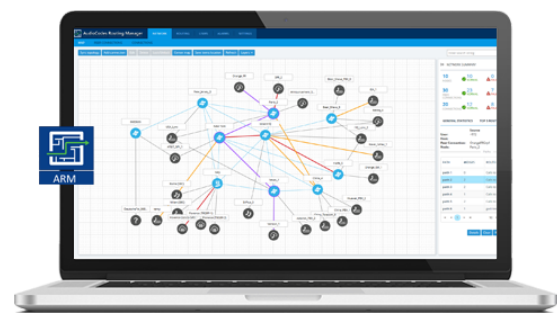


AudioCodes Routing Manager (ARM)

Version 9.6



Notice

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

This document is subject to change without notice.

Date Published: January-17-2022

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 website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

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 website at <https://online.audiocodes.com/documentation-feedback>.

Stay in the Loop with AudioCodes



Related Documentation

Manual Name
ARM Installation Manual
ARM User's Manual

Manual Name
Mediant 9000 SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 3000 Gateway User's Manual
Mediant 2600 E-SBC User's Manual
Mediant SE SBC User's Manual
Mediant SE-H SBC User's Manual
Mediant VE SBC User's Manual
Mediant VE-H SBC User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 500 Gateway and E-SBC User's Manual
Mediant 500 MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 500L MSBR User's Manual
MP-1288 High-Density Analog Media Gateway User's Manual
One Voice Operations Center Server Installation, Operation and Maintenance Manual
One Voice Operations Center Integration with Northbound Interfaces
One Voice Operations Center User's Manual
One Voice Operations Center Product Description
One Voice Operations Center Alarms Guide
One Voice Operations Center Security Guidelines

Document Revision Record

LTRT	Description
41891	Registered Users. Add Routing Rule: Security call score; Destination is a registered user in ARM; Normalization after Routing; Route to user location. Policy Studio > Add Call Item: (1) User/Web Service (2) Destination is a registered user in ARM (3) Resource Groups. Select Multiple Elements and Invert the Selection. 'LDAP Server Settings' screen. Using an External Web Service for Pre-Routing Call Security Score Consultation (SecureLogix). User Group Details. LDAP 'Test'. RADIUS 'Test'. Edit Syslog-INFO. View Registered Users from a Specific Node or Peer Connection.
41892	Uni-directional lock / unlock of a Peer Connection. Combined ARM and SBC routing decision. Combined ARM – SIP based routing decision (route based on Request URI). Enhanced SSH users management for security. Routing Rule matching notification enriched with ARM information. ARM Sessions Count Statistic (License Utilization). Representation of Forking in Test Route. Registered users forking. Maximum number of Routing Attempts per VoIP Peer can be configured. New License Key for security queries and enforcement.
41893	Improved Usability and User Experience (UI). New Login/Welcome Screen. ARM Analytics API. Routing of Registration Messages. Licensing for Registrations Routing. Registrations Routing Settings. Routing Rules for Registration Messages Routing. Policy Studio for Registration Messages Routing. Test Route for Registration Messages. New Statistics for Registrations. Support for Up to 4 Million Users. Support of File Repositories as Source of ARM Users. Total Users Count Button. Export of ARM Users to CSV File. Tag-based Routing. Assigning Tags in Policy Studio Rules. Tags Usage in Routing Rules. CentOS 8 OS. New VM Requirements for ARM 9.2. Users Group as Policy Studio Matching Criterion. Configuring Page Size when Operating with LDAP Server (Active Directory). ARM as an Information Source for Users Credentials. Source URI Manipulation of a Specific Field. Test Route Call Simulation with a Specific SIP Header. Security Extension: 'Monitor' Operator is not Exposed to Administration Tab. Supported cipher suites.
41894	New CdrArmMessage fields. -iu option. -od option. DID Masking. Policy Studio Flow Control. Keep Connection Properties Synchronized. IP Profiles. Microsoft Teams LMO. Prefix/Prefix Group Configured as 'Source' in Policy Studio Condition. Enforcing 16G Memory Config for ARM Router in Deployment of 1M+ Users. Policy Studio 'Site' Condition. Normalization of Combined Property in Property Dictionary. Hexagon.
41895	'Customer' entity: Hosted Teams multi-tenant direct routing. Quota (calls time limit) per Peer Connection / set of Peer Connections. CAC Profiles. Prefix Group usage visibility. New engine for validation of Prefix/DID uniqueness. ARM

LTRT	Description
	integration with Azure AD. Appending deleting Prefixes in a Prefix Group via the REST API. VoIP Peers page. Customized ARM Connection (IP Group Name, user-defined IP Profile & Media Realm. Authentication order.
41896	Calls Details - RegEx, CSV. Centos Stream 8. Server Certificates (Configurator, Routers). Examples of Unselected Rules Reasons. No answer timeout. SecureLogix Orchestra One CAS (Call Authentication Service). Number of standard security queries (per month); Number of advanced security queries (per month). License Details. Statistics Thresholds Based Alarms. Manipulation before route; Manipulation after route. Max # of Unselected Rules in calls. Global Routing Settings (Unselected Rules). Adding Node Info to Call Details. Alternative Routing SIP Reasons.
41897	Device Location

Table of Contents

1	Overview	11
	Features	12
	Benefits	14
	Simplicity	14
	ARM-Routed Devices	14
	Third-Party Open-Source Software	15
2	Getting Started with the ARM	17
	Logging in	17
	Getting Acquainted with the ARM GUI	18
	Getting Acquainted with the Network Map Topology Layer	22
	Getting Acquainted with Network Map Layers	25
	Getting Acquainted with Network Map Page Actions	30
	Node Information and Actions	30
	VoIP Peer Information and Actions	37
	Connection Information and Actions	39
	Peer Connection Information and Actions	41
	Repositioning Elements in the Network Map Page	47
	Peer Connections Page Actions	47
	VoIP Peers Page Actions	49
	Connections Page Actions	50
	Resource Groups Page Actions	51
	IP Profiles Page	52
	Customers Page	61
	Viewing the Customers Page	62
	Defining a 'Customer' Entity (Teams Tenant)	64
	Editing a 'Customer' Entity	67
	Deleting a 'Customer' Entity	67
	Locking-Unlocking a 'Customer' Entity	67
	Defining 'Customer' Entities using ARM Users & Policy Studio	68
	Viewing Network Summary Panes	68
	Overall Network Statistics	69
	Statistics on a Selected Entity	72
3	Defining a Network Topology	74
	Adding an AudioCodes Node to the ARM	74
	Adding a Third-Party Node to the ARM	75
	Adding a VoIP Peer	76
	Attaching a CAC Profile to a Peer Connection	78
	Attaching a CAC Profile to a VoIP Peer	80
	Using the Nodes Page	81
	Configuring a Microsoft Teams LMO Topology	82
	Adding Connections	84

Synchronizing Topology	86
Testing a Route	87
Testing a Route for Registration Messages	91
Testing Call Routing Simulation with a Specific SIP Header	93
Testing 'Customer' Entity	95
Examples of Unselected Rules Reasons	96
During Route – Unselected Rules	96
Before Route (Policy Studio) - Unselected Rules	97
4 Designing a Network Topology in the Offline Planning Page	98
Performing Actions in the Offline Planning Page	99
Adding a Virtual Entity	99
Adding a Virtual Peer Connection to the Offline Page	101
Adding a Virtual Connection	101
Importing a Full Topology	101
Importing a Node from the Live Topology	102
Deleting a Virtual Entity	102
Testing a Route	102
Exporting a Node from the Offline Page to the Live Topology	102
5 Viewing Statistics and Reports	104
Configuring Statistics Thresholds Based Alarms	113
Adding a Statistics Threshold	114
Viewing Statistics Thresholds Based Alarms	117
Editing a Statistics Threshold	118
Deleting a Statistics Threshold	118
Accessing the ARM's Analytics API	118
Examples of ARM Dashboard that can be Achieved using Analytics	121
6 Performing User-Related Administration	123
Adding a User Not Listed in an AD to the ARM	124
Determining Total Users Count	126
Exporting ARM Users to CSV File	127
Incorporating Users into the ARM from a File Repository	128
Viewing Registered Users in the ARM	135
Adding Users Groups to the ARM	136
Adding an LDAP Server to the ARM	141
Adding a Property Dictionary to the ARM	150
Adding a Users Dictionary Attribute Triggered (Combined) by Two Other Attributes	153
Configuring ARM to Provide Information about Device Location	154
7 Configuring Settings	156
Administration Settings	157
Activating Your License	157
Viewing License Details	159
Securing the ARM	160

Configuring Certificates	160
Configuring a Configurator Certificate	161
Generating and Replacing a Private Key and Self-Signed Certificate	163
Generating a Private Key, Self-Signed Certificate and CSR	163
Loading a Certificate	164
Determining ARM Communications with Other Entities	166
Strengthening Security: Certificate Validation	167
Enhancing SSH Users Management for Security	169
Provisioning Operators	170
Manually Provisioning an Operator in the ARM's Operators Page	171
Node Credentials	172
Router Credentials	174
Configurator Credentials	176
Provisioning Operators using an LDAP Server	179
Authenticating Operator Login using Open LDAP	183
Provisioning Operators using a RADIUS Server	184
Managing Authentication Order	187
Authenticating Operator Login Using Azure AD	187
Azure AD for REST Requests Authentication	188
Remote Manager	190
Adding Registered Users to the ARM	191
Network Services Settings	192
Editing a Syslog Server	192
Adding/Editing an NTP Server	194
Prioritizing Traffic Per Class of Service	195
Enabling CDRs	196
Call Flow Configurations	197
Adding a Normalization Group	198
Using Prefix Groups	200
Adding a Prefix Group	200
Searching for a Prefix Group	202
Searching for a Specific Prefix within a Prefix Group	202
Editing a Specific Prefix within a Prefix Group	203
Viewing the Details of the Prefix Group Used for Routing	204
Validating Prefix or DID Uniqueness	205
Normalization Before Routing	207
Policy Studio	208
Example 1 of a Policy Studio Rule	214
Example 2 of a Policy Studio Rule	215
Adding a Policy Studio Rule for Users Credentials Information	216
Tag-based Routing	221
Users Group as Matching Criterion	223
Web-based Services	224
DID Masking	228
Routing Settings	233

Configuring Criteria for a Quality Profile	233
Configuring a Time-Based Routing Condition	234
Configuring Alternative Routing SIP Reasons	237
Configuring a SIP Reason Group	239
Configuring Global Routing Settings	243
Registration Routing Settings	244
Calls Quota	246
CAC Profiles	251
Defining a CAC Profile Threshold	253
Disabling CAC and Session Counting	253
Adding a Routing Server	254
Editing a Routing Server	255
Locking/Unlocking a Routing Server	257
Adding a Routing Server Group with Internal and External Priorities	258
8 Defining Calls Routing	262
Adding a Routing Group	262
Editing a Routing Group	264
Moving a Routing Group	265
Deleting a Routing Group	266
Duplicating a Routing Rule	267
Adding a New Routing Rule	268
Moving a Routing Rule	294
Deleting a Rule	295
Duplicating a Routing Rule	296
Testing a Route	297
Using the Routing Rules Table View Page	297
9 Viewing CDRs and Call Details	299
Call Details	304
Adding Node Information to Call Details	307
Disabling, Limiting the Number of CDRs	309
10 Viewing Alarms	311
Active Alarms History Alarms	311
Journal Page	312
Collecting Info via SNMP to Enhance IP Network Telephony Performance	312
Locating a Specific Alarm	313
Enriching Routing Rule Matching Notifications with ARM Information	314
11 Migrating Device Routing to the ARM	319
AudioCodes Device Application Types	319
ARM Network Routing Logic	319
SBC Routing Logic	319
Gateway Routing Logic	320
Hybrid Device Routing Logic	320

Connecting the Device to the ARM Topology Server	320
Defining an IP Interface Dedicated to ARM Traffic	323
Migrating SBC/Gateway/Hybrid Routing to the ARM	324
Migrating SBC Routing to the ARM	325
Migrating Media Gateway Routing to the ARM	329
Migrating Hybrid Routing to the ARM	331
12 Checklist for Migrating SBC Routing to the ARM	335
13 Prefixes	338
14 Examples of Normalization Rules	339
15 Call Routing	343
16 Configuring an SBC to Send SIP Requests other than INVITE to ARM	344
17 Operating with Azure AD	346
Configuring the ARM in the Azure Portal	346
Azure AD as a Source for Users in the ARM	350
Authenticating Operator Login	353
Revoking Azure User Tokens	353
18 Opening Firewall Ports for the ARM	354
19 About CDRs Sent by ARM to CDR Server	359
20 Supported ARM Configurator and ARM Router Cipher Suites	365

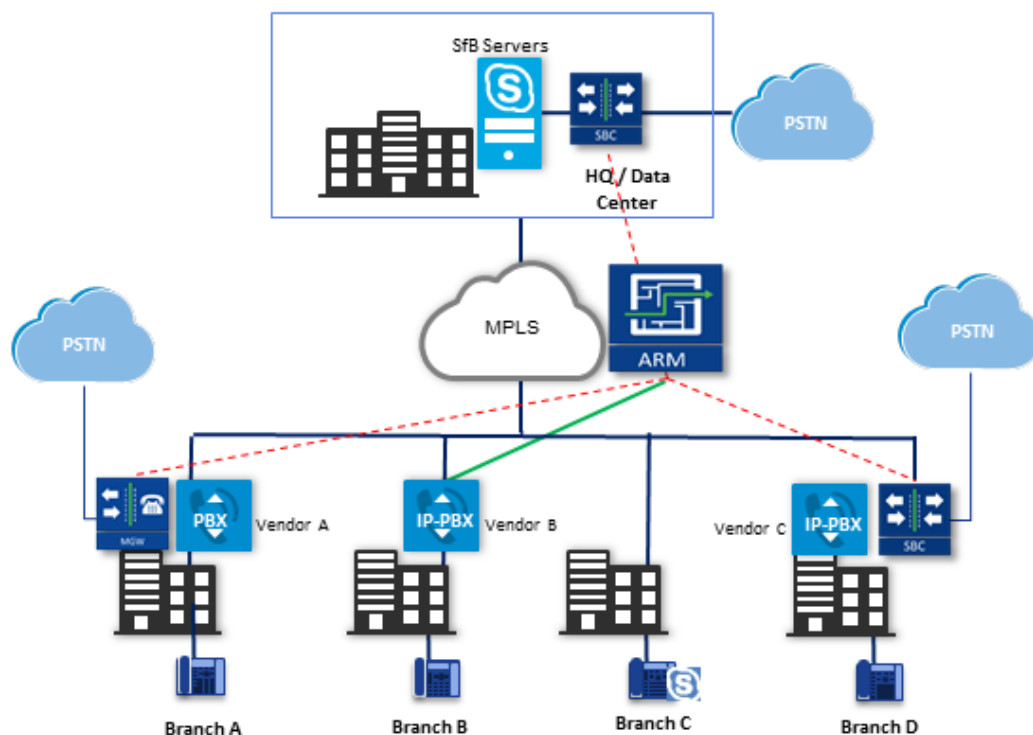
1 Overview

This document shows how to use the AudioCodes Routing Manager (ARM). The ARM is a LINUX-based, software-only, telephony management product which expedites and streamlines IP telephony routing for enterprises with multiple globally distributed branches. The ARM determines the quickest, least expensive, and best call quality routes in packet networks.

Routing data, previously located on the SBC, Unified Communications (UC) application (e.g., Microsoft's Skype for Business), or Media Gateway, is now located on the ARM server. If an enterprise has an SBC in every branch, a single ARM, deployed in HQ, can route all calls in the globally distributed corporate network to PSTN, the local provider, enterprise headquarters, or to the IP network. Routing rules, configured by the IT manager in the ARM's Routing Table, perform the routing.

If an enterprise has only one or two branches, its IT manager can easily independently implement maintenance changes. In globally distributed enterprises, IT managers until now had to laboriously implement changes, multiple times, per branch. With the ARM, IT managers implement changes only once, saving significant labor and time resources and costs.

The following figure shows a typical, globally-distributed, multi-branch enterprise VoIP network.



VoIP networks like this typically require:

- Distributed routing & policy enforcement

- Distributed PSTN
- Multiple VoIP network entities' configurations (i.e., SBC, Media Gateway)
- Multiple Dial Plans
- SIP Interworking between IP PBXs
- Large number of end user policies
- Efficient ARM routing management

Features

ARM features are as follows:

- Centralized, enterprise-wide session routing management
- Fully integrated into AudioCodes' One Voice Operations Center (OVOC) management system (ARM Version 8.4 and later and OVOC Version 7.6 and later)
- Centralized & optimized PSTN routing
- Automatic discovery of VoIP network entities
- Supports third-party devices as well as AudioCodes SBCs and gateways
- Smart Dial Plan management
 - Centralized Dial Plan logic; simple, clear, intuitive and easy to maintain
 - Dialing plan dry test by 'Test Route' simulation; animated path for Test Route
 - Incoming number manipulation
 - Outgoing number manipulation
 - User properties manipulation
- Reduces SIP trunk costs
 - Implements Tail-End-Hop-Off Routing
 - Assigns actions to routing rules with different sequence
 - Source and destination number manipulation
- Advanced routing based on user properties
- Quality-based routing
- Time-based routing
- Flexible load balancing
- Automatic topology network generation
- Manual network generation (simply drawing lines between dots)
- On-the-fly routing calculation:
 - Centralized management of Network Routing Rules

- Routing decision is based on source / destination call parameters, and user properties
- Predefined weights on connections
- User information from external databases, e.g., LDAP and RADIUS; operator login authentication with these servers
- Flexible API
- Intuitive graphical representation of the enterprise VoIP network
- Support for very large networks (topology elements) with high numbers of edges (Connections and Peer Connections)
 - Multiple topology elements can be moved / repositioned simultaneously
 - Lightweight hoover for each topology element
 - Easily accessible Actions on each topology element
- Personalized Call Routing Applications
 - Communication-Enabled Business Process
 - Full on-line management and routing via REST API
 - Fallback to SBC routing table if call does not match ARM configuration

Benefits

The ARM benefits users as follows:

- Reduces operational time spent on designing and provisioning network topology
- Reduces OPEX, avoiding routing configuration of VoIP network entities
- Reduces time spent implementing network evolutions such as:
 - Adding new connections to PSTN (e.g., SIP trunks)
 - Adding new branches to the enterprise VoIP network
 - Modifying user voice services privileges

Simplicity

- VoIP network entities registering in the ARM
- Auto-discovery of VoIP peers
- One-click topology network creation, star formation
- Customized topology network
 - Configuring a connection is as simple as drawing a line
 - Modify by adding, deleting and changing connections
- ARM connects to user data base

ARM-Routed Devices

The following devices can be routed by the ARM:

- Mediant 9000 SBC
- Mediant 4000 SBC
- Mediant 2600 SBC
- Mediant SE/VE SBC
- Mediant 1000B Gateway and E-SBC
- Mediant 800B Gateway and E-SBC
- Mediant 800C
- Mediant 500 E-SBC
- Mediant 500L SBC
- Mediant SBC CE (Cloud Edition)
- Mediant 3000 Gateway only
- Mediant 3100 SBC, Gateway or Hybrid

Third-Party Open-Source Software

The following third-party open-source software is supported by the ARM:

- Apache Commons Apache License 2.0
- JSON.simple by google – apache license 2.0
- json-path - apache license 2.0
- ben-manes/caffeine - apache license 2.0
- TinyRadius - GNU LESSER GENERAL PUBLIC LICENSE
- MongoDB - Server Side Public License (SSPL)
- mongodb-driver - Apache License, Version 2.0
- CentOS Stream 8 operating system
- Spring Framework (released under version 2.0)
- MariaDB relational database management system
- ActiveMQ (using the Apache 2.0 license)
- Hibernate (projects licensed under Lesser General Public License (LGPL) v2.1)
- Log4J (Apache License 2.0)
- Guava (Google core libraries - Apache License 2.0)
- Jackson - The Apache Software License, Version 2.0
- Apache Commons Logging™
- HttpClient - Apache
- XStream (Group: com.thoughtworks.xstream)
- Jersey client
- Joda-Time
- SLF4J (Simple Logging Facade for Java)
- HikariCP - license Apache 2.0
- Aspectj™ extension to Java
- SNMP4J (Open Source SNMP API for Java)
- Mockito
- Tomcat 9 - Apache 2.0
- Angular 8
- microsoft-authentication-library-for-java (MSAL4J) – MIT
- Microsoft Graph SDK for Java - MIT

- Caffeine (Cache) - Apache License 2.0

2 Getting Started with the ARM

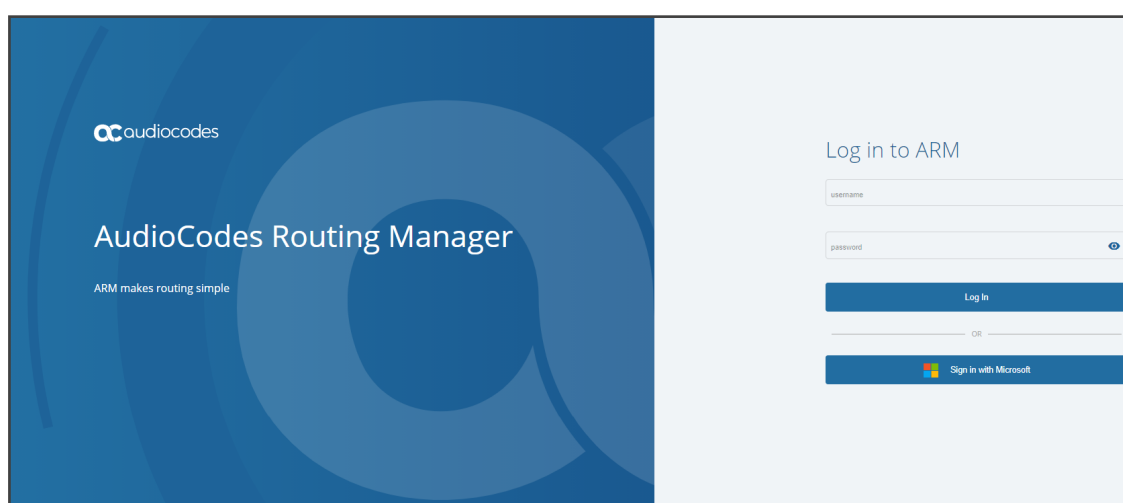
After installing the ARM and performing initial configuration (see the *ARM Installation Manual*), you can get started managing routing with the ARM.

Logging in

Logging in is a prerequisite to getting started with the ARM.

➤ **To log in:**

1. Point your web browser to the ARM's IP address and press enter.



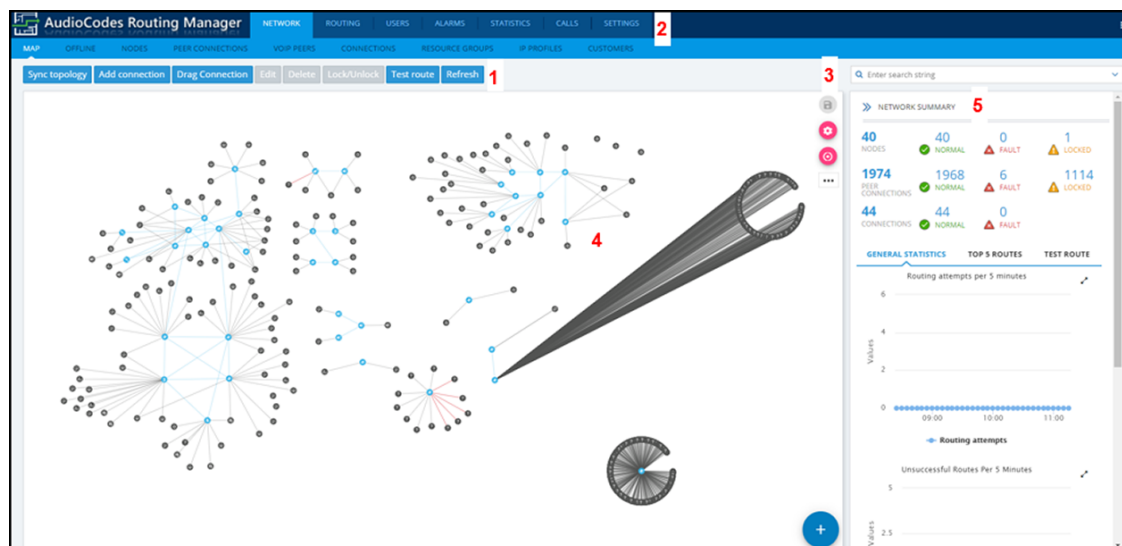
2. In the Login to ARM screen, log in using the default **Operator** and **Operator** username and password. It's advisable to change these as soon as possible (see [Provisioning Operators](#) on page 170 for instructions on how to change them).
3. Click the **Sign in with Microsoft** button if you're operating with Azure Active Directory. See [Authenticating Operator Login Using Azure AD](#) on page 187 for more information.

The ARM opens in the Network page, Map view (default) in your browser. By default, all VoIP entities managed in the network are displayed.

Getting Acquainted with the ARM GUI

The ARM's internet browser based graphic user interface visualizes VoIP network topology and its components, providing centralized, dynamic network management and router rules and logic management. After logging in, the Network page, Map view opens by default.

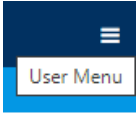
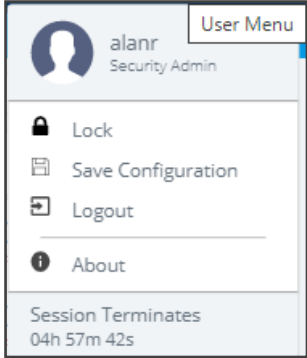


Figure 2-1: ARM GUI - Network Page - Map View

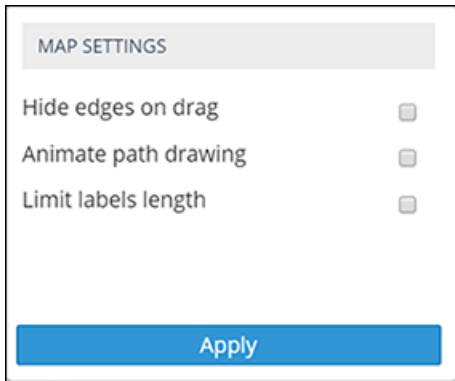

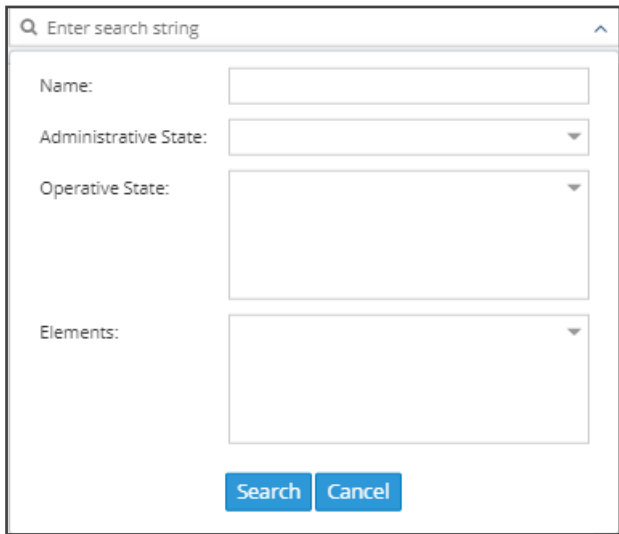


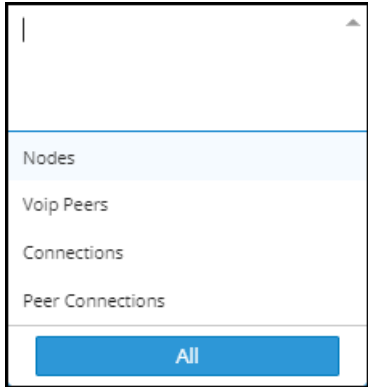
Use the following legend as a reference to the preceding figure.

Table 2-1: ARM GUI – Map View

#	GUI Area	Description
1	Actions Bar	<ul style="list-style-type: none"> ■ Sync Topology ■ Add Connection ■ Drag Connection ■ Edit ■ Delete ■ Lock/Unlock ■ Test Route ■ Refresh ■ Layers <ul style="list-style-type: none"> ✓ topology ✓ quality ✓ quota ✓ CAC

#	GUI Area	Description
2	Toolbar	Toolbar icons let you navigate to the following ARM pages: NETWORK, ROUTING, USERS, ALARMS, STATISTICS, CALLS and SETTINGS.
		<p>Located in the uppermost right corner of the page on the toolbar.</p>  <ul style="list-style-type: none"> ■ View the name of the operator currently logged in and their security / permission level ■ Lock (Terminates user's ARM GUI session) ■ Save Configuration: The ARM_Configuration.zip file (ARM database) is saved locally in the client's 'Downloads' directory. You can send it to AudioCodes for troubleshooting. In parallel, basic ARM backup is performed and the backup file is stored in the configurator's /home/backup directory. You can use it to restore the configuration on the same machine using standard ARM restore procedure. ■ Logout ■ About: Displays the ARM version ■ Session Terminates: Displays how much time remains before the session terminates
3		Save items collapse state and location (saves entities' positions in the Network Map after they're moved).
3		Diagrams Configurations (opens the Map Settings pop-up menu):

#	GUI Area	Description
		<div data-bbox="587 259 1043 638">  </div> <ul style="list-style-type: none"> ■ For more information about Hide edges on drag, see Repositioning Elements in the Network Map Page on page 47 ■ Select Animate path drawing for animated visualizations of Test Route and Top Route actions. ■ Select Limit labels length to limit the lengths of the labels of the displayed Nodes and VoIP Peers to a predefined number of characters, useful with large networks and long Node and / or VoIP Peer names which clutter the Network Map. If selected, the parameter 'Max label length' is displayed in which the maximum number of characters allowed is defined.
3		Center Map (centers the Network Map in the middle of the page)
3	Search	<p>Enables you to locate specific information in the Network Map view, Routing page, Users page, Alarms page and Settings page.</p> <ol style="list-style-type: none"> 1. Click the 'Enter search string' drop-down. <div data-bbox="587 1402 1208 1933">  </div>

#	GUI Area	Description
		<ol style="list-style-type: none"> Define search parameters: Name and/or Administrative State and/or Operative State. At least one item must be selected. You can also search for a Node <i>by the Node's IP address</i>, not only by the Node's name, which is an essential functionality in very large deployments with high numbers of Nodes. Click the Elements drop-down and optionally filter for these: <div data-bbox="587 555 956 940">  </div>
4	Main Screen	The Network page displays a Map view of network entities.
5	Summary Panes	<p>The Network page, Map view, displays these summary panes:</p> <ul style="list-style-type: none"> ■ Network Summary <ul style="list-style-type: none"> ✓ Nodes (Available, Unavailable, Locked) ✓ Peer Connections (Available, Unavailable, Locked) ✓ Connections (Available, Unavailable) ■ General Statistics <ul style="list-style-type: none"> ✓ Routing Attempts per 5 Minutes ✓ Unsuccessful Routes per 5 Minutes ✓ Unsuccessful Routes (Alternative Attempts / Destinations Not Routable) ✓ Calls per 5 Minutes (Destination Calls / Transient Calls) ■ Top 5 Routes (with animation) ■ Test Route



















Getting Acquainted with the Network Map Topology Layer










In the Network page, Map view, you can view node information and perform network map actions. Network Map view shows the four main entities that comprise the network topology:

- Nodes
- VoIP Peers
- Peer Connections
- Connections

The following table explains each.

Table 2-2: Network Map view – Network Entities

Network Entity	Icon	Explanation
Node		Indicates an AudioCodes SBC communicating with the ARM. It's part of the ARM network topology.
		Blue = operative state available/logging in
		Red = operative state unavailable/unrouteable
		Orange = operative state logged out
		Strikethrough = locked
		No strikethrough = unlocked
VoIP Peer		Indicates an AudioCodes gateway communicating with the ARM. It's part of the ARM network topology.
		Blue = operative state available
		Red = operative state unavailable
		INVALID CONFIGURATION
		Orange = operative state logged out
		Strikethrough = locked
Peer Connection		No strikethrough = unlocked
		Indicates a hybrid AudioCodes device (AudioCodes' Gateway and SBC in one).
		Blue = operative state available
		Red = operative state unavailable
		INVALID CONFIGURATION
		Orange = operative state logged out

Network Entity	Icon	Explanation
		Indicates a third-party, non-AudioCodes device (such as Teams) communicating with the ARM. It's part of the ARM network topology.
VoIP Peer		Indicates a non-AudioCodes device or entity that is also part of the ARM network topology: Teams, PBXs, SIP trunks, other vendors' SBCs / gateways. These devices participate in processing ARM network calls and are connected to Nodes by 'Peer Connections'. The ARM operator can configure one of six VoIP Peer types.
		Teams
		SIP trunk
		PSTN
		IP phones
		IP PBX
		Legacy PBX
Connection		Indicated by a blue line (available) or a red line (unavailable). Joins two Nodes. Calls can be routed between two Nodes only if there is a Connection between them. Defined by adding an IP Group (at Node level). From AudioCodes' gateway/SBC perspective, a 'Connection' is an 'IP Group'. Connections between Nodes are added by the ARM operator.
Peer Connection		Indicated by a black line between a Node and a VoIP Peer. Represents a group of routing destinations/sources (connections to a VoIP Peer), 'last mile' connectivity. From AudioCodes' gateway/SBC perspective, a Peer Connection is a 'PSTN Trunk Group' or 'IP Group'. Red line = administrative state is unlocked / operative state is unavailable (no connection between the

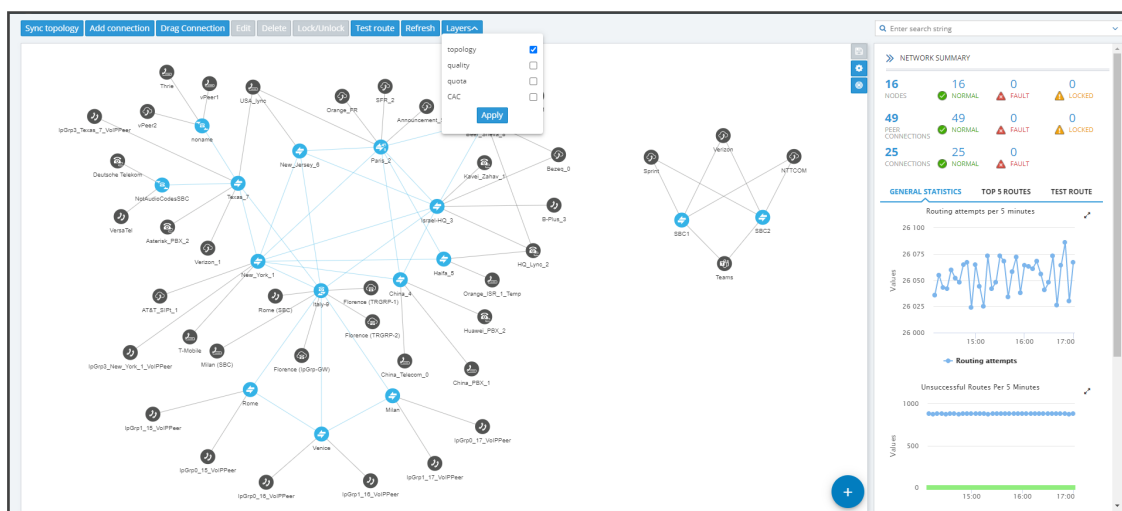
Network Entity	Icon	Explanation
		<p>AudioCodes device and the remote device) / predeleted (IP Group was deleted from the device)</p> <p>Black line through a red sphere = unavailable and locked</p> <p>Black line through a black sphere = available but locked</p> <p>Operators can lock / unlock a Peer Connection as well as select a <i>directional based</i> lock / unlock which allows for example stopping <i>only traffic towards</i> a specific VoIP Peer (for example, a specific IVR) while <i>calls coming from</i> this VoIP Peer will still be routed to their destination. The feature can be used to perform a graceful stoppage of traffic for maintenance reasons (for example). The feature is essential for IVR VoIP Peers when there are always calls in a queue that are not yet connected to an agent. From the IVR's perspective, the connection to the agent is outbound calls; without the uni-directional lock feature, calls fail. The Map page and Peer Connections page indicate a Peer Connection's directional lock.</p>

Getting Acquainted with Network Map Layers

The Network Map view displays a **Layers** tab that allows the operator to choose:

- **topology**
- **quality**
- **quota**
- **CAC**

Figure 2-2: Network Map – Topology Layer

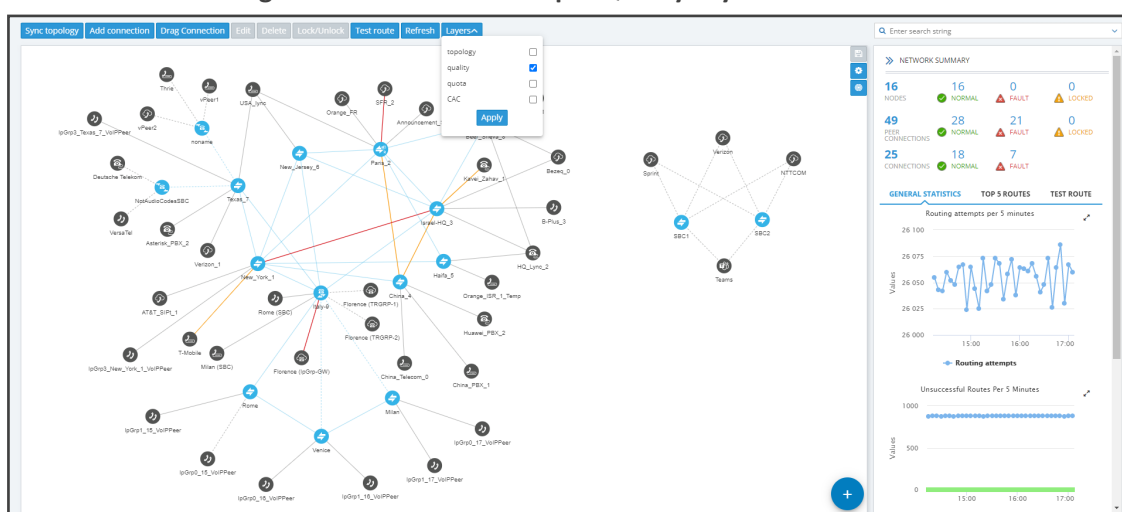


The **topology** layer displays the availability status of network entities.

The **quality** layer displays the quality status of network Connections and Peer Connections.

When both the **topology** layer and the **quality** layer are selected, the Network Map displays the aggregated availability status and quality status.

Figure 2-3: Network Map – Quality Layer



The figure above shows the Network Map when the **Quality Layer** is applied.

The following table describes the different quality color codes.

Table 2-3: Quality Color Codes

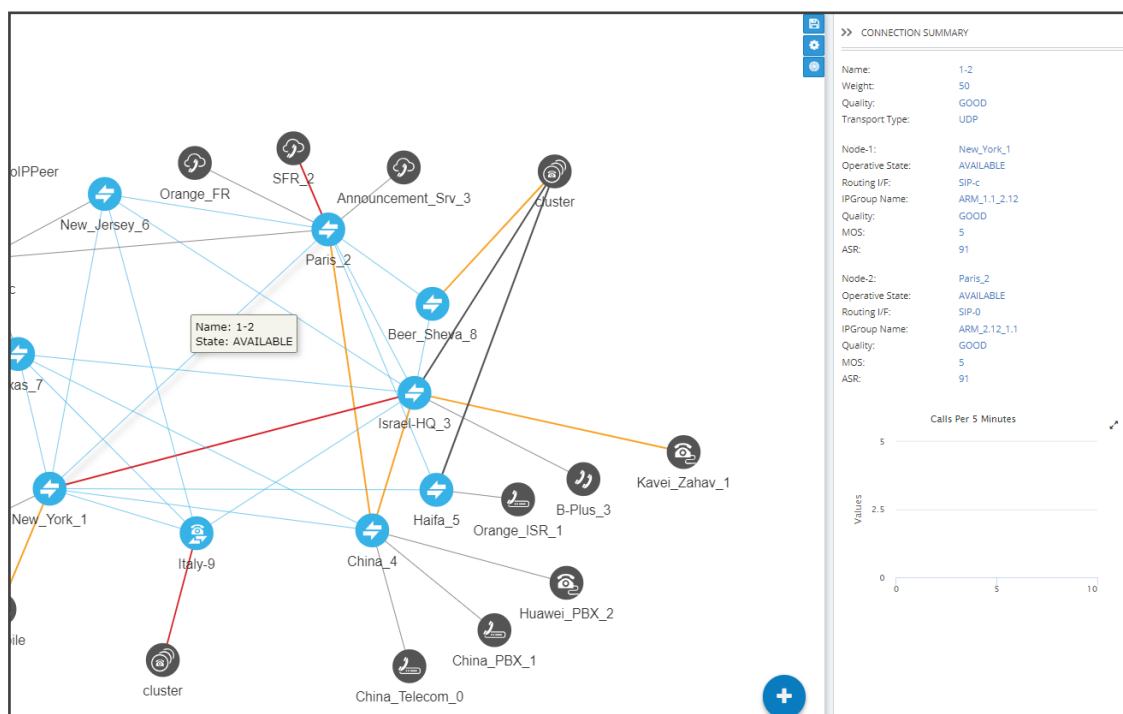
Color	Description
Blue	GOOD quality Connection
Grey	GOOD quality Peer Connection
Orange	FAIR quality Connection / Peer Connection
Red	BAD quality Connection / Peer Connection
Dotted grey	UNKNOWN quality, i.e., there is insufficient data to determine quality statistics. After enough calls are routed by the Connection / Peer Connection, the color changes from grey to the color of the determined quality static.

A glance at the page reveals the quality of each Connection and Peer Connection, indicated by color code.

➤ **To view a summary of a Connection, including quality:**

1. In the Network Map page, select **topology** layer and/or **quality** layer and then click (select) the Connection whose summary you want to view.

Figure 2-4: Connection Summary Including Quality



2. View a summary of the connection in the Connection Summary pane on the right side of the Network Map page. The figure above shows the Connection Summary pane for the

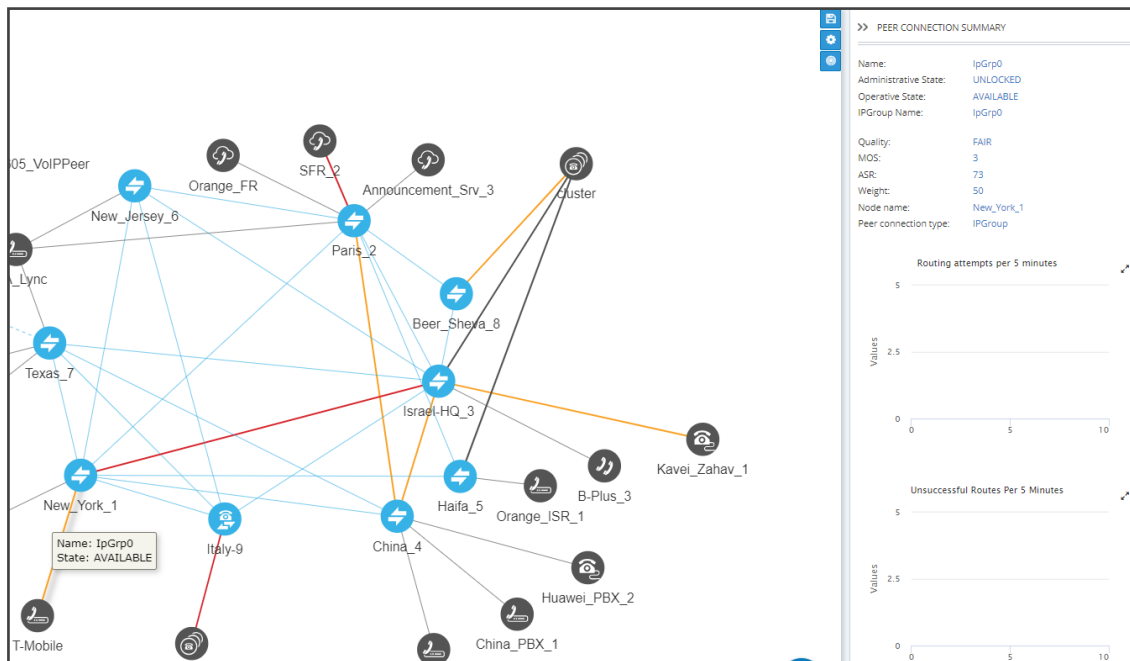
Connection between the node **Paris_2** and **New_York_1**. The 'Quality' parameter for both nodes is 'GOOD'.

3. Use each direction's MOS and ASR values to tune the threshold for quality-based routing [Settings > Routing > Quality Based Routing] and optimize network quality.

➤ **To view a summary of a Peer Connection, including quality:**

1. In the Network Map page, select **topology** layer and/or **quality** layer and then click (select) the Peer Connection whose summary you want to view.

Figure 2-5: Quality Layer - Peer Connection

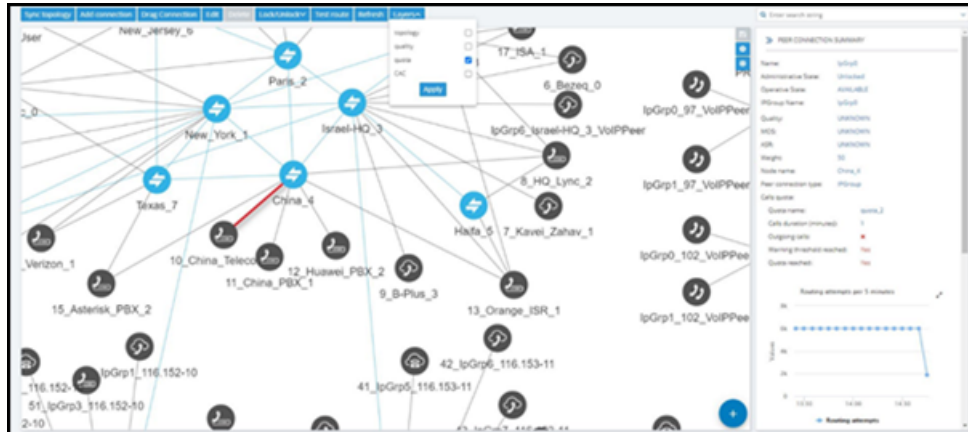


2. In the Peer Connection Summary pane on the right side of the Network Map page, view the Peer Connection Summary for the Peer Connection you clicked (selected). The figure above shows the Peer Connection whose name is 'IpGrp0'. The 'Quality' parameter is 'FAIR'.
3. Use each direction's MOS and ASR values to tune the threshold for quality-based routing [Settings > Routing > Quality Based Routing] and optimize network quality.

➤ **To view the Quota status of the network:**

1. Select the **quota** layer in the ARM Topology Map.

Figure 2-6: Quota Layer



2. View the Quota-related status of the Peer Connection; review which Peer Connections are blocked due to the Calls Quota being reached.



- The Quota layer can be combined with other layers in the customer's network.
- If a Peer Connection is attached to a Resource Group with a Quota, the ARM shows the Resource Group name in the Peer Connection summary; the ARM doesn't show the Quota information.

3. If a Peer Connection has a Quota attached, click the Peer Connection in the Topology Map page to view information about the Quota in the page's Summary.

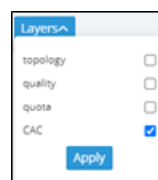
Figure 2-7: Summary Information about Calls Quota

Calls quota:	
Quota name:	quota_2
Calls duration (minutes):	1
Outgoing calls:	✗
Warning threshold reached:	Yes
Quota reached:	Yes

➤ **To view the CAC status of the network:**

1. Select the **CAC** layer in the ARM Topology Map.

Figure 2-8: CAC Layer



2. In the Network Map, view status information related to the CAC Profile of the Peer Connection and review which Peer Connections are blocked due to the CAC being reached.



The CAC layer can be combined with other layers in the customer's network.

3. Blocked entities due to CAC are shown red. You'll also view an indication of direction, if relevant.



- Make sure if you view a red color in the Network Map that it is not due to Quality (for example).
- To correctly correlate colors, make sure of which layers you selected.

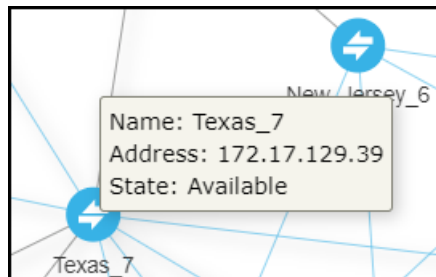
Getting Acquainted with Network Map Page Actions

Node Information and Actions

In the Network Map page you can view node information and perform node actions.

➤ **To view node information:**

1. Point your cursor over the node whose information you want to view.



2. Use the following table as reference.

Table 2-4: Node Information

Item	Description
Name	The name of the Node
Address	The IP address of the Node
State	<p>Available / Unavailable / Unrouteable / Logged out / Logging in. The ARM provides a robust node State Machine based on the node's connectivity to the ARM component. When determining a node's connectivity and ability to process a call in the State Machine, the ARM factors in the node's connectivity to the ARM Configurator (both ways), the node's connectivity to ARM Routers (from the node's perspective) and the node's connectivity to ARM Routers (from the ARM Routers perspective). The ARM Routers attempt to serve the node's routing requests even if the node is reported as disconnected from the ARM Configurator. In this case, the ARM Router routes calls based on last available information about the nodes' interfaces, their availability and quality. This node's 'Unknown' state is reported via ARM alarms. A node becomes Unrouteable only if all ARM Routers report that the node does not communicate with them (neither 'keep-alive' nor 'Get Route' requests).</p> <p>To help you localize a network issue, the Node Summary screen displays a detailed view of the node's connectivity status, as shown in the following figure.</p>

3. Click a node to view the 'Node Summary' on the right side of the Network Map page.

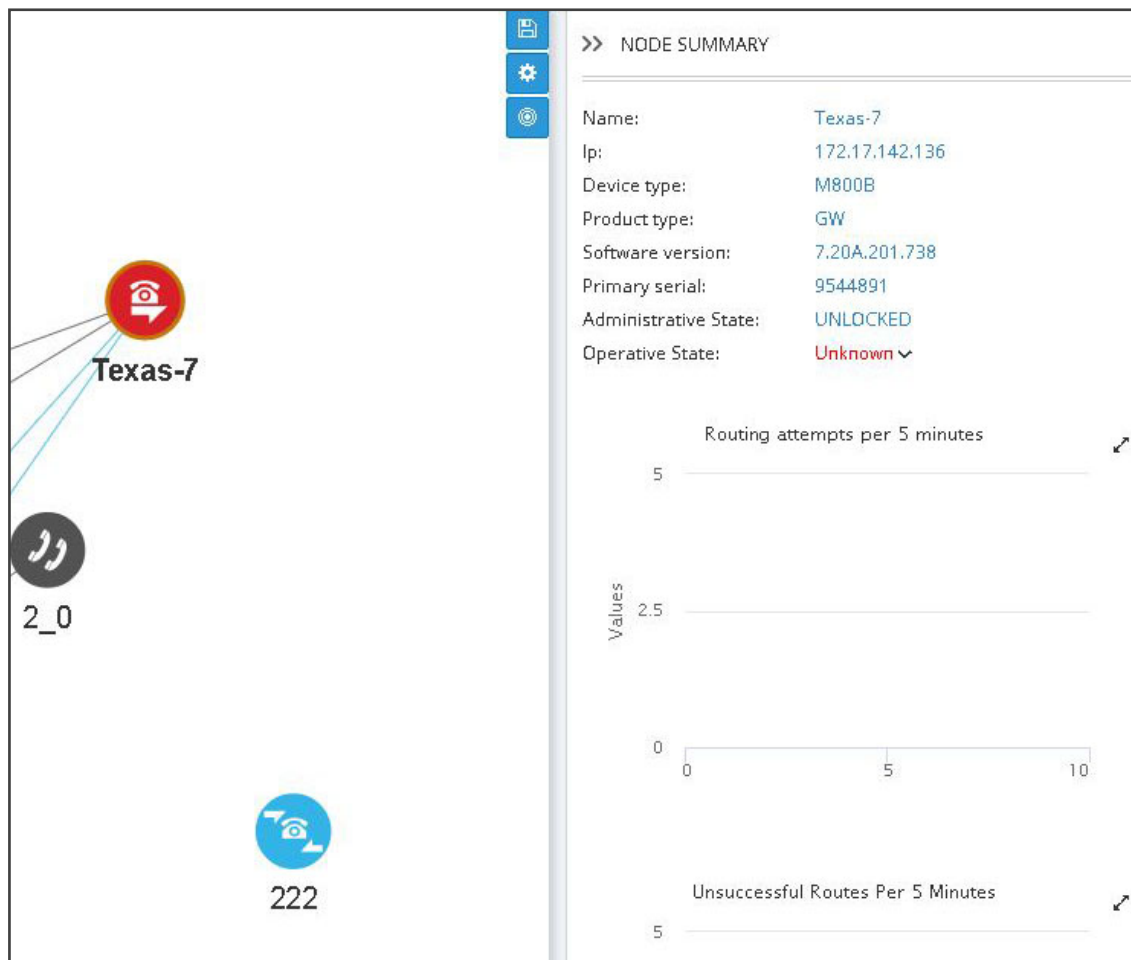
Figure 2-9: Node Summary

» NODE SUMMARY		» NODE SUMMARY	
Name:	Paris_2	Name:	Venice
Teams Role:	REMOTE	Teams Role:	NOT_TEAMS
Address:	172.17.129.34	Address:	172.17.129.16
Device type:	Mediant VE SBC	Device type:	Mediant VE SBC
Product type:	SBC	Product type:	SBC
Software version:	7.20A.260.147	Software version:	7.20A.260.147
Primary serial:	155359658512645	Primary serial:	262674720828826
Secondary serial:	12608608	Secondary serial:	10725168
Administrative State:	UNLOCKED	Administrative State:	UNLOCKED
Operative State:	Available ▾	Operative State:	Available ▾

The preceding figure above left shows the Node Summary of an entity whose Teams Role is REMOTE. The figure above right shows the Node Summary of an entity whose Teams Role is NOT_TEAMS.

The example below shows a node's 'Operative State' as **Unknown** when the ARM Configurator is unable to access the SBC 'Texas-7'. Note that in this state, call routing requests coming from this node to the ARM Routers will be served.

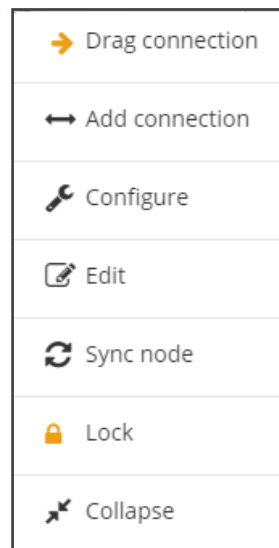
Figure 2-10: Node's 'Unknown' Operative State



➤ **To perform an action on a node:**

1. Right-click the node on which to perform an action.

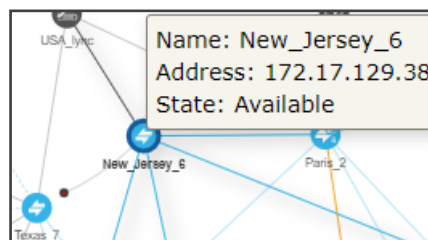
Figure 2-11: Node Actions



2. From the popup menu, choose:

- a. **Drag connection.** Allows you to draw (drag) a connection between two nodes in the Network Map (**New Jersey** and **Texas** in the following figure, where **New Jersey** is the node you right-clicked and from where you begin dragging, and **Texas** is the node in which you end the drag).

Figure 2-12: Drag Connection



- b. **Add Connection** [also available by selecting a node and then clicking the **Add Connection** button]

Figure 2-13: Add Connection

ADD CONNECTION

Name: *

Weight:

Transport Type:

	Node 1	Node 2
Node: *	<input type="text" value="New_Jersey_6"/>	<input type="text"/>
Routing Interface: *	<input type="text" value="SIP-c"/>	<input type="text"/>
Name: *	<input type="text"/>	<input type="text"/>
Ip Profile: *	<input type="text" value="ARM_IP_Profile"/>	<input type="text"/>
Media realm:	<input type="text"/>	<input type="text"/>
SIP Group name:	<input type="text"/>	<input type="text"/>

Advanced Conditions

☒ Keep connection properties synchronized

☒ use global quality definitions

☐ use specific quality definitions

☐ MOS ☐ ASR

OK **Cancel**

- ◆ Make sure the relevant SIP interface in the SBC is provisioned and configured as 'Used by routing server'
 - ◆ In the Add Connection screen shown in the figure above, Node-1 will be configured (the node you initially selected). From the 'Node-2' drop-down menu, select the node *to which* to make the connection, and then click **OK**. See [Adding an AudioCodes Node to the ARM](#) on page 74 for more information.
- c. **Configure.** Lets you directly configure a node (or SIP module) in the node's Web interface without needing to provide the node's credentials (Single Sign-on). See the AudioCodes device's *User's Manual* for detailed information. Nodes version 7.2.150 and later are supported. Earlier node versions do not support single sign-on; you must provide credentials before you can access their Web interface. Choose the option; the node's Web interface opens without prompting the operator for credentials.
- d. **Edit** [also available by selecting the node and then clicking the **Edit** button]
- ◆ In the Edit Node dialog that opens - see the following figure - update the credentials of the device if necessary.

Figure 2-14: Edit Node

The screenshot shows a dialog box titled "EDIT NODE". It contains the following fields and values:

- Name: ***: Texas_7
- Teams Role:**: Not Teams (dropdown)
- Address:**: 172.17.129.39
- Protocol:**: HTTP (dropdown)
- Routing server group:**: group of node New_York_1 (dropdown)
- Resource Groups:**: USANodes
- Credentials**: Configurator → Node (dropdown)
- Configurator → Node**: Texas_7 (dropdown)

At the bottom of the dialog are two buttons: "OK" and "Cancel".

- ◆ From the 'Protocol' drop-down menu, select the protocol that the ARM Configurator (server) uses when communicating with this node. Default: **HTTPS**. If you don't want to encrypt the traffic – e.g., when debugging – use **HTTP**.
- ◆ From the 'Routing server group' drop-down, select the Routing Server Group to which you attached the node, described under [Adding a Routing Server Group with Internal and External Priorities](#) on page 258.

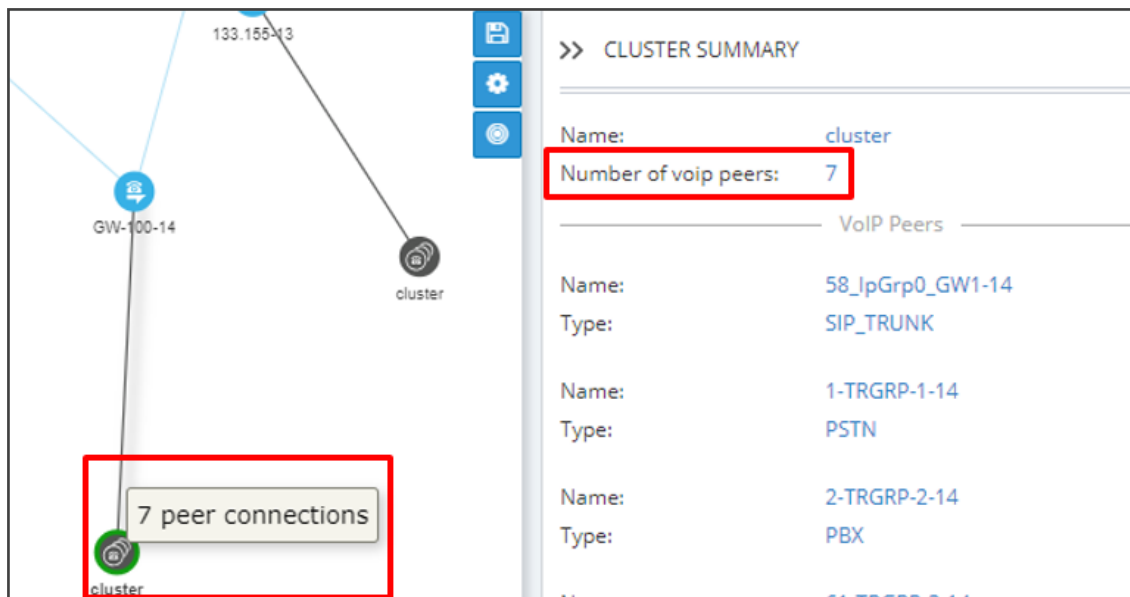
e. Sync Node

f. Lock/Unlock

- g. Collapse.** In Network Map view, you can collapse VoIP Peers associated with a node. In large networks containing multiple VoIP Peers with each VoIP Peer connected to a node, this can significantly simplify (unclutter) the view, facilitating more effective management. To apply a collapse:

- ◆ Select the **Collapse** action from the menu that pops up after right-clicking the node; all VoIP Peers associated with the node collapse.

Figure 2-15: Collapsed VoIP Peers



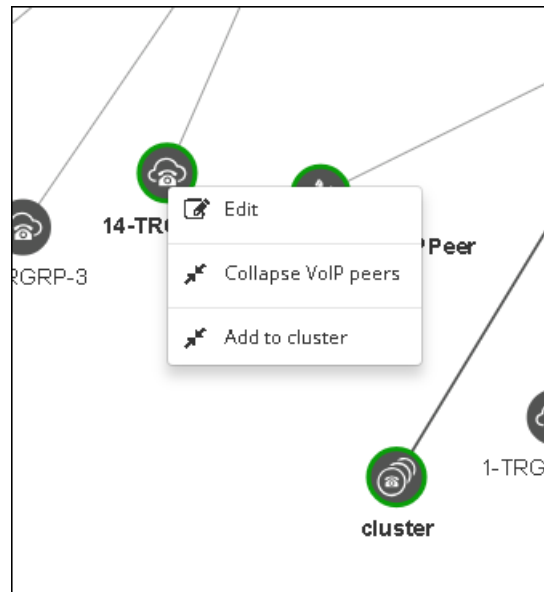
- ◆ [Refer to the preceding figure] The cluster's label in the Network Map *as well as* the Cluster Summary indicate the number of collapsed VoIP Peers / Peer Connections in the cluster.
- ◆ [Refer to the figure following] The Cluster Summary can also indicate the aggregated number of collapsed VoIP Peers / Peer Connections in a cluster.

Figure 2-16: Peer Connection Aggregation Summary: Number of Peer Connections



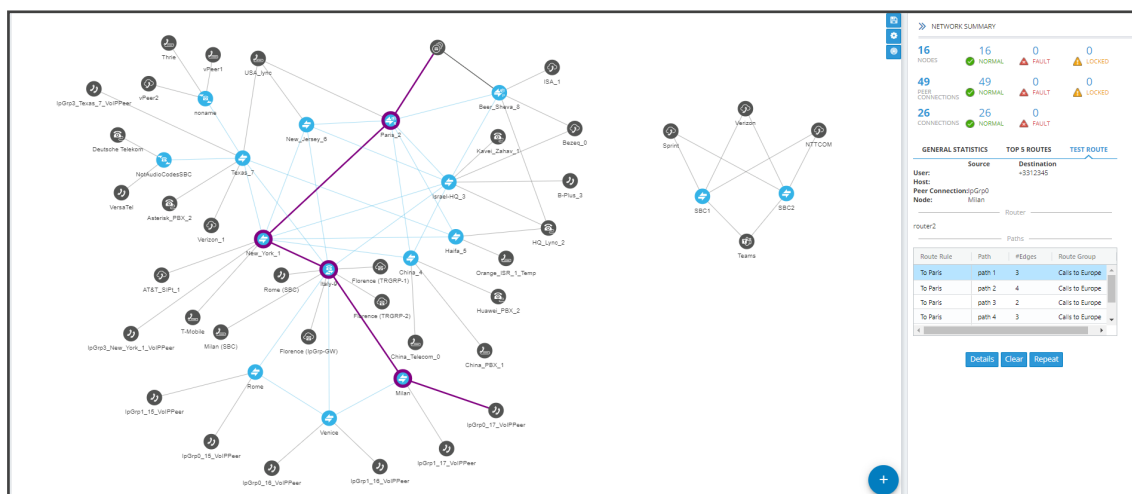
- ◆ **Add to cluster.** You can add an additional VoIP Peer or multiple VoIP Peers to an existing cluster: (1) Select the target cluster to which to add (2) press the **Ctrl** key click one or multiple VoIP Peers to add to the target cluster (3) right-click and from the pop-up menu select the action **Add to cluster**.

Figure 2-17: Add to cluster



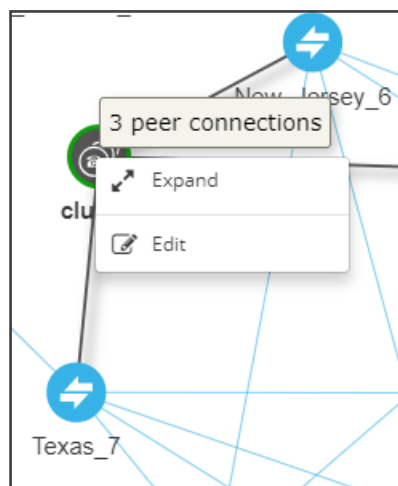
- ◆ VoIP Peers associated with more than one node are included in the collapsed cluster. If a test route is performed that terminates on a collapsed VoIP Peer, the VoIP Peer will not be expanded automatically and the path displayed in the GUI will terminate on the cluster icon.

Figure 2-18: Test Route Path Terminates on Collapsed VoIP Peer



- After collapsing VoIP Peers, you can expand them again by right-clicking the cluster icon and then choosing the **Expand** action from the popup menu.

Figure 2-19: Expand Cluster of VoIP Peers



- i. **Delete.** Only available if the Node has been **Locked** and no routing rules and Policy Studio rules are associated with it. If routing rules *are* associated with the Node or its Peer Connections and you want to delete it, update or delete the rule so it does not refer to the topology entity which is going to be deleted.

VoIP Peer Information and Actions

In the Network page, Map view, you can view VoIP Peer information and perform VoIP Peer actions. There are six types of VoIP Peers:

- SIP Trunk
- PBX
- IP PBX
- PSTN
- IP Phone
- N/A (default)

➤ To view VoIP Peer information:

1. Point your cursor over the VoIP Peer whose information you want to view.

Figure 2-20: SIP Trunk

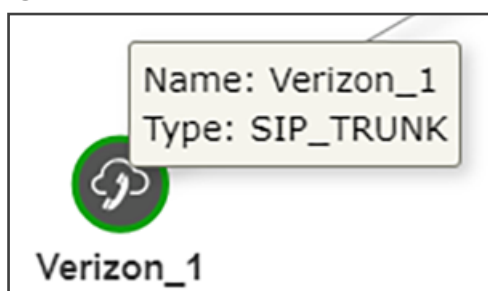


Figure 2-21: PBX | IP PBX

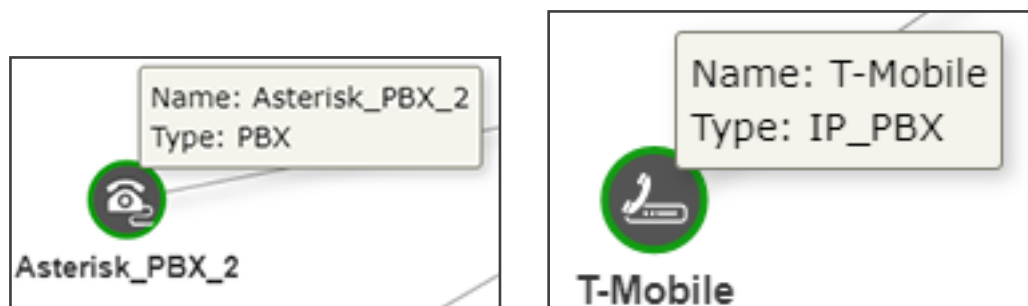


Figure 2-22: PSTN

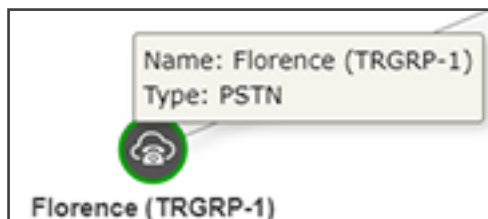
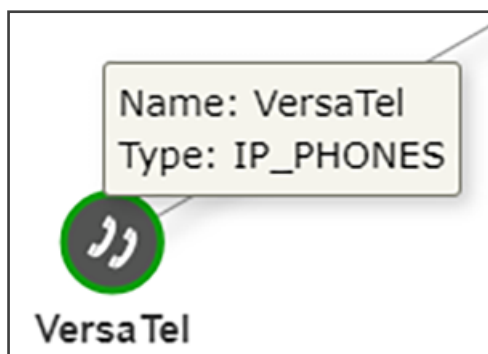


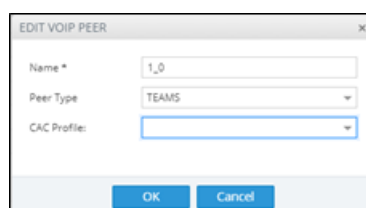
Figure 2-23: IP Phone



➤ **To edit a VoIP Peer:**

- Right-click the VoIP Peer icon and choose **Edit** from the popup.

Figure 2-24: Edit VoIP Peer



- ◆ You can edit the 'Name' of the VoIP Peer and/or select the 'Peer Type' from the drop-down menu.

➤ **To delete a VoIP Peer:**

- Right-click the VoIP Peer icon and then choose **Delete** from the popup menu.



The **Delete** option is only available if no Peer Connection or routing rules are associated with the VoIP Peer. If there are, you must first update / delete routing rules before you can delete the VoIP Peer. You must then associate the Peer Connection with another VoIP Peer.

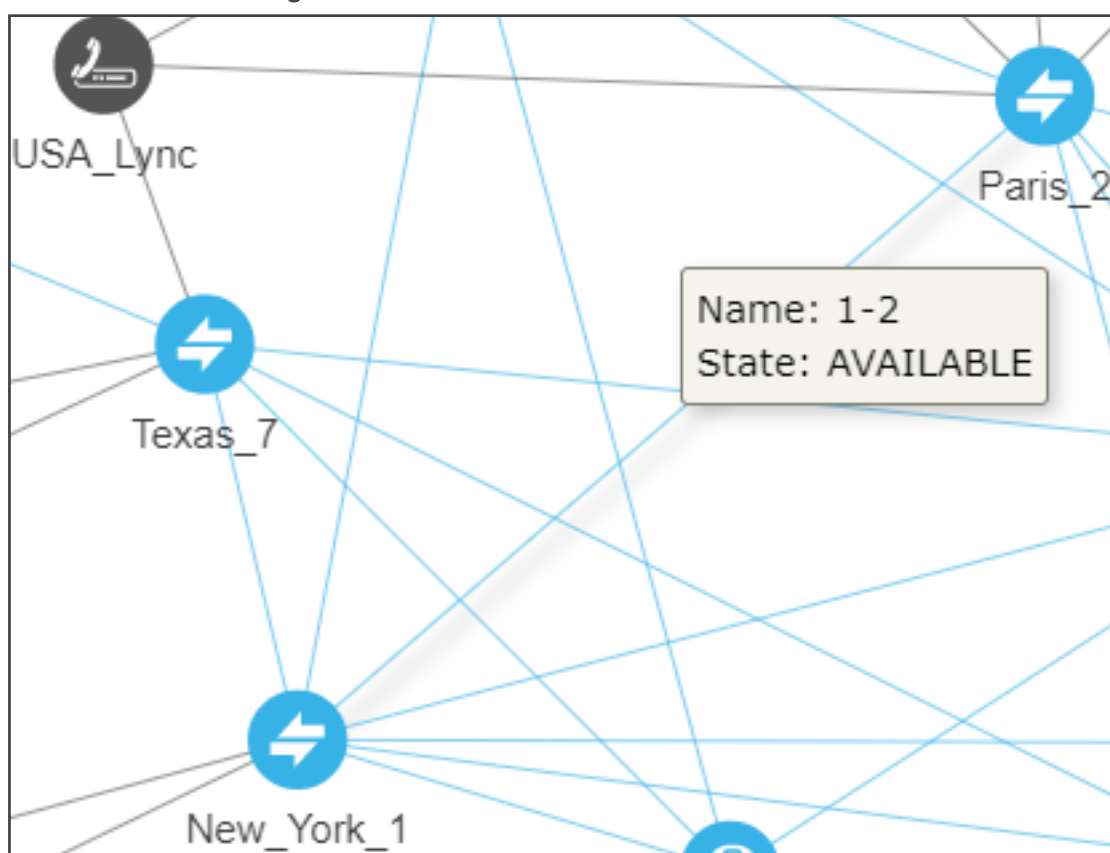
Connection Information and Actions

In the Network page, Map view, you can view connection information and perform connection actions.

➤ To view connection information:

1. Point your cursor over the connection whose information you want to view.

Figure 2-25: Connection Information



2. View the Name and the State of the connection.

➤ To perform an action on a connection:

1. In the popup menu, click **Edit** -or- **Delete**. [Note that **Add connection**, **Edit** and **Delete** are also available as action buttons in the Network Map page].

Figure 2-26: Edit Connection

2. You can edit the:
 - name of the connection
 - Weight (Range: 0-100. Default: 50)
 - Transport Type (Default: UDP)
3. Leave the **Keep connection properties synchronized** option unchanged at its default (selected) or clear it.
 - If selected (enabled), the ARM keeps the connection (IP Group) properties synchronized with the defined connection in the ARM so any change to the connection's IP Group or its Proxy Set in the SBC is corrected to sync with the ARM's defined connection.
 - If the option is cleared, the ARM Configurator will no longer synchronize the properties of the connection (IP Group) and only the Operative state of the connection will be reflected in the ARM.

As part of support for Local Media Optimization (LMO), the feature gives operators greater freedom and more precise control over their connections, whether they're properties which the ARM doesn't have access to or changes to the IP Profile, Media Realm or even the Proxy Set itself.

4. Leave the option **use global quality definitions** at its default for quality-based routing to be applied using global (ARM level) settings. Select **use specific quality definitions** to overwrite the global settings of quality-based routing condition for a specific connection, and then select the enabled 'MOS' and/or 'ASR' option (see [Routing Settings](#) on page 233 for related information).

Peer Connection Information and Actions

In the Network page Map view (**Network > Map**), you can view information about each Peer Connection and perform **Edit**, **Delete**, **Lock/Unlock**, **Test Route** and **Detach** actions on Peer Connections.

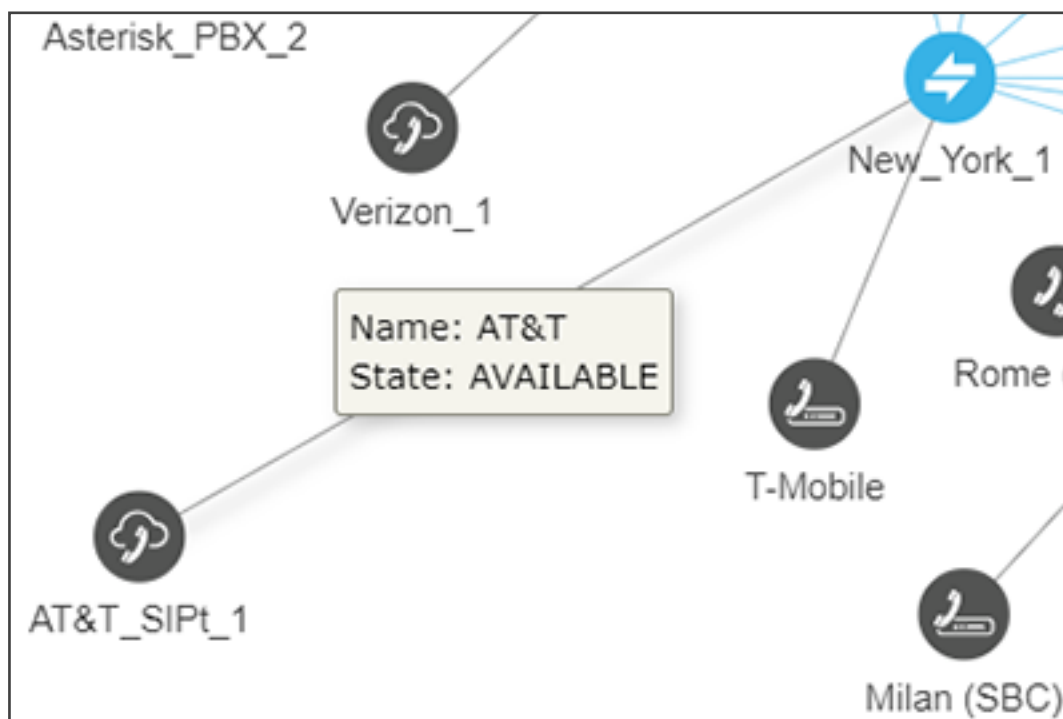


- The **Delete** option is displayed only for Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule.
- The **Detach** option is displayed only if the Peer Connection is connected to a VoIP Peer that is connected to more than one Peer Connection.
- The actions **Edit**, **Delete** and **Lock/Unlock** are also available in the Peer Connections page (**Network > Peer Connections**).

➤ To view Peer Connection information:

1. In the Network page Map view, point your cursor over the peer connection whose information you want to view.

Figure 2-27: Peer Connection Information



2. View the Peer Connection's Name and State.

➤ **To perform an action on a Peer Connection:**

1. In the Network page Map view, right-click the Peer Connection and choose **Edit** from the popup menu. The same action can be performed by selecting the Peer Connection and then clicking the **Edit** button.



The **Edit** action is also available in the Peer Connections page (**Network > Peer Connections**); select the Peer Connection and then click the **Edit** button.

Figure 2-28: Edit Peer Connection

- a. Modify the weight (Range: 0-100; Default: 50) for the ARM to calculate the optimal call path. Use if you have a VoIP Peer as a Routing Rule action and you want to prioritize a specific Peer Connection (e.g., SIP trunk) to be chosen for calls routing. Also use to reflect Peer Connection cost or bandwidth.
- b. From the drop-down menu, select the VoIP Peer that this Peer Connection is connected to.
- c. From the drop-down menus, select the Normalization Rule for Source and Destination URI User if pre-routing manipulation is required for a specific Peer Connection (configured as shown in [Adding a Normalization Group](#) on page 198).
- d. Attach a Calls Quota to the Peer Connection (or to a group of Peer Connections gathered in a Resource Group of type 'Peer Connection'). The same quota can be attached multiple times (reused for multiple Peer Connections or Resource Groups). From the 'Calls quota' drop-down, select a quota (defined as shown in [Calls Quota](#) on

page 246). In the Peer Connections page (**Network > Peer Connections**), the quota is shown in the 'Calls Quota' column.

STATUS	NODE	NAME	VOIP PEER	IP GROUP	OPERATIVE STATE	ADMINISTRATIVE STATE	QUALITY	CALLS QUOTA	CAC PROFILE
✓	172.17...	ipGrp0	1,0	ipGrp0	✓	🔒	UNKNOWN		
✓	172.17...	ipGrp1	1,1	ipGrp1	✓	🔒	UNKNOWN		
✓	172.17...	21819741350535	2,0	ipGrp0	✓	🔒	UNKNOWN		
⚠	172.17...	ipGrp1	2,1	ipGrp1	✓	🔒	UNKNOWN	manual_test	

When the Peer Connections page is used, you can filter all Peer Connections using the same defined quota (and / or CAC Profile filter):

Free Text:

Operative State:

Administrative State:

Quality:

Calls Quota:

CAC Profile:

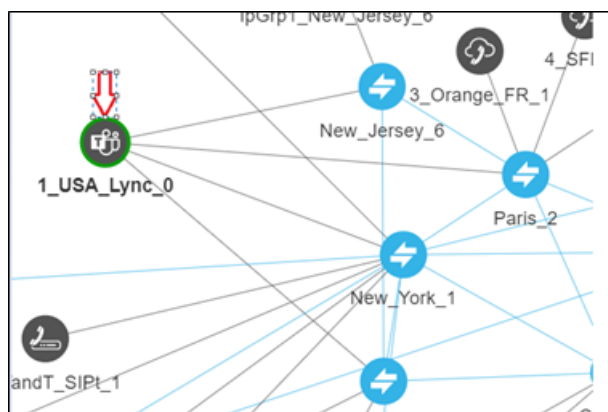
Search

Cancel

When selecting a Peer Connection with an attached quota, the following information related to quota counting is displayed:

Calls quota:	
Quota name:	myQuota
Calls duration (minutes):	0
Outgoing calls:	✓
Warning threshold reached:	No
Quota reached:	No

The Calls Quota can also be attached to several Peer Connections grouped in the same Resource Group. Note that only a Resource Group of type 'Peer Connection' can be associated with a Calls Quota. In this case, the calls balance, in minutes (defined by the Quota), is shared by all Peer Connections in the group. If the operator wants to have a calls balance, in minutes, associated with a VoIP Peer (for example, with a specific PBX), and there are multiple Peer Connections connected to this VoIP Peer, all these Peer Connections should be gathered into a Resource Group (**Network > Resource Group**). After that, the Quota can be attached to this Resource Group. In the following Network Topology, for example, Peer Connections come from four different SBCs to Teams:



To apply a quota to this VoIP Peer, first define a Resource Group made up of these four Peer Connections (coming from four different SBCs – New_Jersey, Paris, New_York and Texas), and then attach the Quota:



The ability to select a 'Calls Quota' becomes available only when you select 'Resource Group type' to be **Peer Connection**.

The attached Quota is shown in the table of the Resource Groups:

NAME	TYPE	ELEMENTS	CALLS QUOTA
1	Peer C...	IpGrp0 (New_York_1)	
pCons	Peer C...	IpGrp2 (69), IpGrp0 (69), IpGrp1 (69)	
Teams_PCons_Group	Peer C...	IpGrp0 (New_York_1), IpGrp0 (Paris_2), IpGrp0 (New_Jersey_6)	Teams_calls_Budget

When a Resource Group with an attached Quota is selected, relevant information about the Calls Quota status is displayed on the right side of the page:

» RESOURCE GROUPS SUMMARY	
Name:	Teams_PCons_Group
Type:	Peer Connection
Elements:	IpGrp0 (New_York_1), IpGrp0 (Paris_2), IpGrp0 (New_Jersey_6)
Calls quota:	
Quota name:	Teams_calls_Budget
Calls duration (minutes):	0
Outgoing calls:	✓
Warning threshold reached:	No
Quota reached:	No



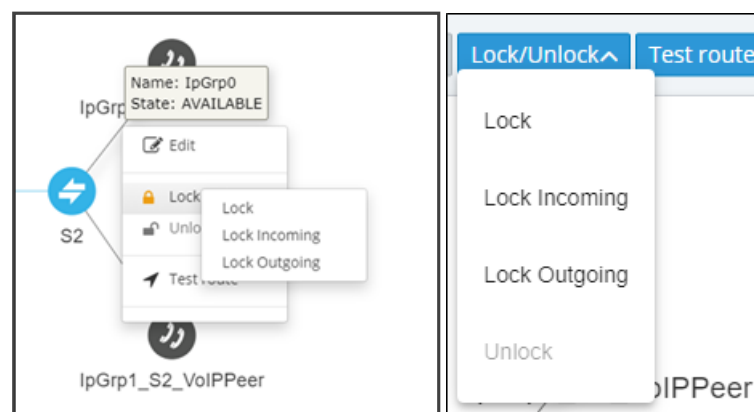
- If the operator tries to attach a Quota to a Resource Group and one of the Peer Connections in this group already has a Quota, the operation will fail.
- If the operator tries to add a Quota to a Peer Connection that is attached to a Resource Group with a Quota, the operation will fail.
- When there are two Resource Groups with the same Peer Connection, if a Quota is attached to one of the groups and the operator tries to attach a Quota to the other group, the operation will fail.

- e. Leave **use global quality definitions** selected (default) for this Peer Connection to use the global quality profile configured as shown in [Configuring Criteria for a Quality Profile](#) on page 233.

Select **use specific quality definitions** for this Peer Connection to use only the 'MOS' or the 'ASR' criteria of the quality profile configured as shown in [Configuring Criteria for a Quality Profile](#) on page 233.

2. In the Network page Map view, right-click the Peer Connection and choose **Lock / Unlock** from the popup menu as shown in the figure below left. The same action can be performed in the Network page Map view by selecting the Peer Connection and then clicking the **Edit** button as shown in the figure below right.

