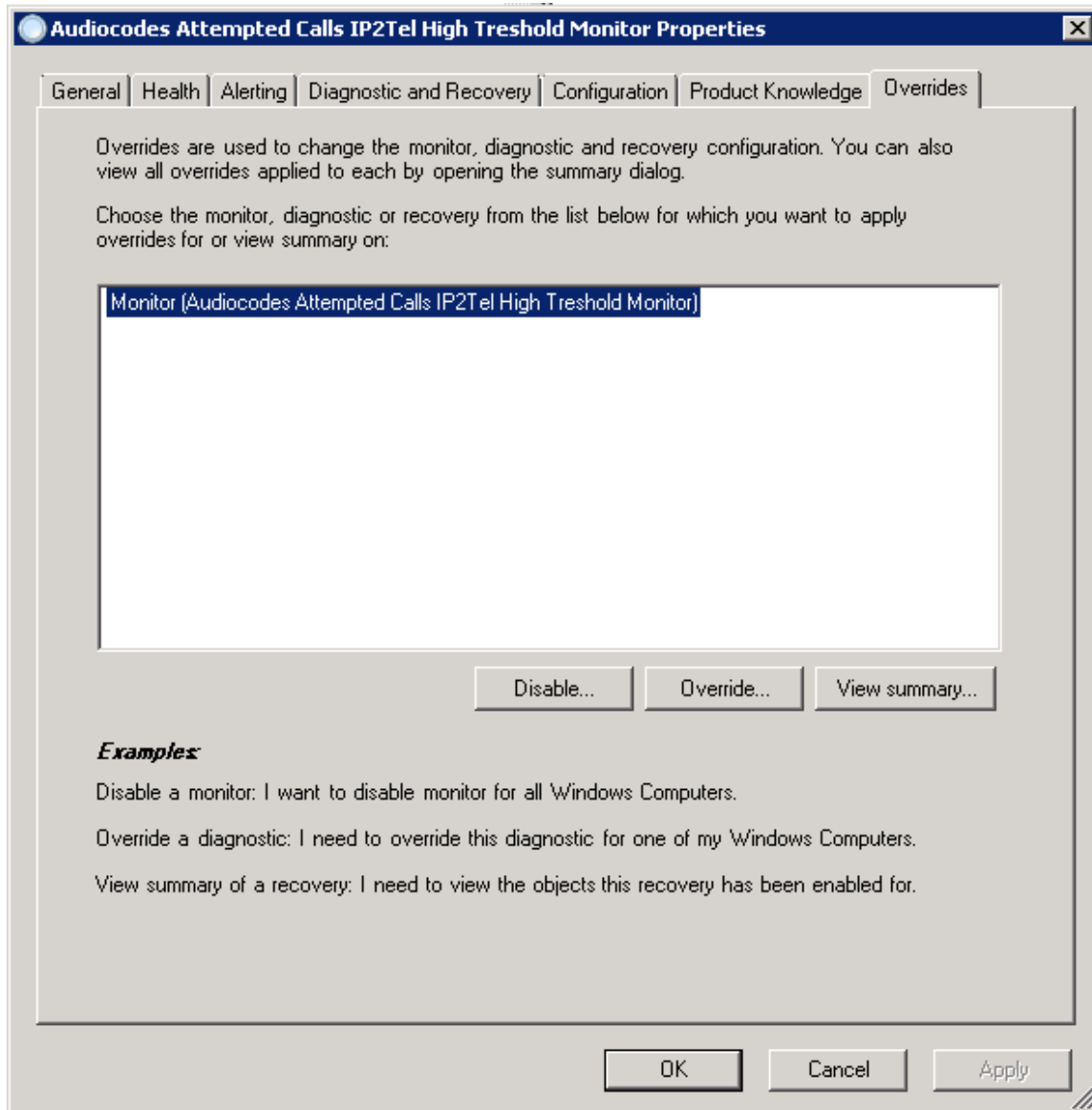
5. Click the **Overrides** tab; the Overrides screen is displayed.
6. Click the **Override** button.

Figure 7-16: Override Thresholds
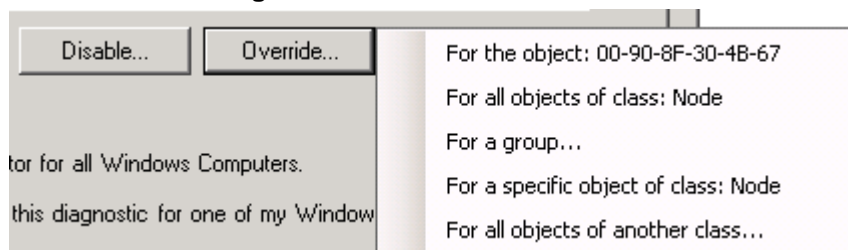
Choose one of the following options:

- **For the object <GW IP>** - only the threshold levels for this specific gateway are changed.

- **For all objects of class: SNMP Network Device** – the threshold levels for all currently discovered SNMP gateways in the network.

The Override Properties window is displayed:

Figure 7-17: Override Properties - High Threshold Monitor
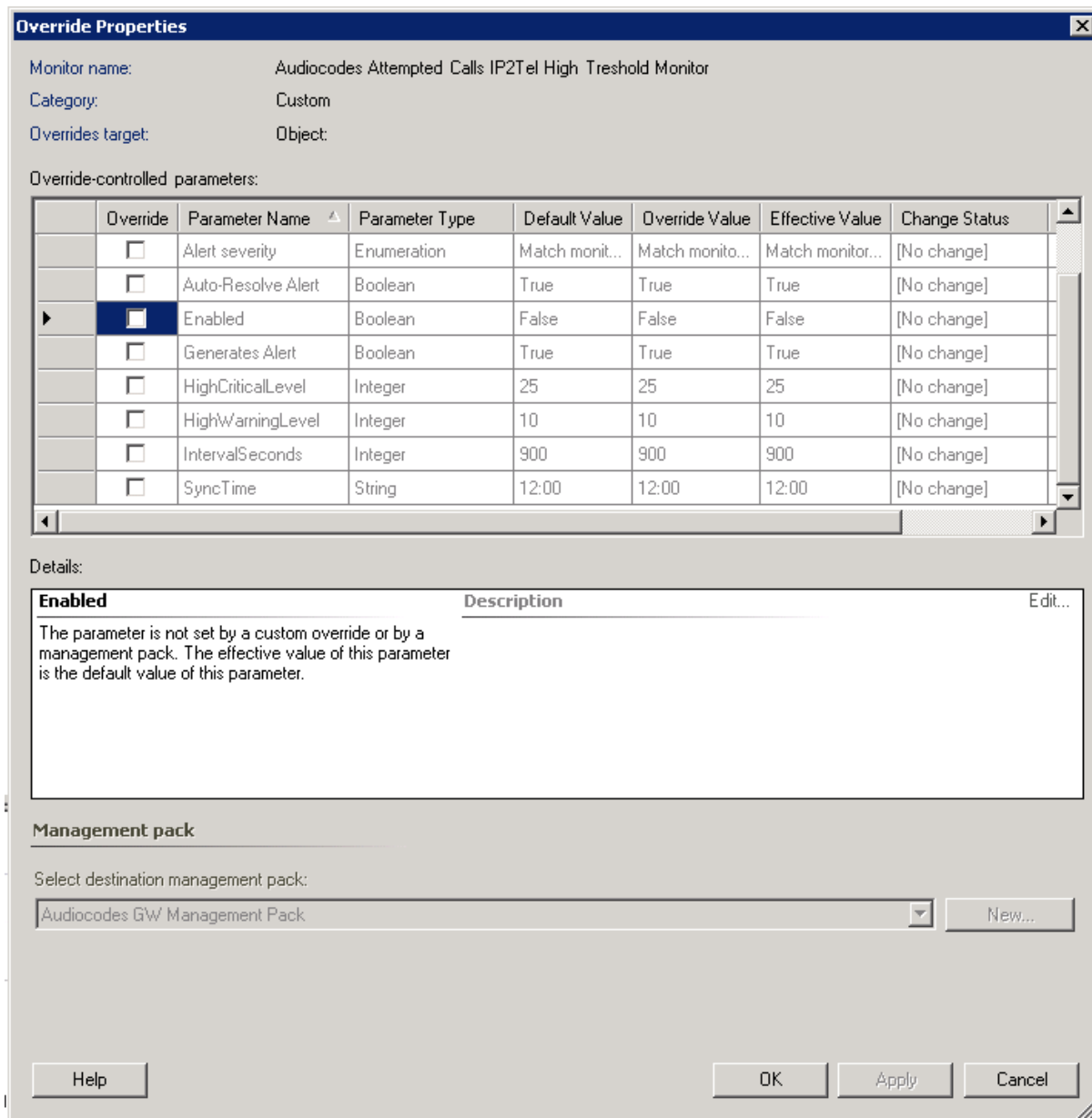
Figure 7-18: Override Properties - Low Level Threshold Monitor

The following parameters define threshold levels for AudioCodes Management Pack monitors:

- **High Threshold Monitors**: 'HighCriticalLevel' and 'HighWarningLevel'
- **Low Threshold Monitors**: 'LowCriticalLevel' and 'LowWarningLevel'

7. In the 'Override' column, select the checkbox adjacent to the parameter whose threshold value you wish to change.

8. In the corresponding 'Override Value' column, set the required value.

> **Note:**
>
> - By default, the High Critical Level Threshold is set to "25". You should change this value according to your site requirements.
> - By default, the Low Critical Level Threshold monitor is set to "-1". You should change this value according to your site requirements.
> - The message in Details pane is context-sensitive. Once you select a check box, the message text changes accordingly.

9. Click **OK** to apply the change.

8 Optimizing SCOM Server Loading

This chapter describes how to optimize the load on the SCOM server for AudioCodes MP-related functional items. The following sections are described in this chapter:

■ Displaying AudioCodes Objects. See Section 8.1.1 on page 92.

■ Optimizing Monitors Load. See Section 8.1.2 on page 95.

■ Optimizing Discoveries Load. See Section 8.1.3 on page 99.

■ Optimizing Rules Load. See Section 8.1.4 on page 81.

> **Note:** For detailed information, see Appendix C on page 173.

8.1 Introduction

One of the key factors affecting the performance of the SCOM server when working with the AudioCodes MP is the overloading on the CPU that is triggered by the disparate launching of AudioCodes MP-related functional items. For example, the discovery of gateways and their modules and trunks. For each of these operations, a script is run. When many of these scripts are run simultaneously, the performance of the SCOM server is significantly affected. When the SCOM server load is optimized, the script running is smoothly distributed over time so as to prevent CPU bottlenecks and therefore maintain performance.

This smooth distribution is achieved by overriding the values of the following parameters for the respective discoveries, monitors and rules:

■ **Polling interval** – defines the polling frequency interval; how often (seconds) functional items are launched (least possible resolution is 60 seconds).

■ **Sync time** – specifies at which time the polling is rearranged; this allows you to set the exact time in minutes within the hour when a functional item is launched. For example, if the IP2Tel Calls counter rule is launched every 10 minutes (i.e. the Polling interval) – this parameter sets the starting time and therefore the subsequent time sequence for launching this item within the hour (in minutes) i.e., 0, 10, 20 or 3, 13, 23, etc.). For example, when the 'Sync time' is set to 00:04, the IP2Tel Calls counter rule is launched in the following time sequence: 4, 14, 24, 34, 44, 54 minutes of each hour.

Note the following:

■ When you override the 'Sync' time to launch functional items at different starting times, this smoothens CPU utilization over time and therefore enhances performance. However, on the other hand leads to delay, as the time between the relative launching of each functional item increases.

■ Generally it is not recommended to override the 'IntervalSeconds' parameter; because most of the counters have a low polling frequency with a default value of fifteen minutes, and depend on the actual information refresh on the gateway devices themselves. The exception is in the case of specific Trunk counters (see Section 8.1.4 on page 102).

■ For a detailed load balancing scenario for SCOM server, see Appendix C on page 173.

8.1.1   Displaying AudioCodes Objects

Before you configure the properties of the monitors, discoveries and rules, for the purposes of easy management, it is recommended to set the object scope to view only AudioCodes functional items.

➢ **To filter the management pack functional items view:**

1.   In the Authoring pane, select **Management Pack Objects** > **Views**.

Figure 8-1: Views
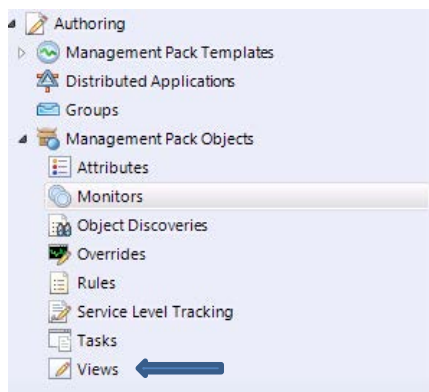
The right-hand pane displays all the functional items that are defined in the current scope.

2.   In the Main Menu, ensure that the Scope setting is selected:

- Select **View > Scope** or press **Ctrl+M**.

Figure 8-2: View Scope
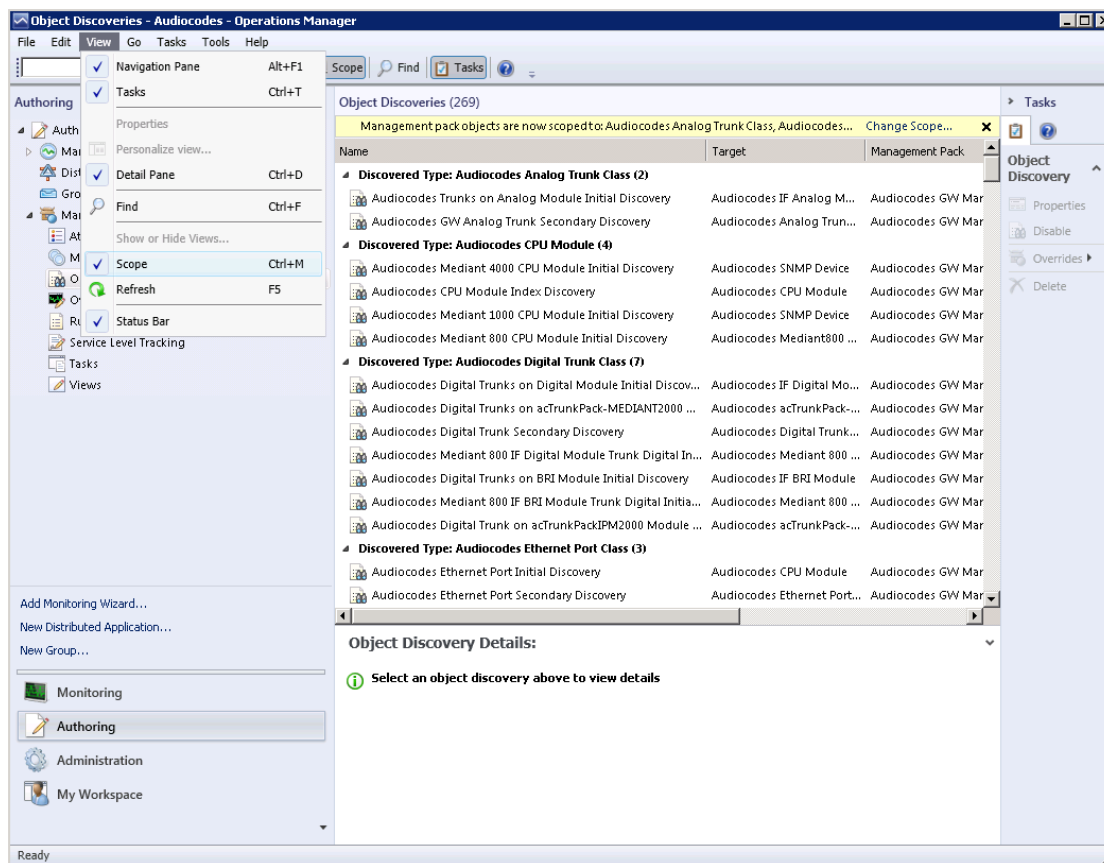
The Scope Management Pack Objects window is displayed:

Figure 8-3: Scope Management Pack Objects
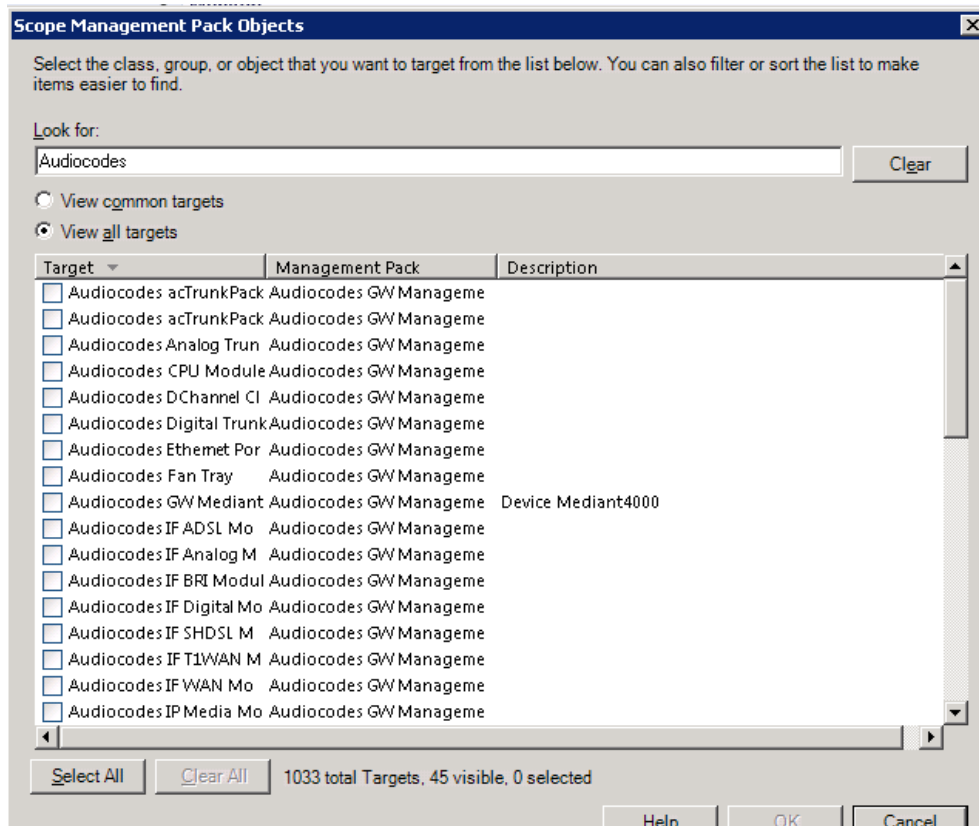
3. In the 'Look for' field, enter ''Audiocodes''.
4. Select the **View all targets** option.
5. Click either **Select All** or select only specific targets whose functional items (monitors, discoveries or rules) should be changed, and then click **OK**.

