

# AudioCodes<sup>™</sup> Management Pack

Version 1.0.5.65



### **Table of Contents**

1	Intro	oduction	15
2	Aud	lioCodes Management Pack - Gateway Support	17
3	Sett	ing up the AudioCodes SCOM Management Pack	19
	3.1 3.2	Running the Setup Wizard Importing Management Pack	.19 .22
4	Disc	covering Gateway Devices	25
	4.1 4.2	Creating Discovery Rule Managing SCOM Accounts 4.2.1 Adding Network Devices to Discovery Rule	25 35 .35
5	Con	figuring SNMP	37
	5.1	Adding SNMPv3 Users5.1.1Adding SNMP V3 Users in the Device Web Interface5.1.2Adding SNMPv3 Accounts in SCOM	.37 .37 .40
	5.2	Disabling SNMP Trap Service	.50
	5.3	Setting up the Device to Send SINNP Traps	.51
6	Viev	ving Gateway Element States	55
	6.1	GW State View	.55
	6.2	Modules – All Modules State View.	57
	6.3	Modules – System Modules State View	58
	6.4	Modules – Fan Tray State View.	.59
	0.0	Modules – Power Supply State View	61
	0.0 6.7	Trunks/Ports – Digital Trunks State View	62
	0.7	Diogram View	62
	0.0	Diagram view	.03 64
	0.9	6.9.1 Pinging AudioCodes Device	.04 64
		6.9.2 Displaying Active Alarms	.67
		6.9.3 Setting Device Display Name	.69
		6.9.4 Testing Call from Gateway	.71
7	Mon	hitoring Gateway Element Health	73
	7.1	Monitoring Types	.73
	7.2	Aggregated Health State	73
		7.2.1 Aggregated Health State-Gateway	.74
	7.3	SNMP-SCOM Object Severity Mapping	74
		7.3.1 Gateway	.74
		7.3.2 Module	.74
		7.3.4 SNMP Traps	.75
	7.4	Alert Monitoring	.76
	-	7.4.1 GW Alerts View	.76
		7.4.2 All Modules Alerts View	.80
		7.4.3 All I runks/Ports Alerts View	.81
	1.5	Performance Monitoring	82

		7.5.1	Performance View	82
	7.6	Rules	Monitoring	83
		761	SIP Performance Monitoring Counters	83
		762	Trunk Service Information	83
	77	Throck	oold Monitoring	Q/
	1.1	THES		04
8	Opt	imizing	J SCOM Server Loading	91
	•	La face de		04
	8.1	Introdu		91
		8.1.1	Displaying AudioCodes Objects	92
		8.1.2	Optimizing Monitor's Load	95
		8.1.3	Optimizing Discoveries' Load	99
		8.1.4	Optimizing Rule's Load	102
Α	SNN	<b>//P</b> Trap	)S	.109
				400
	A.1	Chass	is Alarms	109
		A.1.1	Fan Tray Alarm	109
		A.1.2	Power Supply Alarm	111
		A.1.3	User Input Alarm	112
		A.1.4	PEM Alarm	112
		A.1.5	Hardware Failure Alarm	113
		A.1.6	Timing Module Alarms	113
		A.1.7	IM Inconsistent Remote and Local PLL Status Alarm	113
		A.1.8	IM Reference Status Alarm	114
		A.1.9	IM Reference Change Alarm	115
		A.1.10	I runk Alarms	115
			A.1.10.1 Trunk Near-End LOS Alarm	115
			A.1.10.2 Trunk Near-End LOF Alarm	116
			A.1.10.3 Trunk AIS Alarm	110
			A.1.10.4 Trunk Fal-End LOF Alarm	117
			A. 1.10.5 DST LINE Status Alam	/
			A. 1.10.0 D-Originier Aldrin	110
		A 1 11	A.T.10.7 NEAS Gloup Alaliii	110
		A.I.II	A 1 11 1 SONET Section LOE Alarm	119
			A 1.11.1 SONET Section LOF Aldrin	119
			A 1.11.2 SONET Section ALS Alarm	120
			A.1.11.5 SUNET Section AIS Aldini	120
			A 1 11 5 SONET Bath STS LOD Alarm	120
			A 1 11 6 SONET Path STS LOP Alam	121
			A 1 11 7 SONET Path Upgquipped Alarm	121
			A 1 11 8 SONET Path Signal Label Mismatch Alarm	122
			A 1 11 9 SONET Hardware Failure Alarm	123
		Δ 1 12	DS3 Alarms	124
		A.I.IZ	A 1 12 1 DS3 RAI Alarm	124
			A 1 12 2 DS3 AIS Alarm	125
			A 1 12 3 DS3 I OF Alarm	126
			A 1 12 4 DS3 LOS Alarm	127
			A 1 12.5 DS3 Line Status Change Alarm	127
		A 1 13	SS7 Alarms	128
		7	A 1 13 1 SS7 Link State Change Alarm Trap	128
			A 1 13.2 SS7 Link Congestion State Change Alarm Trap	129
			A.1.13.3 SS7 Link Inhibit State Change Alarm Trap	
			A.1.13.4 SS7 Link Set State Change Alarm	
			A.1.13.5 SS7 Route Set State Change Alarm Trap	130
			A.1.13.6 SS7 SN Set State Change Alarm Trap	131
		A.1.14	Hitless Software Upgrade Alarm	132
		A.1.15	High Availability Alarms	133
			A.1.15.1 HA System Fault Alarm	133
			· · · · · · · · · · · · · · · · · · ·	

		A.1.15.2 HA System Configuration Mismatch Alarm	135
		A.1.15.3 HA System Switch Over Alarm	135
	A.1.16	Device (Board) Alarms	136
		A.1.16.1 Fatal Error Alarm	136
		A.1.16.2 Configuration Error Alarm	137
		A.1.16.3 Temperature Alarm	137
		A.1.16.4 Software Reset Alarm	138
		A.1.16.5 Software Upgrade Alarm	138
		A.1.16.6 Call Resources Alarm	139
		A.1.16.7 Controller Failure Alarm	139
		A.1.16.8 Board Overload Alarm	140
		A.1.16.9 Feature Key Error Alarm	140
		A.1.16.10 Missing SA/M3K Blade (Alarm, Status and Synchronization) Alarm.	141
		A.1.16.11 Administration Status Change Alarm	141
		A.1.16.12 Operational Status Change Alarm	142
	A.1.17	Network Alarms	142
		A.1.17.1 Ethernet Link Alarm	142
		A.1.17.2 Ethernet Group Alarm	143
		A.1.17.3 WAN Link Alarm	143
		A.1.17.4 Data Interface Status Alarm	144
		A.1.17.5 Wireless Cellular Modern Alarm	144
		A 1.17.6 NTP Server Status Alarm	144
		A 1 17 7 NAT Traversal Alarm	145
		A 1 17 8   DAP   ost Connection Alarm	146
		A 1 17.9 OCSP Server Status Alarm	146
		A 1 17 10 IPv6 Error Alarm	147
		A 1 17 11 Active Alarm Table Alarm	147
		A 1 17 12 Audio Staging from APS Server Alarm	148
	A 1 18	Analog Port Alarms	149
	/	A 1 18 1 Analog Port SPI Out-of-Service Alarm	149
		A 1 18 2 Analog Port High Temperature Alarm	149
		A 1 18 3 Analog Port Ground Fault Out-of-Service Alarm	150
	Δ 1 10	Media Alarms	150
	A.1.13	A 1 19 1 Media Process Overload Alarm	150
		A 1 19.2 Media Realm Bandwidth Threshold Alarm	151
	Δ 1 20	Network Monitoring (Probe) between Devices	151
	A.1.20	A 1 20 1 NOM Connectivity Alarm	151
		A 1 20 2 NOM High RTT Alarm	152
		A 1 20 3 NOM High litter Alarm	152
		A 1 20 4 NOM High Packet Loss Alarm	152
		A 1 20 5 NOM Low Conversational MOS Alarm	153
		A 1 20 6 NOM Low Listening MOS Alarm	15/
	Δ 1 21	Intrusion Detection Alarms	15/
	7.1.21	A 1 21 1 IDS Policy Alarm	15/
	Δ 1 22	SAS Alarms	155
	A.1.22	A 1 22 1 Emergency Mode Alarm	155
	A 1 22	High_Availability (HA)	155
	A.1.25	A 1 22 1 Redundant Roard Tran	155
		A. 1.23.1 Returned II Deard Trap	155
		A 1 23 3 Hitless Software Ungrade Status Trap	150
		T. 1.20.0 Thiless Sonware Opyraue Status Hap	107
A.2	Event	raps (Notifications)	158
	A.2.1	IDS Threshold Cross Notification	158
	A.2.2	IDS Blacklist Notification	158
	A.2.3	Web User Access Denied due to Inactivity Trap	159
	A.2.4	Power-Over-Ethernet Status Trap	159
	A.2.5	Keep-Alive Trap	160
	A.2.6	Performance Monitoring Threshold-Crossing Trap	160
	A.2.7	HTTP Download Result Trap	161

		A.2.8 Dial Plan File Replaced Trap	161
		A.2.9 Hitless Software Upgrade Status Trap	162
		A.2.10 Secure Shell (SSH) Connection Status Trap	162
		A.2.11 SIP Proxy Connection Lost Trap	163
		A.2.12 TLS Certificate Expiry Trap	164
		A.2.13 Cold Start Trap	164
		A.2.14 Authentication Failure Trap	164
		A.2.15 Board Initialization Completed Trap	165
		A.2.16 Configuration Change Trap	165
		A.2.17 Link Up Trap	165
		A.2.18 Link Down Trap	
		A.2.19 D-Channel Status I rap	
		A.2.20 Enhanced BIT Status	
В	Perf	formance Monitoring Counters	169
	B.1	IP-to-Tel Performance Monitoring	169
	B.2	SIP Tel-to-IP Performance Monitoring	
	<b>D</b> 0	SPC Derformance Manitoring	
	- К З		171
	B.3	SDC Performance Monitoring	171
С	B.3 Opti	imizing SCOM Server Load-Example Scenario	171 <b>173</b>
С	B.3 <b>Opti</b> C.1	imizing SCOM Server Load-Example Scenario	171 <b>173</b> 173
С	B.3 Opti C.1 C.2	imizing SCOM Server Load-Example Scenario Default Loading Script Load Estimation	171 <b>173</b> 173 174
С	B.3 <b>Opti</b> C.1 C.2	SBC Performance Monitoring         imizing SCOM Server Load-Example Scenario         Default Loading         Script Load Estimation         C.2.1	171 <b>173</b> 173 174 174
С	B.3 <b>Opti</b> C.1 C.2	SBC Performance Monitoring         imizing SCOM Server Load-Example Scenario         Default Loading         Script Load Estimation         C.2.1 Type A Gateways         C.2.2 Type B Gateways	171 173 173 174 174 174 174
С	B.3 <b>Opti</b> C.1 C.2	imizing SCOM Server Load-Example Scenario Default Loading Script Load Estimation C.2.1 Type A Gateways C.2.2 Type B Gateways C.2.3 Type C Gateways	171 173 173 174 174 174 174 174
С	B.3 Opti C.1 C.2 C.3	imizing SCOM Server Load-Example Scenario         Default Loading         Script Load Estimation         C.2.1 Type A Gateways         C.2.2 Type B Gateways         C.2.3 Type C Gateways         Load Analysis	171 173 173 174 174 174 175 176
С	B.3 Opti C.1 C.2 C.3	imizing SCOM Server Load-Example Scenario Default Loading Script Load Estimation C.2.1 Type A Gateways C.2.2 Type B Gateways C.2.3 Type C Gateways Load Analysis C.3.1 Script Execution Without Load Balancing	171 173 173 174 174 174 175 176 177
С	B.3 Opti C.1 C.2 C.3	SBC Performance Monitoring         imizing SCOM Server Load-Example Scenario         Default Loading         Script Load Estimation         C.2.1 Type A Gateways         C.2.2 Type B Gateways         C.2.3 Type C Gateways         Load Analysis         C.3.1 Script Execution Without Load Balancing         C.3.2 Script Execution with Load Balancing	171 173 173 174 174 174 174 175 176 177 178
С	B.3 Opti C.1 C.2 C.3	<b>SBC Performance Wontoning imizing SCOM Server Load-Example Scenario</b> Default Loading Script Load Estimation. C.2.1 Type A Gateways C.2.2 Type B Gateways C.2.3 Type C Gateways Load Analysis C.3.1 Script Execution Without Load Balancing. C.3.2 Script Execution with Load Balancing C.3.2.1 Script Execution Without Overriding Sync Time	171 173 173 174 174 174 174 175 176 176 177 178 178
С	B.3 Opti C.1 C.2 C.3	<ul> <li>imizing SCOM Server Load-Example Scenario</li> <li>Default Loading</li> <li>Script Load Estimation</li> <li>C.2.1 Type A Gateways</li> <li>C.2.2 Type B Gateways</li> <li>C.2.3 Type C Gateways</li> <li>Load Analysis</li> <li>C.3.1 Script Execution Without Load Balancing</li> <li>C.3.2 Script Execution with Load Balancing</li> <li>C.3.2.1 Script Execution Without Overriding Sync Time</li> <li>C.3.2.2 Script Execution when Overriding Sync Time</li> </ul>	171 173 173 173 174 174 174 175 176 177 178 178 179
С	B.3 Opti C.1 C.2 C.3	<ul> <li>imizing SCOM Server Load-Example Scenario</li> <li>Default Loading</li> <li>Script Load Estimation</li> <li>C.2.1 Type A Gateways</li> <li>C.2.2 Type B Gateways</li> <li>C.2.3 Type C Gateways</li> <li>Load Analysis</li> <li>C.3.1 Script Execution Without Load Balancing</li> <li>C.3.2 Script Execution with Load Balancing</li> <li>C.3.2.1 Script Execution Without Overriding Sync Time</li> <li>C.3.2 Script Execution when Overriding Sync Time</li> <li>C.3.3 Resource Monitor</li> </ul>	171 173 173 173 174 174 174 175 176 177 178 178 179 181

### List of Figures

Figure 3-1: AudioCodes Setup Wizard Welcome Screen1	19
Figure 3-2: Select Destination Location2	20
Figure 3-3: Ready to Install2	20
Figure 3-4: AudioCodes Setup Wizard Complete2	21
Figure 3-5: Administration Pane	22
Figure 3-6: Import Management Packs Option	23
Figure 3-7: Select Management Packs	23
Figure 3-8: Online Catalog Connection	24
Figure 3-0: Select AudioCodes Management Packs	2/
Figure 4-1: Open Discovery Wizard	25
Figure 4-1. Open Discovery Wizard	20
Figure 4-2. Computer and Device Management Wizard	20
Figure 4-3: General Properties	27
Figure 4-4: Discovery Method2	28
-Igure 4-5: Default Accounts	28
Figure 4-6: Devices	29
Figure 4-7: Add a Device	30
Figure 4-8: Schedule Discovery	31
Figure 4-9: Summary3	32
Figure 4-10: Discovery Saving Progress	32
Figure 4-11: Network Discovery Rule Confirmation	33
Figure 4-12: Discovery Rules Confirmation	33
Figure 4-13: Network Devices	34
Figure 5-1: SNMP V3 Setting Page - Add Record Dialog Box	37
Figure 5-2: SCOM V3 User Added	38
Figure 5-3: Resetting the Device	38
Figure 5-4: New SNMPv3 User	40
Figure 5-5: Croate Pup as Account	f0 //1
Figure 5-5. Create Rull as Account	+1 40
Figure 5-0. Account Gredenillais	+2 40
Figure 5-7:SINIMPV3 User-Distribution Security	+3
Figure 5-8:SINMPV3 User-Wizard Completed Successfully4	13
Figure 5-9: Run as Profile	14
Figure 5-10: Profile Wizard4	14
Figure 5-11: Select Run As Account4	15
Figure 5-12: Add a Device4	45
Figure 5-13: Devices Page4	<del>1</del> 6
Figure 5-14: Schedule Discovery4	47
Figure 5-15: Summary4	48
Figure 5-16: Warning	48
Figure 5-17: Discovery Saving Progress4	49
Figure 5-18: Network Discovery Rule Confirmation	49
Figure 5-19: SNMP Community String	51
Figure 5-20: SNMP Trap Destinations	51
Figure 5-21: Trusted Manager IP Address	52
Figure 5-21: Prosecting the Device	52
Figure 6-1: CW/ State View	55
Figure 6-1. Gw State view	20
Figure 6-2: Personalize view	30
Figure 6-3: LOOK FOR Flitter	าก
Figure 6-4: All Modules State View	
Figure 6-5: System Modules State View5	57
Figure 6-6: Fan Tray State View5	57 58
	57 58 59
Figure 6-7: Power Supply State View6	57 58 59 30
Figure 6-7: Power Supply State View6 Figure 6-8: Digital Trunks State View6	57 58 59 50 51
Figure 6-7: Power Supply State View	57 58 59 50 51 52
Figure 6-7: Power Supply State View	57 58 59 50 51 52 53
Figure 6-7: Power Supply State View	57 58 59 50 51 52 53 53 54

Figure 6-13: Run Task-Ping	65
Figure 6-14: Task Status-Ping	66
Figure 6-15: Run Task-Show Active Alarms	67
Figure 6-16: Task Status-Show Active Alarms	68
Figure 6-17: Set Device Name	69
Figure 6-18: Task Status-Set Device Name	70
Figure 6-19: Run Task – Test Call	71
Figure 6-20: Task Status-Test Call	72
Figure 7-1: GW Alerts View	76
Figure 7-2: Gateway Module Alert Details	76
Figure 7-3: Alert Properties	77
Figure 7-4: Alert Properties-SNMP Information	78
Figure 7-5: Gateway Monitor Alert Details	78
Figure 7-6: Gateway Alert Monitor Properties	79
Figure 7-7: All Modules Alert View	80
Figure 7-8: Power Module Alert Details	80
Figure 7-9: All Trunk/Ports View	81
Figure 7-10: All Trunk/Ports Alert Details	81
Figure 7-11: GW Performance View	82
Figure 7-12: Rules Monitoring	83
Figure 7-13: Health Monitor-Initial View	85
Figure 7-14: Health Monitor-Expanded View	86
Figure 7-15: Threshold Monitor Properties	87
Figure 7-16: Override Thresholds	87
Figure 7-17: Override Properties - High Threshold Monitor	88
Figure 7-18: Override Properties - Low Level Threshold Monitor	89
Figure 8-1: Views	92
Figure 8-2: View Scope	92
Figure 8-3: Scope Management Pack Objects	93
Figure 8-4: AudioCodes Management Pack Entities	94
Figure 8-5: Monitors Option	96
Figure 8-6: Monitors	96
Figure 8-7: Overriding Object Monitors	97
Figure 8-8: Override Properties-Object Monitors-High Level Threshold Monitor	98
Figure 8-9: Object Discoveries Option	99
Figure 8-10: Object Discoveries	100
Figure 8-11: Overriding Object Discoveries	100
Figure 8-12: Override Properties-Object Discoveries	.101
Figure 8-13: Rules Option	102
Figure 8-14: Object Rules	103
Figure 8-15: Overriding Object Rules-AudioCodes Digital Trunk Channels Probe Rule	104
Figure 8-16: Override Properties-Audiocodes Digital Trunk Channels Probe Rule	105
Figure 8-17: Overriding Object Rules-AudioCodes Failed Calls Tel2IP Counter Rule	106
Figure 8-18: Override Properties-AudioCodes Failed Calls Tel2IP Counter Rule	107
Figure C-1: Load Analysis	176
Figure C-2: Non-Balanced Script Execution	177
Figure C-3: Frequency Without Syncronization	178
Figure C-4: Frequency and Sync	180
Figure C-5: SCOM Server Resource Monitor	181
v v v v v v v v v v v v v v v v v v v	

### List of Tables

Table 5.4. SNMD V2 Llass Deservatore	20
Table 5-1: SNMP V3 Users Parameters	
Table 7-1: Health Indication.	
Table 7-2: SNMP Gateway Objects Health State	74
Table 7-3:SNMP Gateway Modules Objects Health State	74
Table 7-4: Digital Trunk SNMP Polling	75
Table 7-5: Unhealthy State	75
Table 7 6: Allorm States	01
	04
Table A-1: act an TrayAlarm	110
Table A-2: acPowerSupplyAlarm	111
Table A-3: acUserInputAlarm	112
Table A-4: acPEMAlarm	112
Table A-5: acHwFailureAlarm.	113
Table A-6: acTMInconsistentRemoteAndLocalPLL Status Alarm	113
Table A-7: acTMP6forenceStatus Alarm	111
	445
Table A-8: act micelefence change Alarm	115
Table A-9: acTrunksAlarmNearEndLOS	115
Table A-10: acTrunksAlarmNearEndLOF	116
Table A-11: acTrunksAlarmRcvAIS	116
Table A-12: acTrunksAlarmFarEndLOF	117
Table A-13: dsx11 ineStatusChange	117
	118
	110
	110
Table A-16: AcSonetSectionLOFAlarm	119
Table A-17: AcSonetSectionLOSAlarm	119
Table A-18: AcSonetLineAISAlarm	120
Table A-19: AcSonetLineRDIAlarm	120
Table A-20: acSonetPathSTSLOPAlarm	121
Table A-21: acSonetPathSTSAISAlarm	121
Table A-22: acSonetPathSTSRDIAlarm	122
Table A-23: acSonetPathLinequippedAlarm	122
	102
	120
	123
Table A-26: acDS3RAIAIarm	124
Table A-27: acDS3AISAlarm	125
Table A-28: acDS3LOFAlarm	126
Table A-29: acDS3LOSAlarm	127
Table A-30: dsx3LineStatusChangeTrap	127
Table A-31: acSS7 Link State Change Alarm Trap	128
Table A-32: acSS7 Link CongestionState Change Alarm Trap	129
Table A-33: SS7 Link Inhibit State Change Alarm Trap	120
Table A 24: SS7 Link Set State Change Alarm	120
Table A-94, 557 Link Set State Change Alarm	100
Table A-35: SS/ Route Set State Change Alarm Trap	130
Table A-36: SS7 SN Set State Change Alarm Trap	131
Table A-37: SS7 Ual Group State Change Alarm Trap	131
Table A-38: acHitlessUpdateStatus	132
Table A-39: acHASystemFaultAlarm	133
Table A-40: acHASvstemConfigMismatchAlarm	135
Table A-41: acHASvstemSwitchOverAlarm	135
Table A-42: acBoardEatalError	136
Table A-13: acBoardConfigurationError	127
	107
	13/
I able A-45: acBoardEvResettingBoard	138
Table A-46: acSWUpgradeAlarm	138
Table A-47: acBoardCallResourcesAlarm	139
Table A-48: acBoardControllerFailureAlarm	139
Table A-49: acBoardOverloadAlarm	140

Table A-50: acFeatureKeyError	140
Table A-51: acSAMissingAlarm	141
Table A-52: acgwAdminStateChange	141
Table A-53: acOperationalStateChange	142
Table A-54: acBoardEthernetLinkAlarm	142
Table A-55: acEthernetGroupAlarm	143
Table A-56: acBoardWanLinkAlarm (only for MSBR Series)	143
Table A-57: acDataInterfaceStatus	144
Table A-58: acWirelessCellularModemAlarm	144
Table A-59: acNTPServerStatusAlarm	145
Table A-60: acNATTraversalAlarm	145
Table A-61: acLDAPLostConnection	146
Table A-62: acOCSPServerStatusAlarm	146
Table A-63: aclPv6ErrorAlarm (Applicable only to E-SBC Series)	147
Table A-64: acActiveAlarmTableOverflow	147
Table A-65: acAudioProvisioningAlarm	148
Table A-66: acAnalogPortSPIOutOfService	149
Table A-67: acAnalogPortHighTemperature	149
Table A-68: acAnalogPortGroundFaultOutOfService	150
Table A-69: acMediaProcessOverloadAlarm	150
Table A-70: acMediaRealmBWThresholdAlarm	151
Table A-71: acNgmConnectivityAlarm	151
Table A-72: acNgmRttAlarm	152
Table A-73: acNom litterAlarm	152
Table A-74: acNgmPacketLossAlarm	153
Table A-75: acNamCaMosAlarm	153
Table A-76: acNaml aMosAlarm	157
Table A-70: acINSPolicy/Alarm	154
Table A-78: acCW/SASEmergency/ModeAlarm	155
Table A-70: acBedundantBoardAlarm	155
Table A 20: acHANotwork/WatebdogStatus Alarm	155
	150
Table A 92: colDSTbrooboldCroooNctification	107
Table A-02. acIDSTITESHOLUCIOSSNULLICATION	150
Table A-03. dciD/SDidckii/SiiNoliiicalioii	100
Table A-64. acwebuserAccessDisabled	159
Table A-65. acPowerOverEthemetStatus	109
Table A-86: ackeepAlive	160
Table A-87: advertised Desute	160
Table A-00. ach i i PD0willoaukesull	101
Table A-89: acDialPlanFileReplaced	101
Table A-90 acHitlessUpdateStatus	162
Table A-91: acSSHConnectionStatus	102
Table A-92: acProxyConnectionLost	163
Table A-93: acCertificateExpiryNotifiaction Trap.	164
Table A-94: coldStart	164
Table A-95: authentication Failure	164
Table A-96: acBoardEvBoardStarted	165
Table A-97: entConfigChange	165
Table A-98: linkUp	165
Lable A-99: linkDown	165
I able A-100: AcDChannelStatus	166
Table A-101: AcDChannelStatus	167
Table B-1: SIP IP-to-Tel Performance Monitoring	169
Table B-2: SIP Tel-to-IP Performance Monitoring	170
Table B-3: SBC Call Admission Control Performance Monitoring	171
Table C-1: Management Pack Objects and Number of Scripts Run	173
Table C-2: Type A Gateways	174

Table C-3: Type B Gateways	174
Table C-4: Type C Gateways	175
Table C-5: Sync Time Sequence	179



This page is intentionally left blank.

### Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <a href="https://www.audiocodes.com/library/technical-documents">https://www.audiocodes.com/library/technical-documents</a>.

This document is subject to change without notice.

Date Published: January-28-2018

### **WEEE EU Directive**

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

### **Customer Support**

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

### **Abbreviations and Terminology**

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

### **Document Revision Record**

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

### **Documentation Feedback**

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

# **1** Introduction

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

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

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



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



This page is intentionally left blank.

# 2 AudioCodes Management Pack - Gateway Support

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

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



This page is intentionally left blank.

# 3 Setting up the AudioCodes SCOM Management Pack

This chapter describes the following setup procedures:

- Running the Setup Wizard. See below
- Importing Management Pack. See Section 3.2 on page 22.

