User's Manual

One Voice Operations Center

AudioCodes Routing Manager (ARM)

Version 8.6

audiocodes

Notice

Date Published: April-10-2019

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
Mediant 9000 SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 3000 Gateway User's Manual

Manual Name
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
41880	Initial release
41881	New features: Adding ADs, Users and Users Groups, Adding an LDAP Property, Adding a User, Adding a User Property, Adding a User Group, Configuring Settings, Adding Operators, Adding Routing Servers, Configuring a Syslog Server, Adding a Number Manipulation Group, Adding a Prefix Group, Adding an NTP Server, Adding a Software License, Routing
41882	New: Migrating Media Gateway Routing
41883	Modified performance capability, added new GUI screens, deleted Network Table view, added Time-Base Routing, added Policy Studio, other minor additions.

LTRT	Description
41884	Version Release 7.4. Quality-based routing (MOS / ASR). Call Discard. SIP Reason. Test Route Details. Top 5 Routes. Layers. Center Map. Save Items Location. Configure directly in Web interface. Web interface 7.2. Other SIP Request Types.
41885	Time-based routing condition; Pcon Weight; Detach (Pcons); Routing Rules Hits Counting; Load Balancing; Single Sign On; New ARM login; Router Lock/Unlock; Test Routing Rule.
41886	Offline Provisioning | Alarms Journal | Call Detail Records | Add Connection | Advanced Condition: Call Preemption for Emergency Calls
41887	Support for 3rd party nodes. Manually added AudioCodes nodes. Statistics page and reports. Collapse/Expand nodes' associated VoIP peers. Class of Service. More robust node's state machine. Multiple Routing Attempts in Load Balancing Routing Rule Action. Routing Based on Call Trigger. New ARM License Model. SIP P-Asserted-Identity Manipulation in ARM Policy Studio. Upgrade of ARM Machines OS to CentOS 6.9. Enforcement of Memory Requirements for ARM VMs. CDR enhancements. LDAP operator authentication. Saving ARM configuration from GUI.
41888	Redesigned Network Map with new capabilities and extended capacity: larger networks, more elements, higher numbers of edges; multiple elements can be selected-repositioned simultaneously; lighter hoovers; new Actions menus. new ways to add a connection. Animated path for Test Route and Top Routes. Extended VoIP Peers collapse, expand and clustering capabilities. Operator login authentication with an external RADIUS server. Operators Permission Level. Test Route with a specific ARM Router. Improvements to the Prefix Groups UI design. Centralized Log Collection Utility. ARM Machine OS Upgraded with Latest CentOS6.9 Security Patches.
41889	Managed AudioCodes Devices. ARM Integrated into OVOC: ARM Status, ARM Alarms and Events Report to OVOC. Increased Number of ARM Routers. Platform Number Portability and Web-Based Pre-Routing Advisory Service. Extended ARM Router Survivability. Users Dictionary Attribute Triggered (Combined) by Two Other Attributes. Destination Prefix/Prefix Groups as a Condition. Notification on Calls Matching a Rule. Calling Number Privacy. Configuring Credentials for REST Communications. New Network Map Capabilities: Indication of the Aggregated Operative State of a Connection, New Option to Search for a Node by IP Address in Network Map, Number of VoIP Peers / Peer Connections Indicated in Cluster Summary, Adding VoIP Peers to an Existing Cluster, Limited Node/VoIP Peer Label Lengths in Network Map. Extended GUI Capabilities: Selecting Source Node / Peer Connection when Configuring a Routing Rule. Error Messages Display Name of Routing Rule | Users Group. Test Route Results Preserved Even if Moving to Another Tab. Optimized ARM UI for Huge Dial Plans. Indication of Operator's Security (Permission) Level. QoS (MOS and ASR) Displayed in Peer Connections Page.
41890	Hostname (FQDN). Certificate validation. Subject name verification. Open LDAP. Routing Server-Credentials. Routing Servers Group. SIP headers. Calls Forking Routing Method. CDRs. Call Details. Limiting number of CDRs.

Table of Contents

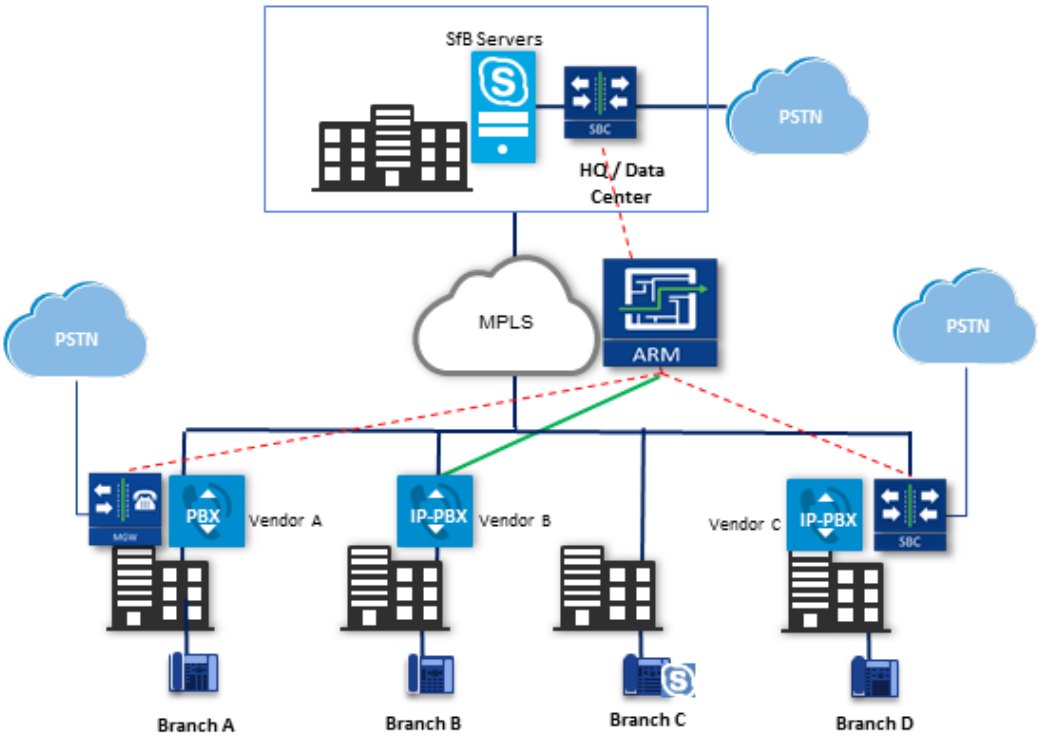
1 Overview

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

Third-Party Open-Source Software

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

- CentOS Linux 6.6
- 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-core
- Apache Commons Logging™
- HttpClient - Apache
- XStream (Group: com.thoughtworks.xstream)
- Jersey client
- Joda-Time
- SLF4J (Simple Logging Facade for Java)
- HikariCP Java 6
- Aspectj™ extension to Java
- SNMP4J (Open Source SNMP API for Java)
- Mockito

2 Getting Started with the ARM

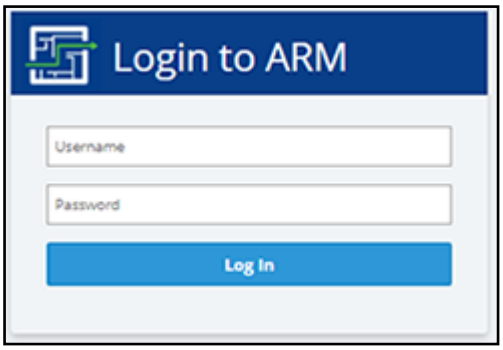
After installing the ARM and performing initial configuration (see the *ARM Installation Manual*), you can get started managing routing with the ARM.

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.



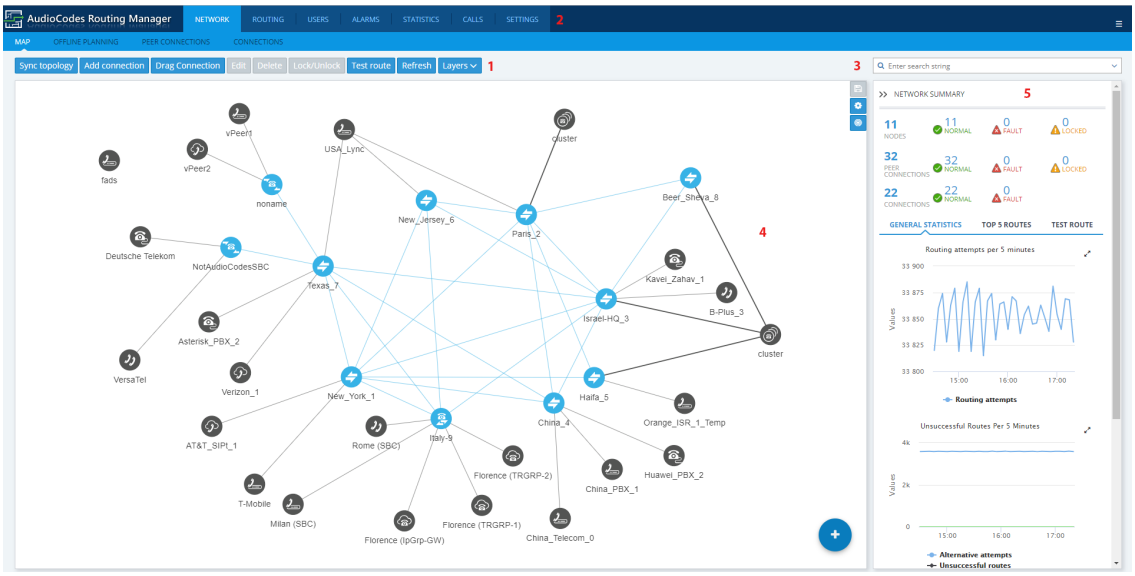
2. In the Login to ARM screen, log in using the default **Operator** and **Operator** username and password. It's advisable to change these as soon as possible (see Provisioning Operators on page 82 for instructions on how to change them).

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.

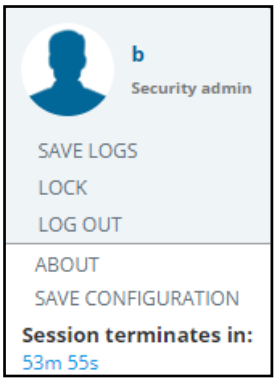
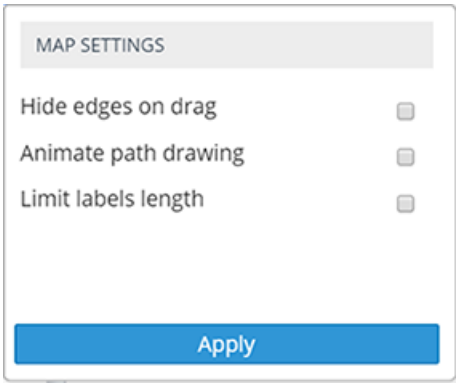
Figure 2-1: ARM GUI - Network Page - Map View

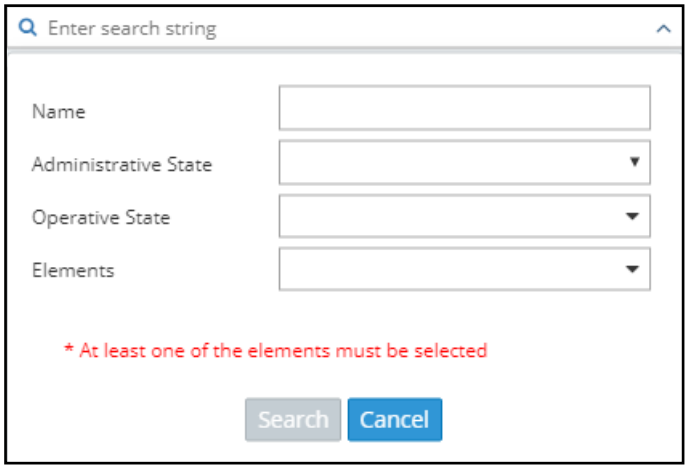


Use the following legend as a reference to the preceding figure.

Table 2-1: ARM GUI – Map View

#	GUI Area	Description
1	Actions Bar	■ Sync Topology ■ Add Connection ■ Drag Connection ■ Edit ■ Delete ■ Lock/Unlock ■ Test Route ■ Refresh ■ Layers ✔ topology ✔ quality

#	GUI Area	Description
2	Toolbar	Toolbar icons let you navigate to the following ARM pages: NETWORK, ROUTING, USERS, ALARMS, STATISTICS and SETTINGS.
		Located in the uppermost right corner of the page on the toolbar.  ■ View the name of the operator currently logged in and their security / permission level ■ Save logs (GUI logs) ■ Lock (Terminates user's ARM GUI session) ■ Log out ■ Display the ARM version (About) ■ 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. ■ Display 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):  ■ For more information about **Hide edges on drag**, see Repositioning Elements in the Network Map Page on page 33 ■ Select **Animate path drawing** for animated visualizations of Test Route and Top Route actions.

#	GUI Area	Description
		■ 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	Enables you to locate specific information in the Network Map view, Routing page, Users page, Alarms page and Settings page. 1. Click ^ adjacent to 'Enter search string'.  2. Define search parameters: Name and/or Administrative State and/or Operative State. At least one item must be selected. 3. You can also search for a Node *by the Node's IP address*, not only by the Node's name, which is an essential functionality in very large deployments with high numbers of Nodes.
4	Main Screen	The Network page displays a Map view of network entities.
5	Summary Panes	The Network page, Map view, displays these summary panes: ■ Network Summary ✔ Nodes (Available, Unavailable, Locked) ✔ Peer Connections (Available, Unavailable, Locked) ✔ Connections (Available, Unavailable) ■ General Statistics ✔ 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

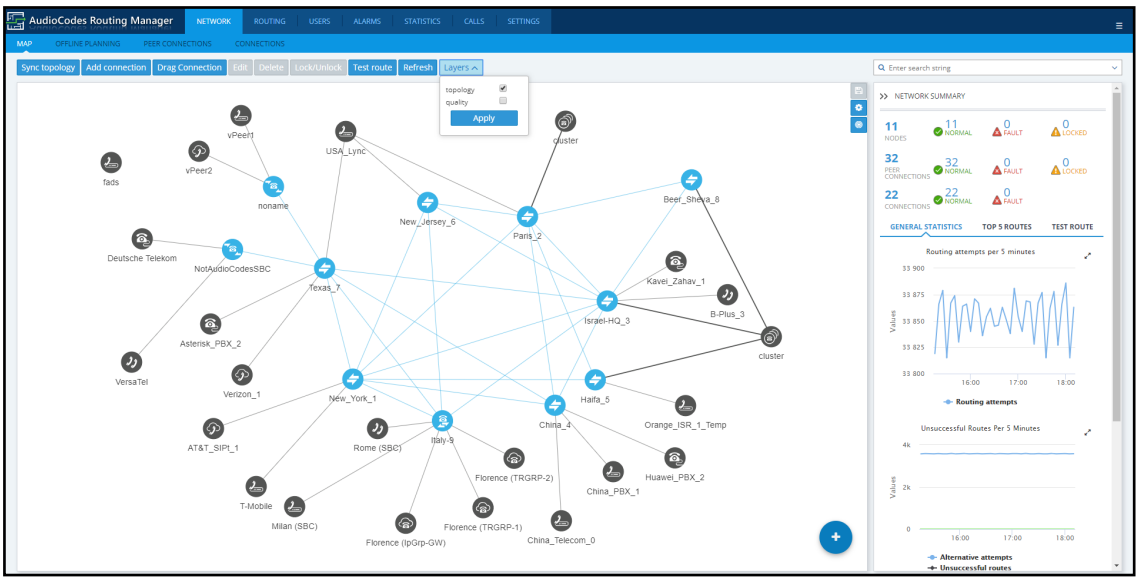
Network Entity	Icon	Explanation
Node		Indicates an AudioCodes SBC communicating with the ARM. It's part of the ARM network topology. Blue = operative state available/logging in Red = operative state unavailable/unrouteable Orange = operative state logged out Strikethrough = locked No strikethrough = unlocked
		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 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 Strikethrough = locked No strikethrough = unlocked
		Indicates a third-party, non-AudioCodes device (SBC or gateway) communicating with the ARM. It's part of the ARM network topology.

Network Entity	Icon	Explanation	
VoIP Peer		Indicates a non-AudioCodes device or entity that is also part of the ARM network topology: 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.	
			SIP trunk
			PSTN
			IP phones
			Legacy PBX | IP PBX
		N/A	Not applicable
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 AudioCodes device and the remote device) / predeleted (IP Group was deleted from the device) Black line through a red sphere = unavailable and locked Black line through a black sphere = available but locked	

Getting Acquainted with the Network Map Quality Layer

The Network Map view displays a **Layers** tab that allows the operator to choose **topology** and / or **quality**.

Figure 2-2: Network Map – Topology Layer

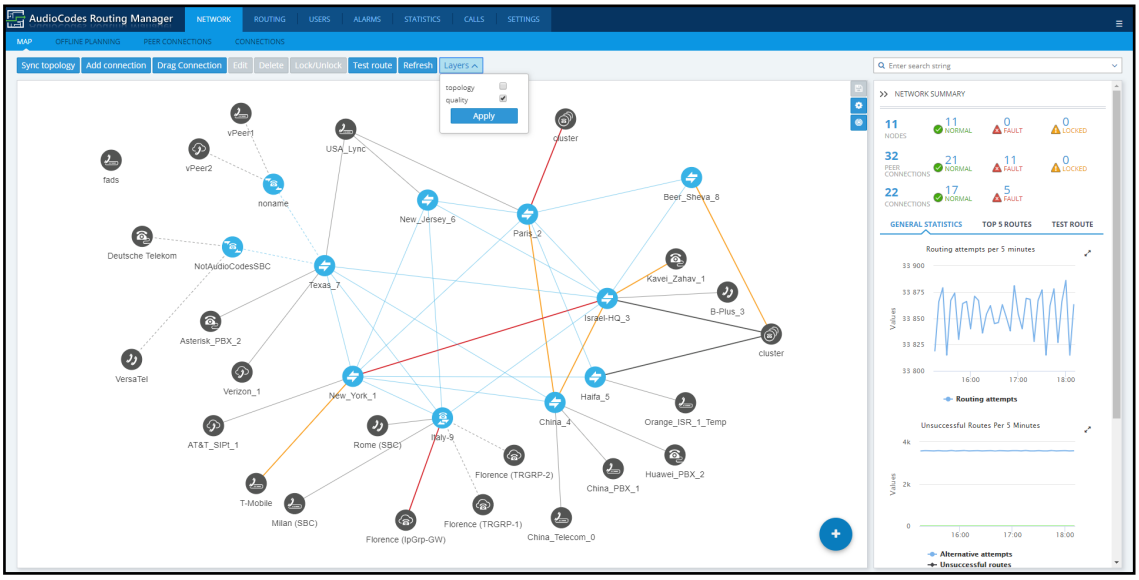


The **topology** layer displays the availability status of network entities.

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

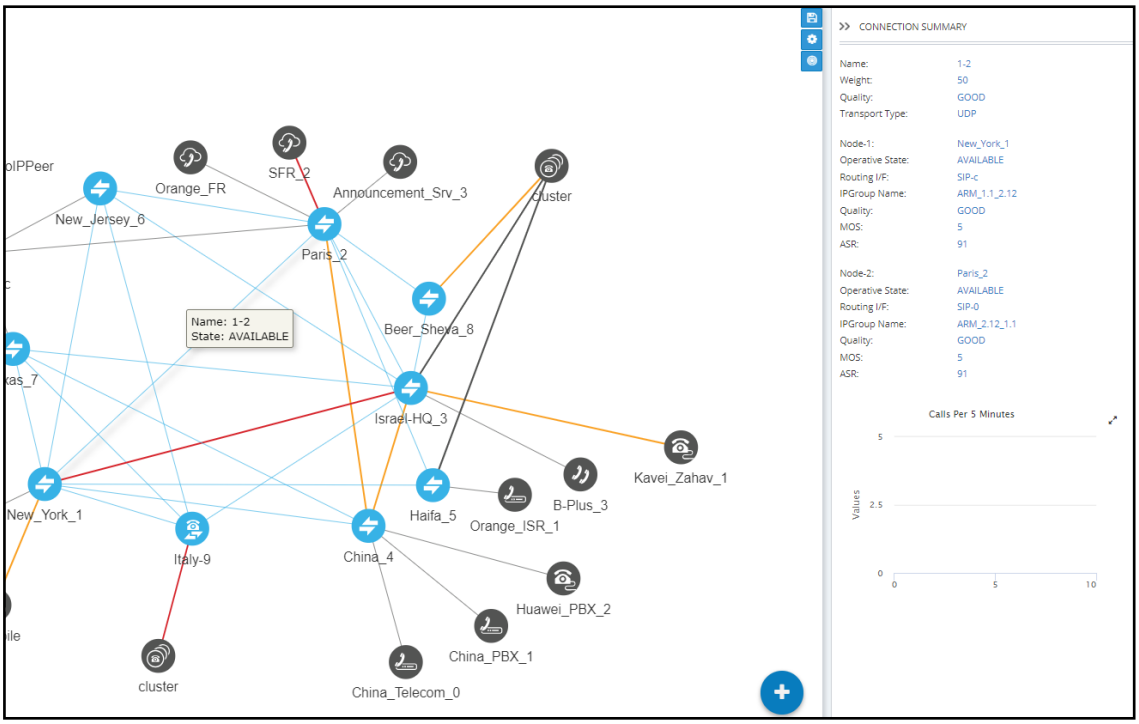
Color	Description
Grey	GOOD quality Peer Connection
Orange	FAIR quality Connection / Peer Connection
Red	BAD quality Connection / Peer Connection
Dotted grey	UNKNOWN quality, i.e., there is insufficient data to determine quality statistics. After enough calls are routed by the Connection / Peer Connection,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

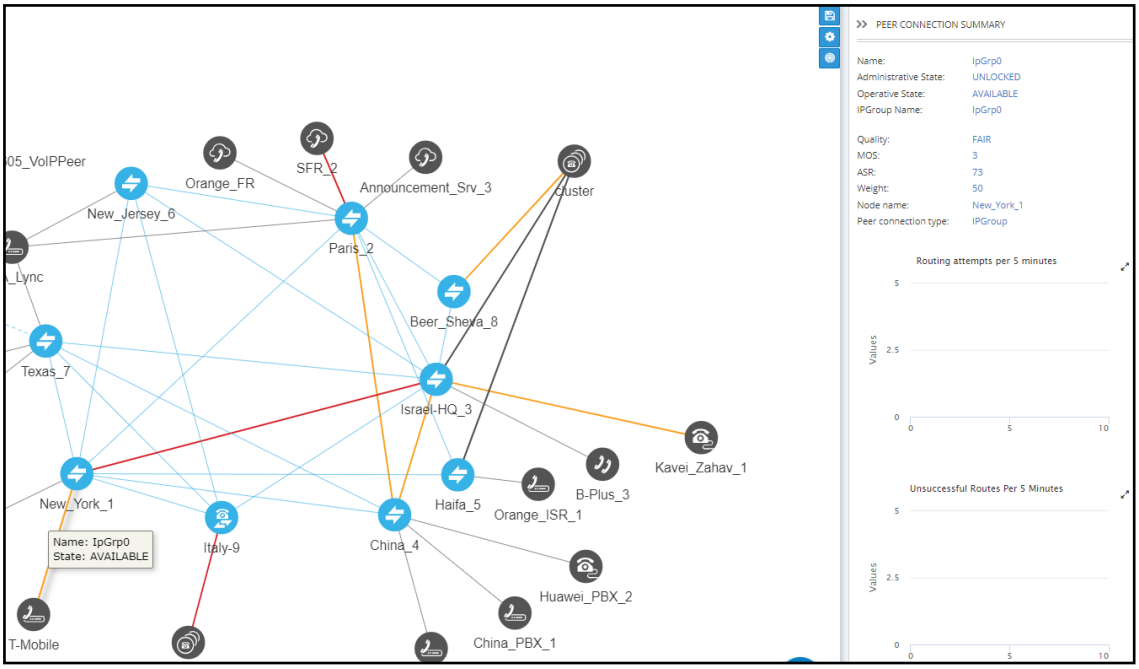


2. View a summary of the connection in the Connection Summary pane on the right side of the Network Map page. The figure above shows the Connection Summary pane for the Connection between the node **Paris_2** and **New_York_1**. The 'Quality' parameter for both nodes is 'GOOD'.
3. Use each direction's 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.

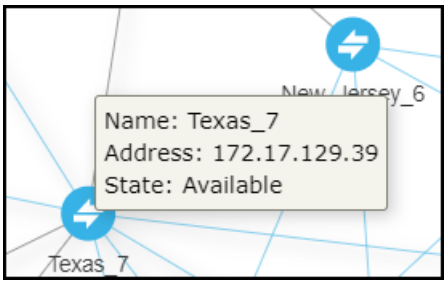
Getting Acquainted with Network Map Page Actions

Node Information and Actions

In the Network page, Map view, 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.

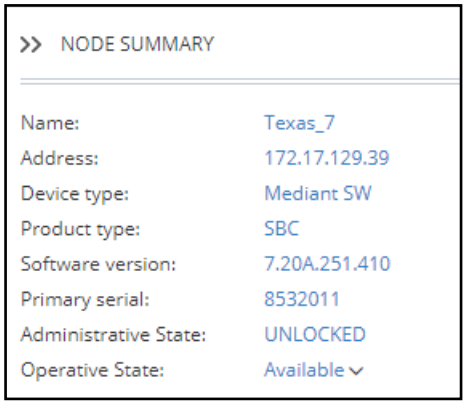


2. Use the following table as reference.

Table 2-4: Node Information

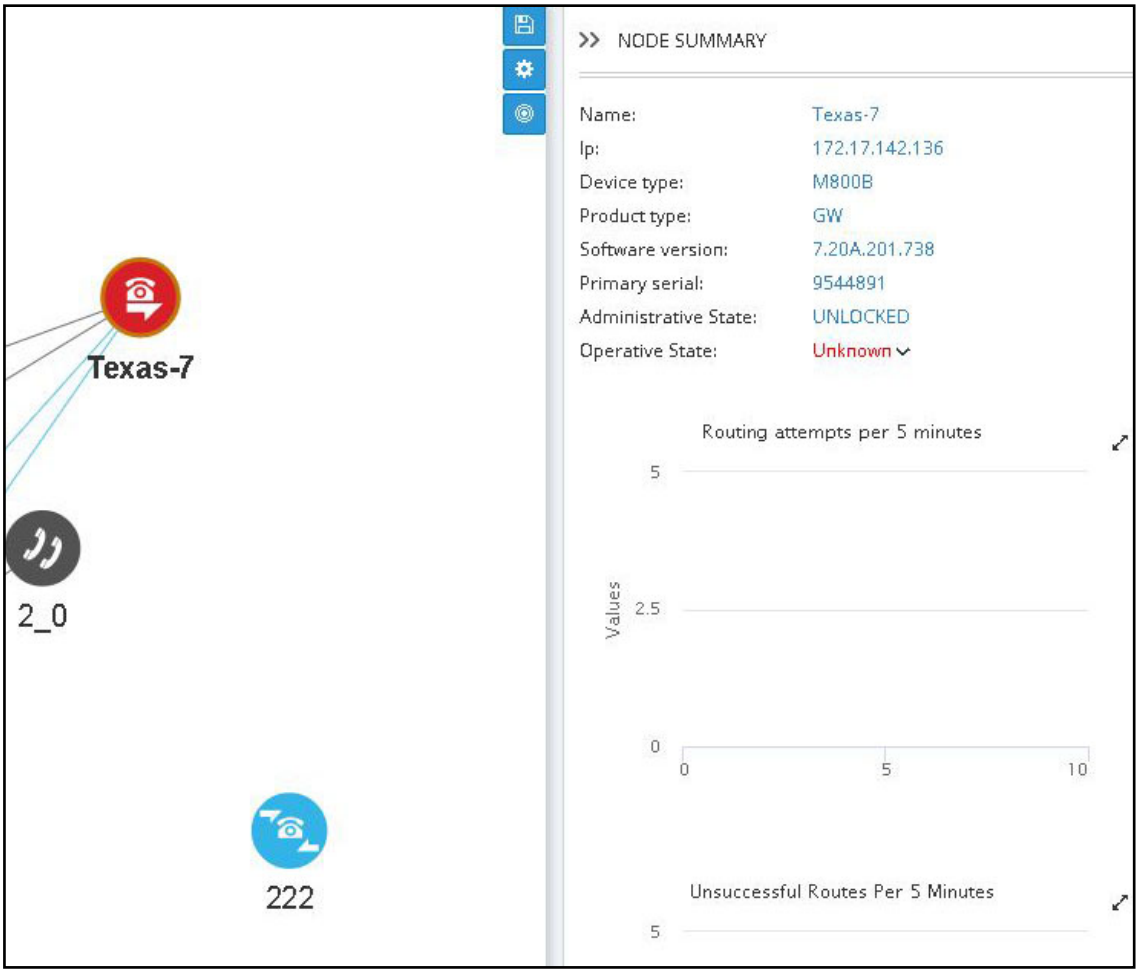
Item	Description
Name	The name of the Node
Address	The IP address of the Node
State	Available / Unavailable / Unrouteable / Logged out / Logging in. The ARM provides a robust node State Machine based on the node's connectivity to the ARM component. When determining a node's connectivity and ability to 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). 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.

Figure 2-6: Node Summary – Operative State



The example below shows a node's 'Unknown' state 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.

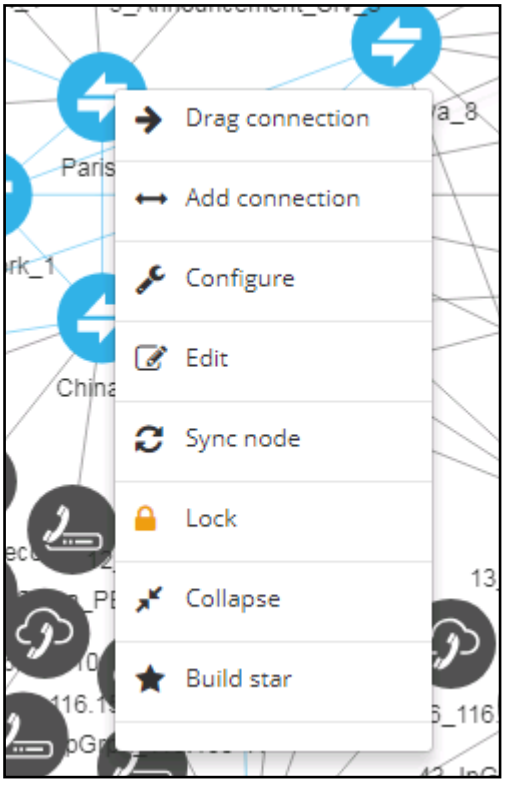
Figure 2-7: Node's 'Unknown' State



➢ **To perform an action on a node:**

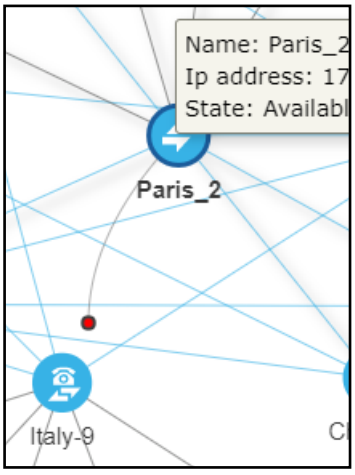
1. Right-click the node on which to perform an action.

Figure 2-8: Node Actions



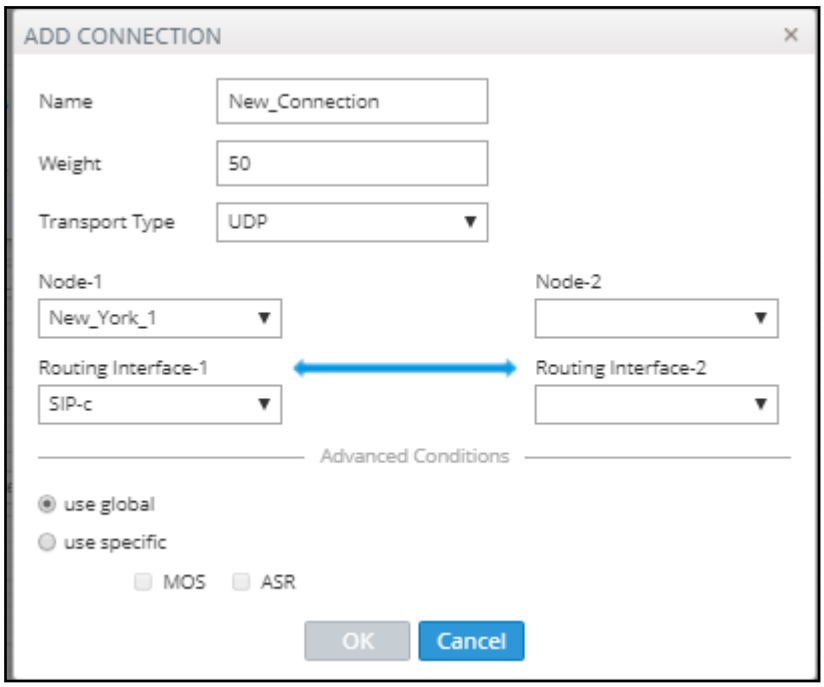
2. From the popup menu, choose:
   a. **Drag connection**. Allows you to draw (drag) a connection between two nodes In the ARM Map (**Paris_2** and **Italy-9** in the following figure, where **Paris_2** is the node you right-clicked and from where you begin dragging, and **Italy-9** is the node in which you end the drag).

Figure 2-9: Drag Connection



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

Figure 2-10: Add Connection

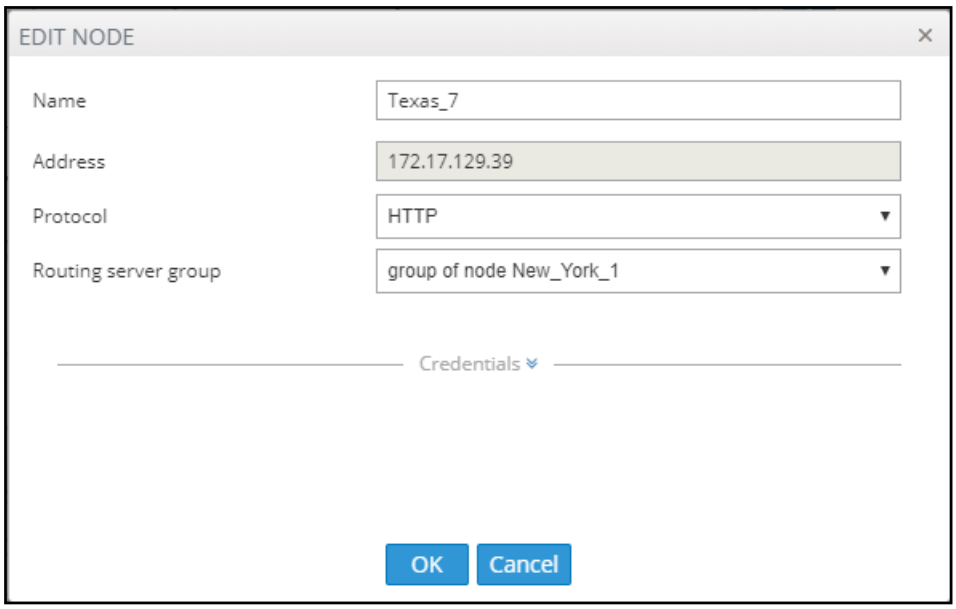


- Make sure the relevant SIP interface in the SBC is provisioned and configured as 'Used by routing server'
- In the Add Connection screen shown in the figure above, Node-1 will be configured (the node you initially selected). From the 'Node-2' drop-down menu, select the node *to which* to make the connection, and then click **OK**. See Adding an AudioCodes Node to the ARM on page 40 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 2-11: Edit Node



- 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 124.