Figure 2-29: Lock / Unlock Peer Connection



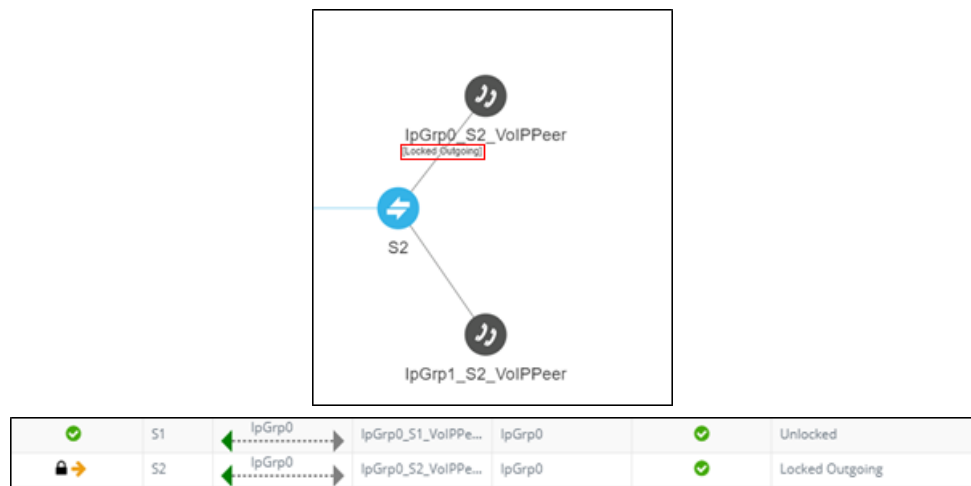


The **Lock / Unlock** action is also available in the Peer Connections page (**Network > Peer Connections**); select the Peer Connection and then click the **Edit** button.

In addition to **Lock / Unlock** of a Peer Connection, you can select a *directional based Lock / Unlock*. This feature allows you to (for example) stop *only traffic towards* a specific VoIP Peer (for example, a specific IVR) while *calls coming from* this VoIP Peer will still be routed to their destination. You can use the feature to perform a graceful stoppage of traffic for maintenance reasons (for example). The feature is essential for IVR VoIP Peers when there are always calls in a queue that are not yet connected to an agent. From the IVR's perspective, the connection to the agent is outbound calls; without the uni-directional lock feature, calls fail.

The directional lock of a Peer Connection is indicated in Map page and in the Peer Connections page.

Figure 2-30: Locked / Unlocked Peer Connection in Map page (L) and in Peer Connections page (R)



3. In the Network Map page, right-click the Peer Connection and choose **Test Route** from the popup menu (see [Testing a Route](#) on page 87 for more information).
4. Optionally, you can **Delete** the Peer Connection. Only Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule, can be deleted.



The action **Delete** is also available in the Peer Connections page (**Network > Peer Connections**); select the Peer Connection and then click the **Delete** button. The **Delete** action is displayed only for Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule.

5. If the Peer Connection is connected to a VoIP Peer that is connected to more than one Peer Connection, you can click **Detach**. You'll be prompted to define a name for a new VoIP Peer. The **Detach** action is displayed only if the Peer Connection is connected to a VoIP Peer that is connected to more than one Peer Connection.

Repositioning Elements in the Network Map Page

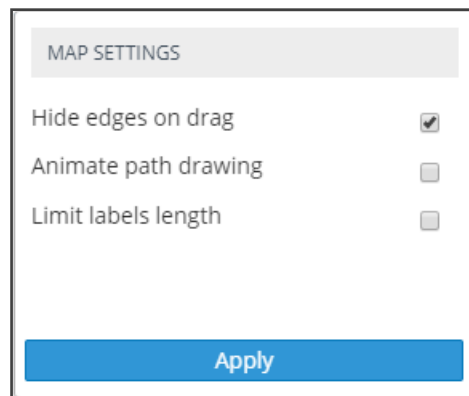
The ARM's Network Map page allows you to move and reposition multiple selected elements - Nodes and VoIP Peers – simultaneously to facilitate a friendlier operator experience and to decrease operator vulnerability to routing configuration errors.

You can select a combination of elements and move and reposition them simultaneously with your mouse device. After moving / repositioning elements, you need to perform a save else they'll be restored to their original position in the following session.

Even when managing very large networks with extended numbers of topology elements (Nodes and VoIP Peers), the ARM agilely performs relocations in the page.

When moving / repositioning elements in the page, you can also use the **hide edges on drag** option available from the 'Diagram Configurations' icon.

Figure 2-31: Hide Edges on Drag



When selected, Connections and Peer Connections are not displayed in the page when an element (or multiple elements) is moved and repositioned. The option provides a less cluttered view of network elements in the page, facilitating more effective relocation.

Peer Connections Page Actions

In the Peer Connections page (**Network > Peer Connections**) you can view the Peer Connections.

Figure 2-32: Peer Connections

STATUS	NODE	NAME	VOIP PEER	IP GROUP	OPERATIVE STATE	ADMINISTRATIVE STATE	QUALITY	CALLS QUOTA	CAC PROFILE	PEER CONNECTIONS SUMMARY
✓	New_York...	ipGrp0	T-Mobile	ipGrp0	✓	✗	FAIR			Name: ipGrp0 Administrative State: Unlocked Operative State: AVAILABLE IPGroup Name: ipGrp0 Weight: 50 Node name: New_York_1 Peer connection type: IPGroup Quality: FAIR MOS: 2.5 ASR: 50
✓	New_York...	AT&T	AT&T_SPL_1	ipGrp1	✓	✗	GOOD			
✓	Paris_2	ipGrp0	USA_lync	ipGrp0	✓	✗	GOOD			
✓	Paris_2	OrangeIPGrp1	Orange_FR	ipGrp1	✓	✗	GOOD			
✓	Paris_2	ipGrp0	SFR_2	ipGrp2	✓	✗	BAO			
✓	Paris_2	Announcement_Srv_3	Announcement_Srv_3	ipGrp3	✓	✗	GOOD			
✓	Israel-HQ_3	BezeqGrp0	Bezeq_0	ipGrp0	✓	✗	GOOD			
✓	Israel-HQ_3	KavotZahavGrp1	KavotZahav_1	ipGrp1	✓	✗	FAIR			
✓	Israel-HQ_3	ipGrp2	HQ_lync_2	ipGrp2	✓	✗	GOOD			
✓	Israel-HQ_3	ipGrp3	B-Plus_3	ipGrp3	✓	✗	GOOD			
✓	China_4	ChinaTelecomGrp0	China_Telecom_0	ipGrp0	✓	✗	GOOD			
✓	China_4	ipGrp1	China_PBX_1	ipGrp1	✓	✗	GOOD			
✓	China_4	HuaweiPBXGrp2	Huawei_PBX_2	ipGrp2	✓	✗	GOOD			
✓	Haifa_5	HQ_lyncGrp0	HQ_lync_2	ipGrp0	✓	✗	GOOD			
✓	Haifa_5	OrangeGrp1	Orange_SSR_1_Temp	ipGrp1	✓	✗	GOOD			
✓	New_Yers...	ipGrp3	USA_lync	ipGrp3	✓	✗	GOOD			
✓	Texas_7	ipGrp0	USA_lync	ipGrp0	✓	✗	GOOD			

The following information on each Peer Connection is displayed:

■ Status

- Node
- Name
- VoIP Peer
- IP Group
- Operative State
- Administrative State
- Quality
- Calls Quota
- CAC Profile
- MOS
- ASR

The information displayed in the Peer Connections page is identical to that displayed in the Network Map view described under [Peer Connection Information and Actions](#) on page 41. You can search for the name of a Node associated with the Peer Connection, the name of a Peer Connection, or a VoIP Peer name. It's useful to find, for example, all Peer Connections of a specific Node.

Use the buttons in the Peer Connections page to perform the following actions:

- **Sync Topology**
- **Edit** after selecting the row of the Peer Connection to edit. For more information, see under [Peer Connection Information and Actions](#) on page 41.
- **Delete** after selecting the row of the Peer Connection to delete. Note that the **Delete** option is displayed only for Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule. for related information, see under [Peer Connection Information and Actions](#) on page 41.
- **Lock/Unlock** after selecting the row of the Peer Connection to lock/unlock. For more information, see under [Peer Connection Information and Actions](#) on page 41.

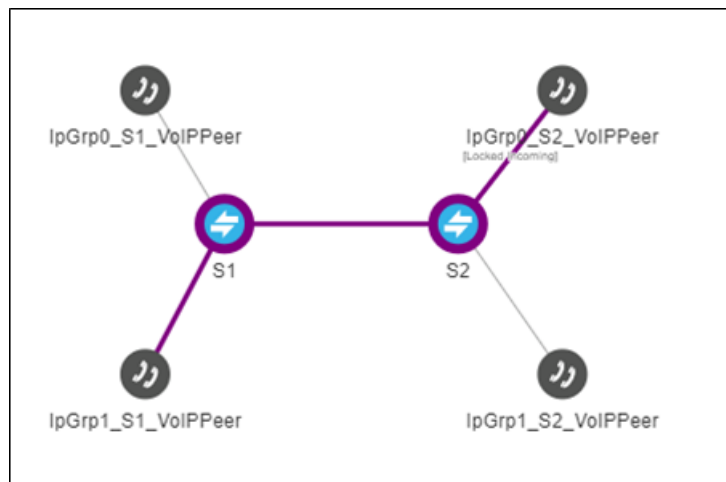
In addition to **Lock / Unlock** of a Peer Connection, you can select a *directional based* **Lock / Unlock**. This feature allows you to (for example) stop *only traffic towards* a specific VoIP Peer (for example, a specific IVR) while *calls coming from* this VoIP Peer will still be routed to their destination. You can use the feature to perform a graceful stoppage of traffic for maintenance reasons (for example). The feature is essential for IVR VoIP Peers when there are always calls in a queue that are not yet connected to an agent. From the IVR's perspective, the connection to the agent is outbound calls; without the uni-directional lock feature, calls fail.

The directional lock of a Peer Connection is indicated in Map page and in the Peer Connections page.



- A lock of the opposite direction automatically unlocks the previous lock direction; it doesn't apply a bi-directional lock; it allows traffic of the previously locked direction. Either direction is applicable.
- The Offline Planning page (**Network > Offline Planning**) as well as the Test Route feature support direction-based lock. In the example shown in the figure below, Test Route is activated (and allowed) for outgoing calls even though the Peer Connection is locked for incoming calls.

Figure 2-33: Test Route Activated for Outgoing Calls even though the Peer Connection is Locked for Incoming Calls



- Multiple rows can be selected; multiple actions (delete, lock/unlock, etc.) are supported.
- For more information about **Sync Topology**, see [Synchronizing Topology](#) on page 86.
- For more information about the **Edit**, **Delete** and **Lock/Unlock** actions, see under [Peer Connection Information and Actions](#) on page 41.

VoIP Peers Page Actions

In addition to the Peer Connections page and the Connections page, the ARM displays a VoIP Peers page (**Network > VoIP Peers**).

Figure 2-34: VoIP Peers Page

Name	Type	CAC Profile	CAC State	Peer Connections
Peer-1_10.0.0.1/16_VoIPPeer	NA			Peer-10.0.0.1/16
Peer-2_10.0.0.1/16_VoIPPeer	NA			Peer-10.0.0.1/16

The page allows operators to manage associating a Network Topology element with a CAC Profile. When you attach a CAC Profile to a VoIP Peer (for example), the VoIP Peers page makes management of the operation very convenient.

The page allows operators to apply **Edit**, **Delete** or **Refresh** actions.

The following information is available per VoIP Peer:

Name (Editable), **Type** (Editable), **CAC Profile** (can be attached by the operator), **CAC State** (available as read-only if a CAC Profile is attached), **Peer Connections** (list of associated Peer Connections).

The following figure shows the search and filters you can use in the page:

Figure 2-35: VoIP Peers Page - Search Filter

Search Filter Dialog:

- Search string:
- Name:
- CAC State:
- Peer Connections:
- CAC Profile:
- Buttons: Search, Cancel

You may find it useful to filter (for example) all VoIP Peers with a specific CAC Profile attached, or to filter VoIP Peers blocked due to an attached CAC Profile.

Connections Page Actions

In the Connections page (**Network > Connections**) you can view the connections you defined.

Figure 2-36: Connections

Sync Topology Add Edit Delete Refresh								Enter search string	
STATUS	NODE 1	ROUTING IF-1	NAME	NODE 2	ROUTING IF-2	WEIGHT	QUALITY		
✓	Beer_Sheva_8	SIP-c	3-8	Israel-HQ_3	SIP-c	10	UNKNOWN		
✓	133.145-13	SIP-c	12-13	133.144-12	SIP-c	10	UNKNOWN		
✓	China_4	SIP-c	1-4	New_York_1	SIP-c	20	UNKNOWN		
✓	Israel-HQ_3	SIP-c	IpGrp0	Paris_2	SIP-c	50	UNKNOWN		
✓	China_4	SIP-c	3-4	Israel-HQ_3	SIP-c	10	UNKNOWN		
✓	133.142-10	SIP-c	10-12	133.144-12	SIP-c	10	UNKNOWN		
✓	133.145-13	SIP-c	10-13	133.142-10	SIP-c	10	UNKNOWN		
✓	133.143-11	SIP-c	10-11	133.142-10	SIP-c	10	UNKNOWN		
✓	133.144-12	SIP-c	12-14	GW-100-14	SIP-c	50	UNKNOWN		
✓	Texas_7	SIP-c	6-7	New_Jersey_6	SIP-c	50	UNKNOWN		

You can view the following information on each connection:

- Status
- Node 1
- Routing Interface 1
- Name
- Node 2
- Routing Interface 2
- Weight
- Quality

The Search functionality is allowed for all the relevant information fields: Node Name, Connection Name, Weight or Routing Interface.

The information displayed in the Network page's Connections view is identical to that displayed in the Network Map view described under [Connection Information and Actions](#) on page 39.

You can perform the following actions:

- Sync Topology
- Add Connection (after selecting the row of the connection to edit)
- Edit Connection (after selecting the row of the connection to edit)
- Delete Connection (after selecting the row of the connection to edit)
- Refresh

Multiple rows can be selected and multiple delete is supported. For more information about Sync Topology, see [Synchronizing Topology](#) on page 86. For more information about the Add, Edit and Delete Connection, see under [Connection Information and Actions](#) on page 39.

Do not modify the SBC-level / gateway-level configuration of the connections created by the ARM. It will disrupt routing decisions/performance.

Resource Groups Page Actions

The Resource Groups feature allows network administrators to add and view a group of ARM topology resources of the same type. The Resource Groups page (**Network > Resource Groups**) allows operators to view defined Resource Groups and determine at a glance the elements defined in each. The page also allows operators to add, edit and delete Resource Groups. Each Resource Group can only comprise one type of element: Node, Peer Connection or VoIP Peer.

Operators can use

- a Resource Group comprising Nodes or Peer Connections as the source of a call in a Routing Rule
- a Resource Group comprising Nodes or Peer Connections as the source Resource Group in a Policy Studio rule
- any Resource Group as the action of a routing rule action

Figure 2-37: Resource Groups

MAP	OFFLINE	PEER CONNECTIONS	VOIP PEERS	CONNECTIONS	RESOURCE GROUPS	IP PROFILES	CUSTOMERS
<div> Add Edit Delete Refresh </div>							
NAME		TYPE	ELEMENTS		CALLS QUOTA		
IsraelSBCs		Node	Israel-HQ_3, Haifa_5				
USANodes		Node	New_York_1, New_Jersey_6, Texas_7				
OVOC_pCons		Peer Connection	IpGrp0 (Venice), IpGrp1 (Venice), IpGrp0 (Milan), IpGrp1 (Milan)				

➤ To add a Resource Group:

1. In the Resource Groups page, click the **Add** button.

Figure 2-38: Add Resource Group

2. Enter a name for the Resource Group that is distinct from the names of other Resource Groups; define a user-friendly name to facilitate intuitive routing management later.
3. From the 'Type' drop-down, select either:
 - Node
 - Peer Connection
 - VoIP Peer
4. From the 'Elements' drop-down, select the Nodes, Peer Connections and / or VoIP Peers to include in the Resource Group and click **OK**.



- To edit or delete a defined Resource Group, select it in the Resource Groups page and then click **Edit** or **Delete**.
- Operators can edit the elements comprising the Resource Group and / or the name of the group.
- After defining a new Resource Group, the group type cannot be changed (for example, from a Nodes group to a VoIP Peers group).

IP Profiles Page

Operators can define IP Profiles as part of support for Local Media Optimization (LMO). Three default IP Profiles are by default shipped with the ARM. These cannot be deleted but can be updated. They're predefined to support:

- Regular connections ('ARM_IP_Profile')
- Connections of Teams Remote to Teams Proxy devices ('ARM_IP_Profile_Remote_to_Proxy')
- Connections between Teams Proxy and Teams Remote devices ('ARM_IP_Profile_Proxy_to_Remote').

➤ **To add a new IP Profile:**

1. Open the IP Profiles page (**Network > IP Profiles**).

Figure 2-39: IP Profiles

<div><div>Add</div><div>Edit</div><div>Delete</div><div>Restore To Default</div><div>Refresh</div></div>									
NAME	SBC MEDIA SECURITY MODE	REMOTE 3XX MODE	REMOTE REFER MODE	REMOTE REPLACES MODE	ICE MODE	SIP UPDATE SUPPORT	REMOTE RE-INVITE	REMOTE DELAYED OFFER SUPPORT	» IP PROFILES DETAILS
ARM_IP_Profile (Default)	As Is	Transparent	Handle Locally	Standard	Disable	Supported	Supported	Supported	Name: ARM_IP_Profile SBC Media Security Mode: As Is Remote 3xx Mode: Transparent Remote REFER Mode: Handle Locally Remote Replaces Mode: Standard ICE Mode: Disable SIP UPDATE Support: Supported Remote re-INVITE: Supported Remote Delayed Offer Support: Supported Remote Representation Mode: According to Operation Mode Remote Hold Format: Transparent
ARM_IP_Profile_Remote_To_Proxy (Default)	Secured	Handle Locally	Handle Locally	Handle Locally	Lite	Not Supported	Supported only with SDP	Not Supported	
ARM_IP_Profile_Proxy_To_Remote (Default)	As Is	Transparent	Regular	Standard	Disable	Supported	Supported	Supported	

2. In the IP Profiles page (**Network > IP Profiles**), click **Add**.

Figure 2-40: Add IP Profile

ADD IP PROFILE

Name: *

SBC Media Security Mode

As Is

Remote 3xx Mode:

Transparent

Remote REFER Mode:

Handle Locally

Remote Replaces Mode:

Standard

ICE Mode:

Disable

SIP UPDATE Support:

Supported

Remote re-INVITE:

Supported

Remote Delayed Offer Support:

Supported

Remote Representation Mode:

According to Operation Mode

Remote Hold Format:

Transparent

OK

Cancel

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

Table 2-5: IP Profile Parameters

Parameter	Description
Name	Configure an intuitive name for the IP Profile, to facilitate effective management later.
SBC Media Security Mode	Select either: <ul style="list-style-type: none"> ■ Not secured [SBC legs negotiate only SRTP/MSRPS media lines and RTP/MSRP media lines are removed from the incoming SDP offer-answer] ■ Secured [SBC legs negotiate only RTP/MSRP media lines and SRTP/MSRPS media lines are removed from the incoming offer-answer] ■ As is (default) [No special handling for RTP/SRTP and MSRP/MSRPS is done] ■ Both [Each offer-answer is extended (if it isn't already) to two media lines - one RTP/MSRP

Parameter	Description
	<p>and the other SRTP/MSRPS]</p> <p>For more information, see the device <i>User's Manual</i> available from AudioCodes.</p>
Remote 3xx Mode	<p>Select either:</p> <ul style="list-style-type: none"> ■ Handle Locally [The device handles SIP 3xx responses on behalf of the dialog-initiating UA and retries the request (e.g., INVITE) using one or more alternative URIs included in the 3xx response. The device sends the new request to the alternative destination according to the IP-to-IP Routing table (the 'Call Trigger' field must be set to 3xx).] ■ Local Host [The device changes the host part of the Contact header in the 3xx response before forwarding the 3xx response to the dialog-initiating UA. If the 'Local Host Name' parameter of the IP Group of the dialoginitiating UA is configured with a non-empty value, the device changes the host part of the Contact header to this value. If the 'Local Host Name' is empty, the device changes the host part to the device's IP address (the same IP address used in the SIP Via and Contact headers of messages sent to the IP Group).] ■ IP Group Name [If the 'SIP Group Name' parameter of the IP Group of the dialog-initiating UA is configured with a non-empty value, the device changes the host part of the Contact header in the 3xx response to this value, before forwarding the 3xx response to the dialog-initiating UA.] ■ Database URL [The device changes the Contact header so that the re-route request is sent through the device. The device changes the URI in the Contact header of the received SIP 3xx response to its own URI and adds a special user prefix ("T~&R_"), which is then sent to the FEU. The FEU then sends a new INVITE to the device, which the device

Parameter	Description
	<p>then sends to the correct destination.]</p> <ul style="list-style-type: none"> ■ Transparent (default) [The device forwards the received SIP 3xx response as is, without changing the Contact header (i.e., transparent handling)] <p>For more information, see the device <i>User's Manual</i> available from AudioCodes.</p>
Remote REFER Mode	<p>Select either:</p> <ul style="list-style-type: none"> ■ Handle Locally (default) [Handles the incoming REFER request itself without forwarding the REFER. The device generates a new INVITE to the alternative destination (transfer target) according to the rules in the IP-to-IP Routing table (the 'Call Trigger' parameter must be set to REFER).] ■ Local Host [In the REFER message received from the transferor, the device replaces the Refer-To header value (URL) with the IP address of the device or with the 'Local Host Name' parameter value configured for the IP Group (transferee) to where the device forwards the REFER message. This ensures that the transferee sends the re-routed INVITE back to the device which then sends the call to the transfer target.] ■ IP Group Name [Changes the host part in the REFER message to the name configured for the IP Group (in the IP Groups table).] ■ Database URL [SIP Refer-To header value is changed so that the re-routed INVITE is sent through the device: <ul style="list-style-type: none"> ✓ Before forwarding the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T~&R_") to the Contact user part. ✓ The incoming INVITE is identified as a REFER-resultant INVITE according to this special prefix.

Parameter	Description
	<ul style="list-style-type: none"> ✓ The device replaces the host part in the Request- URI with the host from the REFER contact. The special prefix remains in the user part for regular classification, manipulation, and routing. The special prefix can also be used for specific routing rules for REFER-resultant INVITEs. ✓ The special prefix is removed before the resultant INVITE is sent to the destination ((transfer target).] ■ Keep URI (user@host) [The device forwards the REFER message without changing the URI (user@host) in the SIP Refer-To header. If you configure the 'Remote Replaces Mode' parameter (see below) to any value other than Keep as is, the device may modify the 'replaces' parameter of the Refer-To header to reflect the call identifiers of the leg. This applies to all types of call transfers (e.g., blind and attendant transfer).] ■ Regular [SIP Refer-To header value is unchanged and the device forwards the REFER message as is. However, if you configure the 'Remote Replaces Mode' parameter (see next) to any value other than (keep) As is, the device may modify the URI of the Refer-To header to reflect the call identifiers of the leg.] <p>For more information, see the device <i>User's Manual</i> available from AudioCodes.</p>
Remote Replaces Mode	<p>Select either:</p> <ul style="list-style-type: none"> ■ Standard (default) [The SIP UA supports INVITE messages containing Replaces headers. The device forwards the INVITE message containing the Replaces header to the SIP UA. The device may change the value of the Replaces header to reflect the call identifiers of the leg.]

Parameter	Description
	<ul style="list-style-type: none"> ■ Handle Locally [The SIP UA does not support INVITE messages containing Replaces headers. The device terminates the received INVITE containing the Replaces header and establishes a new call between the SIP UA and the new call party. It then disconnects the call with the initial call party, by sending it a SIP BYE request.] ■ As is [The SIP UA supports INVITE messages containing Replaces headers. The device forwards the Replaces header as is in incoming REFER and outgoing INVITE messages from/to the SIP UA (i.e., Replaces header's value is unchanged).] <p>For more information, see the device <i>User's Manual</i> available from AudioCodes.</p>
ICE Mode	<p>Enables Interactive Connectivity Establishment (ICE) Lite for the SIP UA associated with the IP Profile. ICE is a methodology for NAT traversal, employing the Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols to provide a peer with a public IP address and port that can be used to connect to a remote peer. For example, (ICE) Lite is required when the device operates in Microsoft Teams Direct Routing (media bypass) environments.</p> <p>Select either:</p> <ul style="list-style-type: none"> ■ Disable (default) ■ Lite <p>For more information, see the device <i>User's Manual</i> available from AudioCodes.</p>
SIP Update Support	<p>Select either:</p> <ul style="list-style-type: none"> ■ Supported Only After Connect [The UA supports receipt of UPDATE messages, but only after the call is connected.] ■ Not Supported [The UA doesn't support receipt of UPDATE messages.]

Parameter	Description
	<ul style="list-style-type: none"> ■ According Remote Allow [For refreshing the timer of currently active SIP sessions, the device sends session refreshes using SIP UPDATE messages only if the SIP Allow header in the last SIP message received from the user contains the value "UPDATE". If the Allow header does not contain the "UPDATE" value (or if the parameter is not configured to this option), the device uses INVITE messages for session refreshes.] ■ Supported (default) [The UA supports receipt of UPDATE messages during call setup and after call establishment.] <p>For more information, see the <i>SBC User's Manual</i> available from AudioCodes.</p>
Remote re-INVITE	<p>Defines if the SIP UA associated with this IP Profile supports receipt of SIP re-INVITE messages.</p> <p>Select either:</p> <ul style="list-style-type: none"> ■ Not Supported [The UA doesn't support receipt of re-INVITE messages. If the device receives a re-INVITE from another UA that is destined to this UA, the device "terminates" the re-INVITE and sends a SIP response to the UA that sent it, which can be a success or a failure, depending on whether the device can bridge the media between the UAs.] ■ Supported only with SDP [The UA supports receipt of re-INVITE messages, but only if they contain an SDP body. If the incoming re-INVITE from another UA doesn't contain SDP, the device creates and adds an SDP body to the re-INVITE that it forwards to the UA.] ■ Supported (default) [The UA supports receipt of re-INVITE messages with or without SDP.] <p>For more information, see the <i>SBC User's Manual</i> available from AudioCodes.</p>
Remote Delayed Offer Support	<p>Defines if the remote UA supports delayed offer (i.e., initial INVITE requests without an SDP</p>

Parameter	Description
	<p>offer).</p> <p>Select either:</p> <ul style="list-style-type: none"> ■ Not Supported ■ Supported (default) <p>For more information, see the <i>SBC User's Manual</i> available from AudioCodes.</p>
Remote Representation Mode	<p>Select either:</p> <ul style="list-style-type: none"> ■ According to Operation Mode (default) [Depends on the setting of the 'Operation Mode' parameter in the IP Groups or SRDs table: ✓ B2BUA: Device operates as if the parameter is set to Replace Contact. ✓ Call State-full Proxy: Device operates as if the parameter is set to Add Routing Headers.] ■ Replace Contact [The URI host part in the Contact header of the received message (from the other side) is replaced with the device's address or with the value of the 'SIP Group Name' parameter (configured in the IP Groups table) in the outgoing message sent to the SIP UA.] ■ Add Routing Headers [Device adds a Record-Route header for itself to outgoing messages (requests\responses) sent to the SIP UA in dialog-setup transactions. The Contact header remains unchanged.] ■ Transparent [Device doesn't change the Contact header and doesn't add a Record-Route header for itself. Instead, it relies on its' own inherent mechanism to remain in the route of future requests in the dialog (for example, relying on the way the endpoints are set up or on TLS as the transport type).] <p>For more information, see the <i>SBC User's Manual</i> available from AudioCodes.</p>

Parameter	Description
Remote Hold Format	<p>Defines the format of the SDP in the SIP re-INVITE (or UPDATE) for call hold that the device sends to the held party.</p> <p>Select either:</p> <ul style="list-style-type: none"> ■ Hold and Retrieve Not Supported [This option can be used when the remote side does not support call hold and retrieve (resume). The device terminates call hold and call retrieve requests received on the leg interfacing with the initiator of the call hold/retrieve, and replies to this initiator with a SIP 200 OK response. Therefore, the device does not forward call hold and/or retrieve requests to the remote side.] ■ Inactive [Device sends SDP with 'a=inactive'] ■ Send Only [Device sends SDP with 'a=sendonly'] ■ Not Supported [This option can be used when the remote side does not support call hold. The device terminates call hold requests received on the leg interfacing with the initiator of the call hold, and replies to this initiator with a SIP 200 OK response. However, call retrieve (resume) requests received from the initiator are forwarded to the remote side. The device can play a held tone to the held party if the 'Play Held Tone' parameter is set to Internal.] ■ Inactive Zero IP [Device sends SDP with 'a=inactive' and 'c=0.0.0.0'.] ■ Send Only Zero IP [Device sends SDP with 'a=sendonly' and 'c=0.0.0.0'] ■ Transparent (default) [Device forwards SDP as is] <p>For more information, see the device <i>User's Manual</i> available from AudioCodes.</p>

4. Click **OK**.



- The new IP Profile is synchronized with all nodes in the deployment.
- Operators can use the IP Profile to define connections in the ARM (see [Configuring a Microsoft Teams LMO Topology](#) on page 82).

Customers Page

The ARM supports a hosted Teams multi-tenant Direct Routing solution (ARM 'customer' entity feature). Microsoft Teams Hosters that implement the Microsoft recommended Super Trunk deployment model for multi-tenancy can use this feature and have each tenant represented by an ARM 'customer' entity. All 'customer' entities can traverse the same Peer Connection/VoIP Peer (SBC IP Group) on the AudioCodes Direct Routing SBC.

The logical entity 'customer' (Teams tenant) can be defined uniquely by either Prefix Groups or by a special tag assigned to a call, in the Policy Studio (Policy Studio Tag) if the operator wants to manage 'customer' entity DIDs in the Users page and use the Policy Studio and other ARM users' capabilities. In this way, the 'customer' entity's DIDs can be managed in both the Prefix Group or the ARM Users page (a combination of the two is also allowed).

The ARM also supports statistics and alarms related to the 'customer' entity.

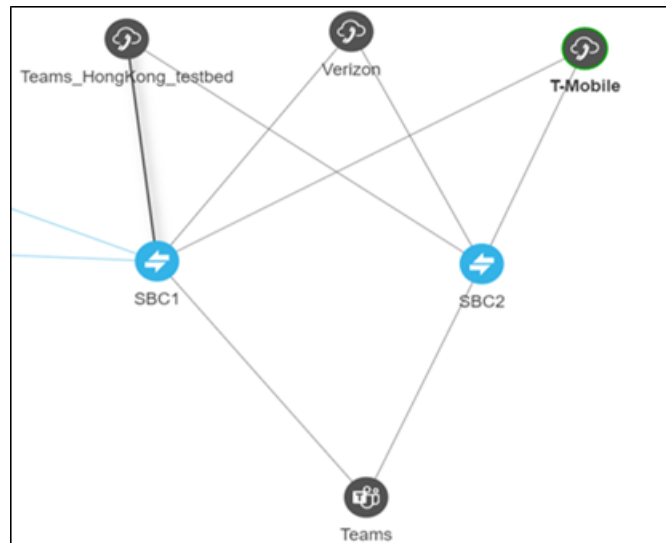
ARM Routing capabilities support the 'customer' entity as a routing condition (specific 'customer' entities or all 'customer' entities). This also includes SIP header manipulations, required by Teams multi-tenancy, that can now easily be performed by the ARM (SIP 'Contact' header).

In addition, the ARM provides CAC capabilities for each Teams tenant. Since a Super Trunk (single IP Group for Teams) is provisioned on the SBC, individual CAC Profiles can't be applied in the SBC for each individual tenant that shares the Super Trunk. The ARM supports this capability by applying and performing CAC for each tenant that shares the same Super Trunk (Peer Connection/VoIP Peer/IP Group). This includes the following CAC capabilities:

- Capability to define ingress CAC for logical customers under a VoIP Peer
- Capability to define egress CAC for logical customers under a VoIP Peer
- Capability to define CAC applicable for both directions

The following network diagram demonstrates this feature's most common use case:

Figure 2-41: CAC Capabilities - Use Case



- Multiple 'customer' entities (Teams tenants) can share the same ARM Peer Connection for Teams access (northbound).
- Operators can share the same Service Providers/PSTN SIP trunks for multiple 'customer' entities (southbound).



Note that for redundancy purposes, multiple SBCs can be used leading to the same VoIP Peers, with local Peer Connections (IP Groups) on each SBC.

- Connectivity to Microsoft using a 'derived trunk' setup.
 - A derived trunk can be considered a Super Trunk using only one (1) IP Group on each SBC (ARM Peer Connection).
 - Each unique 'customer' entity / Teams tenant making outbound calls can be identified by the FQDN in the 'Contact' or 'From' header, or by its DID.
 - Inbound calls from SIP trunks to the Teams 'customer' entity can be identified and associated with a specific 'customer' entity / Teams tenant by the destination DID (which can be managed either in the ARM Users page or by the Prefix Group).
 - This type of trunk eliminates the need for each 'customer' entity to have its own IP Group/Peer Connection with Sip:options requesting health checks.
 - Using the ARM for routing allows a very high number of 'customer' entities to be supported (as it becomes a logical entity).

Viewing the Customers Page

The Customers page (**Network > Customer**) provides operators the capability to view all provisioned 'customer' entities (Teams tenants) in a table (one row per 'customer' entity). In addition to the information configured per 'customer' entity (provided by the operator in the Add/Edit action), the following two columns are shown in the table for each 'customer' entity:

- **Admin State** - can be either Locked or Unlocked; reflects an operator's Lock/Unlock action applied to the 'customer' entity. The ARM rejects a calls routing request for a Locked 'customer' entity.
- **CAC State** - shown only for 'customer' entities with an attached CAC Profile. Reflects the CAC status of the 'customer' entity based on the current number of concurrent sessions of the 'customer' entity, related to the attached CAC profile. It can have one of the following values:
 - **Unblock** - the 'customer' entity didn't reach the allowed number of simultaneous sessions and calls to/from it.
 - **Block** - the 'customer' entity reached the maximum number of allowed simultaneous sessions defined in the attached CAC Profile and calls are currently blocked.
 - **Block Incoming** – the 'customer' entity reached the maximum number of incoming calls and only incoming calls are blocked.
 - **Block Outgoing** – the 'customer' entity reached the maximum number of outgoing calls defined in the attached CAC Profile and outgoing calls are currently blocked.

Figure 2-42: Customer Page Columns

NAME	CAC STATE	ADMIN STATE	PREFIX GROUPS	POLICY STUDIO TAG	SP HEADER NAME	SP HEADER VALUE	CAC PROFILE
customer1			HSLJapan		CONTACT_H05T	shin-audiocodes.com	cac_global
customer2				Version	CONTACT_H05T	cust2.com	cac_incomingfrom team...
customer3				T-Mobile	CONTACT_H05T	cust3.com	cac_subgongs team's cu...
customer4			p01		CONTACT_H05T	cust4.com	cac_global
customer5			p02		CONTACT_H05T	cust5.com	cac_incomingfrom team...
customer6			p03		CONTACT_H05T	cust6.com	cac_subgongs team's cu...
Cust_Temporary				Cust_Temp	CONTACT_H05T	cust_temp	

The 'Customers' page can tabulate thousands of entries; a smart search and filter engine in the uppermost right corner facilitates management. In addition to a string search, the following filters are supported:

Figure 2-43: Customer Page Filter

Q cacProfileId:2

Name:

CAC State:

Prefix Group:

Policy Studio Tag:

Administrative State:

SIP Header Name:

SIP Header Value:

CAC Profile:

For example, you can select one of the CAC Profiles and filter all ‘customer’ entities listed in the page using this specific profile. Alternatively, you can select a ‘customer’ entity in the Customers page filtered by Prefix Groups, etc.

Defining a 'Customer' Entity (Teams Tenant)

Operators can add a logical 'customer' entity (Teams tenant) to the ARM GUI in the Customers page. The page allows **Add**, **Edit**, **Delete**, **Lock/Unlock** and **Refresh** actions for each 'customer' entity.



Before implementing the feature, best practice is for operators to decide how to identify a 'customer' entity: using either Prefix Groups, or ARM Users. Note that a combination of the two is also supported, but may be less convenient.

For more information and a use-case for each 'customer' definition method (either with Prefix Group or with Users), see [Defining 'Customer' Entities using ARM Users & Policy Studio](#) on page 68.

➤ To add a new 'customer' entity':

1. Open the Customers page (**Network > Customers**).

Figure 2-44: Customers Page

NAME	CAC STATE	ADMIN STATE	PREFIX GROUPS	POLICY STUDIO TAG	SIP HEADER NAME	SIP HEADER VALUE	CAC PROFILE
Demo Customer1	✓	🔒	demo_prefix_1		CONTACT_HOST	audiocodes5.com	demo_outgoing_limit
Customer1/ResourceTest	✓	🔒	resource test prefix group 1		CONTACT_HOST	audiocodes.com	cac_profile
Customer2/ResourceTest		🔒	resource test prefix group 2		CONTACT_HOST	audiocodes.com	

2. Click **Add**.

Figure 2-45: Add Customer

ADD CUSTOMER

Name: *

Prefix Group:

Policy Studio Tag: *

SIP Header: * SIP Header Value

CAC Profile:

OK **Cancel**

3. Configure using the following table as reference.

Table 2-6: Add Customer Parameters

Parameter	Description
Name	Mandatory. Unique name of the 'customer' entity. Configure an intuitive name to facilitate effective management later.
Prefix Group	Used if the operator chooses to identify a 'customer' entity with Prefix Groups. The operator can select a Prefix Group or several Prefix Groups previously defined (Settings > Call Flow > Prefix Group). Multiple Prefix Groups are treated as 'or' in terms of 'customer' entity definition (DIDs and ranges from all the selected Prefix Groups are considered to belong to the 'customer' entity). A Prefix Group can include not only full DIDs but also ranges. Note that the same Prefix Group cannot be used for several 'customer' entities as it uniquely identifies 'customer' entity DIDs. However, the ARM does not prevent a collision between the ranges of Prefix Groups; it's the operator's responsibility to prevent a collision of ranges between 'customer' entities.
Policy Studio Tag	Used if the operator chooses to manage 'customer' DIDs in the ARM Users page and thereby benefit from ARM Users capabilities (such as Policy Studio with pre-routing manipulations or Users Groups). The Policy Studio Tag should be provided in the Policy Studio (for incoming and outgoing calls) and is used by the ARM mainly for CAC counting and enforcement for specific 'customer' entities / Teams tenants. The extension for this Tag in a Policy Studio action is described under Customers Page on page 61.
SIP header	Each unique 'customer'/Teams tenant making outbound calls is identified/marked by Teams with the FQDN in the 'Contact' or 'From' header. A call in the direction 'to Teams' should have this 'Contact' header identification as well. From Teams' perspective, this is the way to identify and distinguish between 'customer' entities /

Parameter	Description
	<p>tenants. The ARM provides an easy way to put the predefined string (the one used by Teams to identify a tenant) in the 'Contact' header for calls toward Teams (for more information about this option, see under Customers Page on page 61. The SIP header attribute allows the operator to provide a string to be used for the 'Contact' header. Note that it should be coordinated with the Teams settings for the ARM 'customer' entity / Teams tenant.</p>
CAC profile	<p>Can optionally be attached per 'customer' entity. For a description of a CAC profile and its capabilities, see CAC Profiles on page 251). The operator can attach a CAC profile to a 'customer' entity with both directions or a one-direction sessions limitation (defined under Settings > Routing > CAC profiles). Operators can reuse the same CAC Profile for multiple 'customer' entities.</p> <div data-bbox="810 1016 1402 1402"> </div> <div data-bbox="802 1435 1394 1821"> </div>

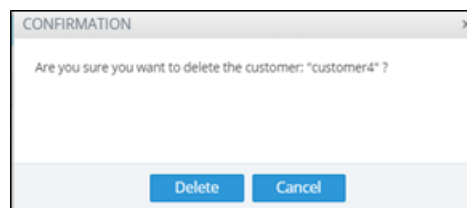
Editing a 'Customer' Entity

The option to **Edit** a 'customer' entity allows the operator to change all the attributes provided in the **Add customer** action (including 'Name').

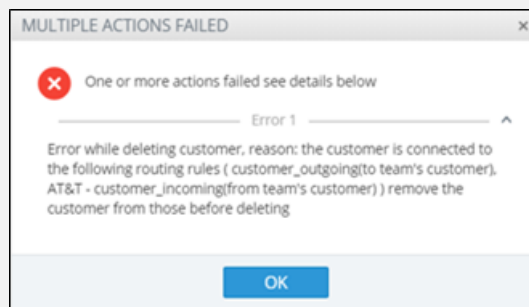
If during **Edit** the operator updates the 'customer' entity's CAC profile (or adds a CAC profile), the ARM verifies if the 'customer' entity should be blocked / unblocked due to the change (from the CAC's perspective).

Deleting a 'Customer' Entity

The action Delete a 'customer' entity should be used to delete an 'existing' 'customer' entity. The operator is asked for confirmation before the delete action:



If a 'customer' entity explicitly appears in a Routing Rules condition, the ARM does not allow deleting it until it is removed:



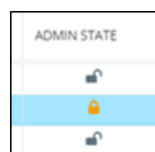
Locking-Unlocking a 'Customer' Entity

This action allows operators to manually Lock or Unlock a specific 'customer' entity for maintenance due to administrative reasons. It blocks incoming and outgoing calls associated with the locked 'customer' entity.



When a Lock action is applied to the 'customer' entity, the ARM does not allow any calls to/from the 'customer' entity (tenant).

The Lock/Unlock action is reflected in the 'customer' entity's Admin state:



Defining 'Customer' Entities using ARM Users & Policy Studio

It's typically easiest to define a 'customer' entity (Teams tenant) in the ARM using a Prefix Group (or multiple Prefix Groups) though some deployments sometimes require (for example) smart DID manipulation or replacement, in which case the Users page (**Users > Users**) or Users Groups page (**Users > Users Groups**) must be used to define DIDs of 'customer' entities.

Figure 2-46: Users page to define DIDs of 'customer' entities

USERS

REGISTERED USERS

USERS GROUPS

SERVICES

FILE REPOSITORY

PROPERTY DICTIONARY

Add

Edit

Delete

Total Users Count

Export

Refresh

NAME	ORIGIN	COUNTRY	OFFICE PHONE	DISPLAY NAME	DEPARTMENT	MS LYNC LINE URI	TENANT
hongkonglyong	ARM		34697577				
lyong	ARM	HongKong	+85234697577			+85297282142	hongkong.audiocodes...
japanilyong	ARM	japan	+815034697577			+81279998800	
User01	users	Canada	1101	User1	AT&T	110	AT&T
User02	users	Canada	1102	User2	AT&T	120	AT&T
User03	users	Canada	1201	User3	AT&T	130	AT&T
User04	users	Canada	1202	User4	AT&T	140	AT&T
User05	users	Canada	1301	User5	Verizon	150	Verizon
User06	users	USA	1302	User6	Verizon	160	Verizon
User07	users	USA	1401	User7	Verizon	170	Verizon
User08	users	USA	1402	User8	Verizon	180	Verizon
User09	users	USA	1501	User9	T-Mobile	190	T-Mobile
User10	users	USA	1502	User10	T-Mobile	200	T-Mobile
User11	users	USA	1601	User11	T-Mobile	210	T-Mobile

An example of a deployment like this is routing based on groups of users as destination. Operators can have cross-tenant (cross-'customer' entities) users who're allowed to dial to specific destinations (specific countries), or long distance. These users can have a property in the Users page which will allow composing a Users Group of 'Allowed for long distance'.

Another use-case for defining a 'customer' entity DID in the Users page is use of short dial within the same 'customer' entity. Microsoft Teams does not support short dial but the functionality can nevertheless be implemented in the ARM. In this case, the Users Dictionary should include 'Full number' and 'short number' properties, which can be manipulated / substituted using Policy Studio. Operators using the Users page to define a 'customer' entity DID must have a Users property identifying the 'customer' entity in the Users Property Dictionary.



- AudioCodes recommends using Policy Studio for 'customer' entity tagging.
- If 'customer' entity DIDs are defined in the ARM's Users page, a *range* of DIDs to be associated with these 'customer' entities cannot be defined.

Viewing Network Summary Panes

Network Summary panes viewed in the right margin of the Network Map page can inform you how to optimize call routing in the network. You can choose to display:

- Overall Network Statistics - statistics related to the *entire network* are displayed by default; no entity in the Network Map is selected. See [Overall Network Statistics](#) on the next page.
- Statistics on a network entity – select the network entity in the Network Map for which to display statistics. See [Statistics on a Selected Entity](#) on page 72.

Overall Network Statistics

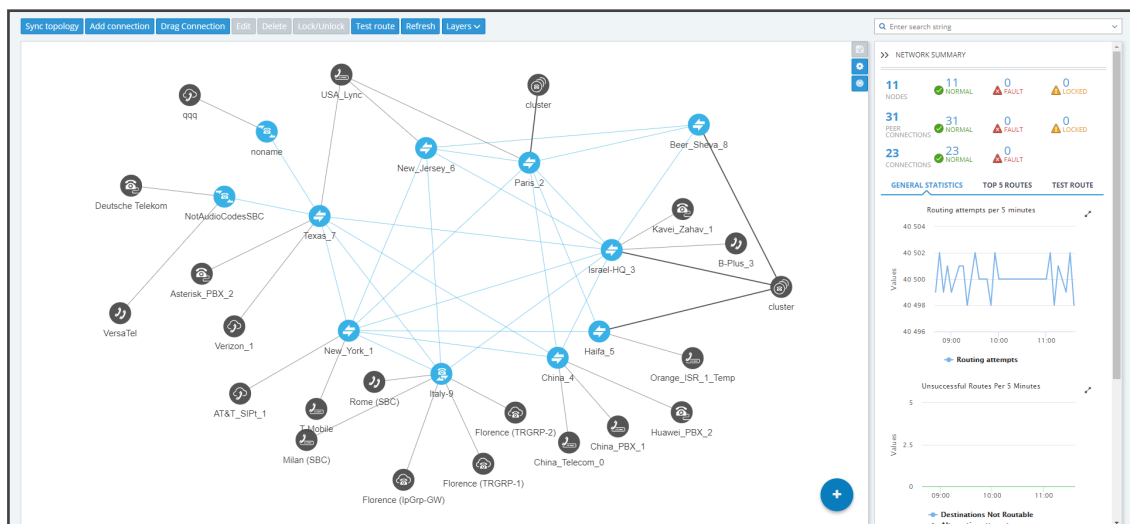
Statistics related to the entire network are by default displayed. No entity in the Network Map is selected. This pane displays four sections:

- Network Summary (see below)
- General Statistics (see [General Statistics](#) on the next page)
- Top 5 Routes (see [Top 5 Routes Pane](#) on page 71)
- Test Route (see [Test Route](#) on page 72)

Network Summary

The Network Summary pane displays routing statistics and availability network statuses which help operators optimize routing in their telephony networks, reducing unnecessary consumption of resources and decreasing expenses.

Figure 2-47: Network Summary



The pane displays:

- Network Entities Statuses (left to right):
 - The total number of nodes/Peer Connections/Connections in the network
 - The number of nodes/Peer Connections/Connections that are unlocked and available, i.e., 'normal'
 - The number of nodes//Peer Connections/Connections that are 'fault', i.e., unavailable
 - The number of nodes/Peer Connections that are 'locked' (Connections cannot be locked/unlocked)

When **Quality Layer** is selected, the 'Faulty' counters for Peer Connections and Connections can change. All **red** (bad), **orange** (fair) or **unknown** Connections / Peer Connections are considered 'Faulty' because they less than perfect.

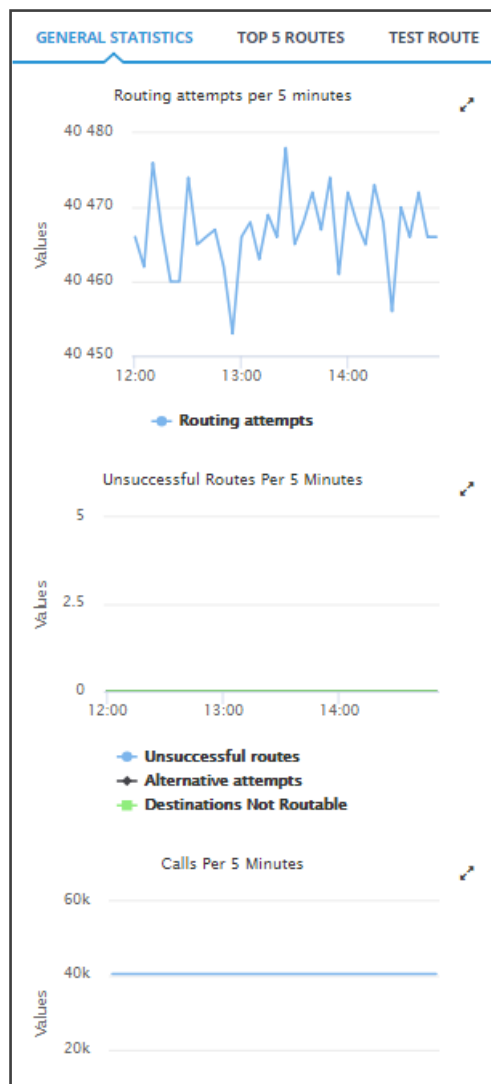
General Statistics

You can display statistics related to the entire network.

➤ To display statistics related to the entire network:

- Open the ARM's Network Map and in the Network Summary window, click the **General Statistics** tab if it isn't activated already.

Figure 2-48: General Statistics Pane



Three graphs are displayed (top to bottom):

- The number of routing attempts made in the entire network every five minutes
- The number of unsuccessful routes made every five minutes, including the number of alternative attempts and the number of unrouteable destinations
- The number of calls made every five minutes, including the number of destination calls and the number of transient calls.

➤ **To facilitate your analysis:**

- Click the expand icon next to any of the three graphs to project a zoomed-in graph to the front.

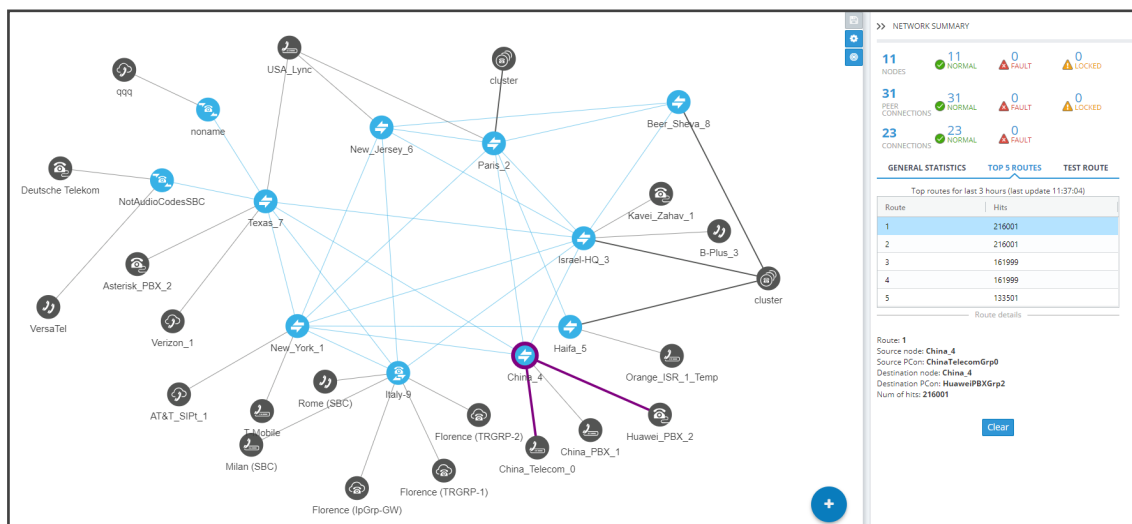
Figure 2-49: Projecting a Zoomed-in Graph to the Front



Top 5 Routes Pane

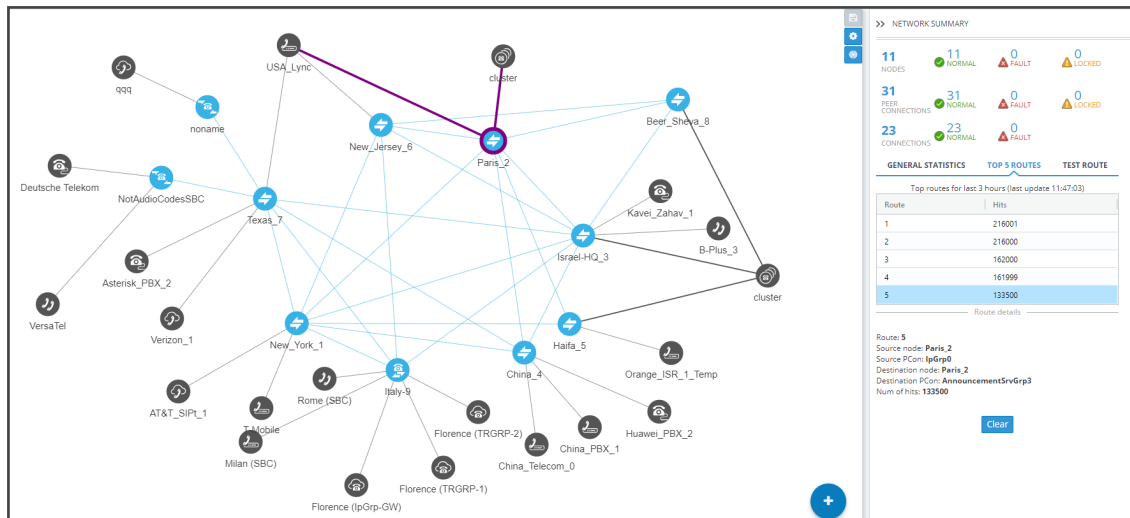
The Top 5 Routes pane under the **Top 5 Routes** tab in the Network Summary pane gives operators visibility into the routes most frequently used over the last three hours.

Figure 2-50: Top 5 Routes



Select a route to display its details. In the preceding figure, Route 1 is selected by default after opening the **Top 5 Routes** tab. In the figure following, Route 5 is selected. Details displayed include Source Node / Peer Connection and Destination Node / Peer Connection.

Figure 2-51: Top 5 Routes – Details of Route 5



Selecting Route 1-5 (one of the top five routes) visualizes the path in **bold purple** in the Network Map as shown in the preceding two figures.

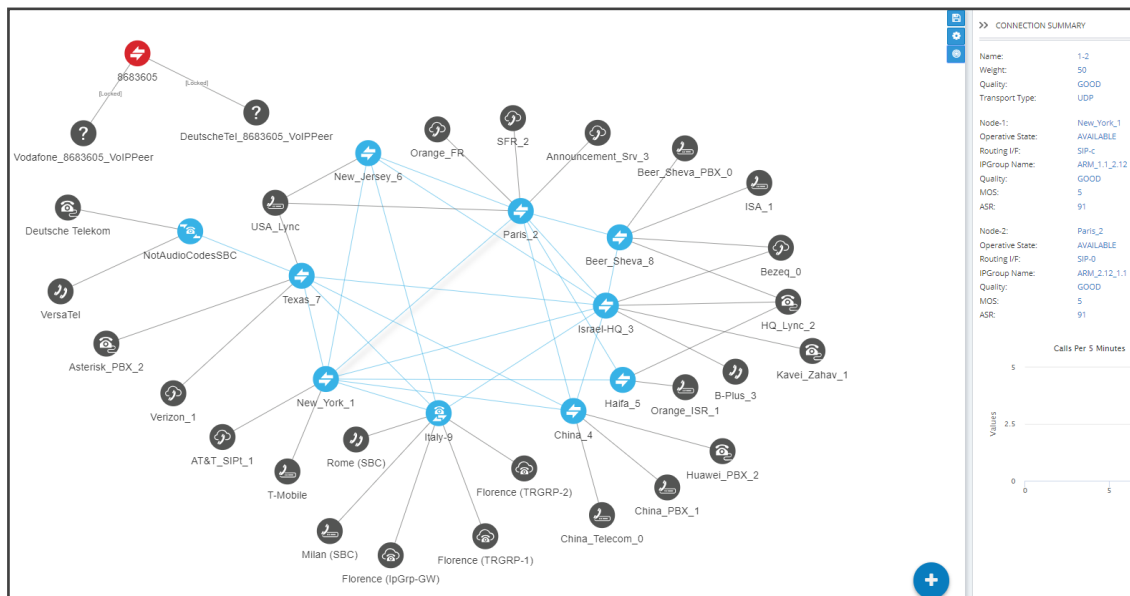
Test Route

See [Testing a Route](#) on page 87 for detailed information.

Statistics on a Selected Entity

When you select one of the entities in the map, the Network Summary window displays statistics related to that selected entity.

Figure 2-52: Summary Pane Displaying Information Related to a Selected Entity - Connection





In the figure above, the entity selected, i.e., the connection between **Paris_2** and **New_York_1**, is shaded. Information about it is displayed in the Summary pane on the right side of the page.

3 Defining a Network Topology

Part of the ARM's network topology is automatically discovered and added to the ARM's Network Map.

Other entities must be provisioned by you.



When defining network topology, for example, when adding a node:

- mandatory fields are marked with an asterix *
- an edited field or a field currently being edited is highlighted yellow
- a field with missing or incomplete information is outlined red

Adding an AudioCodes Node to the ARM

AudioCodes nodes (SBCs and gateways) are automatically detected and displayed in the ARM's Network Map, allowing you to begin configuring actions immediately after auto-detection. However, to prevent potential provisioning mistakes at the Node (SBC or Gateway) level, it's preferable to add Nodes to the ARM from the ARM Network Map page.

When a new node is added either by auto-detection or manually to the ARM, the ARM automatically detects Peer Connections and Routing interfaces associated with the node.

➤ To manually add a node to the ARM:

1. Click the  icon and then drag and drop the AudioCodes node into the Network Map.

Figure 3-1: Add Node

2. In the Add Node screen, provide a name, IP address or Hostname (FQDN), and protocol. The option to use Hostname (FQDN) rather than a hard-coded IP address gives you added flexibility when designing your telephony network.
3. From the 'Routing server group' drop-down, select a Routing Server Group (for more information, see [Adding a Routing Servers Group with Internal and External Priorities](#)).

4. Hostname (FQDN) can be configured for an existing node in the node's Web interface, Network Settings page. The page is opened by right-clicking the node in the ARM's Network Map page to log in, selecting the **IP Network** menu, opening the **Advanced** tab and then selecting the **Network Settings** tab.



When operating in Microsoft Azure with HA systems (SBC Active and Redundant), set the hostname IP / FQDN as it is configured in Azure for the LB (Load Balancer); the device-pair will share the same hostname.

Figure 3-2: Node's Web Interface - Network Settings Page – Host Name (FQDN)

This triggers a new login message from the node to the ARM; the ARM consequently updates the address to the newly added Hostname (FQDN). If the ARM detects a node configured with both Hostname (FQDN) and IP address, Hostname (FQDN) is used. You can change Hostname (FQDN) or IP address. The ARM displays the device's address, i.e., Hostname (FQDN) if it exists, or IP address (if Hostname (FQDN) doesn't exist).

5. View the added AudioCodes node in the Topology Map; all elements associated with the node are automatically provisioned and displayed in the Network Map.

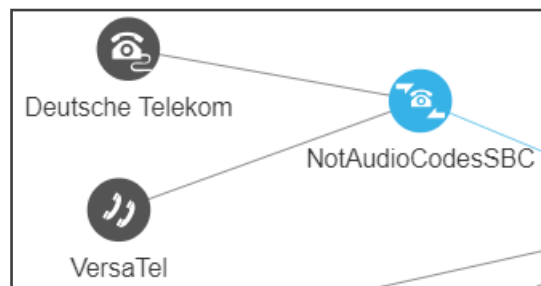


- Peer Connections are displayed in Locked state; you need to perform an unlock for them to provide a service.
- Node provisioning by auto-detection is described in [Migrating Device Routing to the ARM](#) on page 319.



Adding a Third-Party Node to the ARM

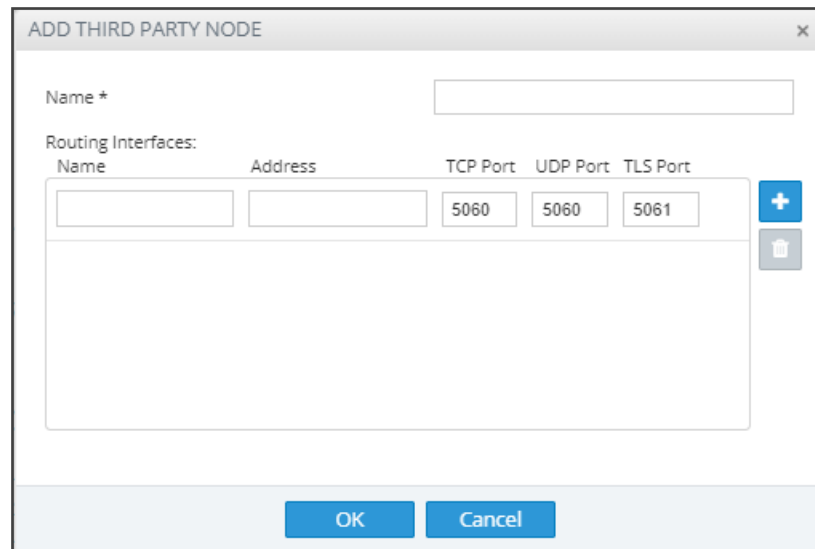
The ARM allows you to add third-party non-AudioCodes nodes (SBCs and Media Gateways) to the Network Map so that the ARM can be used for call routing in heterogeneous environments with a mix of AudioCodes and non-AudioCodes nodes as part of your network.

Figure 3-3: Third-Party Device Added to the Network Map



➤ **To add a third-party node:**

1. In the Network Map page, click the  icon located in the lowermost right corner and then drag and drop the third-party node icon  into the Network Map.



ADD THIRD PARTY NODE				
Name *				
Routing Interfaces:				
Name	Address	TCP Port	UDP Port	TLS Port
		5060	5060	5061

2. Provide the third-party node's properties. The third-party device's remote IP address is used as the destination address of the connection from the AudioCodes device.
3. Click **OK** and then add a VoIP Peer as shown in [Adding a VoIP Peer](#) below.

Adding a VoIP Peer

After adding a third-party non-AudioCodes node (SBC or Media Gateway) to the ARM Network Map as shown in [Adding a Third-Party Node to the ARM](#) on the previous page, add a VoIP Peer.

➤ **To add a VoIP Peer:**



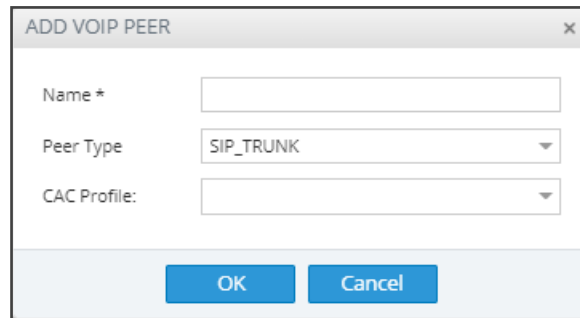
1. Click the  icon and then click the  icon

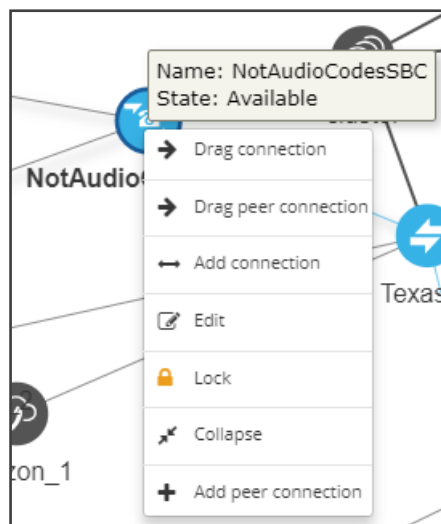
Figure 3-4: Adding a VoIP Peer



2. From the VoIP Peer types displayed, drag the VoIP Peer type you require, e.g., IP PBX or SIP Trunk (you can determine the type from the tooltip displayed when pointing your cursor over it), and then drop it in the Network Map. Use the preceding and following figure as references.

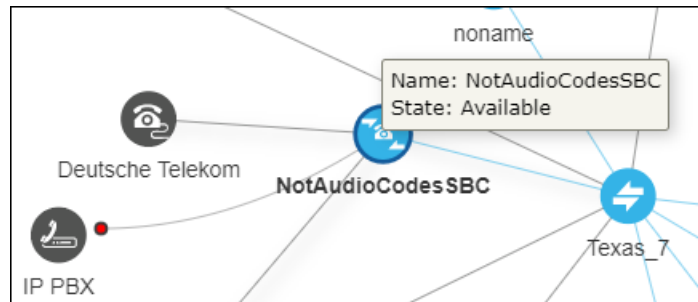
Figure 3-5: Adding a VoIP Peer

3. In the 'Add VoIP Peer' screen that opens, give the VoIP Peer a name.
4. From the CAC Profile drop-down, select a profile. For information about CAC Profiles, see under [CAC Profiles](#) on page 251
5. Click **OK**.
6. Associate the VoIP Peer with the third-party non-AudioCodes node: Right-click the node and from the pop-up menu select the action **Drag peer connection**.

Figure 3-6: Drag peer connection

The action 'Drag peer connection' is available only to third-party non-AudioCodes SBCs or Media Gateways. It's not applicable to AudioCodes SBCs or AudioCodes Media Gateways.

7. From the third-party non AudioCodes node, drag your mouse towards the VoIP Peer as shown here:

Figure 3-7: Drag from the Third-Party Node to the VoIP Peer to Create a Peer Connection**Figure 3-8: Add Virtual Peer Connection**

The screenshot shows the 'ADD VIRTUAL PEER CONNECTION' dialog box. The 'Type' is set to 'Virtual'. The 'Name' and 'TGRP' fields are empty. The 'Weight' is set to 50. The 'Node' is 'NotAudioCodesSBC' and the 'Voip Peer' is 'IP PBX'. The dialog box has 'OK' and 'Cancel' buttons at the bottom.

8. In the Add Virtual Peer Connection screen that opens (shown in the preceding figure), connect the third-party node to the ARM topology - to an AudioCodes node or to a SIP module - for end-to-end routing capabilities.



The ARM uses standard SIP TGRP capabilities to communicate with a third-party device interface that does not support AudioCodes nodes' REST API, so when adding a Peer Connection to a third-party device, you're prompted to provide TGRP. The TGRP must match the configuration in the third-party device. When the ARM chooses to route a call towards a specific Peer Connection of the third-party device, it installs into the SIP Invite the TGRP name configured in the ARM.

The ARM will then perform routing to Peer Connections attached to third-party nodes. In Routing Rules, choose the Peer Connection or VoIP Peer associated with the third-party node and in this way, achieve end-to-end routing in a heterogeneous network.

Attaching a CAC Profile to a Peer Connection

A CAC Profile can be attached to a Peer Connection. The same CAC Profile can be reused for multiple Peer Connections.

➤ **To attach a CAC Profile to a specific Peer Connection:**

1. From the Network Map page or from the Peer Connections page, Select and **Edit** a specific Peer Connection.

Figure 3-9: Edit Peer Connection

The 'EDIT PEER CONNECTION' dialog box contains the following fields and sections:

- Type:** (Label)
- Name:** * (Text input field with value 'IpGrp1')
- Weight:** (Text input field with value '50')
- Node:** (Text input field with value '172.17.133.31-2')
- Voip Peer:** (Dropdown menu with value '2_1')
- Normalization Before Routing:**
 - Source URI User:** (Dropdown menu)
 - Destination URI User:** (Dropdown menu)
- Advance Conditions:**
 - Calls quota:** (Text input field with value 'manual_test' and a multiplier 'x')
 - CAC Profile:** (Dropdown menu)
 - Quality Definitions:**
 - ☒ use global quality definitions
 - ☐ use specific quality definitions
 - ☐ MOS
 - ☒ ASR
- Buttons:** OK, Cancel

2. From the 'CAC Profile' drop-down, select one of the previously defined CAC profiles.
3. In the Peer Connections page (**Network > Peer Connections**), the CAC Profile is shown in the 'CAC Profile' column.

Figure 3-10: Peer Connections Page - CAC Profile Column

STATUS	NODE	NAME	VOIP PEER	IP GROUP	OPERATIVE STATE	ADMINISTRATIVE STATE	QUALITY	CALLS QUOTA	CAC PROFILE
✓	172.17...	IpGrp0	1,0	IpGrp0	✓	🔊	UNKNOWN		
✓	172.17...	IpGrp1	1,1	IpGrp1	✓	🔊	UNKNOWN		
✓	172.17...	*1819741250235	2,0	IpGrp0	✓	🔊	UNKNOWN		
⚠	172.17...	IpGrp1	2,1	IpGrp1	✓	🔊	UNKNOWN	manual_test	cac_profile
✗	172.17...	*1819942622927	1,2	IpGrp2	✗	🔊	UNKNOWN		

4. In the Peer Connections page, (optionally) filter all Peer Connections using the same CAC Profile.

Figure 3-11: Peer Connections Page - Filter

Q Enter search string

Free Text:

Operative State:

Administrative State:

Quality:

Calls Quota:

CAC Profile:

- cac1
- test1
- cac_profile_total_limit_name
- cac_profile_outgoing_limit_name
- demo_outgoing_limit
- cac_profile**
- vpeer_total_limit

MOS:

ASR:

5. In the Peer Connections page, select a Peer Connection with an attached CAC Profile; information about the status of the CAC is displayed.

Figure 3-12: Peer Connections Page - Summary Pane Showing CAC Information

>> PEER CONNECTIONS SUMMARY

Name: IpGrp1

Administrative State: Locked

Operative State: AVAILABLE

IPGroup Name: IpGrp1

Weight: 50

Node name: 172.17.133.31-2

Peer connection type: IPGroup

Quality: UNKNOWN

MOS: UNKNOWN

ASR: UNKNOWN

Calls quota:

Quota name: manual_test

Calls duration (minutes): 0

Outgoing calls: ✓

Warning threshold reached: No

Quota reached: No

CAC Profile: cac_profile

CAC State: UNBLOCK

Attaching a CAC Profile to a VoIP Peer

A CAC Profile can be attached to a VoIP Peer. The same CAC Profile can be reused for multiple topology elements. When attaching a CAC Profile to a VoIP Peer, the ARM counts all sessions of all Peer Connections connected to the VoIP Peer for both incoming and outgoing.

➤ To attach a CAC profile to a VoIP Peer:

1. From the Network Topology Map page or from the VoIP Peers page, select and **Edit** the VoIP Peer.

Figure 3-13: Edit VoIP Peer

2. From the 'CAC Profile' drop-down, select one of the previously defined profiles.
3. In the VoIP Peers page (**Network > VoIP Peers**), view the CAC Profile in the 'CAC Profile' column.

Figure 3-14: VoIP Peers Page - CAC Column

NAME	TYPE	CAC PROFILE	CAC STATE	PEER CONNECTIONS
1_0	TEAMS	cac_profile	UNBLOCK	ipGryd172.17.133.30-1)
1_1	IP_PBX			ipGryd172.17.133.30-1)

4. In the VoIP Peers page, you can (optionally) filter all VoIP Peers using the same CAC Profile.

Figure 3-15: VoIP Peers Page - Search Filter

The ARM generates VoIP Peer CAC Threshold alarms when specified thresholds are crossed. The following severities are supported for CAC Profile related alarms:

Warning – generated for VoIP Peers when the number of sessions reaches the threshold limit (as a percentage) defined in **Settings > Routing > CAC Profiles**.

Critical – generated when the number of sessions reaches the defined session limit.

Clear – generated to clear 'set' alarms when the number of sessions drops under the defined limit or when the CAC Profile is detached.

Using the Nodes Page

The ARM supports a Nodes page (**Network > Nodes**), shown in the next figure, to facilitate more convenient management of high numbers of SBCs | Media Gateways for operators.

Figure 3-16: Nodes page

Sync Node Edit Delete Lock/Unlock Configure Refresh								Q Enter search string
NAME	ADMIN ST...	OPERATIVE...	ADDRESS	SERIAL	SECONDARY SERIAL	SOFTWARE VERSION	PRODUCT TYPE	» NODES SUMMARY
New_York_1			sbcc21.corp.audiocodes.com	146780998695094		7.40A.100.237	SBC	Name: Paris_2
Paris_2			172.17.133.22	255137933019404	16074427	7.40A.100.237	SBC	Teams Role: NOT_TEAMS
Israel-HQ_3			172.17.133.23	141540263879099	194495	7.40A.100.237	SBC	Address: 172.17.133.22
China_4			172.17.133.24	242967268910718	16496495	7.40A.100.237	SBC	Device type: Mediant VE SBC
Hiafa_5			172.17.133.25	21094177800600	2254579	7.40A.100.237	SBC	Product type: SBC
New_Jersey_6			172.17.133.26	246131846699631	5543519	7.40A.100.237	SBC	Software version: 7.40A.100.237
Texas_7			172.17.133.27	44531905846586	445746	7.40A.100.237	SBC	Primary serial: 255137933019404
Beer_Sheva_8			172.17.133.28	228599323948506	6918859	7.40A.100.237	SBC	Secondary serial: 16074427
133.145-13			172.17.133.145	3960763		7.40A.100.237	SBC	Administrative State: UNLOCKED
133.144-12			172.17.133.144	3845684		7.40A.100.114	HYBRID	Operative State: Available v
133.143-11			172.17.133.143	8117390		7.40A.100.237	SBC	
133.142-10			172.17.133.142	4965624		7.40A.100.237	SBC	

Up to 150 Session Border Controllers (SBCs) and/or Media Gateways are supported in ARM Topology and Routing, necessitated by product popularity and extensive global deployments. Some distributed enterprises with multiple branches have required more than 100 nodes to be supported in their deployments.

The page allows operators to perform the same actions for nodes as those in the Network Map page, but in table view / format, viz., **Sync Node**, **Edit**, **Delete**, **Lock / Unlock** and **Configure**.

Selecting a node in the page allows operators to view a 'Node Summary' pane on the right side of the page.

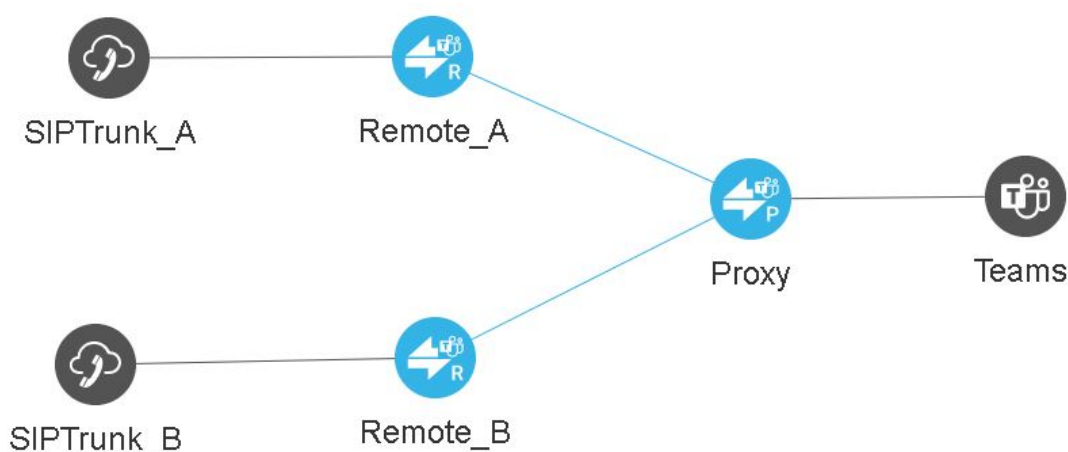
Configuring a Microsoft Teams LMO Topology

Microsoft Teams Local Media Optimization (LMO) is an important feature for enterprise telephone networks seeking to utilize Microsoft Cloud. For detailed information about LMO, see <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-media-optimization>.

Two node roles feature in the topology:

- **Teams Proxy** [The SBC connected directly to the Teams Cloud]
- **Teams Remote** [The SBC connected to the Proxy]

Figure 3-17: Typical Microsoft Teams LMO Topology



➤ **To configure a Microsoft Teams LMO topology:**

1. When defining the connection between the Proxy and the Remote, configure each side to support LMO by predefining the default values for IP Profiles (see [IP Profiles Page](#) on page 52) and the connection itself (IP Group); mandatory fields are indicated with an asterisk *; fields that can be left undefined are not indicated with an asterisk.
2. After selecting the node per Teams role, define a connection between them (by clicking **Drag Connection** and then dragging a line or by clicking **Add connection** and defining a line); when the ARM detects that the connection is between Remote and Proxy, fields will be predefined with correct defaults. For example:

Figure 3-18: Remote-Proxy connection

The screenshot shows the 'EDIT CONNECTION' dialog box. It contains the following fields and settings:

- Name:** * remote_proxy_con
- Weight:** 50
- Transport Type:** TCP
- Node 1:** Remote
 - Routing Interface:** * ProxySBC
 - Name:** * ARM_Con_to_Proxy
 - Ip Profile:** * ARM_IP_Profile_Remote_To_Proxy
 - Media realm:** ProxySBC
- Node 2:** Proxy
 - Routing Interface:** * SitesSIPInterface
 - Name:** * ARM_Con_to_Remote
 - Ip Profile:** * ARM_IP_Profile_Proxy_To_Remote
 - Media realm:** MRLan
- SIP Group name:** * mosbc.audicodes.com
- Advanced Conditions:**
 - ☒ Keep connection properties synchronized

Buttons: OK, Cancel



- Media Realms are synchronized from each node (the ARM Configurator determines Media Realms that are selected as used by the Routing Server).
- IP Profiles are configured in the ARM (see [IP Profiles Page](#) on page 52).

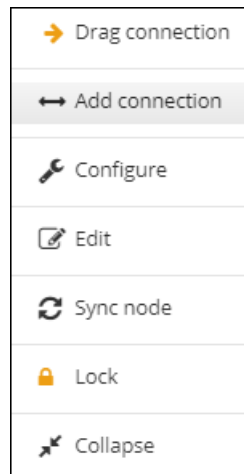
Adding Connections

You can configure a connection between two nodes.

➤ **To add a connection:**

1. In the Network Map view, right-click the node from which to configure the connection and in the popup menu click **Add Connection**.

Figure 3-19: Add Connection



Alternatively, in the Network Map view (1) select the node to which to add a connection and then click the action button **Add connection** or (2) use the **Drag Connection** button.

Figure 3-20: Add Connection

ADD CONNECTION

Name: *

Weight: 50

Transport Type: TCP

	Node 1	Node 2
Node: *	172.17.133.30-1	172.17.133.31-2
Routing Interface: *	SIP-0	SIP-0
Name: *	ARM_2.7_3.9	ARM_3.9_2.7
Ip Profile: *	ARM_IP_Profile	ARM_IP_Profile
Media realm:		
SIP Group name: *		

Advanced Conditions

☒ Keep connection properties synchronized

☐ use global quality definitions

☐ use specific quality definitions

☐ MOS ☐ ASR

OK Cancel

2. Provide an intuitive name for the connection, to later facilitate user-friendly management in the ARM GUI.
3. Select the weight. Default: 50. Range: 1-100.
4. From the 'Transport Type' drop-down menu, select **UDP** (default), **TCP** or **TLS**.
5. From the 'Node-1' drop-down menu, select the name of the node and from the 'Routing Interface-1' drop-down menu, select its routing interface
6. From the 'Node-2' drop-down menu, select the name of the node and from the 'Routing Interface-2' drop-down menu, select its routing interface
7. Select and configure a corresponding name of an IP Group for each node. Default 'Name' options are taken from the SOURCE and DESTINATION interface IDs, for example, **ARM_2.7_3.9**, as displayed in the preceding figure.
8. From the 'IP Profile' drop-down | 'Media realm' drop-down, select an element that is used by or created by the Routing Server in the SBC.



- If one of the IP Profile names exists in the SBC when adding or editing a connection, the connection will fail to be created.
- 'IP Profile' and 'Media Realm' are available from SBC versions 7.20A.258-0313, 7.20A.260-180 and 7.40A.005.

9. To define Advanced Conditions (quality-based routing), see [Routing Settings](#) on page 233.

10. Click **OK**; the connection is made.

Synchronizing Topology

The Sync Topology feature allows you to perform manual synchronization per Node or per global topology synchronization, depending on where the synchronization action was run.

It's important that node status is fully synchronized with the ARM server at all times for the ARM GUI to display the node successfully and for routing to be performed correctly.

For an SBC / Media Gateway to be displayed in the ARM GUI, you need to point it to the ARM server IP address using the Web interface.

The ARM auto-discovers all network entities such as Nodes, Peer Connection and VoIP Peers, associates a VoIP peer with each Peer Connection, and displays them in the Network Map view.

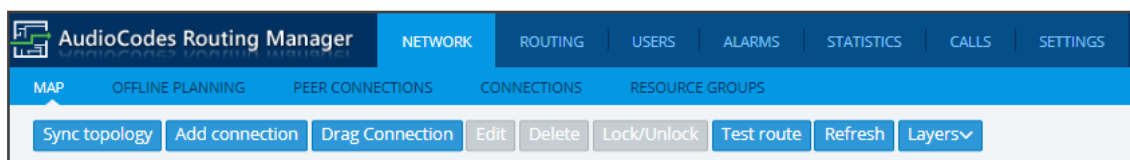
The ARM detects activity originating from a node and puts the node on the map (peer collection). The ARM recognizes a newly added node and extracts all IP groups (i.e., Peer Connections). Users must add connections between nodes and change the VoIP peer types (see under [Adding Connections](#) on page 84).

If a node's status is changed, the ARM detects this when synchronization is performed and automatically maps it. When synchronizing, the ARM obtains the names and statuses of connections and Peer Connections from each node and compares them to what it already knows. The Sync Topology feature therefore makes sure that the ARM is fully identified with the node's identifiers: IP address, credentials, node type, software version.

➤ To sync:

- In the Network Map view or Peer Connections view or Connections view, click **Sync Topology** on the action buttons bar.

Figure 3-21: Sync Topology



Global synchronization of the entire network is performed.

Testing a Route

You can configure and test a route to make sure the call routing rule, the manipulation rule, the topology status, etc., all perform per expectations, without impacting live calls traffic.

➤ **To test a route:**

1. In the Network Map view, select the connection between a node and a VoIP Peer (Peer Connection) and then click the **Test Route** button.

Figure 3-22: Test Route

2. [Optional] Enter the Source and Destination Route. From the drop-down menu, select the **Peer Connection**.

3. Under 'Advanced Options', select the routing rules mode:

- **Live.** When a new call destination is calculated, the Routing Rule is taken into consideration and live traffic may be impacted.
- **Test.** Tests the Routing Rule or Dial Plan *offline* without impacting or disrupting live calls traffic.
- **Live and Test** selected together. The Routing Rule is considered when:
 - ◆ calculating the live routing path -and-
 - ◆ testing a route in the live topology map *and* in the offline planning page

Each routing rule can be enabled or disabled separately for **Live** mode and / or **Test** mode (see also under [Adding a New Routing Rule](#) on page 268).

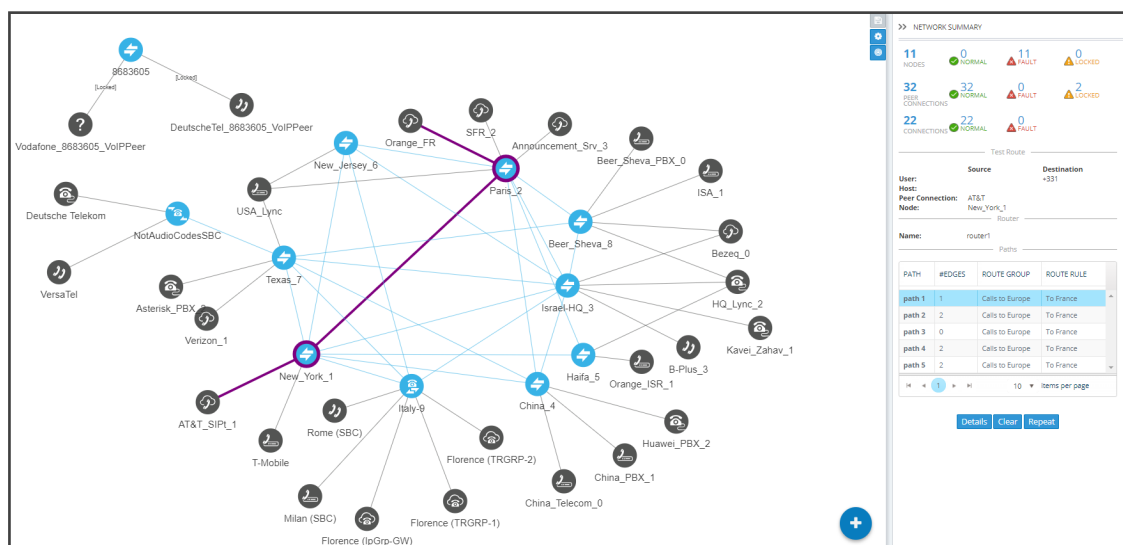
4. Under 'Advanced Options', select the call trigger. By default, the **Initial** option is enabled. See step 11 under [Adding a New Routing Rule](#) on page 268 for more information about call triggers.
5. Optionally, test the route with a specific ARM Router (also supported in 'Test Route' activated from 'Offline Planning'): Under 'Advanced Options', select from the 'Router' drop-down:

- Any (default) = the ARM Configurator contacts any ARM Router to perform a 'Test Route' and get the results; the ARM Router is chosen randomly.
- Select a specific ARM Router for a test call.

