User's Manual

AudioCodes One Voice™ Operations Center

AudioCodes One Voice Operations Center

Version 7.4

audiocodes

Table of Contents

1 Introduction 15

1.1 About the One Voice Operations Center 15
1.2 Benefits 15
1.3 Intended Audience 15
1.4 Network Architecture 15
1.4.1 ITSP Multi-Tenancy Architecture 16
1.4.2 Enterprise Multi-Tenancy Architecture 16
1.4.3 Non Multi-Tenancy Architecture 17
1.4.4 OC Elements in Multi-Tenancy Architecture 17

2 Getting Started 19

2.1 Logging in 19
2.2 Getting Acquainted with the Network Page Topology 19
2.2.1 Returning to 'Home' Page by Clicking AudioCodes' Logo 27
2.2.1.1 Hovering Over a Cluster to Display Information 27
2.2.1.2 Hovering Over a Device to Display Information 28
2.2.1.3 Hovering over a Link to Display Information 29
2.3 Getting Acquainted with the Network Map Page 30
2.4 Configuring Operator Authentication 33
2.4.1 Configuring Operator Authentication Centrally using an LDAP Server 33
2.4.2 Configuring Operator Authentication Centrally with a RADIUS Server 35
2.4.3 Viewing Operator Authentication in the Application Information Window 36
2.4.4 Testing Connectivity with the LDAP / RADIUS Server 37
2.4.5 Configuring Operator Authentication Locally, in the OVOC 38
2.5 Adding an Operator 40
2.5.1 How Multi Tenancy Impacts Operator Capabilities 40
2.5.2 Adding a 'System' Operator 41
2.5.2.1 Editing a 'System' Operator 44
2.5.2.2 Deleting a 'System' Operator 44
2.5.2.3 Deleting Multiple Operators 44
2.5.2.4 Suspending a 'System' Operator 44
2.5.2.5 Releasing a Suspended 'System' Operator 44
2.5.2.6 Forcing a Password Change 45
2.5.3 Adding a 'Tenant' Operator 46
2.5.3.1 Editing a 'Tenant' Operator 49
2.5.3.2 Deleting a 'Tenant' Operator 49
2.5.3.3 Deleting Multiple Operators 49
2.5.3.4 Suspending a 'Tenant' Operator 49
2.5.3.5 Releasing a Suspended 'Tenant' Operator 49
2.5.3.6 Forcing a Password Change 50

3 Managing SBC Licenses 51

3.1 Using the Floating License 51
3.1.1 Performing Floating License Actions 54
3.1.1.1 Unmanage 54
3.1.1.2 Update 54
3.1.1.3 Reset 55
3.1.1.4 Register 55
3.1.2 Configuring OVOC-Floating License Service Communications 55
3.1.3 Viewing Floating License Summaries 56
3.1.3.1 Device Floating License Utilization Pane 56
3.1.3.2 Viewing Floating License Info 57
3.1.3.3 Viewing Device Info 58

3.2 Saving a Usage Data Report to your PC 58
4 Configuring Global (System) Settings 61
4.1 Administration tab 61
4.1.1 Viewing License Summary 62
4.1.2 Allocating Licenses to Tenants 63
4.1.3 Authenticating Operators 64
4.2 Configuration tab 64
4.2.1 Configuring Templates 64
4.2.1.1 SNMP Connectivity 64
4.2.1.2 HTTP Connectivity 66
4.2.1.3 QoE Thresholds 67
4.2.1.4 QoE Status and Alarms 68
4.2.2 Configuring Alarms Settings 70
4.2.3 Adding Configuration Files to the OVOC's Software Manager 71
4.2.3.1 Adding the ini File 72
4.2.3.2 Adding a cmp File 73
4.2.3.3 Adding Auxiliary Files 74
4.2.4 Enabling Connecting Directly to External Applications 75
4.2.4.1 ARM 75
4.2.5 Enabling Automatic Device Backup Periodically 76
4.3 Tasks tab 77
4.3.1 Displaying the Status of Tasks Currently Under Execution 77
5 Defining your Network Topology 79
5.1 Adding a Tenant 79
5.2 Adding a Region 85
5.3 Adding Devices 86
5.3.1 Adding a Generic Device 91
5.3.2 Adding a Microsoft Lync Device 92
5.3.3 Managing Device Licenses in the Fixed License Pool 94
5.3.3.1 Performing License Pool Actions 96
5.3.3.1 Before Performing 'Manage Device' / 'Update Device' 99
5.3.3.2 License Pool Alarms 100
5.3.4 Backing up a Device's Configuration using Backup Manager 101
5.3.4.1 Manually Backing up a Device's Configuration 102
5.3.4.2 Saving the Last Backed-up Configuration to your PC 103
5.3.4.3 Restoring the Last Backed-up Configuration to the Device 103
5.4 Adding Links 104
5.5 Adding Sites 108
5.6 Managing Endpoints 109
5.6.1 Dynamic Allocation of Endpoint Licenses 109
5.6.2 Configuring Endpoints 110
5.6.3 Monitoring Endpoints Status 111
5.6.4 Removing Endpoints from QoE Support 111
6 Assessing Network Health 113
6.1 Assessing Health from the Network Summary 113
6.2 Assessing Health from the Network Topology Page 116
6.2.1 Filtering to Access Specific Information 117
6.2.1.1 Filtering by 'Time Range' 117
6.2.1.2 Filtering by 'Topology' 118
6.2.1.3 Filtering by 'Status' 119
6.2.1.4 Filtering by 'More Filters' 120
6.3 Assessing Network Health in the Statistics Pages 121

6.3.1 Viewing Statistics on Calls over Devices 121
6.3.1.1 Metrics Bar Charts 121
6.3.1.2 Statistics Summary 123
6.3.2 Viewing Statistics on Streams over Links 123
6.3.3 Viewing Statistics on Calls over Sites 123
6.3.4 Viewing Statistics on Calls over Endpoints 123
6.4 Determining Network Health from Alarms 124
6.4.1 Configuring Alarm Settings 124
6.4.2 Monitoring Active Alarms to Determine Network Health 124
6.4.3 Performing Management Actions on Active Alarms 125
6.4.3.1 Filtering by 'Severity' 127
6.4.3.2 Filtering by 'Source Type' 128
6.4.3.3 Filtering by 'More Filters' 129
6.4.3.4 Filtering by 'Type' 130
6.4.3.5 Filtering by 'Alarms Name' 131
6.4.4 Viewing Journal Alarms to Determine Operator Responsibility 131
6.4.5 Viewing History Alarms 132
6.4.5.1 Filtering by 'Type' 133
6.4.5.2 Filtering by 'Alarms Name' 134
6.4.6 Forwarding Alarms 135
6.4.6.1 Forwarding Alarms whose Destination is 'SNMP' 137
6.4.6.2 Viewing the New Rules in the Alarms Forwarding Page 141
7 Managing your Network 143
7.1 Performing Management Actions 143
7.1.1 Upgrading Device Software 144
7.1.2 Upgrading Software on Multiple Devices 144
7.1.3 Resetting a Device 144
7.1.4 Downloading the Backup Software Configuration File to the Device 145
7.1.5 Uploading the Device's Configuration File to the Server 147
7.1.6 Locking or Unlocking a Device 148
7.1.7 Synchronizing Links 149
7.1.8 Moving a Device 150
7.1.9 Saving a Device's Configuration File to the PC 151
7.1.10 Burning a Device's Configuration File to Flash Memory 152
7.1.11 Setting Configuration Factory Defaults 152
7.1.12 Resetting Redundant 153
7.1.13 Performing Switchover 153
7.1.14 Showing Device Information 154
7.1.15 Showing Link Information 155
7.1.16 Showing User Information 156
7.1.17 Editing a Device 157
7.1.18 Deleting a Device 157
7.1.19 Resetting a Device 157
7.1.20 Applying a License to a Device from the Pool 158
7.1.21 Refreshing a Device's Pool License 158
7.2 Monitoring Device-Level Backup and Performing Rollback 158
8 Obtaining Quality Statistics on Calls 159
8.1 Accessing the Calls List 159
8.1.1 Filtering by 'Quality' 161
8.1.2 Filtering by 'More Filters' 162
8.2 Showing Call Details 164
8.2.1 Details of a Call Made over an AudioCodes SBC 164
8.2.1.1 Media 165
8.2.1.2 Signaling 167
8.2.1.3 Trends 168

8.2.1.4 SIP Call Flow 169
8.2.2 Call Details Page – Debug File Button 170
8.2.3 Details of a Call Made over Microsoft Skype for Business (Lync) 171
8.2.3.1 Media 173
8.2.3.2 Signaling 175
8.2.4 Details of a Call Made over an Endpoint Using SIP Publish 176
8.2.4.1 Media 178
8.3 Managing QoE Thresholds Profiles per Tenant 180
8.3.1 Understanding the 3 Sensitivity-Level Profiles 181
8.3.2 Understanding How Call Color is Determined 181
8.3.2.1 Link Profile as Determinant 181
8.3.2.2 MOS Metric as Determinant 182
8.3.3 Adding a QoE Thresholds Profile per Tenant 182
8.3.4 Editing a QoE Thresholds Profile per Tenant 185
8.3.5 Deleting a QoE Thresholds Profile per Tenant 185
8.4 Managing QoE Status and Alarms per Tenant 185
8.4.1 Adding a QoE Alarm Rule per Tenant 185
8.4.2 Editing a QoE Alarm Rule per Tenant 188
8.4.3 Deleting a QoE Alarm Rule 188
9 Getting Information on Users Experience 189
9.1 Adding an Active Directory to the OVOC 189
9.1.1 Editing an Active Directory 190
9.1.2 Deleting an Active Directory 191
9.1.3 Synchronizing an AD with the AD Server 191
9.2 Assessing Overall End Users Experience 192
9.3 Assessing a Specific End User's Experience 194
9.4 Managing End Users 194
9.4.1 Filtering the User Details Page 195
10 Producing Reports 197
10.1 Using Reports Features 199
10.1.1 Producing a Network Status Report 201
10.1.2 Producing Trend Reports 204
10.1.3 Producing Top Users Reports 205
10.2 Scheduling a Report 206
10.2.1 Viewing a Scheduler Generated Report 207
10.2.1.1 Saving the File of a Scheduler Generated Report 208
10.2.1.2 Deleting the File of a Scheduler Generated Report 208
10.2.2 Editing a Schedule 208
10.2.3 Deleting a Schedule 208
10.2.4 Manually Running or Pausing a Schedule 208
A AudioCodes IP Network Telephony Equipment 209
B Enabling Initial Connection Provisioning 215
B.1 Before Enabling the Feature 215
B.1.1 Interfaces Table Excerpted from the ini File 215
B.2 Enabling the Feature 216
B.3 Making Sure First Time Provisioning was Successful 216
B.4 Filtering the Alarms Journal by 'More Filters' 218
C Adding an Unprivileged User to MSSQL Server 219

List of Figures

Figure 1-1: ITSP Multi-Tenancy Architecture 16
Figure 1-2: Enterprise Multi-Tenancy Architecture 16
Figure 1-3: Non Multi-Tenancy Architecture - Enterprise 17
Figure 2-1: Login 19
Figure 2-2: OVOC GUI – Network Page – Topology 19
Figure 2-3: Dynamic Tab for Fast Access to Specific Information 24
Figure 2-4: Menu Bar 24
Figure 2-5: Network Map Page 30
Figure 2-6: Example: Endpoints - 12 Warnings 31
Figure 2-7: Alarms Filtered by Severity Level 32
Figure 2-8: OVOC Operator Authentication Options 33
Figure 2-9: Authentication - LDAP 34
Figure 2-10: Authentication - RADIUS 35
Figure 2-11: Test Connectivity 37
Figure 2-12: Authentication – OVOC 38
Figure 2-13: 'System' Operator Settings - Basic Info 41
Figure 2-14: 'System' Operator Settings – Advanced Info 42
Figure 2-15: 'Tenant' Operator Settings – Basic Info 46
Figure 2-16: 'Tenant' Operator Settings – Advanced Info 47
Figure 2-17: 'Tenant' Operator Settings – Tenants 48
Figure 2-18: 'Tenant' Operator Settings – Tenant Assigned 48
Figure 3-1: Floating License 52
Figure 3-2: Device Floating License Page 52
Figure 3-3: Device Floating License Page Actions 54
Figure 3-4: Device Floating License Page – Unmanage Action 54
Figure 3-5: Device Floating License - Administration Page 55
Figure 3-6: Device Floating License Summary 56
Figure 3-7: Device Floating License Summary – Floating License Info 57
Figure 3-8: Device Floating License Summary – Device Info 58
Figure 3-9: Save Usage Report Data 59
Figure 4-1: License Summary 62
Figure 4-2: Tenants Allocations 63
Figure 4-3: Tenant Allocations Settings 63
Figure 4-4: SNMP Connectivity Template 65
Figure 4-5: HTTP Connectivity Template 66
Figure 4-6: QoE Thresholds Templates 67
Figure 4-7: QoE Thresholds Settings 68
Figure 4-8: QoE Status and Alarms 68
Figure 4-9: Alarms Settings 70
Figure 4-10: Software Manager 72
Figure 4-11: Add Auxiliary File – ini File 73
Figure 4-12: Add Software File 73
Figure 4-13: Add Auxiliary File 74
Figure 4-14: External Applications - ARM 75
Figure 4-15: Link for Single Sign On to the ARM 76
Figure 4-16: Device Backup 76
Figure 4-17: Task - Add Multiple AudioCodes Devices 77
Figure 4-18: Prompt to go to Tasks Page to Assess Status 77
Figure 4-19: Tasks Page Showing Task Status - Adding Multiple AudioCodes Devices 78
Figure 5-1: Add Tenant 79
Figure 5-2: Tenant Details - General 79
Figure 5-3: Tenant Details – SNMP v2 80
Figure 5-4: Tenant Details – SNMP v3 81
Figure 5-5: Tenant Details - HTTP 82
Figure 5-6: Tenant Details – Operators 83
Figure 5-7: Tenant Details - License 83
Figure 5-8: Add Region 85

Figure 5-9: Region Details 85
Figure 5-10: AC Device | Multiple AC Devices 86
Figure 5-11: Device Details – General – FQDN 86
Figure 5-12: Device Details – SNMP v2 87
Figure 5-13: Device Details – SNMP v3 88
Figure 5-14: AudioCodes Device Details – HTTP 89
Figure 5-15: AudioCodes Device Details – SBA 90
Figure 5-16: AudioCodes Device Details – Enable SBA 90
Figure 5-17: AudioCodes Device Details – First Connection 91
Figure 5-18: Add Generic Device 92
Figure 5-19: Generic Device Details 92
Figure 5-20: Lync Device 92
Figure 5-21: Lync Device Details 93
Figure 5-22: Fixed License Pool - Update License 95
Figure 5-23: License Pool Settings 96
Figure 5-24: Make Sure Sufficient Licenses are Allocated on the Device's Tenant 99
Figure 5-25: Make Sure License Pool Operator is Valid 99
Figure 5-26: Make Sure the Device is Connected to the OVOC 100
Figure 5-27: Backup Manager 102
Figure 5-28: Backup Manager – Backing up a Device's Configuration – Confirmation Prompt 103
Figure 5-29: Backup Manager – Restoring a Device's Last Backup – Confirmation Prompt 103
Figure 5-30: Links 104
Figure 5-31: Link Details 104
Figure 5-32: Sites 108
Figure 5-33: Site Details 108
Figure 5-34: Example of Dynamic Allocation of Phone Licenses to Tenants 109
Figure 5-35: Login to IP Phone Manager Pro 110
Figure 5-36: Endpoints - Status 111
Figure 6-1: Network Summary 113
Figure 6-2: Example: 12 Endpoint Warnings 114
Figure 6-3: Alarms Filtered by Severity Level 114
Figure 6-4: Dynamic Tab for Quick Future Access to Device Information 116
Figure 6-5: Real Time | Time Range 117
Figure 6-6: Time Range Filter 117
Figure 6-7: Topology 118
Figure 6-8: Alarm 'Status' Filter 119
Figure 6-9: More Filters – Network Topology Page 120
Figure 6-10: Devices Statistics 121
Figure 6-11: Calls Quality Bar Chart 122
Figure 6-12: Utilization Distribution Bar Chart 122
Figure 6-13: Statistics Summary 123
Figure 6-14: Active Alarms Summary 124
Figure 6-15: Alarms - Active 125
Figure 6-16: Alarms - Actions 125
Figure 6-17: Acknowledge Alarm Confirmation 125
Figure 6-18: Delete Alarms Confirmation 126
Figure 6-19: Alarm 'Severity' Filter 127
Figure 6-20: 'Source Type' Filter 128
Figure 6-21: More Filters – Alarms Active Page 129
Figure 6-22: Type Filter 130
Figure 6-23: Active Alarms - Type Filter 130
Figure 6-24: Journal Alarms 131
Figure 6-25: Alarms - History 132
Figure 6-26: Alarms Page Filters 132
Figure 6-27: Type Filter 133
Figure 6-28: History Alarms - Type Filter 133
Figure 6-29: Alarms Forwarding – Topology Conditions 135
Figure 6-30: Alarms – Forwarding – Rule Conditions 136
Figure 6-31: Alarms – Forwarding – Destination Type - SNMP v2 138
Figure 6-31: Alarms – Forwarding – Destination Type - SNMP v3 138

Figure 6-32: Alarms – Forwarding – Destination – Mail 139
Figure 6-32: Alarms – Forwarding – Destination – Mail – Use Internal Mail Server 140
Figure 6-33: New Rules in the Alarms Forwarding Page 141
Figure 7-1: Actions | Edit | Show 143
Figure 7-2: Software Upgrade 144
Figure 7-3: Resetting the Device 145
Figure 7-4: Lock Device 148
Figure 7-5: Lock Confirmation 148
Figure 7-6: Sync Links 149
Figure 7-7: Move Device 150
Figure 7-8: Actions – Reset Redundant 153
Figure 7-9: Actions – Switchover 154
Figure 7-10: Show Device Information 154
Figure 7-11: Show Link Information 155
Figure 7-12: Link's Summary Page 155
Figure 7-13: Showing Information about a User 156
Figure 7-14: Device Details 157
Figure 7-15: Reset Device – Confirmation 157
Figure 7-16: Apply License - Confirmation 158
Figure 8-1: Calls List 159
Figure 8-2: Quality Filter 161
Figure 8-3: More Filters – Calls List Page 162
Figure 8-4: Call Details – Details of a Call Made over an AudioCodes Device 164
Figure 8-5: Media 165
Figure 8-6: Signaling 167
Figure 8-7: Trends 168
Figure 8-8: SIP Call Flow – Example 1 169
Figure 8-9: SIP Call Flow – Example 2 169
Figure 8-10: Call Details - Microsoft Skype for Business 171
Figure 8-11: Media 173
Figure 8-12: Signaling 175
Figure 8-13: Call Details – Over an Endpoint Using SIP Publish 176
Figure 8-14: Media 178
Figure 8-15: QoE Thresholds Profiles 180
Figure 8-16: QoE Thresholds Settings 182
Figure 8-17: Attachments 182
Figure 8-18: Medium Sensitivity QoE Thresholds Profile 183
Figure 8-19: QoE Threshold Details 184
Figure 8-20: QoE Status & Alarms 185
Figure 8-21: QoE Alarm Rule 186
Figure 9-1: Active Directories 189
Figure 9-2: Active Directory Settings 189
Figure 9-3: Active Directory Settings 191
Figure 9-4: Active Directories 191
Figure 9-5: Users Experience 192
Figure 9-6: Specific End User's Experience 194
Figure 9-7: User Details 195
Figure 9-8: Users Filter 195
Figure 10-1: Login 197
Figure 10-2: SEM Reports 197
Figure 10-3: Create Report 201
Figure 10-4: Network Status Report – Call Statistics by Device 201
Figure 10-5: Displaying the Success/Fail Rate Chart 202
Figure 10-6: Trend Reports – Call Statistics by Device 204
Figure 10-7: Top Users Report – Calls Count 205
Figure 10-8: Scheduled Reports 206
Figure 10-9: Scheduler 207
Figure 10-10: Report Generated by Scheduler 207
Figure B-1: First Connection: Add AudioCodes Device | Add Multiple AudioCodes Devices 216
Figure B-2: Alarms Journal 216

Figure B-3: Alarms Journal – Entity Info....217
Figure B-4: Critical Alarm – Initial Connection Provisioning Failed....217
Figure B-5: More Filters – Alarms Journal Page....218
Figure C-1: New Login....219
Figure C-2: SQL Server Authentication....219
Figure C-3: Login Properties – Servers Role - public....220
Figure C-4: Login Properties – User Mapping – db_datareader | public....220
Figure C-5: Lync Device Details....221

List of Tables

Table 1-1: OVOC Application Elements Defined in Multi-Tenancy Architecture....17
Table 2-1: Network Topology – Network Entities and Statuses....20
Table 1-2: Menu Bar....24
Table 2-3: Cluster Icons in the Network Map Page....30
Table 2-4: OVOC Operator Authentication Parameters....39
Table 2-5: Capabilities Allowed for Each Operator Type / Security Level....40
Table 2-6: 'System' Operator Settings - Basic Info....41
Table 2-7: 'System' Operator Settings – Advanced Info....43
Table 2-8: 'Tenant' Operator Settings – Advanced Info....47
Table 3-1: Floating License Page Column Descriptions....52
Table 3-2: Device Floating License Configuration Parameter Descriptions....55
Table 3-3: Device Floating License Utilization Pane Description....56
Table 3-4: Device Floating License Summary - Floating License Info....57
Table 4-1: System Menu....61
Table 4-2: SNMP Connectivity Template....65
Table 4-3: HTTP Connectivity Template....66
Table 4-4: QoE Thresholds Templates....67
Table 4-5: QoE Status and Alarms....69
Table 4-6: Alarms Settings....70
Table 4-7: OVOC Software File Management per Operator Type....72
Table 5-1: Tenant Details - General....80
Table 5-2: Tenant Details – SNMP v2....80
Table 5-3: Tenant Details – SNMP v3....81
Table 5-4: Tenant Details - HTTP....82
Table 5-5: Tenant Details - Operators....83
Table 5-6: Tenant Details – License....84
Table 5-7: LP Column Indicating License Statuses....98
Table 5-8: Explanation of Backed Up File Name Format....102
Table 5-9: Adding a Link – Parameter Descriptions....105
Table 6-1: Time Range Filter....118
Table 6-2: Topology Filter....119
Table 6-3: Status Filter....120
Table 6-4: More Filters - Network Topology Page....120
Table 6-5: Severity Filter....127
Table 6-6: 'Source Type' Filter....128
Table 6-7: More Filters – Alarms Active Page....129
Table 6-8: Alarms Forwarding – Topology Conditions....135
Table 6-9: Forwarding Alarms – Rule Conditions - Parameter Descriptions....137
Table 6-10: Forwarding Alarms – Destination....137
Table 6-11: OVOC-Syslog Severity Levels Mapping....139
Table 6-12: Forwarding Alarms - Destination – Mail....140
Table 8-1: Calls List Columns....159
Table 8-2: 'Quality' Filter....161
Table 8-3: More Filters – Calls List....162
Table 8-4: Call Details Page....164
Table 8-5: Media Parameters....165
Table 8-6: Signaling Parameters....167
Table 8-7: Error Response Color Codes....170
Table 8-8: SIP Message Color Codes....170
Table 8-9: Call Details - Microsoft Skype for Business....171
Table 8-10: Media Parameters....173
Table 8-11: Signaling Parameters....175
Table 8-12: Call Details - Over an Endpoint Using SIP Publish....176
Table 8-13: Media Parameters....178
Table 8-14: Quality Profile Parameters....181
Table 8-15: QoE Alarm Rule....186
Table 9-1: Active Directory Settings....190

Table 9-2: Users Experience 192
Table 9-3: 'Users' Filter 196
Table 10-1: Reports Categories 198
Table 10-2: Reports Features 199
Table 10-3: Table Columns in Network Status Reports 203
Table 10-4: Table Columns in Top Users Reports 206
Table A-1: Supported AudioCodes IP Network Telephony Equipment 209
Table B-1: More Filters – Alarms Journal Page 218

Notice

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

This document is subject to change without notice.

Date Published: May-23-2018

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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

Related Documentation

Document Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User’s Manual
Mediant 800B MSBR User’s Manual
Mediant 1000B Gateway and E-SBC User’s Manual
Mediant 1000B MSBR User’s Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User’s Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
One Voice Operations Center Server Installation, Operation and Maintenance Manual
One Voice Operations Center Product Description

Document Name
One Voice Operations Center Integration with Northbound Interfaces Guide
IP Phone Manager Pro Administrator's Manual
IP Phone Manager Express Administrator's Manual
ARM User's Manual
One Voice Operations Center Security Guidelines
One Voice Operations Center Alarms Guide

Document Revision Record

LTRT	Description
91036	Initial document release for Version 7.4.
91037	Version 7.4 GA
91039	Updated to patch Version 7.4.1000. Network Map page | SIP Call Flow | QoE Link - regular expression | ARM SSO | RADIUS/LDAP SSO | Calls List – new columns | 'Location' field | Show Grid | New AudioCodes logo and login screen | Hover cursor
91040	Calls List – 3-hour call. Timer defaults (0). Session Inactivity Period. Adding an Unprivileged User to MSSQL Server.
91041	Call Details page's PL parameter > 100%. Limitation note: Calls on HA devices unsupported. Backed-up filename format explanation.
91042	Connect to Ext. Apps: ARM. Endpoints License Allocation. Use Internal Mail Server (Alarms Forwarding) . FQDN (Add Device). 'IP Group Value' (Add Link)

Documentation Feedback

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

1 Introduction

1.1 About the One Voice Operations Center

AudioCodes' One Voice Operations Center (referred to as 'OVOC' for short in this document) is a life-cycle management application for large-scale cloud or premises-based Unified Communications (UC) deployments.

The OVOC provides full coverage of the entire set of actions required to manage a voice network in a UC environment. The application provides a powerful voice Network Operation Center (NOC), complete end-to-end voice network control, service assurance capabilities and comprehensive optimization and planning tools.

The OVOC uniformly manages, monitors and operates the entire AudioCodes One Voice portfolio, including Media Gateways, Session Border Controllers, Microsoft SBAs and IP Phones.

1.2 Benefits

- Easy and secure transition to VoIP deployments including UC, hosted business services and contact centers
- OpEx and TCO reduction by using centralized tools to remotely operate the VoIP network components
- Efficiency and simplified device operation, administration and fault management
- Intuitive real time network view, capturing entire network status in real time
- Reduce MTTR with integrative detection and correction tools
- Powerful analytic reports for effective planning of future network expansion and optimization

1.3 Intended Audience

This *User's Manual* targets three audiences:

- The ITSP administrator whose network features multi-tenancy architecture and whose OVOC application will provide telephony management services to multiple enterprise customers (tenants) in their network. See Section 1.4 below for more information.
- The enterprise administrator whose network does not feature multi-tenancy architecture and whose OVOC application will enable management of the enterprise's distributed offices. See Section 1.4 below for more information.

Note: The enterprise administrator whose network does not feature multi-tenancy architecture can skip documentation related to multi-tenancy.

- The enterprise administrator whose network features multi-tenancy architecture and whose OVOC application will provide telephony management services to multiple regional branches (tenants) in their network. See Section 1.4 below for more information.

1.4 Network Architecture

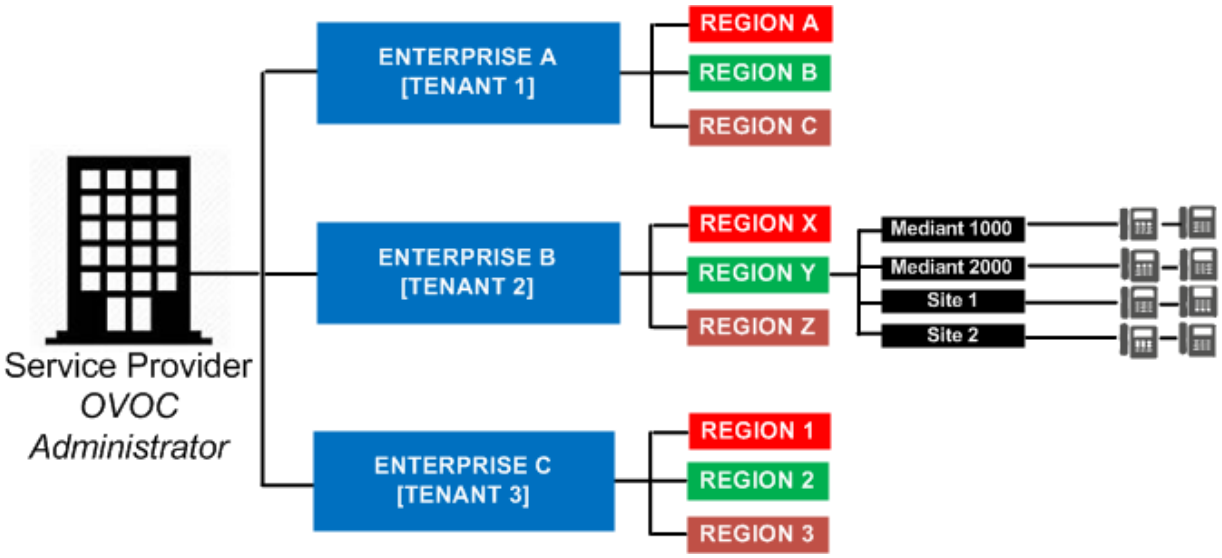
The OVOC features three types of telephony network architecture:

- Multi-Tenancy Architecture (see Section 1.4.1 and 1.4.2)
- Non Multi-Tenancy Architecture (see Section 1.4.3)

1.4.1 ITSP Multi-Tenancy Architecture

ITSP multi-tenancy architecture allows an Internet Telephony Service Provider (ITSP) administrator to deploy a single instance of the OVOC application to provide a telephony network management service to multiple enterprise customers (tenants).

Figure 1-1: ITSP Multi-Tenancy Architecture

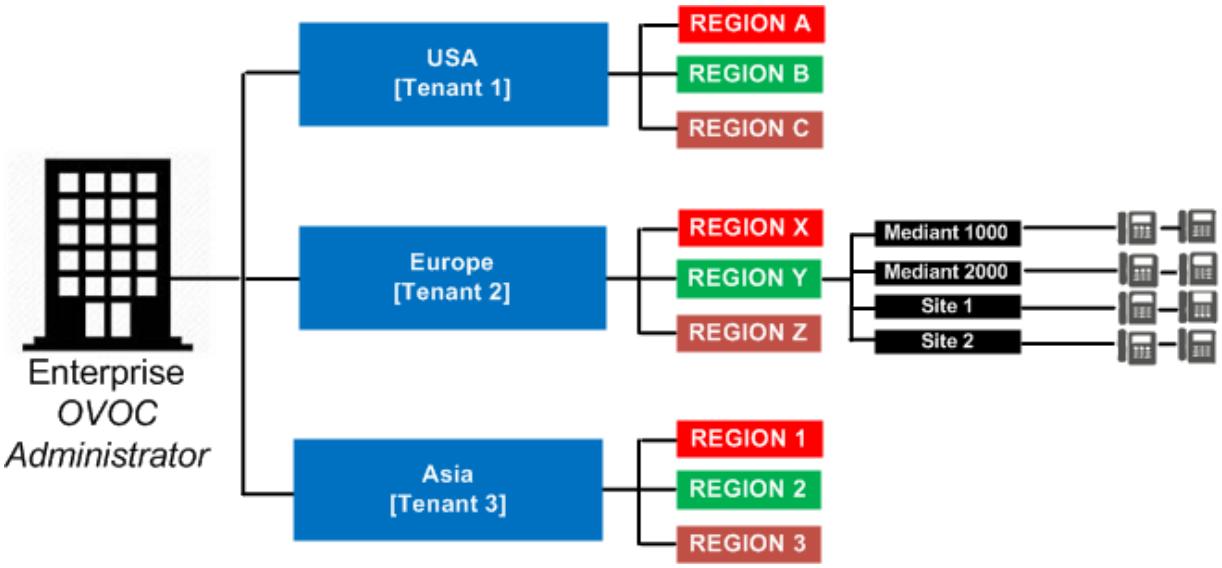


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

1.4.2 Enterprise Multi-Tenancy Architecture

Enterprise multi-tenancy architecture allows an enterprise administrator to deploy a single instance of the OVOC application in order to provide a telephony network management service to multiple regional branches (tenants).

Figure 1-2: Enterprise Multi-Tenancy Architecture

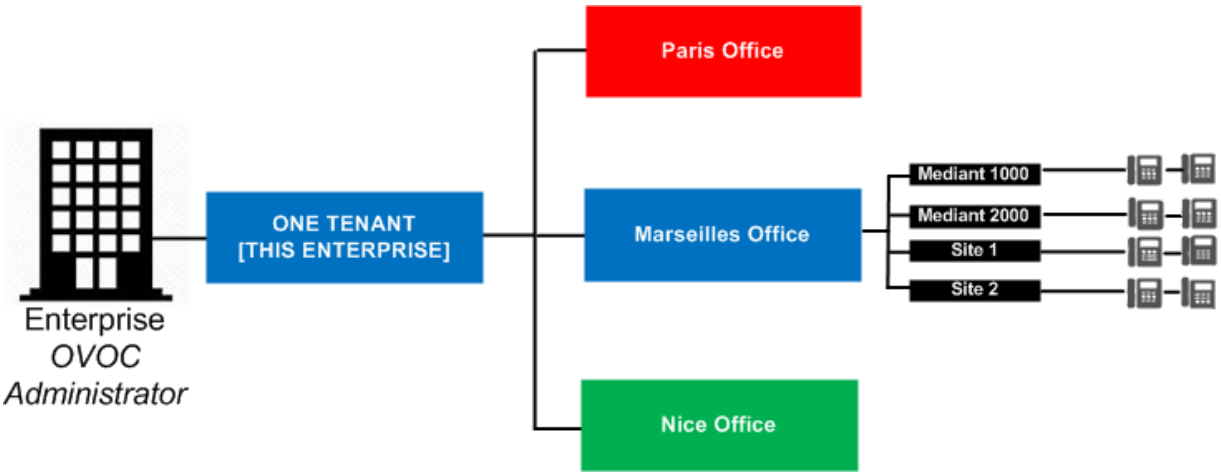


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

1.4.3 Non Multi-Tenancy Architecture

Non multi-tenancy architecture allows an enterprise's network administrator to define a single tenant (themselves) in order to provide a network management service to the enterprise's distributed offices.

Figure 1-3: Non Multi-Tenancy Architecture - Enterprise



1.4.4 OC Elements in Multi-Tenancy Architecture

The table below shows OVOC application elements defined in multi-tenancy architecture.

Table 1-1: OVOC Application Elements Defined in Multi-Tenancy Architecture

Element	Description
OC System	An ITSP managing multiple enterprises using a cloud-based or hosted 'global' OVOC application.
OC Tenant	▪ An ITSP's enterprise customer, using only a portion of the OVOC resources and only some of the OVOC entities. Other tenants (the ITSP's other enterprise customers) in the ITSP's multi-tenant network will be invisible to this tenant. ▪ An enterprise's regional branch, using only a portion of the OVOC resources and only some of the OVOC entities. ▪ An enterprise whose network administrator must define a tenant (that enterprise) under which to define the enterprise's distributed offices.
OC entity	Any element which can be managed or used as a whole: ▪ Tenant entity (managed/assigned by a specific OVOC tenant) ▪ Global entity (managed by the OVOC system; applies to/affects all tenants) ▪ System entity (managed /assigned only by the OVOC system)
OC resource	Any element that can be partly managed/assigned: ▪ Global resource (managed by the OVOC system; applies to/affects all tenants) ▪ Tenant resource (portion of the resource)

This page is intentionally left blank.

2 Getting Started

This section shows how to get started with the One Voice Operations Center.

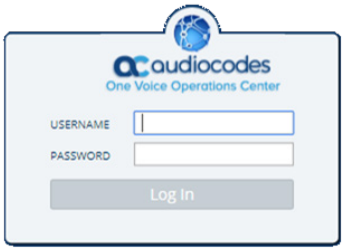
2.1 Logging in

This section covers how to log in to the OVOC.

➢ To log in to the OVOC:

1. Point your browser to the OVOC server's IP address: **https:// <IP Address>**. You only need to enter its IP address; the rest of the URL is automatically added. Logging in can optionally be performed using FQDN rather than IP address.

Figure 2-1: Login



2. Enter your Username and Password:
   - acladmin (default) (case-sensitive) (can be modified later after defining users)
   - pass_1234 (default) (case-sensitive) (can be modified later after defining users)

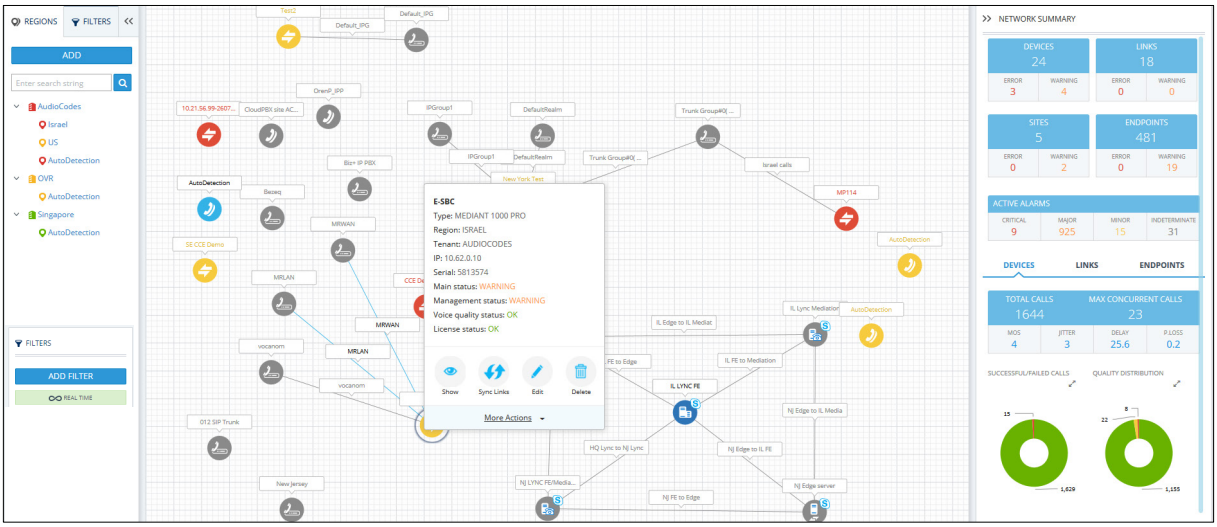
   The GUI opens by default on the Network Topology page (see the figure below).

Note: It's recommended to change the password after initial login.

2.2 Getting Acquainted with the Network Page Topology

This section familiarizes you briefly with the OVOC. Figure 2-2 shows the OVOC's central page - the Network Topology page - which opens by default after logging in.

Figure 2-2: OVOC GUI – Network Page – Topology



The Network Topology page (see Figure 2-2) is divided into three panes: left, middle and right.

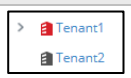
In the left pane, the 'tree' displays network entities, up to the level of tenant (first-level navigation).

The middle pane displays a topological view of devices and links in the network on which operators can quickly obtain basic device information and statuses and perform actions (second-level navigation).

The right pane displays a summary of network statistics from which operators can determine network health.

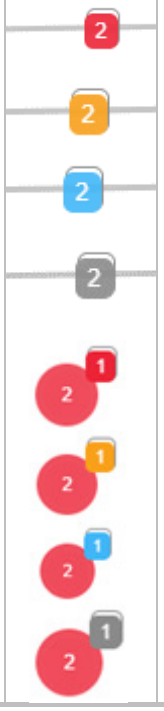
Each entity can be viewed in table view. Table 2-5 below explains the entity icons in the Network Topology page. Icon colors are propagated from the statuses of the entities. Entity status is derived from management status, voice quality status and license status.

Table 2-1: Network Topology – Network Entities and Statuses

Network Entity	Icon	Explanation
Tenant		For detailed information about multi-tenancy architecture, see Section 1.4.1. = Tenant status is Error when one or more of the following exists: ✓ management status of at least one region is Error ✓ voice quality status of at least one region is Error ✓ license status of at least one region is Error ✓ license status of the tenant itself is Error due to one of these [Critical] alarms: QoE Devices Overload, QoE Sessions Overload, QoE Endpoints Overload or Endpoints Management Overload. = Tenant status is Warning when one or more of the following exists: ✓ management status of at least one region is Warning ✓ voice quality status of at least one region is Warning ✓ license status of at least one region is Warning ✓ license status of the tenant itself is Warning due to one of these [Major] alarms: QoE Devices Overload, QoE Sessions Overload, QoE Endpoints Overload or Endpoints Management Overload. ✓ One of the tenant's AD is disconnected = Tenant status is OK when one or more of the following exists: ✓ management status of all regions is OK or Unmonitored ✓ voice quality status of all regions is OK or Unmonitored ✓ license status of all regions is OK or Unmonitored ✓ license status of the tenant itself is free of alarms ✓ All the tenant's ADs are connected = Tenant status is Unmonitored when one or more of the following exists: ✓ management status of all regions is Unmonitored ✓ voice quality status of all regions is Unmonitored ✓ license status of all regions is Unmonitored
Region		= Region status is Error when one or more of the following exists: ✓ management status of at least one device or site is Error ✓ voice quality status of at least one device or site is Error ✓ license status of at least one device or site is Error = Region status is Warning when one or more of the following exists:

Network Entity	Icon	Explanation
		✓ management status of at least one device or site is Warning ✓ voice quality status of at least one device or site is Warning ✓ license status of at least one device or site is Warning = Region status is OK when one or more of the following exists: ✓ management status of all devices and sites is OK or Unmonitored ✓ voice quality status of all devices and sites is OK or Unmonitored ✓ license status of all devices and sites is OK or Unmonitored = Region status is Unmonitored when one or more of the following exists: ✓ management status of all devices and sites is Unmonitored ✓ voice quality status of all devices and sites is Unmonitored ✓ license status of all devices and sites is Unmonitored
Device		Indicates an AudioCodes SBC communicating with the OVOC. = Device status is Error when one or more of the following exists: ✓ management status is Error (if device alarms status or connection status is disconnected) ✓ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ✓ License status is Error only if license pool is failed or expired = Device status is Warning when one or more of the following exists: ✓ management status is Warning (if device alarms status or administration status is Warning) ✓ voice quality status is Warning (if control status or media status or connection status is Warning) ✓ license status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the device or if there is no voice quality license) = Device status is OK when one or more of the following exists: ✓ management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined) ✓ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined) ✓ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Strikethrough = locked No strikethrough = unlocked
Microsoft Lync Device		= Microsoft Lync Mediation Server = Microsoft Lync Edge Server = Microsoft Lync Front End Server
Generic Device		Indicates a non-AudioCodes device or entity that is also part of the OVOC network topology: IP PBX (shown on left), SIP trunk, other vendors' SBC / gateway. These devices participate in processing OVOC network calls and are connected to devices.
Site	-	Color and status are propagated from the endpoints under the site.

Network Entity	Icon	Explanation
Link		A link joins two devices: Red = Voice quality status is Error when one or more of the following exists: ✓ 'Critical' Control Status ✓ 'Critical' Media Status Orange = Voice quality status is Warning when one or more of the following exists: ✓ 'Major' Control Status ✓ 'Major' Media Status Blue = Voice quality status is OK/Clear when one or more of the following exists: ✓ Control Status is OK/Clear ✓ Media Status is OK/Clear ✓ Control Status or Media Status is Unmonitored Gray = Voice quality status is Unmonitored when both of these exist: ✓ Control Status is Unmonitored ✓ Media Status is Unmonitored **Note**: ✓ If no voice quality license exists, status will be Unmonitored. ✓ Link status does not impact device / region ✓ If >> or << is displayed, one-directionality is signified, i.e., the link only aggregates incoming or outgoing calls. ✓ If no arrows are displayed, bi-directionality is signified, i.e., the link aggregates both incoming and outgoing calls.
Device clusters		Indicate aggregated clusters of devices (AudioCodes devices as well as non-AudioCodes devices). The numbers indicate how many devices are in the cluster. ▪ Red = at least one entity in this cluster has a status of Error – see above in this table for the one or more conditions that need to exist for status to be Error ▪ Orange = at least one entity in this cluster has a status of Warning – see above in this table for the one or more conditions that need to exist for status to be Warning ▪ Blue = at least one entity in this cluster has a status of OK – see above in this table for the one or more conditions that need to exist for status to be OK ▪ Gray = at least one entity in this cluster has a status of Unmonitored – see above in this table for the one or more conditions that need to exist for status to be Unmonitored

Network Entity	Icon	Explanation
Link clusters		Square icons indicate aggregated clusters of links. The link indication can be on a line representing a link (left upper) or adjoined to a device cluster (left lower). The number in each square indicates how many links are in the cluster. ▪ Red square = at least one link in this cluster has a voice quality status of Error – see above in this table for the one or more conditions that need to exist for voice quality status to be Error ▪ Orange square = at least one link in this cluster has a voice quality status of Warning – see above in this table for the one or more conditions that need to exist for voice quality status to be Warning ▪ Blue square = at least one link in this cluster has a status of OK – see above in this table for the one or more conditions that need to exist for status to be OK ▪ Gray square = at least one link in this cluster has a voice quality status of Unmonitored – see above in this table for the two conditions that need to exist for voice quality status to be Unmonitored

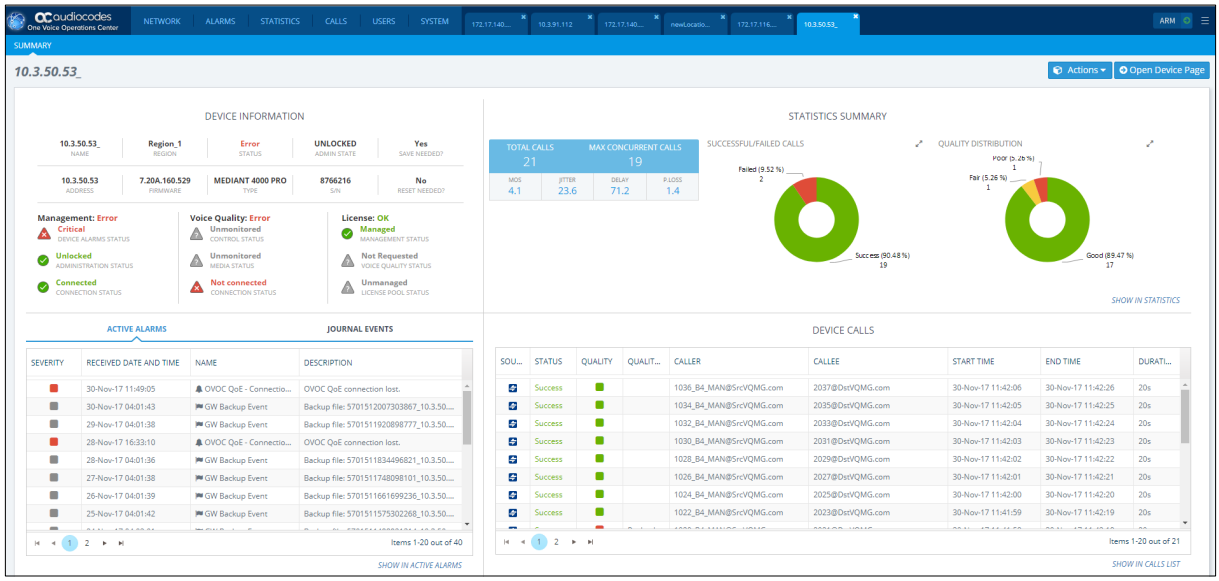
- Click the **+-** icon to zoom in or out of the map.
- Click the **Center Map** button to center the map in the page - useful if the previous operator dragged it off center.
- Click the **Save Map Locations** button to save the map locations.
- Click the **Create Links** button to create a link.

- The **Show Grid** button allows operators to display gridlines; the background of the Network Topology page is by default white.
- **Show Clusters**. If more than 200 devices and sites (aggregated) are defined, the button will not be available and the page will *automatically* be displayed in clusters. The button will only be available if fewer than 200 devices and sites (aggregated) are defined. The feature reduces clutter and improves operational efficiency.
- Select an area: Press the Shift key and press the mouse.

The Network Topology page lets you quickly drill down from a tenant to the core of an issue. Fast access to very specific information makes network management efficient. This capability earns OVOC the title of 'expert system'.

Specific information related to device, user and call is automatically dynamically tabbed on the menu bar, facilitating quick and easy future access and troubleshooting:

Figure 2-3: Dynamic Tab for Fast Access to Specific Information



For more information about the dynamic tab that is created for call details, see Section 8.2.

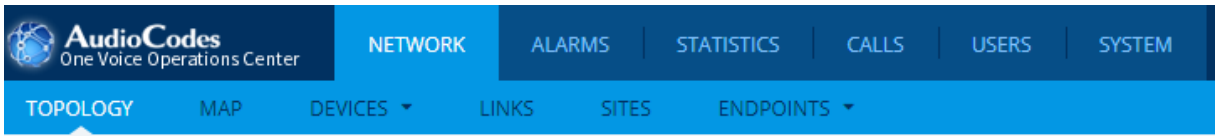
For more information about the dynamic tab that is created for user details, see Section 9.3.

A dynamic tab lets you quickly access a specific page that is automatically dynamically tabbed on the menu bar after for example drilling down in the Topology page from a tenant to the core of an issue. The tab allows quick and easy future access to specific information related to device, user, call, etc., displayed in the page. It can be deleted from the menu bar at any time. The feature simplifies troubleshooting management.

The right pane of the Network Topology page summarizes device statuses and alarms in the network.

Figure 2-4 below shows the OVOC's menu bar.

Figure 2-4: Menu Bar



Use the table below as reference.

Table 1-2: Menu Bar

Menu	Tab	Description
Network	**Topology**	The tab's page lets you: ▪ Assess at a glance the topology of the network ▪ Perform multiple configuration and maintenance actions ▪ Select multiple devices (Ctrl+) and perform multiple actions simultaneously ▪ Filter out unwanted information to facilitate quick access to specific information. The page features two 'modes': ▪ Real Time mode. The page continuously refreshes, presenting up-to-date network information. ▪ Time Filter. The page presents network information valid for the time defined in a Time Filter but invalid in real time. See Section 6.2.1 for information about time filters.

Menu	Tab	Description
	Map	The tab's page lets you: ▪ Assess at a glance the enterprise network's global distribution ▪ Filter The page features two 'modes': ▪ Real Time mode. The page continuously refreshes, presenting up-to-date network information. ▪ Time Filter. The page presents network information valid for the time defined in a Time Filter but invalid in real time. See Section 6.2.1 for information about time filters.
	Devices	The tab lets you: • Add a network component: • Perform a device action • Show device
	Links	Lets you add, edit or delete links.
	Sites	Lets you: ▪ add a set of endpoints based on a network subnet ▪ edit or delete the SIP clients (phones)
	Endpoints	From the tab's dropdown you can select: ▪ **Status**. Lets you view and monitor the status (Quality of Experience) of phones (for example). ▪ **Configuration**. Lets you directly access the IP Phone Manager Pro to configure phones.
Alarms	**Active**	Always displays all the active alarms in the network, in real time.
	Journal	Displays only the operator activity alarms in the network.
	History	Displays time frame historical alarms (default), according to the filter.
	Forwarding	For detailed information about forwarding alarms, see under Section 6.4.5.2.
Statistics	**Devices**	Displays the Devices Statistics page. Filters on the page allow operators to specify which call quality metrics to display. Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	Links	Displays the Links Statistics page. Filters on the page allow operators to specify • which call quality metrics to display (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo) • which links to display (per Topology or Time Range) Quick access to specific information lets operators quickly and effectively maximize users' QoE.

Menu	Tab	Description
	Sites	Displays the Sites Statistics page. Filters on the page allow operators to specify • which call quality metrics to display (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo) • which sites to display (per Topology or Time Range) Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	Endpoints	Displays the Endpoints Statistics page. Filters on the page allow operators to specify • which call quality metrics to display (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo) • which endpoints to display (per Topology or Time Range) Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	Reports	Provides operators with essential reports-generation capability which they can utilize to distribute session experience data and comparative analyses quickly and effectively to responsible persons within the enterprise, and to external authorities associated with the enterprise's network, for accurate diagnosis and correction of degraded sessions and for general network optimization. Opens in another Web page.
Calls	**Calls List**	Displays the Calls List page which presents all the calls made in the enterprise. Filters allow operators to specify which calls to display (Topology, Time Range, Source Type, Quality, etc.). Quick access to specific information allows operators to quickly and effectively maximize users' QoE.
	QoE Thresholds	Lets you apply QoE Threshold profiles for voice quality metrics (MOS, Delay, Packet Loss, Echo and Jitter). A QoE Threshold profile consists of threshold values set for each of these metrics for the 'Poor', 'Fair' and 'Good' call quality categories.
	QoE Status & Alarms	Lets you configure Quality Alarms which are automatically triggered and displayed in the Alarms page if the quality analyzed falls below that defined in the rules. Also lets you determine the status of the voice quality per entity.
Users	**Users Experience**	Calls Count, Total Duration, Success / Failed, Call Quality, MOS, Jitter, Delay, and Packet Loss. Gives operators network health monitoring capability, including alarms and diagnostics. Used to maximize the quality of experience (QoE) of end users in the network.
	User Details	Displays contact information about the end users: Full Name, User Name, Description, Department, Office, Mobile, Home, MS Lync Line URI, Email, Server, Country. Filters allow quick access to specific users. These filters impact the Users Experience page (see previous), so operators can specify which users whose calls quality of experience they want to assess.
	Active Directories	Lets you add an AD. Displays existing ADs. Allows you to edit and to synchronize with the AD server.

Menu	Tab	Description
System	**Administration**	Allows performing administration: • License ✓ Summary ✓ Tenants Allocations • Security ✓ Authentication ✓ Operators
	Configuration	Allows performing OVOC administration: • Templates • Alarms • File Manager (Software Manager) • External Applications • Device Backup
	Tasks	Only displays asynchronous actions performed by the OVOC operator.

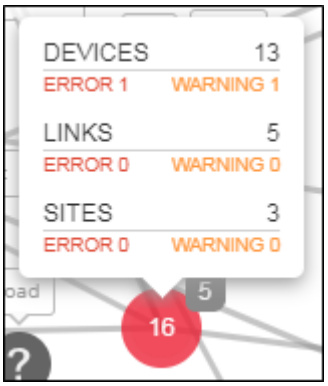
2.2.1 Returning to 'Home' Page by Clicking AudioCodes' Logo

You can click the AudioCodes logo displayed on every page of the OVOC, to return to the Network Topology page.

The AudioCodes logo functions as a 'Home' page button.

2.2.1.1 Hovering Over a Cluster to Display Information

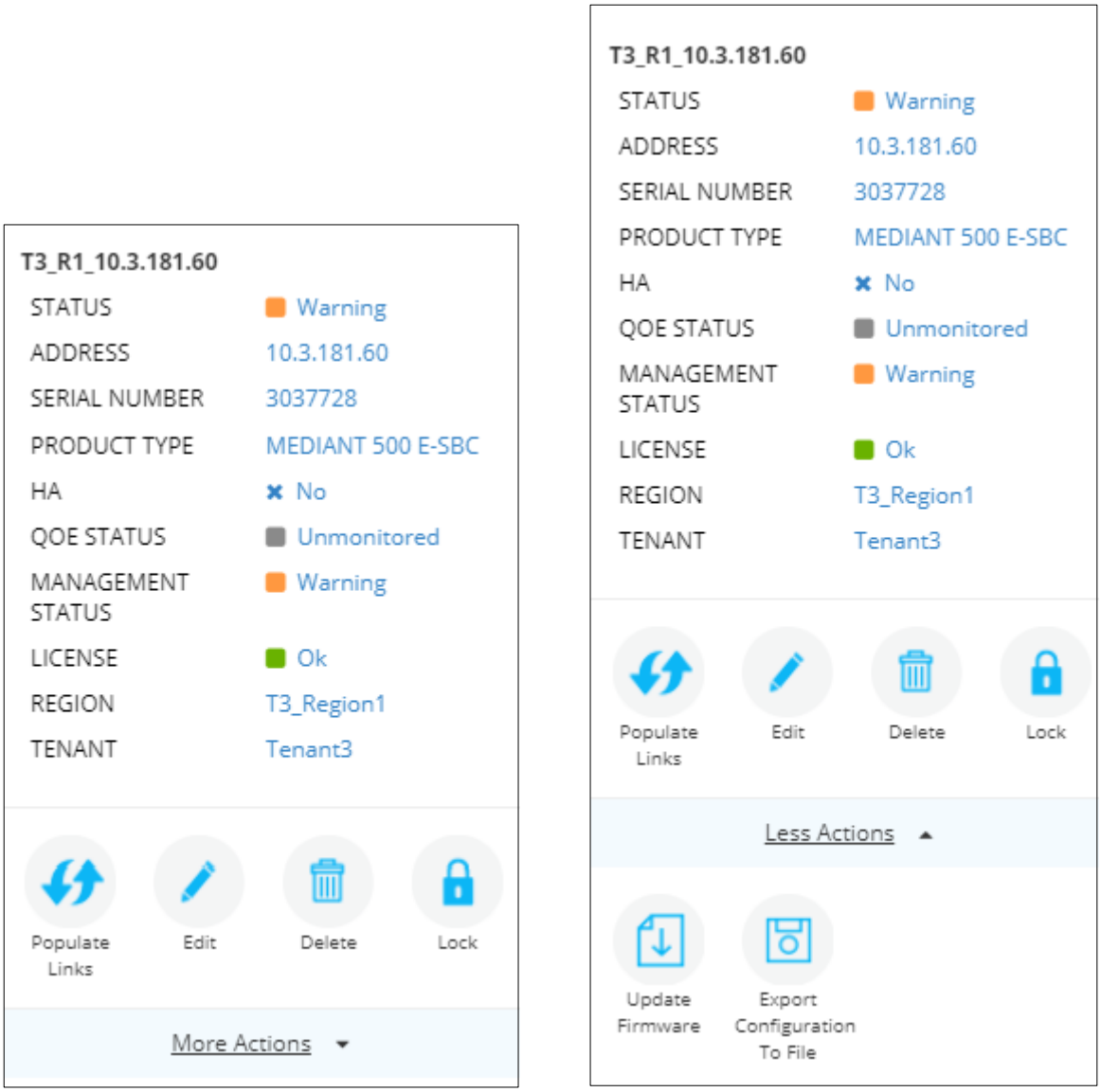
The figure below shows the information displayed when hovering over a cluster.



The popup displays a summary of devices, links and sites. The popup also indicates the number of errors and warnings on each.

2.2.1.2 Hovering Over a Device to Display Information

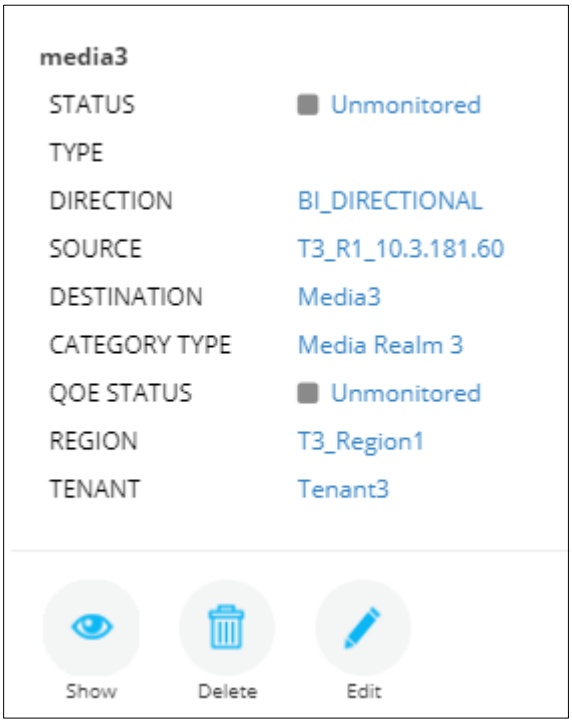
The figure below shows an example of information displayed when hovering over a device.



The popup displays a summary of device information and statuses. The lowermost section of the popup displays the actions that can be performed on the device. More actions can be accessed and performed by clicking the More button. The content displayed in the popup depends on the type of device over which you hover.

2.2.1.3 Hovering over a Link to Display Information

The figure below shows an example of information displayed when hovering over a link.

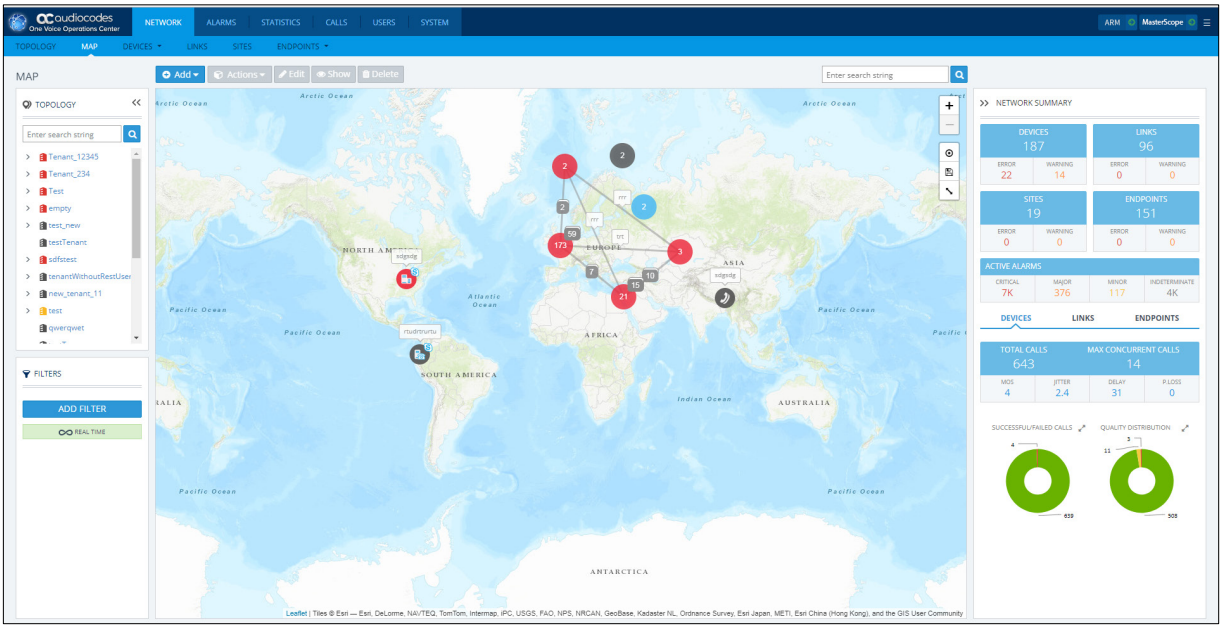


The popup displays a summary of link information and statuses. The lowermost section of the popup displays the actions that can be performed on the link. The content displayed in the popup depends on the type of device over which you hover.

2.3 Getting Acquainted with the Network Map Page

The Network Map page (**Network** > **Map**) allows operators to determine at a glance the geographical global distribution of the enterprise's IP telephony network.

Figure 2-5: Network Map Page



With the exception of cluster icons, entity icons in the Network Map page are identical to those in the Network Topography page described in Table 2-5. A cluster is based on geographical locations of devices in the Network Map page. Clusters show *aggregated numbers of devices*. Cluster status is unrelated to region and/or tenant status. Region and/or tenant status are only reflected in the Network Map tree and Network Topology tree. Selecting a tenant in the Network Map page's tree impacts the Network Map page in the same way as selecting a tenant in the Network Topology page's tree.

Table 2-3: Cluster Icons in the Network Map Page

Cluster Icon	Description
	Cluster status is Error when the status of at least one device or site is Error. Click a cluster to zoom in and view the entities under it.
	Cluster status is Warning when the management status of at least one device or site is Warning. Click a cluster to zoom in and view the entities under it.
	Cluster status is OK when the management status of all devices and sites is OK or Unmonitored. Click a cluster to zoom in and view the entities under it.
	Cluster status is Unmonitored when the management status of all devices and sites is Unmonitored. Click a cluster to zoom in and view the entities under it.

The only difference between Network Map page and the Network Topology page is that in the Network Map page there is no **Show Grid** button. All other buttons are the same. In the Network Map page you can:

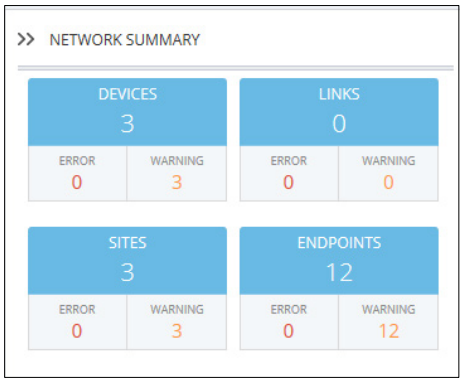
- Click the **+-** icon to zoom in or out of the map.
- Click the **Save Map Locations** button to save the map locations.
- Click the **Center Map** button to center the map in the page - useful if the previous operator dragged it off center.

- Hover the cursor over a network entity to determine its details:

In the pane on the right side of the Network Map page, the Network Summary lets you:

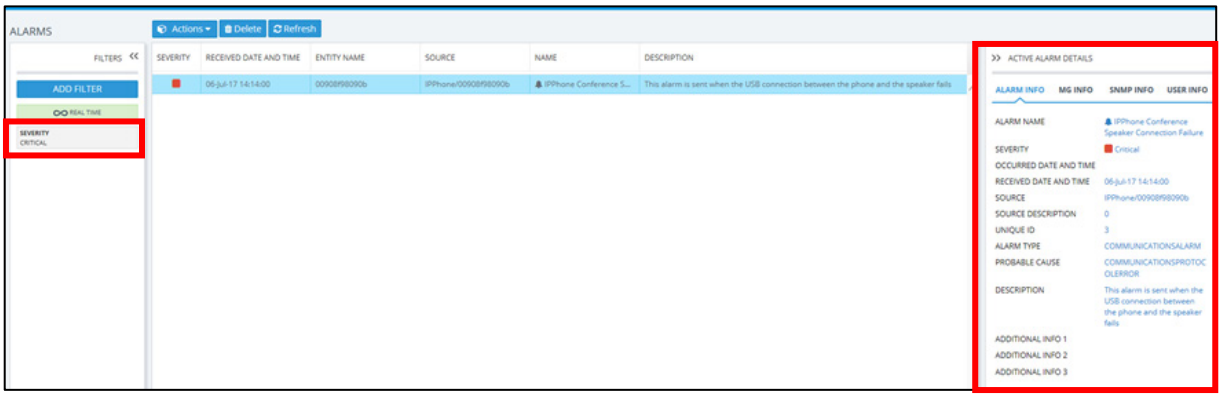
- Determine how many Devices, Links, Sites and Endpoints on which alarms are currently active.
- Determine which Devices, Links, Sites and Endpoints' status is currently Error / Warning (from the color-coded number). If you click the color-coded number of:
  - **Devices** then the Devices Manage page opens displaying all devices whose status is Error / Warning
  - **Links** then the Links page opens displaying all links whose status is Error / Warning
  - **Sites** then the Sites page opens displaying all sites whose status is Error / Warning
  - **Endpoints** then the Endpoints page opens displaying all endpoints whose status is Error / Warning

Figure 2-6: Example: Endpoints - 12 Warnings



The Active Alarms pane allows you to determine the total number of Critical, Major, Minor and Indeterminate active alarms (color-coded) currently active in the network. Click any severity level's total to display only alarms of that severity level in the Alarms page. Example: Under **Critical** in the Active Alarms pane above, click **1**:

Figure 2-7: Alarms Filtered by Severity Level

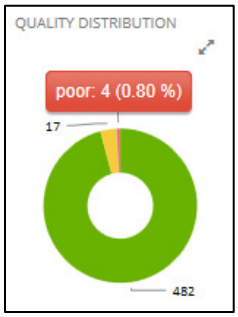


In the Active Alarms pane, you can select an alarm in the page to view detailed information about it in the All Alarm Details pane on the right side of the page.