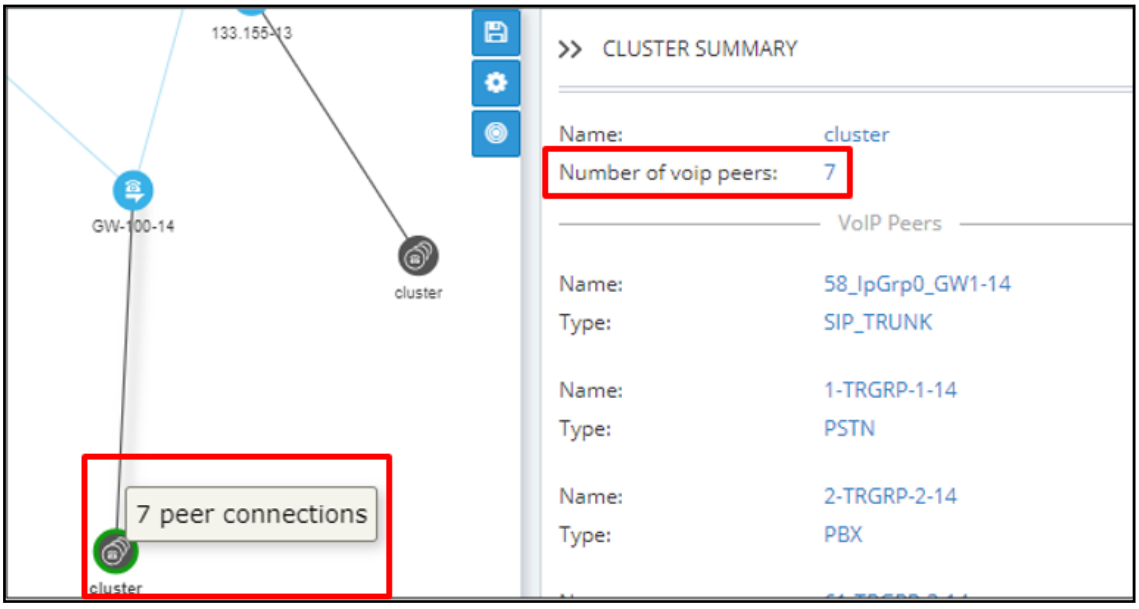
e. **Sync Node**

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 2-12: Collapsed VoIP Peers

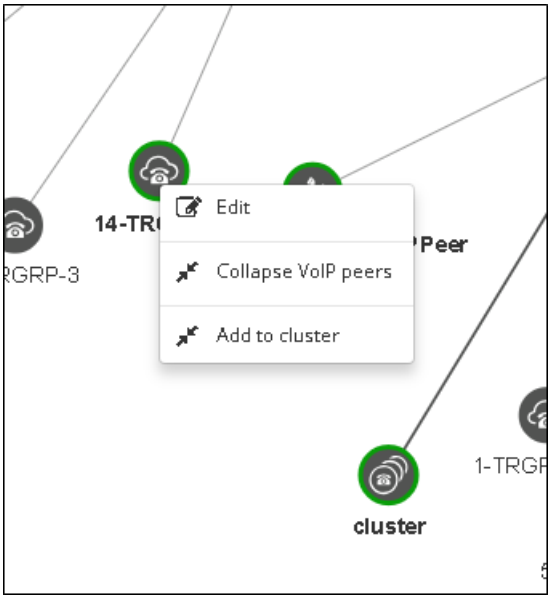


- [Refer to the preceding figure] The cluster's label in the Network Map *as well as* the Cluster Summary indicate the number of collapsed VoIP Peers / Peer Connections in the cluster.
- [Refer to the figure following] The Cluster Summary can also indicate the aggregated number of collapsed VoIP Peers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

Figure 2-13: Peer Connection Aggregation Summary: Number of Peer Connections

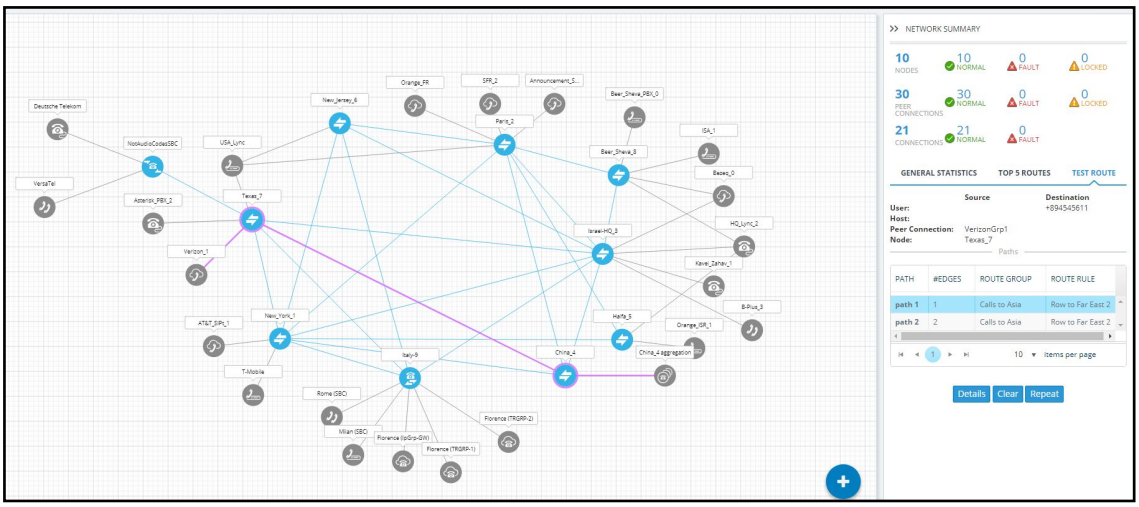
- **Add to cluster**. You can add an additional VoIP Peer or multiple VoIP Peers to an existing cluster: (1) Select the target cluster to which to add (2) press the **Ctrl** key click one or multiple VoIP Peers to add to the target cluster (3) right-click and from the pop-up menu select the action **Add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

Figure 2-14: Add to cluster



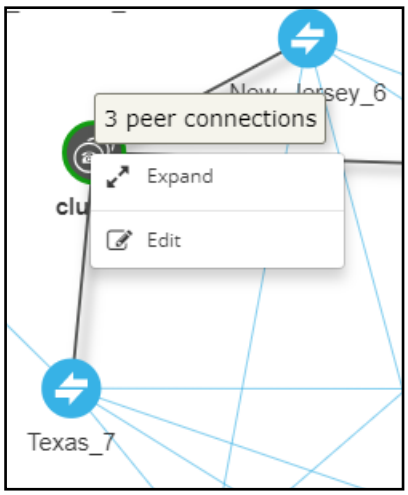
- VoIP Peers associated with more than one node are included in the collapsed cluster. If a test route is performed that terminates on a collapsed VoIP Peer, the VoIP Peer will not be expanded automatically and the path displayed in the GUI will terminate on the cluster icon.

Figure 2-15: Test Route Path Terminates on Collapsed VoIP Peer



h. 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 2-16: 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.

j. **Build Star** (Topology)

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 2-17: SIP Trunk

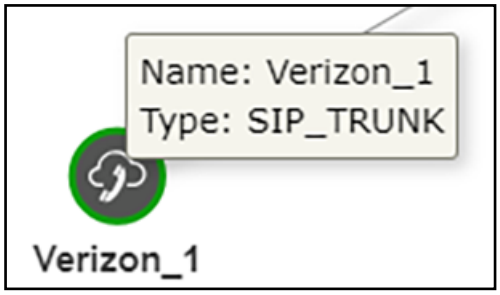


Figure 2-18: PBX | IP PBX

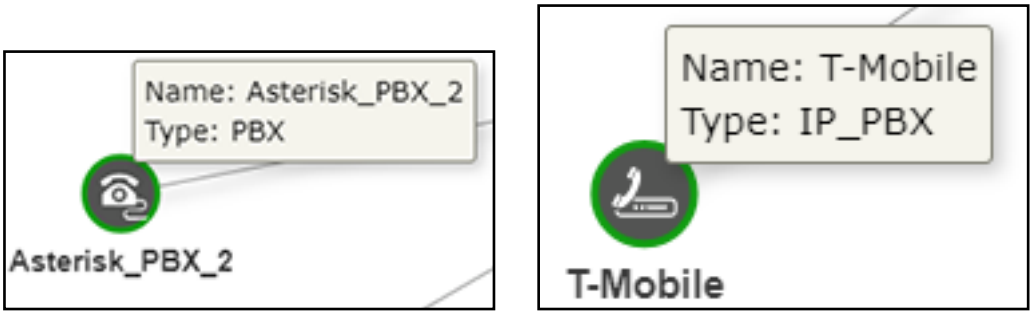


Figure 2-19: PSTN

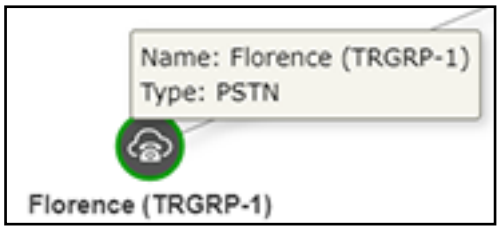
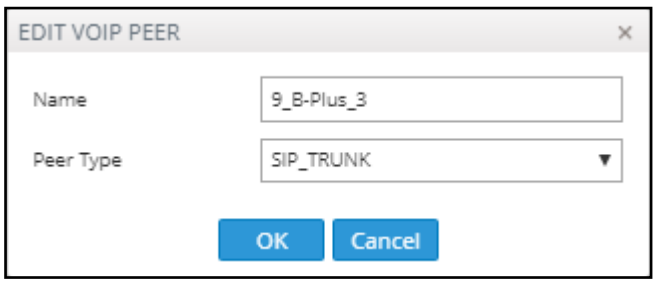


Figure 2-20: IP Phone

➢ **To edit a VoIP Peer:**

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

Figure 2-21: 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.

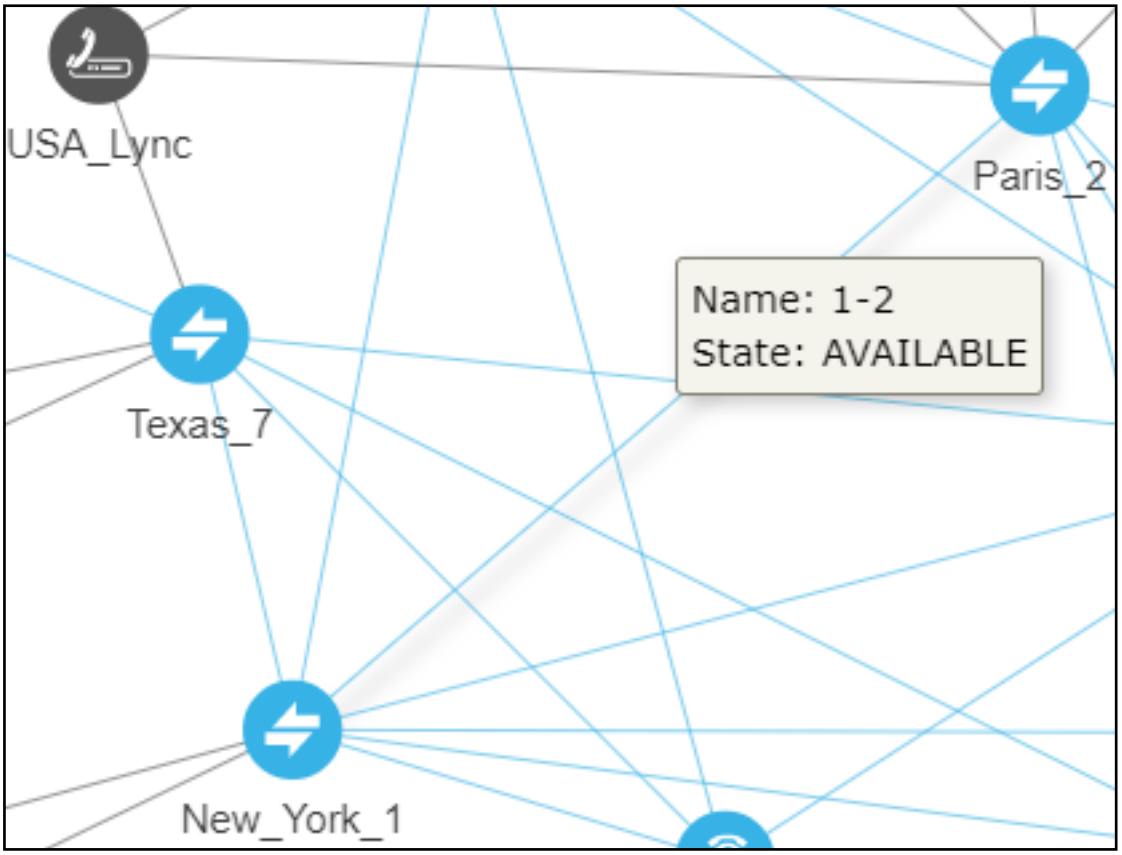
Connection Information and Actions

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 2-22: Connection Information

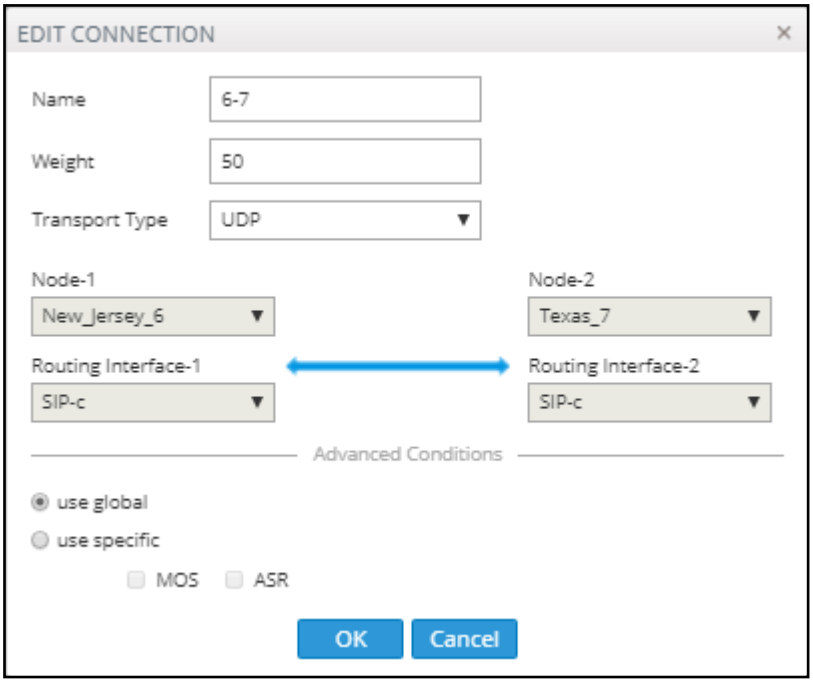


2. View the Name and the State of the connection.

➢ **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 2-23: Edit Connection



2. You can edit the:
   - name of the connection
   - Weight (Range: 0-100. Default: 50)
   - Transport Type (Default: UDP)
3. Leave the option **use global** at its default for quality-based routing to be applied using global (ARM level) settings. Select **use specific** 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 114 for related information).

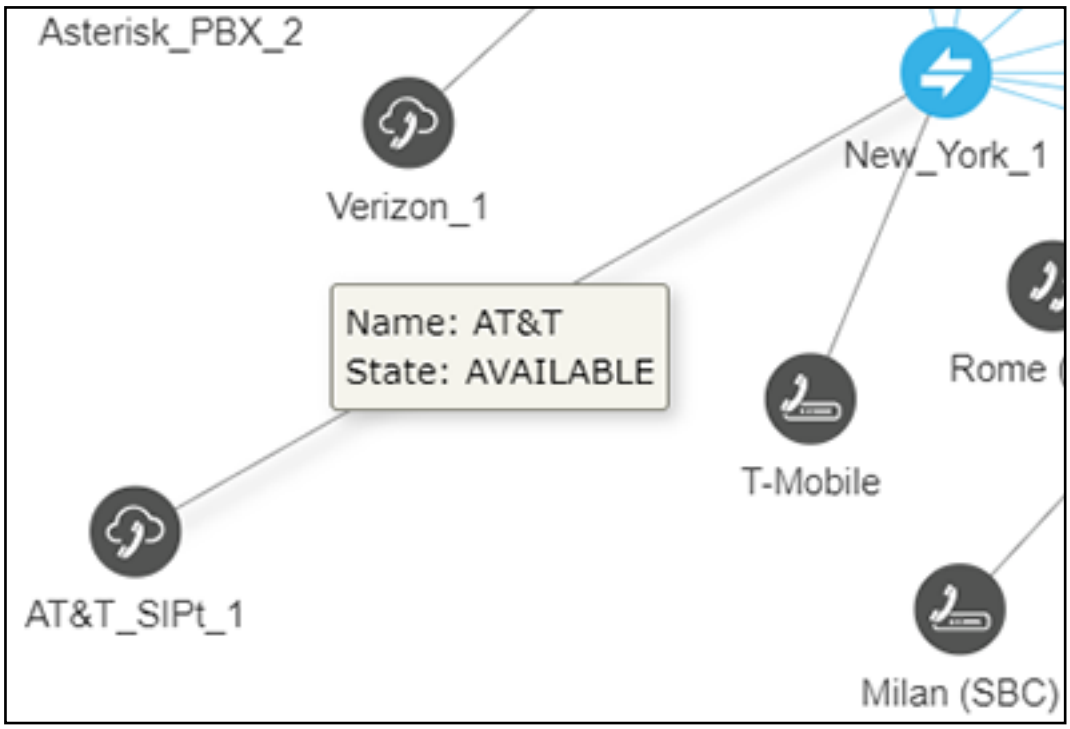
Peer Connection Information and Actions

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

➢ **To view peer connection information:**

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

Figure 2-24: Peer Connection Information

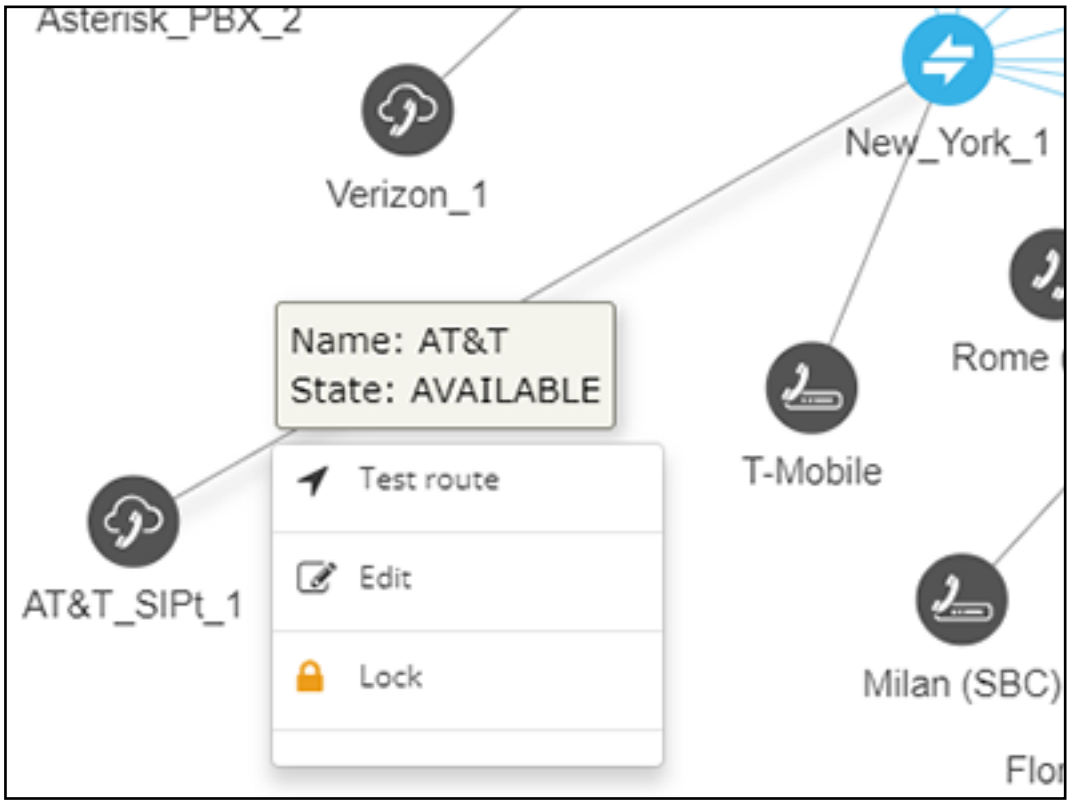


2. View the Peer Connection's Name and State.

➢ **To perform an action on a peer connection:**

1. Right-click the Peer Connection and choose **Test route** from the popup menu (see Testing a Route on page 47 for more information)

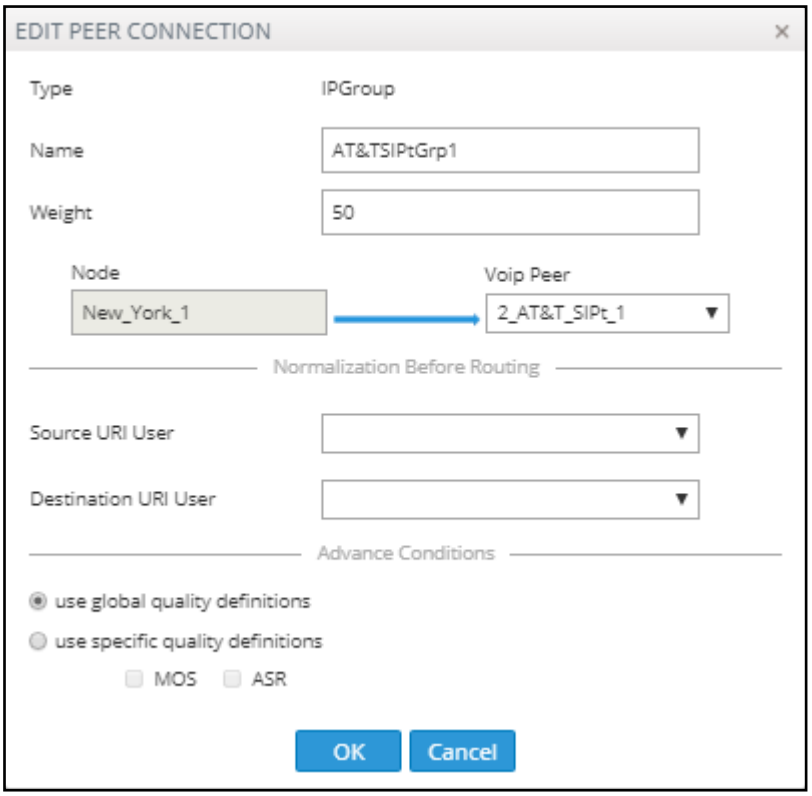
Figure 2-25: Peer Connection Actions



2. Choose **Edit** from the popup menu.

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

Figure 2-26: 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 103).

d. 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 114.
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 114.

3. **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.
4. 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.

Repositioning Elements in the Network Map Page

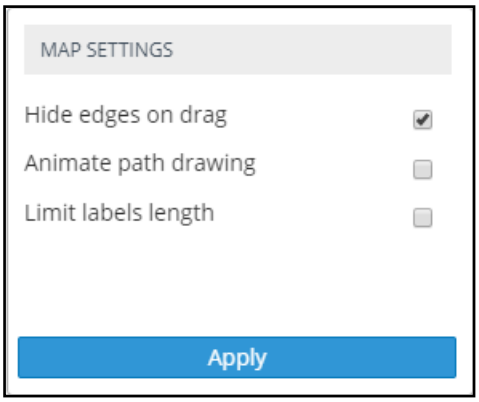
The ARM's Network Map page allows you to move and reposition multiple selected elements - Nodes and VoIP Peers – simultaneously to facilitate a friendlier operator experience and to decrease operator vulnerability to routing configuration errors.

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 2-27: 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** page > **Peer Connections**) you can view the Peer Connections.

Figure 2-28: Peer Connections

You can view the following information on each Peer Connection:

- Status
- Node
- Name
- VoIP Peer
- IP Group
- Operative State
- Administrative State
- Quality
- MOS
- ASR

The information displayed in the Network page's Peer Connection view is identical to that displayed in the Network Map view described under Peer Connection Information and Actions on page 30. You can search for the name of a Node associated with the Peer Connection, its name, or a VoIP Peer name. It's useful to find, for example, all Peer Connections of a specific Node.

You can perform the following actions:

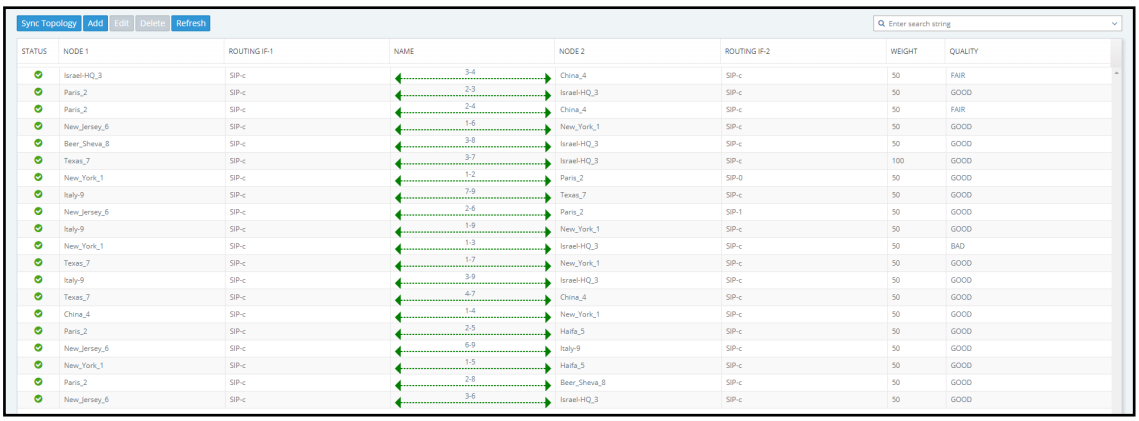
- Sync Topology
- Edit (after selecting the row of the Peer Connection to edit)
- Delete (after selecting the row of the Peer Connection to delete)
- Lock/Unlock (after selecting the row of the Peer Connection to lock/unlock)

Multiple rows can be selected; multiple actions (delete, lock/unlock, etc.) are supported. For more information about Sync Topology, see Synchronizing Topology on page 45. For more information about the Edit, Delete and Lock/Unlock actions, see under Peer Connection Information and Actions on page 30.

Connections Page Actions

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

Figure 2-29: Connections



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 29.

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 45. For more information about the Add, Edit and Delete Connection, see under Connection Information and Actions on page 29.

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

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 below.
- 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 39.

Overall Network Statistics

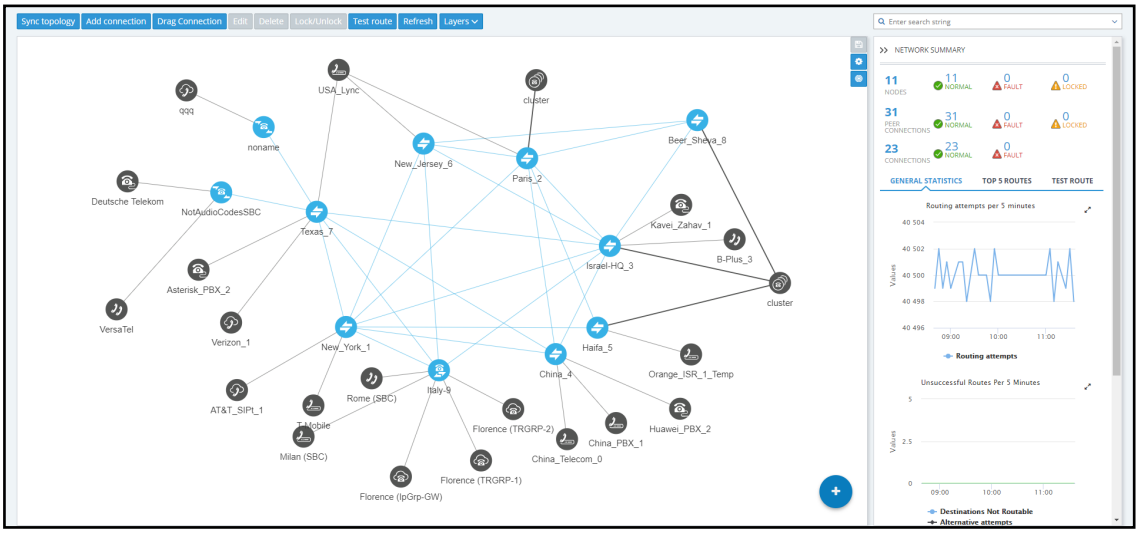
Statistics related to the entire network are by default displayed. No entity in the Network Map is selected. This pane displays four sections:

- Network Summary (see below)
- General Statistics (see General Statistics on the next page)
- Top 5 Routes (see Top 5 Routes Pane on page 37)
- Test Route (see Test Route on page 38)

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 2-30: 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 in the network that are unlocked and available, i.e., 'normal'

- The number of nodes//Peer Connections/Connections in the network that are 'fault', i.e., unavailable
- The number of nodes/Peer Connections in the network 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.

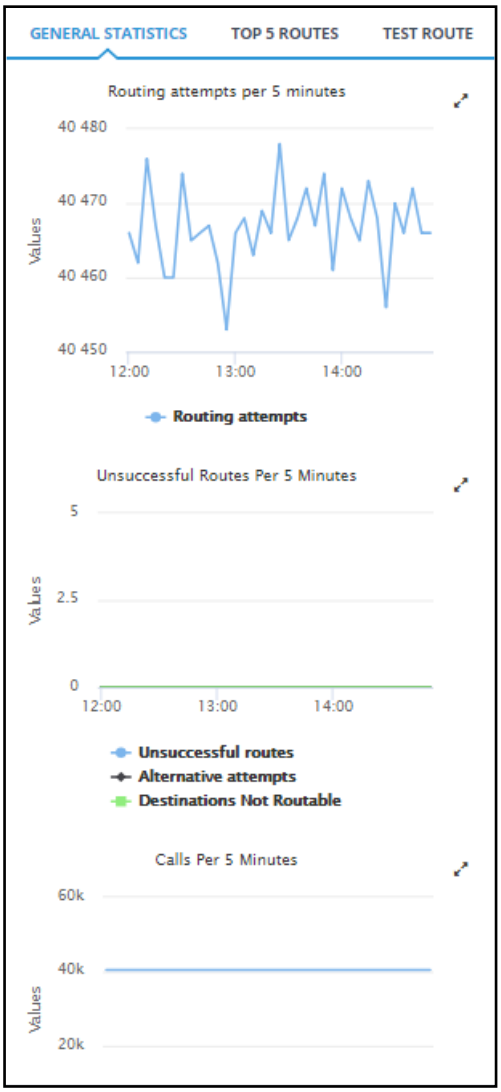
General Statistics

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 2-31: 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:**

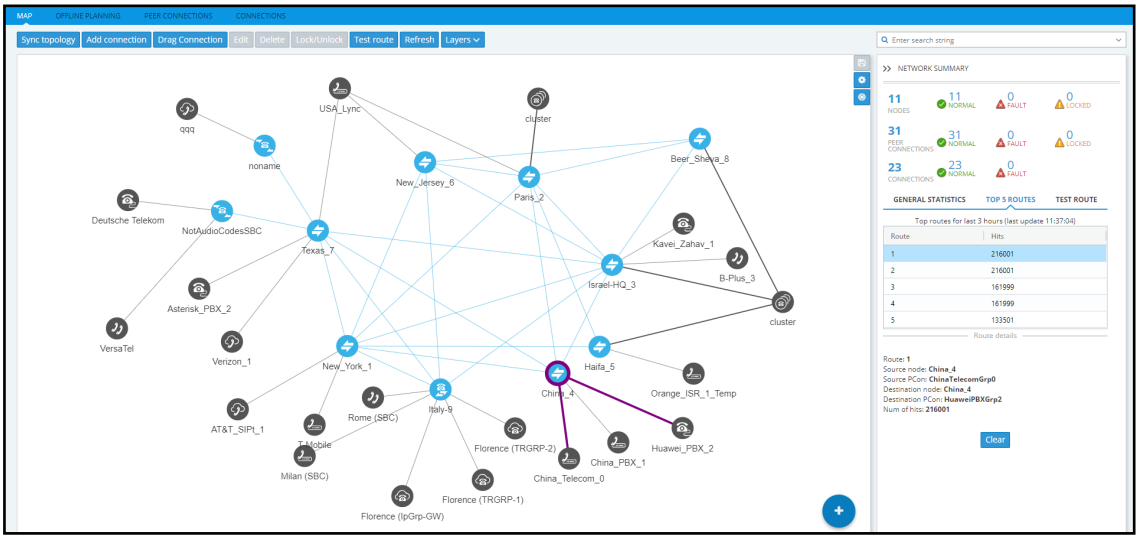
- Click the expand icon next to any of the three graphs to project a zoomed-in graph to the front.

Figure 2-32: Projecting a Zoomed-in Graph to the Front

Top 5 Routes Pane

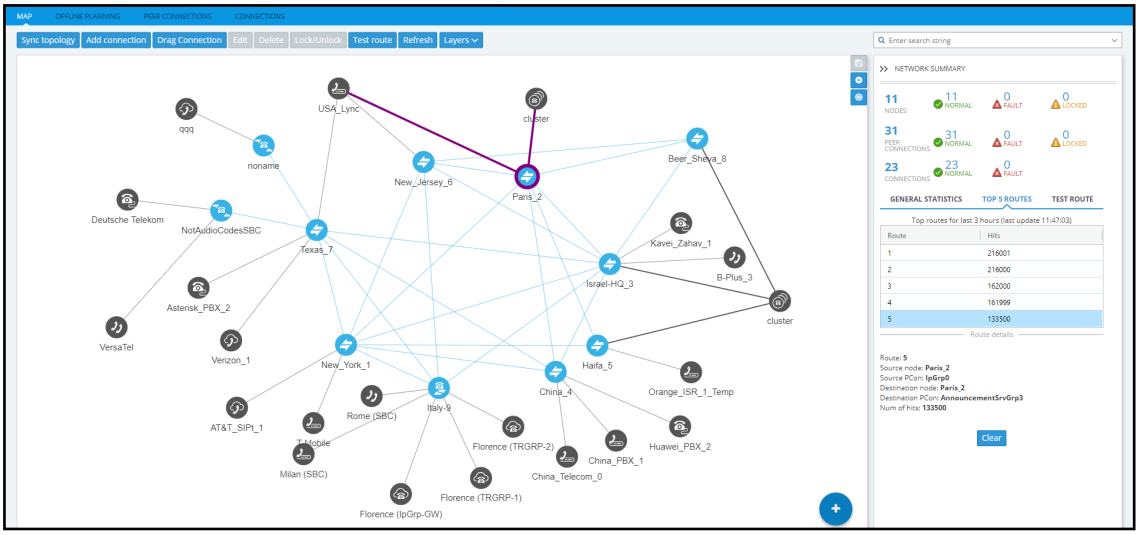
The Top 5 Routes pane under the **Top 5 Routes** tab in the Network Summary pane gives operators visibility into the routes most frequently used over the last three hours.

Figure 2-33: 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 2-34: 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.

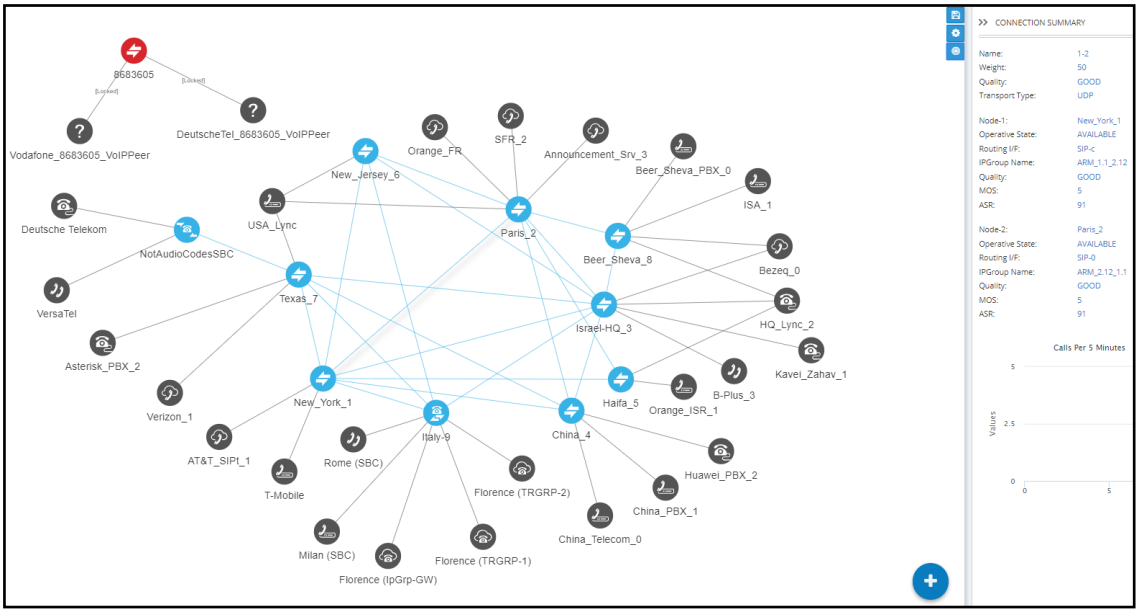
Test Route

See Testing a Route on page 47 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 2-35: Summary Pane Displaying Information Related to a Selected Entity - Connection



Note in the figure above that the entity selected, the connection between **Paris_2** and **New_York_1**, is shaded. Information on the selected entity 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.

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.

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.

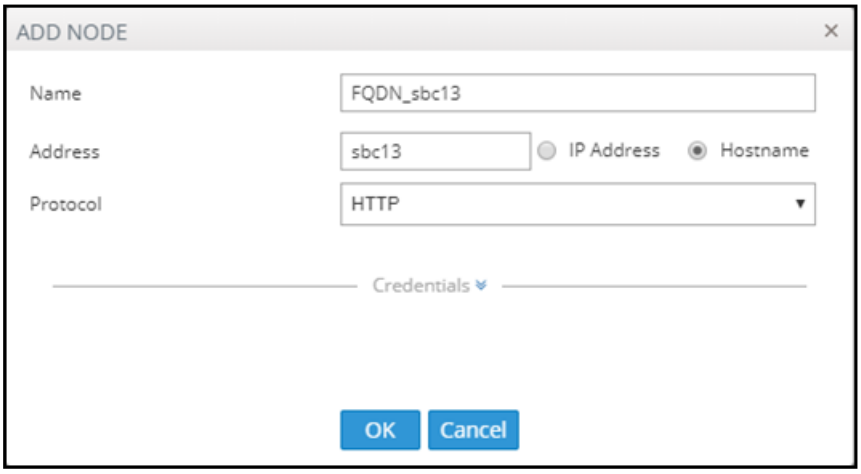
➢ **To manually add a node to the ARM:**

1. Click the icon and then drag and drop the AudioCodes node into the Network Map, as illustrated in the following figure. The icon changes to **x**.

