Session Border Controllers

Microsoft® System Center 2012 Operations Manager (SCOM)

VoIP Media Gateways

User's Guide

AudioCodes SCOM Management Pack

Microsoft Partner Gold Unified Communications

Microsoft® Lync™

AudioCodes

Version 2.0

February 2013

Document # LTRT-30802

Table of Contents

List of Figures

List of Tables

Notice

This document describes the installation and use of the AudioCodes SCOM Management Pack in the Microsoft SCOM 2012 Operations Manager environment.

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. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at http://www.audiocodes.com/downloads.

Date Published: February-3-2013

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

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 service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

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 http://www.audiocodes.com/downloads. Your valuable feedback is highly appreciated.

Abbreviations and Terminology

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

Related Documentation

Manual Name
Mediant 600 and 1000 SIP User's Manual
Mediant 800 Gateway and E-SBC User's Manual
Mediant 800 MSBG SIP User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBG SIP User's Manual
Mediant 2000 User's Manual
Mediant 3000 User's Manual
Mediant 4000 E-SBC User's Manual
MediaPack User's Manual

1 Introduction

This document describes the installation and use of the AudioCodes SCOM Management Pack that 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. Through numerous views that show state, health and performance information, as well as alerts generated according to some availability, performance, configuration or 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. The following AudioCodes gateways are monitored by the SCOM:

- acMediant1000
- acMediant1000-MSBG
- acTrunkPack-MEDIANT2000
- acMediant3000
- acTrunkPack-6310-T3
- acMediant3000-T3
- acMediant-4000
- acMediant800-MSBG
- acMediant800-ESBC
- acMediaPack-124
- acMediaPack-118
- acMediaPack114
- acMediaPack112

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

Reader's Notes

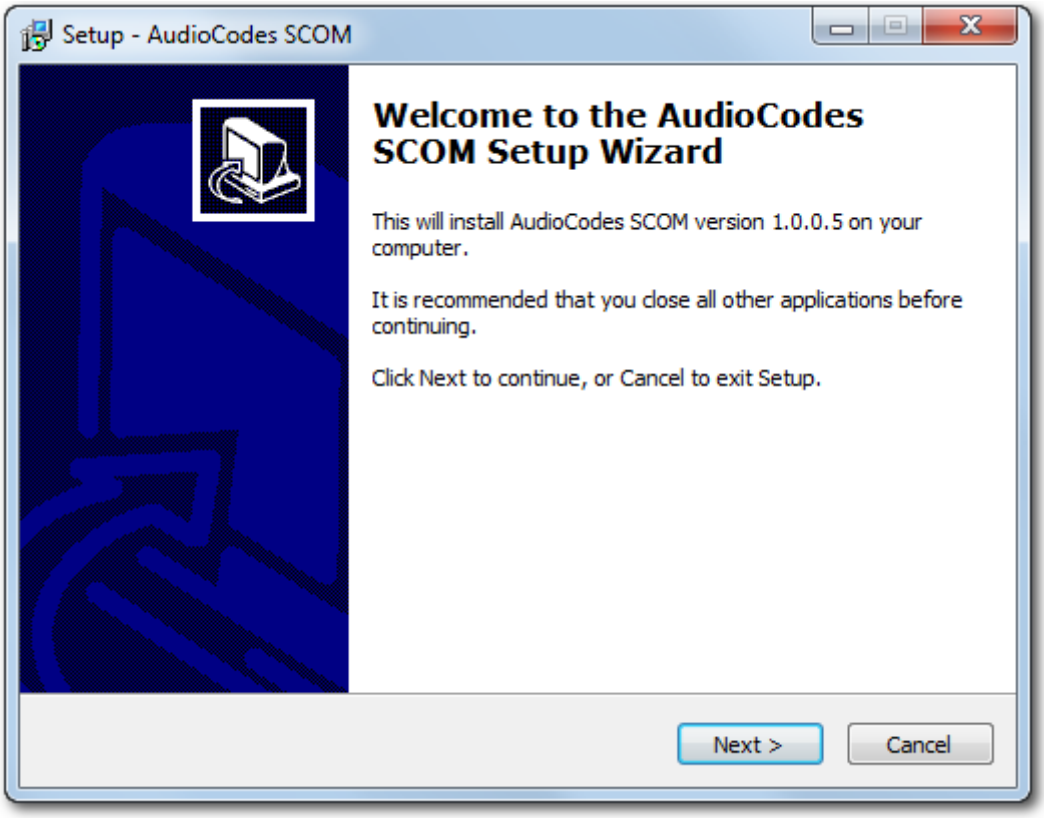
2 Setting up the AudioCodes SCOM Management Pack on your PC

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

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

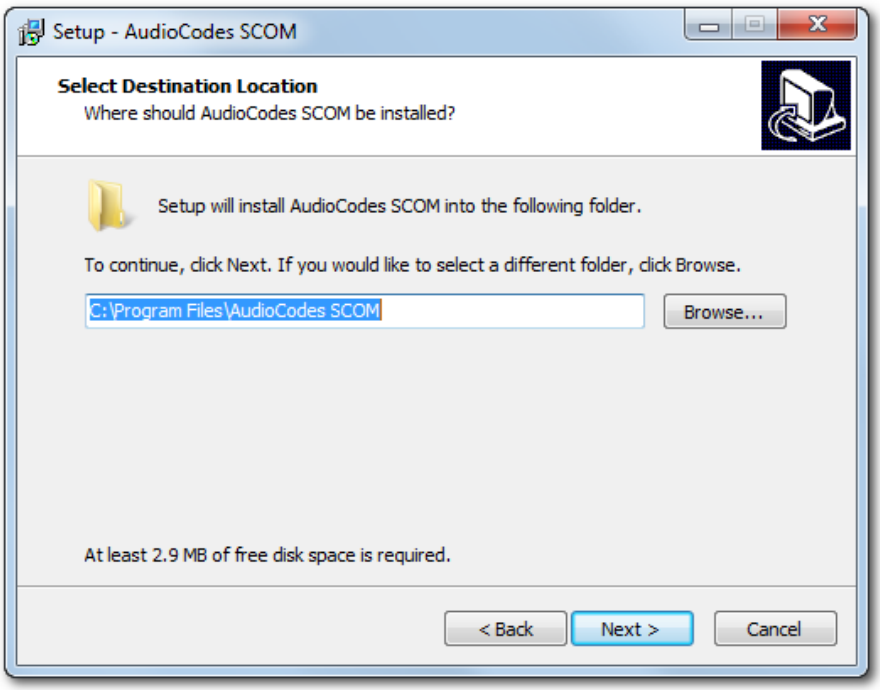
1. Run the **AudioCodesSCOM.exe** file; the AudioCodes SCOM Setup wizard is displayed:

Figure 2-1: AudioCodes Setup Wizard Welcome Screen



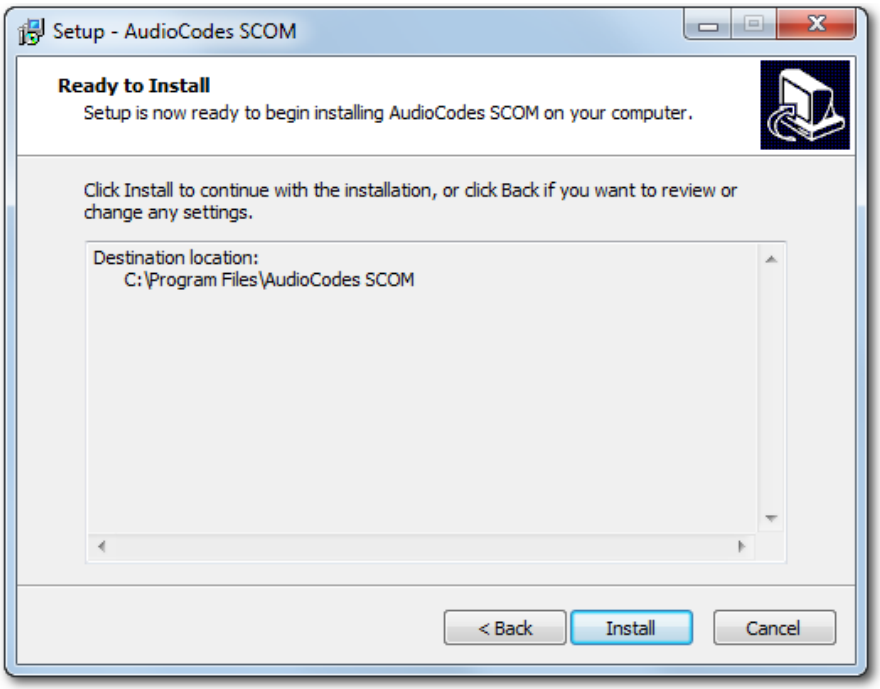
2. Click **Next**; the Select Destination Location screen is displayed:

Figure 2-2: Select Destination Location



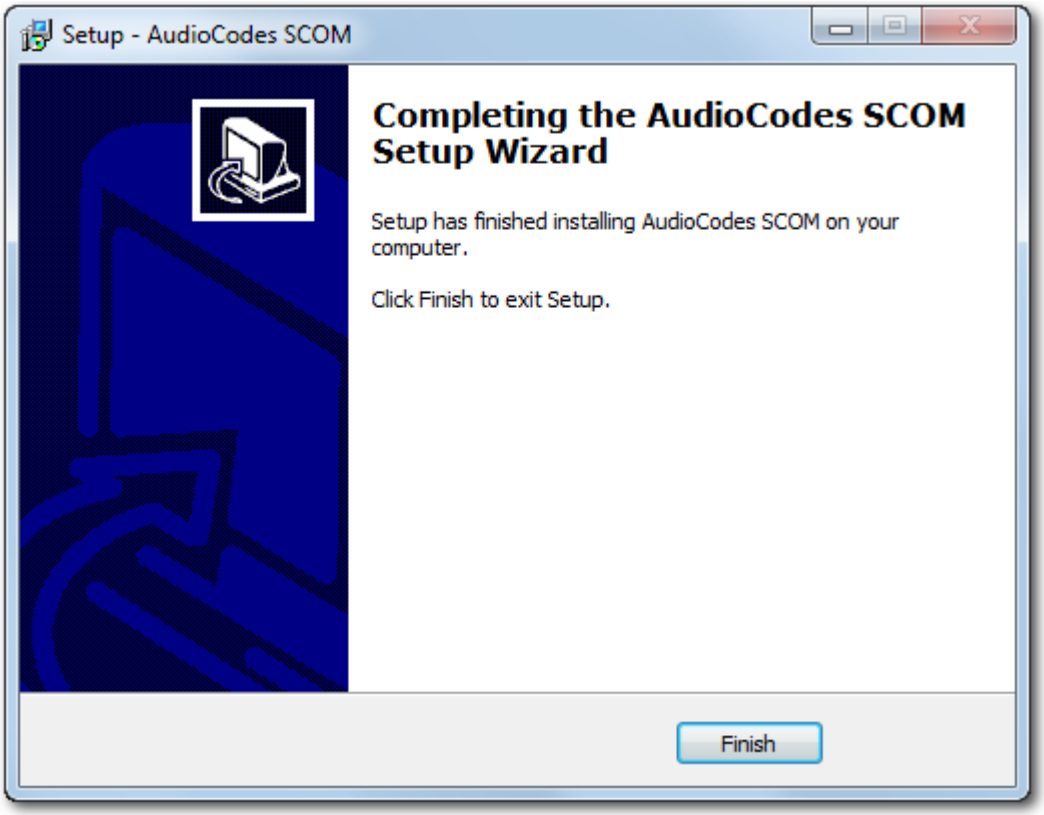
3. Choose the folder for installing the AudioCodes Management Pack, and then click **Next**; the Ready to Install screen is displayed:

Figure 2-3: Ready to Install



4. Verify the installation settings and then click **Install**; the Completion screen is displayed:

Figure 2-4: AudioCodes Setup Wizard Complete



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

Reader's Notes

3 Importing Management Pack

This section describes how to import the AudioCodes Management Pack into the SCOM 2012 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 3-1: Administration Pane

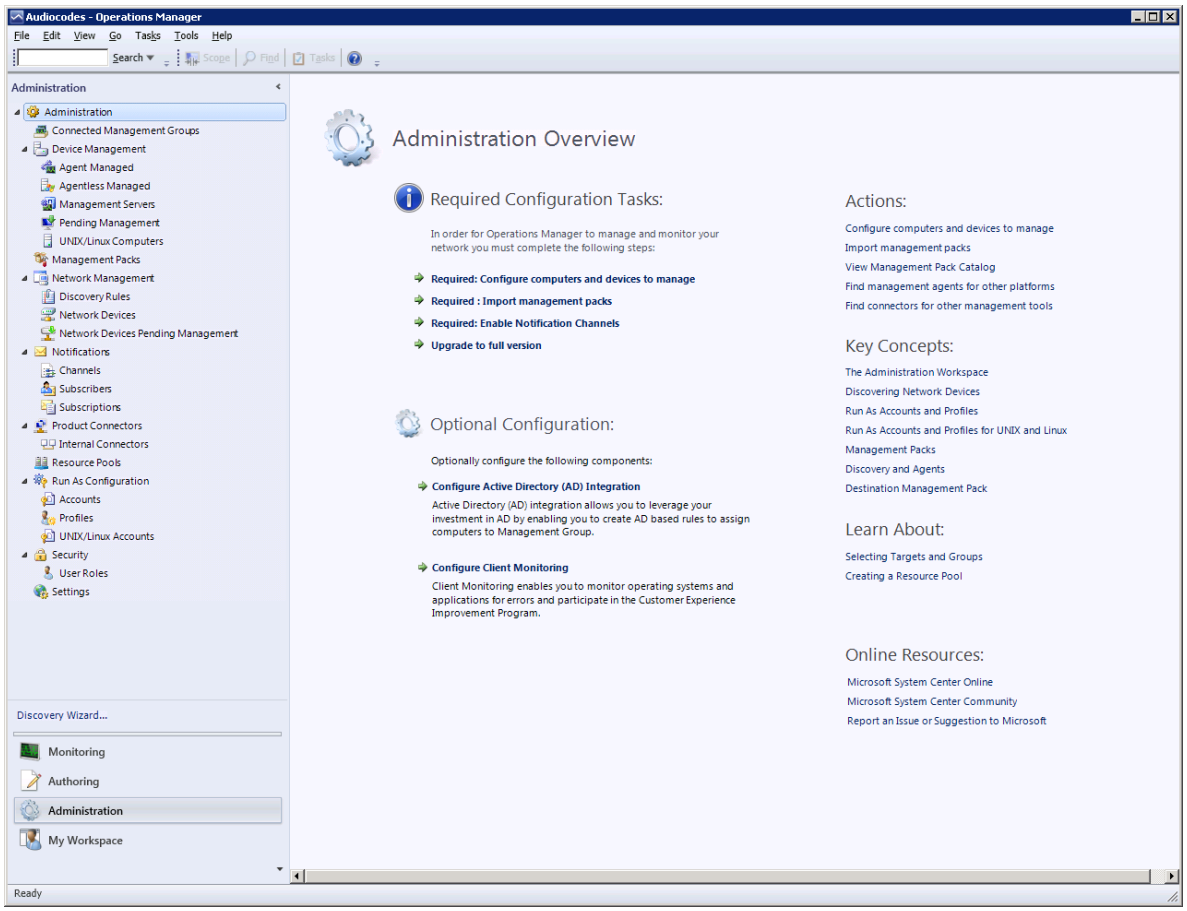
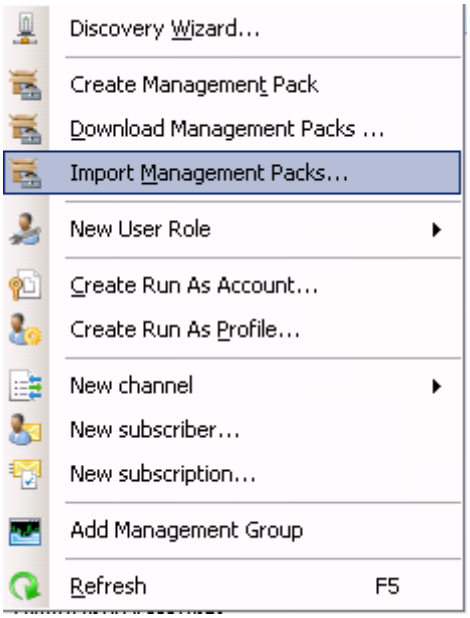
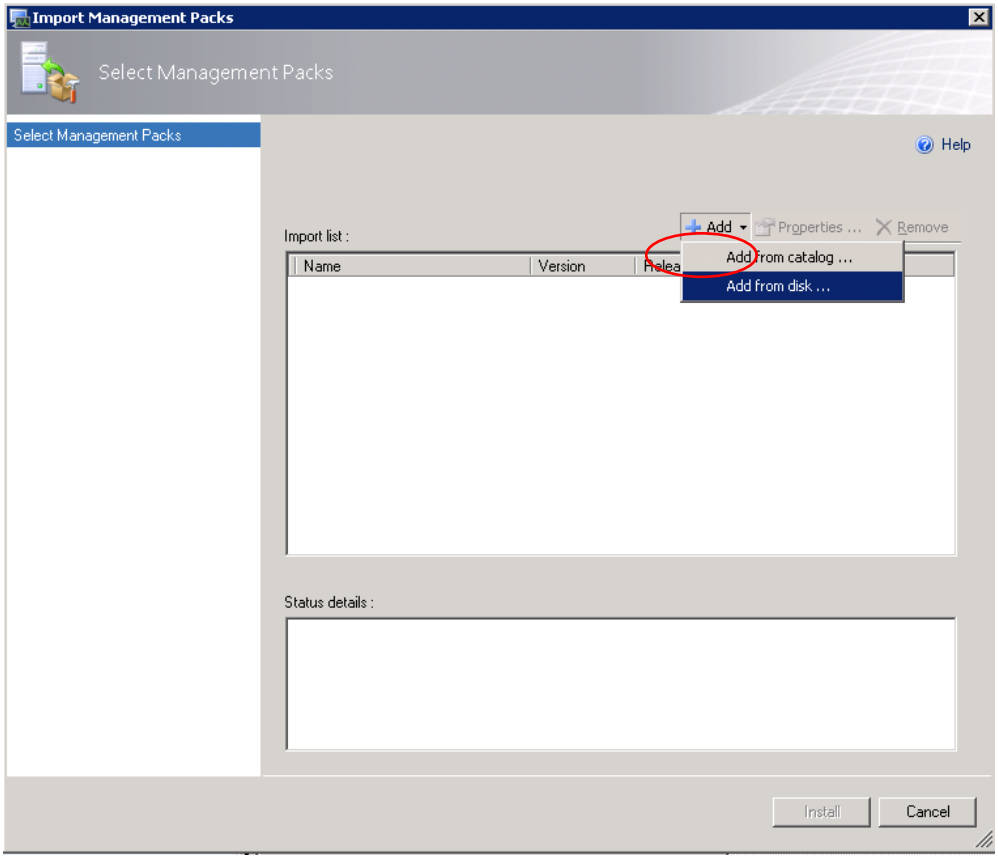


Figure 3-2: Import Management Packs Option



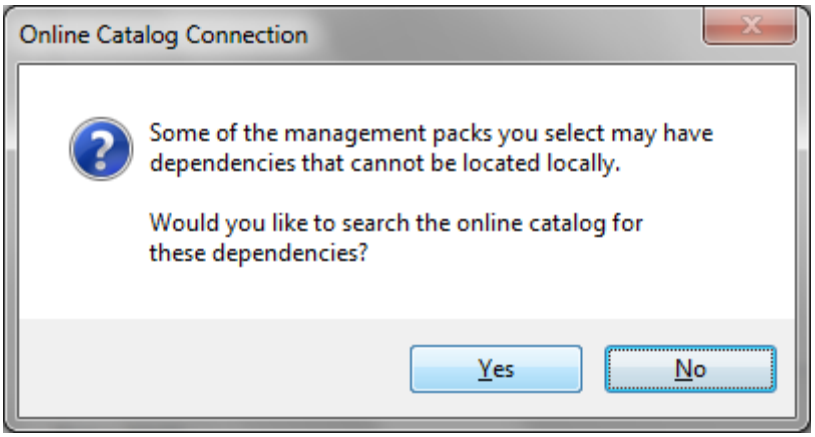
3. In the Navigation tree, right-click **Management Packs**, and then from the pop-up menu, choose **Import Management Packs**; the Select Management Packs window is displayed:

Figure 3-3: Select Management Packs



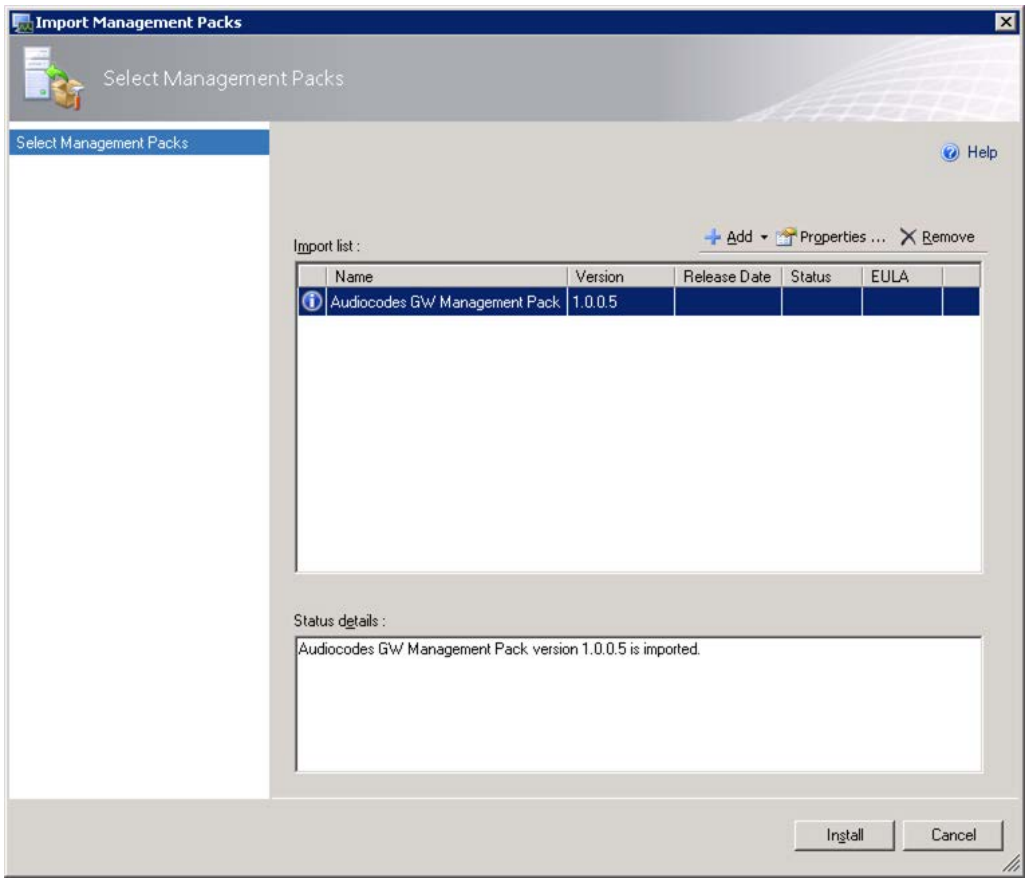
4. Click the **Add** button, and then choose **Add from disk**; the following dialog is displayed:

Figure 3-4: Online Catalog Connection



5. Click **No** to decline choosing Management Pack from a Catalog.
6. Locate the saved AudioCodes Management Pack on you disk (the location that you chose in Section 2 on page 13) and then click the **Open** button; the Select Management Packs window is displayed:

Figure 3-5: Select AudioCodes Management Packs



7. Select the AudioCodes GW Management Pack, and then click the **Install** button.

Reader's Notes

4 Discovering Gateway Device

When Management Packs are installed you have to discover your AudioCodes gateways as Network Elements to enable SCOM to make a full discovery.

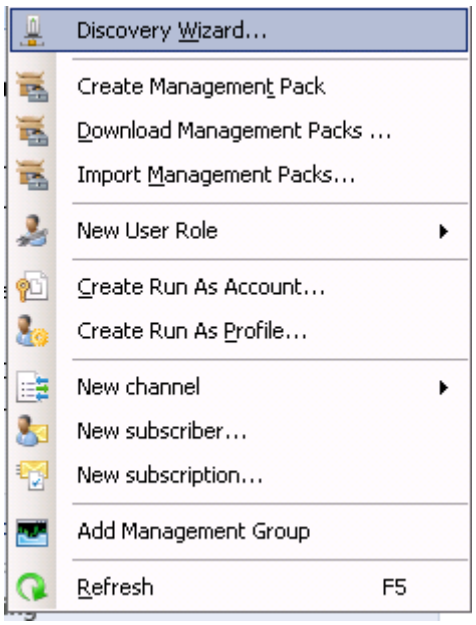
4.1 Gateway Discovery as a Network Device

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

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

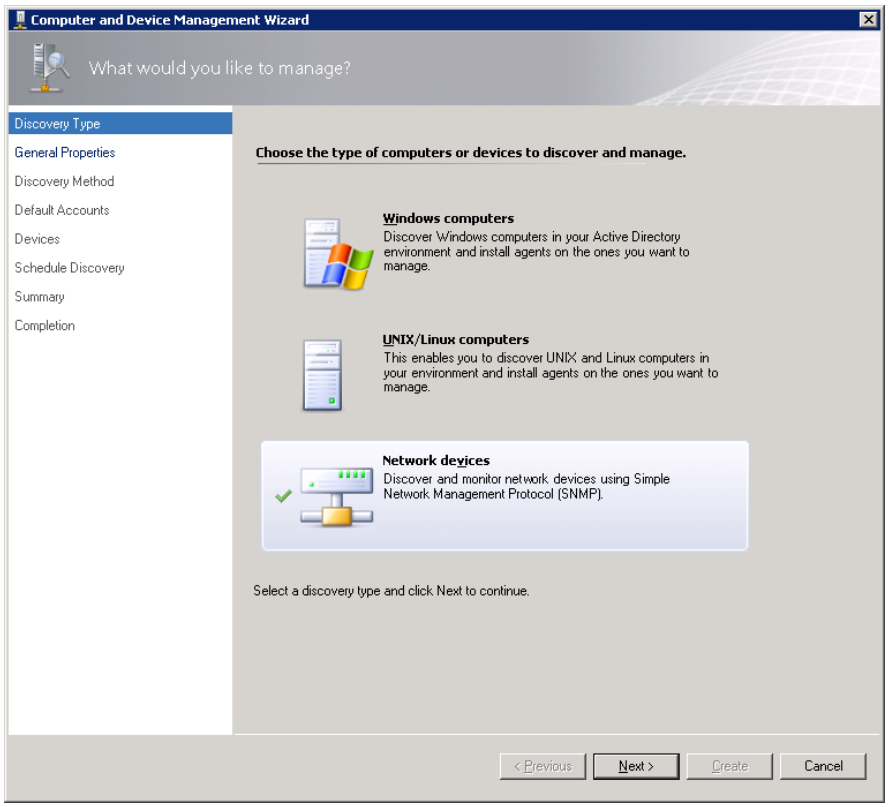
1. In the **Administration** pane, right-click **Network Devices** ,and then in the pop-up menu, choose **Discovery Wizard**:

Figure 4-1: Open Discovery Wizard



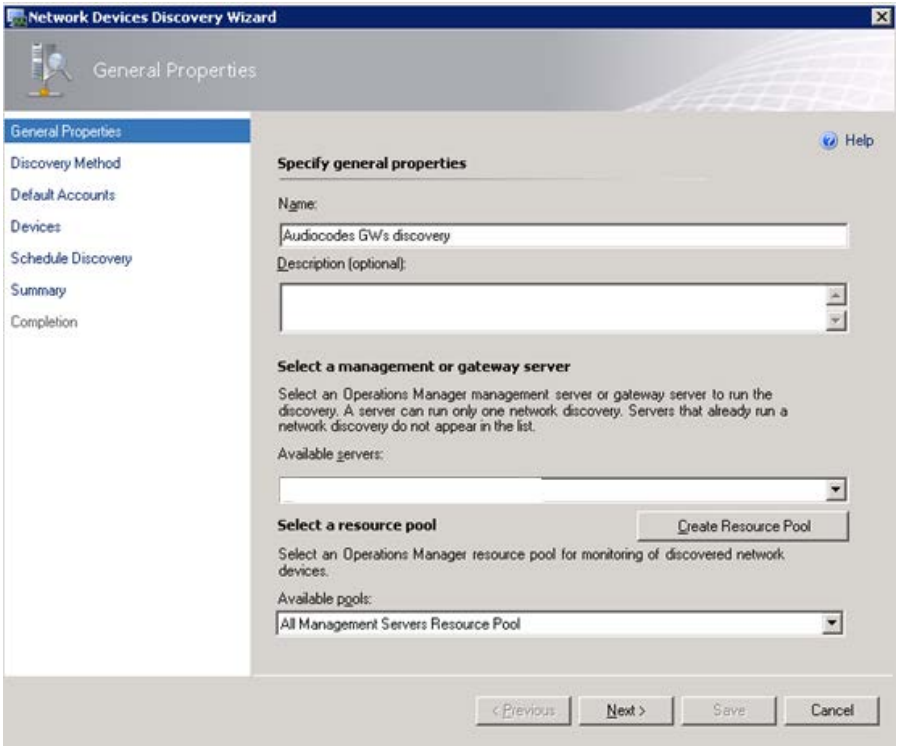
The Computer and Device Management Wizard is displayed:

Figure 4-2: Computer and Device Management Wizard



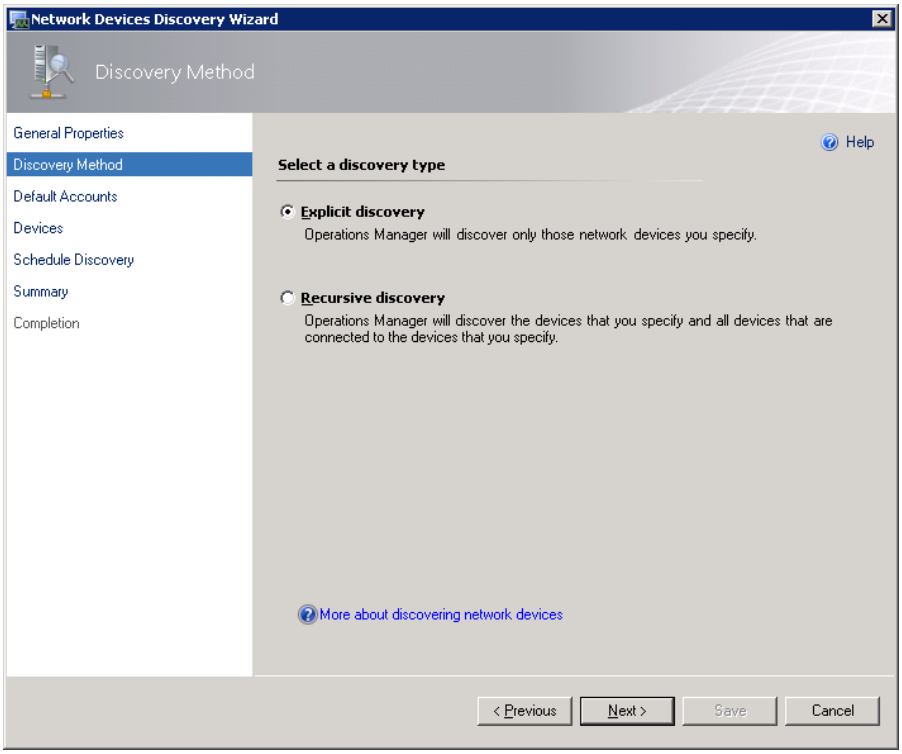
2. Select the **Network devices** option, and then click **Next**; the General Properties window is displayed:

Figure 4-3: General Properties



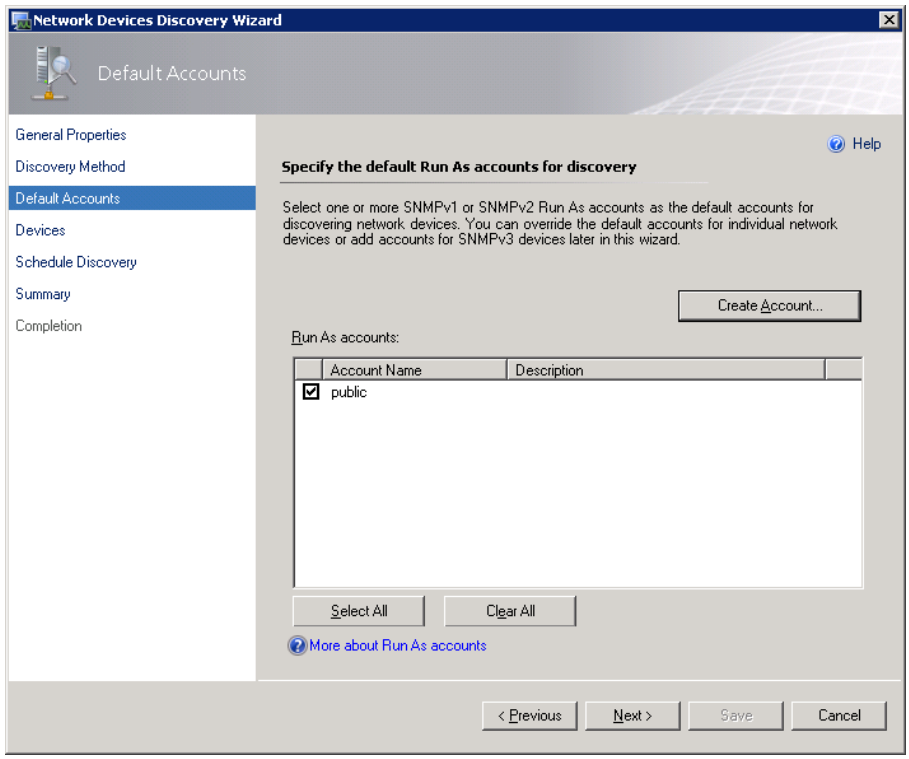
3. Enter the appropriate values, and then click **Next**; the Discovery Method window is displayed:

Figure 4-4: Discovery Method



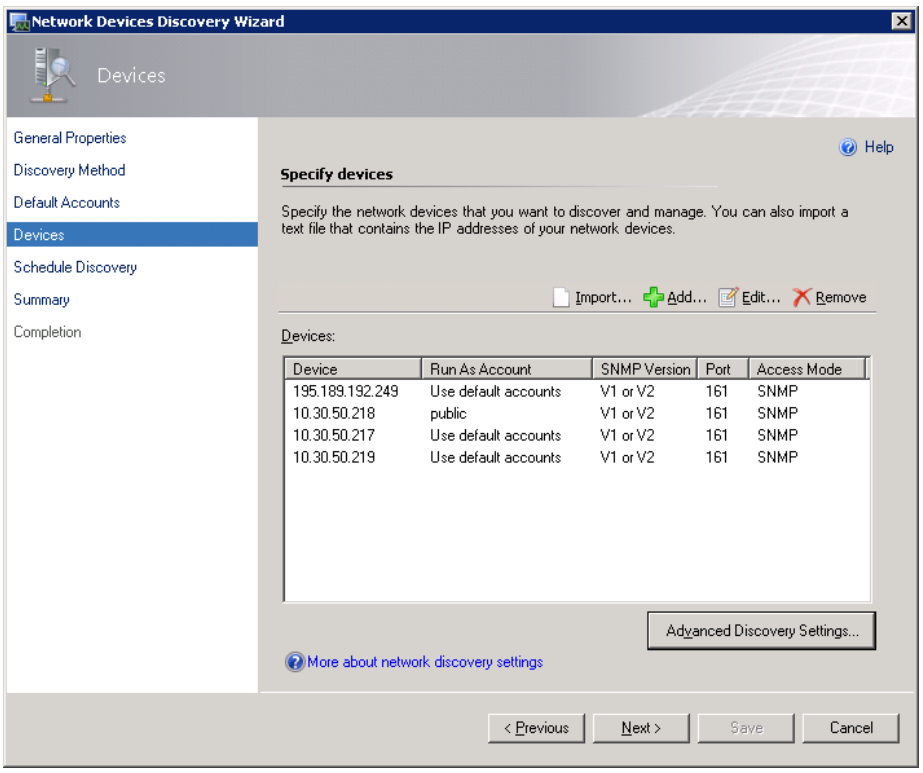
4. Select the appropriate actions, and then click **Next**; the Defaults Accounts page is displayed:

Figure 4-5: Default Accounts



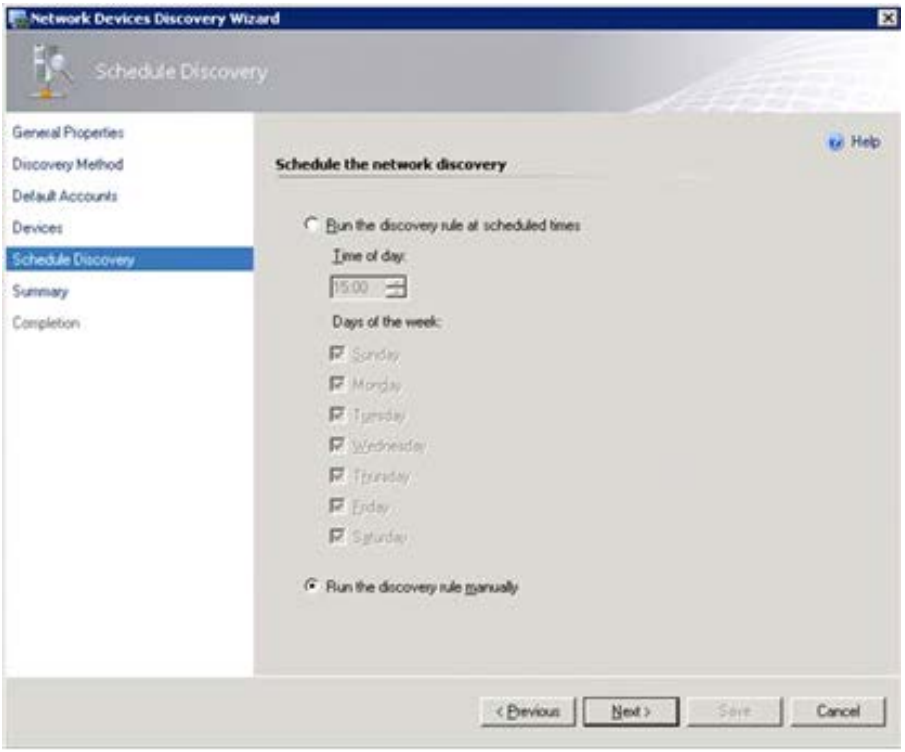
5. Choose the default SNMP SCOM account (this account is always-'public') or create new accounts using the same community string that is configured on the Network Devices that you wish to discover ,and then click **Next**; the Devices page is displayed:

Figure 4-6: Devices



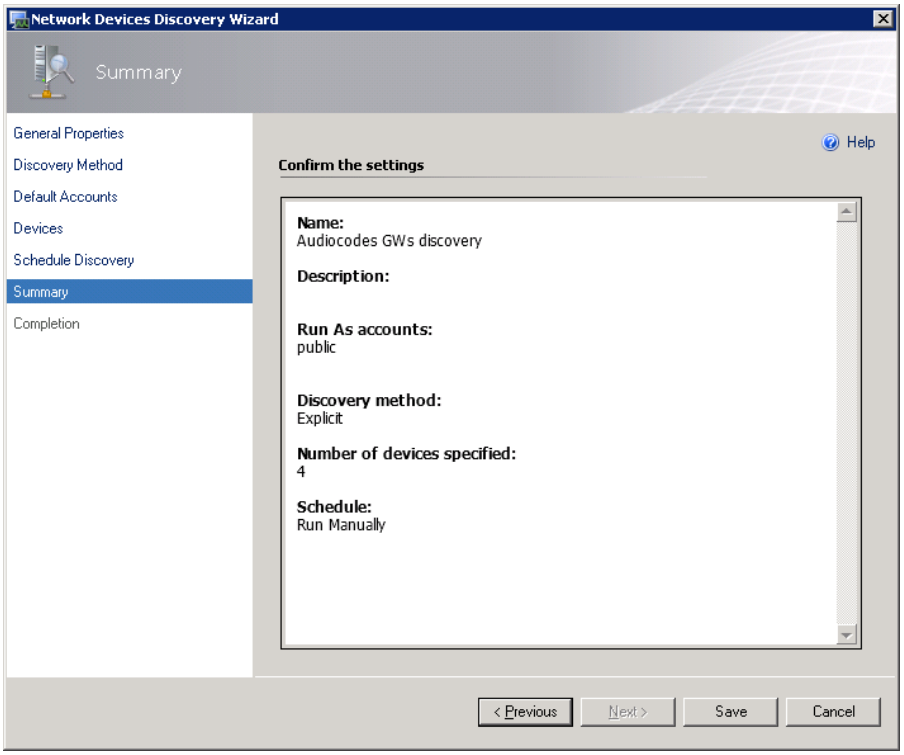
6. Add the IP addresses of devices to be discovered, and then click **Next**; the Schedule Discovery screen is displayed:

Figure 4-7: Schedule Discovery



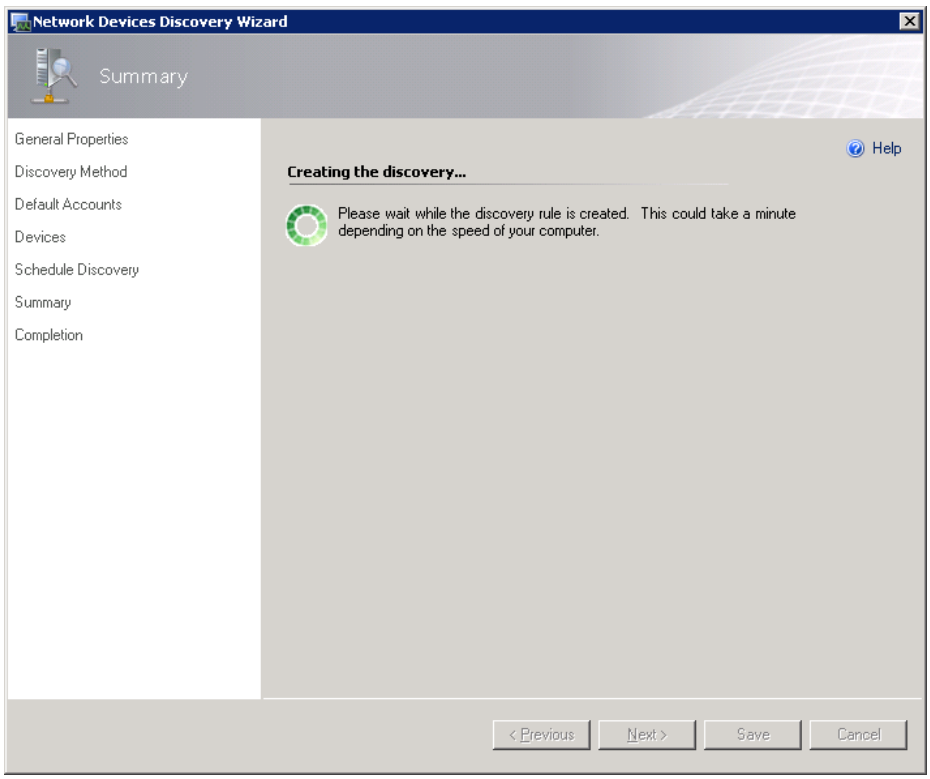
7. Select the **Run the discovery rule manually** option, and then click **Next**; the Summary page is displayed:

Figure 4-8: Summary



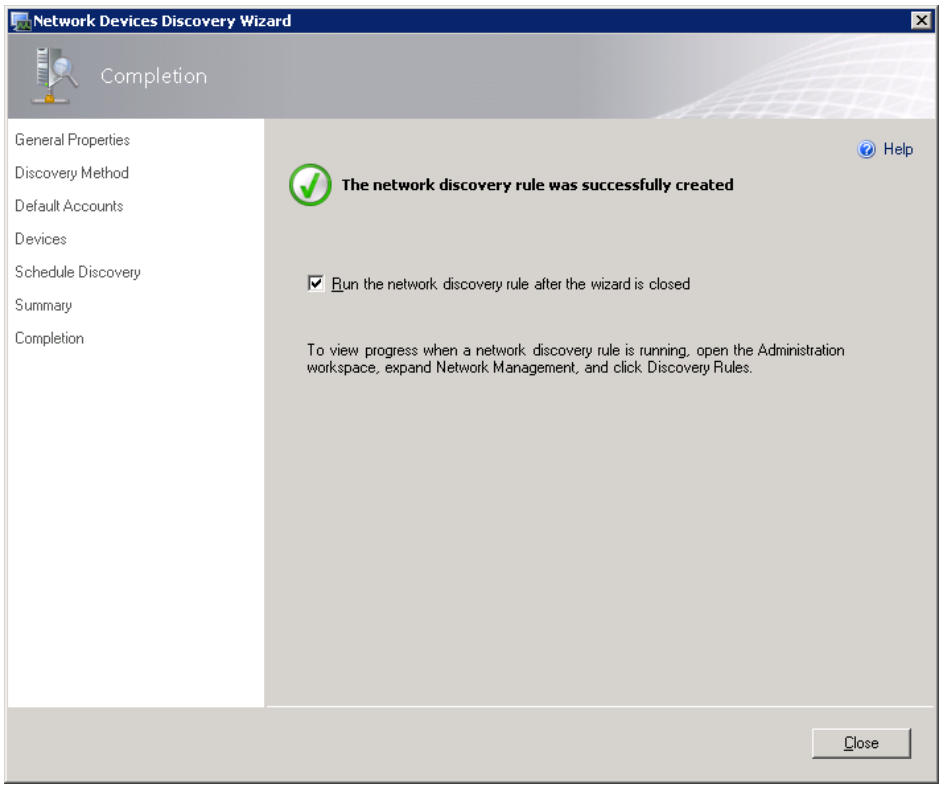
8. Review the settings, and then click **Save**.
9. Wait for the discovery rule to complete saving.

Figure 4-9: Discovery Saving Progress



10. Click the **Close** button; a confirmation window is displayed:

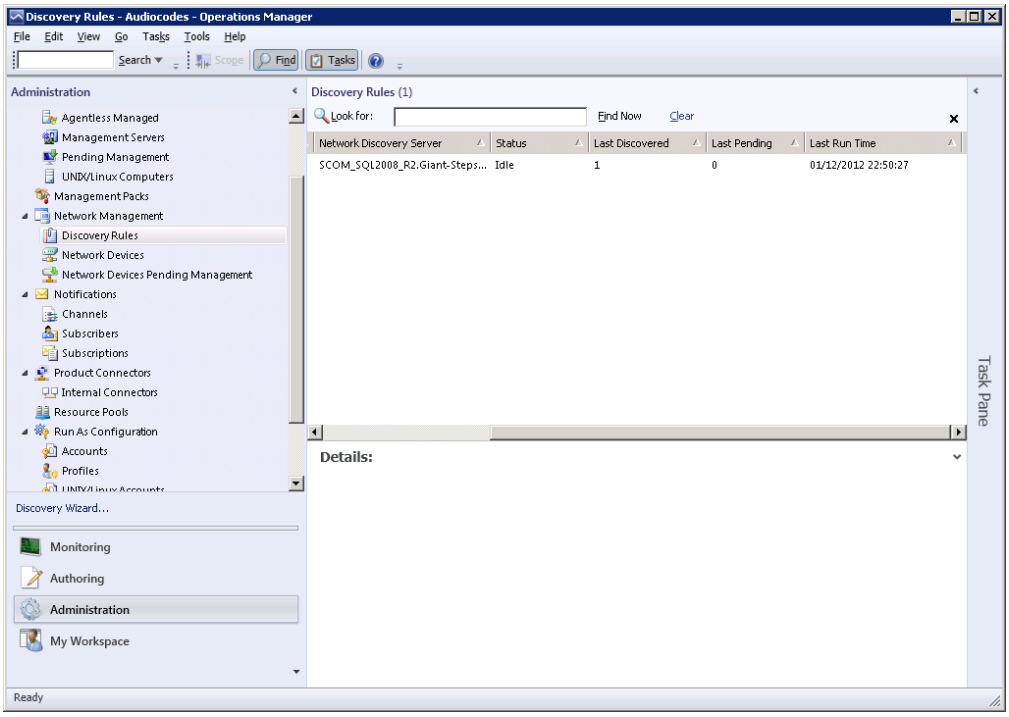
Figure 4-10: Network Discovery Rule Confirmation



The newly created rule should appear in the 'Discovery Rules' pane. When the rule has been successfully created, it should have the status 'Idle'.

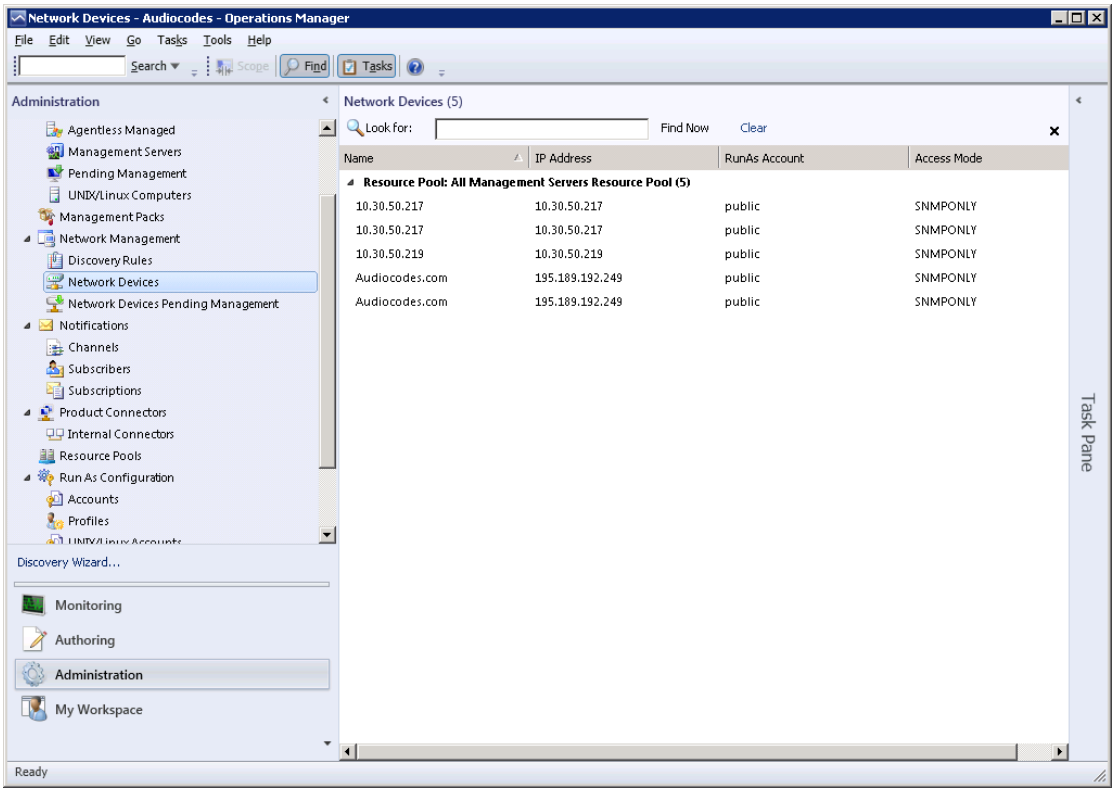
Wait for 5-8 minutes to allow the SCOM to make a full discovery.

Figure 4-11: Discovery Rules Confirmation



11. Click the **Administration** pane, and then in the Navigation tree, select **Network Devices**.

Figure 4-12: 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.

Reader's Notes

5 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 5.1 below.
- Modules - All Modules State View. See Section 5.2 on page 32.
- Modules - System Modules State View. See Section 5.3 on page 33.
- Modules – Fan Tray State View. See Section 5.4 on page 35.
- Modules – Power Supply State View. See Section 5.5 on page 36.
- Trunks/Ports – Digital Trunks State View. See Section 5.6 on page.
- Trunks/Ports – Ethernet Ports State View. See Section 5.7 on page 38.

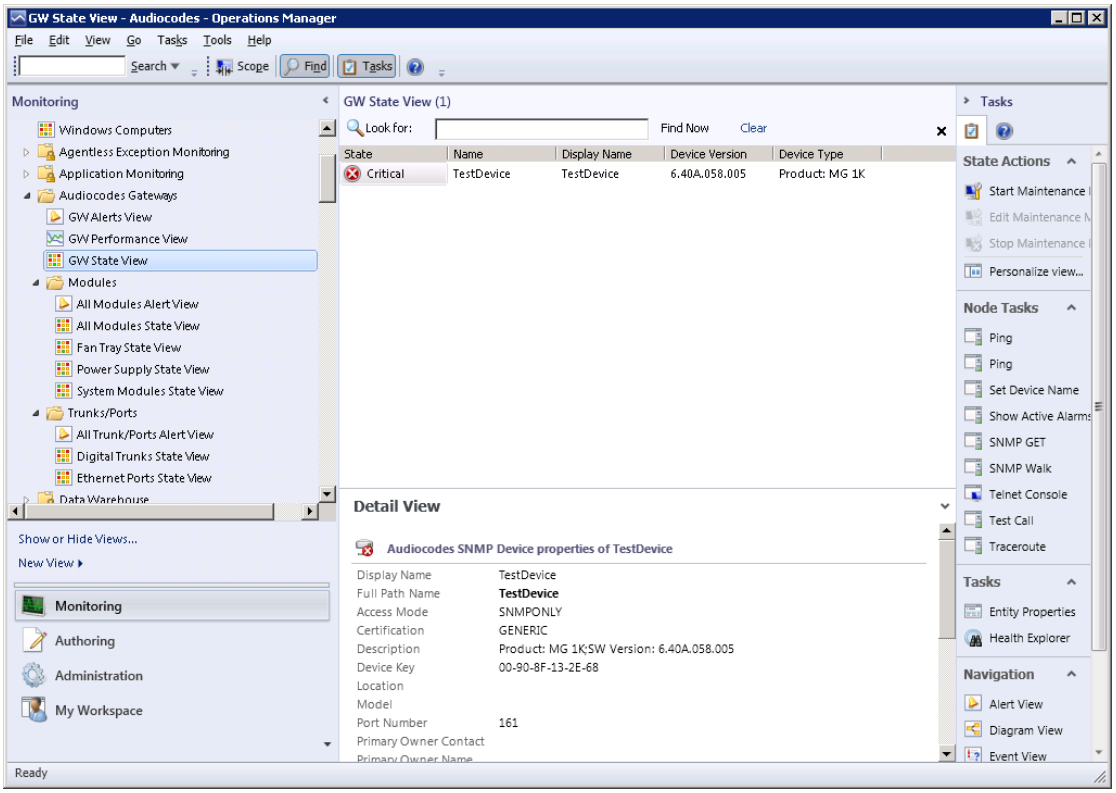
Open the Monitoring pane to access the relevant views for all your gateways.

5.1 GW State View

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.

Figure 5-1: GW State View

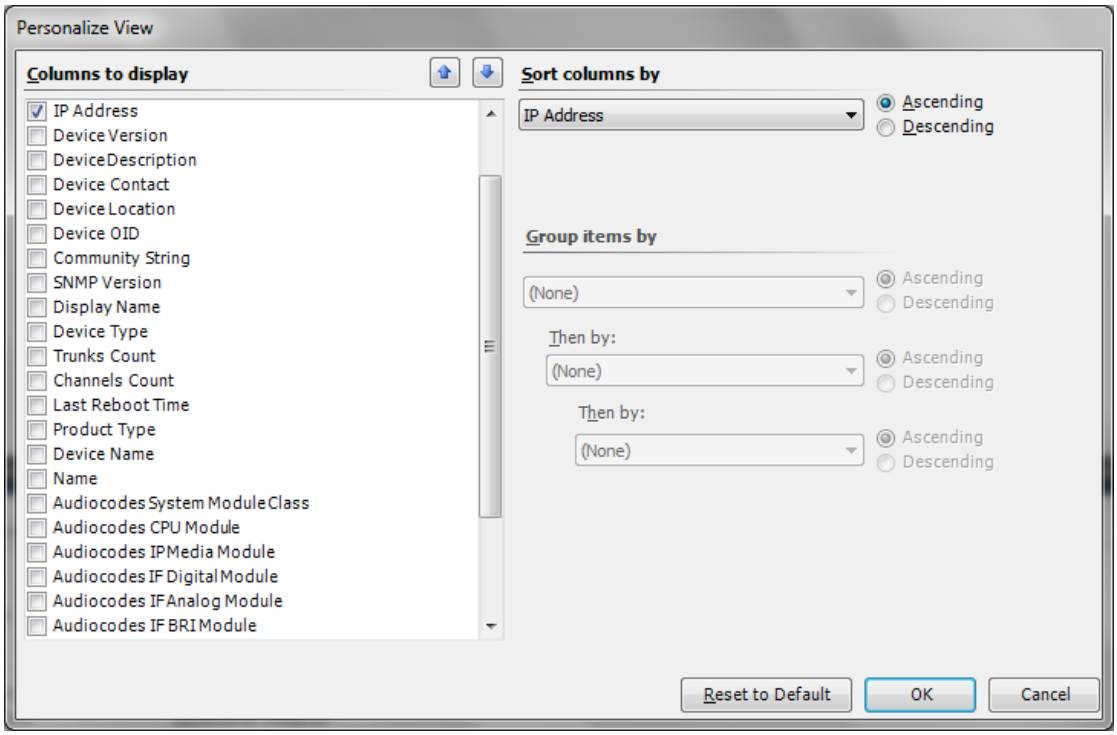


The Management Pack provides support for the following gateways:

- acMediant1000
- acMediant1000-MSBG
- acTrunkPack-MEDIANT2000
- acTrunkPack-STRETTO2000
- acTrunkPack-IPMServer2000
- acIPMedia3000
- acMediant3000
- acStretto3000
- acTrunkPack-6310-IpMedia
- acTrunkPack-6310-SB
- acTrunkPack-6310-T3
- acMediant3000-T3
- acIPmedia3000-T3
- acMediant800-MSBG
- acMediant800-ESBG
- acMediaPack-118
- acMediaPack114
- acMediaPack112

GW State View contains several fields with specific information about the gateway, including 'State' and 'IP Address'. You can change this view using the Personalize option – right-click any column name and select **Personalize View**; the Personalize View window is displayed:

Figure 5-2: Personalize View

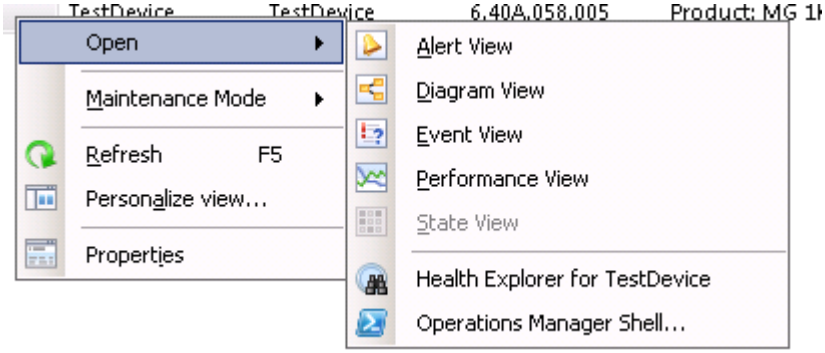


In this window, you can select the fields you wish to view in the GW State View and sort the data inside the view.