### 3.1 Running the Setup Wizard

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



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

#### To setup the AudioCodes Management Pack:

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

#### Figure 3-1: AudioCodes Setup Wizard Welcome Screen



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

谒 Setup - AudioCodes SCOM	
Select Destination Location Where should AudioCodes SCOM be installed?	
Setup will install AudioCodes SCOM into the following folder.	
To continue, click Next. If you would like to select a different folder, click	Browse.
C:\Program Files\AudioCodes SCOM	Browse
At least 2.9 MB of free disk space is required.	
< Back Next >	Cancel

#### Figure 3-2: Select Destination Location

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

Figure 3-3: Ready to Install

🔂 Setup - AudioCodes SCOM	
Ready to Install Setup is now ready to begin installing AudioCodes SCOM on your computer.	
Click Install to continue with the installation, or click Back if you want to review o change any settings.	r
Destination location: C:\Program Files\AudioCodes SCOM	*
	T F
< Back Install	Cancel

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

Figure 3-4: AudioCodes Setup Wizard Complete



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

### 3.2 Importing Management Pack

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

- > To import the AudioCodes Management Pack into the SCOM environment:
- 1. Start the SCOM; the SCOM interface is displayed.
- 2. In the main SCOM window, click the **Administration** pane; the **Administration** pane is displayed:

Audiocodes - Operations Manager		
<u>File Edit View Go Tasks Tools H</u> elp		
Search ▼ <sub>∓</sub> III Scope 9 Find	🖸 Tasks 😡 🖕	
Administration <		
Administration		
👼 Connected Management Groups	Administration Overview	
4 🤚 Device Management	Administration Overview	
📸 Agent Managed		
🍌 Agentless Managed	Demuined Configuration Tester	
Management Servers	Required Configuration Tasks:	Actions:
Vending Management	In order for Operations Manager to manage and monitor your	Configure computers and devices to manage
UNIX/Linux Computers	network you must complete the following steps:	Import management packs
Wanagement Packs		View Management Pack Catalog
Discourse Pules	Required: Configure computers and devices to manage	Find management agents for other platforms
Network Devices	Required : Import management packs	Find connectors for other management tools
Network Devices Pending Management	Required: Enable Notification Channels	
▲ Motifications	Upgrade to full version	Key Concepts:
Channels		The Administration Workspace
Subscribers		Discovering Network Devices
Subscriptions	A Ortigenel Configurations	Run As Accounts and Profiles
Product Connectors	Sector Configuration:	Run As Accounts and Profiles for UNIX and Linux
Pur Internal Connectors	Ontionally configure the following components:	Management Packs
A Bun As Configuration	optionally compare the following components:	Discovery and Agents
Accounts	Configure Active Directory (AD) Integration	Destination Management Pack
Reprofiles	Active Directory (AD) integration allows you to leverage your investment in AD by enabling you to create AD based rules to assign	
UNIX/Linux Accounts	computers to Management Group.	Learn About:
a 🔒 Security		Selecting Targets and Groups
🔱 User Roles	Configure Client Monitoring	Creating a Resource Pool
🍓 Settings	Client Monitoring enables you to monitor operating systems and applications for errors and participate in the Customer Experience	-
	Improvement Program.	
		Online Resources:
		Microsoft System Center Online
		Microsoft System Center Community
Discovery Wizard		Report an Issue or Suggestion to Microsoft
		Report an issue of suggestion to interosoft
Monitoring		
Authoring		
🚳 Administration		
Ky Workspace		
•	1	
Ready		
		14

#### Figure 3-5: Administration Pane



#### Figure 3-6: Import Management Packs Option

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

🌆 Import Management Packs				×
Select Managemer	nt Packs			
Select Management Packs				🕢 Help
	Import list : Name	Version Relea	dd • Properties X   Add)rom catalog Add from disk	Remove
	Status details :			
			Install	Cancel //

Figure 3-7: Select Management Packs

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

Figure 3-8: Online Catalog Connection



- 5. Click **No** to decline choosing Management Pack from a Catalog.
- 6. Locate the saved AudioCodes Management Pack (in XML format) on you disk (the location that you chose in Section 3 on page 19) and then click the **Open** button; the Select Management Packs window is displayed:

Figure 3-9: Select AudioCodes Management Packs	•

🔜 Import Management Packs		×
Select Manageme	nt Packs	
Select Management Packs		@ Help
	Import list :	🕂 Add 🝷 🚰 Properties 🗙 Remove
	Name         Version           ①         Audiocodes GW Management Pack         1.0.2.0	Release Date Status EULA
	Status details :	
	Audiocodes GW Management Pack version 1.0.2.0	is imported.
		Install Cancel
		li li

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

# 4 **Discovering Gateway Devices**

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



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

### 4.1 Creating Discovery Rule

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

- > To discover the gateway as a Network Device:
- 1. In the Administration pane, right-click **Network Devices** ,and then in the pop-up menu, choose **Discovery Wizard**:

. – – – – – – – – – – – – – – – – – – –	, ,
<u>.</u>	Discovery <u>W</u> izard
-	Create Managemen <u>t</u> Pack
雟	Download Management Packs
×	Import <u>M</u> anagement Packs
2	New User Role
1	Create Run As Account
80	Create Run As <u>P</u> rofile
<b>.</b>	New channel
8	New subscriber
2	New subscription
	Add Management Group
Q	Refresh F5

#### Figure 4-1: Open Discovery Wizard

The Computer and Device Management Wizard is displayed:

🚆 Computer and Device Manage	ment Wizard	×
What would you		
Discovery Type		
General Properties	Choose the type of computers or devices to discover and manage.	
Discovery Method		
Default Accounts	Windows computers	
Devices	Discover Windows computers in your Active Directory	
Schedule Discovery	manage.	
Summary		
Completion	UNIX/Linux computers This enables you to discover UNIX and Linux computers in your environment and install agents on the ones you want to manage.	
	Network devices     Discover and monitor network devices using Simple     Network Management Protocol (SNMP).	
	Select a discovery type and click Next to continue.	
	< <u>Previous</u> <u>Previous</u> <u>Create</u> Ca	ancel

Figure 4-2: Computer and Device Management Wizard

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

👼 Network Devices Discovery Wiza	rd	×
General Properties		
General Properties		🕜 Help
Discovery Method	Specify general properties	
Default Accounts	Name:	
Devices	Audiocodes GW discovery	_
Schedule Discovery	Description (optional):	
Summary		<b>A</b>
Completion		-
	Select a management or gateway server Select an Operations Manager management server or gateway server to run the discovery. A server can run only one network discovery. Servers that already run a network discovery do not appear in the list. Available servers: SCOM.ilync15.local Select a resource pool Create Resource Pool	•
	Select an Operations Manager resource pool for monitoring of discovered network	
	devices.	
	Available pools:	
	All Management Servers Hesource Pool	<u> </u>
	< Previous Next > Save C	ancel

#### **Figure 4-3: General Properties**

- 3. In the 'Name' field, enter a description of the Discovery Rule.
- **4.** From the Available servers drop-down list, choose the SCOM server e.g., SCOM.iLync15.local, and then click **Next**; the Discovery Method window is displayed:

#### Figure 4-4: Discovery Method



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

Network Devices Discovery Wize	ard X
Default Accounts	
General Properties	Help
Discovery Method	Specify the default Run As accounts for discovery
Default Accounts	Select one or more SNMPv1 or SNMPv2 Bun As accounts as the default accounts for
Devices	discovering network devices. You can override the default accounts for individual network devices or add accounts for SNMPv3 devices later in this wizard
Schedule Discovery	
Summary	
Completion	Bun és accounts:
	Account Name       Description         Image: Comparison of the second secon
	< <u>P</u> revious <u>N</u> ext > Save Cancel

Figure 4-5: Default Accounts

- 6. Choose the default SNMP SCOM account (this account is always-'public') or click Create Account button to create a new default account; a wizard opens. Enter a Display Name and Community String (use the same community string that is configured on the network device that you wish to discover), and then click Create.
- 7. Click Next; the Devices page is displayed with the new user details:

Network Devices Discovery Wize	ard					×
Devices						
General Properties						) Help
Discovery Method	Specify devices					9
Default Accounts	Specify the network (	devices that you want to dis	cover and manag	e. You	can also import a	3
Devices	text file that contains	the IP addresses of your ne	twork devices.			
Schedule Discovery						
Summary		Iu	nport 🛟 <u>A</u> dd.	🗹	<u>E</u> dit 🗡 <u>R</u> em	ove
Completion	<u>D</u> evices:					
	Device	Run As Account	SNMP Version	Port	Access Mode	
	195.189.192.249	Use default accounts	V1 or V2	161	SNMP	
	10.30.50.218	public	V1 or V2	161	SNMP	
	10.30.50.217	Use default accounts	VI or V2	101	SNMP	
	More about netwo	ork discovery settings	Ad <u>v</u> a	anced D	iscovery Setting:	s
		< <u>P</u> revious	<u>N</u> ext >	Sa	ave Ca	ancel

#### Figure 4-6: Devices

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

#### Figure 4-7: Add a Device

Add a Device	×
Specify the settings for the network device you want to discover.	
Name or IP address: 🥹	
Access mode:	SNMP version: v1 or v2
Port number:	SNMP V1 or V2 Run As account: Use selected default accounts
	Add SNMP V1 or V2 Run As Account
O More about network discovery settings	OK Cancel

- 9. In the 'Name or IP address' field, enter the Enter the Name or IP address of the device.
- 10. From the Access mode field drop-down list, select SNMP.
- **11.** Optional: From the 'SNMP V1 or V2 Run As Account' drop-down list, select a different already configured default account.
  - If you wish to configure a new SNMP V1 or V2 default account, then click the Add SNMP V1 or V2 Run As Account button; a wizard opens. Enter a Display Name and Community String (use the same community string that is configured on the network device that you wish to discover), and then click Create.
  - Note that the same dialog opens as in the 'Default Accounts' step above.
- 12. Click Next; the Schedule Discovery screen is displayed:

hetwork Devices Discovery Wiz	ard	×
Schedule Discover		H
General Properties		🙆 Help
Discovery Method	Schedule the network discovery	S Holp
Default Accounts		
Devices	C Run the discovery rule at scheduled times	
Schedule Discovery	Time of day:	
Summary	00:00 🗮	
Completion	Days of the week:	
	🗖 Sunday	
	🗖 Monday	
	🗖 Tuesday	
	🗖 Wednesday	
	🗖 Thursday	
	Friday	
	🗖 Saturday	
	Run the discovery rule manually	
	< Previous Next > Save	Cancel

Figure 4-8: Schedule Discovery

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

#### Figure 4-9: Summary

Network Devices Discovery V	Vizard	×
Summary		
General Properties		🕢 Help
Discovery Method	Confirm the settings	
Default Accounts		<b>A</b>
Devices	Name: Audiocodes GWs discovery	
Schedule Discovery	Description:	
Summary		
Completion	Run As accounts: public	
	Discovery method: Explicit	
	Number of devices specified: 4	
	Schedule: Run Manually	
		<b>Y</b>
	< Previous Next> Save	Cancel

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



🔜 Network Devices Discovery Wiz	ard	×
Summary		
General Properties		🙆 Help
Discovery Method	Creating the discovery	( in the p
Default Accounts	Please wait while the discovery rule is created. This could take a minute	
Devices	O depending on the speed of your computer.	
Schedule Discovery		
Summary		
Completion		
		o ( 1
	< <u>L'revious</u> <u>N</u> ext > Save	L'ancel

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



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

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

Figure 4-12: Discovery Rules Confirmation

🖾 Discovery Rules - Audiocodes - Operations Man	ager		
<u>File E</u> dit <u>V</u> iew <u>G</u> o Tas <u>k</u> s <u>T</u> ools <u>H</u> elp			
Search 🔻 🝦 🌆 Scope 🔎 Fig	id 🚺 Tasks 🕡 🖕		
File       Edit       Yew       Go       Tasks       Tools       Help         Image: Search       Image: Image       Image: Image: Image       Image: Image: Image       Image: I		Eind Now Gear Last Discovered A Last Pending 1 0	Lask Run Time
Subscriptions  Subscriptions  Product Connectors  Resource Pools  Accounts Profiles Profiles  Classifies Clas	▼ Details: ▼		Task Pane
Ready			11

Network Devices - Audiocodes - Operations Manag	er			-	. 🗆 ×
Search V = Scope Scope	🖸 Tasks 👔 📮				
Administration <	Network Devices (5)				۲.
🍌 Agentless Managed 📃	Q Look for:	Find Now	Clear	×	
🔛 Management Servers	Name	IP Address	RunAs Account	Access Mode	
🔮 Pending Management	A Resource Pool: All Manage	ment Servers Resource Pool (5)			
UNIX/Linux Computers	10.30.50.217	10.30.50.217	public	SNMPONLY	
Management Packs	10.30.50.217	10.30.50.217	public	SNMPONLY	
Discovery Rules	10.30.50.219	10.30.50.219	public	SNMPONLY	
Retwork Devices	Audiocodes.com	195.189.192.249	public	SNMPONLY	
Network Devices Pending Management	Audiocodes.com	195.189.192.249	public	SNMPONLY	
Notifications					
🙀 Channels					
🌆 Subscribers					
Subscriptions					-
4 🔮 Product Connectors					ask
🖳 Internal Connectors					Pa
🟭 Resource Pools					Ine
Run As Configuration					
Accounts					
INTV/Linux Accounts					
Discovery Wizard					
Monitoring					
Authoring					
Administration					
🔣 My Workspace					
•	•				

#### Figure 4-13: Network Devices

All discovered gateways are displayed in this window.



**C** audiocodes

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

### 4.2 Managing SCOM Accounts

SCOM accounts are managed in the Accounts screen.

- > To view currently defined SCOM user accounts:
- 1. Open the Accounts page (Administration > Run as Configuration > Accounts); a screen similar to the following is displayed:

#### Accounts Page

Accounts (13)			<ul> <li>Tasks</li> </ul>
Name	Description	Last Modified	
▲ Type: Action Account (2)			Actions
ILYNC15\Administrator	This is the user account under which all rules run by default on the agent.	11/3/2013 11:39:22 AM	
🌍 Local System Action Account	Built in SYSTEM account to be used as an action account	11/3/2013 11:18:45 AM	Properties
A Type: Community String (1)			X Delete
🎐 public		11/4/2013 3:09:23 PM	PD Create Run As Account
4 Type: SNMPv3 Authentication (7)			
🎐 Brad		11/6/2013 11:36:28 AM	
🎐 Brad		11/5/2013 6:29:53 PM	
🄄 Brad		11/6/2013 11:39:37 AM	
🌆 Daniel		11/6/2013 2:55:07 PM	
🌆 Mike		11/6/2013 2:17:27 PM	
🌆 Mike		11/6/2013 2:13:41 PM	
🔄 💁 Ofer		11/6/2013 2:19:45 PM	
4 Type: Windows (3)			
🌆 Data Warehouse Report Deployment A	Data Warehouse Report Deployment Account	11/3/2013 11:47:10 AM	
🌆 Local System Windows Account	Built in SYSTEM account	11/3/2013 11:18:27 AM	
So Network Service Windows Account	Built in Network service account	11/3/2013 11:18:27 AM	

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

### 4.2.1 Adding Network Devices to Discovery Rule

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

- > To add network devices to an existing discovery rule:
- 1. In the Discovery Rules window, double-click the Discovery Rule; the Network Devices Discovery Wizard is displayed with the existing settings.
- 2. Run the wizard as described above in Section 4.1 on page 25.



This page is intentionally left blank.
# 5 Configuring SNMP

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

The following topics are described:

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

## 5.1 Adding SNMPv3 Users

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



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

### 5.1.1 Adding SNMP V3 Users in the Device Web Interface

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

#### **To configure SNMP v3 users:**

- In the device Web Interface, open the SNMP v3 Users page (Configuration tab > System menu > Management sub-menu > SNMP sub-menu > SNMP V3 Users).
- 2. Click Add; the following dialog box appears:

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

Add Record	×
Index	ρ́
User Name	
Authentication Protocol	None 👻
Privacy Protocol	None 👻
Authentication Key	
Privacy Key	
Group	Read-Write 👻
	🗟 Submit 🗙 Cancel

SNMPv3	Jsers					
	~					
Add +	Edit 🧨 🛛 Delete	• 💼				Show/Hide
		Authentication				
Index :	User Name	Protocol	Privacy Protocol	Authentication Key	Privacy Key	Group
sco	м	MD5	DES	*	*	Read-Write
		I < < Page	1 of 1 → → S	how 10 V records pe	er page	View 1 - 1 o
		14 <4 Page	1 of 1 → ► S	how 10 V records pe	er page	View 1 - 1 o
Gelected Ro	<u>w #0</u>	re <e page<="" td=""><td>1of 1 ⊨&gt; ► ► S</td><td>how 10 V records pe</td><td>r page</td><td>View 1 - 1 o</td></e>	1of 1 ⊨> ► ► S	how 10 V records pe	r page	View 1 - 1 o
Gelected Ra	<u>w #0</u>	re <e page<="" td=""><td>1 of 1 → ► S</td><td>how 10 V records pe</td><td>er page</td><td>View 1 - 1 o</td></e>	1 of 1 → ► S	how 10 V records pe	er page	View 1 - 1 o
Selected Ro	<u>w #0</u>	re <e page<="" td=""><td>1 of 1 → ► S</td><td>how 10 V records pe</td><td>er page</td><td>View 1 - 1 o</td></e>	1 of 1 → ► S	how 10 V records pe	er page	View 1 - 1 o
Selected Ro User Name Authentica	w #0 :: tion Protocol:	SCOM MD5	1 of 1 → ► S	how 10 V records pe Authentication Key: Privacy Key:	er page * *	View 1 - 1 o

Figure 5-2: SCOM V3 User Added

- 3. Configure the SNMP V3 Setting parameters according to the table below.
- 4. Click **Submit** to apply your settings.
- 5. Open the Maintenance Actions page (Maintenance tab > Maintenance menu > Maintenance Actions).

Figure 5-3: Resetting the Device

Reset Board	Reset
Burn To FLASH	Yes 💌
Graceful Option	No
Lock	LOCK
Graceful Option	No
Gateway Operational State	UNLOCKED
<ul> <li>Save Configuration</li> </ul>	
Burn To FLASH	BURN

- 6. Ensure that the 'Burn to FLASH' field is set to Yes (default).
- 7. Click the **Reset** button.

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

Table 5	-1:	SNMP	V3	Users	Parameters
---------	-----	------	----	-------	------------

### 5.1.2 Adding SNMPv3 Accounts in SCOM

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

- **To add SNMPv3 accounts:**
- 1. In the Administration pane, select Run As Configuration > Accounts, and then in the Actions pane, select Create Run as Account.

#### Figure 5-4: New SNMPv3 User



The Create Run as Account wizard is displayed:

Figure	5-5:	Create	Run	as	Account
--------	------	--------	-----	----	---------

鬼	Create Run As Account Wizard	
General Properties		
Introduction		
General Properties	Specify general properties for the Run As account	
Credentials Distribution Security Completion	Select the type of Run As account that you want to create, and then provide a display name and description.	
	Run As account type:       SNMPv3 Account     v	
	Display name:	
	Description (optional):	
	< <u>Previous</u> <u>N</u> ext > <u>C</u> reate Cancel	-

- 2. From the "Run As account type" list box, select **SNMPv3 Account**.
- 3. Enter the desired display name and description.

<u>\$1.</u>	Create Run As Account Mizard
Credentials	
Introduction	
General Properties	Provide account credentials
Credentials Distribution Security Completion	Provide credentials for this Windows Run As account.       User name:      I      Password:      Confirm password:      Domain:      StB
	< <u>Previous</u> <u>N</u> ext > <u>C</u> reate Cancel

#### **Figure 5-6: Account Credentials**

- 4. Create the new account using the same credentials that you configured in Section 4.1 on page 25 and in Section 5.1.1 on page 37.
- 5. Ensure that you set the Distribution Security to the **More Secure....** option.

Distribution Security	
Introduction	
General Properties	Select a distribution security option
Credentials	
Distribution Security	The credentials for this Run As account must be distributed to the agent-managed computers or management servers to perform the monitoring operations that are associated with a Run
Completion	As profile. Distribution cannot occur until the Run As account is added to a Run As profile.
	Select a distribution security option for this Run As account:
	Less secure - I want the credentials to be distributed automatically to all managed computers.
	Caution: Administrators of all recipient computers will be able to access the Run As account credentials.
	More secure · I want to manually select the computers to which the credentials will be distributed.
	< Previous Next > Create Cancel

### Figure 5-7:SNMPv3 User-Distribution Security

6. At the end of the wizard process, click **Create** to create the new **SNMPv3\_User** object. Figure 5-8:SNMPv3 User-Wizard Completed Successfully

彩	Create Run As Account Wizard
Run As Account Cr	reation Progress
Introduction	
General Properties	Wizard completed successfully
Credentials	
Distribution Security	You have successfully created this Hun As account.
Completion	A You must now associate this Run As account with an appropriate Run As profile. You can edit an existing profile or create a new one.
	< <u>P</u> revious <u>N</u> ext > <b>⊆lose</b> Cancel

# **C**audiocodes

7. In the Administration pane, select **Run As Configuration** > **Profiles** and then select the profile that you wish to associate with the new SNMPv3 Run as account.

		Profiles - SCOM-S48 - (	Operations Ma	nager		- 0 ×
Eile Edit View Go Tasks Iools Help Search * . i Bu Komps 🕑 Food 🖸 Tasks 🛛 .						
Administration		Profiles (29)				Tasks
🖌 🥨 Administration		Q Look for:		Eind Now Glear	6	0 0
🙈 Connected Management Groups		Name	Description			
a 🕒 Device Management		Re Microsoft SystemCenter, WebApplicatio				schons
👍 Agent Managed		Le Active Directory Based Agent Assignme	Account used b	AD based agent assignment module to publish assign	ment settings to /	Properties
Agentiess Managed		Agent Health OnsMar Database Account	Account used to	access the Operations Mapager database to collect an	ent status	C Delete
Management Servers		ADM CSM Encention Drofile	The ancention	mobile used to store ensembles key settings for collecting	d canciting data in	Create Run
Pending Management		Automatic Acant Management Account	This account on	none area to submatically dispersive speet follows (s. c.	Handhart failurer	
UNIX/Linux Computers		Castificate Significate Account	This Mondows a	is be used to automatically unights a light randres (e.g.	a computate h	
Management Pada		Client Maniharian Antian Associat	finis windows a	ecount is used for signing the certificates used to secur	e communicate pr	
Discovery Bules		Consistent Management Group Account	This models date	account is used to run an chent monitoring modules p	art or various rule.	
Network Design		a Day West an anagement broup Account	This prome dete	mines which creatinais are used to test connectivity i	between dered ma	
Network Devices Pending Management		No Data Warehouse Account	if specified, this	account is used to run all Data warehouse collection at	nd synchronizatior	
A S Notifications		to bats warehouse Report Deployment Ac	This account is	used by Liata warehouse report auto-deployment proci	dures to execute	
thannels		Lata Warehouse SQL Server Authenticat	If specified, this	login name and password is used by collection and syr	chronization rule:	
Subscribes		5 Default Action Account The default Health Service Action Account				
Subscriptions		So MPUpdate Action Account	This account is i	used by the MPUpdate notifier		
🖌 🙅 Product Connectors		to Notification Account	Windows accou	nt used by notification rules. Use this account's email a	ddress as email ar	
29 Internal Connectors		🗞 Operational Database Account	This account is a	used to read and write information to the Operational E	otabase.	
22 Resource Pools		b Privileged Monitoring Account	This profile is us	ed for monitoring which can only be done with a high	level of privilege t	
# 🍀 Run As Configuration		a Reporting SDK SQL Server Authenticatio	If specified, this	login name and password is used by Data Access service	e to connect to th	
Accounts		Sto Reserved	This profile is re	served and must not be used.		
See Profiles	-	2 Reserved	This profile is re	served and must not be used.		
UNIX/Linux/Accounts		🗞 Reserved	This profile is re	served and must not be used.		
< 🕄 Security	×	3 SNMP Monitoring Account	This account is a	used for SNMP monitoring.		
Discovery Wizard		SNMPv3 Monitoring Account	This account is a	used for SNMPv3 monitoring.		
		♣ SNMPv3_User				
Monitoring		So UNIX/Linux Action Account	This account is a	used for low privilege UNIX and Linux access.		
Authoring		3. UNDVLinux Agent Maintenance Account	This account is used for privileged maintenance operations for UNIX and Linux agents.		d Linux agents. W	
		So UND/Linux Privileged Account	This account is used for accessing protected UNIX and Linux resources and actions that		and actions that n	
Reporting		So Validate Alert Subscription Account	Account used by	y the validate alert subscription module that validates t	hat notification su	
Administration		3 Windows Cluster Action Account	This profile is us	ed for all discovery and monitoring of Windows Cluste	r components. Th	
My Workspace	_	S-Management Action Account	This account is	used for WS-Management access.		
		2				
Provide Sector Sec						

### Figure 5-9: Run as Profile

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

#### Figure 5-10: Profile Wizard

彩.	Run As Profile Wizard
Introduction	
General Properties	Introduction
Run As Accounts	
Completion	Run As prories allow monicoring operations (monitors, rules, and tasks) to run as an account that has surficient privileges to successfully monitor protected resources in the network. For example, you can use a Run As profile to read database properties or to log on to a mailbox.
	In addition, administrators can assign different Run As accounts to different monitored resources. This is useful when multiple resources are monitored by the same agent or management server, but each agent or server has a different security conclust. For example, a single SQL server might host multiple databases, but each database has a different owner.
	Use this wizard to assign a Run As account that has the necessary privileges to the Run As profile.
	To begin the Run As Profile Wizard, click Next,
	Do not show this page again
	< Previous Next> Save Cancel

9. In the General Properties tab, enter the relevant properties and then in the Run As Accounts tab, select the SNMPv3 account that you just added:

🖗 🛛 🕹 Add a Run As Account	_	D X
Select a Run As account to add to this profile. Choose an account that has priv sufficient to monitor the objects that you specify.	vileges that are	
<u>R</u> un As account:		
	¥	<u>N</u> ew
BradSNMPv3 Data Warehouse Report Deployment Account Local System Windows Account Network Service Windows Account SNMPv3_User		
A selected class, group, or object:		
		S <u>e</u> lect
	<u>ok</u>	<u>C</u> ancel

- 10. Click **Save** to save the new account.
- 11. In the Administration pane, click **Network Management > Network Devices** and select **Discovery Wizard**.
- 12. Run the Discovery Wizard to discover Network Devices.
- **13.** Add the device using the new SNMPv3 user account:

#### Figure 5-12: Add a Device

Administration	2 Computer and Device Management Wizard	x	Tasks
By Agentless Managed ∰ Management Servers I Pending Management	Devices		Actions
UNIX/Linux Computers     Management Packs     Management Packs     Discovery Rules     Network Devices     Network Devices	Discovery Type General Properties Specify devices Discove Default Devices Specify the settings for the network device you want to discover.		<ul> <li>Properties</li> <li>Rediscover</li> <li>Change Pro</li> <li>Delete</li> <li>Personalize</li> </ul>
<ul> <li>Notifications</li> <li>Channels</li> <li>Subscriptions</li> <li>Subscriptions</li> <li>Product Connectors</li> <li>Internal Connectors</li> <li>Run As Configuration</li> <li>Accounts</li> <li>Profiles</li> <li>UNIX/Linux Accounts</li> <li>Security</li> </ul>	Schedul Summa Comple To.33 4.30 Access mode: SNMP Port number: T61 SNMP Add SNMP V3 Run As Account Add SNMP V3 Run As Account	-	
<ul> <li>User Roles</li> <li>Settings</li> <li>Discovery Wizard</li> <li>Monitoring</li> <li>Authoring</li> <li>Reporting</li> </ul>	More about network discovery settings     OK Cancel     Advanced Discovery Settings     More about network discovery settings	]	
Administration	< Previous Next > Create Cance	51	

14. Click Create to add the device.



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

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

Figure 5-13: Devices Page

👼 Network Devices Discovery Wiza	ard					×
Devices					11H	
General Properties					0	Help
Discovery Method	Specify devices					noip
Default Accounts						
Daviase	<ul> <li>Specify the network text file that contains</li> </ul>	devices that you want to disc the IP addresses of your net	cover and mana <u>c</u> work devices.	je. You	can also import a	
Devices		, i i i i i i i i i i i i i i i i i i i				
Schedule Discovery						
Summary		In	iport 🛟 Add	🗹	Edit 🗡 Remove	
Completion	Devices:					
	Device	Run As Account	SNMP Version	Port	Access Mode	[
	10.15.7.8	Use default accounts	V1 or V2	161	ICMP and SN	-
	10.8.7.31	Use default accounts	V1 or V2	161	ICMP and SN	
	10.3.90.37	Use default accounts	V1 or V2	161	ICMP and SN	
	10.3.99.230	Use default accounts	V1 or V2	161	ICMP and SN	
	10.15.21.15	Brad	V3	161	ICMP and SN	
			Adv	anced D	iscovery Settings	1
	More about netw	ork discovery settings				_
		< Previous	Next >	S	ave Cance	el

**15.** Click **OK**; the Schedule Discovery screen is displayed:

		-
Network Devices Discovery Wiz	zard	×
Schedule Discover	ry	4
General Properties		) Help
Discovery Method	Schedule the network discovery	
Default Accounts		
Devices	O Run the discovery rule at scheduled times	
Schedule Discovery	Time of day:	
Summary	00:00	
Completion	Days of the week:	
	🗖 Sunday	
	Monday	
	🗖 Tuesday	
	🗖 Wednesday	
	Thursday	
	Friday	
	🗖 Saturday	
	Run the discovery rule manually	
	< Previous Next > Save Can	cel

Figure 5-14: Schedule Discovery

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



Retwork Devices Discovery	Wizard	×
Summary		
General Properties		🕢 Help
Discovery Method	Confirm the settings	
Default Accounts		
Devices	Name: Audiocodes GWs discovery	
Schedule Discovery	Description:	
Summary		
Completion	Run As accounts: public	
	Discovery method: Explicit	
	Number of devices specified: 4	
	Schedule: Run Manually	
		-
	< <u>Previous</u> <u>N</u> ext> Save	e Cancel

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

The following message may be displayed:

Figure 5-16: Warning

₩arning		×
4	The following accounts need to be distributed to the health service 'SCOM.ilync15.local' and the members of the management pool 'All Management Servers Resource Pool' in order for the discovery to work: Brad	
	Would you like Operations Manager to distribute the accounts?	
	Yes: Distribute accounts and create the discovery. No: Do not distribute accounts and do not create the discovery.	
	Yes No	

- **18.** Click **Yes** to confirm.
- **19.** Wait for the discovery rule to complete saving.