Figure 3-1: Drag AC Node

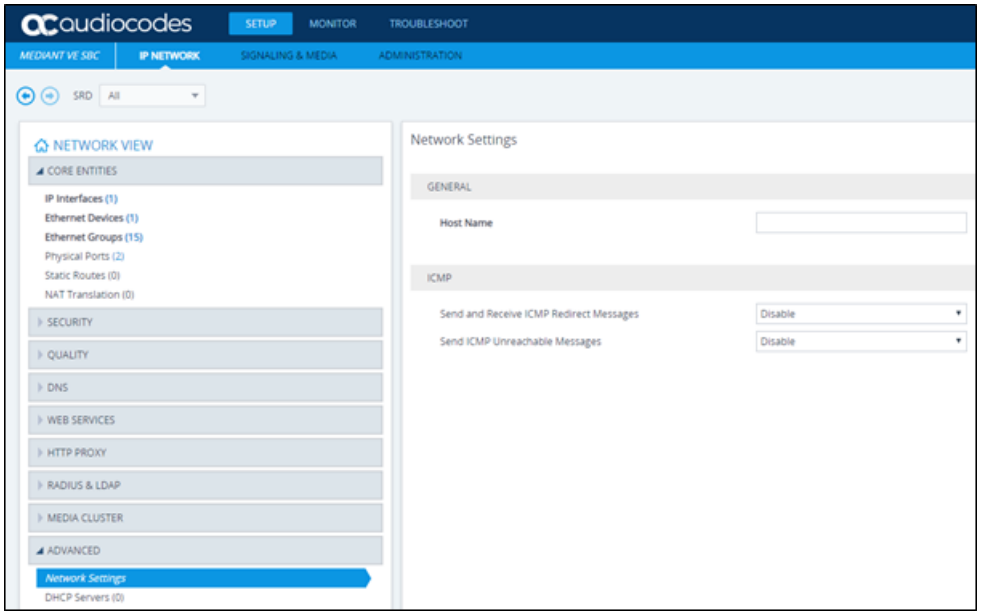
2. In the Add Node screen that opens shown in the figure following, provide a name, IP address or Hostname (FQDN), and protocol. The option to use Hostname (FQDN) rather than a hard-coded IP address gives you added flexibility when designing your telephony network.

Figure 3-2: Node Name | IP Address / Hostname (FQDN) | Protocol



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.

Figure 3-3: 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).

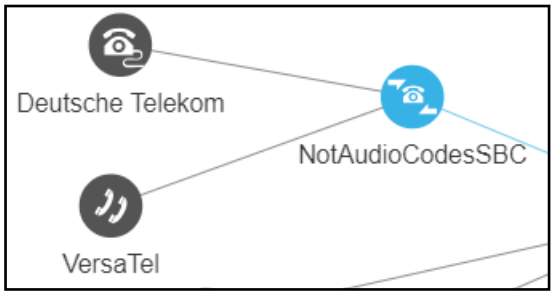
3. View the added AudioCodes node in the Topology Map; all elements associated with the node are automatically provisioned and displayed in the Network Map.

- 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 161.

Adding a Third-Party Node to the ARM

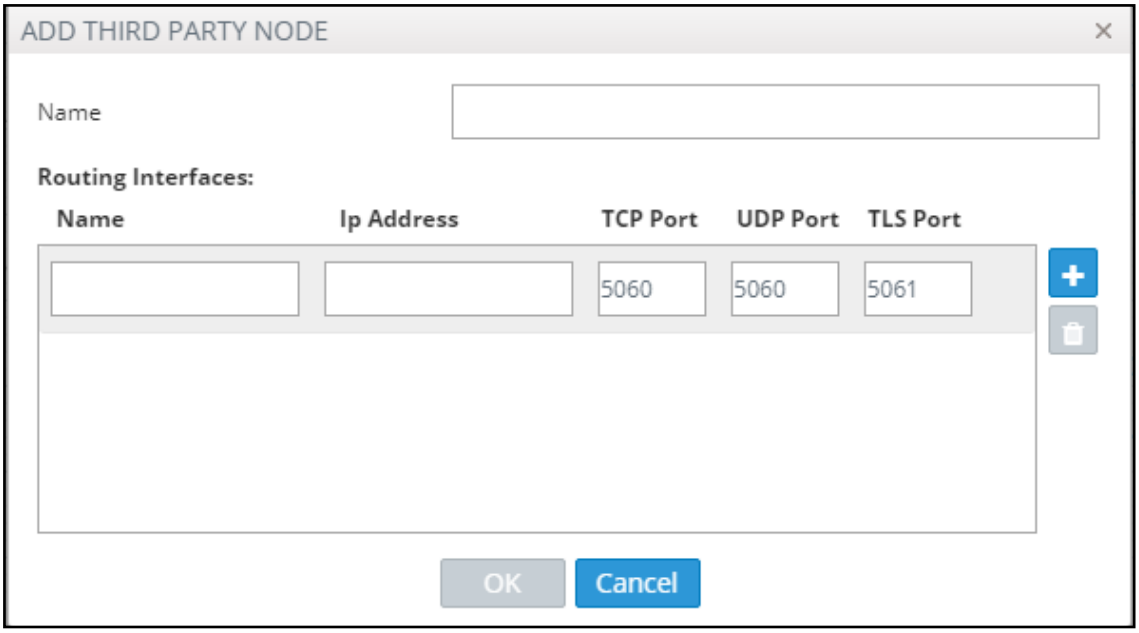
The ARM allows you to add third-party, non-AudioCodes nodes (SBCs and Media Gateways) to the Network Map so that the ARM can be used for call routing in heterogeneous environments with a mix of AudioCodes and non-AudioCodes nodes as part of your network.

Figure 3-4: Third-Party Device Added to the Network Map



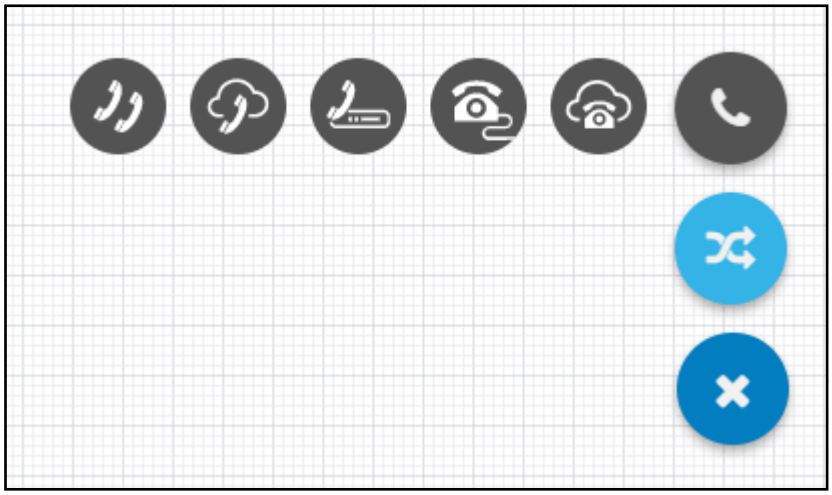
➢ **To add a third-party device:**

1. Click the  icon and then drag and drop the third-party node icon  into the Network Map.



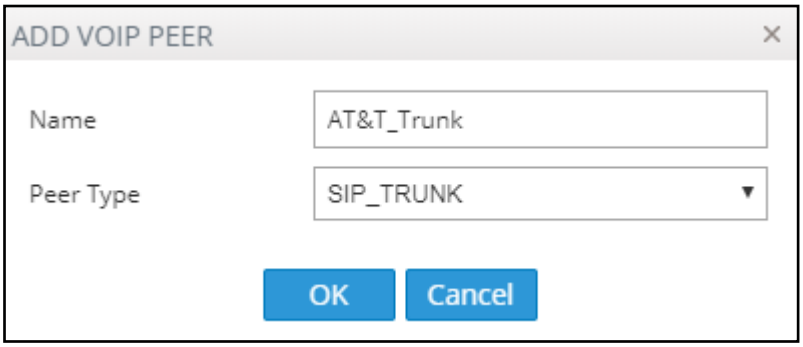
2. Provide the third-party device's properties. The third-party device's remote IP address is used as the destination address of the connection from the AudioCodes device.
3. Add a VoIP Peer per type, e.g., SIP trunk or PBX, and attach it to the third-party node by dragging and dropping it from the 'add voippeer' menu.

Figure 3-5: Adding a VoIP Peer



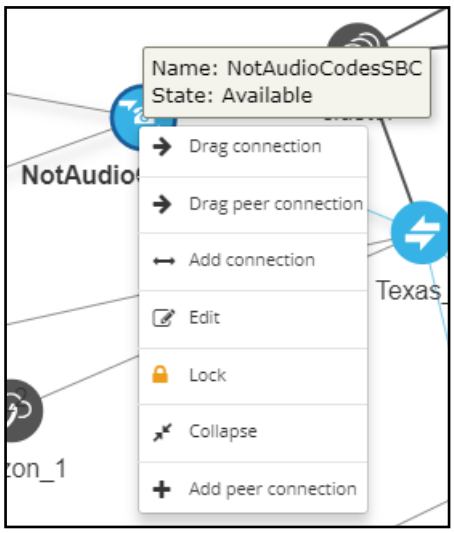
4. In the 'Add VoIP Peer' screen, give the VoIP Peer a name.

Figure 3-6: Adding a VoIP Peer – Giving the VoIP Peer a Name



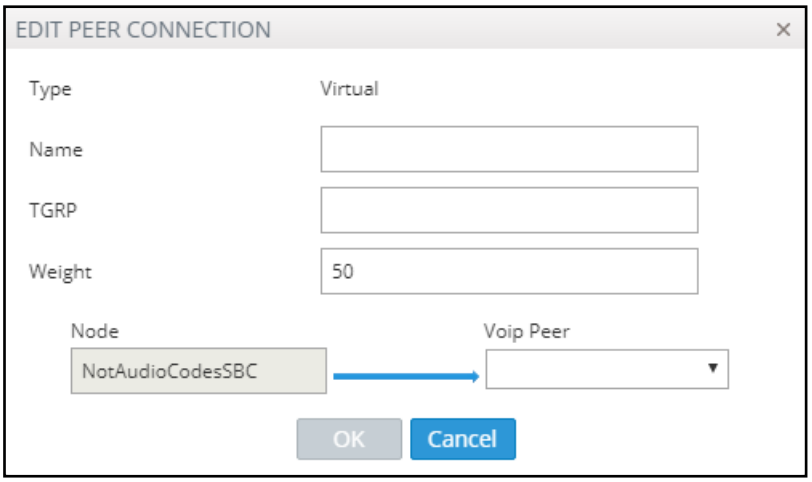
5. Associate the VoIP Peer with the third-party node using a Peer Connection, by drawing a line between the VoIP Peer and the third-party node by right-clicking the node and selecting the action **Add Peer Connection**.

Figure 3-7: Add Peer Connection



The action Add Peer Connection is available only to third-party, non-AudioCodes SBCs or Media Gateways. It's not applicable to AudioCodes SBCs or Media Gateways.

Figure 3-8: Edit Peer Connection



6. You need to connect the third-party device 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 performs routing to Peer Connections attached to third-party devices. In the Routing Rules definition, choose the Peer Connection or VoIP Peer associated with the third-party device and in this way, achieve end-to-end routing in a heterogeneous network.

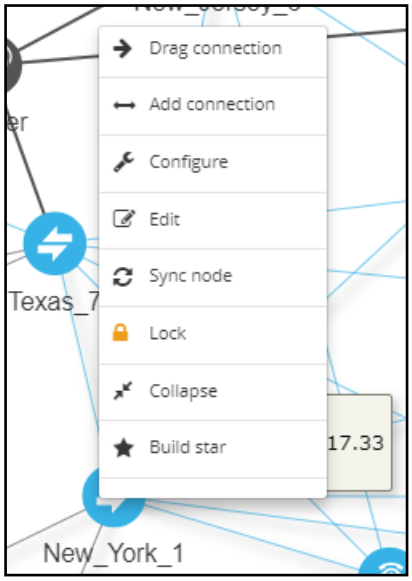
Adding Connections

You can configure a connection between two nodes.

➢ **To add a connection:**

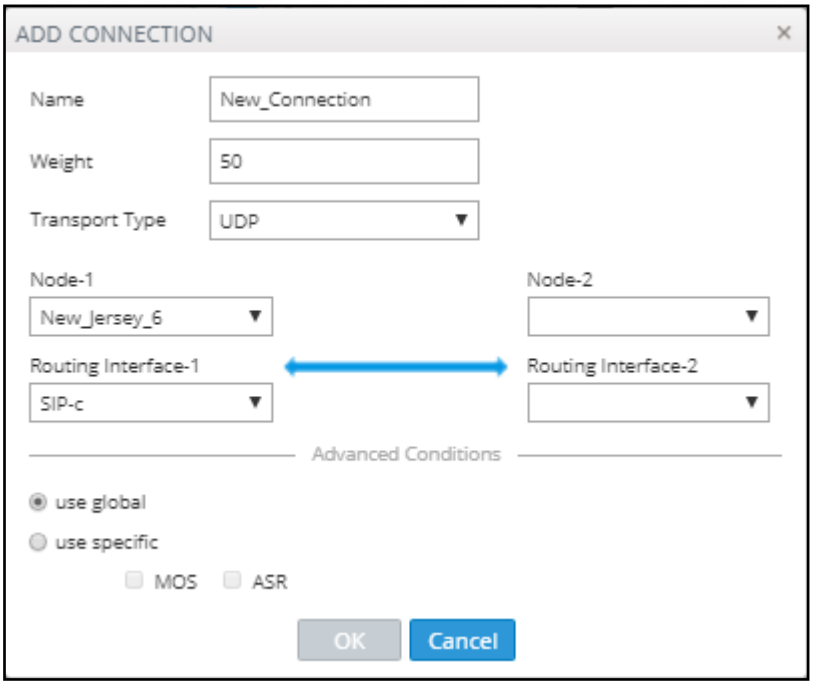
1. In the Network Map view, right-click the node from which to configure the connection and in the popup menu click **Add Connection**.

Figure 3-9: 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 3-10: Add Connection



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. To define Advanced Conditions (quality-based routing), see Routing Settings on page 114.
8. 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.

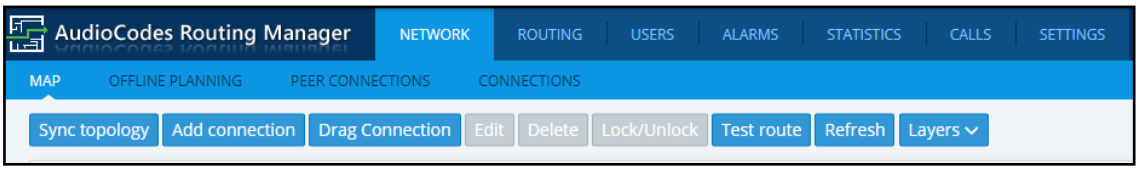
The ARM detects activity originating from a node and puts the node on the map (peer collection). The ARM recognizes a newly added node and extracts all IP groups (i.e., Peer Connections). Users must add connections between nodes and change the VoIP peer types (see under Adding Connections on the previous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

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 3-11: Sync Topology



Global synchronization of the entire network is performed.

Building a Star Topology

You can build a star topology to enhance effective management. In a star topology, every node selected is connected to a central node:

All VoIP traffic from/to connected star nodes passes through the central node.

➢ **To build a star topology:**

1. In the Network Map view, right-click a node and in the popup menu select **Build star**.

Figure 3-12: Build Star

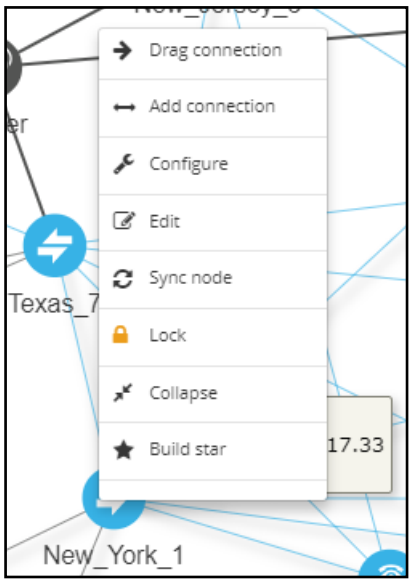
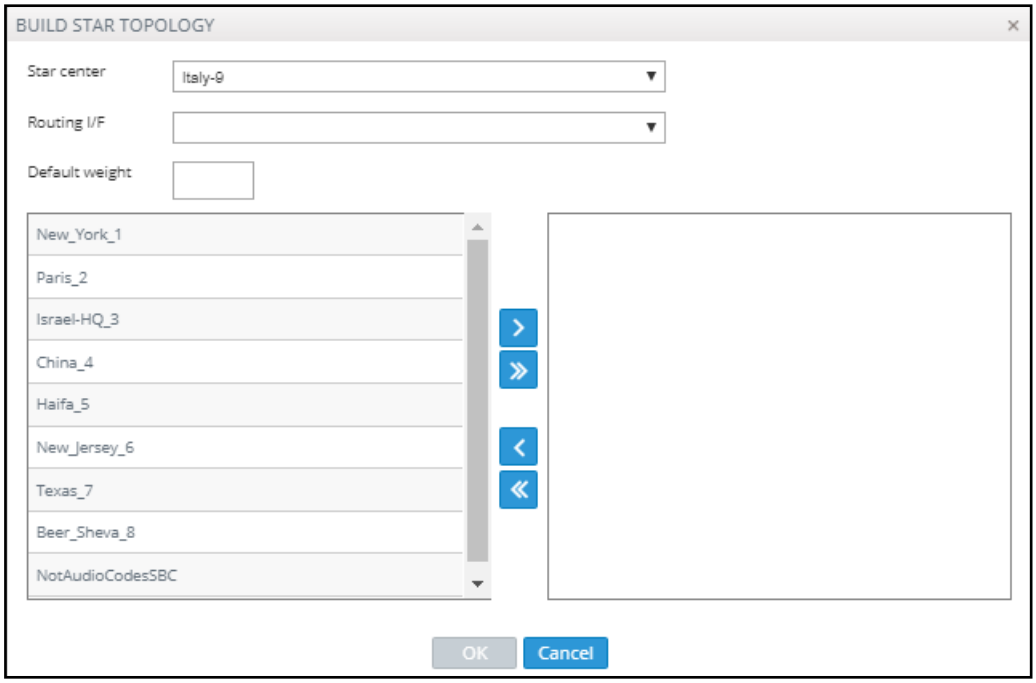


Figure 3-13: Build Star Topology



2. In the left pane of the Build Star Topology screen select the nodes that you want to connect to the star and then click >
3. Configure the screen using the following table as reference.

Table 3-1: Build Star Topology

Parameter	Description
Star center	The node you pointed your cursor to before selecting the 'Build Star' menu option is displayed in the field; it'll be at the center of the star. To select another node to be at the center of the star instead of this node, from the drop-down menu of nodes select the node.
Routing I/F	Select one of the SIP interfaces from which connections will be made from this node in the star center, to the other nodes in the star.

Parameter	Description
	Example: ■ SIP-c ■ SIP-0 ■ SIP-1 ■ SIP-2
Default weight	Enter the weight 1-100 to be applied to *all connections* in the star topology build. Later, you can prioritize *per connection* (see under Connection Information and Actions on page 29 for more information). The ARM uses this setting to select the most optimal routing path for each call. The parameter therefore facilitates more effective network management.
The builder panes	Use the builder panes to build your topology star. From the left pane, select the nodes to include in the star, and then click >> to move them to the right pane. If you select a single node at a time, select it and then click >. To remove a node from the build, in the right pane click <, or << to remove multiple modes after selecting them.

4. Click **OK**; the topology is built. You can view it in Topology Map view.

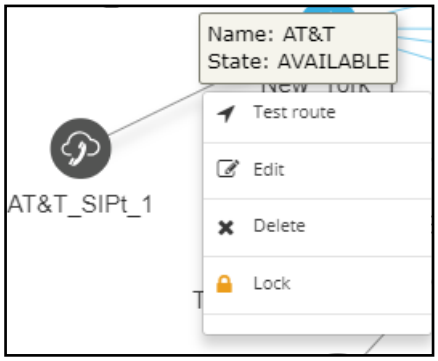
Testing a Route

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:**

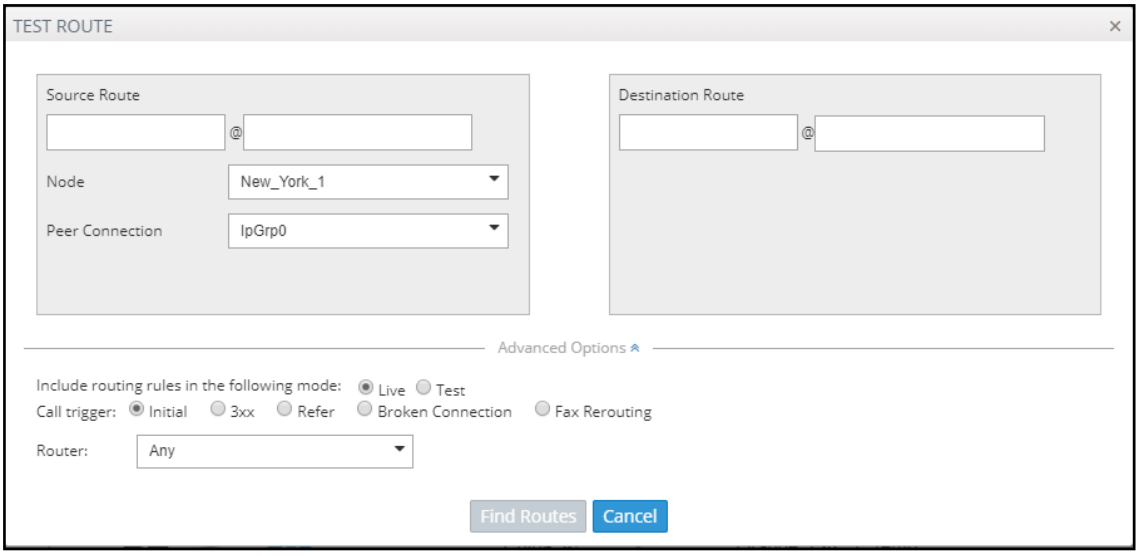
1. In the Network Map view, right-click the connection between a node and a VoIP Peer (Peer Connection). [Alternatively, you can select the connection and then click the **Test Route** button on the Actions Bar].

Figure 3-14: Test Route



2. From the popup menu, select **Test route**.

Figure 3-15: Test Route

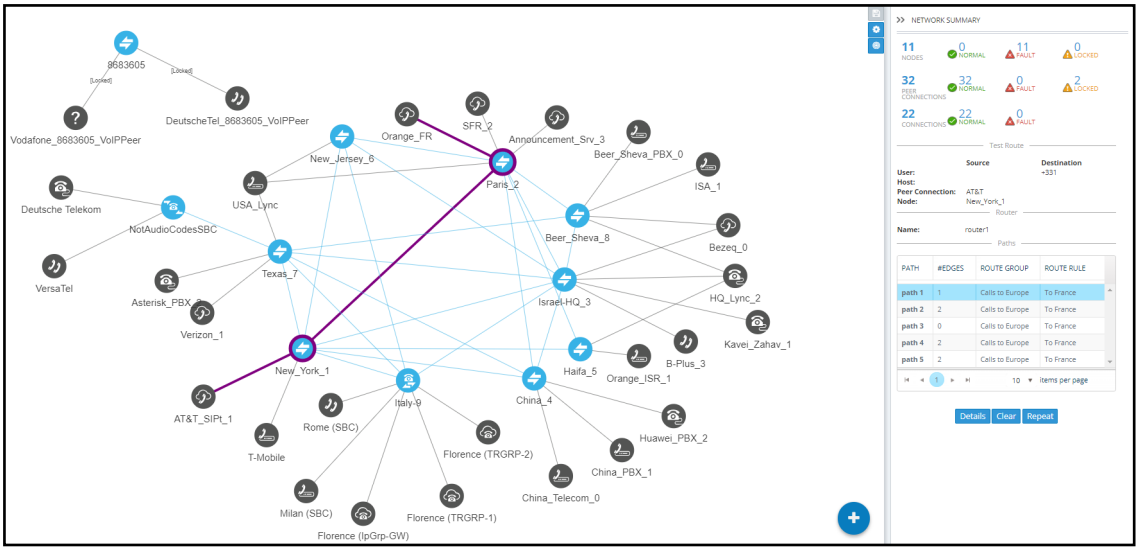


3. [Optional] Enter the Source and Destination Route. From the drop-down menu, select the **Peer Connection**.
4. Under 'Advanced Options', select the routing rules mode:
   - **Live**. When a new call destination is calculated, the Routing Rule is taken into consideration and live traffic may be impacted.
   - **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 133).
5. 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 133 for more information about call triggers.
6. 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.

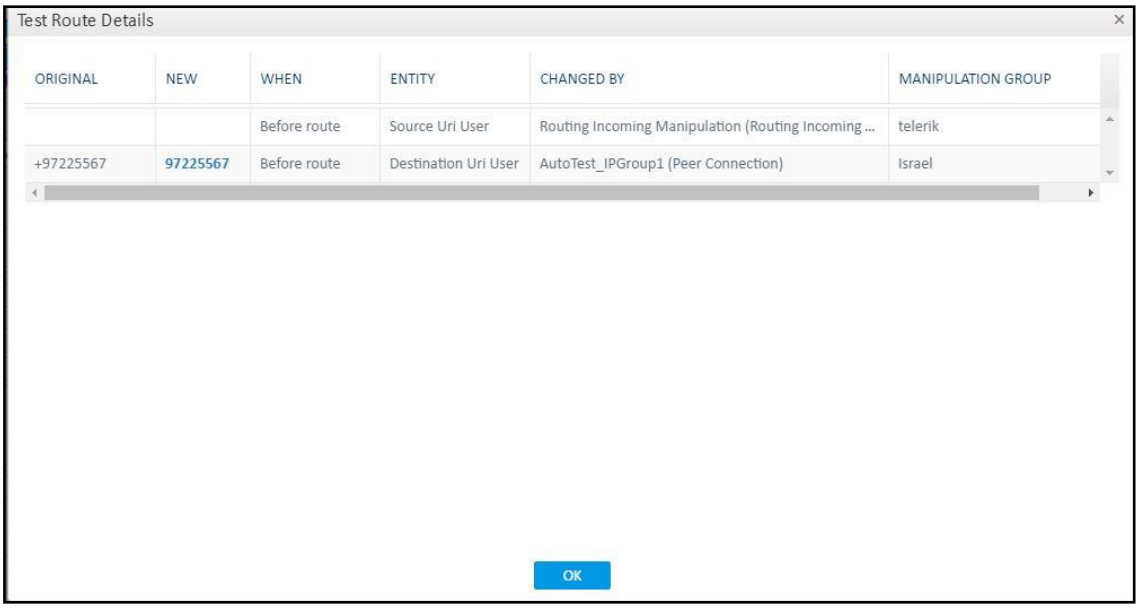
   Use this feature for debugging and locating potential issues.
7. Click **Find Routes**. Test routing is performed *as if* a real call is occurring, taking Operative State and Admin State of topology entities (Connections, nodes, Peer Connections), and the Admin State of routing rules, into account. In 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 3-16: Test Route Paths



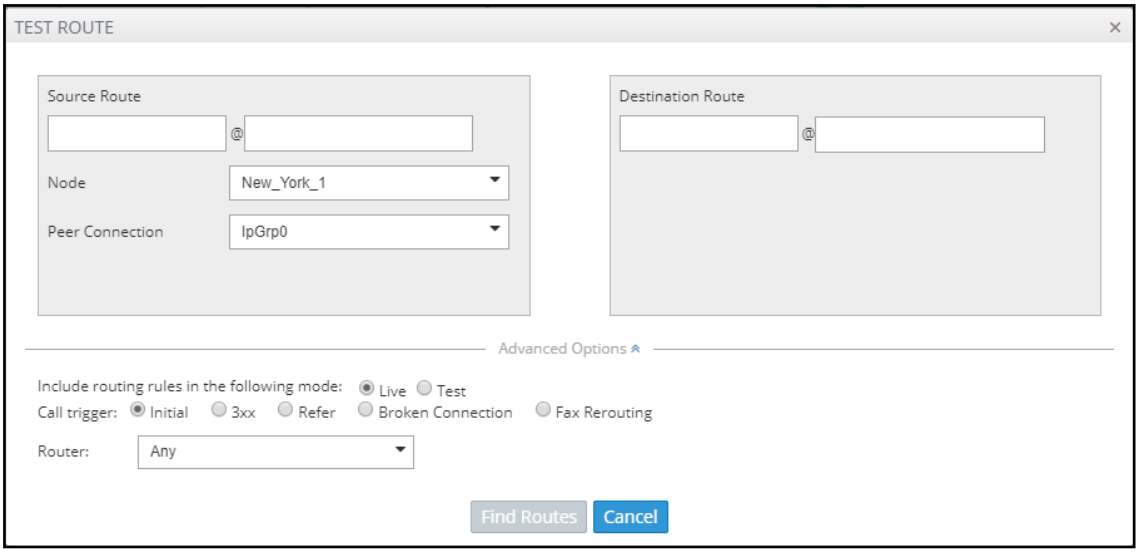
8. In the Test Route pane shown in the preceding figure, click the **Details** button.

Figure 3-17: Test Route Details



9. In the example above:
   - Compare the column ORIGINAL to the column NEW; the number changed because of a normalization rule that was applied. The normalization rule was configured in the Normalization Group rules attached to the Peer Connection.
     For related information, see also under Peer Connections Page Actions on page 33 and Examples of Normalization Rules on page 179.

Figure 3-18: Strip + from the Number



- Column WHEN indicates when manipulation was performed, i.e., *before* or *after* routing. In the example above, manipulation was performed *before routing*.
- 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
- Column CHANGED BY – the first row indicates by global Normalization Group – see under Adding a Normalization Group on page 103 and Normalization Before Routing on page 107 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 30 for detailed information.
- Column NORMALIZATION/MANIPULATION GROUP indicates which 'Manipulation Group' the entity passed through, according to which regular expression the entity was changed.

- 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.

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.

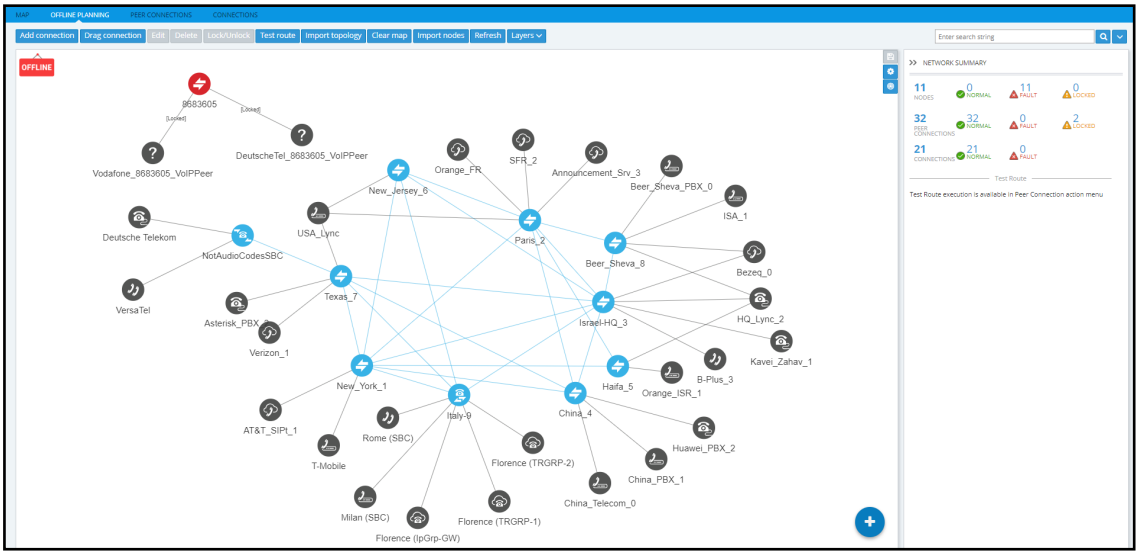
Operators can alternatively import an existing live topology into the page, make changes to entities' configuration and statuses, and test how the changes impact network functionality.

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.

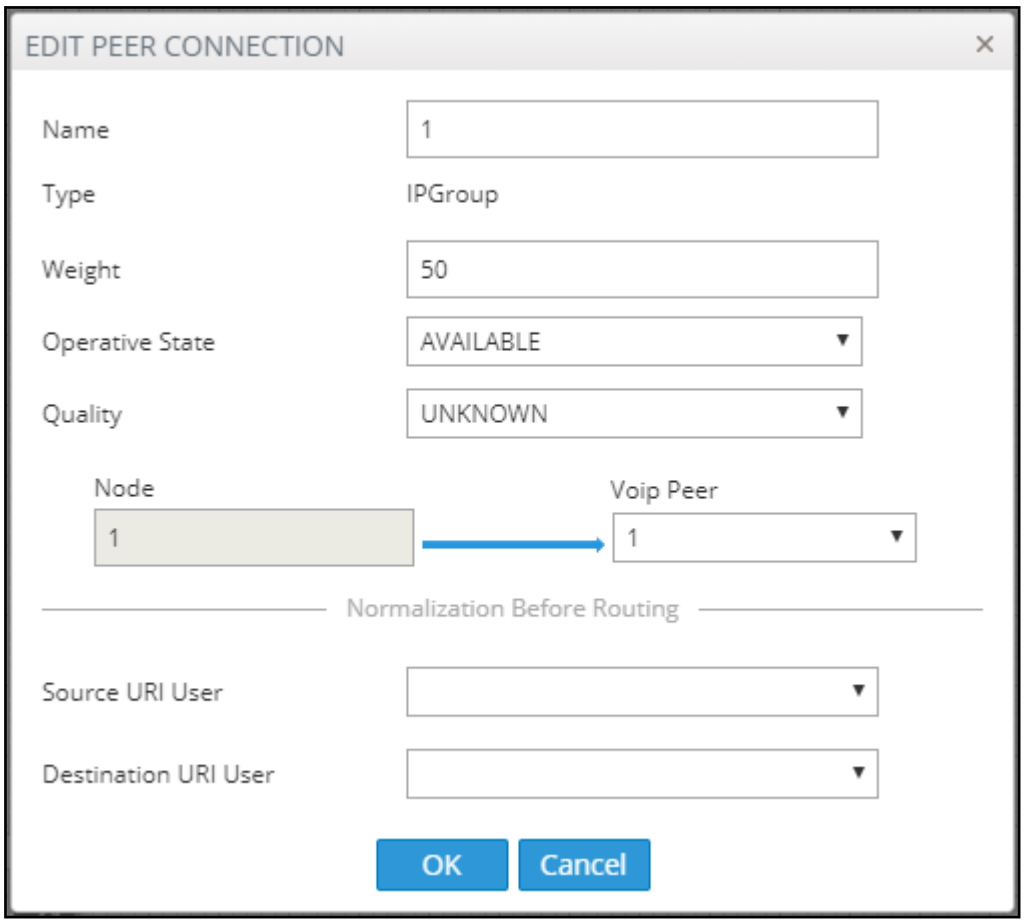
The operator can 'play' with the Administrative State, Operative State, Quality and Weight - if available - of each virtual entity and test how the changes impact call traffic.

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 *hybrid* device onto the Offline Planning page.
	Drag and drop a virtual *gateway* onto the Offline Planning page.
	Drag and drop a virtual *SBC* 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 *PSTN entity* onto the Offline Planning page.
	Drag and drop a *PBX* onto the Offline Planning page.
	Drag and drop an *IP PBX* onto the Offline Planning page.
	Drag and drop a *SIP Trunk* onto the Offline Planning page.
	Drag and drop an *IP phone* onto the Offline Planning page.

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

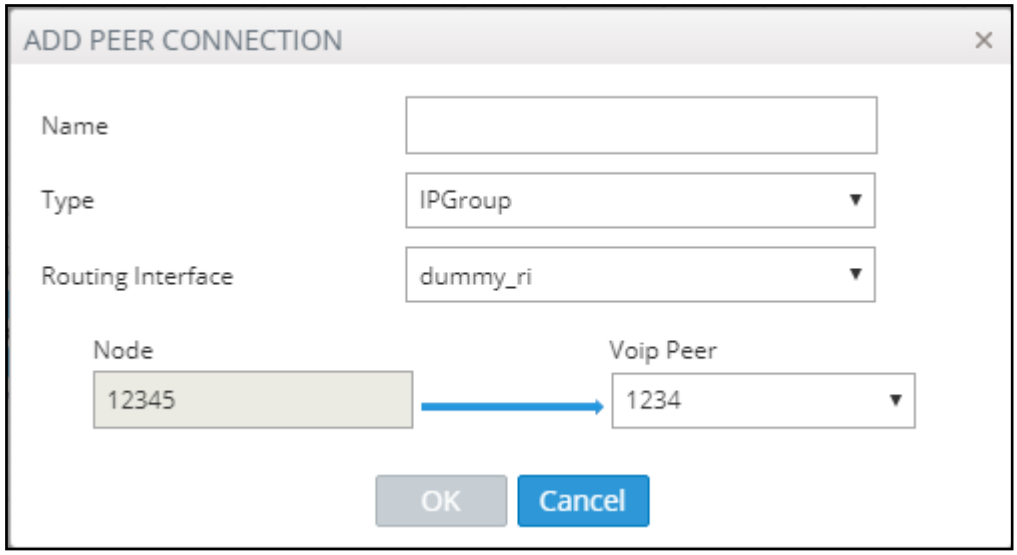
Adding a Virtual Peer Connection to the Offline Planning Page

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

➢ **To add a virtual Peer Connection:**

- Drag a line from the center of a node to a VoIP Peer and then configure it in the Add Peer Connection screen that opens:

Figure 4-3: Add Peer Connection



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 44 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 47). 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

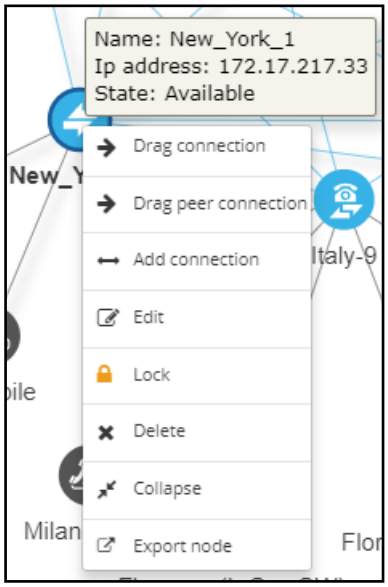
You can export a node from the Offline Planning page to the live topology.