Use this feature for debugging and locating potential issues.

- Click **Find Routes**. Test routing is performed *as if* a real call is occurring, taking Operative State and Admin State of topology entities (Connections, nodes, Peer Connections), and the Admin State of routing rules, into account. In addition, the entity's Quality or Time/Date criteria are taken into consideration if required by the Routing Rule (Advanced Condition). The Route Path is highlighted purple (shown in the following figure); the panes on the right of the page display detailed information.

Figure 3-23: Test Route Paths



Test Route displays forking. If Test Route criteria match a Routing Rule with Forking Routing Method, it's displayed accordingly in the Paths section as shown below.

Figure 3-24: Test Route Paths

GENERAL STATISTICS
TOP 5 ROUTES
TEST ROUTE

Source
Destination

User:
Host:
Peer:
Connection:
Node:

789
IpGrp5
New_York_1

Router

router1

Paths

Route Rule	Path	#Edges	Route Group
my_test	path 1	1	Calls To Israel
	path 2	1	Calls To Israel
	path 3	1	Calls To Israel

Details
Clear
Repeat

7. Select a path (path 1, 2 or 3 in the preceding figure); that path of the call's forking is displayed in a unique color on the map as shown in the following three figures. Note that for each forking leg (forking path), its details are available.

Figure 3-25: Forking Path 1

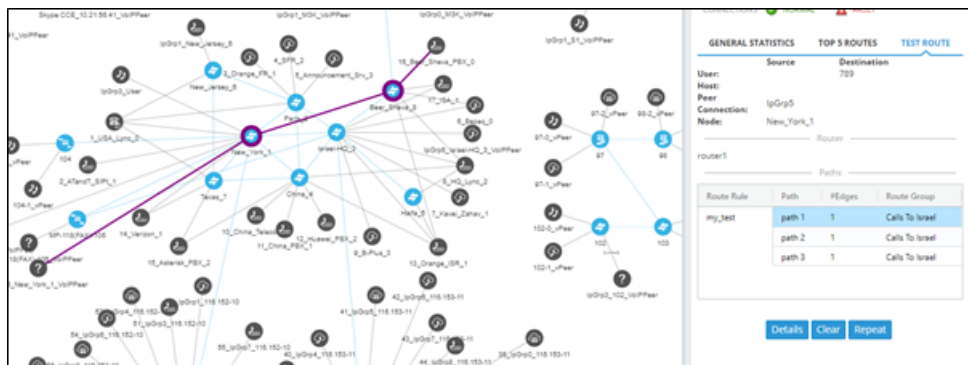


Figure 3-26: Forking Path 2

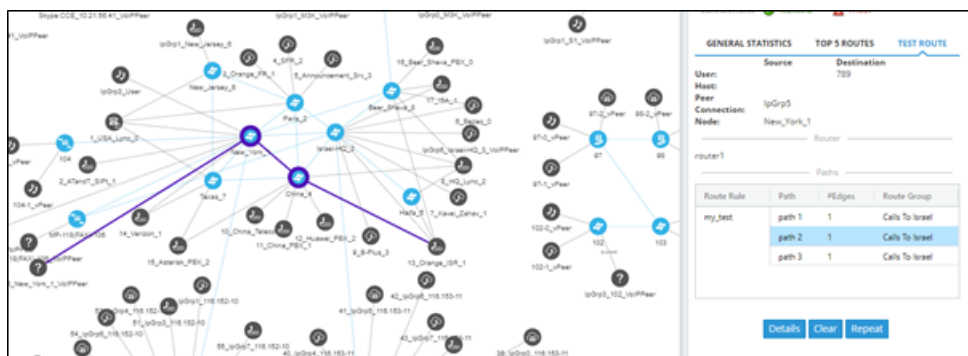
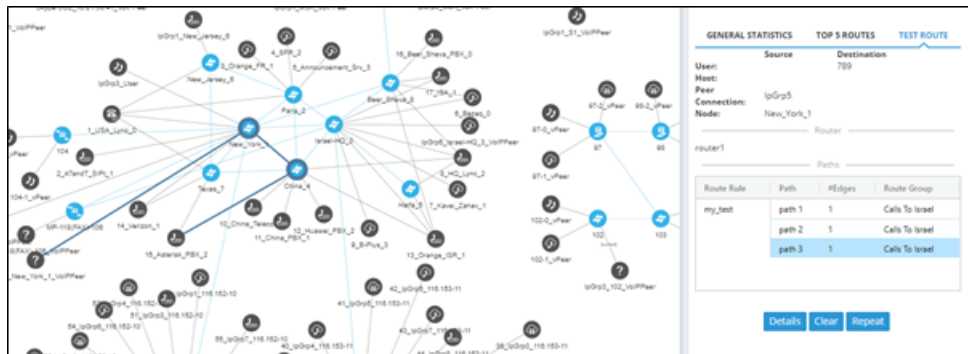


Figure 3-27: Forking Path 3



If there are no paths, the **Details** button will nonetheless be displayed; clicking it will show the Unselected Rules (see the descriptions of the columns CHANGED BY and DESCRIPTION below for more information about Unselected Rules).

8. In the Test Route panel, click the **Details** button.

Figure 3-28: Test Route Details

TEST ROUTE DETAILS						
Manipulation before route						
USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZATION	DESCRIPTION
Yes			Source Uri User	Global: Routing Incoming Manipulation	telerik	
Yes	+97225567	97225567	Destination Uri User	Peer Connection: sipp_in	israel	
No				Policy Studio: web-service1		Web service failed - Puzzle
Manipulation during route						
USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZATION	DESCRIPTION
No				Rule: Rule 1, Action: sipp_out(Node2)		Peer Connection state is invalid
Yes				Rule: rule 2, Action: sbc142_ipg1(Node2)		
Ok						

9. In the above example of the Test Route Details screen:
 - Compare the column ORIGINAL to the column NEW; the number changes if a normalization rule was applied. The normalization rule is configured in the Normalization Group rules attached to the Peer Connection. For related information, see also under [Peer Connections Page Actions](#) on page 47 and [Examples of Normalization Rules](#) on page 339.
 - The screen example indicates *when* manipulation was performed:
 - ◆ Manipulation *before* route (upper screen section)
 - ◆ Manipulation *after* route (lower screen section)
 In the screen example, manipulation was performed *before and during* route.
 - Column ENTITY indicates which part of the SIP Request was manipulated.

- ◆ Possible values: Source URI User, Source URI Host, Destination URI User, Destination URI Host, Destination IP Address, Destination Port, Destination Protocol, User Credential User Name, User Credential Password
- The column CHANGED BY (use the previous figure as reference):
 - ◆ the first row indicates by global Normalization Group – see under [Adding a Normalization Group](#) on page 198 and [Normalization Before Routing](#) on page 207 for detailed information
 - ◆ the second row indicates that the normalization was attached to a Peer Connection - see under [Peer Connection Information and Actions](#) on page 41 for detailed information
 - ◆ the 'No' in the third row under the column USED IN ROUTING indicates an unselected Policy Studio that was *not* applied (see step 8 under [Web-based Services](#) on page 224)
 - ◆ under 'Manipulation during route', the 'No' in the first row under the column USED IN ROUTING indicates that the Unselected Rule that occurred before the selected Test Route path *was* applied
 - ◆ also under 'Manipulation during route', the 'Yes' in the second row under the column USED IN ROUTING indicates the selected Test Route path.
- The column NORMALIZATION indicates which 'Manipulation Group' the entity passed through, according to which regular expression the entity was changed.
- The column DESCRIPTION indicates the reason why the Policy Studio / Routing Rule is unselected. For more information, see under [Examples of Unselected Rules Reasons](#) on page 96



- A new Routing Rule is *by default* added in 'Test Mode' (not 'Live'). To test the rule before switching it to live, use the 'Test' option of 'Test Route'.
- After performing Test Route, the results (including the selected path) are preserved in the Network Map even if you switch to another tab. This is convenient when debugging a Dial Plan, after fixing a Routing Rule and reverting to testing it in the Network Map with the 'Test Route' feature.

Testing a Route for Registration Messages

The ARM gives operators the capability to test routing for registration messages in the same way the test route feature is available for Call Routing. Test Route capabilities can be selected the same way as in previous ARM loads.

➤ To test a route for registration messages:

- In the Test Route screen, select the 'Request type' to be tested. Select **Register** for testing registration messages routing:

Figure 3-29: Request type: Register

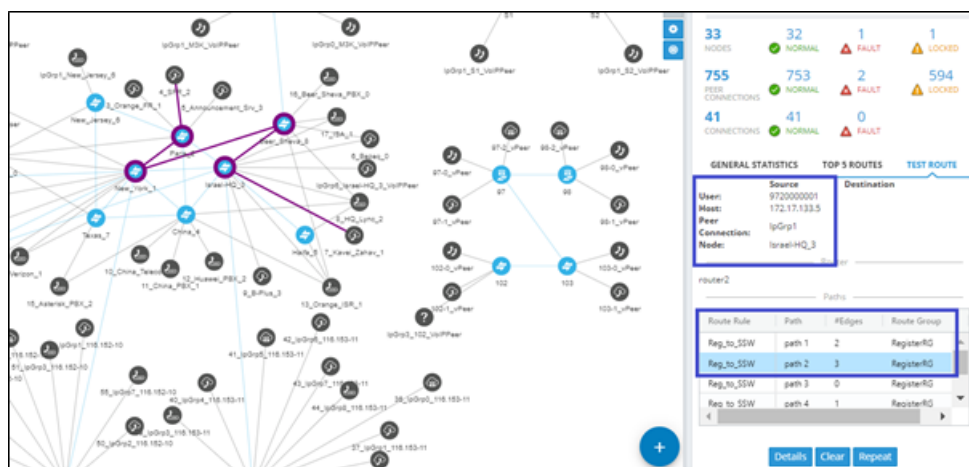
The default is **Call** (for testing call routing).

Figure 3-30: Include routing rules in the following mode: Live

The Test Route screen for testing registration messages routing includes the following parameters:

- **User @ host.** The user and host of the phone simulating sending of the Registration request to be routed.
- **Node.** The Source Node for Registration simulation (where the phone sends its Register).
- **Peer Connection.** The Source Peer Connection of Registration message sent.
- **Advanced options.** The advanced options relevant for Registration routing simulation (Mode – Live or Test) and specific Router selection. Route trigger is not relevant for Registration messages test route.

The result of Test Route for Registration message routing simulation is based on matching appropriate Routing Rules.

Figure 3-31: Result



Test Route for registration message routing simulation is also supported for Offline Map. In this case, the test considers relevant routing rules in Test mode only and can include offline topology elements.

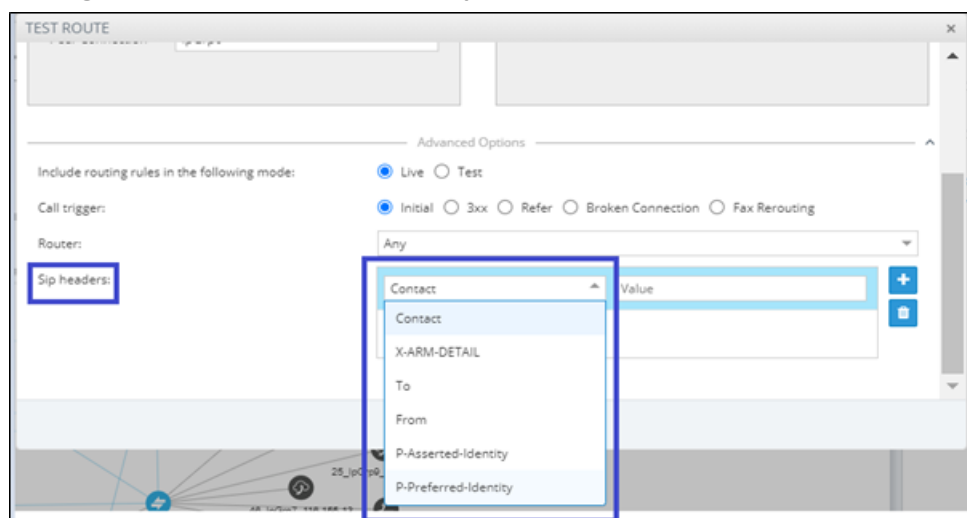
Testing Call Routing Simulation with a Specific SIP Header

The Test Route feature includes the capability to simulate a call with a specific SIP header's value. Before testing call routing simulation with a specific SIP header, you need to configure the manipulation of a specific Source URI header as described in [Adding a New Routing Rule](#) on page 268.

➤ To perform Test Route with simulation of SIP header value:

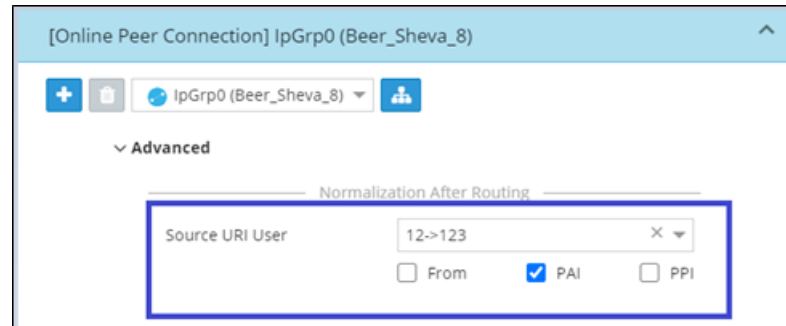
1. In Test Route, open 'Advanced Options', add one of the headers and provide a value. Multiple headers can be provided as input for Test Route (multiple adds). The following SIP header types are supported:
 - Contact
 - X-ARM-DETAIL [for simulation of ARM capabilities to route a call based on any SIP header value (capability also requires manipulation at the SBC level)]
 - To
 - From
 - P-Asserted-Identity
 - P-Preferred-Identity
2. Perform Test Route for SIP header simulation. Only one SIP header of each type can be added. However, more than one SIP header (up to three) of type X-ARM-DETAIL can be added.

Figure 3-32: Test Route on multiple SIP headers simulation



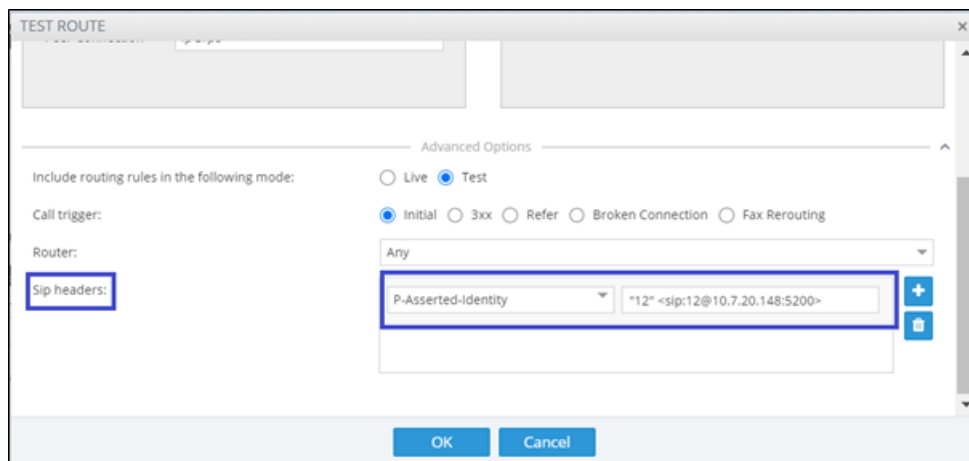
3. View the manipulated value, including the reason for the manipulation and the normalization rule that was applied, in the Test Route result in the details of the selected path. Following is an example of manipulation of P-Asserted-identity and its testing. In the Routing Rule, under the 'Advanced' options under Action, check a specific Source URI User header field:

Figure 3-33: Routing Rule: PAI



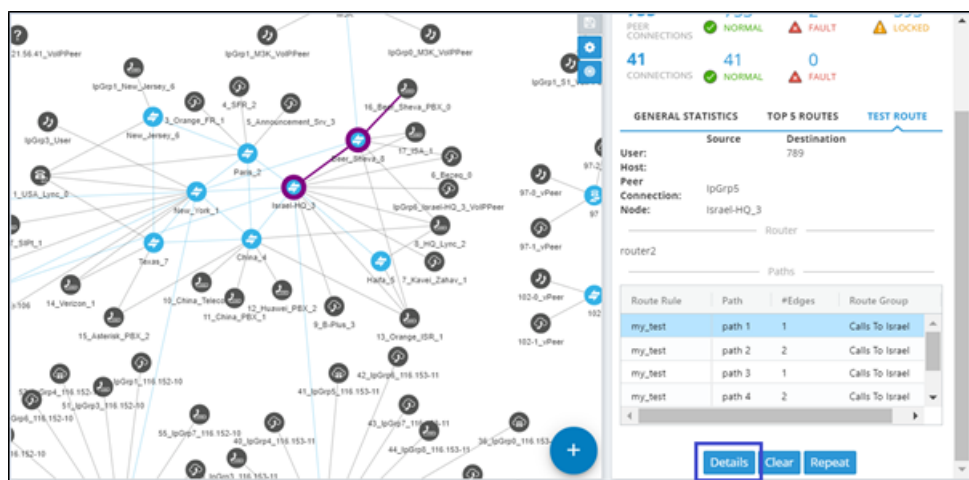
4. Perform a Test Route with the specific P-Asserted-identity value simulation:

Figure 3-34: Testing a route with a specific P-Asserted-identity value simulation



5. View the Test Route results.

Figure 3-35: Viewing the Test Route results



6. View the details of the path showing the manipulation performed on P-Asserted-Identity:

Figure 3-36: Viewing Test Route Details

Manipulation during route						
USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZATION	DESCRIPTION
No				Rule: Rule 1, Action: sipp_out(Node2)		Peer Connection state is invalid
Yes	12	123	P-Asserted-Identity ...	Rule: rule 2, Action: sbcl42_jpg1(Node2)	12->123	

7. Following is an example of manipulation of X-ARM-DETAIL and its testing. In the Routing Rule, under 'SIP headers' under 'Advanced Conditions', add the header name and its value:

Figure 3-37: SIP Headers

8. Perform a Test Route with the specific X-ARM-DETAIL value simulation:

Figure 3-38: Test Route with the specific X-ARM-DETAIL value simulation

9. View the Test Route results.

Testing 'Customer' Entity

The 'customer' entity is also supported by the ARM's Test Route. For detailed information about the 'customer' entity, see under [Customers Page](#) on page 61 and under [Defining a 'Customer' Entity \(Teams Tenant\)](#) on page 64

The example shown in the following figure shows a test call coming from **customer 4 (Teams)** toward Verizon SIP trunk.

Figure 3-39: Testing a Route from a 'Customer' Entity



The ARM identifies the customer (shown in the Test Route Summary) based on the source DID (prefix **pf1** used for identification of **customer4**).

Examples of Unselected Rules Reasons

Examples of unselected rules reasons fall into two categories:

- During Route - Unselected Rules (see [During Route – Unselected Rules](#) below)
- Before Route (Policy Studio) - Unselected Rules (see [Before Route \(Policy Studio\) - Unselected Rules](#) on the next page)

During Route – Unselected Rules

Node state is invalid

Peer Connection state is invalid

Peer Connection quality is invalid for the current action

Trunk is invalid for Request URI action

Destination already exists (with the same normalizations) in the selected rules list

Registered user not found

Gateway invalid action – an IPGroup on the Gateway to another node,

Gateway invalid action – an IPGroup on the Gateway to another IPGroup on the same node

Gateway invalid action – a node to an IPGroup on the Gateway

Hybrid invalid action – an IPGroup on the Gateway side to another node

Hybrid invalid action – an IPGroup on the Gateway side to another IPGroup on the same node

Hybrid invalid action – an IPGroup on the Gateway side to the SBC side on the same node (when a destination Peer Connection does not exist),

Hybrid invalid action – another node to an IPGroup on the Gateway side

Hybrid invalid action – an IPGroup to another IPGroup on the Gateway side

Hybrid invalid action – an IPGroup (connection) to an IPGroup on the Gateway side

There is a destination IP address header and no destination Peer Connection

There is a destination IP address header, and the destination Peer Connection is not an IPGroup

There is a destination IP address header, and the destination Peer Connection is without RoutingInterface

Outgoing Peer Connection CAC limit has been reached

Outgoing VoIP Peer CAC limit has been reached

Outgoing Peer Connection Quota limit has been reached

Outgoing Topology Group Quota limit has been reached

Outgoing customer CAC limit has been reached

Incoming customer CAC limit has been reached

Incoming VoIP Peer CAC limit has been reached"

Incoming Peer Connection CAC limit has been reached"

Before Route (Policy Studio) - Unselected Rules

Web service failed – with proper reason

4 Designing a Network Topology in the Offline Planning Page

The ARM gives operators an add-on to design an IP network in the Offline Planning page starting from the beginning.

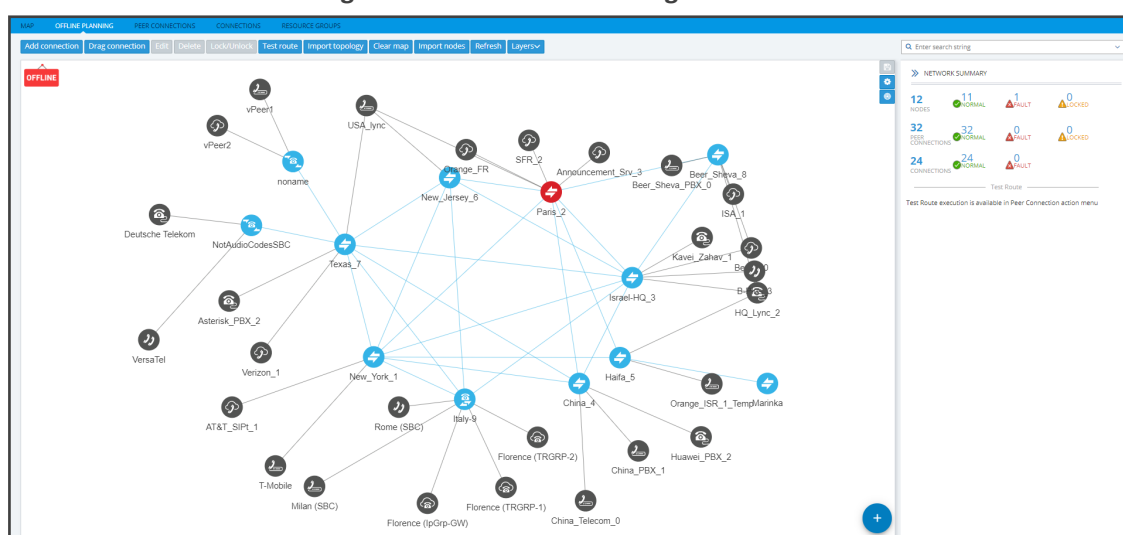
Operators can alternatively import an existing live topology into the page, make changes to entities' configuration and statuses, and test how the changes impact network functionality.

Feature benefits:

- Saves expenses in the network design phase | maintenance phase
- Prevents routing errors from occurring
- Decreases maintenance windows

The Offline Planning page is essentially a Map view that can be used as a sandbox for network design and testing purposes.

Figure 4-1: Offline Planning



In the view, the operator can create virtual nodes, Peer Connections, VoIP Peers, and Connections. The operator can import a full, currently-used topology, or part of one, e.g., a specific node, for making changes and testing offline.

The operator can 'play' with the Administrative State, Operative State, Quality and Weight - if available - of each virtual entity and test how the changes impact call traffic.

After entities are added to the Offline Planning page they can be used in Routing Rules in testing mode; live network traffic will not be impacted.

The feature allows operators to test almost any scenario before transposing the configuration to the live topology.

The following figure shows the Operative State and Quality settings per peer connection.

Figure 4-2: Edit Peer Connection

After designing virtual VoIP network entities, you can export them to the live topology. When you export a newly defined node to the live topology, the node configuration downloads to AudioCodes' device which automatically connects to the live topology.



When exporting an offline node to the live ARM topology, only the *connections* in the live node are provisioned; you need to *manually provision* Peer Connections in the node.

Performing Actions in the Offline Planning Page

In the Offline Planning page, you can perform the following actions:

- Add a virtual entity to the Offline Planning page
- Import an existing node and all entities associated with it from the live topology
- Import a full topology from the live topology
- Combine a virtual configuration with an imported one

Adding a Virtual Entity

Two types of virtual entities can be added to the Offline Planning page:

- Nodes
- VoIP Peers

➤ To add a virtual node:







1. In the Offline Planning page, click  and then click ; then select the virtual node type or third-party node type using the following table as reference.

Table 4-1: Add a Virtual Node

Icon	Used to
	Drag and drop a third-party Node onto the Offline Planning page.
	Drag and drop a virtual <i>hybrid</i> device onto the Offline Planning page.
	Drag and drop a virtual <i>gateway</i> onto the Offline Planning page.
	Drag and drop a virtual <i>SBC</i> onto the Offline Planning page.

2. Drag the selected type of device to the map and configure its name.

➤ **To add a virtual VoIP Peer:**








1. Click  and then ; then select the VoIP Peer type using the following table as reference.

Table 4-2: Add a Virtual VoIP Peer

Icon	Used to
	Drag and drop a <i>PSTN entity</i> onto the Offline Planning page.
	Drag and drop a <i>PBX</i> onto the Offline Planning page.
	Drag and drop an <i>IP PBX</i> onto the Offline Planning page.
	Drag and drop a <i>SIP Trunk</i> onto the Offline Planning page.
	Drag and drop an <i>IP phone</i> onto the Offline Planning page.

2. Drag the icon to the map and configure the name of the VoIP Peer.

Adding a Virtual Peer Connection to the Offline Page

You can add a virtual Peer Connection or a Peer Connection to the Offline page (**Network > Offline**).

➤ To add a virtual Peer Connection:

- In the Offline page, drag a line from the center of a node to a VoIP Peer and then configure it in the Add Virtual Peer Connection screen that opens:

Figure 4-3: Add Virtual Peer Connection

See also under [Adding a VoIP Peer](#) on page 76.



The action 'Drag peer connection' is available only to third-party non-AudioCodes SBCs or Media Gateways. It's not applicable to AudioCodes SBCs or AudioCodes Media Gateways.

Adding a Virtual Connection

You can add a virtual Connection to the Offline Planning page.

➤ To add a virtual connection to the Offline Planning page:

- Click the **Add Connection** button to add a connection between two offline nodes; the same screen as the 'Add Connection' screen shown under [Adding Connections](#) on page 84 is displayed; the procedure is identical to that performed in the live topology.

Importing a Full Topology

You can import a full topology from the live topology map to the Offline Planning page.

➤ To import a full topology:

- Click the **Import topology** button; all network entities in the live topology including nodes, VoIP Peers, Peer Connections and Connections will be imported.

Importing a Node from the Live Topology

You can import a node from the live topology to the Offline Planning page.

➤ To import a node from the live topology:

- Click the **Import nodes** button and select a relevant node from the list that pops up; the node will be added to the Offline Planning map together with Peer Connections and VoIP Peers associated with that node.

Deleting a Virtual Entity

You can delete a virtual entity from the Offline Planning page.

➤ To delete a virtual entity from the Offline Planning page:

- Select an entity and then click **Delete**.
- Click **Clear Map** to delete all entities from the page.

Testing a Route

You can test a route in the Offline Planning page.

➤ To test a route:

- To test a route in a virtual network, select the Peer Connection and then select **Test Route** (see [Testing a Route](#) on page 87). Testing a route in the Offline Planning page factors in all entities configured in the Offline Planning page and their status and voice quality.

Exporting a Node from the Offline Page to the Live Topology

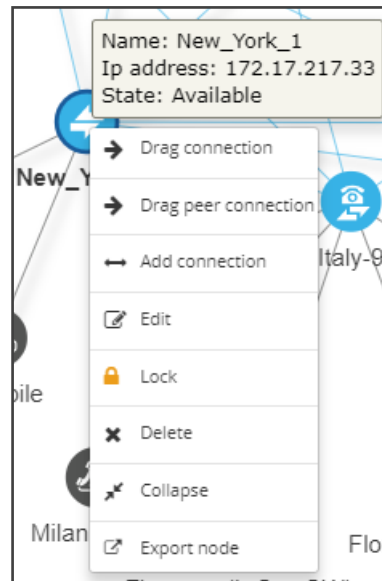
You can export a node from the Offline Planning page to the live topology.

➤ To export a node from the Offline Page to the live topology:



Before exporting a node to the live topology, make sure it's correctly configured in the Offline Planning page. If a node with the same IP address already exists in the live topology, the entire configuration of the node will be transferred to that node in the live topology. Before exporting a node to the live topology, make sure all Peer Connections (IPGroups) are configured on that node.

- In the Offline Planning page, right-click the node and from the popup menu select **Export node**.

Figure 4-4: Export Node

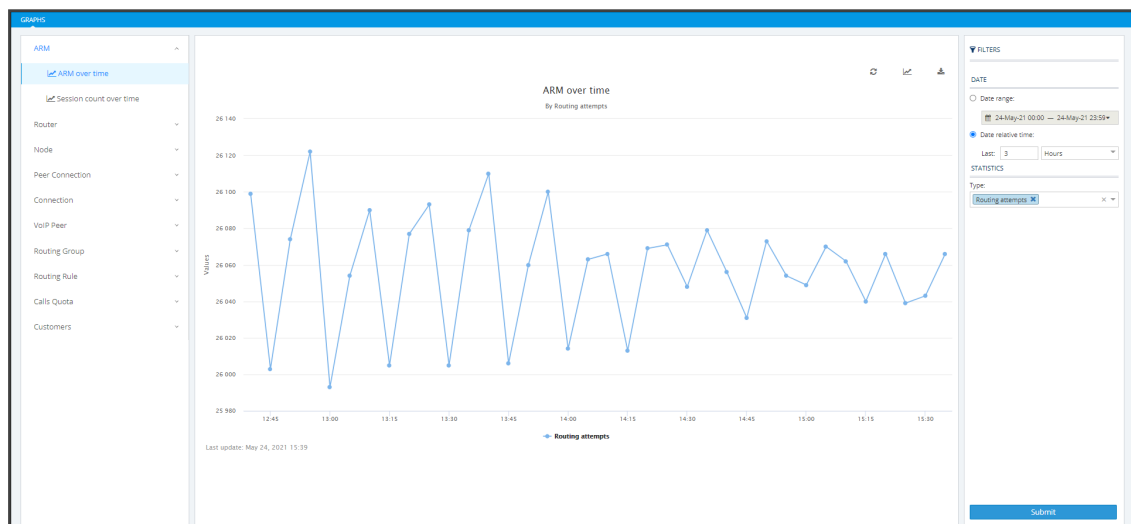
5 Viewing Statistics and Reports

The ARM provides a Statistics Graphs page and ARM-embedded statistics reports, allowing you to debug, monitor and optimize your network and routing. Statistics charts provide you with a clear view of your network and routing performance, helping you better understand, analyze, debug and optimize network routing and resources usage.

➤ To use statistics graphs:

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

Figure 5-1: Statistics Graphs Page – ARM over time



The page is divided into three sections.

Table 5-1: Statistics Graphs Page (From Left to Right)

Element	Filters	Graphical Representation
<p>Statistics are displayed <i>per element</i> and are collected at an interval of every five minutes. Select either:</p> <ul style="list-style-type: none"> ■ ARM (ARM over time, Session count over time) ■ Router (Routers over time, Top routers, Top routers over time) ■ Node (Nodes over time, Top nodes, Top nodes over time, Nodes by peer connections, Top nodes by peer connections) ■ Peer Connection (Peer connections) 	<p>Filters differ depending on the element selected. <i>For all elements except Routing Group and Routing Rule, select from:</i></p> <ul style="list-style-type: none"> ■ 'Date' ('Range' or 'Relative') ■ Statistics Type:* ✓ Routing attempts 	<p>Graphic representation of the statistics of the selected element in a chart, with a range of graph functionalities:</p> <ul style="list-style-type: none"> ■ Refresh ■ Chart type (line, area or stacked area)

Element	Filters	Graphical Representation
<p>over time, Top peer connections, Top peer connections over time, Peer connection sessions over time)**</p> <p>■ Connection (Connections over time, Top connections, Top connections over time)</p> <p>■ VoIP Peer (VoIP Peer sessions over time)</p> <p>■ Routing Group (Routing groups over time, Top routing groups, Top routing groups over time, Top routing groups by rules, Top routing groups by rules)</p> <p>■ Routing Rule (Routing rules over time, Top routing rules, Top routing rules over time, Routing rules by actions, Top routing rules by actions)</p> <p>■ Calls Quota (Quota over time, Peer Connection over time, Resource group over time, Resource group by peer connection)***</p> <p>■ Customers (Customer sessions over time)****</p>	<p>✓ Alternative attempts</p> <p>✓ Unsuccessful routes</p> <p>✓ Destinations Not Routable</p> <p>✓ Destination calls</p> <p>✓ Transient calls (does not apply to Peer Connection) (for Connection, only this filter applies)</p> <p>✓ Drop routing request</p> <p>✓ No match rule</p> <p>■ Elements</p> <p>✓ Search</p> <p>✓ Number</p> <p>■ Stacked Elements</p> <p>✓ Search</p> <p>✓ Number</p> <p>■ Statistics Type (only applies to Routing Group and Routing Rule)</p> <p>✓ Routing rules attempts</p> <p>✓ Routing first match</p> <p>✓ Routing second match</p>	<p>■ Export chart</p>

Element	Filters	Graphical Representation
	<ul style="list-style-type: none"> ✓ Routing third match ✓ Routing rules failures 	

* Here are explanations to help you better understand each 'Statistics Type' filter:

Routing attempt: Any initial routing request from the node is counted

Alternative attempts: Each triggered rule action that is not the first action of the rule

Unsuccessful routes: The call was dropped with some termination reason

Drop routing request: Discard action was triggered

Destination not Routable: If there was no rule matching 'Destination not Routable' and 'Match rules are incremented'

Destination calls: Each time a call reached its destination

No match rules: No matching rule

Transient calls:

- Per node: the call passed via the node and is not the first nor the last in the route chain
- Per connection: any call passed on a connection is counted as transient
- Per router: the sum of transient calls of all nodes
- Per ARM: the sum of transient calls of all routers

Registration routed: REGISTER call was routed

Registration unrouted: REGISTER call was not routed

Registration blocked: REGISTER call was discarded

Average session count: The session count in a bucket of five minutes / 300 sec (average session count per second in a bucket of five minutes)

Total session count: The sum of incoming and outgoing session counts

** If you select the 'Peer Connection' tab and then 'Peer Connection sessions over time', you'll view the screen shown in the following example. Notice the Total CAC Limit which is only present if a CAC was attached to the element.



*** If you select the 'Calls Quota' tab and then 'Quota over time', the accumulated number of calls minutes for all Peer Connections or for Resource Groups associated with a specific quota will be displayed. Select a quota and then the Network Topology element type to be displayed (either Peer Connections or Resource Group); the ARM automatically filters relevant Network Topology elements (for example, a Peer Connection to which the quota is attached).

FILTERS

DATE

☐ Date range:

17-Feb-21 00:00

17-Feb-21 23:59

☒ Date relative time:

Last: 3

Hours

STATISTICS

Type:

Accumulated Duration

Quota name:

Teams_calls_Budget

Quota element type:

Resource Group

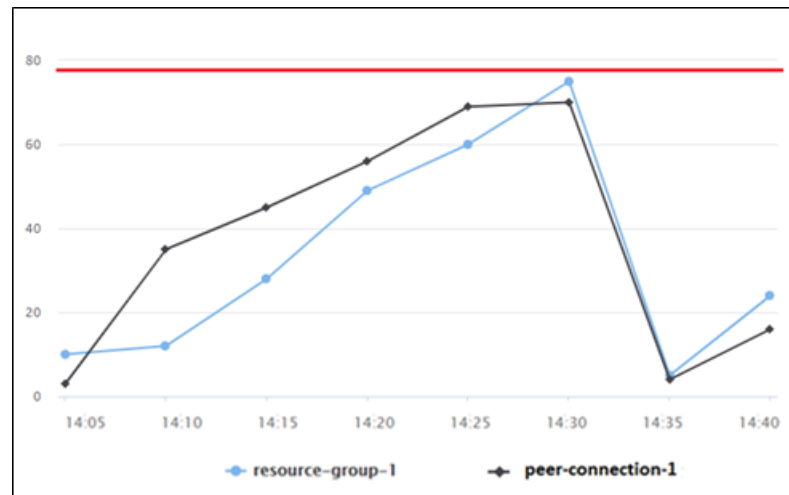
Elements:

Teams_PCons_Group

×

Submit

When submitted, the ARM will display minutes spent by each selected Network Topology element (for example, Peer Connections to which the calls quota was assigned). In the example below, a reset occurred because the period defined in the quota that was assigned to both Peer Connections, ended:

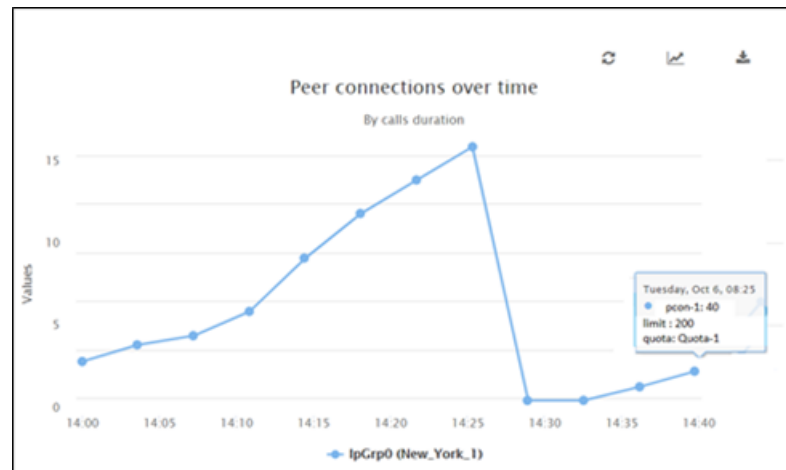


If a call starts before the quota is reached:

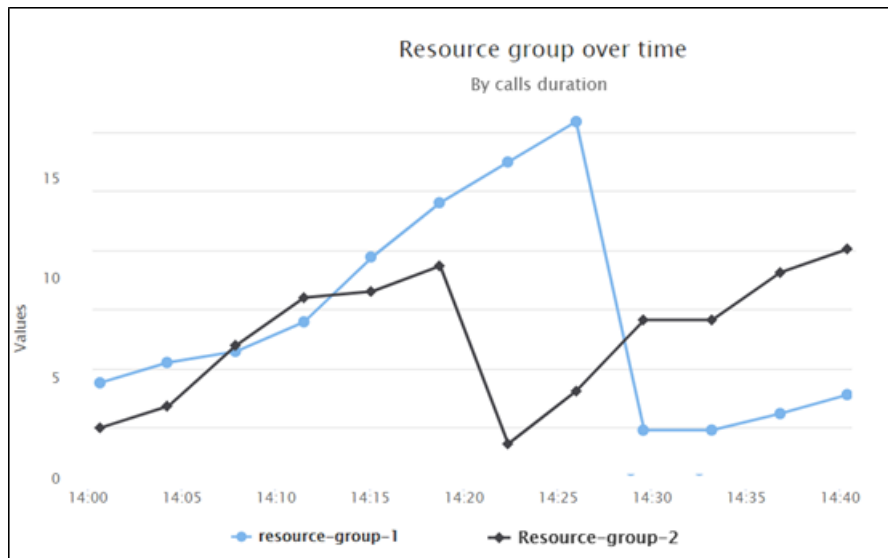
- the ARM will not drop the call
- the call will be calculated

In this case, the quota can be exceeded and it will be shown in the statistics.

If you select the 'Quota' tab and then 'Peer connections over time', you can select a specific Peer Connection (or multiple Peer Connections – where each can have a different Quota) and view the calls time (minutes) over time. A tooltip displays for each graph the name of the quota associated with the Peer Connection and the minutes assigned.

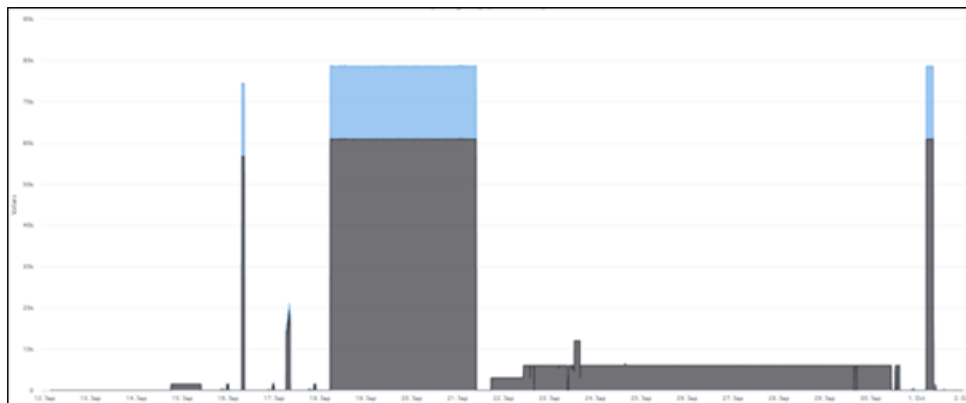


If you select the 'Quota' tab and then 'Resource group over time', you can then select a specific Resource Group (or multiple Resource Groups where each can have a different quota) and view the calls time (in minutes) over a timeline per Resource Group (the accumulated value for all Peer Connections in the Resource Group).



Only Resource Groups of type 'Peer Connection' can be selected. A tooltip displays for each graph the name of the quota associated with the Resource Group, and the limit (the number of minutes defined in the quota balance).

If you select the 'Quota' tab and then 'Resource group by peer connection', you'll view a stacked area (by default) showing consumption of calls minutes per Peer Connection in a specific Resource Group with an attached quota. You'll see, for example, that a quota allocated to a Resource Group connecting Teams is consumed unequally, mainly by one of the group's Peer Connections.



*** If you select the 'Customers' tab and then 'Customer sessions over time', you can then on the right side of the page select a specific 'customer' entity:

Element:

- customer4
- customer6
- customer4
- customer5
- customer1
- customer2
- customer3

The following statistics 'Types' can be selected per 'customer' entity:

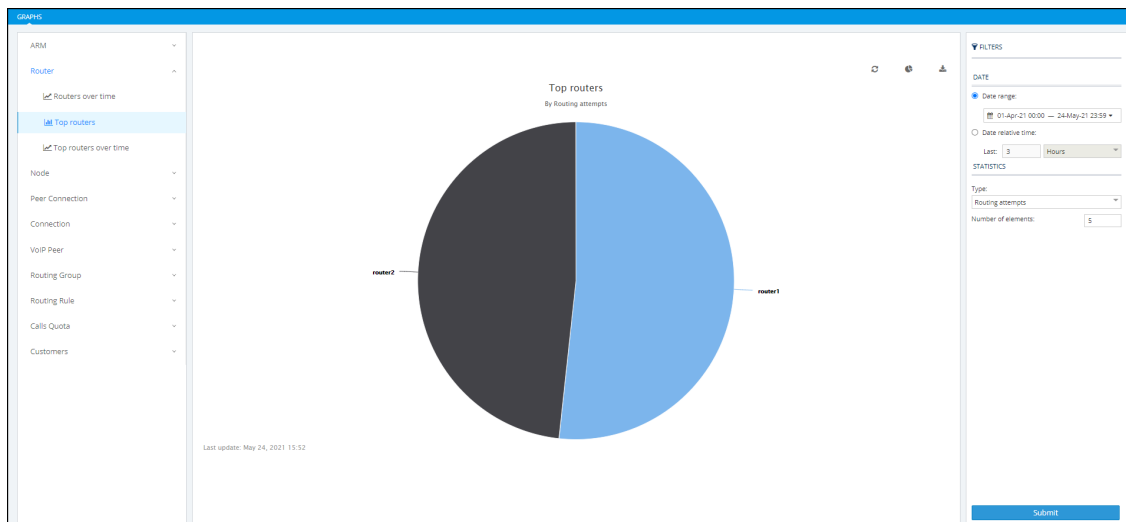
Type:

- Total Average
- Incoming Average
- Incoming Minimum
- Incoming Maximum
- Outgoing Average
- Outgoing Minimum
- Outgoing Maximum
- Total Minimum

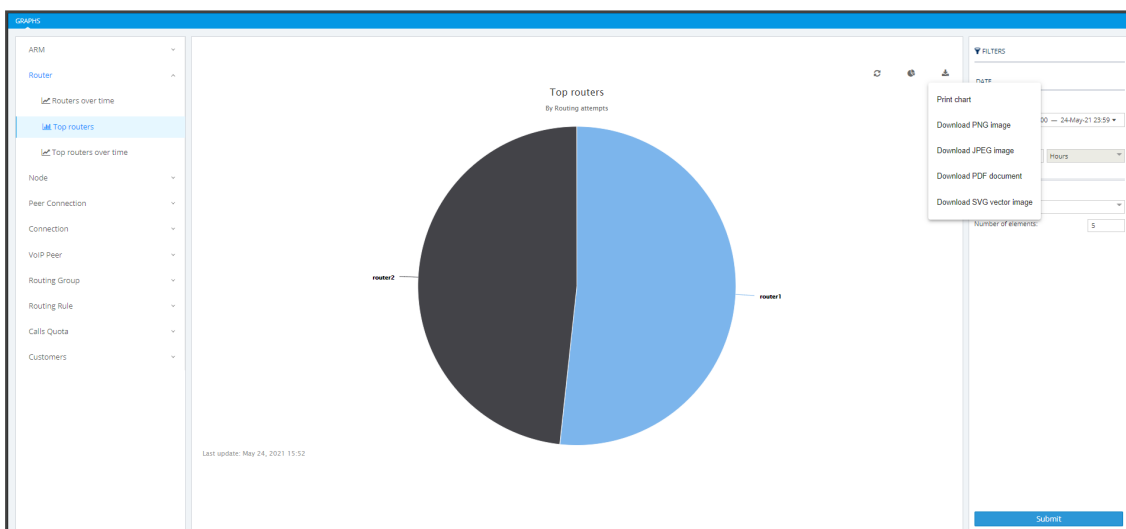
All Clear Invert

When showing statistics over time, the ARM also displays for your convenience the associated CAC Profile simultaneous sessions limit, thus allowing you to view the correlation and the number of sessions available for a 'customer' entity.

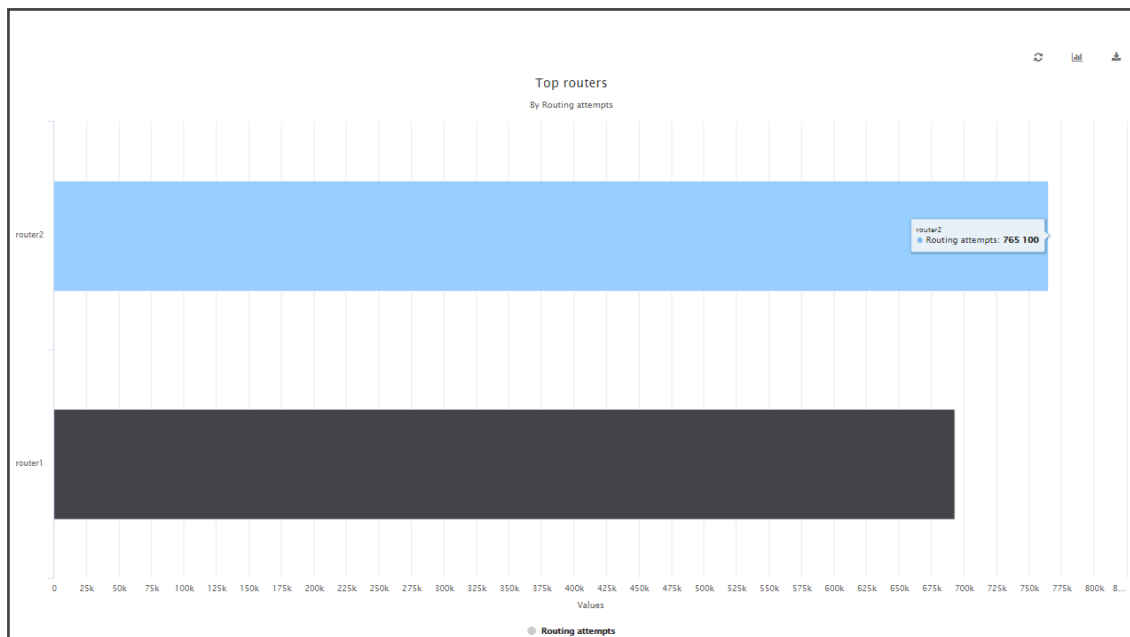


Figure 5-2: Top Routers Filtered by Routing Attempts Displayed as a Pie Chart

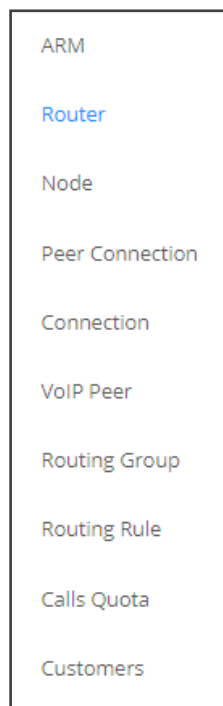
- A glance at the chart immediately reveals the top router. Point your cursor over a segment to display the number of routing attempts attempted by that router.
- You can print the chart or download the statistics in a format of your choice.

Figure 5-3: Downloading Statistics in a Format of Choice

- You can select your preferred graphical representation – bar chart, column chart or pie chart. An icon 'Select chart type' allows you to present statistics according to your preferred graphical representation.

Figure 5-4: Top Routers Filtered by Routing Attempts Displayed as a Bar Chart

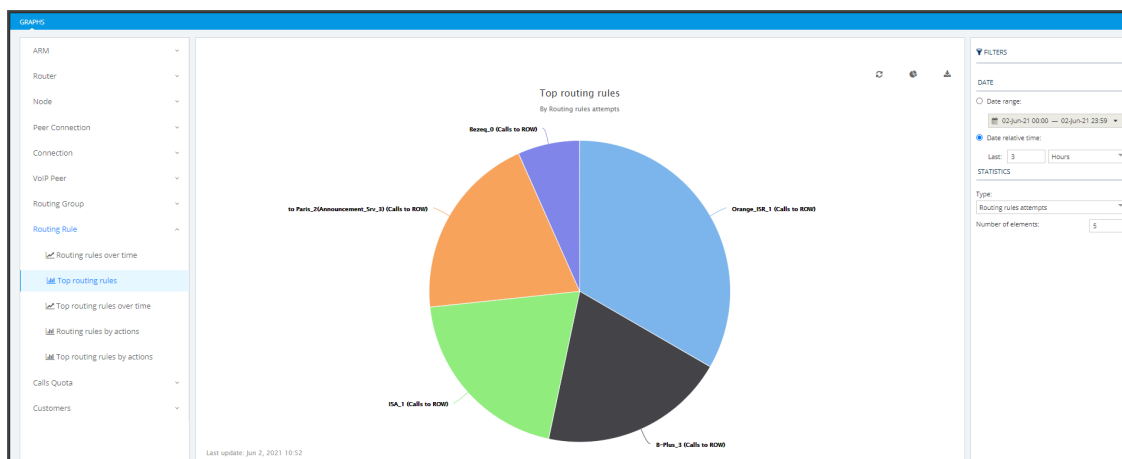
- A glance at this chart also immediately reveals the top router. Point the cursor over a bar to display the number of routing attempts attempted by that router. The following figure shows the elements that hold statistics information.

Figure 5-5: Elements that Hold Statistics Information

Each element displays subcategories. Under Routing Rule, for example, you can select 'Top Routing rules', 'Top Routing rules over time' or 'Top Routing rules by actions'.

In addition, in the Filters section of the page, you can select 'Number of elements'.

Figure 5-6: Top routing rules



Statistics pages feature filters in which network administrators can select multiple elements and then *invert the selection*. The feature improves usability and user experience especially in large networks with high numbers of elements. The feature allows network administrators to

- Select a single element
- Delete a single element (x)
- Select All elements
- Clear all selected elements
- Select All and delete a few (x)
- Select All, delete a few (x) and then invert the selection; the elements deleted will be in the selection
- Select a few elements and then invert the selection; only elements that weren't selected will be in the selection
- Clear a selection

Configuring Statistics Thresholds Based Alarms

The ARM provides the capability to define threshold-based alarms based on ARM statistics. Every five minutes, the ARM analyzes defined threshold rules and checks whether the defined thresholds were exceeded, starting at x2/x7, the last 5 minutes bucket is analyzed, a bucket being a period of x0-x5/x5-x0 minutes.

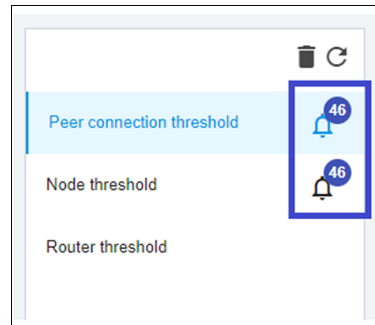
- If a trigger threshold is exceeded and an alarm does not exist, an alarm is issued.
- If the threshold is exceeded and an alarm does exist, the alarm count will be increased
- If an alarm exists and the value drops below the clear threshold, the alarm is cleared.

More than one alarm can be issued for the same threshold rule; an alarm is issued per element and statistic type.

The Statistics page displays a **Thresholds** tab (**Statistics > Thresholds**) under which thresholds are configured. The page allows **Add**, **Edit**, **Delete** and **Refresh** actions.

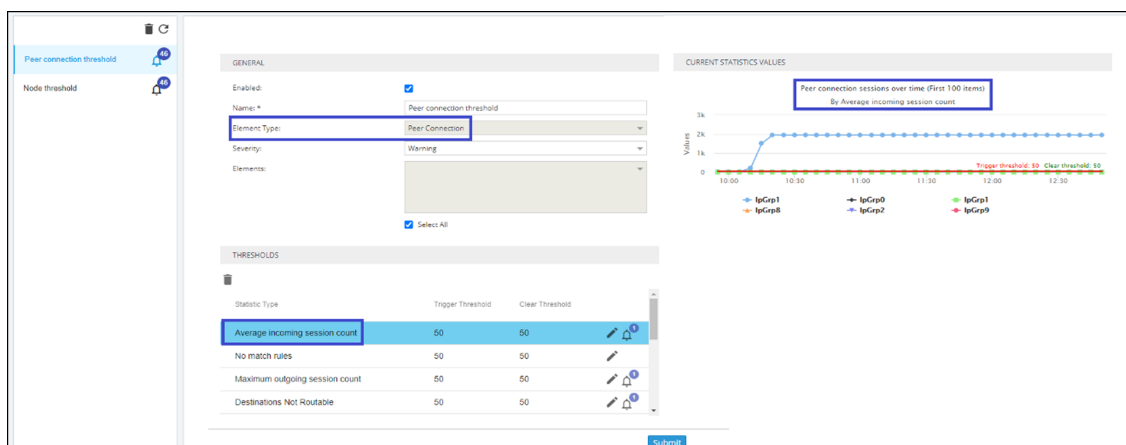
In the page's left pane:

- add a new threshold by clicking the + icon (see also [Adding a Statistics Threshold](#) below)
- delete an existing threshold by selecting the relevant threshold rule and then clicking the trash icon (see also [Deleting a Statistics Threshold](#) on page 118)
- refresh all thresholds by clicking the refresh icon
- edit an existing threshold by clicking a specific threshold, editing it, and then clicking the **Submit** button (see also [Editing a Statistics Threshold](#) on page 118); if there are alarms related to the threshold, an icon displaying the alarms count is shown.

Figure 5-7: # of Alarms per Statistics Threshold

The example in the preceding figure shows that there are currently 46 alarms related to 'Peer connection threshold' and 'Node threshold' and no alarms related to 'Router threshold'.

In the page's right pane, view the alarms distribution by statistic types. Under 'Current statistic values', the chart for the last three hours is displayed; the Current Statistics Values graph changes accordingly to the selected elements and selected statistic type in the Thresholds section. The chart also shows the trigger threshold and clear threshold. If no elements or statistics are selected, the chart will be empty. In the following figure, the chart represents Peer Connections by average incoming session count for the last three hours.

Figure 5-8: Current Statistics Values

Adding a Statistics Threshold

The instructions below show how to add a new statistics threshold.

➤ **To add a new statistics threshold:**

1. Click the **+** button; a new threshold is displayed, including a 'Save' icon in the left pane; this indicates that this threshold must be saved else it will be deleted.

Figure 5-9: New Threshold

2. Click the **Submit** button in the right pane to save the changes after defining the threshold.
3. Provide the following information:

Under the 'General' section of the page:

- **Enabled.** If unchecked, no alarms will be triggered, and the rule will be ignored.
- **Name.** Mandatory. Unique name of the 'threshold'.
- **Element type.** Can be:
 - ◆ ARM
 - ◆ Router
 - ◆ Node
 - ◆ Connection
 - ◆ Peer Connection
 - ◆ Routing Rule
 - ◆ Routing Group
 - ◆ Customer
 - ◆ VoIP Peer
- **Severity.** The alarm severity if the threshold limit is exceeded.
- **Elements.** Either 'All elements' or selecting specific elements.

Figure 5-10: Thresholds - Add | Edit

THRESHOLDS		
Statistic Type	Trigger Threshold	Clear Threshold
Alternative attempts	50	50
Transient calls	50	50
Registration routed	50	50
Destinations Not Routable	50	50

Under the 'Thresholds' section of the page:

- Click the + icon to add a new entry with default values. To edit the values, click the edit icon.

Figure 5-11: Thresholds - Add | Edit

THRESHOLDS		
Statistic Type	Trigger Threshold	Clear Threshold
Alternative attempts	50	50
Transient calls	50	50
Registration routed	50	50
Destinations Not Routable	50	50

For each threshold, provide the following information:

- Statistic type.** The Statistics option depends on the element type selected above.
 - ◆ **ARM Statistics.** Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, transient calls, no match rules, maximum session count, average session count, registration routed, registration unrouted, registration blocked.
 - ◆ **Router Statistics.** Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, transient calls, no match rules, maximum session count, average session count, registration routed, registration unrouted, registration blocked.
 - ◆ **Node Statistics.** Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, transient calls, no match rules.
 - ◆ **Peer Connection Statistics.** Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, no match rules, maximum incoming session count, maximum outgoing session count, maximum total session count, average incoming session count, average outgoing session count, average total session count.
 - ◆ **Connection Statistics.** Transient calls.
 - ◆ **Routing Rule Statistics.** Routing rules attempts, routing rules failures, routing first match, routing second match, routing third match.
 - ◆ **Routing Group Statistics.** Routing rules attempts, routing rules failures, routing first match, routing second match, routing third match.

- ◆ **Customer Statistics.** Maximum incoming session count, maximum outgoing session count, maximum total session count, average incoming session count, average outgoing session count, average total session count.
- ◆ **VoIP Peer Statistics.** Maximum incoming session count, maximum outgoing session count, maximum total session count, average incoming session count, average outgoing session count, average total session count.
- **Trigger threshold.** Exceeding this value causes an alarm to be issued.
- **Clear threshold.** If the statistic value drops below this number, existing alarms will be cleared.

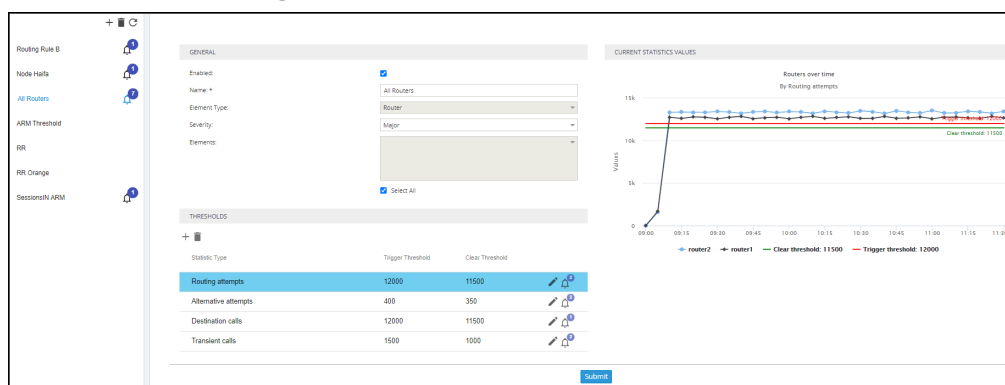
Viewing Statistics Thresholds Based Alarms

The instructions below show how to view statistics thresholds based alarms.

➤ To view statistics thresholds based alarms:

1. Open the Thresholds page (**Statistics > Thresholds**).

Figure 5-12: Thresholds



2. View in the 'Thresholds' section how many alarms exist for each statistics type as shown in this example:

Figure 5-13: # of Alarms per Statistics Type

THRESHOLDS			
Statistic Type	Trigger Threshold	Clear Threshold	
Routing attempts	12000	11500	
Alternative attempts	400	350	
Destination calls	12000	11500	
Transient calls	1500	1000	

In the example shown in the preceding figure, there are two alarms for 'Routing attempts', 'Alternative attempts' and 'Transient calls', and one alarm for 'Destination calls'.

3. Click an icon to navigate to the Alarms page filtered by the relevant thresholds based alarms.

Figure 5-14: Alarms Page Filtered per Statistics Thresholds Based Alarms

SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
Warning	12-04-21 9:12:00	Statistic threshold	Threshold ruleAll RoutersStatisticRoutingAttemptsRouter1	Router router1 Routing attempts crossed the trigger threshold (12000) defined in threshold rule All Routers
Warning	12-04-21 9:12:00	Statistic threshold	Threshold ruleAll RoutersStatisticRoutingAttemptsRouter2	Router router2 Routing attempts crossed the trigger threshold (12000) defined in threshold rule All Routers

Editing a Statistics Threshold

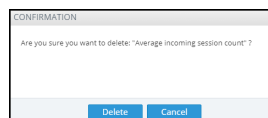
The instruction below shows how to edit a statistics threshold in case the threshold previously configured is too high or too low. The option to edit a statistics threshold allows you to change the same attributes that are provided in the **Add Threshold** action, excluding element type.

➤ To edit a statistics threshold:

- Click the relevant statistics threshold, edit it, and then click **Submit**.
 - If during **Edit** you disable the threshold, related alarms will be cleared, and this threshold rule will be unchecked until it will be changed back to enable.
 - If during **Edit** you delete a statistic threshold, related alarms will be cleared.
 - If during **Edit** you edit the 'trigger threshold' or 'clear threshold' of statistic threshold, alarms will be raised / cleared in the next ARM checking time.
 - If during **Edit** you delete elements, alarms related to the deleted elements will be cleared.

Deleting a Statistics Threshold

The trash icon allows the action to delete a statistics threshold. The ARM prompts you for confirmation before the delete action:

Figure 5-15: Confirm Delete

Alarms related to the deleted threshold rule are cleared.

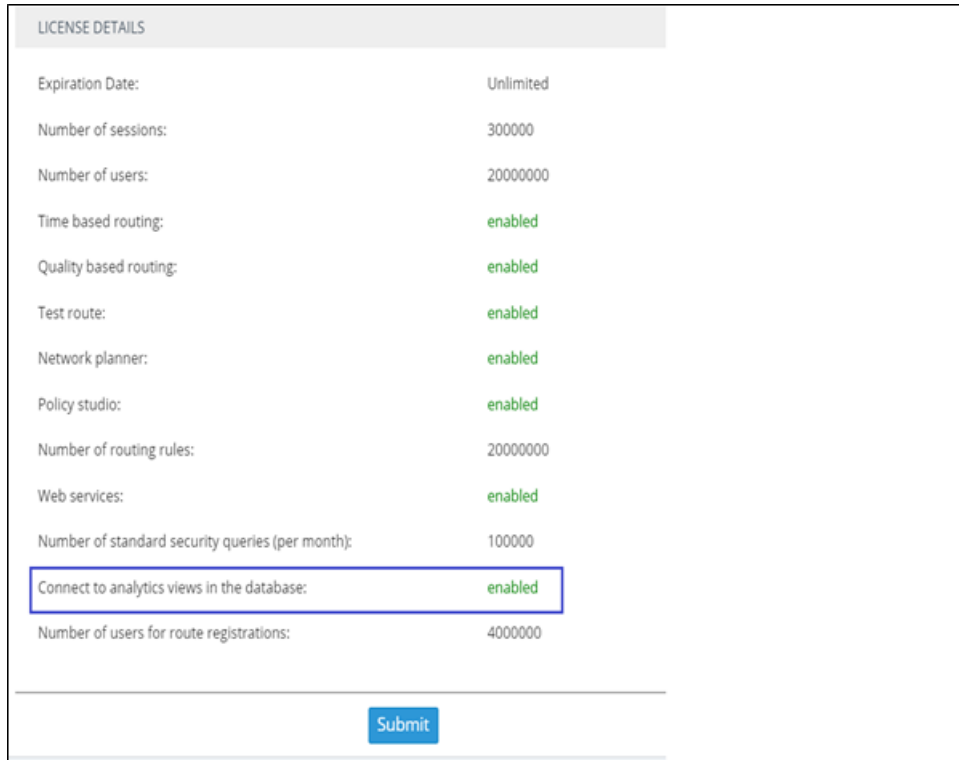
Accessing the ARM's Analytics API

The ARM enables customers to use their preferred analytics and third-party Business Intelligence (BI) tool to visualize ARM data. Customer operators are able to create their own dashboards and reports based on ARM data or combined data from the ARM and other tools (such as the OVOC). The ARM partially exposes summarized information from various database tables using the views capability of MariaDB.

➤ **To access the ARM Analytics API:**

1. Make sure your Feature Key (license) allows access; open the License Details page (**Settings > Administration > License**) and make sure parameter 'Connect to analytics views in the database' is set to **enabled**:

Figure 5-16: Connect to analytics views in the database

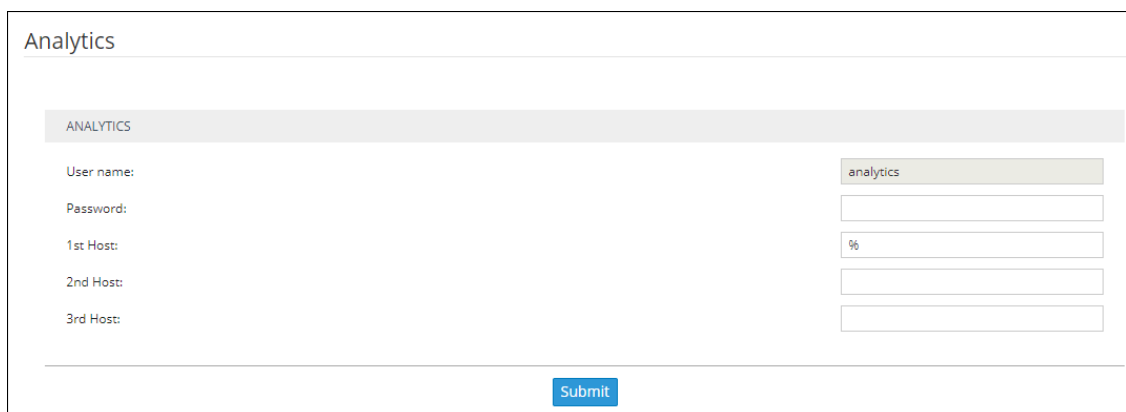


LICENSE DETAILS	
Expiration Date:	Unlimited
Number of sessions:	300000
Number of users:	20000000
Time based routing:	enabled
Quality based routing:	enabled
Test route:	enabled
Network planner:	enabled
Policy studio:	enabled
Number of routing rules:	20000000
Web services:	enabled
Number of standard security queries (per month):	100000
Connect to analytics views in the database:	enabled
Number of users for route registrations:	4000000

Submit

2. Open the Analytics page (**Settings > Administration > Analytics**).

Figure 5-17: Analytics



Analytics

ANALYTICS

User name:

analytics

Password:

1st Host:

%

2nd Host:

3rd Host:

Submit

3. Make sure parameter 'User name' is set to **analytics** (read-only); access to data is allowed using this default user.



The default 'analytics' user will be locked if the feature is disabled in the license. The 'analytics' user has only the select privilege (read-only) enabled only for the predefined views and doesn't have any other access to the regular ARM database. The operator can restrict access to analytics to a specific remote IP addresses (up to three can be defined). If an IP address list is not provided by the operator, access to analytics view will be unrestricted by source IP address.

4. Define a password and up to three IP addresses from which the data can be accessed.

Figure 5-18: Analytics - Password and 1st Host

The following views and statistics are provided as part of the Analytics API:

- **Nodes view.** Predefined view reflecting data from the APM nodes table with Nodes related essential information (such as ID, Serial Number, Name, Admin and Operative State, Software version, etc.)
- **Peer connection view.** Predefined view reflecting data from the Peer Connection table with information such as ID, Peer Connection Name, Admin state, related Node ID, etc.
- **Connection view.** Predefined view reflecting data from the Connection table with information such as Connection ID, Source and Destination Nodes ID and Operative State, etc.
- **VoIP Peer view.** Predefined view reflecting data from the VoIP Peers table with information such as ID, name and type.
- **Routing rules view.** Predefined view reflecting data from the Routing Rules table (ID, Name, Admin state and Routing Group reference).
- **Routing groups view.** Predefined view reflecting data from the Routing Group table (ID and Name of Routing Group)
- **Node Statistics.** Predefined view reflecting data from the Node Statistics table (such as Routing Attempts, alternative routing attempts, failed routing attempts, discard routing attempts, destination calls, transient calls, etc.). Only the last week's statistics are displayed.
- **Connection Statistics.** Predefined view reflecting data from the Connection Statistics table (transient calls). Only the last week's statistics are displayed.

- **Peer Connection Statistics.** Predefined view reflecting data from the Peer Connections Statistics table (such as Routing Attempts, alternative routing attempts, failed routing attempts, discard routing attempts, destination calls, etc.). Only the last week's statistics are displayed.
- **Routing Statistics.** Predefined view reflecting data from the Routing Statistics table (such as Routing Rule first match, routing rule second match, routing rule try, routing rule fail, etc.). Only the last week's statistics are displayed.
- **Alarms View.** Predefined view reflecting data from the Alarms table which includes all ARM alarms field columns (such as Name, Source, Severity, Date, Description, etc.).

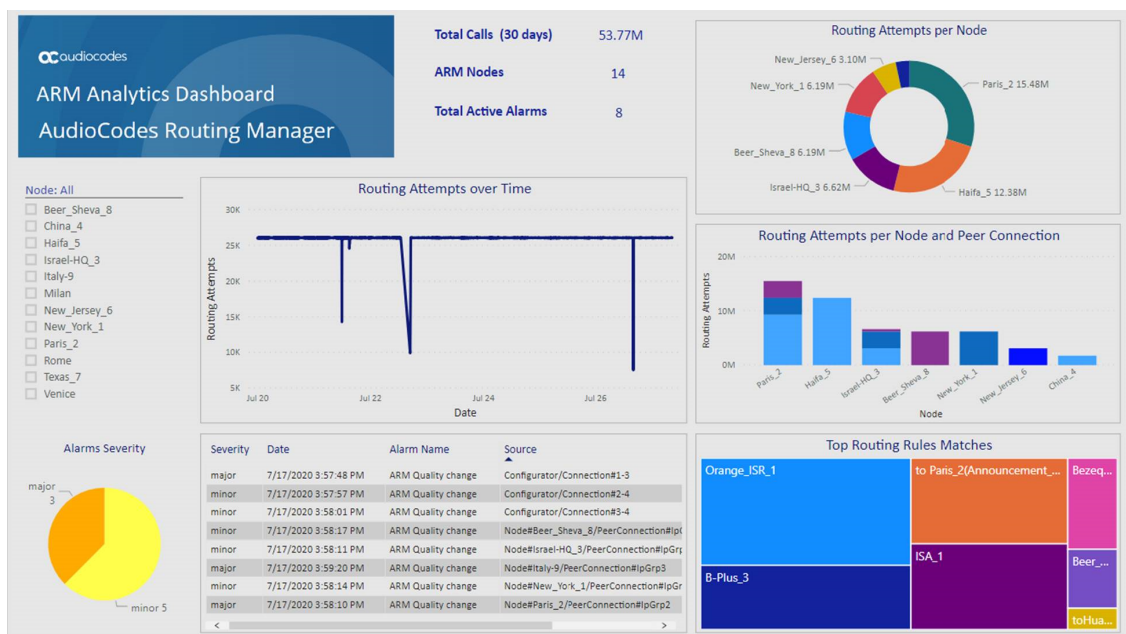
Examples of ARM Dashboard that can be Achieved using Analytics

Here are some examples of what can be achieved with the ARM's new analytics feature. For these examples, Microsoft's Power BI data visualization tool was connected to the ARM database. [Other external tools besides this tool can be used]. The tool provided these interactive visualizations and business intelligence capabilities.

The Dashboard example below shows the total # of calls handled over 30 days, the # of ARM nodes and the total # of active alarms.

- The left side of the screen shows the filter and a pie chart showing Alarms Severity.
- The middle of the screen shows routing attempts over time and a breakdown of the active alarms.
- The panes on the right side of the screen show (top to bottom) a pie chart indicating # of routing attempts per node, a bar chart indicating # of routing attempts per node and peer connection, and top Routing Rule matches.

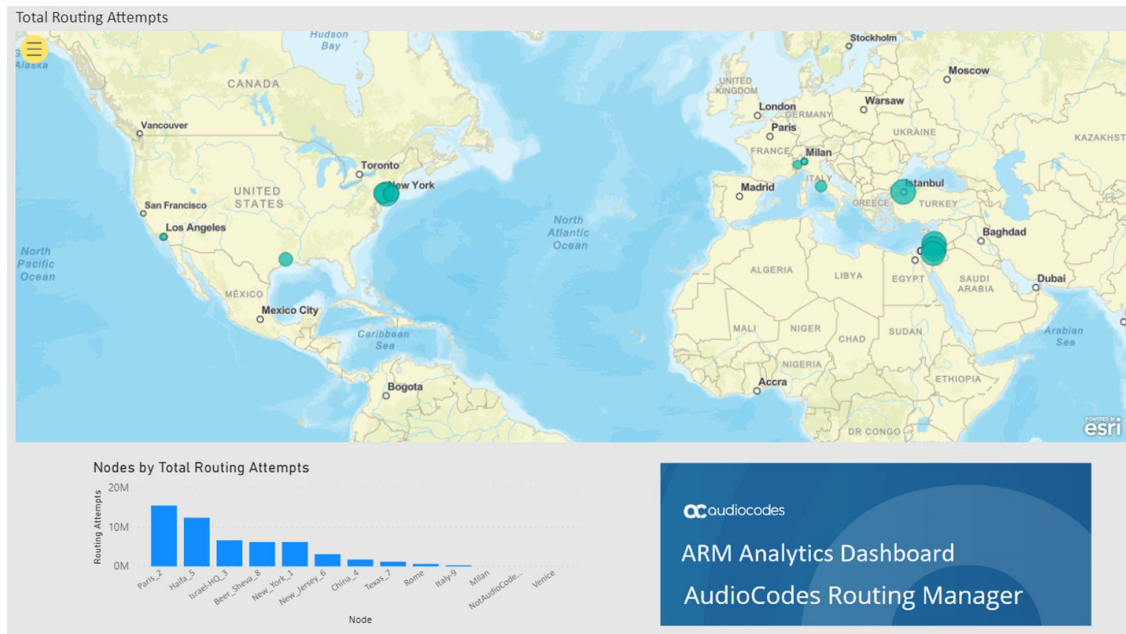
Figure 5-19: Dashboard Example 1



The Dashboard below shows how the total # of routing attempts was distributed across the nodes in the network.

- Smaller green balloons = smaller # of routing attempts
- Larger green balloons = higher # of routing attempts

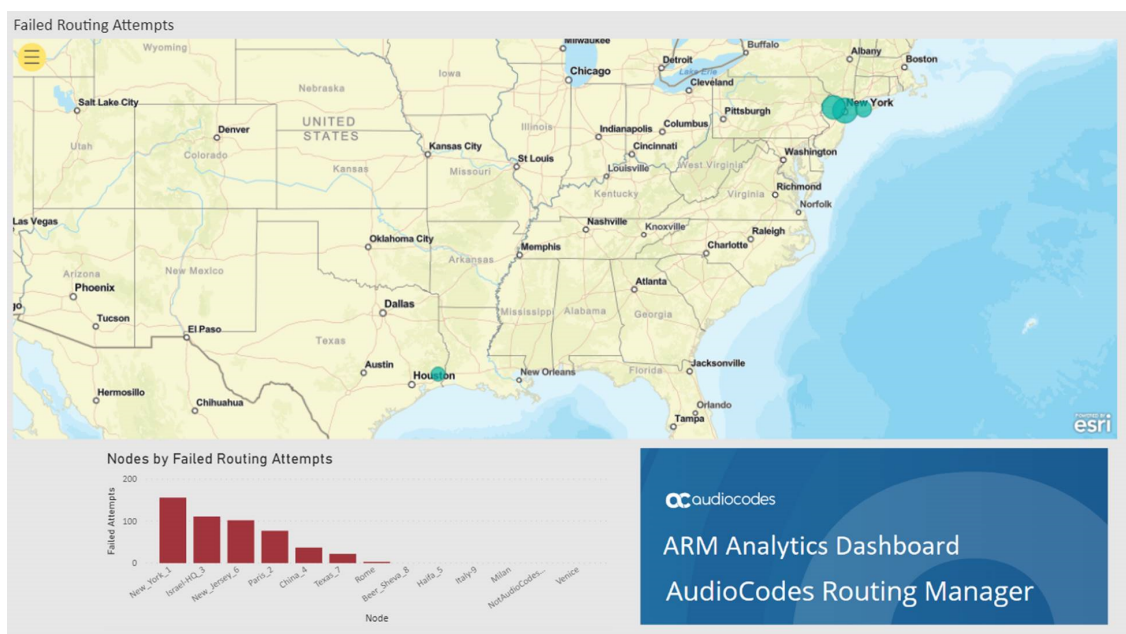
Figure 5-20: Dashboard Example 2



The Dashboard below shows how the total # of failed routing attempts was distributed across the nodes in the network.

- Smaller green balloons = smaller # of failed routing attempts
- Larger green balloons = higher # of failed routing attempts

Figure 5-21: Dashboard Example 3



6 Performing User-Related Administration

The Users page in the ARM allows the ARM operator to:

- Add users to the ARM (see [Adding a User Not Listed in an AD to the ARM](#) on the next page)
- Incorporate users into the ARM from a File Repository (see [Incorporating Users into the ARM from a File Repository](#) on page 128)
- Add Users Groups to the ARM (see [Adding Users Groups to the ARM](#) on page 136)
- Determining the total number of users (see [Determining Total Users Count](#) on page 126)
- Exporting ARM users to csv (see [Exporting ARM Users to CSV File](#) on page 127)
- Add an LDAP Server to the ARM (see [Adding an LDAP Server to the ARM](#) on page 141)
- Add an Azure AD Server to the ARM (see [Azure AD as a Source for Users in the ARM](#) on page 350)
- Add a Property Dictionary to the ARM (see [Adding a Property Dictionary to the ARM](#) on page 150)

The ARM supports up to four million users. They can be inserted from different sources:

- File Repositories (typically the most common source for a high number of users – more than 1 million)
- Multiple Active Directories (LDAPs) – up to 1 million users per LDAP
- Local users

All generic ARM features related to user management are also supported for high numbers of users though some actions like filtering, search, users group creation, users export to csv file, etc., can take longer to perform.

By default, the ARM supports up to 1 million users. To purchase a license for an extended number of users, operators should contact AudioCodes Support.



- An operator who manages more than 1 million users will have to deploy ARM Routers with extended memory – 16 GB (instead of the standard 8 GB). High numbers of users requires more memory for using ARM Routers maps for real-time user-based routing.
- The ARM Routers memory extension should be applied at a VM level prior to applying a Feature Key with an extended number of users.
- In the case of adding a new ARM Router to the ARM with an extended number of users (more than 1 million), the Router's VM should have 16 GB memory.



If the Origin (source) of users is LDAP Server/Active Directory and the operator manages more than 1 million users, the users should be divided among several LDAP servers where each LDAP hosts up to 1 million users.

Adding a User Not Listed in an AD to the ARM

Enterprises have databases in which employee information is stored. Enterprises generally store information related to employees on Microsoft's Active Directory (AD) server. The ARM supports multiple ADs. The ARM's user administration feature can connect to an AD and import user calls routing related information into the ARM database. Operators can alternatively add users who are not listed in an AD database, to the ARM database.

Enterprises that store their users in another format (Excel, for example) can also import these users into the ARM as local ARM users using the ARM northbound REST API. For more information and assistance, contact AudioCodes Professional Services.

To view the users listed in the AD database and their AD attributes, you need to provision the LDAP server as shown under [Adding an LDAP Server to the ARM](#) on page 141.

➤ **To add a user who is not listed in an AD database, to the ARM database:**

1. In the ARM's Users page, click the **Users** tab under the Users menu.

Figure 6-1: Users Page – Users tab

NAME	ORIGIN	AD GROUPS	COUNTRY	OFFICE PHONE	DISPLAY NAME	DEPARTMENTCODE	MS LYNC LINE URI	CHATTERER	TALKERS
AUDC AD	AUDC AD			+97238764454	QACOM7		+97238764454tel+97...		
AUDC AD	Belgium+080078301	Belgium					+080078301tel+0800...		
AUDC AD	+5569082847	HelpDesk-SG					+5569082847tel+556...		
AUDC AD	+97238764572	Guest F-3					+97238764572tel+97...		
AUDC AD	USA+173265346500US...	USA					+173265346500tel+17...		
AUDC AD	+97238764108	Ilanit Sharon 2					+97238764108tel+97...		
AUDC AD	+97238764059	Carmel meeting room					+97238764059tel+97...		
AUDC AD	+97238764231	IT Application					+97238764231tel+97...		
AUDC AD	+97238764145	SKT					+97238764145tel+97...		
AUDC AD	+17326534646	Lync - UM on office 36...					+17326534646tel+17...		
AUDC AD	+97238764453	QACOM6					+97238764453tel+97...		
AUDC AD	+97238764699	RNA-LAB					+97238764699tel+97...		
AUDC AD	+5002	NJ-Somerset-Conf-RM					+5002tel+5002		
AUDC AD	+97238764010	Visitor-B5					+97238764010tel+97...		
AUDC AD	+19192873492	RTP-Alcove-2					+19192873492tel+19...		
AUDC AD	SouthAfrica+0800997...	South Africa					+0800997331tel+080...		
AUDC AD	Austria+0800293821L...	Austria					+0800293821tel+080...		
AUDC AD	+97238764203	LAB3254					+97238764203tel+97...		
AUDC AD	+8675583235280	Tony Li					+8675583235280tel+...		
AUDC AD	+97238764581	ACVR02					+97238764581tel+97...		
AUDC AD	+97238764444	voicem					+97238764444tel+97...		
AUDC AD	+97238764582	QACOM1					+97238764582tel+97...		
AUDC AD	Netherlands+3136346...	Netherlands					+31363461220tel+31...		
AUDC AD	Voordeur						+31363461221tel+31...		
AUDC AD	+17326522168	Israel FAE_1					+17326522168tel+17...		

2. Click **Add**.

Figure 6-2: User Details

The screenshot shows a 'USER DETAILS' dialog box with the following fields:

- User name:
- Origin:
- Groups:
- Contact details section (indicated by a horizontal line):
 - AD groups:
 - Country:
 - Office Phone:
 - Display Name:
 - Department:
 - MS Lync Line URI:
 - Talkers:
- Buttons: OK, Cancel

User Details are taken from the Property Dictionary screen. If a property is added in the Property Dictionary screen, it appears here. To add a property, see [Adding a Property Dictionary to the ARM](#) on page 150.



If an LDAP server is provisioned, the ARM automatically brings users from it to the ARM database, and displays them in the GUI under the **User** tab.

3. Click **OK**; the user is added and displayed in the Users page. To view and / or edit, select the user's row and click **Edit**; the screen shown below is displayed.