Network Devices Discovery W	fizard	×
General Properties		🕜 Help
Discovery Method	Creating the discovery	
Default Accounts	Please wait while the discovery rule is created. This could take a minute	
Devices	depending on the speed of your computer.	
Schedule Discovery		
Summary		
Completion		
	< <u>Erevious</u> <u>Next&gt;</u> Save	Cancel

Figure 5-17: Discovery Saving Progress

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



Figure 5-18: Network Discovery Rule Confirmation

**21.** Wait for the SCOM to make a full discovery.

# 5.2 Disabling SNMP Trap Service

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

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

# 5.3 Setting up the Device to Send SNMP Traps

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

- **To send SNMPv3 traps to the SCOM:**
- 1. Open the SNMP Community String page (SNMP > Community String).

### Figure 5-19: SNMP Community String

SNMP Community String						
L						
				Read Only		<b>^</b>
			R	ead / Write		
			R	ead / Write		
			R	ead / Write		
			R	ead / Write		
			R	ead / Write		
						E
-						
😏 Disable SNMP		No		•		
Trap Communit	y String	public				
Trap Manager H	lost Name	SCOM				Ŧ
					_	

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

Figure 5-20: SNMP Trap Destinations

SNMF	Trap Destinations							
			IP Address	Trap Port	Trap User	Trap Enable		
[	SNMP Manager	1	10.15.25.35	162	Brad 🔹	Enable 🔻		
[	SNMP Manager	2	0.0.0.0	162	v2cParams 👻	Enable 🔻		
[	SNMP Manager	3	0.0.0.0	162	v2cParams 👻	Enable 🔻		
[	SNMP Manager	4	0.0.0.0	162	v2cParams 🔻	Enable 🔻	6	
[	SNMP Manager	5	0.0.0.0	162	v2cParams 💌	Enable 🔻	Su	 ubmit

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

Delete	Trusted Mana	gers IP Address	
	SNMP Trusted Manager 1	10.15.25.35	
	SNMP Trusted Manager 2	0.0.0.0	
	SNMP Trusted Manager 3	0.0.0.0	
	SNMP Trusted Manager 4	0.0.0.0	
	SNMP Trusted Manager 5	0.0.0.0	

### Figure 5-21: Trusted Manager IP Address

SNMP Trap Desti	nations Parameters Description
rameter	Description

Parameter	Description
Web: SNMP Manager [SNMPManagerIsUsed_x]	Enables the SNMP Manager to receive traps and checks the validity of the configured destination (IP address and port number).
	<ul> <li>[0] (check box cleared) = (Default) Disables SNMP Manager</li> <li>[4] (check box calacted) - Enables SNMP Manager</li> </ul>
	<ul> <li>[1] (cneck box selected) = Enables SNMP Manager</li> </ul>
Web: IP Address [SNMPManagerTableIP_x]	Defines the IP address (in dotted-decimal notation, e.g., 108.10.1.255) of the remote host used as the SNMP Manager. The device sends SNMP traps to this IP address.
Trap Port [SNMPManagerTrapPort_x]	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port.
	The valid value range is 100 to 4000. The default is 162.
Web: Trap User [SNMPManagerTrapUser]	Associates a trap user with the trap destination. This determines the trap format, authentication level, and encryption level.
	<ul> <li>v2cParams (default) = SNMPv2 user community string</li> </ul>
	<ul> <li>SNMPv3 user configured in 'Configuring SNMP V3 Users' (see Section 4.1 on page 25)</li> </ul>
Trap Enable	Activates the sending of traps to the SNMP Manager.
	[1] Enable (Default)

- 9. Click **Submit** to apply the changes.
- Open the Maintenance Actions page (Maintenance tab > Maintenance menu > Maintenance Actions).

5	0
Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No
LOCK / UNLOCK Lock	LOCK
Graceful Option	No
Gateway Operational State	UNLOCKED
→ Save Configuration	
Burn To FLASH	BURN

### Figure 5-22: Resetting the Device

- **11.** Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
- **12.** Click the **Reset** button.



This page is intentionally left blank.

# **6** Viewing Gateway Element States

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

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

## 6.1 GW State View

This section describes the GW State View.

#### > To open the GW State View:

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

🖾 GW State View - Audiocodes - Operations Manager						_ 🗆 🗡
<u>File Edit View Go Tasks Tools H</u> elp						
Search 🔻 🝦 🔤 Scope	🖸 Tasks 🕡 🍦					
Monitoring <	GW State View (1)					<ul> <li>Tasks</li> </ul>
🔛 Windows Computers 📃	Q Look for:		Find Now Clear		×	
Agentless Exception Monitoring	State Nam	e Display Name	Device Version	Device Type		
Application Monitoring	🔞 Critical Test	Device TestDevice	6.40A.058.005	Product: MG 1K		State Actions A
a 👝 Audiocodes Gateways	-					📲 Start Maintenance I
SW Alerts View						👫 Edit Maintenance N
🖂 GW Performance View						Stop Maintenance I
III GW State View						
a 🚰 Modules						Personalize view
≽ All Modules Alert View						Node Tasks ^
👯 All Modules State View						
🏭 Fan Tray State View						L_ Ping
📰 Power Supply State View						Ping Ping
🔢 System Modules State View						Set Device Name
a 🚰 Trunks/Ports						Show Active Alarm:
All Trunk/Ports Alert View						SNMP GET
🛄 Digital Trunks State View						SNIMD Walk
📰 Ethernet Ports State View						
Data Warehouse	Detail View				~	Telnet Console
						Test Call
Show or Hide Views	Audiocodes SNI	MP Device properties of TestD	evice			Traceroute
New View 🕨	Display Name	TestDevice				Taska
	Full Path Name	TestDevice				Td5K5 0
Monitoring	Access Mode	SNMPONLY				Entity Properties
Authoring	Certification	GENERIC Bredwate MC 14/504 Version				🙀 Health Explorer
<u></u>	Device Key	00-90-8E-13-2E-68	11: 0.40A.056.005			
Section Administration	Location					Navigation ^
My Workspace	Model					Alert View
	Port Number	161				≤ Diagram View
•	Primary Owner Conta	d			-	Event View
Ready	POINAD/ UW/her Name					4

### Figure 6-1: GW State View

This screen is described as follows:

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

- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.
- You can change the GW State View using the Personalize option right-click any column name and select **Personalize View** or in the Tasks pane, select **Personalize View**; the Personalize View window is displayed:

Personalize View		
<u>C</u> olumns to display	1	Sort columns by
V       IP Address         Device Version         Device Contact         Device Contact         Device Contact         Device OID         Community String         SNMP Version         Display Name         Device Type         Trunks Count         Channels Count         Last Reboot Time         Product Type         Device Name         Name         Audiocodes System Module Class         Audiocodes IF Digital Module         Audiocodes IF Englog Module		IP Address <ul> <li>● Ascending</li> <li>● Descending</li> </ul> Group items by <ul> <li>● Ascending</li> <li>● Descending</li> </ul> (None) <ul> <li>● Ascending</li> <li>● Descending</li> <li>■ Descending</li> </ul>
Audiocodes IF BRI Module	Ŧ	
		Reset to Default OK Cancel

Figure 6-2: Personalize View

- In this window, you can select the fields you wish to view in the GW State View and sort the data inside the view.
- In addition, you can filter the data displayed in the view using the 'Look For' filter: Figure 6-3: Look For Filter



### 6.2 Modules – All Modules State View

This section describes the All Modules State View.

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

Figure 6-4: All Modules State V	iew
---------------------------------	-----

All Modules State View - Audiocodes - Operations	s Manager						_ 🗆 🗵
<u>File Edit View Go</u> Tas <u>k</u> s <u>T</u> ools <u>H</u> elp							
Search 🔻 🝦 🌆 Scope 🔎 Find	1 📝 T <u>a</u> sks 🕡 💡						
Monitoring	<ul> <li>All Modules State View</li> </ul>	(5)					<ul> <li>Tasks</li> </ul>
Discovered Inventory	🔺 🔍 Look for:	Find Now Clear				×	
Distributed Applications				Audiocodes	Audiocodes		Chata
🍰 Task Status	State	Name	V Slot	Class	Clace		Actions
INIX/Linux Computers	() Healthy	TestDevice: PowerSupply Module at Slot 1	Slot 1	0035	Class		No. Charles Mariatanana
1 Windows Computers	Critical	TestDevice: acMediant1000IEDigitalModule at Slot 0	Slot 0	🙉 Critical			Start Maintenar
Agentless Exception Monitoring	Healthy	TestDevice: acMediant1000CPLImodule at Slot 0	Slot 0	•			Edit Maintenani
Application Monitoring	Healthy	M4K-10.30.52.31: PowerSupply Module at Slot 1	Slot 1				Stop Maintenar
4 🦾 Audiocodes Gateways	Healthy	M4K-10-30-52-31: PowerSupply Module at Slot 1	Slot 1				Personalize view
GW Alerts View							Tacke A
CW Performance View							
A C Moduler							Entity Properties
All Modules Alert View							A Health Explorer
All Modules State View							Novigation A
Fan Tray State View							nu rigation - A
Power Supply State View							Alert View
System Modules State View							≤ Diagram View
4 🚰 Trunks/Ports							Event View
All Trunk/Ports Alert View							Network Vicinit
🧱 Digital Trunks State View							Performance Vie
Ethernet Ports State View							State View
Data Warehouse							Juic view
Microsoft Audit Collection Services							
Microsoft Windows Client							
Microsoft Windows Server							
Network Monitoring							
Constructions Manager							
INTX (linux Computers							
Web Application Transaction Monitoring							
Windows Service And Process Monitoring	Detail View					~	
Show or Hide Views	_					*	
New View	Audiocodes Moo	dule Base Class properties of TestDevice: PowerSupply Mo	dule at Slot 1				
	Display Name	TestDevice: PowerSupply Module at Slot 1					
Monitoring	Full Path Name	TestDevice: PowerSupply Module at Slot 1 195 189 197 249					
	Slot	Slot 1					
Authoring	Index	2					
🚳 Administration	Key OID	.1.3.6.1.4.1.5003.9.10.10.4.23.1.3.2					
My Workspace							
- in transpace							
	*					~	
Ready							11.

This screen is described as follows:

- All Modules State View contains all modules of all discovered gateways as they are hosted on the real devices. The data represented in this view can be personalized as described in Section 6.1 on page 55.
- Select a module to load the Detail View pane at the bottom of the All Modules State View window.
- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.



## 6.3 Modules – System Modules State View

This section describes the System Modules State View.

#### > To open the System Modules State View:

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

System Modules State View - Audiocodes - Operat	ions Manager						(	
<u>File Edit View Go Tasks Tools H</u> elp								
Search 🔻 🝦 🖣 Scope 🔎 Find	Tasks 👔	-						
Monitoring <	System Modules	State View (10)					>	Tasks
Discovered Inventory	🛛 🔍 Look for: 🛛	F	Find Now Clear				x 😰	
E Distributed Applications	,				Audiocodes		AL CI	
🛃 Task Status	State	Name	V	Operational State	Class	Slot 😢	Dic SL	ctions ^
UNIX/Linux Computers	🐼 Critical	TestDevice: acMediant1000IFDigitalMo	odule at Slot 0	Unknown: -1	🔞 Critical	Slot 0 🛛 🕵	Cr 🖬	Start Maintenan
Windows Computers	() Healthy	TestDevice: acMediant1000CPUmodule	e at Slot 0	Unknown: -1	-	Slot 0	1	
Agentless Exception Monitoring	🔞 Critical	M1K-10.30.52.5: acMediant1000IFDigit	alModule at Slot 0	Unknown: -1	🐼 Critical	Slot 0 💽	Cr	<ul> <li>Edit Maintenance</li> </ul>
Application Monitoring	A Healthy		odule at Slot 967	Unknown: -1	-	Slot 967	-	§ Stop Maintenan
Audiocodes Gateways	🐼 Critical	M1K-10.30.52.4: acMediant1000IFDigit	alModule at Slot 111	Unknown: -1	🔞 Critical	Slot 111	) Cr 🔳	Personalize view
GW Alerts View	Healthy	M1K-10.30.52.4: acMediant1000CPI Imr	adule at Slot 99	Unknown: -1	•	Slot 99	Т	seke A
GW Performance View	Critical	M1K-10 30 52 3: acMediant1000TEDigit	alModule at Slot 51	Unknown: -1	🛐 Critical	Slot 51		
A C Modules	Healthy	M1K-10-30-52-3: active diamt1000/CPU mr	odule at Slot 2038	Unknown: -1	Citatai	Slot 2038		Entity Properties
All Modules Alert View	Critical	M1K 10 20 52 1; addediant1000tF bird	million at Slot 262	Unknown: 1	🚳 Critical	Slot 262		Health Explorer
All Modules State View		M1K-10.30.52.1, admediant20001 Digit	almodule at slot 205	Unknown1	Citical	510(20)	, ci	A noitepive
Fan Tray State View	Preatitity	MIK-10.50.52.1: admedianciboocPoint	Juule at Slot ou	Onknown: -1		5100.00	144	
Power Supply State View								Alert View
System Modules State View								Diagram View
▲ <sup>™</sup> Trunks/Ports								? Event View
All Trunk/Ports Alert View							39	Network Vicinity
Digital Trunks State View							50	Performance Vie
Ethernet Ports State View								State View
Data Warehouse								June new
Microsoft Audit Collection Services								
Microsoft Windows Client								
Microsoft Windows Server								
Network Monitoring								
Derations Manager								
Synthetic Transaction								
Web Application Transaction Monitoring	4						F	
Windows Service And Process Monitoring	Detail View						<u> </u>	
Show or Hide Views	Audiocod	les System Module Class properties of T	estDevice: acMediant1000IFDi	gitalModule at Slot 0				
New View 🕨	Display Nat	ne TestDevice: acMediant10	000IEDigitalModule at Slot 0					
	Full Path N	ame TestDevice\TestDevice:	acMediant1000IFDigitalModu	le at Slot 0				
Monitoring	IP Address	195.189.192.249						
Authoring	Slot	Slot 0						
	Key OID	1.3.6.1.4.1.5003.9.10.10	4.21.1.3.67387393				_	
W Administration	Geographi	tal Position 0						
My Workspace	Type	acMediant1000IFDigital	Module					
	Presence	missing						
·	Serial Num	LIDL Z					-	
Ready								4

This screen is described as follows:

- System Modules State View contains all system modules of all discovered gateways as they are hosted on the real devices. The data displayed in this view can be personalized as described in Section 6.1 on page 55.
- Select a module to load the Detail View pane at the bottom of the System Modules State View window.
- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.



# 6.4 Modules – Fan Tray State View

This section describes the Fan Tray State View.

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

Figure 6-6: Fan Trav St	ate View
-------------------------	----------

Fan Tray State View - Audiocodes - Operations N	fanager	
<u>File Edit View Go Tasks Tools Help</u>		
Search 🔻 🝦 🏭 Scope 👂 Fin	d 🖸 Tasks 🚱 🛫	
Monitoring	<ul> <li>Fan Tray State View</li> </ul>	<ul> <li>Tasks</li> </ul>
Discovered Inventory	🔟 Q Look for: 🛛 🛛 Find Now Clear 🗙 🗙	
Distributed Applications	State v Name	State
🗞 Task Status	O Healthy         10.10.50.3 Fan         10.10.50.3	Actions
1 UNIX/Linux Computers	⊘ Healthy 10.10.50.2 Fan 10.10.50.2	Start Maintenan
Windows Computers	⊘ Healthy 10.10.50.4 Fan 10.10.50.4	
Agentless Exception Monitoring		Edit Maintenand
Application Monitoring		Stop Maintenan
Audiocodes Gateways		Personalize view
GW Alerts View		
GW Performance View		
GW State View		
Mudules		
All Modules State View		
III Fon Tray State View		
Power Supply State View		
System Modules State View		
Garage System modules state them		
All Trunk/Ports Alert View		
III Digital Trunks State View		
Ethernet Ports State View		
Data Warehouse		
Microsoft Audit Collection Services		
Microsoft Windows Client		
Microsoft Windows Server		
Network Monitoring		
Operations Manager		
Synthetic Transaction		
UNIX/Linux Computers		
Web Application Transaction Monitoring		
Windows Service And Process Monitoring	▼ Detail View V	•
Show or Hide Views	i Select an item in the view above to display its details	
New View >	Sector of new many new operation of appropriate details.	
Monitoring		
Authoring		
Administration		
My Workspace		
	•	
Ready		11

This screen is described as follows:

- Fan Tray State View contains all fan trays of all discovered GWs as they are hosted on the real devices. The data represented in the view can be personalized as described in Section 6.1 on page 55.
- Select a module to load the Detail View pane at the bottom of the Fan Tray State View window.
- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.



# 6.5 Modules – Power Supply State View

This section describes the Power Supply State View.

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

Figure 6-7:	Power	Supply	State	View
-------------	-------	--------	-------	------

Power Supply State View - Audiocodes - Operation	ns Manager		
<u>File Edit View Go Tasks Tools Help</u>			
Search 🔻 🝦 🏧 Scope 🔎 Find	🖸 T <u>a</u> sks 🔞	Ŧ	
Monitoring	Power Supply S	tate View (8)	⊁ Tasks
Discovered Inventory	Look for:	Find Now Clear 🗙	
III Distributed Applications	State	Name v Slot	-
🐊 Task Status	🕢 Healthy	TestDevice: PowerSupply Module at Slot 1 Slot 1	Actions ^
UNIX/Linux Computers	Healthy	M4K-10.30.52.32: PowerSupply Module at Slot 1 Slot 1	-
👯 Windows Computers	Healthy	M4K-10.30.52.31: PowerSupply Module at Slot 1 Slot 1	Start Maintenan
Agentless Exception Monitoring	A Healthy	M4K-10.30.52.31: PowerSupply Module at Slot 1 Slot 1	Edit Maintenanc
Application Monitoring	Healthy	M1K-10 30 52 5: PowerSundy Module at Slot 1 Slot 1	🔢 Stop Maintenan
Audiocodes Gateways	Healthy	Mills (1) (3) 24 Power Stuppy Module at Stort 1 Stort 1	Personalize view
SW Alerts View	C Line Man	Markada Sata Sata Sata Sata Sata Sata Sata S	
GW Performance View	Healthy	MIA-10-30.52.5 Powersuppy Module 4.51011 SIGT	Tasks ^
III GW State View	Healthy	MIX-10.30.32.11 Powersupping Module at slot 1 Slot 1	Entity Properties
4 🚰 Modules			A Health Explorer
All Modules Alert View			'ana
III Modules State View			Navigation ^
III Fan Tray State View			Alert View
III Power Supply State View			C Discourse Minus
🔛 System Modules State View			S Diagram view
Trunks/Ports			Event View
All Trunk/Ports Alert View			Network Vicinity
Digital Trunks State View			Reformance Vie
Ethernet Ports State View			State View
Data Warehouse			
Microsoft Audit Collection Services			
Microsoft Windows Client			
Microsoft Windows Server			
Network Monitoring			
Operations Manager			
Synthetic Transaction			
UNIX/Linux Computers			
Web Application Transaction Monitoring			
Windows Service And Process Monitoring	Detail Viev	· · · · · · · · · · · · · · · · · · ·	
Show or Hide Views	ille a constant		
New View >	Audioco	aes Power Supply Module properties of LestDevice: PowerSupply Module at Slot 1	
	Display Na	me TestDevice: PowerSupply Module at Slot 1	
Monitoring	Full Path I	lame lestDevice/lestDevice: PowerSupply Module at Slot 1	
	Slot	Slot 1	
/ Authoring	Index	2	
Administration	Key OID	.1.3.6.1.4.1.5003.9.10.10.4.23.1.3.2	
	HW Versio	n	
My Workspace	LED5	1 indeterminate	
	Geograph	ical Position 1	
		<u>×</u>	
Keagy			4

This screen is described as follows:

- Power Supply State View contains all power supply modules of all discovered GWs as they are hosted on the real devices. The data represented in the view can be personalized as described in Section 6.1 on page 55.
- Select a module to load the Detail View pane at the bottom of the Power Supply State View window.
- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.



# 6.6 Trunks/Ports – Digital Trunks State View

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

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

Figure 6-8: Digital Trunks State View

File Edit View Go Tasks Tools Help	s Manager					
Search ▼ _ I Stope Some	Tasks 🕢 _					
Monitoring	Digital Trunks State	View (5)			-	> Tacks
E Discoursed Investory	I look for:	View (5)	Now Clear			
Discovered Inventory	COOK IOI.	Fild	I NOW Clean		×	
Task Statut	State V N	ame	de ek Clek û Dielkel Terrek #3	Alarm		State
UNIX / inux Computers		ark to 20 52 5, and disartaneous Digital Modu	te de side de Digital Hank #2	greybisebled		Actions
Windows Computers	Critical is	11k-10.50.52.5: advietiarit10001FD/gitaliv	Addule at Slot 69: Digital Funk #2	greybisabled		💐 Start Maintenan
Agentless Exception Monitoring	Critical N	11K-10.30.52.1: adMediant1000IFDigitalM	vodule at slot 191: Digital Irunk #2	greyDisabled		📲 Edit Maintenand
Application Monitoring	S Critical N	11K-10.30.52.3: adMediant1000IFDigitalM	4odule at Slot 0: Digital Irunk #2	greyDisabled		18 Stop Maintenan
Audiocodes Gateways	🥸 Critical 🛛 🕅	11K-10.30.52.4: adMediant1000IFDigitalM	4odule at Slot 25: Digital Trunk #2	greyDisabled		Remonalize view
GW Alerts View						Personalize view
CW Performance View						Tasks ^
III GW State View						Entity Properties
4 🚰 Modules						Health Explorer
All Modules Alert View						an meanan exprorem
All Modules State View						Navigation 🔺
Fan Tray State View						Alert View
Power Supply State View						C Diagram View
System Modules State View						
4 🧀 Trunks/Ports						Event view
All Trunk/Ports Alert View						Network Vicinity
Digital Trunks State View						Performance Vie
Data Warehoure						🔢 State View
Microroft Audit Collection Servicer						
Microsoft Windows Client						
Microsoft Windows Server						
Network Monitoring						
Derations Manager						
Synthetic Transaction						
UNIX/Linux Computers						
Web Application Transaction Monitoring						
Windows Service And Process Monitoring	Detail View				~	
Show or Hide Views	Audiocodor	Digital Trunk Class properties of TortDo	vice: acMediant1000IEDigitalModulo at Elot 0: F	Digital Trunk #2	-	
New View 🕨	Audiocodes	orginal matrix class properties of resuber	vice, active dianet to our Digital module at SIOL 0: 1	orginal frame #2		
	Display Name	TestDevice: acMediant1000	htp://www.action.com/action/action/action/action/action/ http://www.action/acti	a: acMadiant1000IEDigitalModule at Slot 0: Digital		
Monitoring	T di Patri Naliti	Trunk #2		a acmediantizooon Digitalmoutile at slot o. Digital		
Authoring	Gateway IP	195.189.192.249				
/ Automig	Index Key OID	1 1 3 6 1 4 1 5003 9 10 9 2 1 1	1111			
i Administration	Led Status Col	or off				
Mu Workspace	Led Status Stat	e Unknown: 10				
wy workspace	Channels	11-11-11-11-11-11-11-11	1-11-11-11-11-11-11			
-	V5 Interface N	.im -1 0v110v110v110v110v110v11	0v11 0v11 0v11 0v11 0v11 0v11 0v11 0v11	0v11.0v11	-	
Ready	V D DITK ID	-0411-0411-0411-0411-0411-				

This screen is described as follows:

- Digital Trunks State View contains all digital trunks of all discovered gateways as they are hosted on the real devices. The data represented in the view can be personalized as described in Section 6.1 on page 55.
- Select a module to load the Detail View pane at the bottom of the Digital Trunks State View window.
- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

# 6.7 Trunks/Ports – Ethernet Ports State View

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

#### To open the Trunks/Ports – Ethernet Ports State View:

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

#### Figure 6-9: Ethernet Ports State View

File Edit View Go Tasks Tools Help	ns Manager	
Search 🔻 🔤 🎼 Scope 💭 Find	Tasks 👔 🔤	
Monitoring	Ethernet Ports State View	Tasks
Discovered Inventory	Q Look for: Find Now Clear	× 🕅 🔊
Distributed Applications	State V Name Port Duplex Mode Port Speed Active Port Nu Port State Power Over Et.	
🕉 Task Status	Healthy Ethernet Port #1 at Sl 195.189.192.240;195.189.192.240.1.3.6.1.4.1.5003.9.10.10.4.21.1.	3.68956 Actions
III UNIX/Linux Computers	Healthy Ethernet Port #1 at Sl., 10.10.50.4; 10.10.50.4; 1.3.6.1.4, 1.5003.9, 10.10.4, 21, 1.3.68956161	= 2
iii Windows Computers	Healthy Ethernet Port #2 at Sl., 195, 189, 192, 240; 195, 189, 192, 240, 1, 3, 6, 1, 4, 1, 5003, 9, 10, 10, 4, 21, 1.	3.68956
Agentless Exception Monitoring	Healthy Ethernet Port #3 at Sl., 10.10.50.4; 10.10.50.4; 1.3.6.1.4; 1.5003,9; 10, 10.4; 21, 1.3.68956161	Edit Maintenand
Application Monitoring	Healthy Ethernet Port #2 at Sl., 10, 10, 50, 4; 10, 10, 50, 4, 1, 3, 6, 1, 4, 1, 5003, 9, 10, 10, 4, 21, 1, 3, 68956161	Stop Maintenan
Audiocodes Gateways	Healthy Ethernet Port #0 at Sl 10.10.50.4; 10.10.50.4; 1.3.6, 1.4, 1.5003,9, 10, 10, 4, 21, 1.3, 68956161	Personalize view
GW Alerts View	Healthy Ethernet Port #3 at Sl., 195, 189, 192, 240; 195, 189, 192, 240, 1, 3, 6, 1, 4, 1, 5003, 9, 10, 10, 4, 21, 1,	3.68956
GW Certe View	Healthy     Ethernet Port #0 at \$1     195.189.192.240:195.189.192.240.1.3.6.1.4.1.5003.9.10.10.4.21.1.	3.68956
a Condular		
All Modules Alert View		
All Modules State View		
Fan Tray State View		
Power Supply State View		
III System Modules State View		
4 📸 Trunks/Ports		
All Trunk/Ports Alert View		
iii Digital Trunks State View		
Ethernet Ports State View		
Data Warehouse		
Microsoft Audit Collection Services		
Microsoft Windows Client		
Microsoft Windows Server		
Operation: Manager		
Synthetic Transaction		
UNIX/Linux Computers		
Web Application Transaction Monitoring		
Windows Service And Process Monitoring	Detail View	~
Show or Hide Views		
New View >	Select an item in the view above to display its details.	
Monitoring		
Authoring		
Administration		
My Workspace		
Peady		
Ready		1.