➢ **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



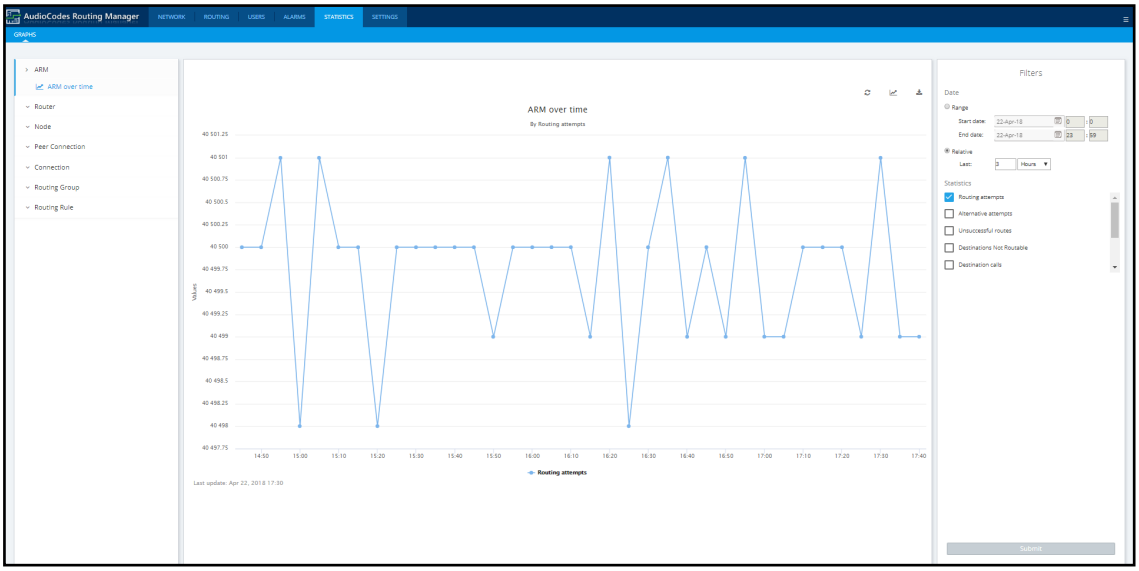
5 Viewing Statistics and Reports

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



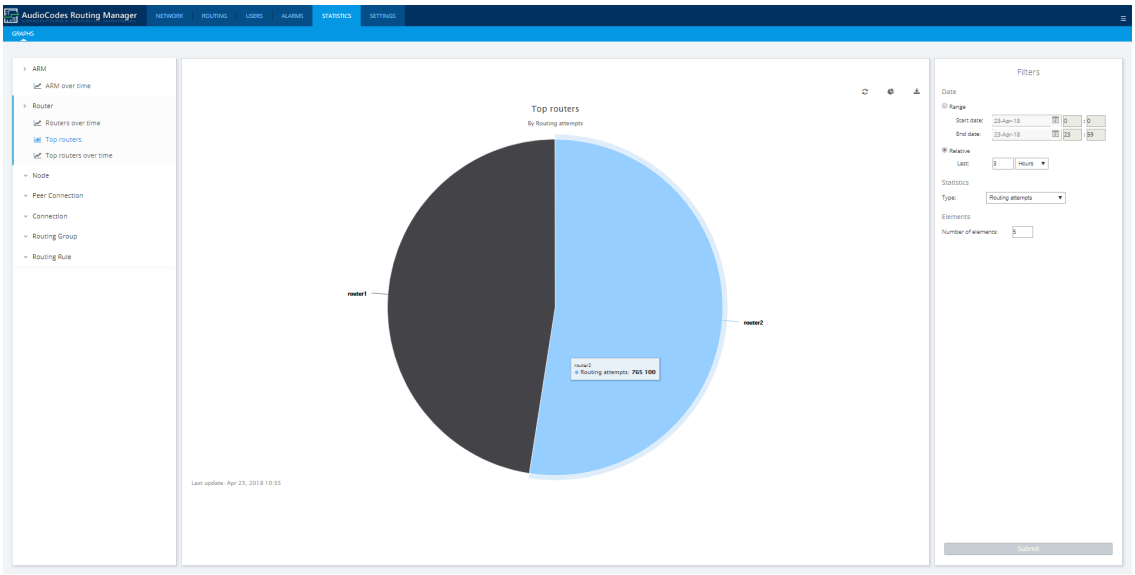
The page is divided into three sections.

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

Element	Filters	Graphical Representation
Statistics are displayed *per element*. Select either: ■ ARM ■ 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 over time, Top peer connections, Top peer connections over time) ■ Connection (Connections over time, Top connections, Top connections over time)	Filters differ depending on the element selected. *For all elements except Routing Group and Routing Rule, select from*: ■ 'Date' ('Range' or 'Relative') ■ Statistics Type: ✔ Routing attempts ✔ Alternative attempts ✔ Unsuccessful routes ✔ Destinations Not Routable ✔ Destination calls	Graphic representation of the statistics of the selected element in a chart, with a range of graph functionalities: ■ Refresh ■ Chart type (line, area or stacked area) Export chart

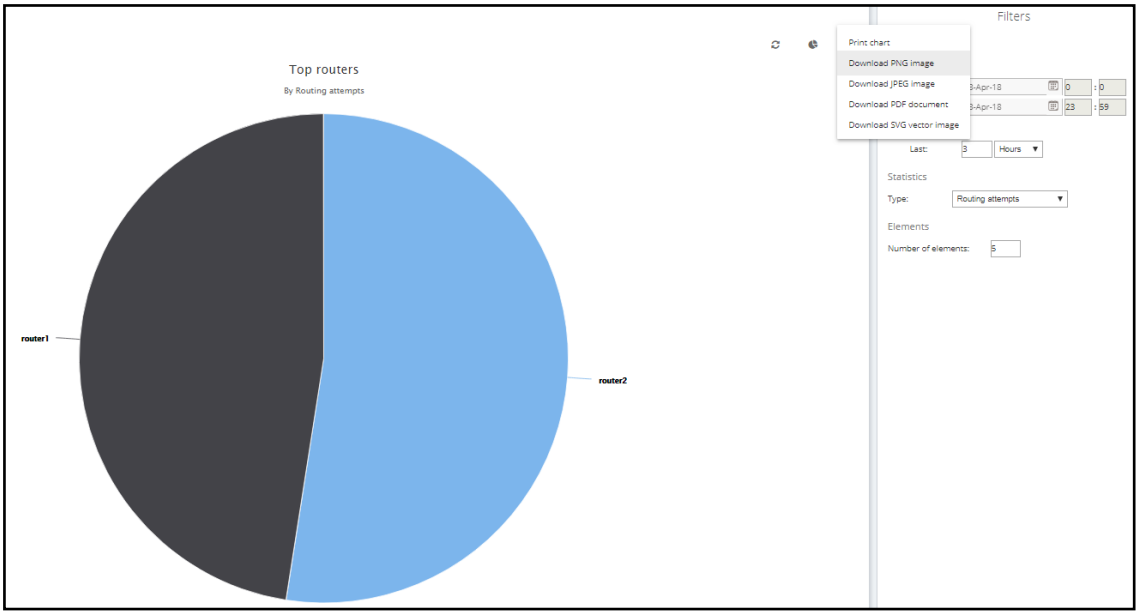
Element	Filters	Graphical Representation
■ Routing Group (Routing groups over time, Top routing groups, Top routing groups over time, Top routing groups by rules, Top routing groups by rules) ■ Routing Rule (Routing rules over time, Top routing rules, Top routing rules over time, Routing rules by actions, Top routing rules by actions)	✔ Transient calls (does not apply to Peer Connection) (for Connection, only this filter applies) ✔ Drop routing request ✔ No match rule ■ Elements ✔ Search ✔ Number ■ Stacked Elements ✔ Search ✔ Number ■ Statistics Type (only applies to Routing Group and Routing Rule) ✔ Routing rules attempts ✔ Routing first match ✔ Routing second match ✔ Routing third match ✔ Routing rules failures	

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



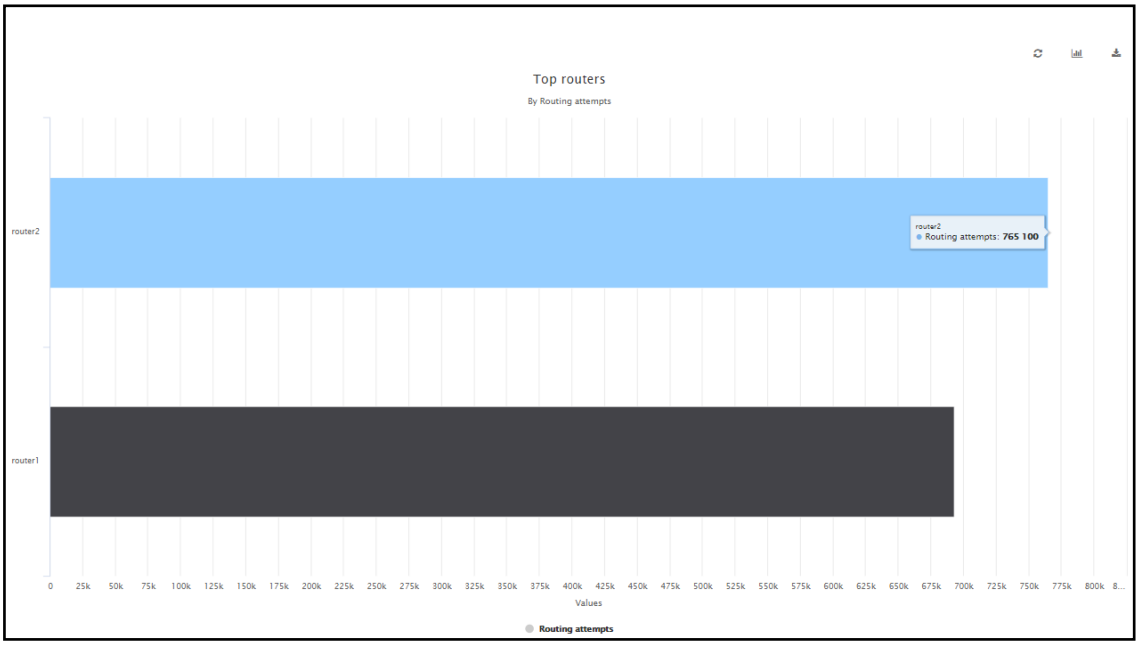
- A glance at the chart immediately reveals the top router. Point your cursor over a segment to display the number of routing attempts attempted by that router.
- You can print the chart or download the statistics in a format of your choice.

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



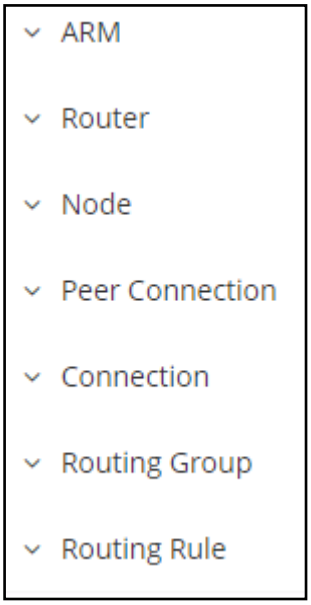
- You can select your preferred graphical representation – bar chart, column chart or pie chart. An icon 'Select chart type' allows you to present statistics according to your preferred graphical representation.

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.

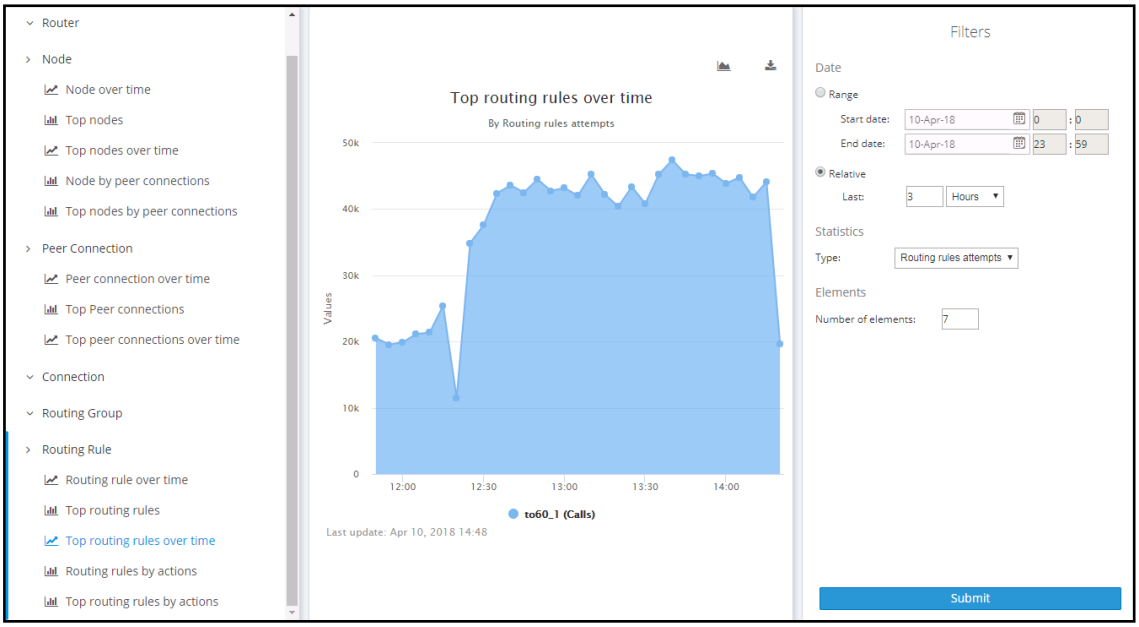
Figure 5-5: Elements that Hold Statistics Information



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

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

Figure 5-6: Top Routing rules over time



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 below)
- Add Users Groups to the ARM (see Adding Users Groups to the ARM on page 63)
- Add an LDAP Server to the ARM (see Adding an LDAP Server to the ARM on page 68)
- Add a Property Dictionary to the ARM (see Adding a Property Dictionary to the ARM on page 73)

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.

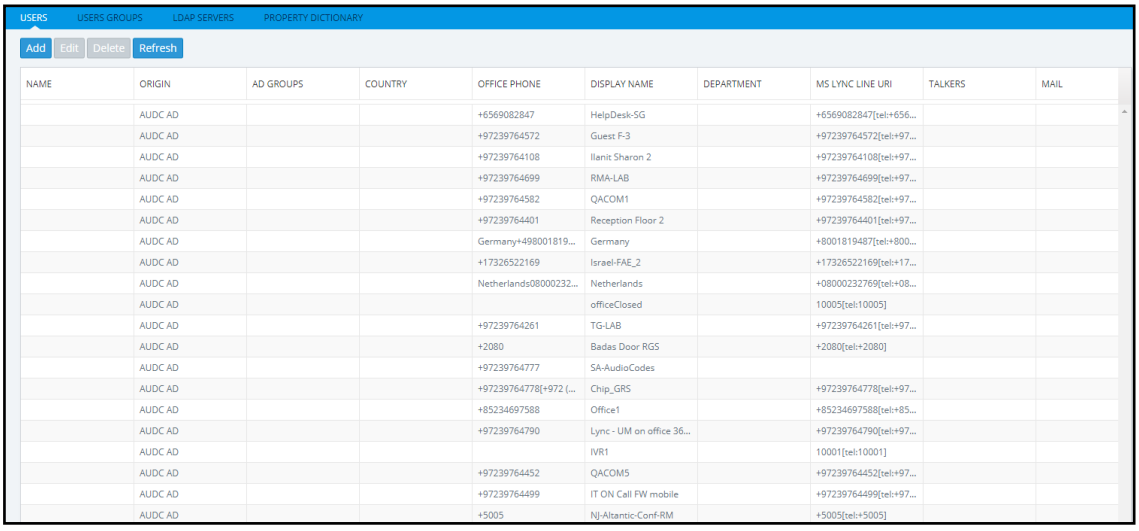
Enterprises that store their users in another format (Excel, for example) can also import these users into the ARM as local ARM users using the ARM northbound REST API. For more information and assistance, contact AudioCodes Professional Services.

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 68.

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

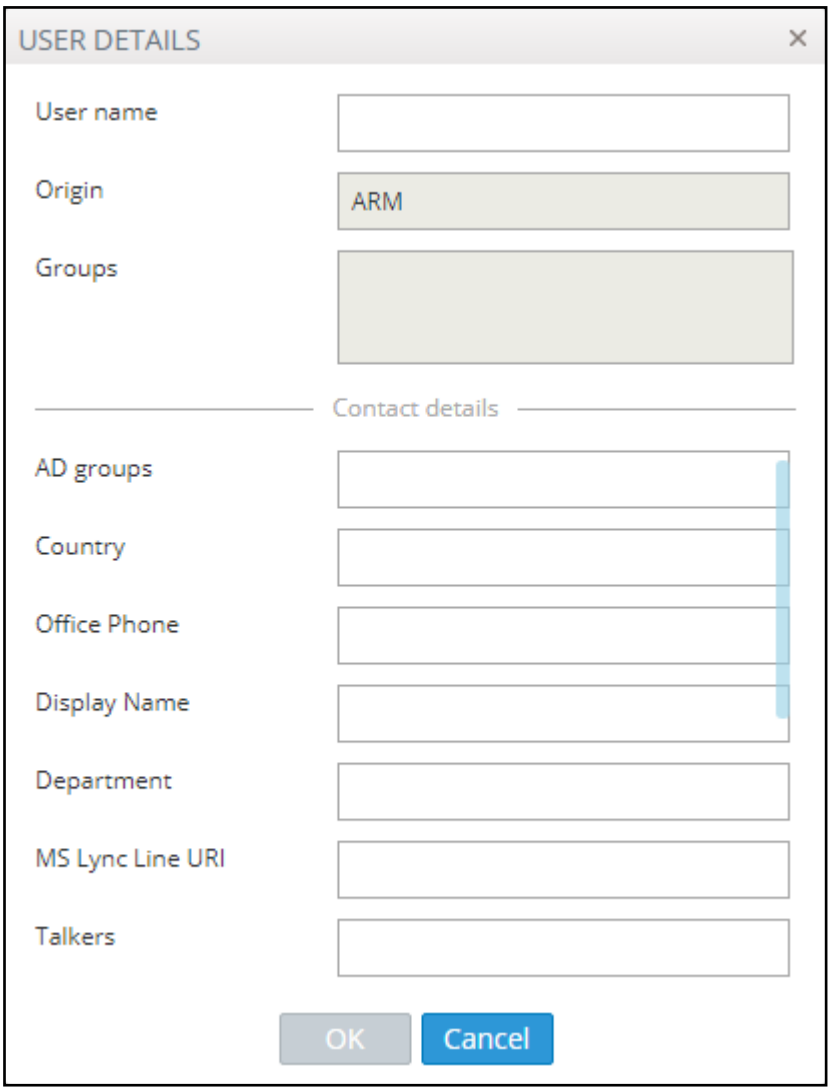
1. In the ARM's Users page, click the **Users** tab under the Users menu.

Figure 6-1: Users Page – Users tab



2. Click **Add**.

Figure 6-2: User Details

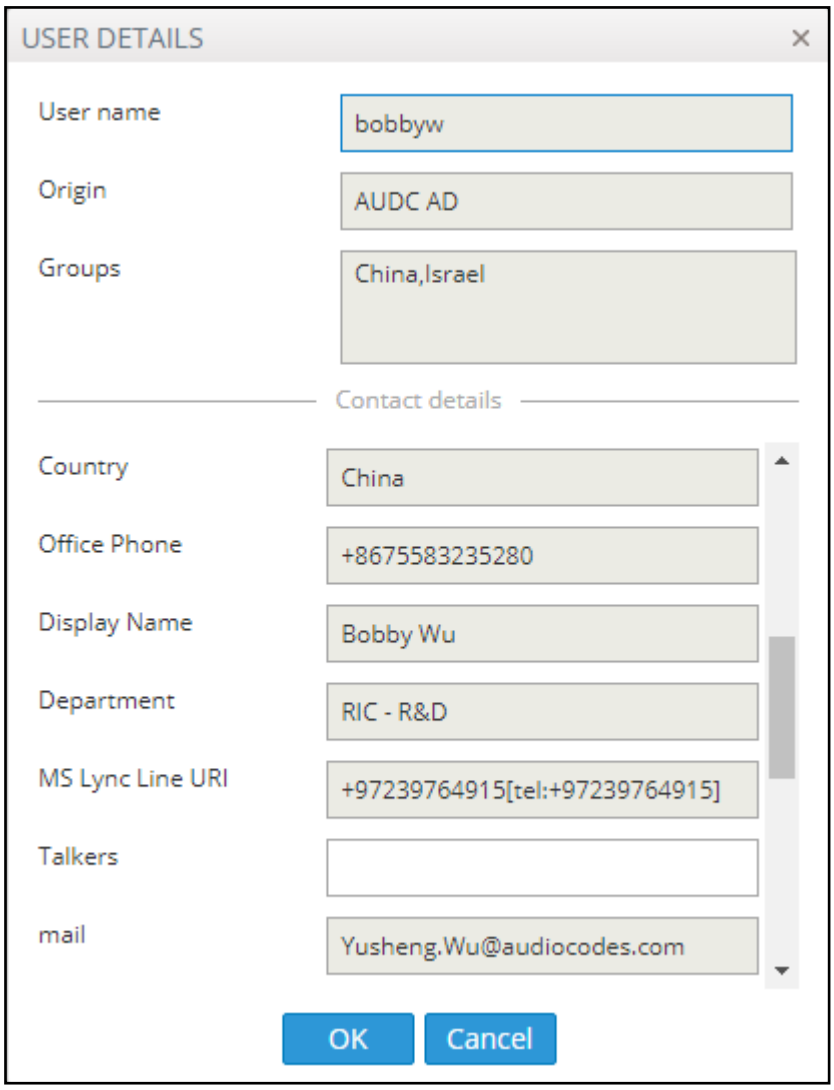


User Details are taken from the Property Dictionary screen. If a property is added in the Property Dictionary screen, it appears here. To add a property, see Adding a Property Dictionary to the ARM on page 73.

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



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.

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.

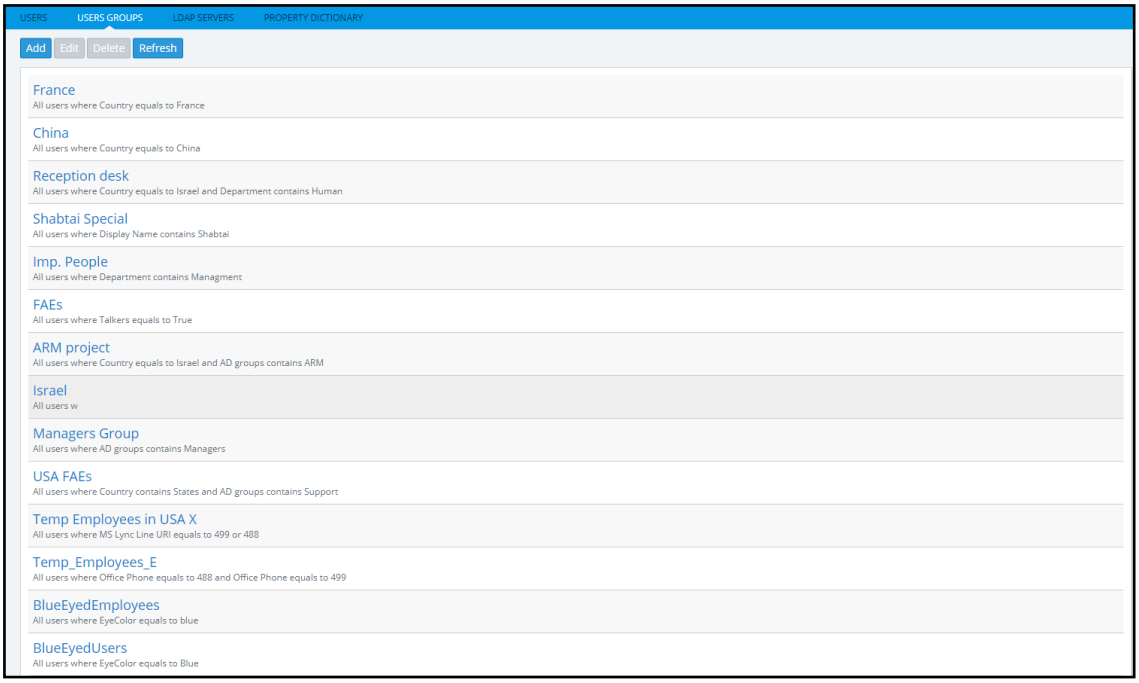
A Users Group can have a single attribute condition or a combination of attributes conditions. For a user to be a part of the Users Group, all the conditions must be matched. A single condition can have a set of values to compare to. If any of the values of the condition are matched, the condition is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

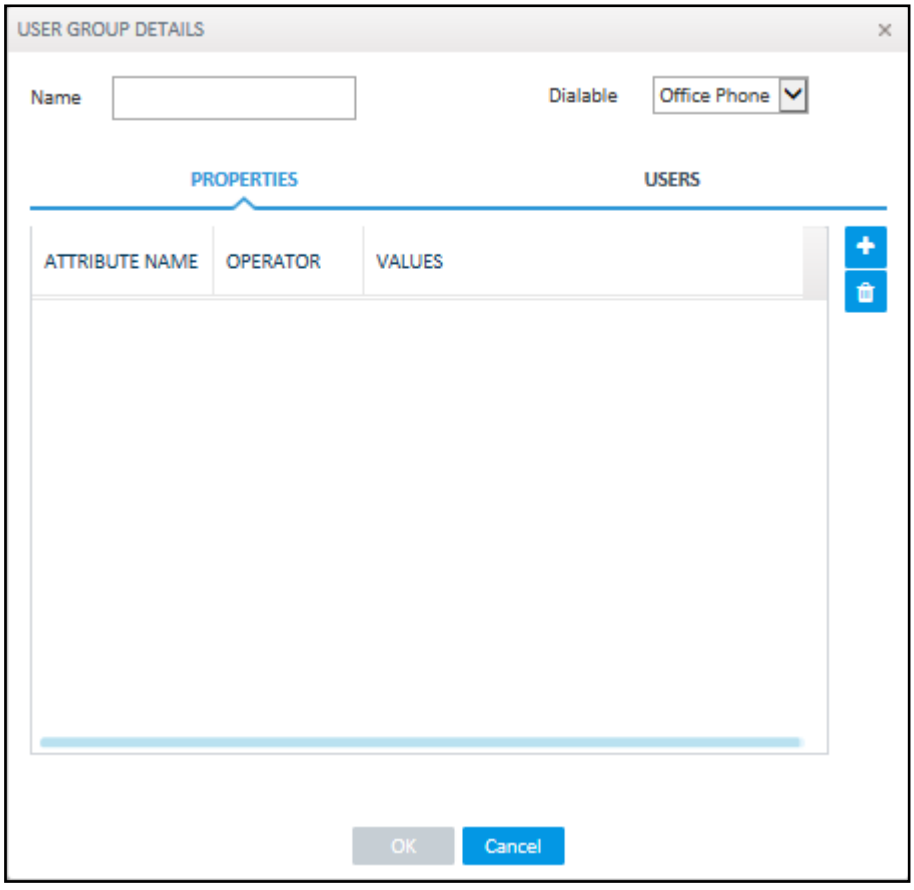
1. In the Users page, click the **Users Groups** tab.

Figure 6-4: Users Groups



2. Click **Add**.

Figure 6-5: Users Group Details



3. Configure the details using this table as reference.

Table 6-1: Users 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 the field and from the drop-down menu, select a user attribute according to which the user will be associated with the group. Example: Country. Click the plus button **+** 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 drop-down menu, select the operation to be used to define the criterion.
Value	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:

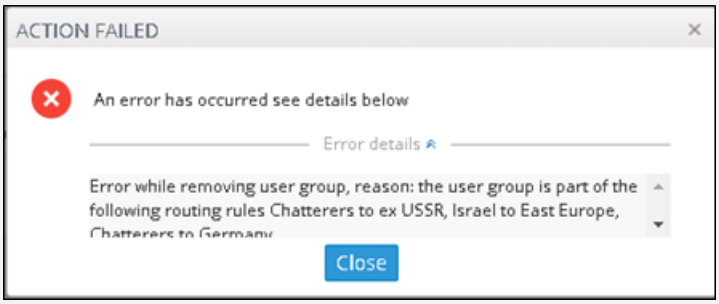
1. In the Users page, select the user group to edit and then click **Edit**; the User Group Details screen opens – under the **Properties** tab. You can see the users who are associated with the group under the **Users** tab of the User Group Details screen.

2. Edit using the table above as reference, and then click the **Users** tab; the screen shown above right opens allowing you to view the users that were associated to the group in the **Users** tab of the User Group Details dialog.

➢ 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.

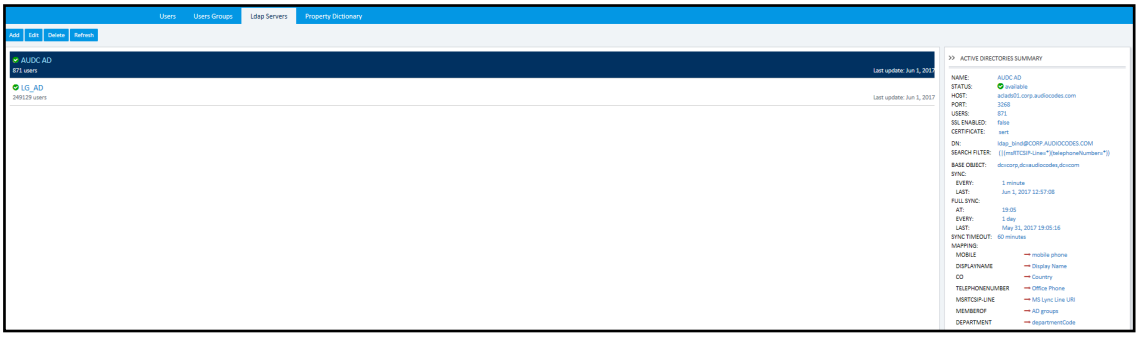
Adding an LDAP Server to the ARM

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

➢ To add an LDAP server:

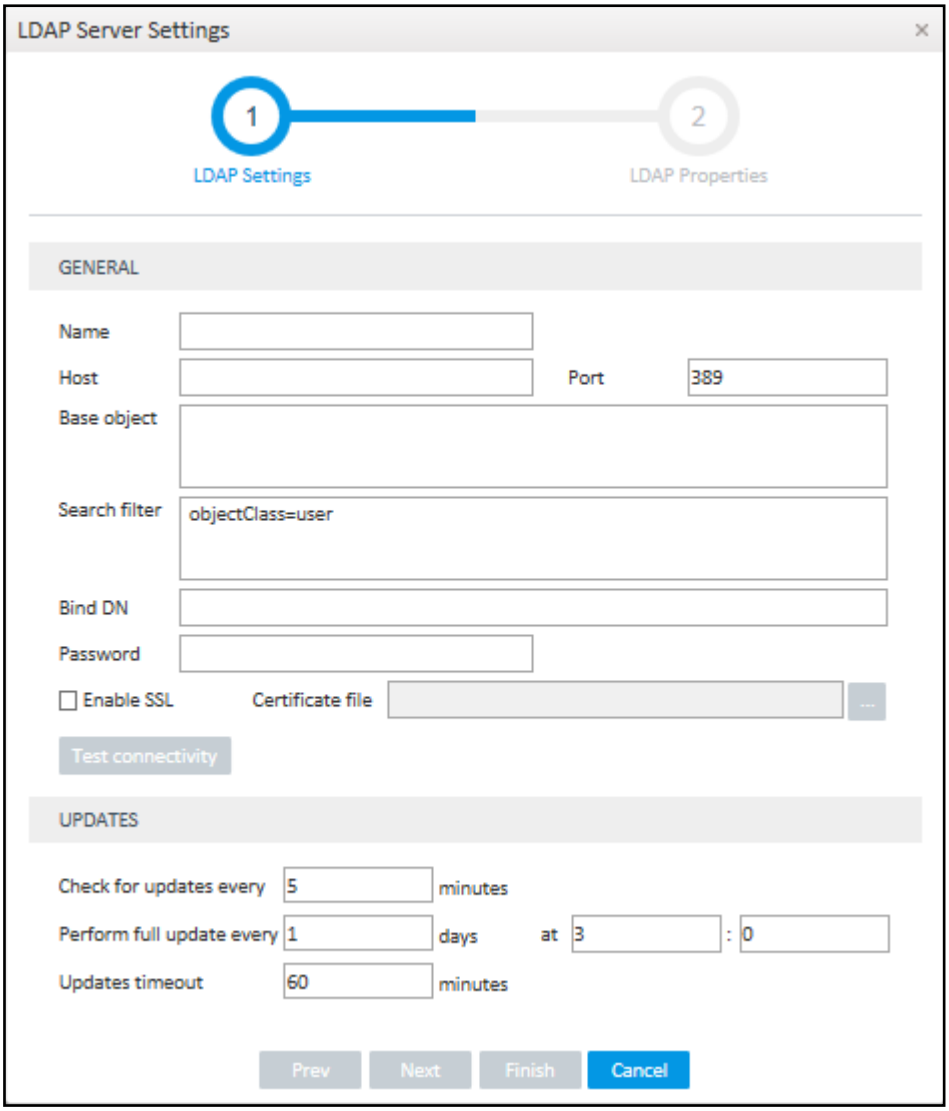
1. In the Users page, click the **LDAP Servers** tab.

Figure 6-6: Users Page – LDAP Servers tab



2. Click **Add**.

Figure 6-7: LDAP Server Settings



3. Configure the settings using this table as reference.

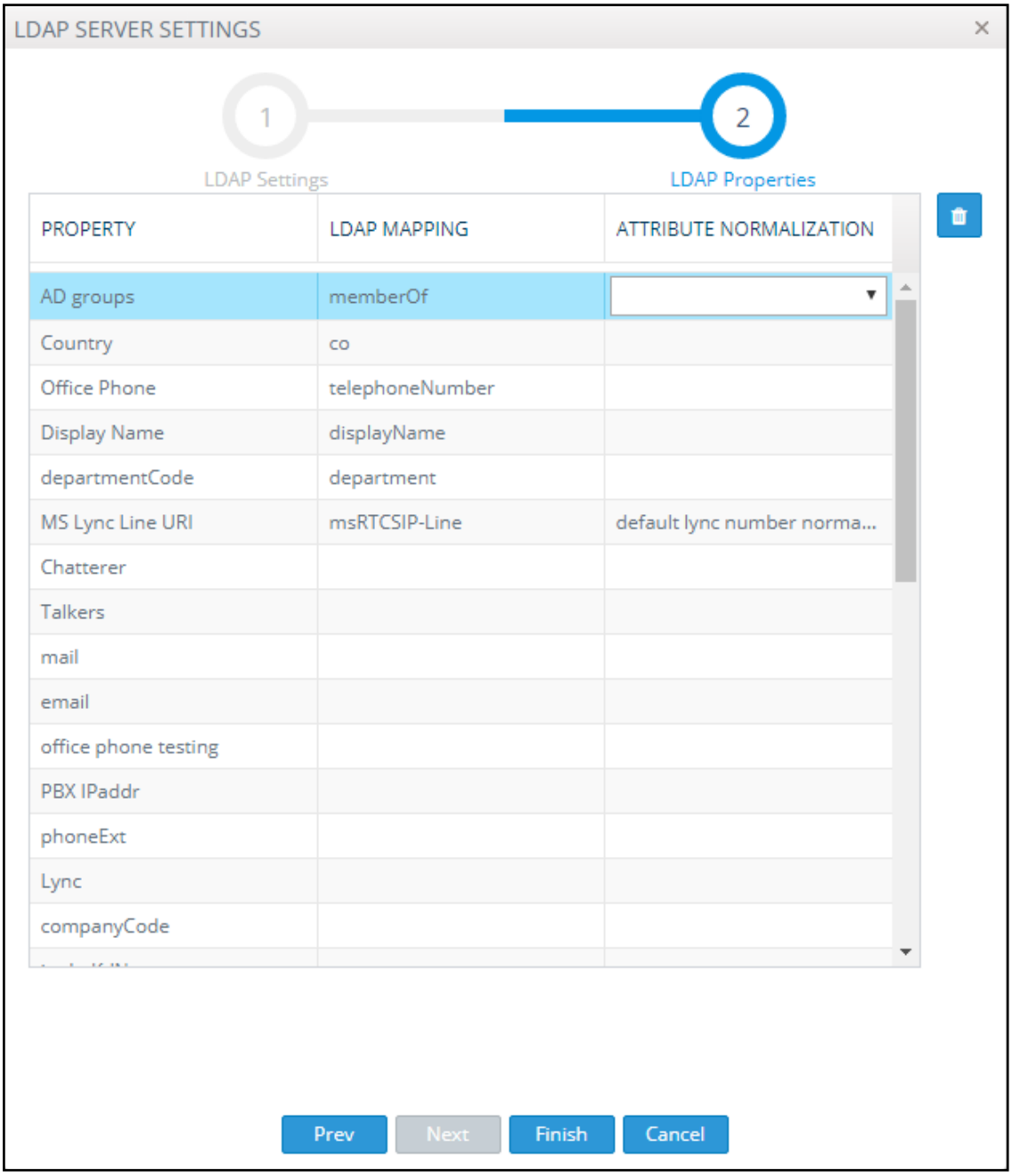
Table 6-2: LDAP Server Settings

Setting	Description
Server 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 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): ou=Users;ou=APC;ou=Israel;ou=AudioCodes;dc=corp;dc=audiocodes;dc=com The DN path is defined by the LDAP names OU (organizational unit) and DC (domain component).
Search Filter	An LDAP search filter used when fetching the users from the LDAP server under the base DN. The default is 'objectClass=user'.
Security Settings	
Bind DN	The DN (distinguished name) or username of the user used to bind to the LDAP server. For example: ldap_bind@corp.audiocodes.com
Password	Defines the LDAP password used to connect.
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	
Check for updates every *n* 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).
Perform full update every *n* 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).