Figure 6-3: User Details

USER DETAILS [X]

User name: bobbyw

Origin: AUDC AD

Groups: China,Israel

Contact details

Country: China

Office Phone: +8675583235280

Display Name: Bobby Wu

Department: RIC - R&D

MS Lync Line URI: +97239764915[tel:+97239764915]

Talkers:

mail: Yusheng.Wu@audiocodes.com

[OK] [Cancel]



Grayed fields in the figure above indicate that the origin of this user isn't ARM and cannot be edited. Non-grayed fields indicate that the origin of the user is ARM and can be edited.

Determining Total Users Count

In the Users page, the **Total number of users** button allows operators to display the overall number of users in the ARM.

Figure 6-4: Total users count

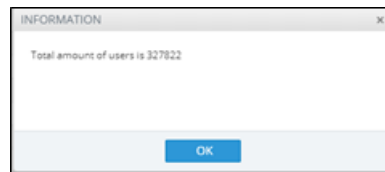
[Add] [Edit] [Delete] **[Total users count]** [Export] [Refresh]

NAME	ORIGIN	AD GROUPS



The total number of users is shown even if there are filters applied.

Figure 6-5: Total users count - Information



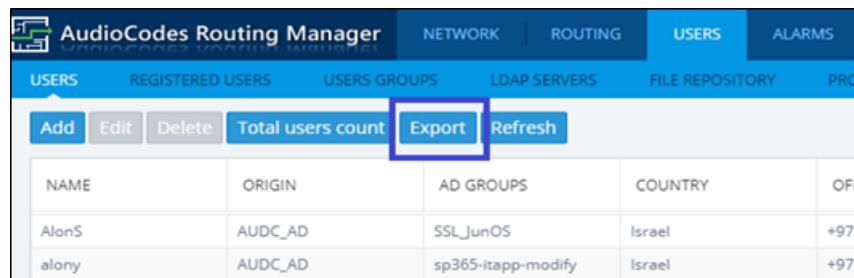
Exporting ARM Users to CSV File

The ARM gives operators the capability to export users to a Comma-Separated Values (CSV) file. The export users action is accessible from an **Export** button in the Users page and can be applied either to exporting a set of users (or all users) from the ARM's Users page or to exporting users belonging to a specific Users Group.

➤ To export users from the Users page (all users or a filtered set of users):

- Open the Users page (**Users > Users**) and locate the button.

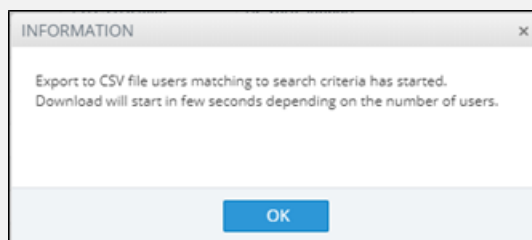
Figure 6-6: Export



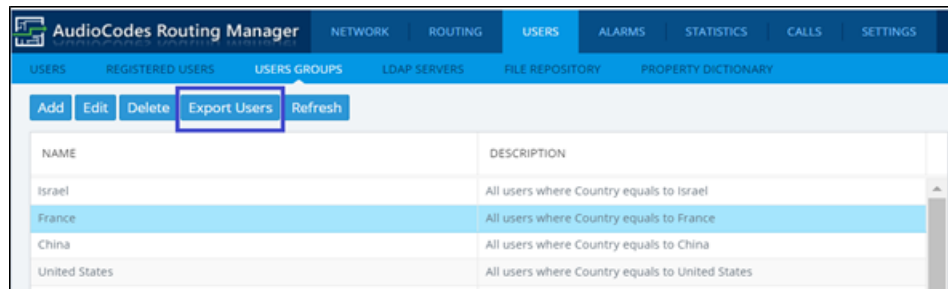
Either export all users or a subset of users filtered by name, Origin or text search filter. For filtered users, first search the users and only then click the **Export** button. For export all users, the search should be cleared.



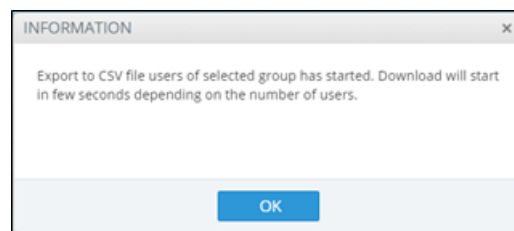
Export of users can take some time if the number of users in the ARM is high (millions) and is performed in the background, as indicated by the following notification displayed:



2. Export users of a specific Users Group - in the Users Groups page (**Users > Users Groups**).
Select a specific Users Group:

Figure 6-7: Export users of a specific Users Group

Only those users belonging to the selected group will be exported to the file. Export of users is performed in the background, as indicated by the following notification displayed:

Figure 6-8: Notification

In both cases, the produced CSV file includes the header in the first line with all the users' property names. The CSV file will include all the Property Dictionary fields defined in the ARM even if they are irrelevant or empty for a specific user.

Figure 6-9: CSV File - header in first line

	A	B	C	D	E	F	G	H	I
1	Id	Name	AD groups	Country	Office	Pho	Display	N	departme
2	9192823	israelz	# All 012 v	Israel	9.72E+10	Israel	Zusr	R&D - Har	tel:+97239764089
3	9192824	remcow	# All ACS#	All Support#	EU FAE	Remco	W	Marketing	tel:+31365461234
4	9192825	WalterV	# All ACS#	Netherlands		Walter	Van Schaik		tel:+31365461226
5	9192826	duncanj	# All ACS#	Oracle Israel-From#	I	Duncan	Jenkins		tel:+31365461213
6	9192827	stevenk	# Abroad#	All ACS#	All Sales	NV	Steven	Kn	Marketing tel:+31365461216

It's important to emphasize that when producing the CSV file, the ARM adds a column with User ID. This is the internal unique ID of the user. This information helps the operator to develop proprietary scripts for users management based on the official ARM REST API. Operators can export either all users or a subset of the users (filtered using the GUI) and use the produced CSV to easily access the users information by unique ID via the REST API in order (for example) to update a specific attribute.

The property values in the derived CSV file are the original vales and not normalized values (even if normalization was applied when they were added from LDAP or File Repository).

The produced CSV can be used for backup /reporting or can be loaded as a file though the File Repository feature.

Incorporating Users into the ARM from a File Repository

Operators can incorporate users into the ARM from a File Repository.



Operators can also incorporate users from the Active Directories (LDAP users) or local users, where all users not sourced and synchronized with any Active Directory are automatically considered to be local ARM users regardless if they're added to the ARM database using the ARM GUI or using the REST API based script from the customer's file or database.

File Repository is a valid source of ARM users information for loading and managing of ARM users from an external customer's CSV files.

➤ **To incorporate users into the ARM from File Repository:**

1. Open the File Repository page (**Users > File Repository**).

Figure 6-10: File Repository

STATUS	NAME	NUMBER OF USERS	DESCRIPTION	LAST UPDATE
✓	reg_users	4000000	4000000 users inserted successfully	15-jun-20 17:06:02
✓	register_routing	0	20 users were not inserted due to licensed nu...	24-jun-20 10:45:35

2. In this page you can Add, Edit, Delete or Refresh a File Repository for ARM users. The principle of managing File Repository is similar to that of LDAP server. ARM allows a flexible CSV file format in terms of fields / properties, and provides capability to map it to the previously defined ARM users dictionary. When managing users with File Repository, you must choose the unique field of the user (usually, 'Name') for unique identification of a user within the File Repository. ARM supports incrementally adding users to an existing File Repository (using the **Edit** feature).



- Automatic synchronization of users with an existing File Repository is not supported.
- Update of an existing user (as part of incremental file) is not supported.
- If the new CSV file contains an existing user (per a unique field defined by the operator), it will be treated as a duplication and will not be added to the ARM during the update.

➤ **To add a new File Repository:**

1. In the File Repository page, click **Add**.

Figure 6-11: File Repository Settings

2. Configure the File Repository Settings screen as follows:

- **Name.** Mandatory identification of the File Repository within the ARM.
- **Unique Property.** One of the properties of the users dictionary defined in the ARM which can be treated as unique and can be seen as key for a user sourced by a specific Repository. Note that the ARM software validates this field uniqueness and will not allow duplicated entries. When adding a new File Repository, the operator is allowed to choose one of the user dictionary attributes to be treated as a unique property. Typically, the 'Name' setting is used.
- **Field delimiter.** The delimiter used in the source CSV (can be ',', ';' or '|').
- **File has headers in the first line.**
 - ◆ If the CSV file has headers in the first line, check (select) this option. In this case, the first line will be taken so you can map the attributes by the column names as defined in the first line of the file.
 - ◆ If the CSV file *does not have* headers in the first line, clear (deselect) this option. In this case, you can map the properties by the columns location - 'column 1', 'column 2'.

It is highly recommended to have headers in the first line of the CSV file; it will be easier for you to map the properties by the headers as defined in the first line.

Following is an example of a CSV file with defined headers in the first line. These column names will be used by the ARM to map information to the ARM-defined Property Dictionary.

Figure 6-12: CSV file with defined headers in the first line

1	Name	Country	Office Phone	Display Name	MS Lync Line URI	Registration	Chatterer	PWD	PBX IPAddr	*MS Lync	*Office Phone:972-111
2	register_1	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_1	password	172.17.133.5			
3	register_2	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_2	password	172.17.133.5			
4	register_3	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_3	password	172.17.133.5			
5	register_4	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_4	password	172.17.133.5			
6	register_5	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_5	password	172.17.133.5			
7	register_6	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_6	password	172.17.133.5			
8	register_7	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_7	password	172.17.133.5			
9	register_8	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_8	password	172.17.133.5			
10	register_9	register_uri	9.72E+09	Disp_registel:+9723C	TRUE	register_9	password	172.17.133.5			

- **Upload file.** Allows you to upload the CSV file from the local file system.



The CSV file must not exceed 1 GB in size.

3. Configure the File Repository Properties screen (similar to the parallel tab of LDAP Properties mapping) as follows:

Figure 6-13: File Repository Properties

PROPERTY	FILE MAPPING	ATTRIBUTE NORMALIZATION
Name	Name	
MS Lync Line URI	MS Lync Line URI	default lync number normaliza...
Display Name	Display Name	
PWD	PWD	
PBX IPAddr	PBX IPAddr	
Country	Country	
Office Phone	Office Phone	972-111
Chatterer	Chatterer	
Registration_Users	Registration_Users	

- **Property.** Name and all the other properties of the ARM users dictionary.
- **File Mapping.** Mapping from the CSV file of the File Repository.

- ◆ If the option **File has headers in the first line** is checked, the file mapping options will be taken from the header line of the CSV file.
- ◆ If the option **File has headers in the first line** is unchecked, the file mapping options will be column 1, column 2, etc., meaning that property mapping options will be by the location of the property in each line in the file.
- **Attribute Normalization.** Information taken from the File Repository can be normalized using predefined Normalization Groups. The original values are saved in the database and are normalized when used (displayed in the GUI, sent to Routers for a routing match, etc.). This is done in the same manner as for information taken from Active Directory.

➤ **To edit a File Repository:**

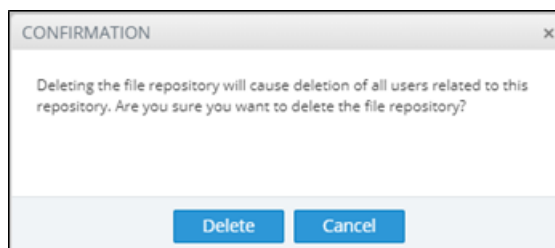
Editing of the File Repository is typically performed to add an incremental bulk of users to an existing File Repository. The ARM allows adding a new file with users which will be handled according to initial File Repository definitions and Properties mapping (provided when adding the File Repository). For this reason, the operator is not allowed to change File Mapping, attribute normalization or the Unique property of the File Repository. The structure of the CSV file and the File Repository is defined by the initial Add action. The configuration that can be changed during the edit are:

- **Name.** Will change the name of File Repository even for existing users who were sourced by that File Repository.
- **Delimiter.** Delimiter used in the CSV file to be added (can be different from the initial one).
- **Upload file.** The new file with users to be incrementally added to the existing File Repository. The file name can be different from the initial one.

➤ **To delete the File Repository:**

Deleting the File Repository causes all users related to it to be deleted. The ARM GUI displays the following warning to the operator:

Figure 6-14: Deleting a File Repository





- The length of time it takes to delete a File Repository depends on the number of users defined in the system.
- It's impossible to delete in bulk a subset of users of a File Repository, such as all users added by a specific bulk (update).
- In the Users page, operators can select users sourced by a specific File Repository.
- Multiple File Repositories are supported and can be synchronized with the ARM separately.
- Each File Repository can have different fields, different mapping to the ARM users dictionary and delimiters. The ARM handles each File Repository separately (the same way as different LDAP servers).

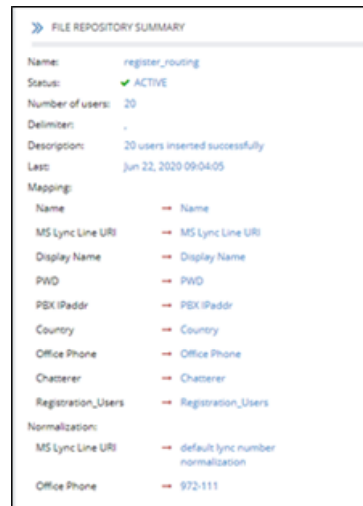
The File Repositories page displays the following information for each File Repository:

- **Status.** Either:
 - ◆ 'Active' (when all valid users are already accepted by the ARM, have become a part of the ARM users database and their information can be used for routing).
 - ◆ 'Synchronizing' (the ARM is processing the file, that is, still reading from the file and adding valid users from the file).
 - ◆ 'Error' (in the case that something is wrong with the file and the ARM fails to read its contents)
- **Name.** Name given to file repository during add/edit
- **Number of users.** The total number of users added from the Repository File.
 - ◆ If you delete a user related to the Repository File with a script using REST, the number will be updated to reflect the deletion.
 - ◆ If you delete a user of the File Repository from the GUI, the number will be updated to reflect the deletion.
- **Description.** Essential information to help the operator successfully manage the File Repository. For example, it will reflect the number of users who were successfully added or the reason of failure if they weren't successfully added (such as duplication). This information refers to the last update only.
- **Last Update.** The time of the last update for a specific repository.

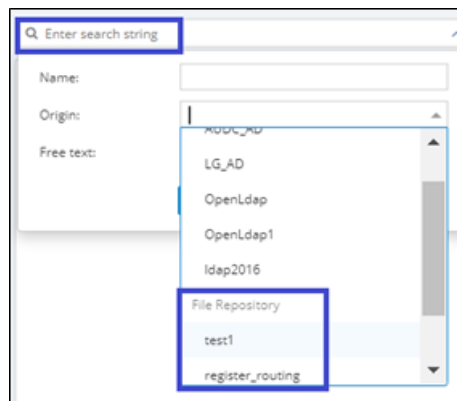
Figure 6-15: Last Update

Add Edit Delete Refresh				
STATUS	NAME	NUMBER OF USERS	DESCRIPTION	LAST UPDATE
✓	test1	20	20 users were not inserted due to duplication	14-jun-20 11:58:41
✓	register_routing	20	20 users inserted successfully	22-jun-20 09:04:05
✗	Temporary/file	0		

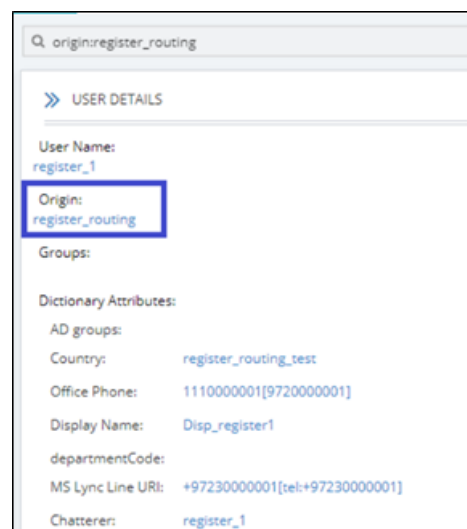
When a File Repository is selected, the basic information summary for this repository is displayed on the right side of the page:

Figure 6-16: File Repository Summary

In the Users page (**Users > Users**), you can filter users sourced from a specific File Repository (in same way as with the LDAP):

Figure 6-17: Filter Users

The indication of a specific File Repository as a source of user information is displayed as part of the user's information:

Figure 6-18: File Repository Origin (Source)

Viewing Registered Users in the ARM

The Registered Users page lets operators view the SBC registered users that were added to the ARM as shown in [Adding Registered Users to the ARM](#) on page 191. After SBC registered users are added to the ARM, the ARM will be capable of performing call routing based on SBC user registrations. When defining a Routing Rule, operators will be able to route calls to SBC registered users (see [Adding a New Routing Rule](#) on page 268). The destination to which to route the call will depend on where - which SBC - the user performed the registration. In the Routing Rule definition, operators will select the appropriate routing condition, namely, that the call destination is an SBC registered user.

➤ **To view SBC registered users added to the ARM:**

1. After adding SBC registered users to the ARM, open the Registered Users page (**Users > Registered Users**).

Figure 6-19: Registered Users

USERS REGISTERED USERS USERS GROUPS LDAP SERVERS PROPERTY DICTIONARY			
Refresh			
USER	HOST	NODE	PEER CONNECTIONS
101	1.1.1.1	New_York_1	IpGrp3
102	1.1.1.1	New_York_1	IpGrp3
103	1.1.1.1	New_York_1	IpGrp3
104	1.1.1.1	New_York_1	IpGrp3
105	1.1.1.1	New_York_1	IpGrp3
106	1.1.1.1	New_York_1	IpGrp3
107	1.1.1.1	New_York_1	IpGrp3
108	1.1.1.1	New_York_1	IpGrp3
109	1.1.1.1	New_York_1	IpGrp3
110	1.1.1.1	New_York_1	IpGrp3
111	1.1.1.1	New_York_1	IpGrp3
112	1.1.1.1	New_York_1	IpGrp3
113	1.1.1.1	New_York_1	IpGrp3
114	1.1.1.1	New_York_1	IpGrp3
115	1.1.1.1	New_York_1	IpGrp3
116	1.1.1.1	New_York_1	IpGrp3
117	1.1.1.1	New_York_1	IpGrp3
118	1.1.1.1	New_York_1	IpGrp3

2. Click the **Refresh** button.
3. Use the following table as reference:

Table 6-1: Registered Users

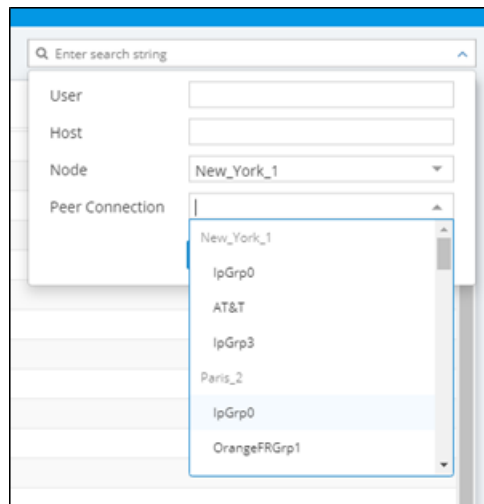
Column	Explanation
User	Displays the SBC registration number of the user.

Column	Explanation
Host	Displays the IP address of the Node (SBC) in which the user was registered. Each Node (SBC) has its own registered users.
Node	Displays the name of the Node (SBC) in which the user was registered.
Peer Connections	Displays the name of the Peer Connection in which the user was registered.

➤ **To view registered users from a specific Node or Peer Connection:**

- In the Registered Users page, use the 'Enter search string' filter.

Figure 6-20: Viewing Registered Users from a Specific Node or Peer Connection



This feature allows network administrators to select and view only users registered with a specific node (SBC/Gateway) and/or Peer Connection (IP Group) (for example). The feature facilitates quick access to information by excluding unwanted information from the page.

Adding Users Groups to the ARM

You can define Users Groups by defining a set of criteria in the user properties. The ARM automatically associates users with the defined Users Group, based on the conditions you define. You can then use the Users Groups in your Routing Rules as match conditions. Each Users Group has one 'Dialable Number' attribute. When a route request is received with a source or destination URI matching the group's 'Dialable Number' property for one of the users in the group, the Routing Rules with this source or destination Users Group are matched.

A Users Group can have a single attribute condition or a combination of attributes conditions. For a user to be a part of the Users Group, all the conditions must be matched. A single condition can have a set of values to compare to. If any of the values of the condition are matched, the condition is considered a match.

Example: You can define a Users Group where the 'Dialable Number' attribute is 'Mobile phone number' and the conditions are Country equals Germany and Department equals Marketing or Sales.

➤ **To add a Users Group:**

1. In the Users page, click the **Users Groups** tab.

Figure 6-21: Users Groups

USERS REGISTERED USERS USERS GROUPS LDAP SERVERS PROPERTY DICTIONARY	
Add Edit Delete Refresh	
NAME	DESCRIPTION
Israel	All users where Country equals to Israel
France	All users where Country equals to France
China	All users where Country equals to China
United States	All users where Country equals to United States
Reception desk	All users where departmentCode contains Human and Country equals to Israel
Shabtai_Special	All users where Display Name contains Shabtai
Imp. People	All users where departmentCode contains Management
Chatterers	All users where Chatterer equals to True

2. Click **Add**.

Figure 6-22: User Group Details

USER GROUP DETAILS

Name *

Dialable *

PROPERTIES

USERS

+


-

OK

Cancel

3. Configure the details using this table as reference.

Table 6-2: User Group Details

Setting	Description
Name	Enter a name for the group for intuitive future reference.
Dialable	From the drop-down menu, select one of the Dialable Number properties. This is the user's property that is compared to the received source or destination URI to determine if the route request is from/to one of the users in this User Group. Example: 'Office phone number'.
Attribute Name	Click  and from the left field's drop-down menu, select a user attribute according to which the user will be associated with the group. Example: Country. Click the button again to add more attributes. All attributes must match for the user to be a member of the group.
equals / not equals contains / not contains	From the right field's drop-down menu, select the operation to be used to define the criterion.
Enter values here	Enter a value for the attribute, according to which the user will be associated with the group. Example: Sweden. Press enter to add more values. At least one of the values must match for the attribute to be considered a match.

➤ **To edit a Users Group:**

1. In the Users Groups page, select the user group to edit and then click **Edit**; the User Group Details screen opens under the **Properties** tab.

USER GROUP DETAILS

Name *

France

Dialable *

Office Phone

PROPERTIES

USERS

Country

Country

EQUALS

EQUALS

Enter values here

France

+

OK

Cancel

USER GROUP DETAILS

Name *

Dialable *

PROPERTIES **USERS**

Enter search string

NAME	ORIGIN	AD GROUPS	COUNTRY	OFFICE PHO
ChristopheP	AUDC_AD	sp365-Sales-Read	France	+3363845069
remib	AUDC_AD	sp365-Sales-Read	France	+3367340887
sergel	AUDC_AD	Sp365-France-modify	France	+3364218150

Items 1-3 items of 3

OK Cancel

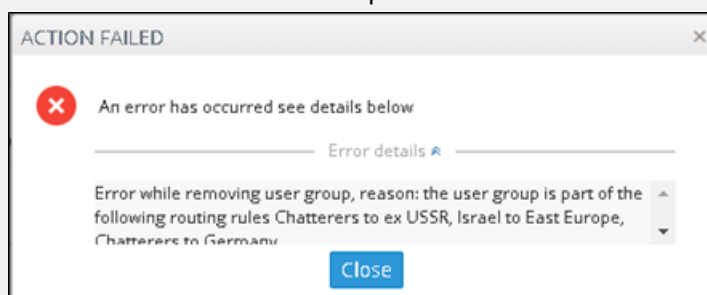
2. Edit using the preceding table as reference and then click the **Users** tab; the screen shown above opens allowing you to view the users who are associated with the group.

➤ **To delete a Users Group:**

- In the Users Groups page, select the user group to delete and then click **Delete**.



An error message is displayed if you attempt to remove a group with which routing rules are associated. For example:



The message indicates the names of the routing rule/s associated with the group so it's easy to find and remove them before deleting the group.

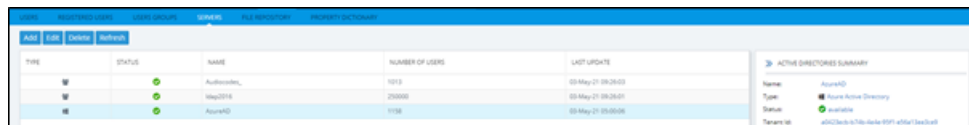
Adding an LDAP Server to the ARM

Network administrators can add multiple Active Directories (ADs) to the ARM database using LDAP protocol.

➤ **To add an LDAP server:**

1. In the Users page, click the **Servers** tab.

Figure 6-23: Users Page – Servers tab



TYPE	STATUS	NAME	NUMBER OF USERS	LAST UPDATE
AD	●	Authentication	1013	03-May-21 09:28:03
AD	●	MyAD18	250000	03-May-21 09:28:01
AD	●	AcmeAD	1138	03-May-21 09:00:08

ACTIVE DIRECTORIES SUMMARY
Name: AcmeAD
Type: Active Active Directory
Status: Available
Tenant ID: 450226c6-87b6-4c0a-b077-4d74a73ad0a0

2. Click **Add**, and from the popup menu, select the **LDAP Server** option.

Figure 6-24: LDAP Server Settings - LDAP Settings

LDAP SERVER SETTINGS

LDAP SETTINGS | LDAP PROPERTIES

GENERAL

Name: *

Host: *

Port:

Base object:

Search filter:

Bind DN:

Password: *

Page size:

Test connectivity

SSL CONFIGURATIONS

Enable SSL: ☐

Certificate file:

UPDATES

OK **Cancel**

3. Configure the settings using this table as reference.

Table 6-3: LDAP Server Settings - LDAP Properties

Setting	Description
Name	Enter an intuitive name for the LDAP server.
Host	IP address or DNS name of the LDAP server on which the AD is located.
Port	The LDAP port. Default: 389
Base Object	Consult your IT manager responsible for the Active Directory in your

Setting	Description
	<p>enterprise. The setting defines the full path (DN) to the object in the AD tree where the user's information is located. The valid value is a string of up to 256 characters. Example (read from right to left):</p> <p>ou=Users;ou=APC;ou=Israel;ou=as;dc=corp;dc=as;dc=com</p> <p>The DN path is defined by the LDAP names OU (organizational unit) and DC (domain component).</p>
Search Filter	An LDAP search filter used when fetching the users from the LDAP server under the base DN. The default is 'objectClass=user'.
Bind DN	<p>The DN (distinguished name) or username of the user used to bind to the LDAP server.</p> <p>For example: ldap_bind@corp.audiocodes.com</p>
Password	Defines the LDAP password used to connect.
Page size	The ARM allows operators to control the page size retrieved from the LDAP server. This may help to reduce some of the strain from the ARM or from the LDAP server. It may also help in some cases where the LDAP server doesn't return all the users defined in it. Note the final value is controlled by the LDAP server itself and cannot be defined above the value configured in the LDAP server. Configure a value in the range 1-10000. Default: 1000.
Test Connectivity	Click the button to test the connectivity between the ARM server and the AD server.
SSL Configurations	
Enable SSL	Enables or disables the connection over SSL. Default: Disable. When disabled, communications with the AD server will be open, i.e., unencoded/unencrypted. When left unchanged at the default; the Browse button adjacent to 'Certificate File to Upload' will be unavailable; when enabled, the Browse button becomes available.
Certificate file	Enables verification that it is the AD server and no other entity that is communicating with the ARM server. Allows you to browse for a root certificate. When the AD server then sends a certificate, the ARM server uses the root certificate to verify that it is the AD server and no other entity on the other side. Following verification, communications are SSL-encoded.
Updates	

Setting	Description
Check for updates every <i>n</i> minutes	Defines how frequently the ARM server checks the AD server for updates. Note that during the update, the ARM only obtains new AD users or relevant user information updates (only the delta). Default: Every 5 minutes
Perform full update every <i>n</i> days at	Defines how frequently the ARM server performs a full update from the AD server. Note that a full update is mainly required to remove users deleted from the organization's AD (this information cannot be obtained by an AD update). Default: Every day
At	At what time of day the full synchronization (in which the ARM server performs a full update from the AD server) will occur. Default: 0:0, i.e., midnight. Use the arrows to navigate to and select a time. In the preceding figure, the sync will occur every 10 days (frequency) at 00:00 hours (midnight). Default: 03:00 a.m.
Updates timeout	If the AD server doesn't answer within the period configured, the ARM server determines that the AD server is disconnected and a refresh is sent. Default: 60 minutes.

4. Click **OK** and then click the **LDAP Properties** tab.

Figure 6-25: LDAP Server Settings - LDAP Properties

LDAP SERVER SETTINGS

LDAP SETTINGS LDAP PROPERTIES

PROPERTY	LDAP MAPPING	ATTRIBUTE NORMALIZATION
8xx	<input type="text" value=""/> × ▾	8 to mobile manip × ▾
Country	co × ▾	<input type="text" value=""/> ▾
Office Phone	telephoneNumber × ▾	<input type="text" value=""/> ▾
AD groups	memberOf × ▾	<input type="text" value=""/> ▾
Display Name	displayName × ▾	<input type="text" value=""/> ▾
MS Lync Line URI	msRTCSIP-Line × ▾	default lync number norm: × ▾
Department	department × ▾	<input type="text" value=""/> ▾
PBX	<input type="text" value=""/> × ▾	<input type="text" value=""/> ▾
mail	mail × ▾	<input type="text" value=""/> ▾
email	<input type="text" value=""/> × ▾	<input type="text" value=""/> ▾
Talkers	<input type="text" value=""/> ▾	<input type="text" value=""/> ▾
mobile phone number	<input type="text" value=""/> ▾	<input type="text" value=""/> ▾
credential	<input type="text" value=""/> ▾	<input type="text" value=""/> ▾
EC	<input type="text" value=""/> ▾	<input type="text" value=""/> ▾
EyeColor	<input type="text" value=""/> ▾	<input type="text" value=""/> ▾

OK Cancel



- Property fields that display LDAP mappings are synced from the LDAP server
 - ✓ From the property field's drop-down, select the property to map to the LDAP server -OR- enter the first letter or number in the name of the property and if necessary enter the second as well; the field is automatically populated (filled). LDAP schema typically include multiple attributes so this feature makes it easy for network operators to find an attribute.
- Property fields not displaying LDAP mappings can be mapped locally, in the ARM:
 - ✓ Leave the property's field empty and then in the Users page (**Users > Users**) open a user's User Details screen and edit the property there according to requirements (see [Adding a User Not Listed in an AD to the ARM](#) on page 124)
- In the Property Dictionary page you can define a new property or edit an already defined property (see [Adding a Property Dictionary to the ARM](#) on page 150)
- Each dialable Dictionary property has a default normalization which is performed on top of the defined normalization, if a defined normalization exists. This default normalization removes white spaces, minuses, semicolons and parentheses. The default normalization can be changed if needed. Contact your AudioCodes representative if you need to change it.

➤ **To attach a Normalization Group (Rule) to an LDAP property:**

1. Select the row of the LDAP property to which to attach a Normalization Group.
2. From the property's Attribute Normalization drop-down menu, select a Normalization Group. See [Adding a Normalization Group](#) on page 198 for information on how to configure a Normalization Group.
3. Click **OK**.

➤ **To view the AD summary:**

- In the Users page, click the **LDAP Servers** tab and select the AD whose summary you want to view.

Figure 6-26: Users Page – LDAP Servers tab – AD Summary

Users			
REGISTERED USERS USERS GROUPS LDAP SERVERS PROPERTY DICTIONARY			
Add Edit Delete refresh			
STATUS	NAME	NUMBER OF USERS	LAST UPDATE
✓	AUDC AD	646	August 14, 2019
✓	LG_AD	249348	August 14, 2019
✓	Openldap	1	August 14, 2019
✓	Openldap1	1	August 14, 2019
✓	Openldap_new	2	August 14, 2019
✓	AUDCrm	2	August 14, 2019

» ACTIVE DIRECTORIES SUMMARY	
NAME:	AUDC AD
STATUS:	Available
HOST:	adtest01.corp.as.com
PORT:	636
USERS:	646
SSL ENABLED:	true
CERTIFICATE:	Subject: CN=AudioCodes CA, 2016.DC=corp.DC=as.DC=com Issuer: CN=CA.AUDC01.corp.as.com Valid from: Wed Oct 19 22:07:44 IDT 2018 Valid to: Thu Oct 19 22:07:44 IDT 2019 Validity: true ldap.jimob@CORP-AS.COM
DN:	
SEARCH FILTER:	((!(msRTCSIP-User*)(telephoneNumber*))
BASE OBJECT:	dc=corp,dc=audiocodes,dc=com
SYNC:	
EVERY:	5 minutes
LAST:	Aug 14, 2019 16:10:21
FULL SYNC:	
AT:	13:23
EVERY:	1 day
LAST:	Aug 14, 2019 13:23:07
SYNCTIMEOUT:	60 minutes
MAPPING:	
MOBILE:	→ mobile phone
MEMBEROF:	→ AD groups
CO:	→ Country
DEPARTMENT:	→ DepartmentCode
TELEPHONENUMBER:	→ Office Phone
DISPLAYNAME:	→ Display Name
MSRTCSIP-LINE:	→ MS Lync Line URI
NORMALIZATION:	
MSRTCSIP-LINE:	→ default lync number normalization

Table 6-4: Active Directories Summary

Sync	ARM and AD databases synchronization schedule. Displays the synchronization frequency: 1-48, i.e., between once every hour (most frequent) to once every two days (most infrequent).
Last Sync	Displays the last time the ARM and the Active Directory databases were synchronized.
Full Sync	Displays the time (hour and minute) at which to start a full synchronization. Also displays the frequency: 1-7, i.e., between once a day (most frequent) to once a week (most infrequent).
Last Full Sync	Displays the last time the ARM and the Active Directory databases were fully synchronized.

➤ **To edit an LDAP server:**

1. In the Users page under the **LDAP Servers** tab, select the server to edit and click **Edit**.

Figure 6-27: LDAP Server Settings

LDAP SERVER SETTINGS

LDAP SETTINGS LDAP PROPERTIES

GENERAL

Name * AUDC AD

Host * as01.corp.as.com

Port 3268

Base object dc=corp,dc=audiocodes,dc=com

Search filter (|(msRTCSIP-Line=*)(telephoneNumber=*))

Bind DN ldap_bind@CORP.AS.COM

Password

Test connectivity

SSL CONFIGURATIONS

Enable SSL ☐

Certificate file

UPDATES

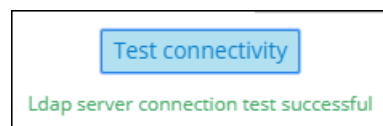
Check for updates every (min) 5

Perform full update every (days) 1

OK Cancel

2. Edit the LDAP Server Settings screen using the parameter descriptions when adding an LDAP server as reference, and then click **Test Connectivity** to test the connection settings.

Figure 6-28: Test connectivity



3. Click the **LDAP Properties** tab; the same screen that opens when *adding* an LDAP server, shown previously, is displayed. Use the parameter descriptions when *adding* an LDAP server, shown previously, as reference.

- For each LDAP property's LDAP Mapping drop-down menu, select a mapping. Properties that have LDAP mappings are synced from the LDAP server. Properties that do not have LDAP mappings are empty and can be configured locally.
- Select the LDAP property to which to attach a Normalization Attribute and then from the property's Attribute Normalization drop-down menu, select a Normalization Group. See [Adding a Normalization Group](#) on page 198 for information about how to configure a Normalization Group.

4. Click **OK**.

After updating an LDAP server, a full sync is started. After a short while (depending on the size and responsiveness of the LDAP server), you can view the updated users in the Users page.

Adding a Property Dictionary to the ARM

The Users page's **Property Dictionary** tab lets the operator administer the Property Dictionary, a set of all the properties that a user can have.

Figure 6-29: Users Page – Property Dictionary tab

PROPERTY DICTIONARY				
NAME	DESCRIPTION	DIALABLE	DISPLAYED IN USERS TABLE	COMBINED
AD groups		x	✓	x
Country		x	✓	x
Office Phone		✓	✓	x
Display Name		x	✓	x
departmentCode	departmentCode	x	✓	x
MS Lync Line URI		✓	✓	x
Chatterer	people who talk too mu...	✓	✓	x
Talkers	people who talk too mu...	✓	✓	x

After adding a property to the dictionary, you can add it to some or all your LDAP servers. Properties added to an LDAP server will automatically be read from the LDAP server. Properties not added can be set locally in the ARM for each user. The Properties from the dictionary can then be used as User Group conditions as well as in 'Policy Studio'.

➤ To add / edit a property:

1. Open the Property Dictionary page (**Users > Property Dictionary**).
2. Click **Add** or **Edit** (after selecting an existing property).

Figure 6-30: Property

PROPERTY

Name: *

Description:

Dialable:

☐

Displayed in users table:

☒

Combined attribute:

☐

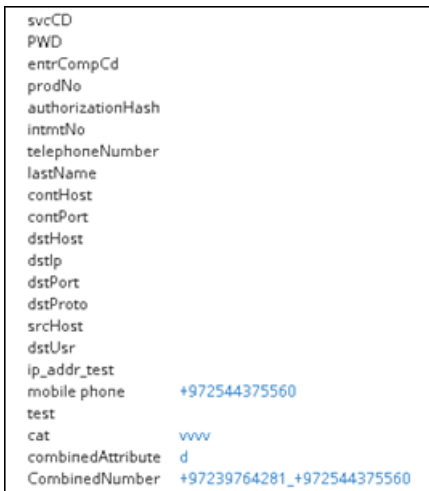
OK

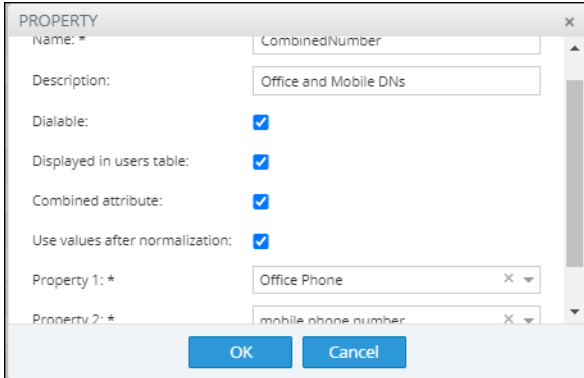
Cancel

3. Use the following table as reference.

Table 6-5: Add Property

Setting	Description
Name	Define an intuitive name for the property, for intuitive future reference.
Description	Enter a brief description of the property, for intuitive future reference.
Dialable	Defines if this property is a dialable number. Only dialable numbers are

Setting	Description
	<p>used for matching with a received source or destination URI in a route request.</p> <p>Examples of dialable number properties: Office phone number, mobile phone number, Skype number, etc.</p>
Display in Users Table	Select the option to display the user property in the Users page. The option can be used to reduce clutter on the Users page. By default, the option is selected.
Combined attribute	<p>Select this option to configure a new attribute in the Users Dictionary as a combined attribute, i.e., triggered by a combination of two other Users Dictionary attributes. If any of the basic attributes [that the new attribute is combined of] changes, the new attribute will change.</p> <p>In the preceding figure, the new attribute whose name is configured as CombinedNumber will be composed of the existing attributes Office Phone and mobile phone, with the delimiter '_' (not shown in the preceding figure). A change to the value of any of the comprising attributes will trigger a change in CombinedNumber. The combined attribute will automatically be created for each user.</p>  <p>The feature allows a Users Group to be configured for routing based on a combination of other attributes. Additionally, you can configure rules using one of the combined attributes (phone numbers) with the option to apply post-routing manipulation to remove any unnecessary prefix or suffix from the combined number.</p>
Use values after normalization	<p>Select this option to apply normalization to a user property combined of two other properties. The combined property can be applied <i>before</i> or <i>after</i> normalization.</p> <ol style="list-style-type: none"> 1. Add a new combined property to the Property Dictionary (Users > Property Dictionary > click Add > select Combined attribute

Setting	Description
	<p>2. Select or clear Use values after normalization:</p>  <p>The screenshot shows a 'PROPERTY' dialog box with the following fields and values:</p> <ul style="list-style-type: none">Name: * CombinedNumberDescription: Office and Mobile DNsDialable: <input checked="" type="checkbox"/>Displayed in users table: <input checked="" type="checkbox"/>Combined attribute: <input checked="" type="checkbox"/>Use values after normalization: <input checked="" type="checkbox"/>Property 1: * Office PhoneProperty 2: * mobile phone number <p>Buttons: OK, Cancel</p>

Adding a Users Dictionary Attribute Triggered (Combined) by Two Other Attributes

The ARM provides the capability to add an attribute in the Users Dictionary triggered by a combination of two other Users Dictionary attributes with a predefined delimiter. If any of the basic attributes [that the new attribute is combined of] changes, the new attribute will change. To accomplish this, you must configure the new attribute as Combined attribute.

Figure 6-31: Property – Combined Attribute

The screenshot shows a 'PROPERTY' dialog box with the following fields and values:

- Name:** CombinedNumber
- Description:** OfficeAndMobileDNs
- Diactable:** ☒
- Displayed in users table:** ☒
- Combined attribute:** ☒
- Property 1:** Office Phone
- Property 2:** mobile phone
- Delimiter:** (field is empty, but the text indicates the delimiter is '_')

[Refer to the example in the figure above] The new attribute whose name is configured as CombinedNumber will be composed of the existing attributes Office Phone and mobile phone, with the delimiter '_' (off-screen in the figure above). A change to the value of any of the comprising attributes will trigger a change in CombinedNumber. The combined attribute will automatically be created for each user.

Figure 6-32: Combined Number

svcCD	
PWD	
entrCompCd	
prodNo	
authorizationHash	
intrmtNo	
telephoneNumber	
lastName	
contHost	
contPort	
dstHost	
dstIp	
dstPort	
dstProto	
srcHost	
dstUsr	
ip_addr_test	
mobile phone	+972544375560
test	
cat	www
combinedAttribute	d
CombinedNumber	+97239764281_+972544375560

The feature allows a Users Group to be configured for routing based on a combination of other attributes. In addition, the operator can configure rules using one of the combined attributes (phone numbers) with the option to apply post-routing manipulation to remove any unnecessary prefix or suffix from the combined number.

Configuring ARM to Provide Information about Device Location

The ARM can be configured to provide information about the location from where emergency calls are made. The information source is the OVOC. The ARM Configurator synchronizes with the OVOC on location information via the designated REST API. In the OVOC, location information is stored per device. Each OVOC device corresponds to an ARM user. The unique property for matching an OVOC device with an ARM user is the number of the user's device.

The ARM Configurator periodically synchronizes with the OVOC. Full sync of data is performed, not just the delta.

The ARM Router provides location information in a response to a GetRoute request sent from the SBC, as defined in a Policy Studio Action.

➤ To enable device location in the ARM:



Phone numbers for all devices must be defined in the ARM user database.

1. Open the Device Location page (**Users > Device Location**).

Figure 6-33: Device Location

2. [Refer to the preceding figure] Under section OVOC PHONES SYNCHRONIZATION, select the **Enable synchronization** check box (for the ARM to synchronize with the OVOC).
3. From the 'Matching property' drop-down under 'ARM', select **Office Phone** (for example) to match with **phoneNumber** under 'OVOC' (read only).

The screenshot shows a configuration interface with two main sections: OVOC and ARM.

OVOC Section:

- Matching property: *** has a dropdown menu with **phoneNumber** selected.
- Location property: *** has a dropdown menu with **locationMatch** selected.

ARM Section:

- A list box is open, showing a scrollable list of properties: **AD groups**, **Country**, **Office Phone** (highlighted), **Display Name**, **Department**, **MS Lync Line URI**, and **Talkers**.

Office Phone (for example) is a property that must be defined in the ARM Property Dictionary before this step. See [Adding a Property Dictionary to the ARM](#) on page 150 for information about how to define a property in the Property Dictionary.

- From the 'Location property' drop-down under 'ARM', scroll down to select the relevant property for device location, to match with **locationMatch** under 'OVOC' (read only). The 'Location property' values are populated during synchronization with the OVOC.

Location (for example) is a property defined in the ARM Property Dictionary. See [Adding a Property Dictionary to the ARM](#) on page 150 for more information about how to define a property in the Property Dictionary.

- In the 'Check for updates every (min)' field under screen section UPDATES, define a regular synchronization time. Default: 60 (minutes). If left at the default, the ARM checks for updates every hour.
- Define 'Perform full update every (days)'. Default: 1 (day). If left at the default, the ARM performs a full update once a day.
- In the 'At:' field, enter the time at which the full update will be performed. Default: 20:00. If left at the default, the ARM performs a full update at 8 pm.
- Click **Submit**.



After configuring and submitting the Device Location settings shown here, you need to define a Policy Studio rule with Action **X_ARM_INFO_1: Location** (for example). See under [Policy Studio](#) on page 208 for more information. Once you complete this step, all configuration related to providing Device Location is complete.

7 Configuring Settings

The Settings page (under the Settings menu) lets you configure

■ Administration

- License (see [Activating Your License](#) on the next page)
- Security (see [Securing the ARM](#) on page 160)
- Operators (see [Provisioning Operators](#) on page 170)
- Node Credentials (see [Node Credentials](#) on page 172)
- Router Credentials (see [Router Credentials](#) on page 174)
- Configurator Credentials (see [Configurator Credentials](#) on page 176)
- LDAP Authentication (see [Provisioning Operators using an LDAP Server](#) on page 179)
- RADIUS Authentication (see [Provisioning Operators using a RADIUS Server](#) on page 184)
- Remote Manager (see [Remote Manager](#) on page 190)
- Certificates (see [Uploading Trusted Certificates](#) on page 167)
- Users (see [Adding Registered Users to the ARM](#) on page 191)

■ Network Services

- Syslogs (see [Editing a Syslog Server](#) on page 192)
- NTP server (see [Adding/Editing an NTP Server](#) on page 194)
- QoS (see [Prioritizing Traffic Per Class of Service](#) on page 195)
- CDR (see [Enabling CDRs](#) on page 196)
- Calls (see [Disabling, Limiting the Number of CDRs](#) on page 309)

■ Call Flow Configurations

- Normalization Groups (see [Adding a Normalization Group](#) on page 198)
- Prefix Groups (see [Adding a Prefix Group](#) on page 200)
- Normalization Before Routing (see [Normalization Before Routing](#) on page 207)
- Policy Studio (see [Policy Studio](#) on page 208)
- Web Services (see [Web-based Services](#) on page 224)

■ Routing

- Configuring a Quality Based Routing Condition (see [Configuring Criteria for a Quality Profile](#) on page 233)
- Configuring a Time-Based Routing Condition (see [Configuring a Time-Based Routing Condition](#) on page 234)

- Configuring SIP Alternative Route Reason (see [Configuring Alternative Routing SIP Reasons](#) on page 237)
- Configuring Global Routing Settings (see [Configuring Global Routing Settings](#) on page 243)
- Routing Servers
 - Servers
 - ◆ Adding a Routing Server (see [Adding a Routing Server](#) on page 254)
 - ◆ Editing a Routing Server (see [Editing a Routing Server](#) on page 255)
 - ◆ Locking/Unlocking a Routing Server (see [Locking/Unlocking a Routing Server](#) on page 257)
 - Groups
 - ◆ Adding a Routing Server Group (see [Adding a Routing Server Group with Internal and External Priorities](#) on page 258)

Administration Settings

The ARM enables the following administrative tasks to be performed:

- Configure a software license (see [Activating Your License](#) below)
- Manage security (see [Securing the ARM](#) on page 160)
- Add an operator (see [Provisioning Operators](#) on page 170)

Activating Your License

The ARM must be licensed with a valid license for the product to become fully operational.

➤ To activate your license:

1. Open the License page (**Settings** menu > **Administration** tab **License** item).

Figure 7-1: License Page

License

LICENSE

Machine Id: EB7CA06B14BB

License Key: * yvGy6z+UeCZkNKUq6jsUxLbwMLSJDj2TgN

LICENSE DETAILS

Expiration Date:	Unlimited
Number of sessions:	300,000
Number of users:	1,000,000
Time based routing:	enabled
Quality based routing:	enabled
Test route:	enabled
Network planner:	enabled
Policy studio:	enabled
Number of routing rules:	20,000,000
Web services:	enabled
Number of standard security queries (per month):	1
Connect to analytics views in the database:	enabled
Number of users for route registrations:	100,000
Number of advanced security queries (per month):	1

Submit

2. Select and copy the 'License Key' (shown in the preceding figure).



Two different fields cover security as shown in the preceding figure:

- Number of standard security queries (per month)
- Number of advanced security queries (per month)

For more information about standard vs. advanced security, see step 10 'Security Based Routing', under [Adding a New Routing Rule](#) on page 268 and step 6 under [Web-based Services](#) on page 224).

3. Activate the product through the AudioCodes License Activation tool at www.audiocodes.com/swactivation. You'll need your Product Key and the Configurator's Machine ID for the activation process. An email will subsequently be sent to you with your License Key.
4. Copy and paste the License Key string that AudioCodes sends you into the 'License Key' field, and then click **Submit**; the number of sessions purchased and the license expiry date are displayed.
5. Make sure the license details (the number of sessions purchased and the license's expiry date) match those that you purchased.

Viewing License Details

License policy is based on the following aspects of ARM functionality and capacity:

- Expiration Date
- Number of Sessions
- Number of Users
- Number of Routing Rules
- Time Based Routing (can be either enabled or disabled)
- Quality Based Routing (can be either enabled or disabled)
- Test Route (can be either enabled or disabled)
- Network Planner (can be either enabled or disabled)
- Policy Studio (can be either enabled or disabled)

➤ **To view information about the license applied to your ARM:**

- Open the License Details page (**Settings > Administration > License**).

Figure 7-2: License Details

License

LICENSE

Machine Id: EB7CA06B14BB
License Key: * yvGy6z+UeCZkNKUq6jsUxLbwMLSJDj2TgN

LICENSE DETAILS

Expiration Date:	Unlimited
Number of sessions:	300,000
Number of users:	1,000,000
Time based routing:	enabled
Quality based routing:	enabled
Test route:	enabled
Network planner:	enabled
Policy studio:	enabled
Number of routing rules:	20,000,000
Web services:	enabled
Number of standard security queries (per month):	1
Connect to analytics views in the database:	enabled
Number of users for route registrations:	100,000
Number of advanced security queries (per month):	1

Submit

Securing the ARM

This ARM enables operators to secure routing management.

➤ To secure the ARM:

1. Open the Security page (**Settings > Administration > Security**).

Figure 7-3: Security Page

2. Use the following table as reference.

Table 7-1: Security Settings

Setting	Description
Session timeout (hours)	After n hours, the user will be logged out, irrespective of whether they're active or inactive. The user will be forced to reenter their password (to reopen the session) if the timeout you define (in hours) expires.
Inactivity period (minutes)	If the user does not interact with the GUI for n minutes, they will be redirected to the login screen and will need to reinsert their password. 0 disables the feature; inactivity will not impact the user's account.
http/https enabled	Enables an HTTP/HTTPS connection between the ARM server and the SBC / Gateway.

3. See [Enabling Client Side Certificate Validation](#) on page 168 and [Enabling Certificate Subject Name Verification](#) on page 168 and click **Submit**; the configuration is saved.

Configuring Certificates

The ARM GUI simplifies the legacy procedure operators had to perform to change the default certificates. To change the default certificates, operators had to use Java Keytool and other tools such as OpenSSL, and had to perform the same procedure in both the Configurator and the Routers.

- To change the server certificates of the **Configurator** using the ARM GUI, see [Configuring a Configurator Certificate](#) below
- To change the server certificates of the **Routers** using the ARM GUI, see [Configuring a Router Certificate](#) on page 165

Configuring Server Certificates

Operators in earlier versions of the ARM needed to manually run a procedure that required using Java Keytool and other tools such as OpenSSL, to change the default certificates, and to perform the same process in both the Configurator and the Routers.

As of version 9.6, the ARM simplifies this process; the ARM GUI enables operators to change the server certificates of both the Configurator and the Routers.

To change the server certificates of the

- **Configurator.** See [Configuring a Configurator Certificate](#) below
- **Routers.** See [Configuring a Router Certificate](#) on page 165

Configuring a Configurator Certificate

The Configurator certificate can be viewed, generated, or uploaded in the new Configurator screen (**Settings > Administration > Configurator Certificates**).

Operators view, download, or copy the currently loaded certificate by pressing the **View Certificate** button.

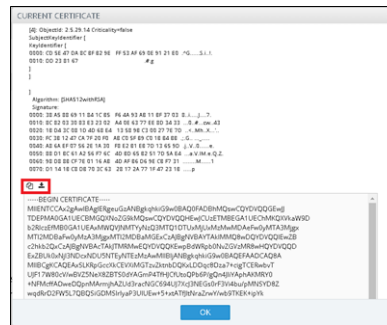
➤ To view a certificate:

1. Open the Configurator Certificates screen (**Settings > Administration > Configurator Certificates**).

Figure 7-4: Configurator Certificates

2. Click **View Certificate**.

Figure 7-5: Current Certificate



3. Download or copy the PEM formatted certificate by pressing one of the icons in the Current Certificate view, as shown in the preceding figure.
4. Generate a self-signed certificate: In the Configurator Certificates page, select the **Generate Private Key and Self-Signed Certificate** option; you can generate and download a Java KeyStore (JKS) file which holds the private key and the self-signed certificate. This file can later be uploaded to the ARM as the Configurator or the Router certificate.
5. Configure the fields using the following descriptions as reference (common for all three operations):
 - **Common name.** The only mandatory field. CN field of the certificate. Typically holds the server hostname or IP address.

The following fields are optional; they typically hold information regarding the organization:

- **Organization unit, Company name, Locality or city name, State, Country code.**
- **Key Algorithm.** Allows you to control whether the private / public key is RSA or EC (Elliptic curve); the default is RSA
- **Private key size.** Allows you to control the private key size. For RSA, one of the following values can be chosen: 2048, 3072, 4096. The default value is 2048. For EC, one of the following values can be chosen: 256, 384, or 521. The default is 256.
- **Signature algorithm.** Allows you to control the signature algorithm for RSA. One of the following can be chosen: SHA256-With-RSA, SHA384-With-RSA, or SHA512-With-RSA. The default is SHA256-With-RSA. For EC, one of the following can be chosen: SHA256-With-ECDSA, SHA384-With-ECDSA, or SHA512-With-ECDSA. The default value is SHA256-With-ECDSA.
- **Validity.** The number of days for which the certificate will be valid. The default value is 365.
- **SAN (Subject Alternative Name) fields.** As the common name can hold only one value, operators can use the SAN fields to reuse the certificate (while keeping it valid) for other hostnames (SAN DNS) or for other IP addresses (SAN IP). This option allows operators to create one certificate for the entire ARM network (Configurator and Routers) with valid hostnames and IP addresses. Other SAN fields can be used (though they are less useful for the ARM) such as Email and URI.

- **Key Usage** (KUEs). Allows you to control the purpose of the generated certificate to allow more tightly controlled usage of it. The following values can be used:
 - ◆ digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, and decipherOnly.
- **Extended Key Usage** (EKUs). An additional key usage option which operators can use to control serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning, or Empty. The default value is Empty, meaning the certificate can be used for any operation.



Selecting a combination of **Key Usage** and **Extended key usage** can invalidate the Certificate for Server certificate purposes. In this case, the ARM will start up without TLS support.

Generating and Replacing a Private Key and Self-Signed Certificate

Operators can generate a new self-signed certificate and replace the currently loaded certificate of the Configurator.

➤ To generate a new self-signed certificate and replace the currently loaded certificate of the Configurator:

1. Open the Configurator Certificates page (**Settings > Administration > Configurator Certificates**) and locate screen section 'Generate Certificate'.

Figure 7-6: Generate Certificate

2. Select the **Generate and Replace Private Key and Self-Signed Certificate** option and click **Generate**.



This option also triggers a reload of the Configurator's port 443 (TLS) configuration.

Generating a Private Key, Self-Signed Certificate and CSR

Operators can generate and download a ZIP file which holds a JKS (Java KeyStore file) of the private key and the self-signed certificate, and a text file with the CSR which can be sent to a

Certificate Authority (CA) for signing. The JKS file and the signed certificate can later be uploaded to ARM (Configurator and Routers), to replace the loaded certificate.

➤ **To generate a private key, self-signed certificate and CSR:**

1. Open the Configurator Certificates page (**Settings > Administration > Configurator Certificates**) and locate screen section 'Generate Certificate'.

Figure 7-7: Generate Certificate

2. Select the **Generate Private Key and CSR** option and click **Generate**.

Loading a Certificate

Operators can either load their own Java **KeyStore** (JKS) file with the private key and the certificate, or the **KeyStore** file that was generated using one of the options through the ARM GUI.

Figure 7-8: Load Certificate

If the **Generate Private Key and CSR** option was selected previously, operators can also upload the **CSR Response** (the signed certificate) together with the original JKS file that was generated.



The **CSR Response** file format must be p7b which holds a full chain of certificates.

If an operator creates their own KeyStore with a non-default password, the KeyStore **Password** must be provided.



A full Tomcat restart will be performed if a password is changed. This operation is longer than the regular upload; it might take few minutes. During this time, the GUI will be unavailable and might time out. If it times out, pressing Ctrl + F5 can solve the issue.

Configuring a Router Certificate

The same certificate operations can be performed *on each Router*, facilitating operator management.

➤ To configure a Router Certificate:

1. Open the Routing Servers page (**Settings > Routing Servers > Servers**).

Figure 7-9: Routing Servers page

STATUS	ADMINISTRATIVE S...	NAME	ADDRESS	PORT	NODE PROTOCOL
✓	🔒	router2	172.17.133.9	443	https
✓	🔒	router1	router8.corp.audioco...	443	https
✓	🔒	router3	172.17.133.162	443	https

2. Select a Router and then click the **Certificate** button; the Server Certificate screen opens.

Figure 7-10: Server Certificate

SERVER CERTIFICATE

View Certificate

GENERATE CERTIFICATE

Common Name [CN]: *

Organizational Unit [OU]:

Company Name [O]:

Locality or city name [L]:

State [ST]:

County code [C]:

Key Algorithm: RSA

Private Key Size: 2048

Signature Algorithm: SHA256withRSA

Validity (days): 365

SAN Email:

SAN URI:

SAN DNS:

SAN IP:

Key Usage: ☐ Critical

Extended Key Usage: ☐ Critical

☒ Generate Private Key and Self-Signed Certificate

☐ Generate and Replace Private Key and Self-Signed Certificate

☐ Generate Private Key and CSR

Generate

Close

3. Configure the parameters using the options described under [Configuring a Configurator Certificate](#) on page 161; they're the same.



- For the Routers, the **View Certificate** link only displays non-default certificates; clicking the **View Certificate** link after selecting a Router that has a default certificate opens a blank screen.
- Changing the certificate of a Router is an asynchronous operation that can take a few minutes, depending on the selected option.

Determining ARM Communications with Other Entities

Operators can determine the way ARM communicates with other entities, e.g., routers and nodes. The ARM Configurator's address configured in these entities can be the Configurator's IP address or Hostname (FQDN).

➤ To configure the way the ARM communicates with other entities:

1. Open the Security page (**Settings > Administration > Security**).

Figure 7-11: Security

2. Under 'ARM Configuration', configure the:
 - ARM IP Address [Drop-down list of available hard-coded IP addresses that the ARM extracted from the machine's local network interfaces]
 - ARM Hostname [The hostname of the ARM's machine; by default, identical to that of the machine's hostname]
 - Communication method [drop-down list to select whether the ARM should configure its IP address or Hostname (FQDN) for the other entities]
 - Support underscore in node's hostname [check this option for an underscore in Hostname (FQDN) to be supported]



This action may take some time depending on the number of nodes in the network and the number of configured ARM Routers. The action will cause entities to be temporarily disconnected. Peer Connections, VoIP Peers and other entities do not impact on the action.

See also [Strengthening Security: Certificate Validation](#) below

Strengthening Security: Certificate Validation

Certificate validation allows stronger ARM communications security. The ARM can validate either the Subject name of the certificate or the entire client certificate that's loaded to the ARM. When initiating TLS communications from the ARM, the ARM will then only accept validated certificates.

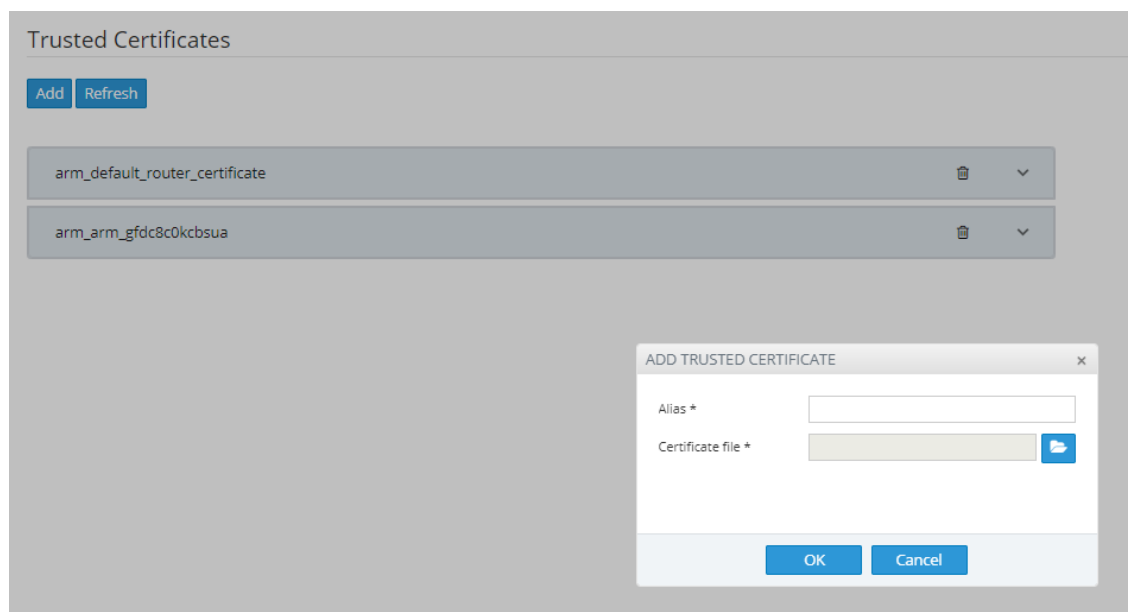
Uploading Trusted Certificates

Operators must first upload trusted certificates to the ARM.

➤ To upload trusted certificates:

1. Open the Add Certificate screen (**Settings > Administration > Trusted Certificates**) and then click **Add**.

Figure 7-12: Add Trusted Certificate



2. In the 'Alias' field, enter the name of the certificate.
3. Click the browse icon adjacent to the 'Certificate file' field, and then navigate to and select a valid Base64-encoded certificate file.



This setting is system wide; you must upload all certificates for all entities (nodes, ARM routers) communicating over TLS / SSL / HTTPS. The ARM is by default released with the default ARM Router certificate trusted, but if this certificate is changed, you must re-upload the changed certificate.

Enabling Certificate Subject Name Verification

The ARM supports capability to validate the subject name received in the server certificate, against the Hostname / IP Address of the entity to which the communication was initiated.

➤ To enable certificate subject name verification:

1. Open the Security page (**Settings > Administration > Security**) and locate the section 'Certificate Verification'.
2. Select the option **Verify certificate subject name when ARM performs https requests** to enable the feature.

Figure 7-13: Verify certificate subject name when ARM performs https requests

CERTIFICATE VERIFICATION	
Verify certificate when ARM performs https requests	<input type="checkbox"/>
Verify certificate subject name when ARM performs https requests	<input checked="" type="checkbox"/>
<div>Submit</div>	



Before enabling the option, make sure all entities communicating over TLS / SSL / HTTPS have a valid certificate with appropriate subject names.

Enabling Client Side Certificate Validation

Operators should only enable validation of certificates after uploading certificates as shown under 'Uploading Trusted Certificates', else the ARM will not be able to communicate with any of the elements which the ARM communicates with over SSL / TLS.

➤ To enable validation of certificates:

1. Open the Security page (**Settings > Administration > Security**) and locate the section 'Certificate Verification'.

Figure 7-14: Certificate Verification

CERTIFICATE VERIFICATION	
Verify certificate when ARM performs https requests	<input checked="" type="checkbox"/>
Verify certificate subject name when ARM performs https requests	<input type="checkbox"/>
<input type="button" value="Submit"/>	

2. Select the option **Verify certificate when ARM performs https requests**.

Enhancing SSH Users Management for Security

For security reasons, the ARM blocks remote **root** login into ARM VM Linux machines for both ARM Configurator and ARM Router. The feature prevents accidental damage of ARM system files available for the **root** user. External hackers typically attack the **root** user because the **root** account is the most vulnerable and can be attacked remotely via SSH. Instead of the **root** user, operators can use the **armAdmin** SSH user. During a first-time installation of the ARM or an upgrade to ARM 9.0 or later, this account is created with a default password and the **root** account is blocked for remote access.



The operator can change the default password for an **armAdmin** SSH user. The same password should be shared by all ARM Routers and it can be different to the Configurator's **armAdmin** password.

➤ To configure enhanced SSH users management for security:

1. Open the Security page (**Settings > Administration > Security**) and locate section SSH Users.

Figure 7-15: SSH Users

SSH USERS

Router SSH Credentials

Username

armAdmin

Password

Confirm password

Configurator SSH Credentials

Username

armAdmin

Password

.....

Confirm password

.....|

The password length must be between 8 and 20.

Must contain at least one letter and one digit.

Starting from ARM 9.0, operators should log in to ARM machines using the **armAdmin** user and to request **root** access only when powerful **root** privileges are required. After a remote login using **armAdmin**, the operator can switch to **root** user by applying the “su-” command. This switch of privileges is required for the following ARM maintenance operations:

- ARM upgrade (starting from ARM V.9.0 and later). Note that upgrade to ARM 9.0 from the customer's previous load still requires root privileges.
- ARM Backup and Restore
- Logs collection (logCollect)

See the *ARM Installation Manual* for more information.

Provisioning Operators

Operators, i.e., network administrators or IT managers, and operator credentials can be provisioned in four ways:

- Using the ARM's Operators page – see [Manually Provisioning an Operator in the ARM's Operators Page](#) on the next page
- Using the enterprise's LDAP authentication server – see [Provisioning Operators using an LDAP Server](#) on page 179
- Using the enterprise's RADIUS authentication server – see [Provisioning Operators using a RADIUS Server](#) on page 184
- Using the enterprise's Open LDAP authentication server – see [Authenticating Operator Login using Open LDAP](#) on page 183

If LDAP / RADIUS is used, the order will be:

- LDAP / RADIUS
- Local storage (database)

If an LDAP / RADIUS authentication server is used but it is down or the operator can't be authenticated with it because either the operator isn't found or the password doesn't match, the local operators table is used.

The LDAP / RADIUS method of provisioning operators therefore coexists with the local storage (database) method.

Manually Provisioning an Operator in the ARM's Operators Page

Operators can be manually provisioned using the ARM's Operators Page.

➤ To manually add an operator:

1. Open the Operators page (**Settings** menu > **Administration** tab **Operators** item).

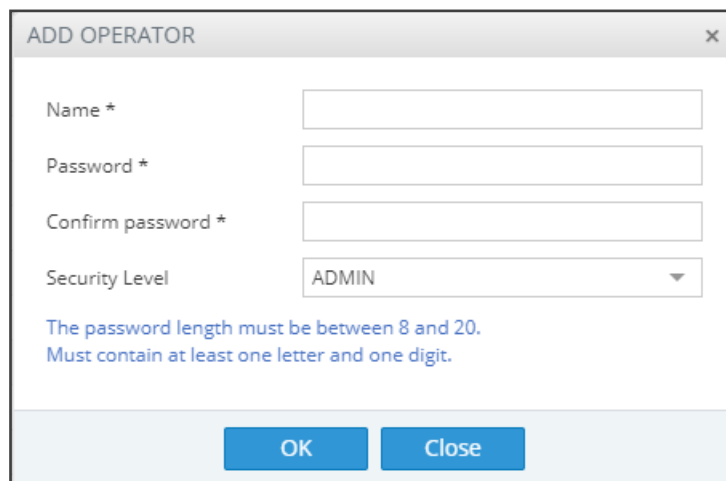
Figure 7-16: Operators



NAME	SECURITY LEVEL
Operator123	SECURITY_ADMIN
1	SECURITY_ADMIN
Operator	SECURITY_ADMIN
b	SECURITY_ADMIN

2. Click **Add**.

Figure 7-17: Add Operator



ADD OPERATOR

Name *

Password *

Confirm password *

Security Level ADMIN

The password length must be between 8 and 20.
Must contain at least one letter and one digit.

OK **Close**

3. Configure the operator details using the following table as reference.

Table 7-2: Add Operator

Setting	Description
Name	Enter a name for the operator to log in with.

Setting	Description
Password	Enter a password for the operator to log in with.
Password confirm	Confirm the password.
Security Level	<p>Select a Security Level for the operator. An operator with a Security Level of:</p> <ul style="list-style-type: none"> ■ Security Admin can perform any action, perform provisioning and define a new operator of any permission level. Only Security Admin can make changes to any ARM credentials such as node credentials or ARM Router/Configurator credentials. ■ Admin can perform any action and provisioning but cannot define new operators ■ Monitor (read-only) cannot perform provisioning or apply any actions. They cannot, moreover, view information under Settings > Administration. License, Security, Certificates, Authentication and Credentials information is only available for viewing and editing to the operator with Security Admin or Admin privileges. Access to view this information by the operator whose security level is Monitor is restricted using the REST API as well.

4. Click **OK**; the operator is added to the local ARM database.

Node Credentials

Operators can apply credentials *per Node* for ARM Configurator-Node communications.



- Only operators whose role is configured as SECURITY_ADMIN can make changes to credentials.
- Before changing the Node's credentials in the ARM Network page, the Web credentials must be updated in the Node itself. See your Node's *User's Manual* for more information.

➤ To apply credentials *per Node* for ARM Configurator - Node communications:

1. Open the Node Credentials page (**Settings > Administration > Node Credentials**).

Figure 7-18: Node Credentials

Node credentials		
Add Edit Delete Refresh		
IDENTIFIER NAME	USER NAME	TYPE
Default node user name and password	Admin	DEVICE
New_York_1	Admin	DEVICE
Paris_2	Admin	DEVICE
Israel-HQ_3	Admin	DEVICE
China_4	Admin	DEVICE
Haifa_5	Admin	DEVICE
New_Jersey_6	Admin	DEVICE
Texas_7	Admin	DEVICE
Beer_Sheva_8	Admin	DEVICE

2. Click **Add**.

Figure 7-19: Add Node Credentials

ADD NODE CREDENTIALS

Identifier name

For NYSBC

User name

NYSBCUser

Password

Confirm password

OK

Cancel

3. Configure the fields using the table as reference.

Table 7-3: Add Node Credentials

Setting	Description
Identifier name	Enter a name to identify this set of device credentials.
User name	Enter the user name.
Password	Enter the password.
Password confirm	Re-enter the password.

4. Click **OK**.



- After adding credentials you can Delete or Edit.
- You can apply one of the previously configured settings to a specific Node (or use the default setting) in the Edit Node screen (**Network > Map > <select the specific node> > Edit**). Expand the 'Credentials' section first.

Figure 7-20: Edit Node - Credentials - Configurator>Node

The 'EDIT NODE' dialog box contains the following fields and values:

- Name: * Texas_7
- Teams Role: Not Teams
- Address: 172.17.129.39
- Protocol: HTTP
- Routing server group: group of node New_York_1
- Resource Groups: USANodes

Below a horizontal separator, the 'Credentials' section includes:

- Configurator → Node: Texas_7
- Node → Configurator: Admin

At the bottom are 'OK' and 'Cancel' buttons.

5. [Optionally] You can apply the same to 'Add Node' and 'Offline Planner'.

The 'ADD NODE' dialog box contains the following fields and values:

- Name *: (empty)
- Teams Role: Not Teams
- Address: * (empty)
- IP Address ☒ Hostname ☐
- Protocol: HTTP
- Routing server group: (empty)

A red error message is displayed: "The node will be unrouteable as no routing server group was picked".

Below a horizontal separator, the 'Credentials' section includes:

- Configurator → Node: (empty)
- Node → Configurator: (empty)

At the bottom are 'OK' and 'Cancel' buttons.

Router Credentials

The operator can change the ARM Routers credentials to be used for ARM Configurator - ARM Routing Server communications.

➤ To configure new credentials:

1. Open the 'Router Credentials' page (**Settings > Administration > Router credentials**).

Figure 7-21: Router Credentials

Router credentials		
Add Edit Delete Refresh		
IDENTIFIER NAME	USERNAME	TYPE
Default router user name and password	Admin	ROUTER



Only operators whose role is configured as SECURITY_ADMIN can make changes to credentials.

2. Click **Add**.

Figure 7-22: Add Router Credentials

ADD ROUTER CREDENTIALS

Identifier name

User name

Password

Confirm password

Password rules

The password length must be between 8 and 20

Must contain at least one letter and one digit.

OK

Cancel

3. Configure the fields using the table as reference.

Table 7-4: Add Router Credentials

Setting	Description
Identifier name	Enter a name to identify this set of router credentials.
User name	Enter the user name.
Password	Enter the password.
Password confirm	Re-enter the password.

4. Click **OK** and then view in the Router Credentials page (shown previously) the new entry for Configurator - Router communications of type 'Router'.
5. To associate the Routing Server with a specific ARM Router, open the Routing Servers page (**Settings > Routing Servers**) and then Add or Edit the specific ARM Router. Expand the 'Credentials' section of the screen to do this.

Figure 7-23: Edit Server: Configurator - Router Credentials

EDIT SERVER

Name *

Address *

Port

Protocol

Advanced Configuration

Configurator - Routing Protocol

Credentials

Configurator → Router

Router → Configurator

OK **Close**

Configurator Credentials

You can configure new **ARM Configurator** credentials to be used for communications between:

- **Node - ARM Configurator**
- and
- **ARM Router - ARM Configurator**

➤ To configure new credentials:

1. Open the Configurator Credentials page (**Settings > Administration > Configurator Credentials**).

Figure 7-24: Configurator Credentials

USER NAME	TYPE	USED IN ELEMENTS
Admin	DEVICE	Used in 30 devices with names: Paris_2, Israel-HQ_3, China_4, Haifa_5, New_Jersey_6, Texas_7,...
AdminNew1	DEVICE	Used in 1 device with name: New_York_1
111zz	DEVICE	Used in 0 devices
Router1234561	ROUTER	Used in 36 routers with names: router1, router2, router3, router4, router5, router6, router7, r...



Only operators whose role is configured as **SECURITY_ADMIN** can make changes to credentials.

2. Click **Add**.

Figure 7-25: Add Credentials - Device

ADD CREDENTIALS [X]

Username:

Password:

Confirm password:

Type:

Password rules [⚙](#)

The password length must be between 8 and 20
Must contain at least one letter and one digit.

- If you're configuring credentials for **Node - ARM Configurator** communications, then from the 'Type' drop-down select **Device** as shown in the preceding figure.
- If you're configuring credentials for **ARM Router - ARM Configurator** communications, then from the 'Type' drop-down select **Router** as shown in the following figure.

Figure 7-26: Add Credentials - Router

EDIT CREDENTIALS [X]

Username:

Password:

Confirm password:

Type:

Password rules [⚙](#)

The password length must be between 8 and 20
Must contain at least one letter and one digit.

3. Configure the fields using the table as reference.

Table 7-5: Add Credentials - Device | Router

Setting	Description
User name	Enter the user name.
Password	Enter the password.
Password confirm	Re-enter the password.

Setting	Description
Type	<ul style="list-style-type: none"> ■ If you're configuring credentials for Node - ARM Configurator communications, select Device. ■ If you're configuring credentials for ARM Router - ARM Configurator communications, select Router.

4. Click **OK**.
5. [Optionally] Apply one of the previously defined settings to a specific
 - **Node** (or use the default Node): Open the Edit Node screen (**Network > Map > <select the node> > Edit**) and expand 'Credentials'.

Figure 7-27: Node - Configurator | Configurator - Node

[The same applies to 'Add Node' and 'Offline Planner']

- **Router**: Open the Routing Servers page (**Settings > Routing Servers**), click **Add** or **Edit** for the specific ARM Router and then expand 'Credentials'.

EDIT SERVER

Name * router1

Address * 172.17.129.31

Port 443

Protocol https

Advanced Configuration

Configurator - Routing Protocol https

Credentials

Configurator → Router Admin

Router → Configurator Router

OK Close

After applying newly configured ARM Configurator credentials to a specific Node, view the Node automatically displayed in the 'Configurator credentials' page in the 'Used in Elements' column, shown previously.

After applying newly configured ARM Configurator credentials to a specific Router, view the Router automatically displayed in the 'Configurator credentials' page in the appropriate 'Used in Elements' column, shown previously.

Provisioning Operators using an LDAP Server

ARM allows using the enterprise's LDAP server for operator login authentication. This feature is in addition to local operator login authentication described under [Manually Provisioning an Operator in the ARM's Operators Page](#) on page 171.

➤ To add an LDAP operator login authentication server:

1. Open the Authentication page (**Settings > Administration > LDAP Authentication**).

Figure 7-28: LDAP Authentication


Only operators with a security level of Admin can edit LDAP authentication server parameters.

2. Configure the LDAP Authentication Server parameters using the following table as reference.

Table 7-6: LDAP Authentication Server Parameters

Parameter	Description
Enable LDAP Authentication	Select or clear this option to enable or disable operator login authentication using an LDAP-compliant authentication server.
LDAP Authentication Server Host	Enter the IP address of the LDAP server's host.
LDAP Authentication Server Port	Enter the LDAP server's port number. Default: 389
LDAP Connectivity DN	Configure the 'LDAP Connectivity DN' parameter as required.
LDAP Connectivity Password	Configure the 'LDAP Connectivity Password' as required.
User DN Search Base	Configure the 'User DN Search Base' as required.

Parameter	Description
Test	This button tests the LDAP server; it tests whether you can connect to it with the bind user, whether the port is correct, etc.

3. Configure the SSL parameters to secure the connection to the LDAP server, using the following table as reference.

Table 7-7: SSL Parameters

Parameter	Description
SSL	Select the 'SSL' option to secure the connection with the LDAP server over SSL. If left unselected (default), the connection with the LDAP server will be non-secured.
Certificate file	Click the 'Certificate file' browse button to browse to and select the certificate file that you want to use to secure the connection with the LDAP server over SSL. If SSL is selected and a certificate is also selected, an HTTPS connection between the ARM and the LDAP server will be opened. The ARM authenticates the SSL connection using the certificate.

4. Configure the Test Connectivity parameters to test the connection to the LDAP server. Use the following table as reference.

Table 7-8: Test Connectivity

Parameter	Description
Name	If 'Name' is undefined (empty), the connectivity test checks if the LDAP authentication server can be logged into per the values defined under the 'LDAP Authentication Server' parameters. If you enter a user name, the connectivity test checks that it's valid for logging into the ARM. Enter the user name assigned to the LDAP server.
Password	If 'Password' is undefined (empty), the connectivity test checks if the LDAP authentication server can be logged into per the values defined under the 'LDAP Authentication Server' parameters. If you enter a user password, the connectivity test checks that it's valid for logging into the ARM. Enter the password required for accessing the LDAP server.
Test	This button tests whether the user and the user's password have authorization. If the user matches the mappings on the right side of the screen, it will also 'test' the connection to the server itself.

Figure 7-29: LDAP Connectivity Test Result

The figure consists of two screenshots of a web interface for testing LDAP connectivity. Both screenshots have a header 'TEST CONNECTIVITY'.

The top screenshot shows a failed test. The 'Name' field contains 'unknown' and the 'Password' field contains '****'. Below the fields, a red error message reads: 'Failed: Authentication error (Check user permissions or that the user exists)'. A blue 'Test' button is at the bottom right.

The bottom screenshot shows a successful test. The 'Name' field contains 'arm' and the 'Password' field contains '...'. Below the fields, a green success message reads: 'RADIUS server connection test successful'. A blue 'Test' button is at the bottom right.

5. View the result of the LDAP server connectivity test; the figure uppermost shows a failed test while the lowermost figure shows a successful connection.
6. Under page section 'Authorization Level Settings', you can provide mapping of the ARM's access rules ('Security Admin' and 'Admin') into the LDAP server's values. Use the following table as reference.

Table 7-9: Test Connectivity

Parameter	Description
User Name Attribute	The name of the LDAP-complaint server's directory folder in which the enterprise's user names are located. Default: sAMAccountName. When the operator logs in, the authentication feature checks <i>in this directory</i> <i>folder</i> that the operator's name exists.
Permissions Attribute	The name of the LDAP-complaint server's directory folder in which the permissions are located. Default: memberOf. When the operator logs in, the authentication feature checks <i>in this directory</i> <i>folder</i> if they have permission to log in.
Security Admin Mapping	The name of the LDAP-complaint server's directory folder in which the ARM's access rule is mapped. Default: ARM_SecurityAdmin. When the operator logs in, the authentication feature checks <i>against this directory</i> <i>folder</i> if login is allowed or not.
Admin Mapping	The name of the LDAP-complaint server's directory folder in which the ARM's access rule is mapped. Default: Default: ARM_Admin. When the operator logs in, the authentication feature checks <i>against this directory</i> <i>folder</i> if login is allowed or not.

If LDAP authentication is enabled, the order used to authenticate operator login is:

- LDAP
- Local storage (Database)

If the LDAP server is down or if the operator can't be authenticated with the LDAP server because either the operator isn't found or the password doesn't match, the local operators table is used.

7. Click **Submit**.

Authenticating Operator Login using Open LDAP

Operator login can optionally be authenticated using Open LDAP.

➤ **To configure operator login authentication using Open LDAP:**

1. Open the LDAP Authentication page (**Settings > Administration > LDAP Authentication**) and then select **Open LDAP** under 'Authorization Level Settings'.

Figure 7-30: Authenticating Operator Login using Open LDAP

The screenshot shows the 'LDAP Authentication' configuration page. It includes sections for LDAP server settings, authorization level settings (with 'Open LDAP' selected), SSL configuration, advanced LDAP settings, test connectivity, and authentication mode. The 'Submit' button is located at the bottom right of the form.

2. Configure the LDAP Authentication settings; the settings under 'Open LDAP' are the same as under 'Active Directory'.
 - User Name Attribute [The LDAP attribute used to identify the username]
 - Group Membership Attribute [The LDAP attribute used to list the members of the LDAP group]
 - Security Admin Group Name [The name of the LDAP group containing operators with Admin security level access to ARM]
 - Admin Group Name [The name of the LDAP group containing operators with Admin access to ARM]
 - Monitor Group Name [The name of the LDAP group containing operators with Monitor access to ARM]
 - Group Name Attribute [The LDAP attribute used to identify the LDAP group name]

- Group ObjectClass Attribute [The value of the ObjectClass attribute that identifies a user group LDAP object]

Figure 7-31: Authorization Level Settings

See also [Adding an LDAP Server to the ARM](#) on page 141

See also [Managing Authentication Order](#) on page 187

Provisioning Operators using a RADIUS Server

ARM allows using the enterprise's external RADIUS server for operator login authentication. This feature is available in addition to local operator login authentication described under [Manually Provisioning an Operator in the ARM's Operators Page](#) on page 171. Only operators with a security level of 'Security_Admin' can edit RADIUS authentication server attributes.



- The default AudioCodes dictionary definition must be used with the RADIUS authentication server for the operator's role definition (same as for the SBC or OVOC).
- Enabling and using both the LDAP server and the RADIUS server for authentication is not allowed.

➤ To add a RADIUS operator login authentication server:

1. Open the RADIUS Authentication page (**Settings > Administration > RADIUS Authentication**).

Figure 7-32: RADIUS Authentication



Only operators with a security level of Admin can edit RADIUS authentication server parameters.