In the Network Summary window, the **Devices** | **Links** | **Endpoints** tabs display the:

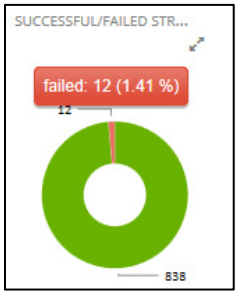
- total # of calls over devices | streams over links | calls over endpoints.
- maximum # of concurrent calls over devices | streams over links.
- average MOS measured over devices | links | endpoints in the network.
- average Jitter measured over devices | links | endpoints in the network.
- average Delay measured over devices | links | endpoints in the network.
- average Packet Loss measured over devices | links | endpoints in the network.

The **Quality Distribution pie chart** in the Network Summary window shown below allows you to point your cursor over a green, yellow or red segment; a popup indicates the # and % of calls over devices | streams over links | calls over endpoints in the network whose quality was measured to be good, fair or poor respectively:



Click any color-coded voice quality segment to open the Calls List filtered by that voice quality score (Good, Fair or Poor).

The **Successful/Failed Streams pie chart** in the Network Summary window shown below allows you to point your cursor over a green or red segment; a popup indicates the # and % of calls over devices | streams over links | calls over endpoints in the network whose performance was measured to be successful or failed respectively:



Click any color-coded segment to open the Calls List filtered by that call performance evaluation (Successful or Failed).

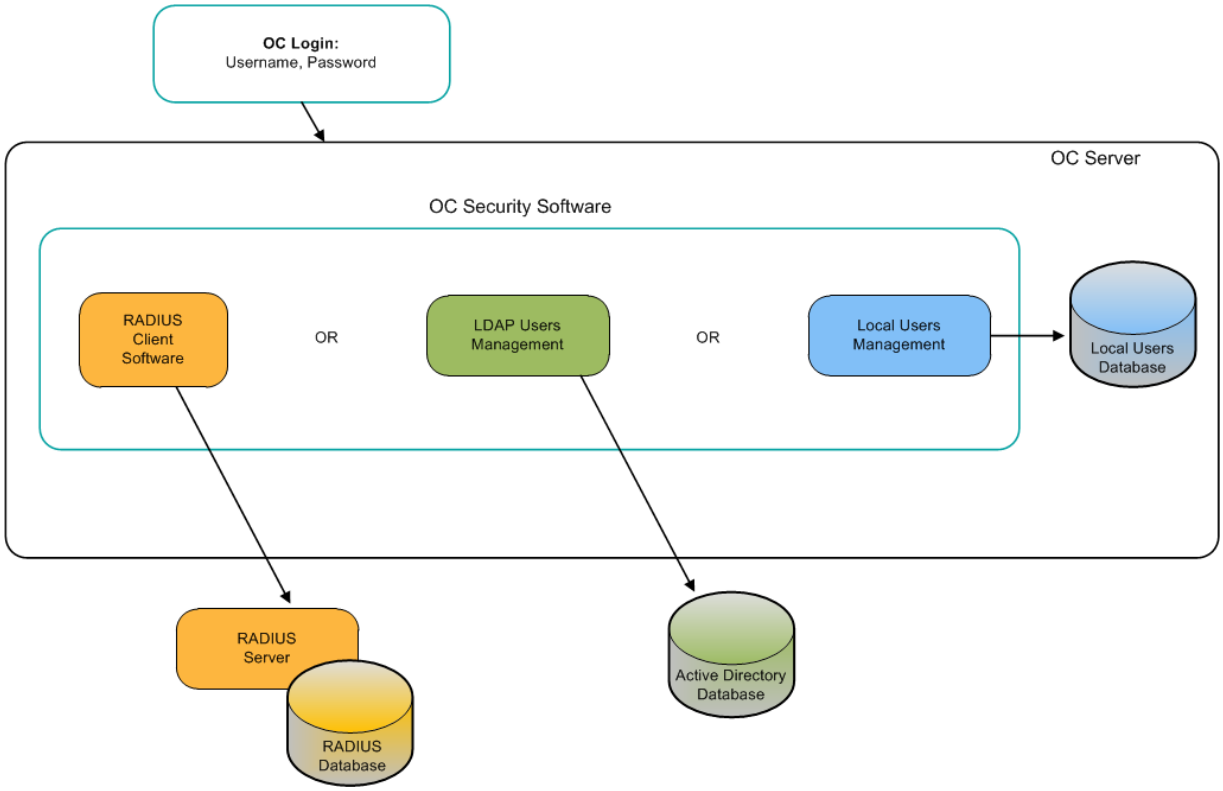
2.4 Configuring Operator Authentication

Authentication of OVOC operators can be configured in three ways:

- Centrally, using an LDAP-compliant server such as Microsoft Active Directory (AD) (see Section 2.4.1)
- Centrally, using a RADIUS server (see Section 2.4.2)
- Locally, in the OVOC (see Section 2.4.5)

The figure below shows the three different operator authentication options.

Figure 2-8: OVOC Operator Authentication Options



For operator authentication, it's *recommended* to implement a third-party LDAP or RADIUS server in the network. When attempting to log in to the OVOC, the OVOC server then verifies the login username and password with the AD server or RADIUS sever. Usernames, passwords and access-level attributes are stored externally on these platforms. The OVOC server in this case doesn't store the username and password for these users (they're not displayed in the OVOC Users List) but but verifies them with the external authentication server.

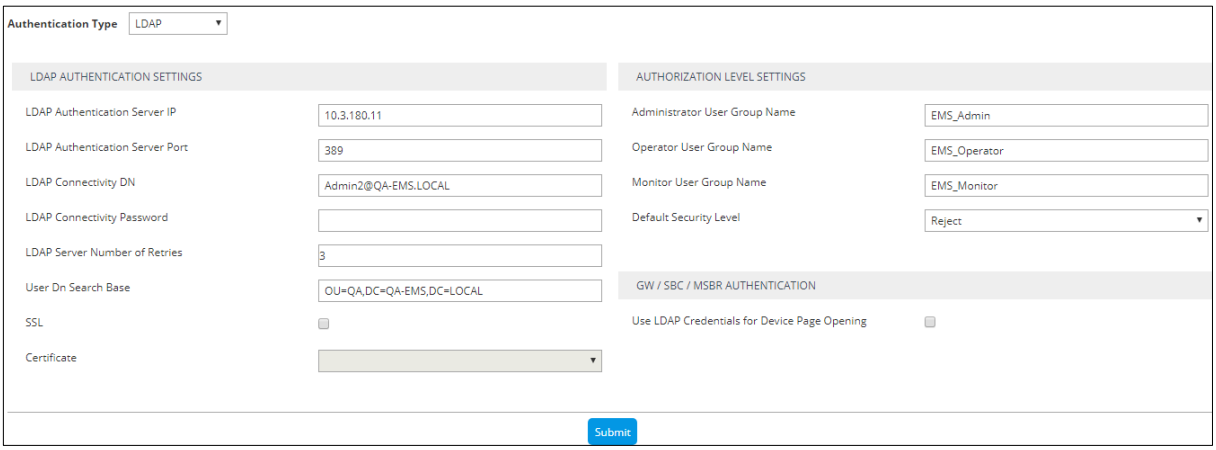
2.4.1 Configuring Operator Authentication Centrally using an LDAP Server

You can centrally configure authentication of OVOC operators using a Lightweight Directory Access Protocol (LDAP) server. When an LDAP-authenticated operator logs into the OVOC, they're assigned one of the OVOC's security levels, e.g., 'Operator'. The equivalent names for these security levels on the LDAP server are shown in Figure 2-9 below. When one of these security levels is not defined on the LDAP server, the OVOC by default allows access to the LDAP-authenticated operator with 'Operator' permissions.

➢ **To centrally configure authentication of OVOC operators using an LDAP server:**

1. In the OVOC, open the Authentication page (**System** > **Administration** > **Security** > **Authentication**).
2. From the 'Authentication Type' dropdown, select **LDAP**.

Figure 2-9: Authentication - LDAP



3. Configure the 'LDAP Authentication Server IP'.
4. Configure the 'LDAP Authentication Server Port'.
5. Configure the 'LDAP Connectivity DN' parameter as required.
6. Configure the 'LDAP Connectivity Password' as required.
7. In the 'LDAP Server Number of Retries' field, enter the number of login attempts the operator can make before they're suspended. When the number is reached, the operator is blocked. Only the 'system' operator whose security level is 'Administrator' can then unblock them. Default: 3 attempts.
8. Configure the 'User DN Search Base' as required.
9. Select the 'SSL' option to secure the connection with the LDAP server over SSL.
10. From the 'Certificate' dropdown, select the certificate file that you want to use to secure the connection with the LDAP server over SSL.
    - **Not selected** (Default). The connection with the LDAP server is non-secured.
    - **SSL With Certificate**: An HTTPS connection between the OVOC and the LDAP server is opened. The OVOC authenticates the SSL connection using a certificate. Make sure you load the SSL certificate file, required by the LDAP Active Directory platform, to the Software Manager. See Section 4.2.3.
11. [Under 'Authorization Level Settings'] In the 'Administrator User Group Name' field, enter the name of the administrator user group.
12. In the 'Operator User Group Name' field, enter the name of the operator user group.
13. In the 'Monitor User Group Name' field, enter the name of the monitor user group.
14. From the 'Default Security Level' dropdown, select: **Reject** (Default), **Amin**, **Monitor** or **Operator**. Use Table 2-5 as a reference.
15. Select the **Use LDAP Credentials for Device Page Opening** option for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to the OVOC. The AudioCodes device will then perform authentication with the LDAP server.
16. Click **Submit**.

Note: If an operator tries to log in to the LDAP server and it's unavailable, a local login to the OVOC is attempted and 'Authentication Type' is automatically switched to **OVOC** (local authentication). When the connection is re-established, the operator must manually switch back authentication mode.

2.4.2 Configuring Operator Authentication Centrally with a RADIUS Server

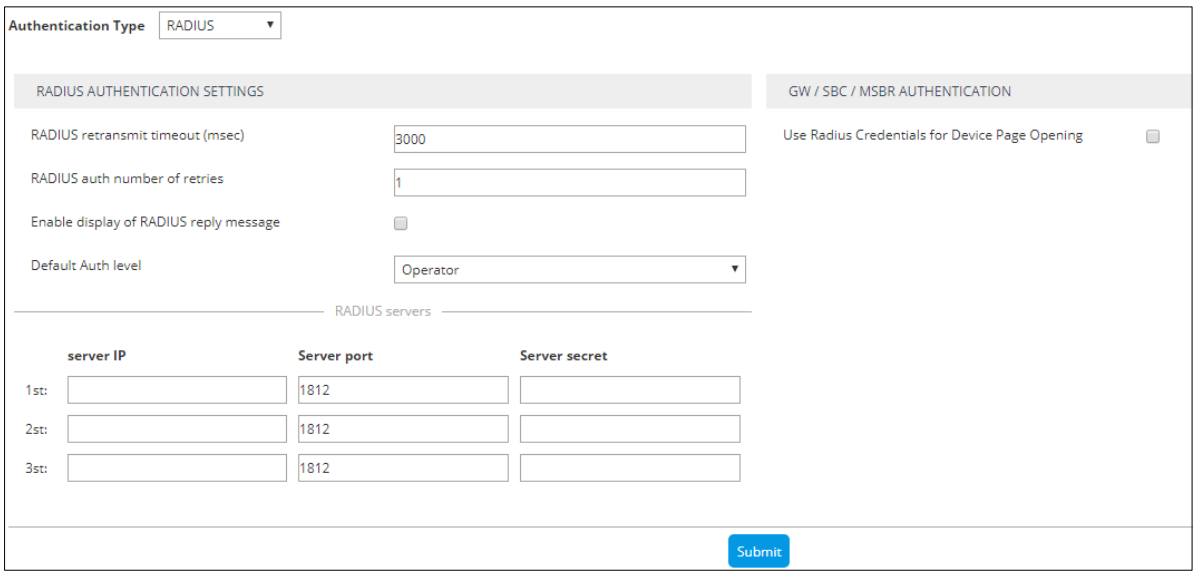
You can centrally configure authentication of OVOC operators using a RADIUS (Remote Authentication Dial-In User Service) server. If the connection to the RADIUS servers fails, the local operators database can be automatically used as a backup after a defined timeout, i.e., if the RADIUS connection fails, the user and password are replicated to the local users database so the operator can log in to the OVOC as a local user (configured by parameter 'Enable Local Authentication on Radius Timeout' and dependent on the timeout value defined in 'RADIUS Auth Retransmit Timeout (msec)').

When the RADIUS-authenticated operator logs into the OVOC, they're assigned one of the OVOC security levels - for example - 'Operator' (see Table 2-5). If it's not defined on the RADIUS server, the OVOC by default allows access for the RADIUS-authenticated operator, with 'Operator' permission.

➢ **To centrally configure authentication of OVOC operators using a RADIUS server:**

1. Open the Authentication page (**System** > **Administration** > **Security** > **Authentication**) and from the 'Authentication Type' dropdown, select **RADIUS**.

Figure 2-10: Authentication - RADIUS



2. Configure the parameters:
   - 'RADIUS retransmit timeout' (Default: 3000 milliseconds). If this timeout expires, local authentication is performed.
   - 'RADIUS auth number of retries' (Default: 1)

   Note that these parameters will be used for each RADIUS Server.
3. Select the **Enable display of RADIUS reply message** option. Default: Cleared.
4. From the 'Default Authentication Level' dropdown, select either **Operator** (default), **Amin**, **Monitor** or **Reject**. Use Table 2-5 as reference.
5. For each of the three RADIUS servers, define the server's IP address, port and secret. At least one server must be provisioned. 'Server Secret' defines the shared secret (password) for authenticating the device with the server. Must be cryptically strong. Also

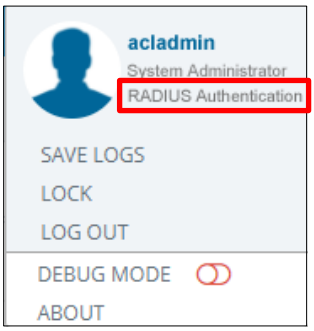
used by the server to verify authentication of RADIUS messages sent by the device (i.e., message integrity). See the device's manual for more information.

6. Select the **Use RADIUS Credentials for Device Page Opening** option for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to the OVOC. The AudioCodes device will then perform authentication with the RADIUS server.
7. Click **Submit**.

Note: If an operator tries to log in to RADIUS and it's inaccessible, a local login to the OVOC is attempted and 'Authentication Type' is automatically switched to **OVOC** (local authentication). When the connection is re-established, the operator must manually switch back authentication mode.

2.4.3 Viewing Operator Authentication in the Application Information Window

When OVOC operator authentication is performed centrally using an LDAP-compliant server or a RADIUS-compliant server, then after the LDAP-authenticated operator or RADIUS-authenticated operator logs in to the OVOC, the application information window displays the operator's authentication type.



The application information window always displays operator security level irrespective of how authentication is performed.

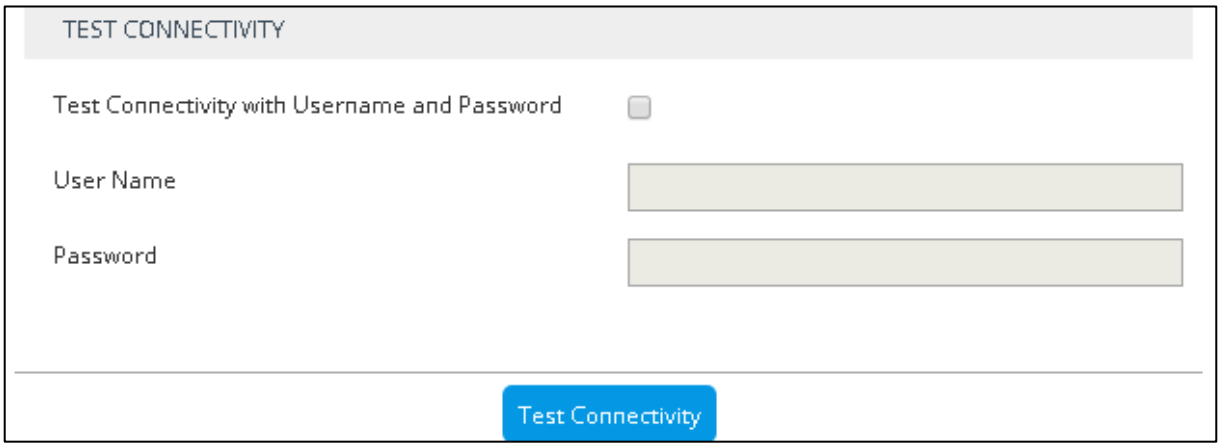
2.4.4 Testing Connectivity with the LDAP / RADIUS Server

The OVOC allows you to test the settings you configured in the LDAP/RADIUS pages described in the two sections above, to make sure your configuration is correct and that connectivity with the server has been established.

➢ **To test the settings you configured in the LDAP/RADIUS pages:**

1. In the LDAP or RADIUS authentication page, scroll down to Test Connectivity.

Figure 2-11: Test Connectivity



2. Click **Test Connectivity**; if prompted that the connection was successful, you configured the page correctly; if not, you need to check the settings you configured.
3. [Optional] To test connectivity with a specific operator authentication:
   - Select the option **Test Connectivity with Username and Password** and then enter an operator's name in the 'User Name' field and their password in the 'Password' field.
   - Click **Test Connectivity**; if the operator's credentials are recognized, you're prompted that the connection was successful.

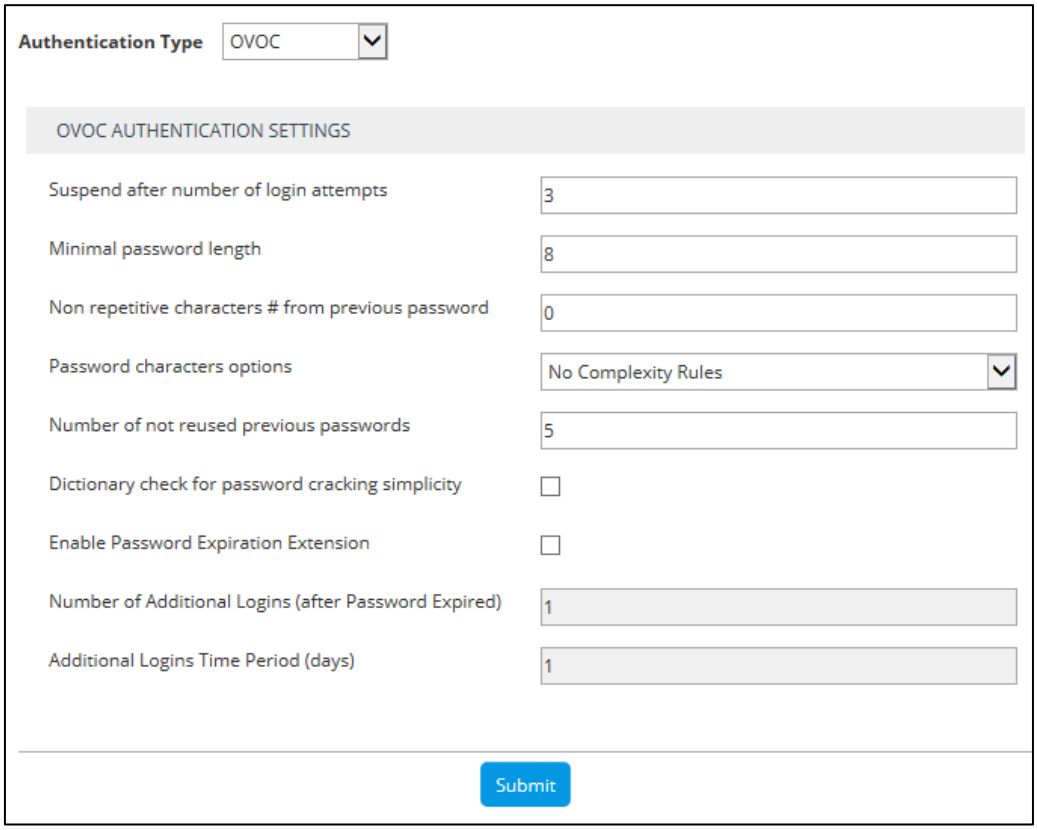
2.4.5 Configuring Operator Authentication Locally, in the OVOC

You can configure authentication of operators locally, in the OVOC. The feature allows the operator with 'Administrator' security level to control other operators' access to system resources. In this way, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexpert operators.

➢ **To locally configure authentication of operators:**

1. In the OVOC, open the Authentication page (**System** > **Administration** > **Security** > **Authentication**).
2. From the 'Authentication Type' dropdown, select **OVOC**.

Figure 2-12: Authentication – OVOC



3. Configure the authentication parameters using Table 2-4 as reference.

Table 2-4: OVOC Operator Authentication Parameters

Parameter	Description
Suspend after number of login attempts	Lets you configure the number of login attempts attempted by the operator before the OVOC application suspends them. When the number of login attempts is reached, the operator is blocked from logging into the OVOC. Only the Administrator can then unblock the suspended operator. Default: 3 attempts.
Minimal password length	Default: 8 characters. Maximum supported: 30 characters.
Non repetitive characters # from previous password	Default: 0. Maximum supported: 10 characters.
Password characters options	From the dropdown, select either: • No complexity rules are applied (default) • Use Plain or Capital letters, Digits and Special Characters • Use Plain and Capital letters, Digits and Special Characters
Number of not reused previous passwords	Default: 5. Possible values: 0-10.
Dictionary check for password cracking simplicity	Select this option for the OVOC server to perform a password weakness check on the OVOC operator's password. Default: Disabled (unselected).
Enable Password Expiration Extension	Select the option to extend the password expiration; the following two parameters are activated.
Number of Additional Logins (after Password Expired)	Defines the number of logins the operator can perform after their password expires. Range: 1-10.
Additional Logins Time Period (days)	Defines the period (in days) during which the operator can perform the number of additional logins defined with the previous parameter. Range: 1-60.

2.5 Adding an Operator

You can add an operator to the OVOC. The operator can be of type:

- 'Tenant' - or-
- 'System'

The table below shows the capabilities permitted for each OVOC operator type and security level. OVOC operators are allocated a security level of either Admin, Operator or Monitoring.

Table 2-5: Capabilities Allowed for Each Operator Type / Security Level

Operator Type	Security Level	Defining operators	Managing tenants	Managing system resources	Managing tenant resources	Monitoring system resources	Monitoring tenant resources
System	Admin	Yes, all operator types and security levels	Yes	Yes	Yes	Yes	Yes
	Operator	No	No	Yes	Yes	Yes	Yes
	Monitoring	No	No	No	No	Yes	Yes
Tenant	Admin	Yes, in their own 'tenant'	No	No	Yes, in their own 'tenant'	No	Yes
	Operator	No	No	No	Yes, in their own 'tenant'	No	Yes
	Monitoring	No	No	No	No	No	Yes

2.5.1 How Multi Tenancy Impacts Operator Capabilities

This section briefly shows how multi tenancy architecture impacts the capabilities of OVOC 'system' operators in contrast to OVOC 'tenant' operators.

Examples also show how operator security level impacts the capabilities of 'system' operators and 'tenant' operators.

The examples will help you deduce the principle. Use the table above as reference.

- A 'system' operator with a security level of 'Admin' will be permitted *every capability*.
- A 'tenant' operator with a security level of 'Monitoring' will *not be permitted any capability* except to monitor their own resources.
- In the OVOC's Software Manager:
  - A 'system' operator can add | delete files.
  - A 'tenant' operator can only *use* files.
  - A 'tenant' operator with Admin security level, however, can add | delete files *if the files only belong to that specific tenant and only devices in that tenant use them*.
- A 'system' operator with Admin security level can allocate licenses to tenants. A 'tenant' operator with Admin security level can only *distribute sessions within their own tenant,* across *that tenant's* devices, from *that tenant's* License Pool. A 'tenant' operator *cannot manage licenses for multiple tenants* like a 'system' operator with Admin security level can.
- Multi-Tenancy impacts what operators view on OVOC pages. In the Network Topology page, for example:
  - a 'tenant' operator with a Monitoring security level will only see part of the network.
  - A 'tenant' operator with Admin security level will only see network entities they are permitted to see.
  - A 'system' operator with an Admin security level will see all tenants and all devices under each tenant.

2.5.2 Adding a 'System' Operator

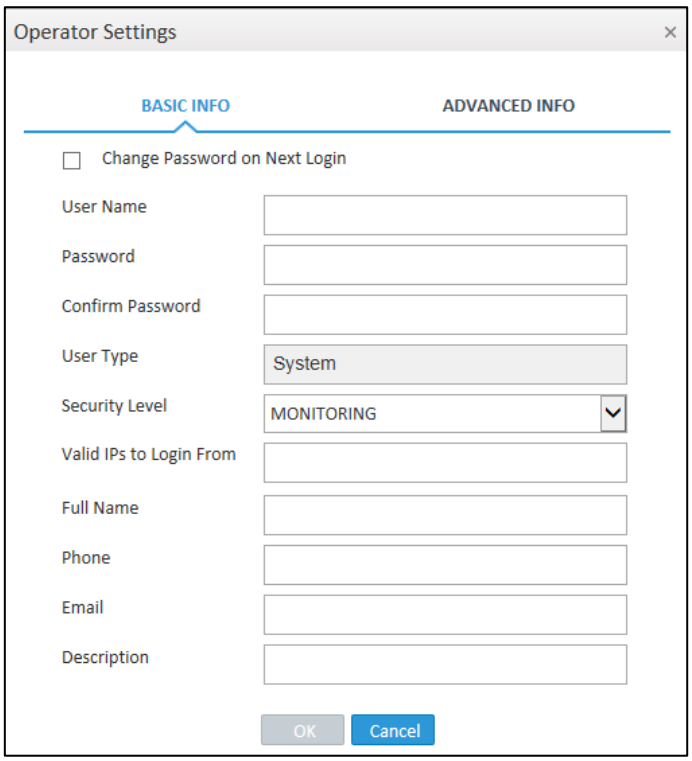
You need to add a 'system' operator to the OVOC. The 'system' operator is typically the ITSP administrator whose network features multi-tenancy architecture and whose OVOC application provides management services to multiple enterprise customers (tenants) in their network. The 'system' operator can also be an *enterprise network administrator* whose network does *not* feature multi-tenancy architecture but whose OVOC application enables management of the enterprise's *distributed offices* ('tenants').

Note: Only a 'system' operator with a security level of 'Admin' can perform tenant management operations (Add/Remove/Update).

➢ **To add a 'system' operator:**

1. In the OVOC, open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Click **Add** and then select **System** from the dropdown menu.

Figure 2-13: 'System' Operator Settings - Basic Info



3. Configure the new operator's basic information using the table below as reference. The screen displays basic operator information and security settings.

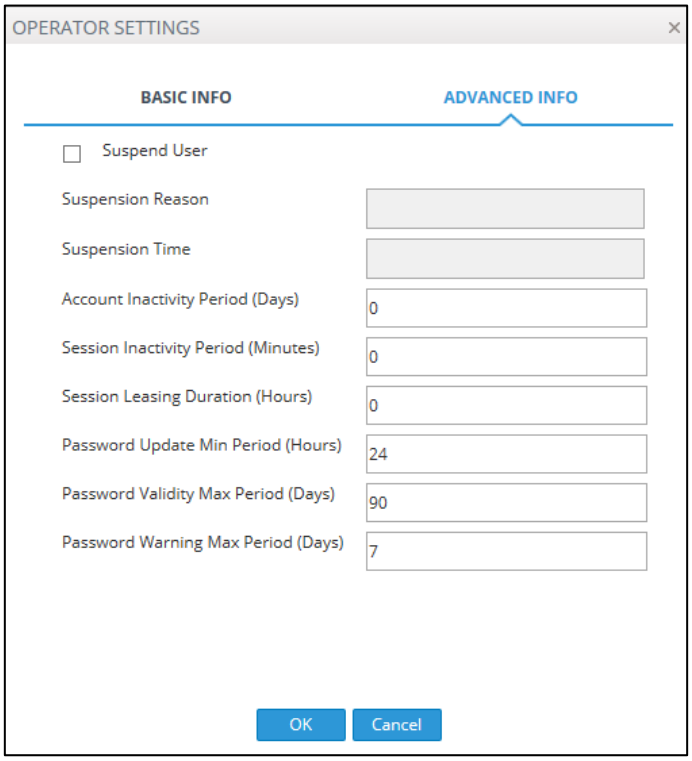
Table 2-6: 'System' Operator Settings - Basic Info

Parameter	Description
User Name	Enter the operator's name. Must be unique.
Password	Enter the operator's password.
Confirm Password	Confirm the operator's password.
User Type	[Read-only] **System** or **Tenant** depending on what you selected in step 2.

Parameter	Description
Security Level	From the dropdown select: ▪ Monitoring (lowest security level – see Table 2-5 for details) ▪ Operator (medium security level – see Table 2-5 for details) ▪ Admin (highest security level – see Table 2-5 for details)
Valid IPs to Login From	Enter IP addresses of devices from which this operator will be allowed to log in. Login from any other IP address will be disallowed.
Full Name	Enter the operator's full name. Facilitates more effective management of operators.
Phone	Enter the operator's phone number. Facilitates more effective management of operators.
Email	Enter the operator's email. Facilitates more effective management of operators.
Description	Enter any information likely to facilitate more effective management of OVOC operators.

4. Click **Advanced Info**.

Figure 2-14: 'System' Operator Settings – Advanced Info



5. Configure the new 'system' operator's advanced information using Table 2-7 below as reference. The screen displays advanced account and password settings.

Table 2-7: 'System' Operator Settings – Advanced Info

Parameter	Description
Suspend User	Select this option to suspend the 'system' operator.
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a reason explaining why the operator is suspended.
Suspension Time	[Only available when 'Suspend User' is checked] Enter the time at which the operator is suspended.
Account Inactivity Period (Days)	If the operator does not log into the OVOC for the number of days specified, their account will be suspended. Maximum: 10 days. Default: 0 (The operator can log into the OVOC at any time irrespective of how long they've been logged off; even if they haven't logged in for an excessive period of time their account will not be suspended).
Session Inactivity Period (Minutes)	Defines how long an OVOC GUI page remains accessible despite operator inactivity. If the period times out, the page locks and the operator is prompted to reenter their password to re-access it; the same page that the operator was on before the period timed out then opens. After the operator logs in to the GUI, every time they interact with it, e.g., by clicking a menu, the timer is reset. Default: 0 (the GUI is always accessible irrespective of operator inactivity).
Session Leasing Duration (Hours)	Enter the session leasing duration, in hours. If it expires, the application will close the client session / force the operator to reenter their password in order to reaccess the application. Default: 0 (the session leasing duration will never expire and the application will never close the client session).
Password Update Min Period (Hours)	Specify a period, in hours. The operator's password cannot be changed more than once within the period specified. Default: 24 hours. If 0 is specified, the password can be changed an unlimited number of times, unrestricted by period.
Password Validity Max Period (Days)	Specify a period, in days. The operator's password must be changed within this number of days after the last password change. Default: 90 days. If 0 is specified, the password can be changed an unlimited number of times, unrestricted by period, after the last password change.
Password Warning Max Period (Days)	Specify the number of days. The operator will receive a warning message this number of days before the date on which the password expires. Default: 7 days (i.e., the operator will receive a warning message a week before their password expires). If 0 is specified, the operator will receive warning messages irrespective of the date on which the password expires.

6. Click **OK**. The operator is added to the OVOC.

2.5.2.1 Editing a 'System' Operator

You can edit the details of a 'system' operator if they change.

➢ **To edit the details of a 'system' operator:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the 'system' operator whose details you need to edit and then click **Edit**; the Operator Settings screen opens as shown in Figure 2-13.
3. Edit the operator's details using Table 2-6 as reference.

2.5.2.2 Deleting a 'System' Operator

You can remove a 'system' operator from the OVOC.

➢ **To remove a 'system' operator:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the 'system' operator to remove and then click **Delete**.

2.5.2.3 Deleting Multiple Operators

You can delete multiple operators from the OVOC simultaneously.

➢ **To delete multiple 'system' operators simultaneously:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the operators to remove and then click **Delete**.

2.5.2.4 Suspending a 'System' Operator

You can suspend a 'system' operator from the OVOC.

➢ **To suspend a 'system' operator:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the 'system' operator to suspend and then click **Actions**.
3. From the dropdown, select **Suspend**; the operator is automatically logged out before suspension.

2.5.2.5 Releasing a Suspended 'System' Operator

You can release a 'system' operator who was previously suspended from the OVOC.

➢ **To release an operator who was previously suspended from the OVOC:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the suspended operator to release and then click **Actions**. Multiple operators can be selected for release from suspension.
3. From the dropdown, select **Release**.

2.5.2.6 Forcing a Password Change

You can force an operator to change their password. The feature can be used if for example you suspect information has been stolen from the enterprise.

➢ **To force a password change:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the operator whose password to change and then click **Actions**. Multiple operators can be selected.
3. From the dropdown, select **Force Password Change**.

Note: The operator is automatically prompted to change their password the next time they log in.

2.5.3 Adding a 'Tenant' Operator

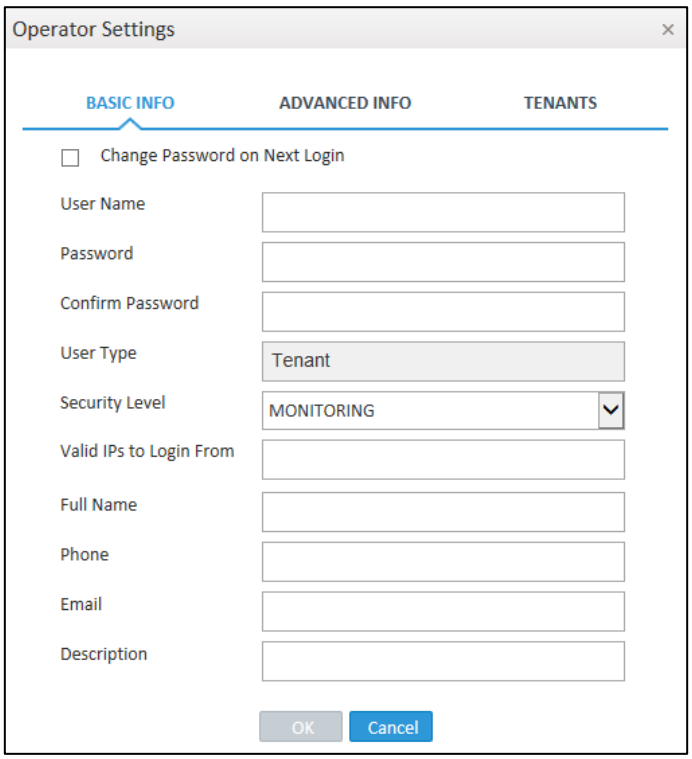
You can add a 'tenant' operator to the OVOC. A 'tenant' operator is typically an enterprise's network administrator whose network does not feature multi-tenancy architecture and whose OVOC application enables management of the enterprise's distributed offices.

Note: Only a 'system' operator with a security level of 'Admin' can perform 'tenant' management operations (Add/Remove/Update/Clone/Suspend).

➢ **To add a 'tenant' operator:**

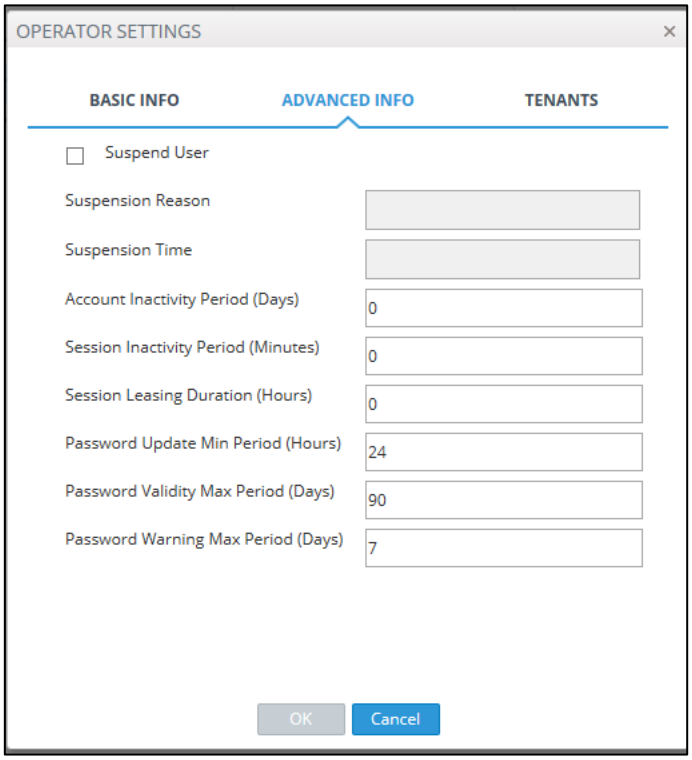
1. In the OVOC, open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Click **Add** and then select **Tenant** from the dropdown menu.

Figure 2-15: 'Tenant' Operator Settings – Basic Info



3. Configure the 'tenant' operator's basic info using Table 2-6 as reference.
4. Click **Advanced Info**.

Figure 2-16: 'Tenant' Operator Settings – Advanced Info



5. Configure the 'tenant' operator's advanced information using the table below as reference. The screen displays advanced account and password settings.

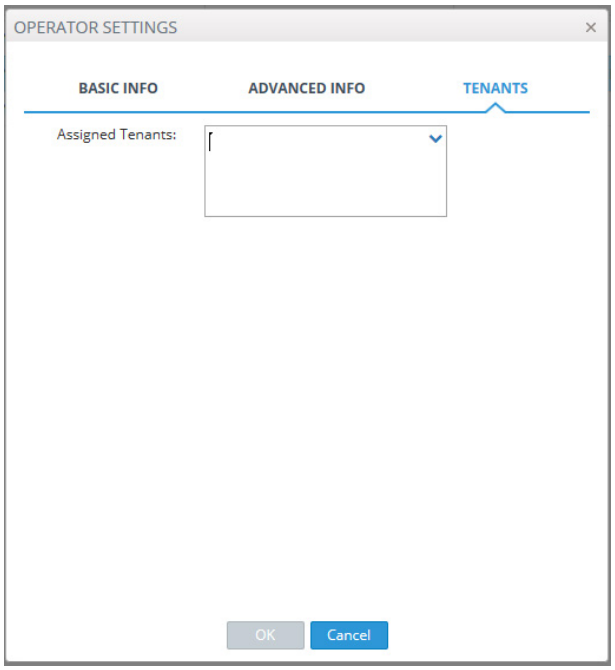
Table 2-8: 'Tenant' Operator Settings – Advanced Info

Parameter	Description
Suspend User	Select this option to suspend the 'system' operator.
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a reason explaining why the operator is being suspended.
Suspension Time	[Only available when 'Suspend User' is checked] Enter the time at which the operator is being suspended.
Account Inactivity Period (Days)	If the operator does not log into the OVOC for the number of days specified, their account will be suspended. Maximum: 10 days. Default: 0.
Session Inactivity Period (Minutes)	Enter the session inactivity period, in minutes. If it expires, the application will close the client session / force the operator to reenter their password in order to reaccess the application. Default: 0.
Session Leasing Duration (Hours)	Enter the session leasing duration, in hours. If it expires, the application will close the client session / force the operator to reenter their password in order to reaccess the application. Default: 0.
Password Update Min Period (Hours)	Specify a period, in hours. The operator's password cannot be changed more than once within the period specified. Default: 24 hours.
Password Validity Max Period (Days)	Specify a period, in days. The operator's password must be changed within this number of days after the last password change. Default: 90 days.

Parameter	Description
Password Warning Max Period (Days)	Specify the number of days. The operator will receive a warning this number of days before the date on which the password expires. Default: 7 days (i.e., the operator will receive a warning message a week before their password expires).

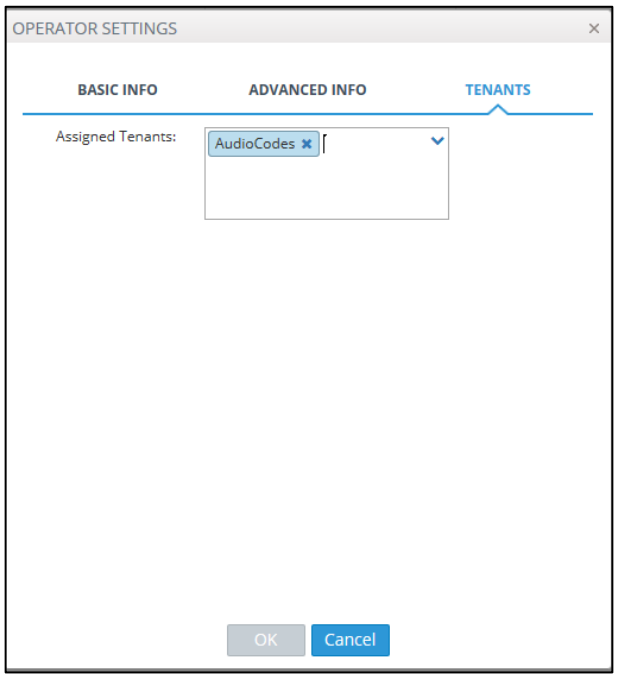
6. Click **Tenants**.

Figure 2-17: 'Tenant' Operator Settings – Tenants



7. [The screen is only available for the 'tenant' operator]. From the 'Assigned Tenant' dropdown, select a tenant for this operator from the list of tenants defined in the server. Multiple tenants can be selected.

Figure 2-18: 'Tenant' Operator Settings – Tenant Assigned



8. Click **OK**; the tenant/s is/are assigned.

2.5.3.1 Editing a 'Tenant' Operator

You can edit the details of a 'tenant' operator if they change.

➢ **To edit the details of a 'tenant' operator:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the 'tenant' operator whose details you need to edit and then click **Edit**; the Operator Settings screen opens as shown in Figure 2-13.
3. Edit the operator's details using Table 2-6 as reference.

2.5.3.2 Deleting a 'Tenant' Operator

You can remove a 'tenant' operator from the OVOC. After removal, the OVOC deletes the 'tenant' operator's entities, frees its portion of license resource, and detaches any operator attached to it.

➢ **To remove a 'tenant' operator:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the 'tenant' operator to remove and then click **Delete**.

2.5.3.3 Deleting Multiple Operators

You can delete multiple operators from the OVOC simultaneously. After deleting, the OVOC deletes the operators' entities, frees their portion of license resource, and detaches any attached operators.

➢ **To delete multiple operators simultaneously:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the operators to remove and then click **Delete**.

2.5.3.4 Suspending a 'Tenant' Operator

You can suspend a 'tenant' operator from the OVOC.

➢ **To suspend a 'tenant' operator:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the 'tenant' operator to suspend and then click **Actions**. Multiple operators can be selected for release from suspension.
3. From the dropdown, select **Suspend**; the operator is automatically logged out before suspension.

2.5.3.5 Releasing a Suspended 'Tenant' Operator

You can release a 'system' operator who was previously suspended from the OVOC.

➢ **To release an operator who was previously suspended from the OVOC:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the suspended operator to release and then click **Actions**.
3. From the dropdown, select **Release**.

2.5.3.6 Forcing a Password Change

You can force an operator to change their password. The feature can be used if for example you suspect information has been stolen from the enterprise.

➢ **To force a password change:**

1. Open the Operators page (**System** > **Administration** > **Security** > **Operators**).
2. Select the operator whose password to change and then click **Actions**. Multiple operators can be selected.
3. From the dropdown, select **Force Password Change**.

Note: The operator is automatically prompted to change their password the next time they log in.

3 Managing SBC Licenses

SBC licenses can be managed using:

- Floating License (see the next section)
- Fixed License Pool (see Section 5.3.3)
- Local license installed on the device (see the device's *User Manual*)

3.1 Using the Floating License

Managed as an AudioCodes cloud service, the Floating License feature is a network-wide license intended for customer deployments featuring multiple SBCs sharing a dynamic pool of resources. The feature simplifies network capacity planning and delivers cost benefits related to aggregated call statistics, follow-the-sun scenarios and disaster recovery setups that involve two or more data centers.

The feature allows customers to 'pay as they grow' by eliminating the need to manually purchase additional SBC licenses when capacity requirements increase. Customers initially purchase license capacity based on estimated requirements but may later experience business growth and therefore require increased session capacity. In this case, customers are billed for the additional sessions. SBCs deployed in the network are 'open' to maximum hardware capacity utilization based on predefined profiles. SBCs can alternatively be configured by operators with customized session capacity profiles. The feature applies to the following SBC call functionalities:

- SBC Sessions (# of concurrent SBC call sessions-media and signaling)
- SBC Signaling Sessions (# of concurrent SIP messages- only signaling)
- Far End Users (FEU) (# of concurrent users that can be registered on the device)
- Transcoding Sessions (# of concurrent codec types)

Note:

- The Floating License feature must first be enabled on the SBC, in the device's Web interface: **Setup** tab > **Maintenance** folder > **Floating License**. When the feature is disabled in the Web interface, the SBC is not displayed in the OVOC.
- If the Floating License is enabled, the 'local' license option will not be available.
- The Floating License cannot exceed the maximum capabilities of the SBC product for concurrent calls/sessions, due to hardware / CPU limitations.

When an SBC is configured to operate with Floating License and a connection is successfully established with the OVOC, it is connected to the OVOC's Floating License application mode.

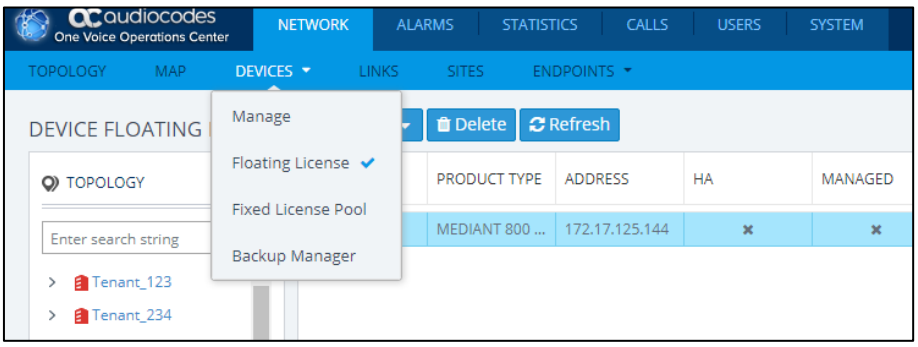
SBCs report to the OVOC every five minutes their capacity consumption for the above call functionalities. The OVOC then sends the information in usage reports to the service for all SBCs managed by OVOC for this feature. The service determines if customers exceed their purchased license limit based on this information. If a customer hasn't met the terms of payment, their license may be revoked and this action is reported to the OVOC which blocks the calling service for all managed SBCs.

If a disconnection of service occurs between the SBC and the OVOC or between the OVOC and the service, a one-month period of grace is given without affecting SBC call service.

➢ **To use the Floating License feature:**

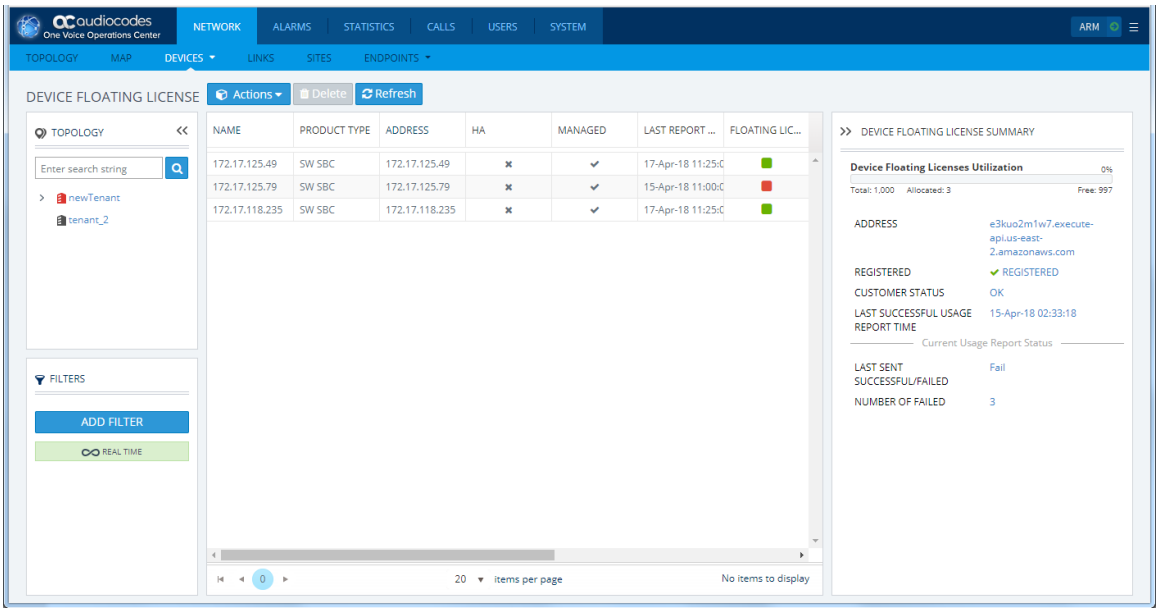
1. Open the Floating License page (**Network** > **Devices** > **Floating License**).

Figure 3-1: Floating License



1. View the SBC licenses in the Floating License page that opens.

Figure 3-2: Device Floating License Page



2. Use the table below as reference to the page's columns.

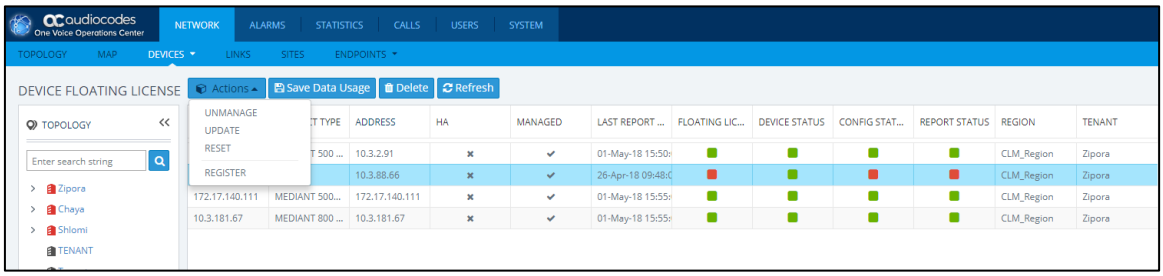
Table 3-1: Floating License Page Column Descriptions

Column	Description
Name	Indicates the name of the managed device
Product Type	Indicates the SBC device type.
Address	Indicates the IP address of the managed device.
HA	Indicates the HA status of the device.
Managed	Indicates whether the device is managed by the Floating License service server.
Last Report	Indicates the date and time that the last usage report was sent from the OVOC to the Floating License service server.
Floating License Status	Indicates the global device status reflecting the Device Status, Config Status and Report Status states.

Column	Description	
	Green	**OK:** Device Status, Config Status and Report Status are green.
	Red	**Error** or **Config Error:** Indicates Device Status, Config Status or Report Status errors (red).
	Grey	**Unmanaged:** Device is unmanaged by OVOC **Unmonitored:** Device is unmonitored by OVOC
Device Status	Green	**Connected:** Device is successfully connected to the Floating License OVOC service.
	Red	**Rejected:** Device Floating License has been revoked by the Cloud Floating License service and as a result the device's CAC is reset to 0. **Not Connected**: Device is unable to establish a connection with the Floating License OVOC service (CAC 0) **Temporarily Disconnected**: Device is temporarily disconnected from the Floating License OVOC service due to problems with the HTTPS TCP connection.
	Grey	**Unmanaged:** The device is currently not managed by the OVOC Floating License service. **Unmonitored:** The device is currently unmonitored by the OVOC Floating License service. **Not Applicable:** The device was loaded with the Floating License feature disabled. The operator must enable the feature on the SBC device and reset it.
Config Status	Green	**Success:** Indicates that the device's SNMP configuration is successfully updated.
	Red	**Failure:** Indicates that the device's SNMP configuration has not been updated successfully. For example, the Floating License REST operator's user password or username has not been updated correctly.
	Grey	**Not applicable:** Indicates that the device was added to the OVOC but is not yet managed. **Unmonitored:** Indicates that the device is currently unmonitored by OVOC.
Report Status	Green	**OK:** Indicates that a report was successfully sent from the device to the OVOC for the last reporting interval.
	Red	**Fail:** Indicates that there was a reporting failure for the last reporting interval.
	Grey	**Unmonitored:** Indicates that the device is currently unmonitored by OVOC.
Region	Indicates the device's region.	
Tenant	Indicates the device's tenant.	

3. Click the **Actions** button.

Figure 3-3: Device Floating License Page Actions



3.1.1 Performing Floating License Actions

The sections following describe the Actions you can perform in the Device Floating License page.

- Unmanage (see the section below)
- Update (see the section below)
- Reset (see Section 3.1.1.3)
- Register (see Section 3.1.1.4)

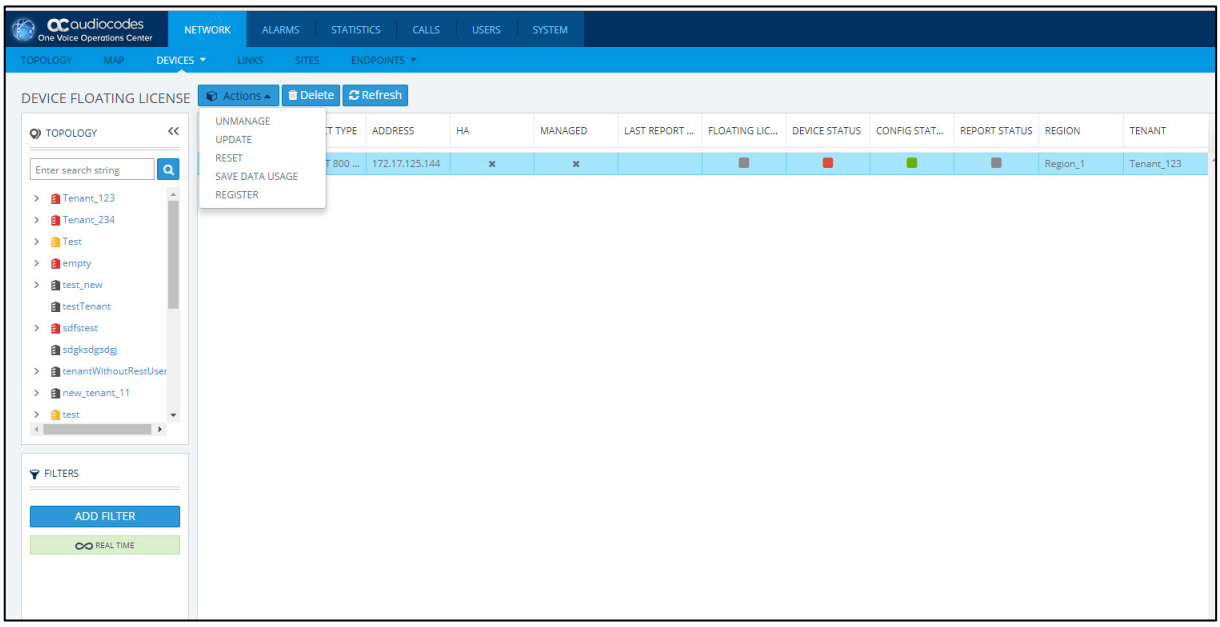
3.1.1.1 Unmanage

This Action allows the device to be unmanaged by the Floating License method.

➢ **To allow the device to be unmanaged by the Floating License method:**

- In the Device Floating License page, select the SBC to unmanage and then from the Actions dropdown menu, select **Unmanage**.

Figure 3-4: Device Floating License Page – Unmanage Action



3.1.1.2 Update

Select this menu option for the action to update the HTTPS Rest connection between the device and OVOC.

3.1.1.3 Reset

Select this menu option when:

- The SBC is connected to the OVOC and Floating License is enabled.
- One of the following SBC Web interface Floating License parameters is updated on the device:
  - Allocation Profile
  - Allocation Signaling Sessions
  - Allocation Media Sessions
  - Allocation Registered Users
- A 'Limit' value is configured for one of the above SBC Web interface Floating License parameters.
- The SBC's ini file parameter 'SoftwareDSP' is updated (only applies to Mediant 9000, Mediant SE and Mediant VE).

3.1.1.4 Register

Select this menu option for the action to perform random registration to the Floating License Cloud service for the device.

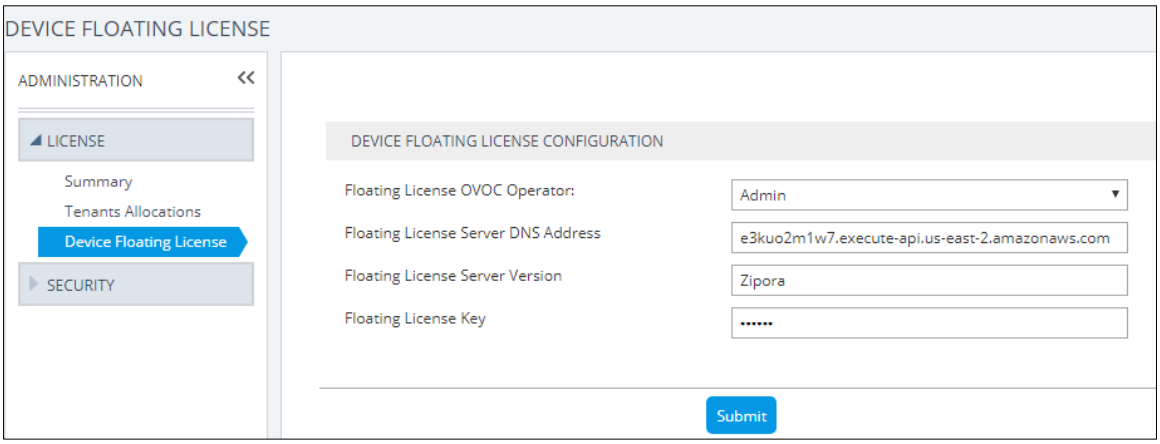
3.1.2 Configuring OVOC-Floating License Service Communications

SBCs are connected to the OVOC over SNMP. Floating License service functions are managed over TCP/HTTPS REST connections. For more information, see the *OVOC IOM* and the *OVOC Security Guidelines*.

➢ **To configure Device Floating License parameters for OVOC-CLM Communications:**

1. Open the Device Floating License page (**System** > **Administration** > **License** > **Device Floating License**).

Figure 3-5: Device Floating License - Administration Page



2. Configure the parameters using the table below as reference.

Table 3-2: Device Floating License Configuration Parameter Descriptions

Parameter	Description
Floating License OVOC Operator	Specifies the OVOC operator with REST authorization to receive and respond to REST requests from the SBC devices. This operator must

Parameter	Description
	be a System operator with either 'Admin' and 'Operator' security permissions.
Floating License Server DNS Address	Specifies the well-known DNS address of the Floating License Service platform: CLM.audiocodes.com (default)
Floating License Key	Enter the AudioCodes provided OVOC Product Key string used to authenticate the connection between the OVOC and the Floating License Service. You can view this string in the License Summary screen (**System** > **Administration** > **License** > **Summary**).

3.1.3 Viewing Floating License Summaries

The OVOC's Device Floating License page displays summary panes on the right side of the page. Panes you can view are:

- Device Floating License Utilization pane (see the section below)
- Floating License Info pane (see Section 3.1.3.2)
- Device Info pane (see Section 3.1.3.3)

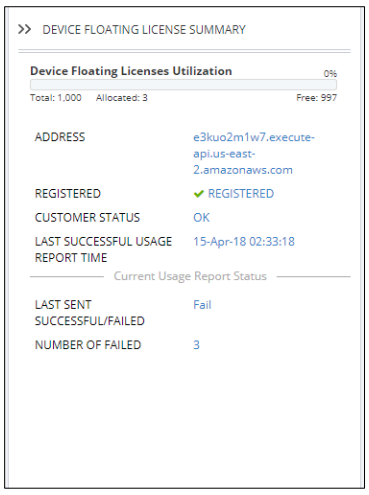
3.1.3.1 Device Floating License Utilization Pane

This pane is only displayed when no device is selected in the page.

➢ **To view the pane if a device is selected:**

1. Press the **Ctrl** key and then click the entry on the page that is selected.

Figure 3-6: Device Floating License Summary



2. Use the table below as reference to the pane.

Table 3-3: Device Floating License Utilization Pane Description

License Utilization	Description
Total/Allocated bar	Indicates the percentage of SBC devices in this OVOC installation that are managed by the Floating license. For example, if the customer has purchased licenses for 100 devices and 50 are currently managed, then this bar displays 50 allocated devices and 50 free devices.

License Utilization	Description	
Address	Indicates the IP address or FQDN of Floating License Service.	
Registered	Indicates whether OVOC is successfully registered to Floating License Service	
Customer Status	Indicates the state of the connection with the Floating License service.	
	OK	Indicates that a successful connection with the CLM has been established.
	Blocked	Customer account has been blocked by the Floating License Service.
	Unknown	Status is undetermined by the OVOC
Last Successful Usage Report Time	Indicates the time and date of the last successful usage report update that was sent from OVOC to the Floating License Cloud service.	
Last Sent Successful/ Failed	Indicates whether the last attempt to send a usage report to the Floating License Cloud service was successful.	
Number of Failed	Indicates the number of failed attempts to send usage reports to the Floating License Cloud service	

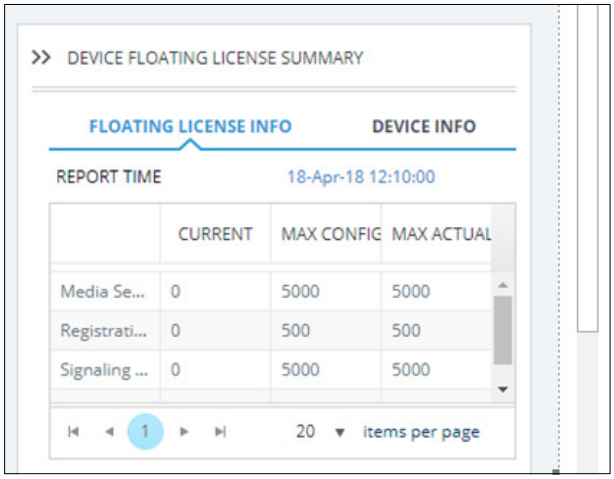
3.1.3.2 Viewing Floating License Info

The OVOC's Device Floating License page displays the 'Floating License Info' summary pane only when a device is selected in the page.

➢ **To view the pane:**

1. Select an entry on the page.

Figure 3-7: Device Floating License Summary – Floating License Info



2. Use the table below as reference to the pane's session capacities displayed.

Table 3-4: Device Floating License Summary - Floating License Info

Session Capacity	Description
Current	Indicates the currently utilized session capacity of the SBC device.

Session Capacity	Description
Maximum Configuration	Indicates the customer configured session capacity on the SBC device.
Maximum Actual	Indicates the maximum physical session capacity of the SBC device.

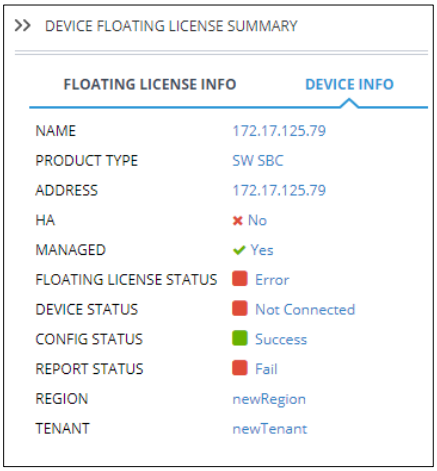
3.1.3.3 Viewing Device Info

The OVOC's Device Floating License page displays the 'Floating License Info' summary pane only when a device is selected in the page.

➢ **To view the pane:**

1. Select an entry on the page if none is selected and then in the Device Floating License Summary pane, click the **Device Info** tab.

Figure 3-8: Device Floating License Summary – Device Info



2. The pane summarizes the columns displayed in the main section of the Device Floating License page, described in Table 2-4.

3.2 Saving a Usage Data Report to your PC

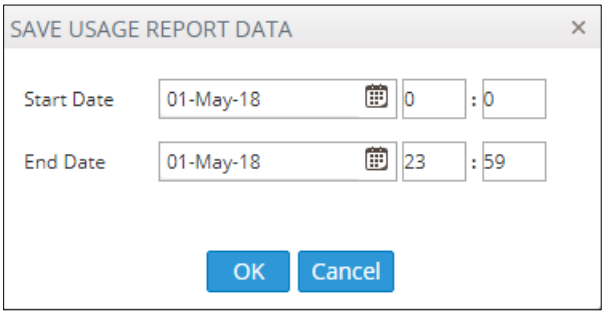
Customers who do not want usage reports sent automatically to AudioCodes but would rather export reports to a CSV file, download to a PC and then send manually to AudioCodes, can benefit from this feature.

If you do not use this feature, the SBC automatically sends usage reports every five minutes to the OVOC. Each report includes the currently configured license session values and the device's HA state.

➢ **To manually export a usage report to a CSV file:**

1. Open the Device Floating License page (**Network** > **Devices** > **Floating License**) and click **Save Data Usage**.