This screen is described as follows:

- Ethernet Ports State View contains all Ethernet ports of all discovered gateways as they are hosted on the real devices. The data displayed in this view can be personalized as described in Section 6.1 on page 55.
- Select a module to load the Detail View pane at the bottom of the Ethernet PortsState View window.
- Double-click a value in the 'Status' column to open the Health Explorer. For more information, see Chapter 7 on page 15.

### 6.8 Diagram View

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

### **To open the Diagram view:**

- 1. In the Monitoring pane, select **GW State View**, and then select the desired entry.
- 2. In the Tasks pane, under Navigation, select **Diagram View**; a screen similar to the following is displayed:

Saucha	Restar and the second second second		
Tearca a	E ⊕ ₽ @ @ 100%	💽   🏚 🎆 🍕 Layout girection 💌 🍨 Filter by health 👻 Layers 🛡 💽 😰 🦣	CR . Bernel Print .
gram View			Yasks
			400
			Maintenanc _
			Start Maintenani
			NS Stop Maintenany
			Tasks ^
		<b>*</b>	Entity Properties
		TestDevice -	Navination A
			Alert View
			S Diagram View
	•		12 Event View
	12750		TT Network Vicinity
	•		The second second
			Performance Vie
	TestDevice 👻		-
	TestDevice : scMedia_		T.
retail View	TestDevice @		
etail View	TestDevice @	00080 OngitalModule at Stort 0	E XI X
Tetail View	TestDevice & Sector	0000FDigitalModule at Slot 0 dule at Slot 0	
Netail View Audiocodes System Mod Display frame 19 Address	TestDevice adMediationU iscMedia_	0008F0igitalModule at Stot 0 dule at Stot 0	
Petail View Audiocodes System Mod Display fame IP Address Sist	Interface of TestDevice adMedian03 (TestDevice adMedian03) (TestDevice adMedia	00009 DigitatiModule at Slot 0 dule at Slot 0	
Audiocodes System Mod Display fame P Address Slot Index	TestDevice @ TestDevice @ activelia. TestDevice adMediatoDiffigitation 195.1892.249 Sixto 6730795	00080 OngitalModuler at Slot 0 dule at Slot 0	
Autilitotudes System Mod Display Name IP Address Slot Index Key OD	Interface of TestDevice adMedian03 (TestDevice adMedian03) (TestDevice adMedia	0000FDigitalModule at Slot 0 dule at Slot 0 393	
Audiocodes System Mod Disply fame P Address Sist Index Key OD Geographical Position	TestDevice adMediantDoorPolyatMor 19:18/19:20 TestDevice adMediantDoorPolyatMor 19:18/19:20 Set0 6793799 1.3.6.14.15009.0.0.0.4.21.1.3.67877 0	00080 OrigitalMeduler at Stort 0 dule at Stot 0 993	
Autilitotudes System Mod Display Name IP Address Slot Index Key OID Geographical Position Type	Interface of TestDevice adMedianDi TestDevice adMedianDi TestDevice adMedianDi TestDevice adMedianDi Sint 0 67037995 1.3.6.1.4.1.5009.9.10.10.4.21.1.3.673077 0 adMedianDI000PDigitalModule	0000FDigitatModule at Slot 0 dule at Slot 0 393	

Figure 6-10: Diagram View

# 6.9 Running Tasks

This section describes how to perform various tasks.

### 6.9.1 Pinging AudioCodes Device

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

### To execute the ping operation:

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

Figure 6-11: Node Tasks Pane

🖾 GW State View - Audiocodes - Operations Manage	r				<u>,                                     </u>	i la seconda de la se Seconda de la seconda de la	- 🗆 ×
<u>File E</u> dit <u>V</u> iew <u>G</u> o Tas <u>k</u> s <u>T</u> ools <u>H</u> elp							
Search V _ Scope O Find	Tasks						
Monitoring <	GW State View (3)					Tasks	
🔺 🧱 Monitoring 📃	Look for:		Eind Now Clea	ar	×	2	
Active Alerts	State Name	Display Name	Device Version	Device Type		State Actions	*
Discovered Inventory	🛕 Warning		6.60A.024.004	Product: MG 4K		📲 Start Maintenance Mode	_
E Distributed Applications	🛕 Warning M1K-	10.30.52.1 M1K-10.30.52.1	6.40A.058.005	Product: MG 1K		Edit Maintenance Mode Sett	
💑 Task Status	A Warning M4K-	10.30.52.31 M4K-10.30.52.3:	6.60A.024.004	Product: MG 4K		Ston Maintenance Mode	
UNIX/Linux Computers	-						
🗰 Windows Computers						Personalize view	
Agentless Exception Monitoring						Tasks	~
Application Monitoring						Entity Droportion	
Audiocodes Gateways						Enuty Properties	
GW Alerts View						A Health Explorer	
GW Performance View						Navigation	~
Modules						Alert View	
All Modules Alert View						C Diagram View	
III All Modules State View							
🔢 Fan Tray State View						Event view	
🔢 Power Supply State View						Network Node Dashboard	_
🔢 System Modules State View						Network Vicinity Dashboard	=
4 🚰 Trunks/Ports						🔀 Performance View	
All Trunk/Ports Alert View						🔢 State View	
🔢 Digital Trunks State View							
🔛 Ethernet Ports State View 💽	1					Node Tasks	^
Show or Hide Views						Ping	
New View 🕨	Detail View				*	Ping	
	a Audio and an Chill		0 20 52 1		<b>^</b>	Set Device Name	
Monitoring	Audiocodes SNN	IP Device properties of M1K-1	0.30.52.1			Show Active Alarms	
Authoring	Display Name	M1K-10.30.52.1				SNIMP GET	
Authorning	Access Mode	SNMPONLY					
C Administration	Certification	GENERIC				C 2NMP Walk	
Mu Westerner	Description	Product: MG 1K;SW Version	: 6.40A.058.005			L Teinet Console	
wy workspace	Device Key	00-90-8F-13-2E-68				Test Call	
-	Location					Traceroute	Ļ
Ready					•		4

### OR

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

GW State View - Audio	codes - Operation	s Manage	27				
File Edit View Go	asks Tools Help	-					
Sea	State Actions	۰d	🖸 Tasks 🔞 💡				
Monitoring	Tasks	• •	GW State View (3)				⊁ Tasks
a 🌆 Monitoring	Navigation	•	1 1 1 and 6 and 1		Eind Now Clear	×	
Active Alerts	Node Tasks	•	Ping	/ Display Name	Device Version Device T	ype	State Actions
📒 Discovered Inver	Resources	•	Ping		6.60A.024.004 Product:	MG 4K	M Start Maintenance Mode
🔢 Distributed Appl	Help	•	Set Device Name	52.1 M1K-10.30.52.1	6.40A.058.005 Product:	MG 1K	Edit Maintenance Mode Settings
nask Status			Show Active Alarms	52.31 M4K-10.30.52.31	6.60A.024.004 Product:	MG 4K	Stop Maintenance Mode
UNIX/Linux Compute	ters m		SNMP GET				Personalize view
Agentless Exception	n Monitorina		SNMP Walk				
Application Monito	ring	1	Telnet Console				Tasks ^
a 👸 Audiocodes Gatewa	ays	E	Test Call				Entity Properties
SW Alerts View		E	Traceroute				🖀 Health Explorer
GW Performance V	view						Navigation ^
GW State View							Alast Mari
All Modules Aler	tView						Pierce Man
All Modules Stat	e View						Diagram view
🧮 Fan Tray State Vi	ew						Lig Event View
👯 Power Supply St	ate View						Network Node Dashboard
🔢 System Modules	State View						Network Vicinity Dashboard
a 🚞 Trunks/Ports							Performance View
All Trunk/Ports A	lert View						State View
Ethernet Ports St	ate view						Node Tasks
contentec for a si			1				
Show or Hide Views			Detail View			~	
New View +			b claim From			-	Ping Ping
Monitoring			Audiocodes SNM	P Device properties of M1K-1	0.30.52.1		Set Device Name
			Display Name	M1K-10.30.52.1			Show Active Alarms
Authoring			Full Path Name	M1K-10.30.52.1		_	SNMP GET
🙆 Administration			Access Mode Certification	GENERIC			SNMP Walk
			Description	Product: MG 1K;SW Version	: 6.40A.058.005		Teinet Console
My Workspace			Device Key	00-90-8F-13-2E-68			Test Call
			Location			-	Traceroute
Ready						<u></u>	

Figure 6-12: Tasks Menu

The Ping Run Task window is displayed:



up the tack on these targets	
Tuest	
	hun Location
<u>a</u> sk Parameters	
Name	Value
Username DivelD	Admin
PingiP Password	127.0.0.1 Admin
<u>D</u> verride	
	Tack description
Override Isk credentials	Task description
Qverride sk credentials Uge the predefined Run As Account Others:	Task description
Qverride sk credentials Use the predefined Run As Account Other: Use predefined Run As Account	Task description
Override       ask credentials       I use the predefined Run As Account       Other:       User name:	Task description
Override       ask credentials       Uge the predefined Run As Account       Other :       User name :       Password :	Task description
Override       ssk credentials       Uge the predefined Run As Account       Other :       User name :       Password :       Domain :	Task description
Override         ssk credentials         Uge the predefined Run As Account         O ther :         User name :         Password :         Domain :	Task description



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

- 4. (Optional) Override the Username and/or Password for the Telnet connection:
  - a. In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.
  - b. Set the new values for Username and/or Password and Device Name.
  - c. Click the **Override** button.
- 5. In the Run Task window, click the **Run** button; the Task Status Ping window is displayed:

Task Ping		Success m800		sk Target 300			
sk Output					Copy Text	Copy HTI	ML
🕑 Ping			Task De	escri	iption		
itatus:	Success						
icheduled "ime:	12/14/2011 2:36:59	РM					
itart Time:	12/14/2011 2:37:02	PM					
iubmitted By:	SCOM- PROJECT\Administra	tor					
tun As: tun Location: 'arget:							
arget Type:	Audiocodes SNMP De	evice					
lategory:	Custom						
ask Output:							
Output	70 72						Ŀ
L cap close this	dialog at any time	Doina so	will pot in	hterri	int executing ta	sks. Vou cap	

### Figure 6-14: Task Status-Ping

This window contains the Task execution status and output details.

### 6.9.2 Displaying Active Alarms

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

- To display the list of active alarms:
- 1. Open the GW State View (see Section 6.1 on page 55) and select the required gateway.
- 2. Do one of the following:
  - a. In the Node Tasks pane, left-click the **Show Active Alarms** task. OR
  - b. In the Main Menu, choose Tasks > Node Tasks > Show Active Alarms.

The Show Active Alarms Run Task window is displayed:

Run the <u>t</u> ask on these targets		
Target	Run Location	
▼ 10.10.50.2		
<u>a</u> sk Parameters		
Name	Value	
Lise second	Admin	
Usemame Pageword	Admin	
Osemame Password	Admin	
Usemane Password	Admin	
<u>Override</u>	Admin	
Qverride sk credentials	Admin Task description	
Qverride ask credentials Use the predefined Run As Acco Other :	Admin Admin	
Qverride ask credentials Use the predefined Run As Acco Other : User name :	Admin Admin	
Qverride         ask credentials         Image: Use the predefined Run As Acco         Other :         Use rname :         Eassword :	Admin Admin ITask description	
Qverride         ask credentials         Image: User the predefined Run As Accol         Other :         User name :         Leassword :         Domain :         GSTEPS	Admin Admin	

#### Figure 6-15: Run Task-Show Active Alarms



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

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

ask Show Active Alarme	Status	Task Target		
Show Active Alarms	Success	test		
isk Output				🗈 <u>C</u> opy Text 🔋 Copy <u>H</u> TML
Show Active Ala	rms		Task Description	
Status:	Success			
Scheduled Time:	02/11/2010 10:03:0	4		
Start Time:	02/11/2010 10:03:0	6		
Submitted By:	GSTEPS\eduardg			
Run As:				
Run Location:				
Target:				
Target Type:	Audiocodes SNMP D	evice		
Category:	Operations			
Task Output:				
Output				
The socket is no	ot connected.			
-				
None		_		
Exit Code: 0				

Figure 6-16: Task Status-Show Active Alarms

This window contains the Task execution status and output details.

### 6.9.3 Setting Device Display Name

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

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

The Set Device Name Run Task window is displayed:

Figure	6-17:	Set	Device	Name
--------	-------	-----	--------	------

			-2
Run the <u>t</u> ask on these targets		0	Help
Target	Run Location		
☑ 10.10.50.2			
T <u>a</u> sk Parameters			
Name	Value		
DeviceName CommunityString	Device Name private		
Override	Task description		
Qverride	Task description		
<u>O</u> verride Task credentials O Use the predefined Run As Account O Uther :	Task description		
Qverride  ask credentials  Uge the predefined Run As Account  Other:  User name:	Task description		
Override         Task credentials         Image: Use the predefined Run As Account         Other :         User name :         Password :	Task description		
Override         Fask credentials         Image: Second Se	Task description		
Qverride         Fask credentials         Image: Uge the predefined Run As Account	Task description		



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

- 3. (Optional) Override the DeviceName and/or CommunityString:
  - **a.** In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.
  - b. Set the new values for DeviceName and/or CommunityString.
  - c. Click the **Override** button.
- 4. In the Run Task window, click the **Run** button; the Task Status Set Device Name window is displayed:

ask		Status		Task Target	
Set Device Nam		ouccess		10.10.50.2	
ask Output				📄 <u>C</u> opy Text	🗈 Copy <u>H</u> TML
Set Device	Name		Task De	scription	
Status: Scheduled Time: Start Time: Submitted By: Run As: Run Location: Target:	Success 12/12/2010 17:1- 12/12/2010 17:1- GSTEPS\eduardg	4:41 4:44			
Target Type: Category: Task Output:	Audiocodes SNMF Custom	Device			
None					

Figure 6-18: Task Status-Set Device Name

This window contains the Task execution status and output details.

### 6.9.4 Testing Call from Gateway

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

- To test a call from the gateway:
- 1. Open the GW State View (see Section 6.1 on page 55) and select the required gateway.
- 2. Do one of the following:

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

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

The Test Call Run Task window is displayed:

Figure	6-19:	Run	Task –	Test	Call
--------	-------	-----	--------	------	------

T .	<b>D</b> 1 1	
1 arget	Run Location	
10.10.30.4		
r <u>a</u> sk Parameters		
Name	Value	
Usemame	Admin	
Password	Admin	
DTMFs	1234	
DestinationPhoneNumber	987654321	
<u>O</u> verride		
	Tack description	
Use the predefined Run As Account     Out		
© Oth <u>e</u> r :		
User name :		
Password :		
Domain : GSTEPS		
Domain : GSTEPS		



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

- 3. (Optional) Override the Username and/or Password for the Telnet connection:
  - a. In the Task Parameters pane, click the **Override** button; the Override Task Parameters window opens.
  - **b.** Set the new values for the Username and/or Password.
  - c. Click the **Override** button.



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

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

🚵 Task Status - Test Cal	L		
The task completed suc	cessfully.		🕑 Help
Task	Status	Task Target	
Test Call	Success	test	
<u>T</u> ask Output			🗈 <u>C</u> opy Text 🗈 Copy <u>H</u> TML
		Task Description	n
Status:	Success		
Scheduled Time:	02/11/2010 10:04:30	)	
Start Time:	02/11/2010 10:04:33	3	
Submitted By:	GSTEPS\eduardg		
Run As:			
Run Location:			
Target:			
Target Type:	Audiocodes SNMP De	vice	
Category:	Operations		
Task Output:			
Output			
The socket is a	not connected.		
Error			
None			
Evit Code: 0			
LAIL COUE. 0			
			~
You can close this dialo	g at any time. Doing so w	ill not interrupt executing tasks. You	can check the status of tasks in a task status view.
			Close
			45

#### Figure 6-20: Task Status-Test Call

This window contains the Task execution status and output details.
# 7 Monitoring Gateway Element Health

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

## 7.1 Monitoring Types

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

- Queries send from the SCOM to the gateway:
  - **Object-based monitoring** is the polling of a specific SNMP object value change i.e., the acSysModuleOperationalState module-related object is changed. For example, there is a power supply failure for a gateway power supply module.
  - **Threshold-based monitoring** is an alert issued when a threshold defined for a performance counter is exceeded. This type of alert is applicable for gateways and trunks. Each performance counter has two types of thresholds 'High' and 'Low'. Each threshold type has two levels: 'Warning' and 'Critical'. Consequently, the final severity of threshold-based alert depends upon which level of threshold has been exceeded. Thresholds levels are described in Section 7.5 on page 82.
- Traps send from the gateway to the SCOM:
  - **Trap-based monitoring** is an alert issued as a result of a trap that was captured from an entire Gateway entity (Gateway, Module or Trunk).

### Notes:

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

## 7.2 Aggregated Health State

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

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

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



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

## 7.2.1 Aggregated Health State-Gateway

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

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

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

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

#### Table 7-1: Health Indication

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

## 7.3 SNMP-SCOM Object Severity Mapping

### 7.3.1 Gateway

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

### Table 7-2: SNMP Gateway Objects Health State

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

### 7.3.2 Module

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

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

 Table 7-3:SNMP Gateway Modules Objects Health State

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

### 7.3.3 Digital Trunks

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

### Table 7-4: Digital Trunk SNMP Polling

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

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

### 7.3.4 SNMP Traps

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

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

acBoardEthernetLinkAlarm

#### Table 7-5: Unhealthy State

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

Critical

Ethernet ports module

## 7.4 Alert Monitoring

The SCOM Management Pack includes the following active alerts views:

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

### 7.4.1 GW Alerts View

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

- > To view gateway alerts:
- 1. Select the Monitoring pane, and then open the AudioCodes Gateways folder.
- 2. Select the GW Alerts View; a screen similar to the following is displayed:

Monitoring <	GW Alerts View (17)						
🔺 🎫 Monitoring 📃	Look for:	Find Now Clear					×
Active Alerts	🔇 Icon Path	Source	Name	Resolution State	Created	Age	Owner
Discovered Inventory	# Severity: Warning (2)	47.07.02	121.00	Loss of the original	AND MODULES AND	01.257	
11 Distributed Applications	4		Network Device is Not Responding	New	11/6/2013 11:20:59 AM	22 Days, 7 Hours	
💑 Task Status			Audiocodes GW acknowl ConfigurationError Monitor Net	Manar	1101/0113 1-15-07 PM	8 Dave 5 Maures	
UNBALinux Computers	A A A A A A A A A A A A A A A A A A A		Autocours shi accouraconingereconcritor monitor were	THEW	10/20/2015 E15/07 PM	e pleys, o hours,	
11 Windows Computers	a serency: Critical CES			1944-000			
Agentiess Exception Monitoring			Audiocodes GW Severity Monitor Alert	New	11/5/2013 10:14:00 AM	23 Days, 8 Hour	
<ul> <li>Application Monitolog</li> </ul>			Audiocodes GW Seventy Monitor Alert	New	11/7/2013 3:46:00 PM	21 Days, 2 Mour	
Applications	3 03-90-0F-0A-93-53	: PowerSupply Module at Slot 2	Audiocodes Power Supply Seventy Monitor Alert	New	11/10/2013 9:37:00 AM	18 Days, 8 Hour	
NETMonitoring	8		Audiocodes GW Severity Monitor Alert	New	11/10/2013 9:37:00 AM	18 Days, 8 Hour	
Web Application Availability Monitorie	0		Audiocodes GW Severity Monitor Alert	New	11/14/2013 11:24:00 AM	14 Days, 7 Hour	
<ul> <li>Audiocodes Gateways</li> </ul>	0		Audiocodes GW Severity Monitor Alert	New	11/14/2013 3:56:00 PM	14 Days, 2 Hour	
GWAlerts View	8 03-90-8F-22-17-D7	: PowerSupply Module at Slot 2	Audiocodes Power Supply Severity Monitor Alert	New	11/15/2013 4:55:00 PM	9 Days, 1 Hour,	
GW Performance View			Audiocodes GW Severity Monitor Alert	New	11/13/2013 6:55:01 PM	8 Days, 23 Hour	
E. GW State View	03.93.85.16.08.0B	: PowerSupply Module at Slot 2	Audiocodes Rower Supply Severity Monitor Alert	New	11/18/2013 7:04:03 PM	8 Davi 23 Hour.	
4 💭 Modules			Audiocodes arth Chappel Status Monitor Alert	New	11/28/2013 1-26-94 PM	& Dave & Hours	
All Modules Alert View	ä		Blacked Channels Migh Tracked Member dist	Manual	11/01/0012 412/02 04	7 David 2 Marcan	
All Modules State View			biologia chemica mgi nestrona manton vent	New	ALCOLOGIA ALCOL PM	r weys, a Hours,	
till Fan Iray State View			Additionales over sevency Monitor Aden	NEW	10202013 12:33:05 PM	1049, 5 Hours,	
Power Supply State View			Audiocodes GW Severity Monitor Alert	New	11/28/2013 11:45:03 AM	6 Hours, 44 Min	
11 System Modules State View			Audiocodes GW Severity Monitor Alert	New	11/28/2813 12:32:02 PM	5 Hours, 57 Min	
Inunks/Ports	8		Network Device is Not Responding	New	11/21/2013 5:50:27 PM	39 Minutes	
All Trunk/Ports Alert View							
The provide the state state							
Enternet Ports State view							
a ca bata watenouse	-						
D All Control of the							
See Calls diag Badamaan							
Collection Performance							
Service Contention Parlaments							- 12 V.
Microsoft Audit Collection Senior							×
Microsoft Windows Clent	Alert Details						Υ.
* )							
Show or Hide Views	Select an item in the view above to	display its details.					
New View >							
1122-07355-2							

### Figure 7-1: GW Alerts View

3. Select a specific Alert; the Alert Details are loaded:



-	Alert Details		ů
	Audiocodes GW actioardConfigurationError Monitor Alert	Alert Description	-
tomos .	Source: S Full Tahh Name: Arel Moniton Additional State ConfigurationError Munitor Created: 11/20/2015 1:15:07 PM		
	Knowledge: No knowledge was available for this alert.	View additional knowledge	
•	Hide knowledge		

4. Click on the **View additional knowledge** Link to view additional information on the alert. The Alert Properties are displayed:

🔡 Alert Properties	X
General Product Know	vledge   Company Knowledge   History   Alert Context   Custom Fields
Audiocodes	GW acBoardConfigurationError Monitor Aleit
Key Details:	
Alert source:	
Severity:	Warning
Priority:	Medium
Age:	8 Days, 5 Hours, 4 Minutes
Owner:	Change
Ticket ID:	
Alert Description:	
	×
Alert Status: Once you have identif the system once chang	ied the problem and taken corrective action, you can select 'Closed' which will remove the Alert from jes are committed.
New	
Previous	ext OK Cancel Apply

Figure 7-3: Alert Properties

Additional Information may be displayed in the Alert Description pane.

## Caudiocodes

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

	any Know	ledge History Alert Context Custom Fields
Source	10	.15.21.15
Destination	12	7.0.0.1
/ersion	2	
ErrorCode	Su	ICCESS
Object Identifier	Syntax	Value
1.3.6.1.2.1.1.3.0	Timeticks	\$ 52094533
1.3.6.1.6.3.1.1.4.1.0	Oid	.1.3.6.1.4.1.5003.9.10.1.21.2.0.2
1.3.6.1.4.1.5003.9.10.1.21.1.1.0	Integer	1
1.3.6.1.4.1.5003.9.10.1.21.1.2.0	Octets	PSTNCheckClockMaster: Clock might be un-stable - Trunk 0 is set as acCLOCK_MASTER_OFF while TDMBusClockSource is Internal. [Tru
1.3.6.1.4.1.5003.9.10.1.21.1.3.0	Octets	Board#1
1.3.6.1.4.1.5003.9.10.1.21.1.4.0	Integer	1
1.3.6.1.4.1.5003.9.10.1.21.1.5.0	Integer	4
1.3.6.1.4.1.5003.9.10.1.21.1.6.0	Integer	4
1.3.6.1.4.1.5003.9.10.1.21.1.7.0	Integer	56
1.3.6.1.4.1.5003.9.10.1.21.1.8.0	Octets	
1.3.6.1.4.1.5003.9.10.1.21.1.9.0	Octets	
1.3.6.1.4.1.5003.9.10.1.21.1.10.0	Octets	

Figure 7-4: Alert Properties-SNMP Information

6. If you wish to configure the Alert Monitor, in the Alert Details screen, click the Alert Monitor, for example, click the **Audiocodes GW acBoardConfigurationError Monitor** link as shown in the figure below.