2. Configure the RADIUS Authentication Server parameters using the following table as reference.

Table 7-10: RADIUS Authentication Server Parameters

Parameter	Description
Enable RADIUS Authentication	Drag the slider to the 'On' position to enable operator login authentication using a RADIUS authentication server. Default: 'Off' position (disabled).
Server IP	Enter the IP address of the RADIUS authentication server host (in dotted-decimal notation).
Server port	Enter the RADIUS authentication server's port number. Default: 1812
Server secret	Enter the 'secret' for authenticating the RADIUS server: it should be a cryptically strong password. The secret is used by the ARM Configurator to verify authentication of RADIUS messages sent by the RADIUS server (i.e., message integrity). By default, no value is defined.
RADIUS retransmit timeout (msec)	If no response is received from the RADIUS authentication server, the ARM Configurator can be configured to <i>resend packets</i> to it. Enter the time (in milliseconds) the ARM Configurator must wait for the RADIUS server to respond before sending a retransmission.
RADIUS auth number of retries	Enter the maximum number of retransmissions the ARM Configurator performs if no response is received from the RADIUS authentication server.
Default Auth level	Select either: <ul style="list-style-type: none"> ■ Security_Admin [in the SBC / gateway, the equivalent value is 200] ■ Admin [mandatory level to edit RADIUS authentication server parameters; in the SBC / gateway, the equivalent value is 100] ■ Monitor [user level; in the SBC / gateway, the equivalent value is 50] ■ Reject [no permission; in the SBC / gateway, the equivalent value is any other number besides 200, 100 or 50]
Test	Click this Test button to test <i>general connectivity</i> .

3. Connectivity with the RADIUS authentication server can also be tested for *specific credentials* by clicking the **Test** button located under the screen section 'Test Connectivity', after configuring the Test Connectivity parameters described in the following table.

Table 7-11: Test Connectivity for Specific Credentials

Parameter	Description
Name	If 'Name' is undefined (empty), the connectivity test checks if the RADIUS authentication server can be logged into per the values defined under the 'RADIUS Authentication Server' parameters. If you enter a user name, the connectivity test checks that it's valid for logging into the ARM. Enter the user name assigned to the RADIUS server.
Password	If 'Password' is undefined (empty), the connectivity test checks if the RADIUS authentication server can be logged into per the values defined under the 'RADIUS Authentication Server' parameters. If you enter a user password, the connectivity test checks that it's valid for logging into the ARM. Enter the password required for accessing the RADIUS server.

Figure 7-33: RADIUS Connectivity Test Result

The figure displays two screenshots of the 'TEST CONNECTIVITY' interface. The top screenshot shows a failed test result with the message 'Failed: Authentication error (Check user permissions or that the user exists)' in red text. The Name field contains 'unknown' and the Password field is masked with dots. The bottom screenshot shows a successful test result with the message 'RADIUS server connection test successful' in green text. The Name field contains 'arm' and the Password field is masked with dots. Both screenshots have a blue 'Test' button at the bottom right.

4. View the result of the RADIUS server connectivity test; the uppermost figure shows a failed test while the lowermost figure shows a successful connection.

If RADIUS authentication is enabled, the order used to authenticate operator login is:

- RADIUS
- Local storage (Database)

If the RADIUS server is down or if the operator can't be authenticated with the RADIUS server because either the operator isn't found or the password doesn't match, the local operators table is used.

5. Configure authentication order. For more information, see [Managing Authentication Order](#) below.
6. Click **Submit**.

Managing Authentication Order

The ARM lets you manage the authentication order for LDAP | RADIUS authentication.

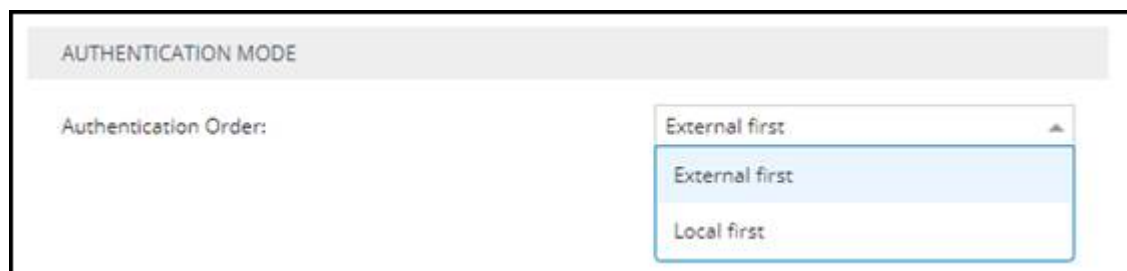
You can define whether the ARM will first check the external service (LDAP | RADIUS), or the local database (the Operators page); the default behavior is to first check the external service.

Change can be applied for each authentication method, depending on which one is used, by navigating in the ARM GUI to:

Settings > Administration > LDAP Authentication

Settings > Administration > RADIUS Authentication

Figure 7-34: Authentication Order

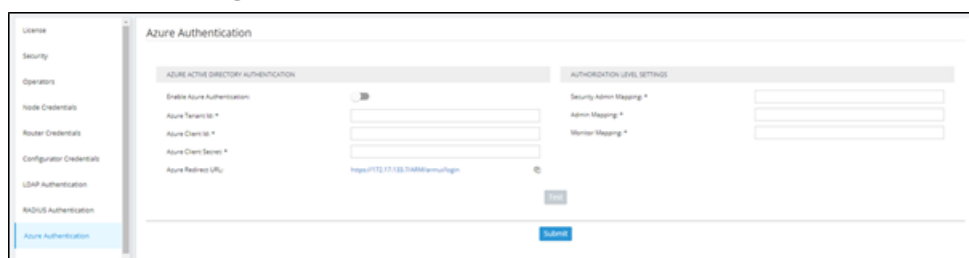


Authenticating Operator Login Using Azure AD

The ARM supports Azure AD for operator login authentication (in addition to support for Azure AD as a source of ARM users). The feature augments local operator login authentication and comes in addition to LDAP and RADIUS authentication.

1. Configure the Azure portal to allow the ARM as a valid application (see [Configuring the ARM in the Azure Portal](#) on page 346); Azure AD is added to the ARM in the Azure Authentication page (**Settings > Administration > Azure Authentication**).

Figure 7-35: Azure Authentication





Only operators with a security level of 'Security Admin' can edit Azure Authentication attributes.

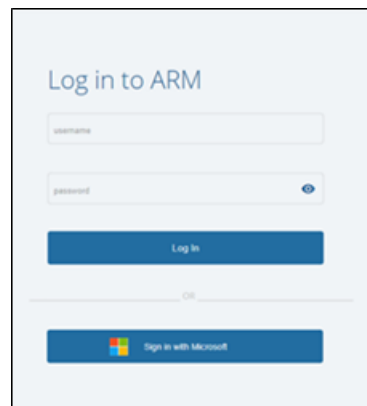
2. Test connectivity with Azure AD. Use the **Test** button shown in the preceding figure (available for operators whose security level is 'Admin' or 'Secure Admin').



In the connectivity test, the ARM also validates the Authorization-level mappings; if an Azure AD membership group does not contain the authorization mappings, a warning message is displayed.

3. Under the section 'Authorization Level Settings', map the ARM's access roles ('Security Admin', 'Admin' and 'Monitor') with the Azure AD's app roles.
4. After Azure authentication is enabled, the **Sign in with Microsoft** button is displayed in the login screen:

Figure 7-36: Log in to ARM



5. Select **Sign in with Microsoft**; the browser redirects to the Microsoft login page and after authentication with Microsoft, it redirects back to the ARM GUI. See also [Logging in](#) on page 17.

Azure AD for REST Requests Authentication

Operators who operate the ARM using the official ARM REST API can also use Azure AD for authentication.

➤ To use the ARM REST API with an Azure AD user:

1. Configuration in Azure portal:

In Azure Active Directory under **Manage** select **App registrations**, select the default ARM application. Under **Manage**, select **Expose an API**:

- a. Click **Add a scope**
- b. Click **Save and continue**; the default value is created: "api://{client-id}".

Register your own REST application for REST authentication.

In the **Azure Active Directory** pane, click **App registrations** and choose **New registration**.

In the new application:

- c. Create a client secret – as described previously.
- d. Add permission to access the default ARM application:

Under **API permissions** click **Add permission**.

Select **my APIs**, select **application** and then select the exposed API previously defined in the app and select the role for the REST authentication (from the app roles defined previously in the application).

Click **Grant admin consent**.

2. Acquire an access token from Microsoft. To acquire access token from Microsoft using REST client:

Send a request to Microsoft Identity platform's token endpoint, as follows:

```
POST
https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token
```

Using **x-www-form-urlencoded** as 'Body content type' and the following 'Body' content:

```
grant_type=client_credentials&
client_id=<rest-app-client-id>&
client_secret=<rest-app-client-secret>&
scope = api://<client-id>/.default
```

Replace **tenant-id** and **client-id** with **tenant id** and **client id** of the default ARM application.

Replace **rest-app-client-id** and **rest-app-client-secret** with the **client id** and **client secret** of your own REST application.

A successful response will contain an access token:

```
{
  "token_type": "Bearer",
  "expires_in": 3599,
  "ext_expires_in": 3599,
  "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsI..."
}
```

3. Access ARM's REST API using the access token:

To access ARM's REST API using the access token, send a Post request with the token received from Microsoft to:

```
POST <ARM_Configurator_IP>/ARM/v1/login/microsoft/authentication/token
```

with the following body:

```
{
  accessToken: String,
  authenticationType: ACCESS_TOKEN
}
```

The ARM validates the Microsoft access token and generates an ARM token with the received role.

4. In any REST Request to the ARM, use the received token in the authorization Header like this:

Figure 7-37: Authorization Header

Header name	Header value
authorization	Bearer (token)

Remote Manager

For ARM status to be indicated in AudioCodes' One Voice Operations Center (OVOC) management platform, ARM-related information such as the IP address of the ARM Configurator, ARM credentials, etc., must be configured in the OVOC (**System > Configuration > External Applications > ARM**) - see the *OVOC User's Manual* for more information.

When the OVOC is connected to the ARM, read-only OVOC information is shown in the ARM (**Settings > Administration > Remote Manager**).

Figure 7-38: Read-Only OVOC Information Displayed in the ARM's Remote Manager Page

ARM-generated alarms and events can be displayed in the OVOC but the feature must be enabled in the ARM (assuming the ARM is already connected to the OVOC).

➤ **To enable ARM alarms and events reports to be sent to the OVOC:**

- In the Remote Manager page (**Settings > Administration > Remote Manager**) under 'OVOC Server', drag the **Enable Alarms/Events forwarding** slider to the 'on' position and click **Submit**.

Figure 7-39: Remote Manager

After enabling the feature, the ARM forwards alarms and events to the OVOC allowing operators to receive all the benefits of ARM-sourced alarms and events handling that already exist in the OVOC such as Active Alarms, History Alarms, Carrier Grade Alarms, Alarms Forwarding (via e-mail or syslog).

ARM status (as well as the statuses of other applications) can then be viewed in the OVOC after the ARM updates the OVOC with its status.

See the *OVOC User's Manual* for more information.

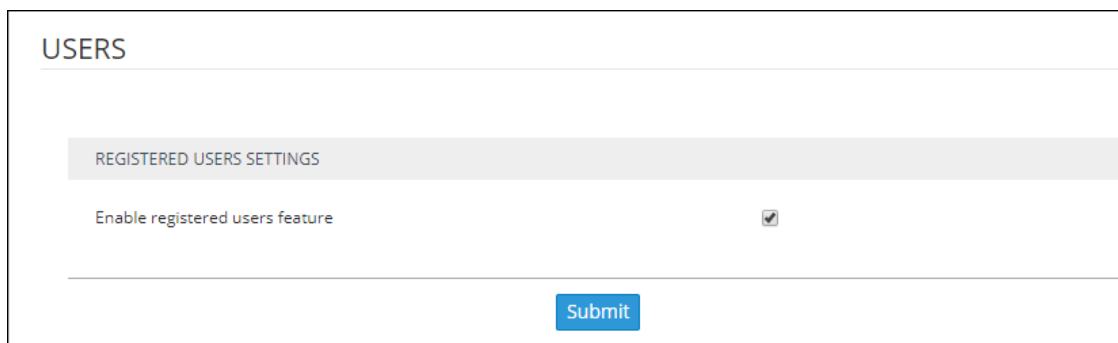
Adding Registered Users to the ARM

SBC registered users can be added to the ARM for the ARM to then be capable of performing call routing based on SBC user registrations. Each SBC has its own registered users. The added SBC registered users and their related information will be viewable in the ARM's Registered Users page shown in [Viewing Registered Users in the ARM](#) on page 135. To add registered SBC users to the ARM, operators need to first enable the feature as shown below. After the feature is enabled, the SBC registered users and their related information are taken from the SBC and added to the ARM. Later, when defining a Routing Rule, for example, operators can then route calls to SBC registered users (see [Adding a New Routing Rule](#) on page 268). The destination to which to route the call will depend on where - which SBC - the user performed the registration. In the Routing Rule definition, operators will select the appropriate routing condition, namely, that the call destination is an SBC registered user.

➤ **To add SBC registered users to the ARM:**

1. Open the Users page (**Settings > Advanced > Users**).

Figure 7-40: Users



2. Make sure the 'Enable registered users feature' option is selected and then click the **Submit** button.

Network Services Settings

The Syslog Server configuration settings can be edited as shown in [Editing a Syslog Server](#) below.

An NTP server can be added and its configuration settings edited as shown in [Adding/Editing an NTP Server](#) on page 194.

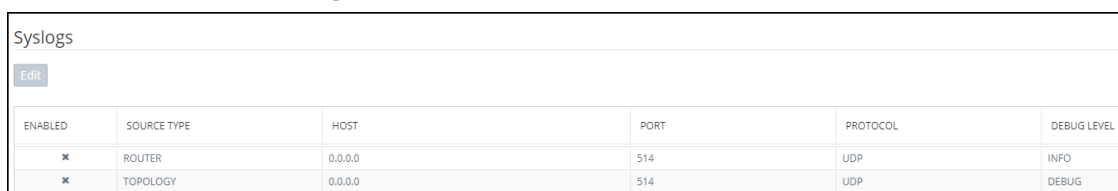
Editing a Syslog Server

The Syslog Server configuration settings can be edited to comply with your requirements.

➤ **To edit a Syslog Server:**

1. Open the Syslogs page (**Settings > Network Services > Syslog**).

Figure 7-41: Network Services



ENABLED	SOURCE TYPE	HOST	PORT	PROTOCOL	DEBUG LEVEL
x	ROUTER	0.0.0.0	514	UDP	INFO
x	TOPOLOGY	0.0.0.0	514	UDP	DEBUG

2. Select the Router or Topology row and then click the enabled **Edit** button.

Figure 7-42: Syslog Details

The figure shows two instances of the 'EDIT SYSLOG' dialog box. The top instance is configured for a Router with the following settings: Enabled (unchecked), Source Type (ROUTER), Host * (172.17.133.5), Port (514), Protocol (UDP), and Debug Level (TRACE). The bottom instance is configured for a Topology with the following settings: Enabled (unchecked), Source Type (TOPOLOGY), Host * (172.17.133.5), Port (514), Protocol (UDP), and Debug Level (DEBUG). Both instances have 'OK' and 'Close' buttons at the bottom.

3. Configure the syslog details using this table as reference.

Table 7-12: Syslog Details

Setting	Description
Host	IP address or host name of the remote syslog server to which messages are sent.
Port	Port of the remote syslog server to which messages are sent.
Protocol	Leave at default (UDP).
Debug Level	<p>From the 'Debug Level' drop-down menu select either:</p> <ul style="list-style-type: none"> ■ TRACE (default level for the Router; only messages whose debug level is TRACE are sent to the syslog server) ■ DEBUG (default level for Topology; only messages whose debug level is DEBUG and higher are sent to the syslog server)

Setting	Description
	<input type="checkbox"/> INFO <input type="checkbox"/> WARN <input type="checkbox"/> ERROR



When enabling syslog for a Router, there's a single syslog server for all Routing servers in the ARM. All ARM Routers send their syslog to this syslog server (at the same 'Debug Level'). This is necessary for proper calls debugging, as a single call can be processed by several different ARM Routers (they are state-less). For the ARM Configurator, however, you can assign a different syslog server.

Adding/Editing an NTP Server

An NTP server can be added and its configuration settings edited.

➤ To add an NTP server:

1. Open the NTP Servers page (**Settings** menu > **Network Services** tab > **NTP Servers** item).

Figure 7-43: NTP Servers

2. Click **Add**.

Figure 7-44: NTP Server Details

3. Configure the NTP server details using the following table as reference. The same details open when editing the server.

Table 7-13: NTP Server Details

Setting	Description
Name	Enter a name for the NTP server.
Address	Enter the IP address or host name of the NTP server.

4. Click **OK**.

Prioritizing Traffic Per Class of Service

The ARM supports Differentiated Services (DiffServ) protocol for specifying and controlling network traffic by class, so that certain types of traffic get priority over others.

DiffServ uses a 6-bit differentiated services code point (DSCP) in the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes.

The ARM lets you configure the DSCP value for outgoing packets coming from the ARM Configurator and from the ARM Routers. Different values for Gold, Silver and Bronze can be configured. The following table shows how protocols are mapped to class of service.

Table 7-14: Protocols Mapped to Class of Service

Application Protocol	Class of Service (Priority)	Traffic Type
HTTP/HTTPs	Gold	<ul style="list-style-type: none"> ■ Signaling/Control ■ Communication between node and ARM Configurator, node and ARM Configurators ■ Some communication between ARM Routers and ARM Configurator
JMS	Gold	Management affecting signaling. Critical communication between ARM Configurator and ARM Routers.
NTP	Gold	Control and Management
SNMP	Silver	Management (SNMP traps)
CDRs and Syslog	Silver	Management
LDAP	Silver	Management (for ARM users)
SSH	Bronze	Management

➤ **To configure the feature:**

1. Open the QoS page (**Settings > Network Services > QoS**).

Figure 7-45: QoS

QoS

QOS VALUES

Gold (HTTP/S, JMS, NTP):	46
Silver (SNMP, CDR, Syslog, LDAP):	24
Bronze (SSH):	12

Submit

2. Configure QoS values using this table as reference.

Table 7-15: QoS Settings

Setting	Description
Gold	[Application protocol: HTTP/S, JMS, NTP] You can change the default value of 46 to suit the requirements of your IP network. As part of IP network planning and optimization, the value can be changed to a value in the range between 0-63. The value determines priority of IP packets related to 'Gold' service.
Silver	[Application protocol: SNMP, CDR, Syslog, LDAP] You can change the default value of 24 to suit the requirements of your IP network. As part of IP network planning and optimization, the value can be changed to a value in the range between 0-63. The value determines priority of IP packets related to 'Silver' service.
Bronze	[Application protocol: SSH] You can change the default value of 12 to suit the requirements of your IP network. As part of IP network planning and optimization, the value can be changed to a value in the range between 0-63. The value determines priority of IP packets related to 'Bronze' service.

Enabling CDRs

The ARM allows you to enable Call Detail Records (CDRs) containing information on all calls routed by the ARM, including source and destination users, call duration and the call path. CDRs

are sent as Syslog packets to a server IP address that you need to configure.

➤ **To enable CDRs:**

1. Open the CDR page (**Settings > Network Services > CDR**).

Figure 7-46: CDR

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

Table 7-16: CDR Parameters

Setting	Description
Enabled	Select or clear the option to enable or disable CDRs.
Host	Enter the IP address of the server.
Port	Enter the server port.
Protocol	From the drop-down menu, select UDP (default) or TCP over which the CDRs will be sent.
Format	From the drop-down menu, select a format. You can select to have CDRs in clear text, JSON format, or in both.

Call Flow Configurations

The ARM's **Call Flow Configurations** tab under the Settings menu allows operators to configure

- Normalization Groups (see [Adding a Normalization Group](#) on the next page)
- Prefix Groups (see [Adding a Prefix Group](#) on page 200)
- Normalization before Routing (see [Normalization Before Routing](#) on page 207)
- Policy Studio (see [Policy Studio](#) on page 208)

- Web Services (see [Web-based Services](#) on page 224)

Adding a Normalization Group

You can add a Normalization Group. A Normalization Group can comprise one rule or multiple rules. If there are multiple rules in a group, manipulation is performed in the order the rules are listed. The output of the first rule will be the input of the next.

➤ **To add a Normalization Group:**

1. Open the Normalization Groups page (**Settings** menu > **Call Flow Configurations** tab > **Normalization Groups**).

Figure 7-47: Normalization Groups

Normalization Groups	
<div>Add Edit Delete Refresh</div>	
NAME	
123->321	
33->YY	
8 to mobile manip	
default lync number normalization	
internationalize local Israeli numbers	
non-USA to a permanent local American number	
remove '+1' from the number	
USA number to +1	
UserGroupMan	

2. Click **Add**.

Figure 7-48: Normalization Groups

The figure consists of two screenshots of a software dialog box titled "NORMALIZATION GROUP".

The top screenshot shows the initial state of the dialog. It has a "Group Name" text field at the top. Below it is a section labeled "Normalization Rules:" containing an empty list box. To the right of the list box are three buttons: a blue "+" button, a grey "-" button, and a grey "x" button. Below the list box is a section labeled "Rules Simulation:" containing a text input field and a blue "Test" button. To the right of the "Test" button is a label "Simulation Result:". At the bottom of the dialog are "OK" and "Cancel" buttons.

The bottom screenshot shows the dialog after one rule has been added to the "Normalization Rules" list. The rule is displayed as a text box with a "replace by:" label to its right. The "Rules Simulation" section remains the same, with the "Test" button and "Simulation Result" label. The "OK" and "Cancel" buttons are still at the bottom.

3. Use the following table as reference.

Table 7-17: Normalization Groups

Setting	Description
Group Name	Enter a Group Name for intuitive future reference.
Normalization Rules	<ol style="list-style-type: none"> 1. Click the + button adjacent to the pane as shown in the figure above. 2. In the left textbox, enter a regular expression. For more information about regular expressions, refer to online tutorials or see Examples of Normalization Rules on page 339. 3. In the replace by field, enter the text that will replace the found regex. You can use groups collected by brackets (...) in the regex in the replacement string using \$1, \$2,... See a regex tutorial for more information.
Rules Simulation: Test	<p>Use the rules simulation to test different possible inputs and verify that the regex sequence you entered produces the result you intended.</p> <ul style="list-style-type: none"> ■ Enter any value you want to test and click Test; the result of each individual rule is displayed to the right; the result of all the rules

Setting	Description
	together is displayed lowermost right.



After a Normalization Group is defined, you can attach it to a:

- Peer connection (see [Peer Connection Information and Actions](#) on page 41).
- Globally (see [Normalization Before Routing](#) on page 207)
- Routing Rule action (see [Adding a New Routing Rule](#) on page 268)
- LDAP attribute (see [Adding an LDAP Server to the ARM](#) on page 141)



The same Normalization Group can be reused/attached several times in any of the above cases.

Using Prefix Groups

Prefix Groups make routing management and Dial Plan management easier, more efficient and more convenient for telephony network operators. The feature also makes it possible to import an existing customer's Dial Plan into the ARM using the northbound REST API.

Every routing rule can have dozens of prefixes. Grouping prefixes and then associating groups with routing rules reduces visual complexity and allows for more effective management. Prefix Groups save operators from repeatedly having to add prefixes to rules.

Once defined, the Prefix Group comprising multiple prefixes is associated with a routing rule (see [Adding a New Routing Rule](#) on page 268 for information on how define a routing rule). If, for example, an enterprise has distributed offices, the following can be defined: If a caller calls from source prefix x, the call is sent from SBC 1; if a caller calls from source prefix 2, the call is sent from SBC 2.

To develop a customer-specific Dial Plan into an ARM Prefix Group, the REST API is available. This can significantly facilitate ARM provisioning.

Adding a Prefix Group

The ARM GUI conveniently allows network telephony operators to add a Prefix Group.

➤ To add a Prefix Group:

1. Open the Prefix Groups page (**Settings** menu > **Call Flow Configurations** tab > **Prefix Groups** item).

Figure 7-49: Prefix Groups

Prefix Groups		
<div> Add Edit Delete Refresh </div> <div>Enter search string <input type="text"/></div>		
NAME	TYPE	VALUES
ROULEAU_SK	PREFIX	306776
SASKATOON_SK	PREFIX	306(715-717,803,844,850,866),306(938,952,954,956,964,966),306(244,249,251,260,262,270,280,281,306)664...
COCAGNE_NB	PREFIX	506(345,576)
PORT PERRY_ON	PREFIX	2899(2,900)962,963,289(225,354,485,653,713)
KLEINBURG_ON	PREFIX	905(352,883),289(202,216,531,586,873)
VICTORIA_BC	PREFIX	250(952,953,978,984,995,999),250(380,389,391,405,410,412-415),778(922,966,967,972,977),250(536,580,588...
CAP PELE_NB	PREFIX	506(332,577)
JOCKVALE_ON	PREFIX	613(843,343)(212,385),613(440,459,512,823,825)
DELSLE_SK	PREFIX	306493
NISKU_AB	PREFIX	587(541,953),780(770,955,979)
HAIFA_NG	PREFIX	902(789,797,800,802,809,817-818),902(448-466,468-471,473-484,486-499,501),902(377,399,401-407,410,412)...
CLARKSON_ON	PREFIX	905(916,918),289(299,326,373,420,628),905(254,403,491,822,823,853),289(727,825,826,848,898,940)
METCALFE_ON	PREFIX	343390,613(274,821)
BALGONIE_SK	PREFIX	306(702,762,771)
ABERDEEN_SK	PREFIX	306253
LORETTE_MB	PREFIX	204(270,878,961)
COALDALE_AB	PREFIX	587360,403(345,405)
GIBBONS_AB	PREFIX	780(578,923)
SCHOMBERG_ON	PREFIX	905(590,939),289(318,557,574,592)
CARP_ON	PREFIX	343376,613(470,839)

- Click the **Add** button.

Figure 7-50: Add Prefix Group

ADD PREFIX GROUP

Name *

Type:

Prefix

Prefixes: *

Click to add a prefix

Showing 0 prefixes from a total of 0

Search for a prefix

Copy to clipboard

OK

Close

- Define a Prefix Group using the following table as reference.

Table 7-18: Add Prefix Group

Setting	Description
Name	Enter a name for the prefix group; the OK button is activated.
Type	Filter; from the drop-down select Prefix or Pool of Numbers . <ul style="list-style-type: none"> ■ Pool of Numbers: DID and emergency calls ■ Prefix: All the rest
Prefixes	<ul style="list-style-type: none"> ■ Click the field to add a prefix and then enter a single prefix or multiple prefixes: <ul style="list-style-type: none"> ✓ The syntax for prefixes in a Prefix Group is the same as for a single prefix in a Routing Rule (see Prefixes on page 338 for more information). ✓ Multiple prefixes can be copied from an external file and pasted into this field. ✓ Using the 'Copy to clipboard' feature, you can copy multiple existing prefixes in this field to the clipboard and then paste into an external file where you can view (for example) all prefix strings at once or count (for example) how many prefixes exist in the group.

4. Click **OK**; the Prefixes Group is created.
 - Associate the group with a rule's condition in the Routing page
 - The group can be associated with Source, Destination or both

Searching for a Prefix Group

The telephony network may include dozens of prefix groups and multiple prefixes within each group. The 'Enter search string' field in the Prefix Groups page allows the operator to quickly locate a group. After locating a group, the operator can view it and/or edit it.

See also [Validating Prefix or DID Uniqueness](#) on page 205.

Searching for a Specific Prefix within a Prefix Group

After locating a group in the Prefix Groups page using the 'Enter search string' field (for example), the operator can conveniently search in that group for a specific prefix (string).

➤ To search for a specific prefix in a group:

1. In the Prefix Groups page, select the group to search in.

Figure 7-51: Prefix Groups Page

NORMALIZATION GROUPS

PREFIX GROUPS

NORMALIZATION BEFORE ROUTING

POLICY STUDIO

Prefix Groups

Add

Edit

Delete

Refresh

toronto

⌵

⌵

NAME	TYPE	VALUES
TORONTO_ON	PREFIX	437[886-889,999],647[313,317-318,321,323-324,328-352],647[843-850,852-899,907,909,918-933],416[556-58...

- Click the activated **Edit** button.

Figure 7-52: Edit Prefix Group – Search for a Prefix

EDIT PREFIX GROUP

Name:

TORONTO_ON

Prefixes:

437[886-889,999] X

647[313,317-318,321,323-324,328-352] X

647[843-850,852-899,907,909,918-933] X

416[556-583,585-609,612-646,648-671,673-710] X

Search for a prefix

Copy to clipboard

OK

Cancel

EDIT PREFIX GROUP

Name:

TORONTO_ON

Prefixes:

647[590-591,599-602,606-609,618,620-639] X

647[267-274,277-278,280-300,302-303,308-309] X

647[360-362,367,376-386,388-393,400-409] X

647[556-560,567,575,580,588] X click prefix twice to edit...

647

Copy to clipboard

OK

Cancel

- In the 'Search for a prefix' field, enter the string to search for and then press Enter; the results are presented in **bold**.

Editing a Specific Prefix within a Prefix Group

After locating the Prefix Group and then the specific prefix within that group to edit, click the prefix twice and edit per requirements. The syntax for prefixes in a Prefix Group is the same as for a single prefix in a Routing Rule.

See [Prefixes](#) on page 338 for more information.

Viewing the Details of the Prefix Group Used for Routing

The ARM helps you determine what Prefix Group is used for routing. As deployment of the ARM has expanded, customer-managed dialing plans have grown more and more extensive (many Prefix Groups are being used in hundreds of Routing Rules and Policy Studio definitions). Sometimes, it's difficult to understand why a specific Routing Rule was selected by the ARM for Call Routing and where a specific Prefix Group is being used.

For this reason, in addition to the **Exact Match** DID search described in [Validating Prefix or DID Uniqueness](#) on the next page, the ARM gives operators a detailed description of the selected Prefix Group used in ARM routing. It covers both Policy Studio (pre-routing mechanism) and Routing Groups/Routing Rules.

When a Prefix Group is selected, its summary is displayed on the right side of the page:

Figure 7-53: Prefix Group Details

The screenshot displays the 'PREFIX GROUP DETAILS' interface. It includes the following elements:

- Name:** test_did
- Type:** NUMBER
- Values:** number1, number2
- Policy studio:** (indicated by a horizontal line)
- Used in policy studio:** numberPS
- Routing rule:** (indicated by a horizontal line)
- Used in routing rules:**
 - customer_test
 - test_prefix_group
 - NUMBER_src
 - NUMBER_dst

If the selected Prefix Group is not used in Policy Studio, Policy Studio will be indicated as 'None'. The same applies to Routing Groups. If a Prefix Group is used in multiple Routing Groups, all of them will be listed.

Figure 7-54: Prefix Group Details

>>

PREFIX GROUP DETAILS

Name:

AG10

Type:

PREFIX

Values:

101000905[1000-9999]#, 101000904[1000-9999]#, 101000193[1000-9999]#, 101000354[1000-9999]#, 101000245[1000-9999]#, 101000017[1000-9999]#, 101000336[1000-9999]#, 101000832[1000-9999]#, 101000522[1000-9999]#, 101000301[1000-9999]#, 101000679[1000-9999]#, 101000632[1000-9999]#, 101000932[1000-9999]#, 101000290[1000-9999]#, 101000697[1000-9999]#,...

Policy studio

Used in policy studio:

None

Routing rule

Used in routing rules:

▼

Calls To Israel

Nati

▼

AttributeGroup1

routingAttributeGroup_19

▼

AttributeGroup4

routingAttributeGroup_49

▼

RG_PHOENIX

RR_PHX_92PORTESDEF16

RR_PHX_92PORTESDEF15

Validating Prefix or DID Uniqueness

The ARM helps you validate a prefix or a specific DID. As deployment of the ARM has expanded, customer-managed dialing plans have grown more and more extensive (many Prefix Groups with hundreds of prefixes, or complete phone numbers in a single group). Sometimes, it's difficult to preserve the uniqueness of a specific DID (or prefix) definition so you may sometimes erroneously define Routing Rules with a specific prefix (or DID) but the same prefix (or DID) matches a different Prefix Group / Routing Rule.

➤ To validate if a specific DID (phone number) is part of an existing Prefix Group:

1. Open the Prefix Groups page (**Settings > Call Flow Configurations > Prefix Groups**).

2. Search for the 'Name' of a Prefix Group, filter its 'Type' and search for an exact string ('Value') if it appeared as part of the Prefix Group. This functionality is preserved when the 'Value' option is selected or a 'Search string' is provided.
3. In the Search filter, select the **Exact Match** option to find all Prefix Groups that match the exact phone number.

Figure 7-55: Exact Match

Enter search string

Name:

Type:

☐ Value:

☒ **Exact Match:**



The **Exact Match** option finds a number even if it fits a 'range' or another pattern in the Prefix Group. In the following example, an **Exact Match** search was applied for DID **2121004811005** and was found as part of Prefix Group **AG21** (for example) because it's in the range **212100481[1000-9999]#**.

Figure 7-56: Search Results

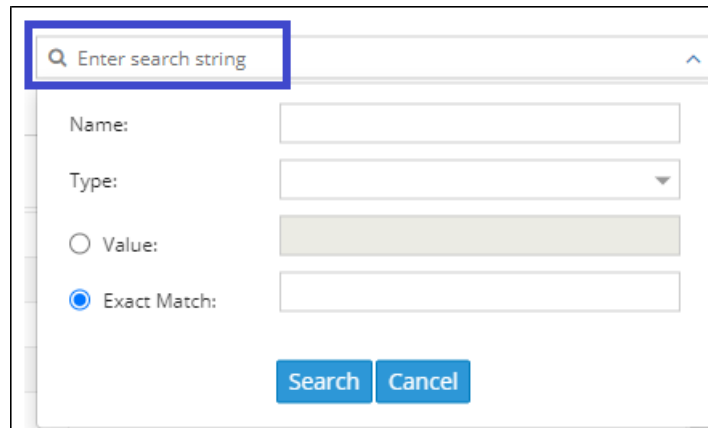
Prefix Groups

NAME	TYPE	VALUES
AG21	PREFIX	212100481[1000-9999]# 212100285[10...
nonEmptyPG	PREFIX	[1-2], [2-3]
tt	PREFIX	1, 2, 3, 4, 5...



Searching in the Search string option doesn't search by **Exact Match**; only searching by 'Name' and 'Value' does.

Figure 7-57: Search by 'Name' and 'Value'

A search dialog box with a search bar at the top containing the placeholder text "Enter search string". Below the search bar are four input fields: "Name:" (text), "Type:" (dropdown), "Value:" (text, preceded by a radio button), and "Exact Match:" (text, preceded by a radio button and selected). At the bottom are "Search" and "Cancel" buttons.

Normalization Before Routing

A normalization rules group can be applied to a routing request's source user part and to a routing request's destination user part. See [Adding a Normalization Group](#) on page 198 for information on how to add a normalization rules group.

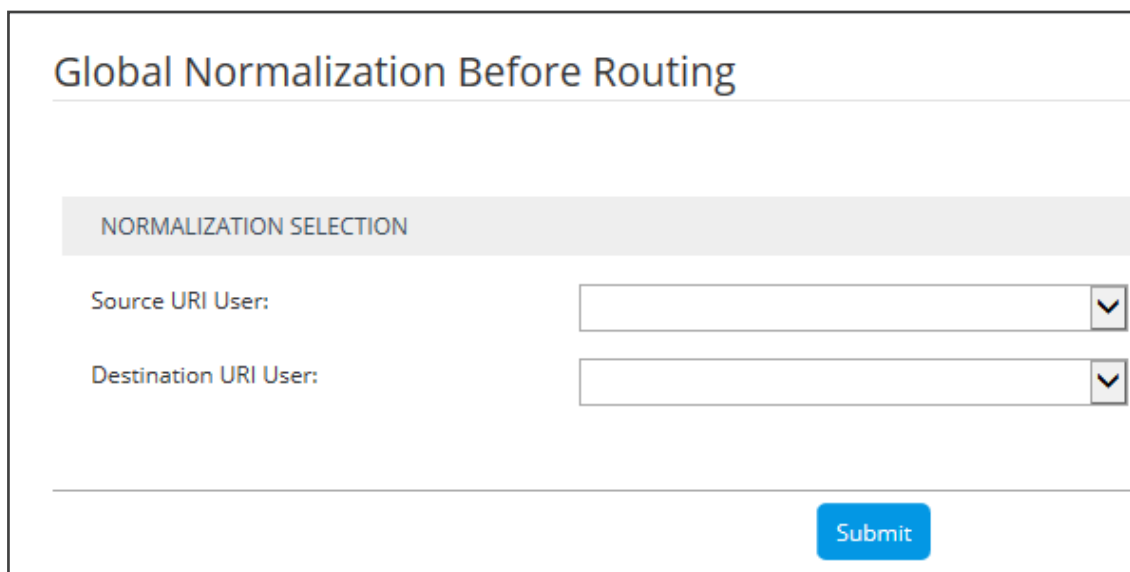
When the ARM receives a routing request, it normalizes the routing request's source user part with the chosen Normalization Group, and the routing request's destination user part with the chosen Normalization Group.

'Global Normalization Before Routing' parameters configured in this page are used globally for the entire network as pre-routing normalization. This global normalization can be overwritten at a Peer Connection level with other Normalization Rules if required (see under [Peer Connection Information and Actions](#) on page 41).

➤ To attach a normalization rules group globally before routing:

1. Open the Normalization Before Routing page (**Settings** menu > **Call Flow Configurations** tab > **Normalization Before Routing** item).

Figure 7-58: Normalization Before Routing

A page titled "Global Normalization Before Routing". Below the title is a section header "NORMALIZATION SELECTION". Under this header are two dropdown menus: "Source URI User:" and "Destination URI User:". At the bottom right is a blue "Submit" button.

2. Use the following table as reference.

Table 7-19: Normalization Before Routing

Setting	Description
Source URI User	From the drop-down menu, select the normalization rules group. This will be the normalization on the Source URI User field.
Destination URI User	From the drop-down menu, select the normalization rules group. This will be the normalization on the Destination URI User field.

3. Click **Submit**.

Policy Studio

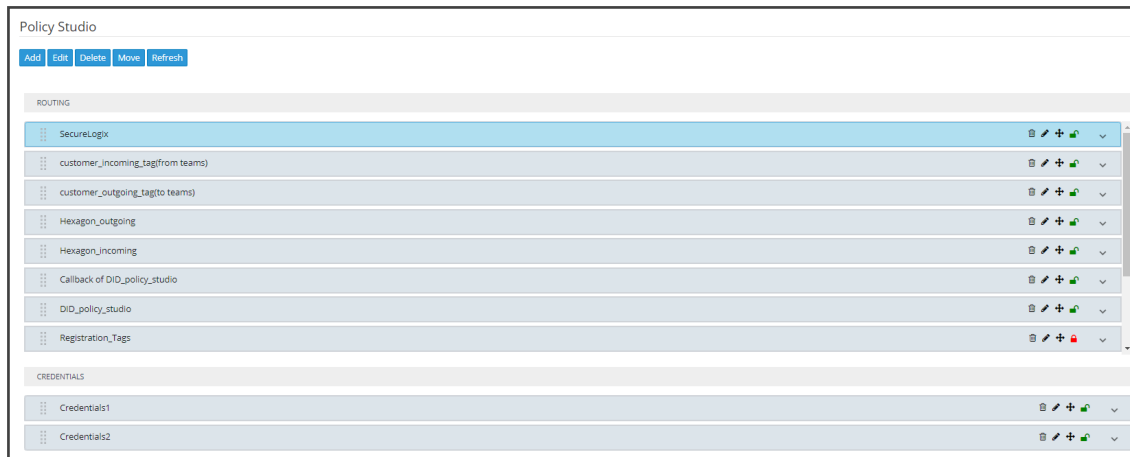
This feature allows adding to route requests information that is not contained in the route requests but which is taken from the Users page. To accomplish this with legacy products without ARM, the LDAP server must be queried for every call using complex query rules, creating delays and straining the server. In the ARM, the Users page is loaded to memory and information gathering is handled internally in real time. Policy Studio Use Examples:

- Each user has an internal 4-digit extension and an unrelated external phone number. When a user makes a call outside the enterprise, the source number, i.e., the user's extension, must be replaced with their external number. When a call comes in from outside, the external number must be replaced with the user's extension.
- Same as the previous example but, in addition, there can be more than one user with the same extension, and what differentiates them is their hostname. The ARM can locate the user based on a combination of the extension and hostname attributes.

Policy Studio is a set of rules. Each rule contains a match condition and an action. The match condition is a set of route request fields to be compared, and a set of user properties to be compared to. The match condition also has a source node or Peer Connection or set of source nodes or Peer Connections. The action is a set of route request or response fields to be replaced, and a set of user fields to replace them with. For every route request received, the ARM processes all the rules from top to bottom. For each, the ARM searches in the users table for a user that matches all the fields. If a user is not found, the ARM proceeds to the next rule. If a user is found, the ARM stops parsing the rules and performs the action in this rule. The action is to replace all the listed fields with the properties of the user, as configured.

➤ To add a Policy Studio rule:

1. Open the Policy Studio page (**Settings > Call Flow Configurations > Policy Studio**).

Figure 7-59: Policy Studio

2. Click **Add**.

Figure 7-60: Add Call Item - User (default)



The 'ADD CALL ITEM' dialog box is shown with 'Type' set to 'User'. The 'MATCH' section on the left contains several dropdown menus for 'Source Nodes', 'Source Peer Connections', 'Source Resource Groups', 'Source Prefix / Prefix Groups', 'Destination Prefix / Prefix Groups', 'Source User Groups', and 'Destination User Groups'. The 'ACTION' section on the right has a 'SOURCE_URI_USER' dropdown and a 'Flow' dropdown set to 'Stop'. There are 'OK' and 'Cancel' buttons at the bottom.

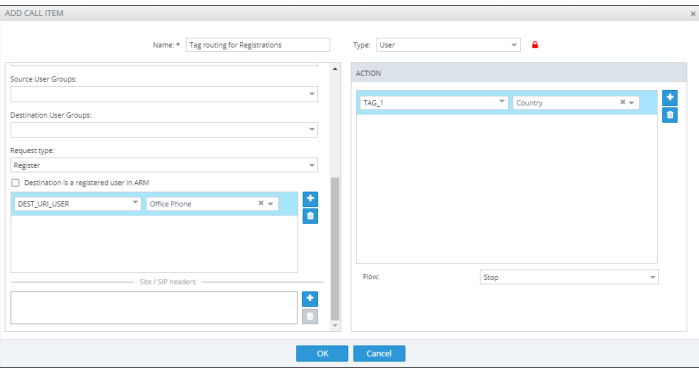
Figure 7-61: Add Call Item - Web Service

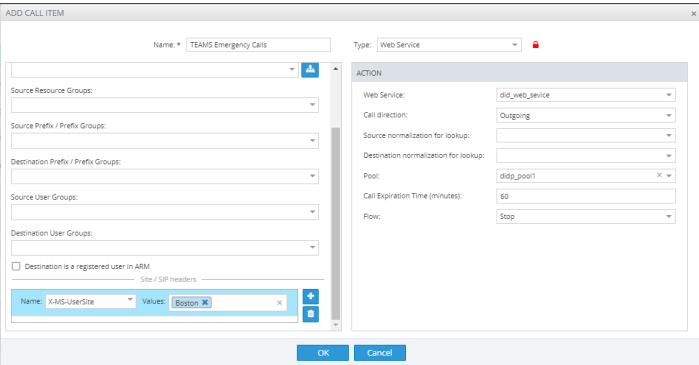
The 'ADD CALL ITEM' dialog box is shown with 'Type' set to 'Web Service'. The 'MATCH' section on the left is identical to the previous dialog. The 'ACTION' section on the right has a 'Web Service' dropdown and a 'Flow' dropdown set to 'Stop'. There are 'OK' and 'Cancel' buttons at the bottom.

3. Configure the settings using the following table as reference.

Table 7-20: Policy Studio Settings

Setting	Description
Name	Defines the name of the Policy Studio rule to add, to facilitate management of the feature.
User / Web Service	<p>Policy Studio supports two uses, as shown in the preceding two figures:</p> <ul style="list-style-type: none"> ■ User (default). Select this option to use Policy Studio based on information taken from ARM Users Data. ■ Web Service. Select this option to use an external web service for pre-routing manipulation. See also Web-based Services on page 224.
MATCH	The set of match conditions for finding a user from the Users table. Click + to add more conditions.
Source Nodes	<p>From the drop-down, select a Node or set of Nodes for which this rule will be used. Alternatively, click the adjacent  button to select a Node or set of Nodes from the Topology Map. If left empty, the rule is used regardless of the origin of the call.</p> <p>Note: To select multiple elements in the Choose Topology Item screen, press Ctrl and click the elements.</p>
Source Peer Connections	<p>Select a Peer Connection or set of Peer Connections for which this rule will be used. Alternatively, click the adjacent  button to select a Peer Connection or set of Peer Connections from the Topology Map.</p> <p>If left empty, the rule is used regardless of the origin of the call.</p> <p>Note: To select multiple elements in the Choose Topology Item screen, press Ctrl and click the elements.</p>
Source Resource Groups	Select a set of Nodes or a set of Peer Connections for which this rule will be used. If left empty, the rule is used regardless of the origin of the call.
Source Prefix / Prefix Groups	Allows a Prefix or a Prefix Group to be configured as the 'Source' in a Policy Studio condition. Optionally add the condition for users' information-based pre-routing.
Destination Prefix / Prefix Groups	Allows a Prefix or a Prefix Group to be configured as the 'Destination' in a Policy Studio condition. Optionally add

Setting	Description
	the condition for users' information-based pre-routing.
Destination is a registered user in ARM	If this option is selected, the Policy Studio rule will be matched <i>only</i> if the destination number is a registered user's number (listed in the Registered Users table).
Request type	<p>This condition in a Policy Studio rule of type 'User' allows differentiation between a Policy Studio rule to be used for call setup and a Policy Studio rule to be used for routing registration messages.</p> <p>Default: Call.</p> <p>Configure (switch) 'Request type' to Register if you want to use the Policy Studio rule for registration messages manipulations / prerouting manipulation.</p> <p>The following example applies pre-routing tagging to all registration messages based on value Country of the Users table, which can later be used for Tag-based routing. For example, route users registration to different SoftSwitches based on the value of Country.</p> 
SIP Header	<p>Select a route REQUEST field from the following available fields (this is a field from the route REQUEST that is compared with the user properties):</p> <ul style="list-style-type: none"> ■ SOURCE_URI_USER (default) ■ SOURCE_URI_HOST ■ DEST_URI_USER ■ DEST_URI_HOST ■ CONTACT_URI_USER ■ CONTACT_URI_HOST ■ CONTACT_URI_PORT

Setting	Description
	<ul style="list-style-type: none"> ■ P_ASSERTED_IDENTITY_DISPLAY_NAME ■ P_ASSERTED_IDENTITY_USER ■ P_ASSERTED_IDENTITY_HOST <p>If a call matches the selected criterion, the manipulative action you select will be performed. For a SIP field manipulation example, see Example 2 under Example 2 of a Policy Studio Rule on page 215.</p>
Site	<p>Allows configuring a 'Site' condition as a matching criterion. This is necessary for DID masking in the case of an E911 (Teams emergency call and call-back). See also DID Masking on page 228. The matching criterion is needed to provide a separate range of DID numbers for Teams emergency calls on a per-site basis.</p> <p>Teams uses a proprietary LMO (Local Media Optimization) header to indicate the user's current site: X-MS-UserSite, shown in the next figure. See also Configuring a Microsoft Teams LMO Topology on page 82.</p>  <p>A DID masking Policy Studio rule matching this attribute enables you to manage emergency numbers with a separate pool of numbers for each site (coordinated with Teams definitions). In the example shown in the preceding figure, the SIP field X-MS-UserSite is set to Boston; emergency calls with a call-back Policy Studio rule will consequently only be applied to calls from the 'Boston' site. Note that this field allows multiple values to be set; the same rule will then be applied to multiple sites.</p>
ACTION	<p>The set of replacement actions that will be performed on the route request and route response fields for a found user.</p>

Setting	Description
Action field	<p>Select a route request or route response field from the following available fields (when a user is found, this field will be replaced with the value of the configured user properties):</p> <ul style="list-style-type: none"> ■ SOURCE_URI_USER ■ SOURCE_URI_HOST ■ DEST_URI_USER ■ DEST_URI_HOST ■ DEST_IP_ADDR ■ DEST_PORT ■ DEST_PROTOCOL ■ USER_CREDENTIALS_USER_NAME ■ USER_CREDENTIALS_PASSWORD ■ P_ASSERTED_IDENTITY_DISPLAY_NAME ■ P_ASSERTED_IDENTITY_USER ■ P_ASSERTED_IDENTITY_HOST <p>Multiple actions can be defined. Click + to define another action.</p> <p>Note: If either USER_CREDENTIALS_USER_NAME or USER_CREDENTIALS_PASSWORD is used in an action, you must add <i>both</i>.</p> <p>For a SIP field manipulation example, see Example 2 under Example 2 of a Policy Studio Rule on page 215.</p>
Request User Property	<p>Select a set of user properties. The request field is compared to these properties of the users. If any of the properties of a user is equal to the value of the field, then this condition is considered a match.</p>
Replacement User Property	<p>Select a set of user properties. The action is to replace the value in the request or response field with the value of this user property. If the found user has no value for this property, then no action is done on this field. If there more than one property is listed here, then ARM replaces the field with the first property if the user has it. If the user does not have it, ARM proceeds to the next property in the list, in the configured order.</p>

Setting	Description
Flow	<p>Allows operators to exercise an option to control the action to be executed after a Policy Studio rule is matched. Use the following as reference when configuring 'Flow':</p> <ul style="list-style-type: none"> ■ Stop. This is the default action. When the rule is matched, the ARM stops and continues to Routing Rule matching. ■ Continue. The ARM continues to the next matching Policy Studio rule. ■ Continue to policy studio rule. The ARM continues to the next matching Policy Studio rule from a specific Policy Studio rule. This essentially triggers execution of the rule.



Fields such as 'Source Nodes' and 'Source Peer Connections' in Policy Studio's Add Call Item screen and Edit Call Item screen feature filters in which network administrators can select multiple elements and then *invert the selection*. The feature improves usability and user experience especially in large networks with high numbers of elements. The feature allows network administrators to

- Select a single element
- Delete a single element (x)
- Select All elements
- Clear all selected elements
- Select All and delete a few (x)
- Select All, delete a few (x) and then invert the selection; the elements deleted will be in the selection
- Select a few elements and then invert the selection; only elements that weren't selected will be in the selection
- Clear a selection

Example 1 of a Policy Studio Rule

Refer to the defined Policy Studio rule shown in the figure depicting the Call Item Settings screen:

- For every route request coming from node New_York_1, the ARM will search for a user whose *office phone* property is equal to the value of the SOURCE_URI_USER field.
- ARM will then replace the SOURCE_URI_USER field with the value of the found user's *External Number* property.

Figure 7-62: Policy Studio Rule Example 1

The figure displays two screenshots of the "ADD CALL ITEM" dialog box, illustrating different configurations for a Policy Studio Rule.

Top Screenshot:

- Name:** Replace extension with external number
- Type:** User
- MATCH Section:**
 - Source Nodes: New_York_1
 - Source Peer Connections:
 - Source Resource Groups:
 - Source Prefix / Prefix Groups:
 - Destination Prefix / Prefix Groups:
 - Source User Groups:
 - Destination User Groups:
- ACTION Section:**
 - Flow: Continue to policy studio rule
 - Continue to rule: *

Bottom Screenshot:

- Name:** Replace extension with external number
- Type:** User
- MATCH Section:**
 - Source User Groups: SOURCE_URI_USER
 - Destination User Groups: SOURCE_URI_USER
 - Request type: Call
 - Destination is a registered user in ARM: ☐
 - Office Phone: SOURCE_URI_USER
 - Site / SIP headers:
- ACTION Section:**
 - Flow: Continue to policy studio rule
 - Continue to rule: *

Example 2 of a Policy Studio Rule

The ARM's Policy Studio Rule allows you to manipulate a rule to provide Location Based Emergency calls routing in a CCE environment with ARM capabilities. Refer to the defined Policy Studio Rule shown in the following figure.

Figure 7-63: Policy Studio Rule Example 2

In the rule above.

- The node sends a route request to the ARM. The request includes the two fields under MATCH and the values configured for them; if one and/or the other exists and their values are those configured, then the manipulations configured under ACTION will be used in response to the route request:
 - DEST_URI_USER will be replaced by *branch emergency number*
 - P_ASSERTED_IDENTITY_USER will be replaced by *company site main number*
 - P_ASSERTED_IDENTITY_DISPLAY_NAME will be replaced by *empty column*

Adding a Policy Studio Rule for Users Credentials Information

The SBC can function as authentication server for SIP messages requests. The SBC is used to store the users (SIP phones) credentials information. Irrespective of under which local SBC in the network the phone is located, the ARM provides a centralized point for global credentials management of all SIP phones in a network. The SBC requests the ARM to provide credentials for specific users. This information is stored in the ARM users database. When the SBC needs to authenticate a user, it sends a REST request to the ARM to obtain the credentials for that user and then sends the 'challenge' for credentials back to the client. The client then resends the request with an Authorization header (containing a response to the 'challenge') and the authentication process continues regularly. Request for authentication is relevant for INVITE and for REGISTER requests coming from a SIP phone. The following figures show the flows:

Figure 7-64: Request for Authentication: Invite Sequence

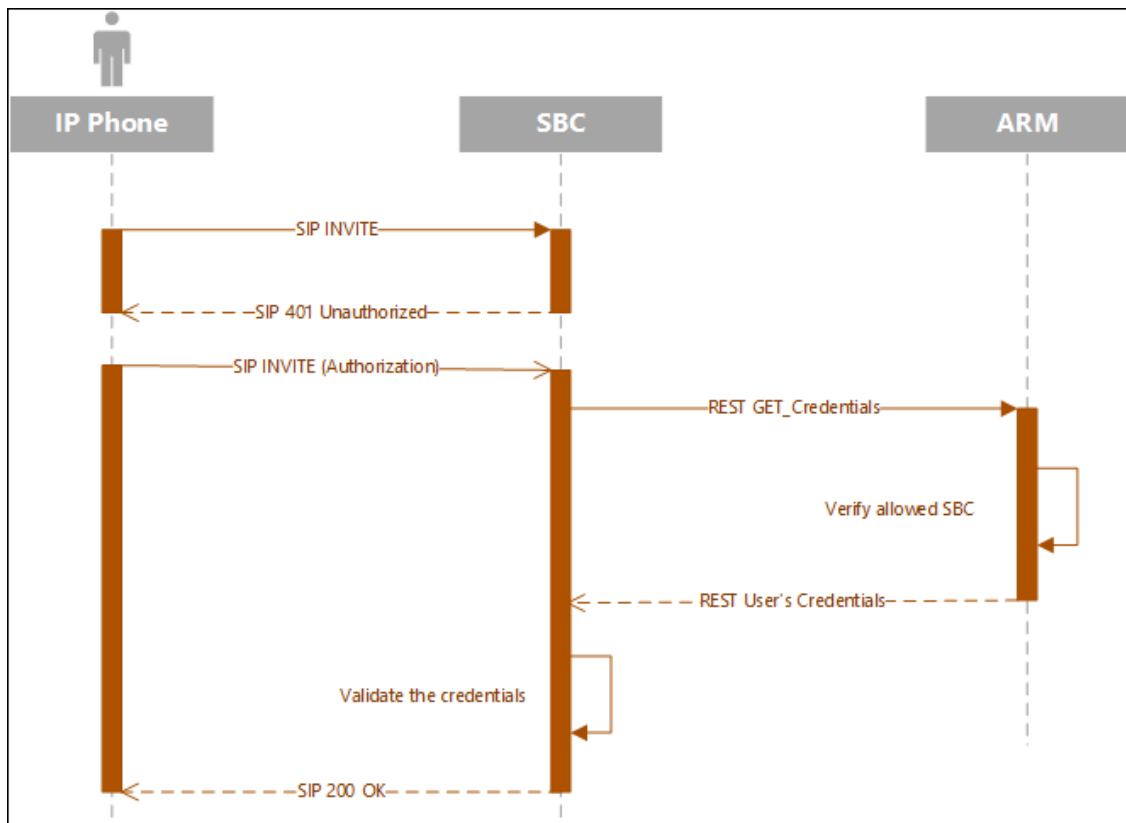
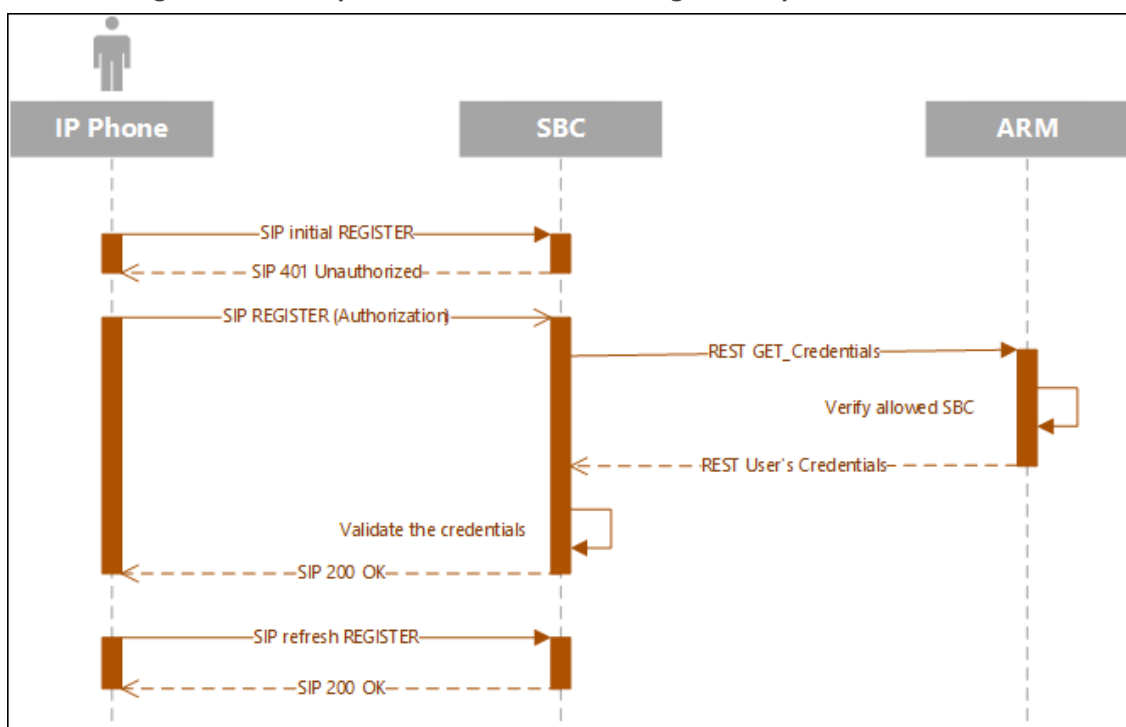


Figure 7-65: Request for Authentication: Register Sequence





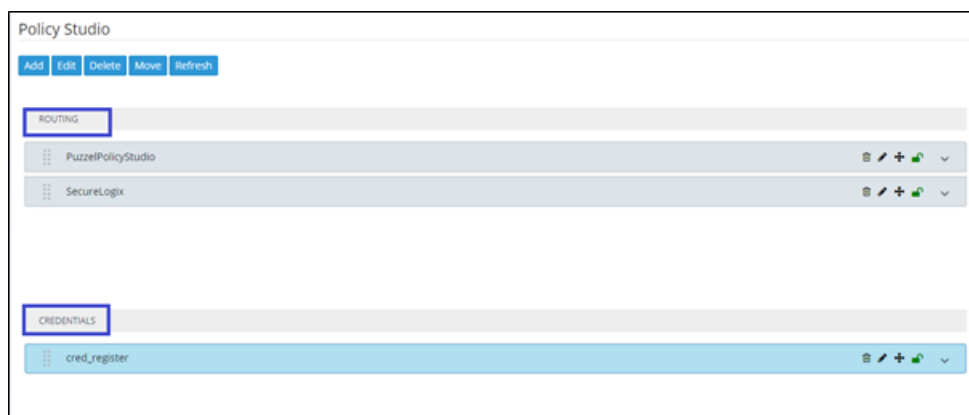
To configure the SBC to send the above REST API to the ARM, you need to configure an IP Group with specific settings in the SBC's Web interface. For more information, see [Configuring the SBC to Send the REST API](#) on page 220.

The operator should prepare credentials information to be provided to the SBC upon credentials requests. The information should be part of the ARM users database. The operator must define a dedicated dictionary attribute where the credentials will be stored for each authorized SIP phone. The information is provided by the ARM using the Policy Studio matching feature. Policy Studio is divided into two types of rules: (1) Policy Studio Rules designated for Routing and (2) Policy Studio Rules designated for Credentials. The operator who does not source ARM credentials information does not need to define Credentials Policy rules and can use the regular functionality of Policy Studio for Calls and Registrations pre-routing smart manipulations.

➤ **To add a Policy Studio rule for credentials information:**

1. Add a rule and select **Credentials** from the rule's 'Type' drop-down. The newly created rule will automatically be placed in the 'Credentials' section in the Policy Studio screen to distinguish it from Routing related rules.

Figure 7-66: Policy Studio - Credentials



2. The matching criteria for Policy Studio of type **Credentials** must be **User_URI** and (optionally) **HOST_URI**. This information is used as a unique identifier to find the correct entry in the Users page to retrieve requested credentials information.



These are the only properties that can be used for matching of the credentials request.

3. Optionally apply the following matching criteria to narrow the group of users to whom this service (of supplying credentials by the ARM) is provided:
 - Source Node
 - Source Peer Connection
 - Source Resources group

- Source users group

Figure 7-67: Add Call Item - Type 'Credentials' - User_URI / HOST_URI matching criteria



If the ARM does not find in the users database a match for a specific URI_USER and (optional) URI_HOST, it will return a 404 (not found) HTTP response to the SBC (and consequentially, to the SIP phone). If you want to have a configuration in which every user (SIP phone) is allowed to register only upon specific conditions (for example, only from certain IP Group/Peer Connection or Group of Peer Connections or Nodes, etc.), it can be done by a combination of Match (condition) part of the Credential Policy Studio rule and a specific action named **Discard_Credentials** relevant for credentials rules only. In this case, although the user is found but is not authorized for the specified IP group or SBC, the ARM will respond with a 403 HTTP response (forbidden).

For example, the following rule of type **Credentials** named **DiscardUnauthorizedCredentialRequests** will not provide credentials for a request coming from node 'China' for users who are part of the 'United States' users group; the ARM will respond with a 403 HTTP response (forbidden).

Figure 7-68: Policy Studio - Add Call Item



The order (priority) of the rules in Policy Studio is important. For example, if an operator added 'Discard Credentials' but there is a higher rule with the same match criteria, all users in the 'Discard Credentials' rule will be authorized (the higher rule will be applied).

Configuring the SBC to Send the REST API

The SBC must be configured to send the REST API to the ARM as described in [Adding a Policy Studio Rule for Users Credentials Information](#) on page 216.

➤ To configure the SBC to send the REST API to the ARM:

- In the SBC's Web interface, configure an IP Group with specific settings.
 - For **REGISTER** messages: In the SBC's Web interface in IP Group settings, under the 'SBC Registration and Authentication' section, configure parameter 'Authentication Method List' to **REGISTER** and from the 'SBC Server Authentication Type' drop-down, select **ARM Authentication**.

Figure 7-69: SBC Web interface - SBC Registration and Authentication - REGISTER

SBC REGISTRATION AND AUTHENTICATION	
Max. Number of Registered Users	-1
Registration Mode	User Initiates Registration
User Stickiness	Disable
User UDP Port Assignment	Disable
Authentication Mode	SBC as Server
Authentication Method List	REGISTER
SBC Server Authentication Type	ARM Authentication
OAuth HTTP Service	-- View
Username	
Password	

- For **INVITE** messages: In the SBC's Web interface in IP Group settings, under the 'SBC Registration and Authentication' section, configure parameter 'Authentication Method List' to **INVITE** and from the 'SBC Server Authentication Type' drop-down, select **ARM Authentication**.



- The INVITE/REGISTER is received in the incoming Pcon.
- To configure INVITE or REGISTER to the same incoming Pcon, configure parameter 'Authentication Method List' to **INVITE|REGISTER**.

Figure 7-70: SBC Web interface - SBC Registration and Authentication - INVITE

SBC REGISTRATION AND AUTHENTICATION	
Max. Number of Registered Users	-1
Registration Mode	User Initiates Registration
User Stickiness	Disable
User UDP Port Assignment	Disable
Authentication Mode	SBC as Server
Authentication Method List	INVITE
SBC Server Authentication Type	ARM Authentication
OAuth HTTP Service	-- View



- The feature involves changes in the SBC ↔ ARM REST internal REST API
- The feature is supported starting from SBC version 7.20A.259.031

Tag-based Routing

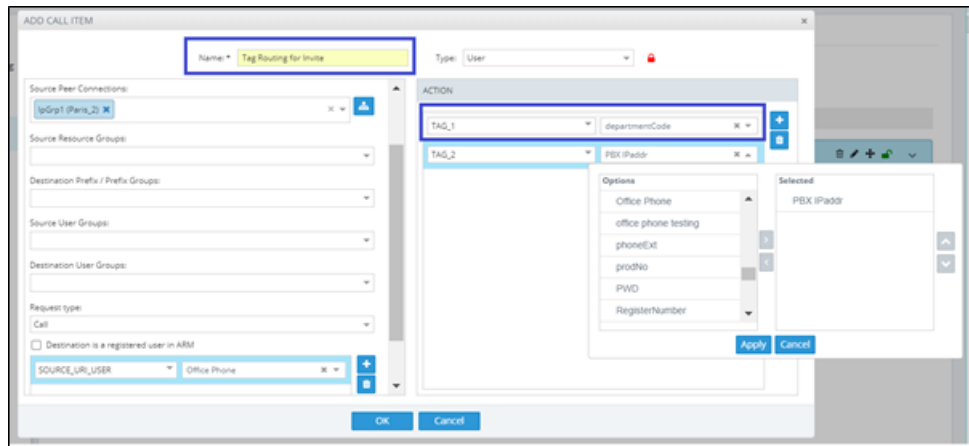
The ARM increases flexibility in the flavors of the routing criteria by adding 'Tag-based routing' as a routing method. This routing method allows operators to assign Tags to the messages to be routed by the ARM, and to use these Tags' values as routing criteria. The feature can be applied for the routing of both call and registration messages. Multiple Tags can be assigned to a single message (up to three) and all these Tags' values can be used for routing matching.

Here's how to assign Tags in Policy Studio rules. The Tag value can be assigned using Policy Studio capabilities (ARM pre-routing functionality engine). The Tag value can be taken from any field of the user's Property Dictionary the operator would like to use for further routing. This capability can only be applied to the Policy Studio rule whose 'Type' parameter is configured to **User**. The regular matching criteria with all the available parameters applies to Tag assigning as well.

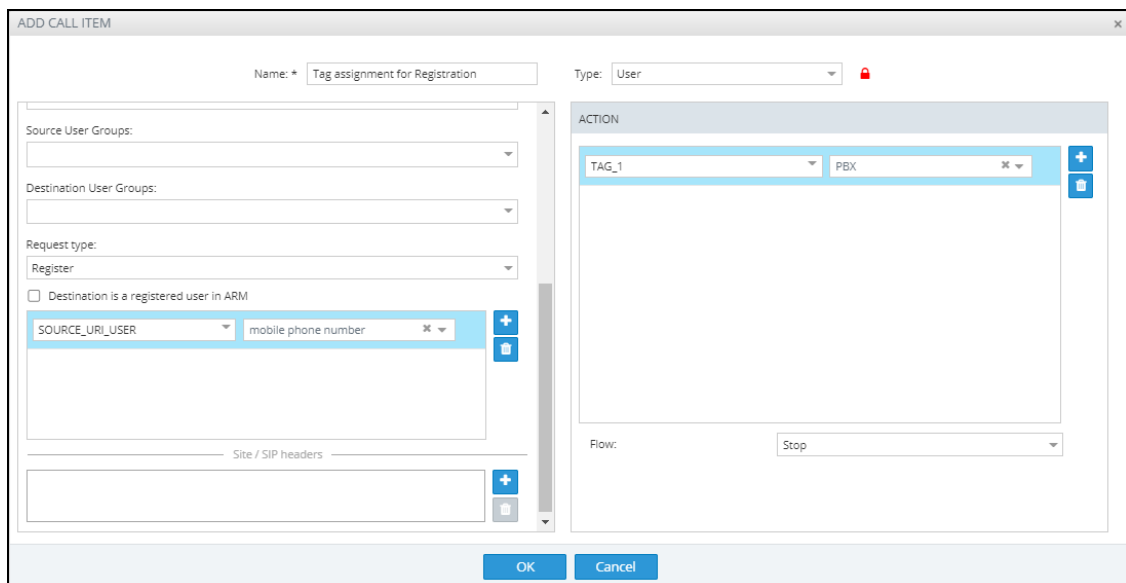
➤ To assign a Tag

- Under the 'Action' section in the 'Add Call Item' screen that opens when adding a Policy Studio rule, select one or more Tags (TAG_1, TAG_2, TAG_3) and assign it with one or more attributes from the Property Dictionary. The value of this Property Dictionary for matching the user will be factored in for the corresponding TAG value and will be used for further routing.

The following example shows a Policy Studio rule named 'Tag Routing for Invite' applicable for calls setup routing coming from a specific Peer Connection to the user's office phone. This Policy Studio rule will assign the value **DepartmentCode** of the user to TAG_1 and **PBXIPAddr** to TAG_2. Both Tags can later be used in Routing Rules.

Figure 7-71: Values assigned to Tags in Policy Studio rule

The next example uses Policy Studio to assign a Tag value for registration messages (rule named 'Tag assignment for registration'. TAG_1 gets the value from the **PBX IP** attribute of the user matching the user's mobile phone.

Figure 7-72: Value assigned to Tag for registration messages in Policy Studio rule

Tag values assigned to a routing request in Policy Studio can be further used as matching criteria in Routing Rules. Tag-based Routing Rules can be applied when 'Request type' is configured to **Calls** or **Registration**. Tag matching criteria are available in ARM Routing Rules under the **Advanced Conditions** tab.

➤ **To apply a Tag-based Routing Rule:**

- In the Add Routing Rule screen (**Routing > Routing Groups > click the Add Rule button**) under the **Advanced Conditions** tab under the 'Tags' section, add a row by clicking the + icon and then select Tag 1, Tag 2 or Tag 3 (according to which Tag was assigned to the routing request in Policy Studio (TAG_1, TAG_2 or TAG_3). Note that it's important that the same Tags in Policy Studio are assigned with values for future matching criteria in Routing Rules. One Routing Rule can have a Tag-matching condition involving multiple values of the

same Tag and involving more than one Tag in the same condition. In this case, matching is calculated as follows:

- Several values for the same Tag are treated as 'or'
- Several Tags in the condition are treated as 'and'

In the following example, the rule named 'RouteCallBased Tagging' has a Tag-based condition as routing criteria. It will be matched if Tag 1's value is either **RandD** or **Sales**. Assuming that Tag1 got its value of **Department IP** in Policy Studio, this Routing Rule allows routing based on this value.

Figure 7-73: Value assigned to Tag in 'Add Routing Rule' screen

In some cases , the same functionality for routing can be achieved using a Users Group or Tag-based routing. You can use either method of implementation but in the case of a high number of users (more than 1 million), using Tag-based routing is more efficient and preferable.

Users Group as Matching Criterion

The ARM allows you to use a Users Group (or multiple Users Groups) as a matching criterion in the Policy Studio. You can specify a User Group (or Groups) as source ('Source User Group') and / or destination ('Destination User Groups') matching criteria. This criterion can be applied for all types of Policy Studio rules:

- **User** 'Type' for Routing based on information from the Users page
- **Web services** 'Type' for Routing
- **Credentials** 'Type' for users credentials data based on groups of users (for example, for users of a certain country)

For Web services, this feature allows narrowing the criteria for accessing the external Web service, which can be very expensive (as in the case of security-based routing consultations). In the following example, it will attempt accessing security services only for United States users:

Figure 7-74: Users Group as matching criterion

Security consultation for USA users

Match

Destination User Groups:
United States

Action

Number Portability: SecureLogix

In the case of user 'Type', this criterion allows you to perform, for example, different manipulations for users of a certain country, with the ability to differentiate them in 'From' and 'To':

Figure 7-75: Users Group as matching criterion

ADD CALL ITEM

Name: Replace Office Dlx with Mobile Type: User

Destination Prefix / Prefix Groups:

Source User Groups:
United States

Destination User Groups:
France

Israel
China
United States
Reception desk
Shabbat_Special
Imp. People
Chatterers

ACTION

DEST_URI_USER mobile phone

All Clear Invert OK Cancel

Web-based Services

The ARM supports number portability solutions for querying an external source for additional information about each call. It also provides a general infrastructure for any future Web-based service that can impact ARM call routing. The prominent example is to query a number portability server that contains a database of every phone number in the country, and the actual carrier network that it currently belongs to.



- The feature is invisible in the ARM *unless enabled in the License Key*.
- The feature can conform to any protocol or design using a plug-in which AudioCodes will provide *per the protocol required by the customer*.

➤ To configure a Web service:

1. Open the Web Services page (**Settings > Call Flow Configurations > Web Services**)

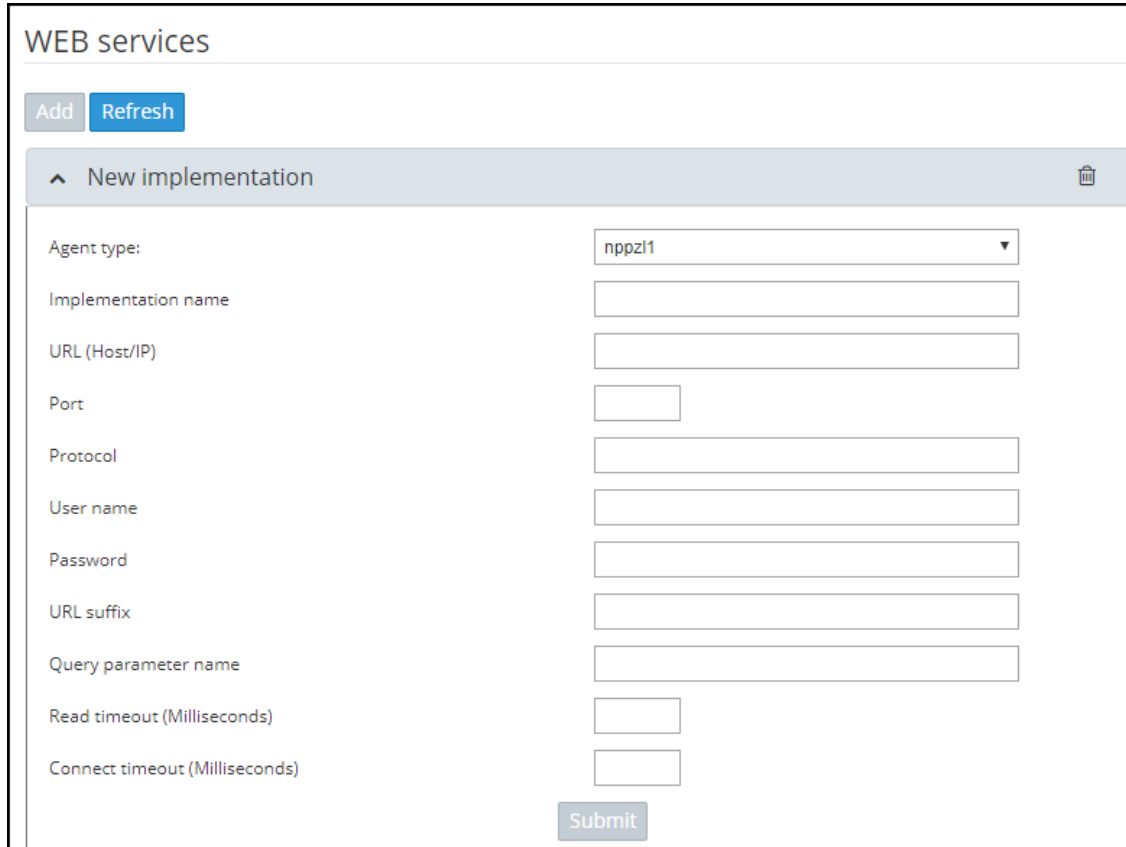
Figure 7-76: Web Services



WEB services


Add Refresh

2. Click **Add**.



WEB services

Add Refresh

^ New implementation 

Agent type:

Implementation name:

URL (Host/IP):

Port:

Protocol:

User name:

Password:

URL suffix:

Query parameter name:

Read timeout (Milliseconds):

Connect timeout (Milliseconds):

Submit

3. Configure the Web service you require in the New Implementation screen.



Parameters in the screen are *per customer* and therefore differ from one customer to the next. Contact your AudioCodes representative if necessary for clarifications.

4. If you're using the SecureLogix's Orchestra One call authentication service plugin for security based routing, define the Web Server as Agent type **npslx1** for communication with SecureLogix's Orchestra One call authentication service, as shown in the figures below. This plugin includes the REST API for ARM communication with Orchestra One.
5. In the field 'Implementation name', define the name of the web server; the name will be used in the ARM's Policy Studio.
6. In the 'Security Mode' field, define **Standard** or **Advanced** and in the 'Strategy' field define **0** or **1** as shown in the next figures.

Figure 7-77: SecureLogix - Standard Mode

Secure Logix

Agent type: npslx1

Implementation name: Secure Logix

Security Mode: Standard

URL (Host/IP): 10.1.2.3

Port: 8181

Protocol: http

Api Key Header Name: x-api-key

Api Key Header Value: 123456

URL suffix: v1/authengine/requestservice/request

Http Read timeout (Milliseconds): 2000

Http Connect timeout (Milliseconds): 1000

Sending SIP headers (Enable/Disable): ☐

Strategy: 0

Remote Server Timeout: 1000

Submit

Figure 7-78: SecureLogix - Advanced Mode

Secure Logix

Agent type: npslx1

Implementation name: Secure Logix

Security Mode: Advanced

URL (Host/IP): 10.1.2.3

Port: 8181

Protocol: http

Api Key Header Name: x-api-key

Api Key Header Value: 123456

URL suffix: v1/authengine/requestservice/request

Http Read timeout (Milliseconds): 2000

Http Connect timeout (Milliseconds): 1000

Sending SIP headers (Enable/Disable): ☒

Strategy: 1

Remote Server Timeout: 1000

Submit

- **Standard mode.** Checks for *basic security verification strategy*. The 'Strategy' field is set to **0** and read-only.
- **Advanced.** Calls are verified with the Orchestra One server. For example:
 - ◆ For 'Strategy' value **1**, Orchestra One will 'Authenticate using the Verizon Call Verification Service (VCVS) when applicable'.
 - ◆ When 'Strategy' is set to **1**, operators will be able to set it to **1** or higher. For **Advanced** mode, it's typically necessary to enable the 'Sending SIP headers' option.

7. Click **Submit**.



If you're using the SecureLogix plugin for security based routing:

- The newly-defined Web Server must then be assigned in Policy Studio for pre-routing processing and consultation with SecureLogix's Orchestra One. See step 8 below for more information, as well as [Policy Studio](#) on page 208.
- When adding a new Routing Rule, the **Security call score** option under Security Based Routing must be selected. See [Adding a New Routing Rule](#) on page 268, step 10 for more information.



If you're using the Hexagon Fraud Management Solution plugin for security based routing:

- Hexagon gives an "OK" to route a call
- Hexagon blocks an illegal call from entering the enterprise
- Hexagon is sent a "Notify" for a call from the enterprise

8. Apply the service: Open the Policy Studio (**Settings > Call Flow Configurations > Policy Studio**) and click **Add**.

Figure 7-79: Policy Studio - Add Call Item

9. Select number portability as shown in the preceding figure. The default is **User** to preserve the existing functionality of Policy Studio. Previously, operators were limited to using Policy Studio based on information taken from ARM Users Data (the default **User** option) but can now select the option to use (an external) **Web Service** for pre-routing manipulation, for example, SecureLogix's Orchestra One (to apply security-based routing). Using the Policy Studio rule's 'condition' feature, operators can reduce the number of consultations that will be made with SecureLogix's Orchestra One. The ARM will perform the consultation only for calls matching the rule criteria. In this way, customers can perform consultations only for calls coming from a specific node (or group of nodes), or from specific Peer Connections or from specific Resource Groups. The destination Prefix (or Prefix Group) also can be used as call matching criteria.
10. Policy Studio can be applied to a specific condition (see under MATCH in the preceding figure):
 - Source Nodes and / or Peer Connections and / or Source Resource groups

- Destination Prefix and / or Prefix groups
- Applicable for ARM registered users

11. View the external Web Service (SecureLogix, for example) configured in Policy Studio:

Figure 7-80: External Web Service 'SecureLogix' Configured in Policy Studio



DID Masking

Network administrators can assign Direct Inward Dialing numbers to AudioCodes' media gateway so that PSTN network users can *directly reach* VoIP network users. The gateway connects the PSTN network to the VoIP network, routing and translating calls between the two. A call from a PSTN user is directed to the VoIP user who holds the corresponding DID number.

The feature has two main applications:

- It masks the enterprise's internal phone numbers while allowing return calls to the original caller. A bank, for example, can use the feature to change an employee's phone number to the bank's global number so that when a customer calls the global number back, they'll directly call the same employee who originated the call.
- It changes the outgoing phone number to a local phone number of the destination location from a predefined pool of numbers while allowing return calls to the original number which is in a different location; this opens a private use case.

The feature supports calling an emergency service (E911) using the local number of a user who is not located in that country / region and also supports receiving a return call from the emergency service. For example, an employee visiting a different office branch must call an emergency service. The call in this case is originated with the telephone number of the branch and when the emergency service operator calls back, they'll get to the employee who called.

The capability is achieved by saving the mapping between the original source number, the destination number and the number used to hide the original caller. This mapping is shared across all the ARM Routers so no matter which ARM Router received the return call, it will be routed to the original caller.

The mapping is saved in a Redis database which operates in a master-slave mode. By default, the master is in the ARM Configurator and the slaves are in the ARM Routers. Each Router has its own Redis instance. The mapping of the outgoing call is saved in the master Redis instance which is replicated to each ARM Router. The incoming call is first looked up in the local Redis instance before going to the master Redis instance. This reduces delay and network traffic.

The default master location can be changed. This should be done mainly for large enterprises whose CPS is high enough to put a high load on the ARM Configurator.



The default behavior is to add the original caller phone number as an X-Header and not manipulate the destination number directly.

➤ **To enable DID in the ARM:**

1. In the ARM GUI's Web Services page (**Settings > Call Flow Configurations > Web Services**), add a new Web Service of agent type **DID masking**.

Figure 7-81: DID Masking

2. Define the service's parameters using the following as a reference:
 - **Agent type:** The type of web service for the DID masking feature, in the preceding figure it is defined as **did_masking**.
 - **Implementation name:** The name of the web service; the name will be used in the ARM's Policy Studio.
 - **Query Timeout:** The timeout of the lookup for a call, in milliseconds.
 - **Connect timeout:** The master Redis instance's timeout. After the time expires the master is indicated as unavailable from the ARM Router's perspective. The time is in milliseconds.
 - **Password:** The password of the master Redis instance
 - **Use Configurator as master:** By default, this option is selected; the ARM Configurator is by default used as the master of the Redis instance. If the option is cleared, a new option is displayed for the host and the port of the new master.
 - **Redis debug level enabled:** By default, this option is cleared. The option enables more detailed logging in the Redis.
3. After you **Submit**, add a Prefix Group of a new type 'Pool of Numbers' and then define a pool of numbers that will be used as the DID masking numbers, as shown in the next figure:

Figure 7-82: Add a Prefix Group of New Type 'Pool of Numbers'

ADD PREFIX GROUP

Name *

Type: Pool Of Numbers

Numbers: * Click to add a number

+972081121 ✕ ✕

Showing 1 numbers from a total of 1

🔍 Search for a number

[Copy to clipboard](#)

OK Close

4. Define the group's parameters using the following as a reference:
 - 'Type': Must be set to **Pool of Numbers**. When the Prefix Group is of this type, the numbers inside will be handled as full numbers (as if they ended in a #).
 - 'Numbers': Defines the numbers inside the pool.
5. Define a new Policy Studio of action type 'Web Service'. Select the DID masking web service and then configure:
 - a. a condition for when to perform masking (under 'Match')
 - b. the direction of the call, either outgoing or incoming, *per the matching condition* because the ARM doesn't have the capability to 'find' the direction of a call.
 - c. Source and Destination normalization for the lookup operation; this only manipulates the URIs for the Redis and has no effect on the URI for the routing operation.

If the direction of the call is *outgoing*, the following must be configured:

- d. Pool of numbers from which the manipulated number will be picked. The field can remain empty. If left empty, the ARM will not perform any manipulation but will simply save the destination and source number mapping which is useful in cases when the manipulation itself is performed after the ARM routing.
- e. Call expiration time
- f. The flow of the Policy Studio

After creating an outgoing Policy Studio rule, the ARM automatically creates an incoming Policy Studio rule above the outgoing rule. The name of the rule will be 'Callback of Outgoing rule name'. Most attributes will automatically be defined. The rule can be updated to give the operator more control over how the callback is executed.