Figure 3-9: Save Usage Report Data

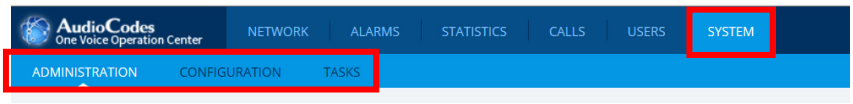


2. In the Save Usage Report Data screen shown above, define the period on which to produce the usage report data and then click **OK**.

This page is intentionally left blank.

4 Configuring Global (System) Settings

After logging in, configuring operator authentication and then adding an operator, you can configure the settings under the OVOC's System menu. These are the OVOC's *global* settings. They are *system-wide*, as opposed to *per tenant*.



Three tabs are displayed under the System menu: **Administration**, **Configuration** and **Tasks**. The table below and the sections following describe the tabs, folders and items under the System menu.

Table 4-1: System Menu

Tab	Folder	Item	Description
Administration	License	Summary	See Section 4.1.1 for details.
		Tenants Allocation	See Section 4.1.2 for details.
	Security	Authentication	Lets you configure LDAP/RADIUS authentication. See Section 2.4 for details.
		Operators	Lets you add operators to the OVOC. See Section 2.5 for details.
Configuration	Templates	SNMP Connectivity	See Section 4.2.1.1 for details.
		HTTP Connectivity	See Section 4.2.1.2 for details.
		QoE Thresholds	See Section 4.2.1.3 for details.
		QoE Status & Alarms	See Section 4.2.1.4 for details.
	Alarms		See Section 4.2.2 for details.
	File Manager	Software Manager	See Section 4.2.3 for details.
	External Applications		See Section 4.2.4 for details.
	Device Backup		See Section 4.2.5 for details.
Tasks			See Section 4.3 for details.

4.1 Administration tab

Under the **Administration** tab's **License** folder you can view a summary of your license and allocate licenses to tenants. See Section 4.1.1 for more information.

Under the **Administration** tab's **Security** folder you can define authentication and add operators. See Section 4.1.2 for more information.

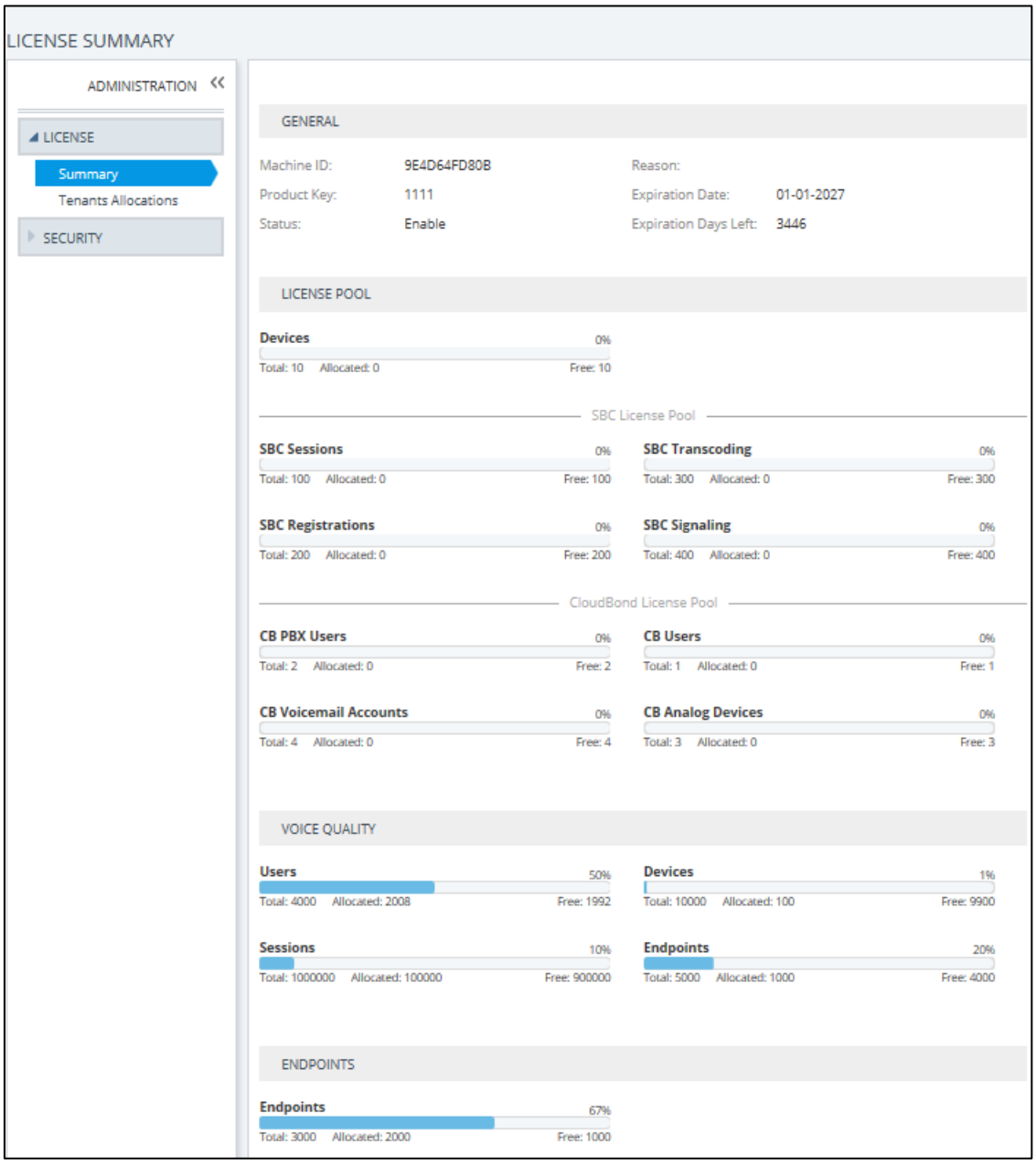
4.1.1 Viewing License Summary

The License Summary page allows you to view a summary of your license. Use the page to make sure the license you purchased provides the capabilities you ordered.

➢ **To view a summary of your license:**

1. Open the License Summary page (**System** > **Administration** > **License** folder > **Summary**).

Figure 4-1: License Summary



Note: The License Summary displays only the parameters that exist in the License Key provided by AudioCodes.

2. Make sure the license you purchased provides the capabilities you ordered.

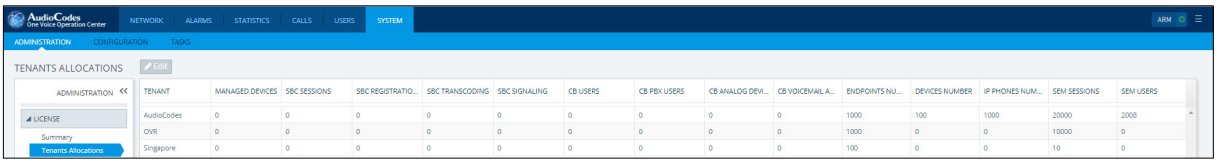
4.1.2 Allocating Licenses to Tenants

After adding tenants as described under Section 5.1, you can allocate licenses to them manually if your network administrator changed the default dynamic automatic allocation (see Section 5.6.1). The Tenants Allocation page lets you manually allocate licenses to tenants.

➢ **To allocate licenses to tenants:**

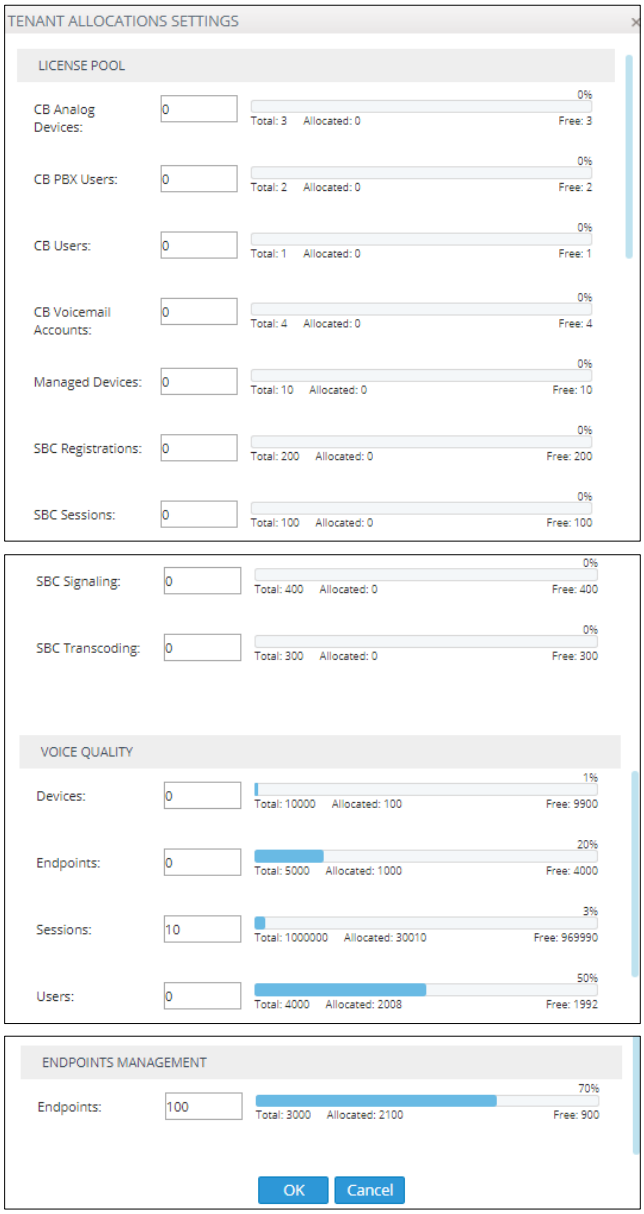
1. Open the Tenants Allocations page (**System** > **Administration** > **License** > **Tenants Allocations**).

Figure 4-2: Tenants Allocations



2. Select the tenant to whom to allocate licenses and then click **Edit**.

Figure 4-3: Tenant Allocations Settings



Note: Only parameters in the License Key provided by AudioCodes are displayed.

3. In the Tenant Allocations Settings shown in the figures above, you can allocate:
   - **Under Fixed License Pool**
     - CB analog devices
     - CB PBX users
     - CB user sessions
     - CB voicemail accounts
     - SBC Registrations (SIP endpoints that can register with the SBC)
     - SBC sessions (media and signaling)
     - SBC Signaling sessions
     - SBC Transcoding sessions
   - **Under Voice Quality**
     - Devices
     - Endpoints
     - Sessions
     - Users
   - **Under Endpoints Management**
     - Endpoints

4.1.3 Authenticating Operators

The 'Security' folder's **Authentication** item lets you configure LDAP and RADIUS authentication. See Section 2.4 for detailed information.

The 'Security' folder's **Operators** item lets you add OVOC operators. See under Section 2.5 for detailed information.

4.2 Configuration tab

The 'Configuration' tab lets you:

- configure global system templates (see Section 4.2.1)
- configure alarms settings (see Section 4.2.2)
- add software and auxiliary files (see Section 4.2.3)
- access external applications (ARM) (see Section 4.2.4)
- configure device backup (see Section)

4.2.1 Configuring Templates

The Templates folder allows you to configure the following global, system-wide templates to facilitate more effective network management:

- SNMP Connectivity (see Section 4.2.1.1)
- HTTP Connectivity (see Section 4.2.1.2)
- QoE Thresholds (see Section 4.2.1.3)
- QoE Status & Alarms (see Section 4.2.1.4)

4.2.1.1 SNMP Connectivity

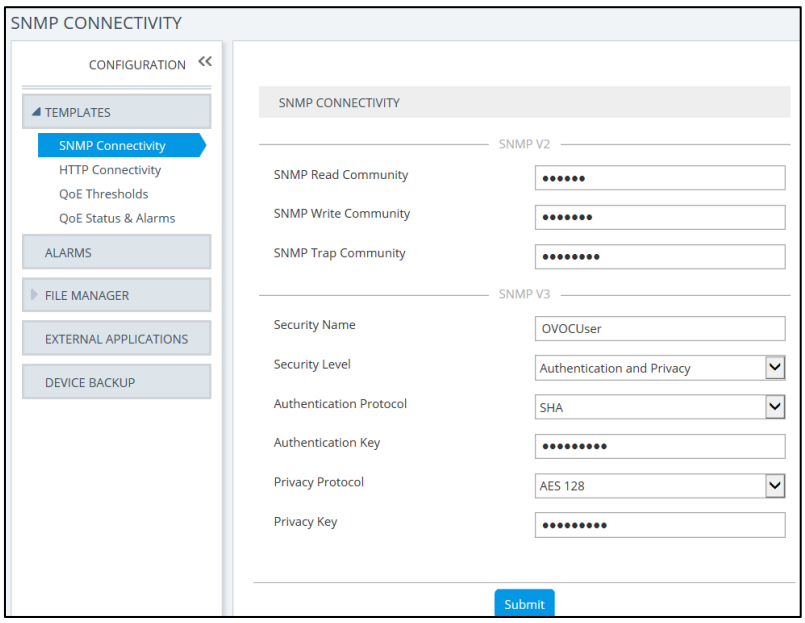
This template lets you configure an SNMP connectivity template whose parameter values can then be applied system-wide (globally). The template facilitates more effective network

management. SNMP/HTTP templates are the default profile values for each defined tenant. The tenant SNMP/HTTP profiles are used as default for the devices under them.

➢ To configure an SNMP Connectivity template:

1. Open the SNMP Connectivity screen (**System** > **Configuration** > **Templates** > **SNMP Connectivity**).

Figure 4-4: SNMP Connectivity Template



2. Use the table below as a reference to the parameters in the figure above.

Table 4-2: SNMP Connectivity Template

Parameter	Description
SNMP v2	
SNMP Read Community	Enter an encrypted SNMP read community string. The default value for the SNMP read community string is 'public'.
SNMP Write Community	Enter an encrypted SNMP write community string. The default value for the SNMP write community string is 'private'.
SNMP Trap Community	Enter the Trap Community string to be received as part of the Notification message.
SNMP v3	
Security Name	Enter a name for SNMP v3. Example: OVOC User.
Security Level	From the dropdown, select either: • **Authentication and Privacy** (default) • **No Security** • **Authentication**
Authentication Protocol	From the dropdown, select either: • **SHA** (default) • **MDS** • **No Protocol**
Authentication Key	Enter an Authentication Key. Default: 123456789.

Parameter	Description
Privacy Protocol	From the dropdown, select either: • **AES 128** (default) • **None** • **DES** • **DES 3** • **AES 192** • **AES 256**
Privacy Key	Enter a Privacy Key. Default: 123456789.

3. Click **Submit**.

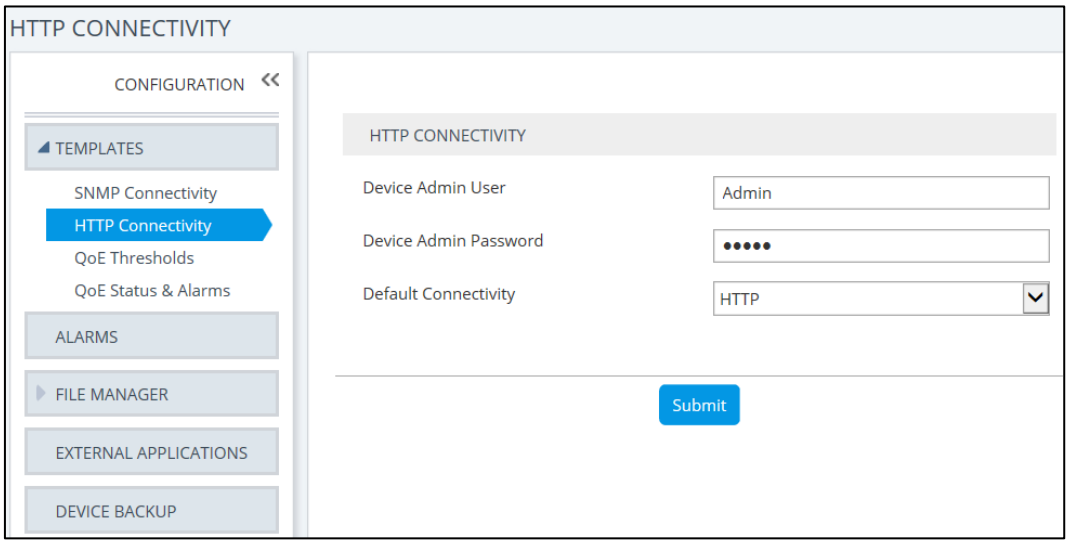
4.2.1.2 HTTP Connectivity

This option lets you configure an HTTP connectivity template whose parameter values can then be applied system-wide (globally) when adding multiple AudioCodes devices, for example. The template facilitates more effective network management for OVOC operators.

➢ **To configure an HTTP Connectivity template:**

1. Open the HTTP Connectivity screen (**System** > **Configuration** > **Templates** > **HTTP Connectivity**).

Figure 4-5: HTTP Connectivity Template



2. Use the table below as a reference to the parameters in the figure above.

Table 4-3: HTTP Connectivity Template

Parameter	Description
Device Admin User	Enter the device Web server user name. Example: **Admin**. Password - "Admin".
Device Admin Password	Enter the Web server password. Example: **Admin**.
Default Connectivity	From the dropdown, select either: • **HTTP** (default) • **HTTPS**

3. Click **Submit**.

4.2.1.3 QoE Thresholds

QoE Thresholds determine *global* (*system-wide*) voice quality thresholds templates.

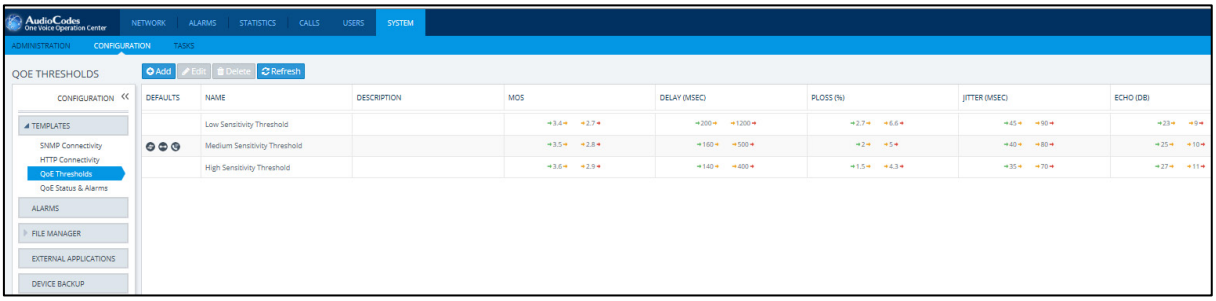
[For information on how to configure QoE Thresholds profiles *per tenant*, see Section 8.3]

Three QoE Thresholds templates (Low | Medium | High Sensitivity) for the voice quality metrics of MOS, Delay, Packet Loss, Echo and Jitter are accessed in the page. In the page, you can add, edit or delete a voice quality thresholds template.

➢ **To access the global QoE thresholds templates:**

1. From the System menu, open the QoE Thresholds page (**System** > **Configuration** > **Templates** > **QoE Thresholds**).

Figure 4-6: QoE Thresholds Templates



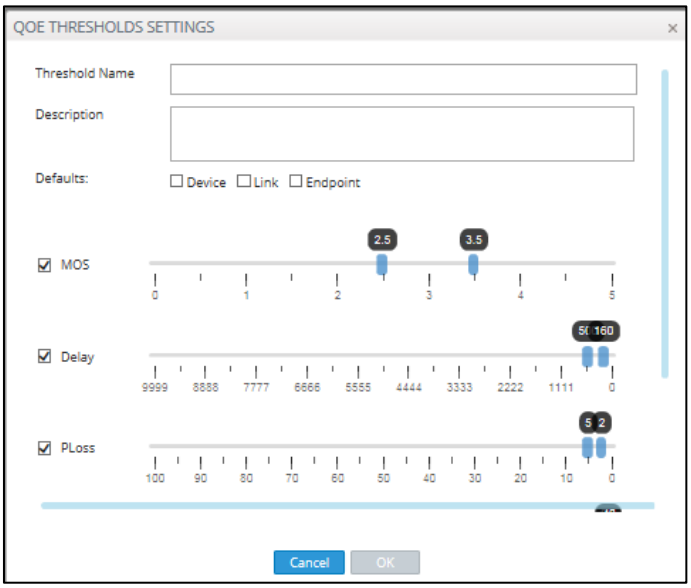
In the page, you can see three *global* (system-wide) QoE thresholds templates displayed. Each consists of threshold values set for the voice quality metrics of MOS, Delay, Packet Loss, Echo and Jitter, for each call quality category of 'Poor', 'Fair' and 'Good'.
Use the table below as reference to the figure above.

Table 4-4: QoE Thresholds Templates

Template	Description
Low Sensitivity Threshold	Threshold values representing recommended data for the 'Low' sensitivity level.
Medium Sensitivity Threshold	Threshold values representing recommended data for the 'Medium' sensitivity level.
High Sensitivity Threshold	Threshold values representing recommended data for the 'High' sensitivity level.

2. Select a template and then click **Edit**.

Figure 4-7: QoE Thresholds Settings



3. Provide an intuitive name for the profile. As a reference, use the names of the three QoE Threshold Templates displayed in Figure 4-6.
4. Enter a description of the profile to facilitate effective intuitive management later.
5. Select the **Device** option to set the profile as devices default.
6. Select the **Links** option to set the profile as links default.
7. Select the **Endpoints** option to set the profile as endpoints default.
8. By default, **All** metrics are included in the profile. To *exclude* a metric, clear its check box. To define the MOS metric, for example, click the bar or drag the markers. Each bar unit increments or decreases the threshold by **0.1 (MOS, Packet Loss)**, or by **1 (Delay, Jitter, Echo)**.
9. Do the same for the other metrics thresholds.
10. Click **OK**; the profile is displayed in the QoE Thresholds screen.

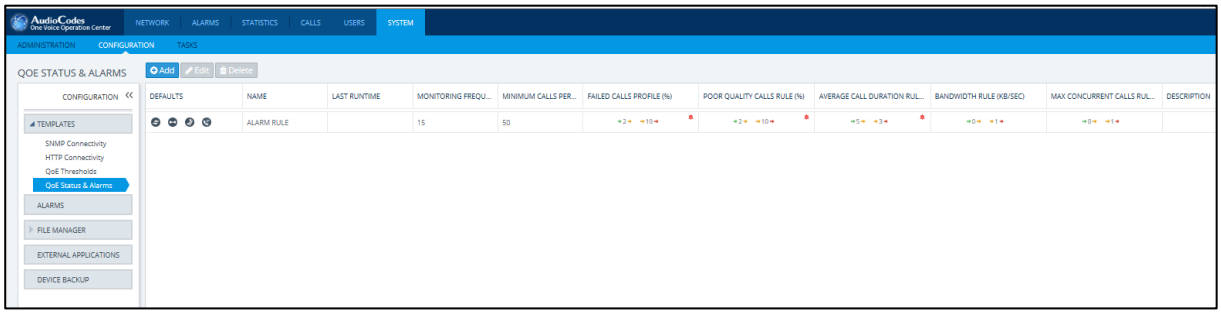
4.2.1.4 QoE Status and Alarms

The QoE Status and Alarms page determines the *global* (*system-wide*) QoE status of devices, sites, links and endpoints. The page provides a centralized view of global QoE alarms and statuses. For information on managing QoE Status *per tenant*, see Section 8.4.

➢ **To view the global QoE status:**

1. From under the System menu, open the QoE Status and Alarms page (**System** > **Configuration** > **Templates** > **QoE Status & Alarms**).

Figure 4-8: QoE Status and Alarms



2. Use Table 4-5 below as reference to the figure above.

Table 4-5: QoE Status and Alarms

Page Indications	Description
Defaults	= displayed when the alarm rule applies to devices = displayed when the alarm rule applies to links = displayed when the alarm rule applies to sites = displayed when the alarm rule applies to IP phones
Name	Indicates the name of the alarm rule.
Last Runtime	Indicates the last time the alarm rule was activated.
Monitoring Frequency Min	Indicates at least how often monitoring is performed. Default: 15
Minimum Calls per Entity to Analyze	Indicates the minimum number of calls to analyze, per entity. Default: 50
Failed Calls (%)	**x** **y** indicates that green changes to orange ('Major' severity) when the **x** percentage of failed calls is exceeded and orange changes to red ('Critical' severity) when the **y** percentage of failed calls is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Section 8.4.1).
Poor Quality Calls (%)	**x** **y** indicates that green changes to orange ('Major' severity) when the **x** percentage of poor quality calls is exceeded and orange changes to red ('Critical' severity) when the **y** percentage of of poor quality calls is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Section 8.4.1).
Average Call Duration (seconds)	**x** **y** indicates that green changes to orange ('Major' severity) when **x** seconds call duration is exceeded and orange changes to red ('Critical' severity) when **y** seconds call duration is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Section 8.4.1).
Bandwidth Rule (Kbps)	**x** **y** indicates that green changes to orange ('Major' severity) when **x** bandwidth is exceeded and orange changes to red ('Critical' severity) when **y** bandwidth is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Section 8.4.1).
Maximum Concurrent Calls (#)	**x** **y** indicates that green changes to orange ('Major' severity) when **x** concurrent calls is exceeded and orange changes to red ('Critical' severity) when **y** concurrent calls is exceeded. indicates alarm issued – displayed if the **Generate Alarm** option is selected in the Alarm Rule Details screen (see Section 8.4.1).

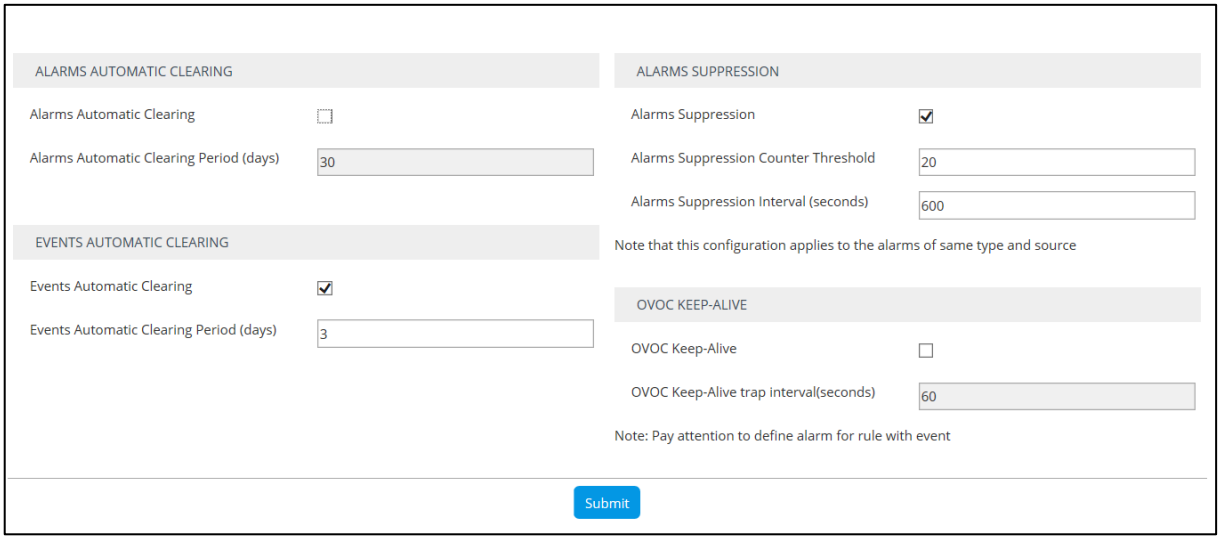
4.2.2 Configuring Alarms Settings

The Alarms screen allows you to configure how alarms and events are displayed in the Alarms pages.

➢ **To configure alarm settings:**

1. Open the Alarms page (**System** > **Configuration** > **Alarms**).

Figure 4-9: Alarms Settings



2. Configure the alarms settings using the table below as reference.

Table 4-6: Alarms Settings

Setting	Description
Alarms Automatic Clearing	Select this option to clear all devices listed in the Alarms page of all active alarms when the system starts up (cold start event): Critical, Major, Minor, Warning or Info. Use this setting to prevent historical, dated alarms from cluttering the Alarms page.
Alarms Automatic Clearing Period (Days)	[Only relevant if the 'Alarms Automatic Clearing' option is selected] Clears old alarms after a defined period of days even though a Clear alarm to stop displaying very old active alarms has not been received from the device.
Events Automatic Clearing	Select this option for device events (events originating from the device) to be automatically cleared from the Alarms page when the system starts up (cold start event). Device events originating in the OVOC, e.g., adding a gateway, are not cleared when the device is reset. The OVOC consequently employs a mechanism to automatically clear these events from the Alarms page. The feature prevents historical, dated events from cluttering the Alarms page.
Events Automatic Clearing Period (days)	Events are by default cleared every three days. You can change the default to suit your requirements.
Alarms Suppression	Select this option for an 'Alarm Suppression' alarm to be generated when the OVOC server identifies that the number of alarms of the same type and from the same source, generated in a time period, is greater than the number defined in the threshold. At

Setting	Description
	this point, these alarms are not added to the database and are not forwarded to configured destinations.
Alarms Suppression Counter Threshold	[Only applicable if 'Alarms Suppression' is selected] Lets you configure a counter threshold (Default: 10 alarms) and interval (Default: 10 seconds). For example, if 10 alarms are generated from 'Board#1/EthernetLink#2 in 10 seconds, then alarms from this source are suppressed and the 'Suppression' alarm is generated. This alarm is cleared if in the subsequent 10 second interval, less than 10 alarms are sent from this source. At this point, updating the OVOC database is resumed (the last received alarm is updated).
Alarms Suppression Interval (seconds)	During the time the suppression alarm is active, the OVOC server updates the database with a single alarm (with updated unique ID) database every minute, until the alarm is cleared.
OVOC Keep-Alive	Select this option for the OVOC to generate SNMP Keep-alive traps to 3rd-party applications, such as a Syslog server. This trap can be sent to either the SNMP, Syslog or Mail server destination. You can send the Keep-Alive trap to the target destination, according to an existing configured forwarding destination rule.
OVOC Keep-Alive trap interval (seconds)	[Only applicable if 'OVOC Keep-Alive' is selected] Determines how frequently the trap is sent from the OVOC to the configured destination. Default: Every 60 seconds. You can configure a different interval to suit your requirements.

4.2.3 Adding Configuration Files to the OVOC's Software Manager

You can add ini files, cmp firmware files, cli files, conf files and auxiliary files to the OVOC's Software Manager in order to load them to devices.

The Software Manager page lets operators view, add or remove files. Filters facilitate quick and easy access to device-specific files.

After defining a device in the OVOC, the OVOC connects to it and automatically determines its version. Each *new* version, fix or software update provided to customers must be added to the Software Manager, to enable upgrading device software.

Files per network device include:

- SBC configuration files (ini, cli, conf)
- SBC software files (cmp)
- MP-202 software files (rms/rmt)
- IP phone firmware files
- IP phone configuration files (templates)
- MP-202 configuration files (conf)
- Auxiliary files (prt, cpt, etc.)

Use Table 4-7 below as a reference with respect to which operator type is permitted to perform what file management.

Table 4-7: OVOC Software File Management per Operator Type

Operator Type	Permitted to Perform this File Management
System (except operators with 'Monitoring' security level)	• Add any global file that will not be assigned to any specific tenant. These files will be visible to both 'tenant' and 'system' operator types. • Add a file and assign it to a specific tenant. These files will be visible to both 'tenant' and 'system' operator types. • Download any file visible by the tenant (Added by 'tenant' and 'system' operator types) to any device in the tenant. • Remove any file added by 'tenant' and 'system' operator types.
Tenant (except operators with 'Monitoring' security level)	• Add any file. This file will be assigned only to the tenant. These files will be visible to both 'tenant' and 'system' operator types. • Download any file visible by the tenant to the devices in the tenant. • Remove any file added by a 'tenant' operator type.

Note:

- Only one SBC software file (cmp) with the same version for a specific product type can be added to a tenant.
- Software files cannot be shared between tenants (except global). If an operator assigned to multiple tenants adds a file, it can be downloaded only on devices in a specific tenant and not to all tenants.

4.2.3.1 Adding the ini File

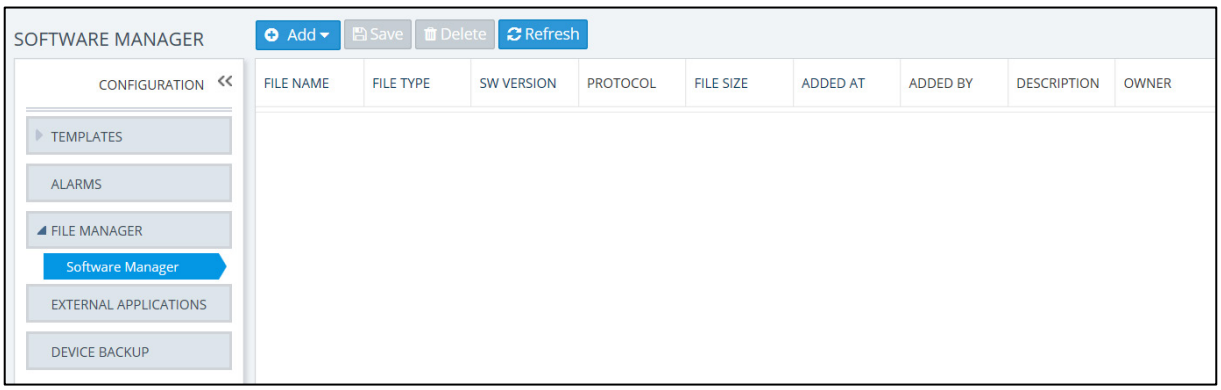
You can add the ini file to the OVOC's Software Manager in order to perform initial configuration of device parameters which cannot be configured after defining the device in the OVOC. When loading the ini file to the device, operators can choose either:

- Full Configuration ini file download – with validation and apply (recommended)
- Full Configuration ini file download – without validation and apply (for software upgrade)
- Incremental ini file download (the previous configuration remains)

➢ **To add the ini file to the OVOC:**

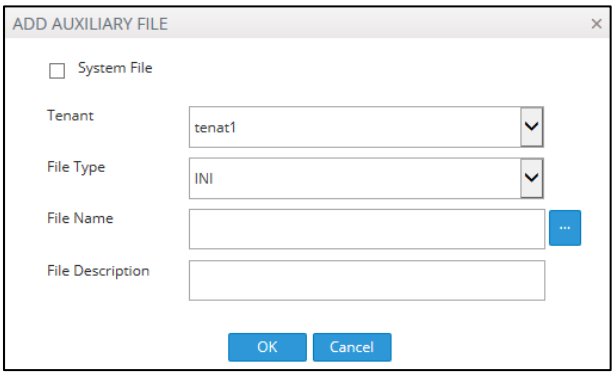
1. Open the Software Manager page (**System** > **Configuration** > **File Manager** > **Software Manager**).

Figure 4-10: Software Manager



2. Click **Add** and select **Add Auxiliary File** from the menu dropdown.

Figure 4-11: Add Auxiliary File – ini File



3. From the 'Tenant' dropdown, select the tenant under which the ini file will be added.
4. From the 'File Type' dropdown, select **INI** (default) if it isn't selected already.
5. Next to the 'File Name' field, click **…** and browse to the ini file's location.
6. Enter a description of the file in the 'File Description' pane for intuitive future file management, and then click **OK**; the ini file is added to the Software Manager.

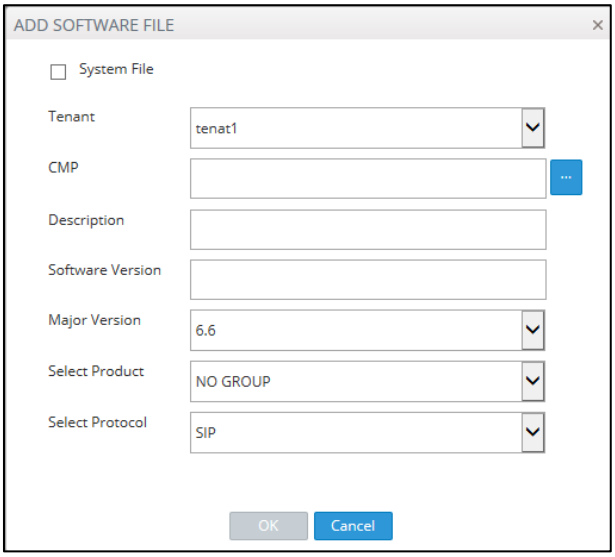
4.2.3.2 Adding a cmp File

You can add a firmware (cmp) file to the OVOC to later load to the device. With the exception of the MP-20x media gateways, the cmp files are the devices' main software firmware image files. You can add a cmp file to the OVOC in order (for example) to change the software version.

➢ **To add a cmp file to the OVOC:**

1. Open the OVOC's Software Manager page (**System** > **Configuration** > **File Manager** > **Software Manager**) (see Figure 4-10).
2. Click **Add** and select **Add Software File** from the dropdown menu.

Figure 4-12: Add Software File



3. From the 'Tenant' dropdown, select the tenant under which the cmp file will be added.
4. Next to the 'CMP' field, click **…** and browse to the cmp file's location.
5. Enter a description of the file in the 'File Description' pane for intuitive future file management.
6. In the 'Software Version' field, enter the version of the software file. If left undefined, the

field will be automatically defined after adding the cmp or rmt/rms file.

7. From the 'Major Version' dropdown, select the device version (Default: 6.6).
8. From the 'Select Product' dropdown list, select the relevant product corresponding to the cmp or rmt/rms file.
9. From the 'Select Protocol' dropdown, select the protocol. Default: SIP. MGCP and MEGACO are also available.
10. Click **OK**; the cmp file is added to the Software Manager.

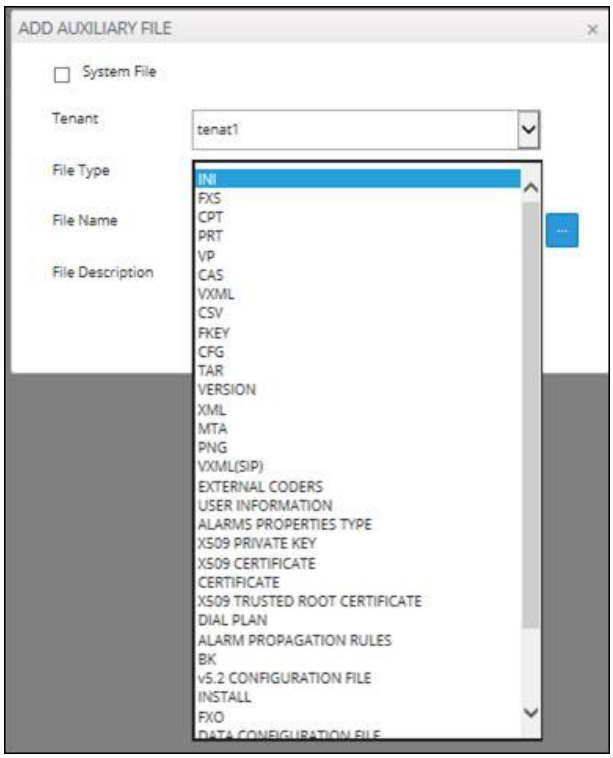
4.2.3.3 Adding Auxiliary Files

Besides the ini file, you can add auxiliary files to the OVOC's Software Manager.

➢ **To add an auxiliary file to the OVOC's Software Manager:**

1. Open the OVOC's Software Manager page (**System** > **Configuration** > **File Manager** > **Software Manager**) (see Figure 4-10).
2. Click **Add** and select **Add Auxiliary File** from the dropdown menu. See the figure below.
3. From the 'Tenant' dropdown, select the tenant under which to add the auxiliary file.
4. From the 'File Type' dropdown list, select the auxiliary file to be added.

Figure 4-13: Add Auxiliary File



Note:

- See the device's *User's Manual* for more information about device-related files.
- The CERTIFICATE file secures the following connections:
  - √ Active Directory server (domain controller)
  - √ MSSQL Front End server
  - √ LDAP User Authentication
- The X.509 PRIVATE KEY, X.509 CERTIFICATE and X.509 TRUSTED ROOT CERTIFICATE files are AudioCodes certificate files that secure the connection between OVOC and the devices.
  - √ The X.509 files are for all the security files, including LDAP.

These files may be default AudioCodes certificate files or files generated by an external CA. For more information about certification implementation, see the *One Voice Operations Center Security Guidelines*.

5. Enter a description of the file in the 'File Description' pane for intuitive future file management.
6. Next to the 'File Name' field, click **…** and browse to the file's location.
7. Enter a description of the file in the 'File Description' pane for intuitive future file management, and then click **OK**; the file is added to the Software Manager.

4.2.4 Enabling Connecting Directly to External Applications

The External Applications page enables directly connecting to other telephony network management tools, AudioCodes' tools as well as other vendors'.

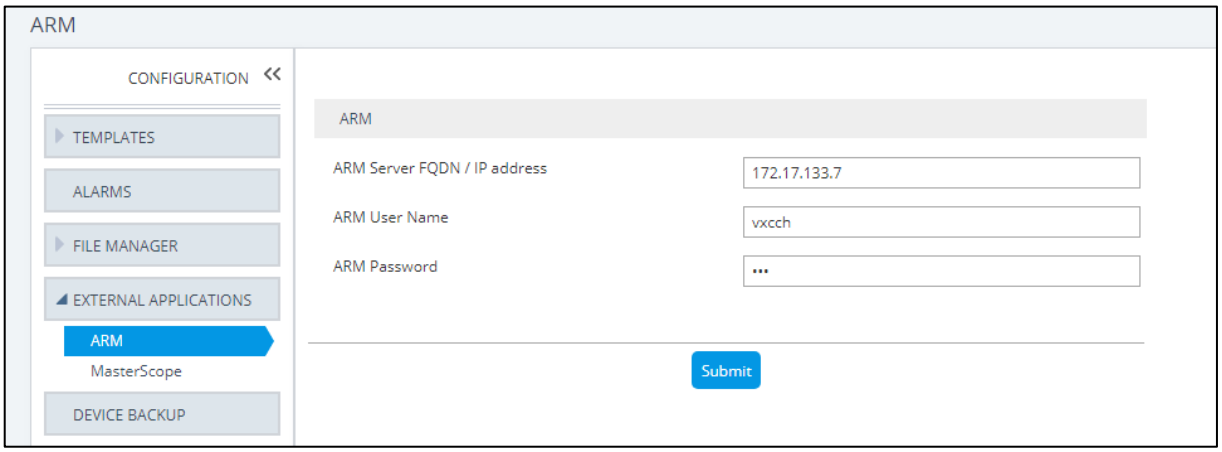
4.2.4.1 ARM

The External Applications page enables connecting directly to the ARM (AudioCodes Routing Manager) in order to manage calls routing over the network. In this page, operators (Admin *and* Operator types) configure this connection, a.k.a. Single Sign On (SSO), to the ARM. An **ARM** link is then displayed on all OVOC pages, visible to all operator types.

➢ **To enable connecting directly to the ARM:**

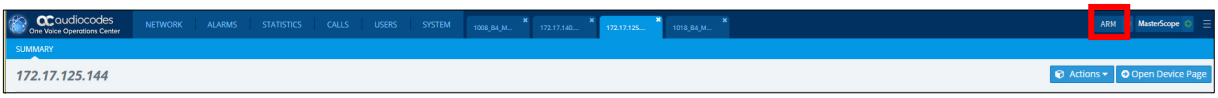
1. Open the External Applications page (**System** > **Configuration** > **External Applications**) as shown in the figure below, and then click the **ARM** option.

Figure 4-14: External Applications - ARM



2. In the field 'ARM Server IP', enter the IP address of the ARM server to connect to.
3. [Optionally] Enter the 'ARM User Name' and 'ARM Password' and click **Submit**.

Figure 4-15: Link for Single Sign On to the ARM



4. In any OVOC screen, click the **ARM** button now displayed in the upper right corner as shown in the figure above; the ARM main screen opens in a new browser tab. Note that this Single Sign On feature applies only to ARM versions that support it.

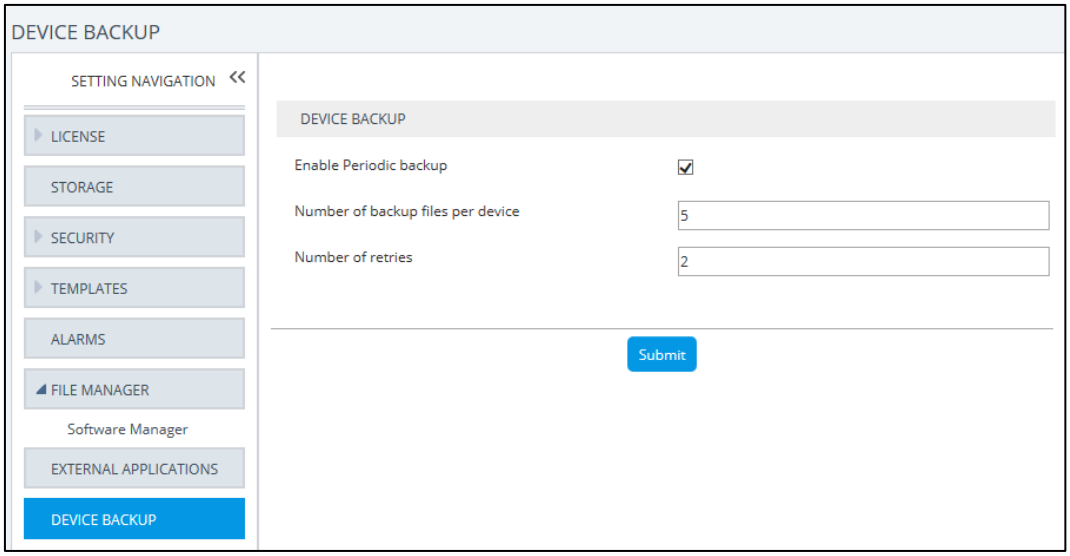
4.2.5 Enabling Automatic Device Backup Periodically

The OVOC can be configured to automatically (daily) back up device configurations (ini, conf or cli script files) according to the OVOC server application's time. The files are saved on the OVOC server. They can be accessed and transferred using SSH and SFTP. The backup files are managed by the Backup Manager.

➢ **To configure automatic device configuration backup:**

1. Open the Device Backup page (**System** > **Configuration** > **Device Backup**).

Figure 4-16: Device Backup



2. Select the 'Enable Periodic backup' option.
   - When enabled, backup is automatically performed daily; all device configuration files (ini, conf and cli) are backed up to the Backup Manager from all devices.
   - When disabled, you can perform manual backup after making changes to a device's configuration (see Section 5.3.4 for information about manually backing up a device's configuration).
3. Configure 'Number of backup files per device' to determine the number of latest backup files to be stored for each managed device. Default: 5.
4. In the 'Number of retries' field, configure the number of retries to be made each connection attempt to the device. Default: 2.
5. Click **Submit**.

4.3 Tasks tab

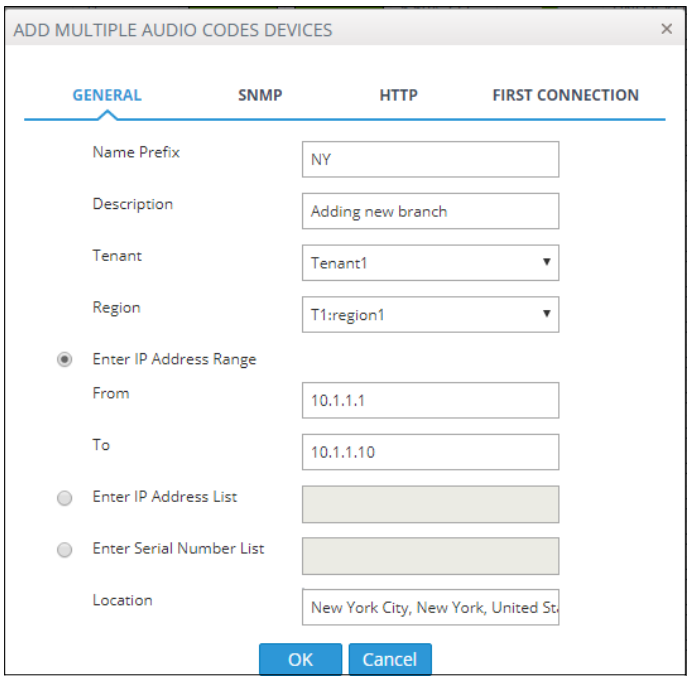
The Tasks page displays asynchronous actions performed by operators, currently under execution. Tasks that are *in progress* are displayed irrespective of how long it takes for them to complete. The OVOC continues to display them 20 minutes after they're completed. They are then removed from the page.

Note: If the operator is not a 'system' operator, *only tasks performed by that operator* are displayed in the Tasks page.

4.3.1 Displaying the Status of Tasks Currently Under Execution

Figure 4-17 shows the configuration of adding multiple AudioCodes devices to the OVOC. OVOC supports many types of multiple tasks. Adding multiple devices, described below, is just one example. As you can see in the figure, the operator is adding ten AudioCodes devices whose IP addresses range from 10.1.1.1 to 10.1.1.10, under the region US.

Figure 4-17: Task - Add Multiple AudioCodes Devices



[Optional] In the 'Location' field, enter the first letters in the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.

After clicking **OK**, the operator is prompted to go to the Tasks page to assess task status:

Figure 4-18: Prompt to go to Tasks Page to Assess Status

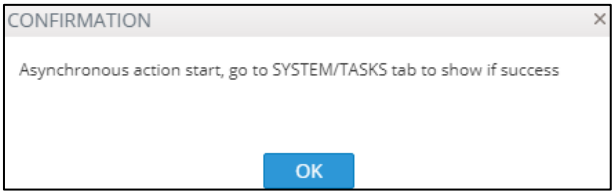
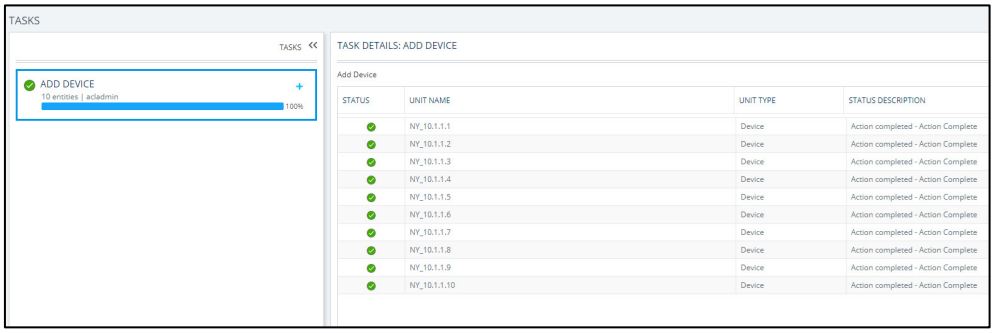


Figure 4-19: Tasks Page Showing Task Status - Adding Multiple AudioCodes Devices



The page helps this operator determine if all ten AudioCodes devices where added successfully, or, if the task isn't complete yet, what percentage is complete and what percentage remains to be completed.

5 Defining your Network Topology

This section covers how to add a network and network entities.

Note: Before you can connect a device to the OVOC you need to:

- Note the server machine's ID and then download the license activation form from AudioCodes' website's 'Services and Support' page: http://www.audiocodes.com/services-and-support .
- Obtain your OVOC license, save it on your PC, and then load it to the server. For detailed information on loading the license to the server, see the *One Voice Operations Center IOM Manual*. You can view the license details in the EMS Server Manager License screen.
- Enable the device's Feature Key.

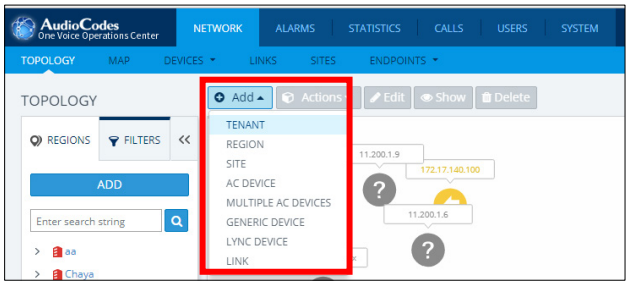
5.1 Adding a Tenant

Note: See Section 1.4 for details on multi-tenancy vs. non multi-tenancy architecture.

➢ **To add a tenant:**

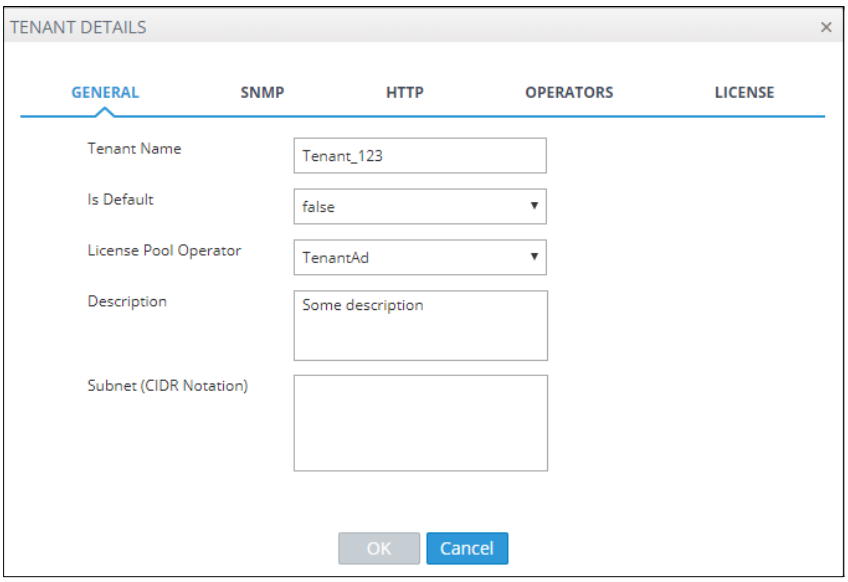
1. In the Network page, click **Add**.

Figure 5-1: Add Tenant



2. Select **Tenant**.

Figure 5-2: Tenant Details - General



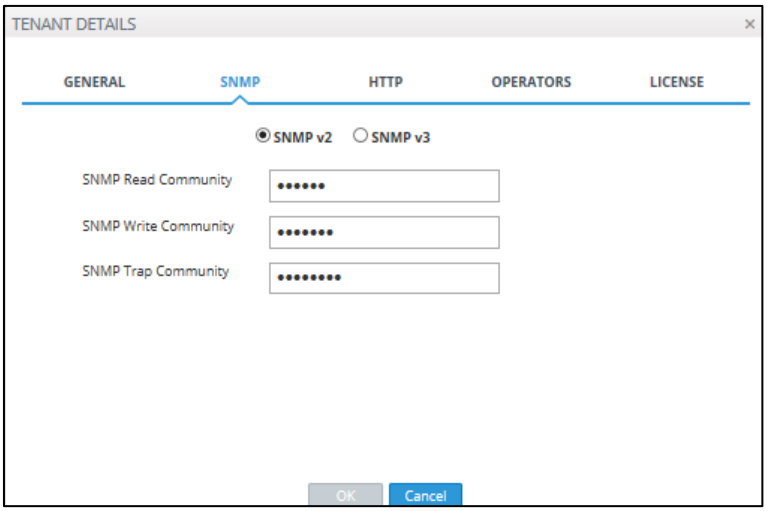
3. Use the table below as reference when configuring the tenant's General parameters.

Table 5-1: Tenant Details - General

Parameter	Description
Tenant Name	Enter an intuitive name to facilitate effective management later.
Is Default	Defines the default tenant. Only one tenant can be the default. The default is used for devices/endpoints auto-detection.
License Pool Operator	This dropdown list shows all the 'tenant' operators with Admin privileges assigned to this tenant. To manage the Fixed License Pool, it is mandatory to select one of these 'tenant' operators from the dropdown (see also under Section 5.3.3). After selecting a 'tenant' operator, the association cannot be removed (see also under Section 2.5.3) and they're automatically displayed under the **Operators** tab (see below).
Description	Enter a tenant description to facilitate effective management later.
Subnet Mask	Enter the tenant's subnet mask. Must be in prefix format x.x.x.x/y. For example: 255.255.0.0/16. For any *region* under the tenant, subnet mask is not mandatory, but if it is configured, its subnet mask must be within the tenant's, for example, 255.255.0.0/1.

4. Click **OK** and then click **SNMP**.

Figure 5-3: Tenant Details – SNMP v2



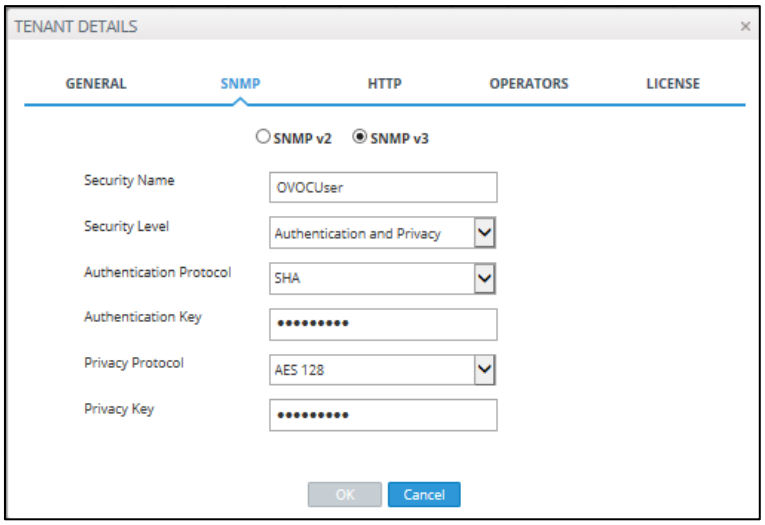
5. Use the table below as reference when configuring the SNMP v2 parameters.

Table 5-2: Tenant Details – SNMP v2

Parameter	Description
SNMP Read Community	Enter an encrypted SNMP read community string. The default value for the SNMP read community string is taken from the SNMP main template.
SNMP Write Community	Enter an encrypted SNMP write community string. The default value for the SNMP write community string is taken from the SNMP main template.
SNMP Trap Community	Enter the Trap Community string to be received as part of the Notification message. The default value for the SNMP trap community string is taken from the SNMP main template.

6. Select the **SNMP v3** option.

Figure 5-4: Tenant Details – SNMP v3



7. Use the table below as reference when configuring the SNMP v3 parameters.

Table 5-3: Tenant Details – SNMP v3

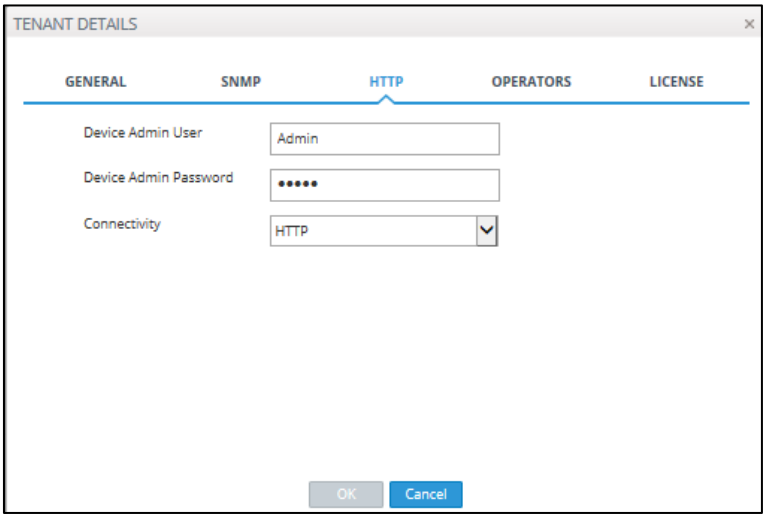
Parameter	Description
Security Name	Enter a name for SNMP v3. Example: OVOC User.
Security Level	From the dropdown, select either: • **Authentication and Privacy** (default) • **No Security** • **Authentication**
Authentication Protocol	From the dropdown, select either: • **SHA** (default) • **MDS** • **No Protocol**
Authentication Key	Enter an Authentication Key. The default is taken from main SNMP template.
Privacy Protocol	From the dropdown, select either: • **AES 128** (default) • **None** • **DES** • **DES 3** • **AES 192** • **AES 256** The default is taken from main SNMP template.
Privacy Key	Enter a Privacy Key. The default is taken from main SNMP template.

8. Click **OK** and then click **HTTP**.

Note to users of CloudBond 365 and CCE Appliance:

SNMPv2/SNMPv3 account credentials are not automatically configured so you must always manually configure them in the EMS Settings screen in the Web interface (see the *CloudBond 365 Administration and Maintenance Manual* and the *Mediant Appliance for Microsoft Skype for Business CCE Administrator's Guide).*

Figure 5-5: Tenant Details - HTTP



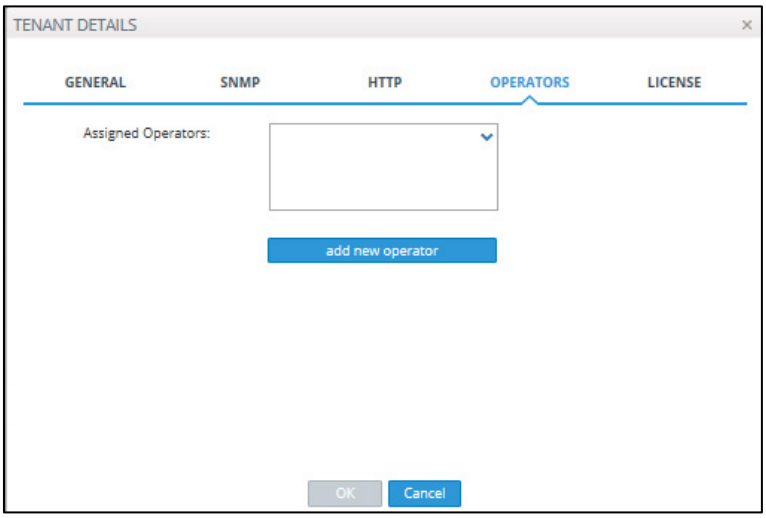
9. Use Table 5-4 below as reference when configuring the HTTP parameters.

Table 5-4: Tenant Details - HTTP

Parameter	Description
Device Admin User	Enter the device Web server user name. Example: **Admin**. Password - "Admin". The default is taken from the main HTTP template.
Device Admin Password	Enter the Web server password. Example: **Admin**. The default is taken from the main HTTP template.
Connectivity	From the dropdown, select either: • **HTTP** (default) • **HTTPS** The default is taken from main SNMP template.

10. Click **OK** and then click **Operators**.

Figure 5-6: Tenant Details – Operators



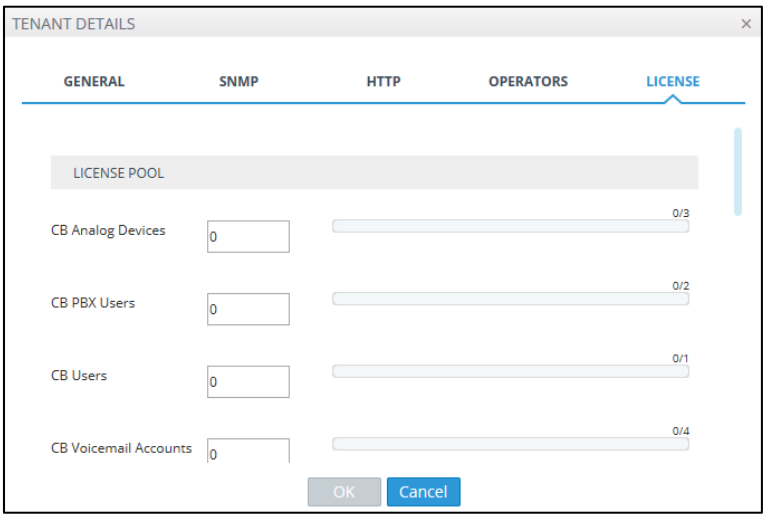
11. Use the table below as reference when configuring the Operators parameters.

Table 5-5: Tenant Details - Operators

Parameter	Description
Assigned Operators	Select an operator from the list of operators. Only operators configured as 'tenant' operators are displayed. The list will be empty if no such operator has been configured, in which case you can click the **Add new operator** button described below. The parameter lets you assign the operator – or operators – to the tenant. See under Section 2.5.3 for more information about configuring 'tenant' operators.
Add new operator	Click to button; the 'Operator Settings' screen opens for 'tenant' type operators. For detailed information, see under Section 2.5.3.

12. Click **OK** and then click **License**.

Figure 5-7: Tenant Details - License



13. Use the table below as reference when configuring the License parameters.

Table 5-6: Tenant Details – License

License Pool	Description
Devices	Enter the total number of devices that can be managed by this tenant's License Pool, i.e., CloudBond 365 devices, SBC devices, gateway devices and MSBR devices allowed by your license. The parameter only defines systems. It does not include phones.
SBC Registrations	Enter the number of SIP endpoints that can register with the SBCs allowed by your license.
SBC Sessions	Enter the number of concurrent call sessions supported by the SBCs in your deployment.
SBC Signaling	Enter the number of SBC signaling sessions supported by the SBCs in your deployment.
SBC Transcoding	Enter the number of SBC transcoding sessions supported by the SBCs in your deployment.
CB Analog Devices	Support pending. Currently unsupported.
CB PBX Users	Support pending. Currently unsupported.
CB Users	Enter the number of CloudBond 365 users per tenant. Divide the total number of CloudBond 365 users allowed by your license, by the number of tenants in your deployment. If you purchased a license for 1000 CloudBond 365 users and you have four tenants in your deployment, 250 users can be allocated to each tenant. You cannot exceed the total number of CloudBond 365 users covered by your license. It's your decision how to distribute them over tenants.
CB Voicemail Accounts	Support pending. Currently unsupported.
Voice Quality	
Devices	Enter the number of SBCs, gateways and MSBRs that can be monitored in this tenant.
Endpoints	Enter the number of endpoints that can be monitored in this tenant.
Sessions	Enter the number of concurrent call sessions the SBCs deployed in this tenant.
Users	Enter the number of users supported by the SBC/s deployed in this tenant.
Endpoints Management	
Endpoints	Enter the number of endpoints the IP Phone Manager Pro application supports for this tenant.

14. Click **OK**; the new tenant is added.

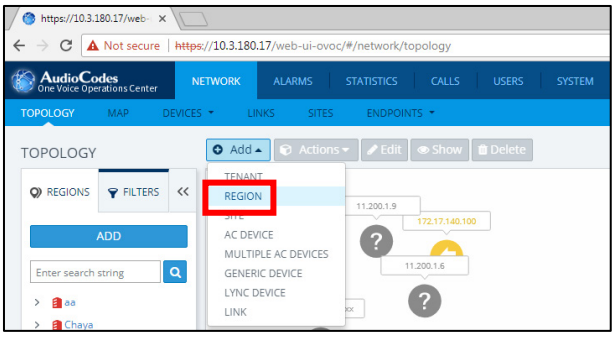
5.2 Adding a Region

ITSPs or enterprises manage devices in regions. A region typically represents a geographical area for the ITSP or the enterprise. Devices are added to the OVOC under a tenant, after defining one.