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

Figure 5-3: Look For Filter

There are several additional GW-related views you can open from the GW State View.

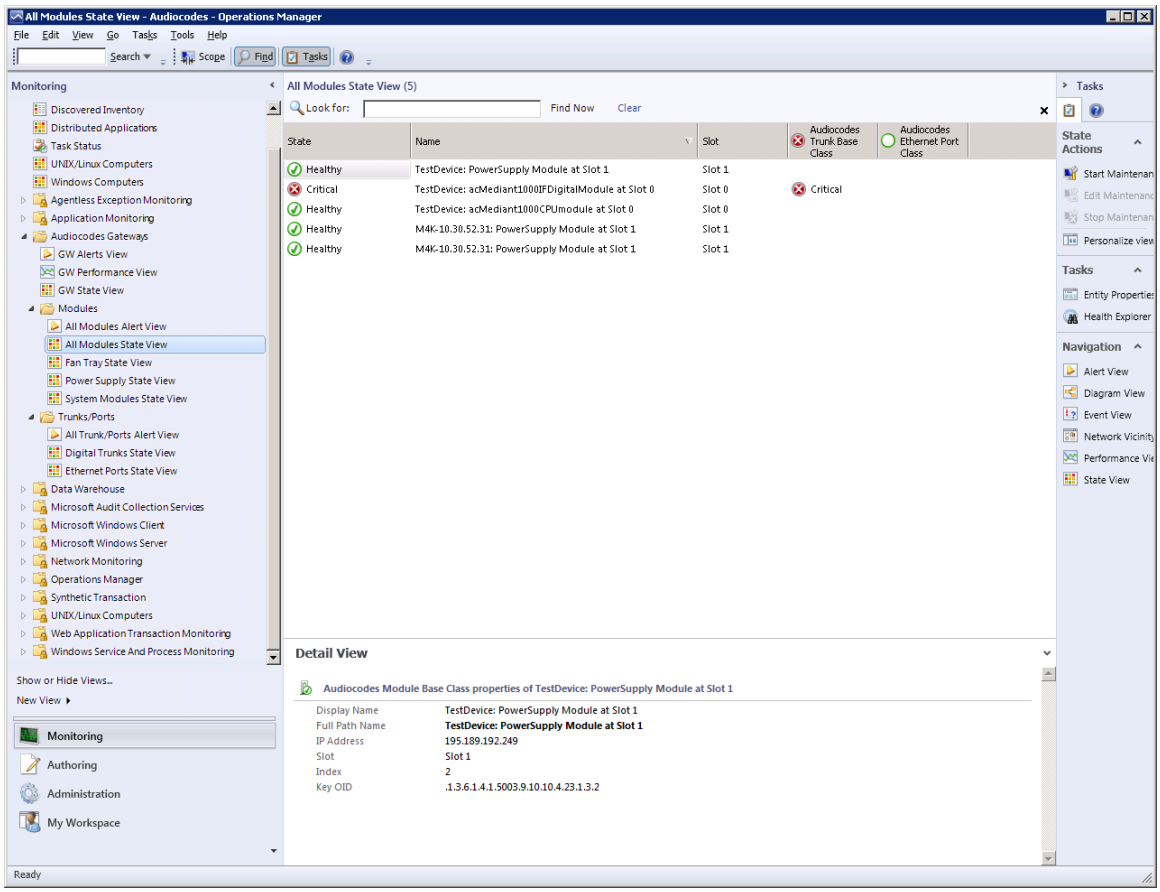


5.2 Modules – All Modules State View

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 5.1 on page 29.

The Detail View pane at the bottom of the All Modules State View window contains the details of each selected module.

Figure 5-4: All Modules State View



Right-clicking a module opens a menu which allows you to open additional views for the selected element, such as Alert view, Diagram view, Event view and several other additional options. For more information, see Section 5.8 on page 39.

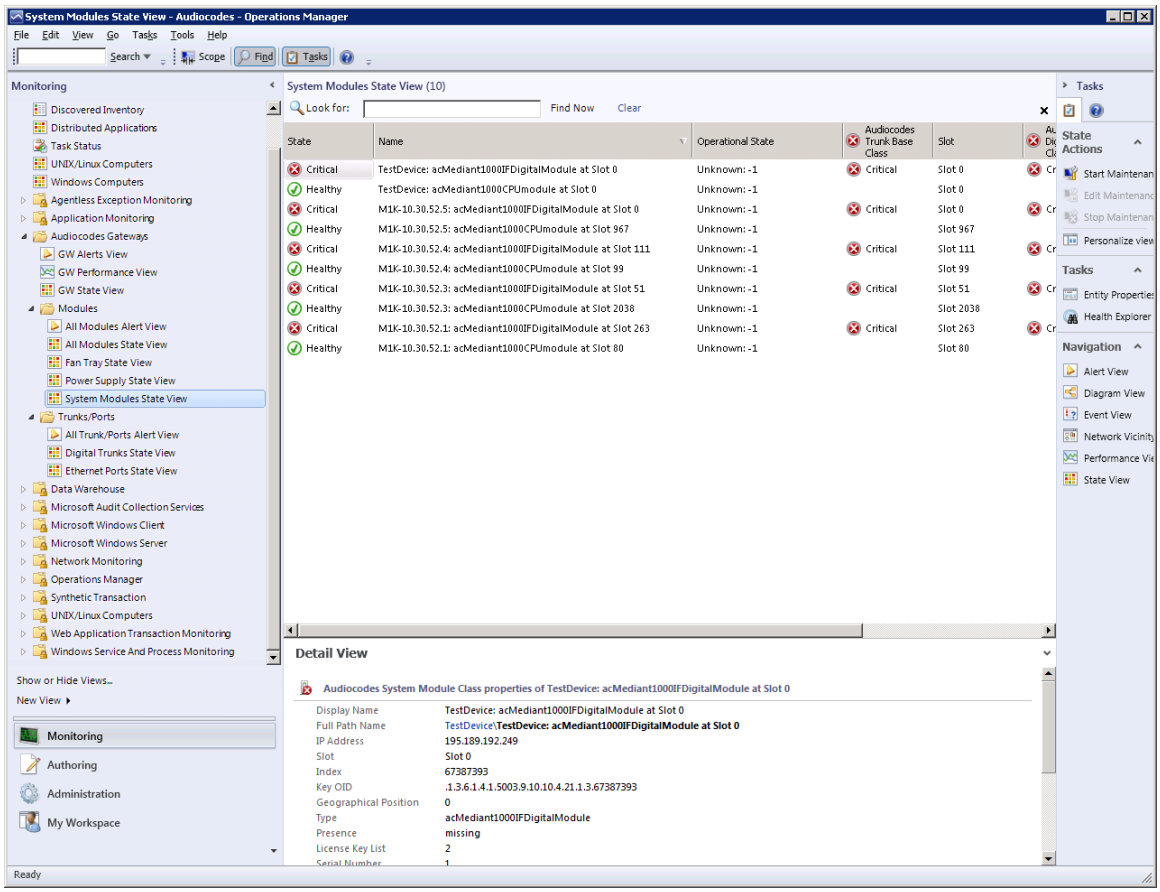
Note: Performance view is not supported at this monitoring level.

5.3 Modules – System Modules State View

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 5.1 on page 29.

The Detail View pane at the bottom of the System Modules State View window contains the details of each selected module.

Figure 5-5: System Modules State View



Right-clicking a module opens a menu, which allows you to open additional views for a selected element, such as Alert view, Diagram view, Event view and several other additional options.

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

The AudioCodes Management Pack provides support for the following modules:

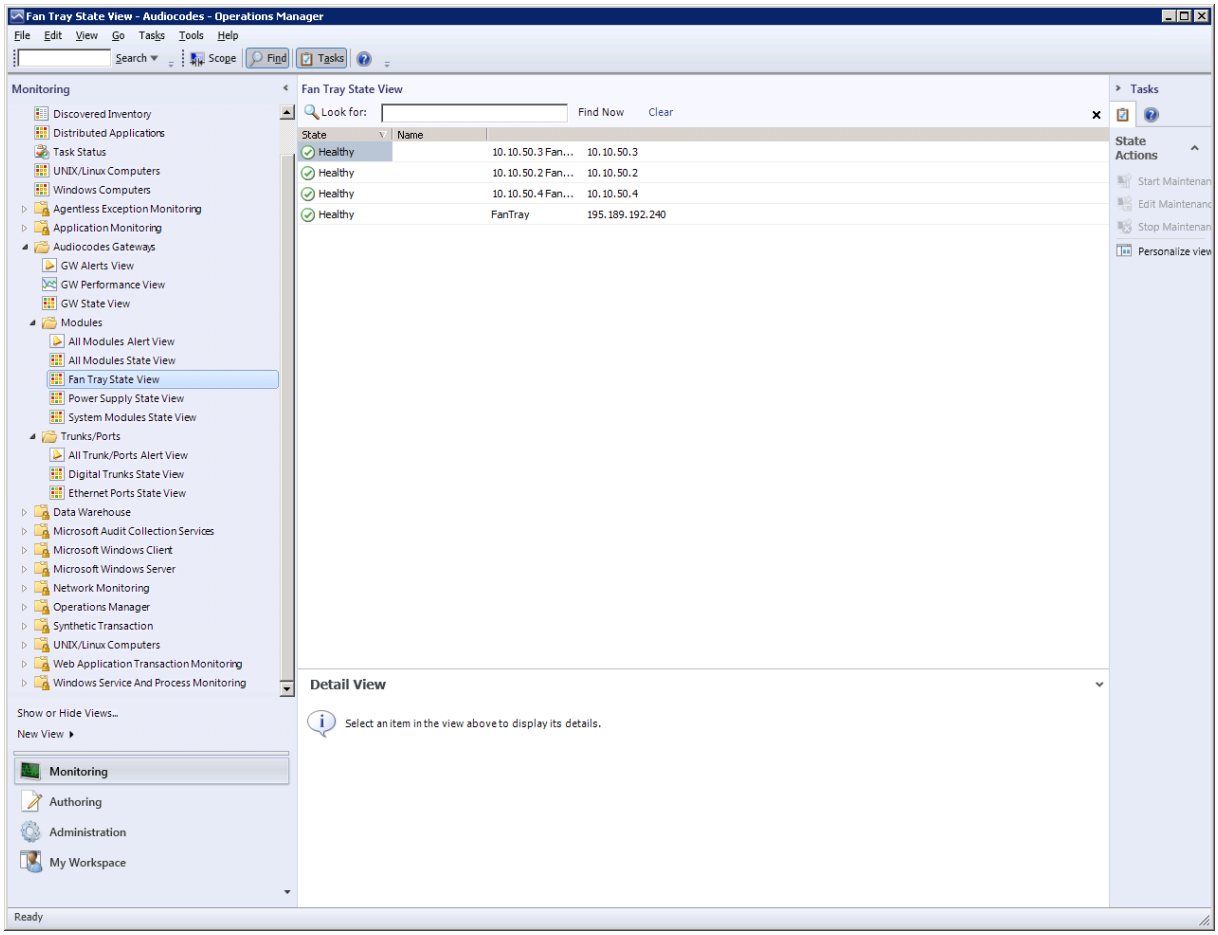
- acTrunkPack-MEDIANT2000
- acMediant1000CPUmodule
- acMediant1000IFADSLModule
- acMediant1000IFAnalogModule
- acMediant1000IFBRIModule
- acMediant1000IFDigitalModule
- acMediant1000IFSHDSLModule
- acMediant1000IFT1WANModule
- acMediant1000IFWANModule
- acMediant1000IPMediaModule
- acMediant800CPUmodule
- acMediant800EthernetModule
- acMediant800IFADSLModule
- acMediant800IFAnalogModule
- acMediant800IFBRIModule
- acMediant800IFDigitalModule
- acMediant800IFSHDSLModule
- acMediant800IFT1WANModule
- acMediant800IFWANModule
- acMediant800IFWiFiModule
- acMediant800IPMediaModule
- acMediaPack112
- acMediaPack114
- acMediaPack-118
- sA1
- sA2
- sA3

5.4 Modules – Fan Tray State View

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 5.1 on page 29.

The Detail View pane in the bottom of Fan Tray State View window contains the details of each selected module.

Figure 5-6: Fan Tray State View



Right clicking a module opens a menu which allows you to open additional views for the selected element, such as Alert view, Diagram view, Event view and several other additional options. For more information, see Section 5.8 on page 39.

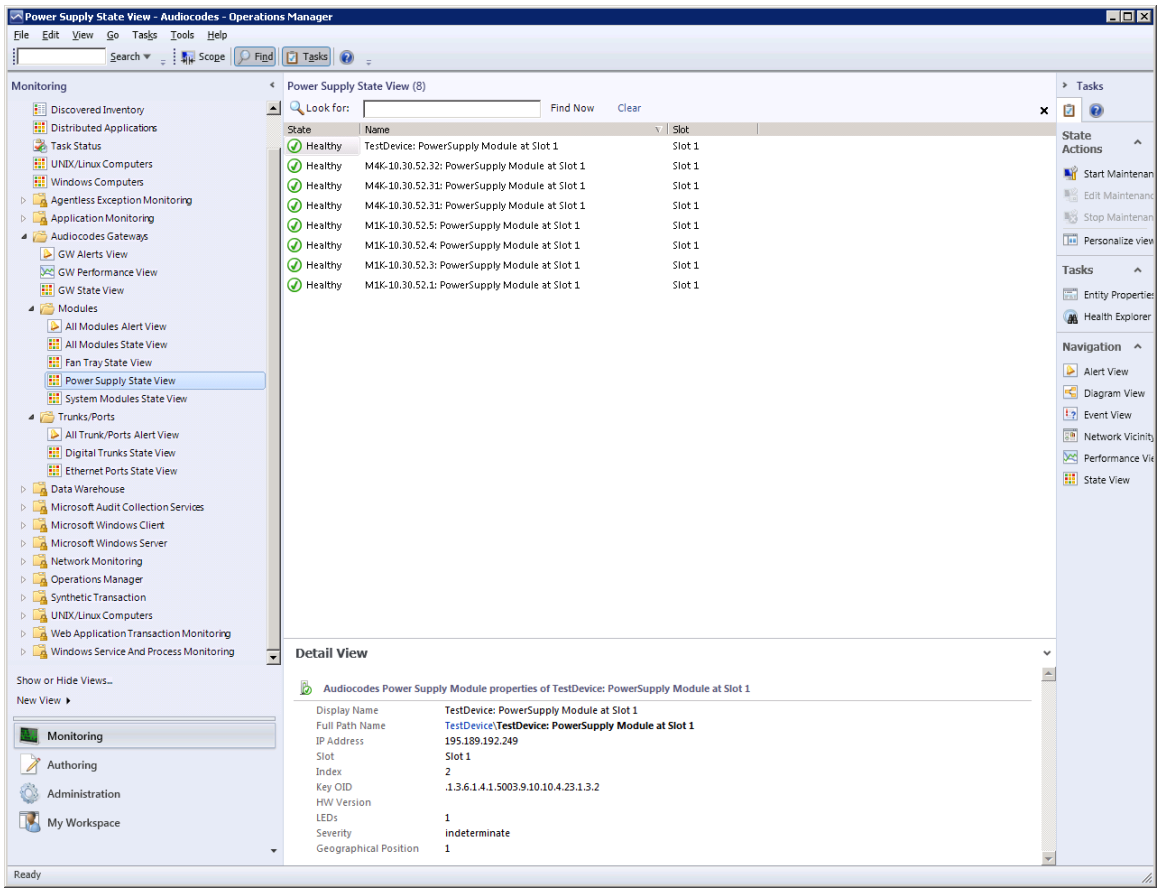
Note: Performance view is not supported at this monitoring level.

5.5 Modules – Power Supply State View

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 5.1 on page 29.

The Detail View pane at the bottom of the Power Supply State View window contains the details of each selected module.

Figure 5-7: Power Supply State View



Right clicking a module opens a menu which allows you to open additional views for selected element, such as Alert view, Diagram view, Event view and several other additional options. For more information, see Section 5.8 on page 39.

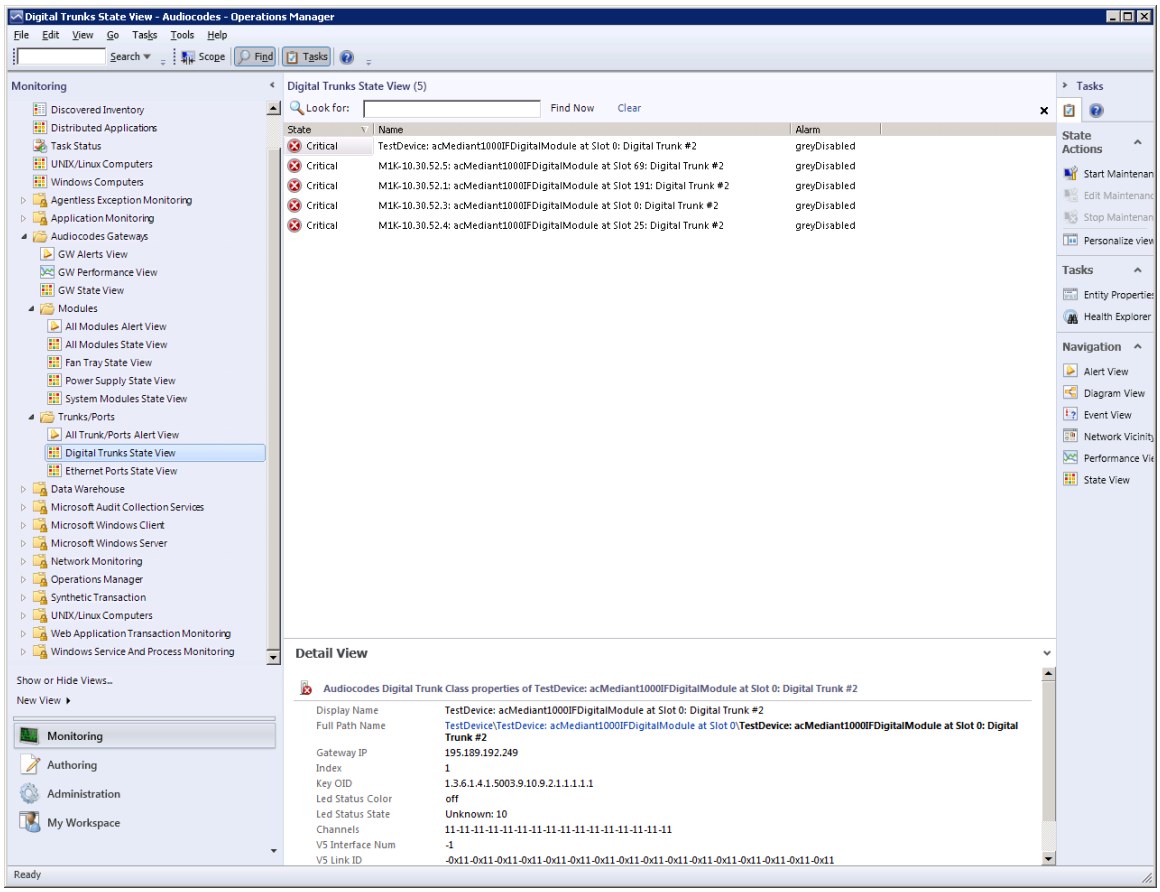
Note: Performance view is not supported at this monitoring level.

5.6 Trunks/Ports – Digital Trunks State View

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 5.1 on page 29.

The Detail View pane at the bottom of the Digital Trunks State View window contains the details of each selected module.

Figure 5-8: Digital Trunks State View



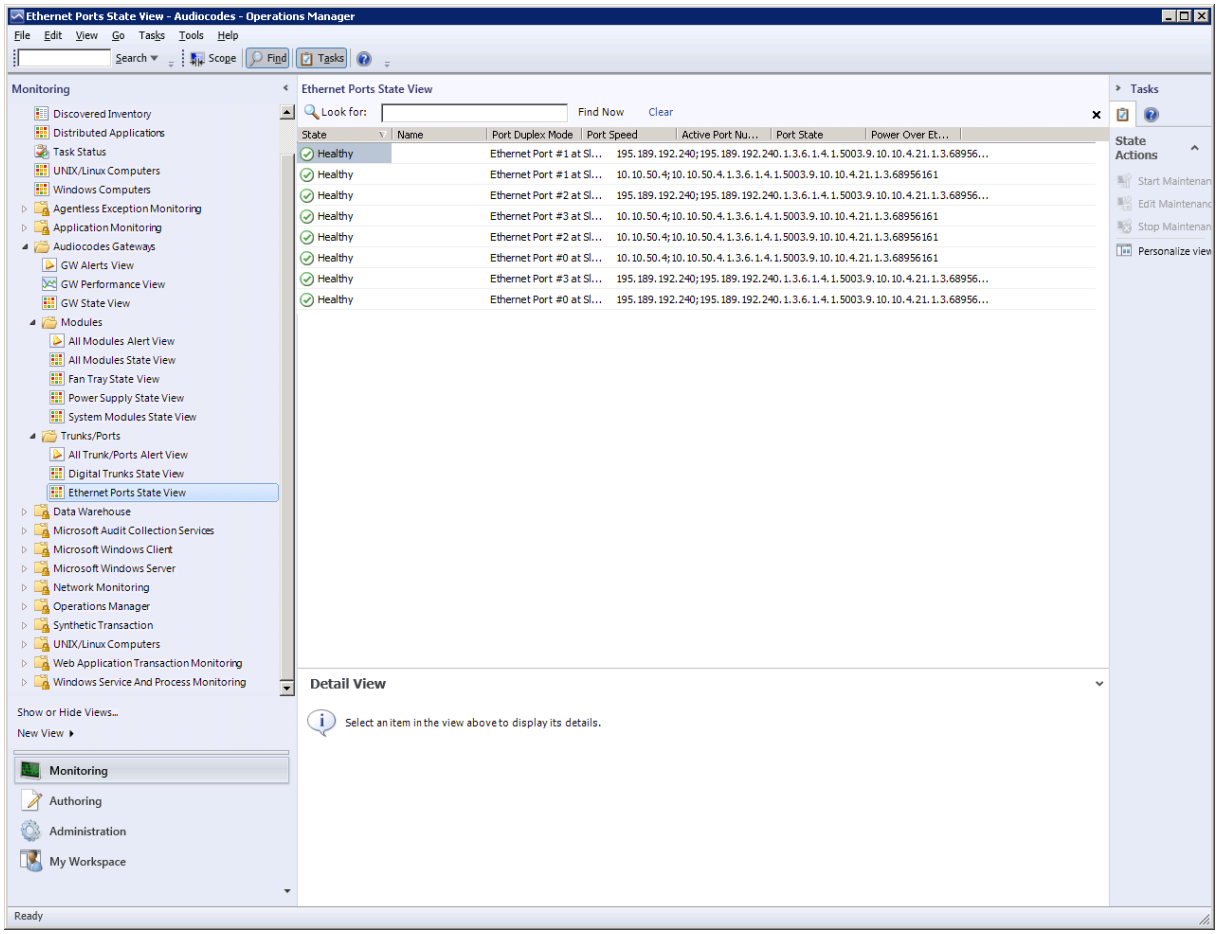
Right-clicking a trunk opens a menu which allows you to open additional views for the selected element, such as Alert view, Diagram view, Event view and several other additional options. For more information, see Section 5.8 on page 39.

5.7 Trunks/Ports – Ethernet Ports State View

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 5.1 on page 29.

The Detail View pane at the bottom of the Ethernet Ports State View window contains the details of each selected module.

Figure 5-9: Ethernet Ports State View

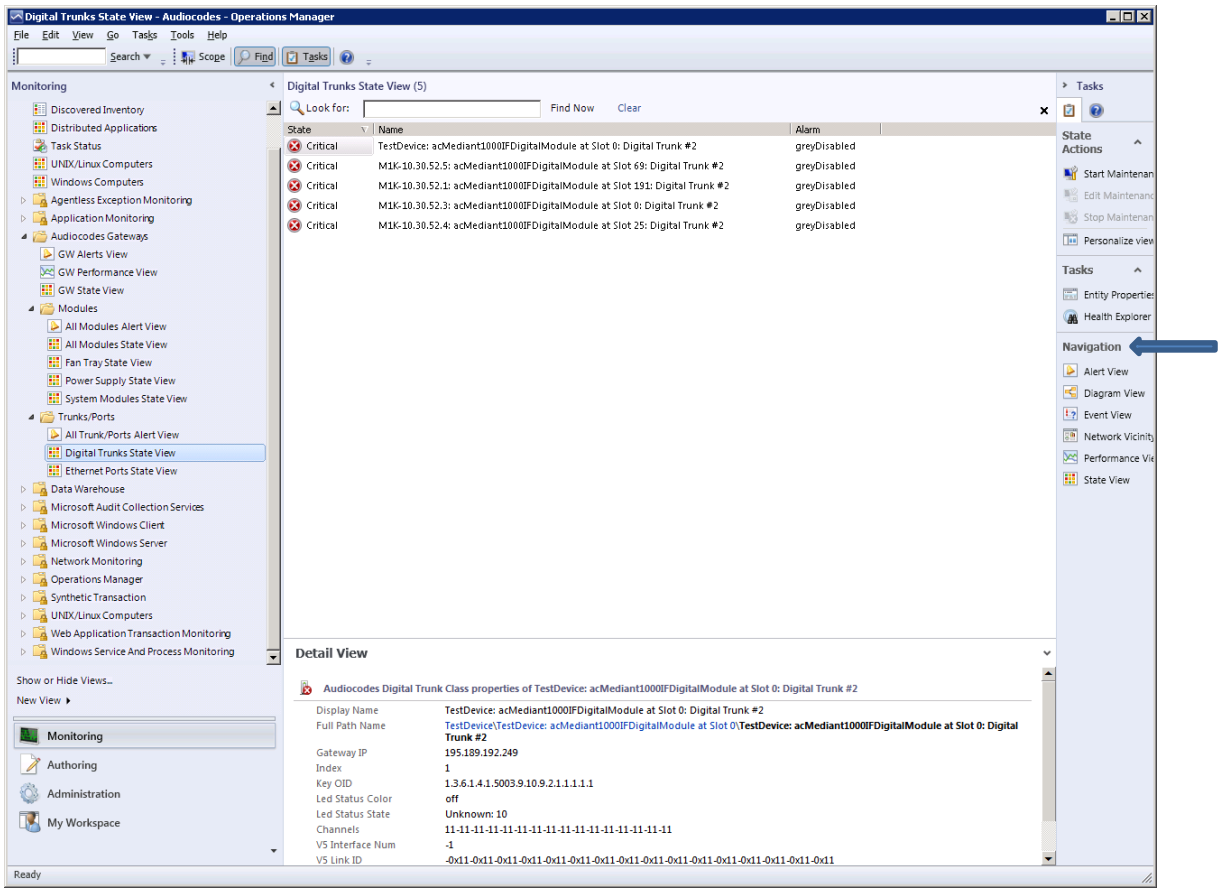


Right-clicking a port opens a menu which allows you to open additional views for the selected element, such as Alert view, Diagram view, Event view and several other additional options. For more information, see Section 5.8 on page 39.

5.8 Navigation Pane Views

There are several sub- views that you can open from the Navigation pane in each Module View. Each of these views displays additional information on the specific View (see the Navigation pane indicated in the Figure below).