All AudioCodes Management Pack related-entities are displayed in the right-hand pane:

Figure 8-4: AudioCodes Management Pack Entities
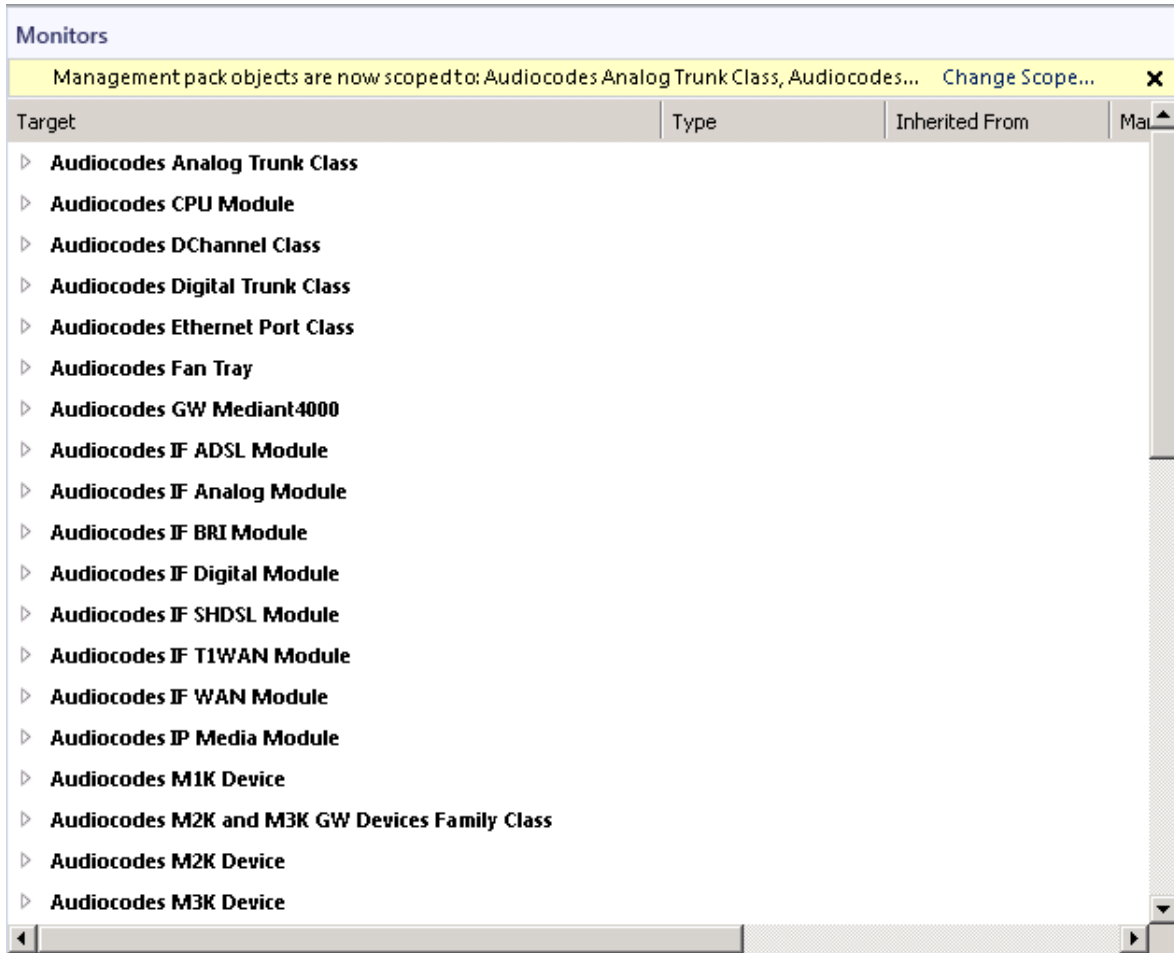
8.1.2   Optimizing Monitor's Load

This section describes how to configure when monitors are launched.

The following monitors have a high level of CPU utilization, and therefore it is highly recommended to synchronize the times when they are launched:

■   Gateways:

- Audiocodes Blocked Channels High Threshold Monitor

- Audiocodes Free Channels Low Threshold Monitor

- *Audiocodes Low Threshold Monitor <PM>– family of monitors

- *Audiocodes High Threshold Monitor <PM> – family of monitors

> **Note:** All threshold monitors have corresponding counter rules. For example, the Audiocodes Blocked Channels High Threshold Monitor has the corresponding rule 'Audiocodes Digital Trunk Blocked Channels Counter Rule (see Section 8.1.4 on page 102.)

■   Trunks:

- AudioCodes Digital Trunk Alarm Monitor (see Section 7.3.3 on page 75).

*For the AudioCodes *Low Threshold Monitor and AudioCodes *High Threshold Monitors family of monitors, where <PM> is the name of the PM (performance monitor), such as 'Tel2IP Failed Calls'.

➢ **To optimize monitors' loading:**

1. In the Authoring pane, select **Management Pack Objects** > **Monitors**.

Figure 8-5: Monitors Option
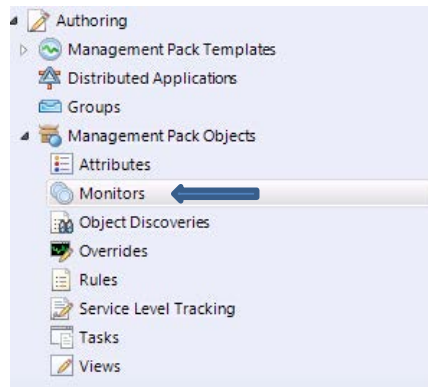
The Monitors window is displayed:

Figure 8-6: Monitors
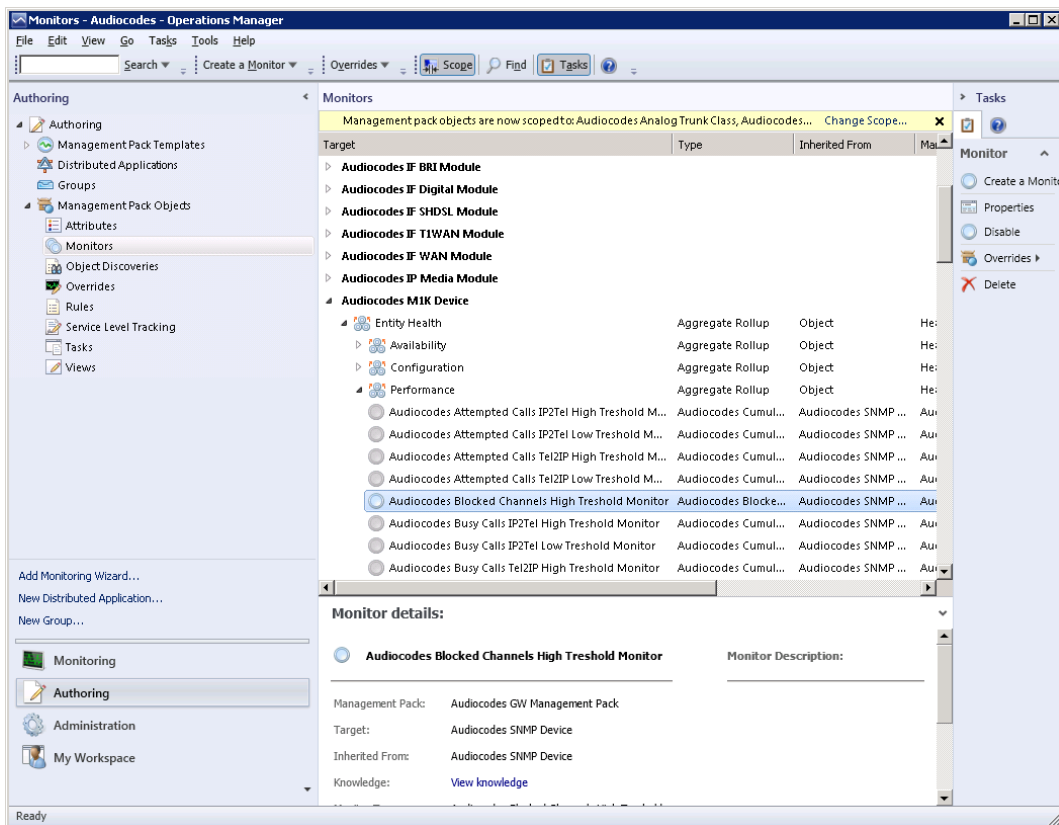
2. In the 'Monitors' list, expand the tree and select the monitor whose value you wish to override.

Figure 8-7: Overriding Object Monitors
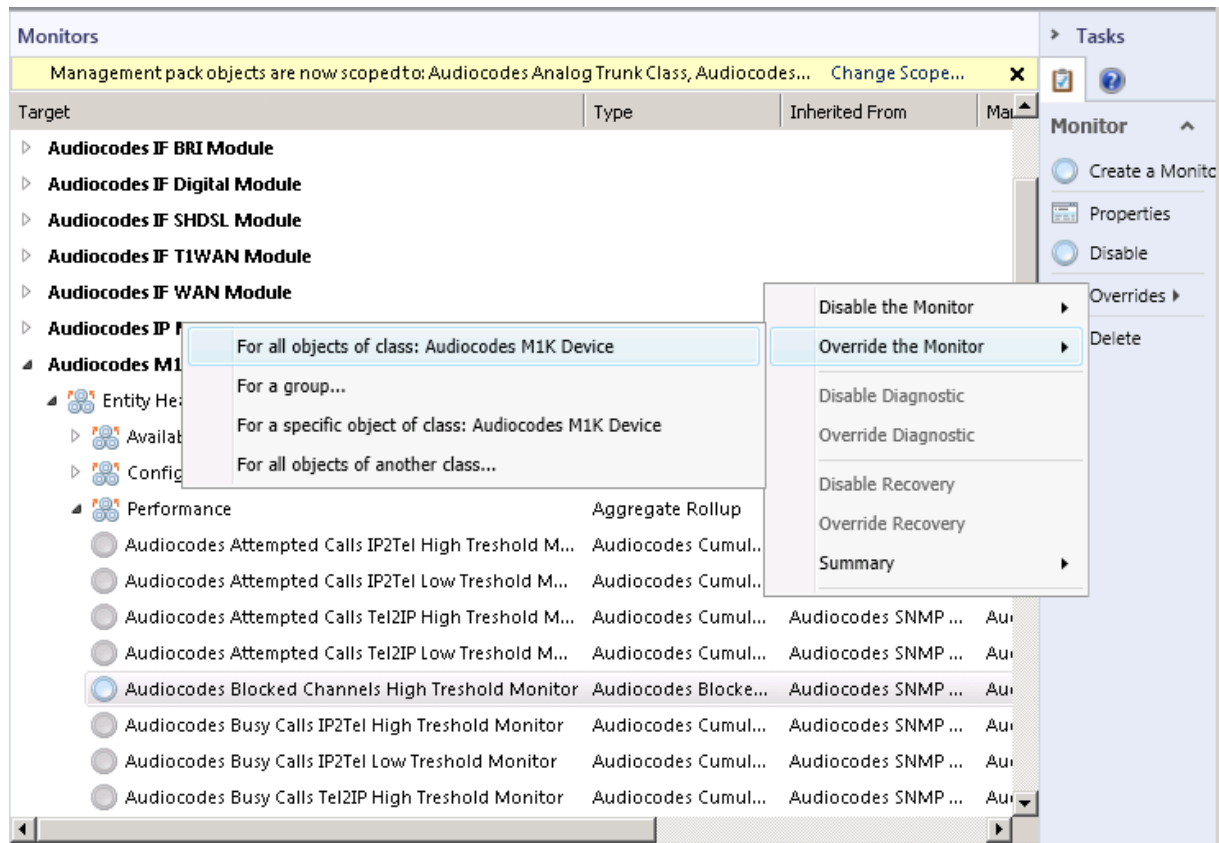
3.   Right-click the monitor, choose **Overrides** > **Override the Monitor**, and then in pop-up dialog, select the scope affected by the modification e.g. "For a group".

The Override Properties window is displayed:

Figure 8-8: Override Properties-Object Monitors-High Level Threshold Monitor
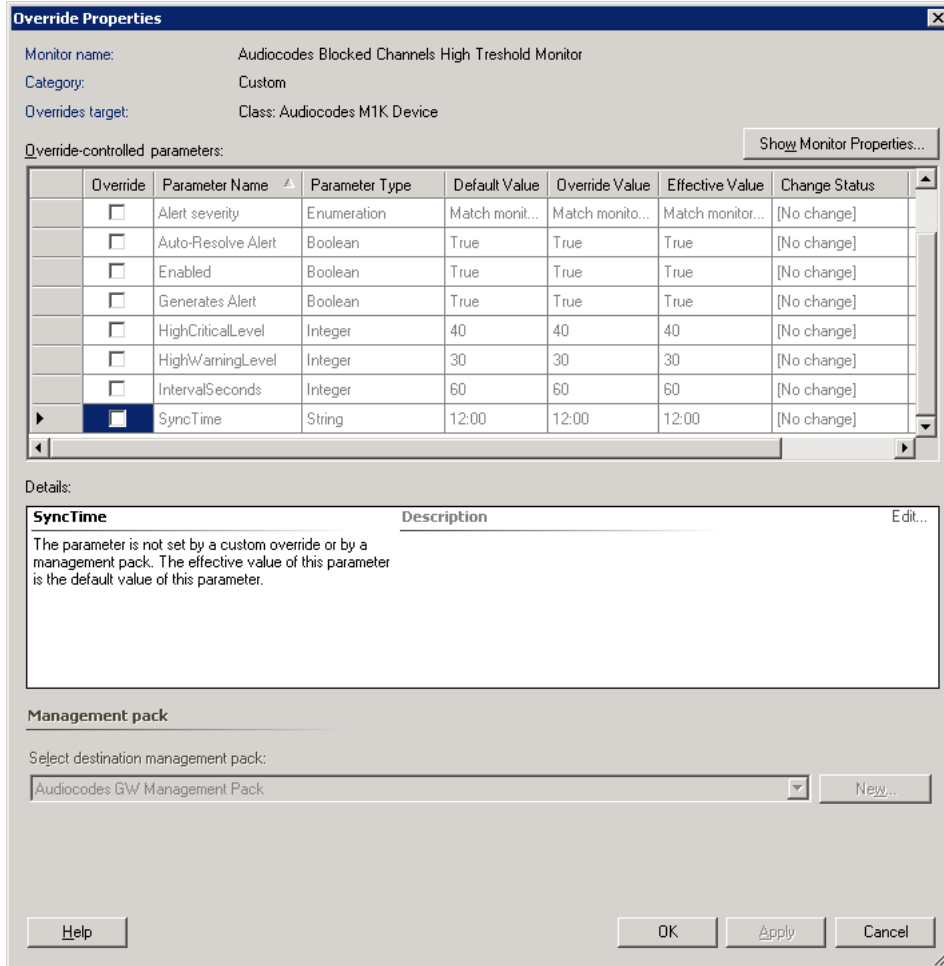
4. Select the 'Override' check box for the 'SyncTime' parameter.

> **Note:** The message in Details pane is context-sensitive. Once you select a check box, the message text changes accordingly.

5. In the 'Override Value' field for 'SyncTime', type the appropriate value.
6. Click **OK**.

8.1.3　Optimizing Discoveries' Load

This section describes how to configure when discoveries are launched. SCOM periodically discovers gateways and their modules and trunks to update their respective health states. The different types of discoveries are described below:

■ Gateways:
  - Device Discovery
■ Modules:
  - Initial Discovery
  - Index Discovery
  - Secondary Discovery
■ Trunks:
  - Initial Discovery
  - Secondary Discovery
■ Ethernet Port:
  - Initial Discovery
  - Index Discovery
  - Secondary Discovery

> **Note:** Since the number of trunks which have to be discovered is much higher relative to the number of modules and gateways, reducing the polling frequency for the number of trunk-related discoveries will significantly improve the performance of the SCOM server. For more information, see Appendix C on page 173.

> ➢ **To optimize discoveries' loading:**

1. In the Authoring pane, select **Management Pack Objects** > **Object Discoveries**.

Figure 8-9: Object Discoveries Option
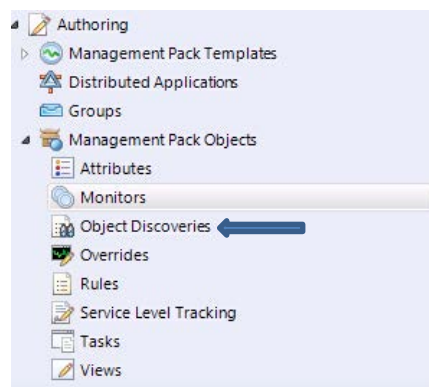
The Object Discoveries window is displayed:

Figure 8-10: Object Discoveries
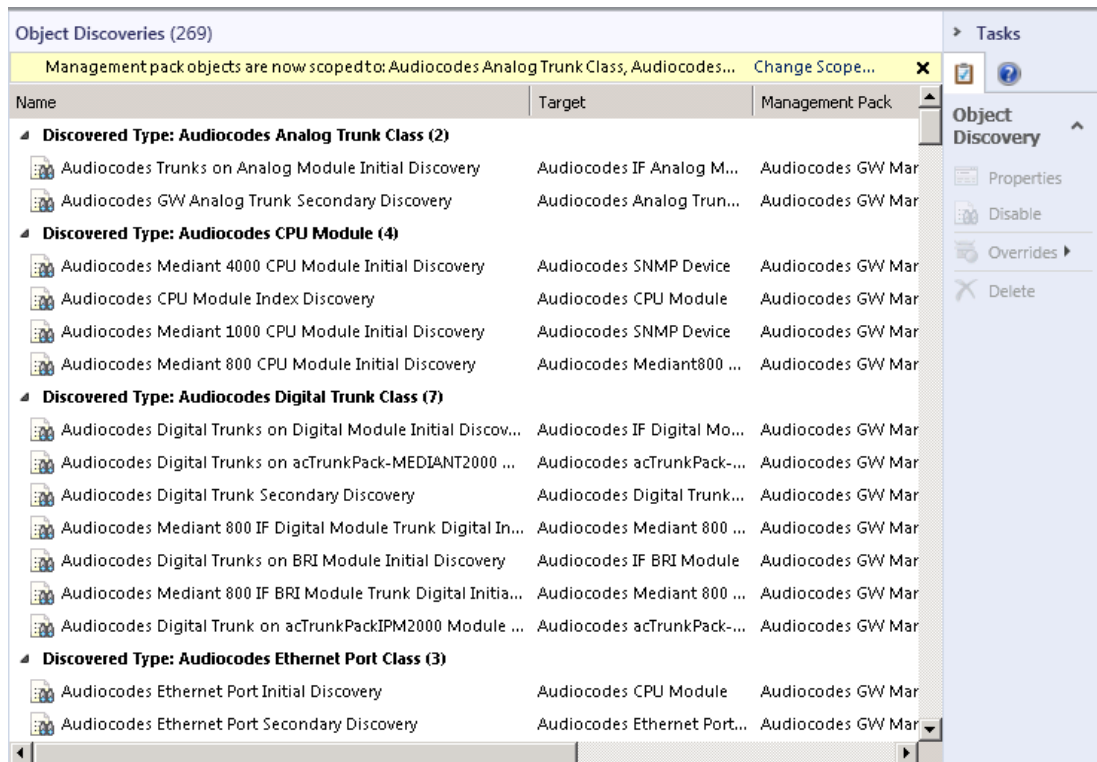
2. In the 'Discoveries' list, expand the tree and select the Discovery object whose value you wish to override.