➢ **To add a region:**

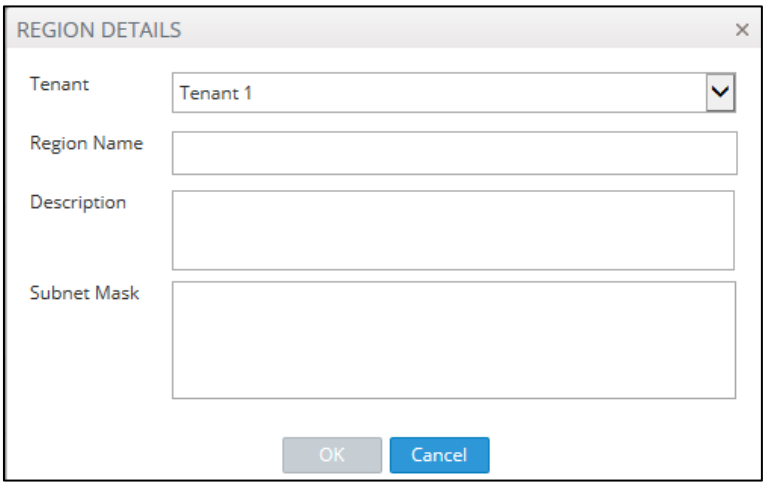
15. Open the Network Topology page (**Network** > **Topology**).
16. Click **Add** and select Region.

Figure 5-8: Add Region



The Region Details screen opens:

Figure 5-9: Region Details



17. From the 'Tenant' dropdown, select a tenant that you configured - shown in the previous section.
18. Define the region's name and type in a description to facilitate operator-friendly management later.
19. [Optional] Enter a subnet mask for the region. If a tenant's subnet mask is 255.255.10.10/16, then the subnet mask of a region under it – if configured – must be *within* that subnet mask, for example: 255.255.10.10/1.
20. Click the now-activated **OK** button; the region is added to the OVOC.

5.3 Adding Devices

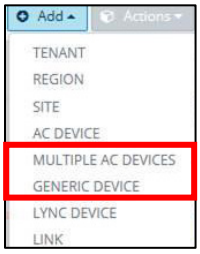
This section shows how to add devices.

- For automatic provisioning, make sure you prepare the device's ini and .cmp firmware files in the Software Manager. See Section 4.2.3 for detailed information.
- Note down the device's SNMPv2 or SNMPv3 credentials. You'll need them when configuring SNMP settings to connect the device and the OVOC.
- Auto Detect occurs when a device detects the OVOC but the OVOC does not detect the device. The device reports to the OVOC with an event. The OVOC takes information from the event and automatically connects the device.

➢ **To add the device/s:**

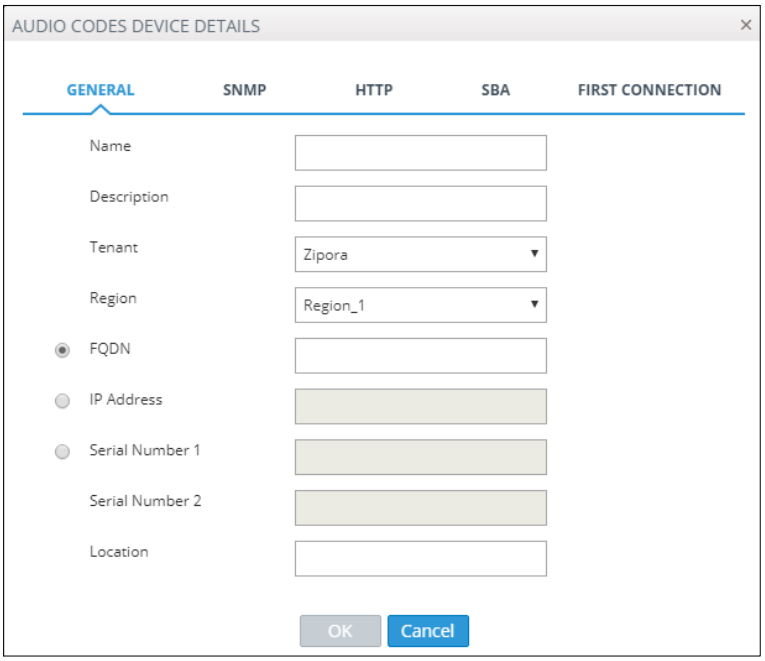
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select **AC Device** or **Multiple AC Devices**.

Figure 5-10: AC Device | Multiple AC Devices



The Device Details screen opens under the **General** tab:

Figure 5-11: Device Details – General – FQDN



3. Define an intuitive device name to facilitate operator-friendly management later. Do not use underscores in the name.
4. Provide a description of the device to facilitate operator-friendly management later.
5. From the 'Tenant' dropdown, select a tenant that you configured as shown under Section 5.1.
6. Select the region under which the device is located.
7. Define the device by selecting one of these three options (refer to the figures above):

- Select and enter the device's **IP address**. If selected, the 'FQDN' and 'Serial Number' fields will be disabled and the device will immediately be connected to the OVOC. If you're adding **Multiple AC Devices**, you need to enter the IP Address *range* in the fields that will be displayed.
- Select and enter the device's **FQDN**. If selected, the 'IP Address' and 'Serial Number' fields will be read-only). This option allows performing SBC SSO in a way that the URL includes only FQDN names (OVOC & SBC) rather than IP addresses.

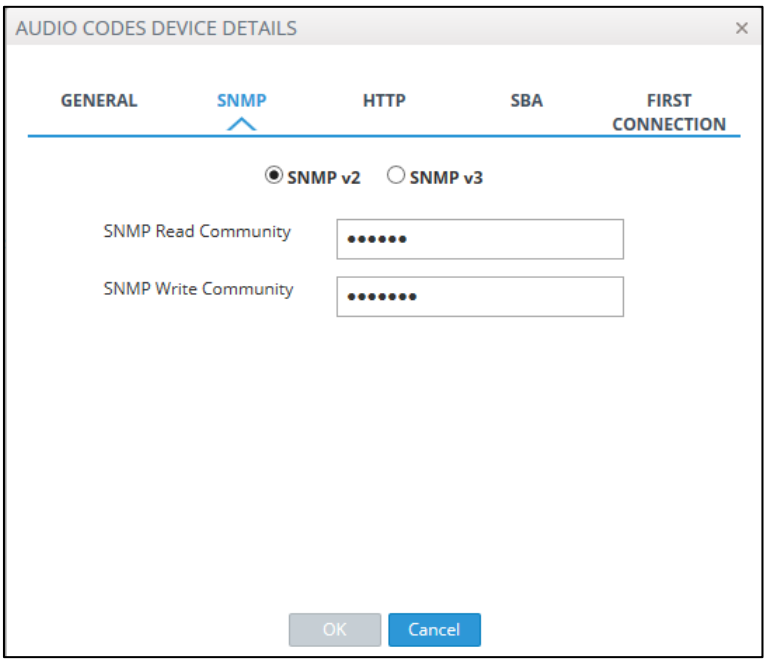
Note:

- If a device is defined using FQDN and the OVOC cannot resolve the IP address, the OVOC will not be able to manage the device until the IP address is resolved. The same applies to the Add and Refresh processes.
- FQDN is not editable after a device is defined using the FQDN option. Same applies to IP Address and Serial Number – they are not editable after defining the device using them.
- The FQDN option is not supported when adding multiple devices.
- Devices behind a NAT and devices added as a result of a keep-alive trap (auto detection) are managed using IP address + port (rather than FQDN).
- Alarm Forwarding is performed using IP address.

- [Optional] Select and enter the device's **Serial Number**. If selected, the 'FQDN' and 'IP Address' fields will be read-only. You can get the SN from the device's Web interface's Information page. The SN is only necessary for auto-detection. Generally, it is not mandatory to enter the serial number when adding a device.

8. [Optional] In the 'Location' field, enter the first letters in the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.
9. You need to configure the device's SNMP settings if you're connecting the device to the OVOC.
   - To configure SNMPv2, click the **SNMP v2** tab:

Figure 5-12: Device Details – SNMP v2

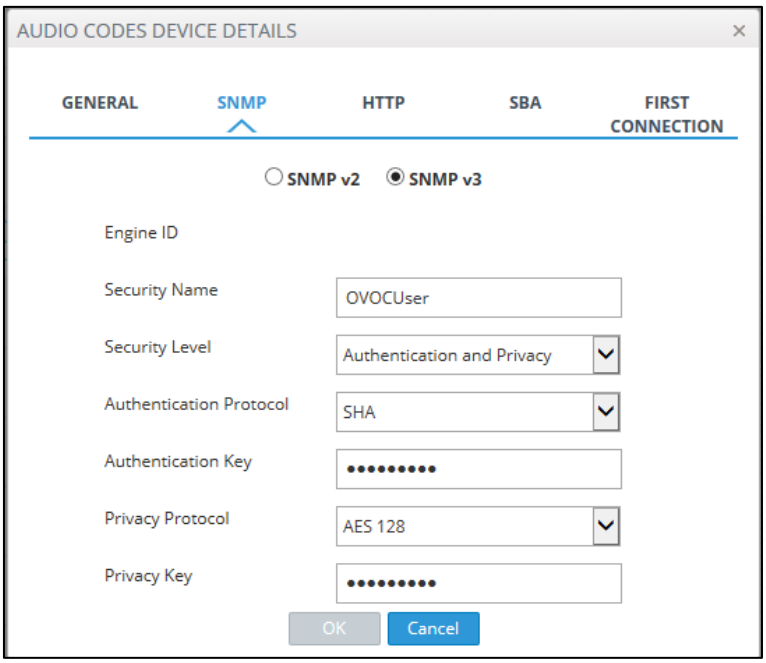


Note: The defaults are taken from the SNMP tenant profile.

- Enter the device's SNMP Read and Write Community strings.

- To configure SNMPv3, select the **SNMP v3** option:

Figure 5-13: Device Details – SNMP v3

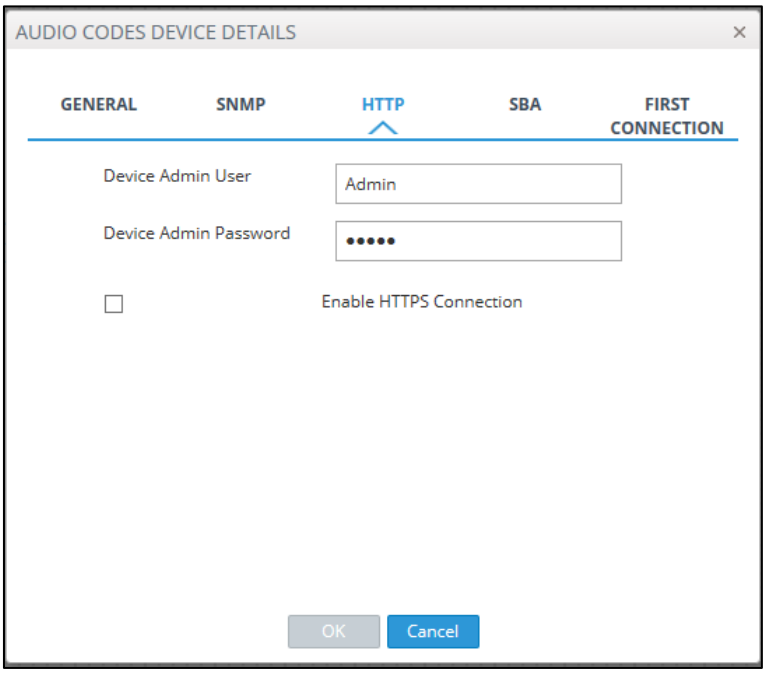


a. In the 'Security Name' field, enter the Security name of the SNMPv3 operator.
b. From the 'Authentication Protocol' dropdown, select an authentication protocol. The corresponding security level is displayed in the 'Security Level' field.
c. In the 'Authentication Key' field, leave the default unchanged or enter an authentication password.
d. From the 'Privacy Protocol' dropdown, leave the default unchanged or select a Privacy Protocol.
e. In the 'Privacy Key' field, leave the default unchanged or enter a privacy password.

Note: The defaults are taken from the SNMP tenant profile.

10. Click the now-activated **OK** button or click the **HTTP** tab.

Figure 5-14: AudioCodes Device Details – HTTP



Note: The defaults are taken from the HTTP tenant profile.

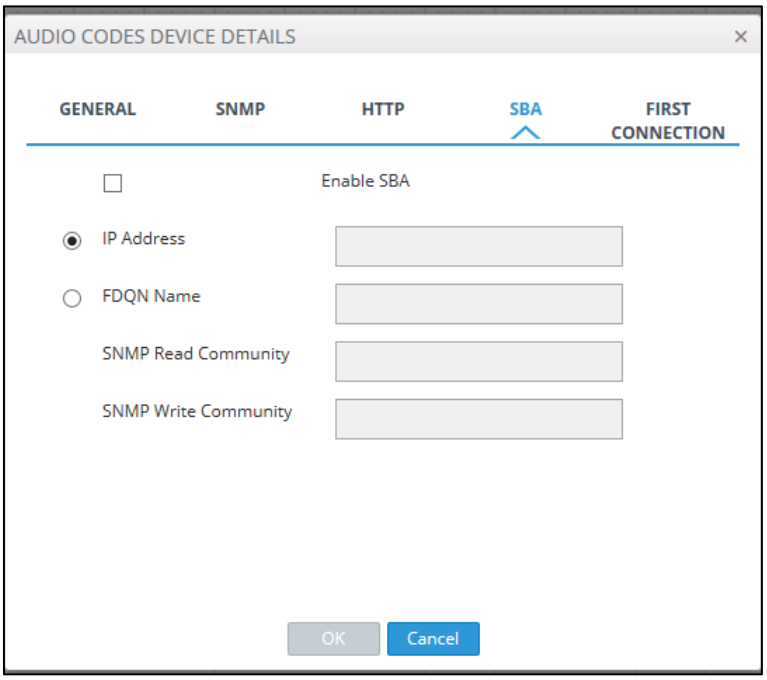
11. [Optional] In the 'Device Admin User' field, enter the device's web server user name and in the 'Device Admin Password' field, enter the web server password.
Example: **Admin**, **Admin**.
12. To secure the connection with the device, select the **Enable HTTPS Connection** option.
Securing the connection between the OVOC server and the AudioCodes device over HTTPS is used for files upload/download and for Web Client Single-Sign On.

Note:

- You can also configure HTTPS on the AudioCodes device (see the *Server IOM* for more information).
- You can also secure the connection using the default AudioCodes self-signed certificate or load custom certificates to the OVOC server (see the *Server IOM* for more information).
- To operate in 'Mutual Authentication' mode:
  - √ Set the HTTPS Authentication option 'Set Mutual Authentication' using the OVOC Server Manager (see the *Server IOM*).
  - √ Load certificates to the device (you must use the same root CA for signing the device certificate as is used for signing the certificate installed on the OVOC server) (see 'Custom X.509 Certificates - Supplementary Procedures' in the *Server IOM*).
  - √ Configure HTTPS on the device (see 'Custom X.509 Certificates - Supplementary Procedures' in the *Server IOM*).

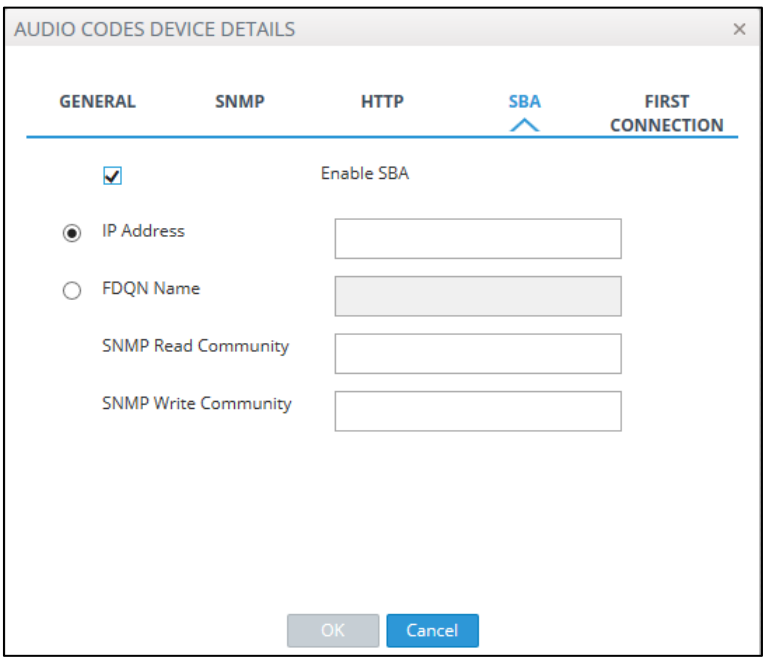
13. Click the now-activated **OK** button or click the **SBA** tab.

Figure 5-15: AudioCodes Device Details – SBA



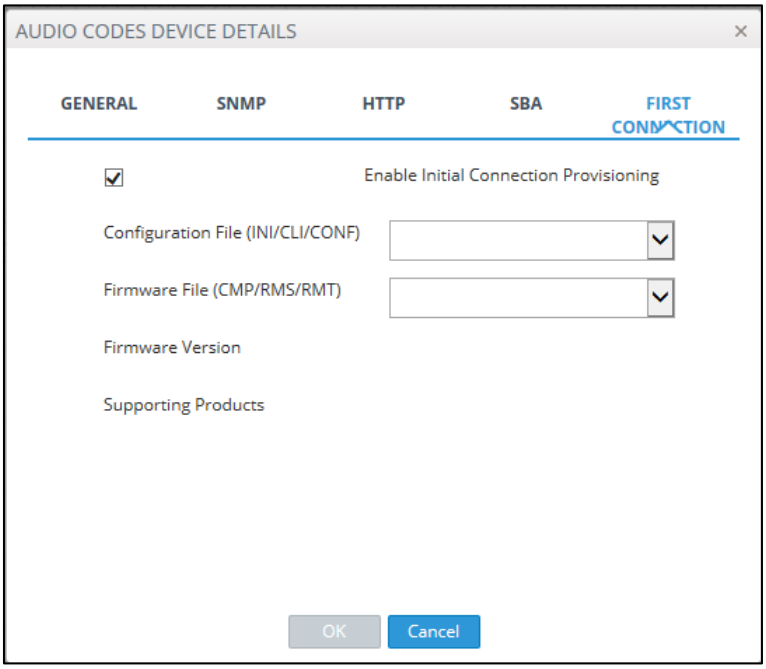
14. Select the **Enable SBA** option. This is only relevant if the device contains an SBA module.

Figure 5-16: AudioCodes Device Details – Enable SBA



15. Enter the IP address of the SBA Management Interface –OR- select the 'FQDN Name' option and in the field 'FQDN Name', enter the FQDN (Fully Qualified Domain Name) of the SBA. Example: **HOST/Branch01.SFB.interop**
16. Enter an encrypted SNMP read community string.
17. Enter an encrypted SNMP write community string.
18. Click the now-activated **OK** button or click the **First Connection** tab.

Figure 5-17: AudioCodes Device Details – First Connection



19. Select the **Enable Initial Connection Provisioning** option. This is the Automatic Provisioning a.k.a. Zero Touch feature. See Appendix B for more information. When adding an AudioCodes device or when adding multiple AudioCodes devices, you can implement this feature to enable the device/s to automatically be provisioned with their firmware and configuration files when they are connected to the OVOC server for the first time.
20. From the now-activated 'Configuration File' dropdown, select the applicable file.
21. From the now-activated 'Firmware File' dropdown, select the applicable file.
22. Click the now-activated **OK** button; the device is added to the OVOC.

Note: AudioCodes' Mediant 2000 Media Gateway device housing two TP-1610 blades can be added to OVOC using a single IP address rather than using two IP addresses (one for each blade) as was the case in OVOC versions earlier than Version 7.4.3000. Existing customers must remove any Mediant 2000 device housing two TP blades that was added to the OVOC using two IP addresses in OVOC versions earlier than Version 7.4.3000, and then add them again using a single IP address. After this action, the Alarms History and QoE calls & statistics history is cleared.

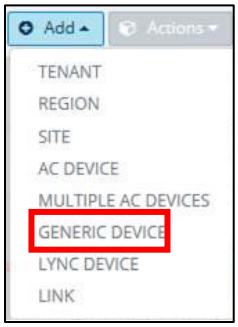
5.3.1 Adding a Generic Device

You can add a generic (non-AudioCodes) device to the OVOC.

➢ **To add a generic device:**

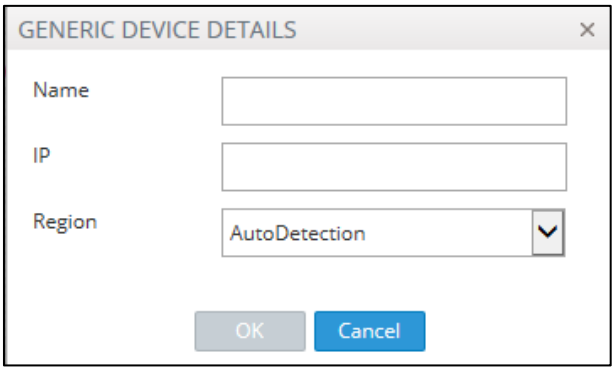
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select **Generic Device**.

Figure 5-18: Add Generic Device



The Generic Device Details screen opens:

Figure 5-19: Generic Device Details



3. Define an intuitive device name to facilitate operator-friendly management later. Do not use underscores in the name.
4. Enter the device's IP address.
5. From the 'Region' dropdown, select the device's region and then click the now-activated **OK** button; the device is added and displayed in the OVOC.

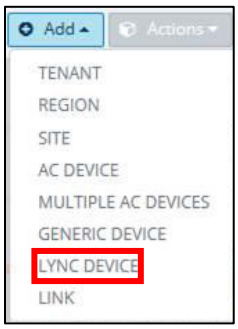
5.3.2 Adding a Microsoft Lync Device

The most commonly used Microsoft device is Lync Server 2010. The OVOC can calculate, for example, call quality for the link defined between AudioCodes devices and Microsoft Lync Server 2010. See also Appendix C.

➢ **To add a Microsoft Lync device:**

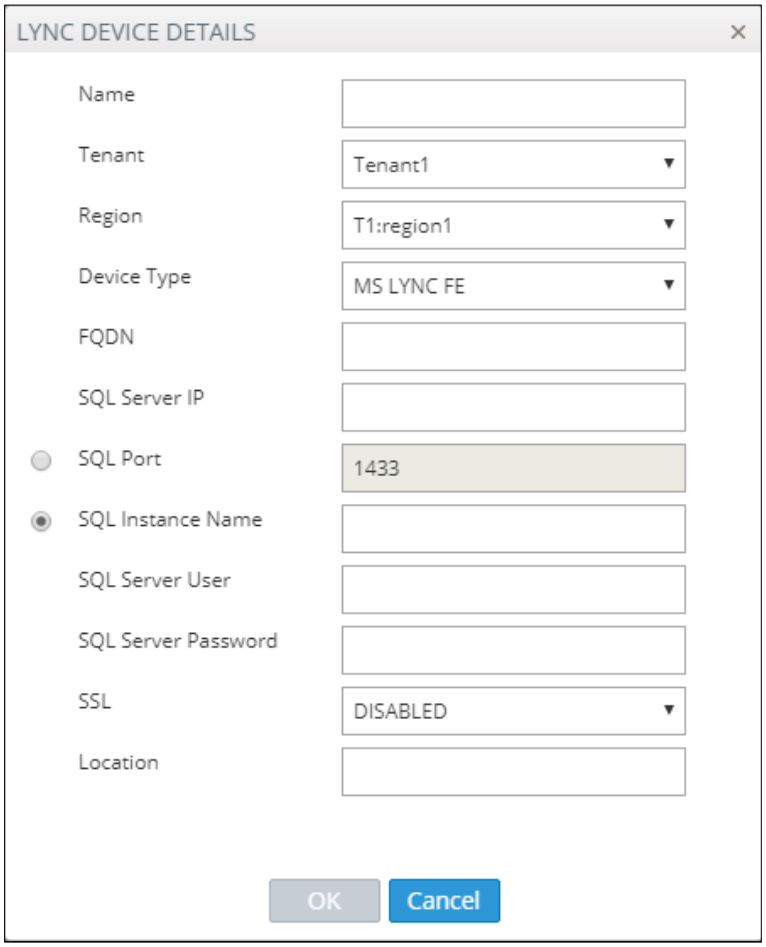
1. Open the Network Topology page (**Network** > **Topology**).
2. Click **Add** and select **Lync Device**.

Figure 5-20: Lync Device



The Lync Device Details screen opens.

Figure 5-21: Lync Device Details



3. Define an intuitive device name to facilitate operator-friendly management later. Do not use underscores in the name.
4. From the 'Region' dropdown, select a region you configured as shown in Section 5.2.
5. From the 'Device Type' dropdown, select:
   - **Microsoft Lync FE (Front End) Server**
     - The main FE parameters are 'NAME' and 'FQDN'. Other SQL parameters are for the SQL Lync Database.
     - FE Server points/reports to the SQL Database. It does not point/report to the Lync FE Services.
     - The SEM server connects to the SQL Monitoring Server and pulls control and media information from it for display.
   - **Microsoft Lync Mediation Server**
     - Implements enterprise voice and dial-in conferencing
     - Translates signaling and media (in some configurations) between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk
   - **Microsoft Lync Edge Server**
     - Deployed in a DMZ
     - Provides access to the Lync system from the Internet
     - Lets your users communicate and collaborate with users outside the enterprise's firewalls
   - **Microsoft Lync SBA (Survivable Branch Appliance)**
     - Ensures access to data and voice services in the event of a WAN outage

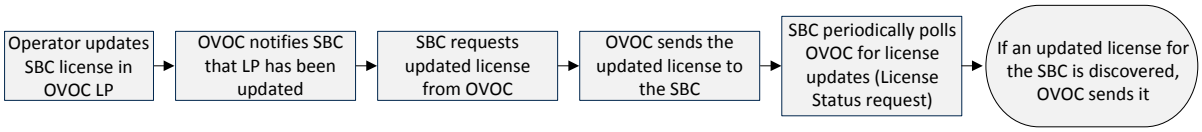
6. In the 'FQDN' field, enter the Microsoft Lync device's Fully Qualified Domain Name.
7. In the 'SQL Server IP' field, enter the IP address of the SQL Server. Applies to the centralized Lync database.
8. Select either the:
   - 'SQL Port' option and in the now-activated field enter the port number of the SQL Server. Applies to the centralized Lync database.
   - 'SQL Instance Name' option (by default selected)
9. In the 'SQL Server User' field, enter the user of the SQL Server. Applies to the centralized Lync database.
10. In the 'SQL Server Password' field, enter the Password of the SQL Server. Applies to the centralized Lync database.
11. From the 'SSL' dropdown, secure the connection between the OVOC and the SQL server over SSL by selecting either:
    - **Trusted:** An SSL connection between the OVOC server and the SQL server is opened, though it's not authenticated using a certificate.
    - **Using Certificate**: An SSL connection between the OVOC and the SQL server is opened. The OVOC authenticates the SSL connection using a certificate. Make sure you load the SSL certificate file, required by the SQL server, to the Software Manager. See Section 4.2.3.

    Default: **Disabled**. The SSL connection with the SQL server is by default non-secured.
12. [Optional] In the 'Location' field, enter the first letters in the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.
13. Click the now-activated **OK** button; the Lync device is added.

5.3.3 Managing Device Licenses in the Fixed License Pool

Note: Only a 'tenant' operator can manage the Fixed License Pool. To configure a 'tenant' operator, see License Pool Operator for more information.

Customers who deploy multiple SBCs and want to *centrally manage* the licenses of all SBCs deployed will benefit best from the Fixed License Pool feature. This feature allows updating a device's license using the process shown here:



- OVOC operator updates SBC license in OVOC's License Pool
- OVOC notifies SBC that the License Pool has been updated
- SBC requests updated license from OVOC
- OVOC sends the updated license to SBC
- SBC polls OVOC for license updates
  - every 12 hours
  - when the SBC is reset
  - (HA) when switchover and synchronization by the new active device are performed
- OVOC sends the license update to the SBC (if an update is discovered)

Note: An SBC's license is valid for seven days but this is reset each time a successful connection is established between it and the OVOC License Pool. If the SBC cannot connect to the License Pool for seven days, its license expires and resets with its initial 'local' license. This feature prevents misuse of issued licenses.

The Fixed License Pool page in the OVOC allows you to:

- centrally distribute session licenses to multiple devices according to capacity requirements
- manage the licenses of multiple devices without changing their local License Key.
- add/remove licenses to/from devices according to site requirements, independently of AudioCodes.
- apply different settings to each device without requiring a new License Key file per device from AudioCodes each time.
- manage licenses for multiple enterprise customers [ITSPs].

The Fixed License Pool supports the following license types:

- SBC sessions (includes both media and signaling)
- SBC Registrations (also referred to as Far-End Users)
- SBC Signaling sessions (includes only signaling)
- Transcoding sessions

The customer purchases a bulk number of licenses of these types and obtains a License Key to install on the OVOC. The customer can then:

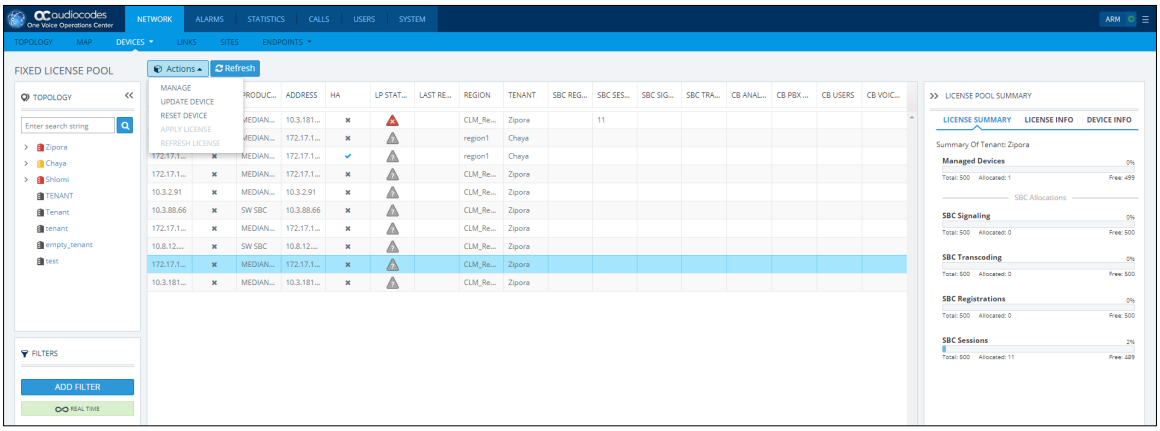
- allocate licenses to any SBC managed by the OVOC
- move licenses from any SBC back to the License Pool
- move licenses from one SBC to another
- purchase additional licenses for the pool at any time

When license capacity is fully utilized, the SBC rejects calls. If the SBC also has a 'local' license, the two are cumulated to constitute a single license.

➢ To update a license using the Fixed License Pool:

1. Open the Fixed License Pool (**Network** > **Devices**) and from the Actions dropdown, select **Update License**.

Figure 5-22: Fixed License Pool - Update License



2. Select a device and then click **Actions**.

5.3.3.1 Performing License Pool Actions

The sections below describe the actions you can perform in the License Pool page.

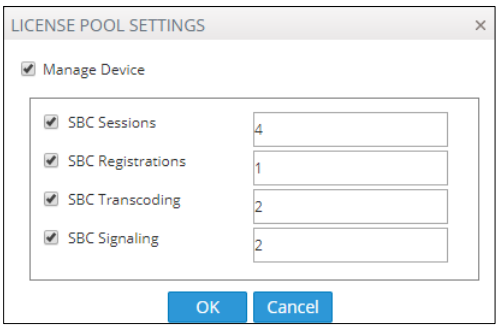
5.3.3.1.1 Allowing the OVOC to Allocate Capacity to an SBC

The OVOC's License Pool is a pool of customer-ordered SBC capacity licenses. Types of licenses in the pool include licenses for media, registration, transcoding and signaling sessions. The OVOC can allocate these capacities to devices from the pool. Capacities sent by the OVOC are added to the current capacities defined by the License Key locally installed on the device. Note that the total capacity, i.e., the local plus the remote, cannot exceed the maximum capacity supported by the specific device model. The License Pool page displays the value in red if maximum capacity is exceeded.

➢ **To allow the License Pool server to allocate capacity:**

1. In the License Pool page, select **Manage** from the **Actions** dropdown.

Figure 5-23: License Pool Settings



2. Select the **Manage Device** option to allow the License Pool to allocate capacities to the device if the capacities allowed by the locally installed License Key are exceeded.

Note:

- The device periodically checks with the pool for SBC capacity licenses. If the pool has one for the device, it sends it.
- A standalone device must be reset for an allocated license to take effect. This impacts service. If communication with the pool is lost for a long period, the device discards the allocated license (i.e., expires) and resets with its initial license according to the License Key (preventing misuse of licenses allocated by the pool).
- When a device operates in High-Availability (HA) mode, the active and redundant devices are installed with a new SBC license from the pool without impacting traffic through a hitless license upgrade mechanism whereby the pool first downloads the license to the redundant device, resets it, and then triggers the devices to perform an HA switchover. It then downloads the same license to the previously active device (now the redundant), resets it, and then triggers another HA switchover. Currently active calls are therefore maintained throughout the process. With HA devices, you need to perform an **Apply License** action (rather than a **Reset Device** action). If you decrease the pool, traffic in HA mode may be impacted. You can optionally perform a **Refresh License** action to check current open sessions.
- For HA systems, the pool automatically allocates an equal number of SBC licenses (sessions) to both the active and redundant devices. For example, if the pool allocates 200 sessions to the active device, it also allocates 200 to the redundant. It's therefore important to take this into consideration when ordering a license pool.
- If the device is restored to factory defaults, the SBC licenses allocated by the pool are removed and those from the locally installed License Key are applied.
- If the pool allocates a device an SBC license that exceeds the maximum number of sessions the device supports, the device sets the number to its maximum supported.

3. Select **SBC Sessions** and enter the number of media sessions (voice calls) the License Pool will allocate to the SBC.
4. Select **SBC Registrations** and enter the number of registration sessions (the number of users that can be registered with the device) the License Pool will allocate to the SBC.
5. Select **SBC Transcoding** and enter the number of transcoding sessions the License Pool will allocate to the SBC.
6. Select **SBC Signaling** and enter the number of SIP signaling sessions the License Pool will allocate to the SBC.

5.3.3.1.2 Updating a Device's License

You can update a device's license after it expires.

➢ **To update a device's license:**

- If a device's license expires, select **Update Device** from the **Actions** dropdown; the action reestablishes the REST connection with the device and sends the latest device license. OVOC allows multiple license update.

Note to users of CloudBond 365 and CCE Appliance

When licenses are applied to a CloudBond/CCE Appliance device (**Update Device**) and an SNMP update is sent to the device, this automatically triggers the device to reset. You do not need to reset the device from the License Pool.

5.3.3.1.3 Resetting a Device

You need to reset the device in order to apply a license update.

➢ **To reset a device:**

- If a device's license expires and you update the device, you then need to reset the device in order to apply the license update. The icon alerts you to this issue (see the table below). From the **Actions** dropdown, select **Reset Device**.

5.3.3.1.4 Applying a License

You can apply a license to an HA-supported device.

Note:

- The number of licenses required for an HA device is twice the number of licenses per device (active device + redundant device). If the License Pool server allocates 200 sessions to the active, it will allocate 200 sessions to the redundant.
- According to AudioCodes licensing policies, HA devices require an equivalent number of licenses for both the active and redundant devices. For more information, contact your AudioCodes representative.

➢ **To apply a license:**

- The icon alerts you to apply a hitless new license to an HA-supported device because the number of active sessions/users on the device is higher than that allocated to the device (see the table below). From the **Actions** dropdown, select **Apply License**; When the action is performed, the device performs a hitless upgrade using the HA switchover mechanism. **Refresh License** (see the next action below) is

also needed until you see that all active license values are displayed with the new reduced values otherwise some of the users/sessions will be disconnected when choosing **Apply License**.

Note: When applying a hitless license update (**Apply License**) to an HA device whose maximum number of sessions exceeds that available in the License Pool, service is affected.

5.3.3.1.5 Refreshing a License

➢ **To refresh a license:**

1. From the **Actions** dropdown, select **Refresh License**; the configured license session values are refreshed according to the current active sessions/users on the device.

Note to users of CloudBond 365 and CCE Appliance

Reset Device, **Apply License** and **Refresh License** are not applicable.

2. Under the 'Managed' column, determine if a device is managed ✔or unmanaged ✖
3. Under the 'HA' column, determine if a device features HA ✔or not ✖
4. Under the 'LP' column, determine license statuses using the table below as reference.

Table 5-7: LP Column Indicating License Statuses

Icon	Status
	Device is not managed by the OVOC's License Pool.
	Device is successfully managed by the OVOC's License Pool.
	Reset Device is needed to apply the license update.
	Apply License (hitless) for HA devices is needed in order to complete the license update.
	Apply License (hitless) for HA devices is needed in order to complete the license update because the number of active sessions/users on the device is higher than that allocated to the device. **Refresh License** is also needed until you see that all active license values are displayed with the new reduced values, otherwise some of the users/sessions will be disconnected when choosing **Apply License**.
	A hitless license update is in progress on the HA device. License configuration is not permitted during this time.
	Either: ▪ OVOC is unable to apply a License Pool configuration on the device ▪ Device never accessed OVOC's License Pool ▪ Device is unable to access OVOC's License Pool: License Expired ▪ License Pool exists in the device but is not managed in the OVOC
	The license update process on the device was unsuccessful. The device failed to update the license. Verify the license configuration and modify as required.

Note:

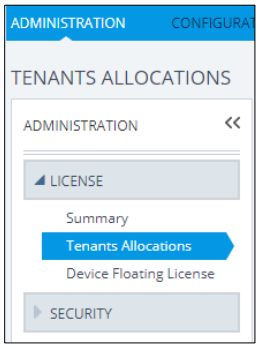
- If a device's capacity is exceeded, the value displayed in the License Pool is red.
- If a devices license expires, the Last Request Time displayed is red.
- Running a hitless license downgrade on an HA device when the current number of active SBC sessions/users on the device is higher than that allocated to the device can lead to service disruption. To avoid this, run the Refresh License action or wait until the number of current SBC sessions/users is aligned to the configured value.
- If you downgrade the transcoding session license so that the number of active transcoding sessions/users is higher than what was allocated to the device, service is not affected, i.e., there is no forceful closure of excess call sessions. No new call sessions can be established, however, until the number of current transcoding sessions is less than / equal to the limit defined in the new session license.

5.3.3.1 Before Performing 'Manage Device' / 'Update Device'

Make sure of the following before performing 'Manage Device' or 'Update Device':

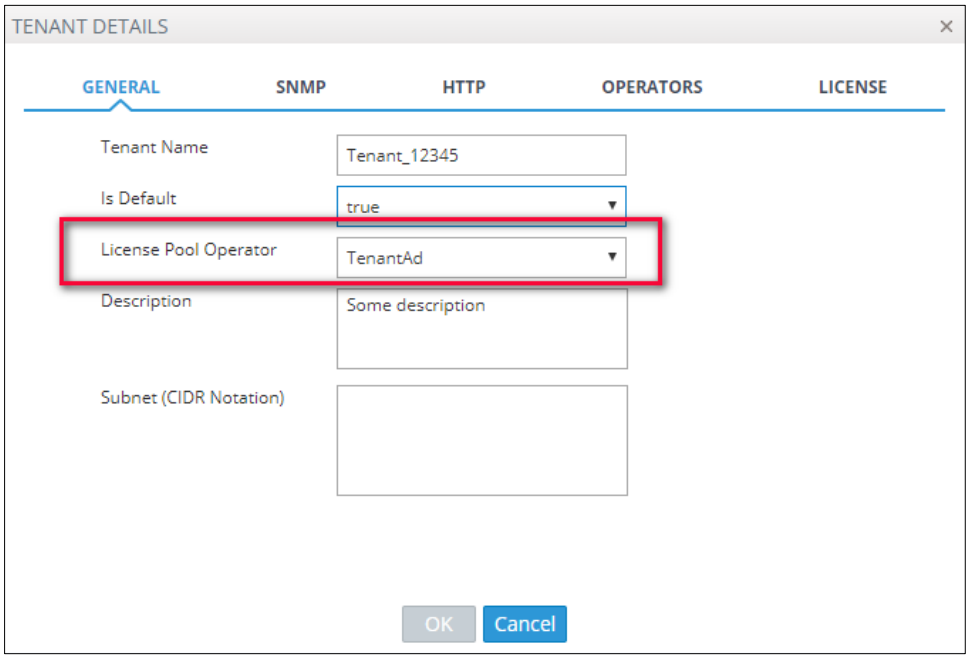
- Make sure sufficient licenses are allocated on the device's tenant (**System** > **Administration** > **License** > **Tenants Allocations**).

Figure 5-24: Make Sure Sufficient Licenses are Allocated on the Device's Tenant



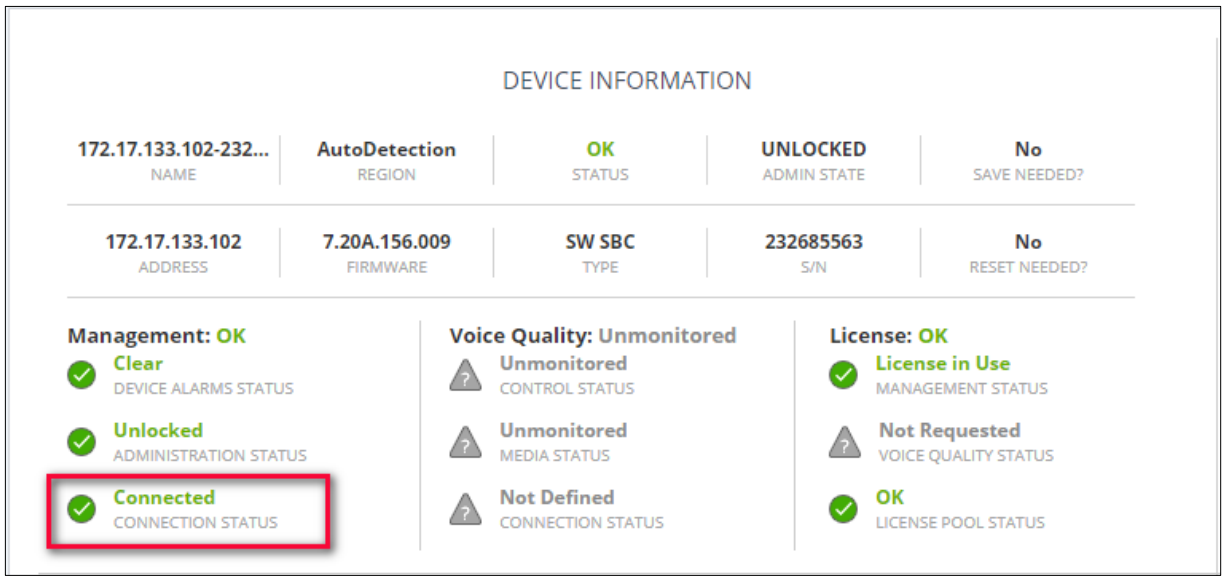
- Make sure the device's tenant's 'License Pool Operator' is valid; make sure their password has not expired (**Network** > **Devices** > **Manage** > select the device > **Edit**).

Figure 5-25: Make Sure License Pool Operator is Valid



- Make sure the device is connected to the OVOC (**Network** > **Devices** > **Manage** > select the device > **Show**).

Figure 5-26: Make Sure the Device is Connected to the OVOC



5.3.3.2 License Pool Alarms

Devices can issue the following License Pool alarms:

- acLicensePoolInfraAlarm
- acLicensePoolApplicationAlarm
- acLicensePoolOverAllocationAlarm
- acLicenseKeyHitlessUpgradeAlarm

For more information about alarms related to the License Pool, see the *Alarms Guide*.

5.3.4 Backing up a Device's Configuration using Backup Manager

You can manually back up a device's configuration to the OVOC server using the Backup Manager. For details on configuring automatic periodic device configuration backups, see Section 4.2.5.

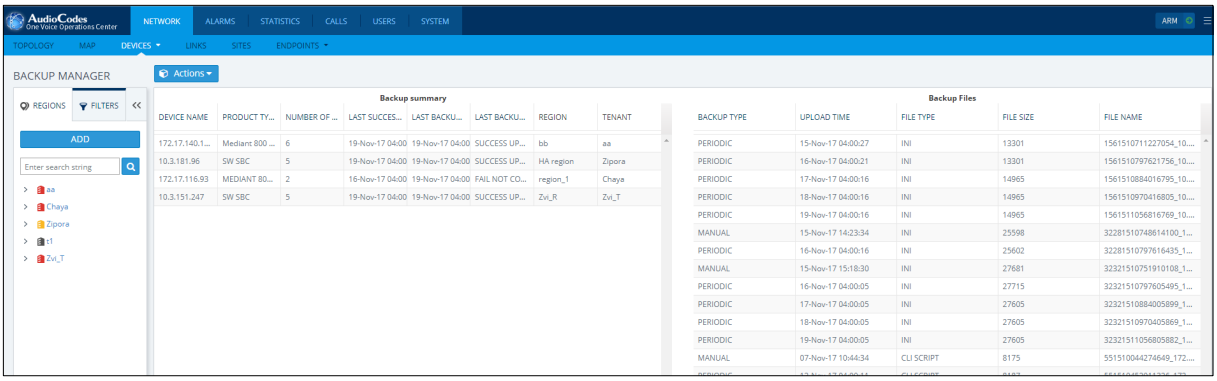
5.3.4.1 Manually Backing up a Device's Configuration

The Backup Manager page lets you manually back up a device configuration on the server.

➢ **To manually back up a device's configuration on the OVOC server:**

1. In the OVOC, open the Backup Manager page (**Network** > **Devices** > **Backup Manager**).

Figure 5-27: Backup Manager



The Backup Manager page displays:

- **Backup Summary** pane**:** For all files that have been backed up to the OVOC for each device.
- **Backup Files** pane: Full list of all the backup ini and CLI script (MSBR devices files) for CPE devices files that have been saved to the Backup Manager for all devices.

Each entry in the summary displays:

- Device Name and Product Type
- The number of files backed up from the device to the OVOC
- The last backup status, e.g., Successful
- The date of the last backup file
- The tenant under which the device is located

You can filter displayed files for more effective access to the specific files you need:

- Click a column header; files are displayed accordingly.

Backed-up file names are in the format:

node id||timestamp _ Device IP Address _ Node ID _ Serial Number _ periodic/manual _ Product type _ INI/CONF/CLI _ Date Formatted

Here's an example of a backed-up filename:

411515387481228_192.168.200.47_41_3968002_m_82_INI_TYPE_2258-Jan-07-2018.ini

Use the table below as reference to the example.

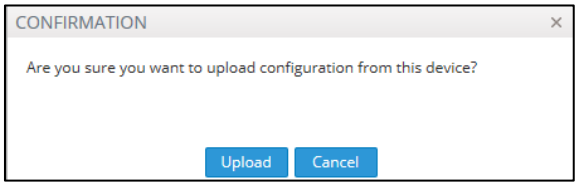
Table 5-8: Explanation of Backed Up File Name Format

File Name Format	Explanation
411515387481228	Indicates the Node ID||Timestamp
192.168.200.47	Indicates the device's IP address
41	Indicates the Node ID
3968002	Indicates the Serial Number
m	Indicates whether backup was periodic or manual. In the example, it was manual.
82	Indicates the product type.

File Name Format	Explanation
INI_TYPE	Indicates the type of backed-up file: INI/CONF/CLI
2258-Jan-07-2018	Indicates the time and date, formatted as: HHmm-MMM-dd-yyyy

2. In the page's Backup Summary, select the device whose configuration (ini or cli script file) you want to back up on the OVOC server.
3. From the Actions' dropdown, select the **Backup** option; you're prompted with a message 'Are you sure you want to upload configuration from this device?'

Figure 5-28: Backup Manager – Backing up a Device's Configuration – Confirmation Prompt



4. Click **Upload**; the configuration is uploaded from the device to the OVOC server.

5.3.4.2 Saving the Last Backed-up Configuration to your PC

You can save the last backed-up device configuration to your PC.

➢ **To save the last backed-up configuration to your PC:**

1. In the Backup Manager page's Backup Summary, select the device whose last backed-up configuration you want to save.
2. From the Actions' dropdown, select the option **Save**; the last backed-up device configuration is saved on your PC.

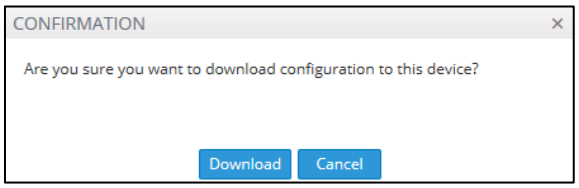
5.3.4.3 Restoring the Last Backed-up Configuration to the Device

You can restore the last backed-up configuration to the device.

➢ **To restore the last backed up configuration to the device:**

1. In the page's Backup Summary pane, select the device whose last backup you want to restore.
2. From the Actions' dropdown, select the option **Restore Last Backup**; you're prompted with a message 'Are you sure you want to download configuration to this device?'.

Figure 5-29: Backup Manager – Restoring a Device's Last Backup – Confirmation Prompt



3. Click **Download**; the configuration is downloaded from the PC to the device.

5.4 Adding Links

Links are logical VoIP communication paths between devices that measure and display key metrics on calls made on them. Links are defined according to IP Group (IP network entity such as a server, e.g., IP PBX, or a group of users, e.g., LAN IP phones, with which the E-SBC communicates), Trunk Group (logical group of physical trunks and channels), Phone Number or SIP IP address.

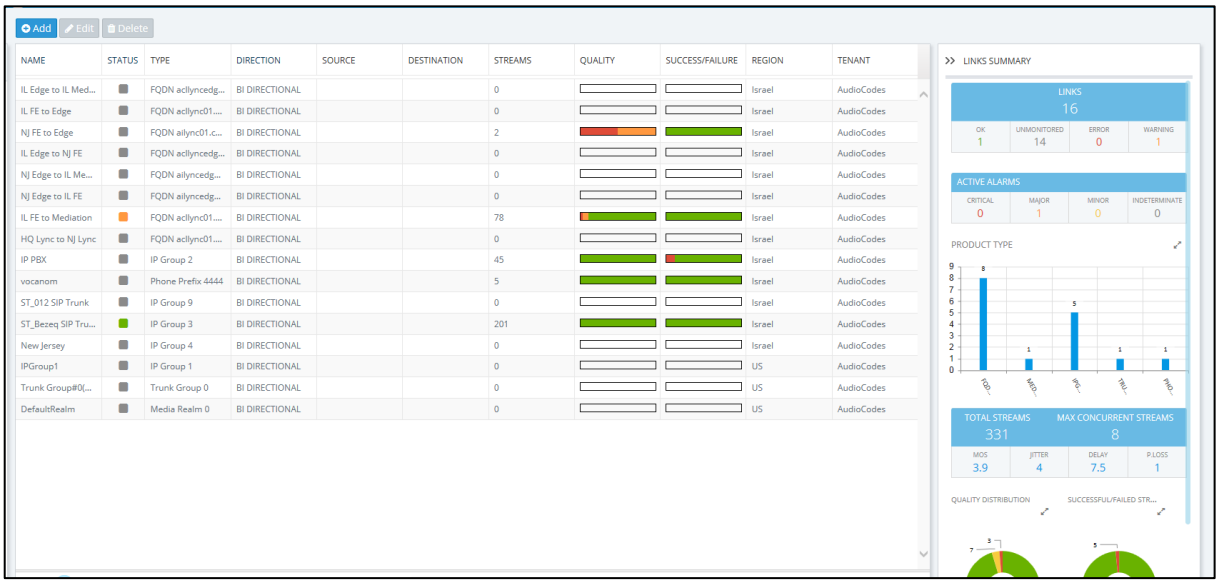
The 'source' device on which key metrics monitoring is based must be an AudioCodes device or Lync device. The second device can be an AudioCodes device, Lync device or a non-AudioCodes device. You can define one or more links between devices. The links are displayed in the Network Topology page. The voice quality status on each device/link is indicated by the color green, yellow or red, i.e., good, fair or poor, based on QoE thresholds described under Section 8.

You can add a link from the Topology page's **Add Link** dropdown or you can pull a line connector from a device and connect it to another device on the page.

➢ **To add a link:**

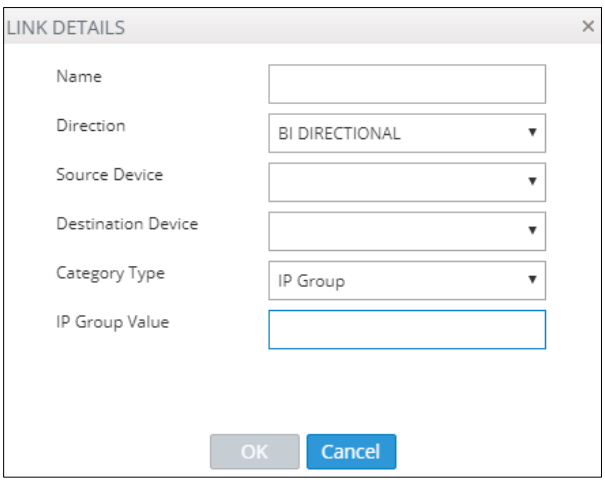
1. After configuring devices, open the Links page (**System** > **Network** > **Links**).

Figure 5-30: Links



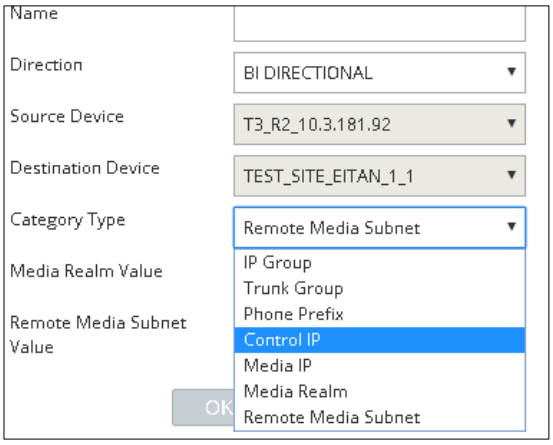
2. Click **Add**.

Figure 5-31: Link Details



3. Use the table below as reference.

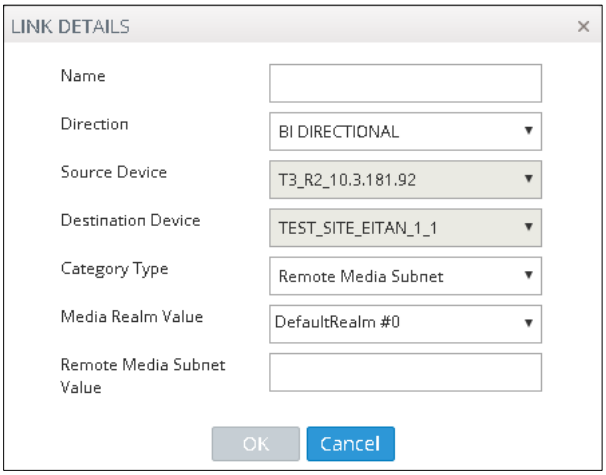
Table 5-9: Adding a Link – Parameter Descriptions

Parameter		Description
Name		Enter an intuitive name for the link to facilitate effective management later.
Direction		Defines the direction of the port link between source and destination device. When the link is configured as **Bi Directional** (for example), a bi-directional port will be used for this connection.
Source Device		From the dropdown list, select the source device *from which* to link to the destination device. You can alternatively search for it.
Destination Device		From the dropdown list, select the destination device *to which* to link from the source device. You can alternatively search for it.
The link counts and computes statistics on all calls that originate in the source device, based on one of the following Category Types (selected from the 'Category Type' dropdown:		
Category Type	From the dropdown select one of the Category Types below. Based on your selection, the link will count and compute statistics on all calls originating in the source device. 	
	IP Group	Defines the source device IP-Group index (a list of options may be available).
	Trunk Group	Lets you configure Trunk Groups, i.e., logical groups of physical trunks and channels each of which can include multiple trunks and ranges of channels. Trunk Groups need to be configured and assigned with telephone numbers to enable and activate the channels of the device. After configuring Trunk Groups, you need to use them for routing incoming IP calls to the Tel side, which is represented by a specific Trunk Group (ID). You can also use Trunk Groups for routing Tel calls to the IP side.
	Phone Prefix	Defines the prefix text of a phone number or SIP URI string. See the Note below for more information.
	Control IP	Defines a valid IP-Address on which SIP control messages are originated.
	Media IP	Defines a valid IP-Address on which SIP media messages (voice/fax) are originated. See the Note below for more information.
	Media Realm	Defines the source device Media Realm index (a list of options may be available).
	Remote Media Subnet	Defines the source device Media Realm subnet index (a list of options may be available; Media Realm must also be defined).
	FQDN	Available only when the source device is a Lync device. The FQDN of the selected source and destination devices.

4. The field below 'Category Type' (see the preceding parameter) is the *category value* field which updates according to what you selected for 'Category Type'. If for 'Category Type' you selected:

- **IP Group** (for example), then **IP Group Value** is displayed in this field. Enter the IP Group's ID.
- **Trunk Group** (for example), then **Trunk Group Value** is displayed. Enter the Trunk Group's ID.
- **Control IP** (for example), then **Control IP Value** is displayed. Enter the IP address (the actual IP address, not the group ID).
- **Media IP** (for example), then **Media IP Value** is displayed. Enter the IP address (the actual IP address, not the group ID).

  Note that some categories for 'Category Type', like **Remote Media Subnet** and **FQDN**, present *two* value fields, as shown in the figure below.



Note: If you configured parameter 'Category Type' as **Phone Prefix**, **Control IP** or **Media IP** (see the previous parameter), you can enter a *regular expression* instead of a string in the field under 'Category Type' which updates according to 'Category Type'. If the regular expression will be matched, the call will be sent over the link. Following are examples of regular expressions:

.* = any value will be accepted, for example, abc, 123, abc123
a.* = any value beginning with the letter 'a' will be accepted, for example, abc, a, abc123
.*a = any value ending with the letter 'a' will be accepted, for example, bca, a, bc123a
\\d = any value containing a single digit will be accepted, for example, 1, 2
\\d\\d\\d\\.\\d\\d\\.\\d\\d\\d\\.\\d\\d\\d = any value that contains (three digits - point - two digits - point - three digits - point - three digits) will be accepted, for example, IP address **172.17.118.165**

To test complex regular expressions use either:
https://www.freeformatter.com/regex-tester.html

-OR-

https://regex101.com/

5. Click **Apply**; the link is added and displayed in the SEM.

Note:

- Statistics obtained from **Links** form a *subset* of those obtained from **Devices**
- Links statistics are obtained from *streams*. A **stream** is a single leg of an SBC call. It's therefore possible for the total links streams statistics to be higher than the total devices calls statistics. For example, when a call is sent from IP Group 1 to IP Group 2 on same device, and there are two links configured to aggregate streams from IP Group 1 and IP Group 2 respectively, the total **Links** statistics will present it as *two streams* but **Devices** statistics will present it as *one call*.
- **Links** are *logical* entities. Multiple links defined on the same device may therefore aggregate statistics on the same streams, so the total number of **links** streams statistics in the network may be higher than the total number of actual streams statistics in the network.

  It's therefore recommended to avoid overlapping links definitions.

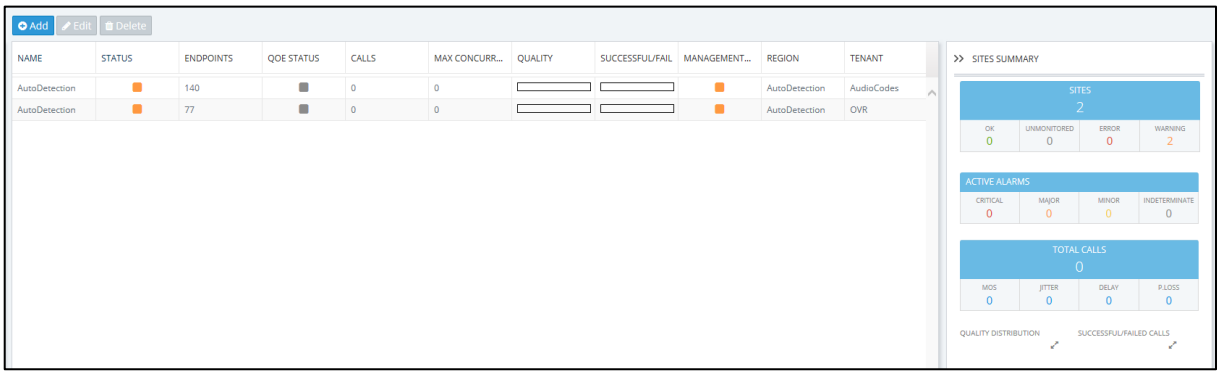
5.5 Adding Sites

A site is a group of endpoints under which endpoints (phones) are located. You need to define a site under a region. The region must be defined under a tenant.

➢ **To add a site:**

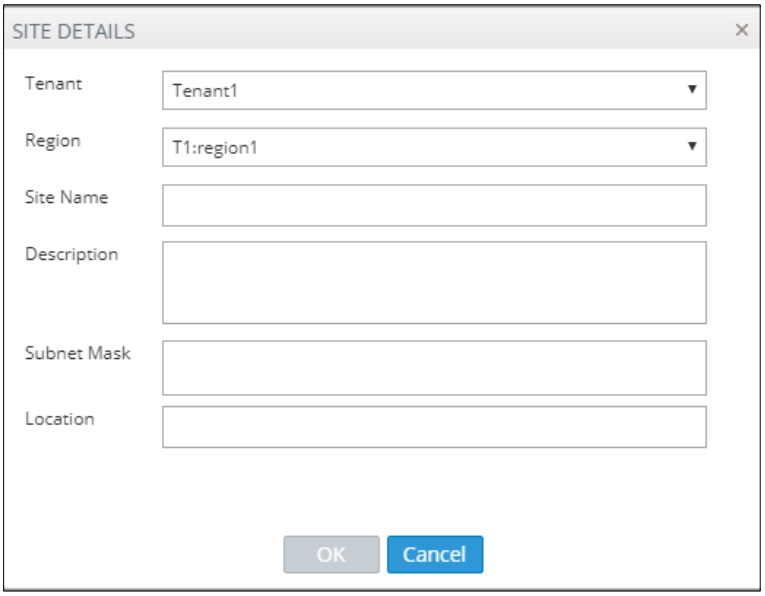
1. After configuring the region under which to locate the site, open the Sites page (**Network** > **Sites**).

Figure 5-32: Sites



2. Click **Add**.

Figure 5-33: Site Details



3. From the 'Region' dropdown, select the region under which to locate the site.
4. Provide an intuitive name for the site to facilitate effective, intuitive management later.
5. Enter a description of the site to facilitate effective, intuitive management later.
6. Enter a Subnet Mask or multiple Subnet Masks. The format must be (for example) 255.255.0.0/1. Used for auto detection of endpoints. Must be contained in the same subnet mask as the subnet mask of the region under which it is defined - if the region was configured with a subnet mask.
7. [Optional] In the 'Location' field, enter the first letters in the name of the city / country in which to locate the site, and then select the city / country from the list that pops up.
8. Click the now-enabled **OK** button; the site is added.

5.6 Managing Endpoints

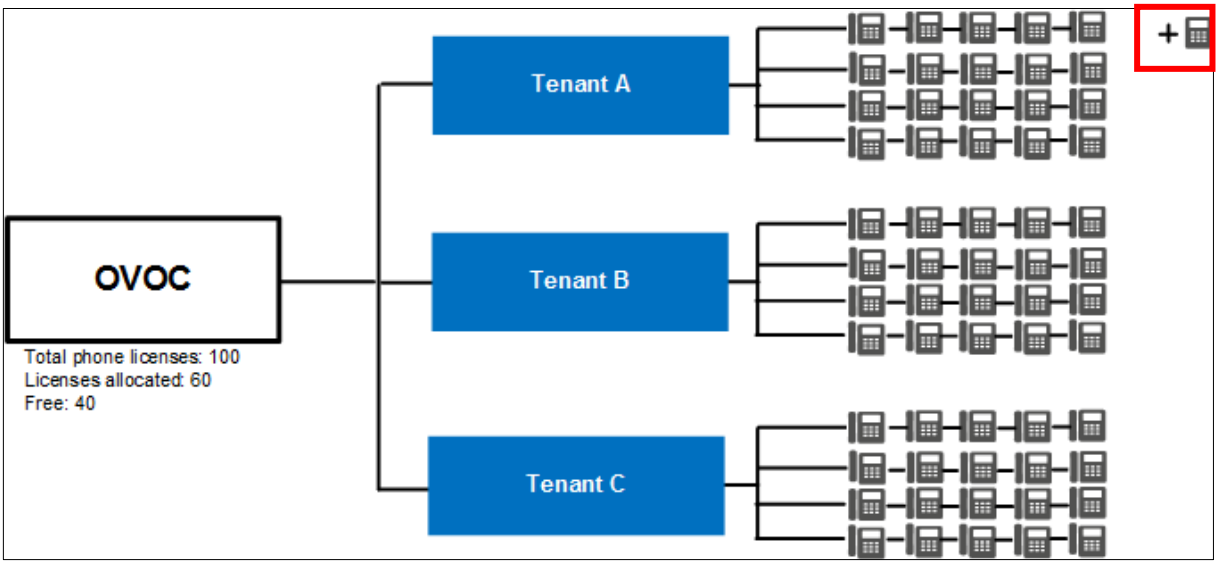
The OVOC supports endpoints management through the directly accessible IP Phone Manager Pro application.

5.6.1 Dynamic Allocation of Endpoint Licenses

The OVOC *dynamically allocates* endpoint licenses to tenants by default, so that distribution is evenly and effectively performed. When a phone (endpoint) is connected to the network for the first time, it reports to the OVOC with a keepalive message. The OVOC adds the phone to its database and dynamically allocates licenses to its tenant.

Here's an example to clarify the principle of dynamic allocation.