Setting	Description
Updates timeout	If the AD server doesn't answer within the period set, the ARM server determines that the AD server is disconnected and a refresh is sent.
Test Connectivity	Click the button to test the connectivity between the ARM server and the AD server.

4. Click **OK** now or click it after the **Next** button. You can also click **Test connectivity;** the LDAP Properties page opens:

Figure 6-8: LDAP Properties



Properties that have LDAP mappings will be synced from the LDAP server. Properties that do not have LDAP mappings can be configured locally.

➢ 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 (Rule).
2. From the property's Attribute Normalization drop-down menu, select a Normalization Group. See Adding a Normalization Group on page 103 for information on how to configure a Normalization Group.
3. Click **Finish**.

➢ 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 6-9: Users Page – LDAP Servers tab – AD Summary

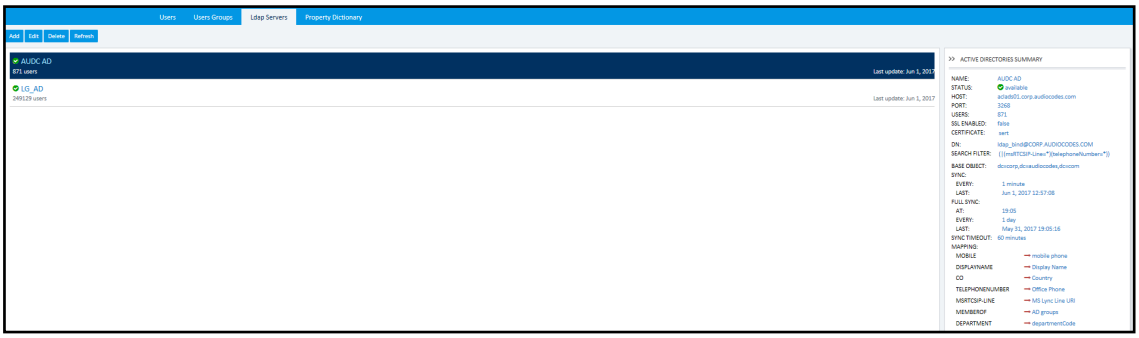


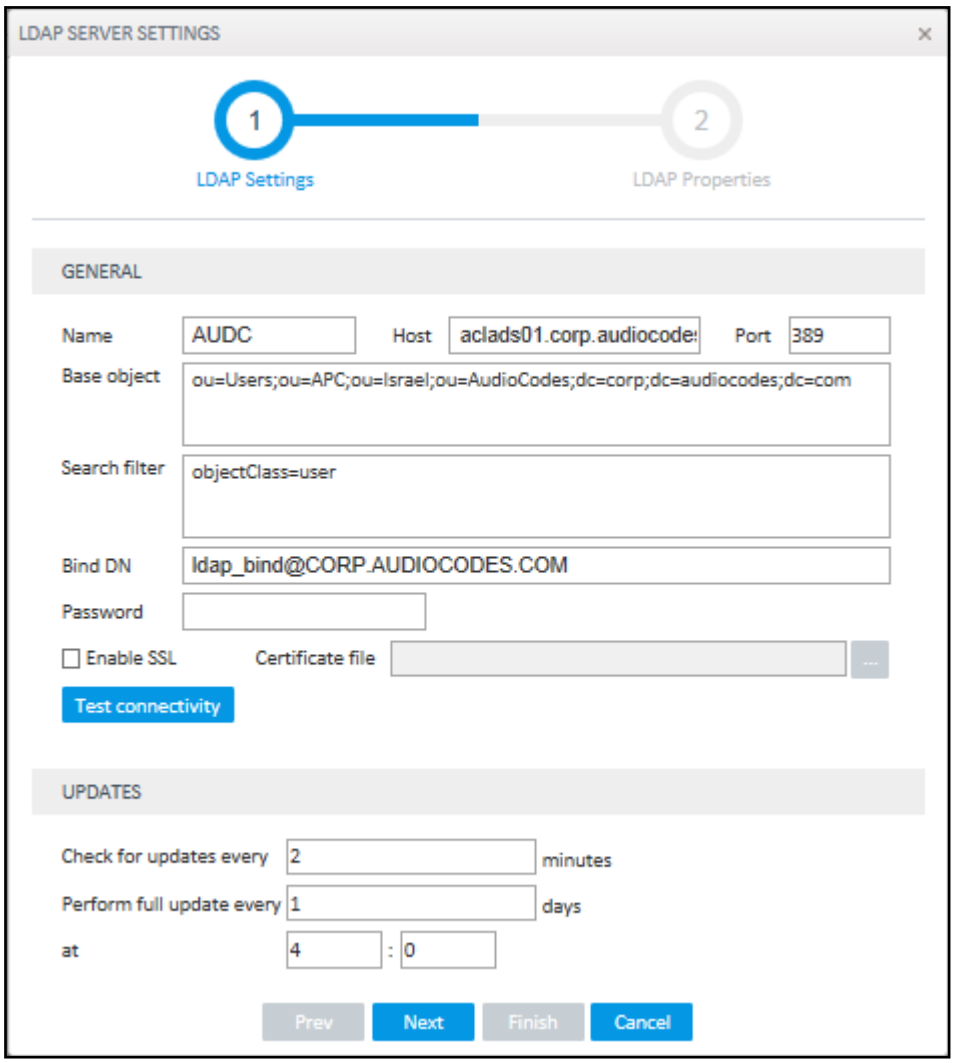
Table 6-3: Active Directories Summary

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 then click **Edit**; the LDAP Server Settings open.

Figure 6-10: LDAP Server Settings



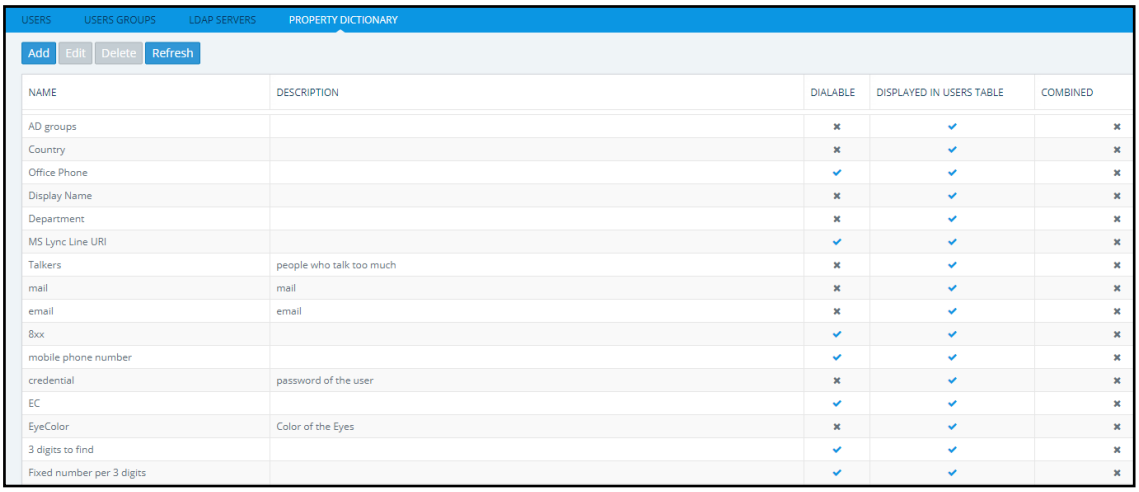
2. Edit the LDAP Server Settings screen, click **Test Connectivity** to test the connection settings and then click **Next**; the LDAP Properties screen opens.
3. For each LDAP property's LDAP Mapping drop-down menu, select a mapping. Properties that have LDAP mappings will be synced from the LDAP server. Properties that do not have LDAP mappings can be configured locally.
4. Select the row of the LDAP property to which to attach a Normalization Group (Rule) and then from the property's Attribute Normalization drop-down menu, select a Normalization Group. See Adding a Normalization Group on page 103 for information about how to configure a Normalization Group.
5. Click **Finish**.

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 6-11: Users Page – Property Dictionary tab

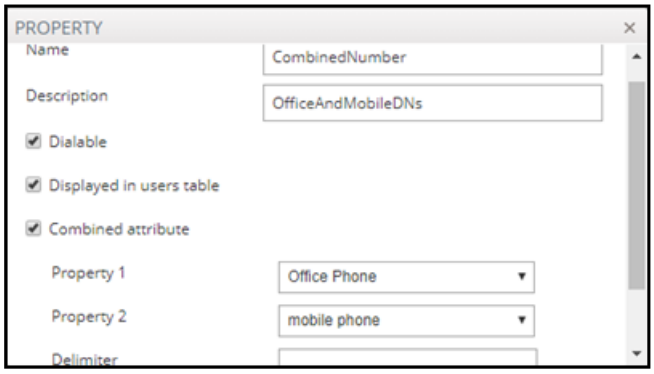


After adding a property to the dictionary, you can add it to some or all your LDAP servers. Properties added to an LDAP server will automatically be read from the LDAP server. Properties not added can be set locally in the ARM for each user. The Properties from the dictionary can then be used as User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

➢ To add / edit a property:

1. Open the Property Dictionary page (**Users** menu > **Property Dictionary** tab).
2. Click **Add** or **Edit**.

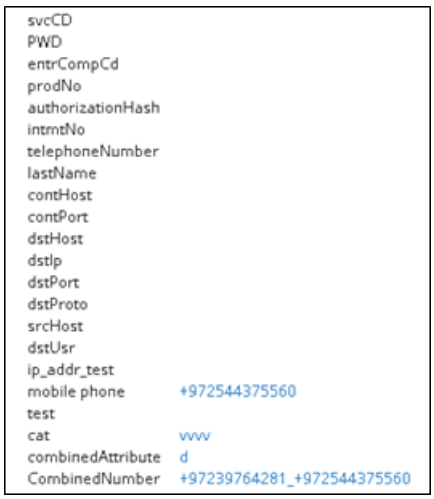
Figure 6-12: Property



3. Use the following table as reference.

Table 6-4: Add Property

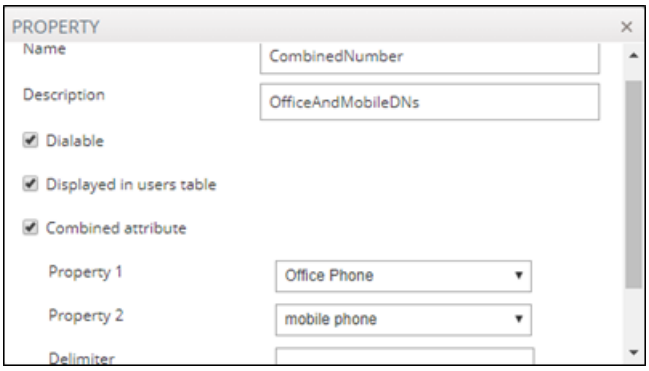
Setting	Description
Name	Define an intuitive name for the property, for intuitive future reference.
Description	Enter a brief description of the property, for intuitive future reference.
Dialable	Defines if this property is a dialable number. Only dialable numbers are used for matching with a received source or destination URI in a route request.

Setting	Description
	Examples of dialable number properties: Office phone number, mobile phone number, Skype number, etc.
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	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. 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.  svcCD PWD entrCompCd prodNo authorizationHash intmtNo telephoneNumber lastName contHost contPort dstHost dstIp dstPort dstProto srcHost dstUsr ip_addr_test mobile phone +972544375560 test cat vvvv combinedAttribute d CombinedNumber +97239764281_+972544375560 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.

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

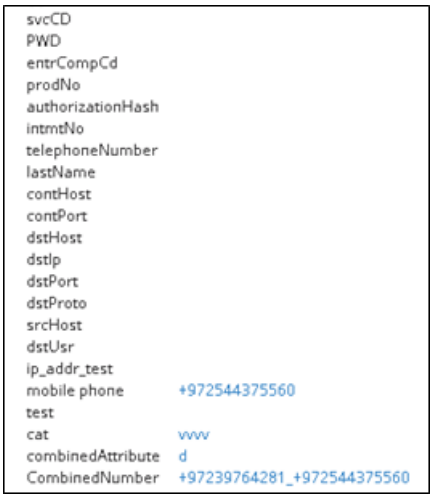
The ARM provides the capability to add an attribute in the Users Dictionary triggered by a combination of two other Users Dictionary attributes with a predefined delimiter. If any of the basic attributes [that the new attribute is combined of] changes, the new attribute will change. To accomplish this,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

Figure 6-13: Property – Combined Attribute



[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 6-14: Combined Number



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.

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 78)
  - Operators (see Provisioning Operators on page 82)
  - Node Credentials (see Node Credentials on page 83)
  - Router Credentials (see Router Credentials on page 85)
  - Configurator Credentials (see Configurator Credentials on page 87)
  - LDAP Authentication (see Provisioning Operators using an LDAP Server on page 90)
  - RADIUS Authentication (see Provisioning Operators using a RADIUS Server on page 93)
  - Remote Manager (see Remote Manager on page 96)
  - Certificates (see Uploading Trusted Certificates on page 81)
- Network Services
  - Syslog server (see Editing a Syslog Server on page 97)
  - NTP server (see Adding/Editing an NTP Server on page 99)
  - QoS (see Prioritizing Traffic Per Class of Service on page 99)
  - CDRs (see Enabling CDRs on page 102)
  - Calls (see Disabling, Limiting the Number of CDRs on page 155)
- Call Flow Configurations
  - Normalization Groups (see Adding a Normalization Group on page 103)
  - Prefix Groups (see Adding a Prefix Group on page 105)
  - Normalization Before Routing (see Normalization Before Routing on page 107)
  - Policy Studio (see Policy Studio on page 108)
  - Web Services (see Web-based Services on page 112)
- Routing
  - Configuring a Quality Based Routing Condition (see Configuring Criteria for a Quality Profile on page 114)
  - Configuring a Time-Based Routing Condition (see Configuring a Time-Based Routing Condition on page 115)
  - Configuring SIP Alternative Route Reason (see Configuring SIP Alternative Route Reason on page 118)
  - Configuring Global Routing Settings (see Configuring Global Routing Settings on page 120)
- Routing Servers
  - Servers
    - Adding a Routing Server (see Adding a Routing Server on page 120)
    - Editing a Routing Server (see Editing a Routing Server on page 122)
    - Locking/Unlocking a Routing Server (see Locking/Unlocking a Routing Server on page 123)
  - Groups
    - Adding a Routing Server Group (see Adding a Routing Server Group with Internal and External Priorities on page 124)

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 the next page)
- Add an operator (see Provisioning Operators on page 82)

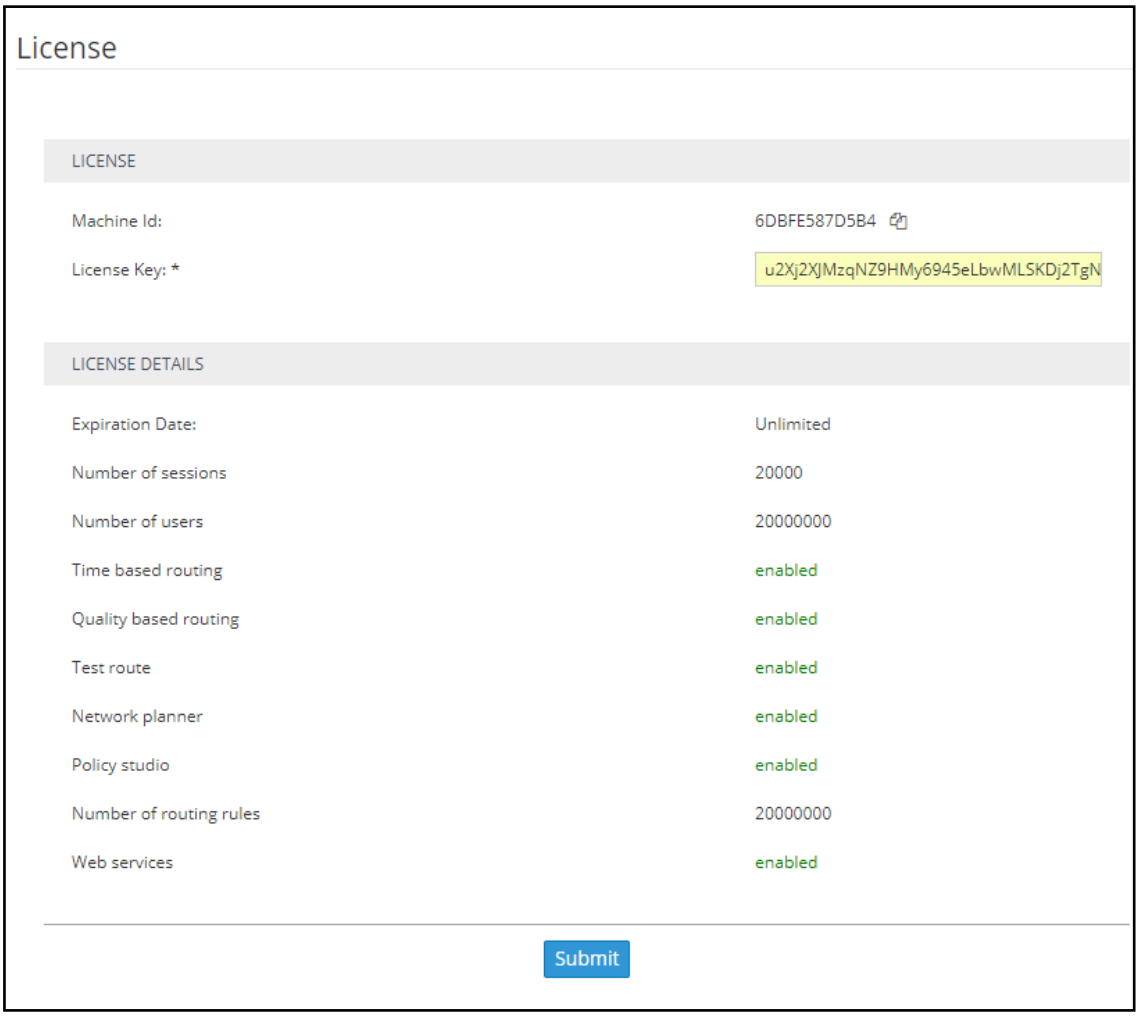
Activating Your License

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



2. Select and copy the 'License Key' shown in the figure above.
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

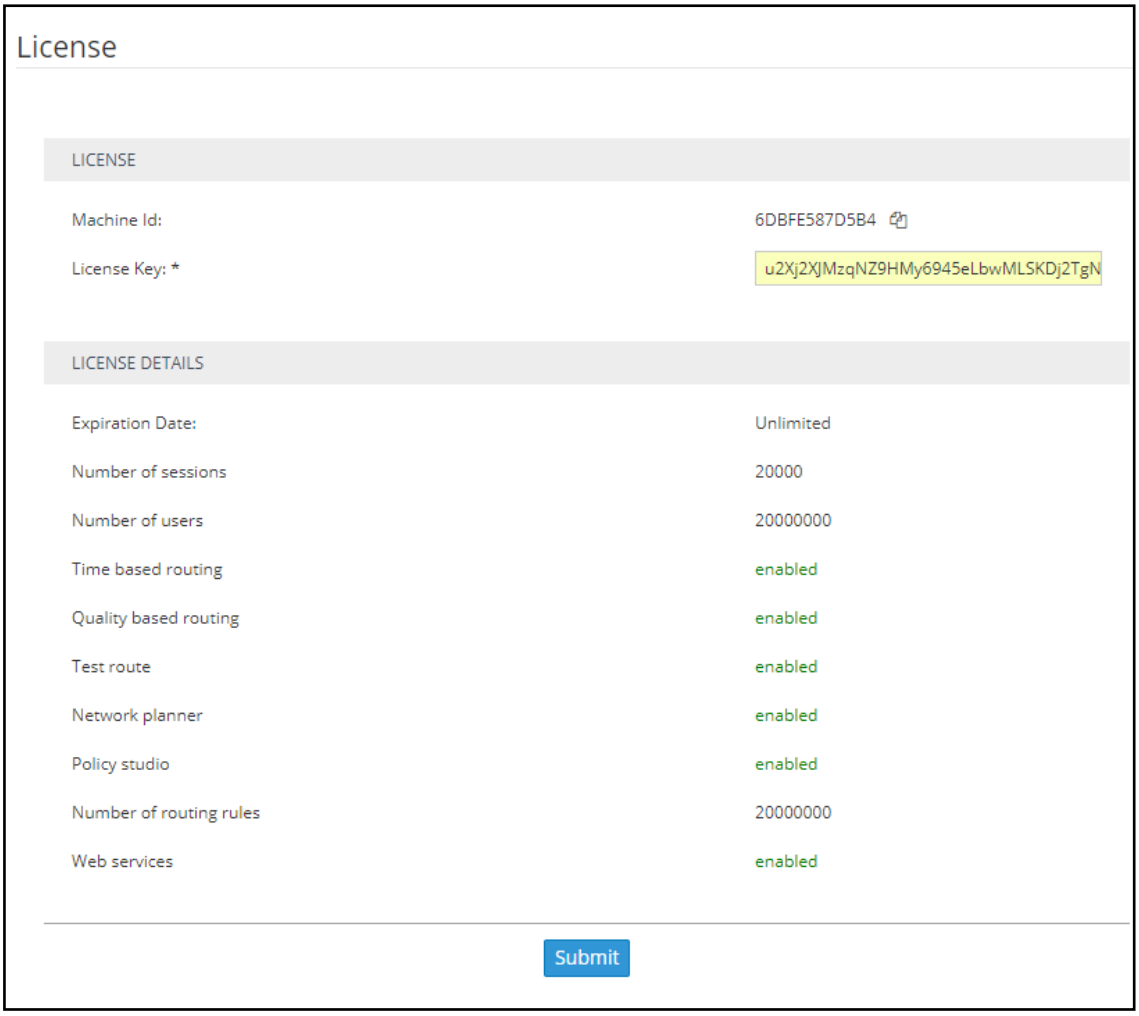
License policy is based on the following aspects of ARM functionality and capacity:

- Expiration Date
- Number of Sessions
- Number of Users
- Number of Routing Rules
- Tune 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



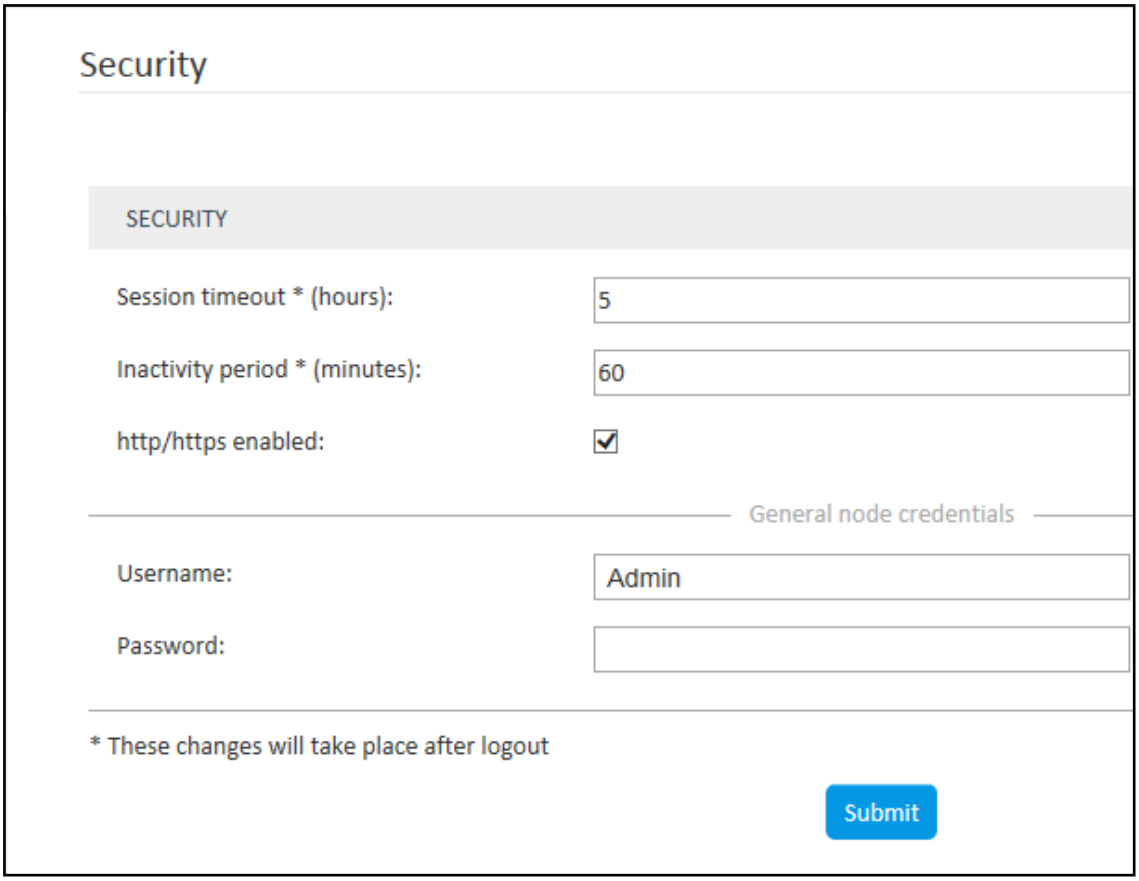
Securing the ARM

This ARM enables operators to secure routing management.

➢ **To secure the ARM:**

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

Figure 7-3: Security Page



2. Use the following table as reference.

Table 7-1: Security Settings

Setting	Description
Session timeout (hours)	Closes the session timeout and forces the user to reenter their password (to reopen the session) if the timeout you define (in hours) expires. Note that this setting only takes effect after logging out and then re-logging in.
Inactivity period (minutes)	Suspends the user's account if the user does not log in to the ARM over the period you define. **0** disables the feature; users accounts will then never be suspended due to inactivity. Note that this setting only takes effect after logging out and then re-logging in.
http/https enabled	Enables an HTTP/HTTPS connection between the ARM server and the SBC / Gateway.
General Node Credentials	
Username	Username and Password are the default credentials that ARM uses when communicating with the node. Default: Admin/Admin. The ARM uses this Username if in the EDIT NODE screen (see under Node Information and Actions on page 21 for more information), you select **Use general credentials**. Change the Username only if the credentials of the node aren't Admin/Admin.

Setting	Description
Password	Username and Password are the default credentials that ARM uses when communicating with the node. Default: Admin/Admin. The ARM uses this Password if in the EDIT NODE screen (see under (see under Node Information and Actions on page 21 for more information), you select **Use general credentials**. Change the Password only if the credentials of the node aren't Admin/Admin.

3. Click **Submit**; the security configuration is saved.

Determining ARM Communications with Other Entities

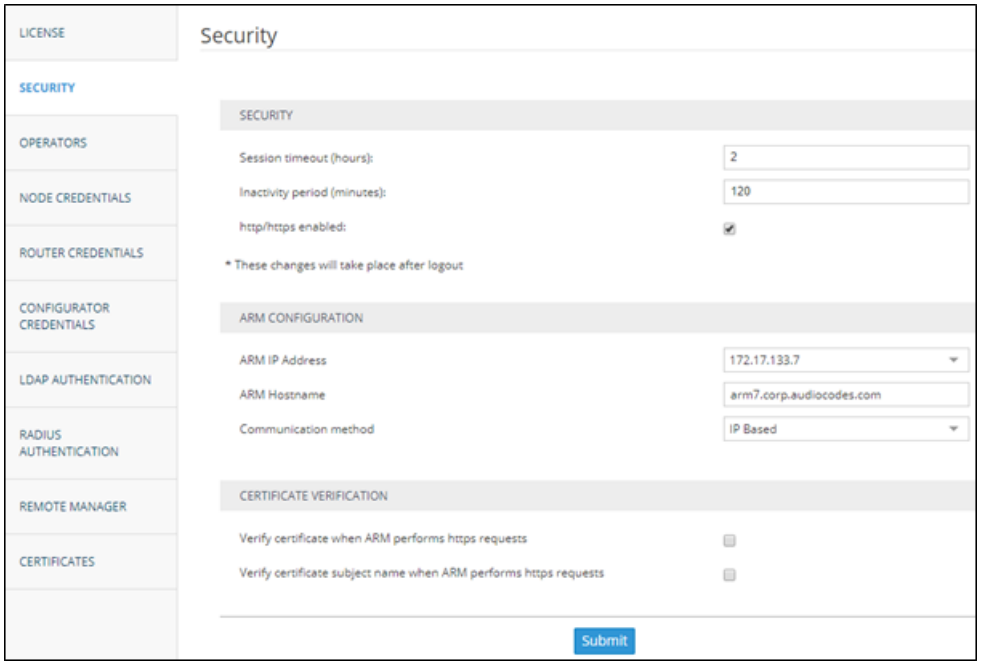
Operators can determine the way ARM communicates with other entities, e.g., routers and nodes. The ARM Configurator's address configured in these entities can be the Configurator's IP address or Hostname (FQDN).

➢ **To configure the way the ARM communicates with other entities:**

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

Figure 7-4: Security

Figure 7-5:



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]

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.

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.

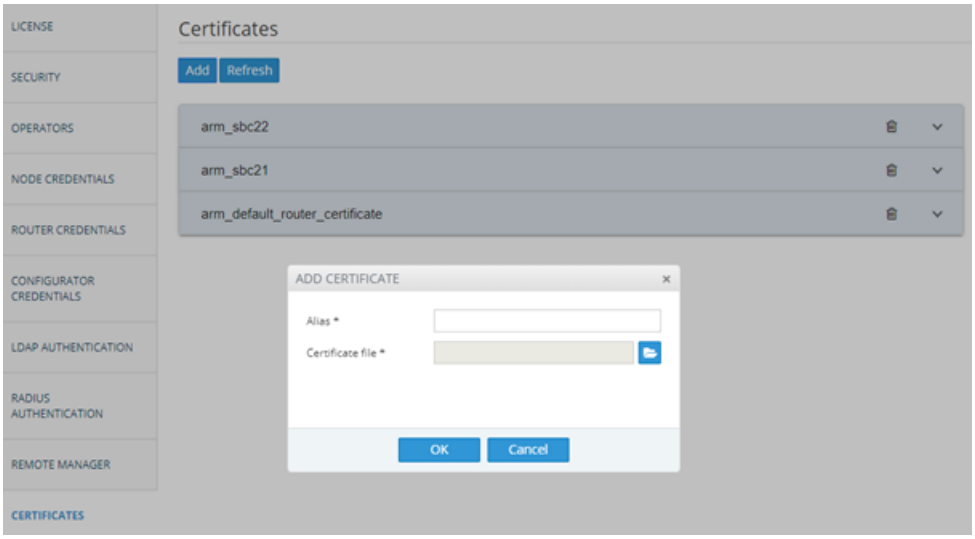
Uploading Trusted Certificates

Operators must first upload trusted certificates to the ARM.

➢ **To upload trusted certificates:**

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

Figure 7-6: Add 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.

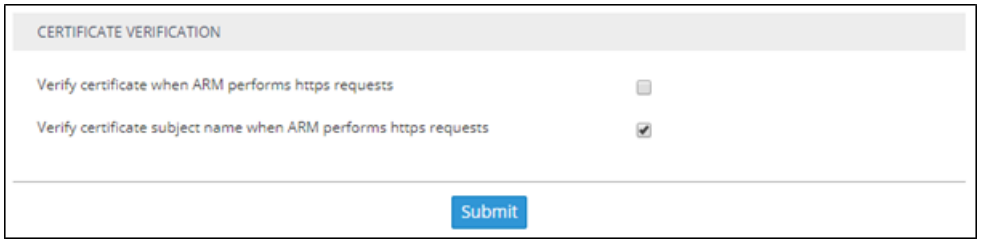
Enabling Certificate Subject Name Verification

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



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

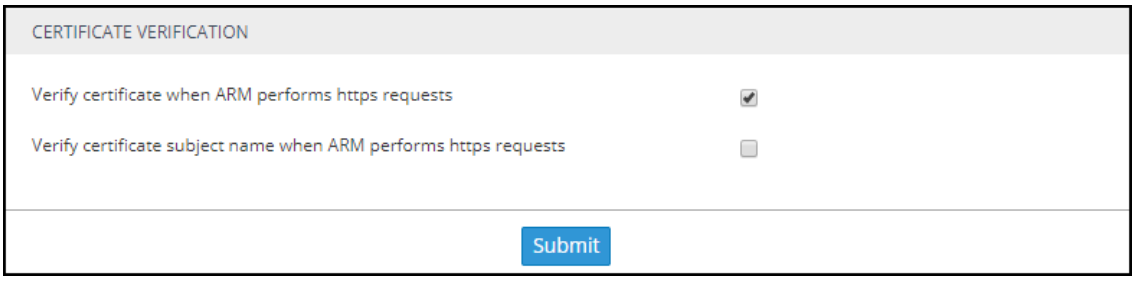
Enabling Client Side Certificate Validation

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 7-8: Certificate Verification



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

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 90
- Using the enterprise's RADIUS authentication server – see Provisioning Operators using a RADIUS Server on page 93
- Using the enterprise's Open LDAP authentication server – see Authenticating Operator Login using Open LDAP on page 93

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.

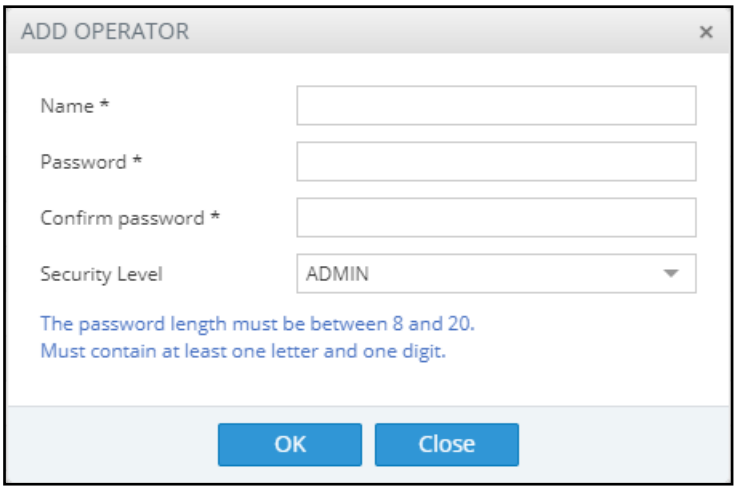
➢ **To manually add an operator:**

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

Figure 7-9: Operators

2. Click **Add**.

Figure 7-10: Add Operator



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.
Password	Enter a password for the operator to log in with.
Password confirm	Confirm the password.
Security Level	Select a Security Level for the operator: **ADMIN** or **SECURITY_ ADMIN**. **ADMIN** cannot (for example) change passwords, add or change operators, or perform licensing.

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

Node Credentials

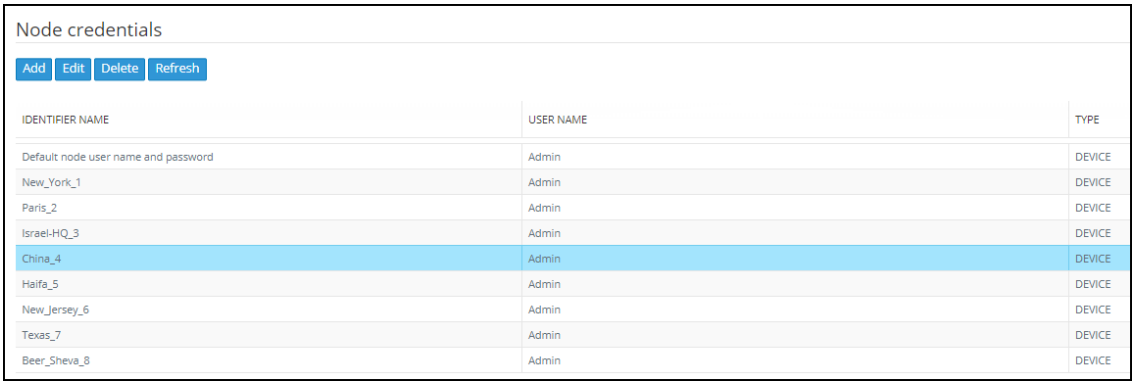
Operators can apply credentials *per Node* for ARM Configurator- Node communications.