Figure 8-11: Overriding Object Discoveries
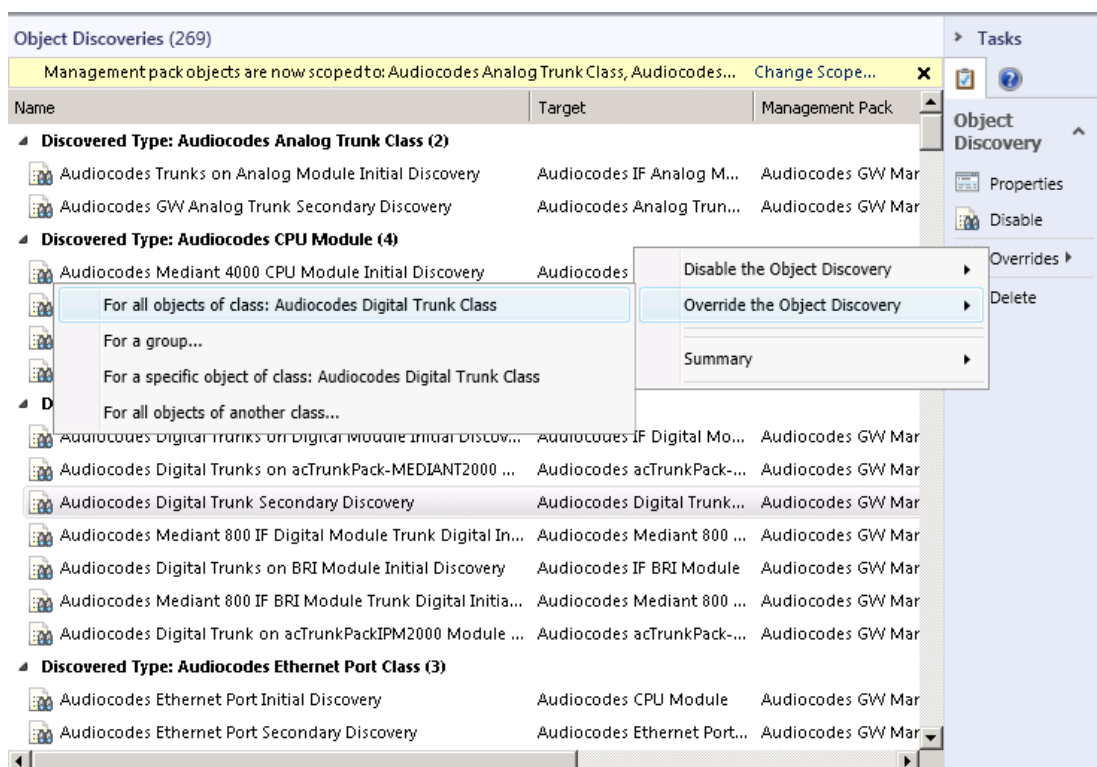
3. Right-click the monitor, choose **Overrides** > **Override the Object Discovery**, and then in pop-up dialog, select the scope affected by the modification e.g. "For all objects of another class".

The Override Properties window is displayed:

Figure 8-12: Override Properties-Object Discoveries

4. Select the 'Override' check box for the 'SyncTime' parameter.

> **Note:** The message in Details pane is context-sensitive. Once you select a check box, the message text changes accordingly.

5. In the 'Override Value' field for 'SyncTime, type the appropriate value.
6. Click **OK**.

8.1.4 Optimizing Rule's Load

This section describes how to configure when rules are launched.

There are two specific rules whose values are recommended to override. These rules (counters) unlike the SIP PMs are not typical device counters; instead they calculate values based upon monitored information about the Channels' state retrieved from the device (in-service or out-of-service). These counters ('AudioCodes Digital Trunk Available Channels Counter Rule' and 'Audiocodes Digital Trunk Blocked Channels Counter Rule') by default collect information every minute and include a large number of monitored entities. Consequently, this high polling frequency leads to high CPU utilization.

Therefore, you can improve performance by reducing the polling frequency of these counters using the rule 'Audiocodes.GW.Management.Pack.Trunk.Digital.Channels.Probe' (see Figure 8-14, Figure 8-15 and Figure 8-16). For this rule, it is recommended to modify both the 'IntervalSeconds' parameter as well as the 'SyncTime parameter'.

> **Note:** This rule queries the Channels state from the device, and then saves the information in a file directory specified by System Environment variable "AudiocodesTempFolder. This information is then aggregated by a script launched by the SCOM.

It is also recommended to poll no more than one counter rule at any one point in time (for details, see Appendix C on page 173).

➢ **To optimize rules' loading:**

1. In the Authoring pane, select **Management Pack Objects** > **Rules**.

Figure 8-13: Rules Option
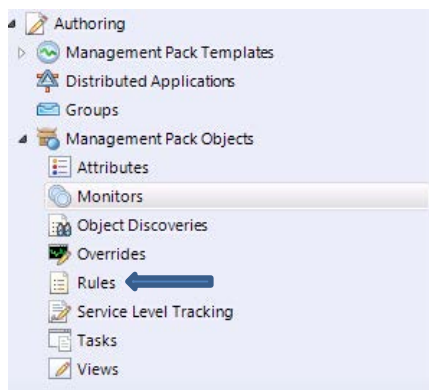
The Rules window is displayed:

Figure 8-14: Object Rules
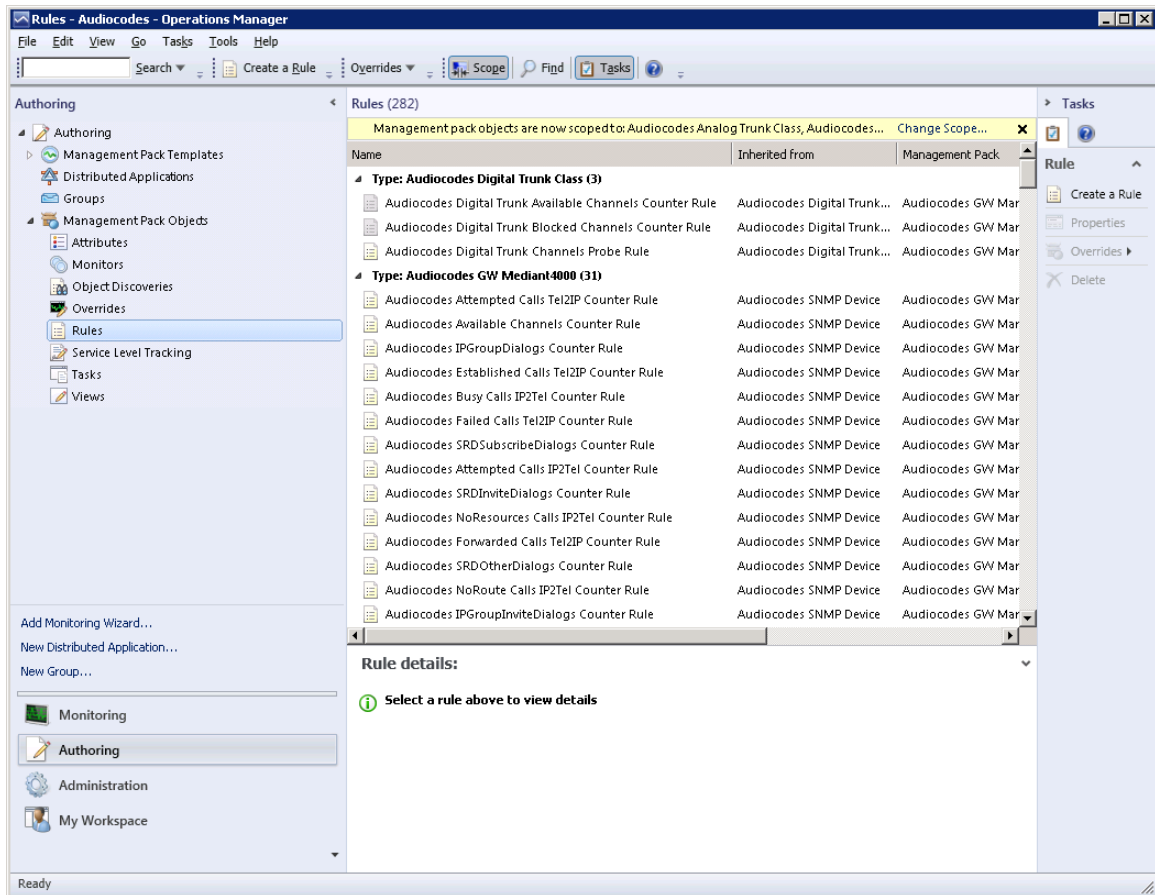
2. In the 'Rules' list, expand the tree and select the rule whose values you wish to override. For example, the 'Digital Trunk Channels Probe Rule'.

Figure 8-15: Overriding Object Rules-AudioCodes Digital Trunk Channels Probe Rule
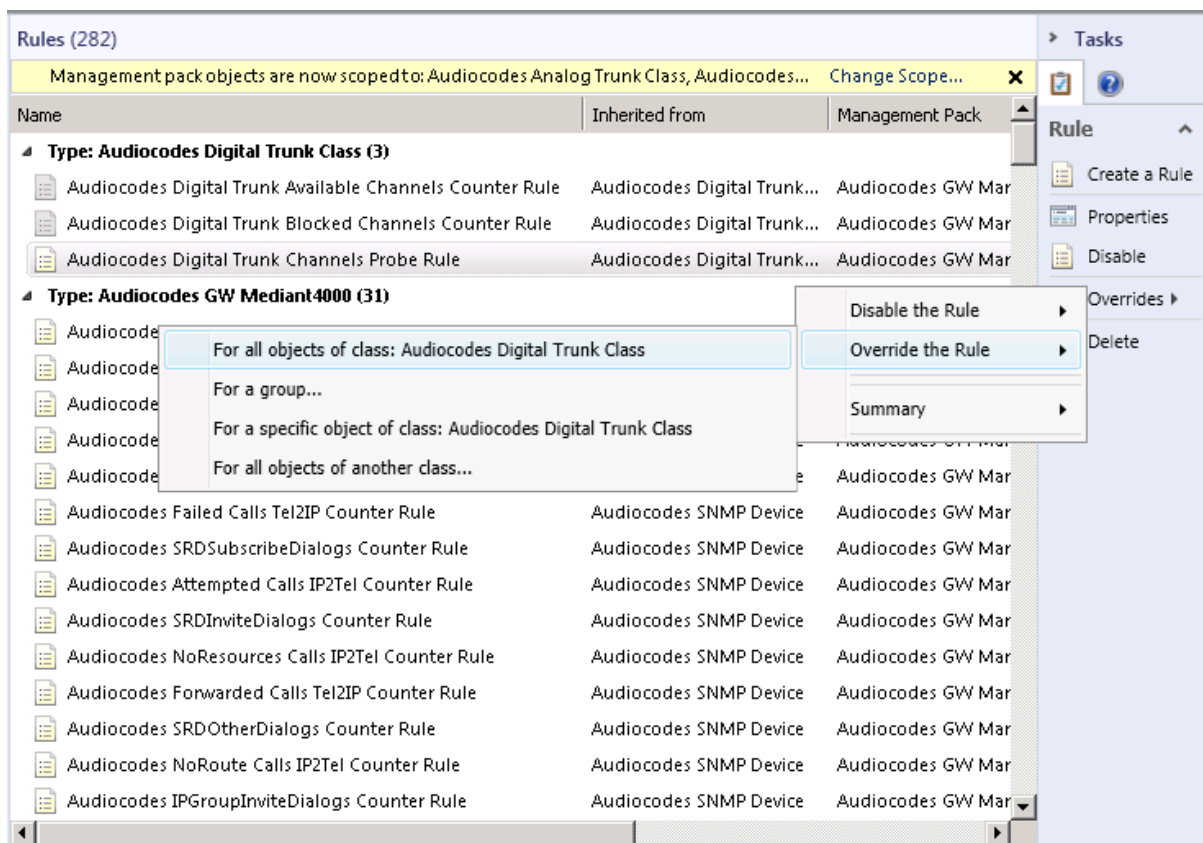
3. Right-click the monitor, choose **Overrides** > **Override the Rule**, and then in pop-up dialog, select the scope affected by the modification e.g. "For a group".

The Override Properties window is displayed:

Figure 8-16: Override Properties-Audiocodes Digital Trunk Channels Probe Rule

4. Select the 'Override' check box for the 'SyncTime' parameter.

> ⚠ **Note:** The message in Details pane is context-sensitive. Once you select a check box, the message text changes accordingly.

5. In the 'Override Value' field for 'SyncTime', type the appropriate value.
6. Select the Override check box for the 'IntervalSeconds' parameter.
7. In the 'Override Value' field for 'IntervalSeconds', type the appropriate value.
8. Click **OK**.
9. In the 'Rules' list, select other rules whose values you wish to override. For example, the 'Audiocodes Failed Calls Tel2IP Counter Rule'.

Figure 8-17: Overriding Object Rules-AudioCodes Failed Calls Tel2IP Counter Rule
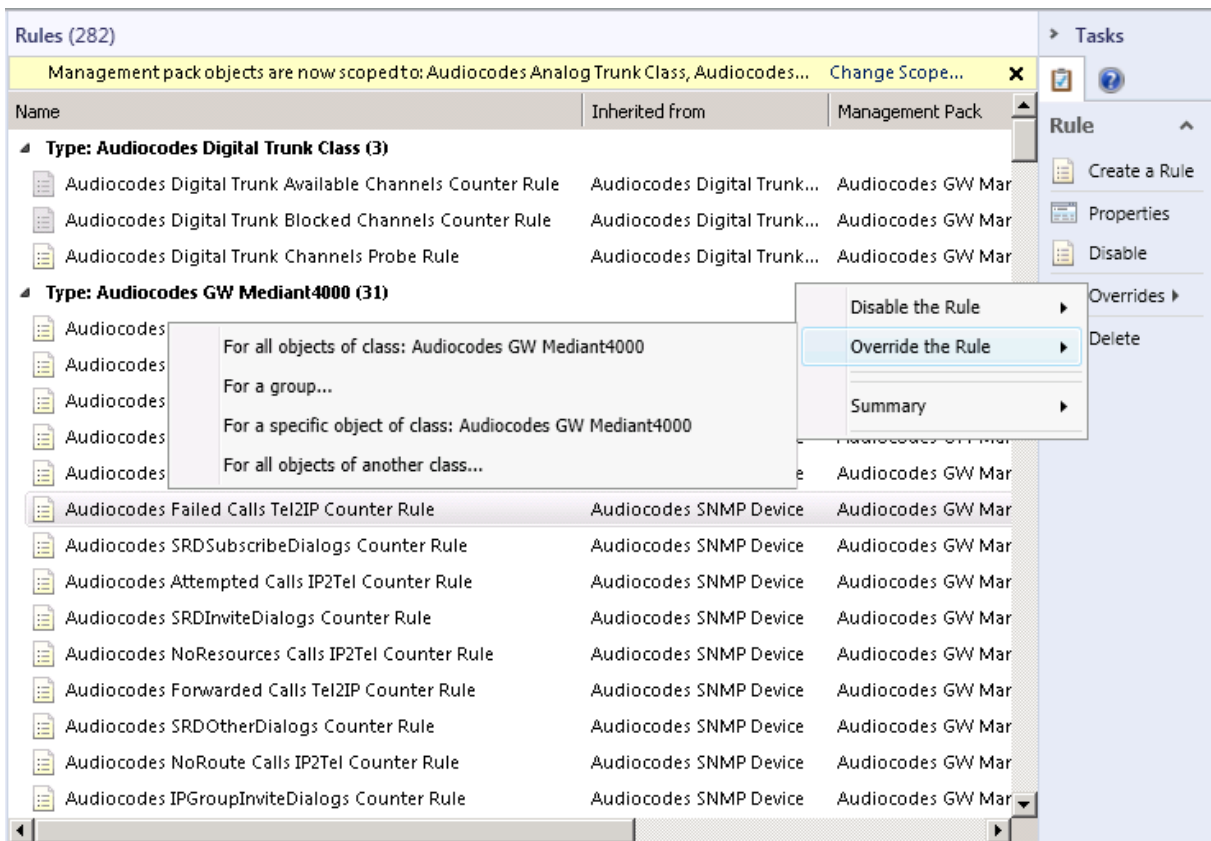
10. Right-click the monitor, choose **Overrides** > **Override the Rule**, and then in pop-up dialog, select the scope affected by the modification e.g. "For a group".

The Override Properties window is displayed:

Figure 8-18: Override Properties-AudioCodes Failed Calls Tel2IP Counter Rule

11. Select the 'Override' check box for the 'SyncTime' parameter.

12. In the 'Override Value' field for 'SyncTime', type the appropriate value.

13. Click **OK**.

This page is intentionally left blank

A   SNMP Traps

The tables in the following subsections provide information on SNMP traps that are sent from the device to the SCOM. The component name (described in each of the following headings) refers to the string provided in the acBoardTrapGlobalsSource trap varbind.

Notes:

- Traps are not sent automatically to the SCOM. You must first configure the SCOM server as a Trap Manager on your managed device (see Section 5.2 on page 50).
- All traps are sent from the SNMP port (default 161).
- To clear a generated alarm, the same notification type is sent; however with the severity set to 'Cleared'.
- All trap-based monitors captured are cleared when a new trap arrives with the same OID and source varbinds.

For detailed information on SNMP, refer to the *SNMP Reference Guide for SIP Enterprise Devices.*

A.1   Chassis Alarms

A.1.1   Fan Tray Alarm

Note: Applicable only to Mediant 1000, Mediant 3000 and Mediant 4000.

Table A-1: acFanTrayAlarm

Alarm	acFanTrayAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.29		
Description	Sent when a fault occurs in the fan tray or a fan tray is missing.		
Source Varbind Text	Chassis#0/FanTray#0		
Alarm Text	Fan-Tray Alarm <text>		
Event Type	equipmentAlarm		
Probable Cause	▪ One or more fans on the Fan Tray module stopped working. ▪ One or more fans on the Fan Tray module works slower than expected (heatingVentCoolingSystemProblem)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Fan-Tray is missing.	Fan-Tray is missing	1. Check if the Fan Tray module is inserted in the chassis. 2. If the Fan Tray module was removed from the chassis, re-insert it. 3. If the Fan Tray module has already been inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes. **Warning:** When removing the Fan Tray module while the power is on (or after it has recently been switched off), the blades may still be rotating at high speeds. Therefore, to avoid bodily harm, make sure that you don't touch the fan blades.
Major	When one or more fans in the Fan Tray are faulty.	Fan-Tray is faulty	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module is in place and fans are working.	-	-

A.1.2   Power Supply Alarm

> ⚠️ **Note:** Applicable only to Mediant 1000, Mediant 3000 and Mediant 4000.

Table A-2: acPowerSupplyAlarm

Alarm	acPowerSupplyAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.30		
Description	Sent when a fault occurs in one of the power supply (PS) modules or a PS module is missing.		
Default Severity	Critical		
Source Varbind Text	Chassis#0/PowerSupply#<m>, where *m* is the power supply's slot number		
Event Type	equipmentAlarm		
Probable Cause	powerProblem		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	The HA (High Availability) feature is active (applicable only to Mediant 3000 and Mediant 4000) and one of the power supply units is faulty or missing.	Power-Supply Alarm. Power-Supply is missing.	1. Check if the unit is inserted in the chassis. 2. If it was removed from the chassis, re-insert it. 3. If it's inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	PS unit is placed and working.	-	-

A.1.3   User Input Alarm

Note: Applicable to Mediant 3000 and Mediant 1000.

Table A-3: acUserInputAlarm

Alarm	acUserInputAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.36		
Description	Sent when the input dry contact is short circuited; cleared when the circuit is reopened.		
Default Severity	Critical		
Source Varbind Text	Chassis#0		
Event Type	equipmentAlarm		
Probable Cause	inputDeviceError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Input dry contact is short circuited.	User input Alarm. User's Input-Alarm turn on.	Reopen the input dry contact.
Cleared	Input dry contact circuit is reopened.	-	

A.1.4   PEM Alarm

Note: Applicable only to Mediant 3000.

Table A-4: acPEMAlarm

Alarm	acPEMAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.31		
Description	Sent when a fault occurs in one of the PEM modules or a PEM module is missing.		
Default Severity	Critical		
Source Varbind Text	hassis#0/PemCard#<m>, where *m* is the power entry module's (PEM) slot number		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	The HA (High Availability) feature is active and one of the PEMs (Power Entry Modules) is missing.	PEM Module Alarm. PEM card is missing.	1. Make sure the PEMs are present and that they're inserted correctly. 2. If it's present and inserted correctly yet the alarm remains active, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	PEM card is placed and both DC wires are in.	-	-

A.1.5   Hardware Failure Alarm

> ⚠ **Note:** Applicable only to Mediant 1000.