Figure 5-34: Example of Dynamic Allocation of Phone Licenses to Tenants



In the example (refer to the figure above):

- Out of the total number of phone licenses which the enterprise purchased (100), indicated by OVOC server parameter 'Managed Endpoints', the OVOC has already allocated 60.
  - Tenant A was allocated 20
  - Tenant B was allocated 20
  - Tenant C was allocated 20
- The OVOC is left with 40 free phone licenses which it can still allocate to tenants (100 total – 60 allocated = 40 free)
- A new phone is connected to the enterprise network
- The OVOC detects the new phone added under Tenant A, adds the phone to the OVOC database and dynamically allocates to the phone's tenant 5% of the number of phone licenses that can still be allocated (5% of 40) or, if this results in less than 5 licenses, then 5 are allocated. 5% of 40 is 2, so in the example, 5 licenses are allocated to Tenant A.

Note:

- Applies to all AudioCodes phones whose management is supported by IP Phone Manager Pro, and to all phones which support SIP PUBLISH protocol and whose QoE management is supported by the OVOC's Session Experience Management.
- Before version 7.4.2000, if a tenant's allocation was full, the OVOC dropped the phone and the user manually added it to another tenant in the OVOC GUI.
- An alarm *endpointsFloatingLicenseEvent* is sent when dynamic allocation occurs. See the *Alarms Guide* for more information.

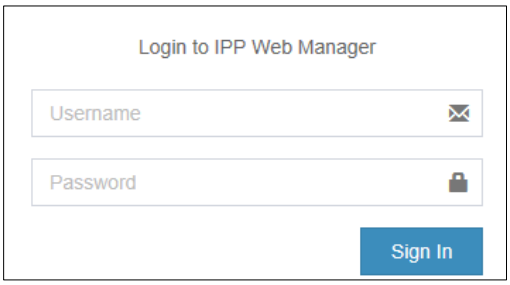
5.6.2 Configuring Endpoints

The OVOC lets you directly access the IP Phone Manager Pro application to configure endpoints (phones).

➢ **To access the IP Phone Manager Pro:**

1. Select **Configuration** from the Endpoints dropdown under the Network menu.

Figure 5-35: Login to IP Phone Manager Pro



2. See the *IP Phone Manager Pro Administrator's Manual* for detailed information on how to configure phones.

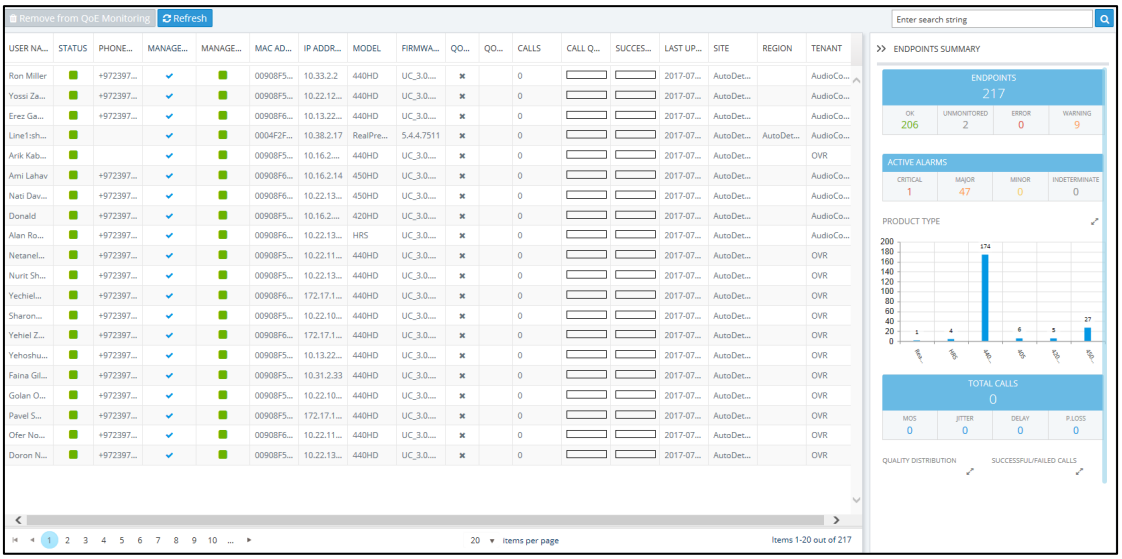
5.6.3 Monitoring Endpoints Status

The OVOC lets you monitor phones statuses.

➢ **To monitor phones statuses:**

1. Open the Endpoints page (**Network** > **Endpoints** dropdown > **Status**).

Figure 5-36: Endpoints - Status



2. See the *IP Phone Manager Pro Administrator's Manual* for detailed information on how to determine phones statuses.

5.6.4 Removing Endpoints from QoE Support

Removing an endpoint from QoE monitoring removes the endpoint from QoE support, freeing the used license. It does not remove the endpoint from display in the Endpoints page of the OVOC.

➢ **To remove an endpoint from QoE support:**

1. Open the Endpoints page as described in the previous section and select the phone to remove from QoE support.
2. Click the button **Remove from QoE Monitoring**; the relevant 'QoE Supported' column is updated with **X** instead of ✓.

This page is intentionally left blank.

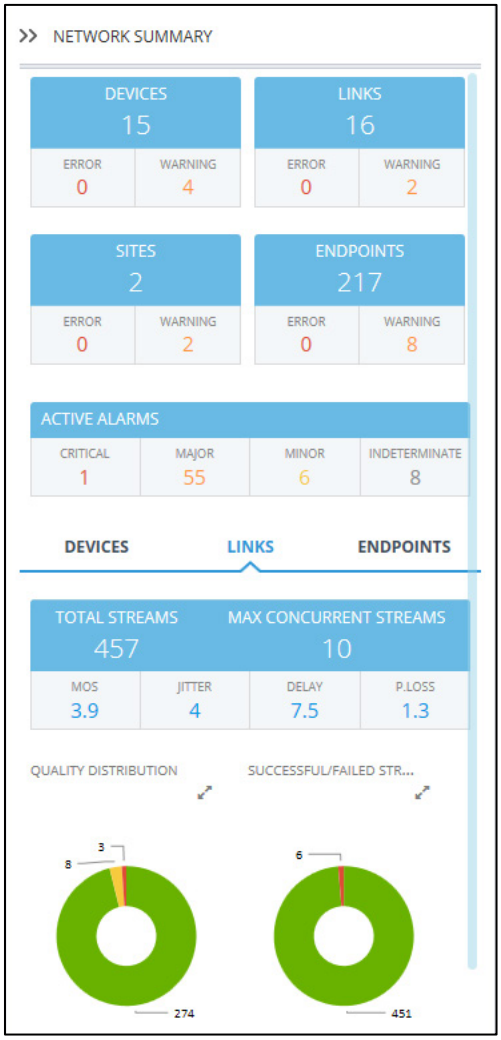
6 Assessing Network Health

This section shows how to determine the health of your IP telephony network. The OVOC provides real-time monitoring as well as historical monitoring of network traffic, giving operators a health monitoring functionality that includes alarms and diagnostics capability.

6.1 Assessing Health from the Network Summary

The Network Topology page displays a Network Summary pane which you can reference to quickly assess the overall health of the network.

Figure 6-1: Network Summary

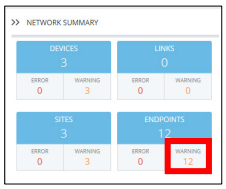


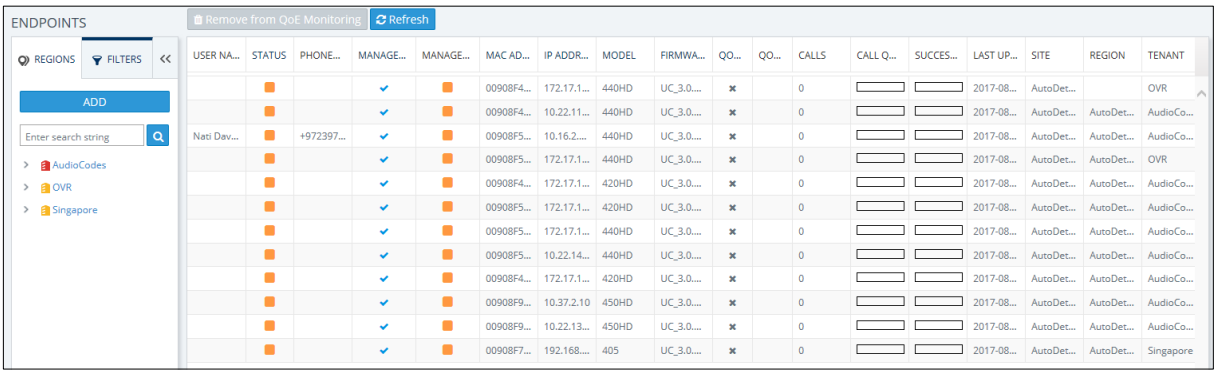
- The four upper Network Summary panes display:
  - The count of Devices, Links, Sites and Endpoints on which alarms are currently active.
  - The color-coded number of Devices, Links, Sites and Endpoints whose status is currently Error / Warning. If you click the # of
    - **Devices** then the Devices Manage page opens displaying all devices whose status is Error / Warning
    - **Links** then the Links page opens displaying all links whose status is Error / Warning
    - **Sites** then the Sites page opens displaying all sites whose status is Error /

Warning

- **Endpoints** then the Endpoints page opens displaying all endpoints whose status is Error / Warning

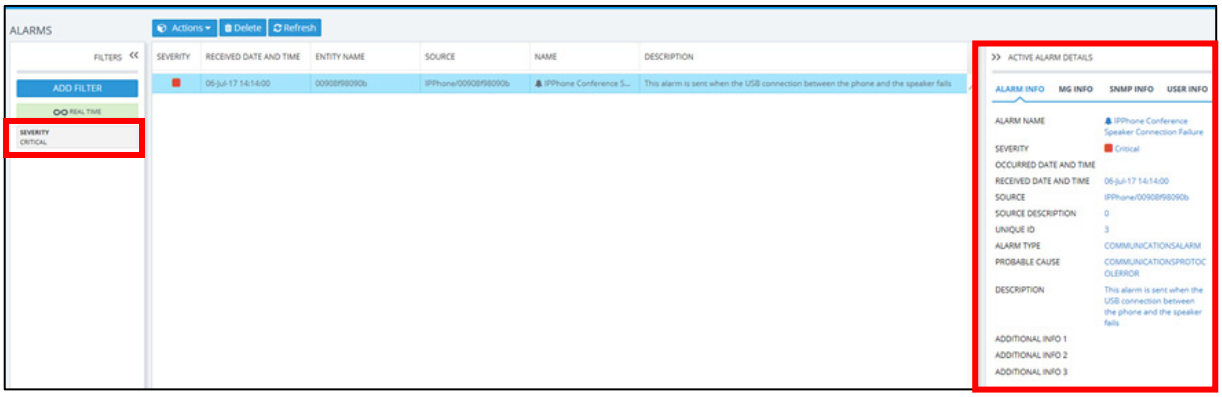
Figure 6-2: Example: 12 Endpoint Warnings





- The Active Alarms pane displays:
  - The total number of Critical, Major, Minor and Indeterminate active alarms (color-coded) currently active in the network.
  - Click any severity level's total to display only alarms of that severity level in the Alarms page. Example: Under **Critical** in the Active Alarms pane above, click **1**:

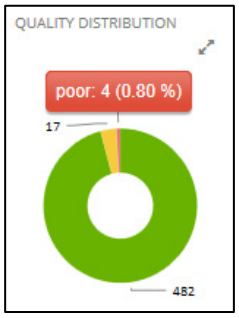
Figure 6-3: Alarms Filtered by Severity Level



You can select an alarm in the page to view detailed information about it in the All Alarm Details pane on the right side of the page.

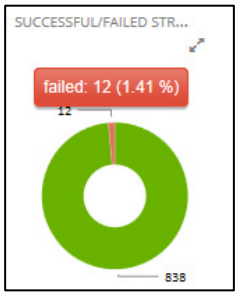
- In the Network Summary window, the (default) **Links** tab displays:
  - The total # of streams over links in the network.
  - The maximum # of concurrent streams over links in the network.
  - The average MOS measured over links in the network.
  - The average Jitter measured over links in the network.
  - The average Delay measured over links in the network.
  - The average Packet Loss measured over links in the network.
  - **Quality Distribution pie chart**

- Point your cursor over a green, yellow or red segment; a popup indicates the # and % of streams over links in the network whose quality was measured to be good, fair or poor respectively. For example:



- Click any color-coded voice quality segment to open the Calls List filtered by that voice quality score (Good, Fair or Poor).

- **Successful/Failed Streams pie chart**
  - Point your cursor over a green or red segment; a popup indicates the # and % of streams over links in the network whose performance was measured to be successful or failed respectively. For example:



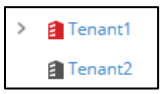
  - Click any color-coded segment to open the Calls List filtered by that call performance evaluation (Successful or Failed).

- Click the **Devices** tab to display:
  - The total # of calls over devices in the network.
  - The maximum # of concurrent calls over devices in the network.
  - The average MOS measured over devices in the network.
  - The average Jitter measured over devices in the network.
  - The average Delay measured over devices in the network.
  - The average Packet Loss measured over devices in the network.
  - **Quality Distribution pie chart**
    - Point your cursor over a green, yellow or red segment; a popup indicates the # and % of calls over devices in the network whose quality was measured to be good, fair or poor respectively.
  - **Successful/Failed Streams pie chart**
    - Point your cursor over a green or red segment; a popup indicates the # and % of calls over devices in the network whose performance was measured to be successful or failed respectively.
- Click the **Endpoints** tab to display:
  - The total # of calls over endpoints in the network.
  - The maximum # of concurrent calls over endpoints in the network.
  - The average MOS measured over endpoints in the network.
  - The average Jitter measured over endpoints in the network.
  - The average Delay measured over endpoints in the network.
  - The average Packet Loss measured over endpoints in the network.

- **Quality Distribution pie chart**
  - Point your cursor over a green, yellow or red segment; a popup indicates the # and % of calls over endpoints in the network whose quality was measured to be good, fair or poor respectively.
- **Successful/Failed Endpoints pie chart**
  - Point your cursor over a green or red segment; a popup indicates the # and % of calls over endpoints in the network whose performance was measured to be successful or failed respectively.

6.2 Assessing Health from the Network Topology Page

The Network Topology page lets you assess overall network health at a glance. The 'tree' in the left window of the page displays an aggregation of statuses in the network, up to the level of region. This is the first-level navigation window:

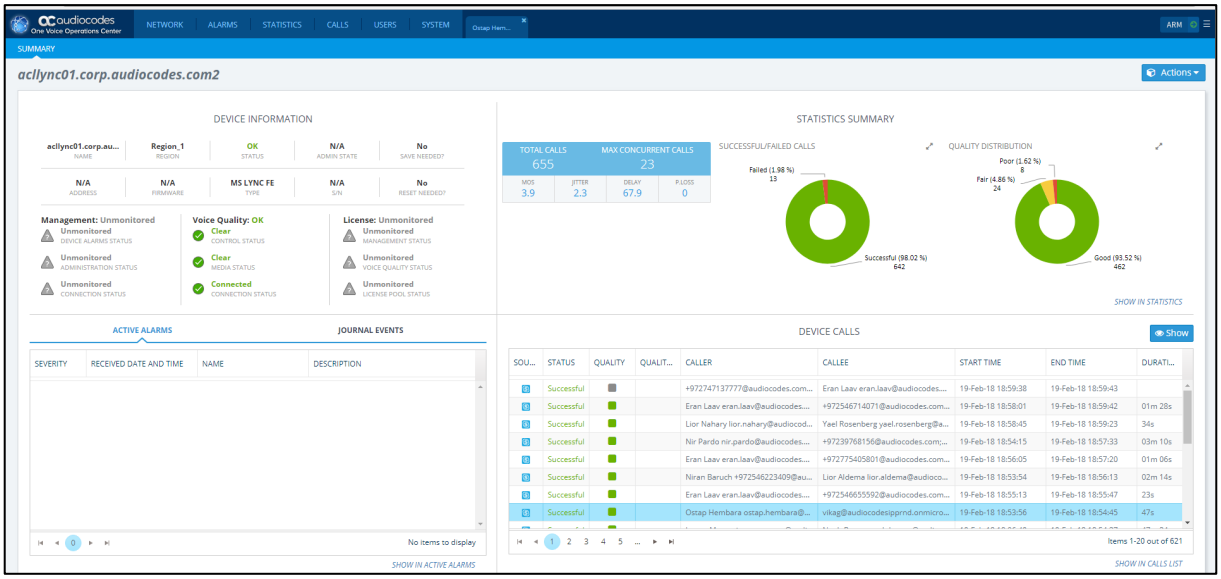


A red-coded tenant icon indicates that there is an alarm in the tenant, or that an OVOC threshold for voice quality has been exceeded in the tenant. This is the first-level navigation level.

In the middle window, a red-coded icon indicates that there is an alarm on a device, or that an OVOC threshold for voice quality has been exceeded on a device. This is the second-level navigation window:

The window lets you quickly drill down from a region to the core of an issue in a device. Very fast access to very specific information facilitates efficient network management and network optimization. For this reason, OVOC is an 'expert system'. A dynamic tab added to the menu bar provides easy future access to that specific information, facilitating troubleshooting:

Figure 6-4: Dynamic Tab for Quick Future Access to Device Information

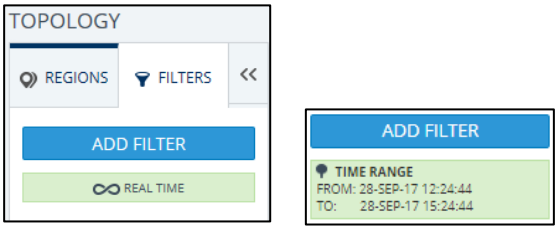


Under 'Device Calls', select a call made over that device and then click the **Show** button to display that call's details.

6.2.1 Filtering to Access Specific Information

You can filter OVOC pages to quickly access specific information. Filters let you exclude unwanted information so that only the specific information you need is displayed. An example of a filter is *Time Range*, available in the Network Topology, Alarms, Calls List and Users Experience pages.

Figure 6-5: Real Time | Time Range

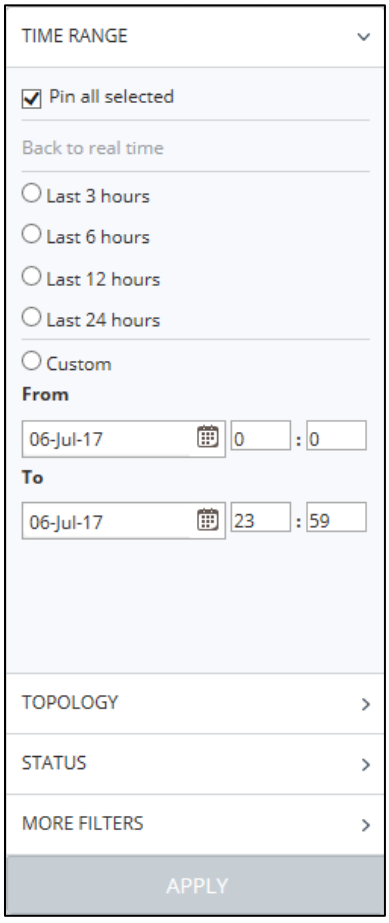


- **Real Time**. Pages by default display real time network information. Pages continuously refresh, presenting up-to-date network information – statistics|calls|history alarms - collected over the last 3 hours (default).
- **Add Filter** > **Time Range**. The page displays network information collected over a time range you specify, e.g., 10:17 - 1:17. The page is fixed. It does not keep updating and is not refreshable. See also the 'Pin all selected' feature described in Table 6-1.

6.2.1.1 Filtering by 'Time Range'

You can filter the Network Topology page and other pages by 'Time Range'. The 'Time Range' filter allows you to display *time range specific* information on the page.

Figure 6-6: Time Range Filter



Use the table below as reference.

Table 6-1: Time Range Filter

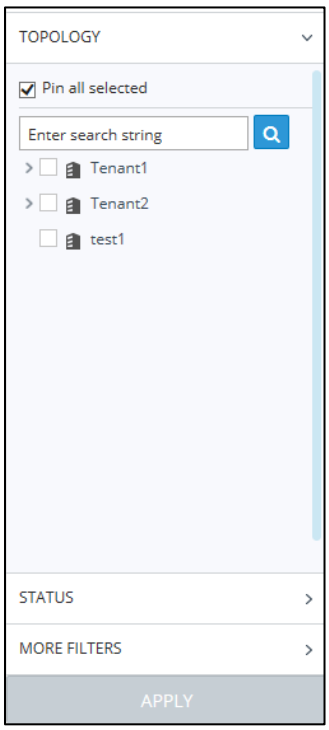
Filter Feature	Description
Pin all selected	Select this option (default) to 'preserve' the filter; the filter will remain displayed *in every page* whose tab you click. If you clear the option, the filter will only apply *locally* - to the page in which you apply the filter. The feature facilitates troubleshooting.
Back to real time	The link is enabled when you select a filter. Clicking the link removes the filter; the OVOC returns to real time.
Last 3 | 6 | 12 | 24 hours	Select one of these 'quick' filters in order to present only network data collected over the last 3 | 6 | 12 | 24 hours, to the exclusion of all other times.
Custom	Select this option to customize dates according to which to filter. Click the 'From' calendar and choose a month and day and optionally enter the time – the hour and the minutes past the hour. Click the 'To' calendar and choose a month and day and optionally enter the time – the hour and the minutes past the hour.
Apply	Click to implement the filter. To remove the filter if necessary, click the **Back to real time** link – see above.

Note: There is no limitation on the time you can define.

6.2.1.2 Filtering by 'Topology'

You can filter by 'Topology'.

Figure 6-7: Topology



Use the table below as reference.

Table 6-2: Topology Filter

Filter Feature	Description
Pin all selected	Select this option (default) in order to 'preserve' the filter; the filter will remain displayed in every screen whose tab you click. If you clear the option, the filter will only apply to the screen in which you apply the filter. The feature facilitates troubleshooting. After the filter is applied, the OVOC becomes non real time.
Search	Enter a search string. Filters out all information except for the information related specifically to the string you entered.
'Tenant'	Filters the page according to the tenant. At least one tenant is always defined – see Section 1.4 for an explanation of multi-tenancy architecture. Allows you to filter further, according to entities defined under the tenant.

6.2.1.3 Filtering by 'Status'

This section shows how to filter a page using the 'Status' filter.

The 'Status' filter applies to the pages under the **Network** menu: Topology, Devices – Manage, Links and Endpoints – Status pages.

Figure 6-8: Alarm 'Status' Filter

Use the table below as reference.

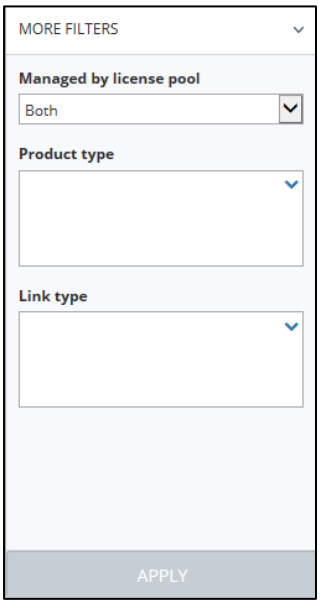
Table 6-3: Status Filter

Filter	Description
OK	Select to display entities whose status is clear (OK), color coded green, for example, indicates a tenant whose status is 'OK' and indicates a region whose status is 'OK'.
WARNING	Select to display entities whose status is warning, color coded orange, for example, indicates a tenant whose status is 'Warning' and indicates a region whose status is 'Warning'.
ERROR	Select to display entities whose status is error, color coded red, for example, indicates a tenant whose status is Error and indicates a region whose status is Error.
UNMONITORED	Select to display entities whose status is unmonitored, color coded black, for example, indicates a tenant whose status is 'Unmonitored' and indicates a region whose status is 'Unmonitored'.

6.2.1.4 Filtering by 'More Filters'

You can filter a page by 'More Filters'.

Figure 6-9: More Filters – Network Topology Page



Use the table below as reference.

Table 6-4: More Filters - Network Topology Page

Filter	Description
Managed by license pool	From the dropdown list, select either Both, Managed or Not managed.
Product type	From the dropdown list, select the product type to display on the page, or enter a search string.
Link type	From the dropdown list, select IPGroup, Trunk Group, Phone Prefix, Control IP, Media IP or Media Realm to display on the page.

6.3 Assessing Network Health in the Statistics Pages

The OVOC graphically and textually displays network-wide statistics on call performance (% and # of calls evaluated as successful or failed), voice quality (% and # of calls whose voice quality scored good, fair or poor), etc. Statistics on calls over devices, links, sites and endpoints are displayed. The pages help operators assess and optimize network health.

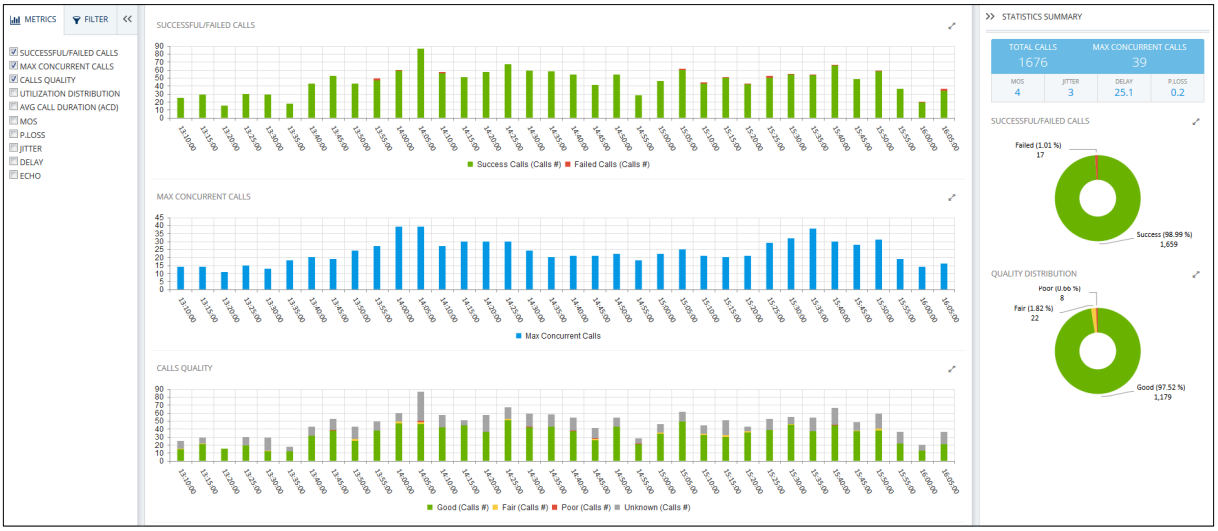
6.3.1 Viewing Statistics on Calls over Devices

The Devices tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of calls over devices.

➢ **To view statistics on calls over devices:**

- Open the Devices Statistics page (**Statistics** > **Devices**).

Figure 6-10: Devices Statistics



You can optionally filter the page by Time Range (see Section 6.2.1) and Topology (see Section 6.2.1.2).

The page displays (from L-R):

- Metrics (see Section 6.3.1.1)
- Bar Charts (see Section 6.3.1.1)
- Statistics Summary (see Section 6.3.1.2)

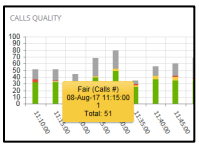
6.3.1.1 Metrics Bar Charts

Three metrics / bar charts are displayed by default:

- Successful / Failed Calls chart shows the % and # of calls whose performance was evaluated as successful or failed, distributed over time (see Section 6.2.1 for information about the time range filter). The chart lets you assess calls performance at a glance. The chart shows *when successful calls peaked* compared to *when failed calls peaked*. You can compare this to other charts to identify correlations.
- Max Concurrent Calls chart shows the maximum concurrent calls distributed over time. The chart shows *when* the maximum concurrent calls *peaked* compared to when they *dipped*. You can compare this to other charts to identify correlation. Max Concurrent Calls is the maximum number of calls opened at the same time in the server. The value can be imprecise if more than one entity is monitored and because a call is defined as opened two seconds after it closes.
- Calls Quality chart shows the distribution of voice quality (% and # of calls whose voice

quality scored ■ Good ■ Fair or ■ Poor) over time. Gray indicates 'Unknown' voice quality. Point the cursor over a color-coded bar segment in any time period to view this popup. The date and time indicates when the period ended.

Figure 6-11: Calls Quality Bar Chart

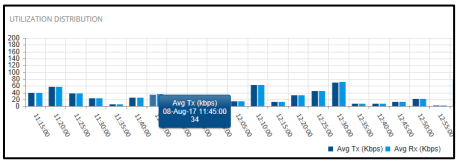


Compare charts. If, for example, you identify a correlation over time between 'Poor' voice quality and Jitter, then Jitter is the reason for the poor voice quality.

Other metrics / bar charts that you can select and display:

- Utilization Distribution chart shows distribution of the media packets network utilization over time. A glance shows when a high rate (in Kbps) was received or transmitted (Rx/Tx rate in Kbps). The chart shows when a network is congested or uncongested, i.e., when voice quality scores may be lower. To view information on a time period, position the cursor over the bar representing the time period; the popup shows the date and time on which the period ended and the Rx / Tx rate in Kbps and the kilobits consumed per second during the time period:

Figure 6-12: Utilization Distribution Bar Chart



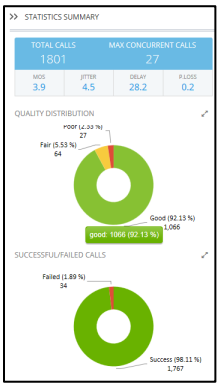
- Average Call Duration (ACD) chart shows distribution of ACD in the network over time. Point your mouse over a bar to determine average call duration in that time interval.
- MOS chart. Point your mouse over a bar to determine the average MOS scored in that time interval.
- Packet Loss chart. Point your mouse over the time axis to determine the average packet loss, as a percentage of the total number of packets sent, measured at that time. Packet Loss can be more than 100%.
- Jitter chart. Point your mouse over the time axis to determine the average jitter measured at that time, in milliseconds.
- Delay chart. Point your mouse over a bar to determine the average delay measured in that time interval, in milliseconds.
- Echo chart. Point your mouse over the time axis to determine the precise average echo measured at that time, in DB.

For more information about these voice quality metrics, see under Table 8-5.

6.3.1.2 Statistics Summary

On the right side of the Devices Statistics page, you can view the Statistics Summary pane.

Figure 6-13: Statistics Summary



The pane displays

- the total # of calls made over devices in the time period
- the maximum concurrent calls measured over devices in the time period
- the values of MOS, Jitter, Delay and Packet Loss quality metrics measured over devices in the time period

The pane also displays two metrics as pie charts:

- Quality Distribution pie chart. Point your mouse over a segment of the color-coded pie chart to determine the # and % of calls whose voice quality scored ■ Good ■ Fair or ■ Poor in that time interval.
- Successful/Failed Calls pie chart. Point your mouse over a segment of the color-coded pie chart to determine the # and % of calls that were evaluated as Successful ■ or Failed ■ in that time interval.

6.3.2 Viewing Statistics on Streams over Links

The Links tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of streams over links. Information in the page is presented identically to information in the Devices Statistics page, described under Section 6.3.1). You can optionally filter the page by Time Range (see Section 6.2.1) and Topology (see Section 6.2.1.2).

6.3.3 Viewing Statistics on Calls over Sites

The Sites tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of calls over sites. Information in the page is presented identically to information in the Devices Statistics page, described under Section 6.3.1). You can optionally filter the page to display only the information that you require. You can filter by Time Range (see Section 6.2.1) and Topology (see Section 6.2.1.2).

6.3.4 Viewing Statistics on Calls over Endpoints

The Endpoints tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of calls over endpoints. Information in the page is presented identically to information in the Devices Statistics page, described under Section 6.3.1). You can optionally filter the page to display only the information that you require. You can filter by Time Range (see Section 6.2.1) and Topology (see Section 6.2.1.2).

6.4 Determining Network Health from Alarms

The Active Alarms page facilitates management of all alarms currently active in the IP telephony network. Management includes performing actions such as deleting, acknowledging and saving alarms to file, as well as monitoring active alarms in the network to determine network health.

6.4.1 Configuring Alarm Settings

For information on how to configure the way alarms and events are displayed in the Alarms pages, see Section 4.1.3.

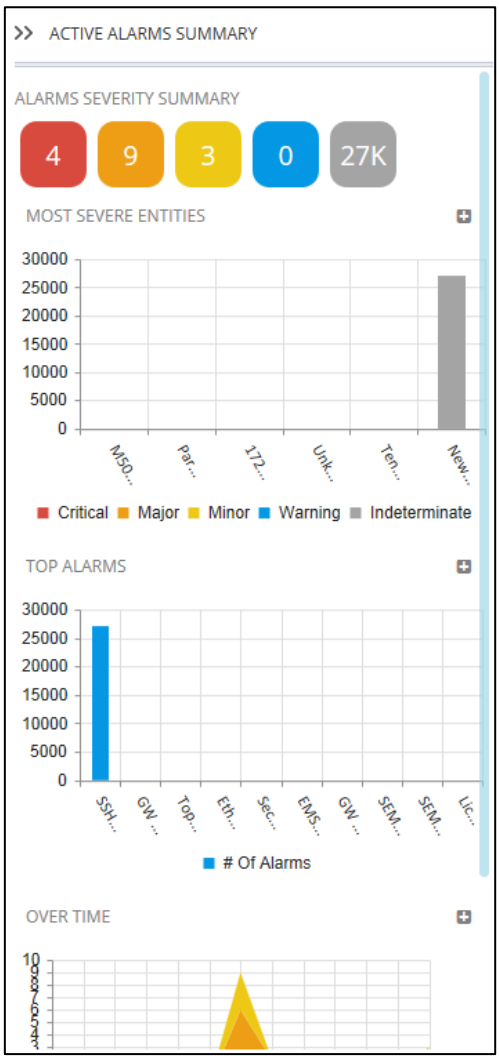
6.4.2 Monitoring Active Alarms to Determine Network Health

The Active Alarms page's Active Alarm Summary pane lets you effectively monitor all the active alarms of all severities in the IP telephony network.

➢ **To monitor the active alarms:**

1. Open the Active Alarms page (**Alarms** > **Active**) and locate the Active Alarms Summary pane on the right side of the page.

Figure 6-14: Active Alarms Summary



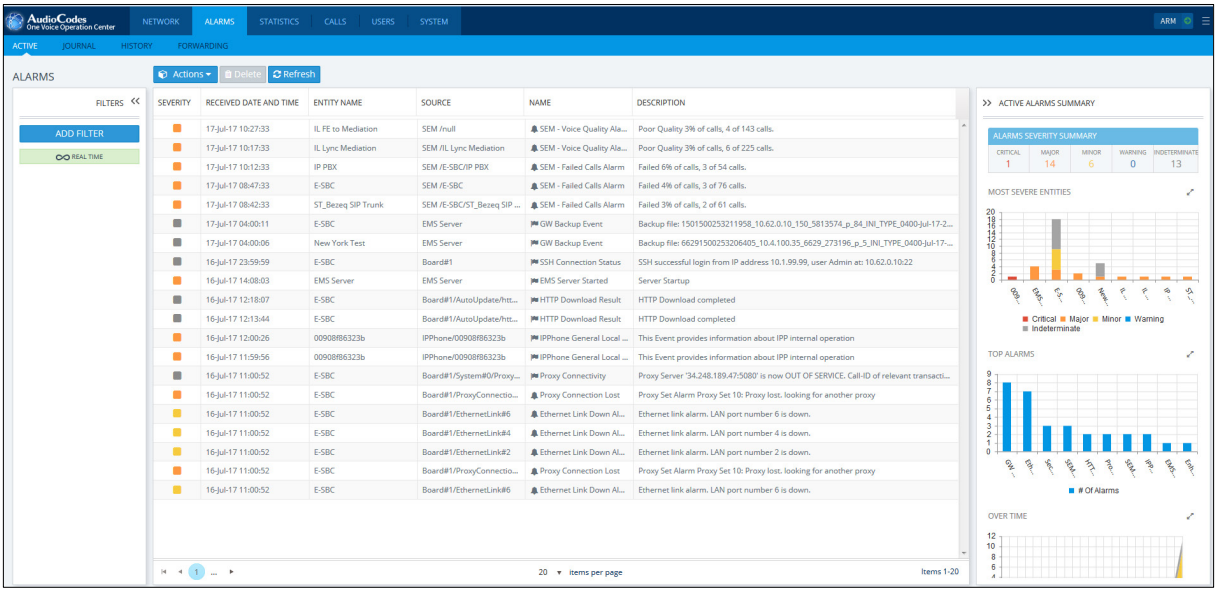
6.4.3 Performing Management Actions on Active Alarms

The Active Alarms page lets you perform management actions on all alarms currently active in the network, including deleting, acknowledging, and saving alarms to file.

➢ **To perform management actions on active alarms:**

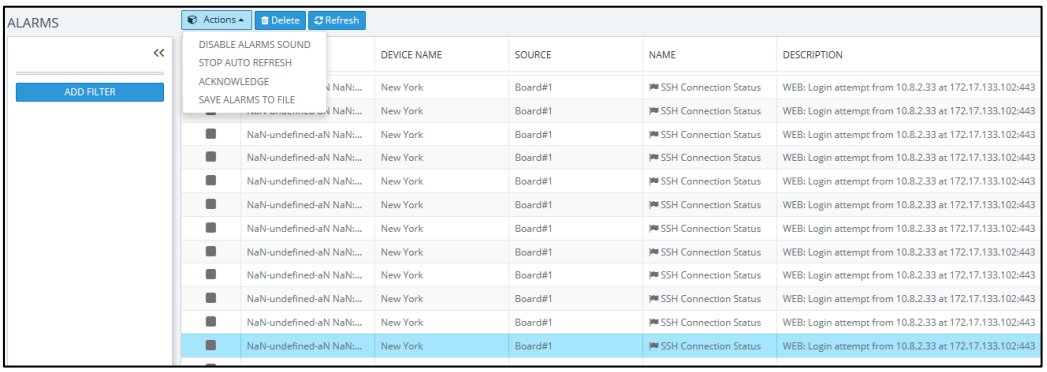
1. Open the Active Alarms page (**Alarms** > **Active**).

Figure 6-15: Alarms - Active



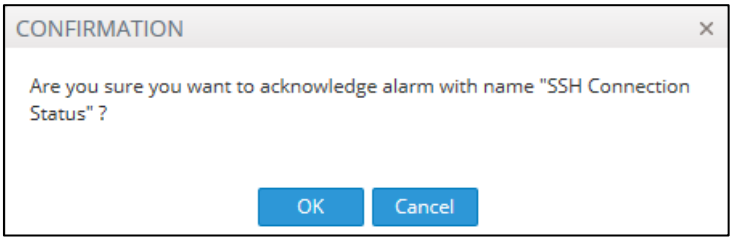
2. Optionally filter the page by Topology (see Section 6.2.1.2), Severity (see Section 6.2.1.3), Source Type (see Section 6.4.3.1), or More Filters (see Section 6.4.3.3), and then select an alarm alarm or multiple alarms and click **Actions**.

Figure 6-16: Alarms - Actions



3. Select **Acknowledge** to acknowledge an alarm.

Figure 6-17: Acknowledge Alarm Confirmation

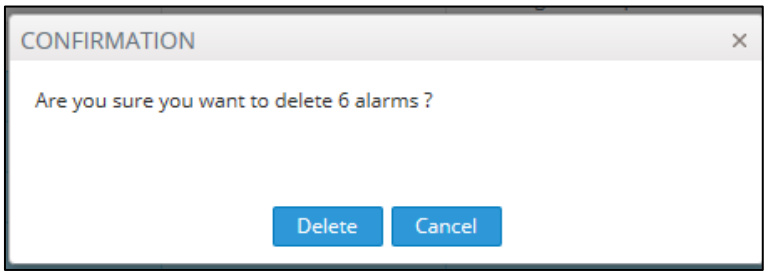


4. Select **Save Alarms to File** to save alarms to file for future reference.

➢ **To delete an alarm or multiple alarms:**

- In the Active Alarms page, select the alarm or multiple alarms to delete, and click the **Delete** button.

Figure 6-18: Delete Alarms Confirmation



➢ **To refresh the page:**

- In the Active Alarms page, select **Refresh**.

➢ **To enable audial alert on incoming alarms:**

- From the **Actions** dropdown, select **Enable Alarms Sound**.

➢ **To disable audial alerts:**

- From the **Actions** dropdown, select **Disable Alarms Sound**.

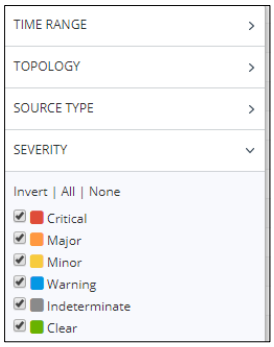
➢ **To stop automatic refresh:**

- From the **Actions** dropdown, select **Stop Automatic Refresh**.

6.4.3.1 Filtering by 'Severity'

The 'Severity' filter applies to the pages under the **Alarms** menu: Active, Journal and History pages.

Figure 6-19: Alarm 'Severity' Filter



The 'Severity' filter lets you select

- one severity level
- more than one severity levels
- all severity levels (**All**)
- no severity levels (**None**)

The 'Severity' filter also lets you *invert* a selection (**Invert**). If you select **Invert** after filtering (for example) for

- **All**, then all severity levels previously selected will be cleared.
- **None**, then all severity levels previously cleared will be selected.
- **Critical**, then the 'Critical' severity level previously selected will be cleared and all other levels will be selected.

Use the table below as reference.

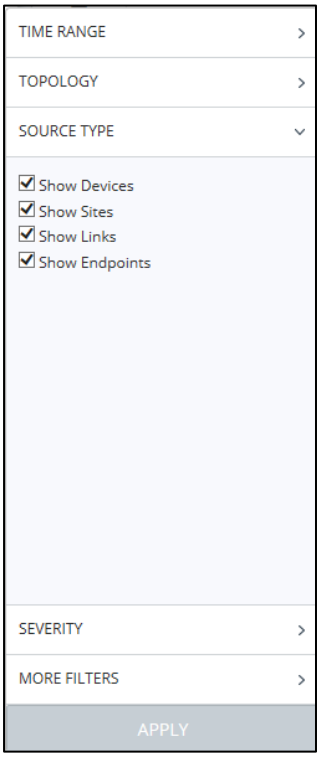
Table 6-5: Severity Filter

Filter	Description
Critical	Select to display entities whose alarm severity level is critical, color coded red.
Major	Select to display entities whose alarm severity level is major, color coded orange.
Minor	Select to display entities whose alarm severity level is minor, color coded yellow.
Warning	Select to display entities whose alarm severity level is warning, color coded blue.
Indeterminate	Select to display entities whose alarm severity level is indeterminate, color coded black.
Clear	Select to display entities whose alarm severity level is clear, color coded green.

6.4.3.2 Filtering by 'Source Type'

This section shows how to filter a page using the 'Source Type' filter. The filter applies to the Calls List page under the Calls menu and the Alarms pages. The filter lets you display calls according to the *entity from which* the calls reported to the OVOC.

Figure 6-20: 'Source Type' Filter



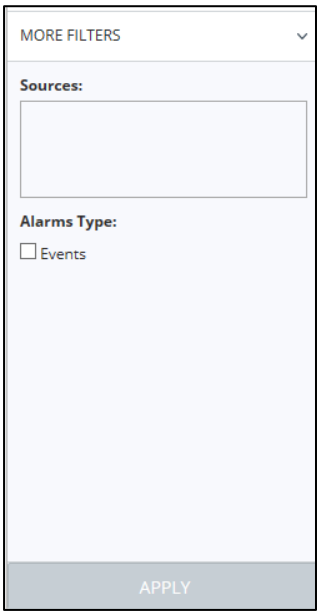
Use the table below as reference.

Table 6-6: 'Source Type' Filter

Filter	Description
Show Devices	Displays only calls whose report was sent to the OVOC *from devices*.
Show Sites	Displays only calls whose SIP Publish report was sent by endpoints to the OVOC *from sites*.
Show Links	Displays only calls transmitted *through links*.
Show Endpoints	Displays only calls whose SIP Publish report was sent to the OVOC *from endpoints*.

6.4.3.3 Filtering by 'More Filters'

Figure 6-21: More Filters – Alarms Active Page



Use the table below as reference.

Table 6-7: More Filters – Alarms Active Page

Filter	Description
Sources	Enter the name of the entity from which the alarm originated.
Alarm Type	Select the 'Events' option for the page to display only alarms that are of type events.

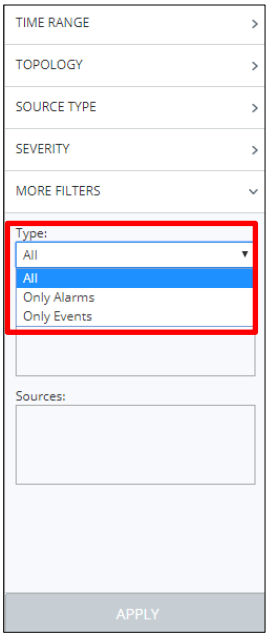
6.4.3.4 Filtering by 'Type'

The 'Type' filter augments existing filtering capability in the Alarms – Active page; you can filter the page for 'Only Alarms' or 'Only Events'.

➢ **To filter for 'Type':**

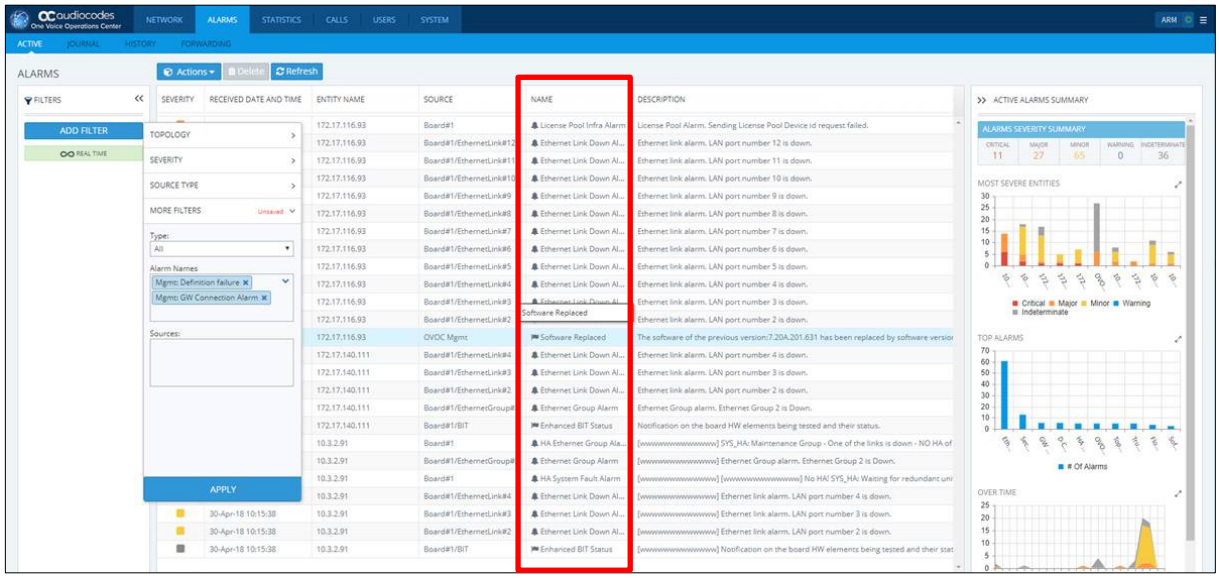
1. In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Type' dropdown, select **All**, **Only Alarms** or **Only Events**.

Figure 6-22: Type Filter



2. In the 'Name' column in the Active Alarms page, you can view:
   - Bell icons, if you filtered for 'Only Alarms'
   - Flag icons, if you filtered for 'Only Events'

Figure 6-23: Active Alarms - Type Filter

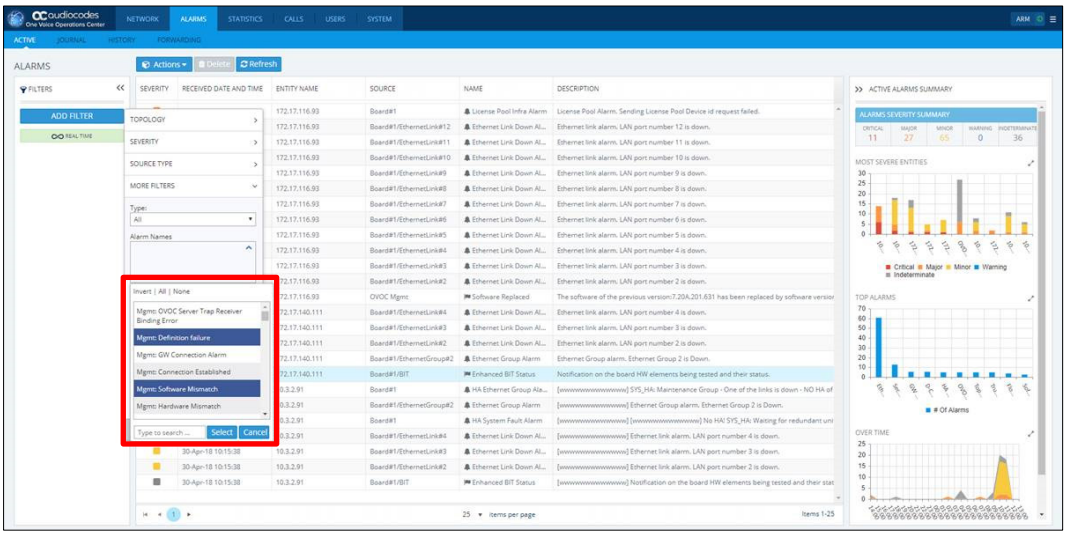


6.4.3.5 Filtering by 'Alarms Name'

The 'Alarms Name' filter augments already existing filtering capability in the Active Alarms page; you can filter the page by alarm name.

➢ **To filter by 'Alarms Name':**

- In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Alarms Name' dropdown, select the filter.

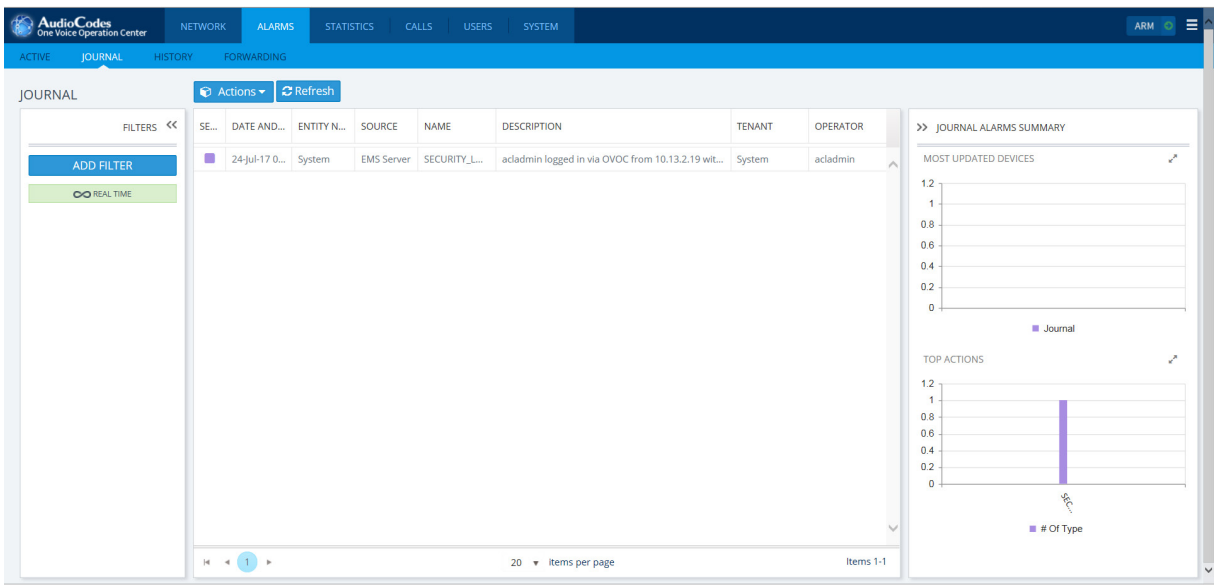


- In the Alarms Forwarding Rule screen (**Alarms** > **Forwarding** > **Add**), click the tab **Rule Conditions** and then from the 'Alarm Names' dropdown, select the alarm.

6.4.4 Viewing Journal Alarms to Determine Operator Responsibility

The Journal Alarms page lets you view actions of operators performed historically in the OVOC up to the present. The page can help you determine if operator activity may have been responsible for an active alarm. You can then reference the History page to verify correlation (see Section 6.4.5).

Figure 6-24: Journal Alarms



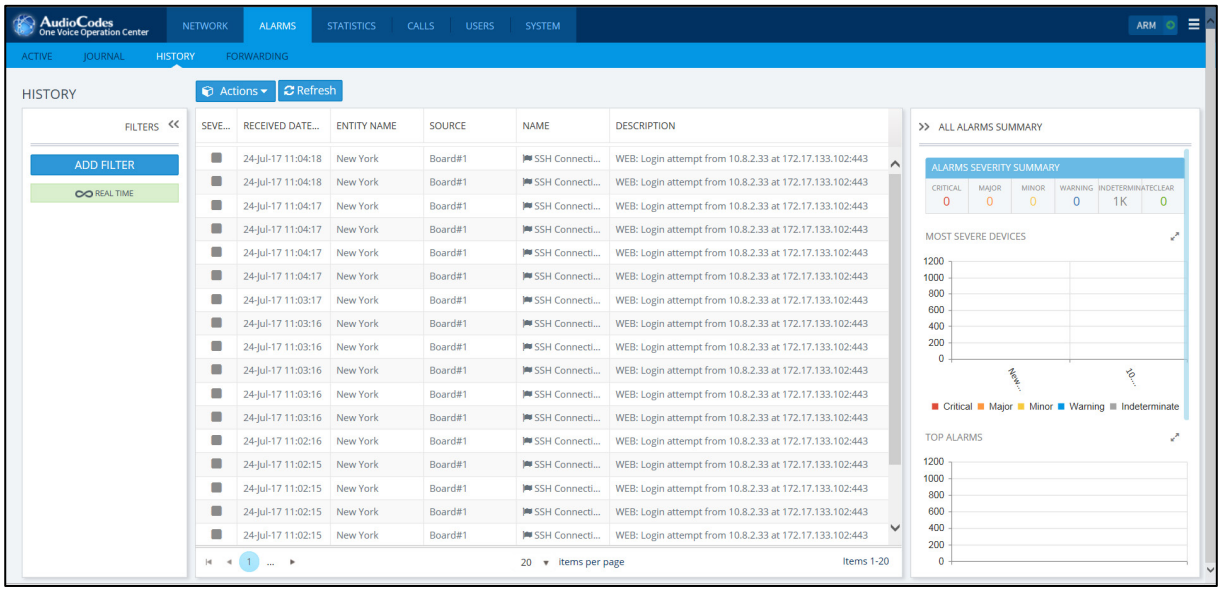
6.4.5 Viewing History Alarms

The History page displays historical alarms. The page can help you verify that an operator's action was responsible for an active alarm.

➢ **To determine if an operator's action was responsible for an active alarm:**

1. Open the History page (**Alarms** > **History**).

Figure 6-25: Alarms - History



2. Click **Add Filter** to filter the page according to Topology, Time Range, Severity or More Filters. For a full description of these filters, see under Section 6.2.1.

Figure 6-26: Alarms Page Filters

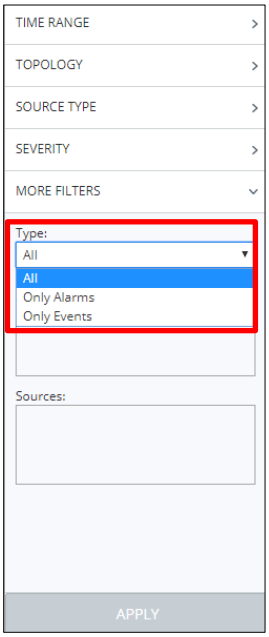
6.4.5.1 Filtering by 'Type'

The 'Type' filter augments existing filtering capability in the History Alarms page; you can filter the page for 'Only Alarms' or 'Only Events'.

➢ **To filter for 'Type':**

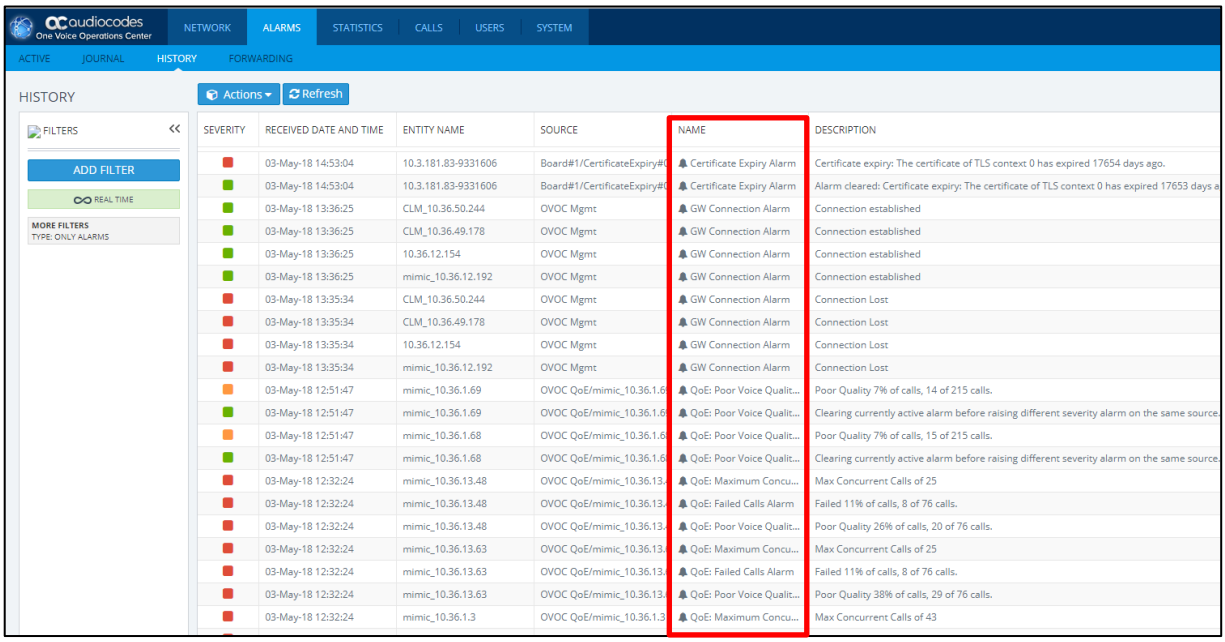
1. In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Type' dropdown, select **All**, **Only Alarms** or **Only Events**.

Figure 6-27: Type Filter



2. In the 'Name' column in the Alarms History page, you can view:
   - Bell icons, if you filtered for 'Only Alarms'
   - Flag icons, if you filtered for 'Only Events'

Figure 6-28: History Alarms - Type Filter

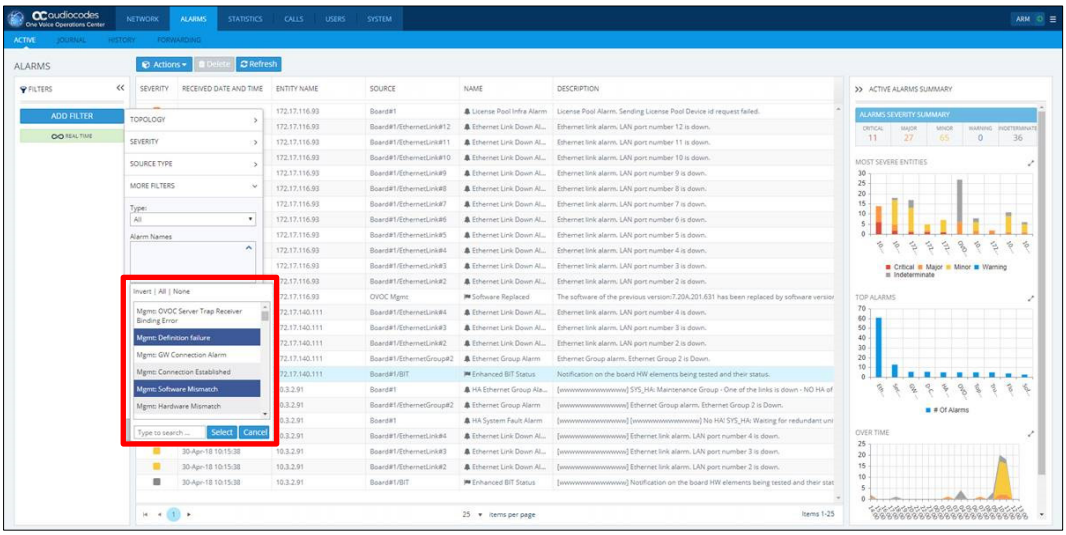


6.4.5.2 Filtering by 'Alarms Name'

The 'Alarms Name' filter augments already existing filtering capability in the History Alarms page; you can filter the page by alarm name.

➢ **To filter by 'Alarms Name':**

1. In the Alarms History page, click **Add Filter**, choose **More Filters** and then from the 'Alarms Name' dropdown, select the filter.



2. In the Alarms Forwarding Rule screen (**Alarms** > **Forwarding** > **Add**), click the tab **Rule Conditions** and then from the 'Alarm Names' dropdown, select the alarm.

6.4.6 Forwarding Alarms

The Forwarding page lets you add an alarm forwarding rule. The OVOC can forward alarms to multiple destinations in these formats:

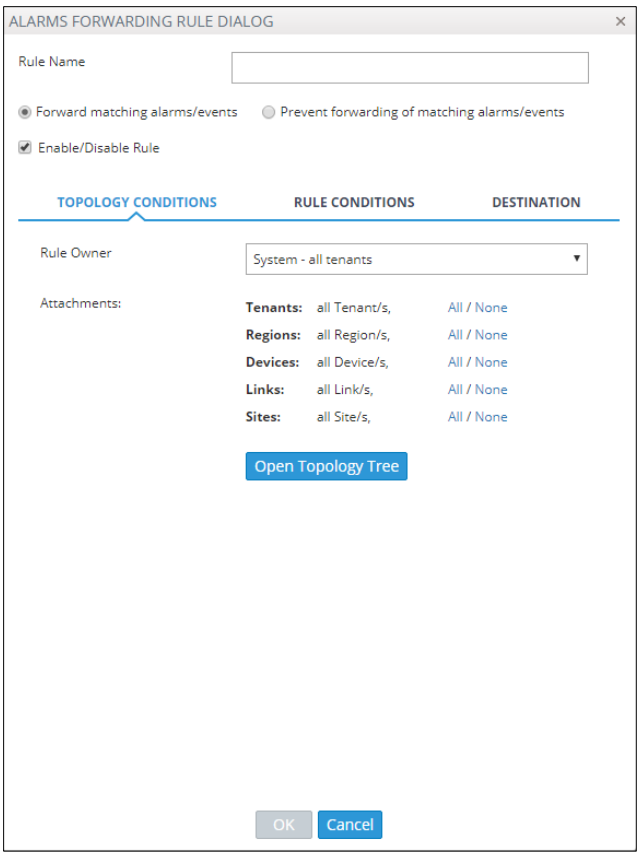
- SNMP Notifications (SNMP 1 / SNMP 2)
- External Mail / Internal Mail
- Syslog

This section shows how to configure these alarm forwarding options.

➢ **To forward alarms:**

1. Open the Alarms Forwarding page (**Alarms** > **Forwarding**).

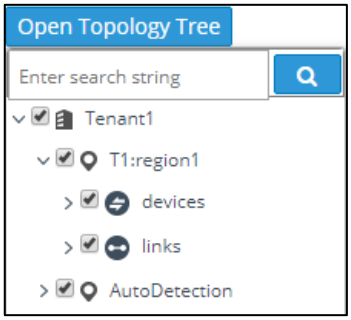
Figure 6-29: Alarms Forwarding – Topology Conditions



2. Configure parameters using Table 6-8 below as reference:

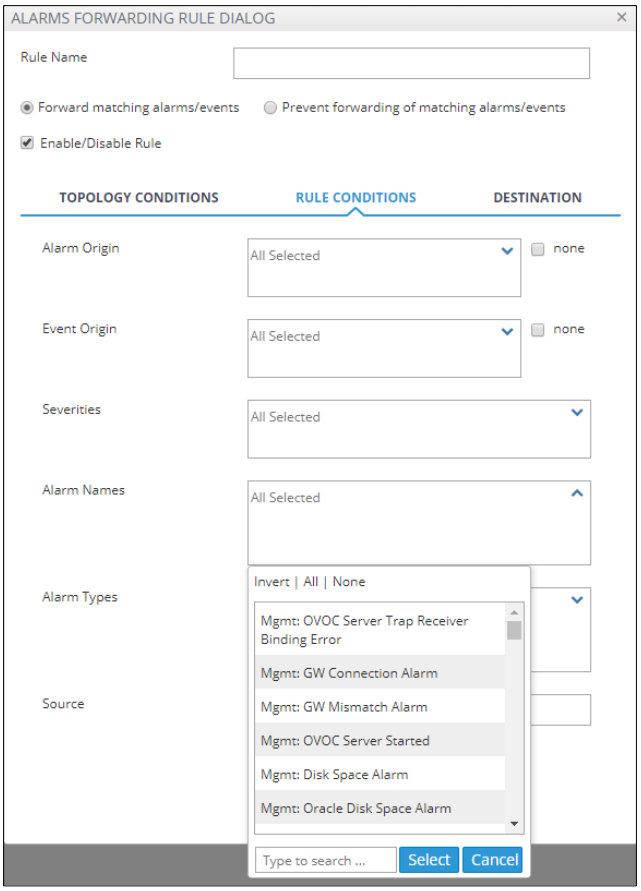
Table 6-8: Alarms Forwarding – Topology Conditions

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	Allows or prevents forwarding alarms depending on the destination you select. If you select **Prevent forwarding matching alarms/events** and then select **Minor Alarms** from the 'Severities' dropdown under the **Rule Conditions** tab, then minor alarms are not forwarded.
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under **Rule Conditions** and **Destinations** are met.

Parameter	Description
Rule Owner	From the dropdown, select **System – all tenants**; the rule will then apply to *all tenants* and to all regions/links/devices/sites under all tenants. Here's what you'll then view next to 'Attachments': **all Tenant/s, all Region/s, all Device/s, all Link/s, all Site/s** If you select *a specific tenant* from the dropdown, the rule will apply by default to *all* entities *under that specified tenant*. Click **Open Topology Tree** and then click **>** to view the entities under that tenant and if you want, to change the default.  Only the operator assigned to that tenant can view and change it. The **All**/**None** filters next to 'Attachments' allow you to quickly specify to which entities rule forwarding will apply, if not to all.