- 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:

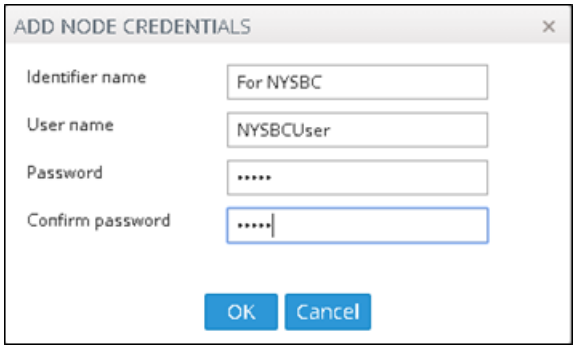
1. Open the Node Credentials page (**Settings** > **Administration** > **Node Credentials**).

Figure 7-11: Node Credentials



2. Click **Add**.

Figure 7-12: Add Node Credentials



3. Configure the fields using the table as reference.

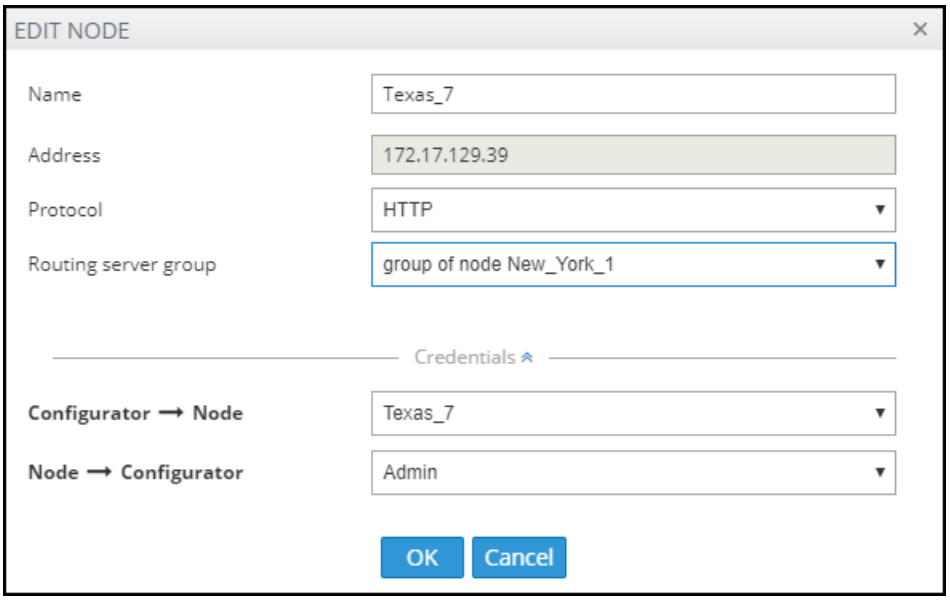
Table 7-3: Add Node Credentials

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.

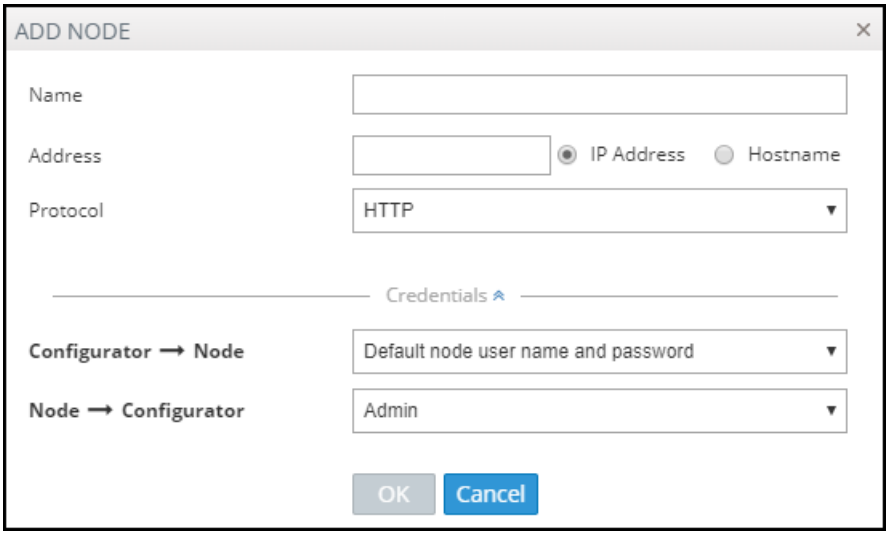
4. Click **OK**.

- 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 7-13: Edit Node - Credentials - Configurator>Node



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



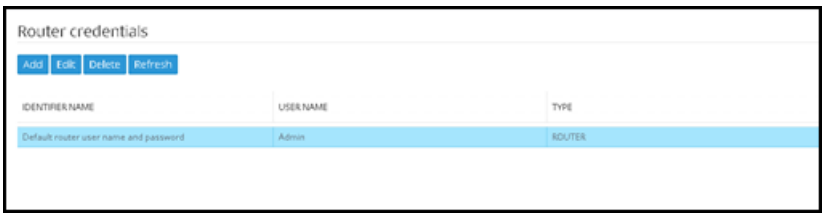
Router Credentials

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**).

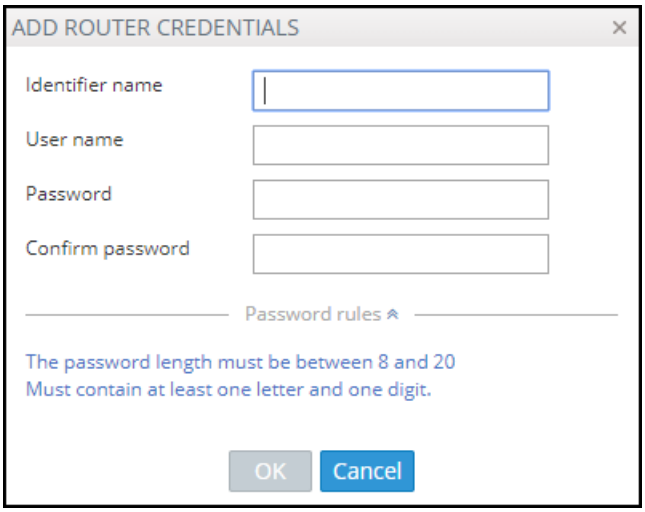
Figure 7-14: Router Credentials



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

2. Click **Add**.

Figure 7-15: Add Router Credentials



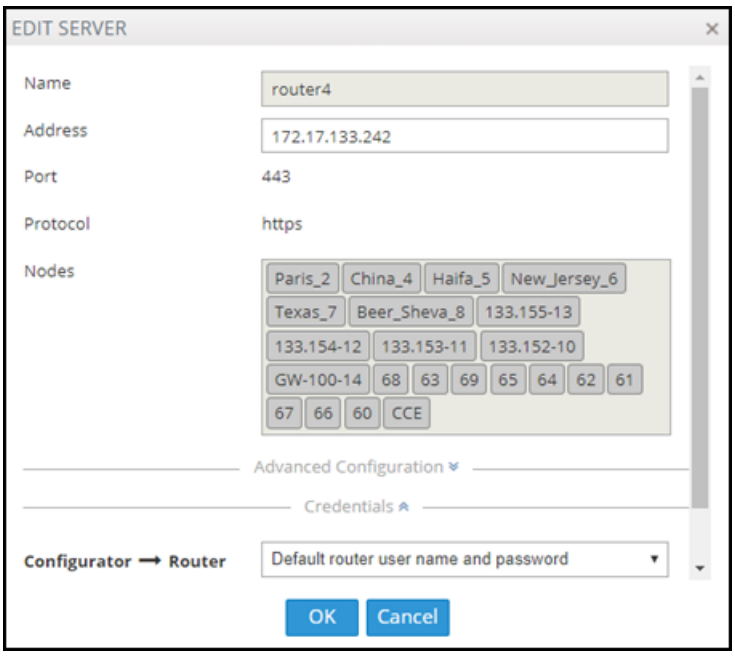
3. Configure the fields using the table as reference.

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 7-16: Edit Server: Configurator - Router Credentials



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:

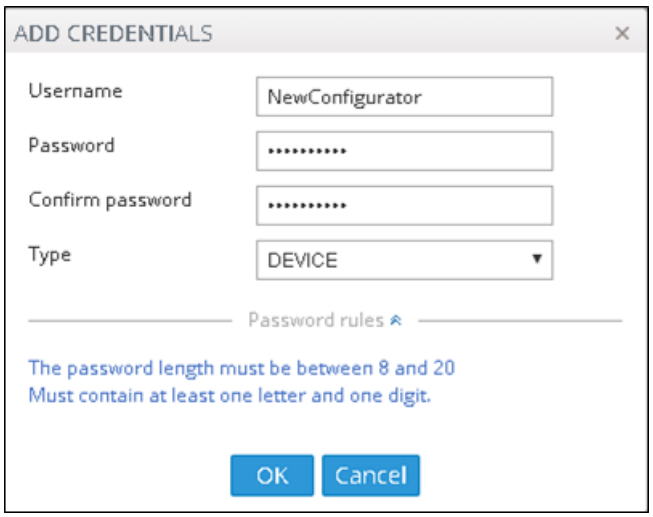
1. Open the Configurator Credentials page (**Settings** > **Administration** > **Configurator Credentials**).

Figure 7-17: Configurator Credentials

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

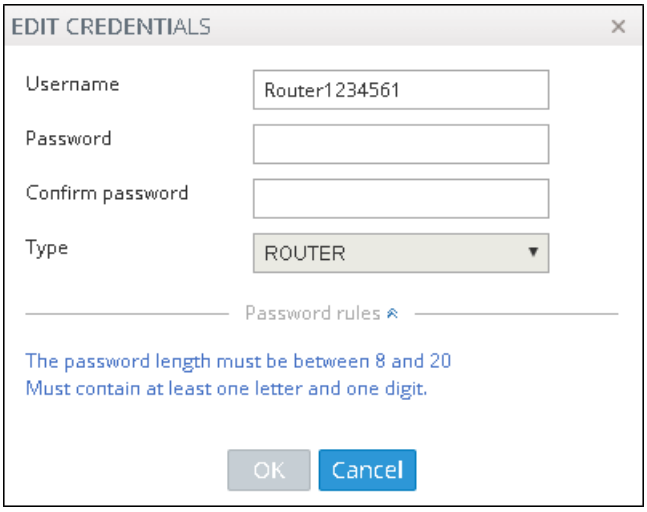
2. Click **Add**.

Figure 7-18: Add Credentials - Device



- 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 7-19: Add Credentials - Router



3. Configure the fields using the table as reference.

Table 7-5: Add Credentials - Device | Router

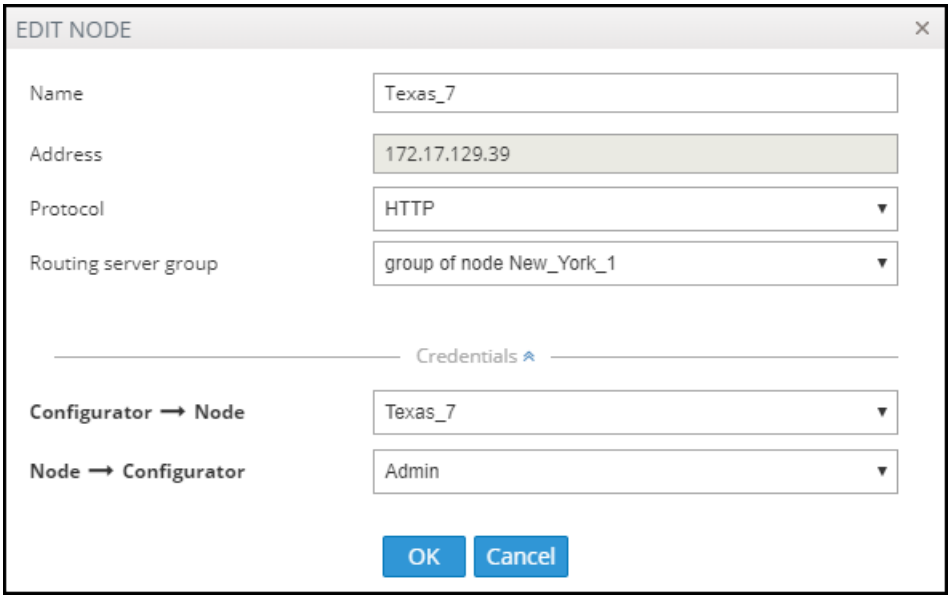
Setting	Description
User name	Enter the user name.
Password	Enter the password.
Password confirm	Re-enter the password.
Type	■ If you're configuring credentials for Node - ARM Configurator communications, select **Device**. ■ If you're configuring credentials for ARM Router - ARM Configurator communications, select **Router**.

4. Click **OK**.

5. [Optionally] Apply one of the previously defined settings to a specific

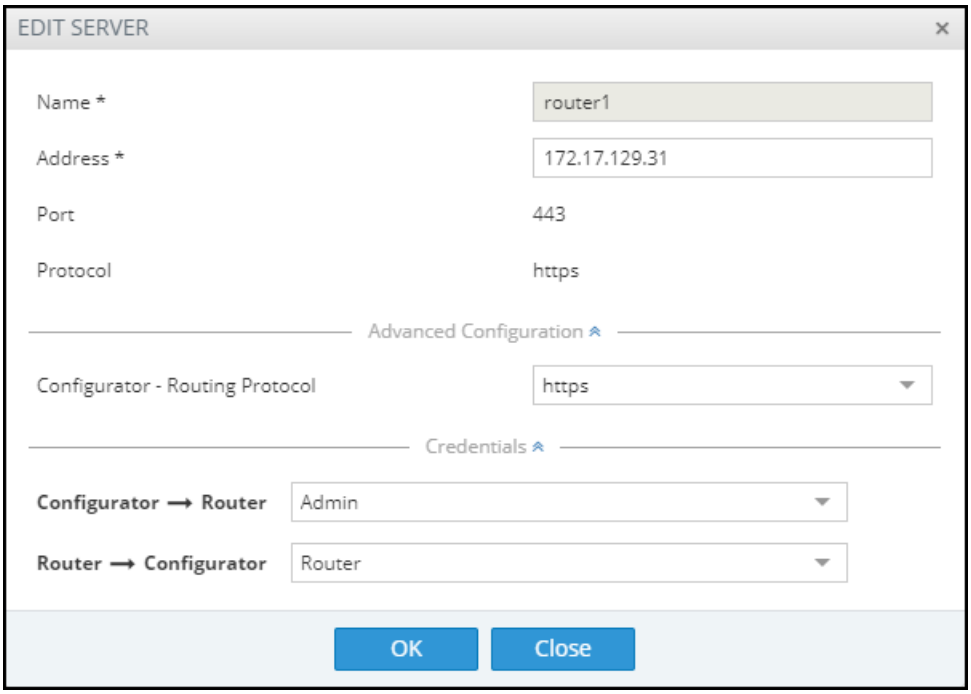
- **Node** (or use the default Node): Open the Edit Node screen (**Network** > **Map** > <select the node> > **Edit**) and expand 'Credentials'.

Figure 7-20: 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'.



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.

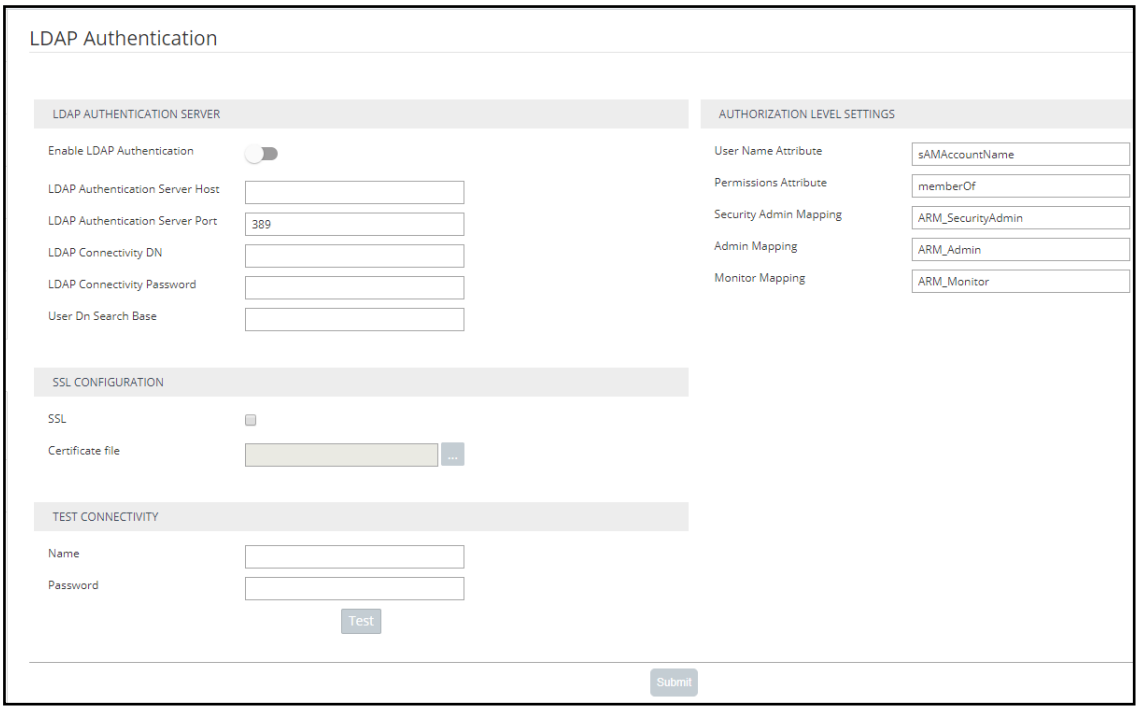
Provisioning Operators using an LDAP Server

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 83.

➢ To add an LDAP operator login authentication server:

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

Figure 7-21: 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.

Parameter	Description
LDAP Connectivity Password	Configure the 'LDAP Connectivity Password' as required.
User DN Search Base	Configure the 'User DN Search Base' as required.

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

Table 7-7: SSL Parameters

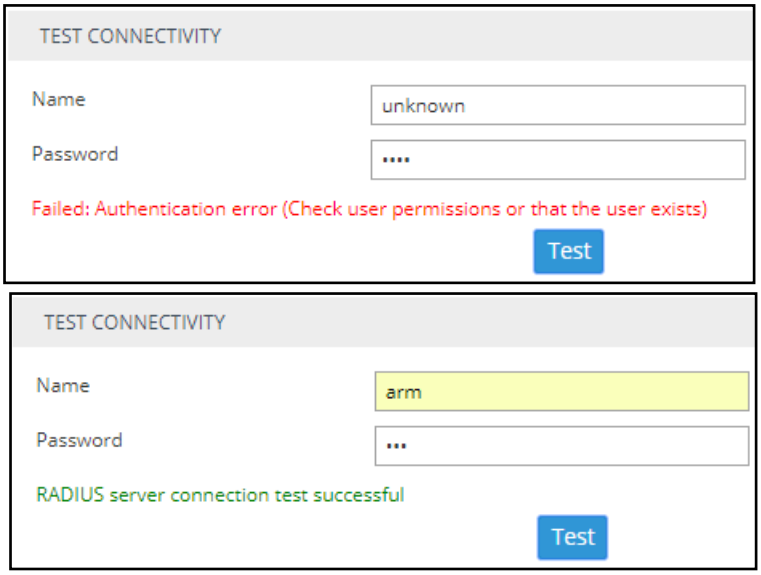
Parameter	Description
SSL	Select the 'SSL' option to secure the connection with the LDAP server over SSL. If left unselected (default), the connection with the LDAP server will be non-secured.
Certificate file	Click the 'Certificate file' browse button to browse to and select the certificate file that 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.

Figure 7-22: LDAP Connectivity Test Result



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 *in this directory* | *folder* 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 *in this directory* | *folder* 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 *against this directory* | *folder* 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 *against this directory* | *folder* 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**.

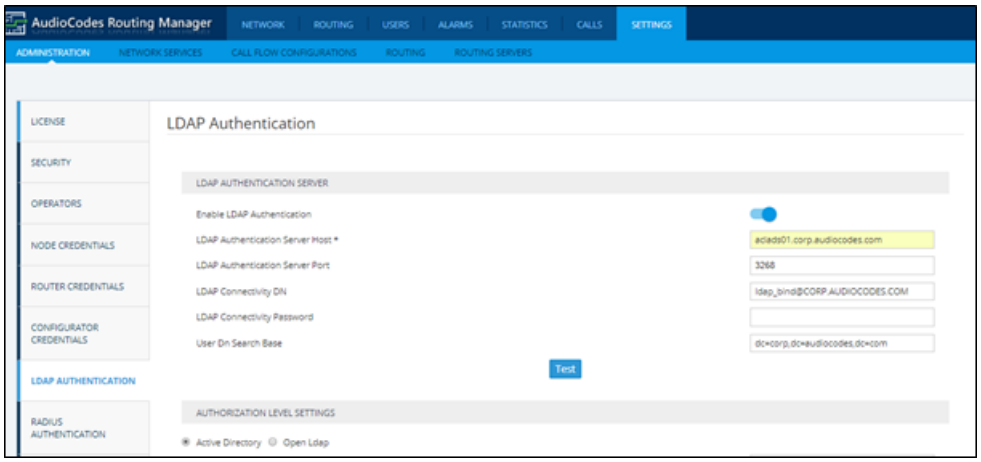
Authenticating Operator Login using Open LDAP

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 7-23: Authenticating Operator Login using Open LDAP



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 7-24: Authorization Level Settings

Provisioning Operators using a RADIUS Server

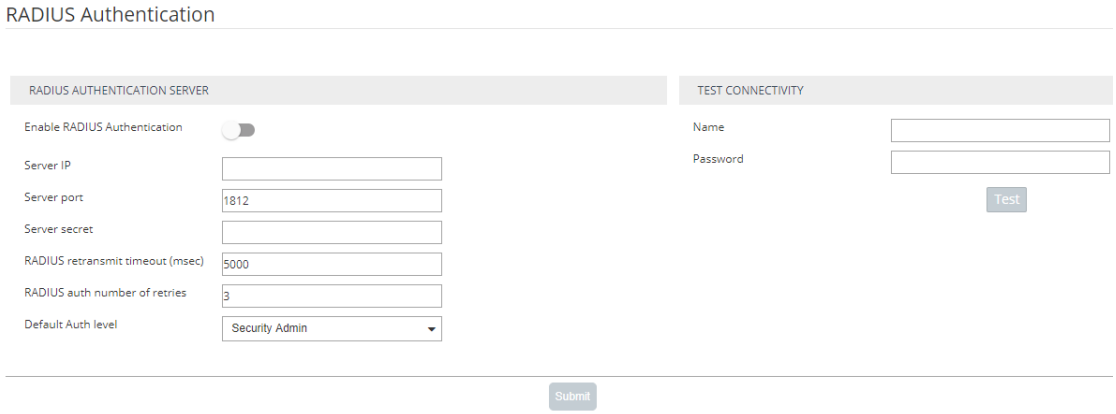
ARM allows using the enterprise's external RADIUS server for operator login authentication. This feature is available in addition to local operator login authentication described under Manually Provisioning an Operator in the ARM's Operators Page on page 83. Only operators with a security level of 'Security_Admin' 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 7-25: 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.

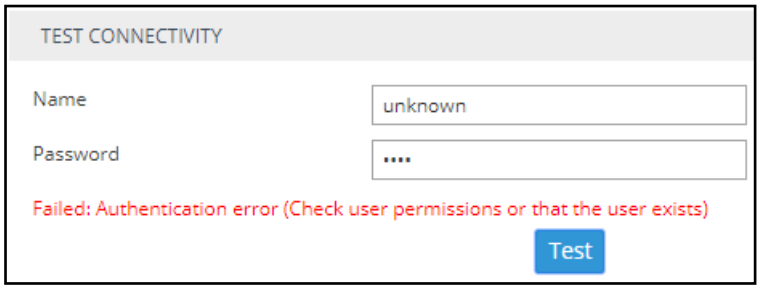
Parameter	Description
RADIUS retransmit timeout (msec)	If no response is received from the RADIUS authentication server, the ARM Configurator can be configured to *resend packets* to it. Enter the time (in milliseconds) the ARM Configurator must wait for the RADIUS server to respond before sending a 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: ■ 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]

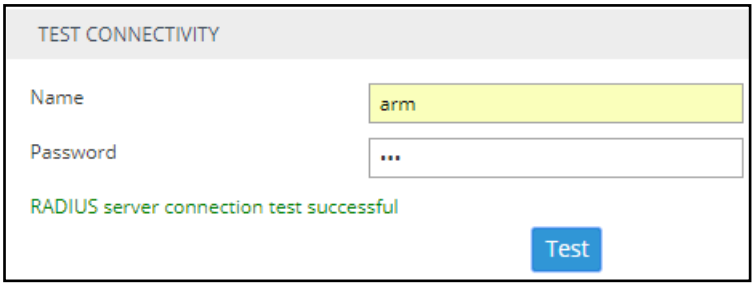
3. Connectivity with the RADIUS authentication server can be tested. Configure the Test Connectivity parameters described in the following table to test the connection with the RADIUS server.

Table 7-11: Test Connectivity

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 7-26: RADIUS Connectivity Test Result





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.

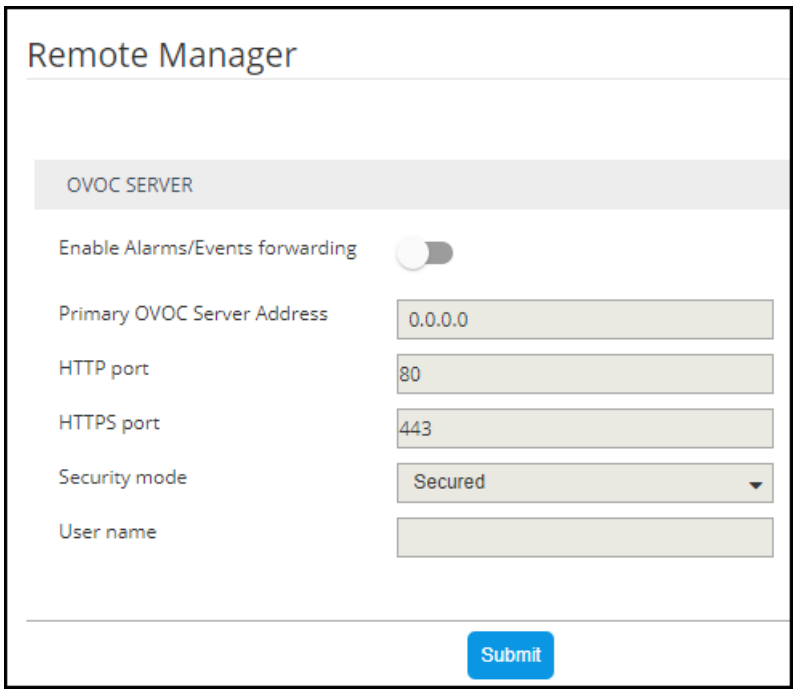
5. Click **Submit**.

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 7-27: Read-Only OVOC Information Displayed in the ARM's Remote Manager Page

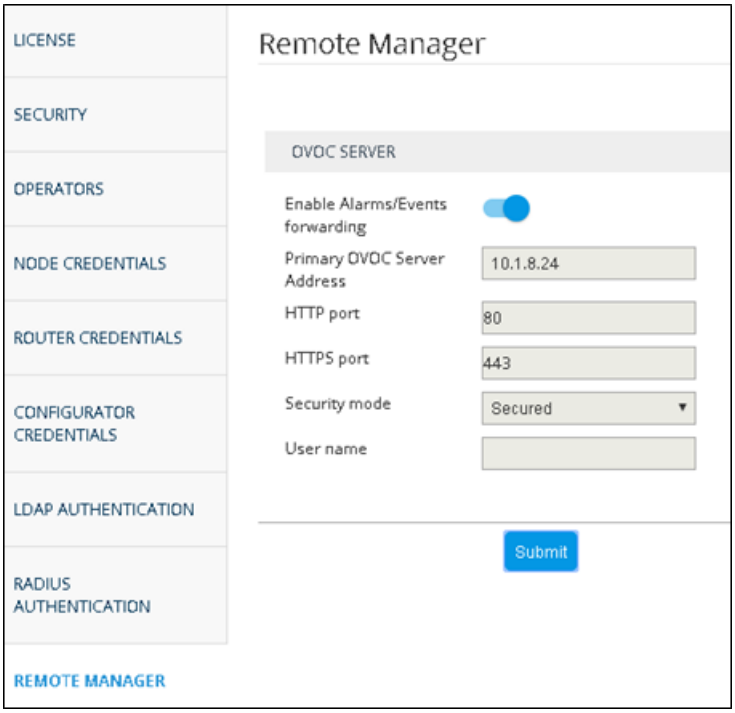


ARM-generated alarms and events can be displayed in the OVOC but the feature must be enabled in the ARM (assuming the ARM is already connected to the OVOC).

➢ **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 7-28: 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.

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 99.

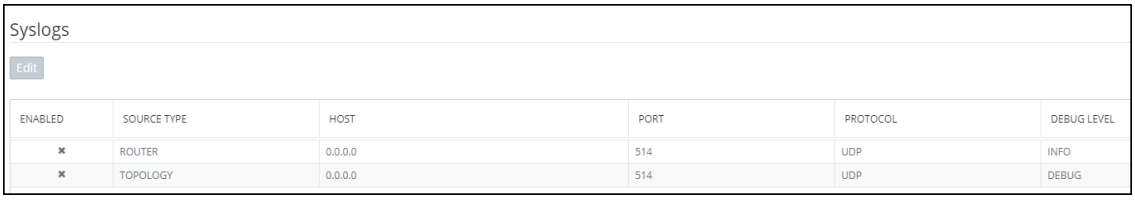
Editing a Syslog Server

The Syslog Server configuration settings can be edited to comply with your requirements.

➢ **To edit a Syslog Server:**

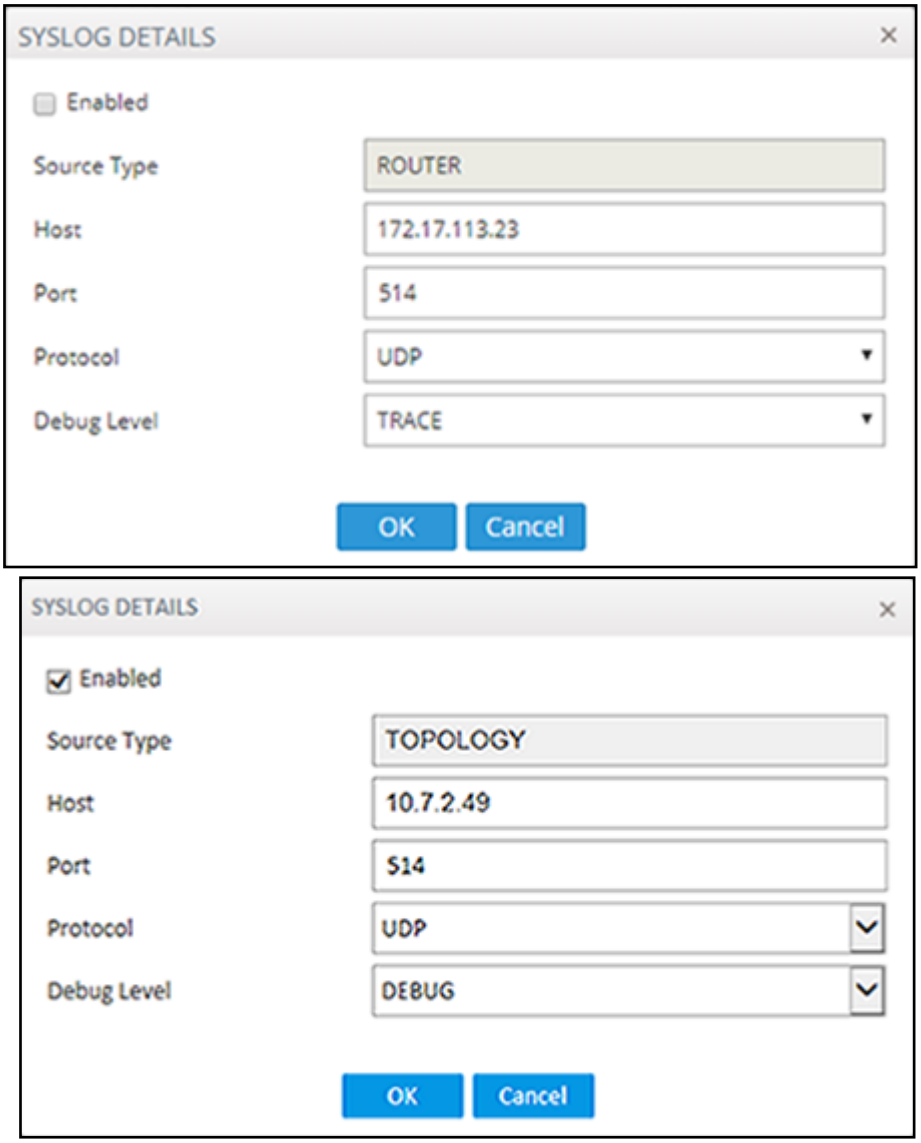
1. Open the Syslogs page (**Settings** > **Network Services** > **Syslog**).

Figure 7-29: Network Services



2. Select the Router or Topology row and then click the enabled **Edit** button.

Figure 7-30: Syslog Details



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	From the 'Debug Level' drop-down menu select either: ■ 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) ■ WARN ■ 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.

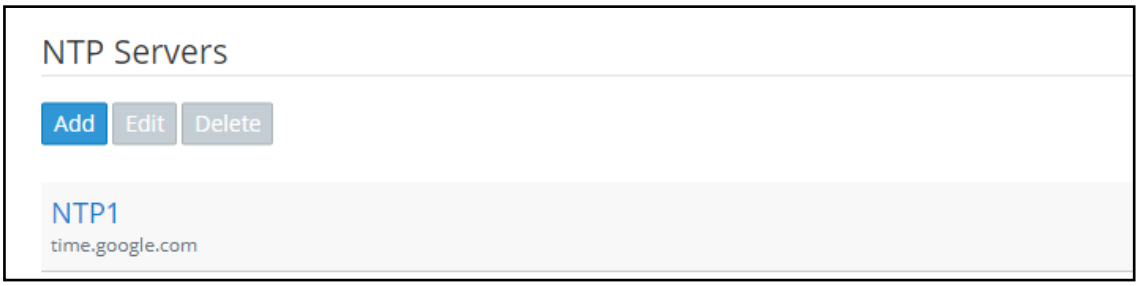
Adding/Editing an NTP Server

An NTP server can be added and its configuration settings edited.

➢ **To add an NTP server:**

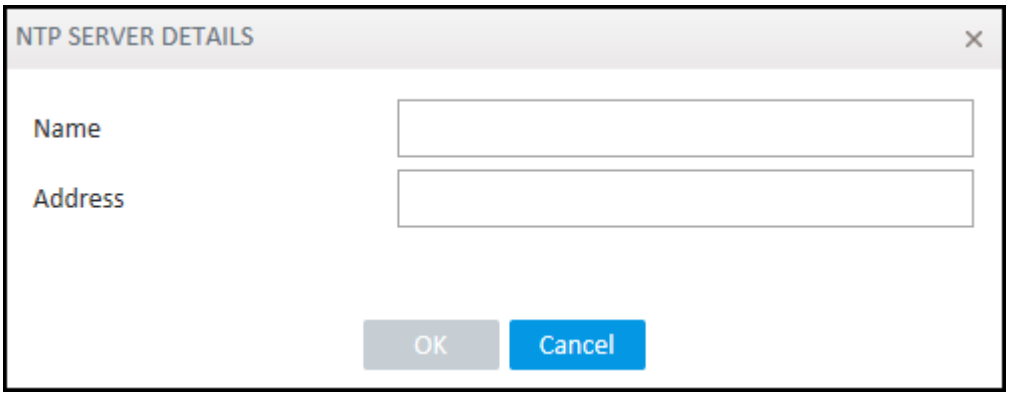
1. Open the NTP Servers page (**Settings** menu > **Network Services** tab > **NTP Servers** item).

Figure 7-31: NTP Servers



2. Click **Add**.

Figure 7-32: 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.