Table A-5: acHwFailureAlarm

Alarm	acHwFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.43		
Default Severity	Critical		
Source Varbind Text	Chassis#0/module#<m>, where *m* is the module's number		
Event Type	equipmentAlarm		
Probable Cause	equipmentMalfunction		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	The module is faulty or has been removed incorrectly.	Module Alarm: Faulty IF-Module	Restart the device to clear this alarm. The alarm is not cleared.
Major	Module mismatch - module and CPU board mismatch.	IF-Module Mismatch	Restart the device to clear this alarm. The alarm is not cleared.

A.1.6   Timing Module Alarms

> ⚠ **Note:** These alarms are applicable only to Mediant 3000.

A.1.7   TM Inconsistent Remote and Local PLL Status Alarm

Table A-6: acTMInconsistentRemoteAndLocalPLLStatus Alarm

Alarm	acTMInconsistentRemoteAndLocalPLLStatus		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.56		
Description	Inconsistent Remote and Local PLL status.		
Default Severity	Major		
Source Varbind Text	Chassis#0/TimingManager#0		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	The alarm is triggered when the system is in 1+1 status and redundant board PLL status is different to the active board PLL status	Timing Manager Alarm. Local and Remote PLLs status is different.	1. Synchronize the timing module. 2. Reboot the system.
Status remains 'Major' until a reboot. A 'Clear' trap is not sent.	-	-	-

A.1.8   TM Reference Status Alarm

Table A-7: acTMReferenceStatus Alarm

Alarm	acTMReferenceStatus		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.57		
Description	Timing manager reference status.		
Default Severity	Major		
Source Varbind Text	Chassis#0/TimingManager#0		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Status Changes	When primary and secondary clock references are down for more than 24 hours, the alarm will be escalated to 'Critical'.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	The alarm is triggered when the primary reference or secondary reference or both are down.	Timing Manager Alarm. PRIMARY REFERENCE DOWN/SECONDARY REFERENCE DOWN/ALL REFERENCES ARE DOWN	1. Synchronize the timing module. 2. Reboot the system.
Status remains 'Major' until a reboot. A clear trap is not sent.	-	-	-

A.1.9   TM Reference Change Alarm

Table A-8: acTMReferenceChange Alarm

Alarm	acTMReferenceChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.58		
Description	Timing manager reference change.		
Default Severity	Indeterminate		
Source Varbind Text	Chassis#0/TimingManager#0		
Event Type			
Probable Cause			
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
-	Log is sent on PLL status change.	Timing Manager	Corrective action is not necessary.

A.1.10 Trunk Alarms

⚠ **Note:** Applicable only to Digital Series.

A.1.10.1 Trunk Near-End LOS Alarm

Table A-9: acTrunksAlarmNearEndLOS

Alarm	acTrunksAlarmNearEndLOS		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.49		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Near-end LOS	Trunk LOS Alarm	Los of Signal (LOS) indicates a physical problem. 1. Check that the cable is connected on the board. 2. Check that the correct cable type is being used (crossed/straight). 3. Contact AudioCodes' Support Center at support@audiocodes.com.
Cleared	End of LOS	-	-

A.1.10.2 Trunk Near-End LOF Alarm

Table A-10: acTrunksAlarmNearEndLOF

Alarm	acTrunksAlarmNearEndLOF			
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.50			
Default Severity	Critical			
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk			
Event Type	communicationsAlarm			
Probable Cause	lossOfFrame			
Alarm Severity	**Condition**	**<text>**	**Corrective Action**	
Critical	Near end LOF	Trunk LOF Alarm	1. Make sure that the trunk is connected to a proper follow-up device. 2. Make sure that both sides are configured with the same (E1 / T1) link type. 3. Make sure that both sides are configured with the same framing method. 4. Make sure that both sides are configured with the same line code. 5. Make sure that the clocking setup is correct. 6. Contact AudioCodes' Support Center at support@audiocodes.com.	
Cleared	End of LOF	-	-	

A.1.10.3 Trunk AIS Alarm

Table A-11: acTrunksAlarmRcvAIS

Alarm	acTrunksAlarmRcvAIS			
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.51			
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk			
Alarm Text	communicationsAlarm			
Event Type	PSTN provider has stopped the trunk (receiveFailure)			
Probable Cause	communicationsAlarm			
Alarm Severity	**Condition**	**<text>**	**Corrective Action**	
Critical	Receive AIS	Trunk AIS Alarm	• Contact your PSTN provider to activate the trunk. • If the alarm persists, contact the AudioCodes Support Center at support@audiocodes.com	
Cleared	End of AIS	-	-	

A.1.10.4 Trunk Far-End LOF Alarm

Table A-12: acTrunksAlarmFarEndLOF

Alarm	acTrunksAlarmFarEndLOF		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.52		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm		
Probable Cause	transmitFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	RAI	Trunk RAI Alarm	Make sure that transmission is correct.
Cleared	End of RAI	-	-

A.1.10.5 DS1 Line Status Alarm

Table A-13: dsx1LineStatusChange

Alarm	dsx1LineStatusChange	
OID	1.3.6.1.2.1.10.18.15.0.1	
Default Severity	Major on raise; Clear on clear	
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk	
Event Type	communicationsAlarm	
Probable Cause		
Alarm Severity	**<text>**	**Additional Info1,2,3**
-	DS1 Line Status	Updated DS1 Line Status. This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms' information. dsx1LineStatus is a bitmap represented as a sum, so it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure Any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded

A.1.10.6 B-Channel Alarm

Table A-14: acBChannelAlarm

Alarm	acBChannelAlarm			
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.85			
Default Severity	Minor			
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk			
Event Type	communicationsAlarm			
Probable Cause	degradedSignal			
Alarm Severity	**Condition**	**<text>**	**Corrective Action**	
Major	Raised when B-channel service state changes to 'Out of Service' or 'Maintenance'	B-Channel Alarm. %s	Corrective action is not necessary	
Clear	B-channel status changes to 'In Service'	%s – additional information	-	

A.1.10.7 NFAS Group Alarm

Table A-15: acNFASGroupAlarm

Alarm	acNFASGroupAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.84		
Default Severity	Major		
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm		
Probable Cause	degradedSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised when an NFAS group goes out-of-service	NFAS Group Alarm. %s	▪ The alarm is sent only when the backup Non-Facility Associated Signaling (NFAS) D-channel also falls, i.e., when *both* D-channels are down. ▪ When at least one of the D-channels (primary or backup) returns to service, the alarm is cleared. ▪ Corrective action is not necessary.
Clear	NFAS group state goes to in- service	%s– Additional information	-

A.1.11 SONET Alarms

Note: These alarms are applicable only to Mediant 3000 with TP-6310 blade.

The source varbind text for the alarms under this component is Interfaces#0/Sonet#<m>, where *m* is the SONET interface number.

A.1.11.1 SONET Section LOF Alarm

Table A-16: AcSonetSectionLOFAlarm

Alarm	acSonetSectionLOFAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.38		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	lossOfFrame		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	LOF condition is present on SONET no.n	SONET-Section LOF	Make sure the framing format on the port matches the format configured on the line. Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value **sonetSectionLOF(4)**
Cleared	LOF condition is not present	LOF	-

A.1.11.2 SONET Section LOS Alarm

Table A-17: AcSonetSectionLOSAlarm

Alarm	acSonetSectionLOSAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.39		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	LOS condition is present on SONET no #n	SONET-Section LOS	1. Make sure the fiber optic cable is plugged in correctly. 2. Make sure it's not damaged. 3. Make sure its remote end is correctly connected and undamaged. 4. Make sure that configuration of the remote port is correct. Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value **sonetSectionLOS (2)**

| Cleared | LOS condition is not present | - | - |

A.1.11.3 SONET Section AIS Alarm

Table A-18: AcSonetLineAISAlarm

Alarm	acSonetLineAISAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.40		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	AIS condition is present on SONET-Line #n	SONET-Line AIS	If an Alarm Indication Signal (AIS) condition is present on a SONET line: 1. Make sure the remote configuration is correct. 2. Check the line status at the remote end of the link. Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value **sonetLineAIS (2)**
Cleared	AIS condition is not present.	-	-

A.1.11.4 SONET Line RDI Alarm

Table A-19: AcSonetLineRDIAlarm

Alarm	acSonetLineRDIAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.41		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	transmitFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	RDI condition is present on SONET-Line #n	SONET-Line RDI	1. Check the *remote site* for alarm conditions. 2. Correct a line problem that has arisen from the *remote interface*. Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value **sonetLineRDI (4)**
Cleared	RDI condition is not present.	-	-

A.1.11.5 SONET Path STS LOP Alarm

Table A-20: acSonetPathSTSLOPAlarm

Alarm	acSonetPathSTSLOPAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.61		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**\<text\>**	**Corrective Action**
Critical	LOP condition is present on Path #m	SONET Path STS Loss of Pointer alarm: LOP	**1.** Verify that the Path configuration is identical on both ends. For example, if the far-end is configured as STS3c instead of STS3, this is causing the alarm. **2.** If the alarm doesn't clear, contact AudioCodes Support Center at: support@audiocodes.com Note that the 'sonetPathCurrentStatus' field in sonetPathCurrentTable has a value of sonetPathSTSLOP(2) STS = Synchronous Transport Signal
Cleared	LOP condition is not present	-	-

A.1.11.6 SONET Path STS AIS Alarm

Table A-21: acSonetPathSTSAISAlarm

Alarm	acSonetPathSTSAISAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.62		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**\<text\>**	**Corrective Action**
Critical	AIS condition is present on Path #n	SONET Path STS AIS alarm: AIS	**1.** Check the configuration of the SONET path. **2.** You may need to check more than just the next hop. You may need to check the far end of the path. Note that the 'sonetPathCurrentStatus' field in sonetPathCurrentTable has a value of **sonetPathSTSAIS(4)**
Cleared	AIS condition is not present	-	-

A.1.11.6.1 SONET Path STS RDI Alarm

Table A-22: acSonetPathSTSRDIAlarm

Alarm	acSonetPathSTSRDIAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.63		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	transmitFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	RDI condition is present on Path #n	SONET Path STS RDI alarm: RDI (Remote Defect Indicator)	Check the stations along the SONET path for alarm statuses, beginning with the nearest hop. The Remote Defect Indicator (RDI) is sent upstream from the path endpoint to inform the provider of a problem with its circuit downstream. Note that 'sonetPathCurrentStatus' in the sonetPathCurrentTable has a value of **sonetPathSTSRDI(8)**
Cleared	RDI condition is not present	-	-

A.1.11.7 SONET Path Unequipped Alarm

Table A-23: acSonetPathUnequippedAlarm

Alarm	acSonetPathUnequippedAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.64		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Unequipped condition is present on Path #n	SONET Path Unequipped alarm: Unequipped	1. Make sure the SONET path has a valid sender. The problem originates with the hub transmitting the signal to the hub reporting the alarm. 2. Make sure the other side is set up correctly. Make sure the carrier's SONET network is set up correctly. If you're set up correctly on both sides, it's probably the carrier's SONET network that is the problem. See also RFC 1595. Note that 'sonetPathCurrentStatus' in the sonetPathCurrentTable has a value of sonetPathUnequipped(16)
Cleared	Unequipped condition is not present		

A.1.11.8 SONET Path Signal Label Mismatch Alarm

Table A-24: acSonetPathSignalLabelMismatchAlarm

Alarm	acSonetPathSignalLabelMismatchAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.65		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Signal Label Mismatch condition is present on Path #n	SONET Path Signal Label Mismatch alarm: SignalLabelMismatch	1. Make sure the SONET Path is correctly provisioned. 2. Make sure the received Synchronous Transport Signal (STS) or VT signal label (the C2 byte or V5 bits 5 through 7 respectively) is equal to either a label value corresponding to the locally provisioned Path-Terminating Equipment (PTE) functionality or the label value corresponding to the equipped, non-specific code. See RFC 1595. Note that 'sonetPathCurrentStatus' in sonetPathCurrentTable has a value of **sonetPathSignalLabelMismatch(32)**
Cleared	Signal Label Mismatch condition is not present	-	-

A.1.11.9 SONET Hardware Failure Alarm

Table A-25: acSonetIfHwFailureAlarm

Alarm	acSonetIfHwFailureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.42
Default Severity	Critical on raise; Clear on clear
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type	communicationsAlarm
Probable Cause	Transmit failure
Alarm Text	SONET/SDH interface Failure Alarm

A.1.12 DS3 Alarms

⚠	**Note:** These alarms are applicable only to Mediant 3000 with TP-6310 blade.

A.1.12.1 DS3 RAI Alarm

Table A-26: acDS3RAIAlarm

Alarm	acDS3RAIAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.66		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.		
Event Type	communicationsAlarm		
Probable Cause	transmitFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	RAI condition is present on DS3-Line #n	DS3 RAI alarm: RAI	To clear the Remote Alarm Indication (RAI) failure, remove the presence of any of the following: ▪ Far-end Severely Errored Frame (SEF) / Alarm Indication Signal (AIS) defect (aka 'yellow'). To correct it, set the two X-bits in the M-frame that are set to zero, to one (RFC 1407). ▪ One or two alarm signals on the far-end alarm channel. Note that the 'dsx3LineStatus' field in dsx3ConfigTable will have a value of **dsx3RcvRAIFailure(2)**
Cleared	RIA condition is not present	-	-

A.1.12.2 DS3 AIS Alarm

Table A-27: acDS3AISAlarm

Alarm	acDS3AISAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.67		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.		
Event Type	communicationsAlarm		
Probable Cause	receiveFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	AIS condition is present on DS3-Line #n	DS3 AIS alarm: AIS	▪ Remove the presence of Alarm Indication Signal (AIS) in contiguous M-frames for a time equal to or greater than T, where 0.2 ms <= T <= 100 ms. ▪ See RFC 3896 for information on DS3 AIS framed with "stuck stuffing". Note that the 'dsx3LineStatus' field in dsx3ConfigTable will have a value of **dsx3RcvAIS(8)**
Cleared	AIS condition is not present	-	-

A.1.12.3 DS3 LOF Alarm

Table A-28: acDS3LOFAlarm

Alarm	acDS3LOFAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.68
Default Severity	Critical
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type	communicationsAlarm
Probable Cause	lossOfFrame

Alarm Severity	Condition	<text>	Corrective Action
Critical	LOF condition is present on DS3-Line #n	DS3 LOF alarm: LOF	**1.** Correct the configuration settings on the line. They're correct for the the port but not correct for the line. **2.** Make sure the framing format configured on the port matches the framing format on the line. **3.** Try see if the other framing format clears the alarm. **4.** Configure a remote loopback on the affected interface. Do this with your provider. Run an unframed Bit Error Rate Tester (BERT) to see if there're problems on the line. **5.** Isolate the problem using hard or soft loopbacks (if you find evidence of a bad line). Note that the 'dsx3LineStatus' field in dsx3ConfigTable will have a value **dsx3LOF (32)**
Cleared	LOF condition is not present	-	-

A.1.12.4 DS3 LOS Alarm

Table A-29: acDS3LOSAlarm

Alarm	acDS3LOSAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.69		
Default Severity	Critical		
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.		
Event Type	communicationsAlarm		
Probable Cause	lossOfSignal		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	LOS condition is present on DS3-Line #n	DS3 LOS alarm: LOS	▪ Achieve an average pulse density of at least 33% over a period of 175 +/- 75 contiguous pulse positions starting with the receipt of a pulse. ▪ The alarm occurs if there are 175 +/- 75 contiguous pulse positions with no pulses of either positive or negative polarity. See the IETF DS3/E3 MIB. Note that the 'dsx3LineStatus' field in dsx3ConfigTable will have a value of **dsx3LOS (64)**
Cleared	LOS condition is not present	-	-

A.1.12.5 DS3 Line Status Change Alarm

Table A-30: dsx3LineStatusChangeTrap

Alarm	dsx3LineStatusChange
OID	1.3.6.1.2.1.10.30.15.0.1
Default Severity	Major on raise; Clear on clear
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type	communicationsAlarm
Probable Cause	A dsx3LineStatusChange trap is sent when the value of an instance of dsx3LineStatus changes. It can be utilized by an NMS to trigger polls. When the line status change results in a lower level line status change (i.e., ds1), then no traps for the lower level are sent.
Alarm Text	DS3 Line Status
Additional Info1,2,3	Updated DS3 Line Status. This variable indicates the Line Status of the interface. It contains loopback state information and failure state information. The dsx3LineStatus is a bit map represented as a sum, therefore it can represent multiple failures and a loopback (see dsx3LoopbackConfig object for the type of loopback) simultaneously. The dsx3NoAlarm must be set if and only if no other flag is set. If the dsx3loopbackState bit is set, the loopback in effect can be determined from the dsx3loopbackConfig object. The various bit positions are: 1 dsx3NoAlarm No alarm present 2 dsx3RcvRAIFailure Receiving Yellow/Remote Alarm Indication 4 dsx3XmitRAIAlarm Transmitting Yellow/Remote Alarm Indication 8 dsx3RcvAIS Receiving AIS failure state 16 dsx3XmitAIS Transmitting AIS 32 dsx3LOF Receiving LOF failure state 64 dsx3LOS Receiving LOS failure state

	128	dsx3LoopbackState	Looping the received signal
	256	dsx3RcvTestCode	Receiving a Test Pattern
	512	dsx3OtherFailure	Any line status not defined here
	1024	dsx3UnavailSigState	Near End in Unavailable Signal State
	2048	dsx3NetEquipOOS	Carrier Equipment Out of Service

A.1.13 SS7 Alarms

A.1.13.1 SS7 Link State Change Alarm Trap

Table A-31: acSS7 Link State Change Alarm Trap

Alarm	acSS7LinkStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.19
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	other
Alarm Text	*** SS7 *** Link %i is %s $s
Status Changes	
1. Condition	Operational state of the SS7 link becomes 'BUSY'.
Alarm status	Major
<text> value	%i - <Link number> %s - <state name>: { "OFFLINE", "BUSY", "INSERVICE"} %s – IF link has MTP3 layer, then this string equals: (SP %i linkset %i slc %i) Where: %i - <SP number> %i - <Link-Set number> %i - <SLC number> Otherwise there is NO additional text.
Additional Info1 varbind	BUSY
2. Condition	Operational state of the link becomes 'IN-SERVICE' or 'OFFLINE'.
Alarm status	cleared
Corrective Action	For full details see the SS7 section and SS7 MTP2 and MTP3 relevant standards.

A.1.13.2 SS7 Link Congestion State Change Alarm Trap

Table A-32: acSS7 Link CongestionState Change Alarm Trap

Alarm	acSS7LinkCongestionStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.22
Default Severity	Major
Alarm Type	communicationsAlarm
Probable Cause	other
Alarm Text	*** SS7 *** Link %i is %s %s %i - <Link number> %s – IF link has MTP3 layer, then this string equals: (SP %i linkset %i slc %i) Where: %i - <SP number> %i - <Link-Set number> %i - <SLC number> Otherwise there is NO additional text. %s - <congestion state>: { "UNCONGESTED", "CONGESTED" }
Status Changes	
1. Condition	SS7 link becomes congested (local or remote).
Alarm status	Major
Additional Info1 varbind	CONGESTED
2. Condition	Link becomes un-congested - local AND remote.
Alarm status	Cleared
Corrective Action	Reduce SS7 traffic on that link.
Note :	This alarm is raised for any change in the remote or local congestion status.