3. Click the **Rule Conditions** tab.

Figure 6-30: Alarms – Forwarding – Rule Conditions



4. Configure the screen using the table below as reference.

Table 6-9: Forwarding Alarms – Rule Conditions - Parameter Descriptions

Parameter	Description
Alarm Origin	Select the origin from which alarms will be forwarded: • Management • QoE • Devices • Endpoints
Event Origin	Select the origin from which events will be forwarded: • Management • QoE • Devices • Endpoints
Severities	From the 'Severities' dropdown, select the severity level of the alarms you want to receive: • Warning • Minor • Major • Critical • Indeterminate Default: All Selected.
Alarm Names	Allows forwarding alarms according to specific alarm names. For example, if you select **Power Supply Failure** then only this alarm will be forwarded. Default: **All Selected**. The search field lets you find an alarm according to name or origin.
Alarm Types	Allows forwarding alarms according to specific alarm types. For example, if you select **communicationsAlarm** then only this alarm type will be forwarded. Default: **All Selected**. The search field lets you find an alarm according to type.
Source	Free text box that allows you to filter according to alarms' 'Source' field (identical to the 'Source' column displayed in the Alarms History page).

5. Click the **Destination** tab.

6.4.6.1 Forwarding Alarms whose Destination is 'SNMP'

The SNMP forwarding option is typically used for integration of the OVOC with a Network Management System (NMS).

For more information about forwarding SNMP notifications, see the *OAM Integration Guide*.

After selecting the **Destination** tab, the screen whose destination type is SNMP v2 or SNMP v3 opens by default (see the figures on the next page).

Use the table below as reference for the 'Destination Type' parameter.

Table 6-10: Forwarding Alarms – Destination

Parameter	Description
Destination Type	Determines the format in which the alarm or event will be forwarded. From the dropdown, select • SNMP (default) ✓ SNMP v2 ✓ SNMP v3 • MAIL • SYSLOG

Figure 6-31: Alarms – Forwarding – Destination Type - SNMP v2

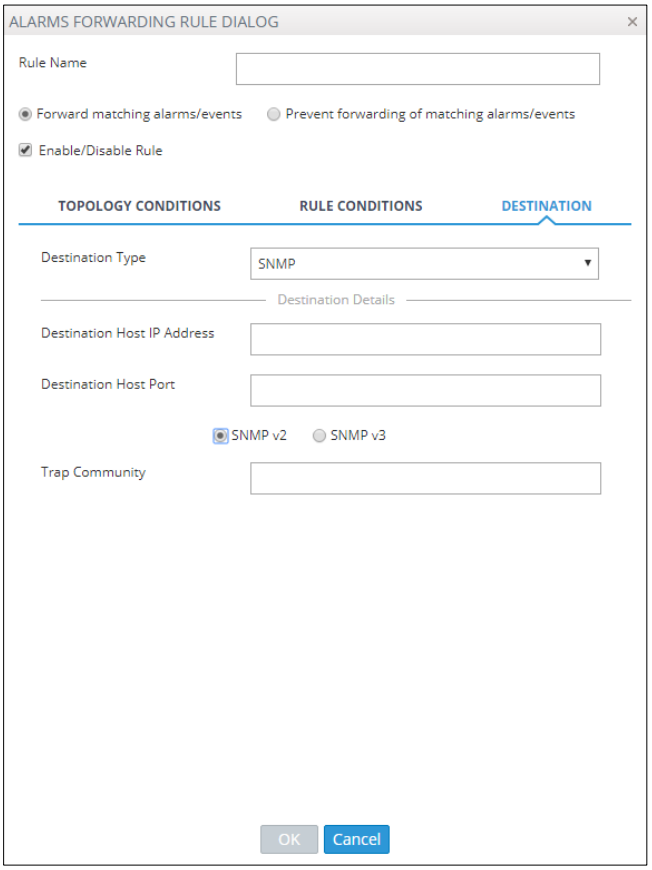
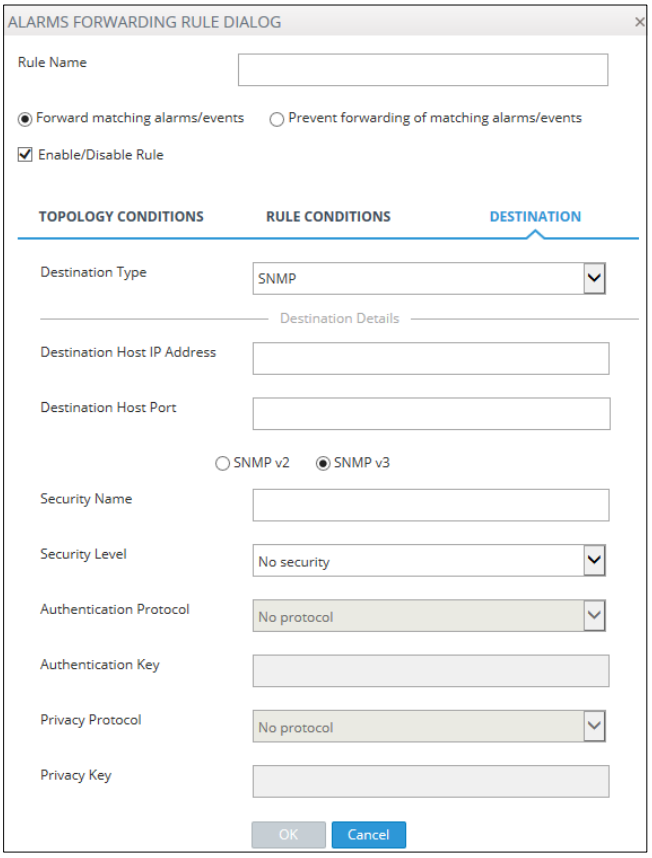


Figure 6-32: Alarms – Forwarding – Destination Type - SNMP v3



6.4.6.1.1 Forwarding Alarms whose Destination Type is 'Syslog'

Syslog features a well-defined message format structure detailed in RFC 3164. The OVOC'S severity levels are adjusted to the severity levels of the Syslog protocol. The table below maps the two:

Table 6-11: OVOC-Syslog Severity Levels Mapping

EMS Severity	Syslog Severity
Critical	Alert
Major	Critical
Minor	Error
Warning	Warning
Indeterminate	Informational
Clear	Notice

The message part of the Syslog protocol contain this structure:

```
Title: <Alarm/Event> <Alarm Name>, received from <Node Name, Node IP> with Severity <Severity>.
Description: <Source>, <Description>
```

If the alarm is forwarded from the source global IP address in an HA configuration, the device IP is the global IP address.

6.4.6.1.2 Forwarding Alarms whose Destination Type is 'Mail'

➢ **To forward alarms whose destination is 'Mail':**

1. From the 'Destination Type' dropdown, select **MAIL**.

Figure 6-33: Alarms – Forwarding – Destination – Mail

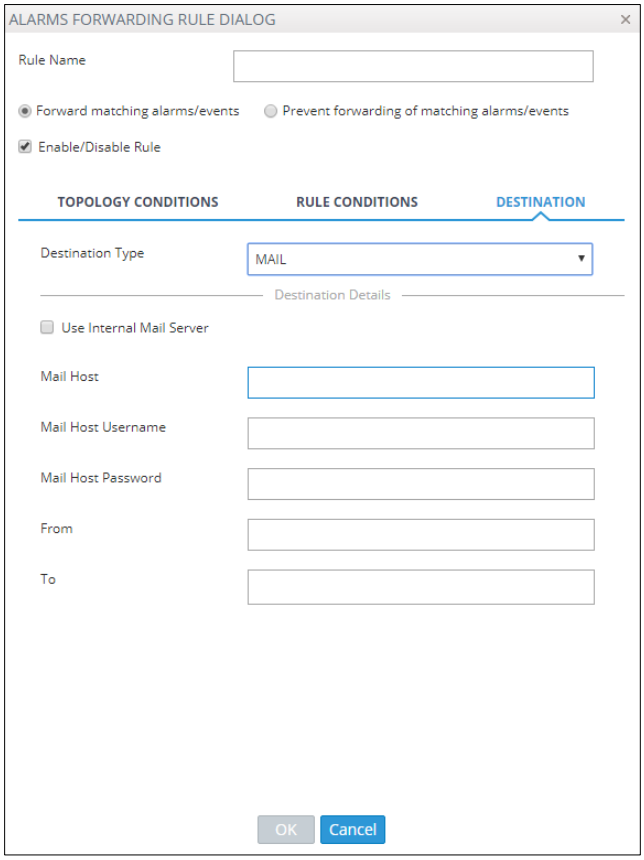
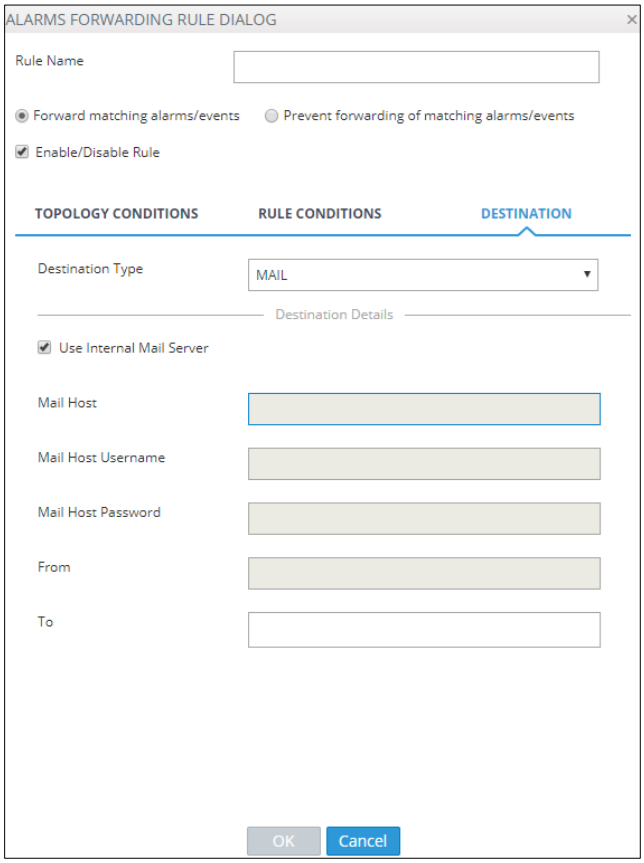


Figure 6-34: Alarms – Forwarding – Destination – Mail – Use Internal Mail Server



2. Configure the parameters using the table below as reference.

Table 6-12: Forwarding Alarms - Destination – Mail

Parameter	Description
Use Internal Mail Server	If this option is selected, all the fields in this table below will be deactivated, except the 'To' field. If selected, it'll only be necessary to configure the internal mail server as the destination to which to forward alarms; it'll be unnecessary to configure a mail host. If the option is cleared, all the fields in this table below will be activated.
Mail Host	Enter the **Mail Host IP address or FQDN (e.g.**, smtp.office365.com).
Mail Host Username	Enter the **mail host username**.
Mail Host Password	Enter the **mail host password**.
From	Enter the **e-mail address** the recipient will see when the mail arrives.
To	Enter the **list of email addresses** (coma separated) to which to send mail. If the option 'Use Internal Mail Server' is selected, 'To' will be the only parameter activated; all others will be deactivated. In this case, configure the internal mail server as the destination to which to forward alarms.

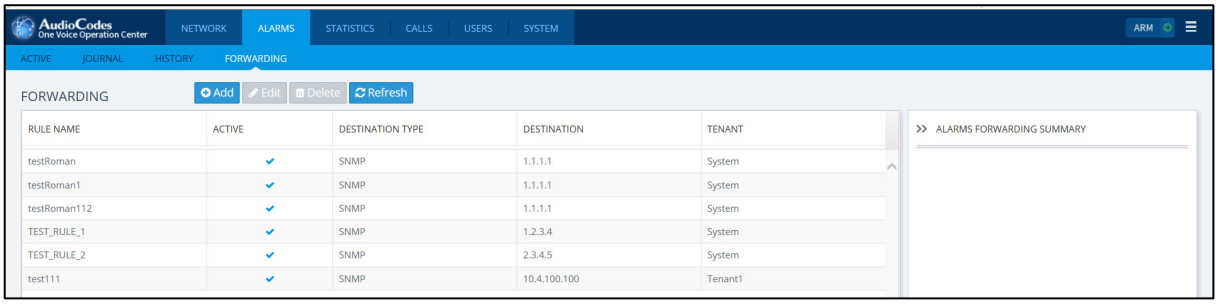
3. Click **OK**; alarms are forwarded to specified email destinations in the following email format:

```
Title: New <Alarm/Event> <Alarm Name>, received from <Node Name> with Severity <Severity>
Message body: will include all the fields we have today in Alarm Item
```

6.4.6.2 Viewing the New Rules in the Alarms Forwarding Page

The new rules are displayed in the Alarms Forwarding page (**Alarms** > **Forwarding**):

Figure 6-35: New Rules in the Alarms Forwarding Page



This page is intentionally left blank.

7 Managing your Network

This section shows how to manage your network using the OVOC.

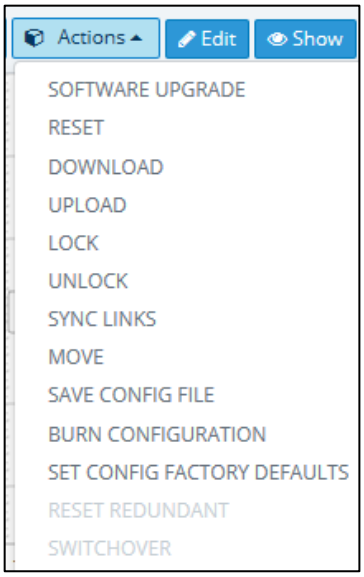
7.1 Performing Management Actions

The OVOC lets operators perform multiple network management actions in the network.

➢ **To perform a management action:**

1. Open the Network page under the **Topology** tab - for example.
2. Select a device or a link on which to perform an action; the **Actions** button, **Edit** button, **Show** button and **Delete** button are activated.

Figure 7-1: Actions | Edit | Show



- Software Upgrade (see Section 7.1.1)
- Upgrading Software on Multiple Devices (see Section 7.1.2)
- Reset (see Section 7.1.3)
- Download (restore a device's configuration) (see Section 7.1.4)
- Upload (back up a device's configuration) (see Section 7.1.5)
- Lock or Unlock (see Section 7.1.6)
- Sync Links (see Section 7.1.7)
- Move a device (see Section 7.1.8)
- Save Config File (see Section 7.1.9)
- Burn Config File (see Section 7.1.10)
- Set Config Factory Defaults (see Section 7.1.11)
- Reset Redundant (see Section 7.1.12)
- Switchover (see Section 7.1.13)
- Show device information (see Section 7.1.14)
- Show link information (see Section 7.1.15)
- Show user information (see Section 7.1.16)
- Edit a device (see Section 7.1.17)
- Delete a device (see Section 7.1.18)

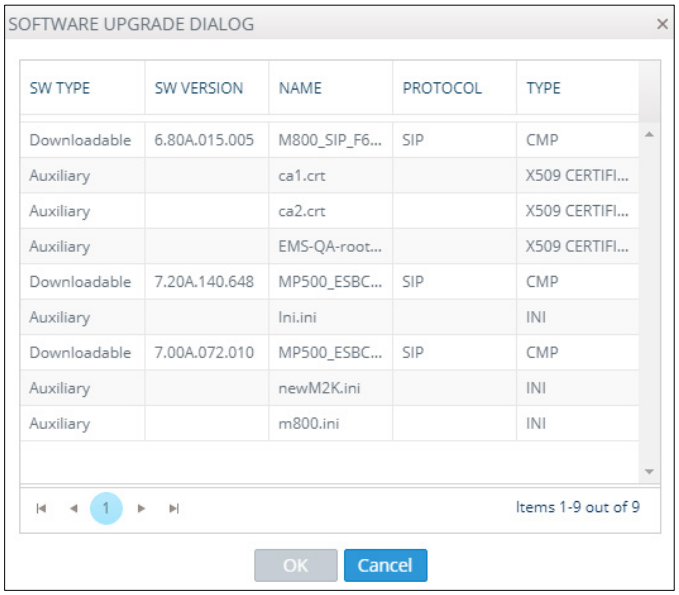
7.1.1 Upgrading Device Software

The OVOC lets you upgrade a device's .cmp software version file. After loading the .cmp file to the device, you can also load an *ini* file and Auxiliary files (e.g., CPT file).

➢ **To upgrade a device:**

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up, as shown above.
2. Click the **More Actions** link and then click the now-displayed **Software Upgrade** icon; the Software Upgrade dialog opens.

Figure 7-2: Software Upgrade



3. Select the software file and click **OK**.

7.1.2 Upgrading Software on Multiple Devices

The OVOC lets you upgrade the .cmp software version file on multiple devices. After loading the .cmp file to the devices, you can also load an *ini* file and Auxiliary files (e.g., CPT file).

➢ **To upgrade software on multiple devices:**

- In the Network Topology page, select the devices whose software you want to upgrade (Ctrl + click devices) and then from the 'Actions' dropdown select **Software Upgrade**. Alternatively, in the Devices Manage page, select the devices whose software you want to upgrade (Ctrl + click devices) and then from the 'Actions' dropdown select **Software Upgrade**.

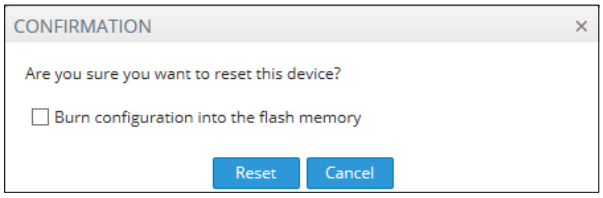
7.1.3 Resetting a Device

For certain settings to take effect a device reset is required. Resetting a device may also be necessary for maintenance purposes.

➢ **To reset a device:**

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up, as shown above.
2. Click the **More Actions** link and then click the now-displayed **Reset** icon.

Figure 7-3: Resetting the Device



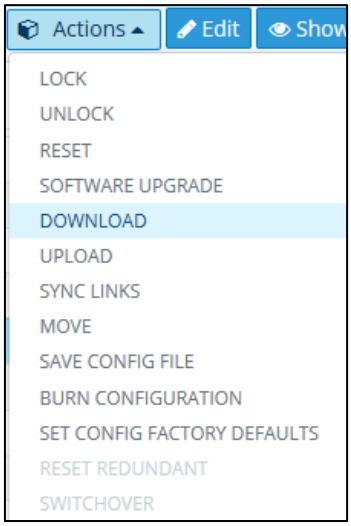
3. [Optional] Select the **Burn configuration into the flash memory** option.
   - If you select the option, the current configuration will be saved (*burned*) to flash memory prior to reset.
   - If you do not select the option, the device resets without saving the current configuration to flash and all configuration performed after the last configuration save will be discarded (lost) after reset.
4. Click **Reset**.

7.1.4 Downloading the Backup Software Configuration File to the Device

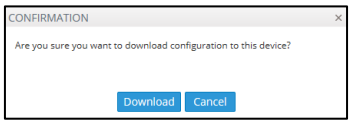
You can restore or download the latest software configuration file, backed up on the server, to the device.

➢ **To download the latest backup software configuration file to the device:**

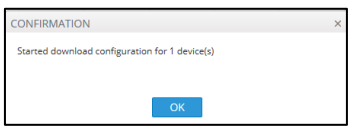
1. Open the Devices page (**Network** > **Devices**) and select the device to which to restore the latest backed-up software configuration file.
2. Click **Actions**.



3. From the menu, select **Download**.



4. In the Confirmation prompt, click **Download**.



5. Click **OK**; the latest file is downloaded to the device from the server.

Note:

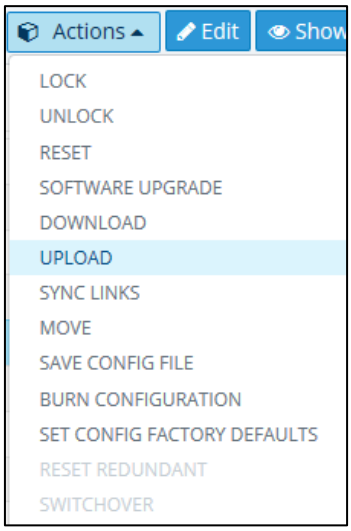
- If the device selected is an AudioCodes MSBR, the latest cli file is downloaded.
- If the device selected is an AudioCodes MP-202 or MP-204, the latest conf file is downloaded.
- If the device selected is any other AudioCodes device (except CloudBond), the latest ini file is downloaded.

7.1.5 Uploading the Device's Configuration File to the Server

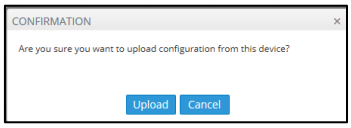
You can upload a device's software configuration file from the device to the server.

➢ **To upload a device's software configuration file from the device to the server:**

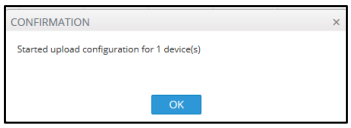
1. Open the Devices page (**Network** > **Devices**) and select the device from which to upload the software configuration file to the server.
2. Click **Actions**.



3. From the menu, select **Upload**.



4. In the Confirmation prompt, click **Upload**.



5. Click **OK**; the latest file is uploaded to the server from the device.

Note:

- If the device selected is an AudioCodes MSBR, the latest cli file is uploaded.
- If the device selected is an AudioCodes MP-202 or MP-204, the latest conf file is uploaded.
- If the device selected is any other AudioCodes device (except CloudBond), the latest ini file is uploaded.

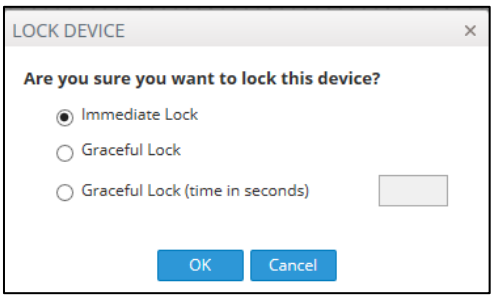
7.1.6 Locking or Unlocking a Device

Locking a device suspends call functionality and places the device in maintenance state, for troubleshooting, for example. Unlock returns it to service.

➢ To lock a device:

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up, as shown in Figure 7-1.
2. Click **More Actions** and then click the **Lock** icon.

Figure 7-4: Lock Device

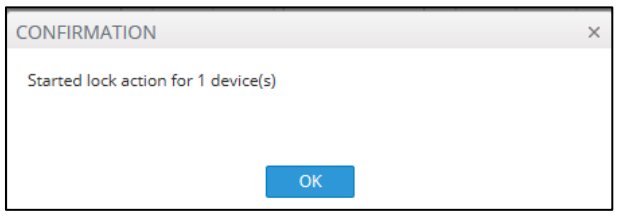


3. Select either:
   - **Immediate Lock**. The device is locked regardless of traffic. Any existing traffic is terminated immediately.
   - **Graceful Lock**. Existing calls first complete and only then is the device locked. No new traffic is accepted.
   - **Graceful Lock (time in seconds)**. The device is locked only after the time configured in the adjacent field. During this time, no new traffic is accepted. If no traffic exists and the time has not yet expired, the device locks immediately.

Note: These options are available only if the current status of the device is in "UNLOCKED" state.

4. Click **OK**.

Figure 7-5: Lock Confirmation



If you selected **Immediate Lock**, the lock process begins immediately. The device does not process any calls.

If you selected **Graceful Lock**, a lock icon is displayed and a window appears displaying the number of remaining (unfinished) calls and time.

➢ To unlock the device:

- In the Network Topology page, position your cursor over the device and from the Actions menu shown above, click the **More Actions** link. Click the now-displayed **Unlock** icon; the device unlocks immediately and accepts new incoming calls.

7.1.7 Synchronizing Links

[See also Adding Links in Section 5.4] The device action **Sync Link** allows links to be automatically generated and updated between SBCs/gateways and their connected entities. Three different SBC configuration tables are managed by the OVOC:

- IP group
- Trunk group
- Media realm (typically, one for internal (LAN) traffic, another for external (WAN) traffic)

Sync Link checks each row in each table and then generates links between AudioCodes devices and generic devices for each row in each table for which a link does not already exist. A new generic device is created for each link.

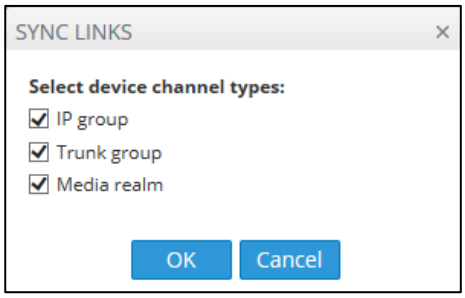
Example:

If two IP Groups, Skype for Business Server 2015 and SIP Trunk ABC, and two Media Realms are configured on an SBC, LAN and WAN, then when **Sync Link** is performed, four links are generated (two IP Groups and two Media Realms).

➢ **To synchronize links:**

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up, as shown in Figure 7-1.
2. Click the **Sync Links** icon.

Figure 7-6: Sync Links



3. If necessary, clear an SNMP table option and then click **OK**; links are generated between AudioCodes devices and generic devices for each row in each table where a link does not already exist, and a new generic device is created for each link.

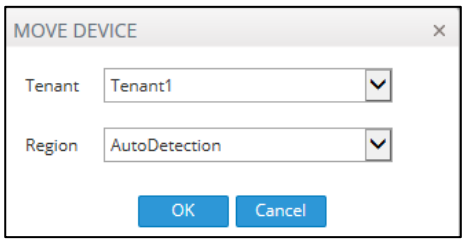
7.1.8 Moving a Device

The device action **Move** lets you move a device across tenants and/or regions. A device cannot be moved if it has a Zero Touch configuration which has not been applied yet.

➢ **To move a device:**

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up, as shown in Figure 7-1.
2. Click the **Move** icon.

Figure 7-7: Move Device



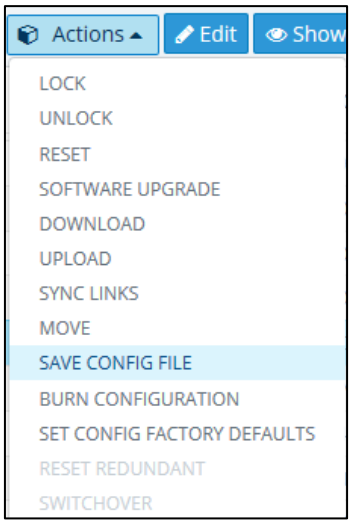
3. From the 'Tenant' dropdown, select from the list of tenants the tenant to move the device to (see Section 5.1 for information on how to add a tenant).
4. From the 'Region' dropdown, select from the list of regions the region to move the device to (see Section 5.2 for information on how to add a region).
5. If the device is an HA device, configure 'Reset redundant'.
6. Click **OK**.

7.1.9 Saving a Device's Configuration File to the PC

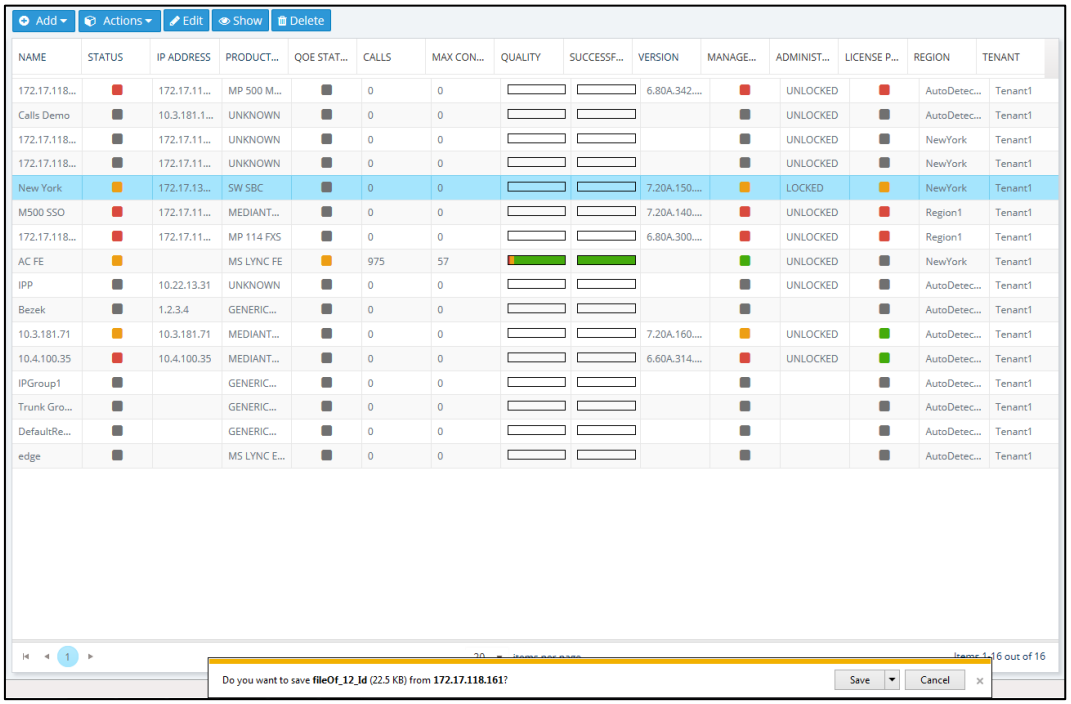
You can save the current configuration of a device to your PC.

➢ **To save a device's configuration to the PC:**

1. Select the device whose configuration you want to save to the PC and click **Actions**.



2. From the Actions menu. select **Save Config File**.



3. Save the configuration file to the PC's download folder or Save As to the location of your choice.

Note:

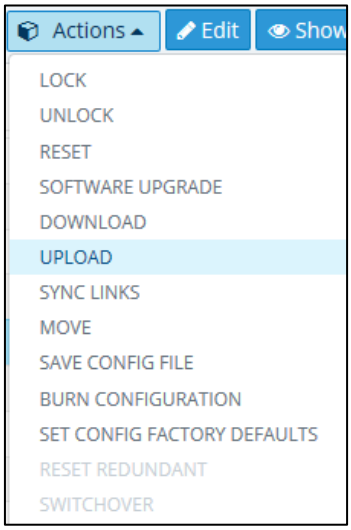
- If the device is an AudioCodes MSBR, an cli file is saved.
- If the device is an AudioCodes MP-202/MP-204, a conf file is saved.
- If the device is another AudioCodes device (except CloudBond), an ini file is saved.

7.1.10 Burning a Device's Configuration File to Flash Memory

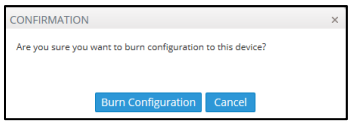
You should save (burn) the current configuration of a device to the device's flash memory (non-volatile) before performing a Reset action (see Section 7.1.3) or before powering down, in order to ensure configuration changes you made are retained.

➢ **To save (burn) a device's software configuration to the device's flash memory:**

1. Open the Devices page (**Network** > **Devices**) and select the device to which to save (burn) the software configuration.
2. Click **Actions**.



3. From the menu, select **Burn Configuration**.



Note: Saving configuration to flash may disrupt current traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (see Section 7.1.6).

7.1.11 Setting Configuration Factory Defaults

You can set a device's configuration to its factory defaults.

Note: The only settings that are not restored to default are the management (OAMP) LAN IP address and the OVOC's login username and password.

7.1.12 Resetting Redundant

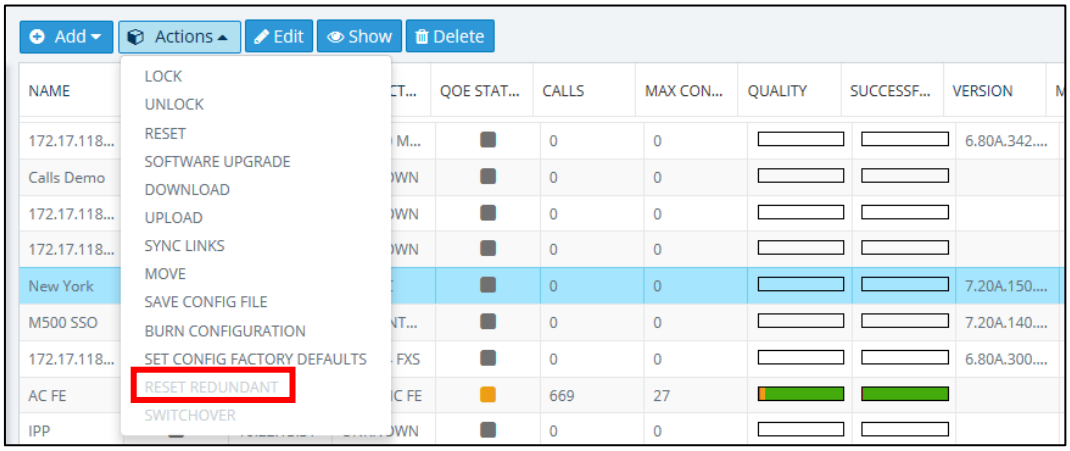
You can reset a device's redundant chassis.

Note: Resetting a device's redundant chassis only applies to HA devices. For detailed information about HA devices, see the relevant device's *User's Manual*.

➢ **To reset a device's redundant chassis:**

1. In the Network page under either the **Topology** or **Devices** tab, select the device to reset and then click the now-activated **Actions** button.

Figure 7-8: Actions – Reset Redundant



2. From the Actions dropdown, select the **Reset Redundant** option. If the menu option is disabled, the device selected does not support HA.

   Resetting a device's redundant chassis is identical to resetting an active device. See Section 7.1.3 for more information.

7.1.13 Performing Switchover

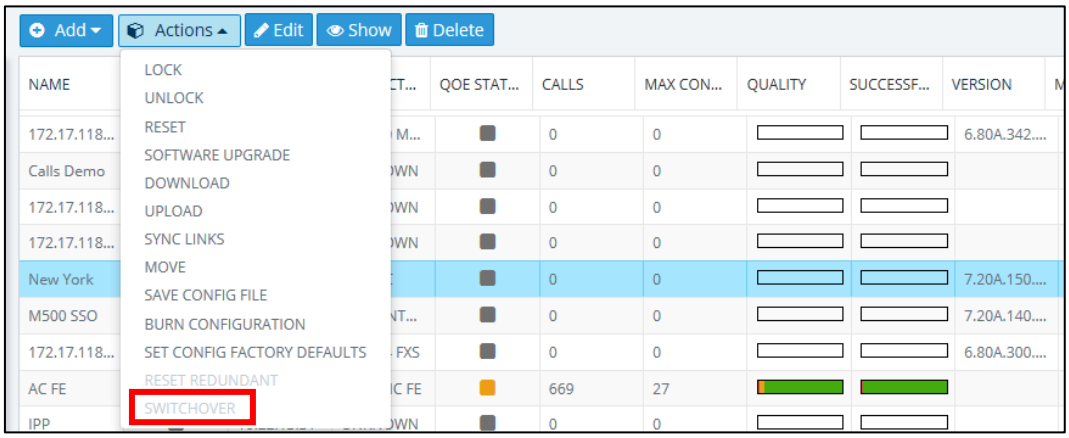
This section only applies to HA devices. For detailed information about HA devices, see the relevant device's *User's Manual*.

If a failure occurs in a device's currently active chassis, a switchover to the redundant chassis occurs. The active chassis becomes redundant and the redundant chassis becomes active. Current calls are maintained and handled by the active chassis (previously the redundant chassis). You can switch from the active chassis (i.e., the previously redundant chassis) to the redundant chassis (i.e., the previously active chassis) to return the device to its original HA state.

➢ **To perform a switchover:**

1. In the Network page under either the **Topology** or **Devices** tab, select the device on which to perform the switchover, and then click the now-activated **Actions** button.

Figure 7-9: Actions – Switchover



2. From the Actions dropdown, select the **Switchover** option. If the menu option is disabled, the device selected does not support HA.

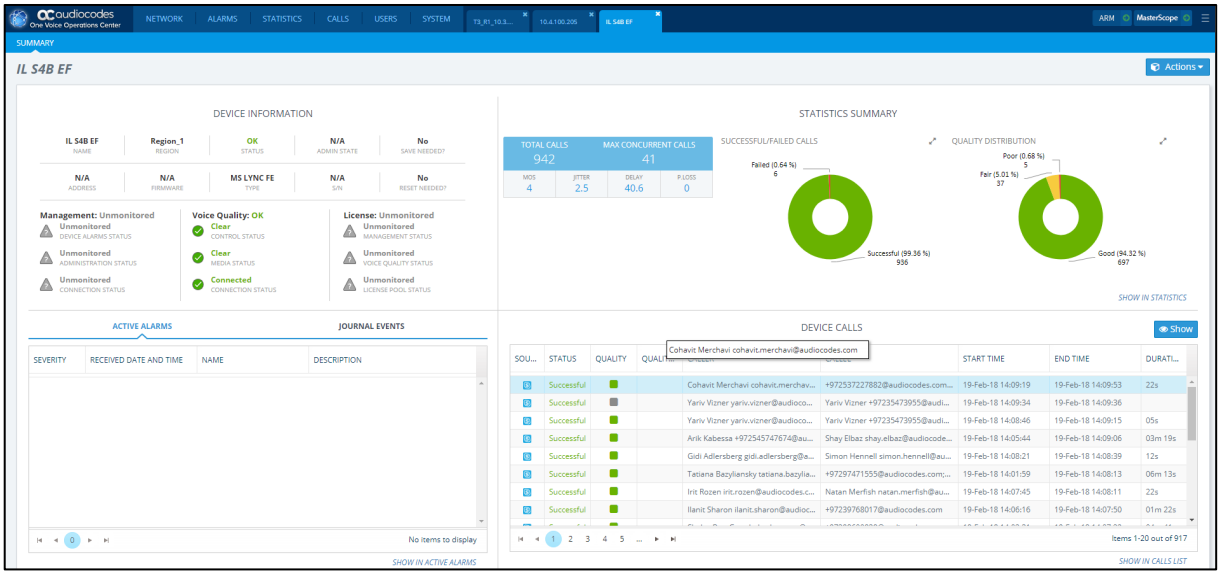
7.1.14 Showing Device Information

The **Show** button lets operators quickly retrieve and assess information related to any device in the network.

➢ **To show device information:**

1. In the Network page under the **Topology** tab or **Devices** > **Manage** tab, select the device and click the activated **Show** button.

Figure 7-10: Show Device Information



The page displays information related to active alarms on the device, journal events, statistics summary and calls made over the device.

The page is dynamically automatically tabbed on the menu bar: **IL S48 EF** in the figure above. Operators can delete the tab at any time. The tab facilitates quick future access to the page from other OVOC pages, for troubleshooting.

Under the 'Statistics Summary' section, the Successful / Failed Calls pie chart and the Quality Distribution pie chart function as filters. Click a color to open the Calls List filtered by these criteria: Device, Time, Successfull / Failed or Quality Color.

Under 'Device Calls' you can select a call made over the device and click the **Show** button to display that call's details; the Call Details page opens (see under Section 8.2 for more information).

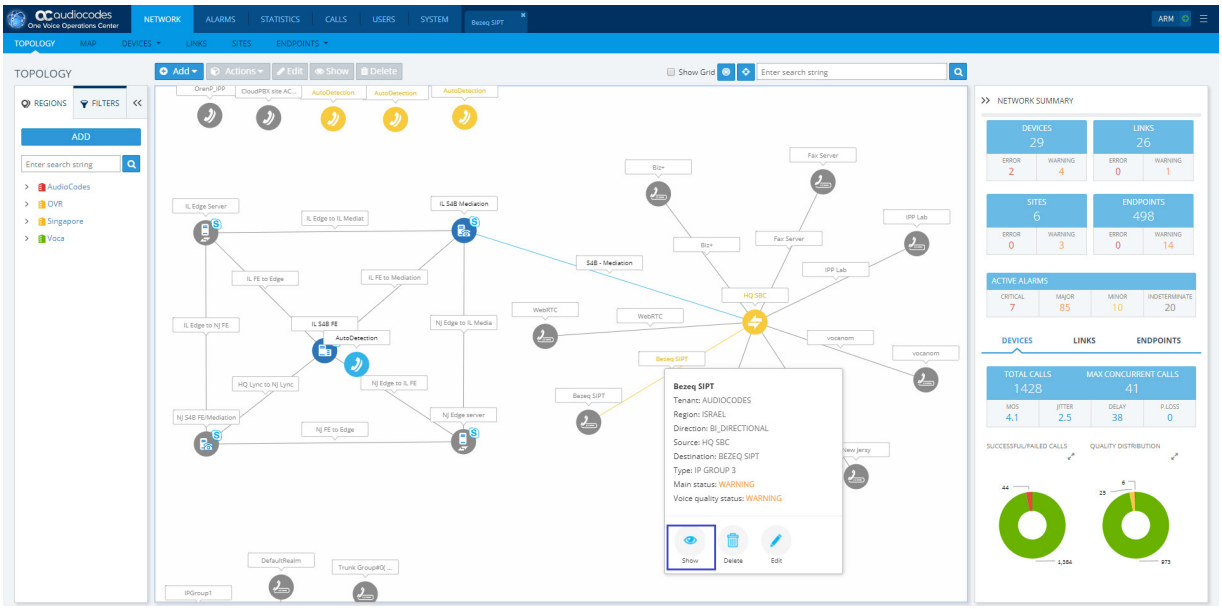
7.1.15 Showing Link Information

The OVOC lets operators quickly retrieve and assess information related to any link in the network.

➢ To show link information:

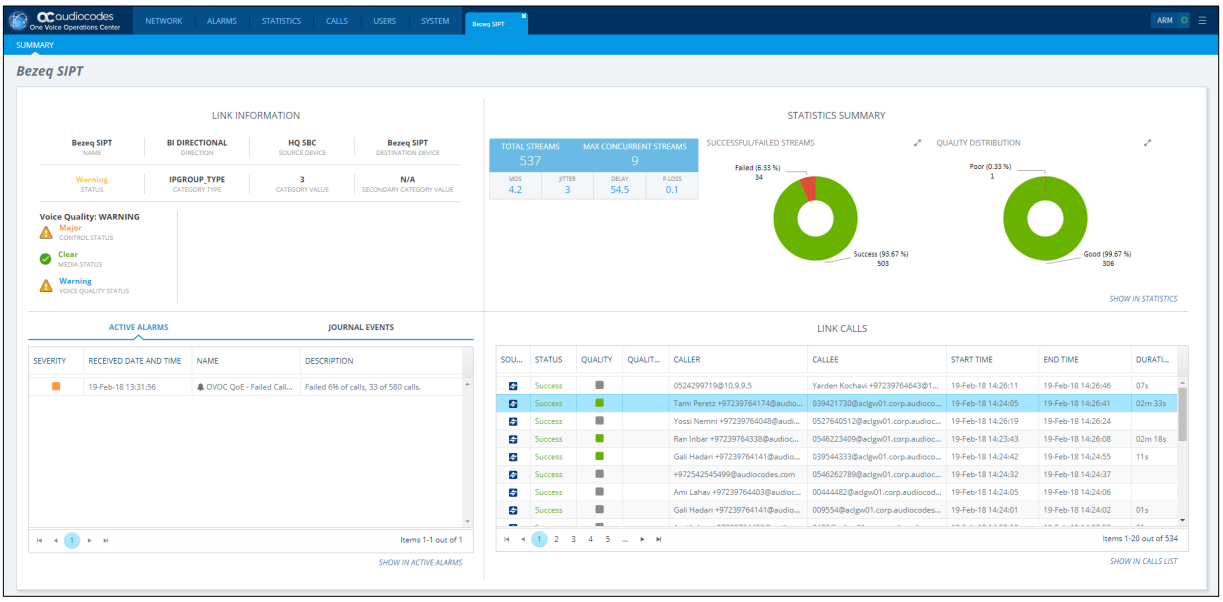
1. In the Network page under the **Topology** or **Links** tab, select the link and click **Show**.

Figure 7-11: Show Link Information



The link's Summary page opens.

Figure 7-12: Link's Summary Page



The page displays information about active alarms on the link, journal events, statistics summary and calls made over the link.

The page is dynamically automatically tabbed on the menu bar: **Bezeq SIPT** in the figure above. Operators can delete the tab at any time. The tab facilitates quick future access to the page from other OVOC pages, for troubleshooting.

Under the 'Statistics Summary' section of the page, the Successful / Failed Streams pie chart and the Quality Distribution pie chart function as filters. Click a color to open the

Calls List filtered by these criteria: Stream, Time, Successfull / Failed or Quality Color.

Under 'Link Calls' select any call made over the link and click **Show** to display that call's details; the Call Details page opens (see under Section 8.2 for more information).

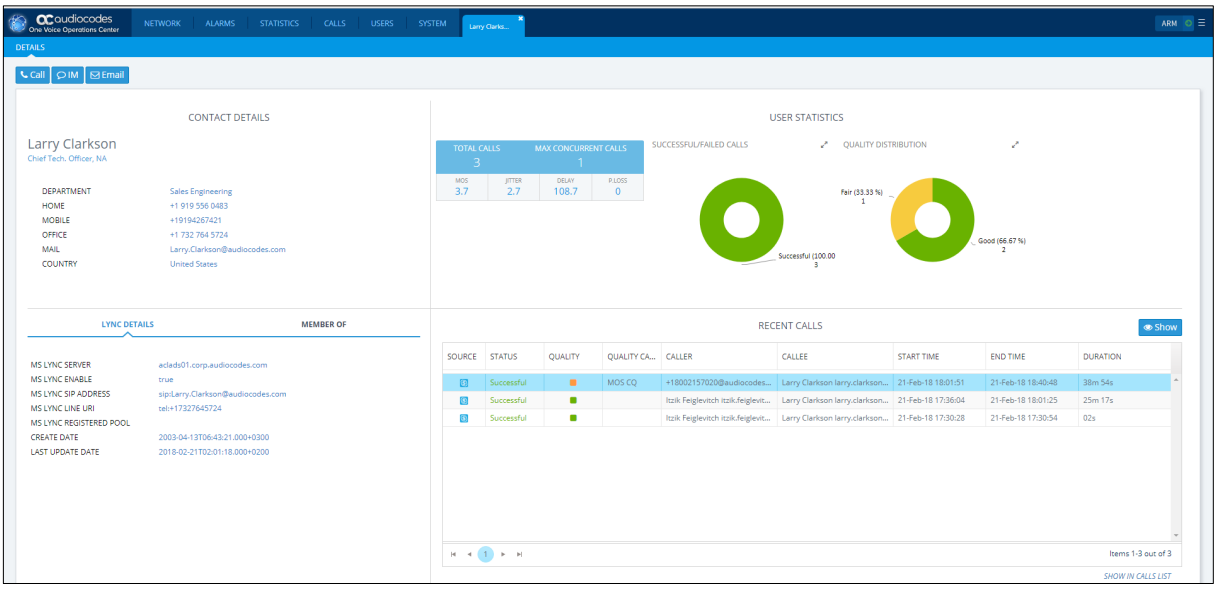
7.1.16 Showing User Information

The OVOC lets operators quickly retrieve and assess telephony information related to any user.

➢ **To show telephony information about a user:**

1. In the Users page under the **Users Experience** or **User Details** tab, select a user and click **Show**.

Figure 7-13: Showing Information about a User



The page displays contact details, Lync details if any, user statistics and recent calls.

The page is dynamically automatically tabbed on the menu bar with the user's name. Operators can delete it at any time. The tab facilitates quick access to the page from other OVOC pages, for future reference.

Under the 'User Statistics' section of the page, the Successful / Failed Calls pie chart and the Quality Distribution pie chart function as filters. Click a color to open the Calls List filtered by these criteria: User, Time, Successfull / Failed or Quality Color.

Under 'Recent Calls' you can select any call made by this user and then click the **Show** button to display that call's details. The Call Details page opens (see under Section 8.2 for more information).

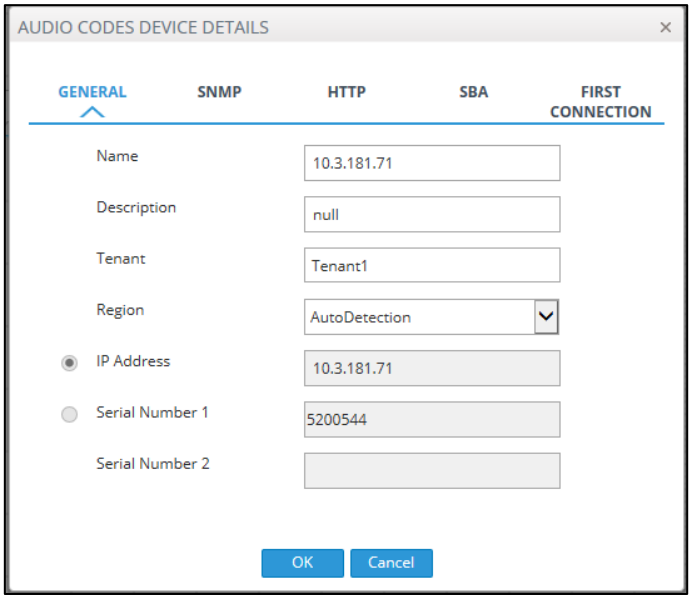
7.1.17 Editing a Device

The **Edit** button lets you edit a device's configuration.

➢ **To edit a device's configuration:**

1. Select the device to edit and then click the **Edit** button.

Figure 7-14: Device Details



2. Edit the device's details. For more information, see Section 5.3.
3. Click **OK**.

7.1.18 Deleting a Device

The **Delete** button lets you delete a device from the OVOC.

➢ **To delete a device:**

- Select the device to delete and then click the **Delete** button.

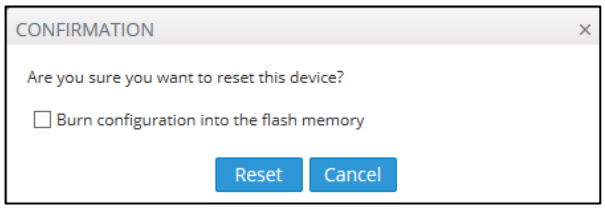
7.1.19 Resetting a Device

You can reset a device.

➢ **To reset a device:**

1. From the Actions menu, select **Reset Device**.

Figure 7-15: Reset Device – Confirmation



2. Select the **Burn configuration into the flash memory** in order to make sure changes are retained. They're burned (saved) to the device's non-volatile memory, i.e., flash memory. See Section 7.1.10 for more information about burning a device's configuration to flash memory.

Note: Without burning, changes are saved to the device's *volatile* memory (RAM). The changes revert to their previous settings if the device subsequently resets (hardware or software) or powers down.

3. Click **Reset**.

7.1.20 Applying a License to a Device from the Pool

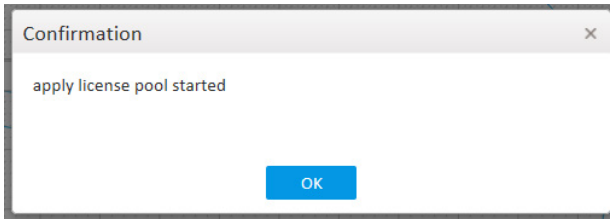
You can apply a license to a device.

Note: Only relevant to HA devices. A switchover is performed in order to apply the license parameter on both devices.

➢ **To apply a license to a device:**

1. From the Actions menu, select **Apply License**.

Figure 7-16: Apply License - Confirmation



2. Click **OK**.

7.1.21 Refreshing a Device's Pool License

You can refresh a device's Pool License.

Note: Only relevant to HA devices. A switchover is performed in order to apply the license parameter on both devices.

➢ **To refresh a device's Pool License:**

- From the Actions menu, select **Refresh License**.

7.2 Monitoring Device-Level Backup and Performing Rollback

The Backup Manager page (**Network** > **Devices** dropdown > **Backup Manager**) allows you to monitor device-level backup and perform rollback. For detailed information, see Section 5.3.4 and the subsections under it.

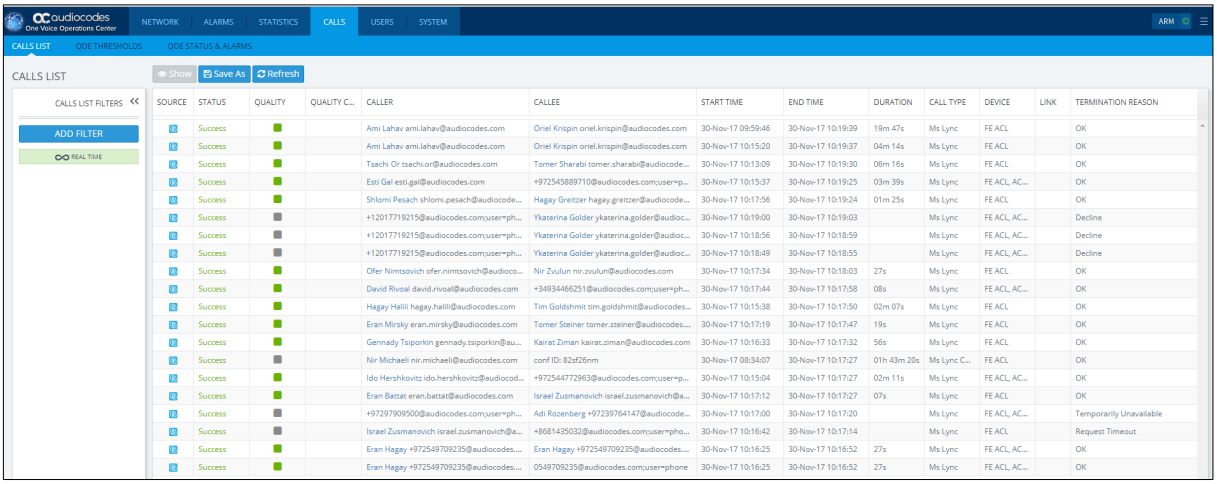
8 Obtaining Quality Statistics on Calls

This section shows how to get quality statistics – a.k.a. Key Quality Indicators (KQIs) - on calls made by end users in your network.

8.1 Accessing the Calls List

The Calls List page (**Calls** > **Calls List**) lists and shows quality information on calls made in the network over the past three hours (default).

Figure 8-1: Calls List



Note: Calls on AudioCodes' High Availability devices during switchover are not supported. The OVOC QoE application does not display and count a call that starts on unit A and is transferred to unit B after device switchover.

The page features filtering capabilities to help obtain precise information on calls quickly and efficiently. Optionally, filter the page by Time Range (see Section 6.2.1), Topology (see Section 6.2.1.2), Source Type (see Section 6.4.3.1), Quality (see Section 8.1.1 below) or More Filters (see Section 8.1.2 below).

Use the table below as reference to the columns in the Calls List.

Table 8-1: Calls List Columns

Column	Description	
Source	indicates the call is from Microsoft Skype for Business indicates the call is from an AudioCodes device. indicates the call is from an AudioCodes IP phone.	
Status	Indicates call control status: **Successful** or **Failed**	
Quality	Indicates the call quality: Green = Good, Yellow = Fair, Red = Poor, Gray = Unknown	
Quality Cause	Delay (msec)	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.

Column	Description	
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter (msec)	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss (%)	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
Caller	The phone number or address of the person who initiated the call.	
Callee	The phone number or address of the person who answered the call.	
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was started.	
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.	
Duration (sec)	The duration of the call, in seconds. See the note below.	
Call Type	Indicates the call type.	
Device	Indicates the device/s over which the call passed.	
Link	Indicates the link/s over which the call passed.	
Termination Reason	Indicates the reason why the call was terminated.	

Note: An SBC call (exclusively) whose duration is longer than three hours (e.g., the session of a participant in a Skype for Business conference call over an SBC) or an SBC call that is incompletely reported to the OVOC server won't be displayed in the Calls List.

The **Save As** button lets you download calls information (numbers and text) in a coma-separated *calls.csv* file format that can later be easily opened and read in any text editor, as well as sent as an attachment in an email to others.

At the foot of the page, the pager shown above lets you (from left to right):

- Click the **|◄ Go to the first page** to return to the first page from any page.
- Click the **Go to the previous page** arrow to return to the page before the presently displayed page.
- Click **… [More pages]** to the left of the page number or **… [More pages]** to the right of

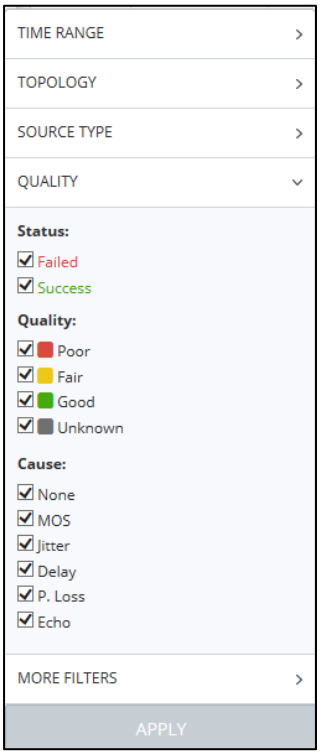
the page number to page backwards or forwards respectively.

- Click the **Go to the next page** arrow to browse to the page after the presently displayed page.
- From the 'Items per page' dropdown, select the number of calls to display per page: **20**, **30** or **50**.

8.1.1 Filtering by 'Quality'

This section shows how to filter a page using the 'Quality' filter. The filter applies to the Calls List page under the Calls menu. The filter lets you display calls according to quality.

Figure 8-2: Quality Filter



Use the table below as reference.

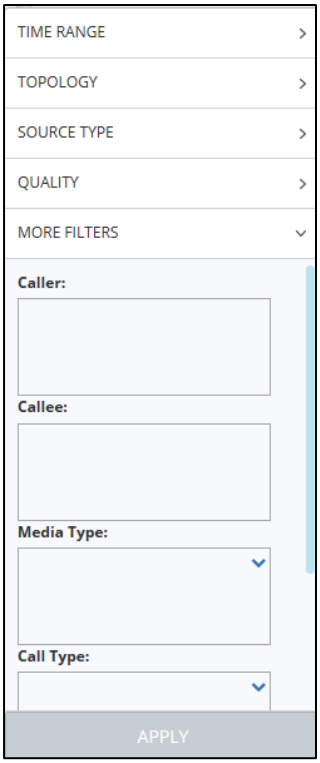
Table 8-2: 'Quality' Filter

Filter	Description
Failed | Success	Filters calls according to their status. If you clear Success and select Failed, only calls whose status was Failed are displayed in the page.
Poor, Fair, Good or Unknown	Filters calls according to their quality. If you clear all except Poor, only calls whose quality was Poor will be displayed.
None, MOS, Jitter, Delay, P. Loss or Echo	Filters calls according to the cause of the quality. If - after displaying only calls whose quality was poor/fair - you clear all except Delay, the page will display only calls *whose quality was poor/fair because there was a delay on the line*.

8.1.2 Filtering by 'More Filters'

This section shows how to filter the Calls List page by 'More Filters'. The filter lets you display calls according to caller, callee, media type, etc.

Figure 8-3: More Filters – Calls List Page



Use the table below as reference.

Table 8-3: More Filters – Calls List

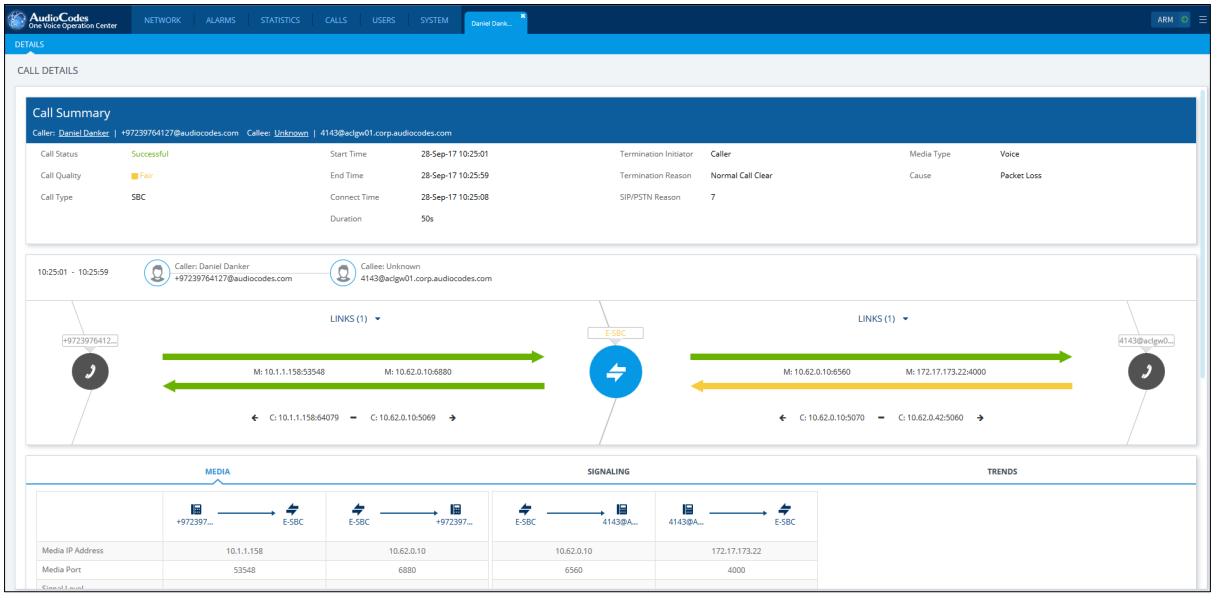
Filter	Description
Caller	Enter the name of a caller (or the names of callers) whose calls you want to display in the page. The filter is case sensitive.
Callee	Enter the name of a called party (or the names of called parties) whose calls you want to display in the page. The filter is case sensitive.
Media Type	From the dropdown list, select the media type to display on the page, or enter a search string. Select either Voice, Video, Audio Video, Image, Data, Unknown, Application Sharing or Chat. By default, all media types are selected.
Call Type	From the dropdown list, select the call type to display on the page, or enter a search string. Select either Gateway, SBC, IP2IP, MS Lync, MS Lync Conference or Endpoint. Microsoft Lync Conference can be of Media Type Audio Video or Chat. The conference participant's name is shown in the 'Caller' column. To retrieve conference calls information, the OVOC uses Microsoft Lync's ConferenceSessionDetailsView Monitoring Server report. For example, from the 'Media Type' dropdown choose Chat; the Media Type column then displays only MS Lync conferences whose Media Type is Chat.

Filter	Description
Termination Reason	Enter the reason why the call was terminated. See the device's *User's Manual* for more information about Termination Reason. Some AudioCodes termination reasons are: ▪ Reason Not Relevant ▪ Unassigned Number ▪ Invalid Information Element Content ▪ The remote equipment received an unexpected message that does not correspond to the current state of the connection. ▪ Recovery on Timer Expiry ▪ Protocol Error Unspecified ▪ Unknown Error ▪ Q931 Last Reason Some MS Lync Termination Reasons are: ▪ OK. Indicates the request was successful. ▪ Accepted. Indicates that the request has been accepted for processing, but the processing has not been completed. ▪ No Notification ▪ Multiple Choices ▪ Moved Permanently ▪ Moved Temporarily ▪ Use Proxy ▪ Alternative Service

8.2 Showing Call Details

You can select a call in the Calls List page (see Figure 8-1) and then click the activated **Show** button. The Call Details page that opens (shown in Figure 8-4) displays detailed information about that call.

Figure 8-4: Call Details – Details of a Call Made over an AudioCodes Device



8.2.1 Details of a Call Made over an AudioCodes SBC

The figure above shows the details of a call made over an AudioCodes SBC. You can also display the details of calls made/received over other entities. The page is automatically dynamically tabbed on the menu bar (**David Mor** in the figure above), for quick and easy future access and troubleshooting. Operators can delete the tab at any time. The page displays detailed diagnostic information, in graphic and textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality. Use the table below as reference.

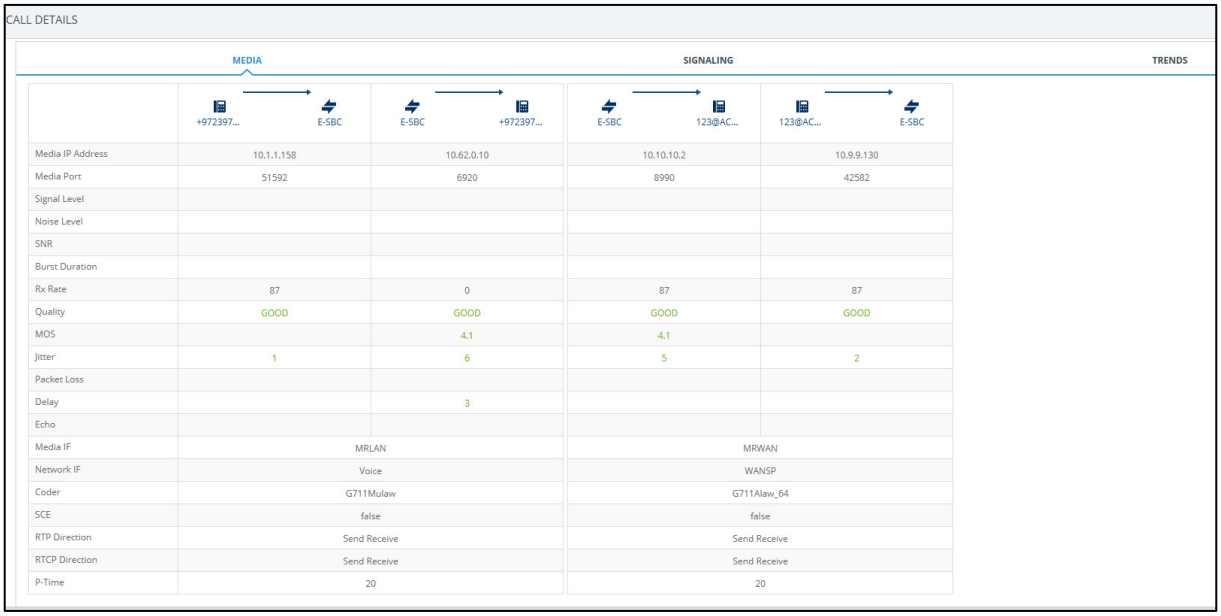
Table 8-4: Call Details Page

Page Subdivision	Description
(Uppermost) Call summary	Displays parameters and values identical to those displayed in the Calls List page.
(Middle) Graphic illustration	Displays a graphical illustration of voice quality on each leg of the call, on both the caller and callee side. Each leg is: ▪ Connected via the VoIP cloud to the device ▪ Color-coded to indicate quality (green = good, yellow = fair, red = poor, grey = unknown) ▪ Tagged by **C** and **M** **C** = Control summary (point cursor to view tooltip) **M** = Media IP address and Port (point cursor to view tooltip)
(Lowermost) Three tabs	Each opens a page displaying detailed information: ▪ **Media** (see Section 8.2.1.1) (includes **Quality**) ▪ **Signaling** (see Section 8.2.1.2) ▪ **Trend** (see Section 8.2.1.3) (Only displayed if there is a trend; if there is not a trend, the tab is not displayed) ▪ **SIP Ladder** (see Section 8.2.1.4)

8.2.1.1 Media

The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-5: Media



Use the table below as reference to the parameters displayed under the Media tab.