Figure 5-10: Digital Trunks State View-Navigation Pane



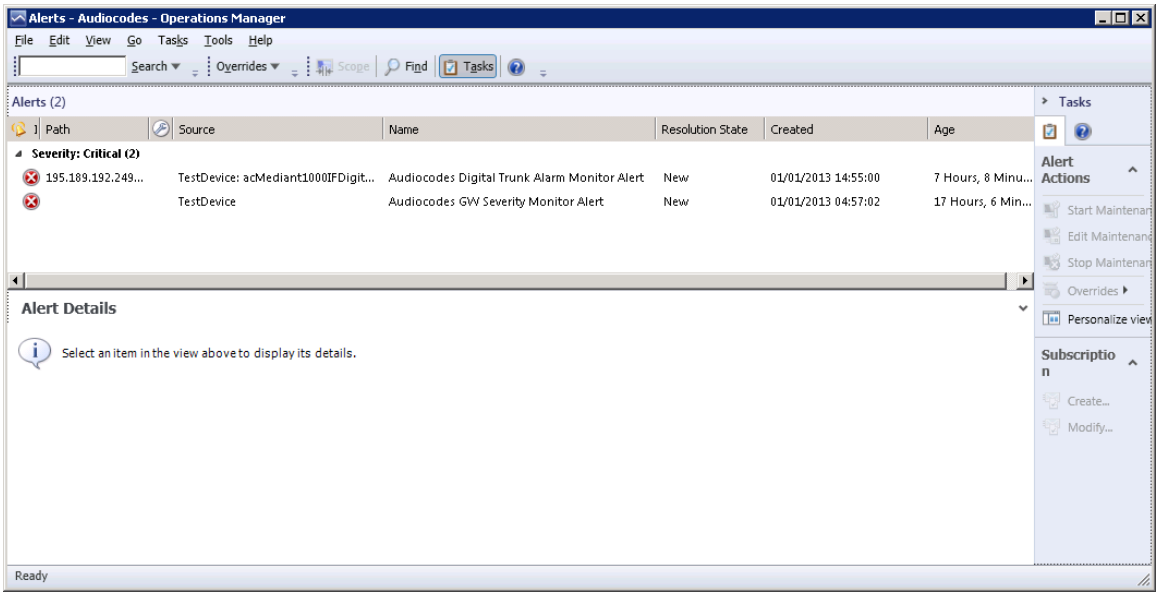
This section describes the following Navigation pane views:

- Alert View. See below.
- Diagram View. See Section 5.8.2 on page 40.
- Event View. See Section 5.8.3 on page 41.
- Performance View. See Section 5.8.4 on page 41.

5.8.1 Alert View

The Alert view displays the alerts for a specific element.

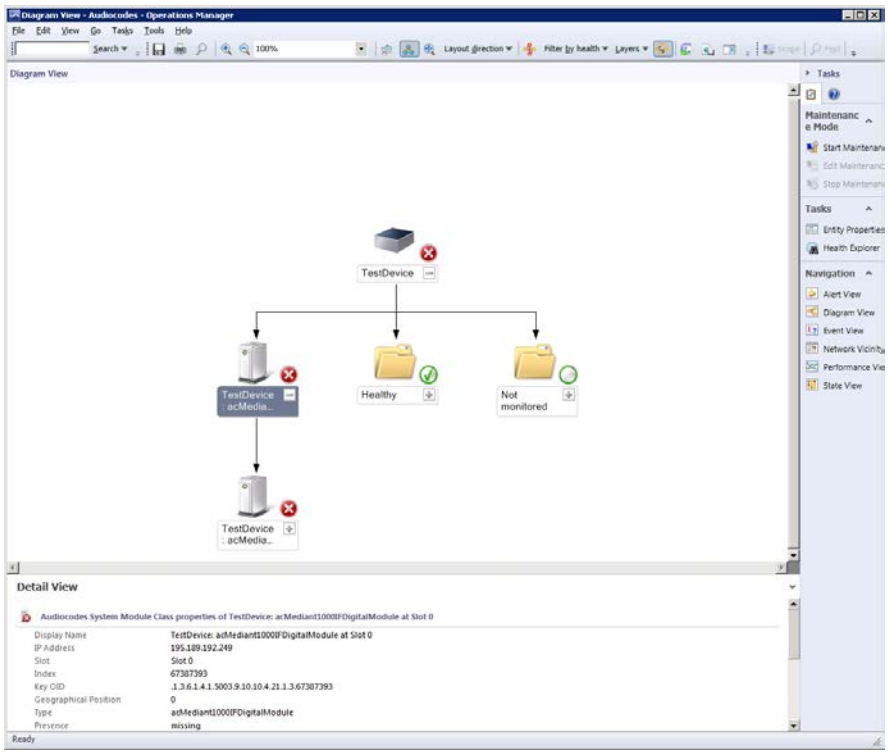
Figure 5-11: Alert View



5.8.2 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.

Figure 5-12: Diagram View



5.8.3 Event View

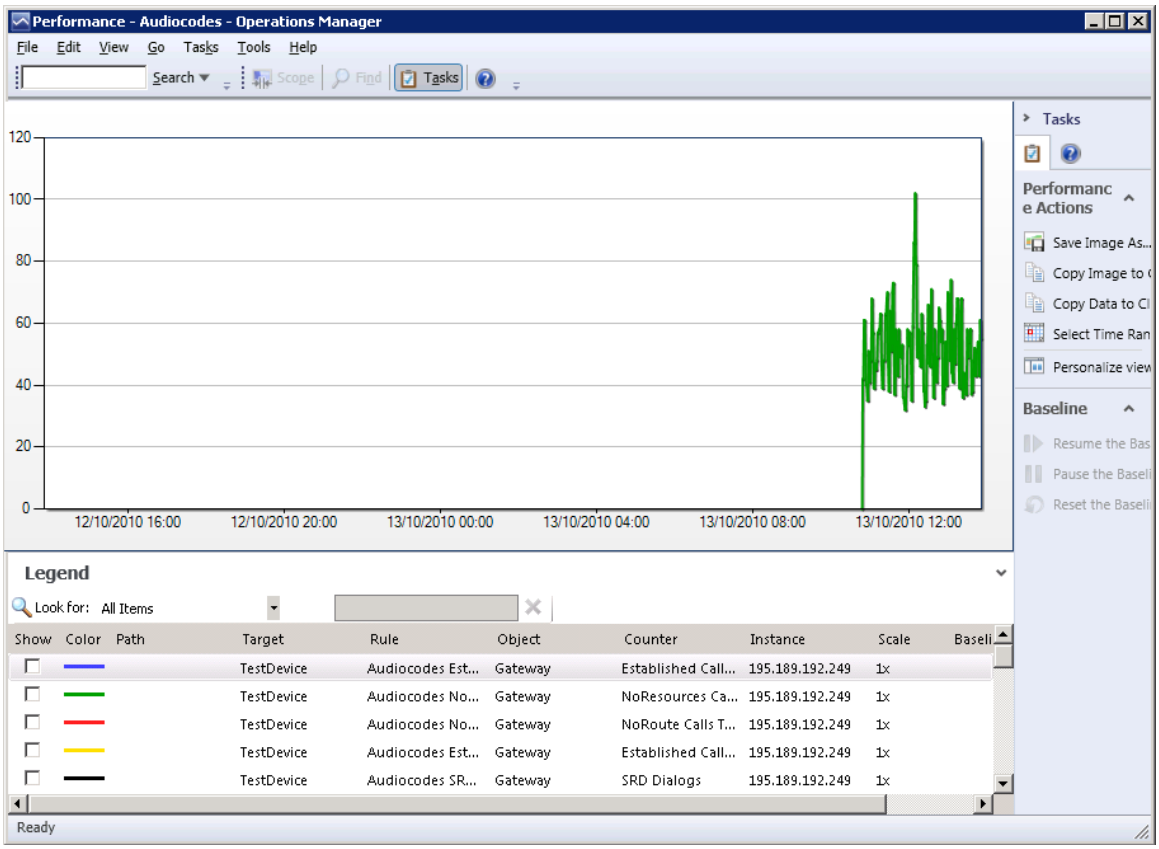
The Event view displays events for a specific element.

Note: The current Management Pack version doesn't allow you to view events.

5.8.4 Performance View

The Performance view displays performance data for a specific element.

Figure 5-13: Performance View



Reader's Notes

6 Monitoring Gateway Element Health

The SCOM Management Pack performs Health Monitoring for each discovered Gateway, Module and Trunk (together referred to as gateway elements). All the views described in Section 5 on page 29 contain the Health state of entire entities (Gateways, Modules and Trunks). 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.

All entities can have one of the following states:

- Critical
- Warning
- Healthy

An Entity has the **Critical** in the event where a trap with Severity 4 and above was captured for this entity. An Entity has the **Warning** in the event where a trap with Severity 1 to 3 was captured for this entity.

All trap-based monitors captured are cleared in the event where the trap has the same OID and Source varbinds and is in the Cleared (0) State.

There are three types of monitoring used to define the health state of an entity:

- **Trap-based monitoring** is an alert issued on the basis of the trap captured from an entire Gateway entity (Gateway, Module or Trunk).
- **Object-based monitoring** is the polling of a specific SNMP object value change (such as a change from 'enable' to 'disable' for an acSysModuleOperationalState module-related object).
- **Threshold-based monitoring** is an alert issued on the basis of thresholds defined for performance counters. This type of alert is applicable at the gateway level only. Each performance counter has two types of thresholds: 'High' and 'Low'. Each threshold type has two levels: 'Warning' and 'Critical'. This means that the final severity of threshold-based alert depends upon which level of threshold has been exceeded. The thresholds levels definition is described in Section 6.2 on page 47.

Together with Rollup Policy (not applicable for threshold-based alerts) define the final health state of an entity. The use of alerts and Rollup Policy for a specific entity is described in Section 6.3 on page 50.

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 indicated 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 indicated as 'Critical'.

6.1 Viewing Active Alerts

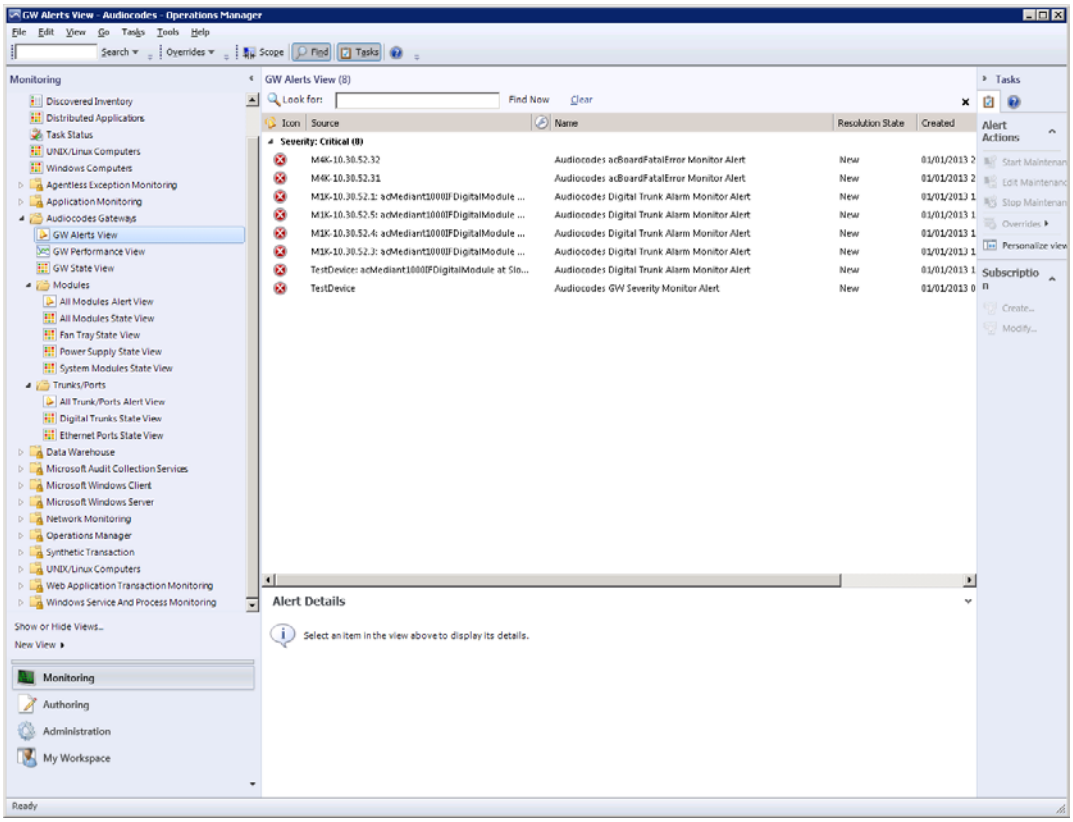
The following views are provided by the SCOM Management Pack for viewing active alerts:

- GW Alerts View. See Section 6.1.1 on page 44.
- All Modules Alerts View. See Section 6.1.2 on page 45.
- All Trunks/Ports Alerts View. See Section 6.1.3 on page 46.

6.1.1 GW Alerts View

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

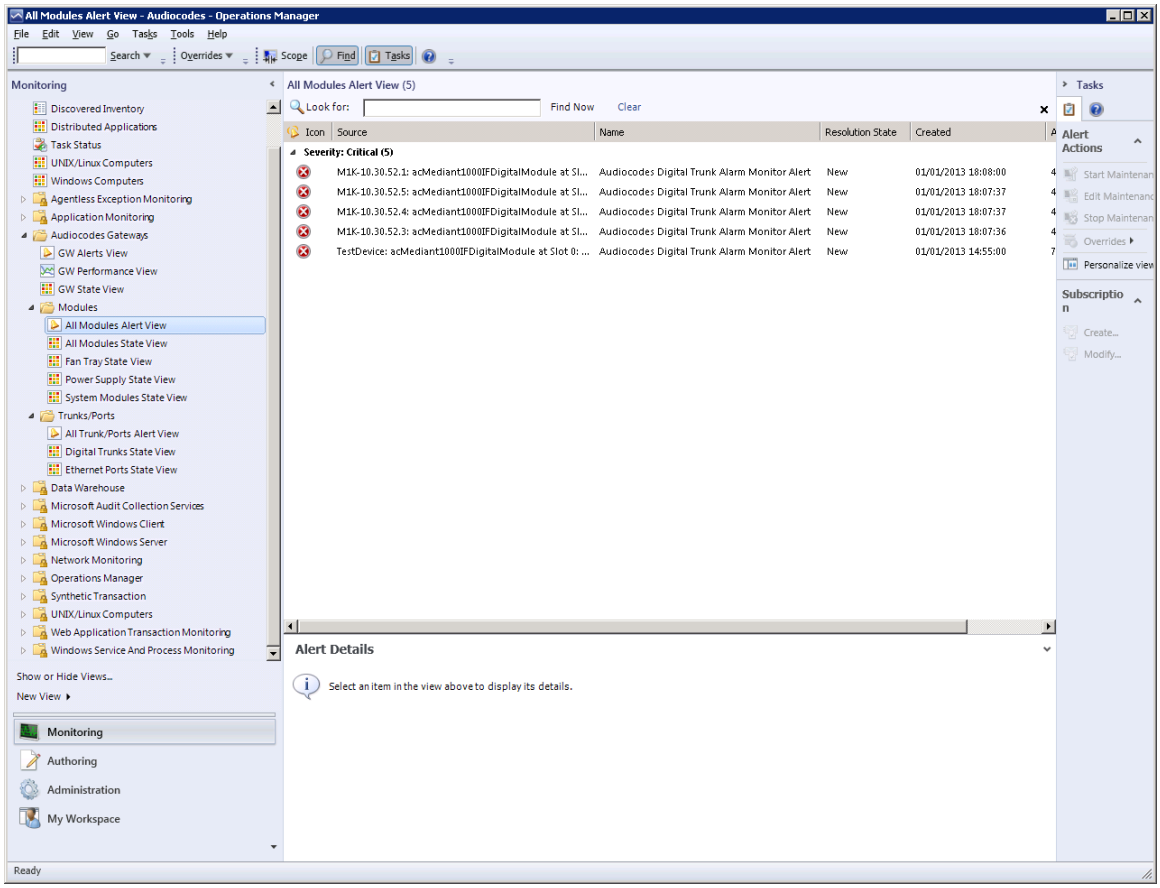
Figure 6-1: GW Alerts View



6.1.2 All Modules Alerts View

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

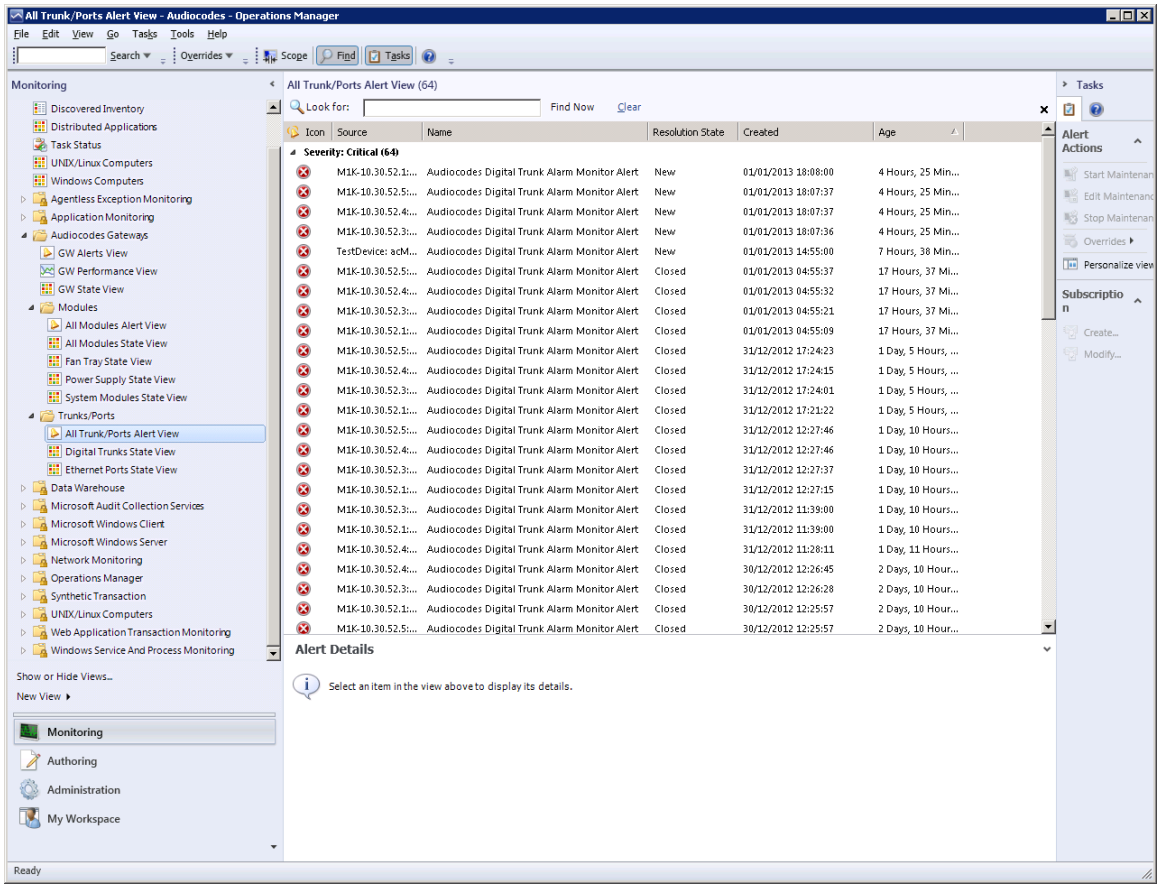
Figure 6-2: All Modules Alert View



6.1.3 All Trunks/Ports Alerts View

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

Figure 6-3: All Trunk/Ports View



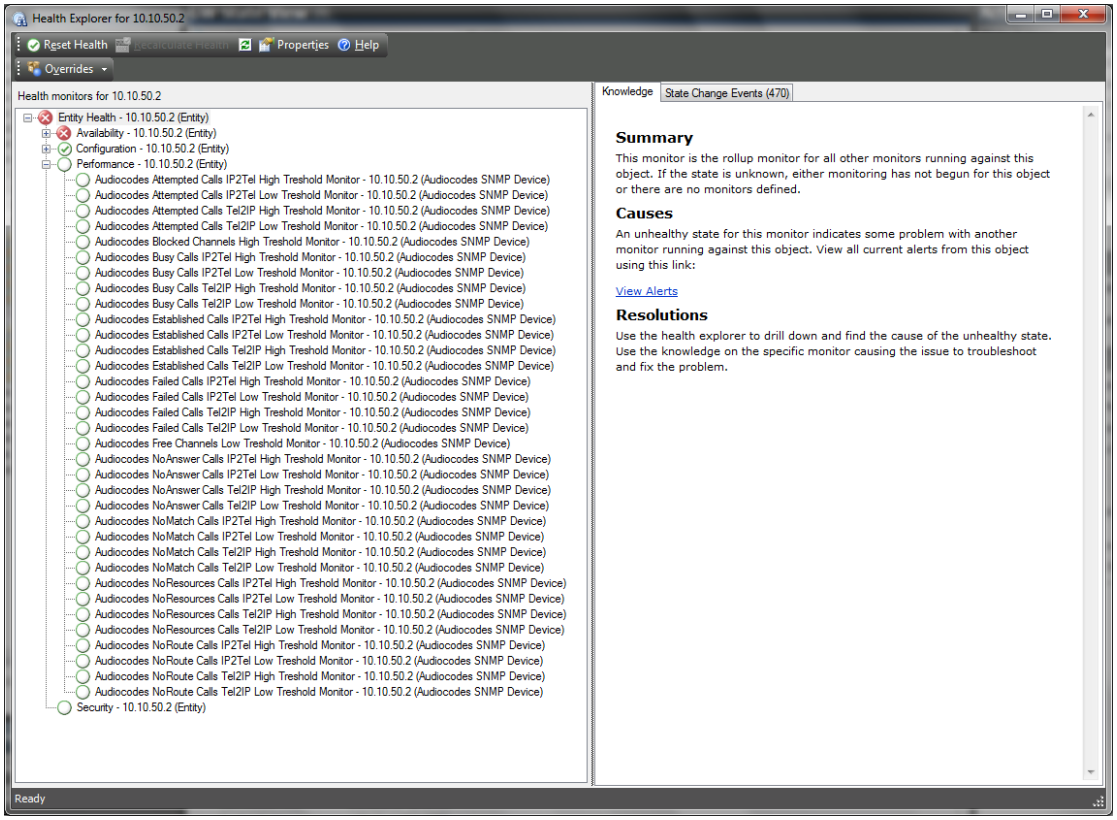
6.2 Configuring Thresholds

This section describes how to configure the Entity Threshold Settings for specific devices i.e. specific IP addresses or specific groups of devices, for example, for all Mediant 800 devices.

➢ To define the thresholds levels:

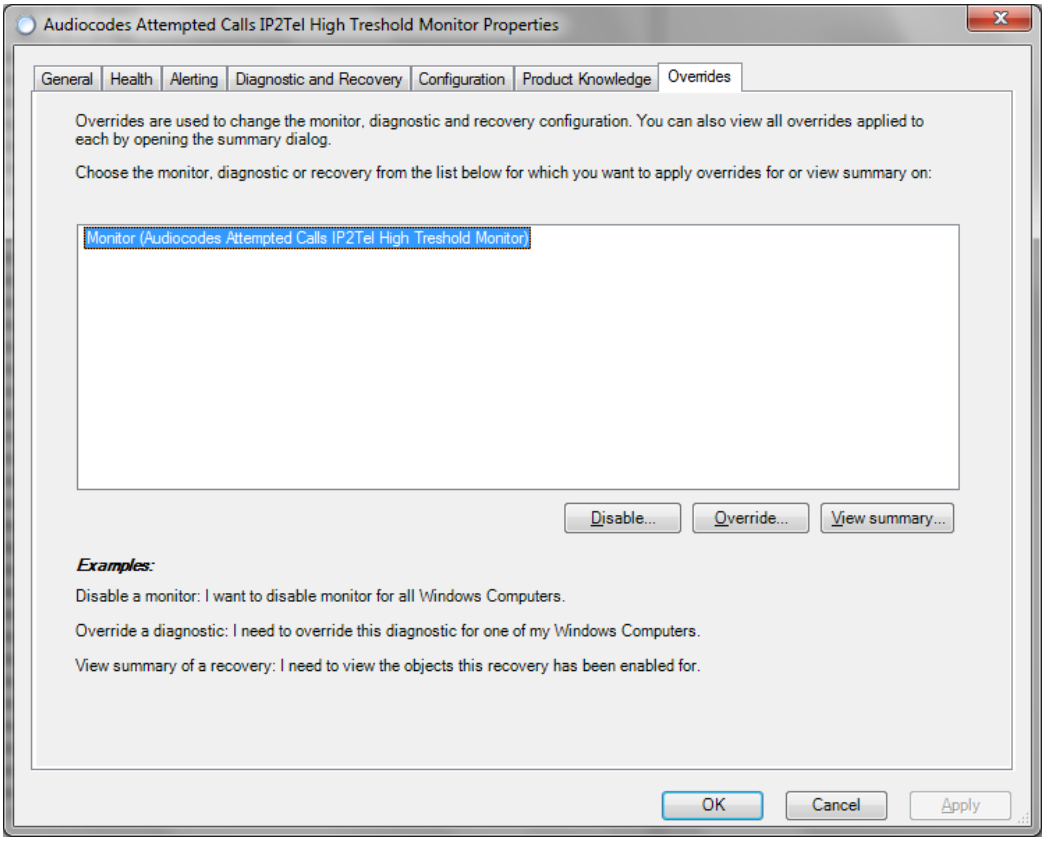
1. In the GW State View, right-click any gateway and choose **Open > Health Explorer for <GW IP>**; the Health Explorer is displayed:

Figure 6-4: Health Explorer



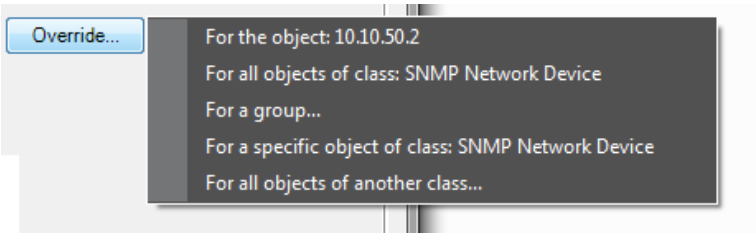
2. In the **Entity Health** tree, expand **Performance** node.
3. Select the required monitor right-click and choose **Monitor Properties**; the Threshold Monitor properties window is displayed:

Figure 6-5: Threshold Monitor Properties



4. Click the **Overrides** tab; the Overrides screen is displayed.
5. Click the **Override** button.

Figure 6-6: Override

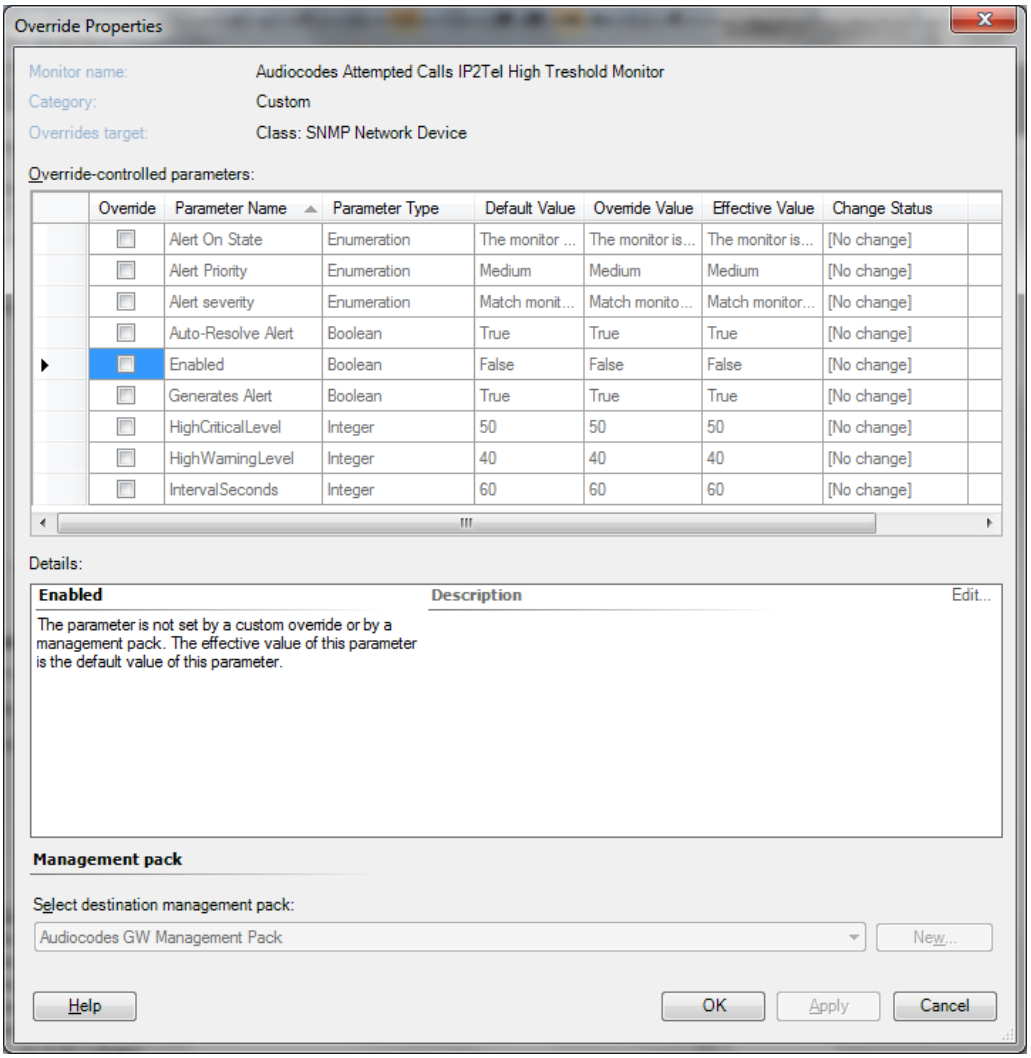


Choose one of the following options:

- **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 6-7: Override Properties



The following parameters define threshold levels:

- 'HighCriticalLevel' and 'HighWarningLevel' for High Threshold Monitor
- 'LowCriticalLevel' and 'LowWarningLevel' for Low Threshold Monitor

6. In the Override column adjacent to the required parameter, select the corresponding checkbox.
7. In the Override Value column, set the required value (s) for the relevant parameters and click OK.
8. In the Threshold Monitor Properties window, click **OK** to complete the procedure.