If the direction of the call is incoming, the following must be configured:

- g. How ARM Routers should look up the incoming call in the Redis:
 - i. Source and Destination number
 - ii. Only the Source number -or-
 - iii. Only the Destination number

Make your selection per your network requirements. For example, if some sort of normalization was performed prior to the ARM routing (e.g., the same destination number for all calls).

Figure 7-83: Add Call Item - How ARM Routers should look up the incoming call in the Redis

6. Configure using the following as reference:
 - **Web Service:** The web service that will be used for the action manipulation.
 - **Call direction:** The direction of the matched call: Outgoing or Incoming.
 - **Source normalization for lookup:** Normalization to perform on the Source URI before the operation in the Redis. The normalization has no effect on the URI itself. It's useful when the Source number changes in one of the directions.

- **Destination normalization for lookup:** Normalization to perform on the Destination URI before the operation in the Redis. The normalization has no effect on the URI itself. It's useful if the Destination number changes in one of the directions.

For *outgoing* calls:

- ◆ **Pool:** The pool of numbers from which the ARM will pick the manipulated number. If this field is empty, the ARM will not perform manipulation and will only save the Source to Destination number mapping.
- ◆ **Call Expiration time:** The time a call is saved in the database. Defines the length of time ARM allows a return call before discarding the mapping.
- ◆ **Flow:** Defines what the ARM should do after this Policy Studio rule is matched

For *incoming* calls:

Figure 7-84: Incoming Calls

7. Configure using the following as reference:

- **Match incoming calls by:** Defines how the ARM looks up a return call that was masked.
 - ◆ **Source and Destination number.** ARM performs the lookup using a combination of both the caller's number and the masked number. The original caller will be retrieved only if the return call came from the same destination number that was originally called.
 - ◆ **Destination.** This is a looser lookup option. The ARM performs it using the masked number. The last number masked to the number is retrieved, allowing a return call from any calling number to the number from the pool. It's typically used for E911 scenarios in which the E911 operator's source number doesn't have to be the E911 number.
 - ◆ **Source.** ARM performs the lookup by the Source number. This option is useful when the Destination number is a static number (like E911) and identification of the call can only be performed using the Source number. The latest number mapped to the number is retrieved.

In the preceding figure, for example, the Policy Studio rule will mask all outgoing calls from **prefix '+033'** with numbers from the pool **'pool for DID traffic'** and save the mapping for the return call for one hour.

When an incoming call matches any number in the pool, the ARM retrieves the original number that initially called and replaces the destination with the original number.

Routing Settings

Configuring Criteria for a Quality Profile

You can configure criteria for a quality profile for bad, fair or good call paths based on the calculation of MOS and ASR. You can configure a specific Peer Connection to exclude either the MOS or the ASR criterion (see [Peer Connection Information and Actions](#) on page 41). After enabling 'Use Quality Based Routing' (see the following figure), the quality status of Peer Connections and Connections will be displayed in the network map's Quality Layer. The configured quality profile can be associated with a Routing Rule (see [Adding a New Routing Rule](#) on page 268) which will be applied only if all Peer Connections and Connections in the route meet the criteria.



The quality of voice on a line is calculated based on the quality of voice measured in multiple calls over a period. The ARM issues alarm indications for quality change.

➤ To configure a quality based routing condition:

1. Open the Advanced Conditions screen (**Settings > Routing > Quality Based Routing**). By default, **Use Quality Based Routing** is selected. If it isn't, select it.

Figure 7-85: Configuring Criteria for a Quality Profile

Quality Based Routing

☒ Use Quality Based Routing

MOS

1 ————— 4 ————— 5

1 < good >= 4
fair < 4
bad <= 1

ASR

0% ————— 25% ————— 75% ————— 100%

25% < good >= 75%
fair < 75%
bad <= 25%

Submit

2. Activate either MOS, ASR or both and then configure criteria by dragging the range indicators to the lower and upper limit you require. Use the following table as reference.

Table 7-21: Configuring Criteria for a Quality Profile

Quality Condition	Description
MOS (Mean Opinion Score)	<p>Specified by ITU-T Recommendation P.800, MOS is the average grade on a quality scale of Good to Failed, given to voice calls made over a VoIP network, after testing.</p> <p>MOS-LQ = listening quality, i.e., the quality of audio for listening purposes; it doesn't take bi-directional effects, such as delay and echo into account.</p> <p>MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects.</p>
ASR (Answer-Seizure Ratio)	Measurement of network quality and rate of successful calls. % of answered calls relative to the total call volume.

3. Click **Submit**; a quality profile is generated which you can associate with a Routing Rule (see [Adding a New Routing Rule](#) on page 268).

Configuring a Time-Based Routing Condition

The time-based routing feature allows you to configure a routing rule activated only at the time specified in a time condition. You can configure a condition and then associate it with a routing group or a routing rule, or both (see [Adding a New Routing Rule](#) on page 268 under 'Advanced Conditions').

➤ To configure a time-based routing condition:

1. Open the Time-Based Routing screen (**Settings > Routing > Time Based Routing**).

Figure 7-86: Time Based Routing

Time Based Routing	
Add Edit Delete Refresh	
NAME	TYPE
Not working hours	PERIOD
Week-ends (Israel)	WEEKLY
Every Day night - not in Sunday	WEEKLY

2. Add a time-based routing condition: Click **Add**; the Time Condition screen is displayed.

Figure 7-87: Time Condition

Time Condition

☒ DAILY ☐ WEEKLY

name:

time selection

start time

end time

all day

UTC:

Local time: 03:00 03:00

start time should be before the end time

time period

☐ enable period

start of period

end of period

UTC:

OK

Cancel

Figure 7-88: Time Condition - Example

TIME CONDITION [X]

name:

time selection

MON TUE WED **THU** **FRI** **SAT** SUN

☐ enable monday

UTC: start time 00 00 end time 00 00 all day ☒

Local time: 03: 00 03: 00

time period

☐ enable period

UTC: start of period 02-Jul-17 00 00 end of period 02-Jul-17 23 55

OK Cancel

3. Configure a time-based routing condition. Use the following table as reference. See the preceding figure for an example.

Table 7-22: Time Condition

Time Condition	Description
Daily/Weekly	<p>Select either Daily or Weekly.</p> <p>Daily - This is a daily recurring period.</p> <p>Weekly - This is a period recurring on given days of the week.</p> <p>The figure above shows a configured weekly condition. Green 'day' button: activated on that day. Blue 'day' button: selected to configure it.</p>
Name	Enter an intuitive name to later easily identify the condition when applying it.
Start time	From the drop-downs, select the hour and the minutes past the hour.

Time Condition	Description
	The times are configured in UTC (Coordinated Universal Time).
End time	From the drop-downs, select the hour and the minutes past the hour
All day	Select this option to base the routing condition on the entire day.
Enable period	Select this option to base the routing condition on a period.
Start of period	From the calendar icon, select the date on which the period will start. From the drop-downs, select the hour and the minutes past the hour.
End of period	From the calendar icon, select the date on which the period will end. From the drop-downs, select the hour and the minutes past the hour.

- Click **OK**; a profile is generated which you can associate with a Routing Rule (see [Adding a New Routing Rule](#) on page 268 under 'Advanced Conditions'). Also, you can associate the configured time condition with a Routing Group. In this case, it will apply to *all* Routing Rules in the Group. Note that the same time condition profile can be reused multiple times.

Configuring Alternative Routing SIP Reasons

Operators can configure SIP responses in the Alternative Routing SIP Reasons page (**Settings > Routing > Alternative Routing SIP Reasons**), in the SIP RESPONSE section; the ARM will then apply alternative routing paths if available. SIP reasons for call re-routing are globally configured here. If a SIP reason in this section is activated, the ARM tries to perform alternative routing if this SIP reason is returned at the initial routing failure.

Figure 7-89: Alternative Routing SIP Reasons

Alternative Routing SIP Reasons		
Add Edit Delete Duplicate Refresh		
NAME	DESCRIPTION	PEER CONNECTIONS
Primary SIP reason group	The default alternative SIP reason group	
sip reason group 1	reason group 1	
sip reason group 2	reason group 2	
sip reason group 3	reason group 3	
sip reason group 4	reason group 4	
sip reason group 5	reason group 5	
AT&T SIP reason group	To be used for AT&T trunk	
Add Edit Delete		
SIP RESPONSE	DESCRIPTION	ACTIVE
10	does not defined	✓
302	Move temporary	✓
404	Not Found	✓
405	Method Not Allowed	✓
408	Request Timeout	✓
413	Request Entity Too Large	✓
414	Request-URI Too Long	✓

Operators, however, sometimes need to apply different *sets* of SIP reasons for alternative routing, *per Peer Connection*, mainly due to the different flavors in the handling of alternative

routing with PBXs or specific SIP trunks and Service Providers. The upper section of the page provides this functionality. So in addition to the global (default) settings in the lower section of the page under SIP RESPONSE, operators can provide a different set of SIP reasons for alternative routing *per Peer Connection*.

Operators can define several 'SIP reasons groups' in the upper section of the page. See [Configuring a SIP Reason Group](#) on the next page for more information. By default, there is a 'Primary SIP reason group' attached and activated for the entire ARM (for all ARM Peer Connections).



If a call fails and the SIP response received from the remote side is not configured in the SIP Alternative Route Reason page, the ARM will not apply an alternative route for the call.

The page allows operators to change the default ARM behavior for an Alternative Routing decision.

➤ **To configure an Alternative Routing SIP Reason:**

1. In the lower section of the Alternative Routing SIP Reasons page (**Settings > Routing > Alternative Routing SIP Reasons**), under SIP RESPONSE, click **Add**.

Figure 7-90: Adding an Alternative Routing SIP Reason

The screenshot shows a dialog box titled "ADD SIP REASON" with a close button (X) in the top right corner. Inside the dialog, there are three input fields: "SIP Response", "Description *", and "Active" (which is a checkbox). At the bottom of the dialog, there are two buttons: "OK" and "Close".

2. Enter the SIP Response number (200-600).
3. Provide a description of the reason.
4. Select the **Active** option to activate the configuration.
5. Click the now-enabled **OK** button.

➤ **To edit a SIP Alternative Route Reason:**

1. In the Alternative Routing SIP Reasons screen, select the SIP response to edit.



SIP responses are listed in numerical order. You can browse to the next page or to the last page of responses. You can browse to the page before the page you are on, if you're not on the first page, or you can browse to the first page.

2. Click **Edit**.

Figure 7-91: Editing an Alternative Routing SIP Reason

3. Edit per your requirements and click **OK**.



By clearing the 'Active' option, the operator can 'deactivate' a SIP reason without deleting its row in the table. If a SIP reason is 'deactivated', the ARM will not apply an alternative route. The ARM will function as if there is no row at all. The 'deactivated' row, however, remains in the table, and if the operator re-decides, it can be 'reactivated' by selecting the 'Active' option.

➤ **To delete an Alternative Routing SIP Reason:**

1. In the Alternative Routing SIP Reasons screen, select the SIP response to delete.

Figure 7-92: Deleting an Alternative Routing SIP Reason

2. Click **Delete**.

Configuring a SIP Reason Group

Operators can define several 'SIP reasons groups' in the upper section of the Alternative Routing SIP Reasons page (**Settings > Routing > Alternative Routing SIP Reasons**). By default, there is a 'Primary SIP reason group' attached and activated for the entire ARM (for all ARM Peer Connections). Additional groups can be defined, either from scratch or duplicated from an existing group, and later attached to a specific Peer Connection (or several Peer Connections). Operators can:

- Add a new group (with an empty SIP reasons table)
- Duplicate group
 - Change the name of the group.
 - View the SIP reasons section and select/unselect the values.

■ Edit group

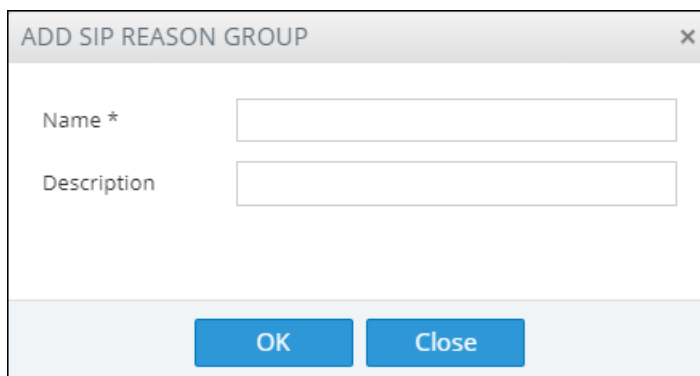
- Edit the name and description of the group.
- Delete group (the default 'SIP reason group' cannot be deleted)
- Refresh

Each 'SIP reason group' has the following properties:

■ Name**■ Description****■ Peer Connection that contains the 'SIP reason group'.****➤ To add a SIP Reason Group:**

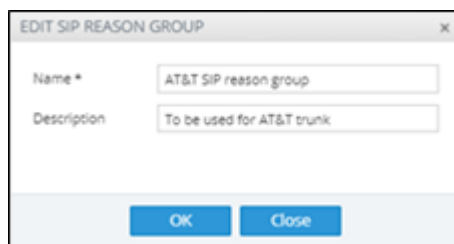
1. In the upper section of the Alternative Routing SIP Reasons page (**Settings > Routing > Alternative Routing SIP Reasons**), click **Add**.

Figure 7-93: Add SIP Reason Group



2. When adding (or editing) a group, provide a name for the group and an optional description.

Figure 7-94: SIP Reason Group - Name, Description



3. Select a group; view and edit the group's SIP reason that is then displayed.

Figure 7-95: Select a SIP Reason Group

Alternative Routing SIP Reasons

[Add](#) [Edit](#) [Delete](#) [Duplicate](#) [Refresh](#)

NAME	DESCRIPTION	PEER CONNECTIONS
Primary SIP reason group	The default alternative SIP reason group	ipGrp0(New_York_1),ipGrp1(New_York_1),ipGrp0(Park_2),ipGrp1(Park_2)
sip reason group 1	reason group 1	
sip reason group 2	reason group 2	
sip reason group 3	reason group 3	
sip reason group 4	reason group 4	
sip reason group 5	reason group 5	
AT&T SIP reason group	To be used for AT&T trunk	

[Add](#) [Edit](#) [Delete](#)

SIP RESPONSE	DESCRIPTION	ACTIVE
480	Temporarily Unavailable	<input checked="" type="checkbox"/>
481	Temporarily Unavailable	<input checked="" type="checkbox"/>
482	Loop Detected	<input checked="" type="checkbox"/>
483	Too Many Hops	<input checked="" type="checkbox"/>
500	Server Internal Error	<input checked="" type="checkbox"/>
501	Not Implemented: The SIP request method is not implemented here	<input checked="" type="checkbox"/>
502	Bad Gateway	<input checked="" type="checkbox"/>
503	Service Unavailable	<input checked="" type="checkbox"/>

- To duplicate an existing SIP reason group, provide a new unique name and an optional description:

Figure 7-96: Duplicate a SIP Reason Group

DUPLICATE SIP REASON GROUP

Name *

Description

SELECTED	SIP RESPONSE	DESCRIPTION	ACTIVE
<input checked="" type="checkbox"/>	421	Extension Required	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	422	Session Interval Too Small	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	480	Temporarily Unavailable	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	481	Temporarily Unavailable	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	482	Loop Detected	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	483	Too Many Hops	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	500	Server Internal Error	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	501	Not Implemented: The SIP r...	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	502	Bad Gateway	<input checked="" type="checkbox"/>

[OK](#) [Close](#)

- Attach a newly-defined SIP reason group to one or more Peer Connections (using both Add and Edit screens), either in the Network Map page or from the Peer Connections page:

Figure 7-97: Attach a SIP Reason Group to Peer Connection/s

EDIT PEER CONNECTION

Type: IPGroup

Name: * IpGrp1

Weight: 50

Node: New_York_1

Voip Peer: 2_ATandT_SIPt_1

Normalization Before Routing

Source URI User:

Destination URI User:

Advance Conditions

Cells quota: q1

CAC Profile:

Alternative SIP reason group: AT&T SIP reason group

☒ use global quality definitions

☐ use specific quality definitions

☒ MOS ☐ ASR

OK

6. View the SIP reason group in the Peer Connection summary and table. The indication of Peer Connection associated with the group is shown in the SIP reason group table:

Figure 7-98: Peer Connection associated with a group


By default, all Peer Connections are associated with the default SIP reason group.

Configuring Global Routing Settings

The ARM enables global routing settings to be configured.

➤ To configure global routing settings:

1. Open the Global Routing Settings page (**Settings** menu > **Routing** tab > **Routing Settings** item).

Figure 7-99: Global Routing Settings

Global Routing Settings

ROUTING ATTEMPTS

Maximum number of routing attempts:

Maximum routes per Peer Connection:

Maximum routes per Voip Peer:

CALLS

Maximum number of unselected rules to be shown:

Submit

- Configure the parameters using the following table as reference.

Table 7-23: Routing Attempts

Setting	Description
Maximum number of Routing Attempts	Defines the maximum number of routing attempts per call. If the maximum number of routing attempts has not yet been reached, the ARM searches for an alternative routing possibility for the specific call.
Maximum number of routing attempts per Peer Connection	Defines the maximum number of routing attempts per Peer Connection. If the maximum number of routing attempts has not yet been reached, the ARM tries to re-route the call to a preferable Peer Connection. Default: 2 attempts.
Maximum Number of Routing Attempts per VoIP Peer	Allows operators to determine the maximum number of routing attempts per VoIP Peer for a specific call. Default: 4.
Maximum number of unselected rules to be shown	Allows configuring for calls a maximum number of unselected Routing Rules / Policies. The default value is 5, limited to a maximum of 25 unselected rules per call.

- Click **Submit**.

Registration Routing Settings

The ARM allows operators to route registration messages using any Dictionary Property mapped to a value of **True** / **False**.

➤ **To perform registration routing:**

1. In the License page (**Settings > Administration > License**), make sure the number of registered users (telephones) you require is configured for the parameter 'Number of users for route registrations'.

Figure 7-100: Number of users for route registrations

License

LICENSE

Machine Id: 83239F6B1A30
License Key: * 0mQmPD94YLzrKxPxghCb3bbwMLSKDj2Tg

LICENSE DETAILS

Expiration Date:	Unlimited
Number of sessions:	300000
Number of users:	20000000
Time based routing:	enabled
Quality based routing:	enabled
Test route:	enabled
Network planner:	enabled
Policy studio:	enabled
Number of routing rules:	20000000
Web services:	enabled
Number of standard security queries (per month):	100000
Connect to analytics views in the database:	enabled
Number of users for route registrations:	4000000

Submit



Make sure the number defined for 'Number of users for route registrations' does not exceed the number defined for 'Number of users' (see the preceding figure). The number defined for 'Number of users for route registration' will only be displayed after you purchase the number of users (telephones) for registrations routing you require. If there is no license for 'Number of users for route registration', the settings described below will not be relevant.

2. Open the Registration Settings page (**Settings > Routing > Registration Settings**).

Figure 7-101: Registration Routing Settings

Registration Routing Settings

REGISTRATION SETTING

Enable users property for registration:

Registration property: *

Number/User property: *

☒

Registration_Users

Chatter@ip_addr

RegisterNumber

Submit

- Use the table below as reference when defining the settings for routing registration messages in the ARM.

Table 7-24: Registration Routing Settings

Setting	Description
Enable users property for registration	Must be switched on for enabling the Registrations routing feature.
Registration property	This property determines whether the user (phone / host) will be used for routing the registration message. It can be any Dictionary Property mapped to a value of True / False .
Number/User property	This property is used by the ARM to identify a specific user/telephone registration for Registration routing. It's usually a combined attribute comprising User@Host attributes. Note that this is the identification information ARM gets from SBCs for Registration routing. Note also that more than one property can be selected from the user dictionary. In this case, the ARM will route the Registration message if there is a match with any of them.



Changes to users are not reflected instantly in the Router. The Router is updated periodically (every 30 minutes) so if there is any change to a user's registration property, number or user property, it will not be reflected immediately.

Calls Quota

The ARM allows you to put a quota on calls duration in minutes, on either a single Peer Connection or on a group of Peer Connections.

Using the ARM GUI or northbound REST API, you can define a time limit on calls, in minutes, and periodicity. Based on these definitions, you can define an action to block outgoing calls if

the quota (limit) is reached, to be automatically applied by the ARM. An alarm is always generated if the limit is reached.

When applying the feature:

- The quota can be attached to either a single Peer Connection or to a group of Peer Connections gathered in a Resource Group of type 'Peer Connection'.
- The ARM counts only outgoing calls time (outgoing Peer Connections).
- You can define an alternative route (an Action in a Routing Rule) with an alternative Peer Connection if they want to handle a call when the primary Peer Connection is blocked due to the quota being reached.
- The ARM starts counting calls minutes from the moment the quota is attached to the Peer Connection or set of Peer Connections (and not from the beginning of the interval).
- Emergency calls are allowed regardless of the quota (even if the resource is blocked).
- If a customer wants to reset the quota, they can detach the quota from the entity or edit an existing one (increase the numbers, for example).
- The 'CDR calls' feature must be enabled in the ARM (**Settings > Advanced > Calls** and then select the option **Enable CDR calls**). The ARM uses calls information to get every call's duration and calculates the accumulated minutes of all calls per Peer Connection.



In rare cases, a call duration might go missing (if a specific call is not present in the CDRs for some reason).

➤ To define a quota:

1. Open the Calls Quota page (**Settings > Routing > Calls Quota**).

Calls Quota			
Add Edit Delete Refresh			
NAME	QUOTA	PERIODICITY	BLOCK CALLS
manual_test	10	DAILY	<input checked="" type="checkbox"/>

The following options are available after selecting an already defined quota: **Add** - to add a new Quota (row); **Edit** - to edit an existing Quota's settings; **Delete**; and **Refresh**.

2. Click **Add**:

3. Define an intuitive unique 'Name' for the quota (mandatory).
4. Define 'Quota (minutes)' (mandatory); this defines the number of minutes allowed in the selected period.
5. Define 'Periodicity', i.e., the period for the quota to be applied:
 - **Daily** – the quota count, in minutes, will be reset daily (00:00-23:59).
 - **Weekly** – the quota count, in minutes, will be reset weekly. In this case, the operator must select from which day in the week counting should start and be reset (Example: Monday).
 - **Monthly** – the quota count, in minutes, will be allocated monthly. In this case, operators must select the day in the month from which counting of the minutes starts (Example: 5 days of each month).



If you select the start day to be after the 28th of the month, you'll receive the following warning:

- **Block calls** – an action to be taken if the quota is reached during the specified period. If you select this option, the Peer Connection's outgoing calls - except for emergency calls - will be blocked when the calls quota is reached. Note that an alarm is always generated when a quota is reached; you cannot disable the alarm.

ADD CALLS QUOTA

Name: *

Quota (minutes): *

Periodicity: ☐ Daily ☒ Weekly ☐ Monthly

Count from

Block Calls: ☐

OK **Close**

☒ Monthly ☐ Daily ☐ Monthly

Count from

Submit

The selected row (quota) can be edited using the **Edit** button. All settings can be edited and reapplied. If operators change the frequency of the period when editing a quota, they must take the following into consideration:

CONFIRMATION

Changing the frequency will reset the calls duration count on a Peer Connection or Resource Group using this quota

Update **Cancel**

➤ To delete an existing quota

- Click **Delete**.



A quota cannot be deleted while it is attached to a Peer Connection or a Resource Group. If you attempt to delete it, an error message is displayed along with the names of the specific topology elements currently using the quota.

The Calls Quota page summarizes all defined quota information:

NAME	QUOTA	PERIODICITY	BLOCK CALLS
q1	2	MONTHLY (1)	✗
VerizonQuota1	1000	MONTHLY (10)	✓
myQuota	10	WEEKLY (MON)	✗

Items per page: 25 Items 1-3 items of 3

➤ **To define a Calls Quota Threshold:**

- In the Calls Quota page (**Settings > Routing > Calls Quota**), locate the section 'Calls Quota Configuration' lowermost in the page.

CALLS QUOTA CONFIGURATION

Calls Quota Threshold: %

Submit



- The ARM can generate two alarms: One on hitting the Quota threshold and the other on crossing the Quota value. The ARM always generates Quota-related alarms regardless of the operator's setting to block (or not to block) a Peer Connection if the Quota is reached.
- The same threshold value (as a percentage) applies to all quotas defined in the ARM.

You can choose whether to block the Peer Connection when the Quota is reached, or not, but the ARM always generates Quota-related alarms regardless of the operator's setting to block (or not to block) a Peer Connection if the Quota balance is reached.

The following severities are supported for Quota-related alarms:

Warning – generated for a Network Topology element when the time spent by a specific Peer Connection (or Resource Group) reaches the Threshold limit (as a percentage) defined in **Settings > Routing > Calls Quota**.

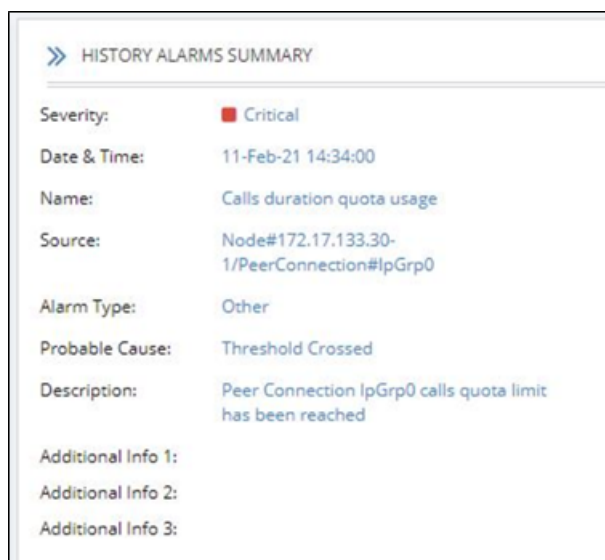
Critical – generated when the Quota is reached for a specific Network Topology element (Peer Connection or Resource Group).

Clear – generated when the end of the period resets the quota for the relevant Network Topology element. The quota alarm also can be cleared when the quota is deleted from the Peer Connection or Resource Group, or when the limit or periodicity of a quota is changed.

The figure below exemplifies a generated alarm and its fields:

Figure 7-102: Quota Threshold Alarm

SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
Green square	11-Feb-21 14:58:32	Calls duration quota usage	Node#172.17.133.30-1/PeerConnection#lgGrp0	Peer Connection lgGrp0 calls quota cleared
Red square	11-Feb-21 14:34:00	Calls duration quota usage	Node#172.17.133.30-1/PeerConnection#lgGrp0	Peer Connection lgGrp0 calls quota limit has been reached



CAC Profiles

Call Admission Control (CAC) is the practice or process of regulating traffic volume in voice communications, usually reflected by a maximum number of allowed simultaneous sessions in the network.

The ARM allows you to define CAC Profiles that can later be attached to 'customer' entities (Teams Super Trunk tenants), Peer Connections and VoIP Peers, giving you another way to balance and control the number of sessions throughout the entire network and to prevent over-subscription.

The CAC Profiles page enables operators to optionally add a CAC profile to be later attached (for example) per 'customer' entity (see also [Defining a 'Customer' Entity \(Teams Tenant\)](#) on page 64).

You can limit the

- incoming Peer Connection / Customer or the connected VoIP Peer
- outgoing Peer Connection / Customer or the connected VoIP Peer
- total session

You can also

- control the threshold of the warning alarm
- disable the entire CAC feature

➤ To add a CAC profile:

1. Open the CAC Profiles page (**Settings > Routing > CAC profiles**).

Table 7-25: CAC Profiles

CAC Profiles			
Add Edit Delete Refresh			
NAME	TOTAL LIMIT	INCOMING LIMIT	OUTGOING LIMIT
cac1	10		
demo_outgoing_limit			10
cac_profile	10		
<div> <div> <div>◀</div> <div>▶</div> <div>1</div> <div>◀</div> <div>▶</div> </div> <div>25 Items per page</div> <div>Items 1-3 Items of 3</div> </div>			
<div> <div>CAC PROFILES CONFIGURATION</div> <div> CAC Profiles Threshold: <input type="text" value="95"/> % </div> <div> Enable Session Counting (for CAC and Statistics): <input checked="" type="checkbox"/> </div> <div>Submit</div> </div>			

Note that after selecting a profile (row), the following actions are all available: **Add**, **Edit**, **Delete** and **Refresh**.

- Click **Add**.

Table 7-26: CAC Profiles

ADD CAC PROFILE

Name *

☒ Global Session Limit: *

☐ Session Limit by Direction:

Incoming:

Outgoing:

OK

Close

- Define an intuitive, unique 'Name' for the CAC Profile (mandatory).
- Define one of the following:
 - Global Session Limit** – the limit on the total count of outgoing and incoming sessions
 - or-
 - Session Limit by Direction** – limit by either or by both:
 - Incoming – Limit by the incoming sessions
 - Outgoing – Limit by the outgoing sessions



- Operators can reuse the same CAC Profile for multiple 'customer' entities.
- In the CAC Profiles page, the selected row (CAC Profile) can be edited using the **Edit** button; all settings can be edited and reapplied.
- If a CAC profile is edited (changed), the status of the network elements to which it is attached will be recalculated and appropriate alarms will be raised or cleared.

Defining a CAC Profile Threshold

The ARM GUI lets operators adjust the threshold for generating a warning alarm.

➤ To adjust the threshold for generating a warning alarm:

- Open the CAC Profiles page (**Settings > Routing > CAC Profiles**) and locate the screen section 'CAC Profiles Configuration' (the lowermost section of the screen).

CAC PROFILES CONFIGURATION

CAC Profiles Threshold: %

Enable Session Counting (for CAC and Statistics): ☒

[Submit](#)



The same CAC Profiles Threshold (percentage) value is applicable for all CAC Profiles defined in the ARM. To change the CAC profile, click **Submit**.

The ARM generates alarms when specified thresholds are crossed. The following severities are supported for CAC Profile related alarms:

- **Warning** – generated for a Peer Connection when the number of sessions reaches the threshold limit (as a percentage) defined under **Settings > Routing > CAC Profiles**.
- **Critical** – generated when the number of sessions reaches the defined session limit.
- **Clear** – Generated to clear 'set' alarms when the number of sessions drops under the defined limit or when the CAC Profile is detached.

SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
■	05-Apr-21 14:16:59	CAC	Node#172.17.133.30-1/PeerConnection#IpGrp0	Peer Connection IpGrp0 total CAC is normal
■	05-Apr-21 14:16:59	CAC	Node#172.17.133.30-1/PeerConnection#IpGrp0	Peer Connection IpGrp0 total CAC has exceeded 95%
■	05-Apr-21 14:16:59	CAC	Node#172.17.133.30-1/PeerConnection#IpGrp0	Alarm with different severity was raised
■	05-Apr-21 14:16:43	CAC	Node#172.17.133.30-1/PeerConnection#IpGrp0	Peer Connection IpGrp0 total CAC has exceeded 100%

Disabling CAC and Session Counting

The ARM GUI lets operators disable CAC and Session Counting.

➤ **To disable CAC and Session Counting:**

1. Open the CAC Profiles page (**Settings > Routing > CAC Profiles**) and locate the screen section 'CAC Profiles Configuration' (the lowermost section of the screen).

CAC PROFILES CONFIGURATION

CAC Profiles Threshold: 95 %

Enable Session Counting (for CAC and Statistics): ☒

Submit

2. Clear the option **Enable Session Counting (for CAC and Statistics)** and click **Submit**.

Adding a Routing Server

A Routing Server can be added to the ARM for handling calls coming from SBCs and Gateways.



- ARM Version 8.4 supports up to 40 Routing Servers - a necessary feature in *very large* ARM deployments of almost unlimited scale.
- ARM Version 8.2 and earlier supported up to 10 ARM Routing Servers.
- In *average size* deployments, an ARM Routing Server can be deployed close to each Node (or small group of Nodes), providing additional Node Survivability. If a network disconnection occurs, a Node's Routing requests are then served by the adjacent, almost co-existing Routing Server.
- If a very high number of Routing Servers is used for survivability purposes, it's recommended to apply the 'Sticky primary' routing policy for a Node (see under [Node Information and Actions](#) on page 30 for more information) and to provide the adjacent Routing Server as the priority for handling the Node's routing requests.

➤ **To add a Routing Server to the ARM:**

1. Open the Routing Servers page (**Settings > Routing Servers**).

Figure 7-103: Routing Servers

STATUS	ADMINISTRATIVE STATE	NAME	ADDRESS	PORT	NODE PROTOCOL	NODES	MEMORY (GB)
		router2	172.17.129.32	443	https	Milan, Israel-HQ_3, Paris_2, Texas_7, Beer_Sheva_8, New_York_1, Ra...	8
		router1	172.17.129.31	443	https	Israel-HQ_3, Rome, China_4, Beer_Sheva_8, Venice, SBC2, Texas_7, ...	8

2. Click **Add**.

Figure 7-104: Server Details


Adding a Routing Server without adding it to a Routing Server Group will have no effect as Routing Servers are as of ARM Version 8.6 not attached directly to nodes (see under [Adding a Routing Servers Group with Internal and External Priorities](#)).

3. Configure the routing server using the following table as reference.

Table 7-27: Routing Server Details

Setting	Description
Name	Enter a name for the ARM Router (routing server).
Address	Enter the IP address or host name for the ARM Router (routing server).
Port	[Read only] ARM Router (routing server) port number. Default: 443
Protocol	[Read only] HTTPS
Credentials	Allows you to specify the credentials which the Configurator will use to communicate with the router and vice versa.

4. Click **OK**; the routing server is added.

Editing a Routing Server

After a routing server is added to the ARM, its configuration can be edited if necessary.

➤ **To edit a Routing Server:**

1. Open the Routing Servers page (**Settings > Routing Servers**).

Figure 7-105: Routing Servers

<div> Add Edit Delete Lock/Unlock Refresh </div> <div> Enter search string </div>							
STATUS	ADMINISTRATIVE STATE	NAME	ADDRESS	PORT	NODE PROTOCOL	NODES	MEMORY (GB)
		router2	172.17.129.32	443	https	Milan, Israel-HQ_3, Paris_2, Texas_7, Beer_Sheva_8, New_York_1, Ro...	8
		router1	172.17.129.31	443	https	Israel-HQ_3, Rome, China_4, Beer_Sheva_8, Venice, SBC2, Texas_7, ...	8

2. Select the row of the routing server to edit, and then click **Edit**.

Figure 7-106: Edit Server

EDIT SERVER

Name *

router1

Address *

172.17.129.31

Port

443

Protocol

https

Advanced Configuration

Credentials




OK

Close

3. Edit the server using the following table as reference.

Table 7-28: Edit Server

Setting	Description
Name	[Read-only] The name of the ARM Router (routing server).
Address	Enter the IP address or host name for the ARM Router (routing server).
Port	[Read only] ARM Router (routing server) port number. Default: 443.
Protocol	[Read only] HTTPS
Nodes	[Read only] The Nodes (SBCs or Gateways) to which the router was added.
Advanced Configuration	

Setting	Description
Configurator – Routing Protocol	To display this parameter, click  adjacent to Advanced Configuration and then from the parameter's drop-down menu, select the protocol between the Configurator and the Router (HTTP or HTTPS). Default: HTTPS. HTTP can temporarily be used for debugging purposes.
Credentials	
Configurator > Router	To display this parameter, click  adjacent to Credentials. Allows you to specify the credentials which the Configurator will use to communicate with the router.
Router > Configurator	To display this parameter, click  adjacent to Credentials. Allows you to specify the credentials which the router will use to communicate with the Configurator.

Locking/Unlocking a Routing Server





The ARM allows users to lock routing servers, for troubleshooting or maintenance purposes. Locking a routing server causes the devices to disconnect from the locked routing server, causing all traffic to divert to the other unlocked and available servers. Unlocking a routing server causes the devices to reconnect, and makes the routing server fully functional.

A locked routing server can also be associated with ARM Nodes without participation in calls routing. This can be useful during the preparation phase for network setup.

➤ To lock or unlock a Routing Server:

1. Open the Routing Servers page (**Settings > Routing Servers**).

Figure 7-107: Routing Servers - Administrative State

Routing Servers							
Add Edit Delete Lock/Unlock Refresh				<input type="text" value="Enter search string"/>			
STATUS	ADMINISTRATIVE STATE	NAME	ADDRESS	PORT	NODE PROTOCOL	NODES	MEMORY (GB)
		router2	172.17.129.32	443	https	Milan, Israel-HQ_3, Paris_2, Texas_7, Beer_Sheva_8, New_York_1, Ro...	8
		router1	172.17.129.31	443	https	Israel-HQ_3, Rome, China_4, Beer_Sheva_8, Venice, SBC2, Texas_7, ...	8

2. Determine from the icon under the 'Administrative State' column whether a routing server is locked or unlocked, and then click the **Lock / Unlock** button.

An unlock performs a restart of the Routing Manager software. The action takes a few seconds, during which time the Routing Manager is unavailable due to the restart.

A lock action is immediate.

These actions can be applied to any particular ARM router. The functionality lets you gracefully take a router temporarily out of service. A locked router responds to all keep-alive and login requests, from all nodes, with a standard 'Service Unavailable' HTML error. This behavior causes all nodes to be disconnected from the router, effectively taking the router out of service. The router still responds to any other request from the nodes or the

configurator, which makes the lock action graceful since calls, statistical calculations and software upgrades are unaffected.

Adding a Routing Server Group with Internal and External Priorities

The ARM allows you to add a single group of routing servers. The ARM also allows you to add multiple groups of ARM Routers with a policy between them. This may be necessary when an ARM deployment is geographically distributed. ARM customers in circumstances like this prefer having (for example) one of the group of the nearest ARM Routers with Round Robin policy and to switch to another group of ARM Routers in case all the nearest ARM Routers fail (or become inaccessible). Customers can configure an ARM Routing Servers Group with internal policies (within a group) and external policies (between groups).

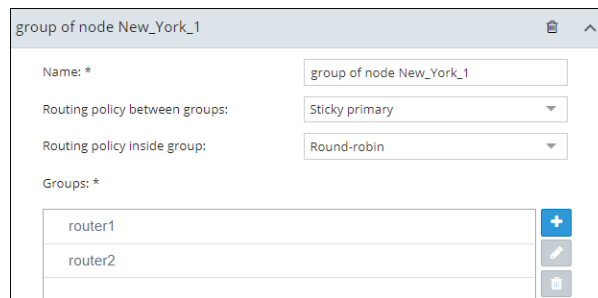
➤ To add a Routing Servers Group:

1. Open the 'Routing server groups' page (**Settings > Routing Servers > Groups**).

Figure 7-108: Routing Server Groups



2. When prompted, configure the:
 - Name of the group to be attached to a node or to multiple nodes
 - Routing Policy to be applied between groups; 'Sticky primary' is the default. Two routing policies between Routing Groups are available:
 - ◆ 'Sticky primary' [the node reverts to the primary group when at least one ARM Router is available]
 - ◆ 'Sticky Last' [after a node switches to the next Routing Group, it uses its ARM Routers while at least one of them is available]
3. Apply a Routing Policy between the ARM Routers inside the Routing Group ('Round Robin' is the default). Three are available: Round Robin, Sticky Primary and Sticky Last.

Figure 7-109: Routing Policy Options


group of node New_York_1

Name: *

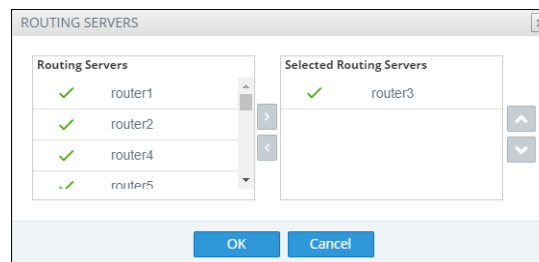
Routing policy between groups:

Routing policy inside group:

Groups: *

router1	<input type="button" value="+"/> <input type="button" value="edit"/> <input type="button" value="delete"/>
router2	

4. Attach one or more ARM Routing Servers to the Routing Group.

Figure 7-110: Attaching Routing Server/s to a Routing Group


ROUTING SERVERS

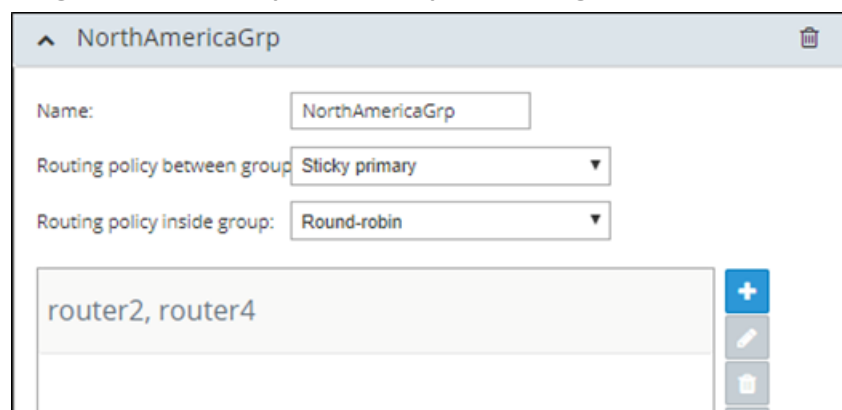
Routing Servers	Selected Routing Servers
✓ router1	✓ router3
✓ router2	
✓ router4	
✓ router5	

OK Cancel

5. To use a single group of routers for a node (or nodes) with a policy between them, one list of selected routing servers is sufficient. When providing multiple sub-groups of Routing Servers, click +.



The maximum number of routing servers allowed for the entire server group is 10, so if you have five sub-groups, each can have up to two routing servers inside).

Figure 7-111: Multiple Sub-Groups of Routing Servers


NorthAmericaGrp

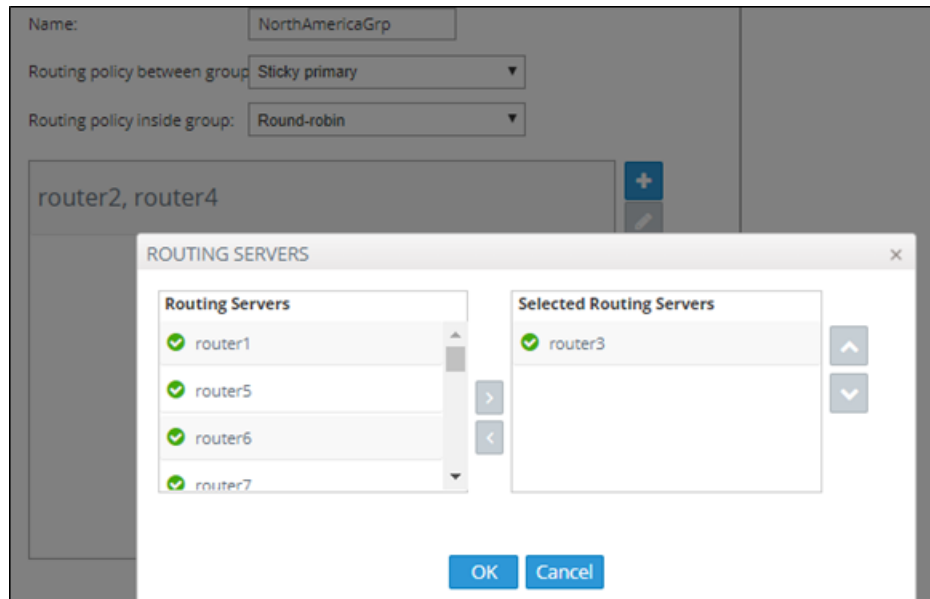
Name:

Routing policy between group:

Routing policy inside group:

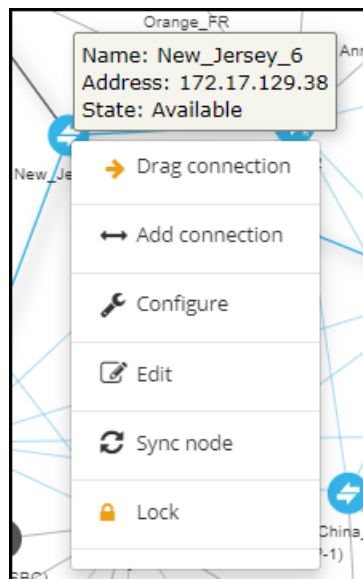
router2, router4	<input type="button" value="+"/> <input type="button" value="edit"/> <input type="button" value="delete"/>

6. Configure a new sub-group of routers with the same Routing Policy inside the group.

Figure 7-112: Sub-Group of Routing Server with the Same Routing Policy

Up to five sub-groups can be configured under the same Name.

- After configuring an ARM Routing Servers group, attach it to a single node or to multiple nodes (SBCs or Gateways). To do this, apply an **Edit** action on the node.

Figure 7-113: Edit Node

- In the Edit Node screen that opens (shown in the next figure), select one of the previously configured groups from the 'Routing server group' drop-down.

Figure 7-114: Edit Node – Selecting Routing Server Group

The screenshot shows the 'EDIT NODE' dialog box with the following fields and values:

- Name: *
- Teams Role:
- Address:
- Protocol:
- Routing server group:
- Resource Groups:
- Credentials:
- Configurator → Node:

At the bottom are 'OK' and 'Cancel' buttons.

The ARM provides the corresponding configuration (per ARM-level definitions) to each node and configures the Routing Servers (per Groups and policies) within the SBC or Media Gateway.



- Support for Routing Server Groups is available from node software version 7.20A.240. If your deployment includes nodes whose software version is earlier than 7.20A.240, the ARM provides a backward-compatible way to define routing servers by creating Routing Server Groups with a single sub-group; Routing Server Groups which have multiple sub-groups are not shown in the drop-down menu.
- When upgrading from previous version releases (when Routing Server Groups were not supported), the ARM upgrade process automatically converts already-configured routers to a Routing Server Group and that group is attached to the node. For example, if a customer has three nodes (N1, N2 and N3), where N1 and N2 use ARM Routers R1 and R2 (Round Robin) and node N3 uses ARM Routers R2 and R3 (Sticky Primary), the ARM during the upgrade automatically creates two Routing Server Groups (N1_group with R1 and R2 with Round Robin, and N3_group with R2 and R3 with Sticky Primary). The N1_group is automatically assigned to nodes N1 and N2. N3_group is automatically assigned to node N3.

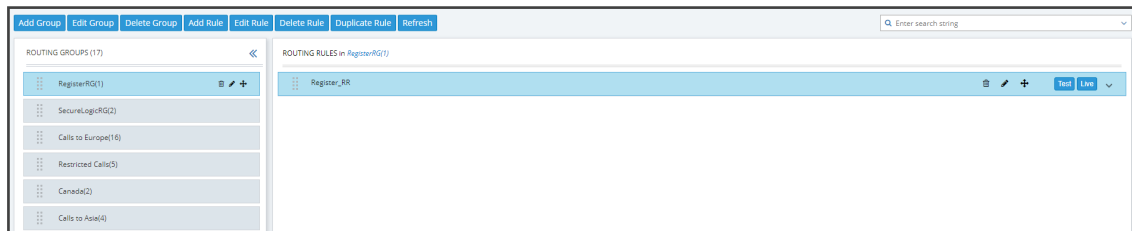
8 Defining Calls Routing

The ARM lets IT managers responsible for enterprise VoIP define call routing. ARM routing provides a comprehensive call routing solution for a telephony network.

➤ To define calls routing:

- Open the Routing Groups page (**Routing > Routing Groups**).

Figure 8-1: Routing – Routing Groups



➤ Follow this procedure when defining calls routing policy (ARM Dial Plan):

1. Add a new Routing Group (see [Adding a Routing Group](#) below)
2. Add a new Routing Rule (see [Adding a New Routing Rule](#) on page 268)
3. Test the route (see [Testing a Route](#) on page 87)

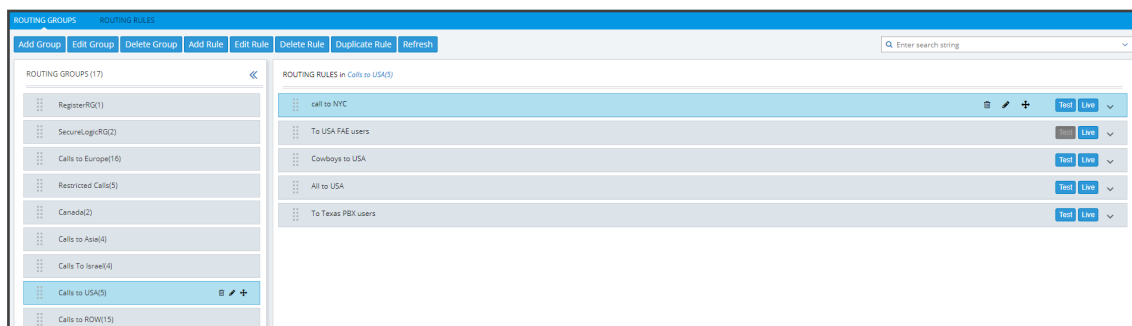
Adding a Routing Group

Before adding a rule, you must add a Routing Group. Routing Groups help present rules in the GUI in an organized fashion, enhancing user experience. Routing Groups also allow you to move a group of Routing Rules, collectively changing their routing priority.

➤ To add a Routing Group:

1. In the Routing Groups page (**Routing > Routing Groups**), click the **Add Group** button.

Figure 8-2: Add Group



The Add Group screen opens.

Figure 8-3: Add Group

2. Define a name for the Routing Group to be added. Define a user-friendly name to facilitate intuitive management by administrators. Some example of groups you can add are 'Restricted Calls', 'Calls to Europe', 'Calls to Far East', 'Calls to ROW', etc.



The routing group's name must be distinct from names of other routing group names, and must be between 1-255 characters.

3. From the drop-down, select the **use time conditions** option to attach a time condition to the Routing Group. See [Configuring a Time-Based Routing Condition](#) on page 234 for related information on how to attach a time condition to a Routing Rule. You can attach multiple time conditions. These conditions will apply to all rules in the group.

Figure 8-4: Add Group with Time Condition

Note that if you attach a time condition to a group, it's indicated visually in the Routing Groups page:

11:19	11:19	JFS test(1)	
11:19	11:19	Calls to ROW(15)	
11:19	11:19	Calls to Africa(0)	
11:19	11:19	M(7)	
11:19	11:19	Novartis(2)	

4. Click **OK**; the new Routing Group is added to the list.



Routing Groups listed higher take precedence over those lower. Routing Groups in the list can be reordered (see [Moving a Routing Group](#) on the next page). Priority is calculated internally, based on Previous and Next groups.

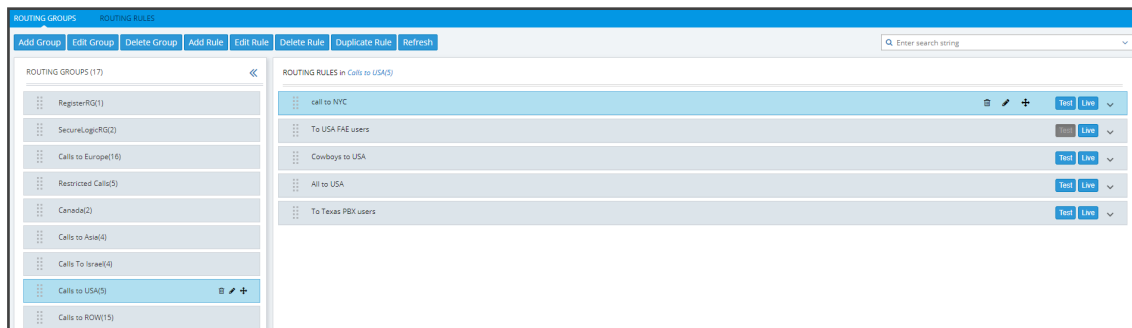
Editing a Routing Group

You can edit a Routing Group if necessary.

➤ To edit a Routing Group:

1. In the Routing Groups page (**Routing > Routing Groups**), select the Routing Group to edit, and then either:
 - a. Click **Edit Group**

Figure 8-5: Edit Group



- b. [Or] Click the group's edit icon in the row


Figure 8-6: Edit Group

2. Edit the 'Name' field. Enter a user-friendly name to facilitate intuitive management by network administrators.
3. Edit the time condition. From the **use time conditions** drop-down, you can clear time conditions if defined. See [Configuring a Time-Based Routing Condition](#) on page 234 for related information. You can alternatively remove a single condition if multiple time conditions are attached.
4. Click **OK**.

Moving a Routing Group

You can promote or demote a Routing Group listed in the Routing Groups page. When moving a Routing Group, all its Routing Rules are moved and the routing priority of all the Routing Rules in the group are collectively changed at once. Routing Groups listed higher in the page take precedence over those listed lower.

➤ **To move a routing group:**

1. In the Routing page, under the **Routing Groups** tab, either drag and drop the Routing Group to where you want to locate it, or select it and then click the then-enabled **Move** icon  next to it.

The Move Routing Group dialog opens:

Figure 8-7: Move Routing Group

MOVE ROUTING GROUP [X]

☒ Before
☐ After

Calls To Israel
Temp. Special Rules
Calls to Europe
Restricted Calls
Calls to USA
Calls to ROW
Calls to China and Far East
rGrp101
rGrp104
rGrp105
rGrp106
rGrp107

OK Cancel

2. Select **Before** or **After**, click the Routing Group before which / after which to move the Routing Group you want to promote/demote, and then click **OK**.
Alternatively, you can move a Routing Group by clicking the icon shown in the following figure, and then dragging it and dropping it in the Routing Groups page.

Figure 8-8: Moving a Routing Group by Dragging and Dropping



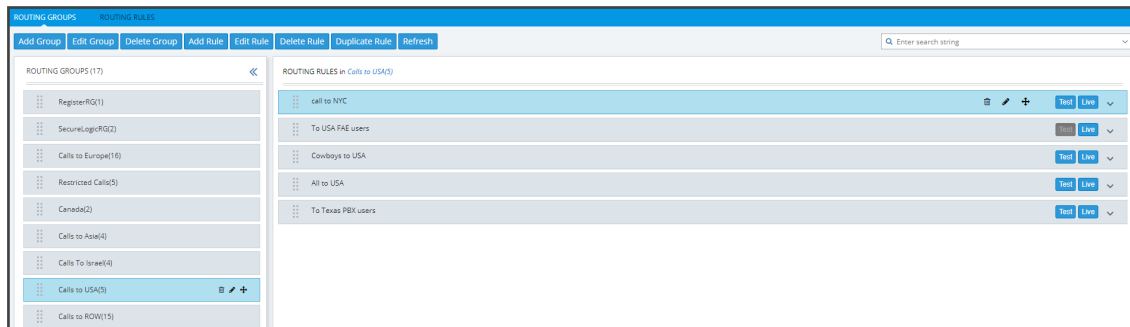
Deleting a Routing Group

You can delete a Routing Group if necessary, including rules associated with the group.


➤ **To delete a Routing Group:**

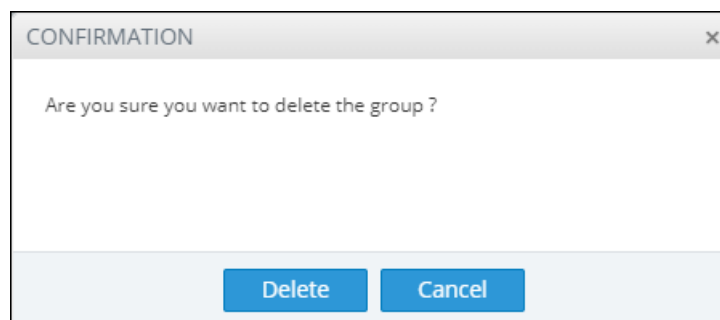
1. In the Routing page under the **Routing Group** icon, select the Routing Group to delete and then either:
 - a. Click **Delete Group**:

Figure 8-9: Delete Routing Group



-Or-

- b. Click the **Delete** icon  in its row which is then enabled. You're prompted to confirm:



2. Click **Delete**.

Duplicating a Routing Rule

You can duplicate a Routing Rule listed in the Routing Rules page (or in the Routing Groups page). The feature can be of particular benefit to support engineers and Field Application Engineers when they need to define *multiple* Routing Rules that are *similar* to rules already defined, for example, a rule that will have the same actions as a previously defined rule but a different prefix and node.

➤ **To duplicate a routing rule:**

1. In the Routing Rules page (**Routing > Routing Rules**) , select the rule to duplicate and then click the then-enabled **Duplicate** button.

Figure 8-10: Add Routing Rule

ADD ROUTING RULE [X]

Name * Live
Test

Group: Register_routing

SOURCE **DESTINATION** **ADVANCED CONDITIONS** **ROUTING ACTIONS**

Prefixes / Prefix Groups

Hosts

User Groups

Customers

☐ Use All Customers

Resource Groups

Nodes

Peer Connections

OK Cancel

2. Modify the duplicated rule to conform to your requirements using [Adding a New Routing Rule](#) below as reference.

Adding a New Routing Rule

After adding a Routing Group, add a new Routing Rule to associate with the Group. Each Routing Rule is given a unique priority within the Routing Group. A rule listed higher than another, even if in the same Routing Group, takes precedence.



- Routing rules are defined within Routing Groups.
 - ✓ To view a specific Routing Group's Routing Rules, click that Group.
 - ✓ To view all Routing Rules, click the Routing Rules tab.
- Any modification to the routing configuration (adding, deleting or modifying) takes effect within 60 seconds after the modification request is answered by the configurator and does not affect active calls.
- Any modification to routing logic because of an operational state change to a node or Peer Connection takes effect within 60 seconds after the status change is identified by the configurator.
- Any modification to routing logic because of a node or Peer Connection administrative state change takes effect within 60 seconds after the status change is identified by the configurator.
- Changes in users or user groups take effect within 60 seconds after the modification is identified by the configurator.

Routing Rules include:

- **Conditions: [Optional]** Define the characteristics of the route request, e.g., the User Group and phone prefix of the originator/destination.
- **Actions: [Mandatory]** Define actions performed if the call matches the rule conditions i.e., routes the call to the specified destination, or discards it specifying a SIP reason.

Figure 8-11: Example of a Routing Rule

The screenshot shows the 'ROUTING RULES in Calls to Europe@' interface. The 'To Paris' rule is selected and expanded, showing its configuration details. The 'CONDITIONS' section includes 'SOURCE' (Nodes: New_York_1, Peer Connections: IpGrp0 (New_York_1) (New_York_1), User Groups: Shabbat_Special, Prefix Groups: @ 70 MILE HS_BC) and 'DESTINATION'. The 'ACTIONS' section shows 'ROUTING' (Method: Sequence, ACTION: Priority: 1, New_York_1, Paris_2). Other rules listed include 'To France' and 'Chatterers to Germany'.

The ARM parses from the top Routing Group listed, to the bottom Routing Group listed, and within each Routing Group from the top Routing Rule listed to the bottom Routing Rule listed. If it finds a matching rule and if Nodes, Connections, Peer Connections and Resource Groups are available, it sends the call to the destination configured for that rule. If it doesn't find a matching rule, it indicates that a route for the call has not been found.

Alternative Routing

The ARM performs alternative routing as follows:

- The ARM attempts to build an alternative path for the same Routing Rule action (Nodes, Peer Connections, VoIP Peers and Resource groups), if available. For more information on Resource Groups, see [Resource Groups Page Actions](#) on page 51.
- ARM attempts to build an alternative action (Nodes, Peer Connections, VoIP Peers and Resource groups), if available, for this call, in the order that actions are listed in the Routing

Rule. For more information on Resource Groups, see [Resource Groups Page Actions](#) on page 51.

- All routing alternatives are sorted by weighted path, cost and then by number of hops.

Load Balancing

The ARM can balance call traffic between multiple destinations of the same Action. Call traffic can be distributed equally between destinations, or the distribution can be defined by the operator. Multiple routing attempts can be configured. Default: 1. Max: 3. The max can't exceed the number of destinations in the load balancing action. If a call to a destination configured in a load balancing action fails, the ARM will try to route it to one of the destinations configured in load balancing before searching for a new rule or action for it.

Registered users

The ARM can route a call only if *the destination number is the number of a registered user in ARM* (listed in the Registered Users table) and the Routing Rule is then matched.

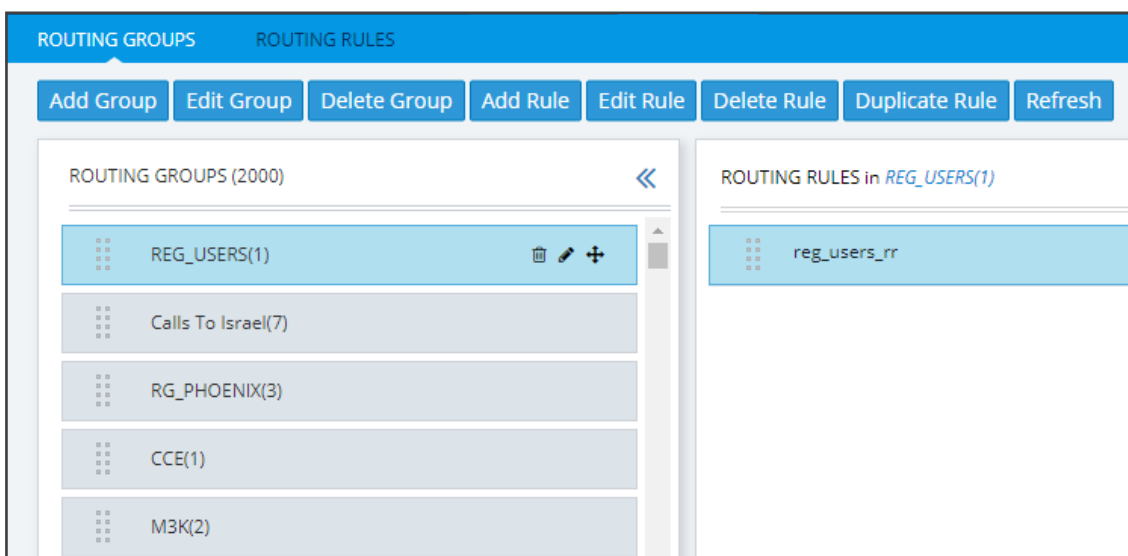
Discard Call

The ARM can be configured to discard calls matching specific conditions as a single action, or as the last action of a rule if previous destinations were unavailable.

➤ To add a new Routing Rule to a Routing Group:

1. In the Routing Groups page under the **Routing Groups** tab, select the Routing Group with which to associate the rule, and then click **Add Rule**.

Figure 8-12: Add Rule



This screen opens:

Figure 8-13: Add Routing Rule

EDIT ROUTING RULE

Name * Live Test

Group: RG1 reroute test

SOURCE **DESTINATION** **ADVANCED CONDITIONS** **ROUTING ACTIONS**

Prefixes / Prefix Groups

Hosts

User Groups × ▲

Customers

Resource Groups

Nodes

Peer Connections

All Clear Invert

If a User Group **and** a Customers are matched, the 'Source' will be matched.

OK Cancel

2. Enter a name for the routing rule that is distinct from the names of the other routing rules in the same group. Define a user-friendly name to facilitate intuitive management by network administrators. The name can be between 1-255 characters.
3. Enable **Live** and/or **Test** mode. See [Testing a Route](#) on page 87.
 - **Live.** The rule will be taken into consideration for live calls traffic.
 - **Test.** The route will be tested offline without impacting live calls traffic.

By default, new routing rules are added with **Test** mode enabled and **Live** mode disabled. It is highly recommended to test the newly added routing rule before enabling it for live calls.

The following table shows the combinations that are supported for a Routing Rule:

Table 8-1: Live | Test Mode Combinations

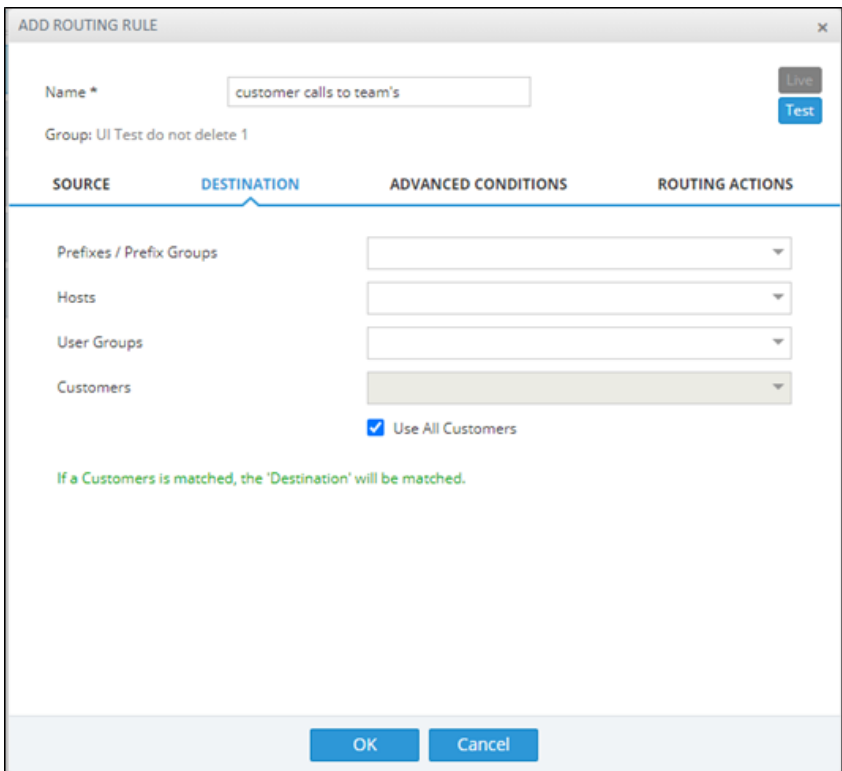
Live Test Combination	Explanation
Live is enabled Test is	The rule will be considered for <i>both test and live traffic</i> .

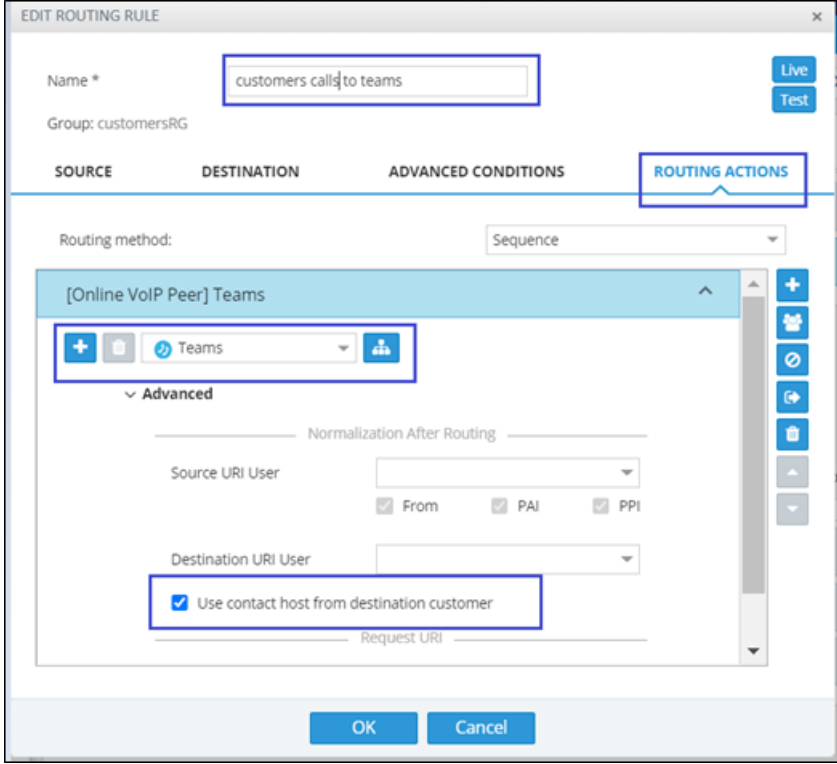


Live Test Combination	Explanation
enabled	
Live is enabled Test is disabled	The rule will be considered only for <i>live traffic</i> . Test mode won't be impacted. Select this option to simulate rule removal.
Live is disabled Test is enabled	The rule will only be considered only for <i>test mode</i> . Live traffic won't be impacted. Select this option to simulate and test a newly added rule.
Live is disabled Test is disabled	The rule will not be considered <i>for test nor live traffic</i> . Select this option to prepare a Dial Plan.

4. Configure the settings under 'Source'. Use the following table as reference.

Table 8-2: Source Settings

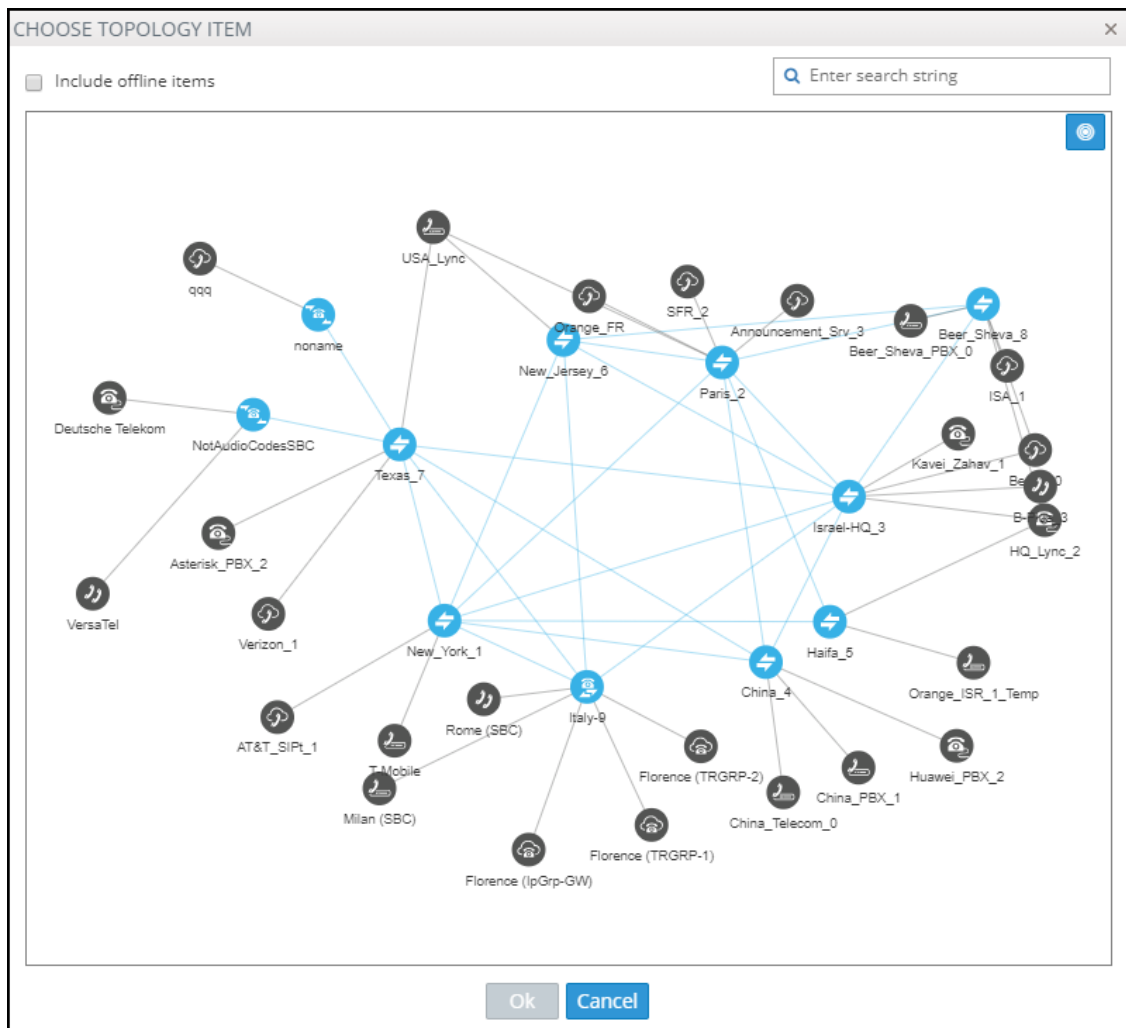
Setting	Description
Prefixes/Prefix Groups	Enter a source number prefix, or list of prefixes. You can also enter the name of a prefix group, or from the drop-down menu select a prefix group or list of prefix groups.
Hosts	Enter a source hostname, or list of hostnames.
User Groups	Enter the name of a source user group or list of source user groups, or select user groups from the drop-down menu. See Adding Users Groups to the ARM on page 136.
Customers	<p>Allows you to select a 'customer' entity / set of 'customer' entities. From the drop-down, select a specific 'customer' entity or a set of 'customer' entities to be used to match the SOURCE field under the Advanced Conditions tab.</p> <p>Select the Use All Customers option for the rule to be applied to all 'customer' entities (without selecting a specific 'customer' entity or a set of 'customer' entities). This is a very powerful functionality especially in the case of a very high number of 'customer' entities.</p> <p>In this way, with a single rule, you can define Calls Routing towards all the 'customer' entities with a Teams Peer VoIP Peer destination (action). This single rule will cover calls toward Teams for all 'customer' entities coming from several SBCs.</p> <p>Following is an example of a rule using Use All Customers in the Destination condition of a rule leading toward Teams.</p>

Setting	Description
	 <p>Each 'customer' entity is identified / indicated by Teams with the FQDN in the 'Contact' or 'From' header. The call in the direction 'to Teams' should have this 'Contact' header identification as well. The ARM provides an easy way to put the predefined string (the one used by Teams to identify the tenant) in the Contact header for calls towards Teams.</p> <p>In a Routing Rule's 'Routing Action', check the Use Contact host from destination customer option under the 'Advanced' section of a specific action; in this case, the ARM automatically installs the value (string) provisioned in the SIP header field of the defined 'customer' entity into SIP Contact header of the invite designated to reach Teams.</p>

Setting	Description
	
Resource Groups	<p>From the drop-down, select a Resource Group. This setting is mandatory to define a routing rule applicable to <i>specific call sources</i> rather than (globally) to the entire network. Resource Groups comprise Nodes, Peer Connections and VoIP Peers.</p>
Nodes	<p>From the drop-down, select a source Node or Nodes, or click the icon  to visually select the element from the Choose Topology Item screen shown in the figure after this table. This setting is mandatory to define a routing rule applicable to <i>specific call sources</i> rather than (globally) to the entire network.</p> <p>Note 1: To select multiple elements in the Choose Topology Item screen, press Ctrl and click the elements to select.</p> <p>Note 2: If the selected 'Nodes' or 'Peer Connections' or Topology group matches one of the conditions specified under the Advanced Conditions tab, the ARM will use this rule.</p>
Peer Connections	<p>From the drop-down, select a source Peer Connection or Peer Connections, or click the icon  to visually select the element from the Choose Topology Item screen shown in the figure following this table. This setting is mandatory to define a routing rule applicable to <i>specific call sources</i> rather than (globally) to the entire network.</p> <p>Note 1: To select multiple elements in the Choose Topology Item</p>

Setting	Description
	<p>screen, press Ctrl and click the elements to select.</p> <p>Note 2: If the selected 'Nodes' or 'Peer Connections' or Topology group matches one of the conditions specified under the Advanced Conditions tab, the ARM will use this rule.</p>

Figure 8-14: Choose Topology Item



5. In the Add Routing Rule screen, click **Destination**.

Figure 8-15: Destination

ADD ROUTING RULE

Name *

Group: Register_routing

Live Test

SOURCE DESTINATION ADVANCED CONDITIONS ROUTING ACTIONS

Prefixes / Prefix Groups

Hosts

User Groups

Customers

☐ Use All Customers

OK Cancel

6. Configure the 'Destination' settings using the following table as reference.

Table 8-3: Destination Settings

Setting	Description
Prefix/Prefix Groups	Enter a destination number prefix, or list of prefixes. You can also enter the names of a prefix group or select prefix groups from the drop-down menu.
Hosts	Enter a destination hostname or list of hostnames.
User Groups	Enter the names of a user group, or list of destination user groups or select user groups from the drop-down menu.
Customers	See Customers on page 272.

7. In the Add Routing Rule screen, click **Advanced Conditions**.

Figure 8-16: Advanced Conditions

8. Under 'Quality Based Routing', select the option **include paths with the following quality**; the drop-down menu becomes available. From it, select the quality criteria that you defined as shown in [Routing Settings](#) on page 233. Criteria for bad, fair and good quality, based on the calculation of MOS and ASR, can be defined. This screen lets you associate the criteria you defined with the Routing Rule.
9. Under 'Time based routing', select from the drop-down menu the time on which routing will be based, configured under **Settings > Routing > Time Based Routing** (see [Routing Settings](#) on page 233 for information about configuring a time range).



- More than one Time Condition can be associated with the same Routing Rule. Activation of the Routing Rule is then performed in 'or' between Time Conditions.
- A Time Condition can be attached to a Routing Rule which belongs to a Routing Group with an already-associated period; the ARM's calculation of this Routing Rule's activation will then be 'and'; the rule will be activated during the period assigned to the Routing Group and the period assigned to the Routing Rule.

10. Under Security Based Routing, select the **Security call score** option only if SecureLogix's Orchestra One™ CAS (Call Authentication Service) is used. The ARM supports security-based routing through integration with SecureLogix's Orchestra One™ CAS.



Using security-based routing requires purchasing SecureLogix's license in addition to the ARM license and must be coordinated with AudioCodes.

Once enabled, the Routing Rule will use the score returned from SecureLogix as part of the match. The slider is used to control the score threshold. If no score is returned from SecureLogix or the score doesn't match the threshold, the rule will not be matched. Based on the score the ARM gets for a specific call, a routing decision is applied. Example:

- For low-scoring calls (bad calls), the routing action may be 'Drop call'.

- For average-scoring calls (suspicious calls), the network administrator can apply number manipulation and display the number with a '?' or with the word 'Suspicious'.

The ARM features two strategy modes:

- **Standard mode.** Calls are verified with the Orchestra One server with a low price. It checks for basic secure. Strategy is set to 0 and as read-only.
- **Advanced.** Calls are verified with the Orchestra One server with a higher price. For example:
 - ◆ For Strategy value 1, Orchestra One will 'Authenticate using the Verizon Call Verification Service (VCVS) when applicable'.
 - ◆ Strategy is set to 1 and as user will be able to set it to 1 or higher. For Advanced mode, it's typically necessary to enable the Sending SIP headers option.

A call's Security Score can be used as basis for a routing decision. Security-based routing can be applied to calls that receive a score from SecureLogix's Orchestra One as part of the pre-routing process. The Routing Rule is applied to a specific range or to a certain value of the call security score received from the ARM ↔ Orchestra One consultation. The range is from -5 to 5.

When enabled, the Routing Rule uses the score returned from SecureLogix's Orchestra One as part of the match. The slider is used to control the score threshold. If no score is returned from Orchestra One or the score doesn't match the threshold, the rule won't be matched. In this way, ARM administrators may use the call's security score as part of the routing decision. For example, calls to a specific (security-sensitive) destination with a score of less than 4 can be dropped, while calls to other destinations with a score of 4 can still be routed normally.

Operators can moreover apply number manipulation to the source call number and turn a source DID with a 'suspicious' security score into a question mark - which will draw the attention of the recipient of the call. The score description shown below is excerpted from the documentation of SecureLogix's Orchestra One:

Orchestra One Scoring Matrix		
5	Verified by the Carrier API's or TRUSTID	
4	Reserved for use by future tools and/or analysis	
3	Verified by SIP header analysis	
2	Reserved for use by future tools and/or analysis	
1	Source analyzed. No anomalies detected; no positive information found	
0	*Toll Free source (Changing from existing score of -5 based on customer feedback)	
-1	International Source (a significant amount of fraud comes from international numbers)	
	*No or blocked CallerID (Changing from existing score of -5 based on customer feedback)	
-2	Source < 10 digits	
-3	Reserved for use by future tools and/or analysis	
-4	*Un-verified by Carrier API's or TRUSTID. (Changing from existing score of -3 based on data analysis customer feedback)	
	Negative SIP header analysis	
-5	Invalid or unassigned phone number	
	Negative SIP header analysis &	Un-verified by the Carrier API's or TRUSTID.
Key	Included in Standard Authentication	Included in Advanced Authentication

* These scores are scheduled for update this calendar year based on customer feedback continued and data analysis.

See also:

- [Web-based Services](#) on page 224 for information on how to configure an external web-based service
- [Policy Studio](#) on page 208 for information on how to configure an external web-based service
- [Activating Your License](#) on page 157 for information related to standard vs. advanced security
- [Viewing License Details](#) on page 159 for information related to standard vs. advanced security

11. Select **Prioritize call when this rule is selected** to prioritize emergency calls over regular calls. The ARM supports emergency call preemption for SBC and gateway calls. If one of the devices is unavailable to process an emergency call because of lack of resources, a regular call will be preempted to free up resources so that the emergency call will be established. The ARM may preempt more than one active call to provide sufficient resources for processing the emergency call. Emergency calls can be identified by the matching rules parameters in the Add Routing Rule screen.
12. Under Registered Users, select **Destination is a registered user in ARM**; the routing rule will then be matched only if the destination number is a registered user number (listed in the Registered Users table).
13. Under 'Advanced Conditions', select a **Call Trigger** to activate the rule for a specific Invite reason (i.e., alternative routing). By default, all 'Call Trigger' options are selected, so routing by default is based on all Call Triggers. At least one must be selected. The node applies to the ARM for a routing decision when it is triggered by another condition – such as a fax call

or a Broken RTP connection. You can configure a rule to be triggered for example only for a fax call or for a 'Refer call'. Call Trigger options are:

- **3xx** [Re-routes the request if it was triggered because of a SIP 3xx response]
- **REFER** [Re-routes the INVITE if it was triggered because of a REFER request]
- **Initial** [This routing rule is used for regular requests that the device forwards to the destination]
- **Broken Connection** [If the Node detects a broken RTP connection during the call and the Broken RTP Connection feature is enabled in Pcon Ip-Profile (IP Profile > Broken Connection Mode = Reroute), you can use this option as an explicit matching characteristic to route the call to an alternative destination.
Note that it's not supported for an incoming call from a third-party Pcon.
- **Fax rerouting** [This trigger will be used if the Node detects a call as a fax and the fax recognition feature is enabled on the Peer Connection. To enable the feature, the device Web interface's 'Routing Mode' parameter must be configured to **Rerouting without delay** (IP Profile > Rerouting Mode). Make sure this IP Profile is associated with the relevant IP Group. You can use this option as an explicit matching characteristic to route the call to an alternative fax destination.



Fax call trigger is unsupported for incoming calls from third-party Peer Connection.

14. Each rule is by default relevant in all circumstances because all Call Triggers are selected by default, but if you want to provide specific routing, for example, for fax calls only, select it as follows:

Figure 8-17: Trigger/s Selected

Call trigger		
<input type="checkbox"/> 3xx	<input type="checkbox"/> Refer	<input type="checkbox"/> Initial
<input type="checkbox"/> Broken connection	<input checked="" type="checkbox"/> Fax rerouting	

In this case, the initial call is routed according to the generic Routing Rules (followed by the SIP Invite message). When the SBC categorizes this call as a fax call, another request for routing is sent to the ARM with the 'Fax Rerouting' trigger. This routing request matches another ARM Routing Rule dedicated for fax rerouting. In this way, you can route fax calls to a 'Fax-to Mail' server (for example).

15. Under 'Rule match' , select **Send notification upon match** to enable a notification on a call (for example, a 911 emergency call) if the call matches a specific rule.

When the ARM receives a call matching this rule condition, a notification (event) with related information is issued by the ARM Configurator. At the ARM level, the event can be sent to an SNMP target. With the ARM integrated into the OVOC, the call notification can trigger the issuance of an email by the OVOC, for example:

```

***** Event Info *****
Alarm Name: General Alarm
Date & Time: 09:24:16 AM September 6, 2018
Source: Router#172.17.113.23
Source Description:
Severity: info
Unique ID: 67
Alarm Type: other
Alarm Probable Cause: other
Description: Routing Rule 911 was matched
Additional Info 1:
Additional Info 2: Routing Rule "911" of Group "911" is
matched.
Call from Pcon "Pcon Pcon-1" , Node "Node 16161104" -
From number "+12345", To number "911".
Additional Info 3:
***** ARM Info *****
ARM IP Address 172.17.113.23

```

Notifications are typically required and used for 911 emergency calls, which should typically be reported via an email application or another notification application. The notification engine, however, can be used for any other matching rule.

16. Optionally use the Routing Rule for routing registration messages: Configure (switch) the 'Request type' condition from its default **Call value** to **Register**.