Table 8-5: Media Parameters

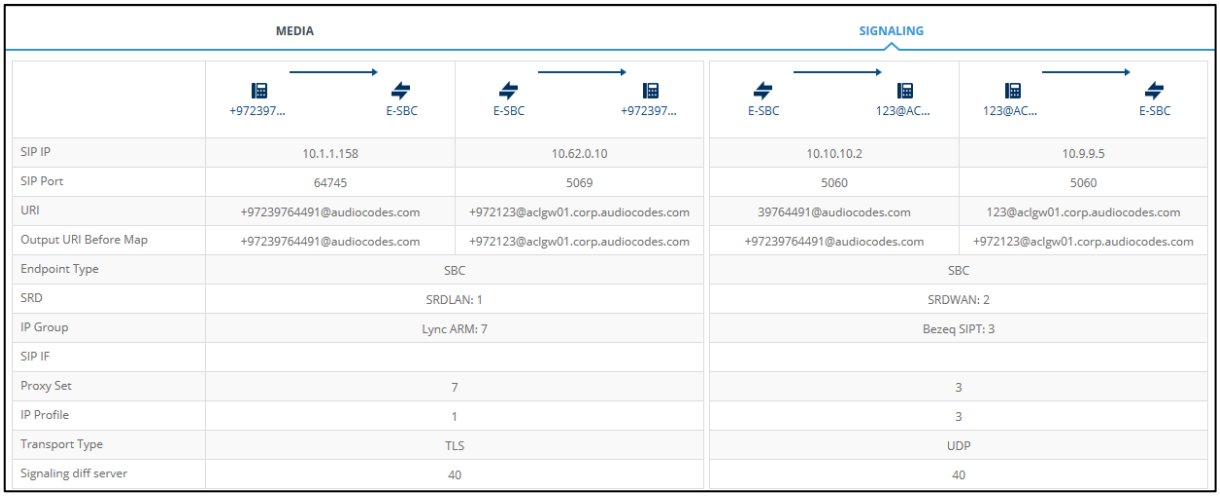
Parameter	Description
Media IP Address	▪ The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network. ▪ The IP address of the destination host / media network.
Media Port	▪ The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. ▪ Port of the destination host / media network.
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.
Noise Level	The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Burst Duration	The mean duration (in milliseconds), of the burst periods that have occurred since the initial call reception.
Rx Rate	Shows the call's reception rate, in Kbps.
Quality	Voice quality: Good (green), Fair (yellow) OR Red (poor).
MOS	Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises: MOS-LQ = listening quality, i.e., the quality of audio for listening purposes.

Parameter	Description
	Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.
Jitter	Jitter can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
Packet Loss	Lost packets are RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, for the caller and for the callee side. Packet Loss can be more than 100%.
Delay	The round trip delay is the estimated time (in milliseconds) that it takes to transmit a packet between two RTP stations. Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two values are shown, one caller side and another for the callee side.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Media IF	Shows the name and index of the Media Realm interface reported by the device. Example: **SIMcmxLAN (n)**, where **n** following the displayed name is the number indicating the Media Interface's index used to facilitate network configuration.
Network IF	Network Interface Name.
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
SCE	Method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. True = Enabled (On), False = Disabled (Off).
RTP Direction	RTP Directional Control. Controlled internally by the device according to the selected coder.
RTCP Direction	RTCP Directional Control. Controlled internally by the device according to the selected coder.
PTime (msec)	Packetization time, i.e., how many coder payloads are combined into a single RTP packet.

8.2.1.2 Signaling

The Signaling tab displays a call's signaling parameters that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-6: Signaling



Use the table below as reference to the parameters displayed under the Signaling tab.

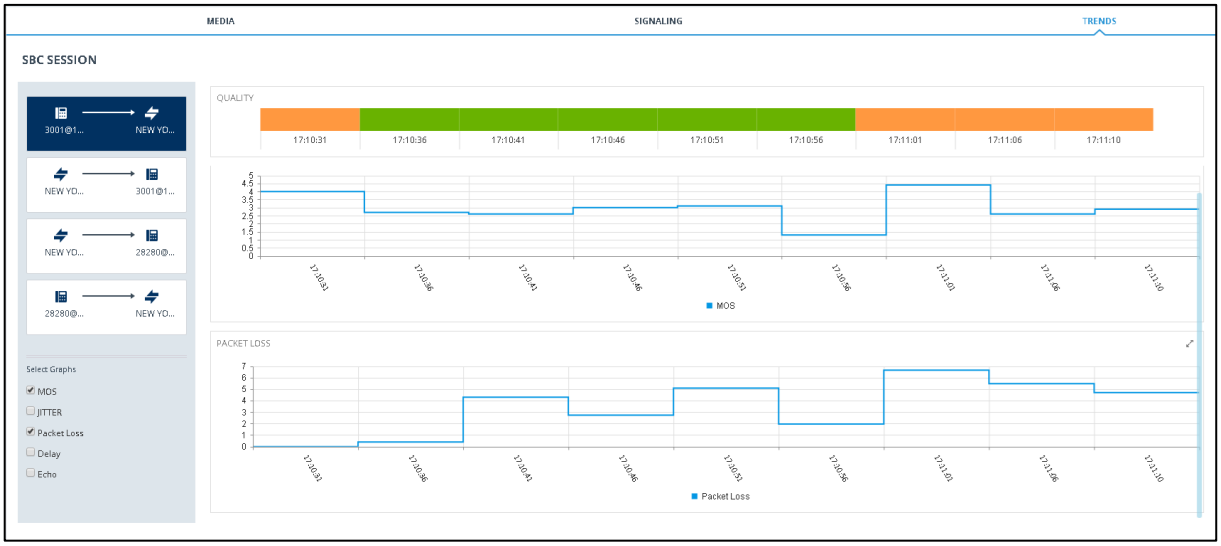
Table 8-6: Signaling Parameters

Parameter	Description
SIP IP	The call's caller/callee (source/destination) IP address.
SIP Port	The port number used for the SIP call.
URI	The URI (Uniform Resource Identifier) of the caller/callee (source/destination). The SIP URI is the user's SIP phone number (after manipulation, if any). The SIP URI resembles an e-mail address and is written in the following format: sip:x@y:Port, where x=Username and y=host (domain or IP).
Output URI Before Map	The SIP URI address of the caller/callee before manipulation (if any) was done on the URI.
Endpoint Type	Indicates the type of endpoint. For example, 'SBC'.
SRD	The unique name and index configured for the signaling routing domain (SRD). Example: **someSRD (n)**, where **n** following the displayed name is the number indicating the SRD's index used to facilitate network configuration.
IP Group	The ID of the IP Group with which the call is associated.
SIP IF	The ID of the SIP Interface with which the call is associated.
Proxy Set	The Proxy Set to which the call is associated. This is a group of Proxy servers. Typically, for IP-to-IP call routing, at least two are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.
IP Profile	The IP Profile assigned to this IP destination call. The IP Profile assigns numerous configuration attributes (e.g., voice codes) per routing rule.
Transport Type	Two options: UDP or TCP
Signaling diff server	The value for Premium Control CoS content (Call Control applications).

8.2.1.3 Trends

The Trends tab shows a call's voice quality trend that operators can refer to for diagnostic, troubleshooting and session management experience issues.

Figure 8-7: Trends



Voice quality applies to the call's:

- Caller leg
  - caller side (of cloud)
  - device side (of cloud)
- Callee leg
  - callee side (of cloud)
  - device side (of cloud)

➢ **To assess voice quality:**

- Select a quality metric graph option (MOS, Jitter, Packet Loss, Delay and/or Echo) and then select a leg; the graph displayed indicates:
  - the voice quality of the call for the selected quality metric across the selected leg
  - how long the leg lasted
  - the time the leg started and ended

Note: Legs over PSTN are not measured for quality, only legs over IP.

➢ **To compare one voice quality metric with another across different legs:**

1. Select multiple voice quality metric graphs, for example, MOS and Packet Loss, as shown in the figure above.
2. Select a leg option and compare the displayed graphs of quality metrics with one another across this leg.
3. Select another leg and compare the same metrics graphs with one another across this leg.

8.2.1.4 SIP Call Flow

The **SIP Call Flow** tab is displayed in the Call Details page when a SIP ladder is available or partially available and found for a specific call over SBC.

Figure 8-8: SIP Call Flow – Example 1

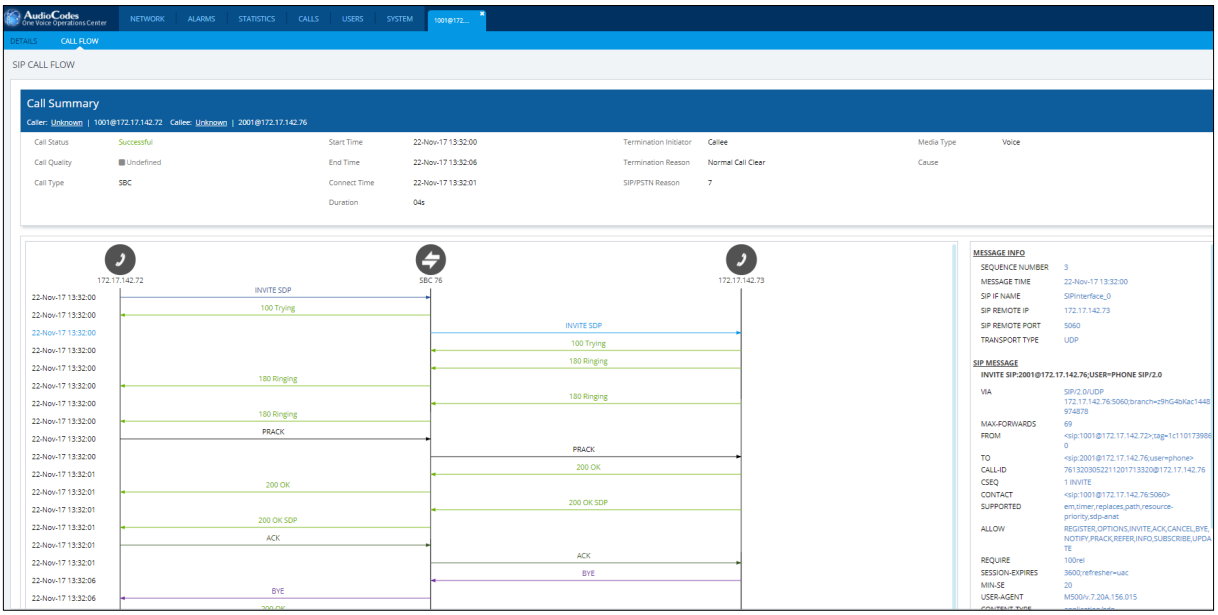
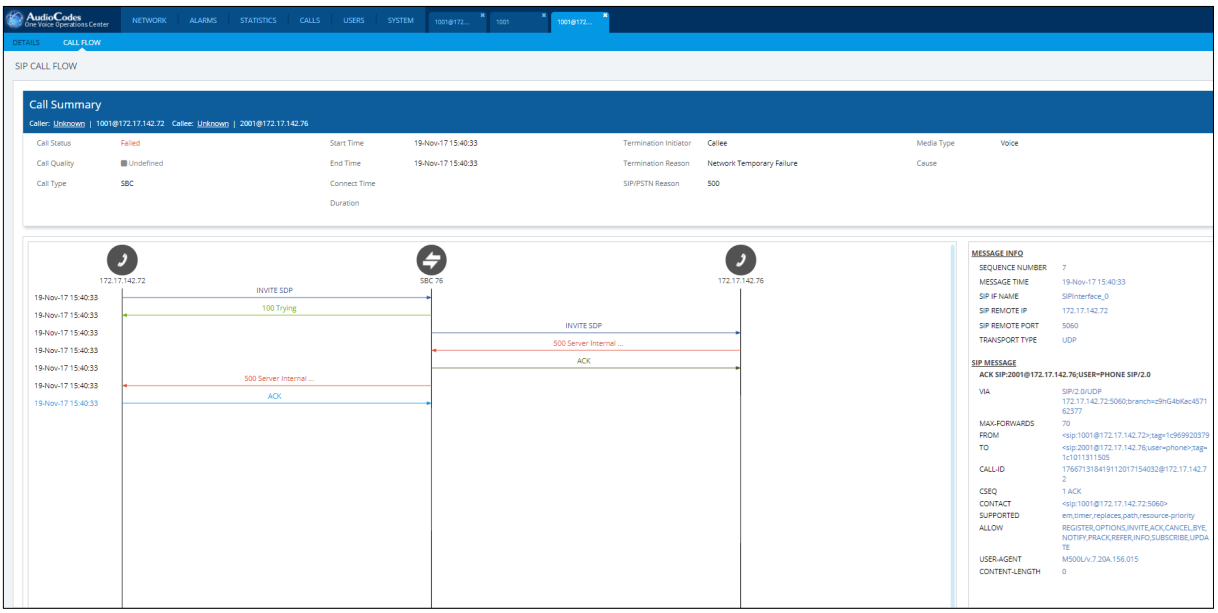


Figure 8-9: SIP Call Flow – Example 2



- Select a SIP message to display its MESSAGE INFO in the right pane

Note: The number of participants indicated in the Call Details and in the Call Flow tabs can be different. The Call Flow tab can include more participants than the Call Details tab, which always includes caller and callee.

Table 8-7 below shows error response color codes.
Table 8-8 shows SIP message color codes.

Table 8-7: Error Response Color Codes

Color	Error Response
Red	Error response message with response code 6xx, 5xx, 4xx, excluding 486 (busy) which is colored green
Green	Error response message with response code 486 (busy) and all other responses
Black	Error response message with response codes 401 and 407

Table 8-8: SIP Message Color Codes

Color	SIP Message
Dark Green	ACK
Dark Blue	INVITE
Brown	CANCEL
Purple	BYE
Black (unbolded)	All other SIP messages and codes

Note that light blue bolded indicates a selected message.

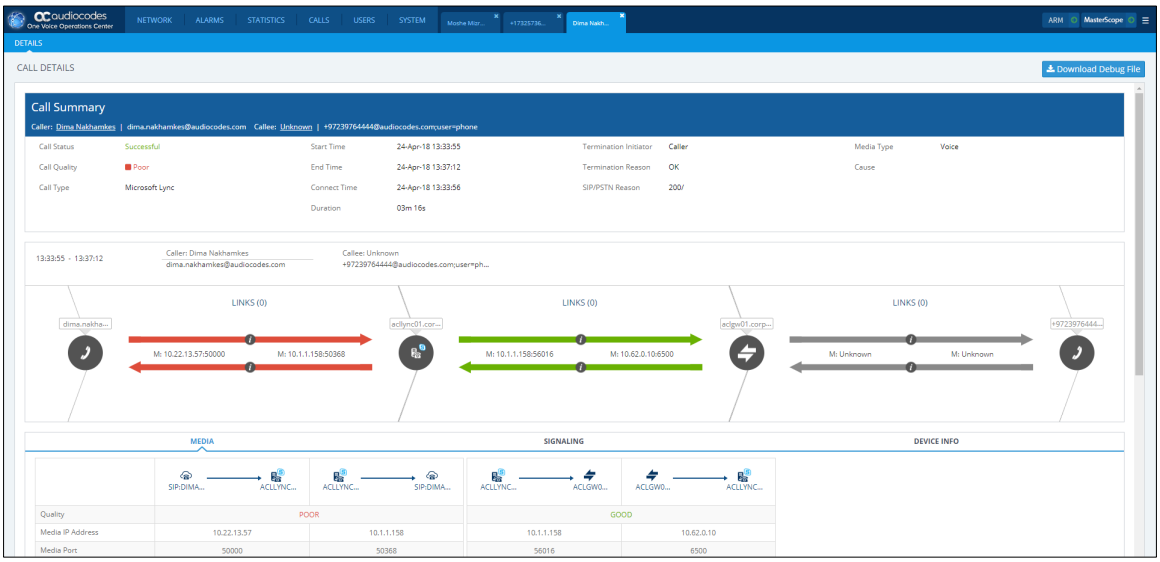
8.2.2 Call Details Page – Debug File Button

To facilitate troubleshooting if for example there's a discrepancy between the Call Details that the OVOC reports and the call details that you report, you can click a **Debug File** button in the Call Details page to save (download) a debug file in *json* format and then send it to AudioCodes FAEs for analysis.

8.2.3 Details of a Call Made over Microsoft Skype for Business (Lync)

The figure below shows the details of a call made over Microsoft Skype for Business (Lync). The Details page displays detailed diagnostic information on the call, in textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality.

Figure 8-10: Call Details - Microsoft Skype for Business



If there's an issue of poor quality with a call over Microsoft Skype for Business (Lync), one of the two legs of the call in the Call Details screen will indicate that there's an issue. The leg that indicates that there's an issue is the leg that scores the worse score of the two legs, i.e., the score indicated in red, as shown in the figure above. Use this table as reference:

Table 8-9: Call Details - Microsoft Skype for Business

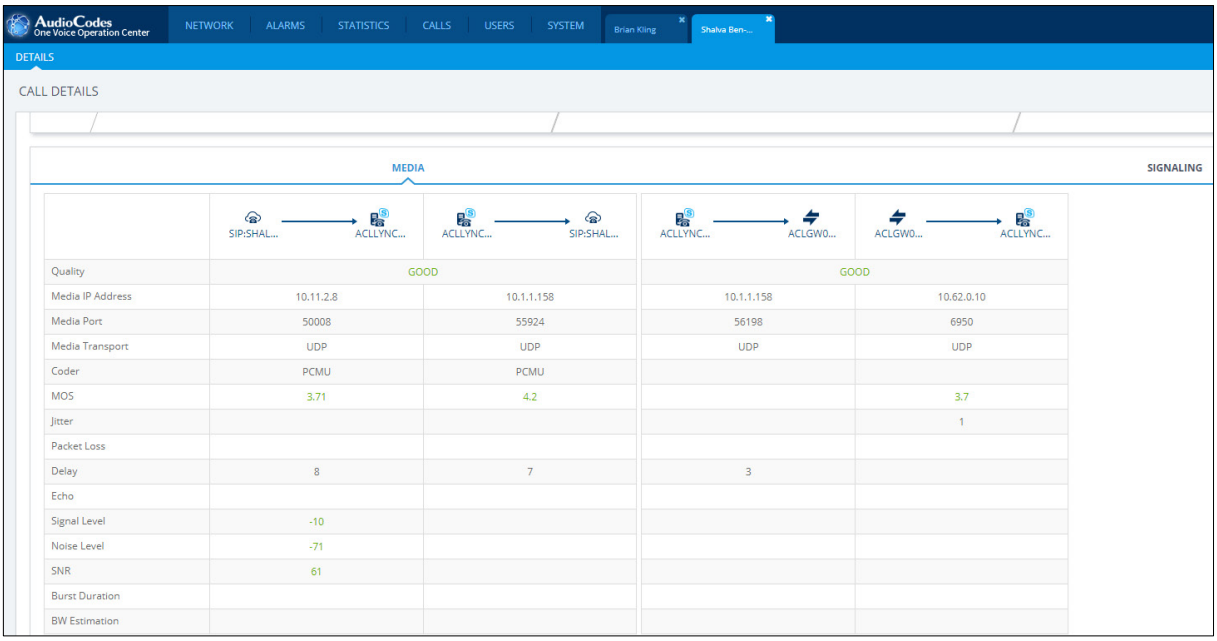
Page Section	Description
Call Summary (Uppermost)	Indicates the caller's full name and email address and callee's full name and email address.
Call Status	**Successful** or **Failed**
Call Quality	**Good** | **Fair** | **Poor** voice quality
Call Type	Microsoft Lync (Skype for Business)
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.
Connect Time	The precise time (hour, minutes and seconds) and date (month, day and year) the connection was established.
Duration	The duration of the call, in seconds.
Termination Initiator	The network entity from which the call was terminated.
Termination Reason	The reason why the call was terminated. See the device's *User's Manual* for more information about Termination Reason. Some MS Lync Termination Reasons are: ▪ OK. Indicates the request was successful. ▪ Accepted. Indicates that the request has been accepted for processing, but the processing has not been completed.

Page Section	Description	
	▪ No Notification ▪ Multiple Choices ▪ Moved Permanently ▪ Moved Temporarily ▪ Use Proxy ▪ Alternative Service	
SIP PSTN Reason	The reason why the call was terminated. See the device's *User's Manual* for more information about Termination Reason.	
Media Type	Voice	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
(Middle) Graphic illustration	▪ Indicates the time the call started and ended ▪ Visualizes a caller in a call with a callee, including full names and email addresses ▪ Displays each leg of the call, on both caller and callee side. Each leg is: ✓ Connected to a device ✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✓ Tagged by **C** and **M** **C** = Control summary (point cursor to view tooltip) **M** = Media IP address and Port (point cursor to view tooltip)	
(Lowermost) Two tabs	Each opens a page displaying detailed information: ▪ **Media** (see Section 8.2.3.1) ▪ **Signaling** (see Section 8.2.1.2)	

8.2.3.1 Media

The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-11: Media



Use the table below as reference to the parameters displayed under the Media tab.

Table 8-10: Media Parameters

Parameter	Description
Quality	Indicates the call's voice quality: **Good** | **Fair** | **Poor**
Media IP Address	▪ The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network. ▪ The IP address of the destination host / media network.
Media Port	▪ The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. ▪ Port of the destination host / media network.
Media Transport	Two options: UDP or TCP
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
MOS	Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises: MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.
Jitter	Jitter can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement,

Parameter	Description
	the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
Packet Loss	Lost packets are RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, for the caller and for the callee side. Packet Loss can be more than 100%.
Delay	The round trip delay is the estimated time (in milliseconds) that it takes to transmit a packet between two RTP stations. Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two values are shown, one caller side and another for the callee side.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.
Noise Level	The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Burst Duration	The mean duration (in milliseconds), of the burst periods that have occurred since the initial call reception.
BW Estimation	The estimated bandwidth consumed.

8.2.3.2 Signaling

The Signaling tab displays a call's signaling parameters that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-12: Signaling

Use the table below as reference to the parameters displayed under the Signaling tab.

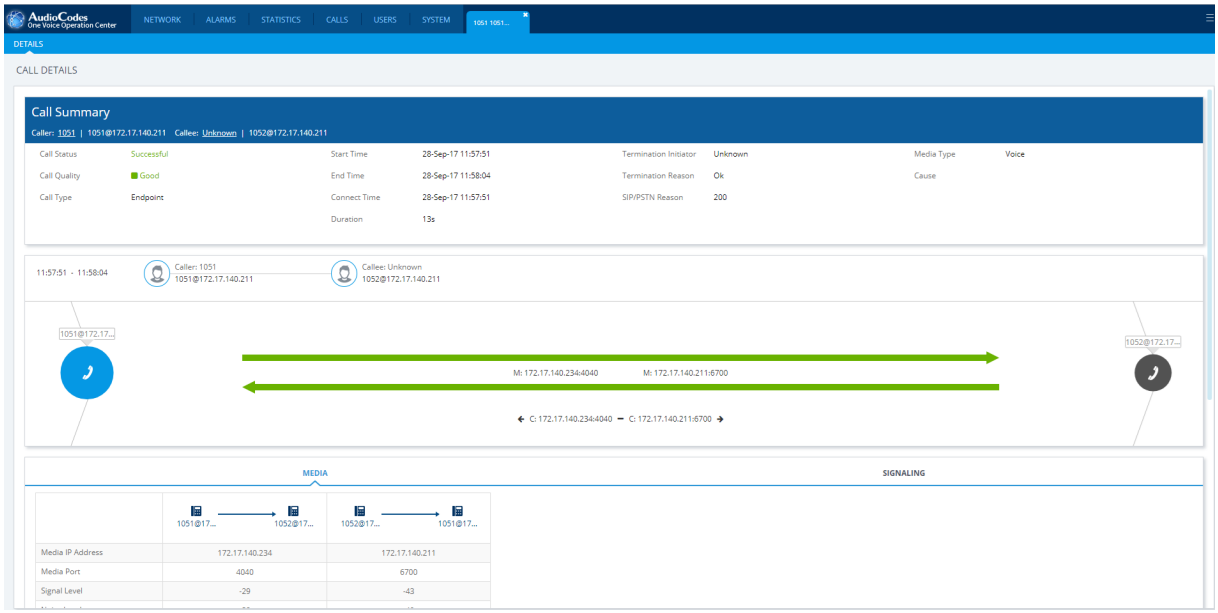
Table 8-11: Signaling Parameters

Parameter	Description
Edge Server	FQDN of the Edge server used by the user who started (caller) / joined (callee) the session.
Gateway	Gateway of the user who started (caller) / joined (callee) the session.
Mediation Server	Mediation Server of the user who started (caller) / joined (callee) the session.
URI	URI of the user who started (caller) / joined (callee) the session.
Phone Number	Phone URI of the user who started (caller) / joined (callee) the session.
Is Internal	Indicates whether the user who started (caller) / joined (callee) the session logged on from the internal network.
Front End	FQDN of the Front End server that captured the data for the session.
Pool	FQDN of the pool that captured the data for the session.
Call Priority	Call priority of the session.

8.2.4 Details of a Call Made over an Endpoint Using SIP Publish

The figure below shows the details of a call made over an endpoint using SIP Publish. The Details page displays detailed diagnostic information on the call, in textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality.

Figure 8-13: Call Details – Over an Endpoint Using SIP Publish



Use the table below as reference.

Table 8-12: Call Details - Over an Endpoint Using SIP Publish

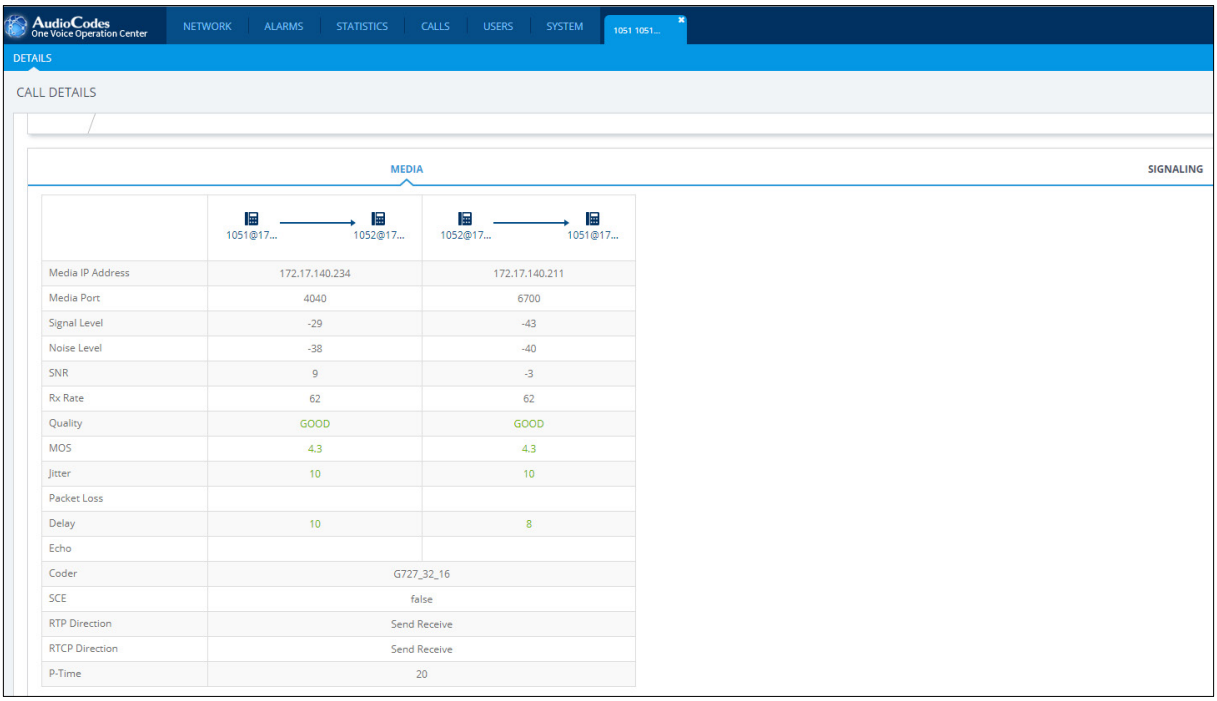
Page Section	Description
Call Summary (Uppermost)	Indicates the caller's full name and email address and callee's full name and email address.
Call Status	**Successful** or **Failed**
Call Quality	**Good** | **Fair** | **Poor** voice quality
Call Type	Endpoint
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.
Connect Time	The precise time (hour, minutes and seconds) and date (month, day and year) the connection was established.
Duration	The duration of the call, in seconds.
Termination Initiator	The network entity from which the call was terminated.
Termination Reason	The reason why the call was terminated. See the device's *User's Manual* for more information about Termination Reason.
SIP PSTN Reason	The reason why the call was terminated. See the device's *User's Manual* for more information about the SIP/PSTN Reason.
Media Type	Voice

Page Section	Description	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
(Middle) Graphic illustration	▪ Indicates the time the call started and ended ▪ Visualizes a caller in a call with a callee, including full names and email addresses ▪ Displays each leg of the call, on both caller and callee side. Each leg is: ✓ Connected to a device ✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown) ✓ Tagged by **C** and **M** **C** = Control summary (point cursor to view tooltip) **M** = Media IP address and Port (point cursor to view tooltip)	
(Lowermost) Two tabs	Each opens a page displaying detailed information: ▪ **Media** (see Section 8.2.4.1) ▪ **Signaling** (see Section 8.2.1.2)	

8.2.4.1 Media

The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

Figure 8-14: Media



Use the table below as reference.

Table 8-13: Media Parameters

Parameter	Description
Media IP Address	▪ The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network. ▪ The IP address of the destination host / media network.
Media Port	▪ The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network. ▪ Port of the destination host / media network.
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.
Noise Level	The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Rx Rate	Shows the call's reception rate, in Kbps.
Quality	Voice quality: Good (green), Fair (yellow) OR Red (poor).
MOS	Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises: MOS-LQ = listening quality, i.e., the quality of audio for listening purposes.

Parameter	Description
	Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.
Jitter	Jitter (in msec) can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
Packet Loss	Lost packets, as a percentage - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Packet Loss can be more than 100%.
Delay	Delay (or latency) (in msec) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
SCE	Method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. True = Enabled (On), False = Disabled (Off).
RTP Direction	RTP Directional Control. Controlled internally by the device according to the selected coder.
RTCP Direction	RTCP Directional Control. Controlled internally by the device according to the selected coder.
PTime (msec)	Packetization time, i.e., how many coder payloads are combined into a single RTP packet.

8.3 Managing QoE Thresholds Profiles per Tenant

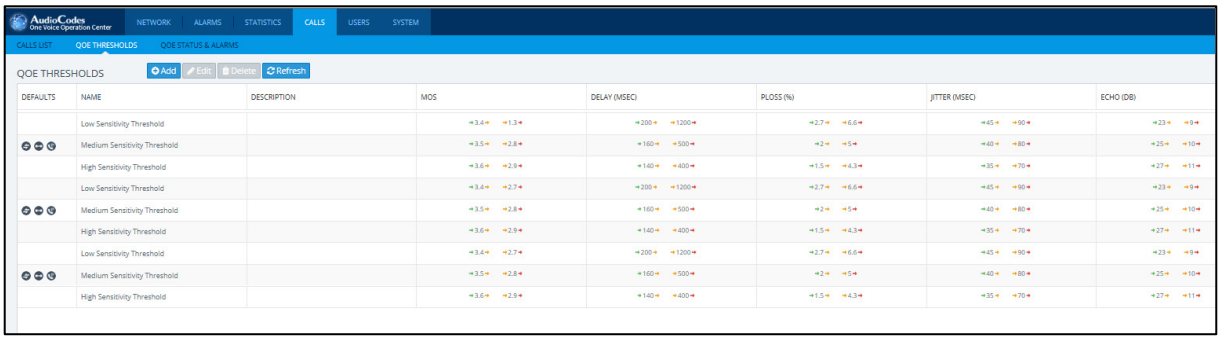
The QoE Thresholds page lets you adding a profile of Quality of Experience threshold values, *per tenant*.

For information about adding a *global* (system) QoE Thresholds template, see Section 4.2.1.3.

➢ To view QoE thresholds profiles:

1. Open the QoE Thresholds page (**Calls** > **QoE Thresholds**).

Figure 8-15: QoE Thresholds Profiles



In the page you can:

- view QoE thresholds profiles and their metrics thresholds (see the sections below)
- add a profile (see Section 8.3.3)
- edit or delete an existing profile (see Section 8.3.4 and 8.3.5)

8.3.1 Understanding the 3 Sensitivity-Level Profiles

The table below shows the monitored parameters MOS, Delay, Packet Loss and Jitter, each associated with each of the 3 sensitivity-level profiles: Low, Default and High. Each parameter's Green-Yellow Threshold and Yellow-Red Threshold differ in association with the configured Profile.

For each monitored parameter, administrators can use the thresholds in the predefined profile, or define their own thresholds.

Table 8-14: Quality Profile Parameters

Parameter (units)	Sensitivity Level	Good-Fair (Green-Yellow) Threshold	Fair-Poor (Yellow-Red) Threshold
MOS	Low	3.4	2.7
	Medium	3.5	2.8
	High	3.6	2.9
Delay (msec)	Low	200	1200
	Medium	160	500
	High	140	400
Packet Loss (%)	Low	2.7	6.6
	Medium	2	5
	High	1.5	4.3
Jitter (msec)	Low	45	90
	Medium	40	80
	High	35	70
Echo (dB)	Low	23	9
	Medium	25	10
	High	27	11

8.3.2 Understanding How Call Color is Determined

This section helps you understand how Lync call color is determined. As shown in the previous section, a default profile is assigned to each Front End server, which you can change. (No profile is attached to the Mediation Server or Edge Server).

A default profile is also assigned to each Link, which you can change and apply to each Link as shown in the previous section.

8.3.2.1 Link Profile as Determinant

Each call comprises one or more legs. Each leg is assigned a color, determined by its associated Link profile. If a call leg passes over few Links and each has a different profile, each Link has its own color (displayed in the Summary Panes) corresponding to its profile. However, the call leg's color is set as the worst color received from all the Links profile; the Call Details screen shows what profile caused the leg color. If a call leg does not match any of the Links, its color is defined based on the FE profile. The color representing worst quality among all the legs will be the call color. (If a call comprises only from one leg, the color of the leg will be the call color).

8.3.2.2 MOS Metric as Determinant

Each profile can be configured with a set of quality metrics (MOS / Packet Loss / Jitter / Delay / Echo). Each call leg's color is determined at the end of the call using its reported metrics. If MOS is reported, the leg will be determined by the MOS' color; if not, the color representing worst quality will be the leg's color. If any of the call leg's reported metrics are excluded from the profile, color calculations will ignore this metric.

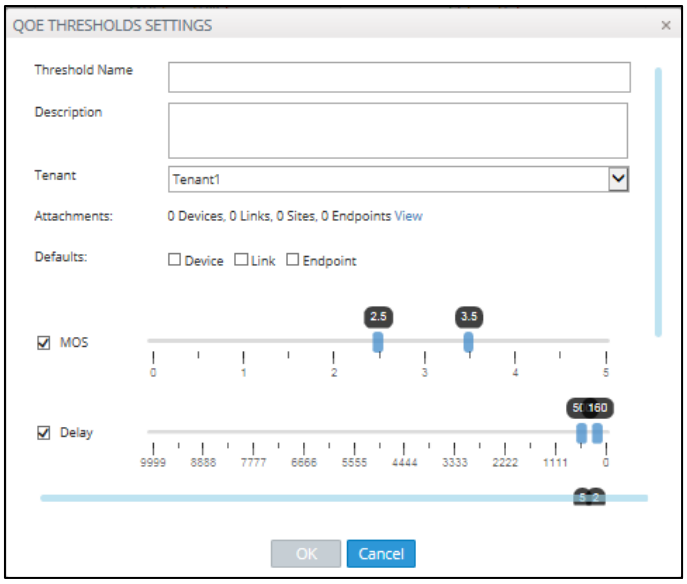
8.3.3 Adding a QoE Thresholds Profile per Tenant

You can add a QoE Thresholds profile.

➢ **To add a QoE thresholds profile:**

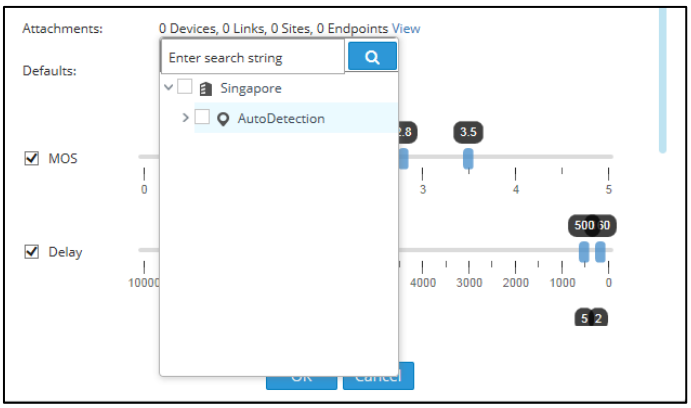
1. Open the QoE Thresholds page (**Calls** > **QoE Thresholds**).
2. Click **Add**.

Figure 8-16: QoE Thresholds Settings



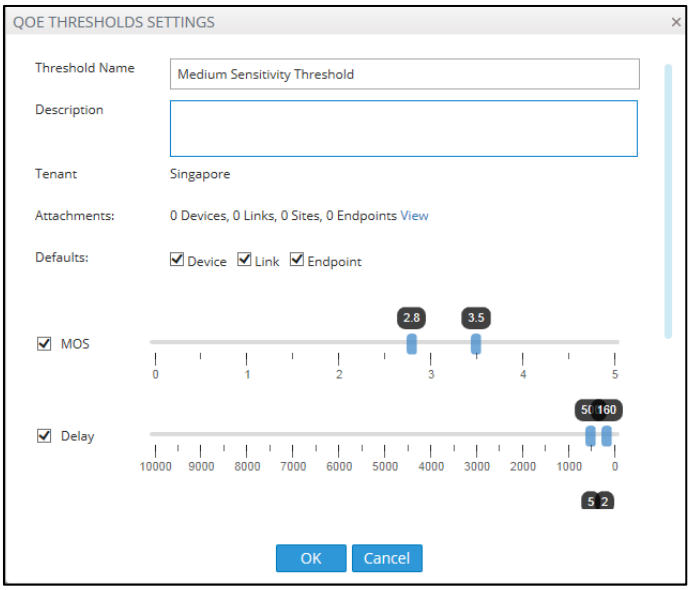
3. Provide an intuitive name for the profile. Use the names of the three predefined QoE profiles, displayed in Figure 8-15, as a reference.
4. In the 'Description' pane, provide an intuitive, friendly description to facilitate future operator management.
5. From the 'Tenant' dropdown, select the tenant for whom you're customizing this profile.
6. Next to 'Attachments', click the **View** button.

Figure 8-17: Attachments



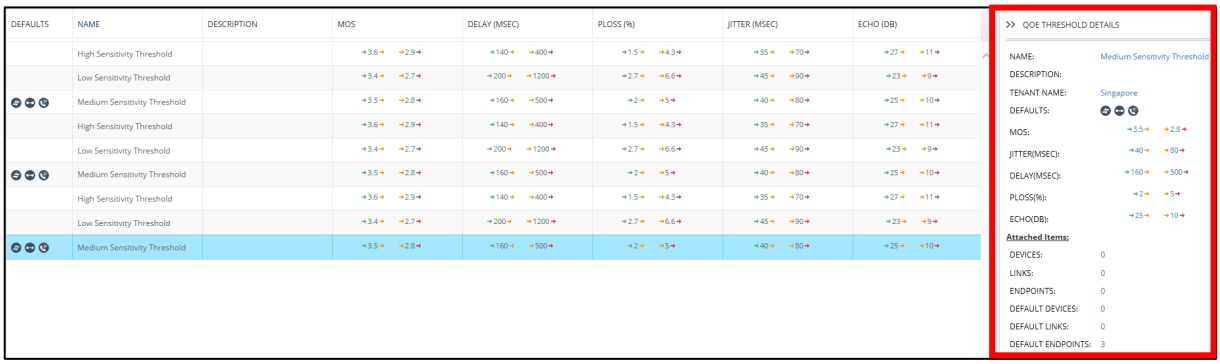
7. Expand the tenant to navigate to and select the entities to which to attach this QoE thresholds profile (devices, links or endpoints).
8. Next to 'Defaults', select:
   - **Devices** in order to set this QoE thresholds profile as the default for all devices. If selected, then every new device that is added to the tenant is automatically set with this QoE thresholds profile and all *previous* devices' default QoE thresholds profile is set with this new default profile.
   - **Links** in order to set this QoE thresholds profile as the default for all links. If selected, then every new link that is added to the tenant is automatically set with this QoE thresholds profile and all *previous* links' default QoE thresholds profile is set with this new default profile.
   - **Endpoints** in order to set this QoE thresholds profile as the default for all endpoints. If selected, then every new endpoint that is added to the tenant is automatically set with this QoE thresholds profile and all *previous* endpoints' default QoE thresholds profile is set with this new default profile.
9. Specify which voice quality metrics to include in or exclude from the profile. You can exclude, for example, the metrics of 'MOS', 'Delay' and 'Echo', but include 'Packet Loss' and 'Jitter'. To *exclude* a voice quality metric, clear its check box. By default, all voice quality metrics are included in the profile.
10. To configure the MOS metric's thresholds (for example), click the bar or drag the markers. Each bar unit increments or decreases the threshold by **0.1** (MOS, Packet Loss) or **1** (Delay, Jitter, Echo). Configure the other metrics' thresholds in the same way. Figure 8-18 below shows the 'Medium Sensitivity Threshold' profile as an example.

Figure 8-18: Medium Sensitivity QoE Thresholds Profile



11. Click **OK**; the profile is displayed in the QoE Thresholds page shown in Figure 8-15.
12. In the page, select the profile; the QoE Threshold Details are displayed.

Figure 8-19: QoE Threshold Details



The QoE Threshold Details window displays under **Attached Items** the number of devices / links / endpoints to which the selected profile is attached.

In the QoE Threshold Details window:

- **x** indicates the *lower* threshold of the quality metric:
  - Up until the threshold value of **x** is reached = **green** = good voice quality
  - If the threshold value of **x** is exceeded = **yellow** = fair voice quality
- **y** indicates the *upper* threshold of the quality metric:
  - Up until the threshold value of **y** is reached = **yellow** = fair voice quality
  - If the threshold value of **y** is exceeded = **red** = poor voice quality

8.3.4 Editing a QoE Thresholds Profile per Tenant

You can edit an existing QoE Thresholds profile per Tenant.

➢ **To edit a QoE Thresholds profile:**

- In the QoE Thresholds page (**Calls** > **QoE Thresholds**), select the profile to edit and click **Edit**; the screen shown in Figure 8-16 opens. Refer to the instructions under the figure.

8.3.5 Deleting a QoE Thresholds Profile per Tenant

You can delete a QoE Thresholds profile per Tenant.

➢ **To delete a QoE Thresholds profile per Tenant:**

- In the QoE Thresholds page (**Calls** > **QoE Thresholds**), select the profile to delete and click **Delete**. Note that default profiles cannot be deleted.

8.4 Managing QoE Status and Alarms per Tenant

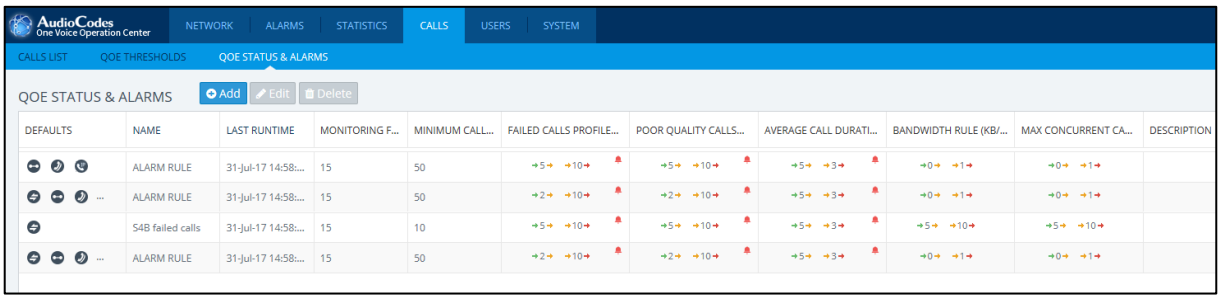
The QoE Status & Alarms page lets you manage QoE statuses and alarms *per tenant*.

For information about managing *global* (*system-wide*) QoE statuses and alarms, see Section 4.2.1.4.

➢ **To view QoE statuses and alarms per tenant:**

- From under the Calls menu, open the QoE Status & Alarms page (**Calls** > **QoE Status & Alarms**).

Figure 8-20: QoE Status & Alarms



The information displayed in the page above - QoE Status & Alarms *per tenant* – is identical to the information displayed in the *global* (*system-wide*) QoE Status & Alarms page. See Section 4.2.1.4 for a detailed description.

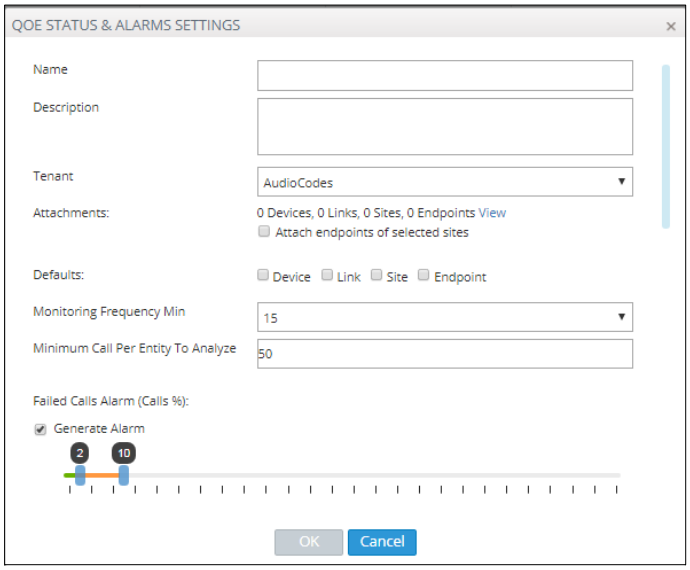
8.4.1 Adding a QoE Alarm Rule per Tenant

You can add a new rule for a QoE alarm per tenant.

➢ **To add a new QoE alarm rule per tenant:**

1. From the QoE Status & Alarms page shown in the figure above, open the Alarm Rule Details screen (**Calls** > **QoE Status & Alarms** and then click **Add**).

Figure 8-21: QoE Alarm Rule



2. Configure the parameters using the table below as reference.

Table 8-15: QoE Alarm Rule

Parameter	Description
Name	Enter an operator-friendly alarm rule name to facilitate intuitive effective management later.
Description	Describe the alarm rule to facilitate effective management later.
Attachments	Click **View** and then navigate to and select the entities to which to attach this QoE Alarm Rule: devices, links, sites and/or endpoints.
Defaults	Select the **Device**, **Link**, **Site** and/or **Endpoint** monitoring filter. • If you select **Link**, the links selection popup opens; select the links to monitor (the default is **All Selected**). • If you select **Device**, the device selection popup opens; select the devices to monitor (the default is **All Selected**).
Monitoring Frequency (min)	Determines how frequently the OVOC automatically performs data analysis. Defines every 15 (default), 30 or 60 minutes.
Minimum Calls to Analyze	Defines the number of calls to analyze. Default = 50 calls. Up to 1000 calls can be defined. If the number of calls made doesn't exceed the defined # of calls to analyze, the OVOC won't perform data analysis.
Failed Calls Alarm	Select the **Generate Alarm** option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: **5**% of calls (default); if this threshold is exceeded, the alarm is triggered. Major Threshold: **3**% of calls (default); if this threshold is exceeded, the alarm is triggered.
Poor Quality Calls Alarm	Select the **Poor Quality Calls Alarm** option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: **10**% of calls (default); if this threshold is exceeded, the alarm is triggered. Major Threshold: **8**% of calls (default); if this threshold is exceeded, the alarm is triggered.

Parameter	Description
Avg Call Duration Alarm	Select the **Avg Call Duration Alarm** option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: **5** seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered. Major Threshold: **10** seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered.
Bandwidth Alarm	Select the **Bandwidth Alarm** option to active the alarm. Clear the option to deactivate the alarm. Major Threshold: if the bandwidth falls below or exceeds the value you configure (minimum of **0** Kbps and a maximum of **1000000** Kbps), an alarm of Major severity is triggered. Critical Threshold: if the bandwidth falls below or exceeds the value you configure (minimum of **0** Kbps and a maximum of **1000000** Kbps), an alarm of Critical severity is triggered. • You must configure a *higher* value for the *Critical* Threshold than for the Major Threshold. • You can configure a minimum of **0** Kbps and a maximum of **1000000** Kbps for either the Critical or the Major Threshold, so long as the value you configure for the *Critical* Threshold is higher than the value you configure for the Major Threshold.
Max Concurrent Calls Alarm	Select the **Max Concurrent Calls Alarm** option to active the alarm. Clear the option to deactivate the alarm. Major Threshold: if the the number of concurrent calls falls below, or exceeds, the value you configure (minimum of **0** and a maximum of **100000**), an alarm of Major severity is triggered. Critical Threshold: if the number of concurrent calls falls below, or exceeds, the value you configure (minimum of **0** and a maximum of **100000**), an alarm of Critical severity is triggered. • You must configure a *higher* value for the *Critical* Threshold than for the Major Threshold. • You can configure a minimum of **0** and a maximum of **1000000** for either the Critical or the Major Threshold, so long as the value you configure for the *Critical* Threshold is higher than the value you configure for the Major Threshold.

3. Click **OK**; the QoE alarm rule is now listed in the QoE Status & Alarms page.

8.4.2 Editing a QoE Alarm Rule per Tenant

You can edit a QoE alarm rule per tenant.

➢ **To edit a QoE alarm rule per tenant:**

- In the QoE Status & Alarms page (**Calls** > **QoE Status & Alarms**), select the QoE alarm rule to edit and then click **Edit**; the Alarm Rule Details screen opens displaying parameters identical to those displayed when adding a rule. Use the table above as reference.

8.4.3 Deleting a QoE Alarm Rule

You can delete a QoE alarm rule if necessary.

➢ **To delete a QoE alarm rule:**

- In the QoE Status & Alarms page (**Calls** > **QoE Status & Alarms**), select the QoE alarm rule to delete and then click **Delete**. Note that default QoE alarm rules cannot be deleted.

9 Getting Information on Users Experience

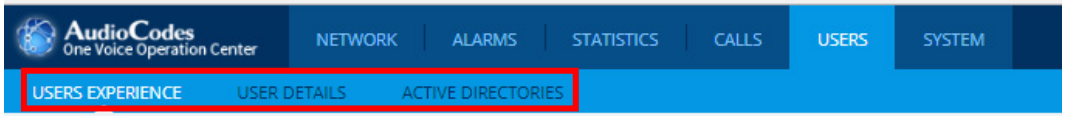
This section shows how to get information about how end users experience IP network telephony.

Note: 'End users' refers to an enterprise's employees. By contrast, 'operators' refers to administrators managing the enterprise's network using the OVOC.

Section 9.1 shows how to add an Active Directory in the Active Directories page.

Section 9.2 and 9.3 show how to get user experience info in the Users Experience page.

Section 9.1 shows how to manage end users in the User Details page.



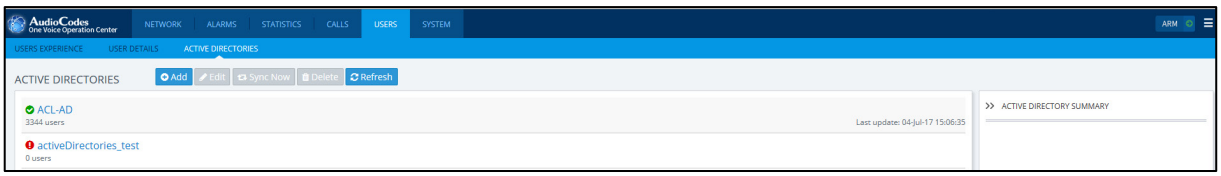
9.1 Adding an Active Directory to the OVOC

You can add an Active Directory to the OVOC.

➢ **To add an Active Directory to the OVOC:**

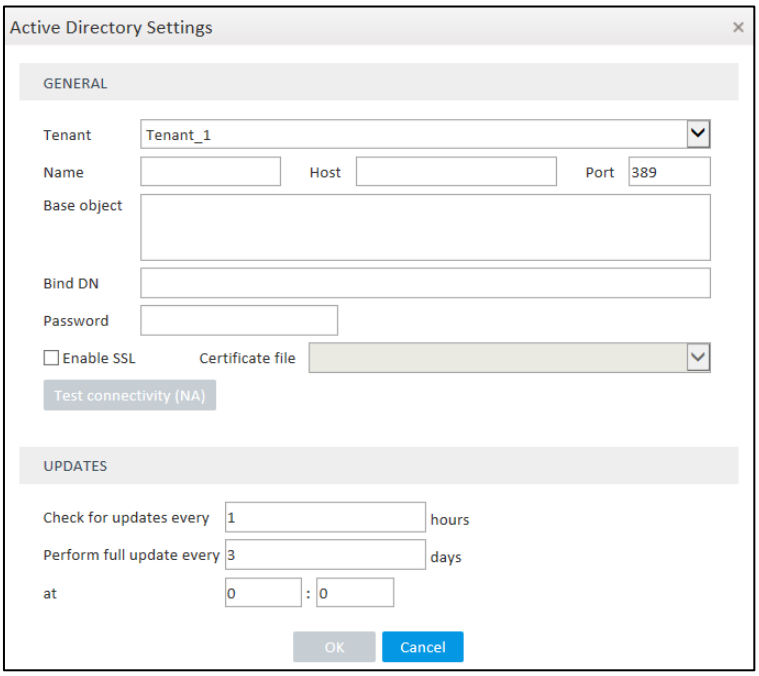
1. Open the Active Directory page (**Users** > **Active Directories**).

Figure 9-1: Active Directories



2. Click **Add**.

Figure 9-2: Active Directory Settings



3. Configure the AD settings using the table below as reference.

Table 9-1: Active Directory Settings

Setting	Description
Tenant	From the dropdown, select the tenant configured as shown under Section 5.1.
Name	Enter an intuitive name for the AD to facilitate operator management later.
Host	Consult with the IT manager responsible for the AD in your enterprise.
Port	The default is typically 389 but consult with the IT manager responsible for the Active Directory in your enterprise.
Base object	Enterprise employees are listed under branches/departments in a tree structure. Enter in the field the branch/department whose employees the AD manages. The AD will then access only to that (relevant) branch/department's employees. For more information, consult with the IT manager responsible for the Active Directory in your enterprise.
Bind DN	For the 'DN' (Domain Name) field, consult with the IT manager responsible for the Active Directory in your enterprise.
Password	Consult with the IT manager responsible for the AD in your enterprise.
Enable SSL	Select the option to secure the connection with the AD server over SSL; an HTTPS connection between the OVOC and the LDAP server is opened. Clear (default) the option for the connection with the LDAP server to be non-secured.
Certificate file	From the dropdown, select the certificate file that you want to use to secure the SSL connection with the LDAP server. The OVOC authenticates the SSL connection using the certificate. Make sure you load the SSL certificate file, required by the LDAP Active Directory platform, to the Software Manager, as described under Section 4.2.3.
Test connectivity (NA)	Click to test synchronization of the OVOC and the Active Directory databases. You can alternatively click **Sync Now** in the Active Directories page.
Check for updates every….hours	Lets you schedule how frequently synchronization of the OVOC and the Active Directory databases takes place. After synchronization is performed, the OVOC's User Details page is updated to reflect the Active Directory.
Perform full update every….days	Lets you schedule how frequently a full synchronization is performed. Select from a range of 1-7, i.e., once a day (most frequent) to once a week (most infrequent). After synchronization is performed, the OVOC's User Details page is updated to reflect the Active Directory.
At 0:0	Lets you schedule the time at which the full synchronization is performed. After it's performed, the OVOC's User Details page is updated to reflect the Active Directory.

4. Click **OK**.

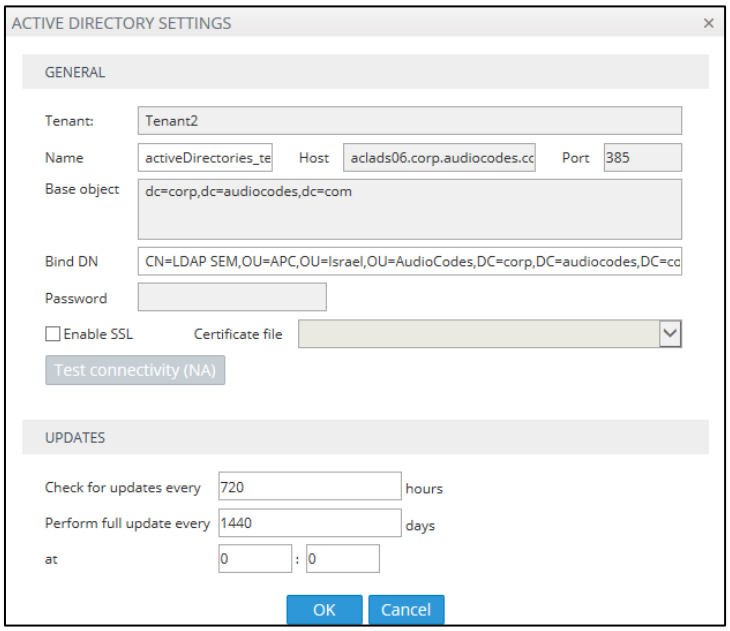
9.1.1 Editing an Active Directory

You can edit an Active Directory after adding one.

➢ **To edit an Active Directory:**

1. Open the Active Directory page (**Users** > **Active Directories**) – see Figure 9-1.
2. Select the Active Directory to edit and click now-enabled **Edit** button.

Figure 9-3: Active Directory Settings



3. Edit using Table 9-1 as reference and then click **OK**.

9.1.2 Deleting an Active Directory

You can delete an Active Directory if necessary.

➢ **To delete an Active Directory:**

1. Open the Active Directory page (**Users** > **Active Directories**) – see Figure 9-1.
2. Select the Active Directory to delete and click now-enabled **Delete** button.

9.1.3 Synchronizing an AD with the AD Server

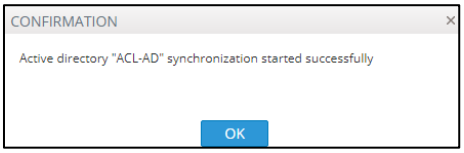
You can manually synchronize an AD with the AD server.

➢ **To synchronize an AD with the AD server:**

1. Open the Active Directories page (**Users** > **Active Directories**).

Figure 9-4: Active Directories

2. Select the AD to synchronize and click **Sync Now**.



3. In the confirmation prompt, click **OK**.

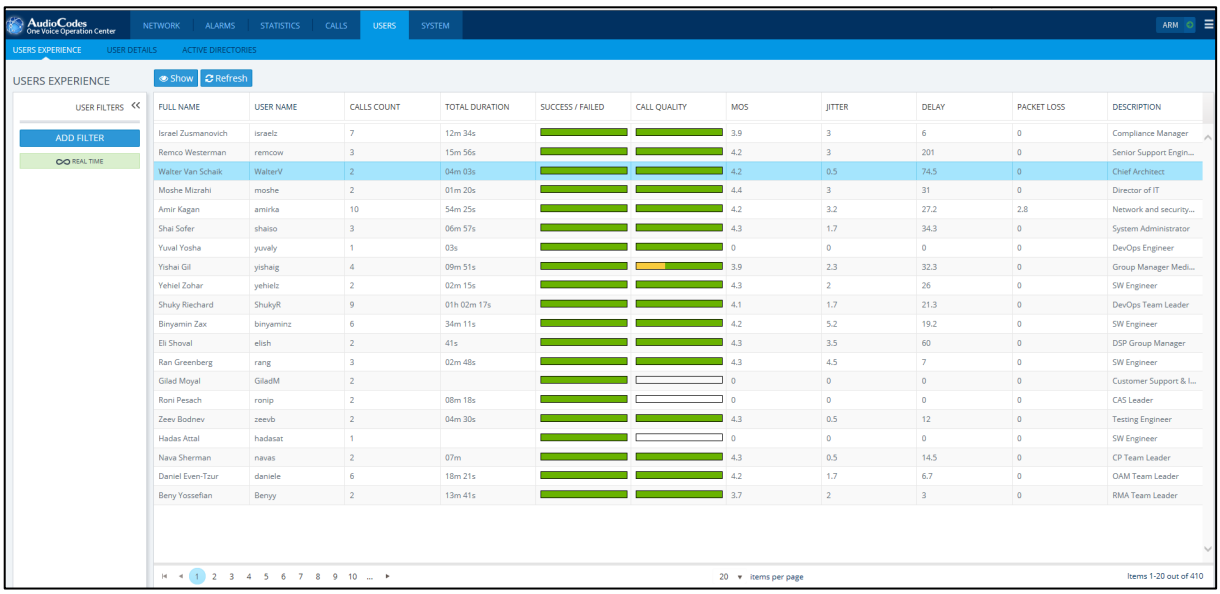
9.2 Assessing Overall End Users Experience

The OVOC enables operators to assess at a glance the overall experience of end users and to tweak the enterprise's telephony network to enhance their experience. Users experience includes statistics related to voice quality (good, fair and poor quality voice) and statistics related to call performance (rate and number of successful versus failed calls).

➢ **To assess end users experience:**

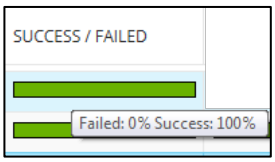
1. Open the Users Experience page (**Users** > **Users Experience**).

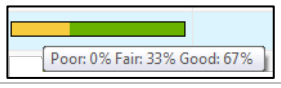
Figure 9-5: Users Experience



2. [Optional] Filter the page to present only information you require. You can filter by Time Range (see Section 6.2.1) or by Users (see Section 9.4.1).
3. Use Table 9-2 as reference to the page.

Table 9-2: Users Experience

Column	Description
Full Name	The first name and the family name of the end user (the employee) in the enterprise.
User Name	The employee's user name, defined by the enterprise's network administrator.
Calls Count	The total number of calls made by the end user (employee).
Total Duration	The total length of time the end user (enterprise employee) spent on the phone.
Success/Failed	Color-coded bar lets you determine at glance the call success/failure rate (percentage) was for end users. Point your cursor over a specific end user's bar to see the rate of successful versus unsuccessful calls. 
Call Quality	Lets you determine at glance end users calls whose voice quality was measured as Good (green), Fair (yellow) or Poor (red).

Column	Description
	Point your cursor over a specific end user's bar to see that specific end user's % of calls whose voice quality was measured as Good (green), Fair (yellow) or Poor (red). 
MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
Jitter	Jitter (in msec) can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
Delay	Delay (or latency) (in msec) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth.
Packet Loss	Lost packets, as a percentage - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Packet Loss can be more than 100%.
Description	The end user's professional position in the enterprise.

4. [Optional] Select an end user's row and then click **Show**; details about that specific user's experience are displayed (see the next section).
5. [Optional] Click **Refresh** to manually synchronize the page with the Active Directory.

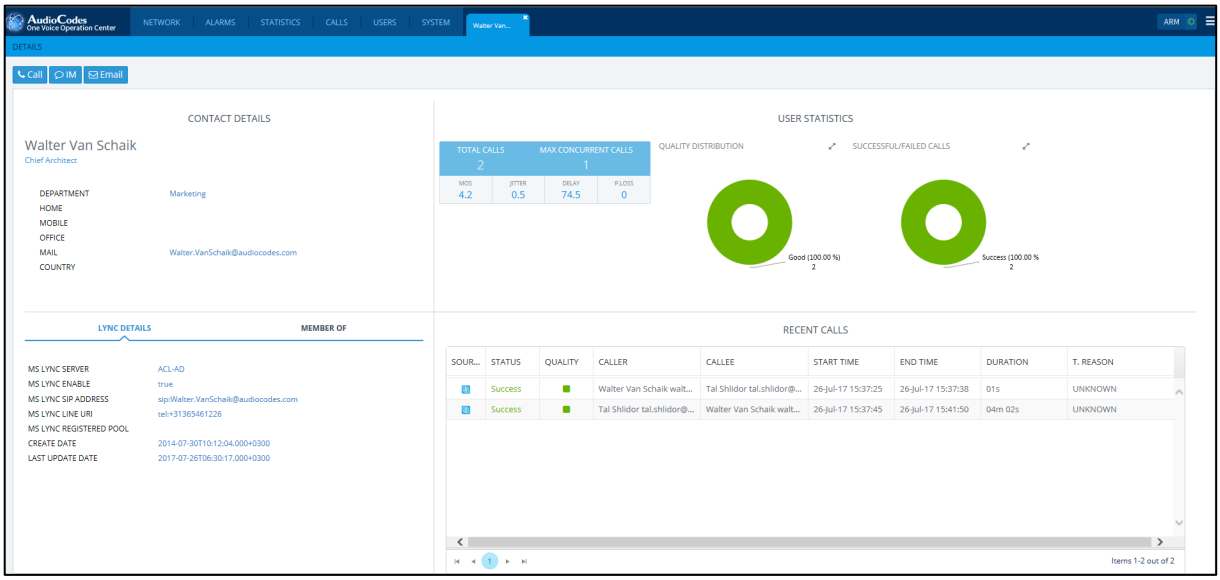
9.3 Assessing a Specific End User's Experience

The OVOC lets operators quickly assess a specific end user's experience, helping operators to tweak the enterprise's telephony network to enhance that experience.

➢ **To assess a specific end user's experience:**

1. Open the Users Experience page (**Users** > **Users Experience**); the page shown in Figure 9-5 opens.
2. Select the row of the end user whose experience you want to assess and then click **Show**; details about this specific end user's experience are displayed.

Figure 9-6: Specific End User's Experience



3. Note that the page shown in Figure 9-6, displaying specific information related to this end user's experience, is automatically dynamically tabbed on the menu bar as a pin (labeled **Walter van…** in the page shown in Figure 9-6), facilitating quick and easy future access and troubleshooting management. Operators can delete the pin from the menu bar at any time.