6.3 Troubleshooting Performance Issues

This section describes how to optimize the load on the SCOM server in cases where a large number of functional items are monitored by the Management Pack. The following sections are described:

- Overriding Monitors. See Section 6.3.2 on page 54.
- Overriding Discoveries. See Section 6.3.3 on page 58.
- Overriding Rules. See Section 6.3.4 on page 46.

For Monitors, Discoveries and Rules objects, overriding the values of the following parameters can significantly affect the load on the SCOM server:

- **IntervalSeconds**

  The Frequency of entity monitoring/discovering can be affected by modifying the parameter 'IntervalSeconds'. This parameter defines how often functional items should be launched.

- **SyncTime**

  The number of monitoring/discovering functional items that can be launched simultaneously can be affected by modifying the 'SyncTime' parameter (specified in the reference point).

Note the following recommendations:

- The following scenario is recommended: where critical functional items are launched once every three minutes and are divided into three groups, where each group has a different SyncTime, then only one third of high-level CPU utilization critical functional items are launched every minute, thereby reducing the ongoing CPU load.
- When you modify the Sync time by reducing the number of functional items that are polled at any one point in time, this leads to improved performance by reducing CPU utilization; however, on the other hand, it leads to delay, as the time between the relative launching of each functional item increases.
- Generally polling of counter intervals 'IntervalSeconds' can be overriden; however, this is not highly recommended for most of the counters have a low polling frequency (once every 15 minutes) and depend on the actual information refresh on the gateway devices themselves - counters on the device are also calculated once every 15 minutes. The exception is in the case of specific Trunk counters (see Section 6.3.4.1 on page 61).

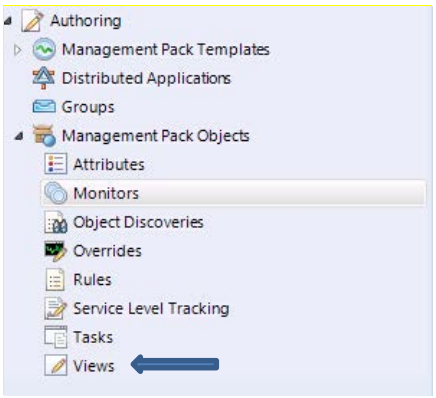
6.3.1 Filtering Management Pack Objects View

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**.

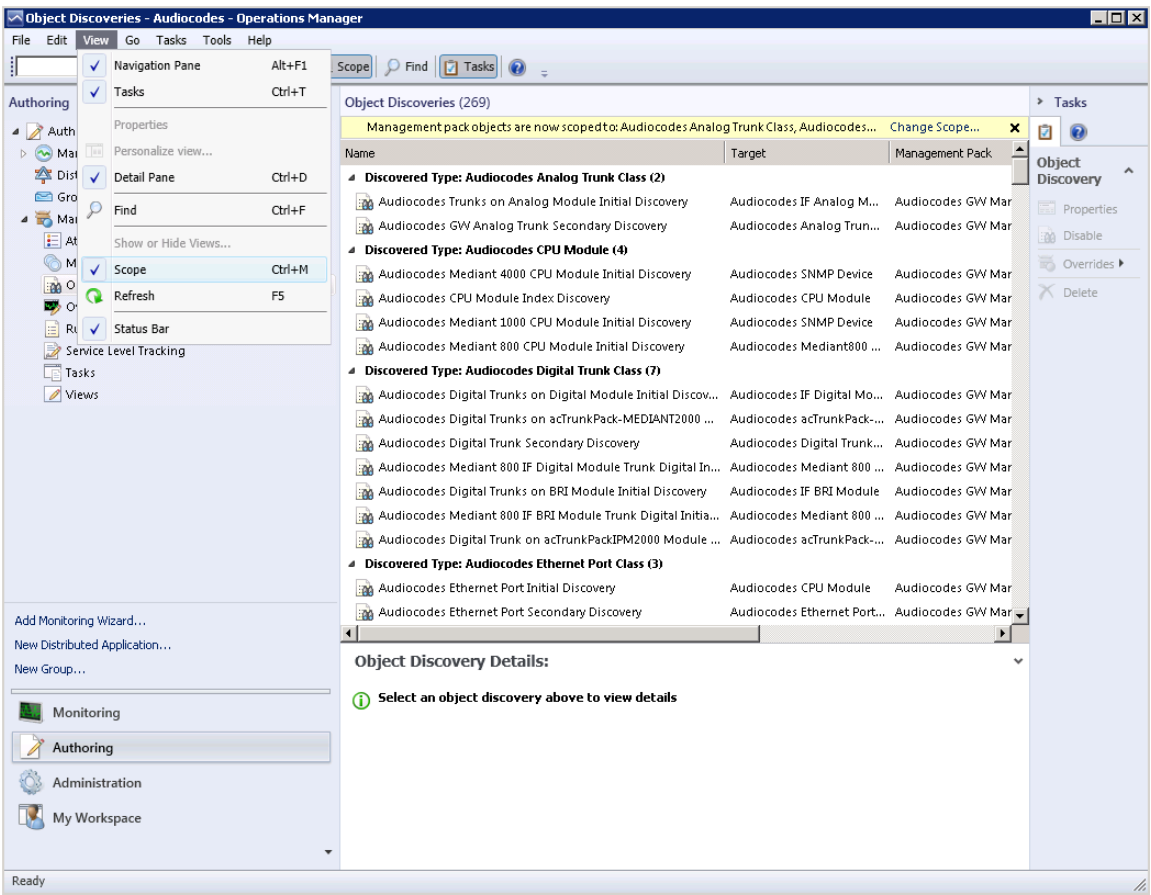
Figure 6-8: Views



The right-hand pane displays all the functional items that are defined in the current scope.

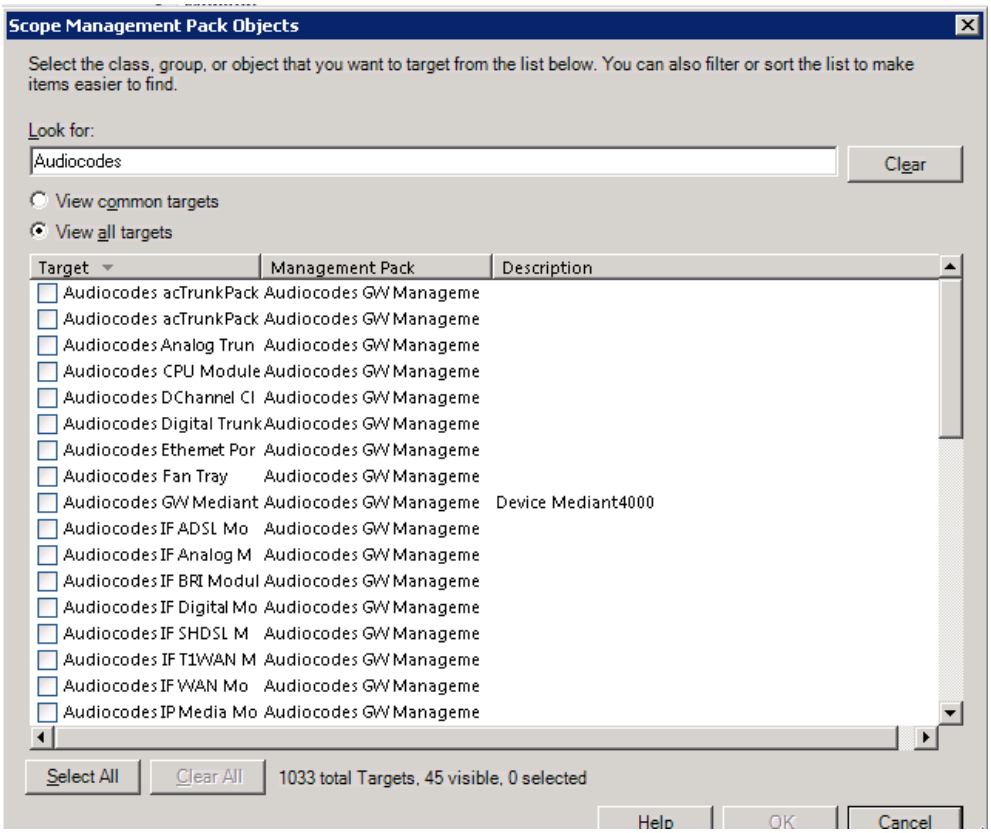
2. In the Main Menu, ensure that the Scope setting is selected:
   - Select **View > Scope** or press **Ctrl+M**.

Figure 6-9: View Scope



The Scope Management Pack Objects window is displayed:

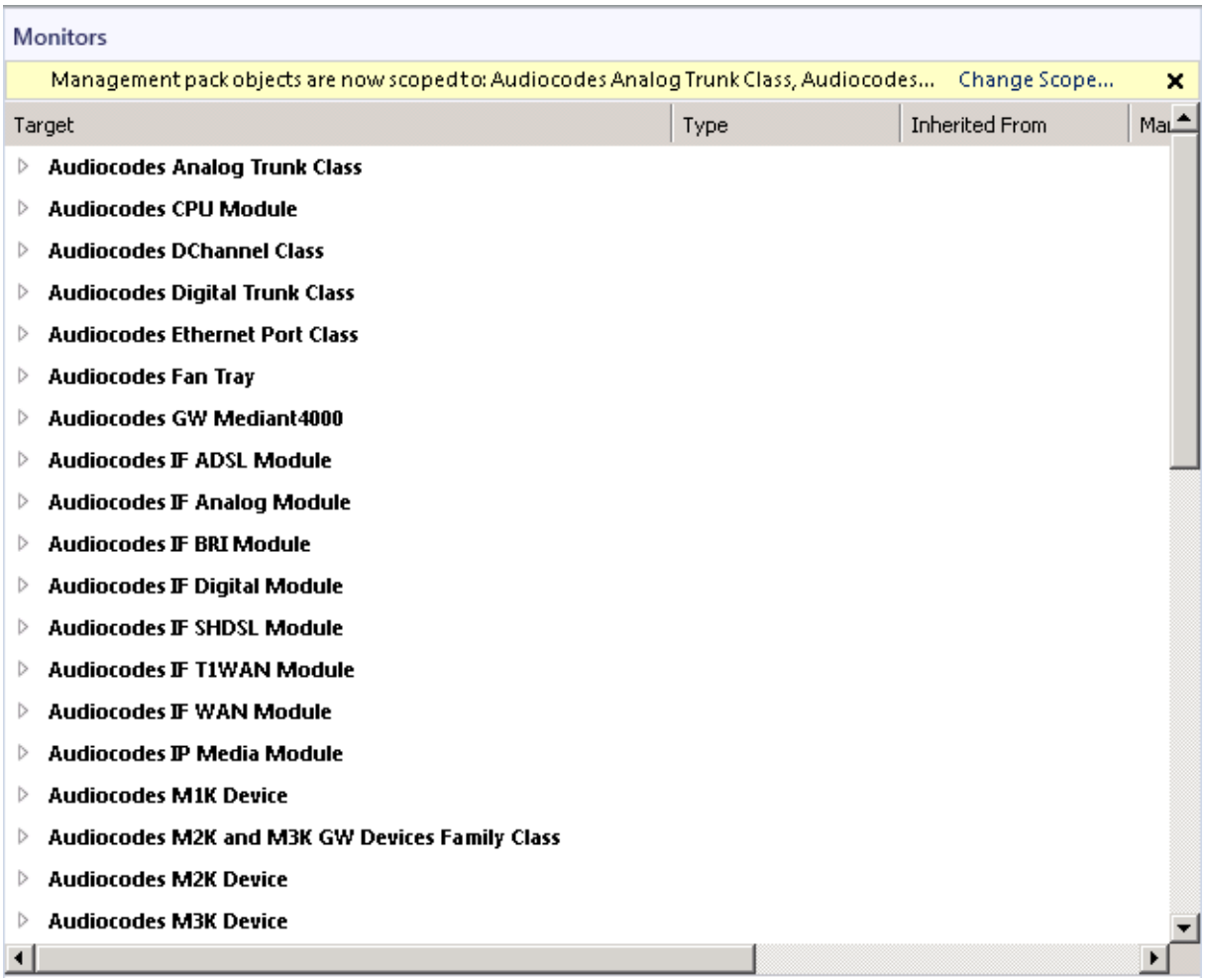
Figure 6-10: Scope Management Pack Objects



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 6-11: AudioCodes Management Pack Entities



6.3.2 Overriding Monitors

This section describes how to modify Monitor parameters, such as how often monitors should be launched and the time to synchronize with the server clock.

The following monitors have a high level of CPU utilization:

- Gateways:
  - Audiocodes Blocked Channels High Threshold Monitor
  - Audiocodes Free Channels Low Threshold Monitor
  - Audiocodes <*> Low Threshold Monitor – family of monitors
  - Audiocodes <*> High Threshold Monitor – family of monitors
- Trunks:
  - Audiocodes Digital Trunk Alarm Monitor

For Audiocodes <*> Low Threshold Monitor and AudioCodes <*> High Threshold Monitors family of monitors where <*> is the actual monitored parameter name, such as 'TelToIP Failed Calls'.

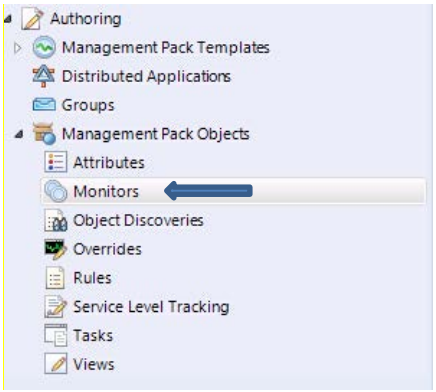
Note:

- Ensure that you filter the view to display only AudioCodes objects in the right-hand pane. See Section 6.3.1 on page 51.
- It is highly recommended to run each monitor at a different time so as to avoid overburdening the CPU resources (i.e. modifying the 'Sync' parameter as described later in this section).

➢ **To override monitors:**

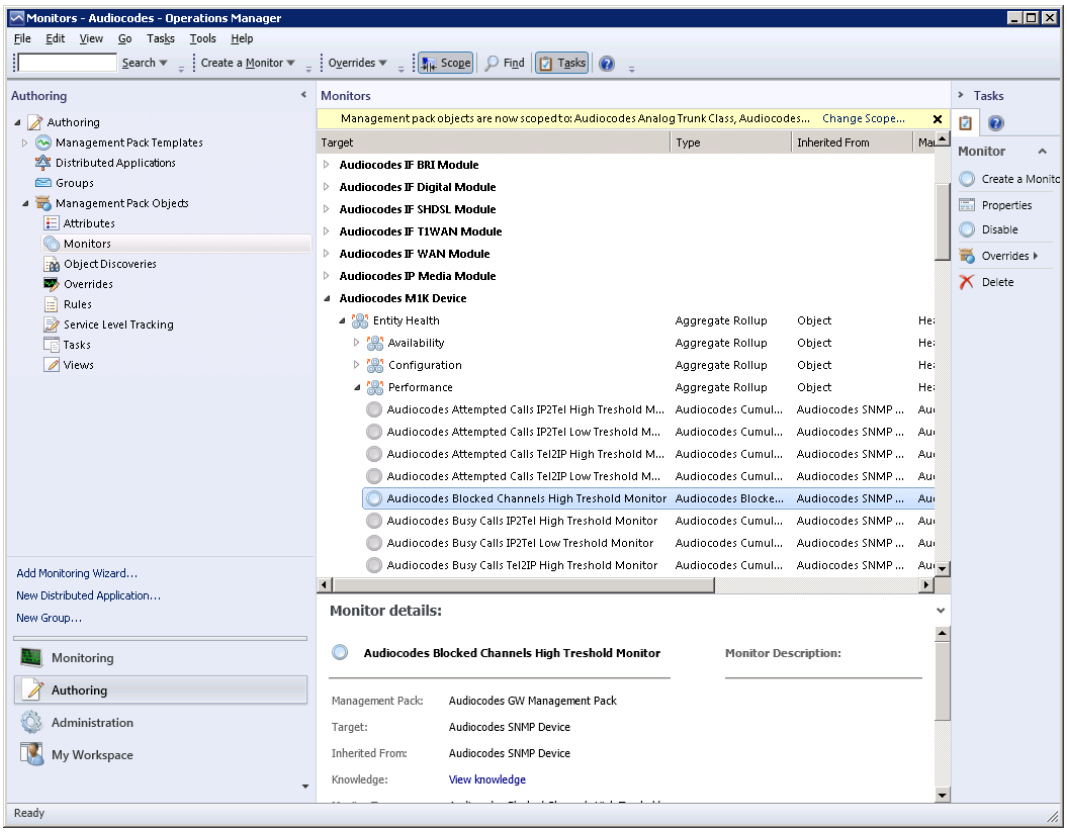
1. In the Authoring pane, select **Management Pack Objects** > **Monitors**.

Figure 6-12: Monitors Option



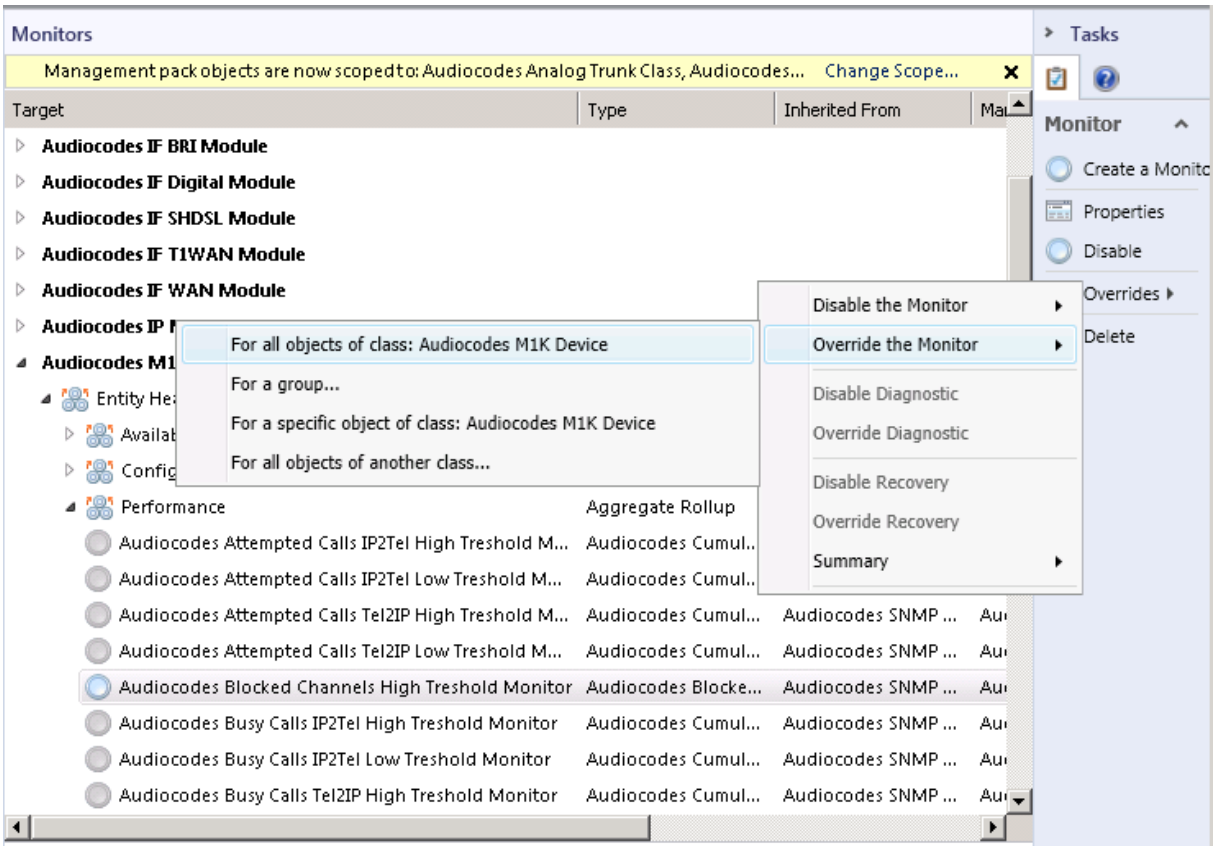
The Monitors window is displayed:

Figure 6-13: Monitors



2. In the 'Monitors' list, expand the tree and select the monitor whose value you wish to override.

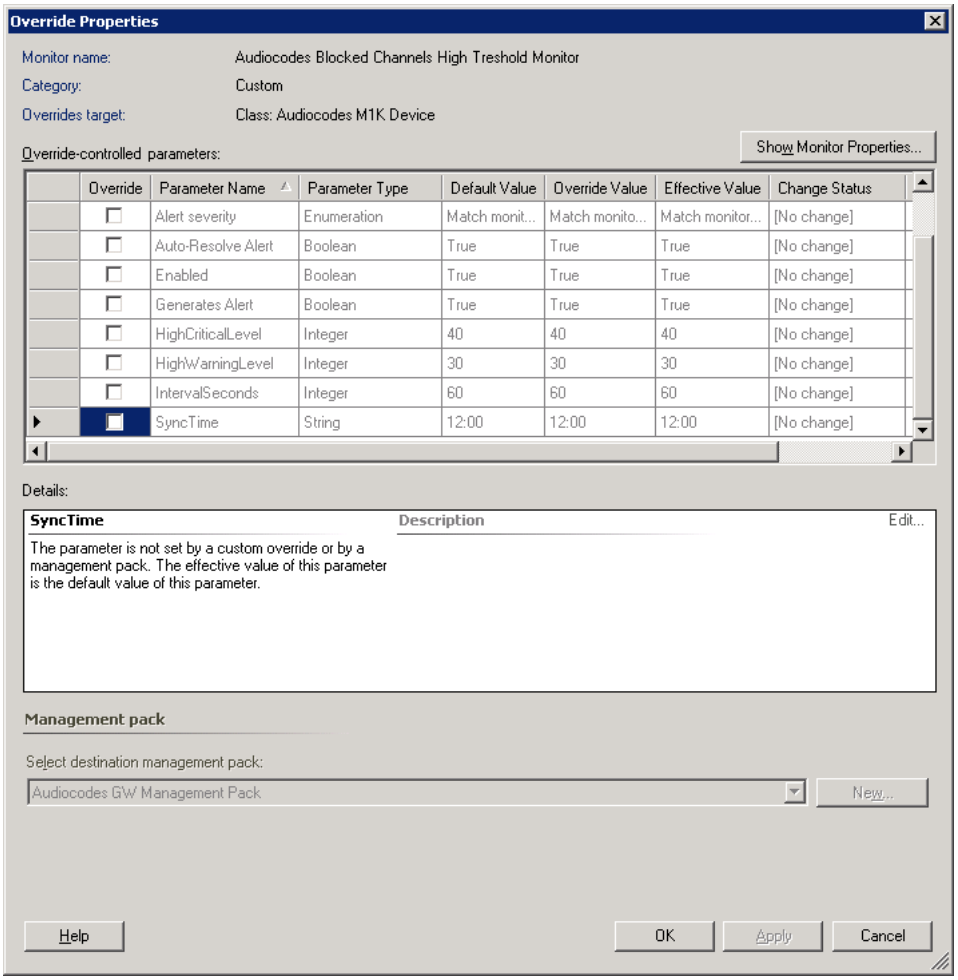
Figure 6-14: Overriding Object Monitors



3. In the Monitor task bar, select **Overrides**, in the displayed Context menu, point to the **Override the monitor** option, and then in displayed pop-up dialog, select the scope affected by the modification e.g. "For a group".

Once you select the scope, the Override Properties window is displayed where you can override specific pre-defined settings:

Figure 6-15: Override Properties-Object Monitors



4. Select the **Override** option adjacent to the 'SyncTime' parameter.
5. In the 'Override Value' field for "SyncTime', set the appropriate value.
6. Click **OK**.

6.3.3 Overriding Discoveries

This section describes how to override specific discovery-related parameters.

The following discoveries have a high level of CPU utilization:

- Gateways
  - Audiocodes <*> Device Discovery – family of discoveries
- Modules
  - Audiocodes <*> Module Secondary Discovery – family of discoveries
  - Audiocodes <*> Module Index Discovery – family of discoveries
- Trunks
  - Audiocodes GW Analog Trunk Secondary Discovery
  - Audiocodes Digital Trunks on <*> Module Initial Discovery – family of discoveries

For Audiocodes <*> Low Threshold Monitor and AudioCodes <*> High Threshold Monitors family of monitors where <*> is the actual monitored parameter name, such as 'TelToIP Failed Calls'.

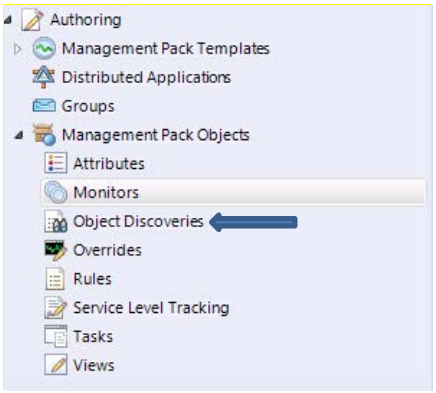
Note:

- Ensure that you filter the view to display only Audiocodes objects items in the right-hand pane. See Section 6.3.1 on page 51.
- Since the number of trunks is much higher than the number of modules and gateways, reducing the frequency of the number of running trunk-related discoveries will have a relatively strong impact on performance (i.e. modifying the 'Sync' parameter as described later in this section).

➢ **To override specific parameters in the discovery process:**

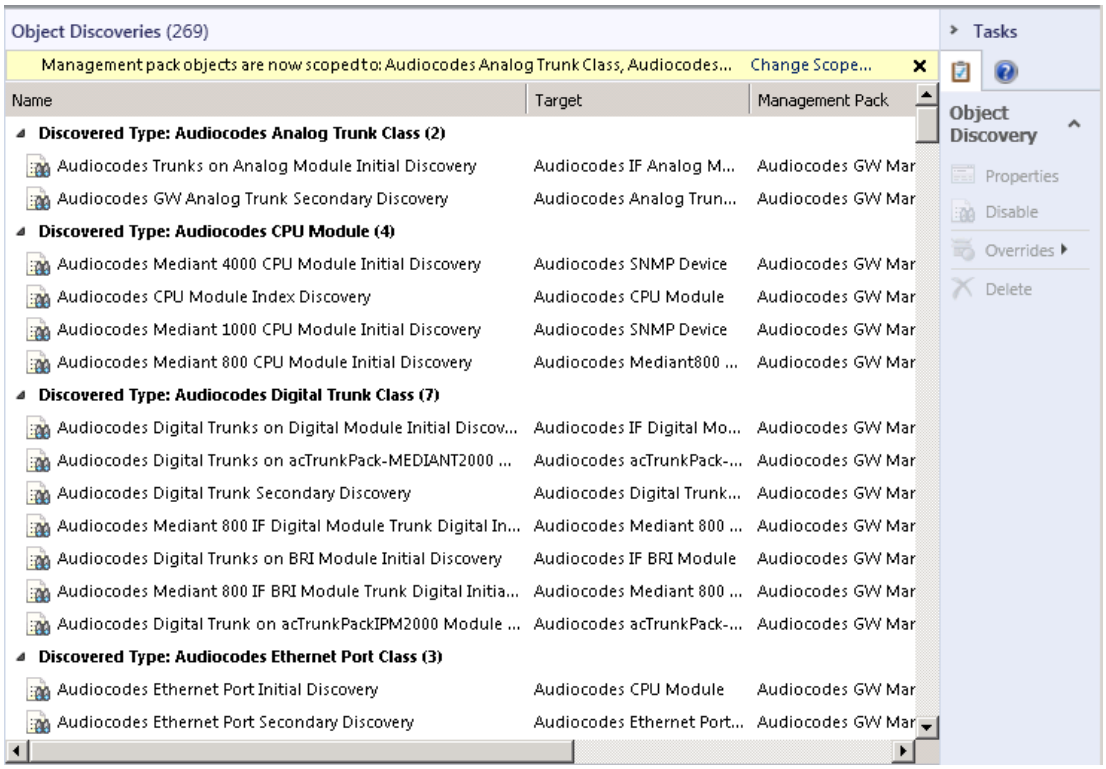
1. In the Authoring pane, select Management Pack Objects > Object Discoveries.