Figure 7-5: Gateway Monitor Alert Details

Alert Details		~
Audiocodes GW actiondConfigurationError Monitor Alert	Alert Description	1
Source Ref Autocodes GW actoardConfigurationError Monitor Arol Monitor Creates: L2020013 115:07 PM		
Knowledge:	III View additional knowledge	
No knowledge was available for this alert.		
<ul> <li>Hide knowledge</li> </ul>		

The gateway alert monitor properties are displayed:

Figure 7-6: Gateway	Alert Monitor	Properties
---------------------	---------------	------------

udiocodes GW acBoard(	ConfigurationError Monitor Properties
eneral Health Alerting	Diagnostic and Recovery   Configuration   Product Knowledge   Overrides
1	
General properties	
Specify the name and dea	scription for the monitor you are creating.
Name:	
Audiocodes GW acBoard	dConfigurationError Monitor
Description (optional):	
	-
Management pack:	Audiocodes GW Management Pack
Monitor target:	
Audiocodes SNMP Devic	ce Select
Parent monitor:	
	•
Configuration	
Configuration	
Configuration Monitor is enabled	

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

## 7.4.2 All Modules Alerts View

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

- To view alerts for all modules:
- 1. Select the **Monitoring** pane, and then open the **AudioCodes Gateways** folder.
- 2. Select the **All Modules Alerts View**; a screen similar to the following is displayed:

Figure 7-7: All Modules Alert View

Each Organization     Each Organiza	M AII Mooulies Aler Yiew - Audiocodes - Uper Actions Manager ■								
Interview of the second sec	Search V Overrides V	Scope D Fin	d 🗊 Tasks 🙆						
Mentoning	1 + + + + + + + + + + + + + + + +	H							
I Diedwarden Austriku   I Diedwarden Stelakova   I Diedwarden St	Monitoring	< All Modules /	Alert View (5)	_					Tasks
In Distributed Application   Im Distributed Application   Im Mark Distribut	Discovered Inventory	Look for:		Find Nov	v Clear			×	2
<ul> <li>Streethy Control State View</li> <li>Addredicts State View</li> <li>Streethy Control State View</li> <li>Streethy Cont</li></ul>	Distributed Applications	🚯 Icon Sou	urce		Name	Resolution State	Created	A	Alert .
Implicing the second	Task Status	🖉 🔺 Severity: C	Critical (5)						Actions
<ul> <li>Mutodavis Angrieges Mutodavis Angrigen Mutodavis Age.</li> <li>Agentiestis Methodavis Agenti Mutodavis Agenti Agenti Agenti Agenti Agenti Agenti Agenti Agenti</li></ul>	UNIX/Linux Computers	🛛 🔞 м1	K-10.30.52.1: acMediant1000IFDigitalMo	dule at SI	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:08:00	4	Start Maintenar
<ul> <li>Marchess Magnomination</li> <li>Application Monitory</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51 Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148737</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51 Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51 Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51 Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51 Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51.0: b Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51.0: b Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51.0: b Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Mais 20.852.5: so Mediant 2009/Digital Module at 51.0: b Audiocodes Digital Trunk Alarm Monitor Alett New 01,002/2013 148730</li> <li>Models State View</li> <li>Models State View</li> <li>Monor 2000 State View</li> <li></li></ul>	Agentiers Exception Monitoring	🛛 🔞 м1	K-10.30.52.5: acMediant1000IFDigitalMo	dule at SI	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:07:37	4	Edit Maintenan
Mul: 13.33:2.3: xdM.damt100007 OptishModule x 31 Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor Ater. New 0.012/2013.14:55:00 Wil: 50.30:2.3: xdM.damt10007/0ptishModule x 51.c Audiocode: Digital Trunk Atam Monitor At	Application Monitoring	🛛 🔞 м1	K-10.30.52.4: acMediant1000IFDigitalMo	dule at SI	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:07:37	4	Stop Maintenar
Work Alerts View   Work Views   Wiew   Work Views   Work Views   Work Views   Work Views	Audiocodes Gateways	🔞 м1	K-10.30.52.3: acMediant1000IFDigitalMo	dule at SI	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:07:36	4	
W Performance View   I W OND dues   I W OND dues State View   I Al Modules State View   I Al Modules State View   I Power Sophy State View   I System Modules State View   I System Modules State View   I Digital TransState View   I Digital TransState View   I Digital TransState View   I Digital TransState View   I Digital Collection Services   I Microsoft Mudows Serve   I Microsoft Mudows Serve   I Web Application Transaction Montoring   I Microsoft Web Application Transaction Montoring   I Microsoft Web Application Transaction Montoring   I Microsoft Web Application Transaction Montoring   I Microsoft Web	GW Alerts View	😵 Tes	tDevice: acMediant1000IFDigitalModule	at Slot 0:	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 14:55:00	7	To Overrides •
Workster View   A Modules   Mathematical State View   Ha Modules State View   Ha Modules State View   Ha Modules State View   Ha Modules State View   Ha System Modules State View   Ha System Modules State View   Ha Displate Tranks Ports   Displate Modules State View   Ha Displate Tranks Ports   Ha Truck Ports   Ha Modules State View   Ha Displate Truck State View   Ha Displate Truck State View   Ha Modules State View   Ha Displate Truck State View   Ha Displate Truck State View   Ha Modules State View   Ha Displate Truck State View   Ha Displate Truck State View   Ha Displate Truck State View   Ha Modules State View   Ha Displate Truck State View   Ha Displate Truck State View   Ha Modules State View   Ha Displate Truck State View   Ha Modules State View   Ha Ma Modules State View   Ha Ma Ma Ma Ma Ma Ma Ma Madules State View   Ha Ma	🗺 GW Performance View								Personalize viev
Modules n   Modules Aett ven   Modules Aett ven   Modules Satt Vens   Modules Satt Vens   Modules Satt Vens   Modules Satt Vens   Modules Satt Vens <t< td=""><td>GW State View</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Subscriptio</td></t<>	GW State View								Subscriptio
Palmaduer Alert View Authoring	4 🚰 Modules								n
III Al Modules State View   III numk/Ports State View   III System Modules State View System View S	All Modules Alert View								💮 Create
If on infly state view   If on infly state views   If on infly state view   If on infly s	All Modules State View								Modify
Inder Subply Subpl	Fan Tray State View								
Spread and the state of the second seco	System Modules State View								
All Turk/Forts Alett View Digital Turk/Forts Alett View Digital Turk/Forts State View Digital Turk/State View Digital Turk/	A C Trunks/Ports								
	All Trunk/Ports Alert View								
Electronic Ports State View Dia Marcosoft Windows Client Dia Marcosoft Windows Stever Stever Authoring Dia Marcosoft Windows Stever Select an item in the view aboveto display its details. Dia Marcosoft Windows Stever Dia Marcosoft Windows Stever Select an item in the view aboveto display its details. Dia Marcosoft Windows Stever Dia Marcosoft W	Digital Trunks State View								
<ul> <li>Deta Warehouse</li> <li>Microsoft Windows Server</li> <li>Deta Warehouse Manager</li> <li>Deta Manager&lt;</li></ul>	Ethernet Ports State View								
<ul> <li>Microsoft Murdows Cliertion</li> <li>Microsoft Windows Server</li> <li>Microsoft Windows Server</li> <li>Methods Server Analysis Analysis</li> <li>Alert Details</li> <li>Show or Hide Views</li> <li>New View &gt;</li> <li>Select an item in the view above to display its details.</li> </ul>	Data Warehouse								
Image: Service And Microsoft Windows Science       Image: Service And Microsoft Windows Science         Image: Service And Process Monitoring       Image: Service And Process Monitoring         Image: Service And Process Monitoring       Image: Service And Process Monitoring         Image: Service And Process Monitoring       Image: Service And Process Monitoring         Image: Service And Process Monitoring       Image: Service And Process Monitoring         Image: Service And Process Monitoring       Image: Service And Process Monitoring         Image: Monitoring       Image: Service And Process Monitoring	Microsoft Audit Collection Services								
Image: Server Control   Image: Server Control   Image: Control	Microsoft Windows Client								
Image: Service And Process Monitoring         Image: Authoring         Image: Authoring         Image: Authoring         Image: Authoring         Image: Authoring         Image: Mixed Authoring         Image: Mixed Authoring         Image: Mixed Authoring         Image	Microsoft Windows Server								
P       Operation Managet         P       Montoring         P       Administration         P       My Workspace         P       Operation Managet         P       Operation Man	Network Monitoring								
Authoring	Operations Manager      Synthetic Transaction								
Wey Application Transaction Monitoring     Windows Service And Process Monitoring     Mert Details     Show or Hide Views.     New View      Select an item in the view above to display its details.     Select an item in the view above to display its details.     Select an item in the view above to display its details.	UNIX/Linux Computers								
<ul> <li>Alert Details</li> <li>Show or Hide Views_ New View &gt;</li> <li>Select an item in the view above to display its details.</li> <li>Select an item in the view above to display its details.</li> <li>Select an item in the view above to display its details.</li> </ul>	Web Application Transaction Monitoring	1						F	
Show or Hide Views New View >  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.  Select an item in the view above to display its details.	Windows Service And Process Monitoring	Alert Det	ails					~	
New View > Select an item in the view above to display its details.	Show or Hide Views_								
Monitoring       Authoring       Authoring       My Workspace	New View	(i) Selec	t an item in the view above to display its	details.					
Monitoring  Authoring  Authoring  My Workspace  Reaf									
Authoring  Administration  My Workspace  Parter	Monitoring								
Autoring  Autoring Autoring  Autoring Autoring  Autoring  Autoring  Autoring  Autoring  Autoring  Autoring Autoring Autoring Autoring Autoring Autoring Autoring Autoring Autor		-							
Administration     My Workspace	Authoring								
My Workspace	🚳 Administration								
- Pashr	K Wy Workspace								
Davide and D		-							
Nooy //	Ready								

3. Select a specific Alert; the Alert Details are loaded.

#### Figure 7-8: Power Module Alert Details

-1	Alert Details		¥
	Audiocodes Power Supply Severity Monitor Alert	Alert Description	<u>^</u>
Print I	Source: PowerSupply Module at Stort 2 Full Table VenewSupply Module at Stort 2 Acet Monitor Created: 11/02/013 9:37:00 AM		
	Knowledge:	View additional knowledge	
	No knowledge was available for this alert. Hide teavleige		

- 4. Click the View additional knowledge link to view additional details on the alert.
- 5. If you wish to configure the Alert Monitor, in the Alert Details screen, click the Alert Monitor, for example, click the **Audiocodes Power Supply Severity Monitor** link as shown in the figure above.
- 6. Select the **Overrides** tab to override the monitor. For more information, see Chapter 8 on page 91.

### 7.4.3 All Trunks/Ports Alerts View

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

- > To view alerts for all trunks/ports:
- 1. Select the **Monitoring** pane, and then open the **AudioCodes Gateways** folder.
- 2. Select the **All Trunk/Ports View**; a screen similar to the following is displayed:

Figure 7-9: All Trunk/Ports View

Image: Trunk/Ports Alert View - Audiocodes - Operations Manager       Image: Trunk/Ports Alert View - Audiocodes - Operations Manager								
Search w Overrider w	Scone End El Tacke	0						
3 Search - ≜ i Alexander - ≜ i Me volde [N - Linda] [C - Linda] (C - Linda								
Monitoring   All Trunk/Ports Alert View (64)  Tasks								
Discovered Inventory	🛛 🔍 Look for:	Find Now Clear				×	0	
1 Distributed Applications	Source	Name	Resolution State	Created	Age 🛆		Alert	
💐 Task Status	A Severity: Critical (64)		1	1		1	Actions	
UNIX/Linux Computers	M1K-10.30.52.1:	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:08:00	4 Hours, 25 Min		Start Maintenar	
Windows Computers	M1K-10.30.52.5:	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:07:37	4 Hours, 25 Min			
Agentless Exception Monitoring	M1K-10.30.52.4:	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:07:37	4 Hours, 25 Min		Edit Maintenan	
Application Monitoring	M1K-10.30.52.3:	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 18:07:36	4 Hours 25 Min		Stop Maintenar	
Audiocodes Gateways	TestDevice: arM.	Audiocodes Digital Trunk Alarm Monitor Alert	New	01/01/2013 14:55:00	7 Hours 38 Min		🐻 Overrides 🕨	
GW Reformance View	M1K-10 30 52 5	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	01/01/2013 04:55:37	17 Hours 37 Mi	1	🔟 Personalize viev	
GW State View	M1K-10.30.52.4	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	01/01/2013 04:55:32	17 Hours 37 Mi		Cubanintia	
4 🚰 Modules	M1K-10.30 52 3	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	01/01/2013 04:55:21	17 Hours 37 Mi		n	
All Modules Alert View	M1K 10 20 52 1	Audiocodes Digital Trunk Alarm Monitos Alert	Closed	01/01/2012 04:55:21	17 Hours 27 Mi	_	Sec.	
III Modules State View	MIK-10.30.52.5	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 17:24:22	1 Days 5 Harris		Or Create	
III Fan Tray State View	MIK-10.30.52.5:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 17:24:25	1 Day, 5 Hours,		Modify	
Power Supply State View	MIK-10.30.52.4	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 17:24:15	1 Day, 5 Hours,			
System Modules State View	MIK-10.30.52.3:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	51/12/2012 17:24:01	I Day, 5 Hours,			
Trunks/Ports	M1K-10.30.52.1:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 17:21:22	1 Day, 5 Hours,			
All Trunk/Ports Alert View	M1K-10.30.52.5:	Audiocodes Digital Irunk Alarm Monitor Alert	Closed	31/12/2012 12:27:46	1 Day, 10 Hours			
Digital Trunks State View	M1K-10.30.52.4:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 12:27:46	1 Day, 10 Hours			
Ethernet Ports State View	M1K-10.30.52.3:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 12:27:37	1 Day, 10 Hours			
Data warehouse	M1K-10.30.52.1:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 12:27:15	1 Day, 10 Hours			
Microsoft Mindows Client	M1K-10.30.52.3:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 11:39:00	1 Day, 10 Hours			
Microsoft Windows Server	M1K-10.30.52.1:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 11:39:00	1 Day, 10 Hours			
Network Monitoring	M1K-10.30.52.4:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	31/12/2012 11:28:11	1 Day, 11 Hours			
Operations Manager	M1K-10.30.52.4:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	30/12/2012 12:26:45	2 Days, 10 Hour			
Synthetic Transaction	M1K-10.30.52.3:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	30/12/2012 12:26:28	2 Days, 10 Hour			
DINIX/Linux Computers	M1K-10.30.52.1:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	30/12/2012 12:25:57	2 Days, 10 Hour			
Veb Application Transaction Monitoring	M1K-10.30.52.5:	Audiocodes Digital Trunk Alarm Monitor Alert	Closed	30/12/2012 12:25:57	2 Days, 10 Hour	-		
Windows Service And Process Monitoring	Alert Details					~		
Show or Hide Views								
New View +	Select an item in the	view above to display its details.						
Monitoring								
Authoring								
Administration								
🔣 My Workspace								
-								
Pandy						_		

3. Select a specific Alert; the Alert Details are loaded.

#### Figure 7-10: All Trunk/Ports Alert Details

Ľ,	Alert Details & Audiocodes Digital Trunk Alarm Monitor Alert	Alert Description	*
	Source: Stated ant BOOT PR/Module at Slot 1: Digital Trunk #3 Full RAIn Name: V schedamt BOOT PR/Module at Slot 1: V schedamt BOOT PR/Module at Slot 1: Digital Trunk #3 Acted Monitor: Acuted Scote Digital Trunk Astern Monitor Created: 11/2020/03.3.01:56 PM	Trunk is in greyDisabled state	
	Knowledge: No knowledge was available for this alert.	III View additional knowledge	
٠	no romage		

- 4. Click the View additional knowledge link to view additional details on the alert.
- 5. If you wish to configure the Alert Monitor, in the Alert Details screen, click the Alert Monitor, for example, click the **Audiocodes Digital Trunk Alarm Monitor** link as shown in the figure above.
- 6. Select the **Overrides** tab to override the monitor. For more information, see Chapter 8 on page 91.

## 7.5 Performance Monitoring

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

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

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

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

### 7.5.1 Performance View

This section describes the performance view.

- To open the Performance View,
- In the Monitoring pane, select **GW Performance View**.

Figure	e 7-11: GW	Performance	View
--------	------------	-------------	------

8		G	W Performance View	- Lync15grp -	Operations Ma	anager			×
Eile Edit View Go Tasks Ioo	ls <u>H</u> elp								
Search * 💡 👫	Scope Plant Tasks 📦 :								
Monitoring <	GW Performance View								<ul> <li>Tasks</li> </ul>
🖌 🌉 Monitoring									2 0
Active Alerts	20-								Performance
Discovered Inventory									Actions
Task Status	1000								🙀 Save Image As
UNIX/Linux Computers	15-								Copy Image to Clipt
👯 Windows Computers									Copy Data to Cipbo
Agentless Exception Monitori									📰 Select Time Range
<ul> <li>Application Monitoring</li> </ul>	10								Fersonalize view
Audiocodes Gatewas									Province of the
GW Alerts View									Baseline
GW Performance View									III Repume the Baselin
E GW State View									II Paule the Baseline
a 🔛 Modules	22.5								$ k_{\rm c}\rangle$ Reset the Baseline
All Modules Alert View	12/9/2015 3:50. 12/9/201	5 3.55_ 12/9/2015 4:00_ 12/9/201	5 4:05. 12/9/2015 4:10.	12/9/2015 4:15. 12	29/2015 4:20. 12	9/2015 4:25	12/9/2015 4:30.	12/9/2015 4:35, 12/9/2015 4:40, 12/9/2015 4:45,	Report Tasks
Fan Tray State View									Agent Counts by Da
E. Power Supply State View	Legend								Alert Looping Laten
5 System Modules State Vie	Look for: All Items	•	×						Alerts
Trunks/Ports	Show Color Path Ta	rget Rule	Object	Counter	<ul> <li>Instance</li> </ul>	Scale	Baseline		Availability
Digital Trucks State View	10.	.33.4.23 Audiocodes No	Gateway	NoRoute Calls I	10.33.4.23	1x	No		Confouration Chan
Ethernet Ports State View	10.	.33.4.23 Audiocodes No	Gateway	NoRoute Calls T.	10.33.4.23	Tx.	No		Tata Volume by Ma
p 🙀 Data Protection Manager 200	10.	.15.50.180 Audiocodes No	Gateway	NoRoute Calls T.	. 10.15.50.180	Tx.	No		Data Volume by Wo
	10.	.33.4.23 ICMP Ping Resp	ICMP Ping	Response Time (.	5	1x	No		T Basel Analysis
Show or Hide Views	10.15.50.180 IPC	Sroup (0) Audiocodes acP	IPGroup (0)	SIP IP Group Invi.	10.15.50.180	T.c	No		RT House
New View a	00-90-8F-2E-EE-22 IPC	Sroup (1) Audiocodes acP	IPGroup (1)	SIP IP Group Invi.	10.33.4.23	18	No		The means
Record Control of Cont	00-90-8F-2E-EE-22 IPO	Group (2) Audiocodes acP	IPGroup (2)	SIP IP Group Invi.	10.33.4.23	1x	No		
Monitoring	10.15.50.180 IPC	Group (1) Audiocodes acP	IPGroup (1)	SIP IP Group Invi.	10.15.50.180	1x	No		
Authoriza	00-90-39-2E-EE-J2 IPG	Sroup (0) Audiocodes acP	IPGroup (D)	SIP IP Group Invi.	10.55.4.25	14	No		-
2 Automag		Group (U) Audiocodes acP	IPGroup (0)	SIP IP Group Inv.	10.33.4.33	14	No		
Reporting	00-90-8P-2E-EE-22 IPC	Stoup (1) Audiocodes acP	IPGroup (0)	SIP IP Group Inv.	10.15.50.180		No		
Administration	0.90.0F.2E.FE.22 180	Stoup (7) Audiocodes acP	IPGroup (2)	SIP IP Group Invi	10.33.4.23	14	No		
17	00.90.8F.2E.FF.33 ID	Group (1) Audiocodes arD	IPGroup (1)	SIP IP Group Intt	. 10.33.4.23	14	No		
My Workspace	00.90.3F-2E-EE-32 IPC	Sroup (0) Audiocodec acP	IPGroup (D)	SIP IP Group Inst	. 10.33.4.23	1x	No		
	00-90-0F-2E-EE-22 IPG	Group (2) Audiocodes acP	IPGroup (2)	SIP IP Group Invi.	10.33,4.23	1x	No		

#### Note:

- The 'Object' field displays the IP Group index, on IP Group counters, and the SRD name on SRD counters.
- IP Group name is not displayed in the SCOM.

- Right-clicking the graph opens the Personalize View and other options which allow you to customize the graph.
- The GW Performance View allows you to view gateway performance counters behavior. In the Legend window, you can select one or more counters to view them on the graph. Each counter on the graph has its own color. Using the 'Look for:' filter, you can limit the Legend to show only the counters on the graph (Items in the Chart) or only the counters which are not shown on the graph (Items not in the Chart) or specific counters (Items by text search). By default, all counters are available for selection in the Legend window (All Items).
- The GW Performance View provides updated information on most counters every 15 minutes. Counters for Channels provide updated information per minute. A graph can be refreshed manually (F5) or automatically.

## 7.6 Rules Monitoring

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

Authoring	<ul> <li>Rules (282)</li> </ul>						
a 📝 Authoring	Management pack objects are now so	oped to: Audio codes acTr	unkPack-3PM2080 Module, Aut	liocodes actrunkPack-MEDGANT2000 Mod	dule, Audiocodes Analog Tr	unk Class, Audiocodes CPU Module, Audiocodes DCh	ennel Class, Audiocodes Digital Tr., Change Scope 🗙
🗈 😁 Management Pack Templates	Q Look for:	Find Now	Clear				×
2 Distributed Applications	Name		Inherited from	Management Pack	Created	Enabled by default	<u> </u>
Construct A set of the set o	Look for:     There     Super Autocodes Dightal Tunk Class     Audiocodes Dightal Tunk Class     Audiocodes Dightal Tunk Classed     Audiocodes Dightal Tunk Classed     Audiocodes Dightal Tunk Classed     Audiocodes Attempted Culti Turk     Audiocodes Internances Culti TUP	Channels Counter Rule Channels Counter Rule Channels Counter Rule Chorbe Rule Dab Counter Rule	Cher Jebertenfinen Austicoster Digital Turuk- Austicoster Digital Turuk- Austicoster Digital Turuk- Austicoster Digital Turuk- Austicoster Staff Dester Austicoster Staff Dester	Management Pack. Auditocolor (IW Management Pack Auditocolor (IW Management Pack	Created 11/4/2013 103/05 PM 11/4/2013 100/05 PM 11/4/200 PM 11/4/2	Evabled by default Ves	×
	Audiosocies JRADNE (cisi SUPIC Audiosocies Ikiliuti (cisi SUPIC Audiosocies Ikiliuti (cisi SUPIC Audiosocies Ikilier (cisi SUPIC Audiosocies Ikilier (cisi SUPIC Audiosocies Ikilier (cisi SUPIC Audiosocies Ikiliuti (cisi SUPIC	nter Rule ounter Rule Counter Rule MC Counter Rule nter Rule Li Counter Rule Li Counter Rule ounter Rule Counter Rule	Audiocodes SNMP Device Audiocodes SNMP Device	Audioodes GM Management Rad Audioodes GM Management Rad	12/4/2013 3:03:55 FM 12/4/2013 3:03:55 FM	Yes Yes Yes Yes Yes Yes Yes Yes	

### Figure 7-12: Rules Monitoring

### 7.6.1 SIP Performance Monitoring Counters

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

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

## 7.6.2 Trunk Service Information

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

## 7.7 Threshold Monitoring

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

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

- When the monitor reaches its HighWarningLevel threshold
- When the monitor reaches its HighCriticalLevel threshold
- When the monitor reaches its LowWarningLevel threshold
- When the monitor reaches its LowCriticalLevel threshold

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



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

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

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

### Table 7-6: Alarm States

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

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

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



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

### > To configure the threshold values:

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

Realth Explorer for						
🕜 Reset Health 📆 Recalculate Health 🛐 Filter Monitors 🕢 Refresh 🔜 Properties 😧 Help 👔 🐻 Overrides 👻						
Health monitors for						
Scope is only unhealthy child monitors.	Knowledge	State Change Events				
4 🐼 Entity Health - 00-90-8F-22-17-D7 (Object)						
a 🔞 Availability - 00-90-8F-22-17-D7 (Object)						
a 🔞 Audiocodes GW Power Supply Dependency Monitor - 00-90-81						
a 🔞 Entity Health - : PowerSupply Module at Slot 2 (Objed)						
🔺 🔞 Availability - : PowerSupply Module at Slot 2 (Objed)						
🐼 Audiocodes Power Supply Severity Monitor - : PowerSupp						
😵 Audiocodes GW Severity Monitor - 00-90-8F-22-17-D7 (Audioc						

Figure 7-13: Health Monitor-Initial View



**Note:** You can also configure thresholds for performance monitors in the Monitors window (**Authoring** > **Monitors**); however, this method is easier if you are currently in the Monitoring pane.