9.4 Managing End Users

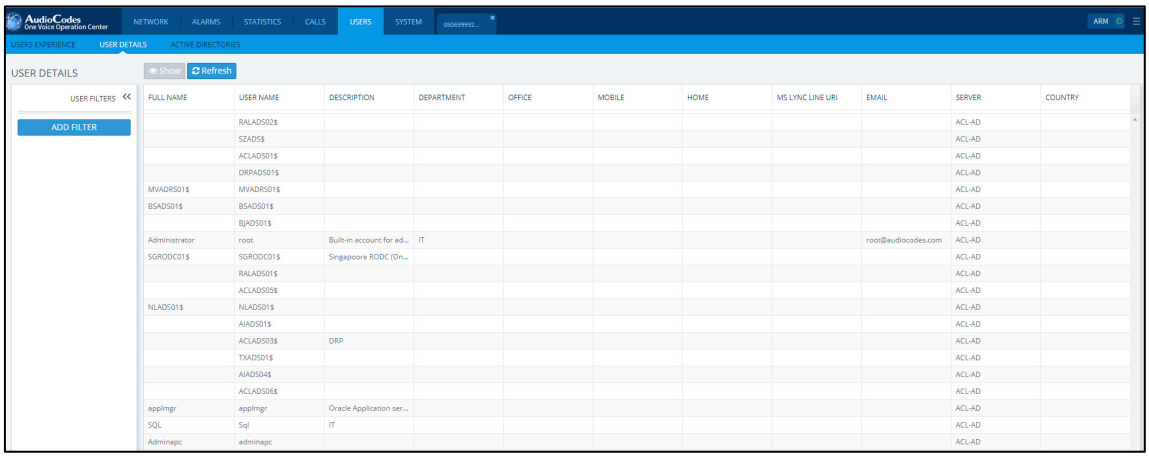
Note: Only OVOC operators with 'Administrator' security level can perform local management of end users.

Usernames and passwords of end users are by default locally stored in the OVOC application's database. The User Details page allows operators to locally manage end users. The page mirrors the Active Directory. Any change to the AD is reflected in the User Details page immediately after synchronization is performed.

➢ **To manage end users:**

1. Open the User Details page (**Users** > **User Details**).

Figure 9-7: User Details

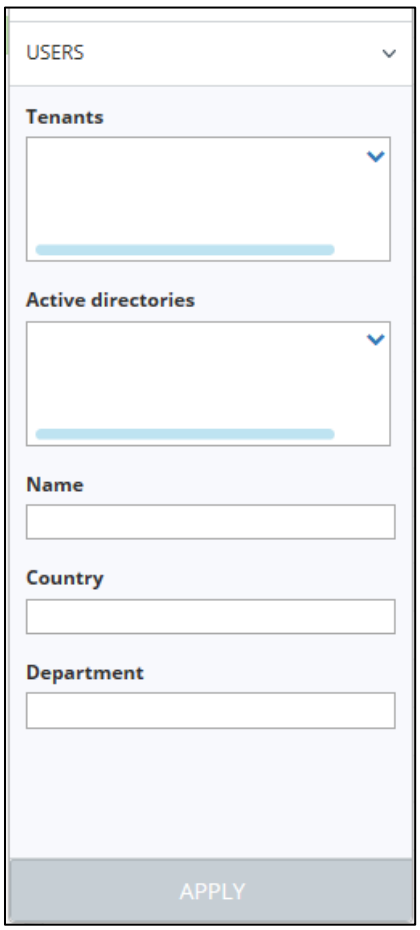


2. Optionally, use filters for quick access to specific users (see the section below).
3. Obtain contact information about end users from under the columns in the table: Full Name, User Name, Description, Department, Office, Mobile, Home, MS Lync Line URI, Email, Server, Country.

9.4.1 Filtering the User Details Page

You can filter the Users Details page using the 'User's filter (click the **Add Filter** button).

Figure 9-8: Users Filter



Use Table 9-3 on the next page as reference.

Table 9-3: 'Users' Filter

Filter	Description
Tenants	From the dropdown, select a configured tenant. Only calls made by and received from users assigned to that tenant will be displayed in the page.
Active directories	From the dropdown, select an Active Directory. Only calls made by and received from users associated with that AD will be displayed in the page.
Name	Enter the name of a user. Only calls made by and received from that user will be displayed in the page.
Country	Enter the name of a country. Only calls made and received by users in that country will be displayed in the page.
Department	Enter the name of a department in the enterprise. Only calls made and received by users in that department will be displayed in the page.

10 Producing Reports

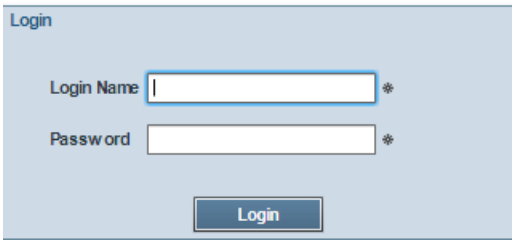
The OVOC features essential reports-generation capability that operators can utilize to distribute session experience data and comparative analyses quickly and effectively to responsible persons within the enterprise and to external authorities associated with the enterprise's IP telephony network, for accurate diagnosis and correction of degraded sessions and for general network optimization. Requirements for the Session Experience Manager (SEM) Reports module are:

- **Microsoft Lync Server** for customers with one Front End server and one SQL server.
  - Up to two **Microsoft Lync** solutions in one SEM application.
  - **Microsoft Lync Server limitation**: When functioning with Lync server pools (FE, Edge and Mediation), the FE server defined in the SEM functions as the monitoring SQL database. After connecting, the SEM presents all Call Details from the Lync network in the SEM's Calls List and Call Details views. When functioning with Lync pools, FE, Edge and Mediation servers cannot be defined in the SEM, so the entire Lync network is presented in the SEM only as a single object, namely, the monitoring SQL database.

➢ **To open the Reports page:**

- Under the Statistics menu, click the **Reports** tab.

Figure 10-1: Login



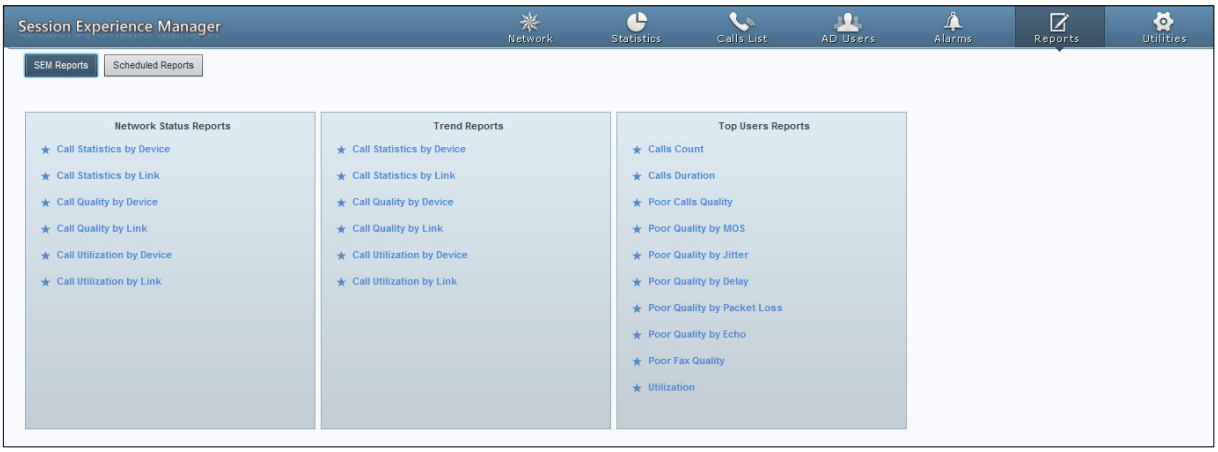
Note: Log in with the same name and password you used to log in to the OVOC.

The default name and password are:

- **acladmin**
- **pass_1234**

The SEM Reports module opens.

Figure 10-2: SEM Reports



Note: Log in with the same name and password you used to log in to the OVOC.

Three categories of reports help users to quickly and thoroughly analyze different aspects of calls made over the VoIP network:

- Network Status Reports
- Trend Reports
- Top Users Reports

Categories 1 and 2 are identical in terms of the information displayed (columns); however the calculation differs.

Category 1 is calculated as a summary of calls made over the entire period for specified entities (devices / links). The x axis represents the specified entities.

Category 2 is calculated per time interval specified, summarizing the same entity in the specified interval. The x axis represents the time interval (hour / day / week / month).

Table 10-1 shows the categories and the reports options in each.

Table 10-1: Reports Categories

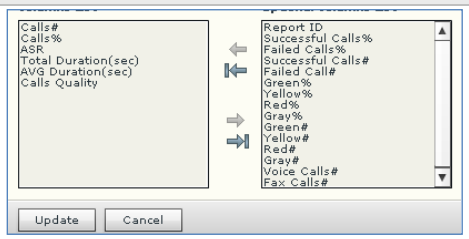
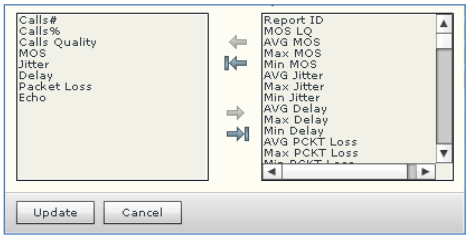
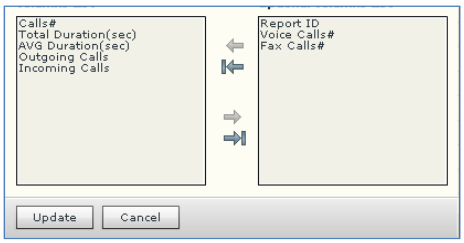
Report Category	Explanation
Network Status Reports ▪ Call Statistics by Device ▪ Call Statistics by Link ▪ Call Quality by Device ▪ Call Quality by Link ▪ Call Utilization by Device ▪ Call Utilization by Link	Displays a summary of key call metrics during a specified time period with a separate row entry for each device/link. Purpose: To compare performance, quality and utilization across devices/links. For example, the 'Call Statistics by Device' report summarizes the % of successful and failed calls and the # of calls that scored in each quality, across specified devices/links. By contrast, a 'Call Quality by Device' report summarizes key metrics affecting voice quality (jitter, delay, packet loss).
Trend Reports ▪ Call Statistics by Device ▪ Call Statistics by Link ▪ Call Quality by Device ▪ Call Quality by Link ▪ Call Utilization by Device ▪ Call Utilization by Link	Displays a summary of key call metrics over specified time intervals of a specified device/link. For example, the 'Calls Trend by Device' report displays 'Number of Calls', 'ASR' and 'Total Duration' in hourly intervals.
Top Users Reports ▪ Calls Count ▪ Calls Duration ▪ Poor Calls Quality ▪ Poor Quality by MOS ▪ Poor Quality by Jitter ▪ Poor Quality by Delay ▪ Poor Quality by Packet Loss ▪ Poor Quality by Echo ▪ Poor Fax Quality ▪ Utilization	Displays users graded according to number of calls made, calls duration, and calls whose quality scored 'Poor' based on specified metrics.

10.1 Using Reports Features

The features below apply to all reports pages across all three reports categories unless stated otherwise:

Table 10-2: Reports Features

Feature	Description
Save as CSV	Lets you save a report as a Comma-Separated Value (CSV) file which represents charts, data bars, sparklines, gauges, indicators, etc., in a standardized, plain-text format easily readable and exchangeable with many applications. You can open the file in a spreadsheet such as Microsoft Excel or use it as an import format for other programs.
Export to PDF	Lets you generate a PDF file of the report reflecting selected filters, columns, graphs, etc.
Filters	Let you specify: • The Time Range for the report to cover (in the Network Status Reports page) • The Time Range and the Interval for the report to cover (in the Trend Report page; Hourly, Daily, Weekly or Monthly) • Devices / Links on which to produce the report • Top 10/20/30 Users on which to produce the report (in the Top Users Report page)
SEM Reports	Click the button at any time to return to the Reports page displaying the three reports categories and the report options available under each. Click an option to produce a report.
Scheduled Reports	Click the button to schedule a report.
Create Report	Displayed after selecting a report to produce in the reports menu. First filter (see above) and then click it; the report is produced and displayed.
Charts view / Table view	Two views are displayed in every report produced: Charts (uppermost) and table (lowermost). Click to expand charts view; table view is eclipsed. Click to revert to both views.
Switch to horizontal / Switch to vertical	Charts are by default displayed vertically, one below the other, in this order: Calls #, Calls %, ASR, Total Duration, AVG Duration and Calls Quality. Use the scrollbar to scroll down from one to the next. They can optionally be displayed horizontally to suit user preference. To display horizontally, click the link. Click next or previous to navigate from chart to chart.
Bar / Linear	[Only applies to Network Status Reports] By default, charts are displayed as bar charts. Click the drop-down to choose linear charts if required.
Add / Remove Columns	Click the icon; optional table view columns are displayed. To add, if required, select an optional column and click or select all and click . To remove a column, select it in the Columns List pane and click or select all and click . Default metrics columns (left pane) and optional metrics columns (right pane) in the Summary/Trend category (except 'Call Quality by Device / Link') are as follows:

Feature	Description
	 Default metrics columns (left pane) and optional metrics columns (right pane) in a 'Call Quality by Device / Link' report in the Summary/Trend category are:  Default metrics columns (left pane) and optional metrics columns (right pane) in the Top Users reports category are:  See under Section 10.1.3 for variations across reports in the Top Users Reports category.
 Show Column Graphical Representation Display column as chart	Table column headers display this icon. Click one to display the metric as a chart. If the chart is already open, you're notified. After report generation, the table's ASR metric column is the only one displayed as a chart in Charts view.
Table Bottom Line (Total)	The table's bottom line shows column's total. For example: • Calls # column's bottom line shows the total sum of all counts of all calls on all devices / links • ASR column's bottom line shows the average success rate of the average success rates of all devices / links. 'Total' is calculated according to the measured parameter. It can be SUM, AVG, MIN or MAX.
Search	Users can use the 'Search' option to search for and find precise information related to a query. When information related to the search query is found, the report exclusively displays only that information.

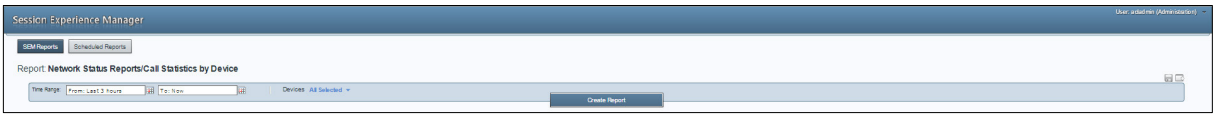
10.1.1 Producing a Network Status Report

Network Status Reports show the sum totals, over the entire period, of calls performance scores, quality scores, #s, %s, total duration and average duration (default metrics). Reports in this category are identical in terms of metrics measured. Metrics columns can optionally be added / removed (see 'Add / Remove Columns' in Table 10-2).

➢ **To produce a Network Status Report:**

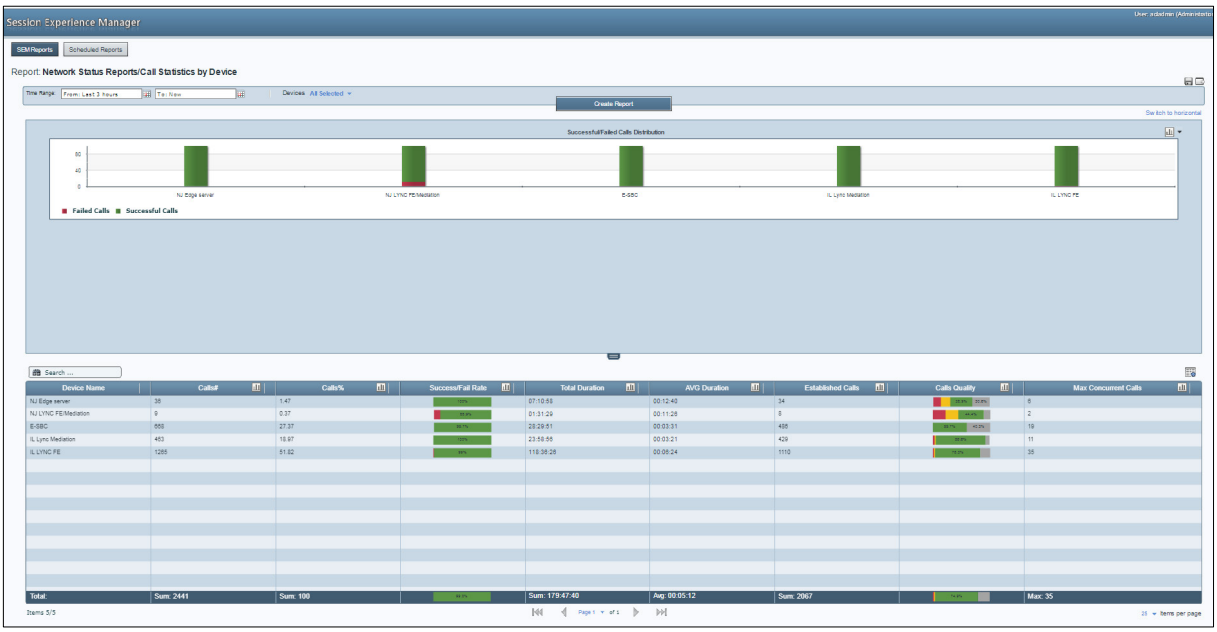
1. Click an option in the 'Network Status Reports' category, for example, click the first option, i.e., Call Statistics by Device.

Figure 10-3: Create Report



2. Filter for 'Time Range' and 'Devices'.
3. Click the **Create Report** button:

Figure 10-4: Network Status Report – Call Statistics by Device

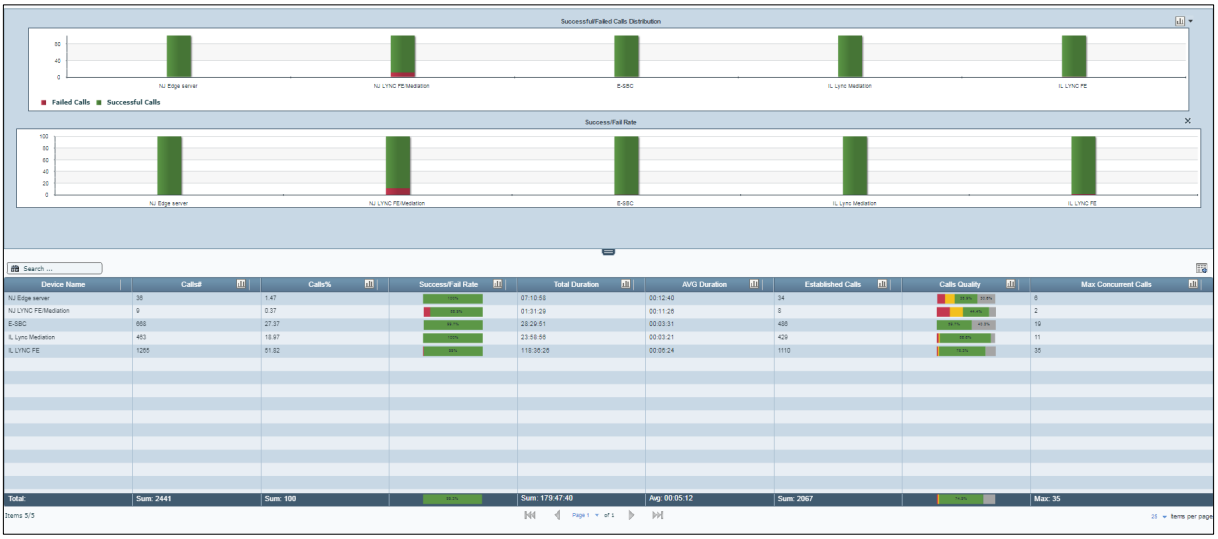


Following report generation, the Success/Fail Rate column is the only one displayed in charts view.

➢ **To display a metric as a chart:**

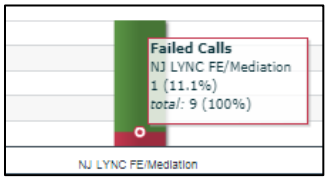
- In the table, click in the metric's column header. For example, click in the Success/Fail Rate column header; the Success/Fail Rate chart is displayed:

Figure 10-5: Displaying the Success/Fail Rate Chart

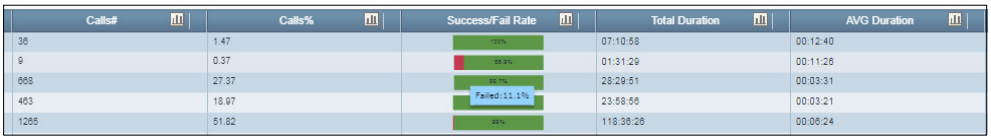


In a Network Status Report you can:

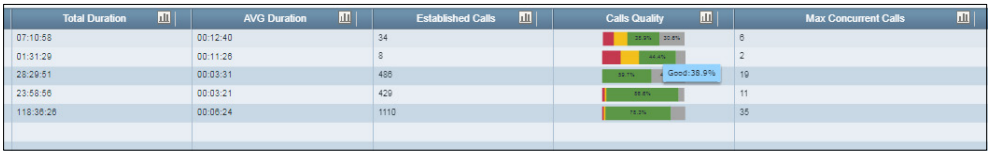
- Click the Switch to horizontal link (see Table 10-2) to switch from vertical view (default) to horizontal view.
- Click t to expand the charts pane. Click it again to contract it.
- Click to switch from bar charts (default) to linear charts. Select from the drop-down (see 'Charts view / Table view' in Table 10-2).
- Click to add/remove a column to/from the table (see 'Add / Remove Columns' in Table 10-2).
- See in the chart which entities registered the highest failed / successful calls rate.
- See in the table on which entities most calls were made, what % of calls were made on each, on which entities most failed / successful calls were made, on which entities most call time was recorded, on which entities the average call duration was longest / shortest and on which entity voice quality scored highest (green = good, yellow = fair, red = poor, grey = unknown).
- See in the chart an entity's success / fail rate (%). Point your cursor over a color in a bar (green = successful, red = failed):



- See in the table an entity's success / fail rate (%). Point your cursor over the entity's row (green = successful, red = failed):



- See in the table quality scores by pointing your cursor over a color in the entity's Calls Quality row (green = good, yellow = fair, red = poor, grey = unknown):



Default and optional table columns in Network Status Reports are:

Table 10-3: Table Columns in Network Status Reports

Network Status Report Type	Default Columns	Optional Columns
Call Statistics by Device	Name, Calls #, Calls %, Success/Fail Rate, Total Duration, AVG Duration, Established Calls, Calls Quality, Max Concurrent Calls	Report ID Successful/Failed Calls % Successful/Failed Calls # Good/Fair/Poor/Unknown % Good/Fair/Poor/Unknown # Voice Calls # Fax Calls # Total Duration AVG Duration
Call Quality by Device	Name, Voice Calls #, Calls %, Calls Quality, MOS, Jitter, Delay, Packet Loss, Echo	Report ID AVG/Max/Min MOS/Jitter/Delay/Packet Loss/Echo AVG SNR Good/Fair/Poor/Unknown % Good/Fair/Poor/Unknown # MOS/Jitter/Delay/Packet Loss/Echo Good/Fair/Poor/Unknown % MOS Calls # Jitter Calls # Delay Calls # Packet Loss Calls # Echo Calls # SNR Calls #
Call Utilization by Device	Name AVG Total Kbps AVG Rx Kbps AVG Tx Kbps AVG Packet Loss	Report ID Calls # Packet Loss Calls #

Note: The table above shows call statistics, quality and utilization *by device*. The same default and optional columns apply to call statistics, quality and utilization *by links*, but in terms of *streams* rather than *calls*.

- You can re-filter and re-run the report (see 'Filters' in Table 10-2).
- You can generate another report. Click the SEM Reports button.
- You can schedule a report. Click the Scheduled Reports button (for details see Section 10.2).

10.1.2 Producing Trend Reports

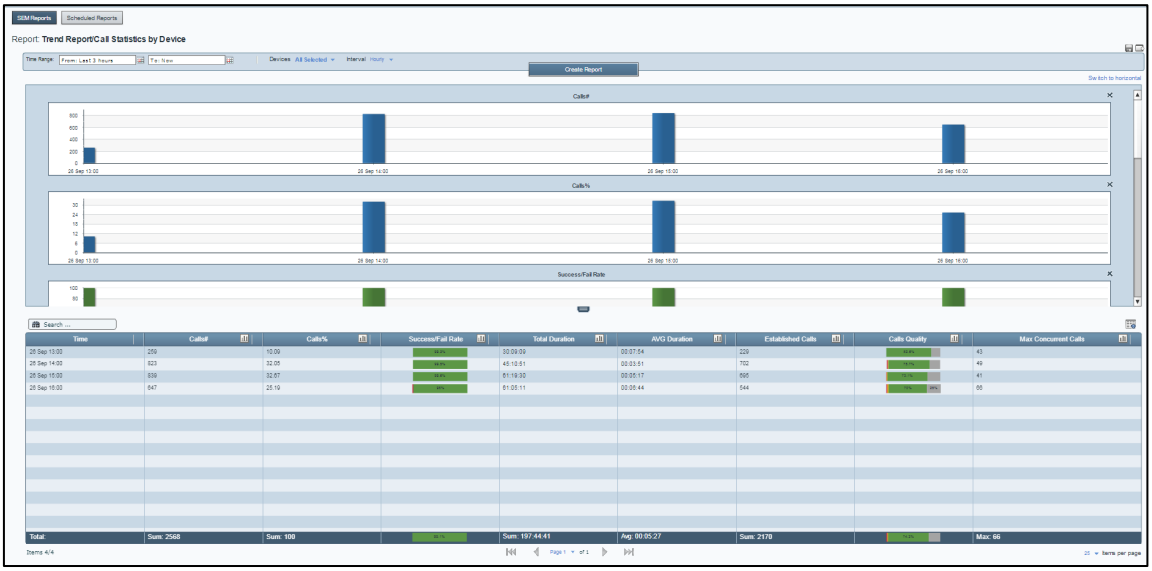
Trend reports show general tendencies over intervals of calls performance, quality, #s, %s, total duration and average duration (default metrics measured).

Reports in this category are identical in terms of metrics columns displayed. Columns can optionally be added / removed (see 'Add / Remove Columns' in Table 10-2).

➢ To produce a trend report:

1. Click an option in the 'Trend Reports' category, e.g., the first; the 'Run now' page opens
2. Filter for 'Time Range' and 'Devices'. For the 'Interval' filter select Hourly, Daily, Weekly or Monthly.
3. Click **Create Report**.

Figure 10-6: Trend Reports – Call Statistics by Device



In a Trend Report you can:

- See when most/least calls were made, how many, % of total, each period's success/fail rate and each period's quality scores.
- Click the Switch to horizontal link to switch from vertically viewed charts (default) to horizontally viewed charts (see Table 10-2).
- Click to switch from bar (default) to linear charts. Select from the drop-down (see 'Charts view / Table view' in Table 10-2).
- Click in a column header in the table to display that column as a chart (see 'Show Column Graphical Representation' in Table 10-2)
- Click to add a column to table view or remove a column from table view (see 'Add / Remove Columns' in Table 10-2). Default columns and optional columns are identical to the 'Call Statistics by Device/Link' and 'Call Quality by Device/Link' reports in the Network Status Reports category.
- Use the pager to navigate to a page if there are multiple pages.
- Re-filter and re-run the report (see 'Filters' in Table 10-2)
- Export the report to PDF. Click (see 'Export…' in Table 10-2)
- Save the report as a CSV file. Click (see 'Save…' in Table 10-2)
- Choose to produce another report by clicking the SEM Reports button.

10.1.3 Producing Top Users Reports

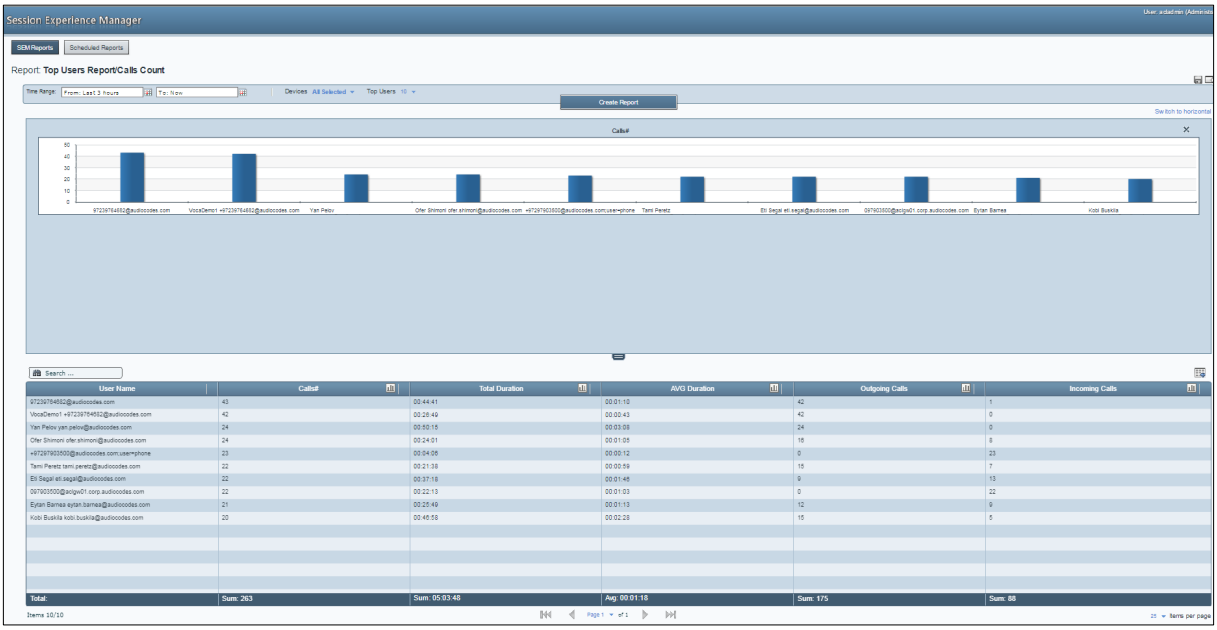
Top Users reports display the top 10, 20 or 30 users in terms of # of calls made, total duration, average duration, outgoing calls and incoming calls (default metrics measured).

Reports in this report category are identical in terms of metrics columns displayed. Metrics columns can optionally be added / removed (see 'Add / Remove Columns' in Table 10-2).

➢ To produce a top users report:

1. Click an option in the 'Top Users Reports' category, for example, click the first report option, i.e., Calls Count; the 'Run now' page opens.
2. Filter for 'Time Range' and 'Devices'. For the 'Top Users' filter, select 10, 20 or 30.
3. Click **Create Report**.

Figure 10-7: Top Users Report – Calls Count



In a Top Users Report you can:

- Save the report as a CSV file. Click (see 'Save…' in Table 10-2)
- Export the report to PDF. Click (see 'Export…' in Table 10-2)
- Click the Switch to horizontal link to switch from vertically viewed charts (default) to horizontally viewed charts (see Table 10-2)
- Click in a column header in the table to display that column as a chart (see 'Show Column Graphical Representation' in Table 10-2)
- Click to add a column to table view or remove a column from table view (see 'Add / Remove Columns' in Table 10-2).

Default and optional table columns in Top Users reports are:

Table 10-4: Table Columns in Top Users Reports

Top Users Report Type	Default Columns	Optional Columns
Calls Count	User Name, Calls #, Total Duration, Average Duration, Outgoing Calls, Incoming Calls	Report ID, Voice Calls #/Fax Calls #, Total Duration (sec), AVG Duration (sec)
Calls Duration	User Name, Total Duration, Calls #, Average Duration, Outgoing Calls, Incoming Calls	Report ID, Total Duration (sec), AVG Duration (sec)
Poor Calls Quality	User Name, Poor Quality Calls, Calls #, Calls Quality	Report ID Unknown / Good / Fair / Poor % Fair # Poor #
Poor Quality by MOS / Jitter / Delay / Packet Loss / Echo	User Name, AVG MOS / Jitter / Delay / Packet Loss / Echo, Calls #, Total Duration	Report ID MOS / Jitter / Delay / Packet Loss / Echo Calls # Total Duration (sec)
Poor Fax Quality	User Name, Poor Quality Faxes, Poor Quality Pages, Total Faxes, Total Pages	Report ID
Utilization	User Name, Total, RX, TX	Report ID

- Use the pager to navigate if there are multiple report pages.
- Re-filter and re-run the report (see 'Filters' in Table 10-2)
- Choose to produce another report by clicking the SEM Reports button.

10.2 Scheduling a Report

You can schedule the SEM to automatically produce a report periodically.

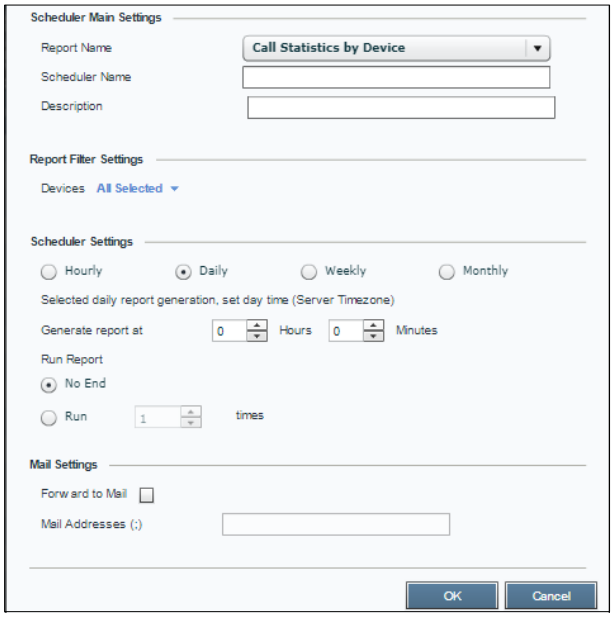
➢ **To schedule a report:**

1. Click the Reports icon; the SEM Reports page opens (see Figure 10-2)
2. Click the **Scheduled Reports** button.

Figure 10-8: Scheduled Reports

3. Click to add a schedule.

Figure 10-9: Scheduler



4. Under 'Report Name', select a report to schedule from the 'Report' drop-down list. All reports under all three report types are listed.
5. In the 'Scheduler Name' field define a name to help you easily identify the schedule.
6. In the 'Description' field, provide a description to help you distinguish this schedule from others.
7. Under 'Report Filter' you can filter the devices on which the report which you're scheduling will be produced. By default, all devices will be included. Click All Selected to change the default. For detailed information on how to filter devices, see Section 6.2.1.3.
8. Under 'Report Frequency', select either Hourly, Daily (default), Weekly or Monthly. If the frequency you select is Daily, set the 'Time'.
9. Under 'Run Times', select Unlimited or Limit to limit the schedule to a limited number of report run times (you can limit to up to 100 run times).
10. Under 'Forward Report', select the Mail option for the report to be automatically forwarded to your email address.
11. In the 'Mail Addresses' field, define the email address/addresses to which to automatically forward the report.
12. Click OK; the report is scheduled; you can expect the first to arrive in your mail according to schedule.

10.2.1 Viewing a Scheduler Generated Report

You can view a report generated by the scheduler.

➢ **To view a report generated by the scheduler:**

1. In the Scheduled Reports page under the Reports column (see Figure 10-8), click the Generated hyperlink in the row of the report generated by the scheduler; the Report Generated by Scheduler opens (see the figure below).

Figure 10-10: Report Generated by Scheduler

2. Click **Show**; the report is generated according to the scheduler.

10.2.1.1 Saving the File of a Scheduler Generated Report

You can save the file of a report generated by the scheduler.

➢ **To save the file:**

1. In the Report Generated by Scheduler (see Figure 10-10), click Save Report File.
2. Select the location on your pc in which to save the file and click Save.

10.2.1.2 Deleting the File of a Scheduler Generated Report

You can delete the file of a report generated by the scheduler.

➢ **To delete the file:**

1. In the Report Generated by Scheduler page (see Figure 10-10), click Delete File; you're prompted 'Delete Generated Report File?'
2. Click Yes; the file is deleted.

10.2.2 Editing a Schedule

You can edit a report schedule.

➢ **To edit a schedule:**

1. In the Scheduled Reports page (see Figure 10-8), click Update Scheduler; the Scheduler opens (see Figure 10-9).
2. Edit the reports schedule and then click **OK**; you're prompted *Previous attachments will be deleted. Are you sure you want to continue?*
3. Click **Yes**; the edited schedule is displayed in the Scheduled Reports page.

10.2.3 Deleting a Schedule

You can delete a report schedule.

➢ **To delete a schedule:**

1. In the Scheduled Reports page (see Figure 10-8), click Delete Scheduler; you're prompted 'Are you sure?'.
2. Click Yes; the report schedule is deleted.

10.2.4 Manually Running or Pausing a Schedule

You can manually run or pause a report schedule.

➢ **To manually run a schedule:**

- In the Scheduled Reports page (see Figure 10-8), click Run Scheduler; the icon changes to and the report scheduler is run.

➢ **To manually pause a schedule:**

- Click Pause Scheduler; the icon reverts to and the scheduler is paused.

A AudioCodes IP Network Telephony Equipment

The table below shows the supported AudioCodes' IP network telephony equipment.

Table A-1: Supported AudioCodes IP Network Telephony Equipment

Supported IP Network Telephony Equipment	Description
   MediaPack	**MP-1xx:** Analog VoIP devices featuring up to 24 analog ports connected directly to an enterprise PBX (FXO), to phones, or to fax (FXS). Support up to 24 simultaneous calls. **MP-20x:** VoIP Gateway. An all-in-one unit featuring (depending on model) a VoIP adapter, FXS lines, FXO interfaces, Ethernet LAN interfaces (with an internal Layer-2 switch), and Ethernet WAN interface. (See product documentation for detailed information)
 Mediant 500 E-SBC **Mediant 500L E-SBC**	Members of AudioCodes' family of Enterprise Session Border Controllers. Enable connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. Provide VoIP SBC functionality. Offer enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.
 Mediant 500 MSBR **Mediant 500L MSBR** **Mediant 800 MSBR** **Mediant 1000 MSBR**	These Multi-Service Business Routers are networking devices that combine multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server. Stand Alone Survivability (SAS) functionality offers service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients, along with PSTN fallback in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX. The devices also provide an integrated Open Solution Network (OSN) Server module. The OSN can host a variety of third-party applications such as IP-PBX, Call Center, and Conferencing. (See the specific product documentation for detailed information)

Table A-1: Supported AudioCodes IP Network Telephony Equipment

Supported IP Network Telephony Equipment	Description
 Mediant 500 Enterprise Session Border Controller (E-SBC)	Member of AudioCodes' family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. Provides VoIP SBC functionality. Offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.
 Mediant 2600 E-SBC	Member of AudioCodes' family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC that provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. The SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.
 AudioCodes Mediant Software Enterprise Session Border Controllers	Mediant Software E-SBCs are pure-software products, enabling connectivity and security between enterprises' and service providers' VoIP networks. Includes the following product variants: **Mediant Server Edition SBC:** x86 server-based platform, which must be installed on a server that complies to the specified hardware requirements. **Mediant Virtual Edition SBC:** Installed and hosted in a virtual machine environment that complies to specified requirements.
Mediant Cloud Edition	The OVOC supports AudioCodes' Mediant Cloud Edition. The feature is offered by the Mediant VE SBC in AWS-based environments. It provides similar functionality to the Media Transcoding Cluster feature but is in the cloud, and its Media Components handle transcoding as well as all media directly, without traversing the Mediant VE SBC.

Table A-1: Supported AudioCodes IP Network Telephony Equipment

Supported IP Network Telephony Equipment	Description
 MP-1288	Cost-effective best-of-breed, high density analog media VoIP gateway. Provides superior voice technology for connecting legacy telephones, fax machines and modems with IP-based telephony networks, as well as for integration with IP PBX systems. Designed and tested to be fully interoperable with leading soft switches, unified communications (UC) servers and SIP proxies. Designed for carrier environments including 1+1 power supplies and 1+1 Ethernet redundancy, maintaining high voice quality to deliver reliable enterprise VoIP communications. Advanced call routing mechanisms, network voice quality monitoring and survivability capabilities (including PSTN fallback) result in minimum communications downtime.
 Mediant 3000 Media Gateway	Medium-sized member of the family of market-ready, standards-compliant Media Gateway systems. Main features: Redundant common equipment (Power, Controller, Ethernet Switch); Optional N+1 protection of DSP Cards; Designed for NEBS Level 3; Optimal, cost-effective channel density; Field-proven, high voice quality; SS7/SIGTRAN Interworking (SS7/PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant Applications: VoP Trunking devices, IP-Centrex devices, VoP Access devices Selected specifications: Up to 2,880 independent VoIP to PSTN voice calls; Voice Coders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fallback to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, MF-R1, SS7/M2UA/SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP (See product documentation for detailed information)

Table A-1: Supported AudioCodes IP Network Telephony Equipment

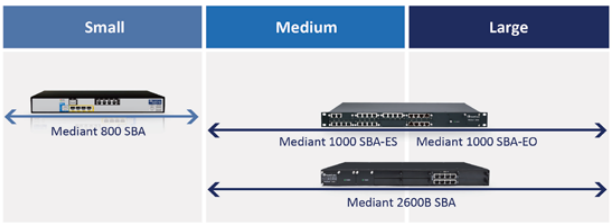
Supported IP Network Telephony Equipment	Description
 Mediant 4000 E-SBC	Member of AudioCodes' family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.
 Mediant 9000 SBC	Highly scalable Session Border Controller designed for deployment in large enterprise and contact center locations and as an access SBC for service provider environments. High-capacity SBC supporting thousands of concurrent sessions and extensive SIP connectivity with wide-ranging interoperability, enhanced perimeter defense against cyber-attacks, and advanced voice quality monitoring. Also supports active/standby (1+1) redundancy (High Availability) by employing two devices in the network. Offers branch survivability during WAN failure, ensuring call service continuity.
Survivable Branch Appliance (SBA) 	The Survivable Branch Appliance (SBA) is an AudioCodes product designed for Microsoft Lync Server which allows remote branch resiliency in a Microsoft Lync Server network (Microsoft Lync Server 2010 and Microsoft Lync Server 2013). The AudioCodes SBA resides on the OSN server platform of the Mediant 800B and the Mediant 1000B running on a Microsoft Windows 2008 Telco R2 operating system. Displayed in the OVOC as a module of the Mediant 800B and the Mediant 1000B devices. When you add either of these platforms to the OVOC, there is an option to enable the SBA module. The SBA module has a separate IP address and FQDN Name.

Table A-1: Supported AudioCodes IP Network Telephony Equipment

Supported IP Network Telephony Equipment	Description
	405HD, 420HD, 430HD, 440HD and 450HD IP phones, based on AudioCodes' High Definition voice technology, providing clarity and a rich audio experience in VoIP calls. All models include a large monochrome multi-language graphic LCD display The phones provide voice communication over an IP network, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, etc. Phone models support both Microsoft Lync, Skype for Business and non-Microsoft environments.
	AudioCodes' CloudBond 365 is a modular, adaptable solution for the data center, customer premises or the branch. A versatile all-in-one Skype for Business appliance designed for hybrid environments, it combines the best of the Skype for Business server, the Cloud-PBX and the service provider's voice services.
	AudioCodes' Mediant Server CCE Appliance bundles AudioCodes field-proven SBCs and gateways with the Skype for Business Cloud Connector Edition into an elegantly packaged 1U chassis that is easy to deploy and manage. Based on a powerful HP server, the AudioCodes Mediant Server CCE Appliance delivers the Cloud Connector integrated with the AudioCodes SBC for organizations or enterprise branches with up to 2500 users and supports up to 500 concurrent sessions.
	AudioCodes' Mediant 800 CCE Appliance bundles AudioCodes field-proven SBCs and gateways with the Skype for Business Cloud Connector Edition into an elegantly packaged 1U chassis that is easy to deploy and manage. For organizations or enterprise branches with up to 1000 users, the AudioCodes Mediant 800 with the integrated OSN server module can host the Cloud Connector on the same self-contained appliance supporting up to 185 concurrent sessions.

This page is intentionally left blank.

B Enabling Initial Connection Provisioning

When adding a single or multiple AudioCodes devices to the network for the first time, you can enable the Initial Connection Provisioning feature (a.k.a. First Time Provisioning) for devices to automatically be provisioned with their firmware and configuration files.

B.1 Before Enabling the Feature

Before enabling Initial Connection Provisioning, you need to validate the ini file.

➢ **To validate the ini file:**

1. Access each device using its default IP address directly through the Web interface or CLI, and then configure its network settings (e.g., OAMP IP address) so that it suits your network environment. Network settings are configured in these tables:
   - IP Interfaces
   - Ethernet Device
   - Ethernet Group
   - Physical Ports
   - Static Route
   - QoS Settings
2. Make sure the IP Interfaces table's indexes, names and application types *are identical* for each device so that the template configuration file will be applied to all devices in the network. In the validation process, each index entry is validated with the equivalent entry in the template file (see Appendix B.1.1 below for a file example).

Note: If any device's IP interface table does not meet these requirements, the Initial Connection Provisioning will fail and an alarm will be sent to the OVOC (see Section B.3).

B.1.1 Interfaces Table Excerpted from the ini File

The example below shows an example of a device's ini file's IP Interfaces table parameters. Validated values are displayed in blue. Not validated values are displayed in red and are only read from the device once the blue parameters are successfully validated.

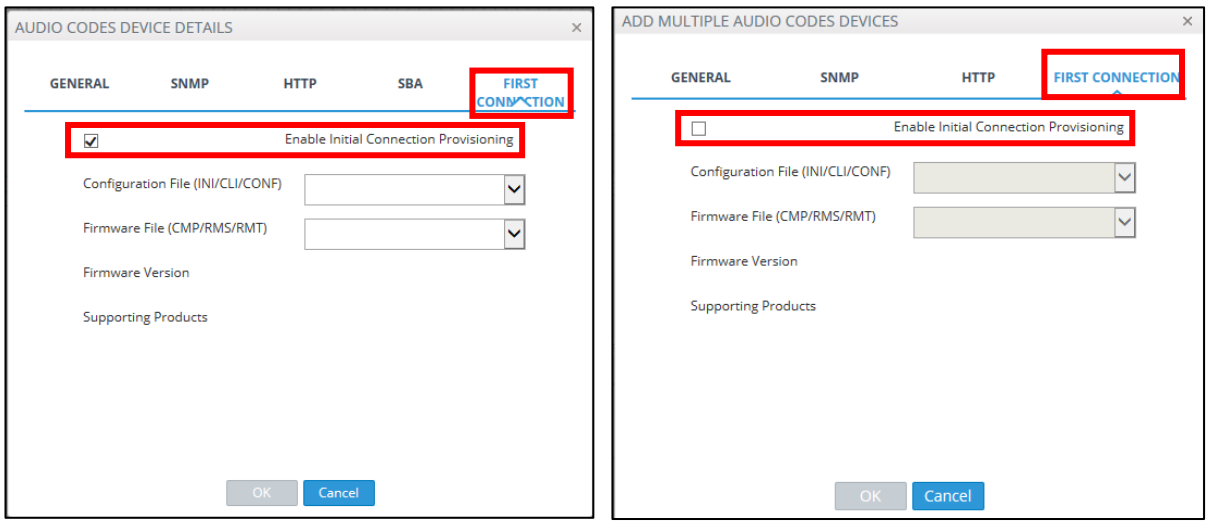
```
[ \InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;

InterfaceTable 0 = 6, 10, 10.15.17.10, 16, 10.15.0.1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";

InterfaceTable 1 = 5, 10, 195.189.192.156, 25, 195.189.192.129,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 2";
```

B.2 Enabling the Feature

The Initial Connection Provisioning feature is implemented by the **First Connection** tab shown in the figure below left - when adding a single AudioCodes device - and in the figure below right when adding multiple AudioCodes devices.

Note: Before adding an AudioCodes device or multiple devices, you must load the device ini and .cmp files to the OVOC's Software Manager. See Section 4.2.3 for details.

Figure B-1: First Connection: Add AudioCodes Device | Add Multiple AudioCodes Devices



➢ **To enable the feature:**

- Make sure the **Enable Initial Connection Provisioning** option shown in the figures above is selected.

  See also under Section 5.3 for related information.

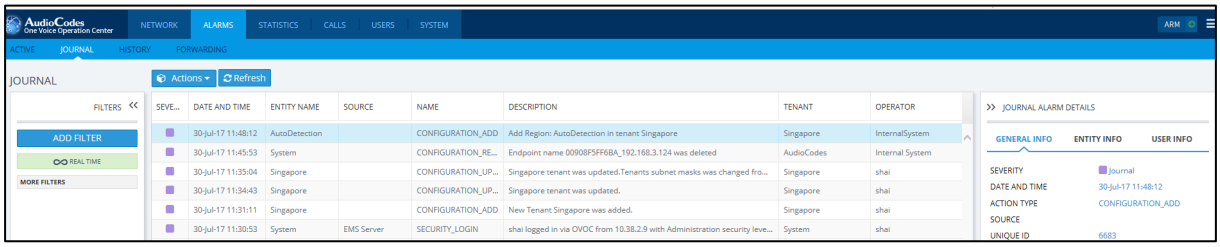
B.3 Making Sure First Time Provisioning was Successful

The Journal page helps you confirm that the configuration and firmware files were automatically loaded to the device after the device was connected to the network.

➢ **To make sure first time provisioning was successful:**

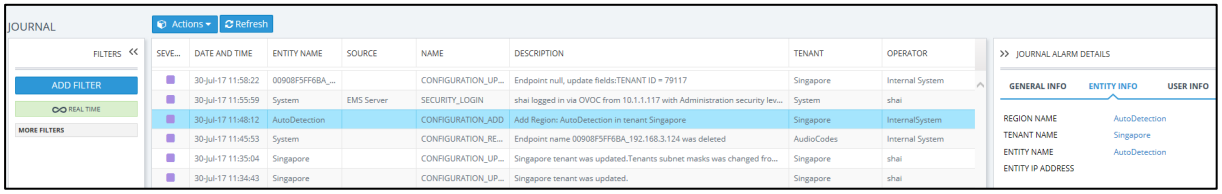
1. Open the Journal page (**Alarms** > **Journal**).

Figure B-2: Alarms Journal



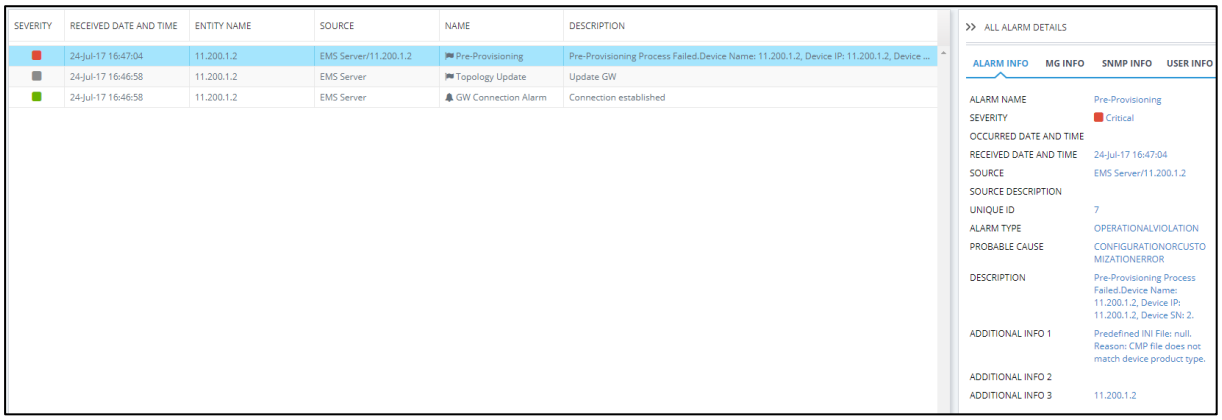
2. Optionally filter the page by Time Range (see Section 6.2.1), Topology (see Section 6.2.1.2), Source Type (see Section 6.4.3.1) or More Filters (see Appendix B.4 below).
3. Locate and select the First Time Provisioning / Initial Connection Provisioning alarm.
4. In the Journal Alarm Details pane on the right side of the page, click the **Entity Info** tab.

Figure B-3: Alarms Journal – Entity Info



5. If Initial Connection Provisioning was unsuccessful, you'll view the following:

Figure B-4: Critical Alarm – Initial Connection Provisioning Failed



Note: If Initial Connection Provisioning was unsuccessful, download the configuration or firmware file to the device as shown under Section 7.1.5.

After an ini or cmp file is deployed on multiple devices, you may need to customize one device's configuration to suite specific requirements.

➢ **To change the .cmp or ini file after successfully automatically provisioning a device:**

- Remove the device from the OVOC and then add it again. When the device is removed, the OVOC server IP address in the Trap Destination Rule is reset to 0.0.0.0, so when you add the device again you need to reconfigure this IP address in the SNMP Trap Destinations table. See the relevant *SIP User's Manual* for more information.

Note: AudioCodes recommends that you consult with AudioCodes Customer Support or Professional Services about special configuration issues.

B.4 Filtering the Alarms Journal by 'More Filters'

You can filter the Alarms Journal page by 'More Filters'.

Figure B-5: More Filters – Alarms Journal Page

Use the table below as reference.

Table B-1: More Filters – Alarms Journal Page

Filter	Description
Sources	Enter the name of the entity from which the alarm originated.
Operator	Enter the name of the operator according to whom to filter.

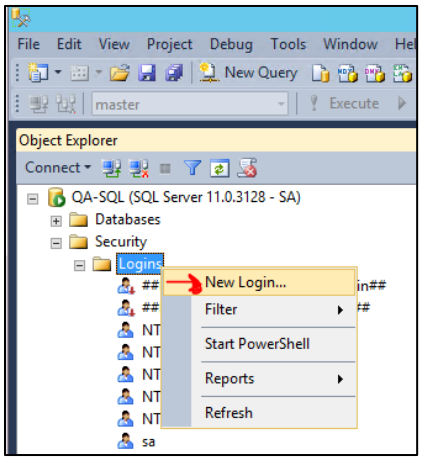
C Adding an Unprivileged User to MSSQL Server

This appendix shows how to add an unprivileged user to the MSSQL server with SQL Server Management Studio.

➢ **To add an unprivileged user to the MSSQL server:**

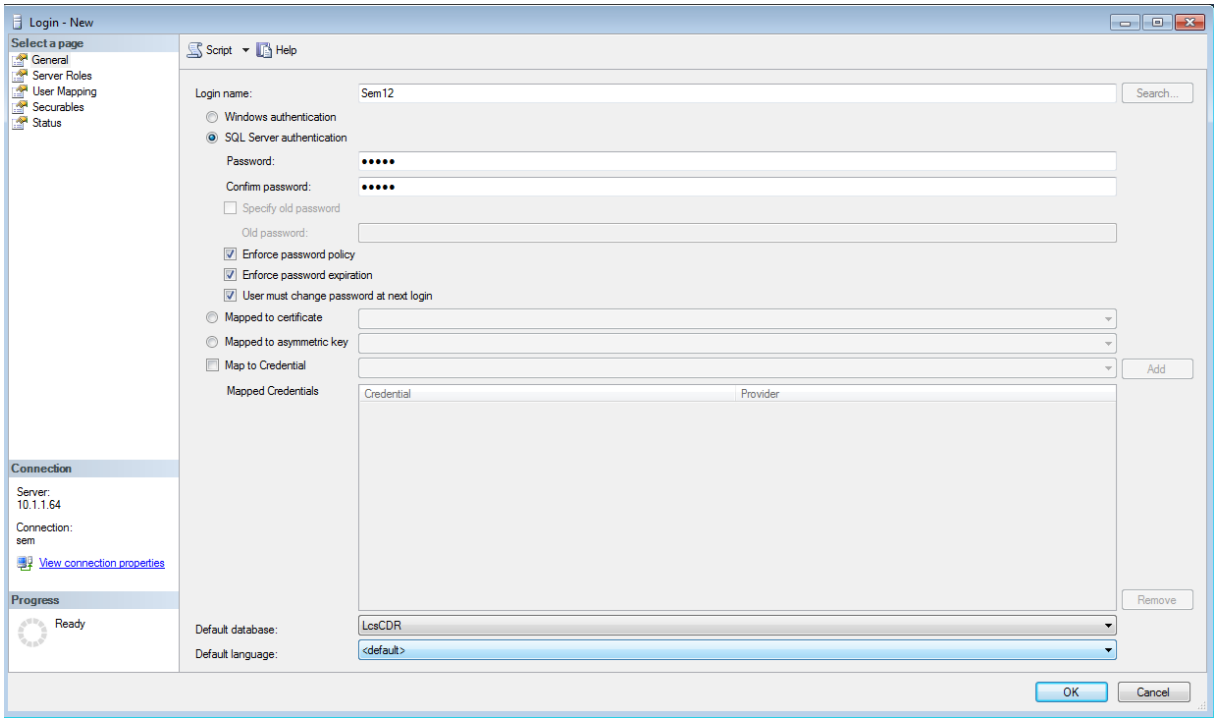
1. In the 'Security' folder, right-click **Logins** and select **New Login**.

Figure C-1: New Login



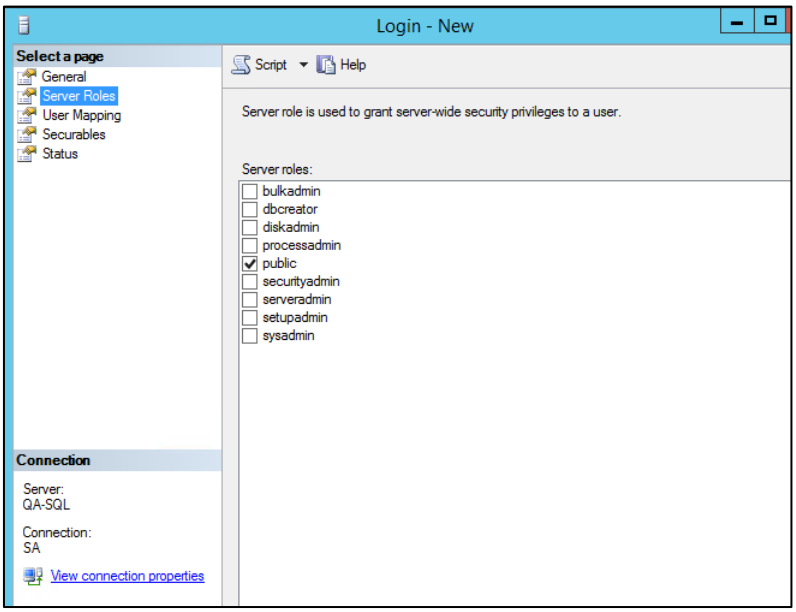
2. Under 'General', enter the Login name, select the **SQL server authentication** option, enter and confirm the password, from the 'Default database' dropdown select the default database to log in with, and then click **OK**.

Figure C-2: SQL Server Authentication



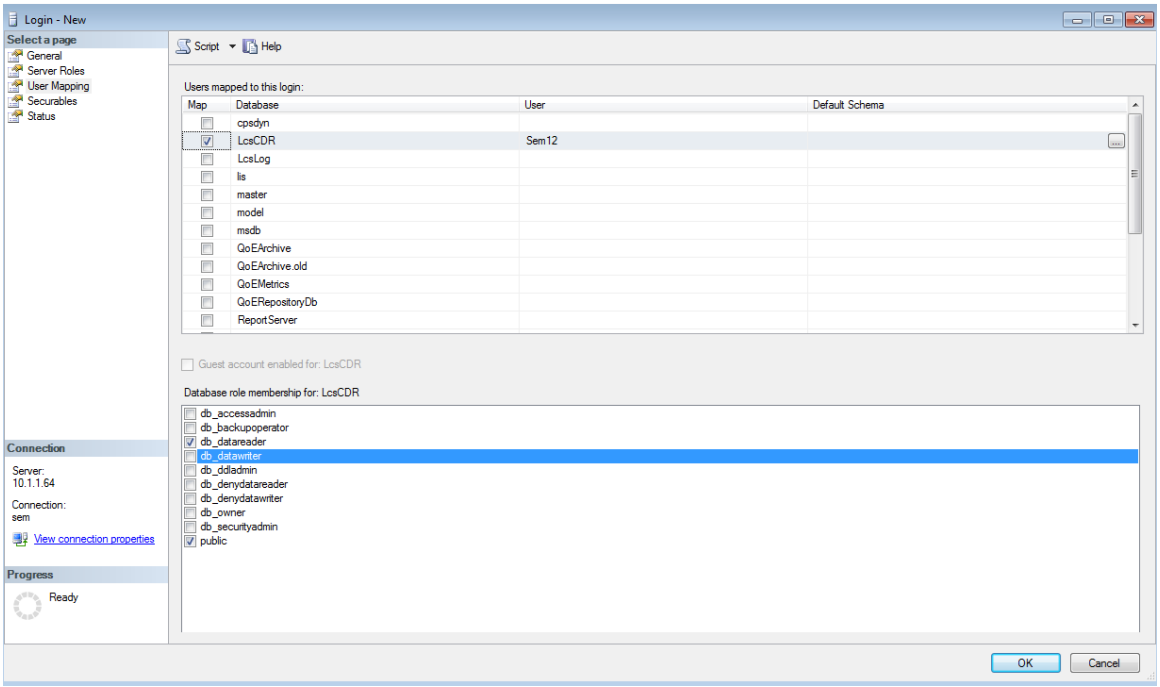
3. Under 'Server Roles' shown in the figure below, select **public**.

Figure C-3: Login Properties – Servers Role - public

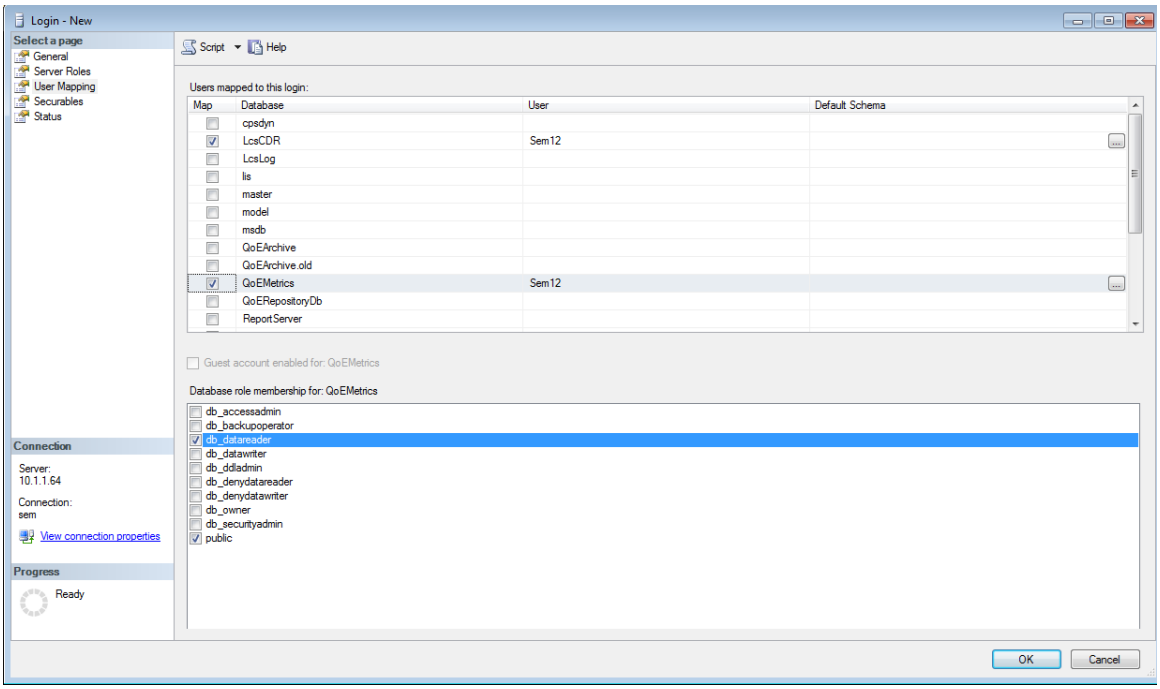


4. Under 'User Mapping' shown in the figure below, in the 'Users mapped to this login' pane, select **LcsCDR** and in the 'Database role membership for LcsCDR' pane, select **db_datawriter** and **public**.

Figure C-4: Login Properties – User Mapping – db_datareader | public



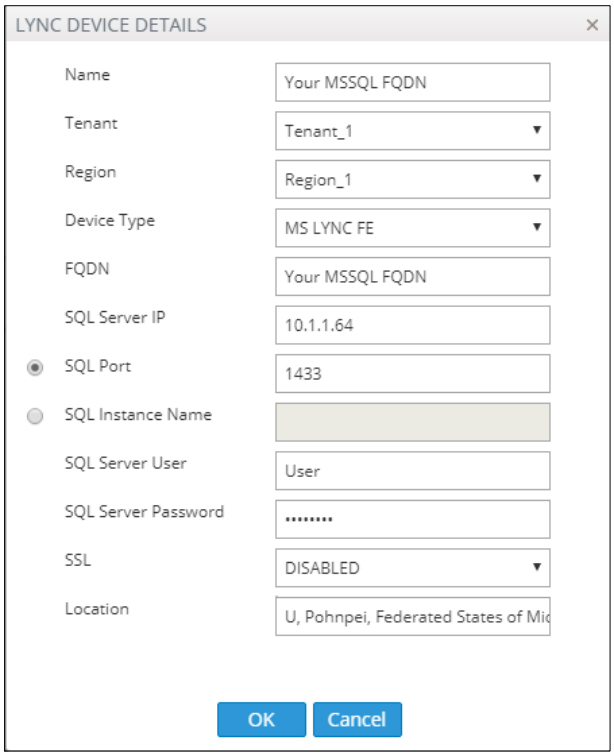
5. Under 'User Mapping' shown in the figure below, in the 'Users mapped to this login' pane, select **QoEMetrics** and then in the 'Database role membership for QoEMetrics' pane, select **db_datareader** and **public**.



The SQL server side is now ready.

6. In the OVOC, under 'Network', click **Add** and then select **Lync Device**.

Figure C-5: Lync Device Details



7. From the 'Device Type' dropdown, select **MS Lync FE**.
8. Enter the SQL Server IP address.
9. Select the **SQL Port** option and leave the default unchanged.
10. Click the 'Location' field and from the list displayed, select the location.
11. Enter the other details about your Microsoft SQL server - use the user credential defined previously in the SQL server.

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

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

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

©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-91043