Figure 8-18: Request type

The screenshot shows the 'EDIT ROUTING RULE' dialog box. The 'Name' field is 'Reg_to_SSW' and the 'Group' is 'RegisterRG'. The 'ADVANCED CONDITIONS' tab is selected. Under 'SOURCE', '3xx' and 'Refer' are checked. Under 'DESTINATION', 'Initial' and 'Fax rerouting' are checked. Under 'ROUTING ACTIONS', 'broken connection' is checked. The 'Request type' dropdown is set to 'Register'. The 'Privacy policy' is set to 'Transparent'. The 'Send notification upon match' checkbox is unchecked. The 'Rule match' field is empty. The 'Sip headers' and 'Tags' fields are also empty. The 'OK' and 'Cancel' buttons are at the bottom.

You can define a dedicated set of Routing Rules for routing registration messages. The registration messages routing rules can be grouped in a separate dedicated Routing Group

(or Groups). The 'Request type' condition differentiates between a Routing Rule to be used for call setup routing and a Routing Rule to be used for registration routing.

If you don't specify any other condition in the Routing Rule but you switch 'Request type' to **Register**, this routing rule will be applied to all the users defined as **True** (enabled) in their registration property, i.e., for all users allowed to route their registration messages. The operator can define multiple Routing Rules for registration messages based on conditions such as:

- Source Node or Peer connection for registration messages coming from a specific topology element.
- Destination Prefix/Prefix group for a group of registration numbers.
- Destination User Groups for groups created with any sophisticated criteria with ARM users group facilities.
- Source URI taken from the SIP 'To' header.
- DEST URI taken from the SIP Request URI.
- Tag based. Very useful criterion. In the Policy Studio, you can assign a Tag to users based on a user's Dictionary Attribute and route registrations to different SoftSwitches based on the Tag's value.

In the example below, the Routing Rule will be applied to users whose registration number starts with prefix 972 and who belong to the previously created Users Group 'register_routing_1'.

Figure 8-19: Routing Rule Example

The screenshot shows the 'EDIT ROUTING RULE' window. At the top, the 'Name' field contains 'Reg_to_SSW' and the 'Group' is set to 'RegisterRG'. There are 'Live' and 'Test' buttons. Below this is a tabbed interface with four tabs: 'SOURCE', 'DESTINATION', 'ADVANCED CONDITIONS', and 'ROUTING ACTIONS'. The 'DESTINATION' tab is selected. Under 'DESTINATION', there are three sections: 'Prefixes / Prefix Groups' with a value of '972', 'Hosts' (empty), and 'User Groups' with a value of 'register_routing_1'. Each section has a dropdown arrow to its right. The 'Prefixes / Prefix Groups' and 'User Groups' sections are highlighted with blue dashed boxes.

Note that not all conditions are relevant for routing of Registration messages. For example, conditions such as Source Prefix, Source Users Group or Call Trigger are not relevant.

17. Under 'Advanced Conditions' in the 'Privacy' section of the Edit Routing Rule screen, you can configure Calling Number Privacy. The ARM supports calling number privacy with different flavors (Privacy policy). The policy is applied per Routing Rule.

Figure 8-20: Edit Routing Rule - Privacy policy

If a call matches the rule, the Privacy Policy is applied. Based on the Privacy Policy of the matching rule, the ARM instructs the SBC or Gateway how to handle calling number privacy in terms of SIP headers. Privacy Policy options are:

Table 8-4: Privacy Policy Options

ARM Value	SBC Value	Comment
Transparent	[0] Transparent	Default. Leave as is.
Transparent with Privacy ID	[1] Don't change privacy	<ul style="list-style-type: none"> Regular call = regular call (as is) Anonymous = Anonymous + Normalization of URI
Anonymous caller	[2] Restrict	Turn the call into anonymous
Identify caller	[3] Remove Restriction	<ul style="list-style-type: none"> If a regular call, stay as is If anonymous, make it exposed in the SIP 'From' header

- 18.** [Optional] You can route calls based on any SIP Invite header value as a Routing Rule matching criterion, for example, based on specific SDP information or on a TGRP value; any information present in the SIP Invite can be used as a condition in the ARM Routing Rule. The feature must be configured at both ARM and SBC level.

19. SIP Headers

- Configure the 'name' field, i.e., the SIP header name
- Configure the 'value' field, i.e., one or more possible values for rule match. The match within the same SIP header name is handled as OR and between the headers as AND. In the following ARM rule, the match is detected when the ARM gets X-ARM-DETAIL-X headers which include: ("tgrp=100" OR "tgrp=200") AND ("coder=711" OR "coder=729").

When the SBC gets a new call (SIP Invite), it sends a REST routing request toward the ARM. This routing request includes parsed SIP information, for example, X-Header. In this way, using SBC-level manipulation, the X-Header can include any information operators want to

pass to the ARM (for further routing decisions). This is the pre-agreed way to pass any SIP header information.

After applying SBC-level manipulation, the operator can configure ARM-level Routing Rules with a condition related to the required attributes and value (pre-installed using SBC-level manipulation).

The ARM is aware of the information followed by the preconfigured 'X-ARM-DETAIL-N' header and ready to use it for routing.

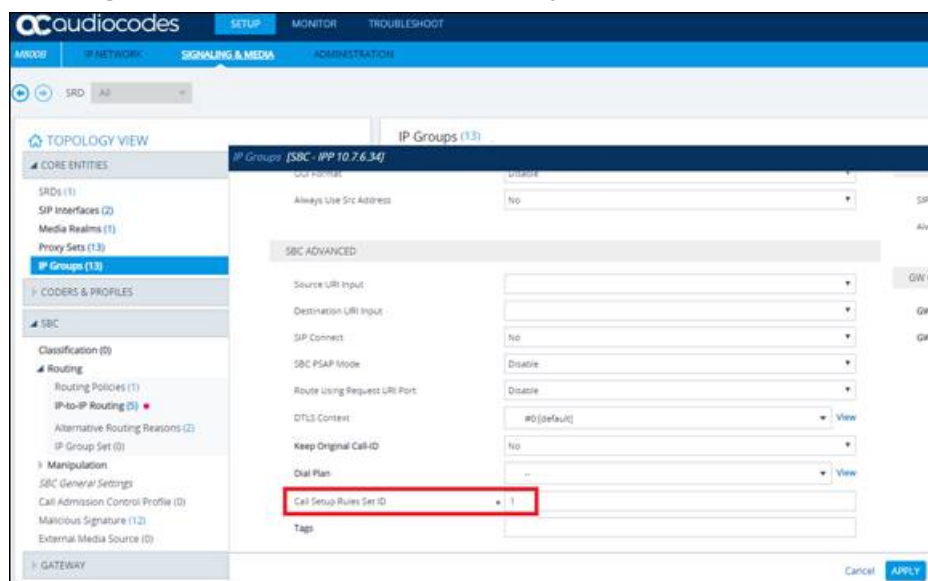
20. [SBC-Level Configuration] To send a parsed information request, add a new header with name "X-ARM-DETAIL-1", "X-ARM-DETAIL-2"... "X-ARM-DETAIL-N" and with information inside taken from the SDP or any other SIP header. X-ARM-DETAIL-X format is "X-ARM-DETAIL-1:<name=value>"

For example:

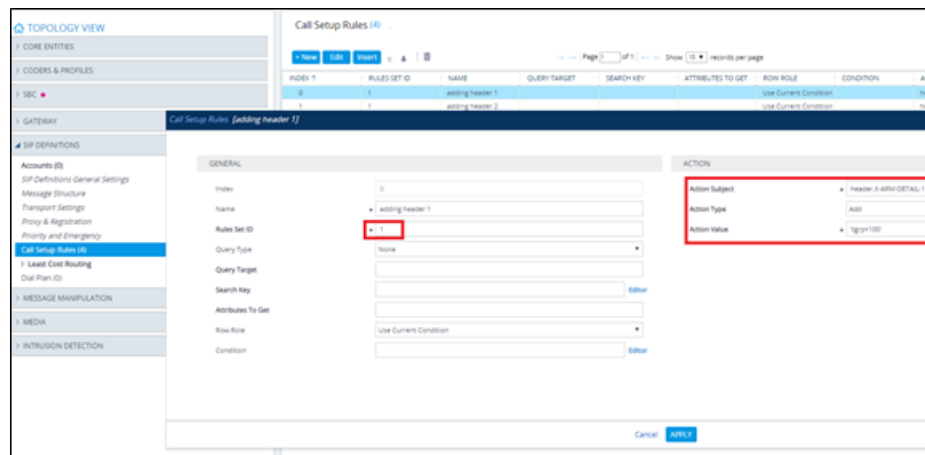
- X-ARM-DETAIL-1: "tgrp=100"
- X-ARM-DETAIL-2: "coder=711"

To create a new header in the SBC, add a new 'Call Setup Rules Set ID' in 'IPGroup' or in 'SIP Interface' in the device's Web interface. The figure below shows 'IPGroup'.

Figure 8-21: [Web Interface] Call Setup Rules Set ID



Setup rules can then be associated with the same Set ID. In the following figure, the manipulation added is 'tgrp=100'. In general, you can use a condition with RegEx and take the attributes into the Action Value.

Figure 8-22: [Web Interface] Viewing SBC Call Setup Rules Configuration

21. In the ARM's Add Routing Rule screen, click **Routing Actions**.

Figure 8-23: Routing Actions

22. From the 'Routing method' drop-down, select **Sequence** or **Forking**.

The parameter 'Routing method' is configured by default to Sequence; Routing Rule Actions are applied sequentially (the only option in ARM versions earlier than 8.6).

If you configure 'Routing method' to Forking, the actions are applied simultaneously and the call is split to all the destinations. The ARM supports calls forking at a network level. SIP forking refers to the process of 'forking' a single SIP call to multiple SIP endpoints. A single call can be split to many endpoints at the same time. The first extension (SIP end-point) to pick up the call receives the call; all other extensions then stop ringing.

Forking implementation in the ARM is designed to split specific calls (matching preconfigured condition) between several network-wide destinations (Peer Connections, VoIP Peers or nodes). Forking is integrated into ARM Routing Rules logic. Forking is applied if a call matches the Routing Rule condition.

Forking implementation in ARM utilizes SBC forking capabilities. When a call matches an ARM routing rule condition with forking, the ARM instructs the SBC to perform forking per the actions configured in ARM Routing Rule.

The ARM supports up to three forking legs (different actions). If one or more of the actions with Forking Routing methods includes load balancing between multiple destinations, the load balancing (with configured percentages) will be applied to choose the correct destination of the forking leg.

Figure 8-24: Calls Forking Routing Rule



- When upgrading from an earlier ARM version than 8.6, all Routing Rules are translated with the Sequence routing method (the default).
- In the ARM, forking capabilities can only be applied to SBCs. Media Gateways aren't supported.
- Forking in the ARM is supported on SBC software 7.20.252 GA or later (release pending). For earlier SBC versions, Forking functions like 'Sequence'.

23. Select the **No answer timeout** option; if the called party does not answer a call within this given interval, the device will disconnect the session. Clear the option for the device to use the default value. The option allows management of the SBC/Gateway's timeout feature for no answer. The option controls the SBC/Gateway 'No answer timeout'.



The option is available only for the 'sequence' routing method.

The feature gives the ARM the capability of managing delayed call forking. If the number is dialed and there is no call pickup after the configured timeout, the call is forked.


1. Under 'Routing Actions', click the 'Add action'  button located on the right side of the screen.

Figure 8-25: Routing Actions – New Action

ADD ROUTING RULE

Name *

Group: Calls To Israel

SOURCE **DESTINATION** **ADVANCED CONDITIONS** **ROUTING ACTIONS**

Routing method:

☐ No answer timeout (sec):

New Action

> Advanced


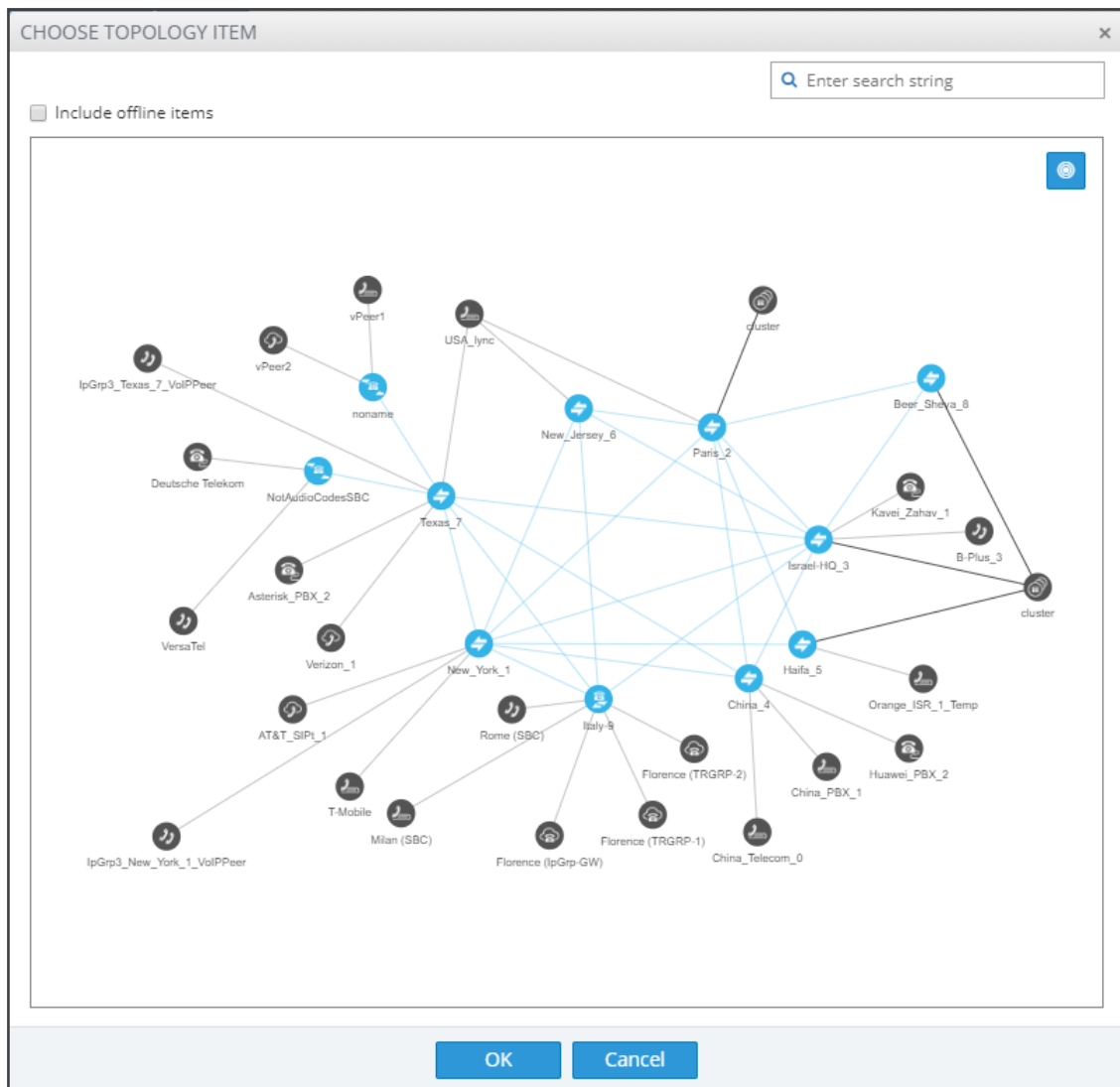
- a. Select from the drop-down menu the Peer Connection, VoIP Peer, Node or Resource Group to which the call will be routed; the list is categorized; best practice is to scroll down the list to the category and then select the entity. Alternatively, click the adjacent  button; the 'Choose Topology Item' screen shown in the next figure is displayed; from this screen you can select the VoIP Peer, Peer Connection or Node. In large networks with high numbers of topology elements, this visual method of selecting the topology element may prevent human error from occurring and facilitate correct selection.

Figure 8-26: Choose Topology Item



If a Resource Group is selected for an action, a 'Resource Attempts' field is displayed, as shown in the following figure.

Figure 8-27: Resource Attempts

- b. Configure the number of 'Resource attempts', i.e., the number of elements the ARM will try before going to the next action. The maximum number of attempts that can be configured = the number of elements in the Resource Group.
- c. Click **> Advanced** to open post routing (after routing) normalization.

Figure 8-28: Normalization After Routing

ADD ROUTING RULE

Name *

Group: Calls to Asia

SOURCE **DESTINATION** **ADVANCED CONDITIONS** **ROUTING ACTIONS**

Routing method:

[Peer Connections group] OVOC_pCons

Figure 8-29: Source URI manipulation for 'From', 'PAI' or 'PPI' field

By default, all three fields are checked when you apply a manipulation to Source URI users. Prior to ARM 9.2, this was the only available behavior. From ARM 9.2, you can check a specific field and clear the others. The functionality is valid for post-routing only. It's supported per Action.

You can also *test a call* with a manipulation of a specific Source URI header, using the Test Route feature extension (support for a specific SIP header simulation). For more information, see [Testing a Route](#) on page 87.

- ◆ From the 'Destination URI User' drop-down, select the destination element (see [Adding a Normalization Group](#) on page 198) to manipulate the destination number in the outgoing call to the Peer Connection. The destination normalization group can only be connected to an IP Group or VoIP Peer. It cannot be connected to a Node.
2. Optionally select the **Route based on Request URI** check box under the 'Request URI' section (under section 'Normalization After Routing') to enable *combined* ARM and SIP based routing decisions on a per-action basis, for when a customer (or a customer's network) provides routing instructions for a call as part of the SIP INVITE message (via REQUEST URI). The Peer Connection (the SBC's IP Group) must be specified in the action as well. SIP based routing takes place in the context of a specific SBC and IP Group. In this way, the ARM will route a call until a specified SBC and request the SBC to use 'REQUEST URI' for further routing. The feature is available for SBCs only.


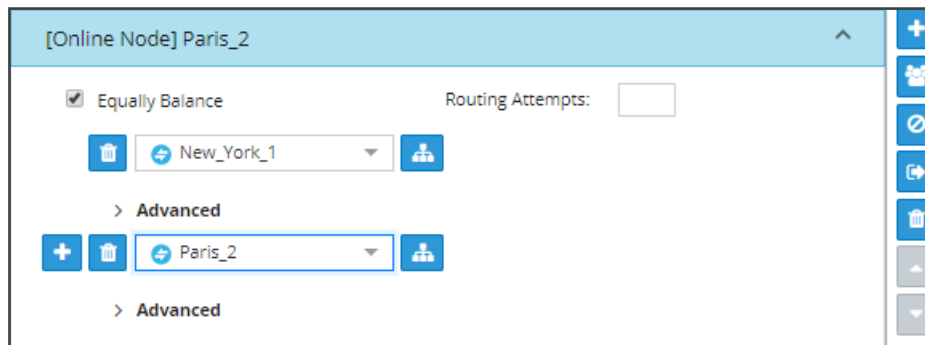
3. Click the 'Add load balancing'  button located to the left of the field displaying the selected Peer Connection, VoIP Peer or Node; the screen adds the following items:
 - **Equally Balance** option (selected by default)
 - 'Routing Attempts' field
 - Drop-down field for selecting Peer Connection, VoIP Peer or Node with an 'Add load balancing' button located next to it

Figure 8-30: Routing Actions – Load Balancing



Load balancing is added between more than one Peer Connection, Node, VoIP Peer or Resource Group. By default, these are equally balanced, i.e., the same percentage is assigned for each option.

4. (Optional) Clear the **Equally Balance** check box to define your own percentage. Any distribution can be chosen, i.e., any percentage of calls can be handled by a specific routing option. Several routing destinations (more than two) are supported by using the 'Add load balancing' button.
5. Enter the percentage of routes that will take this action when load balancing is configured and **Equally Balance** is cleared. Make sure you have 100% in the Action's calls destinations summary else you won't be allowed to enable the action.
6. Configure the parameter 'Routing Attempts' as shown in the following figure. The maximum attempts that can be configured is 3. Default: 1. The maximum number of 'Routing Attempts' can't exceed the number of destinations in the action; see for example the action [Online Node] PARIS_2 in the following figure.

Figure 8-31: Equally Balance: Routing Attempts = 2

The 'Routing Attempts' parameter determines the number of attempts that will be made within the load balancing action. If load balancing is configured within a Routing Rule's Action and a call to a destination configured in this Action fails for some reason, the ARM will try to route the call to one of the destinations configured in load balancing before searching for a new rule or action for the call.

7. Click **> Advanced** in order to apply number manipulation on the Source URI and / or the Destination URI.



- To remove a Peer Connection, Node, VoIP Peer or Resource Group, click the adjacent trash can.
- To remove an entire action, click the trash can on the right side of the screen.


8. (Optional) Click the **Route to user location** button  located on the right side of the screen.

Figure 8-32: Route to user location

The ARM will now attempt to route the call to the location of the registered user (the destination number is used as the key to search for the location).



The ARM supports forking for registered users. If the Routing Rule's 'Routing Method' is set to 'Forking' and the action is set to 'Registered Users' ('Route to user location'), the ARM will attempt to apply forking if the same user is registered in multiple SBCs.


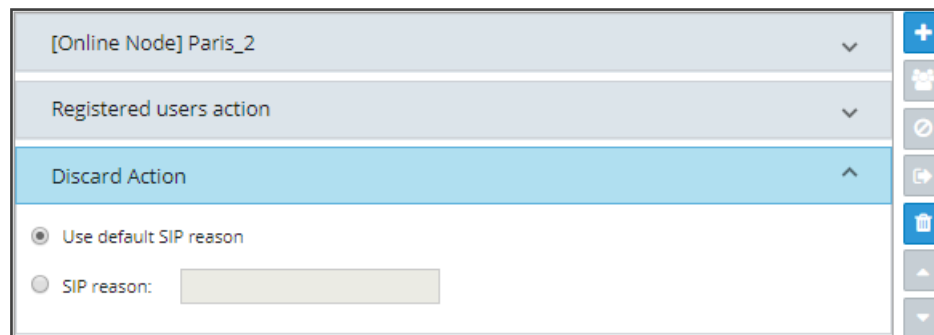
9. (Optional) Add a discard action by clicking the 'Add discard action' button  located on the right side of the screen.

Figure 8-33: Add Discard Action



In a routing rule, you can apply a policy to attempt multiple routing options and to discard the call if none succeed. The action 'Discard Action' can be used - in addition to other routing actions of the same rule - as a last routing rule action or as a sole action.


10. Configure the action using the following table as reference

Table 8-5: Discard Action

Setting	Description
Use default SIP reason	Select the default SIP reason (the last SIP reason received from the SBC or the Gateway) or provide a specific SIP reason as shown in the next parameter description..
SIP Reason	Select this option for a specific SIP reason to be returned to the source peer connection when rejecting the call. Must be a valid SIP reason.

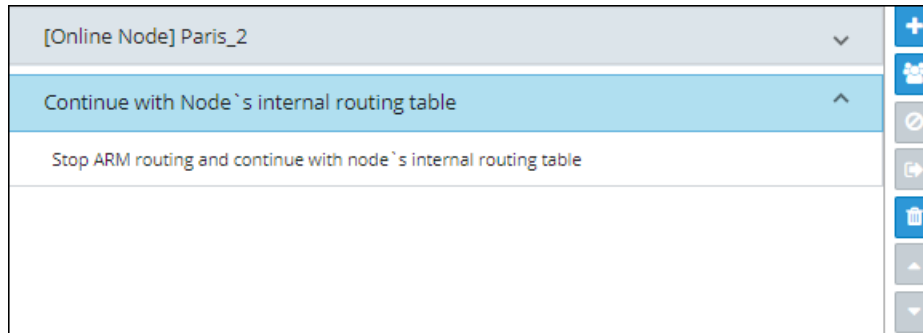


If any field is left empty (Prefix Group/Host/User Group/Node/Peer Connection), the rule will not check it.

11. Click the  button (**Stop ARM routing and continue with node's internal routing**) located on the right side of the screen. This feature enables a combined routing decision taken by the ARM and a node (SBC only). The feature enables customers to specify that after a specific number of routing attempts configured in ARM routing, they'd like to continue with the local SBC routing table. The ARM supports the action in the Routing Rule: **Stop ARM routing**. A second action follows this: **Stop ARM routing and continue with node's internal**

routing. This action is always the last option in a Routing Rule. The feature is only available for SBC nodes.

Figure 8-34: Continue with Node's internal routing table



The feature additionally allows current AudioCodes SBC customers who want to use ARM Security-based Routing (integrated with SecureLogix) without immediately moving to the ARM. These customers can use ARM's SecureLogix integration feature but must indicate in their routing rule that the calls must be routed based on the SBC's existing routing table. ARM routing capabilities can be provisioned in future.



Fields such as 'Nodes', 'Peer Connections' and 'User Groups' in the Add Routing Rule screens and Edit Routing Rule screens feature filters in which network administrators can select multiple elements and then *invert the selection*. The feature improves usability and user experience especially in large networks with high numbers of elements. The feature allows network administrators to

- Select a single element
- Delete a single element (x)
- Select All elements
- Clear all selected elements
- Select All and delete a few (x)
- Select All, delete a few (x) and then invert the selection; the elements deleted will be in the selection
- Select a few elements and then invert the selection; only elements that weren't selected will be in the selection
- Clear a selection

Moving a Routing Rule

You can move a rule within the group under which it is defined, or you can move it to another group, above or below a rule defined within that group.

➤ To move a rule:

1. Click the Routing Group under which the rule is defined and then
 - Drag and drop the rule to the Routing Group you want to move it to -OR-
 - Select the rule to move and then click the 'move' icon; the Move Routing Rule dialog is displayed.

Figure 8-35: Move icon

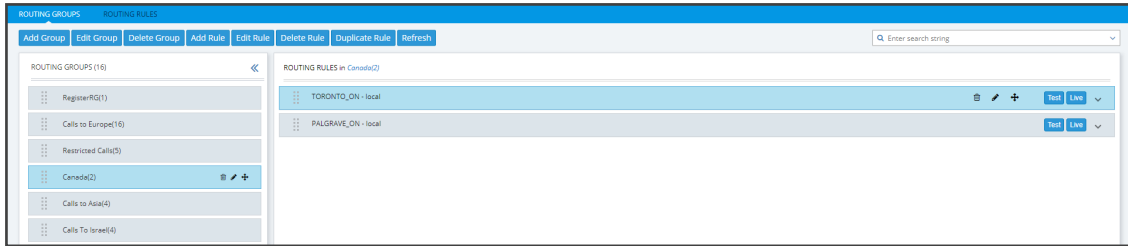
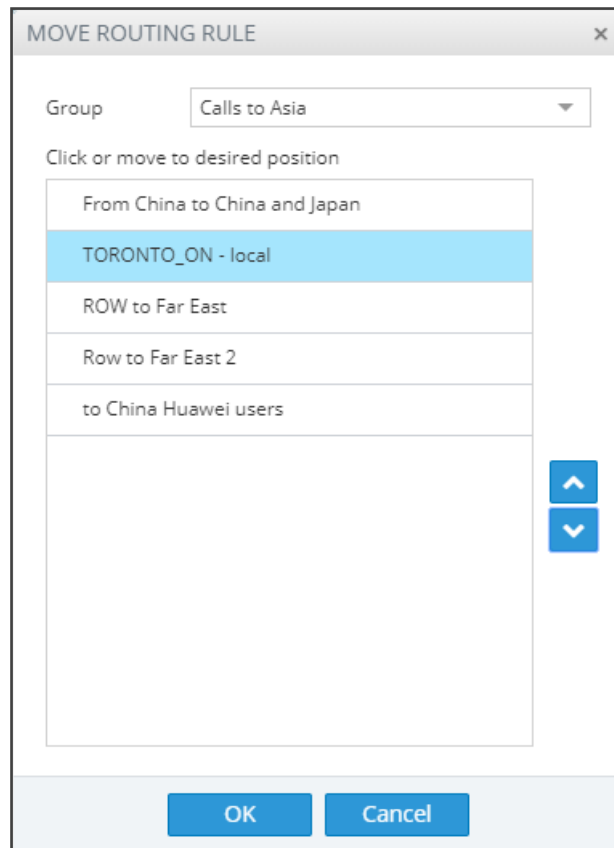




Figure 8-36: Move Routing Rule



2. From the 'Group' drop-down menu, select the new group to which to move the rule to.
3. Click  or  to locate the rule within the new group's rules -OR- click a rule *above* which you want your rule to be moved.
4. Click **OK**; the rule is moved to the location you defined.

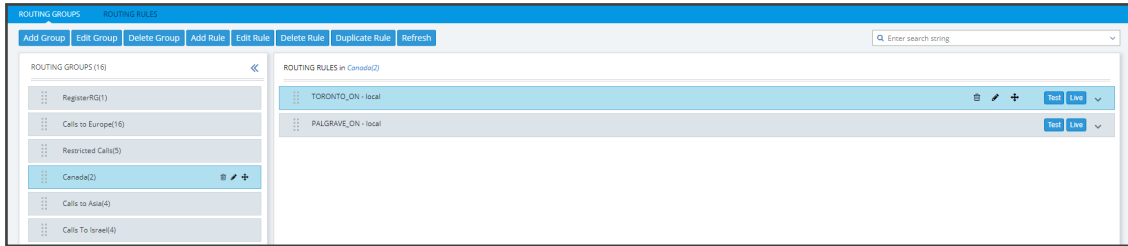
Deleting a Rule

You can delete a rule if necessary.

➤ To delete a rule:

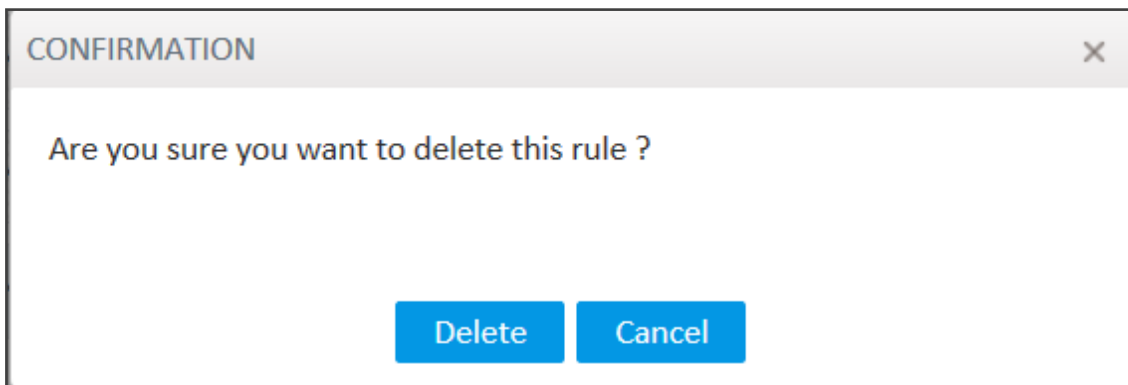
1. Click the group under which the rule is defined and then adjacent to the defined rule that you want to delete, click the now-enabled **Delete** icon shown in the following figure – OR- click the now enabled **Delete Route** button also shown in the following figure.

Figure 8-37: Delete Icon



2. In the Confirmation prompt 'Are you sure you want to delete this rule?' shown in the following figure, click **Delete**.

Figure 8-38: Delete Icon



The rule is deleted.

Duplicating a Routing Rule

You can duplicate a Routing Rule listed in the Routing Rules page (or in the Routing Groups page). The feature can be of particular benefit to support engineers and Field Application Engineers when they need to define *multiple* Routing Rules that are *similar* to rules already defined, for example, a rule that will have the same actions as a previously defined rule but a different prefix and node.

➤ To duplicate a routing rule:

1. In the Routing Rules page (**Routing > Routing Rules**) , select the rule to duplicate and then click the then-enabled **Duplicate** button.

Figure 8-39: Add Routing Rule

ADD ROUTING RULE [X]

Name * Live
Test

Group: Register_routing

SOURCE **DESTINATION** **ADVANCED CONDITIONS** **ROUTING ACTIONS**

Prefixes / Prefix Groups

Hosts

User Groups

Customers

☐ Use All Customers

Resource Groups

Nodes

Peer Connections

OK Cancel

2. Modify the duplicated rule to conform to your requirements using [Adding a New Routing Rule](#) on page 268 as reference.

Testing a Route

You can test a route to make sure it performs according to expectations. See [Testing a Route](#) on page 87 for more information.

Using the Routing Rules Table View Page

Some network administrators prefer to manage routing rules in the Routing Rules table view page. The page offers a significant advantage: Administrators can select multiple rules and perform a multiple-action on the selection.

➤ To open the page:

1. In the Routing page, click the **Routing Rules** menu.

Figure 8-40: Routing Rules Table View Page

ROUTING GROUPS		ROUTING RULES					
		Edit Delete Off Live Duplicate Move Refresh					
		<input type="text" value="Enter search string"/>					
NAME	GROUP	ADMIN STATE	TEST MODE	SOURCE DESCRIPTION	DESTINATION DESCRIPTION	ADVANCED CONDITIONS DESCRIPTION	ACTIONS DESCRIPTION
Register_RR	RegisterRG	UNLOCKED	UNLOCKED			3toInitial/Refer/Fax rerouting/Broken connection	Actions: [#1: #2: Discard: Yes, with SIP reason: null]
To Paris	Calls to Europe	UNLOCKED	UNLOCKED		RR Attributes: Prefix: +3310	Quality: use PRR or GOOD paths; 3toInitial/Refer/F...	Actions: [#1: AT&T_SPL_1, #2: SFR_2, #3: Orange_FR]
Rule2	Calls to Europe	UNLOCKED	UNLOCKED		RR Attributes: Prefix: 055-6865	Prioritize call; 3toInitial/Refer/Fax rerouting/Broken ...	Actions: [#1: HQ_Lync_2, #2: Asterisk_PBX_2]
My black list	Calls to Europe	LOCKED	UNLOCKED		RR Attributes: Prefix: FROUD;	3toInitial/Refer/Fax rerouting/Broken connection;	Actions: [#1: Discard: Yes, with SIP reason: 700, #2: ...]
AT&T To Swift SBO	Calls to Europe	LOCKED	UNLOCKED		User Groups: Imp. People;	3toInitial/Refer/Fax rerouting/Broken connection;	Actions: [#1: SFR_2]
To France	Calls to Europe	UNLOCKED	LOCKED		RR Attributes: Prefix: +330;	Quality: use GOOD paths; 3toInitial/Refer/Fax rer...	Actions: [#1: Israel-HQ_3, BezelGrp0, #2: Paris_2, SF...
To West Europe	Calls to Europe	UNLOCKED	LOCKED		RR Attributes: Prefix: +40, +30;	3toInitial/Refer/Fax rerouting/Broken connection;	Actions: [#1: Texas_2, VerizonGrp1, #2: Paris_2, SFR...

2. Select a rule or select multiple rules; the actions buttons are activated. Administrators can:
 - Edit a rule
 - Delete rules
 - Off - exclude rules from live calls
 - Live - include rules in live calls
 - Duplicate a rule (allows administrators to conveniently and easily add a rule based on an already defined rule)
 - Move rules
3. In the 'Search' field, enter a search string. The functionality allows administrators to search in all the defined rules, not just in a Rules Group.

9 Viewing CDRs and Call Details

The ARM features the capability to store calls information and call-detail records (CDRs). The application displays ARM-routed calls information in the Calls List page. The page helps operators debug call routing. The page displays routing information collected and correlated from multiple routers. Information displayed includes unsuccessful routing attempts, number manipulation information, call routing paths, SIP reason, call session ID, etc. The page helps operators better understand and monitor call routing in their network.

➤ To view CDRs and Call Details:

1. Click the Calls menu to open the Calls List page.

Figure 9-1: Calls List

SOURCE	DESTINATION	DATE	INCOMING NODE	INCOMING PCON	INCOMING CUSTOMER	OUTGOING NODE	OUTGOING PCON	OUTGOING CUSTOMER	ROUTING RULE
16316254203332898@1...	test621@172.17.133.62	14-Sep-21 16:17:03	62	IpGrp0		62	IpGrp1		test62_1
16316248854768172@1...	test621@172.17.133.62	14-Sep-21 16:09:49	62	IpGrp0		62	IpGrp1		test62_1
1631624158575781@1...	test621@172.17.133.62	14-Sep-21 15:56:03	62	IpGrp0		62	IpGrp1		test62_1
16316236238459407@1...	test621@172.17.133.62	14-Sep-21 15:47:08	62	IpGrp0		62	IpGrp1		test62_1
1631623323535202@1...	test621@172.17.133.62	14-Sep-21 15:42:09	62	IpGrp0		62	IpGrp1		test62_1
1631622834039775@1...	test621@172.17.133.62	14-Sep-21 15:34:00	62	IpGrp0		62	IpGrp1		test62_1
16316220762595713@1...	test621@172.17.133.62	14-Sep-21 15:21:23	62	IpGrp0		62	IpGrp1		test62_1
16316219787396808@1...	test621@172.17.133.62	14-Sep-21 15:19:43	62	IpGrp0		62	IpGrp1		test62_1
16316219148377231@1...	test621@172.17.133.62	14-Sep-21 15:18:39	62	IpGrp0		62	IpGrp1		test62_1
1631621189961236700...	test621@172.17.133.62	14-Sep-21 15:06:34	62	IpGrp0		62	IpGrp1		test62_1
test620@172.17.133.5	test621@172.17.133.62	13-Sep-21 14:13:47	62	IpGrp0		62	IpGrp1		test62_1
CombPngNorm1@172...	norm890738680739del...	13-Sep-21 13:07:19	Paris_2	IpGrp1		Israel-HQ_3	IpGrp4		131669 (Deleted)
policyStudio@172.17.13...	0549100670@172.17.13...	12-Sep-21 09:54:00	Paris_2	IpGrp1		Israel-HQ_3	IpGrp4		131666 (Deleted)
policyStudio@172.17.13...	0549100670@172.17.13...	12-Sep-21 09:53:39	Israel-HQ_3	IpGrp1		Israel-HQ_3	IpGrp4		131665 (Deleted)
+97239764095@172.17...	policyStudio@172.17.13...	12-Sep-21 09:51:22	New_York_1	IpGrp2		Israel-HQ_3	IpGrp4		131664 (Deleted)
+97239764095@172.17...	policyStudio@172.17.13...	12-Sep-21 09:51:11	New_York_1	IpGrp2		Israel-HQ_3	IpGrp4		131664 (Deleted)
+97239764095@172.17...	policyStudio@172.17.13...	12-Sep-21 09:50:59	New_York_1	IpGrp2		Israel-HQ_3	IpGrp4		131664 (Deleted)
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:39:41	64	IpGrp1					No match
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:39:30	64	IpGrp1		65	IpGrp0		131655 (Deleted)
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:39:18	64	IpGrp1		65	IpGrp0		131655 (Deleted)
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:37:39	64	IpGrp1					No match
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:37:05	64	IpGrp1		65	IpGrp0		131653 (Deleted)
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:35:34	64	IpGrp1					No match
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:34:59	64	IpGrp1		65	IpGrp0		131651 (Deleted)
any@172.17.133.5	9720000001@172.17.13...	12-Sep-21 09:33:33	64	IpGrp1					No match

Each row in the page represents an ARM-routed end-to-end call which can pass multiple nodes (SBCs or Gateways) and multiple Connections and Peer Connections. Information on a call is collected by the ARM Configurator from ARM Routers, and then correlated to display a single call record.

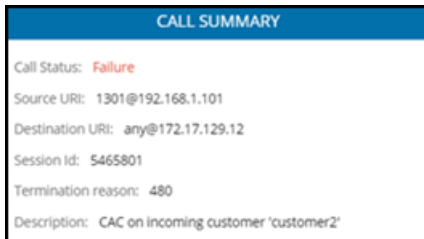
During call processing, each ARM Router periodically sends a bulk of call information (CDRs) to the Configurator for processing. The received CDRs are processed and transformed / correlated into a single call record for each ARM end-to-end call. These records are stored in the ARM Configurator's database (MongoDB).

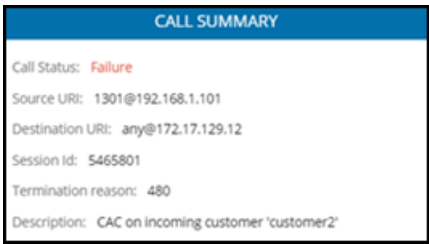
The page displays:

- Filters on the left side of the page, used to facilitate searching for calls and to exclude unwanted calls from the Calls List
- Calls List to the right of the filters, with a predefined call digest (information)

2. Use the following table as reference when using filters:

Table 9-1: Filter Descriptions

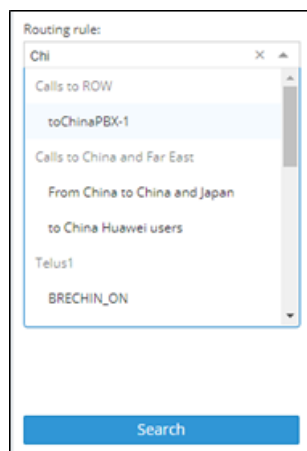
Filter	Description
Source	Enables filtering the Calls List per URI before manipulation.
Destination	Enables filtering the Calls List per URI before manipulation.
Session ID	Enables filtering the Calls List per Unique Session ID identifying a specific call.
Incoming Node	Enables filtering the Calls List per the node from where a call was initiated; selected from the drop-down menu.
Incoming Peer Connection	Enables filtering the Calls List per the Peer Connection from where the call was initiated; selected from the drop-down menu. If an incoming node is selected, the incoming Peer Connection option in the filter will include only relevant Peer Connections, associated with the selected node.
Incoming Customer	<p>Indicates the call is classified as <i>from</i> a 'customer' entity. If a call from a 'customer' entity is dropped due to the number of simultaneous sessions (if a CAC Profile is attached to a 'customer' entity), double-click it in the Call Details page:</p> 
Outgoing Node	Enables filtering the Calls List per the node from where the call exited the ARM network (terminated); selected from the drop-down menu.
Outgoing Peer Connection	From the drop-down menu select an Outgoing Node; the Outgoing Peer Connection option in the filter will include only relevant Peer Connections associated with the selected node.
Outgoing Customer	Indicates the call is classified as <i>to</i> a 'customer' entity. If a call to a 'customer' entity is dropped due to the number of simultaneous sessions (if a CAC Profile is attached to a 'customer' entity), double-click it in the Call Details page:

Filter	Description
	
Routing rule	Enables filtering the Calls List per the name of the Routing Rule matching the call and used for its routing; selected from drop-down menu and organized per the Routing Groups.
SIP reason	Enables filtering the Calls List per the SIP reason for why the call was terminated.
Date range	Enables filtering the Calls List per a range of dates specified.

If you enter a name in a drop-down (e.g., routing rule or incoming node), options are auto populated.

You can remove a filter by clicking **x**.

Figure 9-2: Calls List Filters



Some fields allow a regular expression which operators can use to further narrow down the search.

Figure 9-3: Calls List Filters - Regular Expression

By selecting the Regular Expression search option, you can use any valid regular express pattern to search the following fields:

- Source
- Destination
- Session ID
- SIP reason



Performing a search using regular expression can be extremely slow as a non-prefix (^) search cannot take advantage of the database indexes. The speed depends on the expression and the number of results.

Up to 10000 of the filtered calls can be exported to a CSV file. You can export calls which match the search criteria by pressing the button adjacent to the **Search** option.

The CSV file consists of the following columns:

- Session id
- Setup time
- Release time
- Source URI
- Destination URI
- Incoming node
- Incoming peer connection
- Outgoing node
- Outgoing peer connection
- Incoming customer
- Outgoing customer
- Routing rule
- SIP termination reason
- Voice duration (In milliseconds)

The following columns (call digest) are shown for CDRs / Calls in the Calls List:

- Source
- Destination
- Date
- Incoming node
- Incoming Peer connection
- Outgoing node
- Outgoing Peer Connection
- Routing rule
- SIP reason
- Session ID

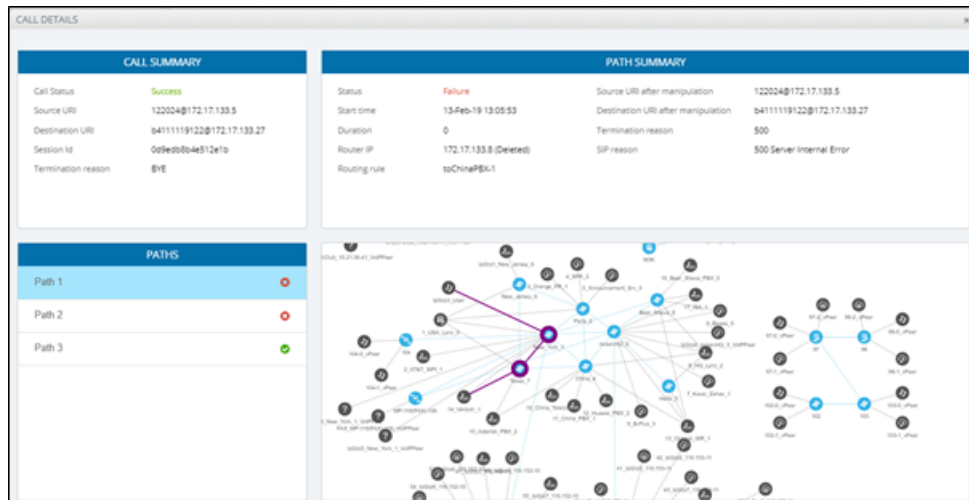
Figure 9-4: Call Columns in the Calls List

SOURCE	DESTINATION	DATE	INCOMING NODE	INCOMING PCON	OUTGOING NODE	OUTGOING PCON	ROUTING RULE	SIP REASON	SESSION ID
16066@172.17.13...	b411119406@172...	13-Feb-19 13:05:58	Texas_7	VerizonGrp1	China_4	IpGrp1	toChinaPBX.1	BYE	4acf039e44...
18727@172.17.13...	b41111845@172...	13-Feb-19 13:05:57	Texas_7	VerizonGrp1	China_4	IpGrp1	toChinaPBX.1	BYE	370896854...

Call Details

The details of a specific call can be viewed. In the Calls List page, filter the list and then double-click a specific call for the Call Details page to open.

Figure 9-5: Call Details



The page displays detailed information on most routing aspects of the call and shows each routing path the ARM attempted.

The Call Summary pane displays the following routing information about the call:

Figure 9-6: 'Call Summary' Pane

CALL SUMMARY	
Call Status	Success
Source URI	122024@172.17.133.5
Destination URI	b411119122@172.17.133.27
Session Id	0d9edb04e512e1b
Termination reason	BYE

The Paths pane displays the list of paths the ARM attempted when routing the call.

Figure 9-7: 'Paths' Pane

PATHS	
Path 1	✗
Path 2	✗
Path 3	✓

Select a path (routing attempt) to view detailed information about that path. After selecting a path, it's highlighted in the ARM Topology map. The Path Summary pane (shown below) changes per the selected path.

Figure 9-8: 'Path Summary' Pane

Use the table as reference to the Path Summary.

Table 9-2: Path Summary

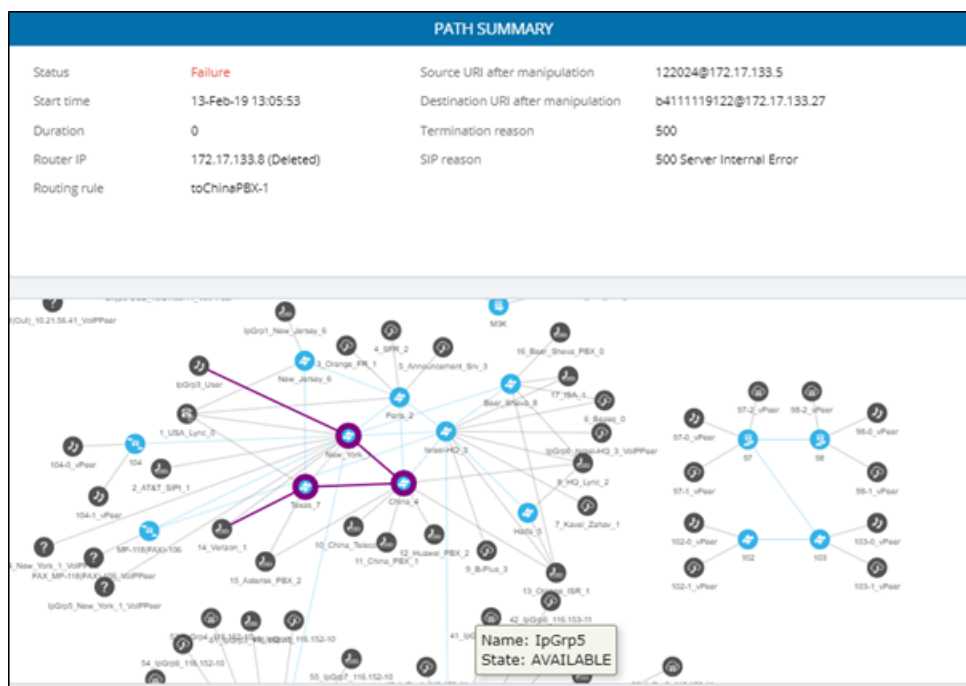
Setting	Description
Status	Displays whether the path was Success or Failure.
Start time	Displays the ARM setup time.
Duration	Displays the call duration; non-zero if 'Status' is Success.
Router IP	Displays the IP of the Router which handled the initial Routing request.
Routing rule	Displays the call matching Routing rule used by the ARM to apply a specific routing path.
Source URI after manipulation	Displays the Source URI after manipulation.
Destination URI after manipulation	Displays the Destination URI after manipulation.
Termination reason	Displays the reason why the specific path was terminated.
SIP reason	Displays the specific path's SIP termination reason.

If Source or Destination URI manipulation was applied for a specific path, the manipulation information will be accessible from the displayed **More** option. The pane's **More** option allows you to review the details of the applied manipulation rules.

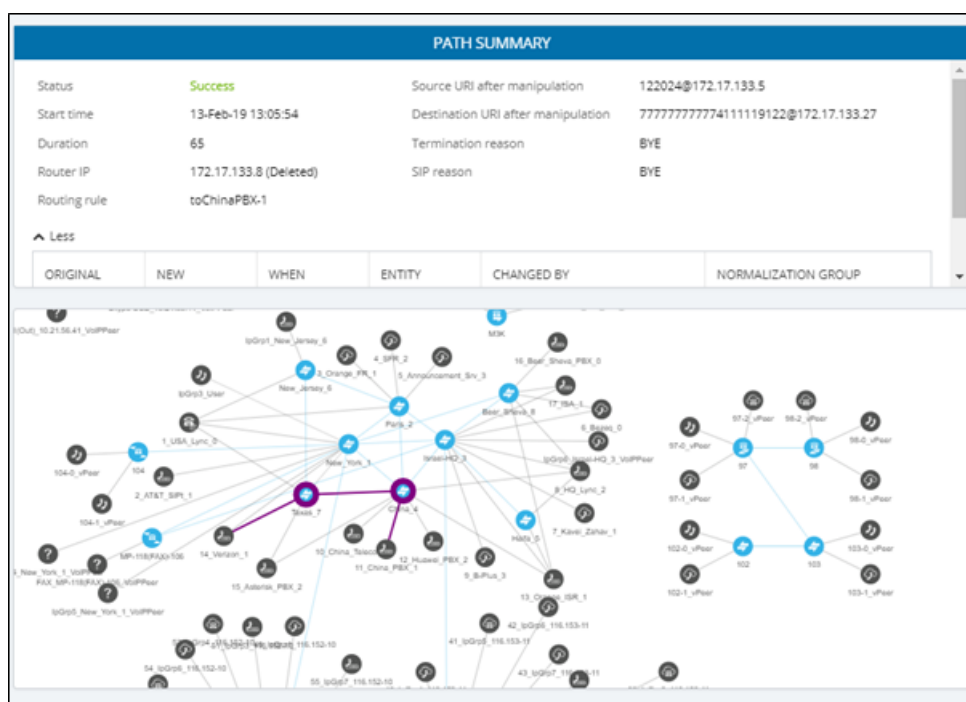
Figure 9-9: 'More' Pane Displaying Details of Applied Manipulation Rules

^ Less					
ORIGINAL	NEW	WHEN	ENTITY	CHANGED BY	NORMALIZATION GROUP
122024	122024	After route	Source Uri User	toChinaPBX-1 (RR Action)	source1
b4111119122	7777777774...	After route	Destination Uri...	toChinaPBX-1 (RR Action)	RR-dest

This figure shows the path of a call's routing attempt whose status was **Failure**:



This figure shows the path of a routing attempt of the same call, whose status was **Success**:



The maximum number of Unselected Rules in calls can be configured in the Global Routing Settings page (see [Configuring Global Routing Settings](#) on page 243). The default value is 5, limited to a maximum of 25 per call. The 'Path Summary' pane under 'Manipulation during route' indicates (after clicking the **More** option) if the maximum number of Unselected Rules has been exceeded and if there are more Unselected Rules that are not shown (see the next figure).

PATH SUMMARY						
Manipulation during route						
USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	N...	DESCRIPTION
No				Rule: Rule 1, Action: sbc142_ipg1(Node2)		Peer Connection state is invalid
No				Rule: Rule 1, Action: pcons		Outgoing Peer Connection Quota limit has been reached

* Maximum number of unselected rules to be shown is reached

For historical calls, the Call Details page's 'Path Summary' pane indicates if the maximum number of Unselected Rules was exceeded and if there are more Unselected Rules that were not shown (see the next figure).

CALL DETAILS	
CALL SUMMARY	PATH SUMMARY
Call Status: Success Source URI: 123456@10.7.20.148 Destination URI: sip201@10.7.12.140 Session Id: f8634b75cc9f0b01 Termination reason: BYE	Status: Success Start time: 24-Aug-21 09:17:03 Duration: 0:115 Sec Router IP: localhost (10.7.2.19) Routing rule: rule1 Termination reason: BYE SIP reason: BYE Source URI after manipulation: 123456@10.7.20.148 Destination URI after manipulation: sip201@10.7.12.140 Incoming Peer Connection: pcn2 (Node1) Outgoing Peer Connection: pcn5 (Node2) * This call does not contain information about unselected rules / policy stubs
PATHS	
Path 1	



Old calls that are not supported by this feature are indicated.

Adding Node Information to Call Details

The ARM enables customers to add information from a node to Call Details, using a variable in the node **Var.call.Src.UserDefined1**.

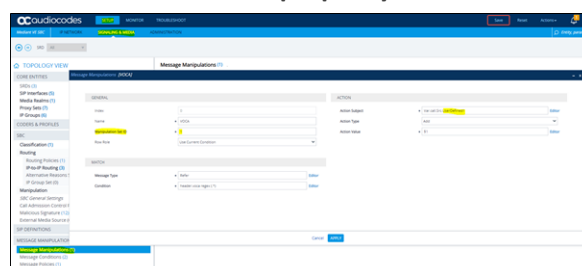
The variable can be created and assigned with a value using Message Manipulation; it's attached to the 'Inbound Message Manipulation Set' of a specific IP Group in the node.

In the example shown in the figure below:

➤ To add information from a node to Call Details:

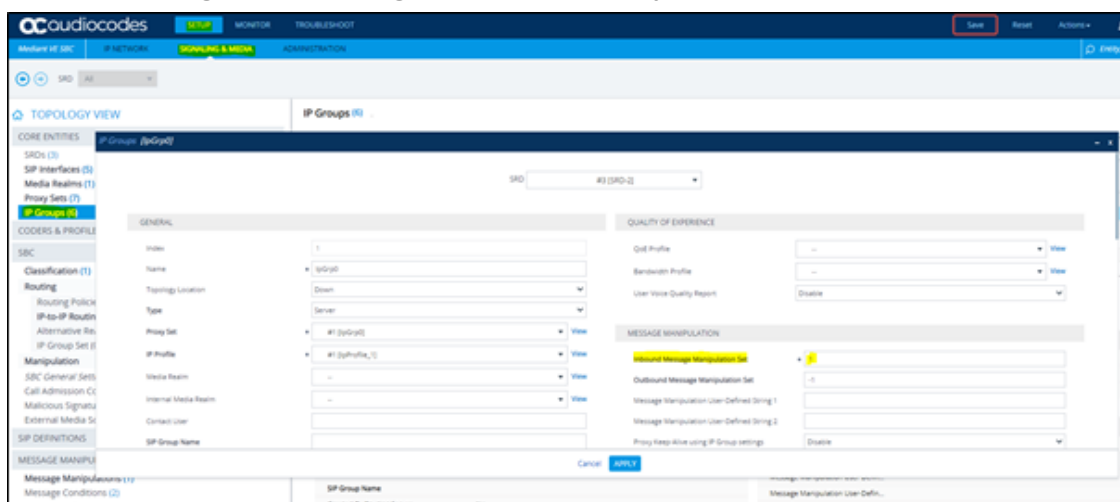
1. Take information from propriety header 'voca' and assign it to the variable **Var.call.Src.UserDefined1**.

Figure 9-10: Information from propriety header 'voca'



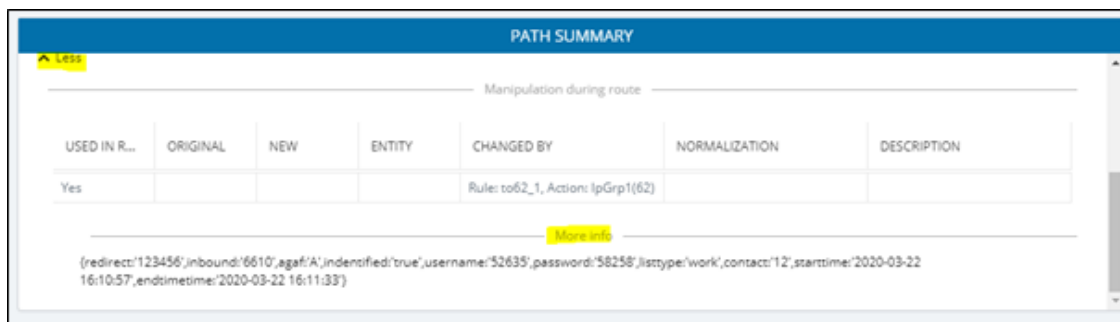
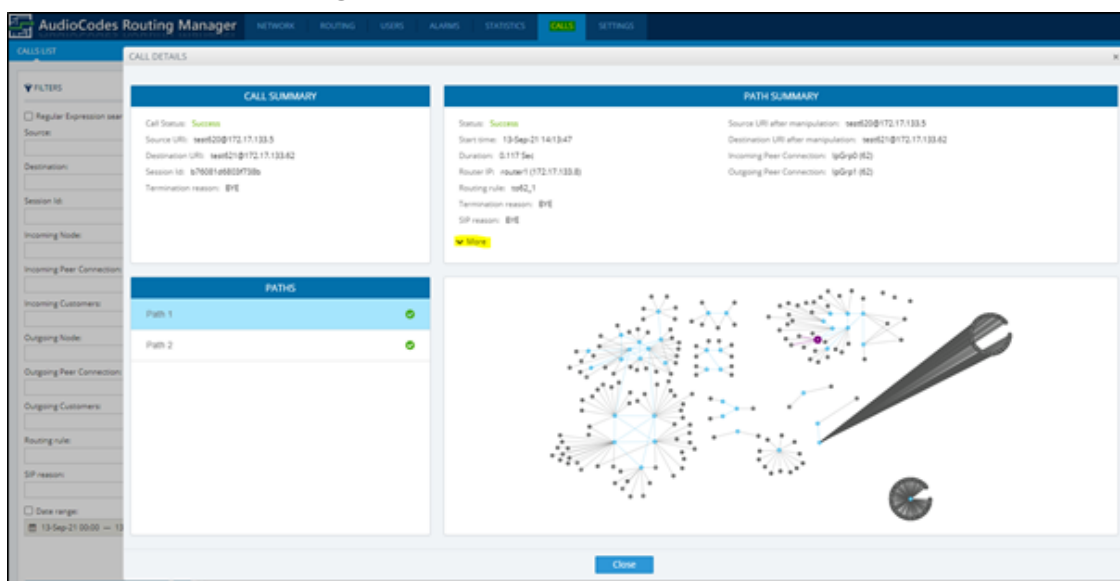
- Assign it to the IP Group in the node:

Figure 9-11: Assign info to the IP Group in the node



- View the information by clicking the **More** option in the Call Details screen (accessed from the **Calls** menu) shown in the figure below, and then locating screen section 'More Info', shown in the figure below it. In the following example, it's a string contained by the 'voca' header.

Figure 9-12: Call Details



Disabling, Limiting the Number of CDRs

The Call Detail Records feature is by default enabled. You can optionally disable it. You can also control the number of records the ARM keeps in the database. The default number of records is 10 million. This is also the maximum number.

➤ To control call records:

1. Open the Calls screen (**Settings > Advanced > Calls**).

Figure 9-13: Calls

2. Use the following table as reference.

Table 9-3: Calls

Setting	Description
Enable CDR Calls	Optionally disable CDRs by clearing the selection. By default, the parameter is selected (enabled).
Keep raw CDRs for calls with partial data	If selected, the ARM saves all CDRs processed to create 'end-to-end calls' for calls terminated before all information about them was received. This parameter impacts database size so the default is unselected; you'll not be able to save 10 million calls. Enable the parameter for debugging purposes only.
Keep raw CDRs for calls with full data	If selected, the ARM saves all CDRs processed to create 'end-to-end calls' for calls terminated successfully. This parameter impacts database size so the default is unselected; you'll not be able to save 10 million calls. Enable the parameter for debugging purposes only.
Limit number of CDR calls to	Enter the number of CDRs to limit the ARM to.
Calls cleanup frequency	Determines how often the ARM checks the size / number of calls. Default: Every 10 minutes. The parameter depends on the number of CAPs. After changing the parameter, restart the ARM Configurator.

Setting	Description
Number of days to keep calls information	Determines how long calls information will be kept (in days). Gives operators the ability to manage resources more effectively. Minimum: 1 day. Maximum: 365 days.

10 Viewing Alarms

The Alarms page shown in the figures below displays alarms generated in the enterprise's network topology, e.g., SBC disconnected. In the page, you can view alarms information displayed under two tabs:

- **Active Alarms** (default)
- **History Alarms**

Active Alarms | History Alarms

The Active Alarms and the History Alarms pages under the Alarms menu display these column headers:

- **SEVERITY**
- **DATE AND TIME**
- **NAME**
- **ALARM SOURCE**
- **DESCRIPTION**

Figure 10-1: Alarms – Active Alarms + Alarm Summary

SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
■	23-Feb-20 12:01:50	ARM Quality change	NodeItaly_9/PeerConnectionIpGrp3	The Quality of Peer Connection IpGrp3 was changed to BAD
■	23-Feb-20 12:01:37	ARM Quality change	NodeBeer_Sheva_8/PeerConnectionIpGrp1	The Quality of Peer Connection IpGrp1 was changed to FAIR
■	23-Feb-20 12:01:37	ARM Quality change	NodeNew_York_1/PeerConnectionIpGrp0	The Quality of Peer Connection IpGrp0 was changed to FAIR
■	23-Feb-20 12:01:37	ARM Quality change	NodeIsrael_HQ_3/PeerConnectionIpGrp1	The Quality of Peer Connection IpGrp1 was changed to FAIR
■	23-Feb-20 12:01:36	ARM Quality change	NodeParis_2/PeerConnectionIpGrp2	The Quality of Peer Connection IpGrp2 was changed to BAD
■	23-Feb-20 12:01:34	ARM Quality change	Configuration/Connection3-4	The Quality of Connection 3-4 was changed to FAIR
■	23-Feb-20 12:01:33	ARM Quality change	Configuration/Connection2-4	The Quality of Connection 2-4 was changed to FAIR
■	23-Feb-20 12:01:31	ARM Quality change	Configuration/Connection1-3	The Quality of Connection 1-3 was changed to BAD

Figure 10-2: Alarms – History Alarms

SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
■	26-Feb-20 3:39:55	Operation status changed	NodeBeer_Sheva_8/Router#router1	Routing Server router1 in Node Beer_Sheva_8 was marked as Avail...
■	26-Feb-20 3:39:55	Operation status changed	NodeRome/Router#router1	Routing Server router1 in Node Rome was marked as Available
■	26-Feb-20 3:39:55	Operation status changed	NodeTexas_7/Router#router1	Routing Server router1 in Node Texas_7 was marked as Available
■	26-Feb-20 3:39:54	Operation status changed	NodeBeer_Sheva_8/Router#router1	Routing Server router1 in Node Beer_Sheva_8 was marked as Un...
■	26-Feb-20 3:39:53	Operation status changed	NodeRome/Router#router1	Routing Server router1 in Node Rome was marked as Unavailable
■	26-Feb-20 3:39:53	Operation status changed	NodeTexas_7/Router#router1	Routing Server router1 in Node Texas_7 was marked as Unavailable
■	23-Feb-20 12:01:50	ARM Quality change	NodeItaly_9/PeerConnectionIpGrp3	The Quality of Peer Connection IpGrp3 was changed to BAD
■	23-Feb-20 12:01:37	ARM Quality change	NodeBeer_Sheva_8/PeerConnectionIpGrp1	The Quality of Peer Connection IpGrp1 was changed to FAIR
■	23-Feb-20 12:01:37	ARM Quality change	NodeNew_York_1/PeerConnectionIpGrp0	The Quality of Peer Connection IpGrp0 was changed to FAIR
■	23-Feb-20 12:01:37	ARM Quality change	NodeIsrael_HQ_3/PeerConnectionIpGrp1	The Quality of Peer Connection IpGrp1 was changed to FAIR
■	23-Feb-20 12:01:36	ARM Quality change	NodeParis_2/PeerConnectionIpGrp2	The Quality of Peer Connection IpGrp2 was changed to BAD
■	23-Feb-20 12:01:34	ARM Quality change	Configuration/Connection3-4	The Quality of Connection 3-4 was changed to FAIR
■	23-Feb-20 12:01:33	ARM Quality change	Configuration/Connection2-4	The Quality of Connection 2-4 was changed to FAIR

Click any alarm listed on any page; that alarm's **ALARM SUMMARY** pane, shown in the preceding figure, displays the column information as well as:

- **ALARM TYPE**
- **PROBABLE CAUSE**
- **ADDITIONAL INFO1**
- **ADDITIONAL INFO2**

■ ACKNOWLEDGED

In the Active Alarms and History Alarms pages you can:

- Sort alarms, according to column header
- Use the 'Search' feature to locate specific alarms (see [Locating a Specific Alarm](#) on the next page below).
- **Refresh** the page / **Stop Auto Refresh**
- **Acknowledge Alarm** [Applies only to the Active Alarms page] Click the button to clear a selected alarm from the page. Note that after acknowledging it, the alarm can be still viewed in the History Alarms page.

Journal Page

The Journal page allows you to view historical actions and activities performed in the ARM by all operators, up to the present time.

The page can help you determine if another operator's action or activity may have changed network functionality and been responsible for an active alarm.

Figure 10-3: Journal Page

DATE AND TIME	SOURCE	NAME	OPERATOR	DESCRIPTION
26-Feb-20 17:56:03	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: admin
26-Feb-20 17:54:42	ARM	Operator logged in	Anonymous	Anonymous failed to login
26-Feb-20 17:54:26	ARM	Operator logged in	Anonymous	Anonymous failed to login
26-Feb-20 17:54:16	ARM	Operator logged in	Anonymous	Anonymous failed to login
26-Feb-20 17:32:41	ARM	Operator logged in	Anonymous	Anonymous failed to login: no username was provided, or username was empty
26-Feb-20 15:37:13	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: b
26-Feb-20 15:37:09	ARM	Operator logged in	Anonymous	Anonymous failed to login
26-Feb-20 12:34:42	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: kfig
26-Feb-20 12:23:26	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: Operator
26-Feb-20 12:22:41	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: igorm
26-Feb-20 12:22:34	ARM	Operator logged in	Anonymous	Anonymous failed to login
26-Feb-20 12:17:46	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: Operator
26-Feb-20 12:09:56	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: kfig
26-Feb-20 11:35:31	ARM	Operator logged in	Anonymous	Anonymous successfully logged in as: meriner

The page helps you 'debug' a routing issue that may occur in the network. Each row chronologically indicates an operator action | activity. Selecting a row displays the details of that action | activity in a Journal Summary pane located on the right side of the page.

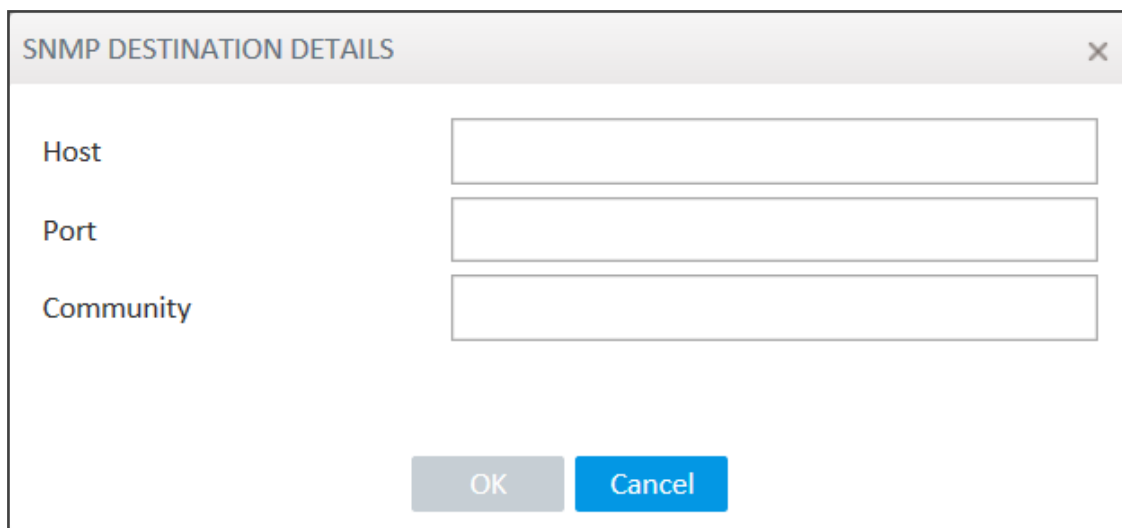
Collecting Info via SNMP to Enhance IP Network Telephony Performance

This feature provides enterprise network administrators the option to collect information on devices via Operations Support Systems (OSS) traps sent over Simple Network Management Protocol (SNMP). Network administrators can then modify that information to enhance telephony network performance.

➤ To collect information via SNMP:

1. In the Alarms page, click the **SNMP Destinations** tab and then click **Add**.

Figure 10-4: SNMP Destination Details



The dialog box titled "SNMP DESTINATION DETAILS" contains three input fields: "Host", "Port", and "Community". At the bottom, there are "OK" and "Cancel" buttons.

2. Use the following table as reference.

Table 10-1: SNMP Destination Details

Setting	Description
Host	Enter the IP address of the OSS host.
Port	Enter the number of the port to which to send OSS traps.
Community	SNMP Community String. Sent with each Get-Request as a type of password to allow or deny access.

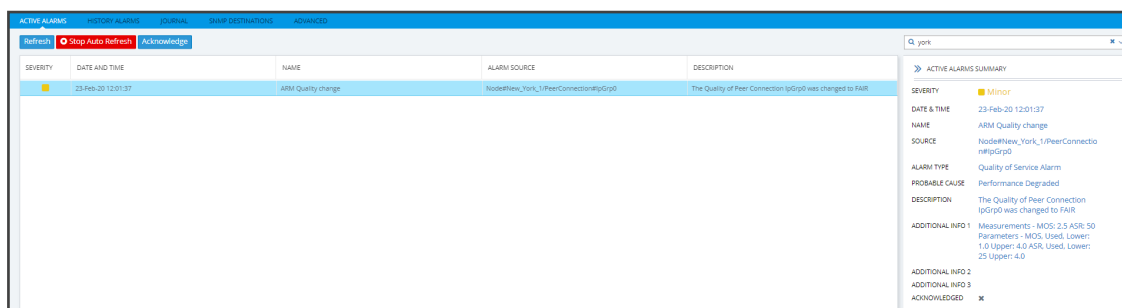
Locating a Specific Alarm

The search feature helps administrators quickly and easily locate specific alarms. This facilitates effective management which in turn leads to improved network performance.

➤ To search for a specific alarm:

1. Enter a search string in the search field shown in the following figure. To perform an advanced search, click the drop-down menu arrow; the figure shown after the next figure is displayed.

Figure 10-5: Search Field



The interface shows a search bar at the top right with the text "york". Below it, a table lists active alarms. The first alarm is highlighted:

SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
Minor	23-Feb-20 12:01:37	ARM Quality change	NodeBNew_York_1/PeerConnectionGrp0	The Quality of Peer Connection (pGrp0) was changed to FAIR

On the right side, there is a detailed view of the selected alarm, including fields for SEVERITY, DATE & TIME, NAME, SOURCE, ALARM TYPE, PROBABLE CAUSE, DESCRIPTION, and ADDITIONAL INFO.

Figure 10-6: Searching for a Specific Alarm

2. Enter any information about the alarm you know. You must enter information in at least one field.
 - The 'Name' field is identical to the simple search string field.
 - From the 'Severity' drop-down menu, select Clear, Indeterminate, Warning, Minor, Major or Critical. All alarms whose severity level match your selection will be displayed.
 - From the 'Acknowledged' drop-down menu, select True (the default is False). All acknowledged alarms will be displayed.
 - For the alarm 'Source', enter the node name or the Peer Connection name, if you know it. All alarms originating from that source will be displayed.
 - In the 'Description' field, enter a key word used to describe the alarm.
 - Select either **Between Times**, **Last 24 hours**, **Last week** or **Last 30 days**. All alarms whose timestamp matches your selection will be displayed.
3. Click **Search**.

Enriching Routing Rule Matching Notifications with ARM Information

In addition to supporting notification on a call matching a specific rule, the ARM also allows operators to *customize information provided with the notification*. The feature - notification sent on a call matching a rule - is usually applied for emergency calls such as 911 calls. The notifications usually require additional information such as user name, building, floor, country or

office branch name. This information is not part of the SIP INVITE message but it can be added to the ARM users database and used for additional information in notifications.

➤ **To implement the feature, follow this procedure:**

- Add the corresponding Property Dictionary property (**Users > Property Dictionary**) to the ARM's Users table and add the information to these columns; this data will be used as the additional information in generated notifications. See [Adding a Property Dictionary to the ARM](#) on page 150 for more information.
- Customize the notification in the 'Routing Rule match' screen (**Alarms > Advanced > Routing Rule match**) as described below.

➤ **To enrich routing rule matching notifications with ARM information:**

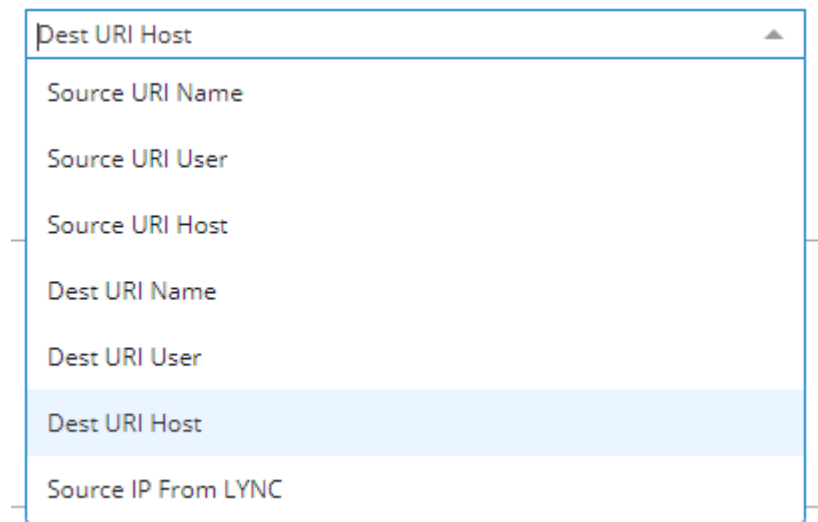
1. Open the 'Routing Rule match' screen (**Alarms > Advanced > Routing Rule match**) to customize the notification.

Figure 10-7: Routing Rule match

2. Enable the feature using parameter 'Add custom additional info'.
3. Define the notification in the uppermost screen section relating to matching and in the middle screen section displaying parameter 'Additional info pattern' shown in the preceding figure.

- The uppermost screen section relating to matching is used to identify the exact row (the exact record) in the Users table to be used to extract additional information for the notification. It includes:
 - ◆ **Request attribute to match.** Defines which **SIP INVITE message** property will be used as the matching criteria. The information is taken by the ARM Router from the SIP message and used to find the corresponding row in the Users table. Operators can select one of the following options from the drop-down:

Figure 10-8: Request attribute to match: SIP INVITE message properties



- ◆ **Match method.** Defines how to look for the corresponding entry in the Users table. Available values are Full (for an exact match), Contains (for the Users table value to contain the SIP message field) or Network Mask (for the value of the subnet mask).
- ◆ **User property to match.** Defines one of the properties (available in the ARM Users table) to be used for matching; the operator can select any property from the Property Dictionary.

In the preceding example, the Routing Rule match criteria are configured to make the following match:

If the IP address is taken from 'Dest URI Host' of the SIP Invite message belonging to the subnet (the matching method 'Network Mask') defined in the 'Remote Site' property of the ARM Users table, it will be considered as a match and this row in the Users table will be used for 'Additional info pattern'.

Using parameter 'Additional Info pattern', the operator defines information (and format) to be added as 'Additional Info 2' in the notification. This information is taken from the Users table (per matching row). The information to be presented is formatted using the @ symbol after which the operator can select a specific property:

Figure 10-9: Add custom additional info

Routing Rule match

Add custom additional info: ☒

Request attribute to match: *

Match method: *

User property to match: *

Additional info pattern:

* Press @ for properties options.
* Only first 255 characters will be shown.

4. Use the 'Test request attribute value' field shown in the figure below to test the definition.
 - Enter any potential value for 'Request attribute to match' (that can potentially be received in the appropriate SIP header) and thereby validate the required definitions.
 - This is the pattern that will be displayed in 'Additional Info 2' in a real notification in the case of a real call.

Figure 10-10: Test request attribute value

Routing Rule match

Add custom additional info: ☒

Request attribute to match: *

Match method: *

User property to match: *

Additional info pattern:

* Press @ for properties options.
* Only first 255 characters will be shown.

Test request attribute value:

Texas site calling from USA with number +1123456789

If there is no match, the message shown in the figure below is displayed:

Figure 10-11: No user info found

The screenshot shows a web interface with a form and a message. At the top, there is a label "Test request attribute value:" followed by a text input field containing the value "1.2.3.4". To the right of the input field is a blue button labeled "Test". Below the form, a light blue shaded area contains the text "No User info found".

11 Migrating Device Routing to the ARM

Existing device routing can be migrated to the ARM.



- Familiarity is assumed with the AudioCodes device whose routing is to be migrated to the ARM. See [Related Documentation](#) for references to AudioCodes' device documentation.
- The screenshots shown here are of Web interface version 7.2. If you're using Web interface version 7.0 or earlier, refer to earlier versions of this document.

AudioCodes Device Application Types

Before migrating device routing to the ARM, it's best to first get acquainted with the routing logic of AudioCodes' device application types. The routing logic of the three AudioCodes device application types are described:

- SBC device application
- Gateway device application
- Hybrid device running both a Gateway application and an SBC application

ARM Network Routing Logic

AudioCodes device's routing logic is centralized in its local routing table independently of the ARM. The SBC's routing logic is centralized in the IP-to-IP Routing Table. The Gateway's routing logic is centralized in the Tel-to-IP and IP-to-Tel routing table.

To integrate a device into the ARM network, the routing logic must be migrated to the ARM so that:

- All calls will be routed by the ARM.
- If a device disconnects from the ARM, calls will be managed by the device's internal routing table.
- If the ARM cannot find any route that matches a specific call, the call will be managed by the device's internal routing table.
- If the device fails to establish a call according to the ARM's routing directive (for example, a SIP error is received), the call will be discontinued.

SBC Routing Logic

AudioCodes' SBC routes and handles IP-to-IP calls. The SBC routing logic is centralized in the IP-to-IP Routing Table. For the ARM to route calls, you must configure a related routing rule in the SBC's internal IP-to-IP Routing Table as described in [Migrating SBC Routing to the ARM](#) on page 325.

Gateway Routing Logic

AudioCodes' Media Gateway routes and handles IP-to-Tel, Tel-to-IP and Tel-to-Tel calls using an internal loopback IP Group.

Gateway routing logic is configured in the device's internal IP-to-Tel and Tel-to-IP tables. To migrate the gateway application's routing logic to the ARM network, you must set the routing parameter 'Gateway Routing Server' to Enable. When this configuration is applied in the gateway, all its routing goes through the ARM and internal routing configuration is ignored.

Hybrid Device Routing Logic

The ARM routes calls from the hybrid device's PSTN (gateway application) to IP (SBC application) or vice versa.

Calls cannot be routed from an IP Group (PCon in ARM) associated with a gateway application, to an IP Group associated with an SBC application on the same hybrid device.

To support a hybrid device, two internal IP Groups must be configured:

- From the SBC application to the Media Gateway application
- From the Media Gateway application to the SBC application

The ARM GUI does not display these two internal IP Groups. Routing is performed per the logic described under [SBC Routing Logic](#) on the previous page and [Gateway Routing Logic](#) above, respectively.

See [Migrating Hybrid Routing to the ARM](#) on page 331 for information about how to migrate hybrid device routing to the ARM.

Connecting the Device to the ARM Topology Server

You need to connect the device to the ARM Topology Server.



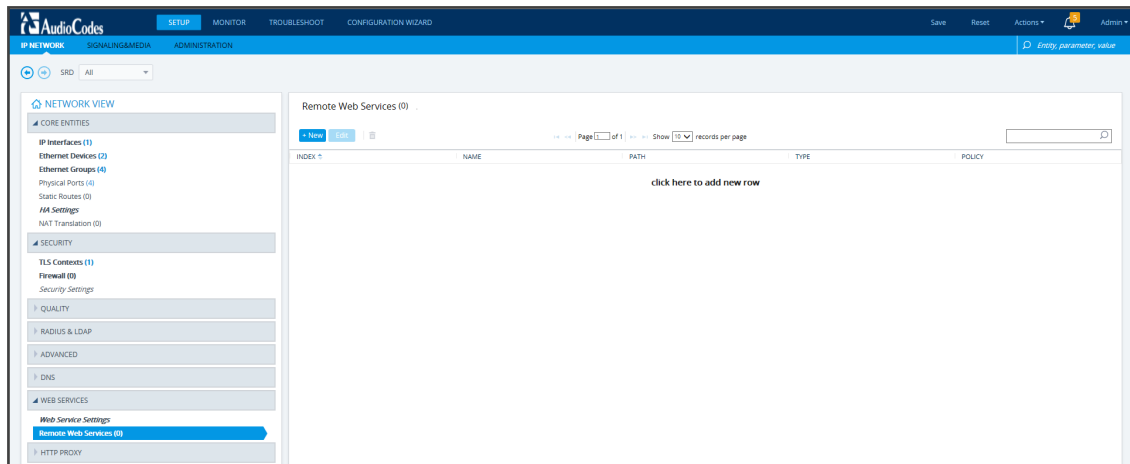
AudioCodes recommends starting a migration by manually adding a device in the ARM Network page as shown in [Adding an AudioCodes Node to the ARM](#) on page 74.

For auto-discovery provisioning, take the steps below to connect the device to the ARM network.

➤ To connect the device:

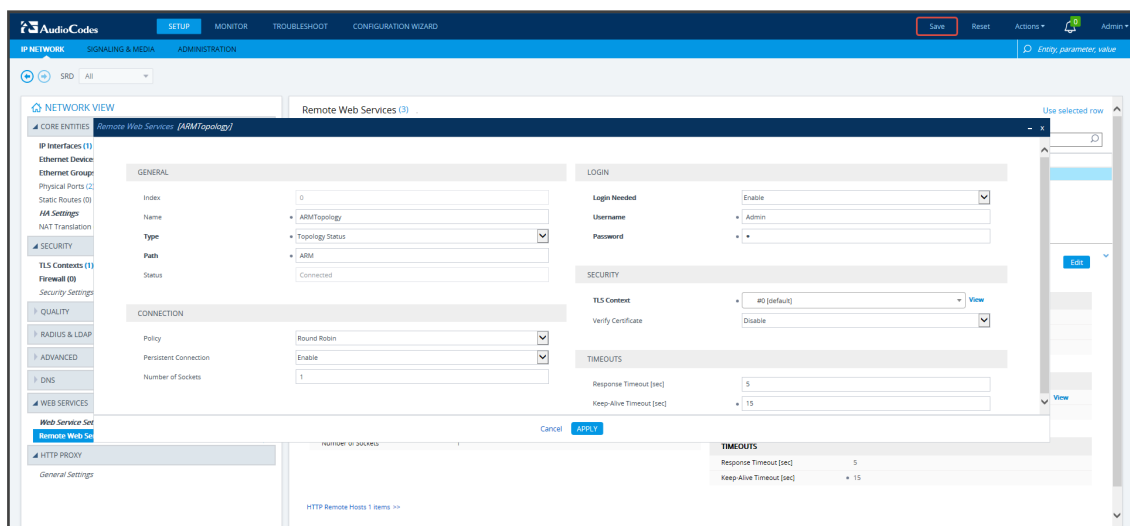
1. In your internet browser, enter the device's IP address in the Address bar, and then in the login page that opens, enter the User Name and Password (**Admin**, **Admin** are the defaults).
2. In the device's Web interface that opens, check the **Setup** menu and then navigate to the HTTP Remote Services page (**IP Network** > **Web Services** > **Remote Web Services**).