A.1.13.3 SS7 Link Inhibit State Change Alarm Trap

Table A-33: SS7 Link Inhibit State Change Alarm Trap

Alarm	acSS7LinkInhibitStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.20
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	other
Alarm Text	*** SS7 *** Link %i (SP %i linkset %i slc %i) is %s
Status Changes	
1. Condition	SS7 link becomes inhibited (local or remote).
Alarm status	Major
<text> value	%i - <Link number> %i - <SP number> %i - <Link-Set number> %i - <SLC number> %s - <congestion state>: { "UNINHIBITED", "INHIBITED" }

Additional Info1 varbind	INHIBITED
2. Condition	Link becomes uninhibited - local AND remote
Alarm status	cleared
Corrective Action	Make sure the link is uninhibited – on both local and remote sides
Note	This alarm is raised for any change in the remote or local inhibition status.

A.1.13.4 SS7 Link Set State Change Alarm

Table A-34: SS7 Link Set State Change Alarm

Alarm	acSS7LinkSetStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.23
Default Severity	Major
Alarm Type	communicationsAlarm
Probable Cause	other
Alarm Text	*** SS7 *** Linkset %i on SP %i is %s
Status Changes	
1. Condition	Operational state of the SS7 link-set becomes BUSY.
Alarm status	Major
<text> value	%i - <Link-Set number> %i - <SP number> %s - <state name: { "OFFLINE", "BUSY", "INSERVICE"}
Additional Info1 varbind	BUSY
2. Condition	Operational state of the link-set becomes IN-SERVICE or OFFLINE
Alarm status	cleared
Corrective Action	For full details see the SS7 section and SS7 MTP3 relevant standards

A.1.13.5 SS7 Route Set State Change Alarm Trap

Table A-35: SS7 Route Set State Change Alarm Trap

Alarm	acSS7RouteSetStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.24
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	Other
Alarm Text	*** SS7 *** Routeset %i on SP %i is %s
Status Changes	
1. Condition	Operational state of the SS7 route-set becomes BUSY
Alarm status	Major
<text> value	%i - <Route-Set number> %i - <SP number> %s - <state name: { "OFFLINE", "BUSY", "INSERVICE"}
Additional Info	BUSY
2. Condition	Operational state of the route-set becomes IN-SERVICE or OFFLINE.
Alarm status	Cleared

Alarm	acSS7RouteSetStateChangeAlarm
Corrective Action	For full details see the SS7 section and SS7 MTP3 relevant standards.

The source varbind text for all the alarms under the component above is System#0/SS7#0/ SS7RouteSet#<m> where m is the route set number. **(Applicable to Mediant 3000 devices**.)

A.1.13.6 SS7 SN Set State Change Alarm Trap

Table A-36: SS7 SN Set State Change Alarm Trap

Alarm	acSS7SNSetStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.25
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	Other
Alarm Text	*** SS7 *** SP %i is %s
Status Changes	
1. Condition	Operational state of the SS7 node becomes BUSY
Alarm status	Major
<text> value	%i - <SP number> %s - <state name: { "OFFLINE", "BUSY", "INSERVICE"}
Additional Info1 varbind	BUSY
2. Condition	Cleared when the operational state of the node becomes IN-SERVICE or OFFLINE
Alarm status	Cleared
Corrective Action	Signaling Node must complete its MTP3 restart procedure and become un-isolated For full details see the SS7 section and SS7 MTP3 relevant standards.

The source varbind text for all the alarms under the component above is System#0/SS7#0/SS7SN#<m> where m is the SN (signaling node) number. **(Applicable to Mediant 3000 devices.)**

Table A-37: SS7 Ual Group State Change Alarm Trap

Alarm	acSS7UalGroupStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.74
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	other
Alarm Text	*** SS7 *** Group Id %j Asp status is %s
Status Changes	
Condition	Group ASP status changes.
Alarm status	Major
<text> value	%i - Group number %s - New state ("NO_SCTP", "SCTP_ASSOCIATE", SCTP_FAILURE", "ASP_DOWN", "ASP_INACTIVE", "ASP_ACTIVE")
Additional Info1 varbind	
Condition	When group ASP status changes to "ASP_ACTIVE"
Alarm status	cleared

Alarm	acSS7UalGroupStateChangeAlarm
Corrective Action	

The source varbind text for all the alarms under the component above is System#0/SS7#0/ss7ualgroup#<m> where m is the ual group number. (Applicable to 3000 devices.)

A.1.14 Hitless Software Upgrade Alarm

Note: These alarms apply to Mediant 800B GW & E-SBC HA, Mediant 3000 HA, Mediant 2600 HA, Mediant 4000 HA, Mediant SE SBC HA, and Mediant VE SBC HA.

Table A-38: acHitlessUpdateStatus

Alarm	acHitlessUpdateStatus		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48		
Default Severity	-		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Indeterminate	A notification trap sent at the *beginning* and *end* of a hitless software update. Failure *during* the software update also activates the trap.	Hitless Update Event	The corrective action for each condition is described below.
	Hitless: Start software upgrade.		Corrective action is not required.
	Hitless fail: Invalid cmp file file - missing Version parameter.		Replace the cmp file with a valid one.
	Hitless fail: The software version stream name is too long.		Replace the cmp file with a valid one.
	Hitless fail: Invalid cmp file - missing UPG parameter.		Replace the cmp file with a valid one.
	Hitless fail: Hitless software upgrade is not supported.		Replace the cmp file with a valid one that supports hitless upgrade of the software from the current version to the new one.
	Hitless: Software upgrade ended successfully.		Corrective action is not required.

A.1.15 High Availability Alarms

⚠️ **Note:** These alarms apply to Mediant 800B GW & E-SBC HA, Mediant 3000 HA, Mediant 4000 HA, Mediant SE SBC HA and Mediant VE SBC HA.

A.1.15.1 HA System Fault Alarm

Table A-39: acHASystemFaultAlarm

Trap	acHASystemFaultAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.33		
Description	Sent when the High Availability (HA) system is faulty (i.e., no HA functionality).		
Default Severity	Critical		
Source Varbind Text	System#0/Module#<m>, where *m* is the blade module's slot number		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	HA feature is active but the system is not working in HA mode	Fatal exception error	High Availability (HA) was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		TCPIP exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Network processor exception error (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		SW WD exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		HW WD exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		SAT device is missing (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		SAT device error (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		DSP error (applicable only to Mediant 3000 and Mediant 4000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		BIT tests error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.

		PSTN stack error (applicable only to Mediant 3000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Keep Alive error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Software upgrade	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Manual switch over	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Manual reset	HA was lost due to a *system reset* and should return automatically after few minutes. Corrective action is not required.
		Board removal (applicable only to Mediant 3000)	Return the removed board to the system.
		TER misplaced (applicable only to Mediant 3000)	Place the TER card according to the *User's Manual*
		HW fault. TER in slot 2 or 3 is missing (applicable only to Mediant 3000)	Place the TER card according to the *User's Manual*
		HW fault. TER has old version or is not functional (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. invalid TER Type (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. invalid TER active/redundant state (applicable only to Mediant 3000)	Replace the TER card.
		HW fault. Error reading GbE state (applicable only to Mediant 3000)	Replace the TER card.
		Redundant module is missing (applicable only to Mediant 3000)	1. Insert the redundant module into the system. 2. If the error continues, reset / replace the module.
		Redundant is not connecting (applicable only to Mediant 3000)	Reset / replace the redundant module.
		Redundant is not reconnecting after deliberate restart	Reset / replace the redundant module.
		No Ethernet Link in redundant module	Connect Ethernet links to the redundant module
		SA module faulty or missing (applicable only to Mediant 3000)	Make sure the Shelf Alarm module is inserted correctly.
		Eth link error	HA was lost due to switchover, Connect the Eth link back.
		Higher HA priority (Not applicable to Mediant 3000)	HA was lost due to switchover to unit with higher HA priority and should return automatically after a few minutes. Corrective action is not required.
		Network watchdog error	HA was lost due to switchover , Fix the network connectivity from failed unit

Minor	HA feature is active and the redundant module is in startup mode and hasn't connected yet	Waiting for redundant to connect (applicable only to Mediant 3000)	Corrective action is not required.
Cleared	HA system is active	-	-

A.1.15.2 HA System Configuration Mismatch Alarm

Table A-40: acHASystemConfigMismatchAlarm

Trap	acHASystemConfigMismatchAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34		
Description	Sent when the configuration of the modules in the HA system is not identical, causing instability.		
Default Severity	Major		
Source Varbind Text	System#0/Module#<m>, where m is the blade module's slot number		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	HA feature is active:	Configuration mismatch in the system:	The actions for the conditions are described below.
	License Keys of Active and Redundant modules are different.	Active and Redundant modules have different feature keys.	Update the Feature Keys of the Active and Redundant modules.
	The Active module was unable to pass on to the Redundant module the License Key.	Fail to update the redundant with feature key.	Replace the Feature Key of the Redundant module – it may be invalid.
	License key of the Redundant module is invalid.	Feature key did not update in redundant module.	Replace the Feature Key of the Redundant module – it may be invalid.
Cleared	Successful License Key update	The feature key was successfully updated in the redundant module	**-**

A.1.15.3 HA System Switch Over Alarm

Table A-41: acHASystemSwitchOverAlarm

Trap	acHASystemSwitchOverAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35		
Description	Sent when a switchover from the active to the redundant module has occurred.		
Default Severity	Critical		
Source Varbind Text	System#0/Module#<m>, where m is the blade module's slot number		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**

Trap	acHASystemSwitchOverAlarm		
Critical	A switchover from the active to the redundant unit has occurred	Switch-over: See the acHASystemFaultAlarm table above	.
Cleared	10 seconds have passed since the switchover	-	-

A.1.16 Device (Board) Alarms

The source varbind text for all the alarms under this component depends on the device:

■ 3000 Series: **Board#0<n>**

■ All other devices: **System#0<n>**

Where *n* is the slot number in which the blade resides in the chassis. For Mediant 1000 and MediaPack, *n* always equals to 1.

A.1.16.1 Fatal Error Alarm

Table A-42: acBoardFatalError

Alarm	acBoardFatalError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1		
Description	Sent whenever a fatal device error occurs.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Any fatal error	Board Fatal Error: A run-time specific string describing the fatal error	1. Capture the alarm information and the Syslog clause, if active.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After fatal error	-	2. Contact AudioCodes' Support Center at support@audiocodes.com which will want to collect additional data from the device and perform a reset.

A.1.16.2 Configuration Error Alarm

Table A-43: acBoardConfigurationError

Alarm	acBoardConfigurationError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2		
Description	Sent when the device's settings are invalid. The trap contains a message stating/detailing/explaining the invalid setting.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	A configuration error was detected	Board Config Error: A run-time specific string describing the configuration error	1. Check the run-time specific string to determine the nature of the configuration error.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After configuration error	-	2. Fix the configuration error using the appropriate tool: Web interface, EMS, or *ini* file. 3. Save the configuration and if necessary reset the device.

A.1.16.3 Temperature Alarm

Table A-44: acBoardTemperatureAlarm

Alarm	acBoardTemperatureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3		
Description	Sent when the device exceeds its temperature limits. Applies only to 2000 and 3000 Series devices.		
Source Varbind Text	System#0		
Event Type	equipmentAlarm		
Probable Cause	▪ The air filter is saturated. ▪ One of the fans work slower than expected. temperatureUnacceptable (50)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Temperature is above 60°C (140°F)	Board temperature too high **For Mediant 3000:** Fans at High speed - check your ventilation outlet and environment temperature.	1. Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels. 2. Clean the air filter – refer to the *Hardware Installation Manual* on how to clean/replace the air filter. 3. If after cleaning the air filter the alarm still exists: Check if all fans in the system are properly operating. **For Mediant 3000:** Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. **For Mediant 1000:** Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Temperature falls below 55°C (131°F)	-	-

A.1.16.4 Software Reset Alarm

Table A-45: acBoardEvResettingBoard

Alarm	acBoardEvResettingBoard			
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5			
Description	Sent after the device resets.			
Default Severity	Critical			
Event Type	equipmentAlarm			
Probable Cause	outOfService (71)			
Alarm Severity	**Condition**	**<text>**		**Corrective Action**
Critical	When a soft reset is triggered via the Web interface or SNMP	User resetting board		A network administrator has taken action to reset the device. Corrective action is not required.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After raise			

A.1.16.5 Software Upgrade Alarm

Table A-46: acSWUpgradeAlarm

Alarm	acSWUpgradeAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.70		
Description	Sent for software upgrade process errors.		
Default Severity	Major		
Alarms Source	System#0		
Event Type	processingErrorAlarm		
Probable Cause	softwareProgramError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised upon software upgrade errors	SW upgrade error: Firmware burning failed. Startup system from Bootp/tftp.	Start up the system from BootP/TFTP.

A.1.16.6 Call Resources Alarm

Table A-47: acBoardCallResourcesAlarm

Alarm	acBoardCallResourcesAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.8		
Description	Sent when no free channels are available.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Percentage of busy channels exceeds the predefined RAI high threshold	Call resources alarm	▪ Expand system capacity by adding more channels (trunks) -OR- ▪ Reduce traffic
Cleared	Percentage of busy channels falls below the predefined RAI low threshold	-	Note that to enable this alarm, the Remote Alarm Indication (RAI) mechanism must be activated (EnableRAI = **1**).

A.1.16.7 Controller Failure Alarm

Table A-48: acBoardControllerFailureAlarm

Alarm	acBoardControllerFailureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.9
Description	▪ Sent when the Proxy is not found or registration fails. Internal routing table may be used for routing. ▪ Sent when the physical network link is up or down ("BusyOut Trunk/Line n Link failure"). ▪ GWAPP_TRAP_BUSYOUT_CONNECTIVITY: Sent when the connection to the Proxy is up or down ("BusyOut Trunk/Line n Connectivity Proxy failure"). ▪ GWAPP_TRAP_BUSYOUT_TDM_OVER_IP: Sent when a failure occurs in TDM over IP (transparent T1/E1 without signaling) - "BusyOut Trunk n TDM over IP failure (Active calls x Min y)". (**Note:** Applicable only to Digital Series.) ▪ GWAPP_TRAP_BUSYOUT_PROXY_SET: Sent when the connection to the Proxy Set associated with this trunk/line is up/down ("BusyOut Trunk/Line n Proxy Set Failure"). ▪ GWAPP_TRAP_BUSYOUT_REGISTRATION: Sent when a failure occurs in server registration for this trunk/line ("BusyOut Trunk/Line n Registration Failure"). ▪ GWAPP_TRAP_BUSYOUT_SERVING_IPGROUP: Sent when a failure occurs in a Serving IP Group for this trunk ("BusyOut Trunk n Serving IP Group Failure"). (**Note:** Applicable only to Digital Series.) ▪ GWAPP_TRAP_PROXY_SET: Sent when a failure occurs in a Proxy Set (not per trunk/line, but per Proxy Set) - "Proxy Set ID n".
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	softwareError (46)

Alarm	acBoardControllerFailureAlarm		
Alarm Severity	**Condition**	**\<text>**	**Additional Information**
Major	Proxy has not been found or the physical network link is up or down ("BusyOut Trunk/Line n Link failure").	Controller failure alarm: Proxy not found. Use internal routing. -OR- Proxy lost. Looking for another Proxy.	▪ Check the network layer ▪ Make sure that the proxy IP and port are configured correctly.
Cleared	Proxy is found. The 'Cleared' message includes the IP address of this Proxy.	-	-

A.1.16.8 Board Overload Alarm

Table A-49: acBoardOverloadAlarm

Alarm	acBoardOverloadAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11		
Description	Sent when there is an overload in one or some of the system's components.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**\<text>**	**Corrective Action**
Major	An overload condition exists in one or more of the system components	"System CPU overload condition - IdleUtilization percentage=%d" Where *%d* is the percentage of available CPU resources remaining	1. Make sure that the syslog level is 0 (or not high). 2. Make sure that DebugRecording is not running. 3. If the system is configured correctly, reduce traffic.
Cleared	The overload condition passed	"System CPU overload condition - IdleUtilization percentage=%"	-

A.1.16.9 Feature Key Error Alarm

Table A-50: acFeatureKeyError

Alarm	acFeatureKeyError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.6
Description	Sent to relay Feature Key errors etc.
Default Severity	Critical
Event Type	processingErrorAlarm
Probable Cause	configurationOrCustomizationError (7)
Alarm Text	Feature key error
Status Changes	
Note	Support for this alarm is pending.

A.1.16.10 Missing SA/M3K Blade (Alarm, Status and Synchronization) Alarm

⚠️ **Note:** Applicable only to Mediant 3000.

Table A-51: acSAMissingAlarm

Alarm	acSAMissingAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.32		
Description	Sent when the Shelf Alarm (SA) module is missing or non operational.		
Default Severity	Critical		
Source Varbind Text	Chassis#0/SA#<m>, where *m* is the shelf Alarm module's slot number		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	SA module removed or missing	SA Module Alarm. SA-Module from slot #n is missing.	▪ Reinsert the Shelf Alarm (SA) module into slot #n ▪ Make sure it's correctly inserted in the slot.
Cleared	SA module is in slot 2 or 4 and working.	-	**-**

A.1.16.11 Administration Status Change Alarm

Table A-52: acgwAdminStateChange

Alarm	acgwAdminStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7		
Description	Sent when Graceful Shutdown commences and ends.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Admin state changed to shutting down	Network element admin state change alarm: Gateway is shutting down. No time limit.	▪ No corrective action is required. ▪ A network administrator took an action *to gracefully lock the device*.
Major	Admin state changed to locked	Locked	▪ No corrective action is required. ▪ A network administrator took an action *to lock the device, or a graceful lock timeout occured*.
Cleared	Admin state changed to unlocked	-	▪ No corrective action is required. ▪ A network administrator has taken an action *to unlock the device*.

A.1.16.12 Operational Status Change Alarm

Table A-53: acOperationalStateChange

Alarm	acOperationalStateChange
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.15
Description	Sent if the operational state of the node goes to disabled; cleared when the operational state of the node goes to enabled.
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	outOfService (71)

Alarm Severity	Condition	\<text\>	Corrective Action
Major	Operational state changed to disabled	Network element operational state change alarm. Operational state is disabled.	▪ The alarm is cleared when the operational state of the node goes to enabled. ▪ In IP systems, check for initialization errors - in IP systems the operational state of the node is disabled if the device fails to properly initialize. ▪ Look for other alarms and Syslogs that might provide additional information about the error.
Cleared	Operational state changed to enabled	-	-

A.1.17 Network Alarms

A.1.17.1 Ethernet Link Alarm

Table A-54: acBoardEthernetLinkAlarm

Alarm	acBoardEthernetLinkAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Description	Sent when the Ethernet link(s) is down.
Default Severity	Critical
Source Varbind Text	All except 3000 Series: Board#\<n\>/EthernetLink#0 (where n is the slot number) 3000 Series: Chassis#0/Module#\<n\>/EthernetLink#0 (where n is the blade's slot number) This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link).
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable (56)

Alarm Severity	Condition	\<text\>	Corrective Action
Major	Fault on single interface	Ethernet link alarm: Redundant link is down	1. Ensure that both Ethernet cables are plugged into the back of the system. 2. Observe the system's Ethernet link lights to determine which interface is failing. 3. Reconnect the cable or fix the network problem
Critical	Fault on both interfaces	No Ethernet link	

Cleared	Both interfaces are operational	-	Note that the alarm behaves differently when coming from the redundant or the active modules of a High Availability (HA) system. The alarm from the redundant is raised when there is an operational HA configuration in the system. There is no critical severity for the redundant module losing both its Ethernet links as that is conveyed in the no HA alarm that follows such a case.

A.1.17.2 Ethernet Group Alarm

> ⚠️ **Note:** Applicable only to Mediant 500 GW & E-SBC, Mediant 800B GW & E-SBC, and Mediant 1000B GW & E-SBC.