Figure 6-16: Object Discoveries Option



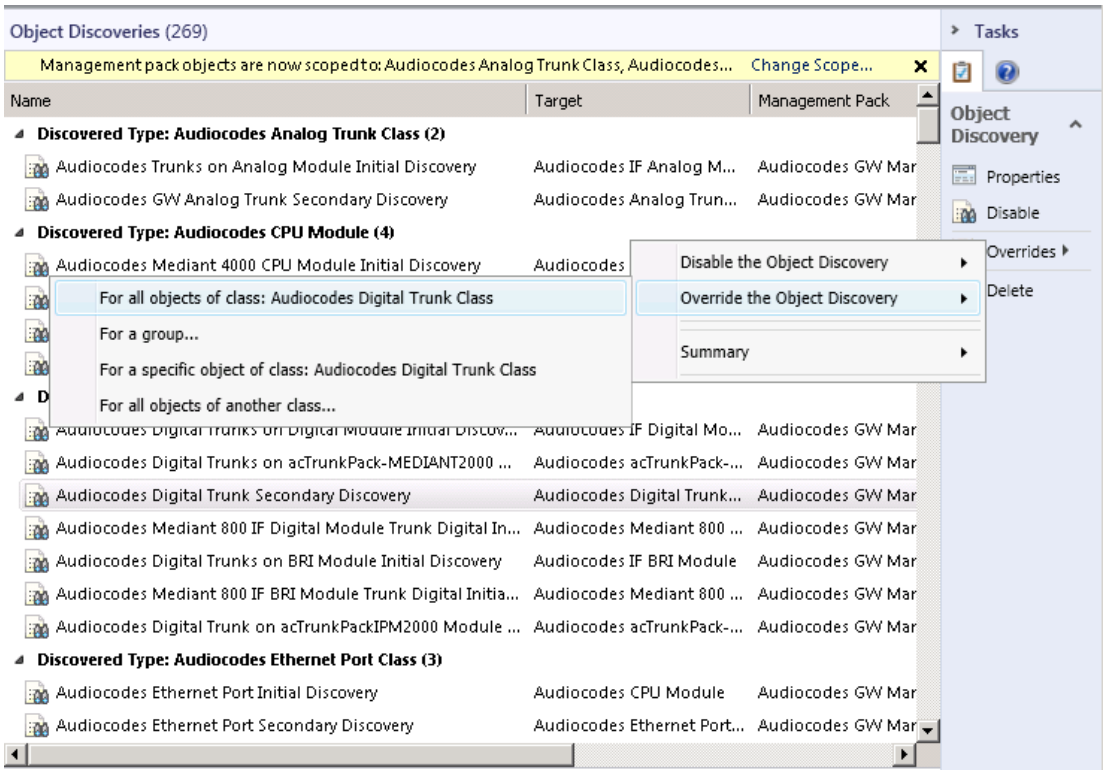
The Object Discoveries window is displayed:

Figure 6-17: Object Discoveries



2. In the 'Discoveries' list, expand the tree and select the Discovery object whose value you wish to override.

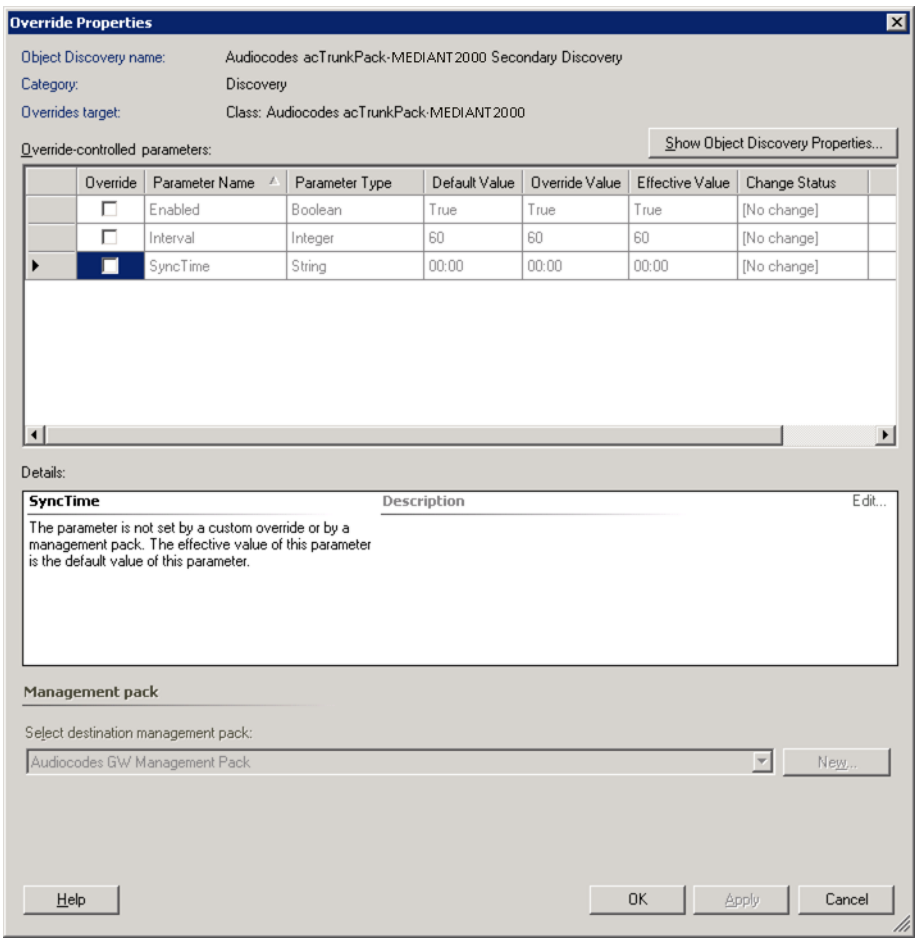
Figure 6-18: Overriding Object Discoveries



3. In the Object Discovery task bar, select **Overrides**, point to **Override the Object Discovery**, and then in the displayed pop-up, select the scope affected by the modification e.g. 'For all objects of another class'.

   The Override Properties window is displayed where you can override specific pre-defined settings:

Figure 6-19: Override Properties-Object Discoveries



4. Select the **Override** option adjacent to the 'SyncTime' parameter.
5. In the 'Override Value' field for 'SyncTime, set the appropriate value.
6. Click **OK**.

6.3.4 Overriding Rules

Rules are responsible for two kind of data collection – counters and service information on channels.

Note: It is recommended to reduce the scope of displayed items so only AudioCodes items are shown in the right-hand pane. See Section 6.3.2 on page 54.

6.3.4.1 Overidding the Counter Polling Interval

Two counters are calculated on the basis of monitored information about the Channels state (not on the basis of existing counters on the device). 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, if you use these counters, this leads to high CPU utilization due to their high polling frequency. 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 6-21, Figure 6-22 and Figure 6-23) - this rule is responsible for querying Channels states from the device and saving information in a pre-defined folder for future use. For this rule, it is recommended to modify both the 'IntervalSeconds' parameter as well as the 'SyncTime parameter'.

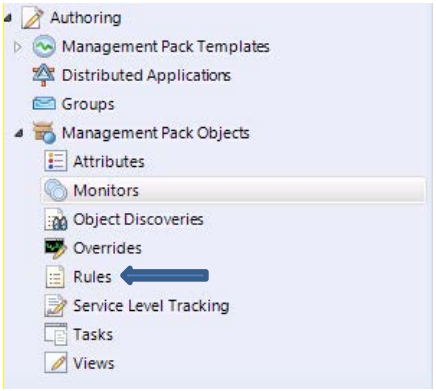
6.3.4.2 Overidding the Counter Sync Time

It is recommended to poll no more than one counter rule at any one point in time (see Figure 6-23 and Figure 6-24 example rule 'Audiocodes Failed Calls Tel2IP Counter Rule') to balance the current CPU load.

➢ **To override rules:**

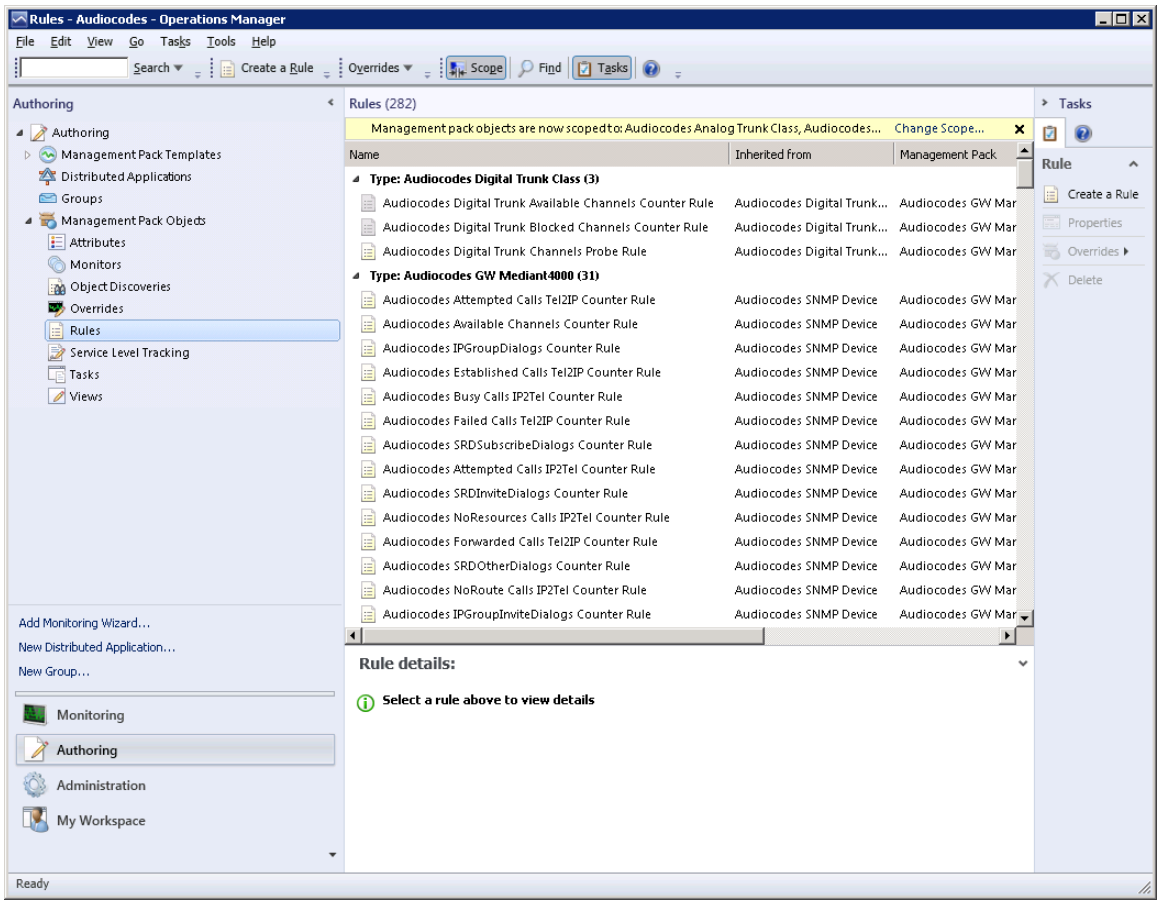
1. In the Authoring pane, select **Management Pack Objects** > **Rules**.

Figure 6-20: Rules Option



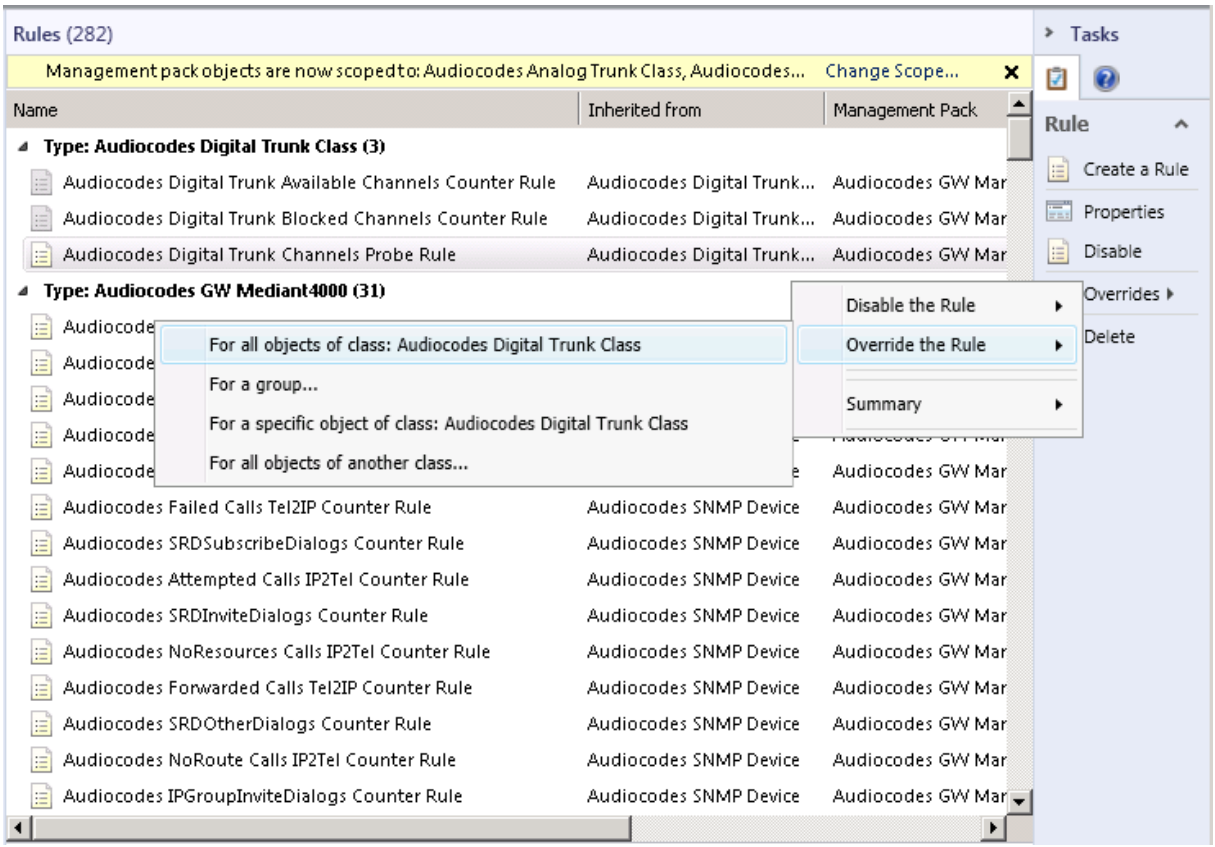
The Rules window is displayed:

Figure 6-21: 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'.

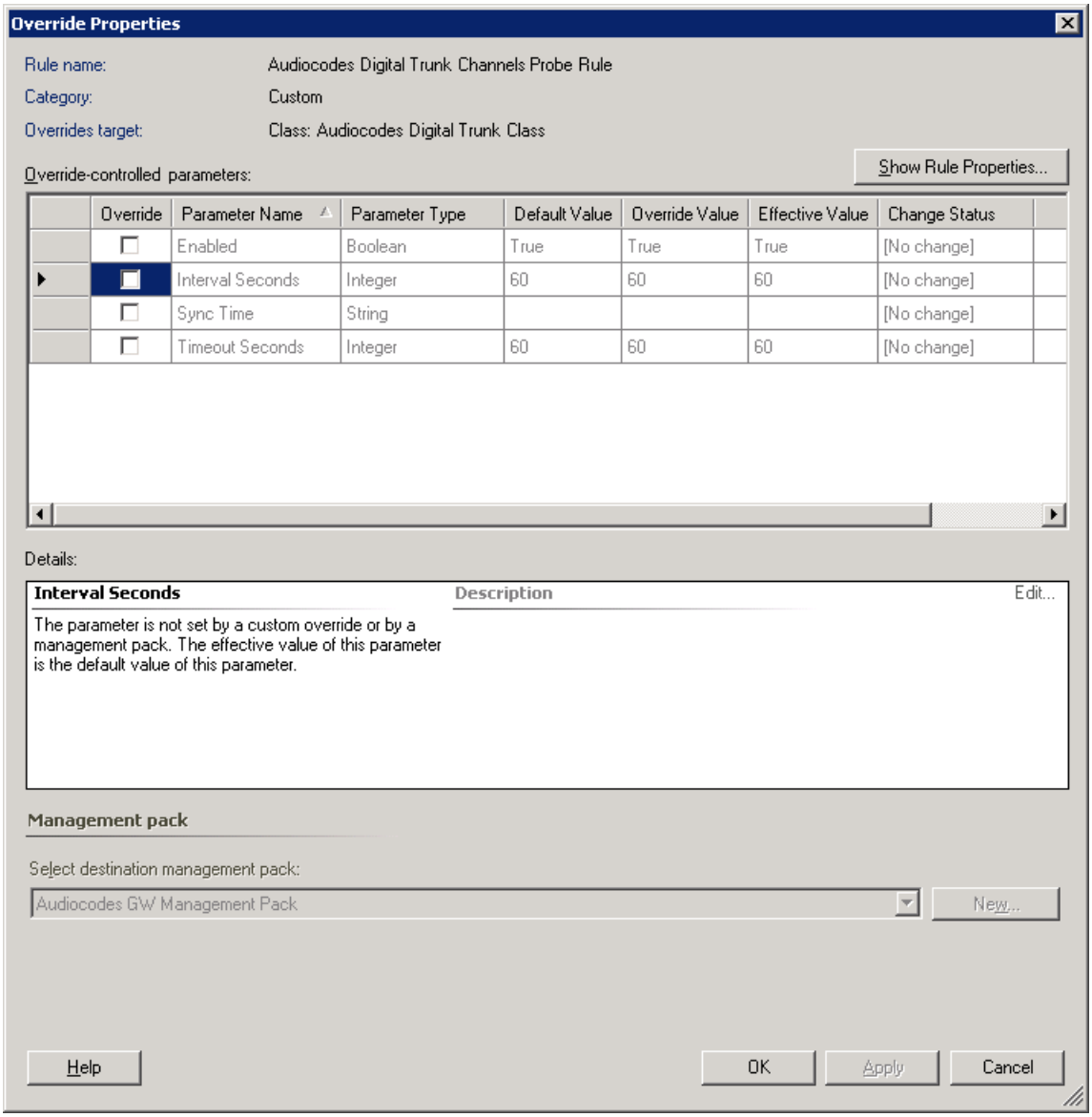
Figure 6-22: Overriding Object Rules-AudioCodes Digital Trunk Channels Probe Rule



3. In the Rule task bar, select **Overrides**, point to **Override the Rule**, and then in the displayed pop-up, select the scope affected by the modification e.g. "For a group".

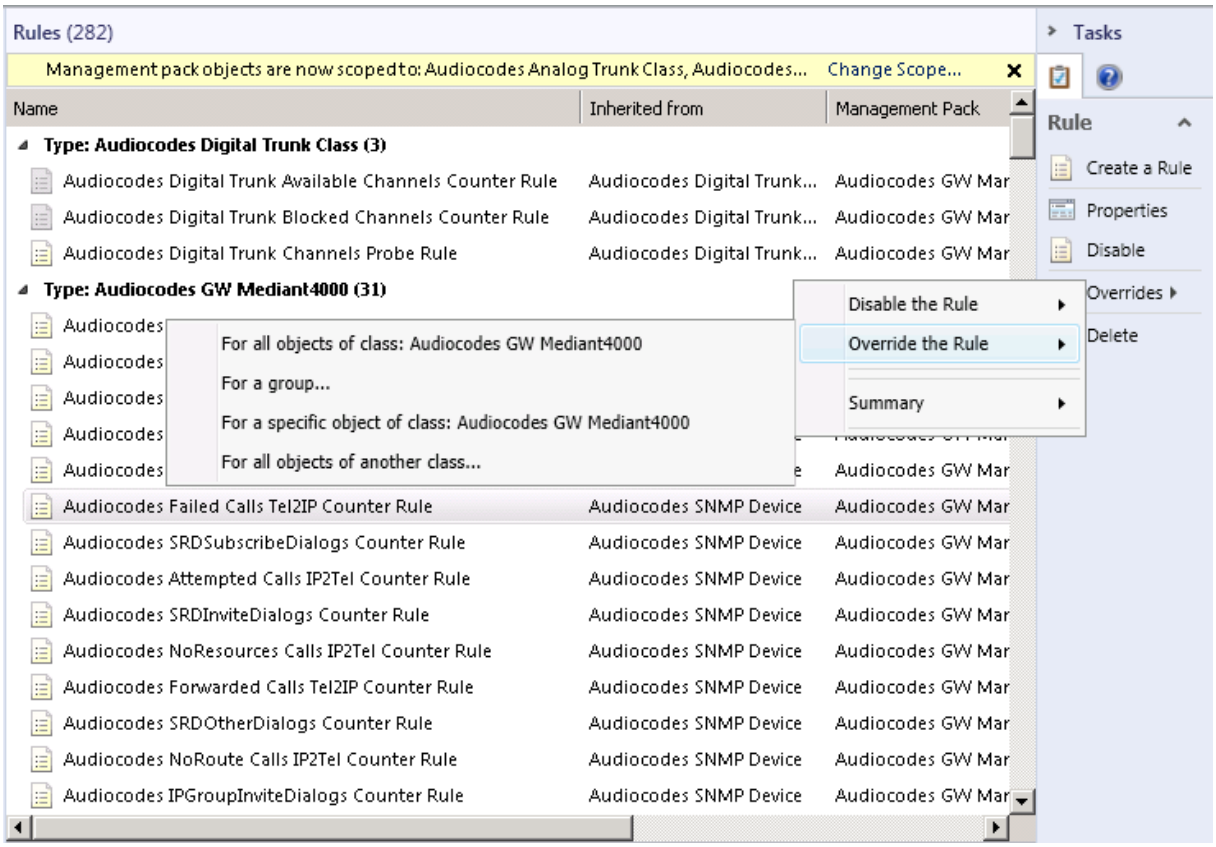
The Override Properties window is displayed where you can override specific pre-defined settings:

Figure 6-23: Override Properties-Audiocodes Digital Trunk Channels Probe Rule



4. Select the **Override** option adjacent to the 'SyncTime' parameter.
5. In the 'Override Value' field for 'SyncTime', set the appropriate value.
6. Select the **Override** option adjacent to the 'IntervalSeconds' parameter.
7. In the 'Override Value' field for 'IntervalSeconds', set 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'.

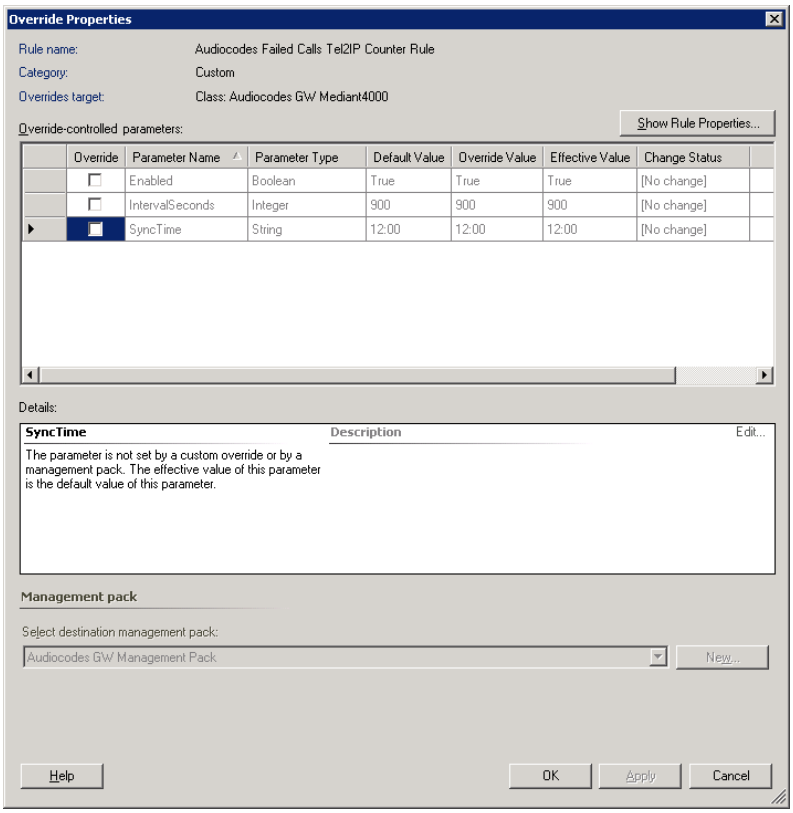
Figure 6-24: Overidding Object Rules-Audiocodes Failed Calls Tel2IP Counter Rule



10. In the Rule task bar, select **Overrides**, point to **Override the Rule**, and then in the displayed pop-up, select the scope affected by the modification e.g. "For a group".

The Override Properties window is displayed where you can override specific pre-defined settings:

Figure 6-25: Override Properties-Audiocodes Failed Calls Tel2IP Counter Rule



11. Select the **Override** option adjacent to the 'SyncTime' parameter.
12. In the 'Override Value' field for 'SyncTime', set the appropriate value.
13. Click **OK**

6.4 Monitoring Health States

This section describes the monitoring of the Health states of the SNMP objects.

6.4.1 Monitoring Gateway SNMP Alarms

The following SNMP traps cause the gateway to become unhealthy, indicating either the 'Warning' or 'Critical' Health State:

- acBoardFatalError
- acBoardOverloadAlarm
- acBoardControllerFailureAlarm
- acDChannelStatus
- acBoardConfigurationError
- acBoardCallResourcesAlarm
- acBoardEvBoardStarted in case when there is no acBoardEvResettingBoard trap within acActiveAlarmTable SNMP table
- acUserInputAlarm
- acPEMAlarm
- acHwFailureAlarm
- acTMInconsistentRemoteAndLocalPLLStatus
- acTMReferenceStatus
- acTMReferenceChange
- acSonetSectionLOFAlarm
- acSonetSectionLOSAlarm
- acSonetLineAISAlarm
- acSonetLineRDIAlarm
- acSonetPathSTSLOPAlarm
- acSonetPathSTSAISAlarm
- acSonetPathSTSRDIAlarm
- acSonetPathUnequippedAlarm
- acSonetPathSignalLabelMismatchAlarm
- acDS3RAIAlarm
- acDS3AISAlarm
- acDS3LOFAlarm
- acDS3LOSAlarm
- acHitlessUpdateStatus
- acHASystemFaultAlarm
- acHASystemConfigMismatchAlarm
- acHASystemSwitchOverAlarm
- acBoardTemperatureAlarm
- acBoardEvResettingBoard
- acFeatureKeyError
- acSAMissingAlarm
- acNTPServerStatusAlarm
- acIPv6ErrorAlarm

- acgwAdminStateChange
- acOperationalStateChange
- acSWUpgradeAlarm
- acActiveAlarmTableOverflow
- acSS7LinkStateChangeAlarm
- acSS7LinkCongestionStateChangeAlarm
- acSS7LinkInhibitStateChangeAlarm
- acSS7LinkSetStateChangeAlarm
- acSS7RouteSetStateChangeAlarm
- acSS7SNSetStateChangeAlarm
- acSS7UalGroupStateChangeAlarm
- acAnalogPortGroundFaultOutOfService
- acBoardWanLinkAlarm
- acLDAPLostConnection
- acOCSPServerStatusAlarm
- acWirelessCellularModemAlarm

For detailed information on the above alarms, see Section B on page 85.

6.4.1.1 Polling Gateway SNMP Objects

The Polling of the gateway SNMP object 'acSysStateGWSeverity' is described in the table below.

Table 6-1:SNMP Gateway Objects Health State

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

6.4.1.2 Monitoring Thresholds

For information on monitoring thresholds, see Section 6.5 on page 71.

6.4.1.3 Aggregated Health State

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

6.4.2 Monitoring Gateway Modules

The following traps cause the Gateway modules (System and Power modules) to become unhealthy, indicating either the 'Warning' or 'Critical' Health State:

- 'acHwFailureAlarm' for system modules
- 'acPowerSupplyAlarm' for Power Supply module
- 'acFanTrayAlarm' for Fan Tray module

6.4.2.1 Polling Gateway Module SNMP Objects

The polling of the SNMP objects for the gateway modules is described in the table below.

Table 6-2:SNMP Gateway Modules Objects Health State

SNMP Object	Object Health State	Health State Indicator
acSysModuleOperationalState (System module)	enable(2)	Healthy
	disable(1)	Critical
acSysPowerSupplySeverity (Power Supply module)	Cleared(1)	Healthy
	Indeterminate(2)	Warning
	minor(4)	Warning
	Major(5)	Critical
	Critical(6)	Critical

6.4.2.2 Dependence Rollup Worst State

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

6.4.3 Monitoring Digital Trunk Module

The following traps cause the Digital Trunk module to become unhealthy with the 'Critical' Health State:

- acTrunksAlarmNearEndLOS
- acTrunksAlarmNearEndLOF
- acTrunksAlarmRcvAIS
- acTrunksAlarmFarEndLOF

6.4.3.1 Digital Trunk SNMP Object Polling

The polling of the SNMP objects for the Digital module is described in the table below.

Table 6-3: Digital Trunk SNMP Polling

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

6.4.4 Monitoring Analog Trunk Module

The following traps cause the analog trunk module to become unhealthy with the 'Critical' Health State:

- acAnalogPortHighTemperature
- acAnalogPortSPIOutOfService

6.4.5 Monitoring Ethernet Module Ports

The following traps cause the Ethernet ports module to become unhealthy with the 'Critical' Health State:

- acBoardEthernetLinkAlarm

6.5 Monitoring Gateway Performance

This section describes the monitoring of gateway performance.