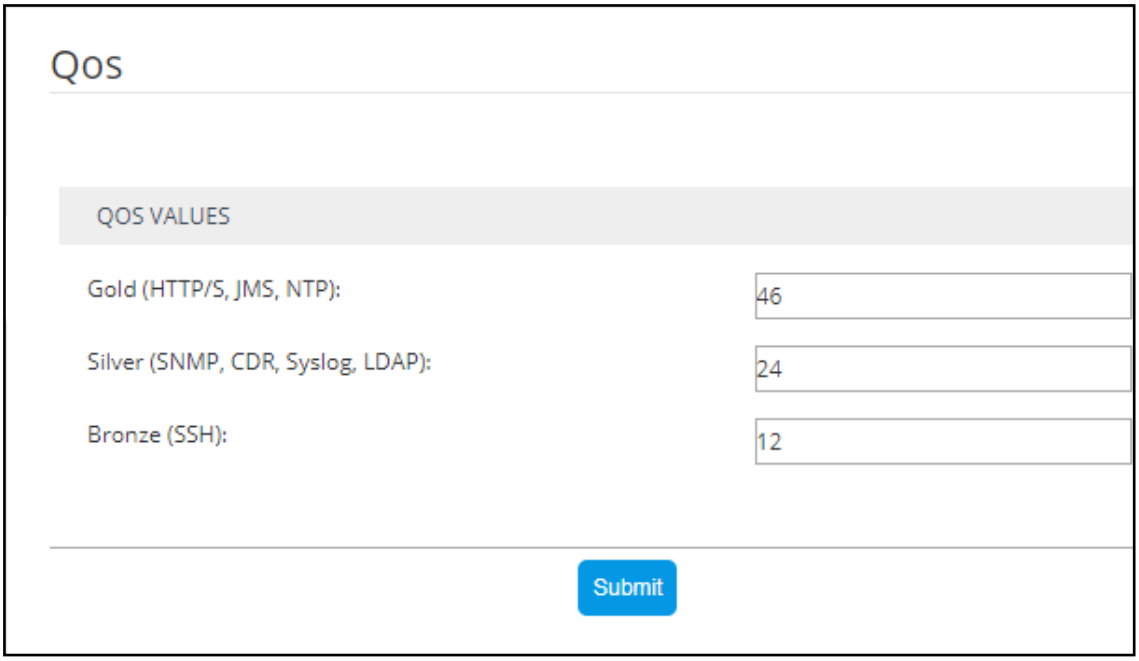
Table 7-14: Protocols Mapped to Class of Service

Application Protocol	Class of Service (Priority)	Traffic Type
HTTP/HTTPs	Gold	■ 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 7-33: QoS



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.

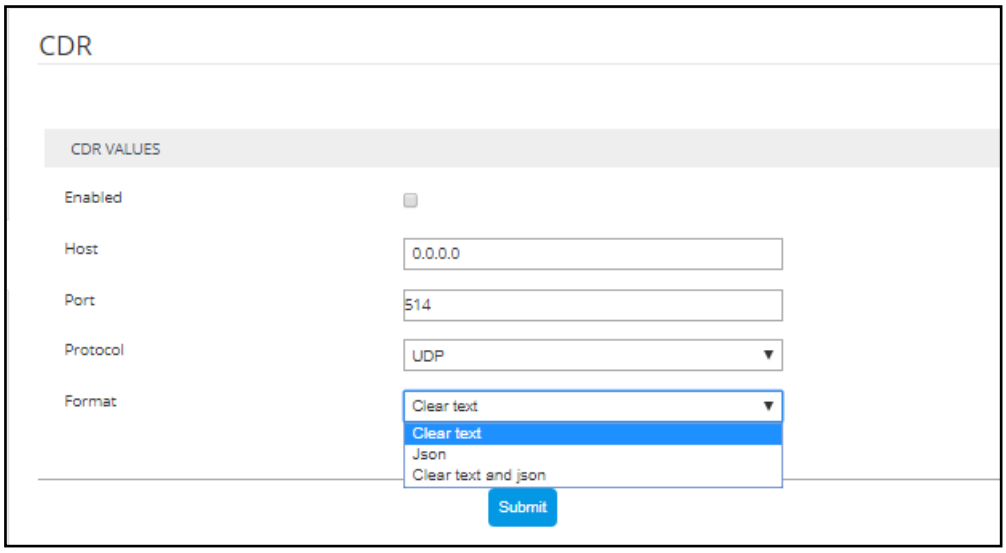
Enabling CDRs

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 7-34: 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 Settings

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 105)
- Normalization before Routing (see Normalization Before Routing on page 107)
- Policy Studio (see Policy Studio on page 108)

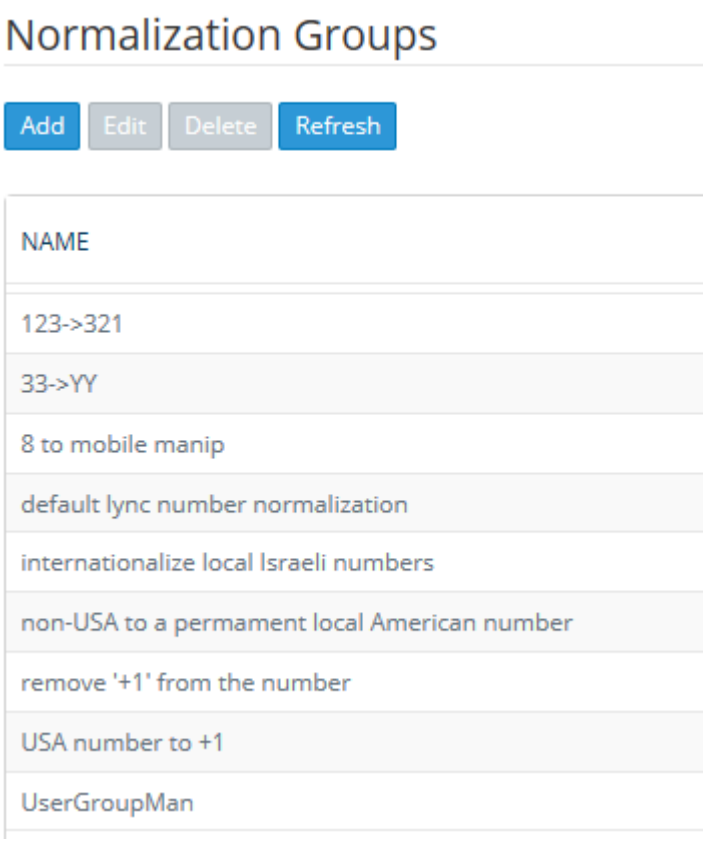
Adding a Normalization Group

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:**

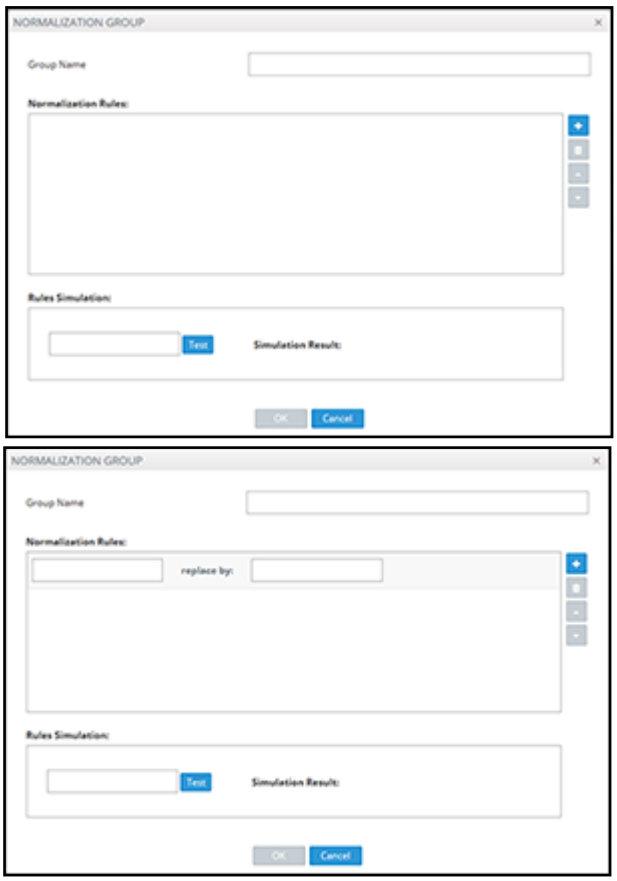
1. Open the Normalization Groups page (**Settings** menu > **Call Flow Configurations** tab > **Normalization Groups**).

Figure 7-35: Normalization Groups



2. Click **Add**.

Figure 7-36: Normalization Groups



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	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 179. 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	Use the rules simulation to test different possible inputs and verify that the regex sequence you entered produces the result you intended. ■ 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 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 30).
- Globally (see Normalization Before Routing on page 107)
- Routing Rule action (see Adding a New Routing Rule on page 133)
- LDAP attribute (see Adding an LDAP Server to the ARM on page 68)

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 133 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.

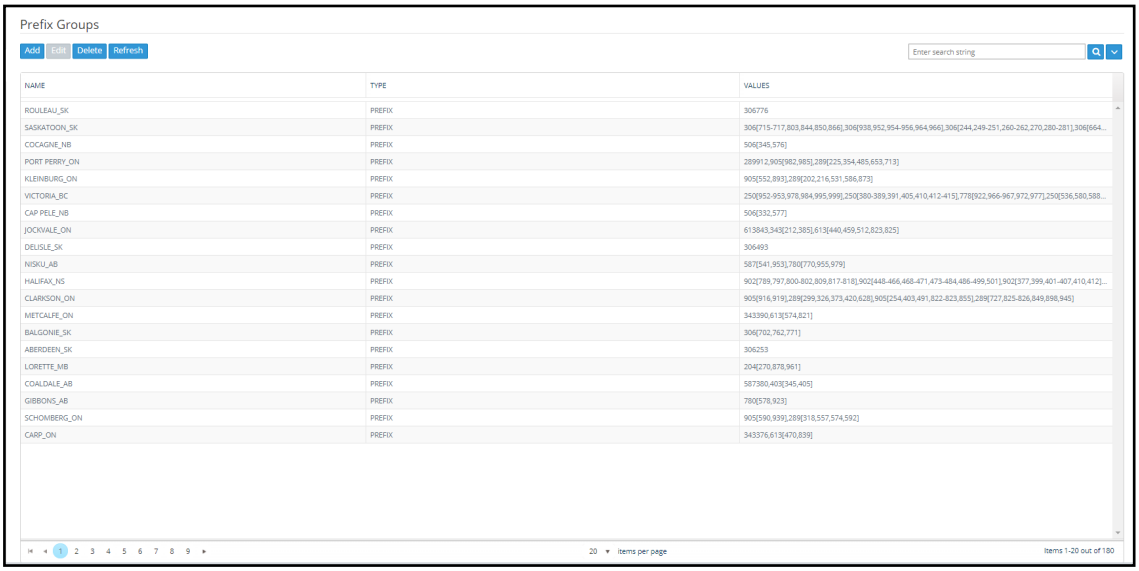
Adding a Prefix Group

The ARM GUI conveniently allows the network telephony operator to add a Prefix Group.

➢ **To add a Prefix Group:**

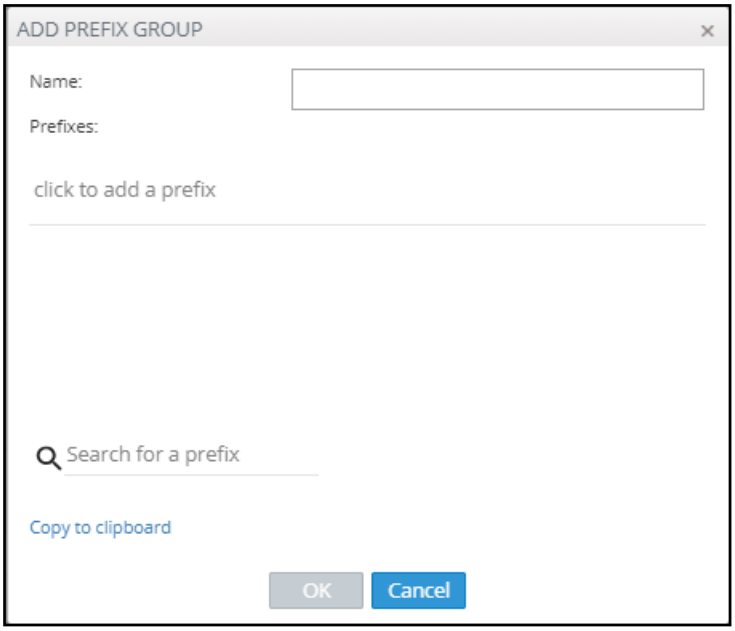
1. Open the Prefix Groups page (**Settings** menu > **Call Flow Configurations** tab > **Prefix Groups** item).

Figure 7-37: Prefix Groups



2. Click the **Add** button.

Figure 7-38: Add Prefix Group



3. 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.
Prefixes	■ Click the field to add a prefix and then enter a single prefix or multiple prefixes: ✔ The syntax for prefixes in a Prefix Group is the same as for a single prefix in a Routing Rule (see Prefixes on page 178 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.

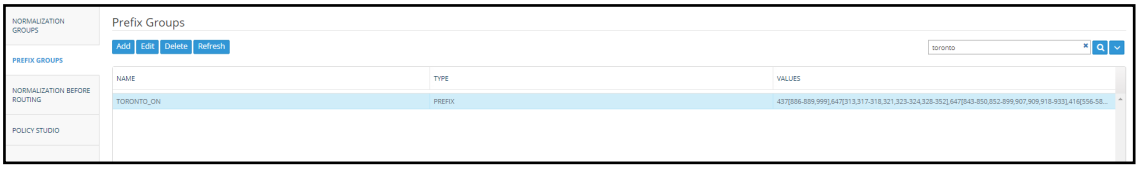
Searching for a Specific Prefix within a Prefix Group

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:**

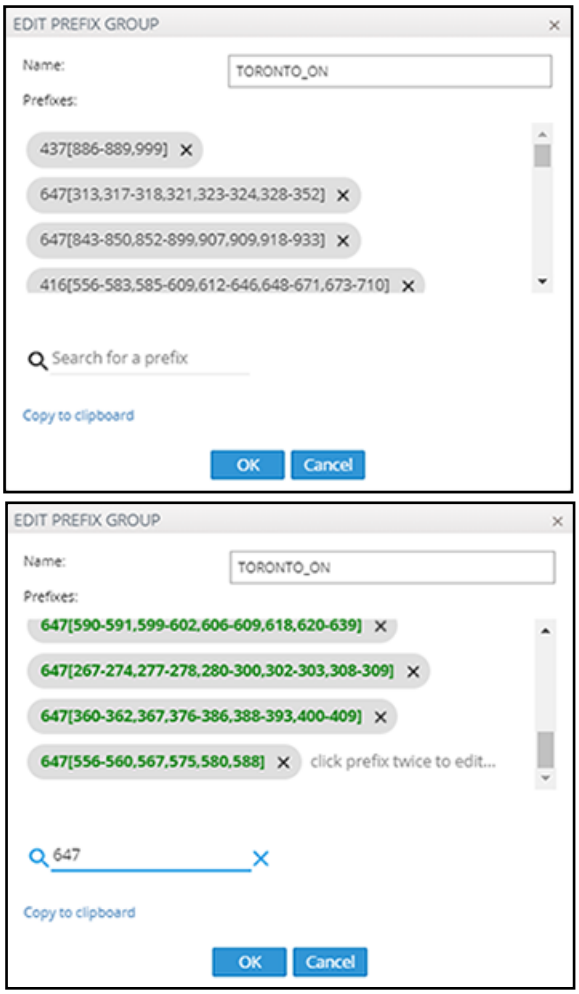
1. In the Prefix Groups page, select the group to search in.

Figure 7-39: Prefix Groups Page



2. Click the activated **Edit** button.

Figure 7-40: Edit Prefix Group – Search for a Prefix



3. 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 178 for more information).

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 103 for information on how to add a normalization rules group.

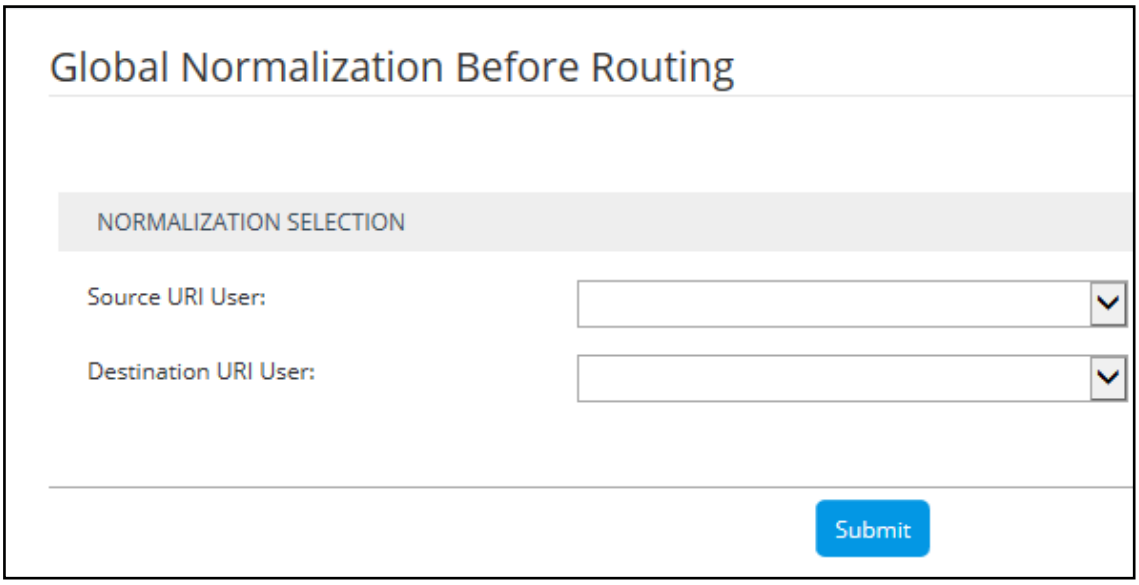
When the ARM receives a routing request, it normalizes the routing request's source user part with the chosen Normalization Group, and the routing request's destination user part with the chosen Normalization Group.

'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 30).

➢ **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 7-41: Normalization Before Routing



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 information to route requests that is not contained in the route requests but is taken from the user table. 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 user table 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.

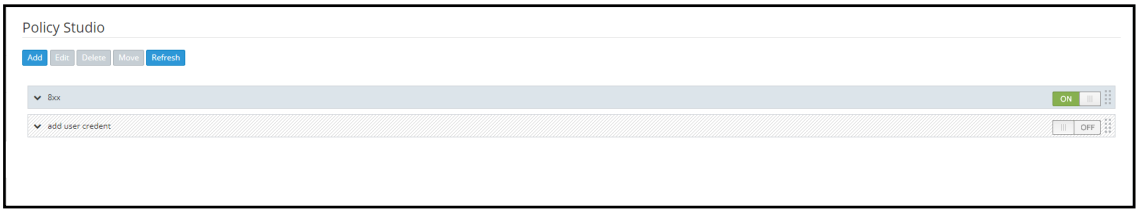
- Same as the previous example but, in addition, there can be more than one user with the same extension, and what differentiates them is their hostname. The ARM can locate the user based on a combination of the extension and hostname attributes.

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:

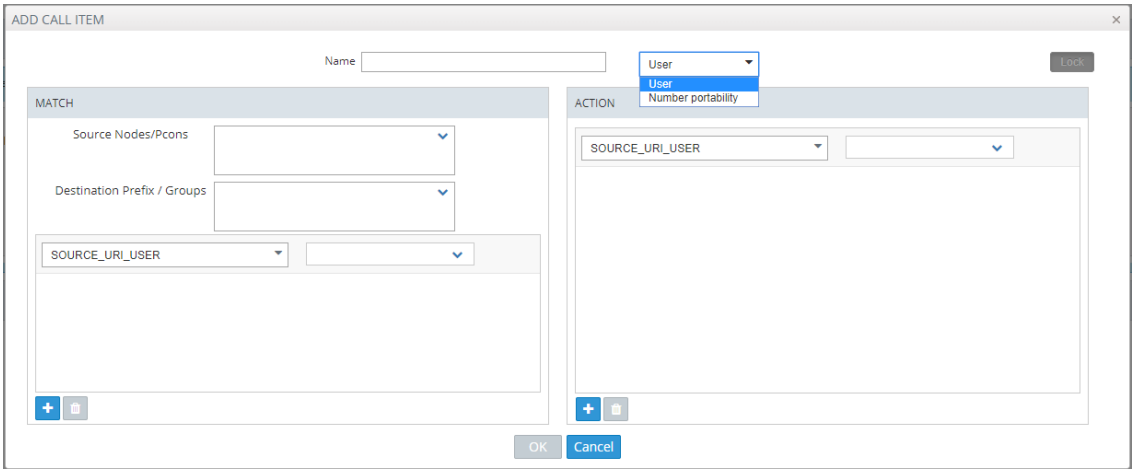
1. Open the Policy Studio page (**Settings** menu > **Call Flow Configurations** tab > **Policy Studio** item).

Figure 7-42: Policy Studio



2. Click **Add**.

Figure 7-43: Add Call Item



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 / Number Portability	Policy Studio supports two uses: ■ User (default). Select this option to use Policy Studio based on information taken from ARM Users Data.

Setting	Description
	■ Number Portability. Select this option to implement Number Portability as a pre-routing Web service. See Web-based Services on page 112 for more information.
MATCH	The set of match conditions for finding a user from the Users table. Click **+** to add more conditions.
Source Nodes / Peer Connections	Select a Node or Peer Connection - or set of Nodes or Peer Connections - for which this rule will be used. If left empty, the rule is used regardless of the origin of the call.
Destination Prefix / Groups	[Optionally] Add an additional condition for users' information-based pre-routing.
Request field	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): ■ SOURCE_URI_USER ■ SOURCE_URI_HOST ■ DEST_URI_USER ■ DEST_URI_HOST ■ CONTACT_URI_USER ■ CONTACT_URI_HOST ■ CONTACT_URI_HOST 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 the next page.
Action	The set of replacement actions that will be performed on the route request and route response fields for a found user.
Action field	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): ■ SOURCE_URI_USER ■ SOURCE_URI_HOST ■ DEST_URI_USER ■ DEST_URI_HOST ■ DEST_IP_ADDR ■ DEST_PORT ■ DEST_PROTOCOL [the P-ASSERTED_IDENTITY_USER will be replaced by company site main number P-ASSERTED_IDENTITY_DISPLAY_NAME] ■ USER_CREDENTIALS_USER_NAME ■ USER_CREDENTIALS_PASSWORD Multiple actions can be defined. Click **+** to define another action.

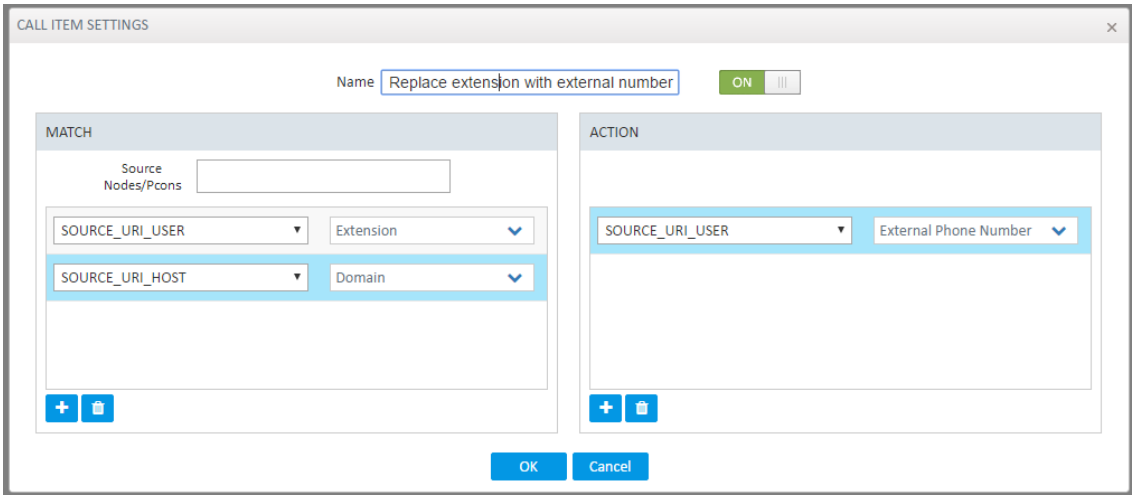
Setting	Description
	Note: If either USER_CREDENTIALS_USER_NAME *or* USER_CREDENTIALS_PASSWORD is used in an action, you must add *both*. For a SIP field manipulation example, see Example 2 under Example 2 of a Policy Studio Rule below.
Request User Property	Select a set of user properties. The request 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.
Replacement User Property	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.

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, ARM will search for a user whose *extension* property is equal to the value of the SOURCE_URI_USER field and whose *domain* property is equal to the SOURCE_URI_HOST field.
- ARM will then replace the SOURCE_URI_USER field with the value of the found user's *external phone number* property.

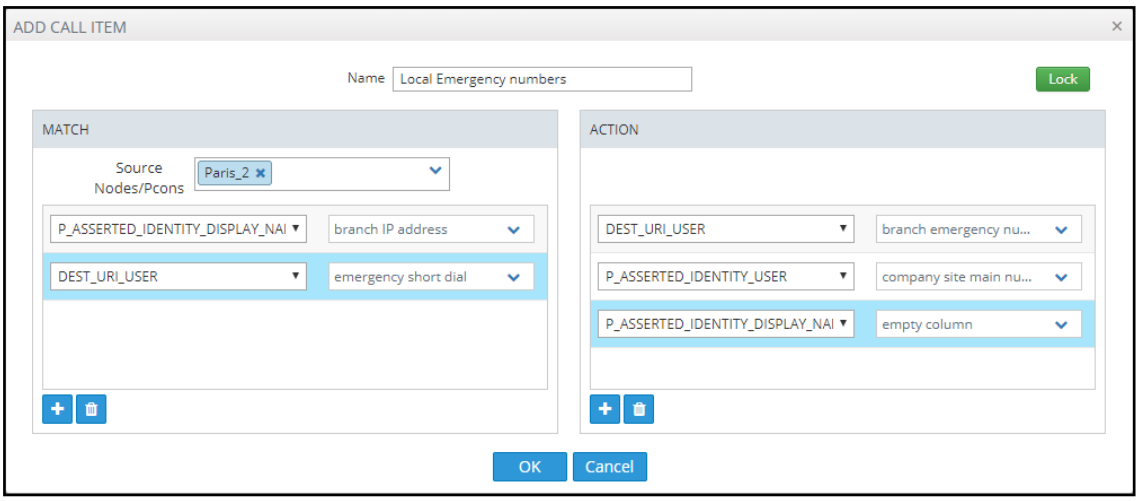
Figure 7-44: Policy Studio Rule Example 1



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 7-45: 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*

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.

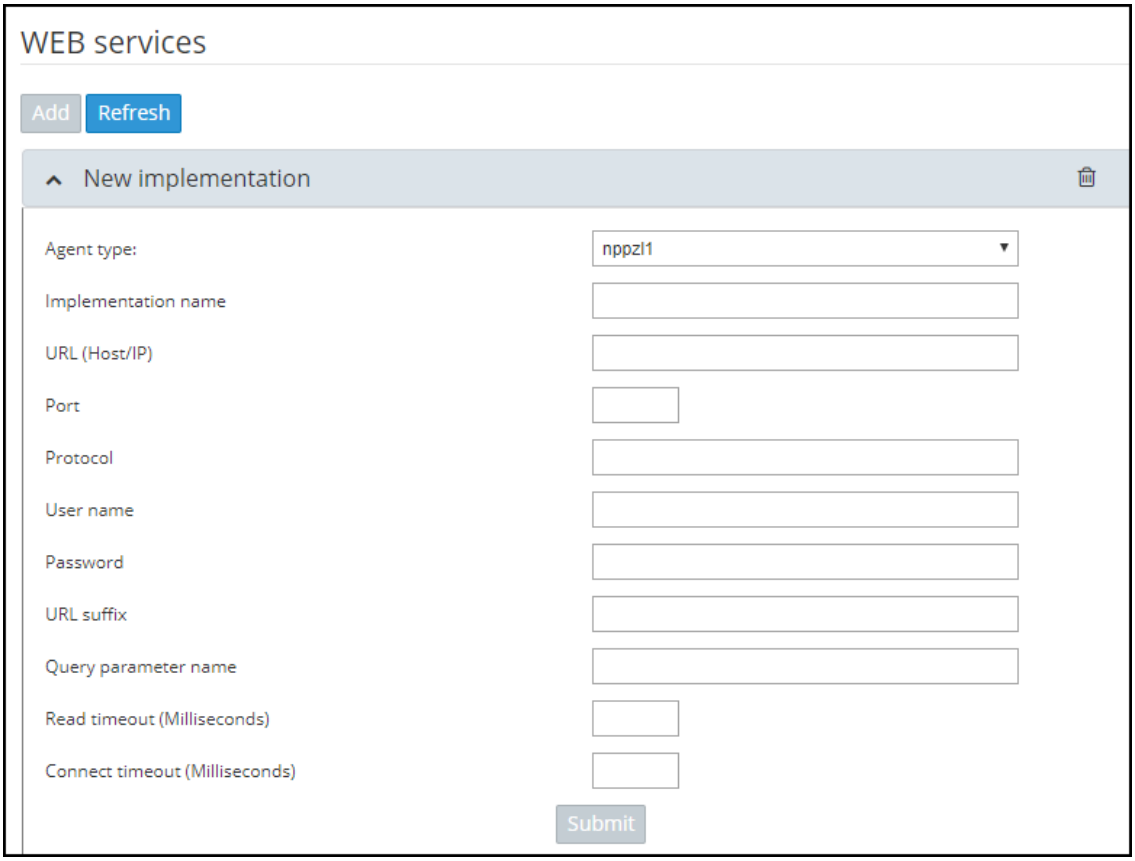
- The feature is invisible in the ARM *unless enabled in the License Key*.
- The feature can conform to any protocol or design using a plug-in which AudioCodes will provide *per the protocol required by the customer*.

➢ To configure a Web service:

1. Open the Web Services page (**Settings** > **Call Flow Configurations** > **Web Services**)

Figure 7-46: Web Services

2. Click **Add**.

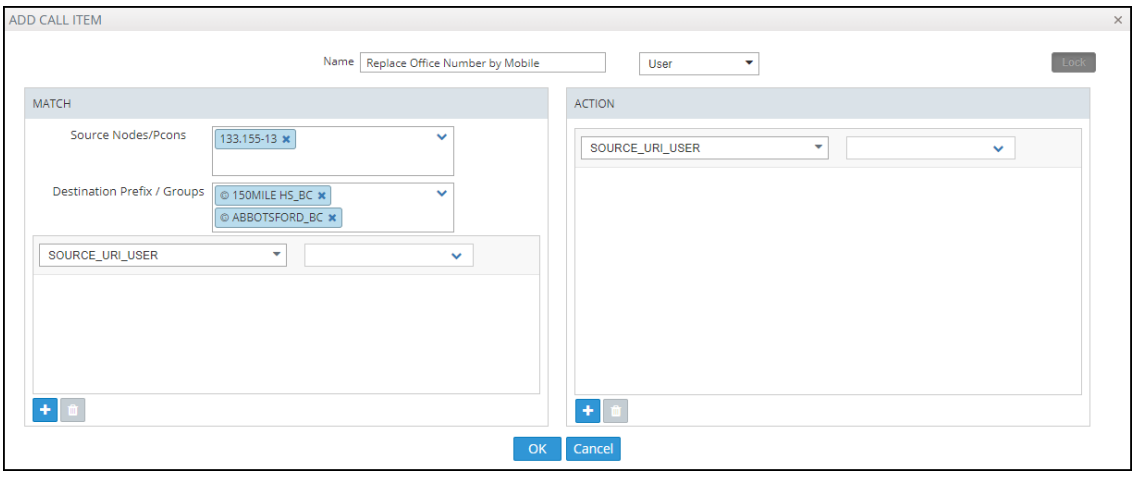


3. Configure the Web service you require in the New Implementation screen.

> 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. Click **Submit**.
5. Apply the service: Open the Policy Studio (**Settings** > **Call Flow Configurations** > **Policy Studio**) and click **Add**. See also Policy Studio on page 108.

Figure 7-47: Policy Studio - Add Call Item



6. Select number portability as shown in the preceding figure. The default is **User** to preserve the existing functionality of Policy Studio.
7. Number Manipulation can be applied to specific conditions (see under MATCH in the preceding figure):

- Source Nodes and/or Peer Connections

and

- Specific Destination Prefixes or Prefix Groups

Routing Settings

Configuring Criteria for a Quality Profile

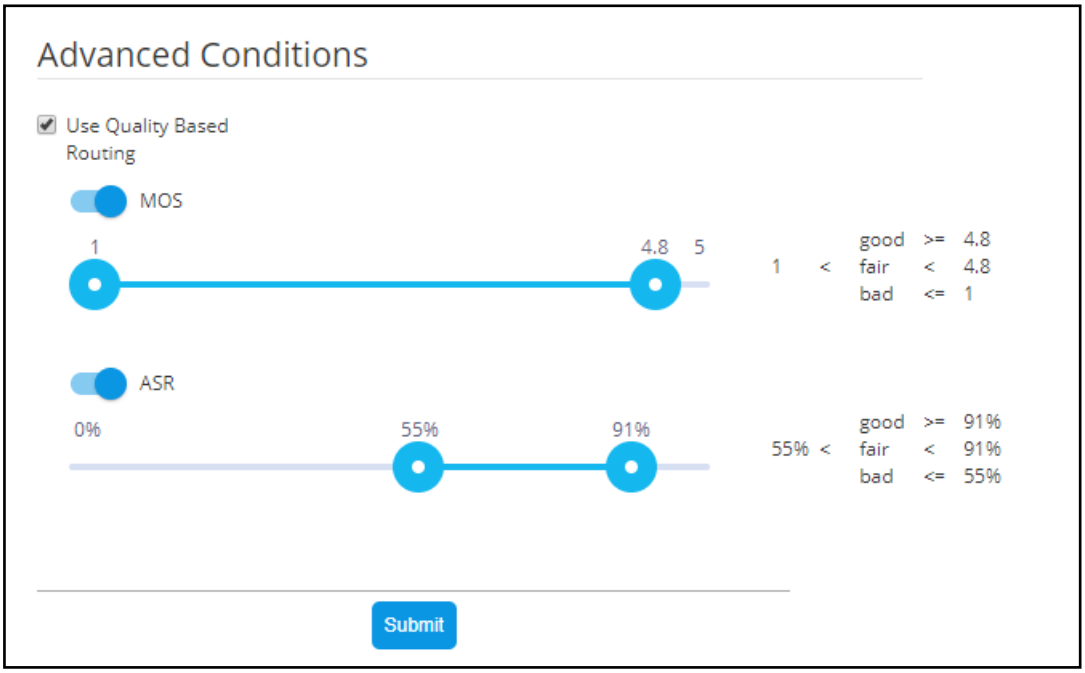
You can configure criteria for a quality profile for bad, fair or good call paths based on the calculation of MOS and ASR. You can configure a specific Peer Connection to exclude either the MOS or the ASR criterion (see Peer Connection Information and Actions on page 30). After enabling 'Use Quality 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 133) 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 7-48: Configuring Criteria for a Quality Profile



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)	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. 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. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects.
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 133).

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 133 under 'Advanced Conditions').