Table A-55: acEthernetGroupAlarm

Alarm	acEthernetGroupAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.86
Description	This alarm is raised when both ports in an Ethernet port-pair group (1+1) are down, and cleared when at least one port is up.
Default Severity	Major
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Alarm Text	Ethernet Group alarm. %s
Status Changes	
1. Condition	Raised when both ports in a group are down
2. Condition	Cleared when at least one port is up

A.1.17.3 WAN Link Alarm

Table A-56: acBoardWanLinkAlarm (only for MSBR Series)

Alarm	acBoardWanLinkAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.79		
Description	This alarm is raised when the WAN Link is down (and cleared when link is up again).		
Default Severity	Major / Clear		
Event Type	equipmentAlarm		
Source Varbind Text	Board#x/WanLink#y		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	WAN link down	-	Connect the WAN port
Clear	WAN link up	-	-

A.1.17.4 Data Interface Status Alarm

⚠	**Note:** Applicable only to MSBR series.

Table A-57: acDataInterfaceStatus

Alarm	acDataInterfaceStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.83
Default Severity	Indeterminate
Event Type	communicationsAlarm
Probable Cause	
Alarm Text	
Status Changes	
1. Condition	
Alarm Status	
<text> Value	
Corrective Action	No corrective action is required as this is an event, not an alarm.

A.1.17.5 Wireless Cellular Modem Alarm

⚠	**Note:** Applicable only to Mediant 500 MSBR and Mediant 800B MSBR.

Table A-58: acWirelessCellularModemAlarm

Alarm	acWirelessCellularModemAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.82		
Description	This alarm is raised when either the wireless modem is down or in backup mode, and cleared when modem is up.		
Default Severity	Major / Clear		
Source Varbind Text	Board#x/WanLink#y		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised when either the wireless modem is down or in backup mode, and cleared when modem is up.	WAN wireless cellular modem alarm	Get the link up. Investigate the possibility of an electronics failure or a problem with the radio frequency (RF) path.
Clear	WAN link up	-	-

A.1.17.6 NTP Server Status Alarm

Table A-59: acNTPServerStatusAlarm

Alarm	acNTPServerStatusAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.71		
Description	NTP server status alarm. Raised when the connection to the NTP server is lost. Cleared when the connection is reestablished. Unset time (as a result of no connection to NTP server) may result with functionality degradation and failure in device.		
Default Severity	Major		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Alarm Severity	**Condition**	**\<text\>**	**Corrective Action**
Major	No initial communication to Network Time Protocol (NTP) server.	NTP server alarm. No connection to NTP server.	Repair NTP communication (the NTP server is down or its IP address is configured incorrectly in the device).
Minor	No communication to NTP server after the time was already set once.	-	**-**

A.1.17.7 NAT Traversal Alarm

Table A-60: acNATTraversalAlarm

Alarm	acNATTraversalAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.17
Description	Sent when the NAT is placed in front of a device and is identified as a symmetric NAT. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.
Default Severity	Indeterminate
Event Type	-
Probable Cause	other (0)
Alarm Text	NAT Traversal Alarm
Status Changes	The STUN client in the device is enabled and has either identified a NAT or is not finding the STUN server. Keep-alive is sent out every 9/10 of the time defined in the 'NatBindingDefaultTimeout' parameter.
Corrective Action	See http://tools.ietf.org/html/rfc5389

A.1.17.8 LDAP Lost Connection Alarm

Table A-61: acLDAPLostConnection

Alarm	acLDAPLostConnection
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.75
Default Severity	Minor
Event Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure If a connection is idle for more than the maximum configured time in seconds that the client can be idle before the LDAP server closes the connection, the LDAP server returns an LDAP disconnect notification and this alarm is raised.
Alarm Text	LDAP Lost Connection
Status Changes	This alarm is raised when there is no connection to the LDAP server
1. Condition	
Alarm Status	

A.1.17.9 OCSP Server Status Alarm

Table A-62: acOCSPServerStatusAlarm

Alarm	acOCSPServerStatusAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.78
Default Severity	Major / Clear
Event Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure
Alarm Text	OCSP server alarm
Corrective Action	▪ Repair the Online Certificate Status Protocol (OCSP) server -OR- ▪ Correct the network configuration

A.1.17.10 IPv6 Error Alarm

Table A-63: acIPv6ErrorAlarm (Applicable only to E-SBC Series)

Alarm	acIPv6ErrorAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.53		
Default Severity	Critical		
Source Varbind Text	System#0/Interfaces#<n>.		
Event Type	operationalViolation		
Probable Cause	communicationsProtocolError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Bad IPv6 address (already exists)	IP interface alarm: IPv6 configuration failed, IPv6 will be disabled.	▪ Find a new IPV6 address. ▪ Reboot the device.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After the alarm is raised.	-	-

A.1.17.11 Active Alarm Table Alarm

Table A-64: acActiveAlarmTableOverflow

Alarm	acActiveAlarmTableOverflow		
OID	1.3.6.1.4.15003.9.10.1.21.2.0.12		
Description	Sent when an active alarm cannot be entered into the Active Alarm table because the table is full.		
Default Severity	Major		
Source Varbind Text	*System#0<n>/AlarmManager#0*		
Event Type	processingErrorAlarm		
Probable Cause	resourceAtOrNearingCapacity (43)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Too many alarms to fit in the active alarm table	Active alarm table overflow	▪ Some alarm information may be lost but the ability of the device to perform its basic operations is not impacted. ▪ A reboot is the only way to completely clear a problem with the active alarm table. ▪ Contact AudioCodes' Support Center at support@audiocodes.com
Remains 'Major' until reboot. A 'Clear' trap is not sent.	After the alarm is raised	-	Note that the status remains 'Major' until reboot as it denotes a possible loss of information until the next reboot. If an alarm is raised when the table is full, it is possible that the alarm is active, but does not appear in the active alarm table.

A.1.17.12 Audio Staging from APS Server Alarm

> ⚠ **Note:** Applicable only to Mediant 1000B series.

Table A-65: acAudioProvisioningAlarm

Alarm	acAudioProvisioningAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.14		
Description	Sent if the device is unable to provision its audio.		
Default Severity	Critical		
Source Varbind Text	System#0/AudioStaging#0		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError (7)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Media server times out waiting for a successful audio distribution from the APS (Audio Provisioning Server)	Unable to provision audio	• From the Audio Provisioning Server (APS) GUI, ensure that the device is properly configured with audio and that the device has been enabled. • Ensure that the IP address for the APS has been properly specified on the device. • Ensure that both the APS server and application are in-service. • For more information regarding the problem, view the Syslogs from the device as well as the APS manager logs.
Cleared	After the alarm is raised, the media server is successfully provisioned with audio from the APS	-	

A.1.18 Analog Port Alarms

⚠️ **Note:** These alarms are applicable only to Analog Series.

A.1.18.1 Analog Port SPI Out-of-Service Alarm

Table A-66: acAnalogPortSPIOutOfService

Alarm	acAnalogPortSPIOutOfService		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.46		
Default Severity	Major		
Source Varbind Text	System#0/analogports#<n>, where *n* is the port number		
Event Type	physicalViolation		
Probable Cause	equipmentMalfunction		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Analog port has gone out of service	Analog Port SPI out of service	▪ No corrective action is required. ▪ The device shuts down the port and activates it again when the Serial Peripheral Interface (SPI) connection returns.
Cleared	Analog port is back in service	-	-

A.1.18.2 Analog Port High Temperature Alarm

Table A-67: acAnalogPortHighTemperature

Alarm	acAnalogPortHighTemperature		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.47		
Default Severity	Major		
Source Varbind Text	System#0/analogports#<n>, where *n* is the port number		
Event Type	physicalViolation		
Probable Cause	equipmentMalfunction		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Analog device has reached critical temperature. Device is automatically disconnected.	Analog Port High Temperature	▪ No corrective action is required. ▪ The device shuts down the analog port and tries to activate it again later when the device's temperature drops.
Cleared	Temperature is back to normal - analog port is back in service.	-	-

A.1.18.3 Analog Port Ground Fault Out-of-Service Alarm

Table A-68: acAnalogPortGroundFaultOutOfService

Alarm	acAnalogPortGroundFaultOutOfService
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.76
Default Severity	Major / Clear
Source Varbind Text	System#0/analogports#<n>, where *n* is the port number
Event Type	physicalViolation
Probable Cause	equipmentMalfunction (this alarm is raised when the FXS port is inactive due to a ground fault)
Alarm Text	Analog Port Ground Fault Out Of Service
Corrective Action	▪ No corrective action is required. ▪ The device shuts down the port and tries to activate it again when the relevant alarm is over.
Note	Relevant to FXS only.

A.1.19 Media Alarms

A.1.19.1 Media Process Overload Alarm

> **Note:** This alarm is applicable only to the MSBR series, Mediant 1000B GW & SBC, Mediant 2000, and Mediant 3000.

Table A-69: acMediaProcessOverloadAlarm

Alarm	acMediaProcessOverloadAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.81		
Description	Sent when there is overload of the device's media processing and interfaces.		
Default Severity	Major		
Event Type	environmentalAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	-	Media Process Overload Alarm. %s	▪ Avoid making new calls. Although not corrective, this action eventually causes the alarm to drop.
Cleared	-	-	None

A.1.19.2 Media Realm Bandwidth Threshold Alarm

⚠	**Note:** This alarm is applicable only to Digital Series and E-SBC Series.

Table A-70: acMediaRealmBWThresholdAlarm

Alarm	acMediaRealmBWThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.87		
Default Severity			
Event Type	ProcessingErrorAlarm		
Probable Cause	Raised when a bandwidth threshold is crossed		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	-	Media Realm BW Threshold Alarm	Cleared when bandwidth threshold returns to normal range

A.1.20 Network Monitoring (Probe) between Devices

⚠	**Note:** This alarm is applicable only to Mediant 800B MSBR.

A.1.20.1 NQM Connectivity Alarm

Table A-71: acNqmConnectivityAlarm

Alarm	acNqmConnectivityAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.88		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsSubsystemFailure		
Probable Cause	Raised when Connectivity with NQM probe destination is lost		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Connectivity with NQM probe destination is lost	Cleared when connectivity with the Noise Quality Measure (NQM) probe destination is re-established

A.1.20.2 NQM High RTT Alarm

Table A-72: acNqmRttAlarm

Alarm	acNqmRttAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.89		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsSubsystemFailure		
Probable Cause	Raised when Detected high RTT towards NQM probe destination		
Alarm Severity	**Condition**	**\<text>**	**Corrective Action**
Minor	-	Detected high RTT towards NQM probe destination	To correct long RTT (Round Trip Time): ▪ Test with traceroute. ▪ Contact your ISP with the traceroute results. ▪ Use Wireshark or any other diagnostic tool to perform a traffic capture and determine who is contaminating the network.

A.1.20.3 NQM High Jitter Alarm

Table A-73: acNqmJitterAlarm

Alarm	acNqmJitterAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.90		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	CommunicationsAlarm		
Probable Cause	Raised when Detected high Jitter towards NQM probe destination - thresholdCrossed		
Alarm Severity	**Condition**	**\<text>**	**Corrective Action**
Minor	-	Detected high Jitter towards NQM probe destination	To correct high jitter: ▪ Test with traceroute. ▪ Contact your Internet Service Provider (ISP) with traceroute results. ▪ Implement Quality of Service (QoS). ▪ Note that there's no simple solution for high jitter. A systemic level solution may be required.

A.1.20.4 NQM High Packet Loss Alarm

Table A-74: acNqmPacketLossAlarm

Alarm	acNqmPacketLossAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.91		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	CommunicationsAlarm		
Probable Cause	Raised when Detected high Packet Loss towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected high PL towards NQM probe destination	To correct high packet loss (PL): ▪ Eliminate interference problems: Distance your modem from electrical devices ▪ Do not coil up any excess signal or power cables. ▪ Check the statistics counters of network nodes to determine where loss is occurring. Typically, each node in the network has a packet loss counter. Isolate the network segment where loss has been occurring.

A.1.20.5 NQM Low Conversational MOS Alarm

Table A-75: acNqmCqMosAlarm

Alarm	acNqmCqMosAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.95		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsAlarm		
Probable Cause	Raised when Detected low conversational voice quality towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected low conversational voice quality towards NQM probe destination	To fix the Noise Quality Measure (NQM) result: ▪ Perform corrective action for jitter. See Section A.1.20.3. ▪ Perform corrective action for Real Time Protocol (RTP) packet loss. See Section A.1.20.4. ▪ Perform corrective action for long Round-Trip Time (RTT) - the time it takes for packets to travel from source to destination. See Section A.1.20.2. To fix the poor Conversational Quality (CQ) that the test indicates: ▪ Try changing the coder ▪ Try using RTP-Redundancy ▪ Perform corrective action for RTP packet loss. See Section A.1.20.4.

A.1.20.6 NQM Low Listening MOS Alarm

Table A-76: acNqmLqMosAlarm

Alarm	acNqmLqMosAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.96		
Default Severity			
Alarm Source	Board#%d/NqmSender#%d		
Event Type	communicationsAlarm		
Probable Cause	Raised when detected low listening voice quality towards NQM probe destination		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	-	Detected low listening voice quality towards NQM probe destination	To fix the Noise Quality Measure (NQM) result: ■ Perform corrective action for Real Time Protocol (RTP) packet loss. See Section A.1.20.4. To fix the poor listening quality that the test indicates: ■ Try changing the coder ■ Try using RTP-Redundancy ■ Perform corrective action for RTP packet loss. See Section A.1.20.4.

A.1.21 Intrusion Detection Alarms

A.1.21.1 IDS Policy Alarm

Table A-77: acIDSPolicyAlarm

Alarm	acIDSPolicyAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.99
Description	The alarm is raised whenever a threshold is crossed in the IDS system. The alarm is associated with the MO pair IDSMatch & IDSRule.
Default Severity	
Event Type	Other
Probable Cause	
Alarm Text	Policy NUM (NAME) minor/major/critical threshold (NUM) of REASON cross in global/ip/ip+port scope (triggered by IP)
Status Changes	
Corrective Action	1. Identify additional traps (acIDSThresholdCrossNotification) that were sent alongside this Intrusion Detection System (IDS) alarm. 2. Locate the remote hosts (IP addresses) that are specified in the traps. 3. Examine the behavior of those hosts (with regard to the reason specified in the alarm), and attempt to fix incorrect operation. 4. If necessary, change the configured thresholds in the IDS Rule table under the IDS Policy table.

A.1.22 SAS Alarms

A.1.22.1 Emergency Mode Alarm

Table A-78: acGWSASEmergencyModeAlarm

Alarm	acGWSASEmergencyModeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.59
Description	Sent by the Stand-Alone Survivability (SAS) application when switching from "Normal" mode to "Emergency" mode. This alarm is cleared once the SAS returns to "Normal" mode. **Note:** Applicable only to Analog and Digital Series.
Default Severity	
Event Type	Other
Probable Cause	Other
Alarm Text	-
Status Changes	Sent by the Stand-Alone Survivability (SAS) application when switching from 'Normal' mode to 'Emergency' mode. The alarm is cleared once the SAS returns to 'Normal' mode.
Corrective Action	▪ This alarm is only for informative purposes. ▪ No corrective action is required.

A.1.23 High-Availability (HA)

> **Note:** These SNMP events are applicable only to devices that support the High-Availability (HA) feature.

A.1.23.1 Redundant Board Trap

Table A-79: acRedundantBoardAlarm

Trap	acRedundantBoardAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.97
Description	Active board sends notification when an alarm or notification is raised in the redundant board.
Default Severity	Indeterminate
Event Type	Other (0)
Probable Cause	Other (0)
Condition	Alarm or notification is raised in the redundant board
Trap Text	

A.1.23.2 HA Network Watchdog Status Alarm

⚠️ **Note:** This SNMP event is applicable to all HA-supporting devices except Mediant 3000.

Table A-80: acHANetworkWatchdogStatusAlarm

Trap	acHANetworkWatchdogStatusAlarm	
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.98	
Description	This alarm indicates that the device's HA Network Reachability (network watchdog) feature is configured, but is not functioning correctly due to, for example, the Ethernet Group being down from where the ping is sent to the network entity. The device's HA Network Reachability feature is used to configure a network IP address to test reachability using pings. When the tested peer stops replying to the Active unit, a switchover is made to the Redundant unit. For configuring the HA Network Reachability feature, refer to the *User's Manual*.	
Default Severity	Major	
Source Varbind Text	System#0/Module#<m>, where *m* is the blade module's slot number	
Event Type	alarmTrap	
Probable Cause	outOfService	
Trap Text	**Condition**	**Corrective Action**
Failed sending ping	Some network configuration error	-
Network watchdog is disabled while HA priority is in use	When HA Priority is in use, the network watchdog module is disabled	**-**
Network watchdog is disabled while Redundant units has less Eth groups available	One or more of the Redundant unit's Ethernet Groups are down	**-**
Disabling network watchdog due to network interface error in Redundant unit	One or more of the Redundant unit's Ethernet Groups are down	**-**

A.1.23.3 Hitless Software Upgrade Status Trap

⚠️ **Note:** Applicable only to Mediant 500 E-SBC, Mediant 800B Gateway & E-SBC, Mediant 3000, Mediant 2600 E-SBC, Mediant 4000 SBC, Mediant 9000 SBC, and Mediant Software SBC.

Table A-81: acHitlessUpdateStatus

Alarm	acHitlessUpdateStatus	
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48	
Description	A notification trap sent at the beginning and end of a Hitless Software Upgrade. Failure during the software upgrade also activates the trap.	
Default Severity	Indeterminate	
Event Type	Other (0)	
Probable Cause	Other (0)	
Source	Automatic Update	
Trap Text	**Condition**	**Corrective Action**
"Hitless: Start software upgrade."	Hitless Upgrade has begun.	Corrective action is not required
"Hitless: SW upgrade ended successfully."	Successful Hitless Upgrade.	Corrective action is not required
"Hitless: Invalid cmp file - missing Ver parameter."	Hitless Upgrade failed because the cmp file is invalid. The cmp file's version parameter is incorrect.	Replace the cmp file with a valid one.
"Hitless fail: SW ver stream name too long." **Note:** Applicable only to Mediant 3000.	Hitless Upgrade failed because the cmp file is invalid. The number of characters defining the software version stream name in the cmp file has been exceeded.	Replace the cmp file with a valid one
"Hitless fail: Invalid cmp file - missing UPG parameter."	Hitless Upgrade failed because the cmp file is invalid. An upgrade parameter is missing from the file.	Replace the cmp file with a valid one.
"Hitless fail: Hitless SW upgrade not supported."	Hitless Upgrade failed because the cmp file is invalid. The cmp file does not support Hitless Upgrade of the current software version to the new software version.	Replace the cmp file with a valid one that supports hitless upgrade of the software from the current version to the new one.

A.2 Event Traps (Notifications)

This subsection details traps that are not alarms. These traps are sent with the severity varbind value of 'Indeterminate'. These traps don't 'Clear' and they don't appear in the alarm history or active tables. (The only log trap that does send 'Clear' is acPerformanceMonitoringThresholdCrossing).

A.2.1 IDS Threshold Cross Notification

Table A-82: acIDSThresholdCrossNotification

Alarm	acIDSThresholdCrossNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Description	Sent for each scope (IP or IP+Port) crossing a threshold of an active alarm.
Description	The trap is sent for each scope (IP or IPport) crossing a threshold of an active alarm.
Default Severity	
Event Type	Other
Probable Cause	
Alarm Text	Threshold cross for scope value IP. Severity=minor/major/critical. Current value=NUM
Status Changes	
Corrective Action	**1.** Identify the remote host (IP address / port) on the network which the Intrusion Detection System (IDS) has indicated is malicious. Note that the IDS determines a host to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). **2.** Block the malicious activity.