## **C**audiocodes

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



#### Figure 7-14: Health Monitor-Expanded View

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

🕽 Audiocodes Attempted Calls IP2Tel High Treshold Monitor Properties 🛛 🛛 🔀
General Health Alerting Diagnostic and Recovery Configuration Product Knowledge Overrides
view all overrides applied to each by opening the summary dialog.
Choose the monitor, diagnostic or recovery from the list below for which you want to apply overrides for or view summary on:
Monitor (Audiocodes Attempted Calls IP2T el High Treshold Monitor)
Disable Override View summary
Examples
Disable a monitor: I want to disable monitor for all Windows Computers.
Override a diagnostic: I need to override this diagnostic for one of my Windows Computers.
View summary of a recovery: I need to view the objects this recovery has been enabled for.
OK Cancel Apply

#### Figure 7-15: Threshold Monitor Properties

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

### Figure 7-16: Override Thresholds

Disable	Override		For the object: 00-90-8F-30-4B-67
			For all objects of class: Node
			For a group
tor for all Windows Lomputers. this diagnostic for one of my Window			For a specific object of class: Node
			For all objects of another class

Choose one of the following options:

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

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

The Override Properties window is displayed:

#### Figure 7-17: Override Properties - High Threshold Monitor

regory: remides target:	Category: Custom					
venues target:	Custom					
	object.					
verride-controll	ed parameters:	During	D.C. IV-L	0	Effective Meloc	Cl
Uvern	de Parameter Name -	Fourmerstion	Match monit	Match monito	Match monitor	Unange Status
	Alert Severity	Boolean	True	True	True	[No change]
	Enabled	Boolean	Falca	Falca	Falca	[No change]
	Generates Alert	Boolean	Тпре	Тпе	True	[No change]
	HighCriticalLevel	Integer	25	25	25	[No change]
	HighWarningLevel	Integer	10	10	10	[No change]
	IntervalSeconds	Integer	900	900	900	[No change]
	SyncTime	String	12:00	12:00	12:00	[No change]
etails: E <b>nabled</b> The parameter	is not set by a custom ove	Tride or by a	cription			Ec
etails: Enabled The parameter management pa is the default va	is not set by a custom ove ack. The effective value o alue of this parameter.	rride or by a of this parameter	cription			Ec
etails: <b>Enabled</b> The parameter management pa is the default va	is not set by a custom ove ack. The effective value o alue of this parameter.	rride or by a of this parameter	cription			Ec
etails: Enabled The parameter management p is the default va	is not set by a custom ove ack. The effective value o alue of this parameter.	Prride or by a fithis parameter	cription			Ec
retails: Enabled The parameter management pa is the default va 1anagement	is not set by a custom ove ack. The effective value o alue of this parameter.	Present of this parameter	cription			Ec
Details: Enabled The parameter management pa is the default va Management	is not set by a custom ove ack. The effective value o alue of this parameter. <b>pack</b>	Preserved and the parameter of this parameter	cription			Ec

Override	Propertie	5					×
Monitor n	iame:	Audiocod	es Attempted Calls IF	2Tel Low Tresho	old Monitor		
Category:	:	Custom					
Overrides	s target:	Object:					
Override-	Override-controlled parameters:						
	Override	Parameter Name 🗠	Parameter Type	Default Value	Override Value	Effective Value	Change Status
		Alert severity	Enumeration	Match monit	Match monito	Match monitor	[No change]
		Auto-Resolve Alert	Boolean	True	True	True	[No change]
•		Enabled	Boolean	False	False	False	[No change]
		Generates Alert	Boolean	True	True	True	[No change]
		IntervalSeconds	Integer	900	900	900	[No change]
		LowCriticalLevel	Integer	-1	-1	-1	[No change]
		LowWarningLevel	Integer	-1	-1	-1	[No change]
		SyncTime	String	12:00	12:00	12:00	[No change]
The par manage is the de	ameter is n ement pack efault value	ot set by a custom over The effective value of of this parameter.	ide or by a this parameter				
Management pack         Select destination management pack:         Audiocodes GW Management Pack         Y							
Hel	lp					<b>ОК А</b>	pply Cancel

### Figure 7-18: Override Properties - Low Level Threshold Monitor

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

- High Threshold Monitors: 'HighCriticalLevel' and 'HighWarningLevel'
- Low Threshold Monitors: 'LowCriticalLevel' and 'LowWarningLevel'
- 7. In the 'Override' column, select the checkbox adjacent to the parameter whose threshold value you wish to change.

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

### Note:



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

# 8 Optimizing SCOM Server Loading

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

- Displaying AudioCodes Objects. See Section 8.1.1 on page 92.
- Optimizing Monitors Load. See Section 8.1.2 on page 95.
- Optimizing Discoveries Load. See Section 8.1.3 on page 99.
- Optimizing Rules Load. See Section 8.1.4 on page 81.



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

## 8.1 Introduction

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

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

- Polling interval defines the polling frequency interval; how often (seconds) functional items are launched (least possible resolution is 60 seconds).
- Sync time specifies at which time the polling is rearranged; this allows you to set the exact time in minutes within the hour when a functional item is launched. For example, if the IP2Tel Calls counter rule is launched every 10 minutes (i.e. the Polling interval) this parameter sets the starting time and therefore the subsequent time sequence for launching this item within the hour (in minutes) i.e., 0, 10, 20 or 3, 13, 23, etc.). For example, when the 'Sync time' is set to 00:04, the IP2Tel Calls counter rule is launched in the following time sequence: 4, 14, 24, 34, 44, 54 minutes of each hour.

Note the following:

- When you override the 'Sync' time to launch functional items at different starting times, this smoothens CPU utilization over time and therefore enhances performance. However, on the other hand leads to delay, as the time between the relative launching of each functional item increases.
- Generally it is not recommended to override the 'IntervalSeconds' parameter; because most of the counters have a low polling frequency with a default value of fifteen minutes, and depend on the actual information refresh on the gateway devices themselves. The exception is in the case of specific Trunk counters (see Section 8.1.4 on page 102).
- For a detailed load balancing scenario for SCOM server, see Appendix C on page 173.

## 8.1.1 Displaying AudioCodes Objects

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

- > To filter the management pack functional items view:
- 1. In the Authoring pane, select **Management Pack Objects > Views**.



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

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

Figure 8-2: View Scope

🚾 Object D	iscov	veries - Audiocodes - Op	erations Man	ager		
File Edit	View	Go Tasks Tools H	Help			
	✓	Navigation Pane	Alt+F1	Scope 🔎 Find 🔯 Tasks 🕡 🖕		
Authoring	✓	Tasks	Ctrl+T	Object Discoveries (269)	,	Tasks
🖌 📝 Auth		Properties		Management pack objects are now scoped to: Audiocodes Analog Trunk Class, Audiocodes Change Scope >	< 1	2
🕞 🖉 Mai		Personalize view		Name Target Management Pack	<u> </u>	
🐴 Dist	~	Detail Pane	Ctrl+D	Discovered Type: Audiocodes Analog Trunk Class (2)		Discovery
🔛 Gro		rad.	and in the	Audiocodes Trunks on Analog Module Initial Discovery Audiocodes IF Analog M Audiocodes GW Mar		Droportion
a 🛒 Mai	P	Find	Ctri+F	Audiocodes GW Analog Trunk Secondary Discovery Audiocodes Analog Trun Audiocodes GW Mar		Properties
E At		Show or Hide Views		Discovered Type: Audiocodes CPU Module (4)		an Disable
M (	$\checkmark$	Scope	Ctrl+M	🙀 Audiocodes Mediant 4000 CPU Module Initial Discovery 💦 Audiocodes SNMP Device 🛛 Audiocodes GW Mar		🕤 Overrides 🕨
	Q	Refresh	F5	Audiocodes CPU Module Index Discovery Audiocodes CPU Module Audiocodes GW Mar		🔨 Delete
PI PI		Status Bar		Audiocodes Mediant 1000 CPU Module Initial Discovery Audiocodes SNMP Device Audiocodes GW Mar		
se	rvice	Level Tracking		🙀 Audiocodes Mediant 800 CPU Module Initial Discovery 💦 Audiocodes Mediant800 Audiocodes GW Mar		
Ta	sks	-		Discovered Type: Audiocodes Digital Trunk Class (7)		
📝 Vi	ews			🙀 Audiocodes Digital Trunks on Digital Module Initial Discov Audiocodes IF Digital Mo Audiocodes GW Mar		
				📷 Audiocodes Digital Trunks on acTrunkPack-MEDIANT2000 🛛 Audiocodes acTrunkPack Audiocodes GW Mar		
				🙀 Audiocodes Digital Trunk Secondary Discovery 🛛 🗛 Audiocodes Digital Trunk Audiocodes GW Mar		
				📷 Audiocodes Mediant 800 IF Digital Module Trunk Digital In Audiocodes Mediant 800 Audiocodes GW Mar		
				👔 Audiocodes Digital Trunks on BRI Module Initial Discovery 🛛 Audiocodes IF BRI Module 🛛 Audiocodes GW Mar		
				📷 Audiocodes Mediant 800 IF BRI Module Trunk Digital Initia Audiocodes Mediant 800 Audiocodes GW Mar		
				📷 Audiocodes Digital Trunk on acTrunkPackIPM2000 Module Audiocodes acTrunkPack Audiocodes GW Mar		
				A Discovered Type: Audiocodes Ethernet Port Class (3)		
				addiocodes Ethernet Port Initial Discovery Audiocodes CPU Module Audiocodes GW Mar		
Add Monitor	ina W	izard		Audiocodes Ethernet Port Secondary Discovery Audiocodes Ethernet Port Audiocodes GW Mar	-	
New Distrib	ited A	volication				
New Group.				Object Discovery Details:	~	
				Collect on abject discovery above to view details		
🛄 Mor	itorii	ng				
A.14		_				
Auti	iorin	9				
🚫 Adn	ninist	ration				
My My	Nork	space				
Log Wy		space				
			*			
Ready						1

### Figure 8-1: Views

The Scope Management Pack Objects window is displayed:

Figure 8-3: Scope Management Pack Objects

Scope Management Pack Ob	jects		×
Select the class, group, or obj items easier to find.	ect that you want to target from	the list below. You can also filter or	sort the list to make
Look for:			
Audiocodes			Cl <u>e</u> ar
C View common targets			
View all targets			
Target =	Management Dack	Description	
Audiocodes acTrunkPack	Audiocodes GA(Manageme	Description	
	Audiocodes GW Manageme		
	Audiocodes GW Manageme		
Audiocodes Analog Trun	Audiocodes GW Manageme		
Audiocodes CFO Moduli	Audiocodes GW Manageme		
Audiocodes Denaniel C	Audiocodes GW Manageme		
Audiocodes Ethemet Por	Audiocodes GW Manageme		
Audiocodes Ean Trav	Audiocodes GA/Manageme		
Audiocodes GA(Mediand	Audiocodes GA/Manageme	Device Mediant4000	
Audiocodes IE ADSL Mo	Audiocodes GA(Manageme	Device Mediant4000	
Audiocodes II Abst Mo	Audiocodes GA(Manageme		
Audiocodes IF Analog M	Audiocodes GA(Manageme		
	Audiocodes GA/Manageme		
Audiocodes IE SHDSL M	Audiocodes GA(Manageme		
Audiocodes IE T1\AAN M	Audiocodes GA(Manageme		
Audiocodes IE WAN Mo	Audiocodes GA(Manageme		
Audiocodes IP Media Mo	Audiocodes GA(Manageme		-
	Additional of the state of the s		
	1		
Select All Clear All	1033 total Targets, 45 visibl	e, 0 selected	
		Help	OK Cancel

- **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:

M	onitors	
	Management pack objects are now scoped to: Audiocodes Analog Trunk Class, Audiocodes Change Scope	×
Ta	arget Type Inherited From M	la 📥
⊳	Audiocodes Analog Trunk Class	
⊳	Audiocodes CPU Module	
⊳	Audiocodes DChannel Class	
⊳	Audiocodes Digital Trunk Class	
⊳	Audiocodes Ethernet Port Class	
⊳	Audiocodes Fan Tray	
⊳	Audiocodes GW Mediant4000	
⊳	Audiocodes IF ADSL Module	
⊳	Audiocodes IF Analog Module	
⊳	Audiocodes IF BRI Module	
⊳	Audiocodes IF Digital Module	
⊳	Audiocodes IF SHDSL Module	
⊳	Audiocodes IF T1WAN Module	
⊳	Audiocodes IF WAN Module	
⊳	Audiocodes IP Media Module	
⊳	Audiocodes M1K Device	
⊳	Audiocodes M2K and M3K GW Devices Family Class	
⊳	Audiocodes M2K Device	
⊳	Audiocodes M3K Device	╶
•		

### Figure 8-4: AudioCodes Management Pack Entities

## 8.1.2 Optimizing Monitor's Load

This section describes how to configure when monitors are launched.

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

- Gateways:
  - Audiocodes Blocked Channels High Threshold Monitor
  - Audiocodes Free Channels Low Threshold Monitor
  - \*Audiocodes Low Threshold Monitor <PM>- family of monitors
  - \*Audiocodes High Threshold Monitor <PM> family of monitors



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

### Trunks:

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

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

### > To optimize monitors' loading:

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

#### Figure 8-5: Monitors Option



The Monitors window is displayed:

Figure 8-6: Monitors



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

Monitors		> Tasks
Management pack objects are now scoped to: Audiocodes Analog Trunk Class, Audio	ocodes Change Scope 🗙	2
Target Type	Inherited From Mal	Monitor A
Audiocodes IF BRI Module		
Audiocodes IF Digital Module		Create a Monito
Audiocodes IF SHDSL Module		Properties
Audiocodes IF T1WAN Module		<ul> <li>Disable</li> </ul>
Audiocodes IF WAN Module	Disable the Monitor	Overrides 🕨
Audiocodes IP I     For all objects of class: Audiocodes M1K Device	Override the Monitor	Delete
A Audiocodes M1		-
A 🔐 Entity He	Disable Diagnostic	
Availat For a specific object of class: Audiocodes M1K Device	Override Diagnostic	
Config For all objects of another class	Disable Recovery	
4 🎆 Performance Aggregate Rollup	Override Recovery	
Audiocodes Attempted Calls IP2Tel High Treshold M Audiocodes Cumu	II Summany	
Audiocodes Attempted Calls IP2Tel Low Treshold M Audiocodes Cumu	II	-
Audiocodes Attempted Calls Tel2IP High Treshold M Audiocodes Cumu	il Audiocodes SNMP Au	
Audiocodes Attempted Calls Tel2IP Low Treshold M Audiocodes Cumu	il Audiocodes SNMP Au	
Audiocodes Blocked Channels High Treshold Monitor Audiocodes Block	e Audiocodes SNMP Au	
Audiocodes Busy Calls IP2Tel High Treshold Monitor Audiocodes Cumu	il Audiocodes SNMP Au	
Audiocodes Busy Calls IP2Tel Low Treshold Monitor Audiocodes Cumu	ıl Audiocodes SNMP Au	
Audiocodes Busy Calls Tel2IP High Treshold Monitor Audiocodes Cumu	ıl Audiocodes SNMP Au 🖵	
•		

### Figure 8-7: Overriding Object Monitors

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

The Override Properties window is displayed:

Figure 8-8: Override Properties-Object Monitors-High Level Threshold Monitor

uorridoo toracti	Classe Ar	idiooodoo M1K Dovid	~			
venides (arget.	Class. A		c		9	Show Monitor Propert
/erriae-controli	ed parameters:					
Uvern	de Parameter Name Alort eouoritu	Parameter Type	Match monit	Uverride Value	Effective Value	E Change Status
	Alert seventy	Poolean	True	True	True	[No change]
	Enabled	Pooloan	True	True	True	[No change]
	Generates Alert	Boolean	True	Тпіе	Тпіе	[No change]
	HighCritical evel	Integer	40	40	40	[No change]
	HighWarningLevel	Integer	30	30	30	[No change]
	IntervalSeconds	Integer	60	60	60	[No change]
	SuncTime	String	12:00	12:00	12:00	[No change]
etails: <b>yncTime</b> he parameter	is not set by a custom ove	rride or by a	cription			
etails: SyncTime The parameter hanagement p the default va	is not set by a custom ove ack. The effective value c alue of this parameter.	rride or by a f this parameter	cription			
etails: <b> yncTime</b> the parameter hanagement p the default va	is not set by a custom ove ack. The effective value o alue of this parameter.	Des rride or by a f this parameter	cription			
etails: <b>SyncTime</b> The parameter nanagement p the default va	is not set by a custom ove ack. The effective value o alue of this parameter.	Des rride or by a f this parameter	cription			
atails: yncTime he parameter hanagement p the default va	is not set by a custom ove ack. The effective value o alue of this parameter.	rride or by a f this parameter	cription			
atails: <b>SyncTime</b> the parameter tanagement p the default w anagement	is not set by a custom ove ack. The effective value o alue of this parameter.	Des rride or by a f this parameter	cription			
etails: iyncTime ihe parameter anagement p the default van lanagement	is not set by a custom ove ack. The effective value o alue of this parameter. <b>pack</b>	Des rride or by a f this parameter	cription			
etails: ine parameter anagement p the default vi anagement anagement	is not set by a custom ove ack. The effective value of alue of this parameter. pack on management pack:	Des rride or by a f this parameter	cription			

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



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

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

## 8.1.3 Optimizing Discoveries' Load

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

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



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

### > To optimize discoveries' loading:

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

### Figure 8-9: Object Discoveries Option





The Object Discoveries window is displayed:

### Figure 8-10: Object Discoveries

Object Discoveries (269)			Tasks
Management pack objects are now scoped to: Audiocodes Analo	g Trunk Class, Audiocodes	Change Scope 🗙	
Name	Target	Management Pack 📃 📥	Object
Discovered Type: Audiocodes Analog Trunk Class (2)			Discovery
📸 Audiocodes Trunks on Analog Module Initial Discovery	Audiocodes IF Analog M	Audiocodes GW Mar	Properties
📸 Audiocodes GW Analog Trunk Secondary Discovery	Audiocodes Analog Trun	Audiocodes GW Mar	Disable
Discovered Type: Audiocodes CPU Module (4)			
📸 Audiocodes Mediant 4000 CPU Module Initial Discovery	Audiocodes SNMP Device	Audiocodes GW Mar	Overrides •
📸 Audiocodes CPU Module Index Discovery	Audiocodes CPU Module	Audiocodes GW Mar	📉 Delete
📸 Audiocodes Mediant 1000 CPU Module Initial Discovery	Audiocodes SNMP Device	Audiocodes GW Mar	
🙀 Audiocodes Mediant 800 CPU Module Initial Discovery	Audiocodes Mediant800	Audiocodes GW Mar	
A Discovered Type: Audiocodes Digital Trunk Class (7)			
📸 Audiocodes Digital Trunks on Digital Module Initial Discov	Audiocodes IF Digital Mo	Audiocodes GW Mar	
📸 Audiocodes Digital Trunks on acTrunkPack-MEDIANT2000	Audiocodes acTrunkPack	Audiocodes GW Mar	
🙀 Audiocodes Digital Trunk Secondary Discovery	Audiocodes Digital Trunk	Audiocodes GW Mar	
📸 Audiocodes Mediant 800 IF Digital Module Trunk Digital In	Audiocodes Mediant 800	Audiocodes GW Mar	
📸 Audiocodes Digital Trunks on BRI Module Initial Discovery	Audiocodes IF BRI Module	Audiocodes GW Mar	
📸 Audiocodes Mediant 800 IF BRI Module Trunk Digital Initia	Audiocodes Mediant 800	Audiocodes GW Mar	
🙀 Audiocodes Digital Trunk on acTrunkPackIPM2000 Module	Audiocodes acTrunkPack	Audiocodes GW Mar	
Discovered Type: Audiocodes Ethernet Port Class (3)			
audiocodes Ethernet Port Initial Discovery	Audiocodes CPU Module	Audiocodes GW Mar	
📸 Audiocodes Ethernet Port Secondary Discovery	Audiocodes Ethernet Port	Audiocodes GW Mar 🚽	

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

Object Discoveries (269)	Tasks				
Management pack objects are now scoped to: Audiocodes Analog Trunk Class, Audiocodes Change Scope 🗙					
Name Target Management Pack	Object				
Discovered Type: Audiocodes Analog Trunk Class (2)					
🙀 Audiocodes Trunks on Analog Module Initial Discovery 👘 Audiocodes IF Analog M 🛛 Audiocodes GW Mar	Properties				
🙀 Audiocodes GW Analog Trunk Secondary Discovery 🛛 🛛 Audiocodes Analog Trun 🛛 Audiocodes GW Mar	Disable				
Discovered Type: Audiocodes CPU Module (4)	Cuencides b				
Audiocodes Mediant 4000 CPU Module Initial Discovery Audiocodes Disable the Object Discovery	Overrides				
For all objects of class: Audiocodes Digital Trunk Class Override the Object Discovery	Delete				
For a group					
For a specific object of class: Audiocodes Digital Trunk Class	•				
D For all objects of another class					
🕍 คนแบ่ดอนตร อายาเสา ทนาหรายทายามูแลา พบนนายากและ อารดอง คนนายดอนตราโF Digital Mo Audiocodes GW Mar					
📷 Audiocodes Digital Trunks on acTrunkPack-MEDIANT2000 🛛 Audiocodes acTrunkPack Audiocodes GW Mar					
Audiocodes Digital Trunk Secondary Discovery Audiocodes Digital Trunk Audiocodes GW Mar					
📷 Audiocodes Mediant 800 IF Digital Module Trunk Digital In Audiocodes Mediant 800 Audiocodes GW Mar					
🙀 Audiocodes Digital Trunks on BRI Module Initial Discovery 🛛 Audiocodes IF BRI Module 🛛 Audiocodes GW Mar					
📷 Audiocodes Mediant 800 IF BRI Module Trunk Digital Initia Audiocodes Mediant 800 Audiocodes GW Mar					
📷 Audiocodes Digital Trunk on acTrunkPackIPM2000 Module Audiocodes acTrunkPack Audiocodes GW Mar					
Discovered Type: Audiocodes Ethernet Port Class (3)					
🙀 Audiocodes Ethernet Port Initial Discovery 🛛 🗛 Audiocodes CPU Module 🔹 Audiocodes GW Mar					
📷 Audiocodes Ethernet Port Secondary Discovery 🛛 🗛 Audiocodes Ethernet Port Audiocodes GW Mar 🚽					

### Figure 8-11: Overriding Object Discoveries

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

The Override Properties window is displayed:

)verride	Propertie	s						×
Object Di	scovery na	me: Audiocod	es acTrunkPack-MED	ANT2000 Seco	ondary Discovery			
Category:	Category: Discovery							
Overrides	target:	Class: Au	diocodes acTrunkPack	K-MEDIANT 2000	)			
<u>O</u> verride-	Override-controlled parameters:							
	Override	Parameter Name 🔺	Parameter Type	Default Value	Override Value	Effective Value	Change Status	
		Enabled	Boolean	True	True	True	[No change]	
		Interval	Integer	60	60	60	[No change]	
•		SyncTime	String	00:00	00:00	00:00	[No change]	
Details:								
SyncTime         Description         Edit           The parameter is not set by a custom override or by a management pack. The effective value of this parameter is the default value of this parameter.         Edit         Edit								
Manage	ement pa	ck						
Select de	estination m	nanagement pack:						,
Audioco	odes GW M	fanagement Pack					Ne <u>w</u>	
<u>H</u> el	Þ					ОК	pply Can	cel

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



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

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

6. Click OK.

## 8.1.4 Optimizing Rule's Load

This section describes how to configure when rules are launched.

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

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



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

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

- To optimize rules' loading:
- 1. In the Authoring pane, select Management Pack Objects > Rules.



### Figure 8-13: Rules Option

The Rules window is displayed:

Figure	8-14:	Object	Rules
--------	-------	--------	-------

Rules - Audiocodes - Operations Manager							
Elle Edit View Go Tasks Iools Help							
Search 🔻 🛫 📋 Create a <u>R</u> ule 🖕 Overrides 🔻 🛫 🖡 Scope 🖉 Find 🔽 Tasks 🔞 👙							
Authoring <	< Rules (282) >						
Management pack objects are now scoped to: Audiocodes Analog Trunk Class, Audiocodes Change Scope							
🗟 🕟 Management Pack Templates	Name	Bula					
🕿 Distributed Applications	4 Type: Audiocodes Digital Trunk Class (3)	Kule o					
🗠 Groups	Audiocodes Digital Trunk Available Channels Counter Rule	Audiocodes Digital Trunk	Audiocodes GW Mar	📃 Create a Rule			
🖉 💑 Management Pack Objeds	Audiocodes Digital Trunk Blocked Channels Counter Rule	Audiocodes Digital Trunk	Audiocodes GW Mar	Properties			
E Attributes	Audiocodes Digital Trunk Channels Probe Rule	Audiocodes Digital Trunk	Audiocodes GW Mar	📷 Overrides 🕨			
Monitors	4 Type: Audiocodes GW Mediant4000 (31)			X Delete			
Object Discoveries	Audiocodes Attempted Calls Tel2IP Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
Rules	Audiocodes Available Channels Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
Service Level Tracking	Audiocodes IPGroupDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
Tasks	Audiocodes Established Calls Tel2IP Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
Views	Audiocodes Busy Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes Failed Calls Tel2IP Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes SRDSubscribeDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes Attempted Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes SRDInviteDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes NoResources Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes Forwarded Calls Tel2IP Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes SRDOtherDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
	Audiocodes NoRoute Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar				
A did Manifester (1994) and	Audiocodes IPGroupInviteDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar 🖵				
Add Monitorning Wizard	•		Þ				
New Distributed Application	Rule details:		~				
New Group							
Monitoring	<ol> <li>Select a rule above to view details</li> </ol>						
Authoring							
Administration							
My Workspace							
Ready				11.			

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'.

Rules (282)			Tasks
Management pack objects are now scoped to: Audiocodes Analo	g Trunk Class, Audiocodes	Change Scope 🗙	2
Name	Inherited from	Management Pack 🔺	Rule A
4 Type: Audiocodes Digital Trunk Class (3)			
📄 Audiocodes Digital Trunk Available Channels Counter Rule	Audiocodes Digital Trunk	. Audiocodes GW Mar	Create a Rule
📄 Audiocodes Digital Trunk Blocked Channels Counter Rule	Audiocodes Digital Trunk	. Audiocodes GW Mar	Properties
📄 Audiocodes Digital Trunk Channels Probe Rule	Audiocodes Digital Trunk	. Audiocodes GW Mar	🧾 Disable
Type: Audiocodes GW Mediant4000 (31)		Disable the Rule	Overrides
Audiocode For all objects of class: Audiocodes Digital Tru	nk Class	Override the Rule	Delete
E Audiocode For a group			=
Eor a specific object of class: Audiocodes Digit	al Trunk Class	Summary	•
Audiocode	-	Hadrocoacy of Final	
Audiocode For all objects of another class	е	Audiocodes GW Mar	
Audiocodes Failed Calls Tel2IP Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
Audiocodes SRDSubscribeDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
Audiocodes Attempted Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
Audiocodes SRDInviteDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
📄 Audiocodes NoResources Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
Audiocodes Forwarded Calls Tel2IP Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
Audiocodes SRDOtherDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
📄 Audiocodes NoRoute Calls IP2Tel Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar	
📄 Audiocodes IPGroupInviteDialogs Counter Rule	Audiocodes SNMP Device	Audiocodes GW Mar 🗸	
•			

### Figure 8-15: Overriding Object Rules-AudioCodes Digital Trunk Channels Probe Rule

3. Right-click the monitor, choose **Overrides** > **Override the Rule**, and then in pop-up dialog, select the scope affected by the modification e.g. "For a group".