6.5.1 GW Performance View

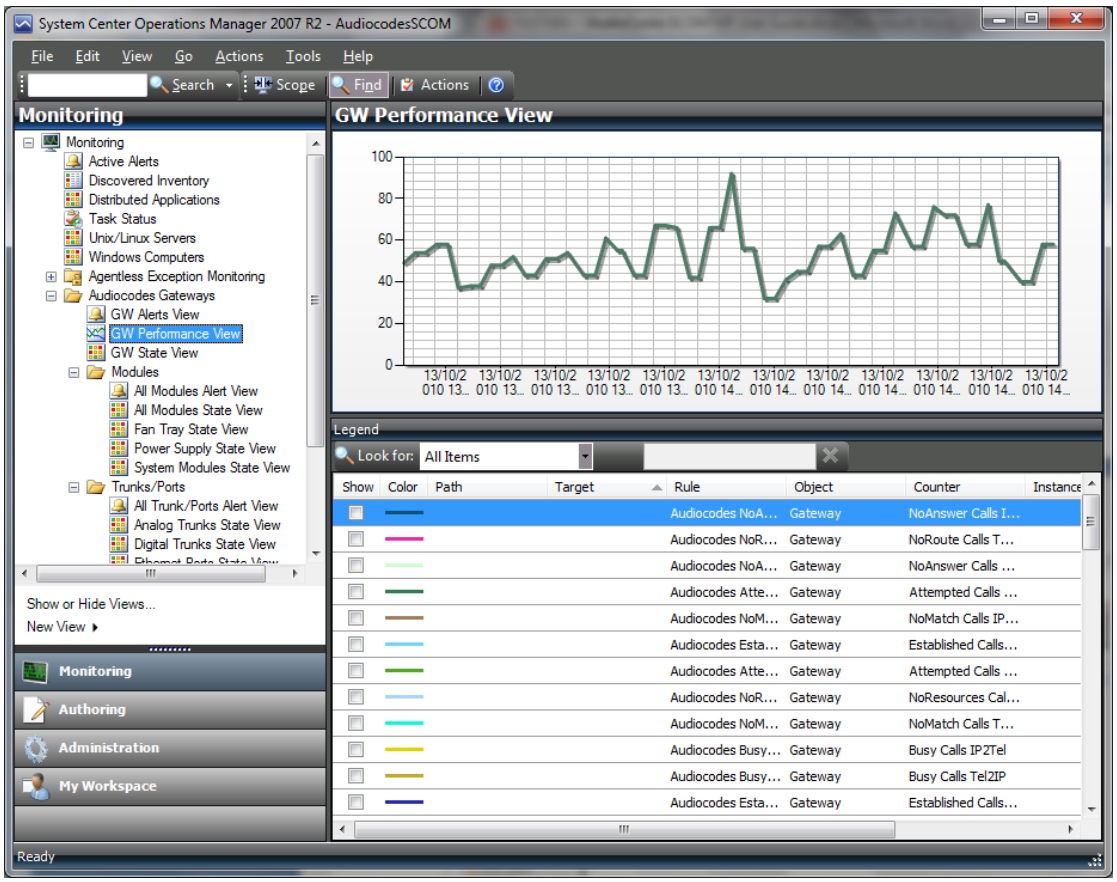
GW Performance View allows you to view gateway performance counters behavior. The following Performance counters are handled by the SCOM Management Pack:

- Attempted Calls Tel2IP
- Attempted Calls IP2Tel
- No Match Calls Tel2IP
- No Match Calls IP2Tel
- Busy Calls Tel2IP
- Busy Calls IP2Tel
- No Answer Calls Tel2IP
- No Answer Calls IP2Tel
- No Route Calls Tel2IP
- No Route Calls IP2Tel
- Fail Calls Tel2IP
- Fail Calls IP2Tel
- Established Calls Tel2IP
- Established Calls IP2Tel
- No Resources Calls Tel2IP
- No Resources Calls IP2Tel
- Forwarded Calls Tel2IP
- Forwarded Calls IP2Tel
- Blocked Channels
- Available Channels

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, the user 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 every one minute. A Graph can be refreshed manually (F5) or automatically.

Figure 6-26: GW Performance View



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

For details on the specific performance monitoring counters, see Section C on page 115.

6.6 Running Tasks

This section describes how to perform various tasks.

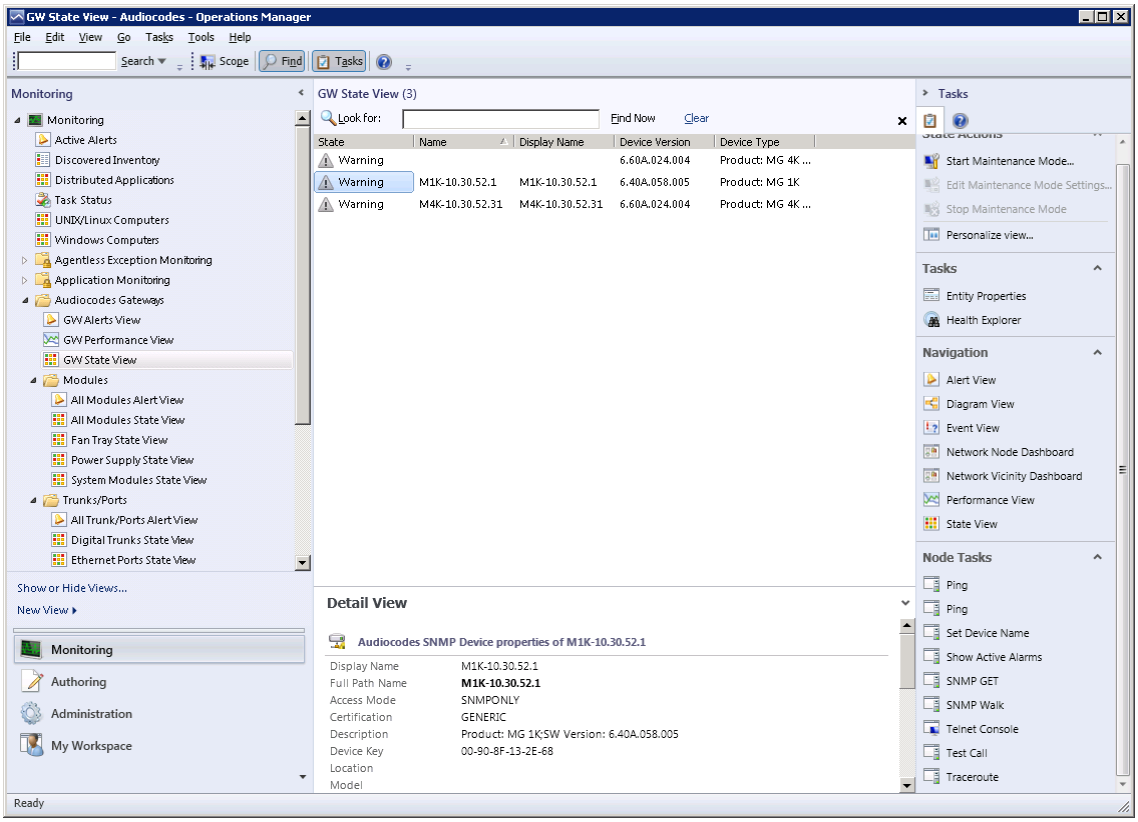
6.6.1 Pinging AudioCodes Device

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 5.1 on page 29) and select the required gateway.
2. Do one of the following:
   a. In the Node Tasks pane, left-click the **Ping** task.

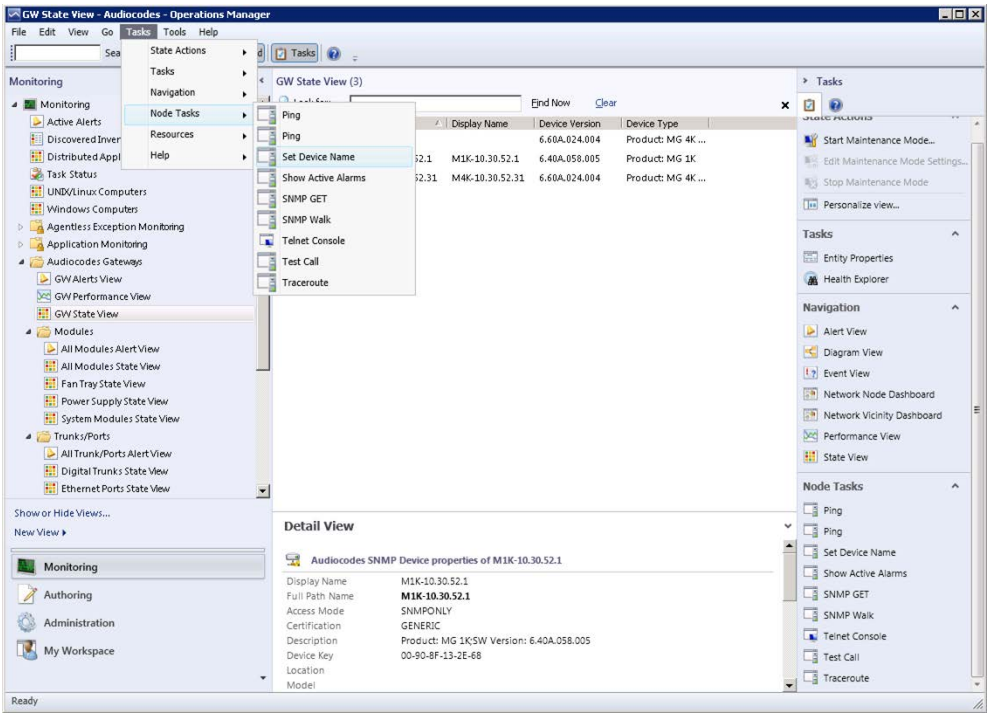
Figure 6-27: Node Tasks Pane



OR

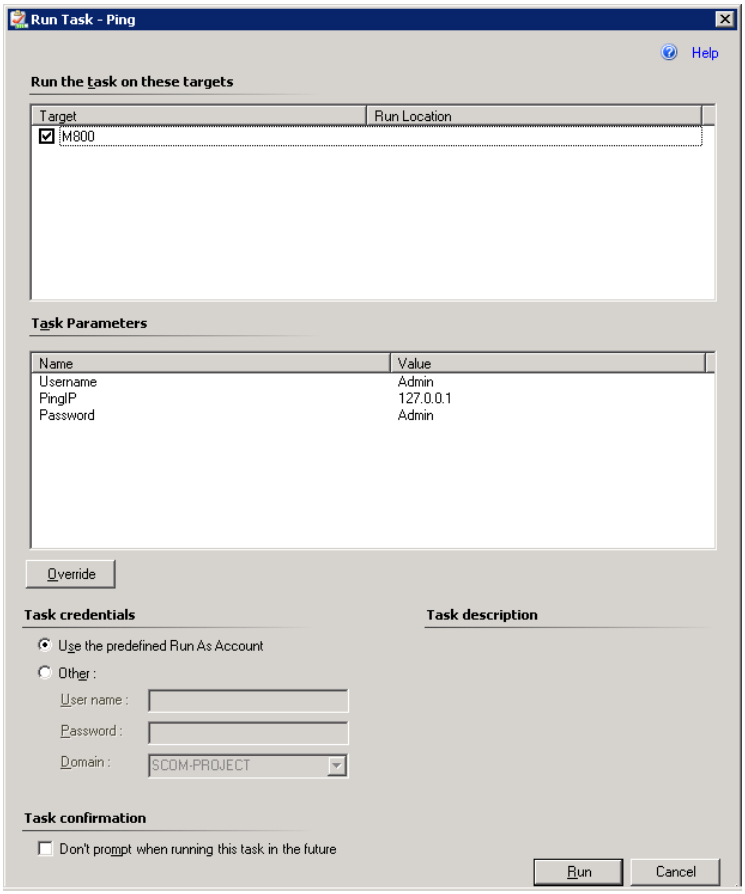
b. In the Main Menu, choose **Tasks** > **Node Tasks** > **Ping**.

Figure 6-28: Tasks Menu



The Ping Run Task window is displayed:

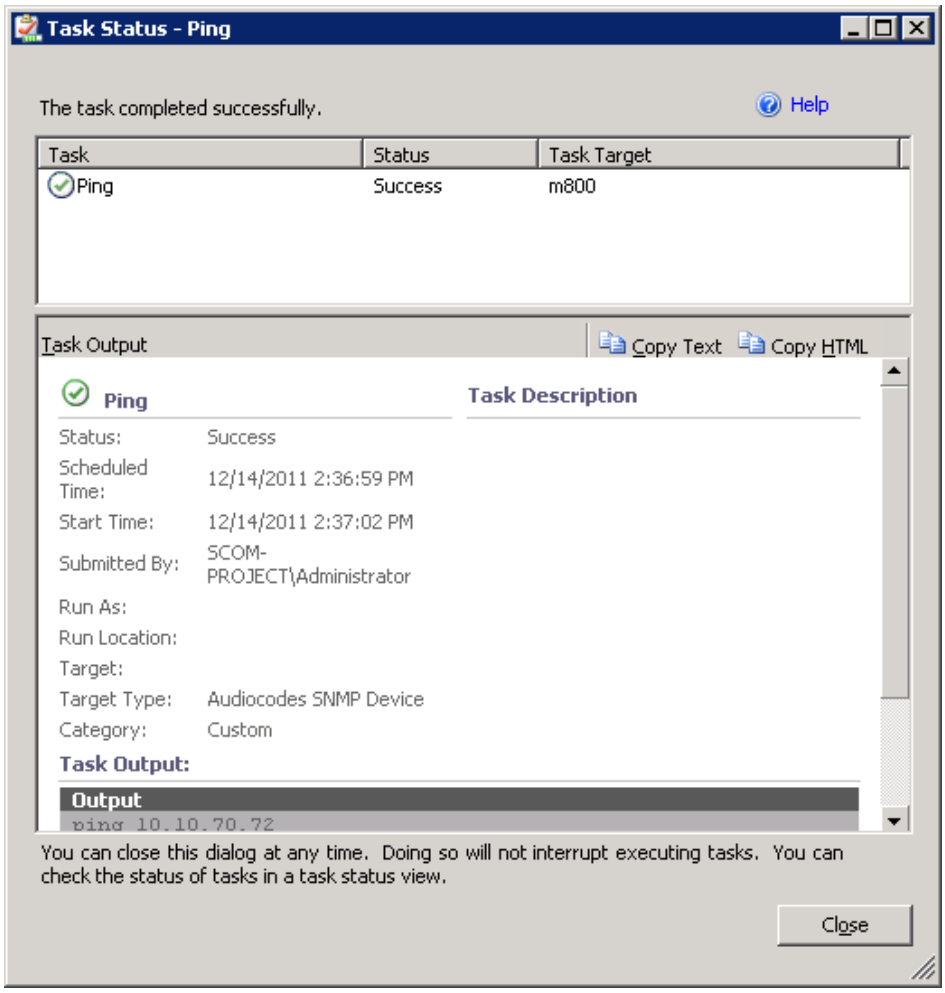
Figure 6-29: Run Task-Ping



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 6-29), the next time the Ping task is run immediately without the ability 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 and Device Name.
   c. Click the **Override** button.
4. In the Run Task window, click the **Run** button; the Task Status – Ping window is displayed:

Figure 6-30: Task Status-Ping



This window contains the Task execution status and output details.

6.6.2 Displaying Active Alarms

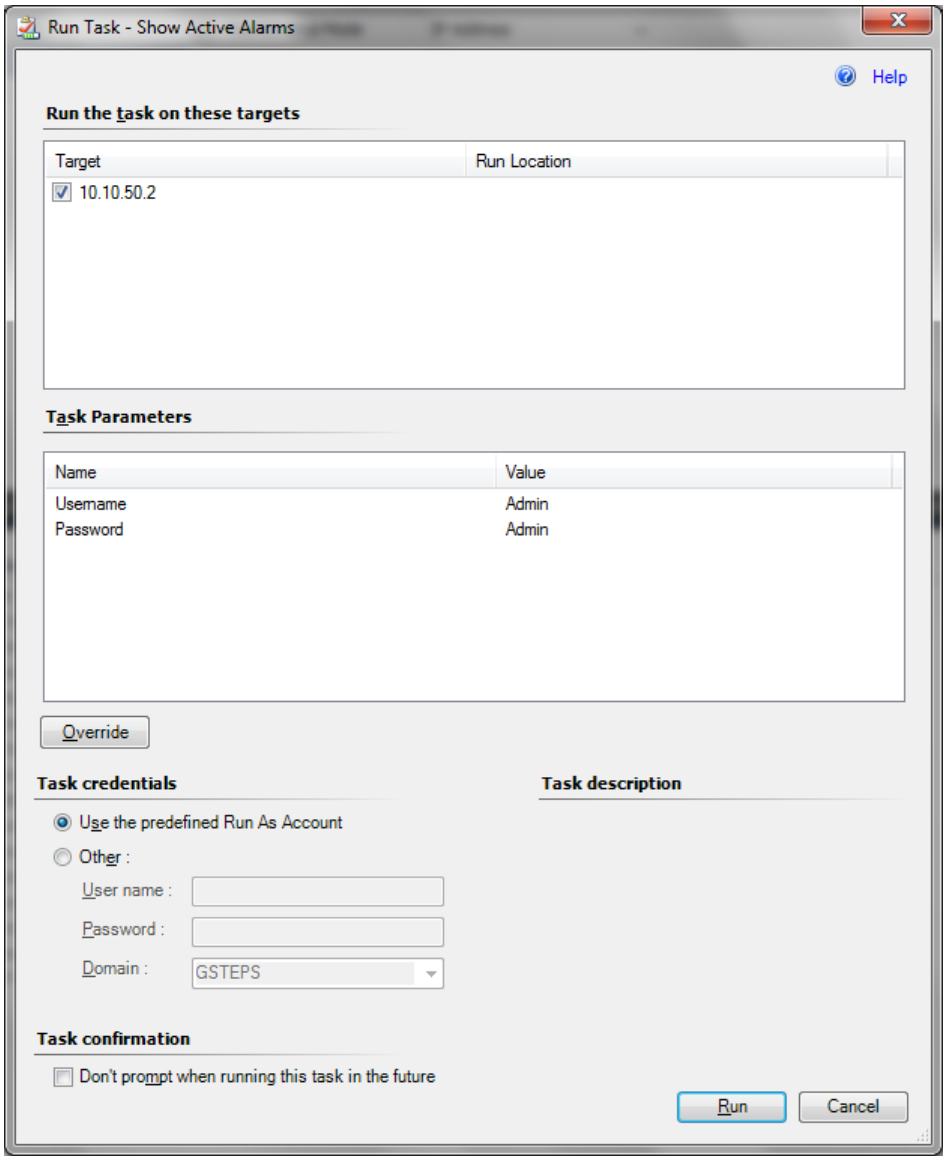
This task describes how to display the active alarms in the 'acActiveAlrmTable' table.

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

1. Open the GW State View (see Section 5.1 on page 29) 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:

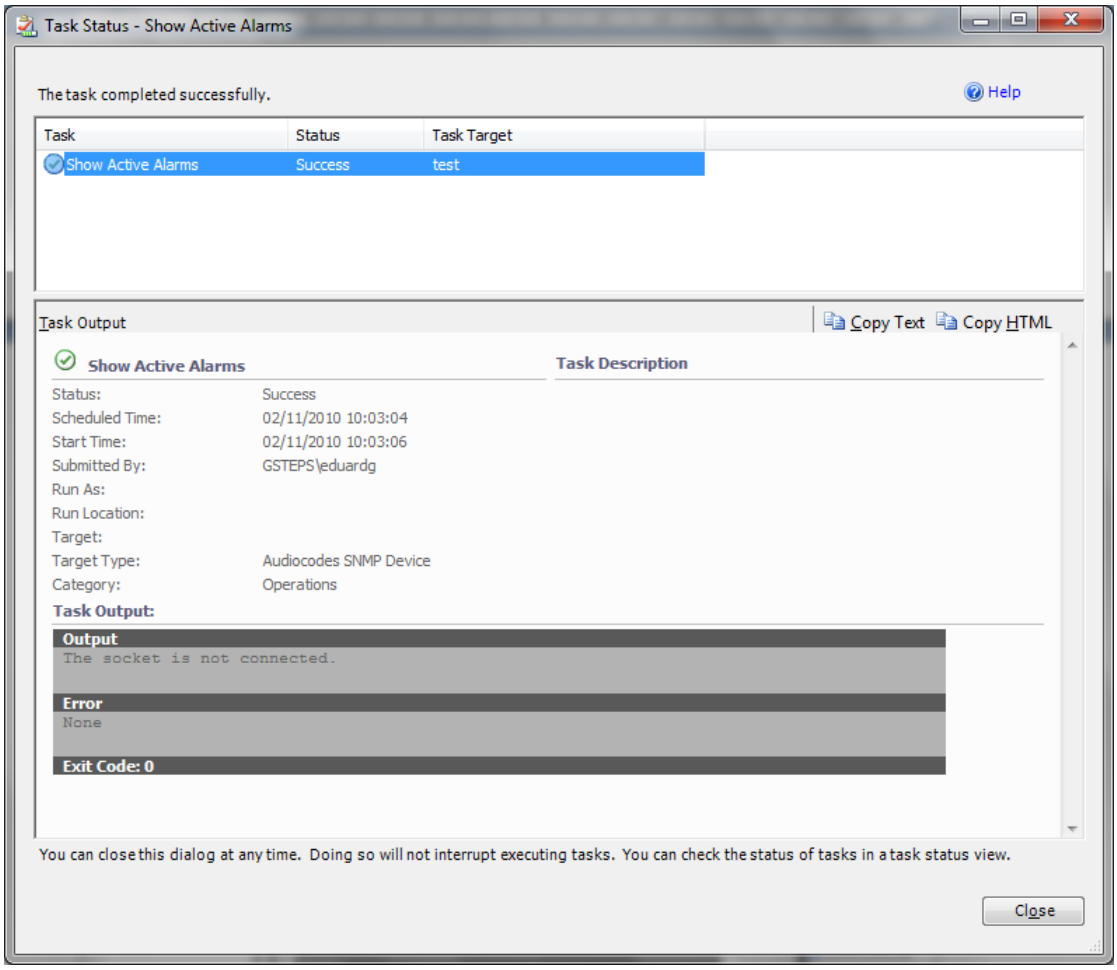
Figure 6-31: Run Task-Show Active Alarms



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 6-31), 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 6-32: Task Status-Show Active Alarms



This window contains the Task execution status and output details.

6.6.3 Setting Device Display Name

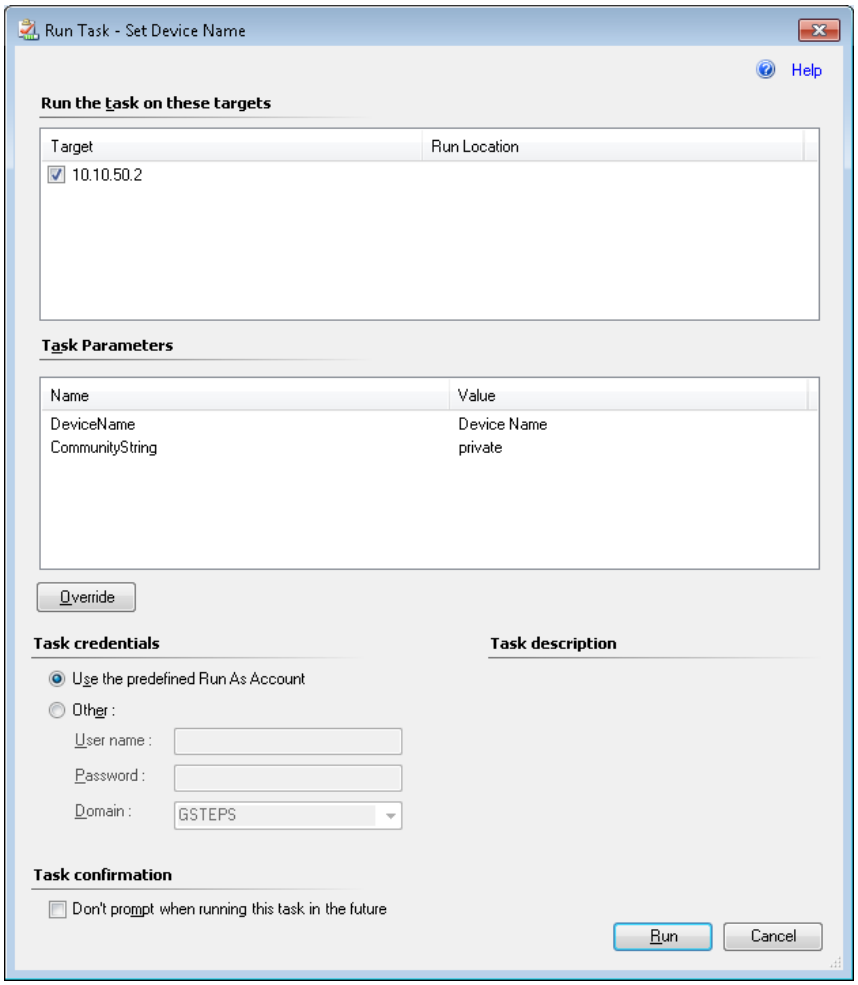
This task describes how to change the device Display Name in the GW State View table.

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

1. Open the GW State View (see Section 5.1 on page 29) 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:

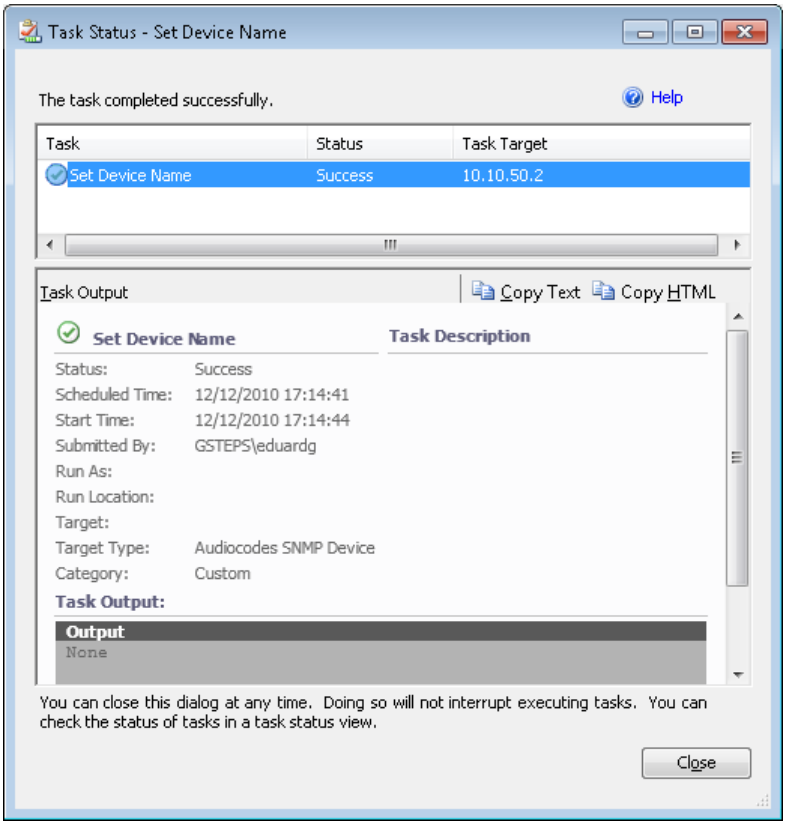
Figure 6-33: Set Device Name



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 6-31), 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 6-34: Task Status-Set Device Name



This window contains the Task execution status and output details.

6.6.4 Testing Call from Gateway

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

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

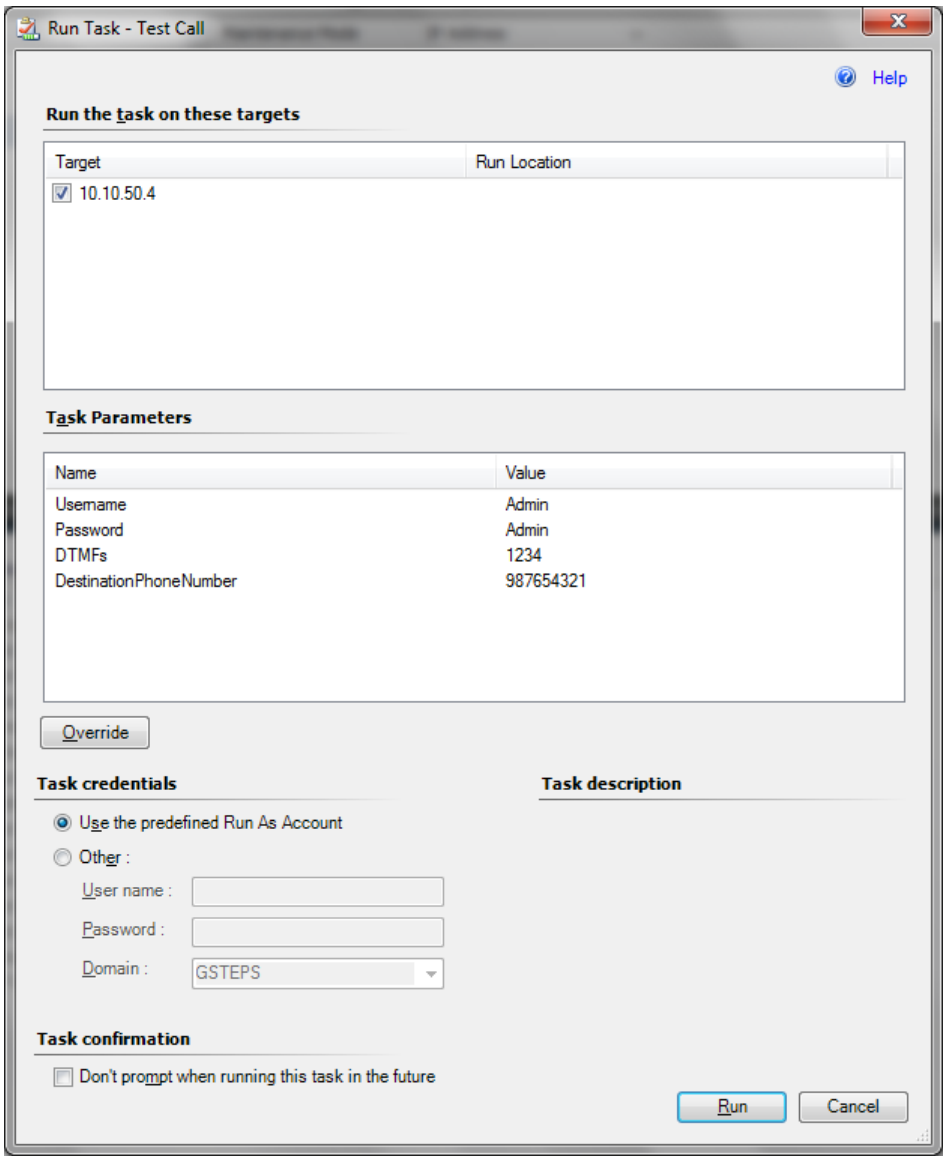
1. Open the GW State View (see Section 5.1 on page 29) and select the required gateway.
2. Do one of the following:
   a. In the Node Tasks pane, left-click the **Test Call** task.