Figure 11-1: Services



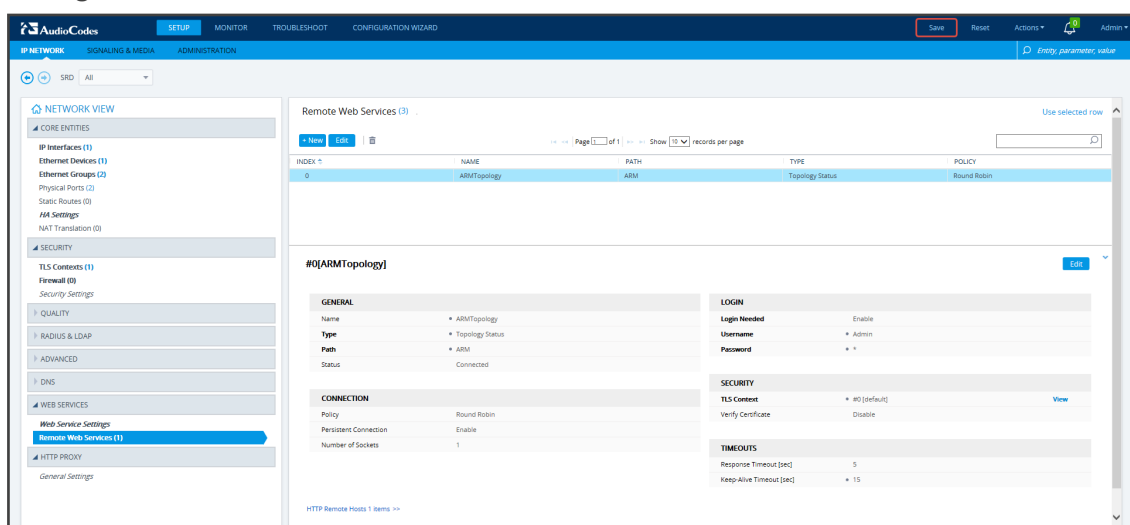
3. Click **+New** or click here to add new row.

Figure 11-2: Web Interface - HTTP Remote Services – Add Row



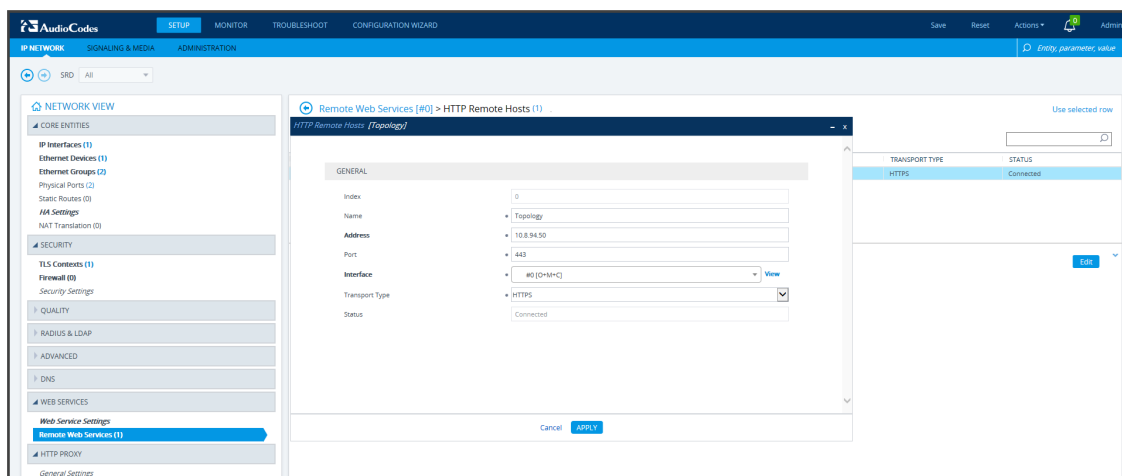
4. Configure the dialog using the figure above as reference, and click **Apply**.

Figure 11-3: Web Interface - Remote Web Services – HTTP Remote Hosts



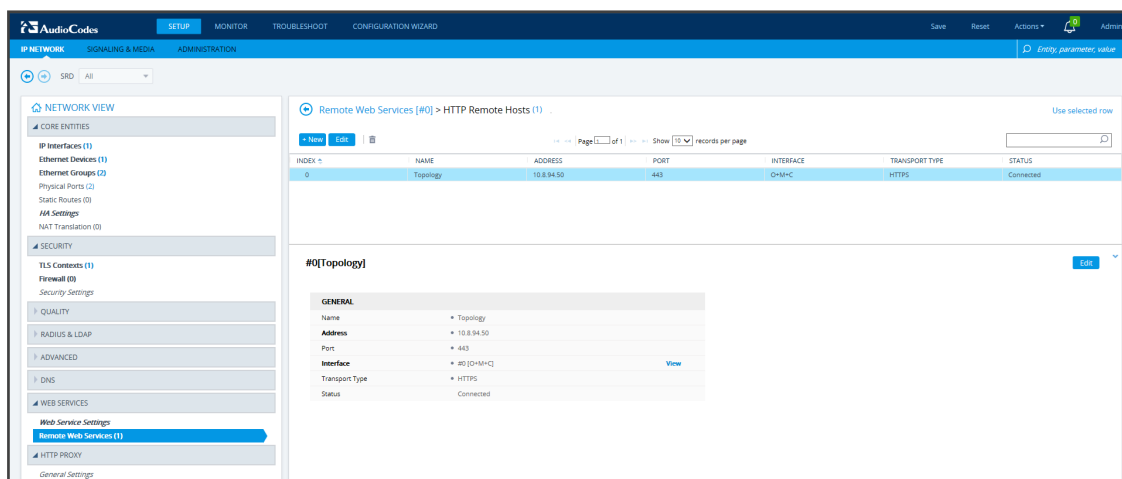
5. Click the **HTTP Remote Hosts** link shown in the figure above.
6. In the HTTP Remote Hosts page that opens, click the **Add** tab.

Figure 11-4: Web Interface - Remote Web Services - HTTP Remote Hosts - Add



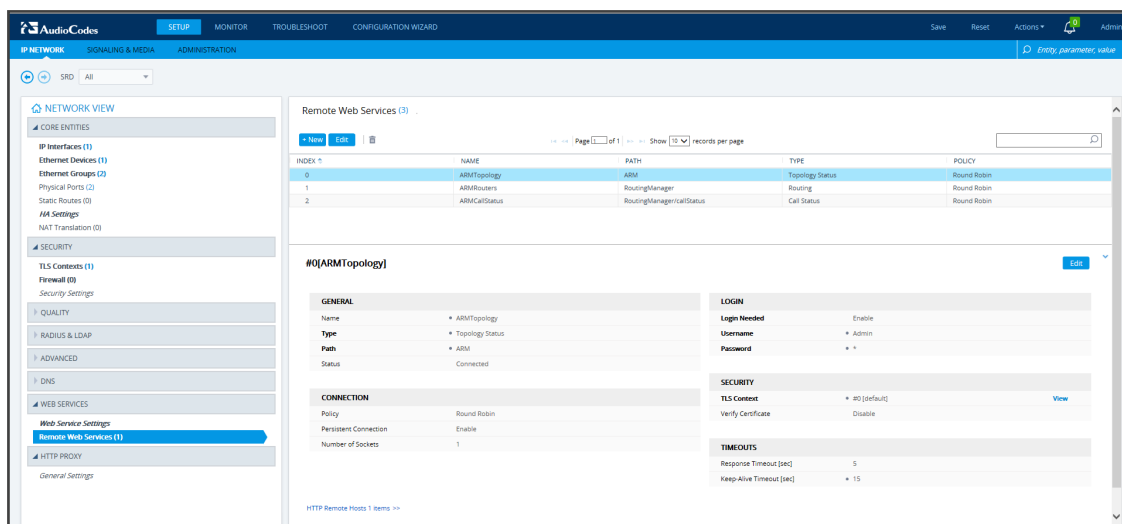
7. Define the IP Address of the ARM Topology Server to which you want to point the device and define the ARM Topology Server settings, and then click **Save**; wait until connected.

Figure 11-5: Web Interface – Device Connected to ARM Topology Server



8. Make sure in the Remote Web Services – HTTP Remote Hosts screen shown in the figure above that the status of the host, i.e., of the ARM Topology Server, is **Connected**.
9. Connect to the router/s.

Figure 11-6: Web Interface – Remote Web Services - Routers



10. Make sure that the device is connected to all HTTP ARM services i.e., ARM Topology Server *and* router/s, as shown in the figure above.

Defining an IP Interface Dedicated to ARM Traffic

ARM version 7.8 and nodes (SBC or Gateway) version 7.20A.154.044 and later support the capability to define on AudioCodes devices additional IP interfaces for management on any application type (Media and/or Control, not OAMP) and different TLS contexts for each IP interface.

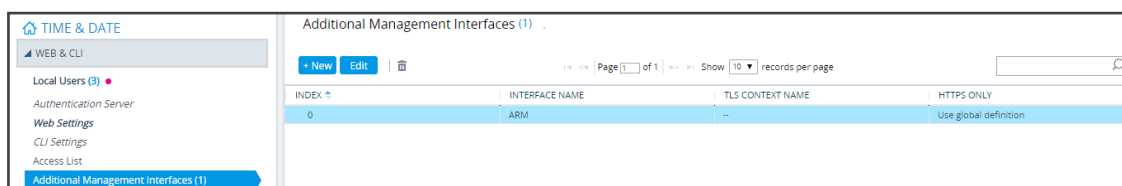
Defining a dedicated IP interface on the device for ARM traffic allows keeping ARM traffic internal, if required, separating ARM traffic from other device management traffic such as Web, SNMP and NTP.

When defining ARM on the node, you must assign an IP interface to the remote host (ARM) and a TLS context for the HTTP Service. The ARM automatically adds its routers to all nodes. When the ARM does this, it uses the same IP interface and TLS context that you defined for the ARM Configurator HTTP Service. If either the IP interface or the TLS context of the ARM Configurator will be changed, the ARM will synchronize the new values to the ARM routers.

➤ To provide an AudioCodes device with a dedicated ARM interface:

- Connect to the device's Web interface and in the Web interface, navigate to **Administration > Web & CLI > Additional Management Interfaces**. Configure an additional IP interface for device routing management as shown in the following figure.

Figure 11-7: Additional Management Interfaces



IP Interfaces (2)						
<div> + New Edit </div> <div> Page 1 of 1 Show 10 records per page </div>						
INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY
0	O+M+C	OAMP + Media + C	IPv4 Manual	172.17.133.17	24	172.17.133.1
1	ARM	Media + Control	IPv4 Manual	172.17.133.63	24	172.17.133.1

Migrating SBC/Gateway/Hybrid Routing to the ARM

AudioCodes devices can be migrated to the ARM network. After making sure that the device is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing logic from that configured in the device, to the ARM. The screenshots shown here are for illustrative purposes. The changes described here are the general changes that must be made.

➤ To migrate an AudioCodes device to the ARM network:

■ Configure IP Groups and SIP interfaces used by the ARM:

1. In the device's Web interface, navigate to the SIP Interface Table Page (**Setup > Signaling & Media > Core Entities > SIP Interfaces**).
2. Navigate to the SIP Interface Table Page (**Setup > Signaling & Media > Core Entities > SIP Interfaces**).
3. Locate the SIP Interface to expose the enterprise network to the ARM environment.

Figure 11-8: Web Interface – SIP Interfaces

The screenshot shows the AudioCodes Web Interface. The left sidebar contains a navigation menu with categories like TOPOLOGY VIEW, CORE ENTITIES, MEDIA, CODERS & PROFILES, SBC, and ACCOUNTS. The main content area is titled 'SIP Interfaces (1)' and shows a table with one interface. Below the table, the configuration details for the selected interface are shown in a tabbed format.

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_0	DefaultSRD (#0)	O+M+C	SBC	5060	5060	5061	No encapsulation	--

Below the table, the configuration details for the selected interface are shown:

- GENERAL**
 - Name: SIPInterface_0
 - Topology Location: Down
 - Network Interface: #0 (O+M+C)
 - Application Type: SBC
 - UDP Port: 5060
 - TCP Port: 5060
 - TLS Port: 5061
 - Encapsulating Protocol: No encapsulation
 - Enable TCP Keepalive: Disable
 - Used By Routing Server: Used
- CLASSIFICATION**
 - Classification Failure Response T...: 500
- MEDIA**
 - Media Realm: --
 - Direct Media: Disable
- SECURITY**
 - TLS Cert Name: #0 (default)
 - TLS Mutual Authentication: --
 - Message Policy: --
 - User Security Mode: Not Configured
 - Enable Un-Authenticated Regis...: Not configured
 - Max. Number of Registered Users: -1

Figure 11-9: Web Interface – SIP Interfaces Table - Configuring a SIP Interface

4. Set the 'Used by Routing Server' parameter to **Used**.
5. Click **Save**.

Migrating SBC Routing to the ARM

SBC routing can be migrated to the ARM network. After making sure the SBC is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing logic from that configured in the SBC, to the ARM. The screenshots shown here are for illustrative purposes only.



- See also [Checklist for Migrating SBC Routing to the ARM](#) on page 335.
- 'IP Group' and 'Trunk Group' in the Web are called 'Peer Connection' in the ARM.

➤ To migrate routing logic to the ARM:

1. In the Web interface, navigate to the IP Groups page (**Setup > Signaling & Media > Core Entities > IP Groups**).
2. Locate the IP Group to expose the enterprise network to the ARM environment. Make sure the SIP interface associated with this IP Group is configured as 'used by routing server'. See [Migrating SBC/Gateway/Hybrid Routing to the ARM](#) on the previous page.

Figure 11-10: Web Interface – IP Groups

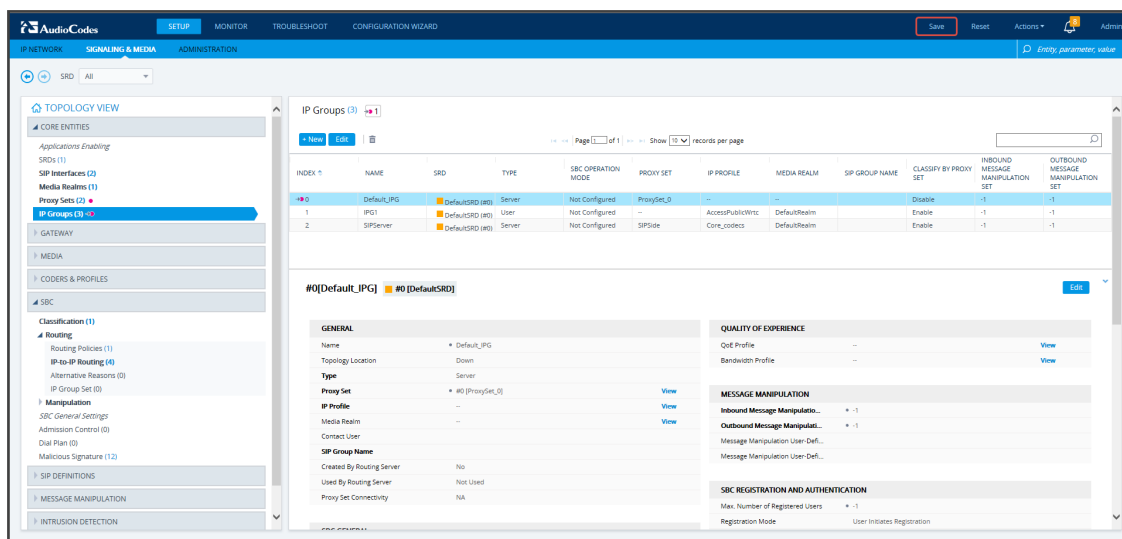
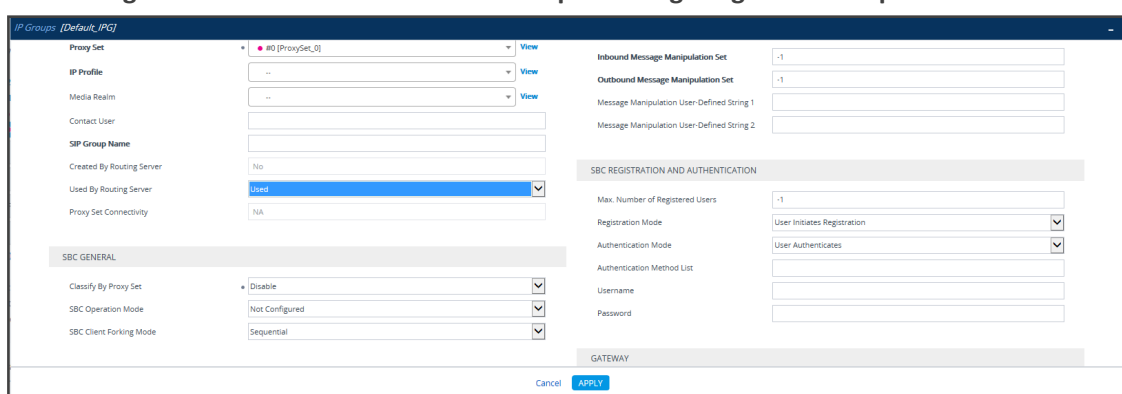


Figure 11-11: Web Interface – IP Groups - Configuring an IP Group



3. [Mandatory] Enter a unique name for the IP Group.
4. [Mandatory] Set the 'Used by Routing Server' parameter to **Used**.
5. Click **Save**.
6. In the ARM GUI, make sure the device is displayed in the Network page, Map view. Verify that the peer connection you configured is displayed. Unlock it and make sure its color is green (see [VoIP Peer Information and Actions](#) on page 37).



After configuring an IP group and then viewing it in the ARM, it is strongly recommended not to change its unique name. Changing its unique name will prevent routing by the ARM of calls to this Peer Connection (IP group) and receipt by the ARM of calls from this Peer Connection (IP group).

7. In the Web interface, open the IP-to-IP Routing page (**Setup > Signaling & Media > SBC > IP-to-IP Routing**). The screen below shows an example of two routing rules.

Figure 11-12: Web Interface – IP-to-IP Routing

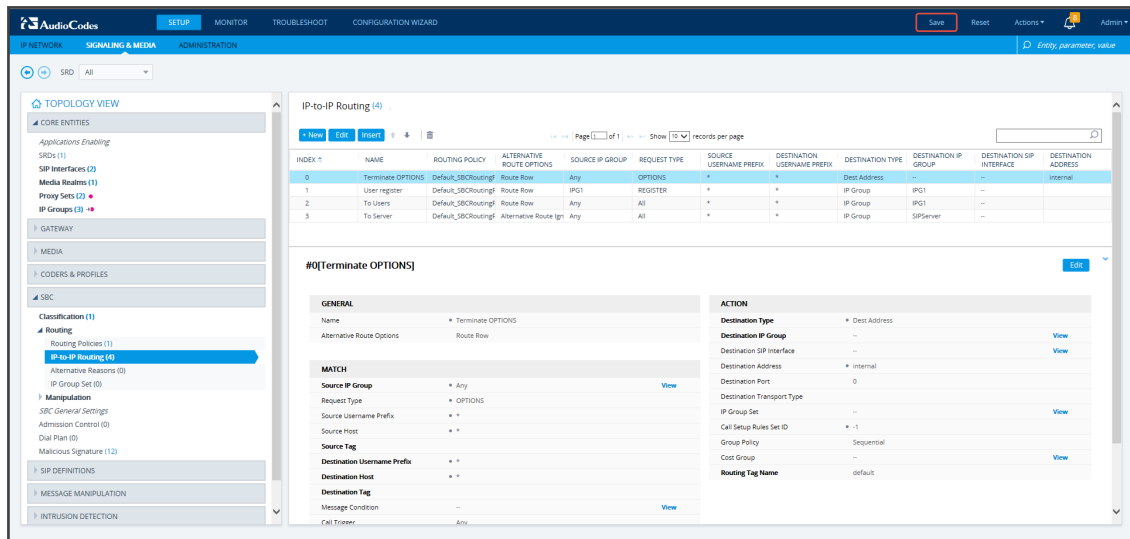
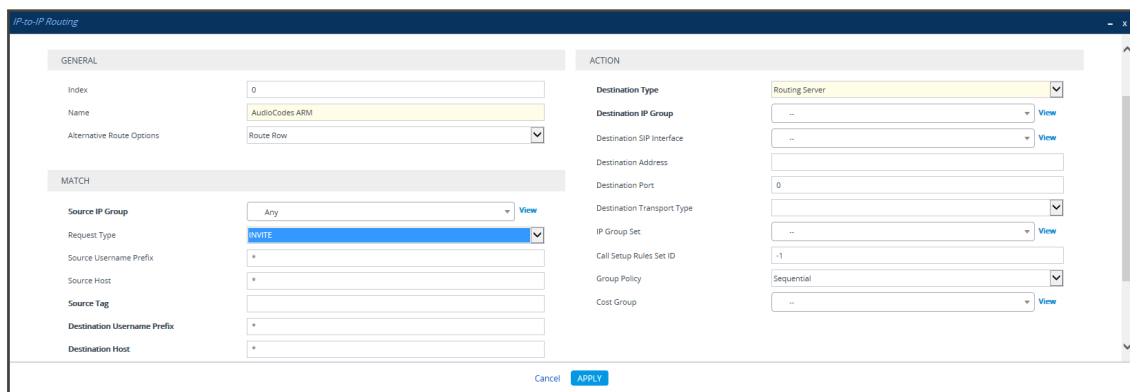


Figure 11-13: Web Interface – IP-to-IP Routing Table – Add Row – Rule tab

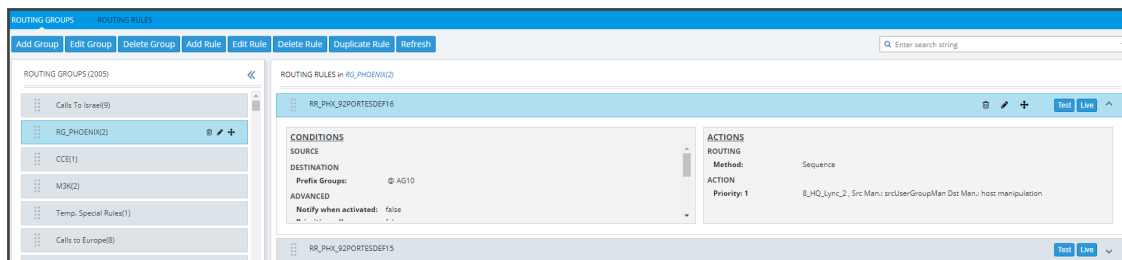


8. Define a 'Name' and for 'Request Type', define **INVITE** (see [Configuring an SBC to Send SIP Requests other than INVITE to ARM](#) on page 344 if you need to use the ARM to route other SIP Request Types such as MESSAGE or NOTIFY). Leave all other conditions fields undefined (i.e., No Conditions, or Any).
9. From the 'Destination Type' drop-down menu, select **Routing Server**. This rule will serve to perform routing via the ARM.
10. Leave all other fields undefined, and then click **Add**.

At this point, your routing service will still be operating according to that defined in the IP-to-IP Routing page in the SBC's Web interface.

11. In the ARM GUI's Routing page, configure a rule parallel to one of the rules configured in the Web interface's IP-to-IP Routing page (see [Adding a Routing Group](#) on page 262).

Figure 11-14: Configuring a Routing Rule in the ARM



12. In the ARM GUI, switch **Live** the routing rule; rule is now activated in the ARM.
13. In the Web interface, delete the routing rule. The transition is now complete.
14. Perform a Test Route (see [Testing a Route](#) on page 297 for detailed information).
15. Make a call and make sure it was established by the ARM.

Configure manually using the ini file, or in the Web interface's 'Admin' page, configure 'SendAcSessionIDHeader' = **1** for the SBC/Gateway to preserve the Call ID when a call passes through multiple SBCs/Gateways.



See also [Checklist for Migrating SBC Routing to the ARM](#) on page 335.

Migrating Media Gateway Routing to the ARM

After making sure that the device (the gateway in this case) is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing rules from those defined in the Web interface to the ARM. Screenshots are for illustrative purposes.

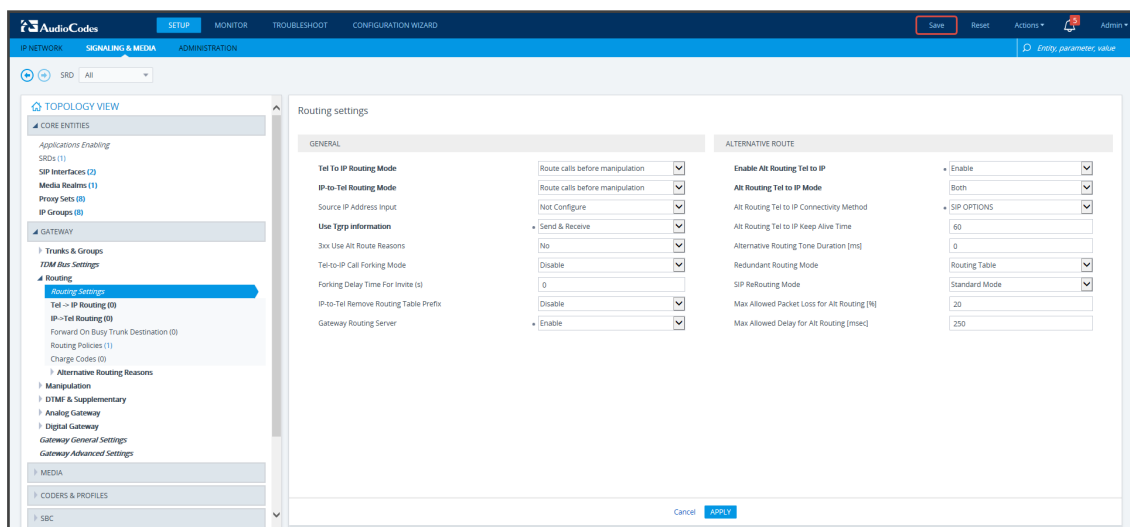


'Trunk Group' and 'IP Group' in the Web are called 'Peer Connection' in the ARM.

➤ To migrate gateway routing rules to the ARM:

1. In the Web interface, navigate to the Routing Settings page, and set the parameter 'Gateway Routing Server' to **Enable**.

Figure 11-15: Web Interface - Routing Settings Page



2. Navigate in the Web interface to the IP Groups page.
3. Locate the IP Group to expose the enterprise network to the ARM environment.
4. [Mandatory] Enter a unique name for the IP Group as shown in the following figure.
5. Set the 'Used by Routing Server' parameter to **Used** as shown in the following figure, and then click **Apply**.

Figure 11-16: Web Interface - IP Groups Page

6. Navigate to the Trunk Group Settings page (**Setup > Signaling & Media > Gateway > Trunk Group Settings**) shown in the following figure.
7. Locate the Trunk Group to expose the enterprise network to the ARM environment.
8. [Mandatory] Enter a unique name for the Trunk Group.
9. Set the 'Used by Routing Server' parameter to **Used**, and then click **Apply**.

Figure 11-17: Web Interface - Trunk Group Settings

10. In the ARM GUI, make sure the device is displayed in the Network page, Map view. Make sure the Peer Connection you configured is displayed. Unlock it and make sure its color is green.



After viewing the trunk group or IP Group in the ARM, it is strongly recommended not to change its unique name. Changing its unique name will prevent routing by the ARM of calls to this Peer Connection (trunk / IP group) and receipt by the ARM of calls from this Peer Connection (trunk / IP group).

At this point, your routing service will still be operating per that defined in the Tel- to-IP Routing and IP-to-Tel Routing pages in the gateway's Web interface.

In the ARM GUI's Routing page, configure a rule parallel to one of the rules configured in the Web interface's Tel-to-IP Routing or IP-to-Tel Routing pages.

11. Unlock the configured gateway Routing Rule in the ARM and check using the Test Route feature that the rules are functioning as required.
12. Delete the parallel rules configured in the Web interface's Tel-to-IP Routing or IP-to-Tel Routing pages.

Migrating Hybrid Routing to the ARM

After making sure that the hybrid device is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing rules from those defined in the Web interface to the ARM.

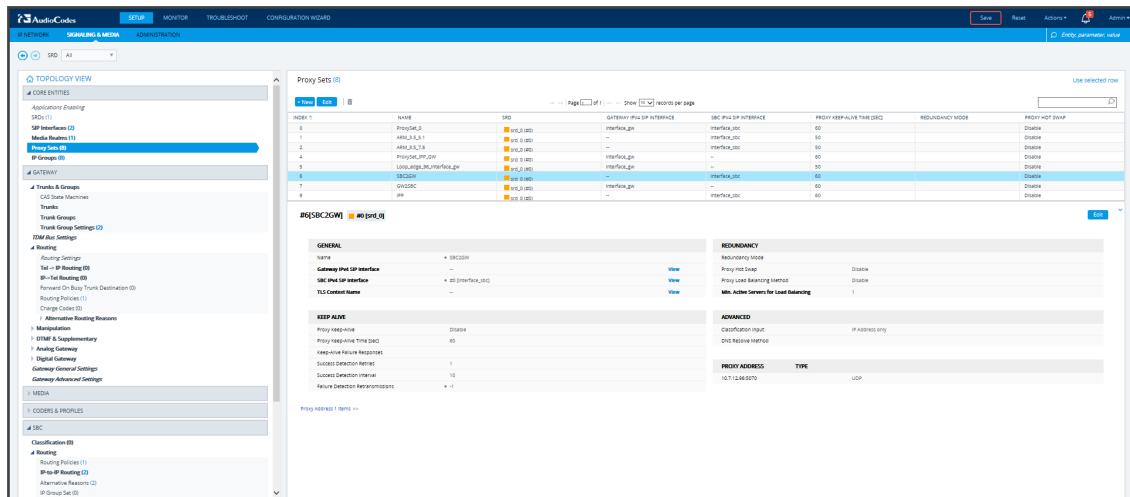
➤ To migrate hybrid routing rules to the ARM:

1. Perform migration of the SBC per the instructions in [Migrating SBC Routing to the ARM](#) on page 325.
2. Perform migration of the Media Gateway per the instructions in [Migrating Media Gateway Routing to the ARM](#) on page 329.
3. Open the hybrid device's Web interface.
4. Create an IP Group (Peer Connection) for the SBC application:
 - a. Open the Proxy Sets page (**Setup > Signaling & Media > Core Entities > Proxy Sets**) and then add a Proxy Set for the SBC application:

Figure 11-18: Add Proxy Set – for SBC

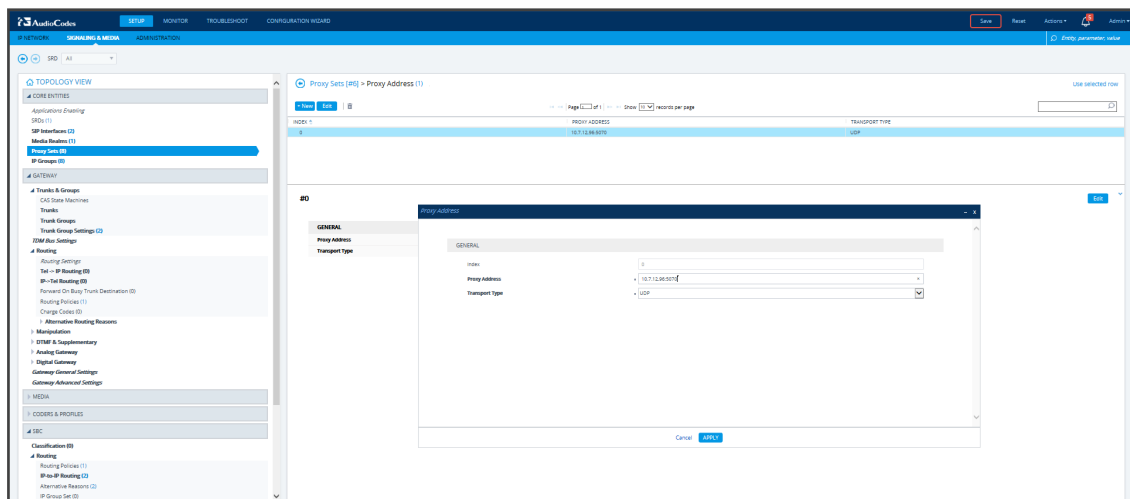
- b. From the 'SBC IPv4 SIP Interface' drop-down menu, select **SBC SIP Interface** and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

Figure 11-19: Proxy Sets



5. From the Proxy Sets list shown in the figure above, select the proxy set you added and then click the Proxy Address link.

Figure 11-20: Add New Proxy Address



- a. Enter the Proxy IP Address in the format **<IPAddress>:Port**. This address must point to the Gateway SIP interface address so a loop between the SBC SIP application and the Gateway SIP application is created.
- b. Open the IP Groups page (**Setup > Signaling & Media > IP Groups**), add an IP Group (click **New**) and associate it with the Proxy Set you added in Step 4a.

Figure 11-21: IP Group for the SBC Application

The screenshot shows the 'IP Groups' configuration page for the SBC application. The left sidebar lists various configuration categories. The main area contains fields for:

- Index:** 6
- Name:** IPG_sbc2gw
- Topology Location:** Down
- Type:** Server
- Proxy Set:** #6 [SBC2GW]
- IP Profile:** --
- Media Realm:** --
- Contact User:** --
- SIP Group Name:** --
- Created By Routing Server:** No
- Used By Routing Server:** Used
- Proxy Set Connectivity:** NA
- QoS Profile:** --
- Bandwidth Profile:** --
- MESSAGE MANIPULATION:**
 - Inbound Message Manipulation Set:** -1
 - Outbound Message Manipulation Set:** -1
 - Message Manipulation User-Defined String 1:** --
 - Message Manipulation User-Defined String 2:** --
- SBC REGISTRATION AND AUTHENTICATION:**
 - Max. Number of Registered Users:** -1
 - Registration Mode:** User Initiates Registration
 - Authentication Mode:** User Authenticates

 At the bottom, there are 'Cancel' and 'Apply' buttons.

6. Create an IP Group (Peer Connection) for the *Media Gateway* application:

- Open the Proxy Sets page (**Setup > Signaling & Media > Core Entities > Proxy Sets**) and then add a Proxy Set (click **New**) for the Media Gateway application:

Figure 11-22: New Proxy Set for Media Gateway Application

The screenshot shows the 'New Proxy Set' configuration page for the Media Gateway application. The left sidebar lists various configuration categories. The main area contains fields for:

- GENERAL:**
 - Index:** 7
 - Name:** GW2SBC
 - Gateway IPv4 SIP Interface:** #1 [Interface_gw]
 - SBC IPv4 SIP Interface:** --
 - TLS Context Name:** --
- KEEP ALIVE:**
 - Proxy Keep-Alive:** Disable
 - Proxy Keep-Alive Time [sec]:** 60
 - Keep-Alive Failure Responses:** --
 - Success Detection Retries:** 1
 - Success Detection Interval:** 10
- REDUNDANCY:**
 - Redundancy Mode:** --
 - Proxy Hot Swap:** Disable
 - Proxy Load Balancing Method:** Disable
 - Min. Active Servers for Load Balancing:** 1
- ADVANCED:**
 - Classification Input:** IP Address only
 - DNS Resolve Method:** --

 At the bottom, there are 'Cancel' and 'Apply' buttons.

- Select **Gateway SIP Interface** from the 'Gateway IPv4 SIP Interface' drop-down menu and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

Figure 11-23: Proxy Sets

The screenshot shows the 'Proxy Sets' list page. It includes a table with the following columns: INDEX, NAME, SBC, GATEWAY IPv4 SIP INTERFACE, SBC IPv4 SIP INTERFACE, PROXY KEEP-ALIVE TIME [SEC], REDUNDANCY MODE, and PROXY HOT SWAP. The table lists several proxy sets, including the newly added 'GW2SBC' set. Below the table, there is a detailed view of the 'GW2SBC' proxy set configuration, showing the same fields as in Figure 11-22.

INDEX	NAME	SBC	GATEWAY IPv4 SIP INTERFACE	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
1	ProxySet1	IPV4 (SBC)	Interface_gw	Interface_sbc	60	Disable	Disable
2	ProxySet2	IPV4 (SBC)	--	Interface_sbc	60	Disable	Disable
3	ProxySet3	IPV4 (SBC)	Interface_gw	--	60	Disable	Disable
4	ProxySet4	IPV4 (SBC)	Interface_gw	Interface_sbc	60	Disable	Disable
5	ProxySet5	IPV4 (SBC)	--	Interface_sbc	60	Disable	Disable
6	ProxySet6	IPV4 (SBC)	Interface_gw	Interface_sbc	60	Disable	Disable
7	GW2SBC	IPV4 (SBC)	Interface_gw	Interface_sbc	60	Disable	Disable
8	ProxySet8	IPV4 (SBC)	Interface_gw	Interface_sbc	60	Disable	Disable

- From the Proxy Sets list shown in the figure above, select the proxy set you added and then click the Proxy Address link.

Figure 11-24: Add New Proxy Address

The screenshot shows the AudioCodes SBC configuration interface. On the left is a navigation tree with categories like CORE ENTITIES, GATEWAY, MEDIA, CODERS & PROFILES, SBC, Routing, and MESSAGE MANIPULATION. The 'Proxy Sets' section is highlighted. A modal window titled 'Proxy Sets [87] > Proxy Address (1)' is open. It contains a 'GENERAL' tab with the following fields: Index (0), Proxy Address (10.7.12.96:5060), and Transport Type (UDP). At the bottom of the modal are 'Cancel' and 'APPLY' buttons. The top of the interface shows tabs for SETUP, MONITOR, TROUBLESHOOT, and CONFIGURATION WIZARD, with a 'Save' button highlighted in red.

- a. Enter the Proxy IP Address in the format **<IPAddress>:Port**. This address must point to the SBC SIP interface address so a loop between the Gateway SIP application and the SBC SIP application is created.
- b. Open the IP Groups page (**Setup > Signaling & Media > IP Groups**), add an IP Group (click **New**) and associate it with the Proxy Set you added:

Figure 11-25: IP Group for the SBC Application

The screenshot shows the 'IP Groups [IPG_gw2sbc]' configuration window. It has a 'GENERAL' tab with fields for Index (7), Name (IPG_gw2sbc), Topology Location (Down), Type (Server), Proxy Set (#7 [GW2SBC]), IP Profile, Media Realm, Contact User, SIP Group Name, Created By Routing Server (No), Used By Routing Server (Used), and Proxy Set Connectivity (NA). There are also 'Cancel' and 'APPLY' buttons at the bottom. To the right of the 'GENERAL' tab is a 'QUALITY OF EXPERIENCE' section with dropdowns for QoS Profile and Bandwidth Profile, and a 'MESSAGE MANIPULATION' section with dropdowns for Inbound and Outbound Message Manipulation Set, and two text fields for Message Manipulation User-Defined String 1 and 2. Below that is an 'SBC REGISTRATION AND AUTHENTICATION' section with a dropdown for Max. Number of Registered Users and a dropdown for Registration Mode (User Initiates Registration).

8. Click **Apply**. Check in the ARM that calls can be routed to and from the hybrid device.

12 Checklist for Migrating SBC Routing to the ARM

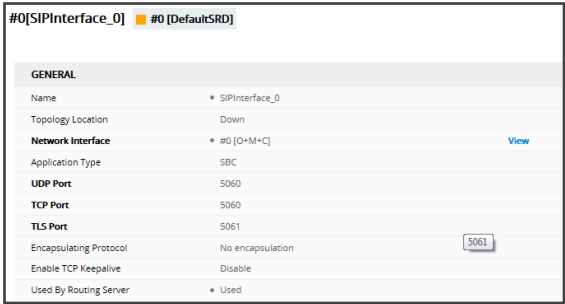
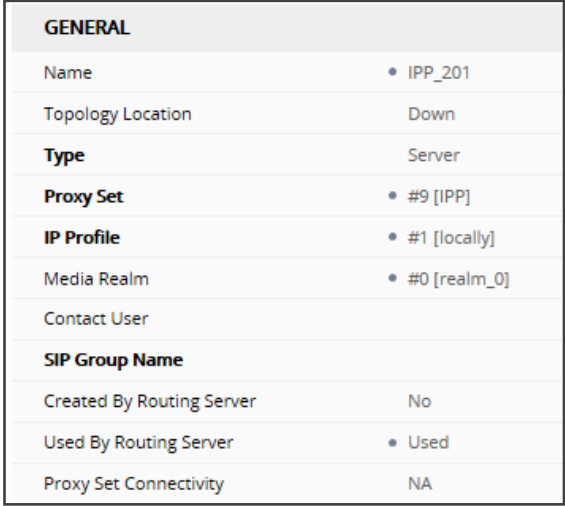
Administrators can use the checklist shown in the following table when migrating SBC routing to the ARM. Tick off the items in the list as you proceed.

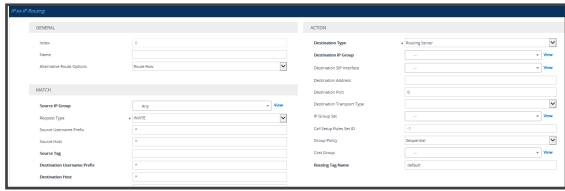


The screen shots shown here are of Web interface version 7.2. If you're using Web interface version 7.0 or earlier, refer to earlier versions of this document.

Table 12-1: SBC Migration Checklist

Item	SBC-Level	What should be viewed in the ARM																		
1	Configure the SBC in the way you used to, including all the IP Groups for connectivity with external SIP trunks and PBXs.	Unrelated to ARM																		
2	<p>Configure the IP address of the ARM's 'Configurator'</p> <p>Note: Do not configure Routers independently. Only configure 'Configurator' IP address and credentials:</p> <ul style="list-style-type: none">■ Configure in the SBC's Web interface (Setup > IP Network > Web Services > Remote Web Services):<ul style="list-style-type: none">✓ IP address of the Configurator✓ User name and Password for connecting to the Configurator. Default: Admin/Admin <div><div>#0[ARMTopology]</div><table><tr><th colspan="2">GENERAL</th></tr><tr><td>Name</td><td>• ARMTopology</td></tr><tr><td>Type</td><td>• Topology Status</td></tr><tr><td>Path</td><td>• ARM</td></tr><tr><td>Status</td><td>Connected</td></tr><tr><th colspan="2">CONNECTION</th></tr><tr><td>Policy</td><td>Round Robin</td></tr><tr><td>Persistent Connection</td><td>Enable</td></tr><tr><td>Number of Sockets</td><td>1</td></tr></table></div> <ul style="list-style-type: none">■ Make sure the status of each ARM service is 'Connected'.	GENERAL		Name	• ARMTopology	Type	• Topology Status	Path	• ARM	Status	Connected	CONNECTION		Policy	Round Robin	Persistent Connection	Enable	Number of Sockets	1	<p>View the new Node.</p> <p>Make sure it becomes green-coded, indicating that it's available.</p>
GENERAL																				
Name	• ARMTopology																			
Type	• Topology Status																			
Path	• ARM																			
Status	Connected																			
CONNECTION																				
Policy	Round Robin																			
Persistent Connection	Enable																			
Number of Sockets	1																			
3	Choose the SIP interfaces you want to use in the ARM (for ARM Peer Connections and ARM Connections) to be 'Used by Routing Server'.	You're able to select the chosen SIP Interfaces as ARM 'Routing Interfaces' for ARM																		

Item	SBC-Level	What should be viewed in the ARM
	<ul style="list-style-type: none"> Open the SBC Web interface (Setup > Signaling & Media > Core Entities > SIP Interfaces) 	Connections between the Nodes (SBCs)
4	<p>Select each IP Group you want to use in the ARM as a Peer Connection for routing, to be Used by Routing Server. These should be, for example, SIP trunks and connections to IP PBXs.</p> <ul style="list-style-type: none"> Open the IP Groups page (Setup > Signaling & Media > Core Entities > IP Groups). 	<p>View the selected IP Groups as ARM Peer Connections and attached VoIP Peers.</p> <p>View their availability status (green/red).</p> <p>In the ARM, unlock these Peer connections.</p>
5	<p>At this stage, the ARM does not route calls, though you can apply a 'test route' at the ARM level. The Node (SBC) does not send a routing request to the ARM after a SIP invite.</p>	<p>In the ARM you can now:</p> <ul style="list-style-type: none"> View and create ARM topology (connections between the Nodes) Add ARM routing groups

Item	SBC-Level	What should be viewed in the ARM
		<p>and Routing rules, manipulation groups, etc.</p> <ul style="list-style-type: none"> ■ Test yourself using the ARM's 'test route'
6	<p>Command the SBC to route calls using the ARM:</p> <ul style="list-style-type: none"> ■ Open the SBC Web interface IP-to-IP Routing (Setup > Signaling & Media > SBC > IP-to-IP Routing). ■ Make sure the rule that routes all INVITE requests to the ARM is configured. The following parameters are mandatory: 'Request Type' = INVITE; 'Destination Type' = Routing Server. 	<p>Calls are now routed by the ARM:</p> <ul style="list-style-type: none"> ■ SBC gets an INVITE ■ Sends routing Request to ARM ■ Get reply from ARM ■ Sends INVITE further according to the ARM's instructions
7	<p>Configure manually using the ini file (or in the 'Admin' Web interface page):</p> <p>SendAcSessionIDHeader = 1</p>	<p>Causes the SBC to preserve Call ID when a call passes through several SBCs.</p>

13 Prefixes

Use the following table as reference when defining prefixes.

Table 13-1: Prefixes

Notation	Description	Examples
[n-m]	Represents a range of numbers. Note: numbers “n” and “m” should be of the same length.	[5551200-5551300]#: represents all numbers from 5551200 to 5551300. 123[100-200]: represents all numbers from 123100 to 123200.
[n,m,...] or n,m,l, ...	Represents multiple numbers or strings.	[2,3,4,5,6]#: represents a one-digit number starting with 2, 3, 4, 5, or 6. [11,22,33]XXX#: represents a five-digit number that starts with 11, 22, or 33. [111,222]XXX#: represents a six-digit number that starts with 111 or 222. [2X,3X,4X,50,54]XXXXXX#: represents a 8 digit number starting with 2, 3, 4, 50 or 54 aaa,bbb,ce,field : represents names that start with one of the strings: aaa, bbb, ce or field.
[n1-m1,n2-m2, a,b,c,n3-m3]	Represents a mixed notation of multiple ranges and single numbers.	[123-130,455,766,780-790]: represents numbers 123 to 130, 455, 766, and 780 to 790.
X (capital only)	Represents any single digit or character.	BobX: represents names starting with bob1 or bob2@audiocodes.com AliceX#: represents names of 6-character length, starting with Alice, such as Alice1.
Pound sign (#) at the end of a number	Represents the end of a number.	54324XX#: represents a 7-digit number that starts with 54324.
Empty	Represents any number or string	

14 Examples of Normalization Rules

Here are some examples of Normalization Rules and regular expressions for your reference.

- Remove any non-number text from the prefix of the number:

The screenshot shows a dialog box titled "ATTRIBUTE MANIPULATION GROUP" with a close button (X) in the top right corner. Inside the dialog, there is a "Group Name" field containing the text "remove text from # prefix". Below this is a section labeled "Manipulation Rules:". It contains a list of rules, with the first rule having a regular expression "[^0-9]+" in the first column, "replace by:" in the second column, and "+9723456789" in the third column. To the right of the rules list are four buttons: a blue "+" button, a trash icon, and two gray arrow buttons (up and down). Below the rules list is a "Rules Simulation" section. It contains a text input field with "tel: +9723456789", a blue "Test" button, and a "Simulation Result:" label followed by the text "+9723456789" in green. At the bottom of the dialog are two blue buttons: "OK" and "Cancel".

- Strip the + from the number.

The screenshot shows a dialog box titled "Attribute Manipulation Group". It has a close button (X) in the top right corner. The "Group Name" field contains "Israel". Below this, the "Manipulation Rules:" section contains a table with one rule:

Rule	replace by:	Preview
\+972	972	97239764263

To the right of the table are buttons: a blue "+" button, a trash icon, and up/down arrow buttons. Below the table is the "Rules Simulation:" section. It contains a text input field with "+97239764263", a blue "Test" button, and a "Simulation Result:" label followed by "97239764263" in green text. At the bottom of the dialog are "OK" and "Cancel" buttons.

- Skype for Business: Remove "tel:" from the prefix and any text from the number's suffix. In the **Test** field, the full number is <tel:+97239762938> (ext:2938).

ATTRIBUTE MANIPULATION GROUP

Group Name

Skype for Business

Manipulation Rules:

tel:(\+?\d+).*\$

replace by:

\$1

+97239762938

+

✖

▲

▼

Rules Simulation

tel:+97239762938 (ext.293

Test

Simulation Result:

+97239762938

OK

Cancel

- If the fourth digit from the right is **4**, change it to **8**, and if the first digit is **0**, change it to **+972**.

ATTRIBUTE MANIPULATION GROUP

Group Name

8 to mobile

Manipulation Rules:

4(...)\$	replace by:	8\$1	039768653
^0	replace by:	+972	+97239768653

Rules Simulation

039764653

Test

Simulation Result: +97239768653

OK

Cancel

- Click **OK** and then click **Submit**.

15 Call Routing

The following describes call routing:

- A routing request results in an HTTP error response if no routing is available.
- A routing request from a source node which has an alternate route option returns the next alternate route option. The call route is not recalculated. If the alternate route list is empty, a 404 result is returned.
- A routing request from a node which is not the source node returns the next hop in the routing chain according to the original route selection. The routing logic is not performed again.

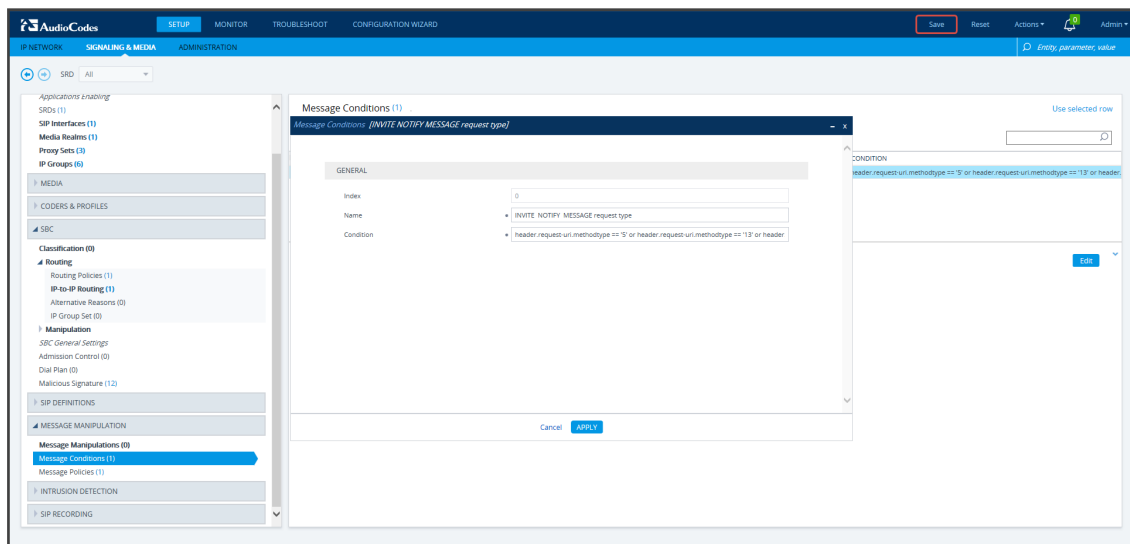
16 Configuring an SBC to Send SIP Requests other than INVITE to ARM

The SBC can be configured to send MESSAGE and NOTIFY SIP requests to the ARM. To get not only INVITE but also NOTIFY and MESSAGE, create a new Condition in the Condition table with the value: "header.request-uri.methodtype == '5' or header.request-uri.methodtype == '13' or header.request-uri.methodtype == '14'".

➤ **To configure the SBC to send SIP Requests other than INVITE to the ARM:**

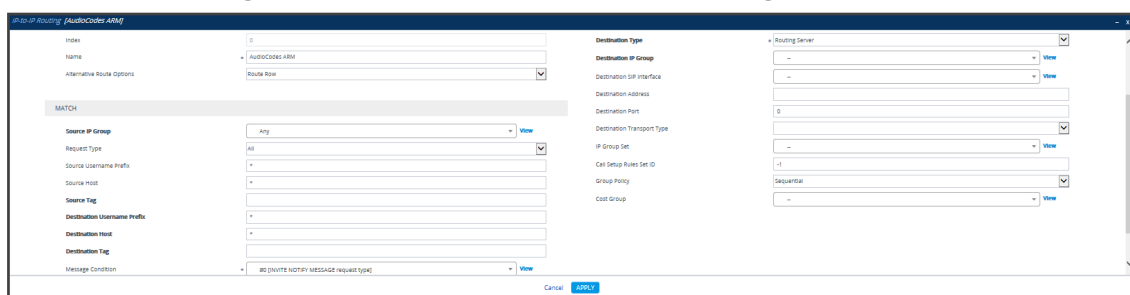
1. Open the Message Conditions page (**Setup > Signaling & Media > Message Manipulation > Message Conditions**) and click **Add**.

Figure 16-1: Web Interface – Message Conditions



2. Add the condition as shown in the figure above, and click **Apply**.
3. Open the IP-to-IP Routing page (**Setup > Signaling & Media > SBC > Routing > IP-to-IP Routing**), select the row of the Routing Rule that directs calls to the ARM, and click **Edit**.

Figure 16-2: Web Interface – IP-to-IP Routing



4. Edit the Routing Rule (see the preceding figure):
 - Change 'Request Type' from **Invite** to **All**.
 - Select the 'Message Condition' you configured.

5. Click **Apply**.
6. Make a call and make sure the call was established by the ARM.

Configure manually using the ini file, or in the Web interface's 'Admin' page, configure 'SendAcSessionIDHeader' = **1**. Note that this step is temporary and that a permanent solution is pending. It causes the SBC/Gateway to preserve Call ID when a call passes through several SBC/Gateways.

17 Operating with Azure AD

The ARM supports Microsoft Azure AD (in addition to LDAP and Microsoft Azure AD (Active Directory) on-premises) in compliance with the requirements of customers who operate fully in an Azure cloud environment and who want to utilize Azure AD based on the Graph REST API (rather than LDAP).

The feature covers two aspects:

- Azure AD as source for users in the ARM (see [Azure AD as a Source for Users in the ARM](#) on page 350)
- Azure AD for operator authentication (see [Azure AD for REST Requests Authentication](#) on page 188)

Configuring the ARM in the Azure Portal

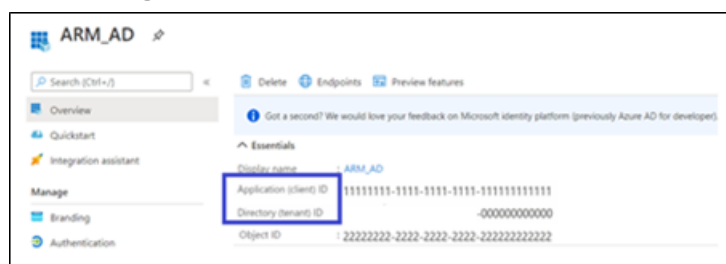
The following is relevant to both Azure AD authentication and Azure AD users. To add Azure AD to the ARM, first register the ARM as an application and provide the ARM with:

- Tenant ID
- Client ID
- Client secret

➤ To configure the ARM in the Azure Portal:

1. Register the ARM as an application; see instructions [here](#).
2. Retrieve the **Client ID** and the **Tenant ID**.
3. When registration finishes, provide the **Client ID** and **Tenant ID** displayed in the app registration's 'Overview' pane.

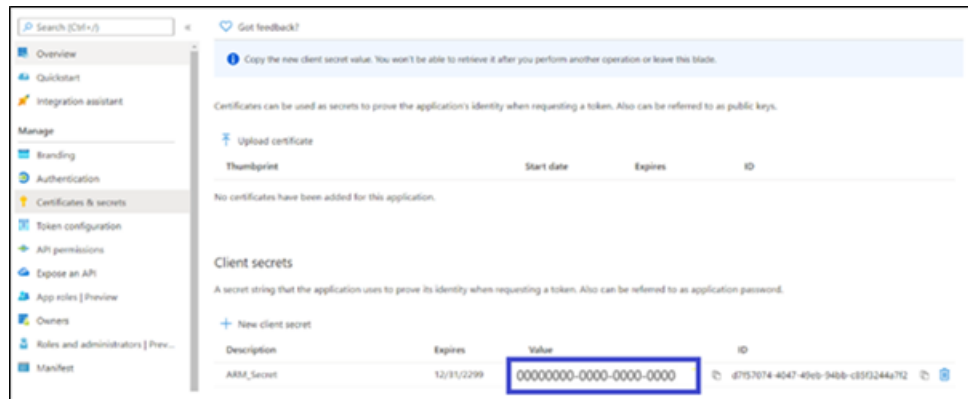
Figure 17-1: Azure Portal



4. Client secret

- a. Create a client secret by clicking **New client secret**.
- b. Copy the client secret value (not the ID) to a safe location; it becomes visible immediately after creation; only then can it be copied; later, it's displayed with stars, e.g., `hsjfhj*****k` and cannot be copied.

Figure 17-2: Client secret



5. Add Redirect URL

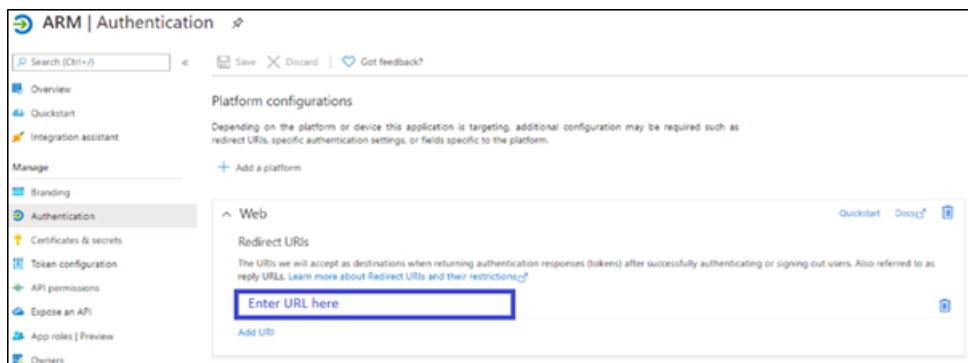
[Relevant for Azure AD authentication and not for Azure AD users]

Enter the ARM Redirect URL to the registered application in the Azure portal.

In your Azure AD:

- Under Manage: Authentication, click **add platform**.
- Choose **Web**.
- In 'Redirect URIs', enter the URL.
- Click **Configure**.

Figure 17-3: Redirect URIs



Make sure the format is **https://{IP address/Hostname}}/ARM/armui/login**

The selected communication method (IP address or hostname) must match the 'Communication method' configured in the ARM (under **Settings > Administration > Security** tab).

For simplicity, copy the Redirect URL from the **Settings > Administration > Azure Authentication** tab.

Figure 17-4: Azure Authentication

The screenshot shows the 'Azure Authentication' configuration page. On the left is a sidebar with navigation links: License, Security, Operators, Node Credentials, Router Credentials, Configurator Credentials, LDAP Authentication, RADIUS Authentication, Azure Authentication (selected), and Remote Manager. The main content area is titled 'Azure Authentication' and contains a section for 'AZURE ACTIVE DIRECTORY AUTHENTICATION'. It includes a toggle for 'Enable Azure Authentication', and input fields for 'Azure Tenant Id', 'Azure Client Id', 'Azure Client Secret', and 'Azure Redirect URL'. The 'Azure Redirect URL' field is highlighted with a blue box and contains the text 'https://10.7.2.30/ARM/armui/login'. There are 'Test' and 'Submit' buttons at the bottom right of the form.



Any change made to the 'Communication method' setting (**Settings > Administration > Security**) is automatically reflected in the Azure Redirect URL link. Make sure that the same is configured in the Azure AD.

6. API Permissions

The ARM uses Microsoft's Graph API v.1.0 to retrieve a user's information and app roles. In your Azure AD, go to the **API permissions** tab and add the following permissions (of Microsoft Graph):

- **User.Read (Delegated)** – allows the ARM to sign in on behalf of the user and read the user profile.
- **Application.Read.All** (Application) – allows the ARM to retrieve all app roles in the Azure AD for the purpose of testing connectivity.

For AD users, operators must also add the following permission:

- **User.Read.All** (Application) - allows the ARM to retrieve all the users and their properties from Azure AD.
- **Group.Read.All** (Application) – allows the ARM to retrieve the user's membership groups.

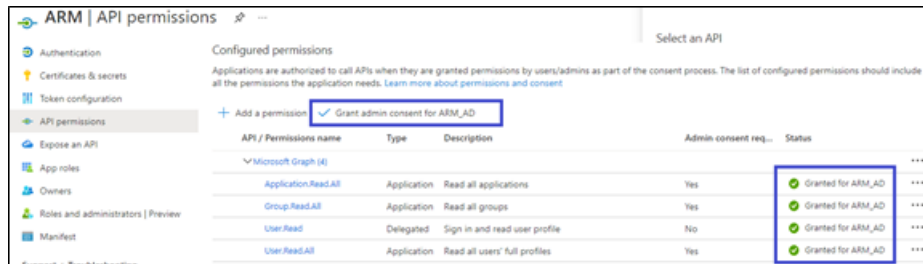
Figure 17-5: API Permissions

The screenshot shows the 'API permissions' page in the Azure AD portal. The left sidebar has 'API permissions' selected. The main content area is titled 'Configured permissions' and shows a table of permissions. The 'Add a permission' button is highlighted with a blue box. The right sidebar shows 'Request API permissions' with a 'Microsoft Graph' section highlighted by a blue box.

API / Permissions name	Type	Description
Group.Read.All	Delegated	Read all groups
Application.Read.All	Application	Read all groups
User.Read	Delegated	Sign in and read user profile

- Click **Grant admin consent** to enable these permissions.

Figure 17-6: Grant admin consent



7. Add app roles

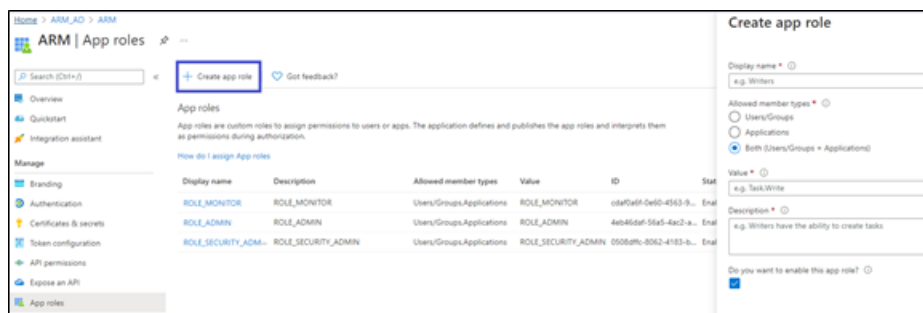
Create app roles that will be mapped to ARM access roles – Security Admin, Admin and Monitor. In Azure Active Directory, under **Manage**, select **App registrations** and select the application you defined in the first step.

Select **App roles | Preview** and then select **Create app role**.

In the **Create app role** pane, enter the settings for the role.

- Allowed member types** - Specifies whether this app role can be assigned to users, applications, or both. To support authentication via the REST API, both (**Users/Groups** + **Applications**) options should be selected, else select **Users/Groups**. AudioCodes recommends selecting the **Both** option which supports authentication of both the REST API and the GUI.
- Value** - Specifies the value of the roles claim that the application should expect in the token. This value should match the roles mapping in **Authorization level settings** in the ARM.

Figure 17-7: Authorization level settings



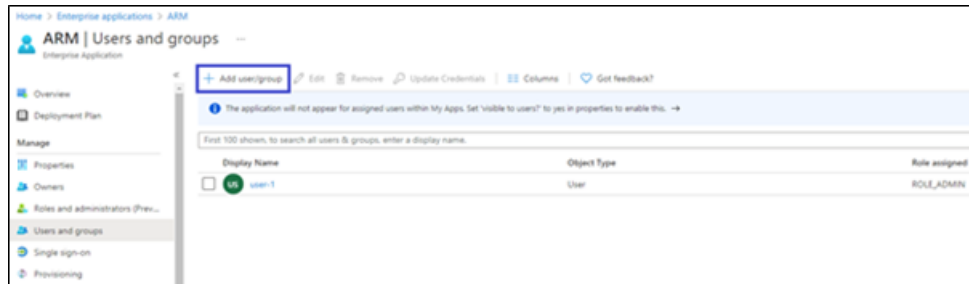
8. Assign users / groups to roles.

After you add app roles in your application, you can assign users and groups to the roles.

- In **Azure Active Directory** under **Manage**, select **Enterprise applications** in the left-hand navigation menu.
- Select **All applications** to view a list of all your applications and then select the application in which you want to assign users or a security group to roles.
- Under **Manage**, select **Users and groups**.
- Select **Add user/group** to open the **Add Assignment** pane.

- e. Select the **Users** or **groups** selector from the **Add Assignment** pane; a list of users and security groups is displayed.
- f. After you have selected users and groups, select the **Select** button to proceed.
- g. Select **Select a role** in the **Add assignment** pane; all the roles you defined for the application are displayed.
- h. Choose a role and select the **Select** button.
- i. Select the **Assign** button to finish the assignment of users and groups to the app.

Figure 17-8: Assign



- If you're using Azure B2C, adding app roles and assigning users / groups to roles is performed differently.
- Customers without Azure AD Premium cannot assign app roles to security groups. For these customers, app role assignment to users must be done individually by the administrator or an owner of the app.

More information about the app roles configuration and assignment is available [here](#).

Azure AD as a Source for Users in the ARM

The ARM allows you to access Azure AD natively and to add users from it. 'Azure AD Domain Services' is used as the interface between Azure AD and regular LDAP protocol to access users from Azure AD (without interfacing Azure AD with the REST API).

Microsoft's Graph API v.1.0 is used to retrieve users and the groups in which they're members. These users are treated as regular users in the ARM and can be used for regular operations - such as Users Groups.

The ARM supports most Azure AD flavors such as B2C and to a certain extent B2B (due to limitations in Microsoft's Graph API, for example, B2C doesn't support mapping of the "memberOf" attribute).



Operators cannot map Teams / Skype for Business properties such as EnterpriseVoiceEnabled, OnPremLineURI, HostedVoiceMail, VoiceRoutingPolicy as they're currently not retrievable by Microsoft's Graph API.

➤ **To add the Azure AD to the ARM:**

1. Register the ARM as an application and provide the ARM with the following information (as described previously):

- Tenant ID
- Client ID
- Client secret

You can also define parameters such as the frequency (in days) and the time, for the synchronization process.



Due to limitations in Microsoft's Graph API, the ARM doesn't support regular synchronization (Delta) against Azure AD; only full synchronization is supported.

2. Open the Servers page (**Users > Servers**).

Figure 17-9: Servers

SERVERS				
TYPE	STATUS	NAME	NUMBER OF USERS	LAST UPDATE
LDAP Server	✓	Audiodotcom	1013	20-May-21 09:26:03
LDAP Server	✓	Map2016	250000	20-May-21 09:26:01
LDAP Server	✓	AzureAD	1158	20-May-21 05:00:06

3. Click **Add** and select **Azure Active Directory**.

Figure 17-10: Servers > Azure Active Directory

SERVERS				
TYPE	STATUS	NAME	NUMBER OF USERS	LAST UPDATE
LDAP Server	✓	Audiodotcom	1013	20-Apr-21 10:19:58
Azure Active Directory	✓	Map2016	250000	20-Apr-21 10:19:56
LDAP Server	✓	AzureAD	1158	20-Apr-21 05:00:06

4. Provide information from Azure (as described in [Configuring the ARM in the Azure Portal](#) on page 346) and perform **Test connectivity**. The parameters under 'Updates' are related only to *full synchronization*.

Figure 17-11: Test connectivity

The screenshot shows the 'AZURE AD SETTINGS' dialog box. It has two tabs: 'AZURE AD SETTINGS' (active) and 'AZURE AD PROPERTIES'. The 'GENERAL' section contains the following fields:

Field	Value
Name: *	AzureAD
Tenant Id: *	a0423ecb-b74b-4e4e-95f1-e56a13ee3ce9
Client Id: *	5ad1366c-994c-4ae0-8604-b4c0a051e192
Client Secret:	
Page size:	999

Below these fields is a blue 'Test connectivity' button. The 'UPDATES' section contains the following fields:

Field	Value
Perform full update every (days):	1
At:	3 0
Sync timeout (min):	60
Query Timeout (seconds):	120

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

5. After successfully connecting to Azure AD, map the local properties to the values from Azure AD; the 'Azure AD Properties' drop-down fields display the relevant attributes from the Azure AD.

Figure 17-12: Azure AD Properties

PROPERTY	LDAP MAPPING	ATTRIBUTE NORMALIZATION
Display Name	displayName	ARMUI
Phone	mail	
Address	streetAddress	
Mobile	mobilePhone	0->+972
Country	country	
Office Phone	businessPhones	
2		
Physical address		
Emergency		
registration		
Origin		
SMS Line Line URI		



- Most fields of the type 'User' resource are available for mapping.
- See the list in Microsoft's documentation [here](#).

Authenticating Operator Login

See [Authenticating Operator Login Using Azure AD](#) on page 187 for details.

Revoking Azure User Tokens

Operators with a security level of 'Security Admin' can revoke all tokens created for Azure AD users.

➤ To revoke all tokens:

- Send the following REST request:

```
DELETE <ARM_Configurator_IP>/ARM/v1/security/authentication/token/revoke
```

18 Opening Firewall Ports for the ARM

Ports for the ARM must be opened in the Firewall. Use the following table as reference.

Table 18-1: Opening Firewall Ports for the ARM

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
ARM and Devices (SBCs / Gateways / Hybrid nodes)					
Device ↔ ARM Configurator (REST)	TCP (HTTPS) - default	✓	443	Topology Auto-discovery, Topology Status update, Quality information, long call sessions information (for licensing)	Bi-Directional
	TCP (HTTP) – debug only	✗	80	Topology Auto-discovery, Topology Status update, Quality information, long calls session information (for licensing)	Bi-directional
Device ↔ ARM Router (REST)	TCP (HTTPS) - default	✓	443	Routing requests and calls status	Bi-Directional
	TCP (HTTP) – debug only	✗	80	Routing requests and calls status	Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
ARM and LDAP Active Directory Server					
ARM Configurator ↔ Active Directory LDAP server	TCP (LDAP)	✗	389 (Default, can be configured at ARM)	Getting of ARM AD users and updating ARM user database	Bi-directional
	TCP (TLS - LDAPS)	✓	636 3268 for 'Global catalog' Default, can be configured at ARM)	Getting of ARM AD users and updating ARM user database LDAPS (TLS) is configured at ARM	Bi-directional
ARM GUI and North bound Interface					
UI (REST communication) → ARM Configurator	TCP (HTTPS)	✓	443	ARM component status updates, GUI, Provisioning, Alarms indications	Incoming (from ARM Configurator perspective)
Third-party application (via official REST API) → ARM Configurator	TCP (HTTPS)	✓	443	ARM component status updates, GUI, Provisioning, Alarms indications	Incoming (from ARM Configurator perspective)
ARM Configurator → SNMP Target	UDP (SNMP)	✗	161, 162 or configurable	ARM generates SNMP traps/alarms toward predefined	Outgoing

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				SNMP Target.	
ARM Management / Maintenance Interfaces					
ARM Configurator ↔ NTP Server	UDP (NTP server)	✗	123	ARM Configurator acts as NTP client toward external (pre-configured) NTP server. It also acts as NTP Server toward ARM Routers.	Bi-directional
ARM Router → NTP Server (ARM Configurator)	UDP (NTP)	✗	123	ARM Router acts as NTP client	Outgoing
ARM Configurator ↔ Client PC (SSH)	TCP	✓	22	SSH communication between ARM Configurator and external PC initiated by client PC: For ARM maintenance	Bi-directional
ARM Router ↔ Client PC (SSH)	TCP	✓	22	SSH communication between ARM Router and external PC initiated by client PC: For ARM maintenance	Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
ARM Configurator → Syslog server	TCP	✗	514 (by default) or configurable	ARM Configurator logs can be forwarded to external syslog server.	Outgoing
ARM Router → Syslog server	TCP	✗	514 (by default) or configurable	ARM Routers logs can be forwarded to external syslog server.	Outgoing
ARM Inter-Components Communication (Configurator ↔ Routers)					
ARM Configurator ↔ ARM Routers	TCP (HTTPS)	✓	443	Getting call statistics from the ARM Configurator; getting call sessions information for ARM licensing	Bi-directional
	TCP (HTTP) - debug only	✗	80	Getting call statistics from the ARM Configurator; getting call sessions information for ARM licensing	Bi-directional
ARM Configurator ← JMS Broker	TCP (TLS)	✓	8080	Informing ARM Routers about topology changes (including	Incoming

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				topology status and quality changes)	
ARM Router → JMS Broker	TCP (TLS)	✓	8080	Getting Topology updates from ARM	Outgoing
ARM Configurator ← Redis from Router	TCP (TLS)	✓	6379 (Router uses same 80 and 443)	Needed only if DID Masking is used in ARM for Redis synchronization between Routers and Configurator.	Bi-directional

19 About CDRs Sent by ARM to CDR Server

ARM Routers send CDRs (Call Detail Records) to a CDR Server. CDR messages contain information about all calls routed by the ARM, for example, source and destination users, call duration and call path. CDR messages also provide billing details. CDRs are sent as syslog packets to a predefined IP address configured by the operator. CDR syslog messages comply with RFC 3164 and are identified by Facility 17 (local1) and Severity 6 (Informational). CDR messages are built using `getRoute` and `CallStatus_callEnd` messages, by the first node in the paths. CDR types are `CALL_START` and `CALL_END`.

Calls from an SBC node:

1. One `CALL_START` message is sent per route (path)
2. Two `CALL_END` messages are sent at the end of the call

Calls from a gateway node:

1. One `CALL_START` message is sent per route (path)
2. One `CALL_END` message is sent at the end of the call (not per route)

SessionId is identical for all CDR messages related to the same call.

The **routeSeq**:

1. Represents the route (path) the ARM attempts
2. The count starts from 0
3. For example, for an SBC call, when there are three paths to attempt, the ARM sends:
 - a. First route (path): One `CALL_START` message and one `CALL_END` (outgoing leg) message. `routeSeq` = 0.
 - b. Second route (path): One `CALL_START` message and one `CALL_END` (outgoing leg) message. `routeSeq` = 1.
 - c. Third route (path): One `CALL_START` and two `CALL_END` (incoming and outgoing legs) messages. `routeSeq` = 2.

The following table describes all CDR fields.

Table 19-1: CDR Field Descriptions

CDR Field	Description	CDR Report Type	Format
RouterIp	IP address of the Router that sends the CDR.	All	String (15)
Seq	Each router sends its own sequence CDR starting with 1.	All	String (10)
CreationDate	The creation date of the CDR.	All	String (40)
CdrReportType	Report type: <div> <div></div> "CALL_START": CDR is sent upon an <code>getRoute</code> message on the first node. </div>	-	String (13)

CDR Field	Description	CDR Report Type	Format
	<ul style="list-style-type: none"> ■ "CALL_END": CDR is sent upon a CALL_STATUS_END_CALL message from the node. 		
AppType	Endpoint type: <ul style="list-style-type: none"> ■ "SBC" ■ "GW" ■ "HYBRID" ■ "THIRD_PARTY" 	All	String (13)
SessionId	Unique Session ID	All	String (20)
callId	CallId of the relevant leg	"CALL_START" – incoming leg. "CALL_END" – both legs.	String (55)
direction	Direction of the call: Incoming or Outgoing	"CALL_START"	String (10)
pconOrConnectionName	Pcon or connection name	All	String (35)
nodeId	ARM node database ID address	All	String (11)
nodeName	Node name as described in the GUI	All	String (25)
nodeIp	Node IP address	All	String (20)
pconId	Pcon database ID	"CALL_START"	String (10)
conId	Connection database ID	"CALL_START"	String (10)
pconOrConnectionType	Pcon or connection type	"CALL_START"	String (25)
outPconId	Outgoing Peer Connection database ID	"CALL_START"	String (10)
outConId	Outgoing Connection database ID	"CALL_START"	String (10)
outPconOrConType	Outgoing leg type	"CALL_START"	String (25)
lastNodeId	ID of the last node	"CALL_START"	String (10)
lastNodeName	Name of the last node	"CALL_START"	String (25)
lastPconId	ID of the last Peer Connection	"CALL_START"	String (10)
lastPconName	Name of the last Peer Connection	"CALL_START"	String (35)
srcUri	Source URI as actually sent (after manipulation).	All	String (50)
srcUriBeforeMap	Source before manipulation.	"CALL_START"	String (50)
from	From URI as actually sent (after manipulation).	"CALL_START"	String (50)

CDR Field	Description	CDR Report Type	Format
fromBeforeMap	From URI before manipulation.	"CALL_START"	String (50)
pai	P-Asserted-Identity URI as actually sent (after manipulation).	"CALL_START"	String (50)
paiBeforeMap	P-Asserted-Identity URI before manipulation.	"CALL_START"	String (50)
ppi	P-Preferred-Identity URI as actually sent (after manipulation).	"CALL_START"	String (50)
ppiBeforeMap	P-Preferred-Identity URI before manipulation.	"CALL_START"	String (50)
dstUri	Destination URI as actually sent (after manipulation).	All	String (50)
dstUriBeforeMap	Destination before manipulation.	"CALL_START"	String (50)
armSetupTime	ARM Router time when sending CALL_START.	"CALL_START"	String (30)
armReleaseTime	ARM Router time when sending CALL_END.	"CALL_END"	String (30)
sbcSetupTime	Gateway / SBC time when start handling Invite message.	"CALL_END"	String (40)
sbcConnectTime	Gateway / SBC time when 200 OK response (i.e., call is established)	"CALL_END"	String (40)
sbcReleaseTime	Gateway / SBC time when a BYE message (i.e., call ends)	"CALL_END"	String (40)
sbcAlertTime	Gateway / SBC time when start ringing	"CALL_END"	String (40)
alertDuration	Time of ringing in milliseconds (should be configured in the SBC /gateway to send in milliseconds)	"CALL_END"	String (13)
voiceDuration	Time of voice streamed in milliseconds (should be configured in the SBC /Gateway to send in milliseconds)	"CALL_END"	String (13)
completeDuration	Time of the whole call in milliseconds (from the first incoming Invite until ending the call)	"CALL_END"	String (16)
sipTerminationReason	SIP termination reason	"CALL_END"	String (20)
sipTerminationReasonDesc	SIP termination reason – more detailed	"CALL_END"	String (35)
routeSeq	Each route (path) of a call has a number. Starting from 0.	"CALL_START"	String (8)
sipInterface	sipInterface ID of the Connection or Peer Connection in the SBC / Gateway	"CALL_START"	String (20)
legId	Leg id of the SBC / Gateway	"CALL_END"	String (11)
routingRuleId	The Routing Rule ID of the match rule	"CALL_START"	String (13)
routingRuleName	The Routing Rule name of the match rule	"CALL_START"	String (30)
discardingByRoutingRule	The Routing Rule ID in case of discarding rule	"CALL_START"	String (24)

CDR Field	Description	CDR Report Type	Format
continueWithNodeInternalTablesByRoutingRule	Stop ARM routing and continue with node's internal routing	"CALL_START"	String (44)
fork	Is a fork call	"CALL_START"	String (5)
Path	String – describes the path.	"CALL_START"	String (200)

Two CDR format options are available:

- Clear text (separating each value with "|")
- As JSON

Here's an example of an ARM signaling CDR as *clear text*, sent at the end of a call (which was terminated normally):

Format:

```
|routerIp|seq|creationDate|cdrReportType|appType|sessionId|callId|direction
|pconOrConName
|nodeId|nodeName|nodeIp|pconId|conId|pconOrConType|sipInterface
|outPconId|outConId|outPconOrConType|lastPconId|lastNodeId|lastNodeName
|lastPconName|srcUri|srcUriBeforeMap|from|fromBeforeMap|pai|paiBeforeMap
|ppi|ppiBeforeMap|dstUri|dstUriBeforeMap|armSetupTime|armReleaseTime
|sbcSetupTime|sbcConnectTime|sbcReleaseTime|sbcAlertTime|alertDuration
|voiceDuration
|completeDuration|sipTerminationReason|sipTerminationReasonDesc|routeSeq
|legId|routingRuleId|routingRuleName|discardingByRoutingRule
|continueWithNodeInternalTablesByRoutingRule|fork|path
```

Value:

```
|10.7.6.102|4|2020-12-06T09:21:23.729Z|CALL_START|SBC|33a4b1cfb37733a5
|1-24960@10.7.20.148|RMT|SIPP|1|SBC_
102|10.7.12.102|70|null|IPGroup|SIPP|null
|1|IPGroup|71|3|Hybrid_96|SIPP|401@10.7.20.148
|123456@10.7.20.148|sipp201@10.7.12.102|sipp201@10.7.12.102|2020-12-
06T09:21:23.728Z|0|0|-1|47|src_uri|-1|-1|false|IncomingLeg=
[nodeId=1,nodeName=SBC_102,pconId=70,pconOrConnectionName=SIPP],
Outgoing Leg=[nodeId=3,nodeName=Hybrid_
96,pconId=71,pconOrConnectionName=SIPP], Edges=[Edge [connSrcNode=1,
connDestNode=5, connectionId=1], Edge [connSrcNode=5, connDestNode=3,
connectionId=2]]
```

Here's an example of an ARM signaling CDR as JSON, sent at the end of a call (that was terminated normally):

```
jsonCdr={"creationDate":"2020-12-06T09:21:23.729Z","sessionKey":"1_
33a4b1cfb37733a5","routerIp":"10.7.6.102","routerId":10,"seq":4,"cdrReportType":
"CALL_
START","cdrApplicationType":"SBC","sessionId":"33a4b1cfb37733a5","callId":"1-
24960@10.7.20.148","callOrig":"RMT","pconOrConName":"SIPP","nodeId":1,
"nodeName":"SBC102","nodeIp":"10.7.12.102","pconId":70,"conId":null,
"pconOrConType":"IPGroup","sipInterface":"SIPP","outPconId":null,"outConId":1,
"outPconOrConType":"IPGroup","lastPconId":71,"lastNodeId":3,
"lastNodeName":"Hybrid96","lastPconName":"SIPP","srcUri":"401@10.7.20.148",
"srcUriBeforeMap":"123456@10.7.20.148","from":"","fromBeforeMap":"","pai":"","
"paiBeforeMap":"","ppi":"","ppiBeforeMap":"","dstUri":"sipp201@10.7.12.102",
"dstUriBeforeMap":"sipp201@10.7.12.102","armSetupTime":"2020-12-
```

```
06T09:21:23.728Z",
"armReleaseTime":"","sbcSetupTime":"","sbcConnectTime":"","sbcReleaseTime":"","sbcAlertTime":"","alertDuration":"","voiceDuration":"0","completeDuration":"","sipTerminationReason":"","sipTerminationReasonDesc":"","routeSeq":0,"legId":-1,"routingRuleId":47,"routingRuleName":"src_uri","path":"Incoming Leg=[nodeId=1,nodeName=SBC_102,pconId=70,pconOrConnectionName=SIPP], Outgoing Leg=[nodeId=3,nodeName=Hybrid_96,pconId=71,pconOrConnectionName=SIPP], Edges=[Edge [connSrcNode=1, connDestNode=5, connectionId=1], Edge [connSrcNode=5, connDestNode=3, connectionId=2]]","discardingByRoutingRule":-1,"continueWithNodeInternalTablesByRoutingRule":-1,"fork":false,"httpResponse":200,"description":""}
```


20 Supported ARM Configurator and ARM Router Cipher Suites

Listed here are the cipher suites supported by the ARM server (ARM Configurator and ARM Router). The list following this list shows the client-supported cipher suites.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Listed here are the client-supported (when the ARM interfaces SBCs) cipher suites (most of the TLS available ciphers):

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Website: <https://www.audiocodes.com/>

Documentation Feedback: <https://online.audiocodes.com/documentation-feedback>

©2022 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, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience 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-41897