The Override Properties window is displayed:

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

Override I	Propertie	5						×
Rule name: Audiocodes Digital Trunk Channels Probe Rule								
Category:	Category: Custom							
Overrides	Overrides target: Class: Audiocodes Digital Trunk Class							
<u>O</u> verride-	Override-controlled parameters: Show Rule Properties							s
	Override	Parameter Name 🔺	Parameter Type	Default Value	Override Value	Effective Value	Change Status	
		Enabled	Boolean	True	True	True	[No change]	
•		Interval Seconds	Integer	60	60	60	[No change]	
		Sync Time	String				[No change]	
		Timeout Seconds	Integer	60	60	60	[No change]	
The parameter is not set by a custom override or by a management pack. The effective value of this parameter is the default value of this parameter.								
Manage	ement pa	ck						
Se <u>l</u> ect de	estination n	nanagement pack:						
Audioco	odes GW M	lanagement Pack					Ne <u>w</u>	
<u>H</u> el	р					OK A	pply Cance	:

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



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

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



Rules (282)			<b>&gt;</b> т	asks
Management pack objects are now scoped to: Audiocodes Analog Trunk Class, Audiocodes Change Scope 🗙				
Name	Inherited from	Management Pack 🔺	Rul	0 0
<ul> <li>Type: Audiocodes Digital Trunk Class (3)</li> <li>Audiocodes Digital Trunk Available Channels Counter Rule</li> <li>Audiocodes Digital Trunk Blocked Channels Counter Rule</li> <li>Audiocodes Digital Trunk Channels Probe Rule</li> <li>Type: Audiocodes GW Mediant4000 (31)</li> <li>Audiocodes</li> <li>For all objects of class: Audiocodes GW Media</li> <li>For a group</li> </ul>	Audiocodes Digital Trunk Audiocodes Digital Trunk Audiocodes Digital Trunk ant4000	Audiocodes GW Mar Audiocodes GW Mar Audiocodes GW Mar Disable the Rule Override the Rule		Create a Rule Properties Disable Overrides Delete
Audiocodes       For a specific object of class: Audiocodes GW         Audiocodes       For all objects of another class	/ Mediant4000	Summary Audiocodes GW Mar	•	
Audiocodes Failed Calls Tel2IP Counter Rule  Audiocodes SRDSubscribeDialogs Counter Rule  Audiocodes Attempted Calls IP2Tel Counter Rule  Audiocodes SRDInviteDialogs Counter Rule  Audiocodes NoResources Calls IP2Tel Counter Rule  Audiocodes Forwarded Calls Tel2IP Counter Rule  Audiocodes SRDOtherDialogs Counter Rule  Audiocodes NoRoute Calls IP2Tel Counter Rule  Audiocodes IPGroupInviteDialogs Counter Rule	Audiocodes SNMP Device Audiocodes SNMP Device	Audiocodes GW Mar Audiocodes GW Mar		
•		►		

### Figure 8-17: Overriding Object Rules-AudioCodes Failed Calls Tel2IP Counter Rule

 Right-click the monitor, choose Overrides > Override the Rule, and then in pop-up dialog, select the scope affected by the modification e.g. "For a group". The Override Properties window is displayed:

Dverride Properties 🗙								
Rule nam	ie:	Audiocod	es Failed Calls Tel2IP	Counter Rule				
Category:		Custom						
Overrides	Dverrides target: Class: Audiocodes GW Mediant4000							
Qveride-controlled parameters:							Show Rule Properties	
	Override	Parameter Name 🗠	Parameter Type	Default Value	Override Value	Effective Value	Change Status	
		Enabled	Boolean	True	True	True	[No change]	
		IntervalSeconds	Integer	900	900	900	[No change]	
•		SyncTime	String	12:00	12:00	12:00	[No change]	
Details:				de Mara				
The para manager is the de	ameter is n ment pack. sfault value	ot set by a custom over The effective value of of this parameter.	ide or by a this parameter	TPCOT			LUK.	
Manage	ement pa	ck						
Select de	estination n	hanagement pack:						
Audioco	odes GW M	lanagement Pack					▼ Ne <u>w</u>	
Hel	P					OK A	Cancel	

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

- **11.** Select the 'Override' check box for the 'SyncTime' parameter.
- **12.** In the 'Override Value' field for 'SyncTime', type the appropriate value.
- 13. Click OK.



This page is intentionally left blank


# **SNMP** Traps

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

### Notes:

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

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

## A.1 Chassis Alarms

## A.1.1 Fan Tray Alarm



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

### Table A-1: acFanTrayAlarm

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

## A.1.2 Power Supply Alarm



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

### Table A-2: acPowerSupplyAlarm

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

## A.1.3 User Input Alarm



Note: Applicable to Mediant 3000 and Mediant 1000.

### Table A-3: acUserInputAlarm

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

## A.1.4 PEM Alarm



Note: Applicable only to Mediant 3000.

### Table A-4: acPEMAlarm

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

## A.1.5 Hardware Failure Alarm



Note: Applicable only to Mediant 1000.

#### Table A-5: acHwFailureAlarm

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

## A.1.6 Timing Module Alarms



Note: These alarms are applicable only to Mediant 3000.

## A.1.7 TM Inconsistent Remote and Local PLL Status Alarm

#### Table A-6: acTMInconsistentRemoteAndLocalPLLStatus Alarm

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

## A.1.8 TM Reference Status Alarm

#### Table A-7: acTMReferenceStatus Alarm

Alarm	acTMReferenceStatus				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5	7			
Description	Timing manager reference statu	S.			
Default Severity	Major				
Source Varbind Text	Chassis#0/TimingManager#0				
Event Type	equipmentAlarm				
Probable Cause	underlyingResourceUnavailable				
Status Changes	When primary and secondary clowill be escalated to 'Critical'.	ock references are down for mo	ore than 24 hours, the alarm	۱	
Alarm Severity	Condition	<text></text>	<b>Corrective Action</b>		
Major	The alarm is triggered when the primary reference or secondary reference or both are down.	Timing Manager Alarm. PRIMARY REFERENCE DOWN/SECONDARY REFERENCE DOWN/ALL REFERENCES ARE DOWN	<ol> <li>Synchronize the timi module.</li> <li>Reboot the system.</li> </ol>	ng	
Status remains 'Major' until a reboot. A clear trap is not sent.	-	-	-		

## A.1.9 TM Reference Change Alarm

### Table A-8: acTMReferenceChange Alarm

Alarm	acTMReferenceChange				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0	1.3.6.1.4.1.5003.9.10.1.21.2.0.58			
Description	Timing manager reference cha	ange.			
Default Severity	Indeterminate				
Source Varbind Text	Chassis#0/TimingManager#0				
Event Type					
Probable Cause					
Alarm Severity	Condition	<text></text>	Corrective Action		
-	Log is sent on PLL status change.	Timing Manager	Corrective action is not necessary.		

## A.1.10 Trunk Alarms



Note: Applicable only to Digital Series.

## A.1.10.1 Trunk Near-End LOS Alarm

### Table A-9: acTrunksAlarmNearEndLOS

Alarm	acTrunksAlarmNearEndLOS					
OID	1.3.6.1.4.1.500	1.3.6.1.4.1.5003.9.10.1.21.2.0.49				
Default Severity	Critical					
Source Varbind Text	Interfaces#0/T	runk# <m>, where <i>m</i> is</m>	s the	trunk interface number, 1 being the first trunk		
Event Type	communicationsAlarm					
Probable Cause	lossOfSignal					
	Condition <text> Corrective Action</text>					
Alarm Severity	Condition	<text></text>		Corrective Action		
Alarm Severity Critical	Condition Near-end LOS	<text> Trunk LOS Alarm</text>	Los 1. 2. 3.	Corrective Action of Signal (LOS) indicates a physical problem. Check that the cable is connected on the board. Check that the correct cable type is being used (crossed/straight). Contact AudioCodes' Support Center at <u>support@audiocodes.com.</u>		

## A.1.10.2 Trunk Near-End LOF Alarm

Alarm	acTrunksAlarmNearEndLOF					
OID	1.3.6.1.4.1.500	1.3.6.1.4.1.5003.9.10.1.21.2.0.50				
Default Severity	Critical					
Source Varbind Text	Interfaces#0/T	runk# <m>, where <i>m</i></m>	is the trunk interface number, 1 being the first trunk			
Event Type	communication	nsAlarm				
Probable Cause	lossOfFrame					
Alarm Severity	Condition	<text></text>	Corrective Action			
Critical	Near end LOF	Trunk LOF Alarm	1. Make sure that the trunk is connected to a prope follow-up device.			
			<ol> <li>Make sure that both sides are configured with the same (E1 / T1) link type.</li> </ol>			
			3. Make sure that both sides are configured with the same framing method.			
			4. Make sure that both sides are configured with the same line code.			
			5. Make sure that the clocking setup is correct.			
			6. Contact AudioCodes' Support Center at support@audiocodes.com.			
Cleared	End of LOF	-	-			

#### Table A-10: acTrunksAlarmNearEndLOF

### A.1.10.3 Trunk AIS Alarm

### Table A-11: acTrunksAlarmRcvAIS

Alarm	acTrunksAlarmRcvAIS				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.	1.3.6.1.4.1.5003.9.10.1.21.2.0.51			
Source Varbind Text	Interfaces#0/Trunk# <m>, wher</m>	e m is the trunk interfac	e number, 1 being the first trunk		
Alarm Text	communicationsAlarm	communicationsAlarm			
Event Type	PSTN provider has stopped the trunk (receiveFailure)				
Probable Cause	communicationsAlarm				
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	Receive AIS	Trunk AIS Alarm	<ul> <li>Contact your PSTN provider to activate the trunk.</li> <li>If the alarm persists, contact the AudioCodes Support Center at support@audiocodes.com</li> </ul>		
Cleared	End of AIS	-	-		

## A.1.10.4 Trunk Far-End LOF Alarm

#### Table A-12: acTrunksAlarmFarEndLOF

Alarm	acTrunksAlarmFarEndLOF				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0	1.3.6.1.4.1.5003.9.10.1.21.2.0.52			
Default Severity	Critical	Critical			
Source Varbind Text	Interfaces#0/Trunk# <m>, whe</m>	re <i>m</i> is the trunk interfa	ce number, 1 being the first trunk		
Event Type	communicationsAlarm	communicationsAlarm			
Probable Cause	transmitFailure				
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	RAI Trunk RAI Alarm Make sure that transmission is correct.				
Cleared	End of RAI	-	-		

### A.1.10.5 DS1 Line Status Alarm

## Table A-13: dsx1LineStatusChange

Alarm	dsx1Lin	dsx1LineStatusChange			
OID	1.3.6.1.	1.3.6.1.2.1.10.18.15.0.1			
Default Severity	Major o	n raise; (	Clear on clear		
Source Varbind Text	Interfac	es#0/Tru	nk# <m>, where <i>m</i> is the trunk</m>	interface number, 1 being the first trunk	
Event Type	commu	nications	Alarm		
Drahahla Causa	commu	meations			
Probable Cause					
Alarm Severity	<text></text>		Additio	nal Info1,2,3	
-	DS1 Line Status	Updated DS1 Line Status. This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms' information.			
		dsx1LineStatus is a bitmap represented as a sum, so it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined fro the dsx1loopbackConfig object. The various bit positions are:			
		1	dsx1NoAlarm	No alarm present	
		2	dsx1RcvFarEndLOF	Far end LOF (a.k.a., Yellow Alarm)	
		4	dsx1XmtFarEndLOF	Near end sending LOF Indication	
		8	dsx1RcvAIS	Far end sending AIS	
		16	dsx1XmtAIS	Near end sending AIS	
		32	dsx1LossOfFrame	Near end LOF (a.k.a., Red Alarm)	
		64	dsx1LossOfSignal	Near end Loss Of Signal	
		128	dsx1LoopbackState	Near end is looped	
		256	dsx1T16AIS	E1 TS16 AIS	
		512	dsx1RcvFarEndLOMF	Far End Sending TS16 LOMF	
		1024	dsx1XmtFarEndLOMF	Near End Sending TS16 LOMF	
		2048	dsx1RcvTestCode	Near End detects a test code	
		4096	dsx1OtherFailure	Any line status not defined here	
		8192	dsx1UnavailSigState	Near End in Unavailable Signal State	
		16384	dsx1NetEquipOOS	Carrier Equipment Out of Service	
		32768	dsx1RcvPayloadAIS	DS2 Payload AIS	
		65536	dsx1Ds2PerfThreshold	DS2 Performance Threshold Exceeded	

## A.1.10.6 B-Channel Alarm

### Table A-14: acBChannelAlarm

Alarm	acBChannelAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.21.2	1.3.6.1.4.1.5003.9.10.1.21.2.0.85			
Default Severity	Minor				
Source Varbind Text	Interfaces#0/Trunk# <m>, where <i>m</i> is the trunk interface number, 1 being the first trunk</m>				
Event Type	communicationsAlarm				
Probable Cause	degradedSignal				
Alarm Severity	Condition <text> Corrective Action</text>				
Major	Raised when B-channel service state changes to 'Out of Service' or 'Maintenance'	B-Channel Alarm. %s	Corrective action is not necessary		
Clear	B-channel status changes to 'In Service'	%s – additional information	-		

## A.1.10.7 NFAS Group Alarm

### Table A-15: acNFASGroupAlarm

Alarm	acNFASGroupAlarm			
OID	1.3.6.1.4.1.5003.9.10.1.21.2	2.0.84		
Default Severity	Major			
Source Varbind Text	Interfaces#0/Trunk# <m>, w</m>	here <i>m</i> is the trunk interfa	ace number, 1 being the first trunk	
Event Type	communicationsAlarm			
Probable Cause	degradedSignal			
Alarm Severity	Condition	<text></text>	Corrective Action	
Major	Raised when an NFAS group goes out-of-service	NFAS Group Alarm. %s	<ul> <li>The alarm is sent only when the backup Non-Facility Associated Signaling (NFAS) D-channel also falls, i.e., when <i>both</i> D-channels are down.</li> <li>When at least one of the D-channels (primary or backup) returns to service, the alarm is cleared.</li> <li>Corrective action is not necessary.</li> </ul>	
Clear	NFAS group state goes to in- service	%s– Additional information	-	

## A.1.11 SONET Alarms



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

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

### A.1.11.1 SONET Section LOF Alarm

Alarm	acSonetSectionLOFAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.2	21.2.0.38			
Default Severity	Critical	Critical			
Source Varbind Text	Interfaces#0/Sonet# <m>, where <i>m</i> is the SONET interface number</m>				
Event Type	communicationsAlarm				
Probable Cause	lossOfFrame				
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	LOF condition is present on SONET no.n	SONET-Section LOF	Make sure the framing format on the port matches the format configured on the line. Note that the 'sonetSectionCurrentStatus' field in the sonetSectionCurrentTable will have a value <b>sonetSectionLOF(4)</b>		
Cleared	LOF condition is not present	LOF	-		

### Table A-16: AcSonetSectionLOFAlarm

## A.1.11.2 SONET Section LOS Alarm

### Table A-17: AcSonetSectionLOSAlarm

Alarm	acSonetSectionLOSAlarm			
OID	1.3.6.1.4.1.5003.9.10.1.21	1.2.0.39		
Default Severity	Critical			
Source Varbind Text	Interfaces#0/Sonet# <m>,</m>	where <i>m</i> is the SONET	interface number	
Event Type	communicationsAlarm			
Probable Cause	lossOfSignal			
Alarm Severity	Condition	<text></text>	Corrective Action	
Critical	LOS condition is present on SONET no #n	SONET-Section LOS	<ol> <li>Make sure the fiber optic cable is plugged in correctly.</li> <li>Make sure it's not damaged.</li> <li>Make sure its remote end is correctly connected and undamaged.</li> <li>Make sure that configuration of the remote port is correct.</li> <li>Note that the 'sonetSectionCurrentStatus'</li> </ol>	
			field in the sonetSectionCurrentTable will have a value <b>sonetSectionLOS (2)</b>	

Cleared	LOS condition is not	-	-
	present		

## A.1.11.3 SONET Section AIS Alarm

### Table A-18: AcSonetLineAlSAlarm

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</m>	is the SONET interface n	umber		
Event Type	communicationsAlarm				
Probable Cause	receiveFailure	receiveFailure			
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	AIS condition is present on SONET- Line #n	SONET-Line AIS	<ul> <li>If an Alarm Indication Signal (AIS) condition is present on a SONET line:</li> <li>Make sure the remote configuration is correct.</li> <li>Check the line status at the remote end of the link.</li> <li>Note that the 'sonetLineCurrentStatus' field in the sonetLineCurrentTable will have a value sonetLineAIS (2)</li> </ul>		
Cleared	AIS condition is not present.	-	•		

## A.1.11.4 SONET Line RDI Alarm

### Table A-19: AcSonetLineRDIAlarm

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

## A.1.11.5 SONET Path STS LOP Alarm

Alarm	acSonetPathSTSLOPAlan	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>, w</m>	here <i>m</i> is the SONET interfac	ce number		
Event Type	communicationsAlarm				
Probable Cause	receiveFailure	receiveFailure			
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	LOP condition is present on Path #m	SONET Path STS Loss of Pointer alarm: LOP	<ol> <li>Verify that the Path configuration is identical on both ends. For example, if the far-end is configured as STS3c instead of STS3, this is causing the alarm.</li> <li>If the alarm doesn't clear, contact AudioCodes Support Center at: <u>support@audiocodes.com</u></li> </ol>		
			Note that the 'sonetPathCurrentStatus' field in sonetPathCurrentTable has a value of sonetPathSTSLOP(2) STS = Synchronous Transport Signal		
Cleared	LOP condition is not present	-	-		

#### Table A-20: acSonetPathSTSLOPAlarm

## A.1.11.6 SONET Path STS AIS Alarm

### Table A-21: acSonetPathSTSAISAlarm

Alarm	acSonetPathSTSAISAlarm					
OID	1.3.6.1.4.1.5003.9.10.1.21	.2.0.62				
Default Severity	Critical					
Source Varbind Text	Interfaces#0/Path# <m>, w</m>	Interfaces#0/Path# <m>, where <i>m</i> is the SONET interface number</m>				
Event Type	communicationsAlarm					
Probable Cause	receiveFailure					
Alarm Severity	Condition	<text></text>	Corrective Action			
Critical	AIS condition is present on Path #n	SONET Path STS AIS alarm: AIS	<ol> <li>Check the configuration of the SONET path.</li> <li>You may need to check more than just the next hop. You may need to check the far end of the path.</li> <li>Note that the 'sonetPathCurrentStatus' field in sonetPathCurrentTable has a value of sonetPathSTSAIS(4)</li> </ol>			
Cleared	AIS condition is not present	-	-			

## A.1.11.6.1 SONET Path STS RDI Alarm

Alarm	acSonetPathSTSRDIAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0	1.3.6.1.4.1.5003.9.10.1.21.2.0.63			
Default Severity	Critical				
Source Varbind Text	Interfaces#0/Path# <m>, when</m>	Interfaces#0/Path# <m>, where <i>m</i> is the SONET interface number</m>			
Event Type	communicationsAlarm	communicationsAlarm			
Probable Cause	transmitFailure				
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	RDI condition is present on Path #n	SONET Path STS RDI alarm: RDI (Remote Defect Indicator)	Check the stations along the SONET path for alarm statuses, beginning with the nearest hop. The Remote Defect Indicator (RDI) is sent upstream from the path endpoint to		
			inform the provider of a problem with its circuit downstream.		
			Note that 'sonetPathCurrentStatus' in the sonetPathCurrentTable has a value of <b>sonetPathSTSRDI(8)</b>		
Cleared	RDI condition is not present	-	-		

### Table A-22: acSonetPathSTSRDIAlarm

## A.1.11.7 SONET Path Unequipped Alarm

### Table A-23: acSonetPathUnequippedAlarm

Alarm	acSonetPathUnequippedAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.	1.3.6.1.4.1.5003.9.10.1.21.2.0.64			
Default Severity	Critical				
Source Varbind Text	Interfaces#0/Path# <m>, whe</m>	re <i>m</i> is the SONET interface nur	nber		
Event Type	communicationsAlarm				
Probable Cause	receiveFailure				
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	Unequipped condition is present on Path #n	SONET Path Unequipped alarm: Unequipped	<ol> <li>Make sure the SONET path has a valid sender. The problem originates with the hub transmitting the signal to the hub reporting the alarm.</li> <li>Make sure the other side is set up correctly. Make sure the carrier's SONET network is set up correctly. If you're set up correctly on both sides, it's probably the carrier's SONET network that is the problem.</li> <li>See also RFC 1595.</li> <li>Note that 'sonetPathCurrentStatus' in the sonetPathUrrentTable has a value of sonetPathUnequipped(16)</li> </ol>		
Cleared	Unequipped condition is not present				

## A.1.11.8 SONET Path Signal Label Mismatch Alarm

### Table A-24: acSonetPathSignalLabelMismatchAlarm

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

## A.1.11.9 SONET Hardware Failure Alarm

### Table A-25: acSonetIfHwFailureAlarm

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

## A.1.12 DS3 Alarms



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

## A.1.12.1 DS3 RAI Alarm

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 n</m>	Interfaces#0/DS3# <m>, where <i>m</i> is the DS3 interface number.</m>		
Event Type	communicationsAlarm			
Probable Cause	transmitFailure	transmitFailure		
Alarm Severity	Condition	<text></text>	Corrective Action	
Critical	RAI condition is present on DS3- Line #n	DS3 RAI alarm: RAI	<ul> <li>To clear the Remote Alarm Indication (RAI) failure, remove the presence of any of the following:</li> <li>Far-end Severely Errored Frame (SEF) / Alarm Indication Signal (AIS) defect (aka 'yellow'). To correct it, set the two X-bits in the M-frame that are set to zero, to one (RFC 1407).</li> <li>One or two alarm signals on the far-end alarm channel.</li> <li>Note that the 'dsx3LineStatus' field in dsx3ConfigTable will have a value of dsx3RcvRAlFailure(2)</li> </ul>	
Cleared	RIA condition is not present	-	-	

### Table A-26: acDS3RAIAlarm

## A.1.12.2 DS3 AIS Alarm

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

#### Table A-27: acDS3AISAlarm

## A.1.12.3 DS3 LOF Alarm

Alarm	acDS3LOFAlarm	acDS3LOFAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.68			
Default Severity	Critical	Critical		
Source Varbind Text	Interfaces#0/DS3# <m>, where m</m>	Interfaces#0/DS3# <m>, where <i>m</i> is the DS3 interface number.</m>		
Event Type	communicationsAlarm			
Probable Cause	lossOfFrame			
Alarm Severity	Condition	<text></text>	Corrective Action	
Critical	LOF condition is present on DS3- Line #n	DS3 LOF alarm: LOF	1. Correct the configuration settings on the line. They're correct for the the port but not correct for the line.	
			2. Make sure the framing format configured on the port matches the framing format on the line.	
			3. Try see if the other framing format clears the alarm.	
			<ol> <li>Configure a remote loopback on the affected interface. Do this with your provider. Run an unframed Bit Error Rate Tester (BERT) to see if there're problems on the line.</li> </ol>	
			<ol> <li>Isolate the problem using hard or soft loopbacks (if you find evidence of a bad line).</li> </ol>	
			Note that the 'dsx3LineStatus' field in dsx3ConfigTable will have a value dsx3LOF (32)	
Cleared	LOF condition is not present	-	-	

#### Table A-28: acDS3LOFAlarm

## A.1.12.4 DS3 LOS Alarm

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

#### Table A-29: acDS3LOSAlarm

## A.1.12.5 DS3 Line Status Change Alarm

### Table A-30: dsx3LineStatusChangeTrap

Alarm	dsx3L	dsx3LineStatusChange		
OID	1.3.6.	1.3.6.1.2.1.10.30.15.0.1		
Default Severity	Major	on raise; Clear on clear		
Source Varbind Text	Interfa	aces#0/DS3# <m>, where m</m>	is the DS3 interface number.	
Event Type	comm	nunicationsAlarm		
Probable Cause	A dsx chang in a lo	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 I	DS3 Line Status		
Additional Info1,2,3	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 v	The various bit positions are:		
	1	dsx3NoAlarm	No alarm present	
	2	dsx3RcvRAIFailure	Receiving Yellow/Remote Alarm Indication	
	4	dsx3XmitRAIAlarm	Transmitting Yellow/Remote Alarm Indication	
	8	dsx3RcvAIS	Receiving AIS failure state	
	16	dsx3XmitAIS	Transmitting AIS	
	32	dsx3LOF	Receiving LOF failure state	
	64	dsx3LOS	Receiving LOS failure state	

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

## A.1.13 SS7 Alarms

## A.1.13.1 SS7 Link State Change Alarm Trap

Table A-31: acSS7	' Link State Change	Alarm Trap
-------------------	---------------------	------------

Alarm	acSS7LinkStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.19
Default Severity	Major
Event Type	communicationsAlarm
Probable Cause	other
Alarm Text	*** SS7 *** Link %i is %s \$s
Status Changes	
1. Condition	Operational state of the SS7 link becomes 'BUSY'.
Alarm status	Major
<text> value</text>	%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 - <link-set number=""> %i - <slc number=""> Otherwise there is NO additional text.</slc></link-set></link-set></sp></state>
Additional Info1 varbind	BUSY
2. Condition	Operational state of the link becomes 'IN-SERVICE' or 'OFFLINE'.
Alarm status	cleared
Corrective Action	For full details see the SS7 section and SS7 MTP2 and MTP3 relevant standards.

### A.1.13.2 SS7 Link Congestion State Change Alarm Trap

### Table A-32: acSS7 Link CongestionState Change Alarm Trap

Alarm	acSS7LinkCongestionStateChangeAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.22
Default Severity	Major
Alarm Type	communicationsAlarm
Probable Cause	other
Alarm Text	<pre>*** 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 - <link-set number=""> %i - <slc number=""> Otherwise there is NO additional text. %s - <congestion state="">: { "UNCONGESTED", "CONGESTED" }</congestion></slc></link-set></link-set></sp></pre>
Status Changes	
1. Condition	SS7 link becomes congested (local or remote).
Alarm status	Major
Additional Info1 varbind	CONGESTED
2. Condition	Link becomes un-congested - local AND remote.
Alarm status	Cleared
Corrective Action	Reduce SS7 traffic on that link.
Note :	This alarm is raised for any change in the remote or local congestion status.

## A.1.13.3 SS7 Link Inhibit State Change Alarm Trap

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

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

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

## A.1.13.4 SS7 Link Set State Change Alarm

### Table A-34: SS7 Link Set State Change Alarm

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

## A.1.13.5 SS7 Route Set State Change Alarm Trap

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

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

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

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

### A.1.13.6 SS7 SN Set State Change Alarm Trap

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

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

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

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

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

Alarm	acSS7UalGroupStateChangeAlarm
Corrective Action	

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

## A.1.14 Hitless Software Upgrade Alarm



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

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

### Table A-38: acHitlessUpdateStatus

## A.1.15 High Availability Alarms



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

## A.1.15.1 HA System Fault Alarm

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

#### Table A-39: acHASystemFaultAlarm

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

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

## A.1.15.2 HA System Configuration Mismatch Alarm

### Table A-40: acHASystemConfigMismatchAlarm

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

## A.1.15.3 HA System Switch Over Alarm

### Table A-41: acHASystemSwitchOverAlarm

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

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

## A.1.16 Device (Board) Alarms

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

- 3000 Series: Board#0<n>
- All other devices: **System#0<n>**

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

### A.1.16.1 Fatal Error Alarm

Alarm	acBoardFatalError					
OID	1.3.6.1.4.1.5003.9.	1.3.6.1.4.1.5003.9.10.1.21.2.0.1				
Description	Sent whenever a fa	tal device error occurs.				
Default Severity	Critical	Critical				
Event Type	equipmentAlarm					
Probable Cause	underlyingResourceUnavailable (56)					
Alarm Severity	Condition	<text></text>		Corrective Action		
Critical	Any fatal error	Board Fatal Error: A run-time specific string describing the fatal error	1. 2.	Capture the alarm information and the Syslog clause, if active. Contact AudioCodes' Support Center at		
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After fatal error	-		support@audiocodes.com which will want to collect additional data from the device and perform a reset.		