   OR

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

   The Test Call Run Task window is displayed:

Figure 6-35: Run Task – Test Call



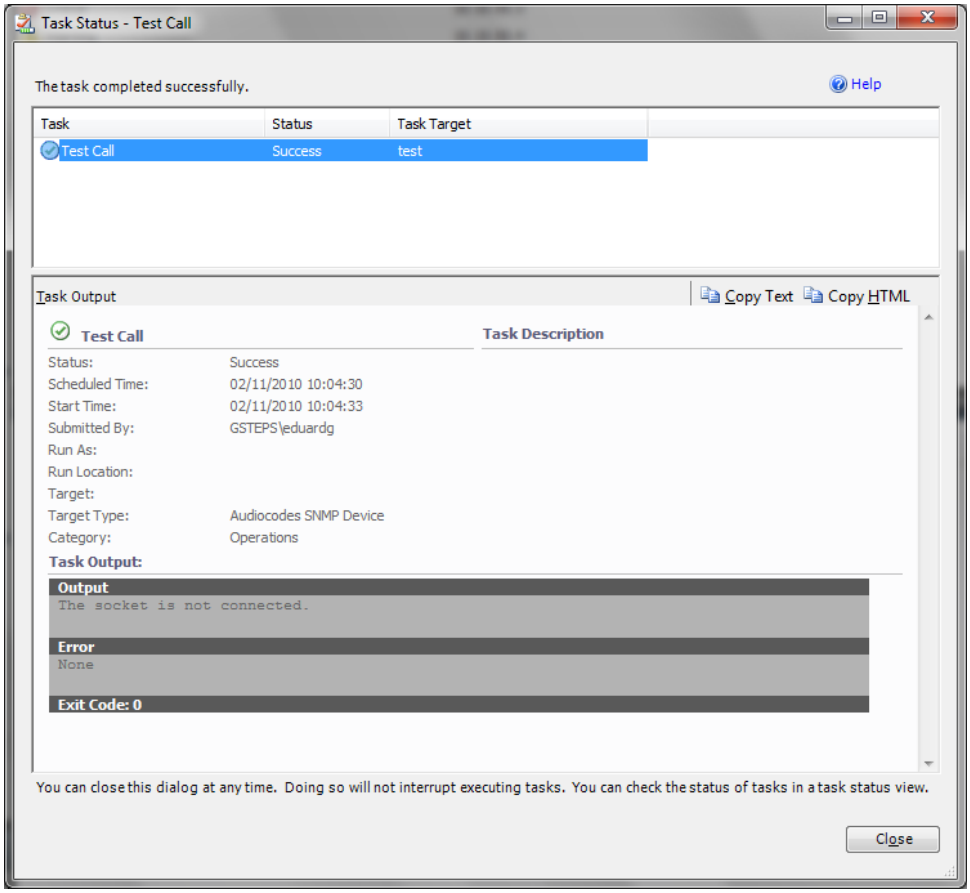
Note: If you check the checkbox "Don't prompt when running this task in the future" in Task confirmation of the task configuration window (see Figure 6-36 below), the next time you run the 'Test Call' task, it is run immediately without you being able to change the task configuration.

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 6-36: Task Status-Test Call



This window contains the Task execution status and output details.

Reader's Notes

A Updating Gateway Health State Manually

Some alerts can't be cleared automatically because the device does not support trap clearing (in the case of the AudioCodes Management Pack, this refers to the 'GW Unplanned Restart Alert' for trap 'acBoardEvBoardStarted'). In such cases, the SCOM supports the manual closing of the alert.

➢ **To update the health state manually:**

1. Right click the required gateway.
2. Select menu item **Open** > **Health Explorer for <GW IP>**.
3. Select the alert-related monitor.
4. In the Health Explorer window toolbar, click the **Reset Health** button.

Reader's Notes

B SNMP Traps

This section provides a reference to the SNMP traps supported by the AudioCodes Management Pack

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 1000B and MediaPack, *n* always equals to 1.

This section describes the Proprietary alarms: traps originated by the media gateway and defined in the gateway proprietary MIB.

Each alarm described in this section includes the following information:

Table B-1: Information Included in Each Alarm

Alarm	The alarm name, as it appears in the EMS Alarm Browser.
OID	NOTIFICATION-TYPE OID as it appears in the MIB.
Default Severity	Possible values of severities. This value is displayed from the variable-binding tgTrapGlobalsSeverity.
Alarm Type	Alarm type according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsType.
Alarm Source	Possible values of sources if applicable to a specific alarm. This value is displayed from the variable-binding tgTrapGlobalsSource.
Probable Cause	Alarm probable cause according to ITU X.733 definition. This value is displayed from the variable-binding tgTrapGlobalsProbableCause.
Alarm Text	Textual description of specific problem. This value is displayed from the variable-binding tgTrapGlobalsTextualDescription. The document includes a few examples of the possible values of this field.
Status Changes	The changes in the alarm status once it's severity is identified.
1. Condition:	The conditions upon which the alarm occurs.
Alarm Status:	
Additional Info	Additional information fields provided by MG application, depending on the specific scenario. These values are displayed from tgTrapGlobalsAdditionalInfo1, tgTrapGlobalsAdditionalInfo2 and tgTrapGlobalsAdditionalInfo3. The document includes a few examples of the possible values of this field.
Corrective Action	Possible corrective action when applicable.

B.1 List of Alarms and Traps

Table B-2: acBoardFatalError

Alarm	acBoardFatalError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Default Severity	Critical
Alarm Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable (56)
Alarm Text	Board Fatal Error: <text>
1. Condition	Any fatal error
Alarm Status	Critical
<text> Value	A run-time specific string describing the fatal error
2. Condition	After fatal error
Alarm Status	Status stays critical until reboot. A clear trap is not sent.
Corrective Action	Capture the alarm information and the Syslog clause, if active. Contact your first-level support group. The support group will likely want to collect additional data from the device and perform a reset.

Table B-3: acBoardOverloadAlarm

Alarm:	acBoardOverloadAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.11
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	softwareError (46)
Alarm Text	Board overload alarm
1. Condition	An overload condition exists in one or more of the system components.
Alarm Status	Major
2. Condition	The overload condition passed
Alarm Status	Cleared

Table B-4: acBoardControllerFailureAlarm

Alarm:	acBoardControllerFailureAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.9
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	softwareError (46)
Alarm Text	Controller failure alarm
1. Condition	Proxy has not been found or physical network link is up or down ("BusyOut Trunk/Line n Link failure").
Alarm Status	Major
Additional Info	Proxy not found. Use internal routing or Proxy lost. looking for another Proxy
2. Condition	Proxy is found. The clear message includes the IP address of this Proxy.
Alarm Status	Cleared

Table B-5: AcDChannelStatus

Trap	acDChannelStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.37
Default 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).
1. Condition	D-Channel un-established.
Trap Status	Trap is sent with the severity of Minor.
2. Condition	D-Channel established.
Trap Status	Trap is sent with the severity of Cleared.

Table B-6: acBoardConfigurationError

Alarm	acBoardConfigurationError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2
Default Severity	Critical
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable (56)
Alarm Text	Board Config Error: <text>
Status Changes	
1. Condition	A configuration error was detected
Alarm Status	critical
<text> Value	A run-time specific string describing the configuration error.
2. Condition	After configuration error
Alarm Status	Status stays critical until reboot. A clear trap is not sent.
Corrective Action	Inspect the run-time specific string to determine the nature of the configuration error. Fix the configuration error using the appropriate tool: Web interface, EMS, or *ini* file. Save the configuration and if necessary reset the device.

Table B-7: acBoardCallResourcesAlarm

Alarm	acBoardCallResourcesAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.8
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	softwareError (46)
Alarm Text	Call resources alarm
Status Changes	
1. Condition	Percentage of busy channels exceeds the predefined RAI high threshold.
Alarm Status	Major
Note	To enable this alarm the RAI mechanism must be activated (EnableRAI = 1).
2. Condition	Percentage of busy channels falls below the predefined RAI low threshold.
Alarm Status	Cleared

Table B-8: acBoardEvBoardStarted

Trap Name	acBoardEvBoardStarted
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
Severity	cleared
Event Type	equipmentAlarm
Probable Cause	Other(0)
Alarm Text	Initialization Ended
Note	This is the AudioCodes Enterprise application cold start trap.

Table B-9: acUserInputAlarm

Alarm	acUserInputAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.36
Default Severity	Critical
Source Varbind Text	Chassis#0
Event Type	equipmentAlarm
Probable Cause	inputDeviceError
Alarm Text	User input Alarm. User's Input-Alarm turn on.
Status Changes	
1. Condition	Input dry contact is short circuited.
Alarm Status	Critical
2. Condition	Input dry contact circuit is reopened.
Alarm Status	Cleared

Table B-10: acPEMAlarm

Alarm	acPEMAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.31
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 Text	PEM Module Alarm.
Status Changes	
1. Condition	The HA (High Availability) feature is active (applicable only to Mediant 3000) and one of the PEM units is missing (PEM – Power Entry Module)
Alarm status	Critical
<text> Value	PEM card is missing.
2. Condition	PEM card is placed and both DC wires are in.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000.

Table B-11: 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 Text	Module Alarm: <text>
Status Changes	
1. Condition	The module is faulty or has been removed incorrectly.
Alarm Status	Critical
<text> Value	Faulty IF-Module
Note	This alarm is not cleared. The device must be restarted to clear this alarm.
2. Condition	Module mismatch - module and CPU board mismatch.
Alarm Status	Major
<text> Value	IF-Module Mismatch
Note:	This alarm is not cleared. The device must be restarted to clear this alarm.

Note: This alarm is only applicable for the Mediant 1000B.

Table B-12: acTMInconsistentRemoteAndLocalPLLStatus Alarm

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

Note: This alarm is applicable only for the Mediant 3000.

Table B-13: acTMReferenceStatus Alarm

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

Note: This alarm is applicable only for the Mediant 3000.

Table B-14: acTMReferenceChange Alarm

Alarm	acTMReferenceChange
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.58
Default Severity	Indeterminate
Source Varbind Text	Chassis#0/TimingManager#0
Event Type	
Probable Cause	
Alarm Text	Timing Manager
Status Changes	
1. Condition	Log is sent on PLL status change.

Note: This alarm is applicable only for the Mediant 3000.

Table B-15: 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 Text	SONET-Section LOF.
Status Changes	
1. Condition	LOF condition is present on SONET no.n
Alarm Status	Critical
<text> Value	LOF
Note	The sonetSectionCurrentStatus field in the sonetSectionCurrentTable will have a value sonetSectionLOF (4).
2. Condition	LOF condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-16: 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 Text	SONET-Section LOS.
Status Changes	
1. Condition	LOS condition is present on SONET no #n
Alarm Status	Critical
<text> Value	LOS
Note:	The sonetSectionCurrentStatus field in the sonetSectionCurrentTable will have a value sonetSectionLOS (2).
2. Condition	AIS condition is present (LOS condition is not present)
Alarm Status	Critical
3. Condition	LOS condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-17: 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 Text	SONET-Line AIS.
Status Changes	
1. Condition	AIS condition is present on SONET-Line #n.
Alarm Status	Critical
<text> Value	AIS
Note:	The sonetLineCurrentStatus field in the sonetLineCurrentTable will have a value sonetLineAIS (2).
2. Condition	AIS condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-18: 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 Text	SONET-Line RDI.
Status Changes	
1. Condition	RDI condition is present on SONET-Line #n.
Alarm Status	Critical
<text> Value	RDI
Note	The sonetLineCurrentStatus field in the sonetLineCurrentTable will have a value sonetLineRDI (4).
2. Condition	RDI condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-19: 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 Text	SONET Path STS AIS alarm.
Status Changes	
1. Condition	LOP condition is present on Path #n.
Alarm Status	Critical
<text> Value	LOP
Note	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSTSLOP (2).
2. Condition	LOP condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-20: 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 Text	SONET Path STS AIS alarm.
Status Changes	
1. Condition	AIS condition is present on Path #n.
Alarm Status	Critical
<text> Value	AIS
Note	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSTSAIS(4).
2. Condition	AIS condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-21: 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 Text	SONET Path STS RDI alarm.
Status Changes	
1. Condition	RDI condition is present on Path #n.
Alarm Status	Critical
<text> Value	RDI
Note	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSTSRDI(8).
2. Condition	RDI condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-22: 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 Text	SONET Path Unequipped alarm.
Status Changes	
1. Condition	Unequipped condition is present on Path #n.
Alarm Status	Critical
<text> Value	Unequipped
Note:	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathUnequipped(16).
2. Condition	Unequipped condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-23: 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 Text	SONET Path Signal Label Mismatch alarm.
Status Changes	
1. Condition	Signal Label Mismatch condition is present on Path #n.
Alarm Status	Critical
<text> Value	SignalLabelMismatch
Note	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSignalLabelMismatch(32).
2. Condition	Signal Label Mismatch condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-24: 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

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-25: 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 Text	DS3 RAI alarm.
Status Changes	
1. Condition	RAI condition is present on DS3-Line #n.
Alarm Status	Critical
<text> Value	RAI
Note	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3RcvRAIFailure(2).
2. Condition	RIA condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-26: 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 Text	DS3 AIS alarm.
Status Changes	
1. Condition	AIS condition is present on DS3-Line #n.
Alarm Status	Critical
<text> Value	AIS
Note	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3RcvAIS(8).
2. Condition	AIS condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-27: 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 Text	DS3 LOF alarm.
Status Changes	
1. Condition	LOF condition is present on DS3-Line #n.
Alarm Status	Critical
<text> Value	LOF
Note	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3LOF (32).
2. Condition	LOF condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-28: 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 Text	DS3 LOS alarm.
Status Changes	
1. Condition	LOS condition is present on DS3-Line #n.
Alarm Status	Critical
<text> Value	LOS
Note	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3LOS (64).
2. Condition	LOS condition is not present.
Alarm Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-29: 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

Note: This alarm is only applicable for the Mediant 3000 with TP-6310 blade.

Table B-30: 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 Text	Hitless Update Event
Status Changes	
Condition	A Notification trap that is sent out at the beginning and the end of a Hitless SW update. Failure during the process will also instigate the trap. May include the following information: Hitless: start SW upgrade. Hitless: Stream read error, aborting CMP file processing. Hitless: Invalid cmp file - missing Ver parameter. Hitless fail: Hitless SW upgrade is not supported under version 5.2. Hitless fail: SW ver stream name too long. Hitless fail: Invalid cmp file - missing UPG parameter. Hitless fail: Hitless SW upgrade not supported. Hitless fail: Communication with redundant module failed. Hitless: SW upgrade ended successfully.
Alarm Status	Indeterminate
Corrective Action	

Note: This alarm is only applicable for the Mediant 3000.

Table B-31: acHASystemFaultAlarm

Trap:	acHASystemFaultAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.33
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
Trap Text	No HA! <text>
Status Changes	
1. Condition	HA feature is active but the system is not working in HA mode.
Trap Status	Critical

Trap:	acHASystemFaultAlarm
<text> Value	There are many possible values for the text: Fatal exception error TCPIP exception error Network processor exception error SW WD exception error HW WD exception error SAT device is missing SAT device error DSP error BIT tests error PSTN stack error Keep Alive error Software upgrade Manual switch over Manual reset Board removal Can't read slot number TER misplaced HW fault. TER in slot 2 or 3 is missing HW fault. TER has old version or is not functional HW fault. invalid TER Type HW fault. invalid TER active/redundant state HW fault. Error reading GbE state Redundant module is missing Unable to sync SW versions Redundant is not connecting Redundant is not reconnecting after deliberate restart No Ethernet Link in redundant module SA module faulty or missing
2. Condition	HA feature is active and the redundant module is in start up mode and hasn't connected yet.
Trap Status	Minor
<text> Value	Waiting for redundant to connect
3. Condition	HA system is active.
Trap Status	Cleared

Note: This alarm is only applicable for the Mediant 3000 HA.

Table B-32: acHASystemConfigMismatchAlarm

Trap	acHASystemConfigMismatchAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34
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
Trap Text	Configuration mismatch in the system.
Status Changes	
1. Condition	HA feature is active: ▪ License Keys of Active and Redundant modules are different. ▪ The Active module was unable to pass on to the Redundant module the License Key. ▪ License key of the Redundant module is invalid.

Trap	acHASystemConfigMismatchAlarm
Trap Status	Major
<text> Value	▪ Active and Redundant modules have different feature keys. ▪ Fail to update the redundant with feature key. ▪ Feature key did not update in redundant module.
2. Condition	Successful License Key update.
Trap Status	Cleared
<text> Value	The feature key was successfully updated in the redundant module

Note: This alarm is only applicable for the Mediant 3000 HA.

Table B-33: acHASystemSwitchOverAlarm

Trap	acHASystemSwitchOverAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35
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
Trap Text	Switch-over: <text>
Status Changes	
1. Condition	A switch over from the active to the redundant blade has occurred.
Trap Status	Critical
<text> Value	See the acHASystemFaultAlarm table above.
2. Condition	10 seconds have passed since the switch over.
Trap Status	cleared

Note: This alarm is only applicable for the Mediant 3000 HA.

Table B-34: acBoardEthernetLinkAlarm

Trap	acBoardEthernetLinkAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Default Severity	Critical
Source Varbind Text	Chassis#0/Module#<m>/EthernetLink#0, where *m* is the blade's slot number
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable (56)
Trap Text	Ethernet link alarm: <text>
Status Changes	

Trap	acBoardEthernetLinkAlarm
1. Condition	Fault on single interface of the Active module.
Trap Status	Major
<text> Value	Redundant link (physical link n) is down
2. Condition	Fault on both interfaces
Trap Status	Critical
<text> Value	No Ethernet link
3. Condition	Fault on single interface of the Redundant module.
Trap Status	Major
<text> Value	Redundant link in the redundant module (physical link n) is down
4. Condition	Both interfaces are operational
Trap Status	Cleared
Corrective Action	Ensure that both Ethernet cables are plugged into the back of the system. Inspect the system's Ethernet link lights to determine which interface is failing. Reconnect the cable or fix the network problem
Note:	The alarm behaves differently when coming from the redundant or the active modules of an 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.

Note: This alarm is only applicable for the Mediant 3000 HA.

Table B-35: acBoardTemperatureAlarm

Alarm	acBoardTemperatureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3
Default Severity	Critical
Event Type	equipmentAlarm
Probable Cause	temperatureUnacceptable (50)
Alarm Text	Board temperature too high
Status Changes	
1. Condition	Temperature is above 60°C (140°F)
Alarm Status	Critical
2. Condition	After raise, temperature falls below 55°C (131°F)
Alarm Status	Cleared
Corrective Action	Inspect the system. Determine if all fans in the system are properly operating.

Table B-36: acBoardEvResettingBoard

Alarm	acBoardEvResettingBoard
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5
Default Severity	Critical
Event Type	equipmentAlarm
Probable Cause	outOfService (71)
Alarm Text	User resetting board
Status Changes	
1. Condition	When a soft reset is triggered via the Web interface or SNMP.
Alarm Status	Critical
2. Condition	After raise
Alarm Status	Status stays critical until reboot. A clear trap is not sent.
Corrective Action	A network administrator has taken action to reset the device. No corrective action is required.

Table B-37: acFeatureKeyError

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

Table B-38: acSAMissingAlarm

Alarm	acSAMissingAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.32
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 Text	SA Module Alarm. SA-Module from slot #n is missing.
Status Changes	
1. Condition	SA module removed or missing
Alarm Status	Critical
2. Condition	SA module is in slot 2 or 4 and working.
Alarm Status	Cleared

Note: This alarm is applicable only for the Mediant 3000.

Table B-39: acNTPServerStatusAlarm

Alarm	acNTPServerStatusAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.71
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	communicationsSubsystemFailure
Alarm Text	NTP server alarm. No connection to NTP server.
Status Changes	
1. Condition	No initial communication to Network Time Protocol (NTP) server.
Alarm Status	Major
2. Condition	No communication to NTP server after the time was already set once.
Alarm Status	Minor
Corrective Action	Repair NTP communication. (The NTP server is down or its IP address is configured incorrectly in the device.)

Table B-40: acIPv6ErrorAlarm

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 Text	IP interface alarm. <text>
Status Changes	
1. Condition	Bad IPv6 address (already exists)
Alarm Status	Critical
<text> Value	IPv6 Configuration failed, IPv6 will be disabled.
2. Condition	After alarm raise
Alarm Status	Status stays critical until reboot. A clear trap is not sent.
Corrective Action	Find new IPV6 address and reboot.

Note: This alarm is applicable only to for the Mediant 800 E-SBC/3000 series.

Table B-41: acgwAdminStateChange

Alarm	acgwAdminStateChange
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	outOfService (71)
Alarm Text	Network element admin state change alarm Gateway is <text>
Status Changes	
1. Condition	Admin state changed to shutting down
Alarm Status	Major
<text> Value	shutting down. No time limit.
2. Condition	Admin state changed to locked
Alarm Status	Major
<text> Value	locked
1. Condition	Admin state changed to unlocked
Alarm Status	cleared
Corrective Action	A network administrator has taken an action to lock the device. No corrective action is required.

Table B-42: acOperationalStateChange

Alarm	acOperationalStateChange
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.15
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	outOfService (71)
Alarm Text	Network element operational state change alarm. Operational state is disabled.
Note	This alarm is raised if the operational state of the node goes to disabled. The alarm is cleared when the operational state of the node goes to enabled.
Status Changes	
1. Condition	Operational state changed to disabled
Alarm Status	Major
2. Condition	Operational state changed to enabled
Alarm Status	cleared
Note	In IP systems, the operational state of the node is disabled if the device fails to properly initialize.
Corrective Action	In IP systems, check for initialization errors. Look for other alarms and Syslogs that might provide additional information about the error.

Table B-43: acSWUpgradeAlarm

Alarm	acSWUpgradeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.70
Default Severity	Major
Alarms Source	System#0
Event Type	processingErrorAlarm
Probable Cause	softwareProgramError
Alarm Text	SW upgrade error. <text>
Note	
Condition	Raised upon software upgrade errors.
Alarm Status	major
<text> value	Firmware burning failed. Startup system from Bootp/tftp.
Corrective Action	Start up system from BootP/TFTP.

Table B-44: acActiveAlarmTableOverflow

Alarm	acActiveAlarmTableOverflow
OID	1.3.6.1.4.15003.9.10.1.21.2.0.12
Default Severity	Major
Source Varbind Text	*System#0*<n>*/AlarmManager#0*
Event Type	processingErrorAlarm
Probable Cause	resourceAtOrNearingCapacity (43)
Alarm Text	Active alarm table overflow
Status Changes	
1. Condition	Too many alarms to fit in the active alarm table
Alarm Status	Major
2. Condition	After raise
Alarm Status	Status remains Major until reboot. A Clear trap is not sent.
Note	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.
Corrective Action	Some alarm information may have been lost, but the ability of the device to perform its basic operations has not been impacted. A reboot is the only way to completely clear a problem with the active alarm table. Contact your first-level group.

Table B-45: acSS7LinkStateChangeAlarm 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.

Table B-46: acSS7LinkCongestionStateChangeAlarmTrap

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.

Table B-47: acSS7LinkInhibitStateChangeAlarm 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

Table B-47: acSS7LinkInhibitStateChangeAlarm Trap

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.

Table B-48: acSS7LinkSetStateChangeAlarm

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

Table B-49: acSS7RouteSetStateChangeAlarm 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
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**.)

Table B-50: acSS7SNSetStateChangeAlarmTrap

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 B-51: acSS7UalGroupStateChangeAlarm 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
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.)

Table B-52: 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	-
Note	Relevant to FXS only.

Note: This alarm is only applicable for Analog devices.

Table B-53: acBoardWanLinkAlarm

Alarm	acBoardWanLinkAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.79
Default Severity	Major / Clear
Event Type	equipmentAlarm
Source Varbind Text	Board#x/WanLink#y
Probable Cause	underlyingResourceUnavailable
Alarm Text	
Status Changes	
1. Condition	WAN link down
Alarm Status	Major
<text> Value	
2. Condition	WAN link up
Alarm Status	Clear
<text> Value	
Corrective Action	Connect WAN port

Note: This alarm is only applicable for MSBR devices.

Table B-54: 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	

Table B-55: 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	-

Table B-56: acWirelessCellularModemAlarm

Alarm	acWirelessCellularModemAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.82
Default Severity	Major / Clear
Source Varbind Text	Board#x/WanLink#y
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Alarm Text	WAN wireless cellular modem alarm.
Status Changes	
1. Condition	Raised when either the wireless modem is down or in backup mode, and cleared when modem is up.
Alarm Status	Major
2. Condition	WAN link up
Alarm Status	Clear

Note: This alarm is only applicable for the Mediant 800 MSBR.

Reader's Notes

C Performance Monitoring

Performance measurements for the AudioCodes devices can be polled at scheduled intervals by the SCOM or by an external poller or utility.

The AudioCodes device provides performance measurements in the form of Counters. 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.

The log trap 'acPerformanceMonitoringThresholdCrossing' (non-alarm) is sent every time the threshold of a Performance Monitored object is exceeded. The severity field is 'indeterminate' when the crossing is 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 user can configure monitors and rules in the SCOM based on the data polled from these counters. In addition, the user can change the polling interval parameters for these rules. For more information, see Section 6.3.4 on page 61.

C.1 Performance Monitoring Parameters

This section lists the device's SNMP PM counters.

C.1.1 IP-to-Tel Performance Monitoring

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

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

Counter	Description
acPMSIPAttemptedCallsVal	Indicates the number of attempted calls for IP to Tel direction, during last interval.
acPMSIPEstablishedCallsVal	Indicates the number of established calls for IP to Tel direction, during last interval.
acPMSIPBusyCallsVal	Indicates the number of calls that failed as a result of a busy line for IP to Tel direction, during last interval.
acPMSIPNoAnswerCallsVal	Indicates the number of calls that weren't answered for IP to Tel direction, during last interval.
acPMSIPForwardedCallsVal	Indicates the number of calls that were terminated due to a call forward for IP to Tel direction, during last interval.
acPMSIPNoRouteCallsVal	Indicates the number of calls whose destinations weren't found for IP to Tel direction, during last interval.
acPMSIPNoMatchCallsVal	Indicates the number of calls that failed due to mismatched media server capabilities for IP to Tel direction, during last interval.
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.
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.
acPMSIPCallDurationAverage	Indicates the average call duration of established calls for IP to Tel direction, during last interval.
IP2TelTrunkGroupEstablishedCalls	Indicates the current number of established calls pertaining to a Trunk Group for IP to Tel direction.
IP2TelTrunkEstablishedCalls	Indicates the current number of established calls pertaining to a trunk for IP to Tel direction.

C.1.2 SIP Tel-to-IP Performance Monitoring

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

Counter Name	Description
acPMSIPAttemptedCallsVal	Indicates the number of attempted calls for Tel to IP direction, during last interval.
acPMSIPEstablishedCallsVal	Indicates the number of established calls for Tel to IP direction, during last interval.
acPMSIPBusyCallsVal	Indicates the number of calls that failed as a result of a busy line for Tel to IP direction, during last interval.
acPMSIPNoAnswerCallsVal	Indicates the number of calls that weren't answered for Tel to IP direction, during last interval.
acPMSIPForwardedCallsVal	Indicates the number of calls that were terminated due to a call forward for Tel to IP direction, during last interval.
acPMSIPNoRouteCallsVal	Indicates the number of calls whose destinations weren't found for Tel to IP direction, during last interval.
acPMSIPNoMatchCallsVal	Indicates the number of calls that failed due to mismatched media server capabilities for Tel to IP direction, during last interval.
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.
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.
acPMSIPCallDurationAverage	Indicates the average call duration of established calls for Tel to IP direction, during last interval.
Tel2IPTrunkEstablishedCalls	Indicates the current number of established calls pertaining to a trunk for Tel to IP direction.
Tel2IPTrunkGroupEstablishedCalls	Indicates the current number of established calls pertaining to a Trunk Group for Tel to IP direction.

Reader's Notes

AudioCodes SCOM Management Pack

www.audiocodes.com