A.2.2 IDS Blacklist Notification

Table A-83: acIDSBlacklistNotification

Alarm	acIDSBlacklistNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.101
Description	
Default Severity	
Event Type	securityServiceOrMechanismViolation
Probable Cause	thresholdCrossed
Alarm Text	Added IP * to blacklist Removed IP * from blacklist
Status Changes	
Corrective Action	Identify the malicious remote host (IP address / port) that the Intrusion Detection System (IDS) has automatically blacklisted or removed from the blacklist. Note that a host is determined to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). The malicious source is automatically blacklisted for a user-defined period, after which it is removed from the blacklist.

A.2.3   Web User Access Denied due to Inactivity Trap

Table A-84: acWebUserAccessDisabled

Alarm	acWebUserAccessDisabled
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.93
Default Severity	Indeterminate
Event Type	
Probable Cause	Sent when Web user was disabled due to inactivity
Alarm Text	
Status Changes	
Corrective Action	Contact your Web security administrator. Only the Web security administrator can unblock a user whose access to the Web interface was denied (for example, because the user made 3 unsuccessful attempts at access). The Web security administrator must: 1. In the Web interface, access the Accounts page (**Configuration** > **System** > **Management** > **Web User Accounts**). 2. Identify in the list of users table that user whose access has been denied. 3. Change the status of that user from **Blocked** to **Valid** or **New**.

A.2.4   Power-Over-Ethernet Status Trap

⚠️ **Note:** This alarm is applicable only to Mediant 800B MSBR.

Table A-85: acPowerOverEthernetStatus

Trap	acPowerOverEthernetStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.80
Description	Sent when Power over Ethernet (PoE) for a specific port is disabled.
Default Severity	Indeterminate
Event Type	environmentalAlarm
Probable Cause	underlyingResourceUnavailable
Trap Text	"POE Port %d Was Not Powered Due To Power Management" where %d is the Ethernet port number
Condition	This trap is sent when insufficient power is available for a plugged-in PoE client in a PoE-enabled LAN port.
Trap Status	Trap is sent

A.2.5   Keep-Alive Trap

Table A-86: acKeepAlive

Trap	acKeepAlive
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Description	Part of the NAT traversal mechanism. If the STUN application in the device detects a NAT, this trap is sent on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the device.
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	Keep alive trap
Status Changes	
Condition	The STUN client is enabled and identified as a NAT device or doesn't locate the STUN server. The *ini* file contains the following line 'SendKeepAliveTrap=1'
Trap Status	Trap is sent
Note	Keep-alive is sent every 9/10 of the time defined in the parameter NatBindingDefaultTimeout.

A.2.6   Performance Monitoring Threshold-Crossing Trap

Table A-87: acPerformanceMonitoringThresholdCrossing

Trap	acPerformanceMonitoringThresholdCrossing
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Description	Sent every time the threshold of a Performance Monitored object ('Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') is crossed. The severity field is 'Indeterminate' when the crossing is above the threshold and 'Cleared' when it goes back under the threshold. The 'Source' varbind in the trap indicates the object for which the threshold is being crossed.
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	"Performance: Threshold trap was set", with source = name of performance counter which caused the trap
Status Changes	
Condition	A performance counter (for the attributes 'Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') has crossed the high threshold.
Trap Status	Indeterminate
Condition	A performance counter has returned to under the threshold
Trap Status	Cleared

A.2.7   HTTP Download Result Trap

Table A-88: acHTTPDownloadResult

Trap	acHTTPDownloadResult
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Description	Sent upon success or failure of the HTTP Download action.
Default Severity	Indeterminate
Event Type	processingErrorAlarm (3) for failures and other (0) for success.
Probable Cause	other (0)
Status Changes	
Condition	Successful HTTP download.
Trap Text	HTTP Download successful
Condition	Failed download.
Trap Text	HTTP download failed, a network error occurred.
Note	There are other possible textual messages describing NFS failures or success, FTP failure or success.

A.2.8   Dial Plan File Replaced Trap

> **Note:** This alarm is applicable only to Digital Series.

Table A-89: acDialPlanFileReplaced

Alarm	acDialPlanFileReplaced
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.45
Default Severity	Indeterminate
Event Type	Other (0)
Probable Cause	Other (0)
Status Change	
Condition	Successful dial plan file replacement
Trap Text	Dial plan file replacement complete.

A.2.9   Hitless Software Upgrade Status Trap

⚠️ **Note:** This alarm is applicable only to Mediant 3000.

Table A-90 acHitlessUpdateStatus

Alarm	acHitlessUpdateStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48
Default Severity	Indeterminate
Event Type	Other (0)
Probable Cause	Other (0)
Source	Automatic Update
Status Changes	
Condition	Successful SW upgrade
Trap Text	Hitless: SW upgrade ended successfully
Condition	Failed SW upgrade
Trap Text	Hitless fail: Waiting for module in slot <n> to burn new SW and reboot Timed out. (n – slot number).

A.2.10 Secure Shell (SSH) Connection Status Trap

Table A-91: acSSHConnectionStatus

Alarm	acSSHConnectionStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.77
Default Severity	indeterminate
Event Type	environmentalAlarm
Probable Cause	other
Alarm Text	"SSH logout from IP address <IP>, user <user>" "SSH successful login from IP address <IP>, user <user> at: <IP>:<port>" "SSH unsuccessful login attempt from IP address <IP>, user <user> at: <IP>:<port>. <reason>" "WEB: Unsuccessful login attempt from <IP> at <IP>:<port>. <reason>"
Status Changes	
Condition	SSH connection attempt
<text> Value	%s – remote IP %s – user name
Condition	SSH connection attempt – success of failure

A.2.11 SIP Proxy Connection Lost Trap

Table A-92: acProxyConnectionLost

Alarm	acProxyConnectionLost
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.94
Description	Sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up.
Source Varbind Text	System#0
Alarm Text	Proxy Set Alarm <text>
Event Type	communicationsAlarm
Probable Cause	▪ Network issue (connection fail due to network/routing failure). ▪ Proxy issue (proxy is down). ▪ AudioCodes device issue.

Alarm Severity

Severity	Condition	<text>	Corrective Action
Major	When connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table.	Proxy Set %d: Proxy not found. Use internal routing	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. 3. If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue. 4. Check that routing using the device's (internal) routing table is functioning correctly. 5. Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Major	When Proxy Set includes more than one proxy IP with redundancy and connection to one of them is lost.	Proxy Set %d: Proxy lost. looking for another proxy	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. 3. If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue. 4. Check if routing via the redundant proxy is operating correctly. If it is, then this could mean that it's not a network issue. 5. Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to proxy is available again	Proxy found. ip:<IP address>:<port #> Proxy Set ID %d	-

A.2.12 TLS Certificate Expiry Trap

Table A-93: acCertificateExpiryNotifiaction Trap

Alarm	acCertificateExpiryNotifiaction
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.92
Description	Sent before (in days) the expiration of the installed certificate credentials, which cannot be renewed automatically.
Source Varbind Text	System#0
Alarm Text	environmentalAlarm
Event Type	The certificate key expired (keyExpired)
Probable Cause	acCertificateExpiryNotifiaction

Alarm Severity			
Severity	**Condition**	**<text>**	**Corrective Action**
Intermediate	The certificate key is about to expire.	Either: ▪ The device certificate has expired %d days ago -OR- ▪ The device certificate will expire in %d days -OR- ▪ The device certificate will expire in less than 1 day %d – number of days	Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically). To replace certificates, refer to the section 'Replacing the Device's Certificate' in the *User's Manual*.

A.2.13 Cold Start Trap

Table A-94: coldStart

Trap Name	ColdStart
OID	1.3.6.1.6.3.1.1.5.1
MIB	SNMPv2-MIB
Note	This is a trap from the standard SNMP MIB.

A.2.14 Authentication Failure Trap

Table A-95: authenticationFailure

Trap Name	authenticationFailure
OID	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB

A.2.15 Board Initialization Completed Trap

Table A-96: acBoardEvBoardStarted

Trap Name	acBoardEvBoardStarted
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
Description	Sent after the device is successfully restored and initialized following reset.
MIB	AcBoard
Severity	cleared
Event Type	equipmentAlarm
Probable Cause	Other(0)
Alarm Text	Initialization Ended
Note	This is the AudioCodes Enterprise application cold start trap.

A.2.16 Configuration Change Trap

Table A-97: entConfigChange

Trap Name	entConfigChange
OID	1.3.6.1.2.1.4.7.2
MIB	ENTITY-MIB

A.2.17 Link Up Trap

Table A-98: linkUp

Trap Name	linkUp
OID	1.3.6.1.6.3.1.1.5.4
MIB	IF-MIB

A.2.18 Link Down Trap

Table A-99: linkDown

Trap Name	linkDown
OID	1.3.6.1.6.3.1.1.5.3
MIB	IF-MIB

A.2.19 D-Channel Status Trap

⚠️ **Note:** This alarm is applicable only to Digital Series.

Table A-100: AcDChannelStatus

Trap Name	acDChannelStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.37
Description	Non-alarm trap sent at the establishment, re-establishment or release of LAPD link with its peer connection occurs. The trap is sent with one of the following textual descriptions: ▪ D-channel synchronized ▪ D-channel not-synchronized
MIB	AcBoard
Severity	Minor
Event Type	communicationsAlarm
Probable Cause	communicationsProtocolError
Alarm Text	D-Channel Trap.
Source	Trunk <m> where m is the trunk number (starts from 0).
Status Changes	
Condition	D-Channel un-established.
Trap Status	Trap is sent with the severity of 'Minor'.
Condition	D-Channel established.
Trap Status	Trap is sent with the severity of 'Cleared'.

A.2.20 Enhanced BIT Status

Note: This alarm is not applicable to MSBR.

Table A-101: AcDChannelStatus

Alarm	acEnhancedBITStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.18
Description	Sent for the status of the BIT (Built In Test). The information in the trap contains blade hardware elements being tested and their status. The information is presented in the Additional Info fields.
Default Severity	Indeterminate
Source Varbind Text	BIT
Event Type	Other
Probable Cause	other (0)
Alarm Text	Notification on the board hardware elements being tested and their status.
Status Changes	
Additional Info-1	BIT Type: Offline, startup, perodic
Additional Info-2	BIT Results: BIT_RESULT_PASSED BIT_RESULT_FAILED
Additional Info-3	Buffer: Number of bit elements reports
Corrective Action	Not relevant

This page is intentionally left blank

B   Performance Monitoring Counters

This section lists the supported SNMP PM counters. These counters are polled by the SCOM at default interval of 15 minutes. In the SCOM, the PM data that is polled from the AudioCodes devices is represented in the SCOM by the following entities:

- **Rules:** Each counter is represented by a separate rule. For example, "Attempted Calls IP2Tel Counter Rule".
- **Threshold Monitors:** Each counter includes a corresponding pair of threshold monitors (High Threshold Monitor and a Low Threshold Monitor). For example, "Attempted Calls IP2Tel High Threshold Monitor" and "Attempted Calls IP2Tel Low Threshold Monitor"

The SCOM supports the following PM counter groups:

- IP-to-Tel Performance Monitors. See below.
- Tel-to-IP Performance Monitors. See Section B.2 on page 170.
- SBC Performance Monitors. See Section B.3 on page 171.

For more information, see Section 7.5 on page 82.

B.1   IP-to-Tel Performance Monitoring

The table below describes the SIP IP-to-Tel Performance Monitoring counters.

> **Note:** These PM counters are not applicable to Mediant 4000.

Table B-1: SIP IP-to-Tel Performance Monitoring

SCOM Name	Counter (MIB Name)	Description
Attempted Calls IP2Tel High Threshold Monitor	acPMSIPAttemptedCallsVal	Indicates the number of attempted calls for IP to Tel direction, during last interval.
Attempted Calls IP2Tel Low Threshold Monitor		
Established Calls IP2Tel High Threshold Monitor	acPMSIPEstablishedCallsVal	Indicates the number of established calls for IP to Tel direction, during last interval.
Established Calls IP2Tel Low Threshold Monitor		
Busy Calls IP2Tel High Threshold Monitor	acPMSIPBusyCallsVal	Indicates the number of calls that failed as a result of a busy line for IP to Tel direction, during last interval.
Busy Calls IP2Tel Low Threshold Monitor		
No Answer Calls IP2Tel High Threshold Monitor	acPMSIPNoAnswerCallsVal	Indicates the number of calls that weren't answered for IP to Tel direction, during last interval.
No Answer Calls IP2Tel Low Threshold Monitor		
Forwarded Calls IP2Tel High Threshold Monitor	acPMSIPForwardedCallsVal	Indicates the number of calls that were terminated due to a call forward for IP to Tel direction, during last interval.
Forwarded Calls IP2Tel Low Threshold Monitor		

SCOM Name	Counter (MIB Name)	Description
No Route Calls IP2Tel High Threshold Monitor	acPMSIPNoRouteCallsVal	Indicates the number of calls whose destinations weren't found for IP to Tel direction, during last interval.
No Route Calls IP2Tel Low Threshold Monitor		
No Match Calls IP2Tel High Threshold Monitor	acPMSIPNoMatchCallsVal	Indicates the number of calls that failed due to mismatched media server capabilities for IP to Tel direction, during last interval.
No Match Calls IP2Tel High Threshold Monitor		
No Resources Calls IP2Tel High Threshold Monitor	acPMSIPNoResourcesCallsVal	Indicates the number of calls that failed due to unavailable resources or a media server lock for IP to Tel direction, during last interval.
No Resources Calls IP2Tel Low Threshold Monitor		
SIPFailCalls IP2Tel High Threshold Monitor	acPMSIPFailCallsVal	This counter is incremented as a result of calls that fail due to reasons not covered by the other counters for IP to Tel direction, during last interval.
SIPFailCalls IP2Tel Low Threshold Monitor		

B.2   SIP Tel-to-IP Performance Monitoring

This table below describes the SIP Tel-to-IP PM counters supported by the SCOM.

Note: These PM counters are not applicable to Mediant 4000.

Table B-2: SIP Tel-to-IP Performance Monitoring

SCOM Name	Counter (MIB Name)	Description
Attempted Calls Tel2IP High Threshold Monitor	acPMSIPAttemptedCallsVal	Indicates the number of attempted calls for Tel to IP direction, during last interval.
Attempted Calls Tel2IP Low Threshold Monitor		
Established Calls Tel2IP High Threshold Monitor	acPMSIPEstablishedCallsVal	Indicates the number of established calls for Tel to IP direction, during last interval.
Established Calls Tel2IP Low Threshold Monitor		
Busy Calls Tel2IP High Threshold Monitor	acPMSIPBusyCallsVal	Indicates the number of calls that failed as a result of a busy line for Tel to IP direction, during last interval.
Busy Calls Tel2IP Low Threshold Monitor		
No Answer Calls Tel2IP High Threshold Monitor	acPMSIPNoAnswerCallsVal	Indicates the number of calls that weren't answered for Tel to IP direction, during last interval.
No Answer Calls Tel2IP Low Threshold Monitor		
Forwarded Calls Tel2IP High Threshold Monitor	acPMSIPForwardedCallsVal	Indicates the number of calls that were terminated due to a call forward for Tel to IP direction, during last interval.
Forwarded Calls Tel2IP Low Threshold Monitor		

SCOM Name	Counter (MIB Name)	Description
No Route Calls Tel2IP High Threshold Monitor	acPMSIPNoRouteCallsVal	Indicates the number of calls whose destinations weren't found for Tel to IP direction, during last interval.
No Route Calls Tel2IP Low Threshold Monitor		
No Match Calls High Threshold Monitor	acPMSIPNoMatchCallsVal	Indicates the number of calls that failed due to mismatched media server capabilities for Tel to IP direction, during last interval.
No Match Calls Low Threshold Monitor		
No ResourcesCalls Tel2IP High Threshold Monitor	acPMSIPNoResourcesCallsVal	Indicates the number of calls that failed due to unavailable resources or a media server lock for Tel to IP direction, during last interval.
No ResourcesCalls Tel2IP Low Threshold Monitor		
FailCalls Tel2IP High Threshold Monitor	acPMSIPFailCallsVal	This counter is incremented as a result of calls that fail due to reasons not covered by the other counters for Tel to IP direction, during last interval.
FailCalls Tel2IP Low Threshold Monitor		

B.3   SBC Performance Monitoring

This table below describes the SBC PM counters supported by the SCOM.

Note:

- This section applies to the E-SBC series only.
- Only the 'IP Group Invite Dialogs' counter is by default enabled.
- Other counters are by default not enabled in order to optimize SCOM performance. Selectively enable Performance Monitors.

Table B-3: SBC Call Admission Control Performance Monitoring

SCOM Name	Counter (MIB Name)	Description
SRD Dialogs High Threshold Monitor	acPMSIPSRDDialogsTable	Indicates all dialogs currently being handled by the SBC per SRD.
SRD Dialogs Low Threshold Monitor		
SRD Invite Dialogs High Threshold Monitor	acPMSIPSRDInviteDialogsTable	Indicates all calls (initiated by SIP:INVITE) currently being handled by the SBC per SRD.
SRD Invite Dialogs Low Threshold Monitor		
SRD Subscribe Dialogs High Threshold Monitor	acPMSIPSRDSubscribeDialogsTable	Indicates all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC per SRD.
SRD Subscribe Dialogs Low Threshold Monitor		
SRD Other Dialogs High Threshold Monitor	acPMSIPSRDOtherDialogsTable	Indicates dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per SRD.
SRD Other Dialogs Low Threshold Monitor		
Group Dialogs High Threshold Monitor	acPMSIPIPGroupDialogsTable	Indicates all dialogs currently being handled by the SBC per IP Group

SCOM Name	Counter (MIB Name)	Description
Group Dialogs Low Threshold Monitor		
Group Invite Dialogs High Threshold Monitor	acPMSIPIPGroupInviteDialogsTable	Indicates all calls (initiated by SIP:INVITE) currently being handled by the SBC per IP Group
Group Invite Dialogs Low Threshold Monitor		
Group Subscribe Dialogs High Threshold Monitor	acPMSIPIPGroupSubscribeDialogsTable	Indicates all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC per IP Group
Group Subscribe Dialogs Low Threshold Monitor		
Group Other Dialogs High Threshold Monitor	acPMSIPIPGroupOtherDialogsTable	Indicates all other dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per IP Group
Group Other Dialogs Low Threshold Monitor		
Group In Invite Dialogs High Threshold Monitor	acPMSIPIPGroupInInviteDialogsTable	Indicates the number of incoming calls (SIP INVITE) per IP Group
Group In Invite Dialogs Low Threshold Monitor		
Group Subscribe Dialogs High Threshold Monitor	acPMSIPIPGroupInSubscribeDialogsTable	Indicates the number of incoming SUBSCRIBE dialogs per IP Group
Group Subscribe Dialogs Low Threshold Monitor		
Group Out Invite Dialogs High Threshold Monitor	acPMSIPIPGroupOutInviteDialogsTable	Indicates the number of outgoing calls (SIP INVITE) per IP Group.
Group Out Invite Dialogs Low Threshold Monitor		
Group Out Subscribe Dialogs High Threshold Monitor	acPMSIPIPGroupOutSubscribeDialogsTable	Indicates the number of outgoing SUBSCRIBE dialogs per IP Group.
Group Out Subscribe Dialogs Low Threshold Monitor		
Invited Dialogs High Threshold Monitor	acPMSIPInvitedDialogsTable	Indicates the number of calls (SIP INVITE).
Invited Dialogs Low Threshold Monitor		
Subscribe Dialog High Threshold Monitor	acPMSIPSubscribeDialogTable	Indicates the number of SUBSCRIBE dialogs.
Subscribe Dialog Low Threshold Monitor		
SBC Registered Users High Threshold Monitor	acPMSBCRegisteredUsersTable	Indicates the number of registered users.
SBC Registered Users Low Threshold Monitor		

C   Optimizing SCOM Server Load-Example Scenario

This appendix describes how to balance the loading of the AudioCodes MP-related functional items (Discoveries, Monitors and Rules) running on the SCOM server. For each functional item launched, a script is run. Each script represents an equivalent CPU utilization percentage. This appendix presents a scenario with models of gateways with different numbers of trunks. The scenario shows the affect on the CPU utilization both before and after load balancing is performed. Load balancing is achieved by overriding the polling frequency and Sync time for each functional item (see Chapter 8 on page 91).