### Table A-42: acBoardFatalError

## A.1.16.2 Configuration Error Alarm

Table A-43	acBoardConfigurationError
------------	---------------------------

Alarm	acBoardConfigurationError					
OID	1.3.6.1.4.1.5003.9.	10.1.21.2.0.2				
Description	Sent when the devi the invalid setting.	Sent when the device's settings are invalid. The trap contains a message stating/detailing/explaining the invalid setting.				
Default Severity	Critical	Critical				
Event Type	equipmentAlarm					
Probable Cause	underlyingResourceUnavailable (56)					
Alarm Severity	Condition	<text></text>		Corrective Action		
Critical	A configuration error was detected	Board Config Error: A run- time specific string describing the configuration error	1.	Check the run-time specific string to determine the nature of the configuration error.		
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After configuration error	-	2.	Fix the configuration error using the appropriate tool: Web interface, EMS, or <i>ini</i> file.		
			J.	reset the device.		

## A.1.16.3 Temperature Alarm

### Table A-44: acBoardTemperatureAlarm

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

## A.1.16.4 Software Reset Alarm

Alarm	acBoardEvResettingBoard				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.	5			
Description	Sent after the device resets.				
Default Severity	Critical				
Event Type	equipmentAlarm	equipmentAlarm			
Probable Cause	outOfService (71)				
Alarm Severity	Condition	<text></text>	Corrective Action		
Critical	When a soft reset is triggered via the Web interface or SNMP	User resetting board			
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After raise		A network administrator has taken action to reset the device. Corrective action is not required.		

### Table A-45: acBoardEvResettingBoard

## A.1.16.5 Software Upgrade Alarm

### Table A-46: acSWUpgradeAlarm

Alarm	acSWUpgradeAlarm					
OID	1.3.6.1.4.1.5003.9.10.1.21	.2.0.70				
Description	Sent for software upgrade	process errors.				
Default Severity	Major	Major				
Alarms Source	System#0	System#0				
Event Type	processingErrorAlarm					
Probable Cause	softwareProgramError	softwareProgramError				
Alarm Severity	Condition	Condition <text> Corrective Action</text>				
Major	Raised upon software upgrade errors     SW upgrade error: Firmware burning failed. Startup system from Bootp/tftp.     Start up the system from BootP/TFTP.					

### A.1.16.6 Call Resources Alarm

Table A-47: acBoard	<b>ICallResourcesAlarm</b>
---------------------	----------------------------

Alarm	acBoardCallResourcesAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.21	.2.0.8			
Description	Sent when no free channe	els are available.			
Default Severity	Major	Major			
Event Type	processingErrorAlarm				
Probable Cause	softwareError (46)				
	Condition <text> Corrective Action</text>				
Alarm Severity	Condition	<text></text>	Corrective Action		
Alarm Severity Major	Condition Percentage of busy channels exceeds the predefined RAI high threshold	<text> Call resources alarm</text>	Corrective Action <ul> <li>Expand system capacity by adding more channels (trunks)</li> <li>-OR-</li> <li>Reduce traffic</li> </ul>		

## A.1.16.7 Controller Failure Alarm

### Table A-48: acBoardControllerFailureAlarm

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

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

## A.1.16.8 Board Overload Alarm

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

### Table A-49: acBoardOverloadAlarm

## A.1.16.9 Feature Key Error Alarm

### Table A-50: acFeatureKeyError

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

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



Note: Applicable only to Mediant 3000.

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

### Table A-51: acSAMissingAlarm

## A.1.16.11 Administration Status Change Alarm

### Table A-52: acgwAdminStateChange

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

## A.1.16.12 Operational Status Change Alarm

Table	A-53:	acO	peratio	nalStat	eChange
I GINIO		400	poratio	naiotat	oonango.

Alarm	acOperationalStateChange				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0	1.3.6.1.4.1.5003.9.10.1.21.2.0.15			
Description	Sent if the operational state o goes to enabled.	Sent if the operational state of the node goes to disabled; cleared when the operational state of the node goes to enabled.			
Default Severity	Major				
Event Type	processingErrorAlarm				
Probable Cause	outOfService (71)				
Alarm Severity	Condition	Condition <text> Corrective Action</text>			
Major	Operational state changed to disabled	Network element operational state change alarm. Operational state is disabled.	<ul> <li>The alarm is cleared when the operational state of the node goes to enabled.</li> <li>In IP systems, check for initialization errors - in IP systems the operational state of the node is disabled if the device fails to properly initialize.</li> <li>Look for other alarms and Syslogs that might provide additional information about the error.</li> </ul>		
Cleared	Operational state changed to enabled	-	-		

## A.1.17 Network Alarms

## A.1.17.1 Ethernet Link Alarm

### Table A-54: acBoardEthernetLinkAlarm

Alarm	acBoardEthernetLinkAlarm			
OID	1.3.6.1.4.1.5003.9.10.1.21.2.	1.3.6.1.4.1.5003.9.10.1.21.2.0.10		
Description	Sent when the Ethernet link(s	s) is down.		
Default Severity	Critical			
Source Varbind Text	All except 3000 Series: Board# <n>/EthernetLink#0 (where n is the slot number) 3000 Series: Chassis#0/Module#<n>/EthernetLink#0 (where n is the blade's slot number) This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link).</n></n>			
Event Type	equipmentAlarm			
Probable Cause	underlyingResourceUnavailable (56)			
Alarm Severity	Condition	<text></text>	Corrective Action	
Major	Fault on single interface	Ethernet link alarm: Redundant link is down	1. Ensure that both Ethernet cables are plugged into the back of the	
Critical	Fault on both interfaces	No Ethernet link	<ol> <li>Observe the system's Ethernet link lights to determine which interface is failing.</li> <li>Reconnect the cable or fix the network problem</li> </ol>	

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

### A.1.17.2 Ethernet Group Alarm



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

### Table A-55: acEthernetGroupAlarm

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

### A.1.17.3 WAN Link Alarm

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

Alarm	acBoardWanLinkAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0	0.79			
Description	This alarm is raised when the	This alarm is raised when the WAN Link is down (and cleared when link is up again).			
Default Severity	Major / Clear				
Event Type	equipmentAlarm				
Source Varbind Text	Board#x/WanLink#y				
Probable Cause	underlyingResourceUnavailable				
Alarm Severity	Condition <text> Corrective Action</text>				
Major	WAN link down - Connect the WAN port				
Clear	WAN link up				

## A.1.17.4 Data Interface Status Alarm



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

#### Table A-57: acDataInterfaceStatus

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

### A.1.17.5 Wireless Cellular Modem Alarm



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

#### Table A-58: acWirelessCellularModemAlarm

Alarm	acWirelessCellularModemAlarm				
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0	0.82			
Description	This alarm is raised when either the wireless modem is down or in backup mode, and cleared when modem is up.				
Default Severity	Major / Clear				
Source Varbind Text	Board#x/WanLink#y				
Event Type	equipmentAlarm				
Probable Cause	underlyingResourceUnavailable				
Alarm Severity	Condition <text> Corrective Action</text>				
Major	Raised when either the wireless modem is down or in backup mode, and cleared when modem is up.	WAN wireless cellular modem alarm	Get the link up. Investigate the possibility of an electronics failure or a problem with the radio frequency (RF) path.		
Clear	WAN link up	-	-		

## A.1.17.6 NTP Server Status Alarm
#### Table A-59: acNTPServerStatusAlarm

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

### A.1.17.7 NAT Traversal Alarm

#### Table A-60: acNATTraversalAlarm

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

### A.1.17.8 LDAP Lost Connection Alarm

#### Table A-61: acLDAPLostConnection

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

### A.1.17.9 OCSP Server Status Alarm

#### Table A-62: acOCSPServerStatusAlarm

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

### A.1.17.10 IPv6 Error Alarm

Table A-63: acIPv6ErrorAlarm (	Δn	nlicable	only	to F	F-SBC	Series	۱
TADIE A-05. ACIF VOLITOTAIATIT	rμ	pilcable	Unity		-300	Selles	,

Alarm	acIPv6ErrorAlarm					
OID	1.3.6.1.4.1.5003.9.10.1.21.2.	1.3.6.1.4.1.5003.9.10.1.21.2.0.53				
Default Severity	Critical					
Source Varbind Text	System#0/Interfaces# <n>.</n>					
Event Type	operationalViolation	operationalViolation				
Probable Cause	communicationsProtocolError					
Alarm Severity	Condition	<text></text>	Corrective Action			
Critical	Bad IPv6 address (already exists)	IP interface alarm: IPv6 configuration failed, IPv6 will be disabled.	<ul><li>Find a new IPV6 address.</li><li>Reboot the device.</li></ul>			
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After the alarm is raised.	-	-			

### A.1.17.11 Active Alarm Table Alarm

### Table A-64: acActiveAlarmTableOverflow

Alarm	acActiveAlarmTableOverflow					
OID	1.3.6.1.4.15003.9.10.1.21.2.0.12					
Description	Sent when an active al	larm cannot be entered ir	to the Active Alarm table because the table is full.			
Default Severity	Major					
Source Varbind Text	System#0 <n>/AlarmM</n>	System#0 <n>/AlarmManager#0</n>				
Event Type	processingErrorAlarm					
Probable Cause	resourceAtOrNearingCapacity (43)					
	Condition <text> Corrective Action</text>					
Alarm Severity	Condition	<text></text>	Corrective Action			
Alarm Severity Major	Condition Too many alarms to fit in the active alarm table	<text> Active alarm table overflow</text>	<ul> <li>Corrective Action</li> <li>Some alarm information may be lost but the ability of the device to perform its basic operations is not impacted.</li> <li>A reboot is the only way to completely clear a problem with the active alarm table.</li> <li>Contact AudioCodes' Support Center at support@audiocodes.com</li> </ul>			

### A.1.17.12 Audio Staging from APS Server Alarm



Note: Applicable only to Mediant 1000B series.

Alarm	acAudioProvisioningAlarm					
OID	1.3.6.1.4.1.5003.9.10.	1.3.6.1.4.1.5003.9.10.1.21.2.0.14				
Description	Sent if the device is ur	hable to provision its aud	dio.			
Default Severity	Critical	Critical				
Source Varbind Text	System#0/AudioStagir	System#0/AudioStaging#0				
Event Type	processingErrorAlarm	processingErrorAlarm				
Probable Cause	configurationOrCustomizationError (7)					
Alarm Severity	Condition	<text></text>	Corrective Action			
Critical	Media server times out waiting for a successful audio distribution from the APS (Audio Provisioning Server)	Unable to provision audio	<ul> <li>From the Audio Provisioning Server (APS) GUI, ensure that the device is properly configured with audio and that the device has been enabled.</li> <li>Ensure that the IP address for the APS</li> </ul>			
Cleared	After the alarm is raised, the media server is successfully provisioned with audio from the APS	-	<ul> <li>has been properly specified on the device.</li> <li>Ensure that both the APS server and application are in-service.</li> <li>For more information regarding the problem, view the Syslogs from the device as well as the APS manager logs.</li> </ul>			

#### Table A-65: acAudioProvisioningAlarm

# A.1.18 Analog Port Alarms



Note: These alarms are applicable only to Analog Series.

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

#### Table A-66: acAnalogPortSPIOutOfService

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

### A.1.18.2 Analog Port High Temperature Alarm

### Table A-67: acAnalogPortHighTemperature

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

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

#### Table A-68: acAnalogPortGroundFaultOutOfService

Alarm	acAnalogPortGroundFaultOutOfService
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.76
Default Severity	Major / Clear
Source Varbind Text	System#0/analogports# <n>, where <i>n</i> is the port number</n>
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	<ul><li>No corrective action is required.</li><li>The device shuts down the port and tries to activate it again when the relevant alarm is over.</li></ul>
Note	Relevant to FXS only.

### A.1.19 Media Alarms

### A.1.19.1 Media Process Overload Alarm



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

#### Table A-69: acMediaProcessOverloadAlarm

Alarm	acMediaProcessOverloadAlarm				
OID	1.3.6.1.4.1.500	1.3.6.1.4.1.5003.9.10.1.21.2.0.81			
Description	Sent when ther	e is overload of the device's media proce	ssing and interfaces.		
Default Severity	Major	Major			
Event Type	environmentalAlarm				
Probable Cause	underlyingResourceUnavailable				
Alarm Severity	Condition <text> Corrective Action</text>				
Major	-	Media Process Overload Alarm. %s	<ul> <li>Avoid making new calls.</li> <li>Although not corrective, this action eventually causes the alarm to drop.</li> </ul>		
Cleared	-	-	None		

### A.1.19.2 Media Realm Bandwidth Threshold Alarm



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

#### Table A-70: acMediaReaImBWThresholdAlarm

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

# A.1.20 Network Monitoring (Probe) between Devices



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

### A.1.20.1 NQM Connectivity Alarm

#### Table A-71: acNqmConnectivityAlarm

Alarm	acNqmConnectivityAlarm			
OID	1.3.6.1.4.1.500	1.3.6.1.4.1.5003.9.10.1.21.2.0.88		
Default Severity				
Alarm Source	Board#%d/NqmSender#%d			
Event Type	communicationsSubsystemFailure			
Probable Cause	Raised when Connectivity with NQM probe destination is lost			
Alarm Severity	Condition	<text></text>	Corrective Action	
Minor	-	Connectivity with NQM probe destination is lost	Cleared when connectivity with the Noise Quality Measure (NQM) probe destination is re-established	

### A.1.20.2 NQM High RTT Alarm

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

#### Table A-72: acNqmRttAlarm

### A.1.20.3 NQM High Jitter Alarm

### Table A-73: acNqmJitterAlarm

Alarm	acNqmJitterAlarm			
OID	1.3.6.1.4.1.500	1.3.6.1.4.1.5003.9.10.1.21.2.0.90		
Default Severity				
Alarm Source	Board#%d/Nqm	Board#%d/NqmSender#%d		
Event Type	CommunicationsAlarm			
Probable Cause	Raised when Detected high Jitter towards NQM probe destination - thresholdCrossed			
Alarm Severity	Condition	<text></text>	Corrective Action	
Minor		Detected high Jitter towards NQM probe destination	<ul> <li>To correct high jitter:</li> <li>Test with traceroute.</li> <li>Contact your Internet Service Provider (ISP) with traceroute results.</li> <li>Implement Quality of Service (QoS).</li> <li>Note that there's no simple solution for high jitter. A systemic level solution may be required.</li> </ul>	

### A.1.20.4 NQM High Packet Loss Alarm

Alarm	acNqmPacketLossAlarm			
OID	1.3.6.1.4.1.5003	1.3.6.1.4.1.5003.9.10.1.21.2.0.91		
Default Severity				
Alarm Source	Board#%d/Nqm	nSender#%d		
Event Type	Communication	CommunicationsAlarm		
Probable Cause	Raised when Detected high Packet Loss towards NQM probe destination			
Alarm Severity	Condition	<text></text>	Corrective Action	
Minor	-	Detected high PL towards NQM probe destination	<ul> <li>To correct high packet loss (PL):</li> <li>Eliminate interference problems: Distance your modem from electrical devices</li> <li>Do not coil up any excess signal or power cables.</li> <li>Check the statistics counters of network nodes to determine where loss is occurring. Typically, each node in the network has a packet loss counter. Isolate the network segment where loss has been occurring.</li> </ul>	

### A.1.20.5 NQM Low Conversational MOS Alarm

#### Table A-75: acNqmCqMosAlarm

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

### A.1.20.6 NQM Low Listening MOS Alarm

#### Table A-76: acNqmLqMosAlarm

Alarm	acNqmLqMosAlarm			
OID	1.3.6.1.4.1.500	1.3.6.1.4.1.5003.9.10.1.21.2.0.96		
Default Severity				
Alarm Source	Board#%d/Nqm	nSender#%d		
Event Type	communication	communicationsAlarm		
Probable Cause	Raised when detected low listening voice quality towards NQM probe destination			
Alarm Severity	Condition <text> Corrective Action</text>			
Minor	-	Detected low listening voice quality towards NQM probe destination	To fix the Noise Quality Measure (NQM) result:	
			<ul> <li>Perform corrective action for Real Time Protocol (RTP) packet loss.</li> </ul>	
			See Section A.1.20.4.	
			To fix the poor listening quality that the test indicates:	
			<ul> <li>Try changing the coder</li> </ul>	
			<ul> <li>Try using RTP-Redundancy</li> </ul>	
			<ul> <li>Perform corrective action for RTP packet loss.</li> </ul>	
			See Section A.1.20.4.	

### A.1.21 Intrusion Detection Alarms

### A.1.21.1 IDS Policy Alarm

### Table A-77: acIDSPolicyAlarm

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

# A.1.22 SAS Alarms

### A.1.22.1 Emergency Mode Alarm

#### Table A-78: acGWSASEmergencyModeAlarm

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

# A.1.23 High-Availability (HA)



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

### A.1.23.1 Redundant Board Trap

#### Table A-79: acRedundantBoardAlarm

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

### A.1.23.2 HA Network Watchdog Status Alarm



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

#### Table A-80: acHANetworkWatchdogStatusAlarm

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

### A.1.23.3 Hitless Software Upgrade Status Trap



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

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

#### Table A-81: acHitlessUpdateStatus

# A.2 Event Traps (Notifications)

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

# A.2.1 IDS Threshold Cross Notification

### Table A-82: acIDSThresholdCrossNotification

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

### A.2.2 IDS Blacklist Notification

#### Table A-83: acIDSBlacklistNotification

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

# A.2.3 Web User Access Denied due to Inactivity Trap

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

### Table A-84: acWebUserAccessDisabled

# A.2.4 Power-Over-Ethernet Status Trap



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

#### Table A-85: acPowerOverEthernetStatus

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

# A.2.5 Keep-Alive Trap

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

#### Table A-86: acKeepAlive

# A.2.6 Performance Monitoring Threshold-Crossing Trap

Table A-87:	acPerformance	MonitoringTh	resholdCrossi	ina
		, monitoring in		

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

# A.2.7 HTTP Download Result Trap

### Table A-88: acHTTPDownloadResult

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

# A.2.8 Dial Plan File Replaced Trap



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

#### Table A-89: acDialPlanFileReplaced

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

# A.2.9 Hitless Software Upgrade Status Trap



Note: This alarm is applicable only to Mediant 3000.

#### Table A-90 acHitlessUpdateStatus

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

# A.2.10 Secure Shell (SSH) Connection Status Trap

### Table A-91: acSSHConnectionStatus

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

# A.2.11 SIP Proxy Connection Lost Trap

### Table A-92: acProxyConnectionLost

Alarm		acProxyCor	connectionLost		
OID		1.3.6.1.4.1.5003.9.10.1.21.2.0.94			
Description		Sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up.			
Source Varbind Text		System#0			
Alarm Tex	t	Proxy Set A	larm <text></text>		
Event Type	e	communica	tionsAlarm		
Probable Cause		<ul> <li>Network issue (connection fail due to network/routing failure).</li> <li>Proxy issue (proxy is down).</li> <li>AudioCodes device issue.</li> </ul>			
Alarm Sev	verity				
Severity	Conditi	on	<text></text>		Corrective Action
Major	When connection t Set is lost and this configured with fall	o the Proxy Proxy Set is back to	Proxy Set %d: Proxy not found. Use internal routing	1.	Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.
	routing table.	routing table.		2.	Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.
				3.	If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue.
				4.	Check that routing using the device's (internal) routing table is functioning correctly.
				5.	Contact AudioCodes support center ( <u>support@audiocodes.com</u> ) and send a syslog and network capture for this issue.
Major	Major When Proxy Set ind than one proxy IP v redundancy and co		Proxy Set %d: Proxy lost. looking for another proxy	1.	Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down.
	one of them is lost.	one of them is lost.		2.	Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue.
				3.	If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue.
				4.	Check if routing via the redundant proxy is operating correctly. If it is, then this could mean that it's not a network issue.
				5.	Contact AudioCodes support center ( <u>support@audiocodes.com</u> ) and send a syslog and network capture for this issue.
Cleared	When connection t available again	o proxy is	Proxy found. ip: <ip address&gt;:<port #=""> Proxy Set ID %d</port></ip 	-	

# A.2.12 TLS Certificate Expiry Trap

	acCertificateExpiryNotifiaction			
	1.3.6.1.4.1.5003.9.10.1.21.2.0.92	1.3.6.1.4.1.5003.9.10.1.21.2.0.92		
	Sent before (in days) the expiration be renewed automatically.	Sent before (in days) the expiration of the installed certificate credentials, which cannot be renewed automatically.		
nd Text	System#0	System#0		
	environmentalAlarm	environmentalAlarm		
	The certificate key expired (keyExpired)			
se	acCertificateExpiryNotifiaction			
у				
Condition	<text></text>	Corrective Action		
The certificate key is about to expire.	<ul> <li>Either:</li> <li>The device certificate has expired %d days ago -OR-</li> <li>The device certificate will expire in %d days -OR-</li> <li>The device certificate will expire in less than 1 day</li> <li>%d – number of days</li> </ul>	Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically). To replace certificates, refer to the section 'Replacing the Device's Certificate' in the <i>User's Manual</i> .		
	nd Text se y Condition The certificate key is about to expire.	acCertificateExpiryNotifiaction         1.3.6.1.4.1.5003.9.10.1.21.2.0.92         Sent before (in days) the expiration be renewed automatically.         be renewed automatically.		

#### Table A-93: acCertificateExpiryNotifiaction Trap

# A.2.13 Cold Start Trap

#### Table A-94: coldStart

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

# A.2.14 Authentication Failure Trap

### Table A-95: authenticationFailure

Trap Name	authenticationFailure
OID	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB

# A.2.15 Board Initialization Completed Trap

### Table A-96: acBoardEvBoardStarted

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

# A.2.16 Configuration Change Trap

### Table A-97: entConfigChange

Trap Name	entConfigChange
OID	1.3.6.1.2.1.4.7.2
MIB	ENTITY-MIB

# A.2.17 Link Up Trap

#### Table A-98: linkUp

Trap Name	linkUp
OID	1.3.6.1.6.3.1.1.5.4
MIB	IF-MIB

### A.2.18 Link Down Trap

### Table A-99: linkDown

Trap Name	linkDown
OID	1.3.6.1.6.3.1.1.5.3
MIB	IF-MIB

# A.2.19 D-Channel Status Trap



Note: This alarm is applicable only to Digital Series.

#### Table A-100: AcDChannelStatus

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

# A.2.20 Enhanced BIT Status



Note: This alarm is not applicable to MSBR.

#### Table A-101: AcDChannelStatus

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



This page is intentionally left blank

# **B** Performance Monitoring Counters

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

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

The SCOM supports the following PM counter groups:

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

For more information, see Section 7.5 on page 82.

# **B.1 IP-to-Tel Performance Monitoring**

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



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

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

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

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

# **B.2** SIP Tel-to-IP Performance Monitoring

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



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

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

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

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

# **B.3 SBC Performance Monitoring**

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

### Note:

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

Table B-3:	SBC Call	Admission	Control	Performance	Monitorina
		Admission	001101		monitoring

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



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

# C Optimizing SCOM Server Load-Example Scenario

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

# C.1 Default Loading

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

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

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

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

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

# C.2 Script Load Estimation

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

### C.2.1 Type A Gateways

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

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

Table C-2: Type A Gateways

# C.2.2 Type B Gateways

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

### Table C-3: Type B Gateways

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

# C.2.3 Type C Gateways

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

Table C-4: Type C Gateways

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

# C.3 Load Analysis

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

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





The following summarizes the specific limitations and restrictions on possible frequencies for different kinds of processes:

- Performance counters rules (see Section 7.6 on page 83) have to be launched precisely every 15 minutes due to their dependency on SNMP counters on devices. For example, Tel2IP Calls.
- High and Low Threshold Monitors must also be launched precisely every 15 minutes due to their dependency on SNMP counters on devices. For example, Tel2IP Calls High Threshold Monitor and Tel2IP Calls Low Threshold Monitor.
- Trunk monitor rules 'Audiocodes Digital Trunk Available Channels Counter Rule' and 'Audiocodes Digital Trunk Blocked Channels' Counter Rule and the corresponding threshold monitors 'Audiocodes Blocked Channels High Threshold Monitor' and 'Audiocodes Free Channels Low Threshold Monitor' by default are launched once per minute. This is due to the relatively large number of trunk objects and their dynamic states. For more information, see Section 8.1.4 on page 102.
- Discoveries for Gateways and Modules can be launched at very low polling frequencies because the probability of any parameter changing is low to impossible. At the same time, the trunks discoveries should be launched much more frequently since the probability of any parameter modification is relatively higher.

### C.3.1 Script Execution Without Load Balancing

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

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



Figure C-2: Non-Balanced Script Execution

### C.3.2 Script Execution with Load Balancing

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

- Since gateways and modules do not need to be frequently discovered, it is recommended to set the launching of these processes to once per 60 minutes.
- For the discoveries of trunks, it is recommended to set their launching to once every three minutes (instead of the one minute default).
- All performance measurements (counter rules) and gateway threshold monitors should still be launched once per 15 minutes.
- Performance measurements of trunks (see Section 8.1.4 on page 102) are not dependent on PM counters of devices; and in the SCOM indicate which trunk channels are in-service and which trunk channels are out-of-service. Therefore, we recommend to reduce the polling frequency for running these scripts from the default one minute to once every three minutes.

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

### C.3.2.1 Script Execution Without Overriding Sync Time

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

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



#### Figure C-3: Frequency Without Syncronization

### C.3.2.2 Script Execution when Overriding Sync Time

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

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

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

Table	C-5:	Sync	Time	Sequence
-------	------	------	------	----------

In addition, note the following:

- The corresponding threshold monitors of the above-mentioned counters will have the same minute of synchronization.
- There are 252 discoveries of trunks with scripts that represent 35% of all remaining scripts. Let's set their synchronization minute to 00:01.
- At the same time, there are 288 performance measuring rules of gateways of type C that represent 40% of all remaining counters. Let's set their synchronization time to 00:02.

The figure below shows the results following the above modifications.

The key observation of the figure is that peaks are much lower and smoother over the time axis, which consequently implies lower CPU utilization.




# C.3.3 Resource Monitor

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

You can change the service name of the SCOM ?

## > To open the Resource Monitor on the Windows Server:

Press Cntrl+ Shift + Esc.

#### Figure C-5: SCOM Server Resource Monitor

	1	and the second second					
Overview CPU Mem	iory   Di:	sk Network					
Processes	3% CPU Usage		🧧 66% Maximum Frequency		▲ <b>^</b>	•	Views 👻
✓ Image	PID	Description *	Status	Threads	C 🔺	CPU - Total	100% ¬
explorer.exe	5204	Windows Explorer	Running	19			1
MOMPerfSnapshotHelp	23072	Used to create list of p	Terminated	14			
MOMPerf5napshotHelp	16644	Used to create list of p	Terminated	14			
MonitoringHost.exe	1740	System Center Manag	Running	49			$\sim$
MonitoringHost.exe	3580	System Center Manag	Running	19			N .
MonitoringHost.exe	23364	System Center Manag	Running	10		at the di	
MonitoringHost.exe	2368	System Center Manag	Running	55		60 Seconds	0%
MonitoringHost.exe	12964	System Center Manag	Running	11		Service CPU Usag	e 100% <sub>7</sub>
MonitoringHost.exe	14628	System Center Manag	Terminated	9	-		
Associated Handles			Search Hand	es 😰 😭	•		
Associated Modules						CPU 0	100% <sub>T</sub>
						CPUL1	100% -

### **International Headquarters**

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

#### AudioCodes Inc.

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

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

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond 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.

Document #: LTRT-30808