C.1   Default Loading

The following describes the default loading for the different monitored AudioCodes gateway models:

- Six gateways with six modules where each module includes one trunk, one Fan Tray module and one power supply module– type **A**.

- Six gateways with six modules where each module includes four trunks, one Fan Tray module and one power supply module – type **B**.

- Six gateways with six modules where each module includes 16 trunks, one Fan Tray module and one power supply module – type **C**.

The table below shows the maximum number of scripts that are run for each of the SCOM elements for the different AudioCodes MP-related objects.

Table C-1: Management Pack Objects and Number of Scripts Run

Management Pack Object	Discoveries	Monitors	Performance
Gateway	One discovery with 1 script.	80 monitors with 52 scripts.	26 performance counters with 26 scripts.
Module	three discoveries with two scripts.	two monitors with no scripts (Fan Tray has one monitor with no scripts).	-
Trunk	two discoveries with two scripts.	eight monitors with no scripts.	Three rules with three scripts.

C.2   Script Load Estimation

The tables below describe the different script load estimations for the different models that are described in Section C.1 on page 173.

C.2.1   Type A Gateways

The following table describes the script load estimations for Type A Gateway models.

Table C-2: Type A Gateways

Management Pack Object	Gateway Scripts	Module Scripts	Trunk Scripts	Total
Discovery	1	16	12	29
Monitors	52	0	0	52
Performance Counters	26	0	18	54
Total				**143**

C.2.2   Type B Gateways

The following table describes the script load estimations for Type B Gateway models.

Table C-3: Type B Gateways

Management Pack Object	Gateway Scripts	Module Scripts	Trunk Scripts	Total
Discovery	1	16	48	65
Monitors	52	0	0	52
Performance Counters	26	0	72	98
Total				**215**

C.2.3   Type C Gateways

The following table describes the script load estimations for Type C Gateway models.

Table C-4: Type C Gateways

Management Pack Object	Gateway Scripts	Module Scripts	Trunk Scripts	Total
Discovery	1	16	192	209
Monitors	52	0	0	52
Performance Counters	26	0	288	316
Total				**577**

C.3 Load Analysis

The figure below shows a comparison of the number of scripts that are run (Y-axis) for the different model types (described in Section C.1 on page 173).

The key observation from the graph is that an increasing number of trunks significantly affects the number of loaded scripts.

Figure C-1: Load Analysis
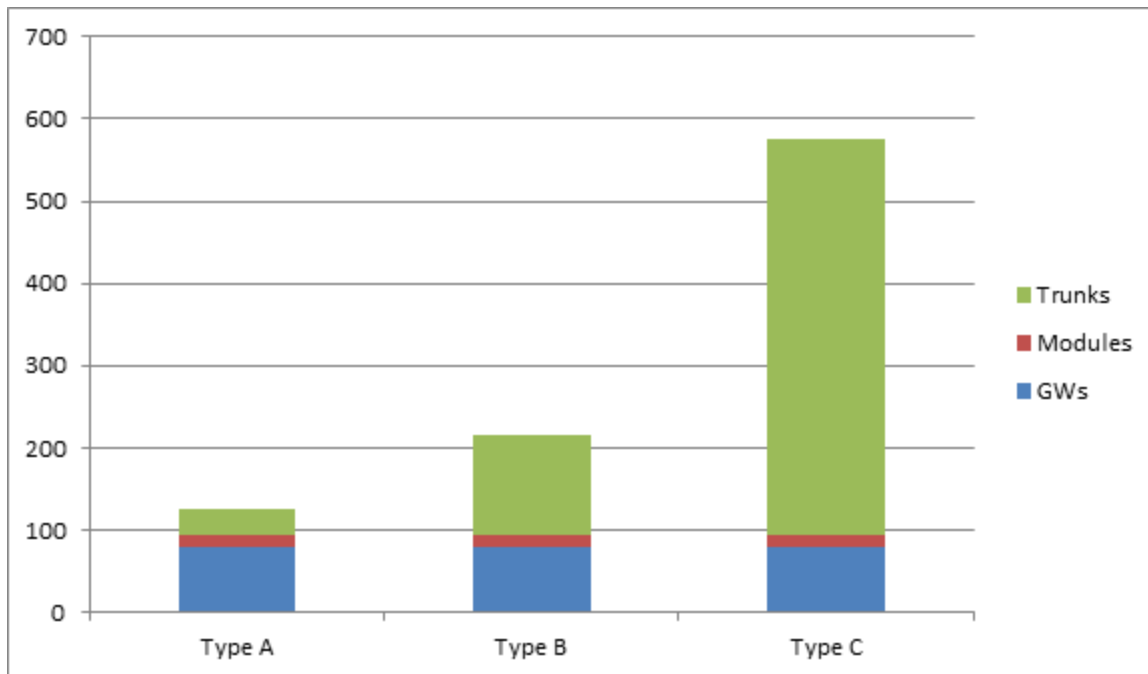
The following summarizes the specific limitations and restrictions on possible frequencies for different kinds of processes:

■ Performance counters rules (see Section 7.6 on page 83) have to be launched precisely every 15 minutes due to their dependency on SNMP counters on devices. For example, Tel2IP Calls.

■ High and Low Threshold Monitors must also be launched precisely every 15 minutes due to their dependency on SNMP counters on devices. For example, Tel2IP Calls High Threshold Monitor and Tel2IP Calls Low Threshold Monitor.

■ Trunk monitor rules 'Audiocodes Digital Trunk Available Channels Counter Rule' and 'Audiocodes Digital Trunk Blocked Channels' Counter Rule and the corresponding threshold monitors 'Audiocodes Blocked Channels High Threshold Monitor' and 'Audiocodes Free Channels Low Threshold Monitor' by default are launched once per minute. This is due to the relatively large number of trunk objects and their dynamic states. For more information, see Section 8.1.4 on page 102.

■ Discoveries for Gateways and Modules can be launched at very low polling frequencies because the probability of any parameter changing is low to impossible. At the same time, the trunks discoveries should be launched much more frequently since the probability of any parameter modification is relatively higher.

C.3.1 Script Execution Without Load Balancing

The figure below shows the number of scripts executed (Y-axis) over a 60 second time period (X-axis) without load balancing.

The key observation from the figure is that aproximately once every 15 minutes, there is a peak in the script execution due to the running of the counter rules and threshold monitor scripts.

Figure C-2: Non-Balanced Script Execution
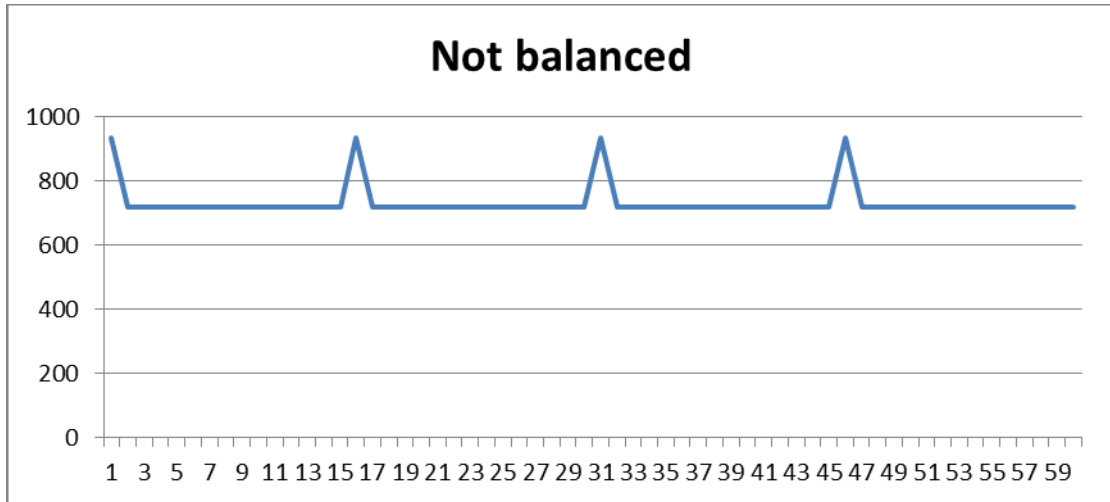
C.3.2 Script Execution with Load Balancing

For the implementation of load balancing, it is recommended to make the following overrides:

■ Since gateways and modules do not need to be frequently discovered, it is recommended to set the launching of these processes to once per 60 minutes.

■ For the discoveries of trunks, it is recommended to set their launching to once every three minutes (instead of the one minute default).

■ All performance measurements (counter rules) and gateway threshold monitors should still be launched once per 15 minutes.

■ Performance measurements of trunks (see Section 8.1.4 on page 102) are not dependent on PM counters of devices; and in the SCOM indicate which trunk channels are in-service and which trunk channels are out-of-service. Therefore, we recommend to reduce the polling frequency for running these scripts from the default one minute to once every three minutes.

The overidding of Discoveries, Monitors and Rules are described in Section 8 on page 91.

C.3.2.1 Script Execution Without Overriding Sync Time

The figure below shows the number of scripts executed (Y-axis) run over a one minute time axis (X-axis) following the modifications described above (without overidding the Sync time values).

The key observation of the figure shows an improvement; however, there are still a lot of loading peaks.

Figure C-3: Frequency Without Syncronization
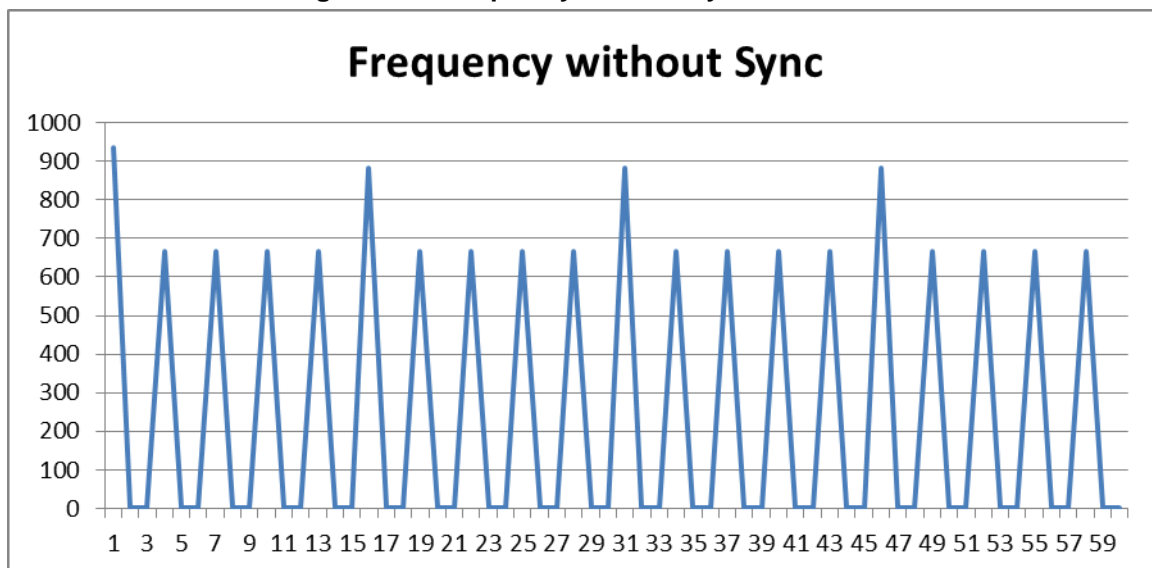
C.3.2.2 Script Execution when Overriding Sync Time

This section describes how to modify the Synchronization time. Highest peaks are defined as peaks when gateway counters and monitors are executed. It is possible to modify them so every counter and monitor will have its own designated minute of synchronization where the starting minute will be the second minute because discoveries of gateways and modules will be executed at the first minute of an hour.

The table below shows an example of setting a sequence of different Sync times for the different counters.

Table C-5: Sync Time Sequence

Counter	Sync Time
AttemptedCalls	00:01
BusyCalls	00:02
EstablishedCalls	00:03
FailCalls	00:04
ForwardedCalls	00:05
IPGroupDialogs	00:06
IPGroupInviteDialogs	00:07
NoAnswerCalls	00:08
NoMatchCalls	00:09
NoResourcesCalls	00:10
NoRouteCalls	00:11
SRDDialogs	00:12
SRDOtherDialogs	00:13
SRDSubscribeDialogs	00:14

In addition, note the following:

■ The corresponding threshold monitors of the above-mentioned counters will have the same minute of synchronization.

■ There are 252 discoveries of trunks with scripts that represent 35% of all remaining scripts. Let's set their synchronization minute to 00:01.

■ At the same time, there are 288 performance measuring rules of gateways of type C that represent 40% of all remaining counters. Let's set their synchronization time to 00:02.

The figure below shows the results following the above modifications.

The key observation of the figure is that peaks are much lower and smoother over the time axis, which consequently implies lower CPU utilization.
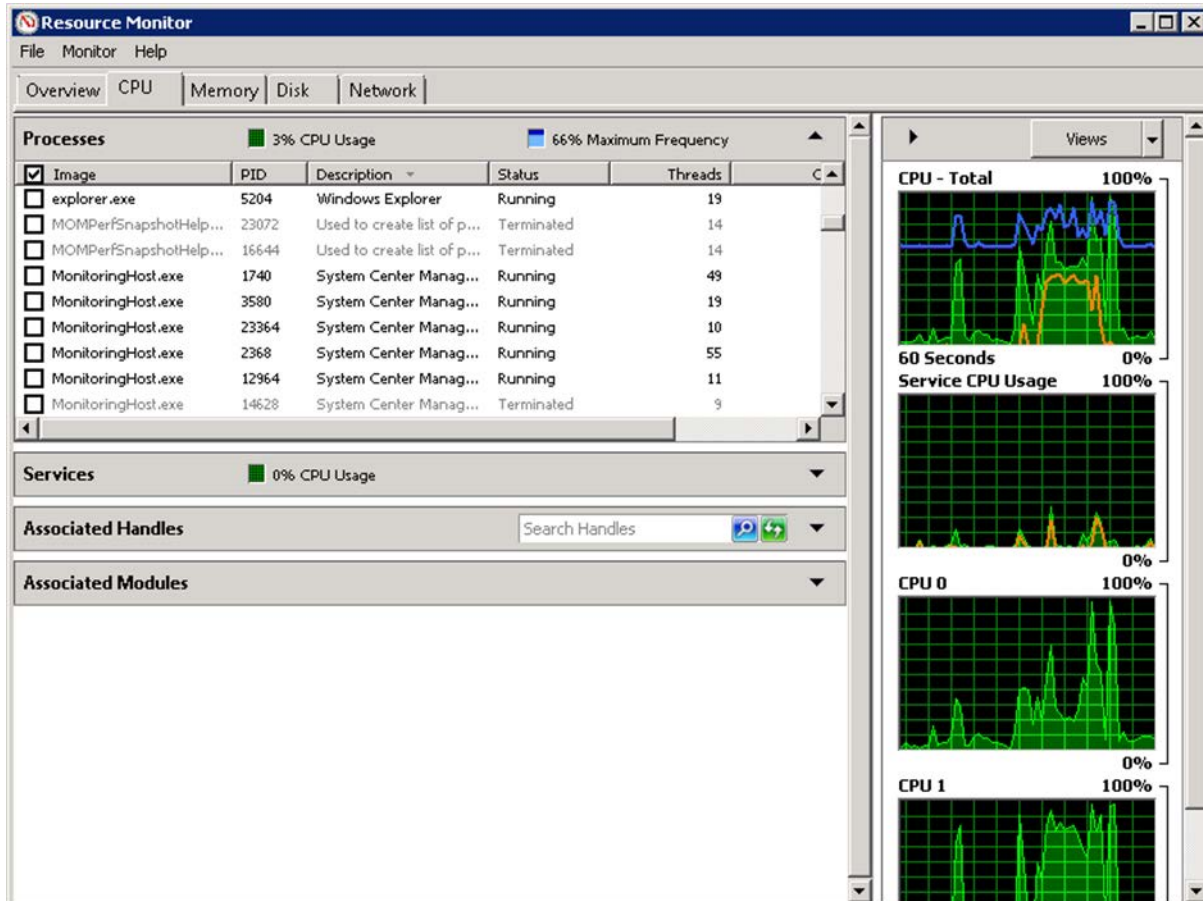
Figure C-4: Frequency and Sync
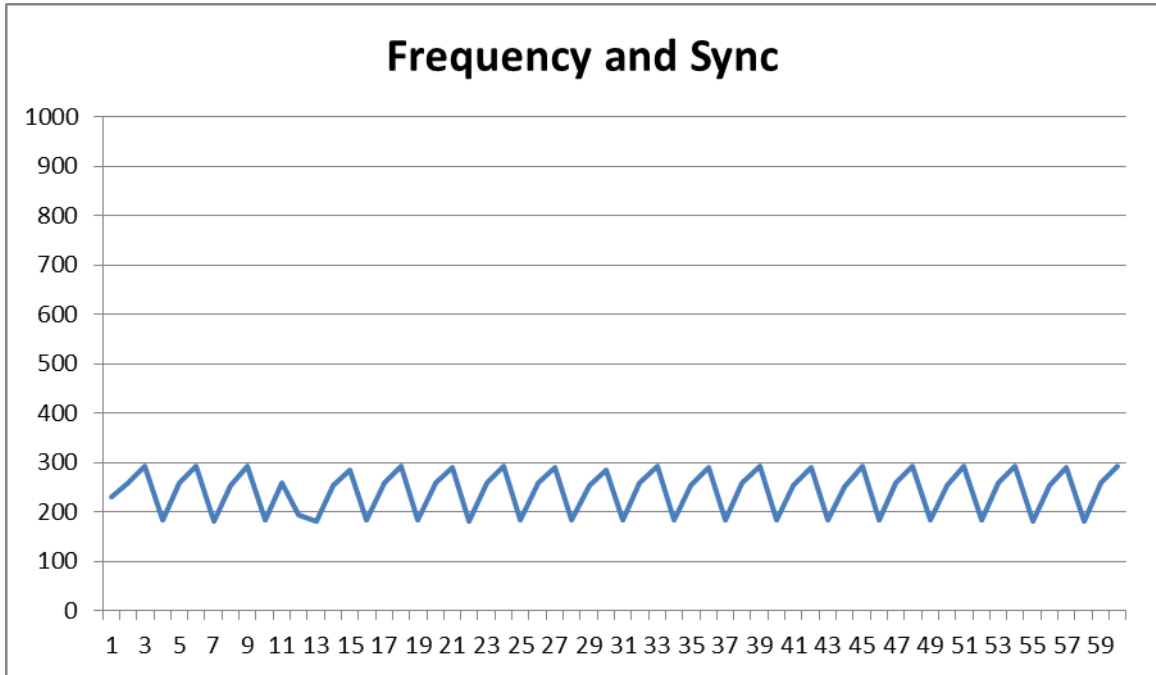
C.3.3   Resource Monitor

You can monitor the running SCOM processes in the SCOM Server Resource Monitor as shown in the figure below.

You can change the service name of the SCOM ?

➢   **To open the Resource Monitor on the Windows Server:**

■   Press Cntrl+ Shift + Esc.

Figure C-5: SCOM Server Resource Monitor

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

Document #: LTRT-30808