➢ To configure a time-based routing condition:

1. Open the Time-Based Routing screen (**Settings** > **Routing** > **Time Based Routing**).

Figure 7-49: Time Based Routing

2. Add a time-based routing condition: Click **Add**; the Time Condition screen is displayed.

Figure 7-50: Time Condition

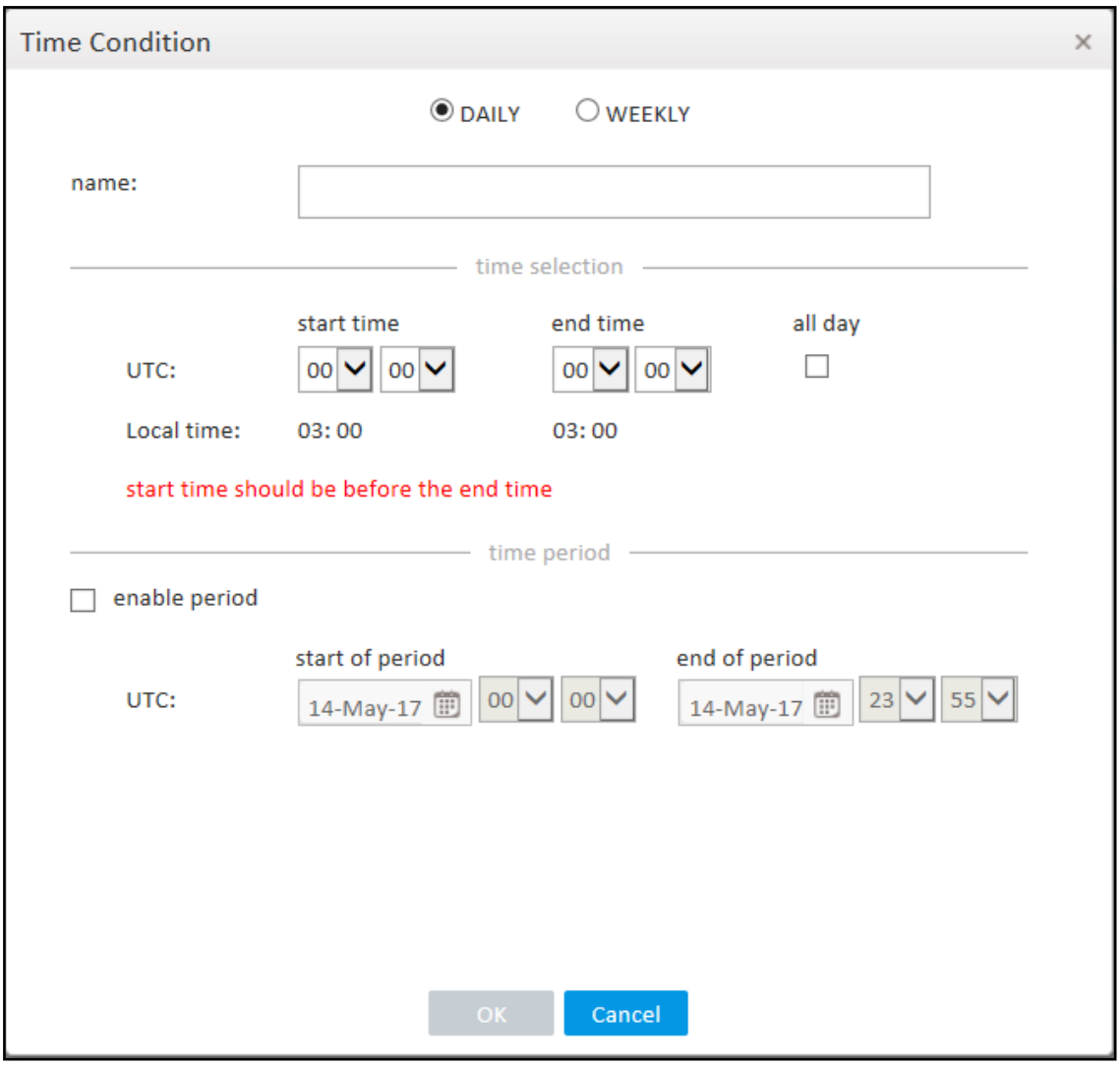
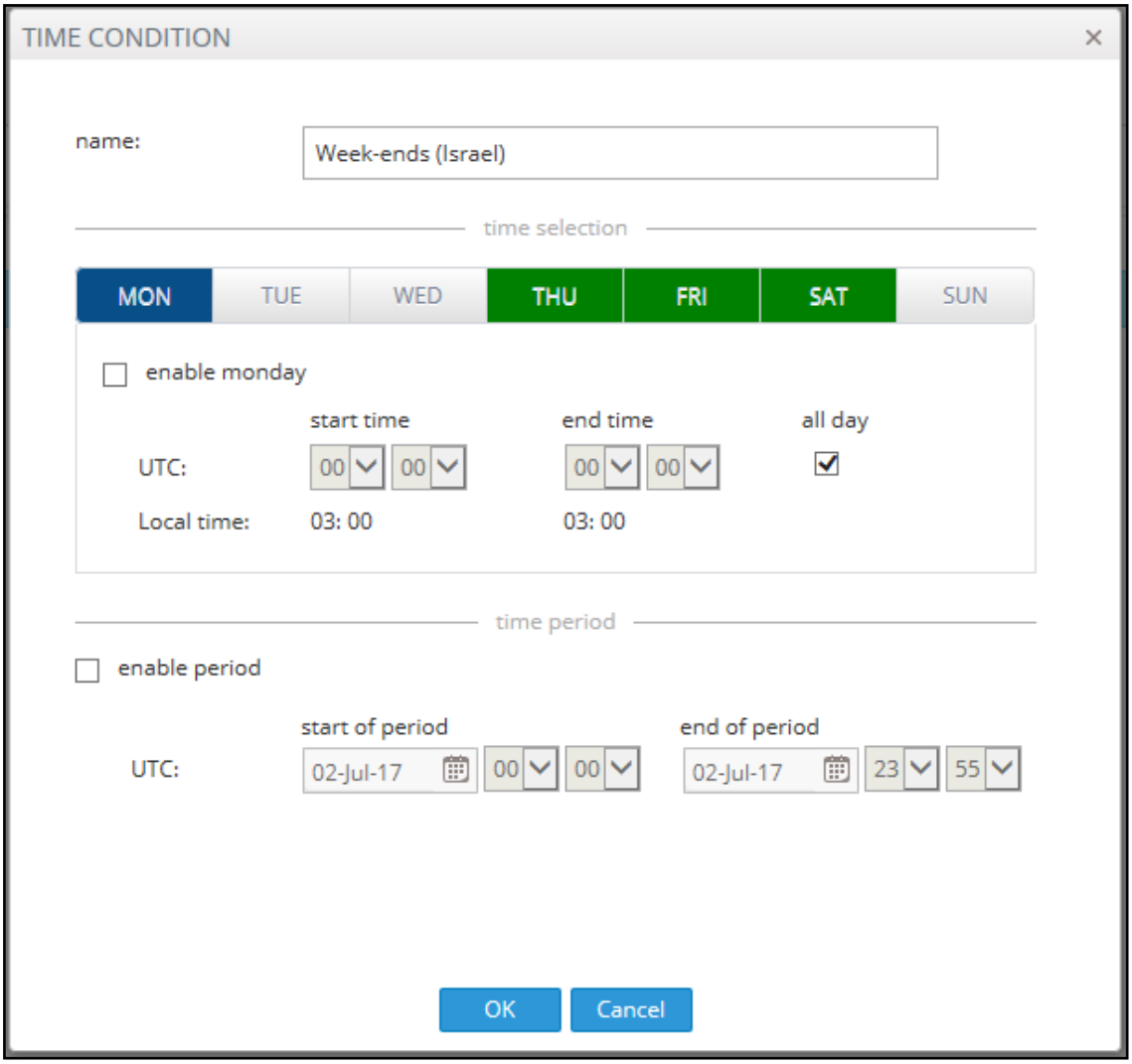


Figure 7-51: Time Condition - Example



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	Select either Daily or Weekly. Daily - This is a daily recurring period. Weekly - This is a period recurring on given days of the week. The figure above shows a configured weekly condition. Green 'day' button: activated on that day. Blue 'day' button: selected to configure it.
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. 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.

Time Condition	Description
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.

4. Click **OK**; a profile is generated which you can associate with a Routing Rule (see Adding a New Routing Rule on page 133 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 SIP Alternative Route Reason

The ARM operator can configure SIP responses in the SIP Alternative Route Reason page, which will cause the ARM to apply alternative routing paths if available.

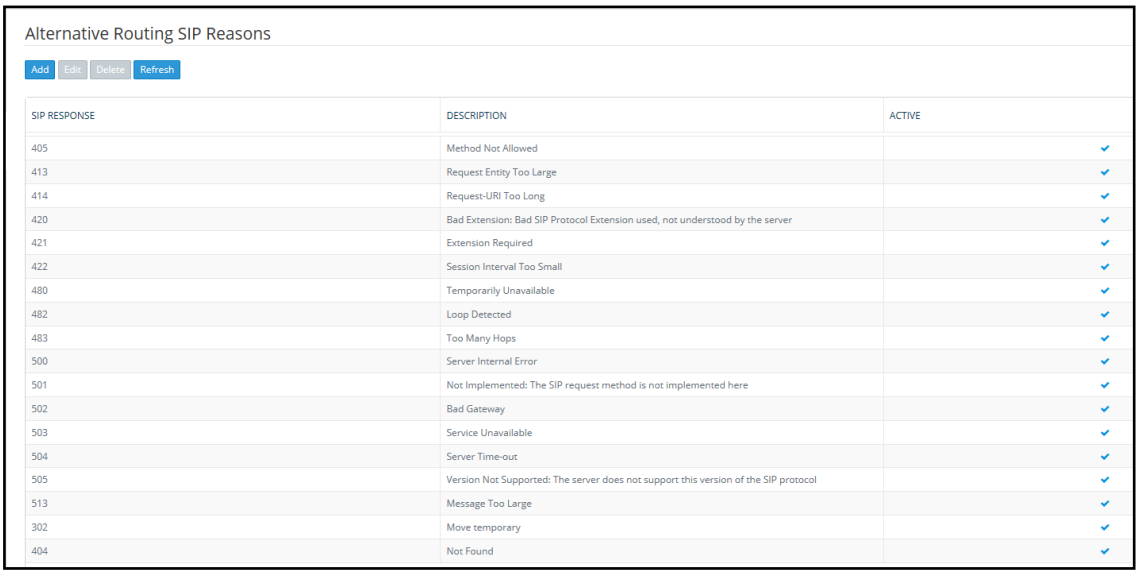
If a call fails and the SIP response received from the remote side is not configured in the SIP Alternative Route Reason page, the ARM will not apply an alternative route for the call.

The page allows operators to change the default ARM behavior for an Alternative Routing decision.

➢ To configure a SIP Alternative Route Reason:

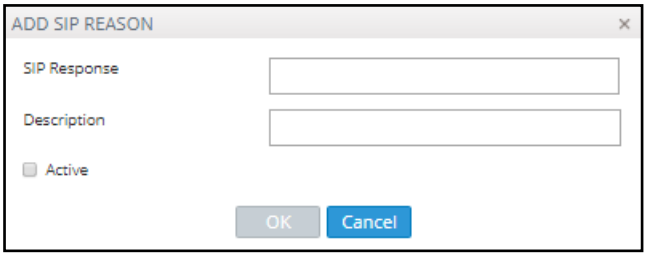
1. Open the Alternative Routing SIP Reasons page (**Settings** > **Routing** > **Alternative Routing SIP Reasons**).

Figure 7-52: Alternative Routing SIP Reasons Page



2. Click the **Add** tab.

Figure 7-53: Adding an Alternative Routing SIP Reason



3. Enter the SIP Response number (200-600).
4. Provide a description of the reason.
5. Select the **Active** option to activate the configuration.
6. Click the now-enabled **OK** button.

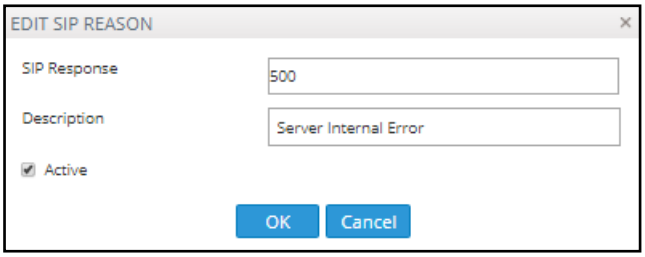
➢ To edit a SIP Alternative Route Reason:

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 7-54: Editing an Alternative Routing SIP Reason



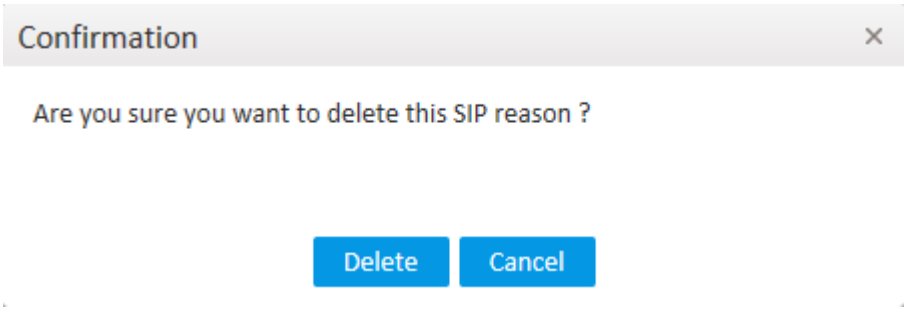
3. Edit per your requirements and click **OK**.

> 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 a SIP Alternative Route Reason:

1. In the Alternative Routing SIP Reasons screen, select the SIP response to delete.

Figure 7-55: Deleting an Alternative Routing SIP Reason



2. Click **Delete**.

Configuring Global Routing Settings

The ARM enables global routing settings to be configured.

➢ **To configure global routing settings:**

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

Figure 7-56: Global Routing Settings

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

Table 7-23: Routing Settings

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.

3. Click **Submit**.

Adding a Routing Server

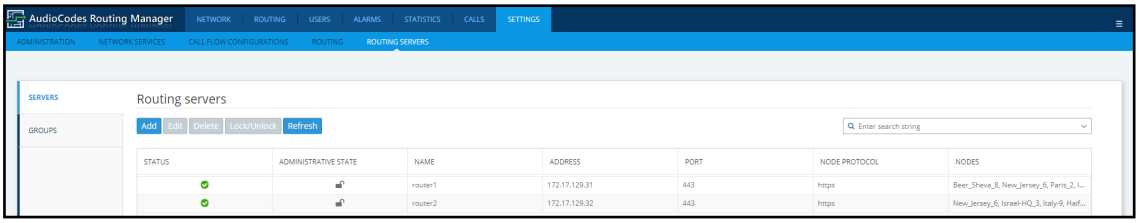
A Routing Server can be added to the ARM for handling calls coming from SBCs and Gateways.

- 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 21 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:

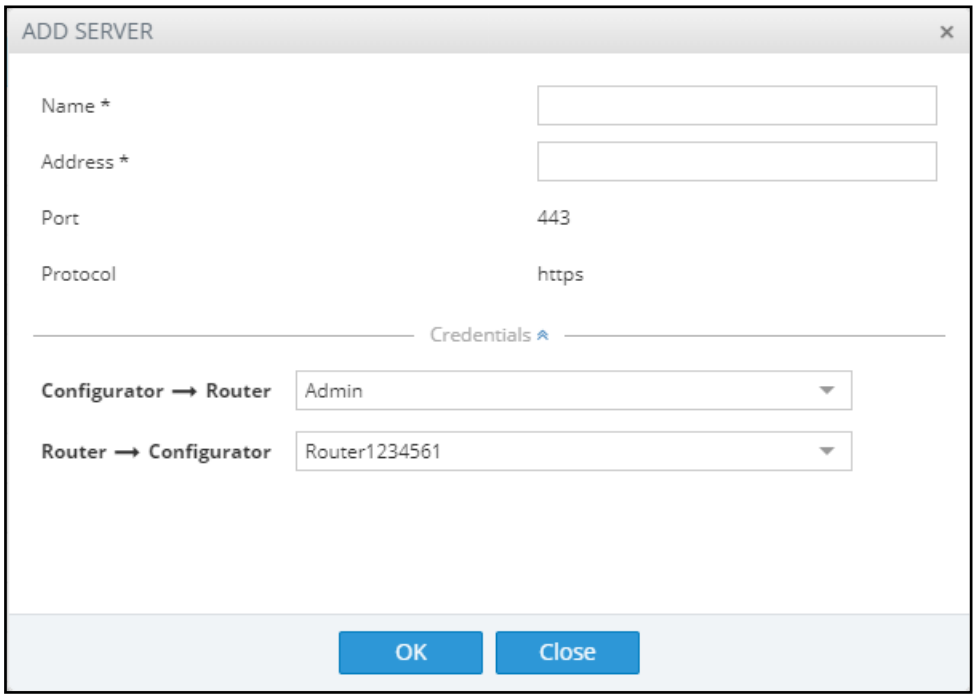
1. Open the Routing Servers page (**Settings** > **Routing Servers**).

Figure 7-57: Routing Servers



2. Click **Add**.

Figure 7-58: 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 7-24: 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.

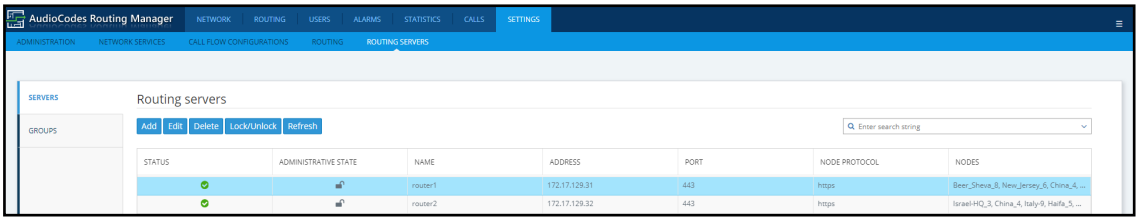
Editing a Routing Server

After a routing server is added to the ARM, its configuration can be edited if necessary.

➢ To edit a Routing Server:

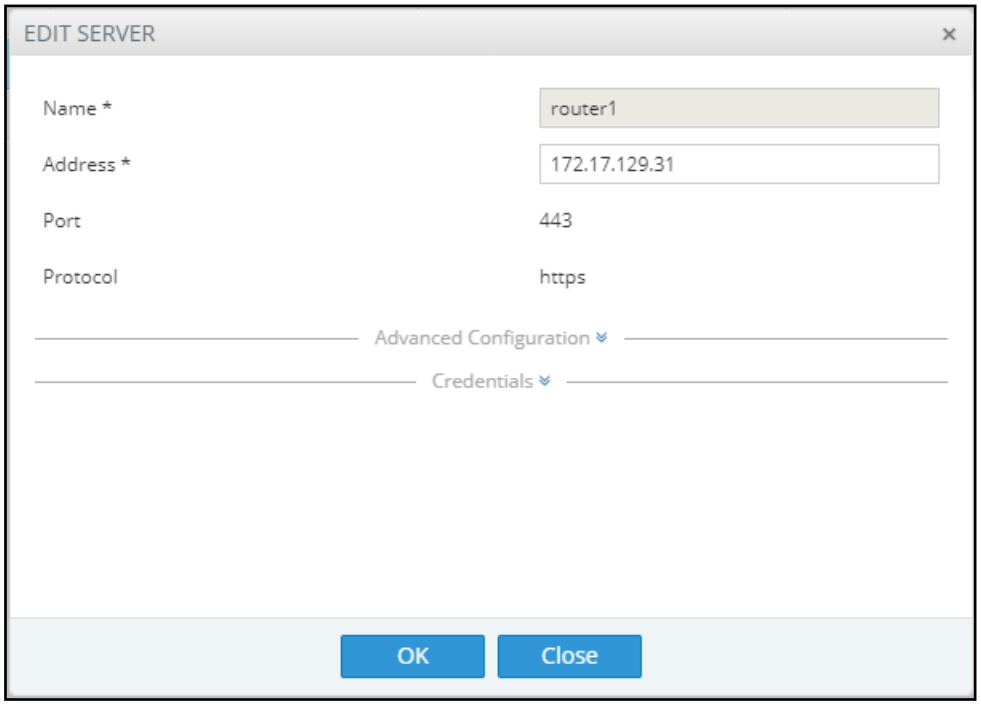
1. Open the Routing Servers page (**Settings** > **Routing Servers**).

Figure 7-59: Routing Servers



2. Select the row of the routing server to edit, and then click **Edit**.

Figure 7-60: Edit Server



3. Edit the server using the following table as reference.

Table 7-25: 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	
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

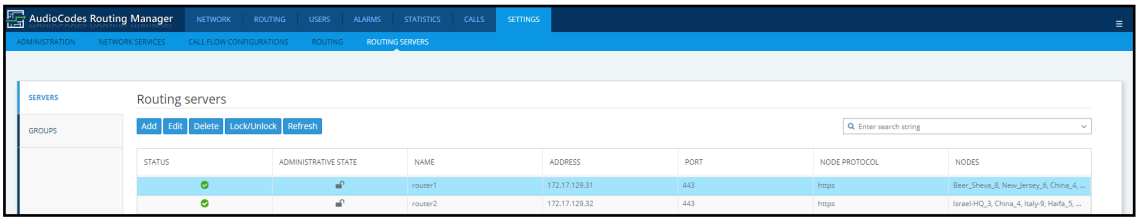
The ARM allows users to lock routing servers, for troubleshooting or maintenance purposes. Locking a routing server causes the devices to disconnect from the locked routing server, causing all traffic to divert to the other unlocked and available servers. Unlocking a routing server causes the devices 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 7-61: Routing Servers - Administrative State



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.

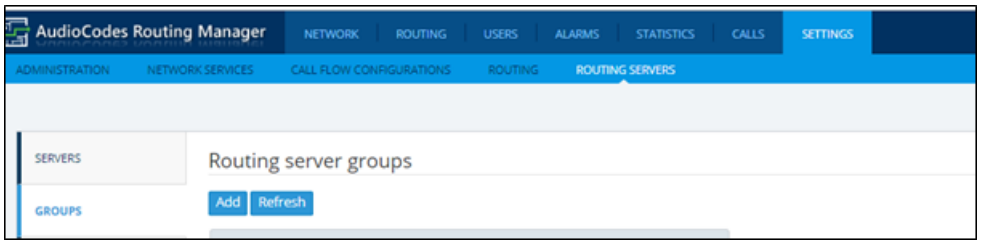
Adding a Routing Server Group with Internal and External Priorities

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:

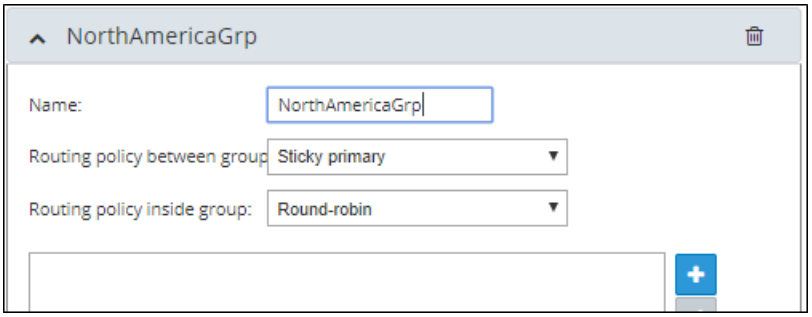
1. Open the 'Routing server groups' page (**Settings** > **Routing Servers** > **Groups**).

Figure 7-62: Routing Server Groups



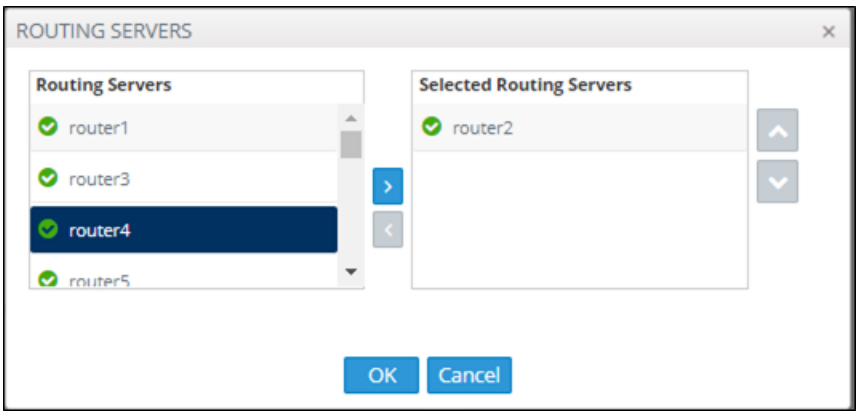
2. When prompted, configure the:
   - Name of the group to be attached to a node or to multiple nodes
   - Routing Policy to be applied between groups; 'Sticky primary' is the default. Two routing policies between Routing Groups are available:
     - 'Sticky primary' [the node reverts to the primary 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 7-63: Routing Policy Options



4. Attach one or more ARM Routing Servers to the Routing Group.

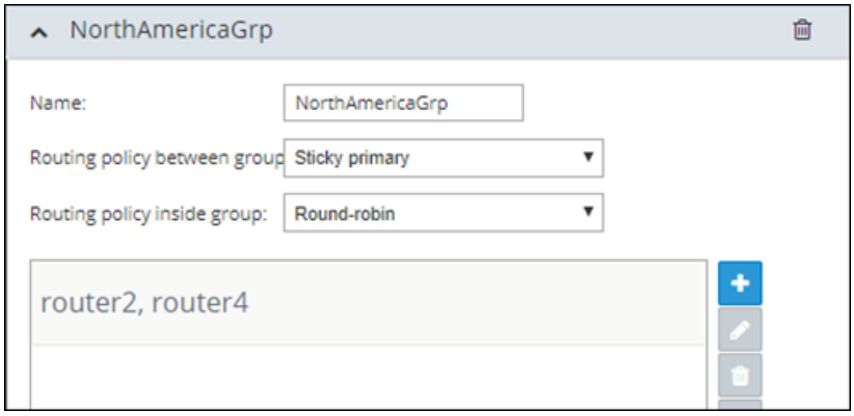
Figure 7-64: Attaching Routing Server/s to a Routing Group



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 **+**.

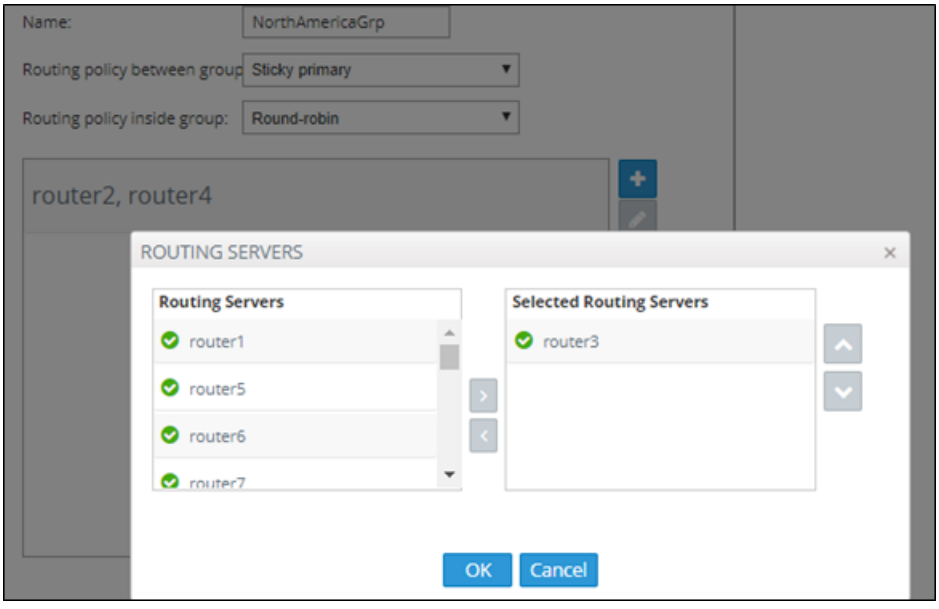
> The maximum number of routing servers allowed for the entire server group is 10, so if you have five sub-groups, each can have up to two routing servers inside).

Figure 7-65: Multiple Sub-Groups of Routing Servers



6. Configure a new sub-group of routers with the same Routing Policy inside the group.

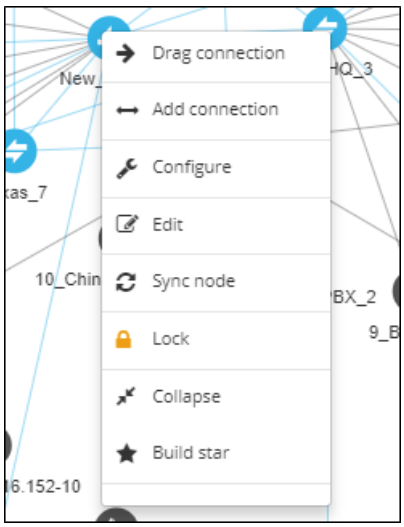
Figure 7-66: Sub-Group of Routing Server with the Same Routing Policy



Up to five sub-groups can be configured under the same Name.

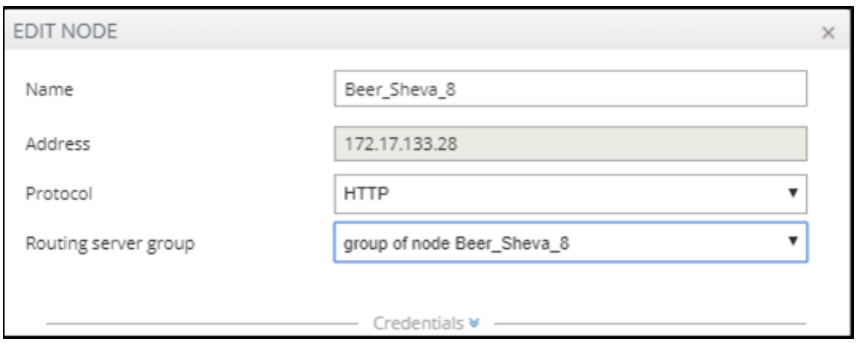
7. After configuring an ARM Routing Servers group, attach it to a single node or to multiple nodes (SBCs or Gateways). To do this, apply an **Edit** action on the node.

Figure 7-67: Edit Node



8. From the drop-down, select the Routing Server Group (one of the previously configured groups).

Figure 7-68: Edit Node – Selecting Routing Server Group



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 page ('Routing' menu); the page opens under the **Routing Groups** tab by default.

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 133)
3. Test the route (see Testing a Route on page 47)

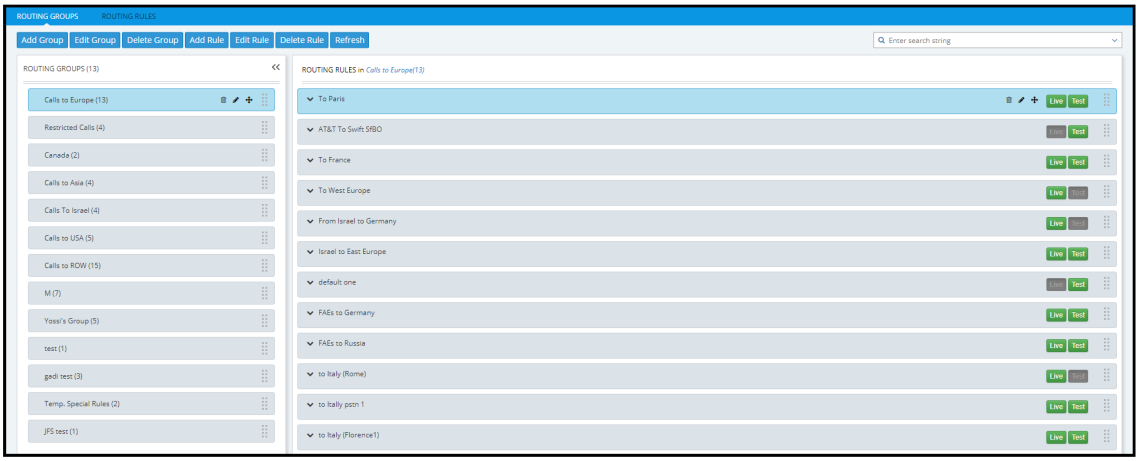
Adding a Routing Group

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:**

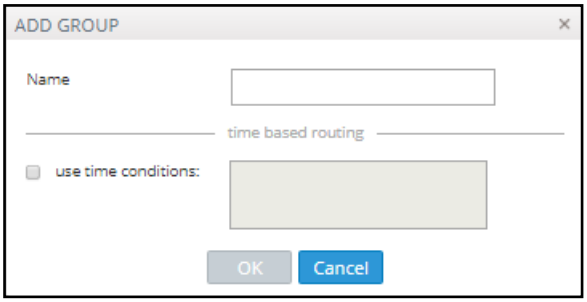
1. In the Routing page under the **Routing Groups** tab, click **Add Group**.

Figure 8-2: Add Group



The Add Group screen opens.

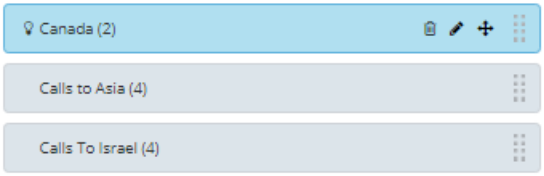
Figure 8-3: Add Group



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 1-999 characters.

3. Select the **use time conditions** option to attach a time condition to the Routing Group. See Configuring a Time-Based Routing Condition on page 115 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. Note that if you attach a time condition to a group, it's indicated visually in the Routing Groups page as follows:



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.

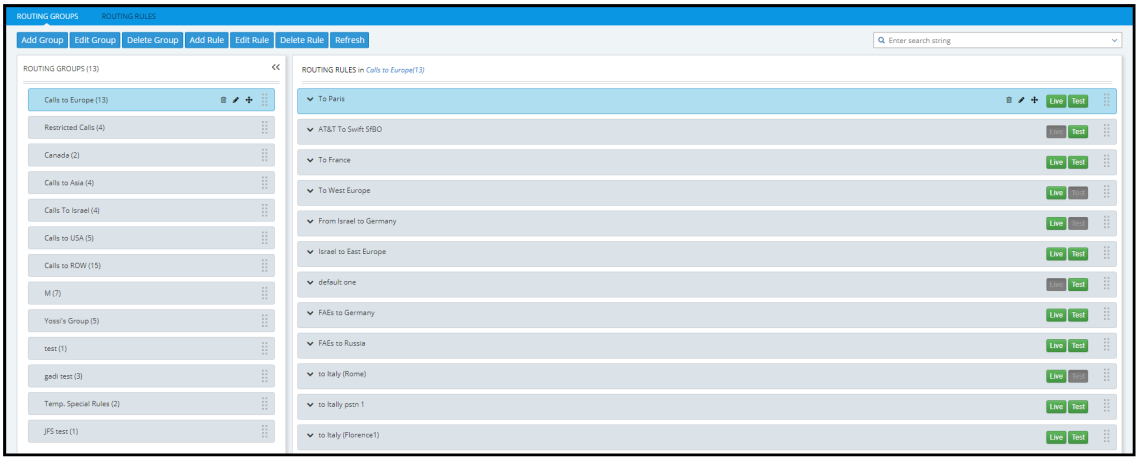
Editing a Routing Group

You can edit a Routing Group if necessary.

➢ **To edit a Routing Group:**

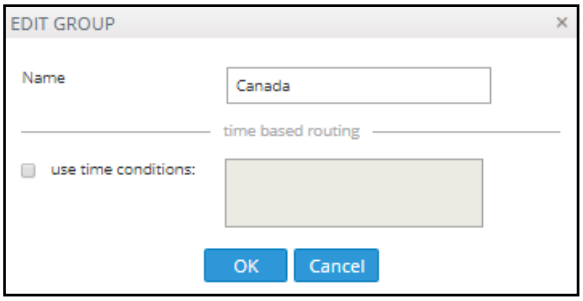
1. In the Routing page under the **Routing Groups** tab, select the Routing Group to edit, and then either:
   a. Click **Edit Group**

Figure 8-4: Edit Group



b. [Alternatively] Click the group's edit icon in the row

Figure 8-5: Edit Group



2. Edit the 'Name' field. Enter a user-friendly name to facilitate intuitive management by network administrators.
3. Edit the time condition. You can clear the **use time conditions** option to remove the condition. See Configuring a Time-Based Routing Condition on page 115 for related information. You can alternatively remove a single condition if multiple time conditions are attached.
4. Click **OK**.

Moving a Routing Group

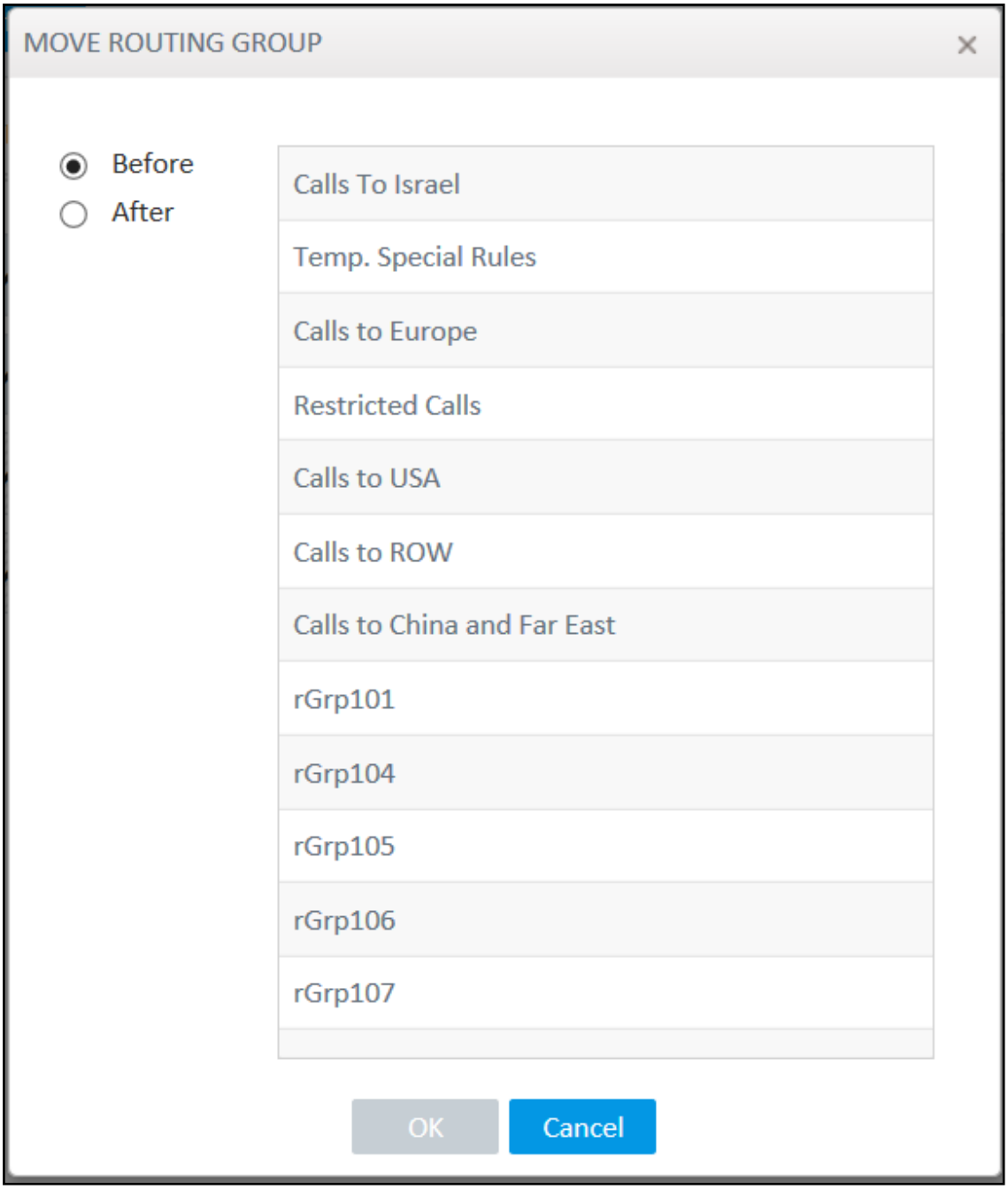
You can promote or demote a Routing Group listed in the Routing Groups page. When moving a Routing Group, all its Routing Rules are moved and the routing priority of all the Routing Rules in the group are collectively changed at once. Routing Groups listed higher in the page take precedence over those 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 8-6: Move Routing Group



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 8-7: Moving a Routing Group by Dragging and Dropping

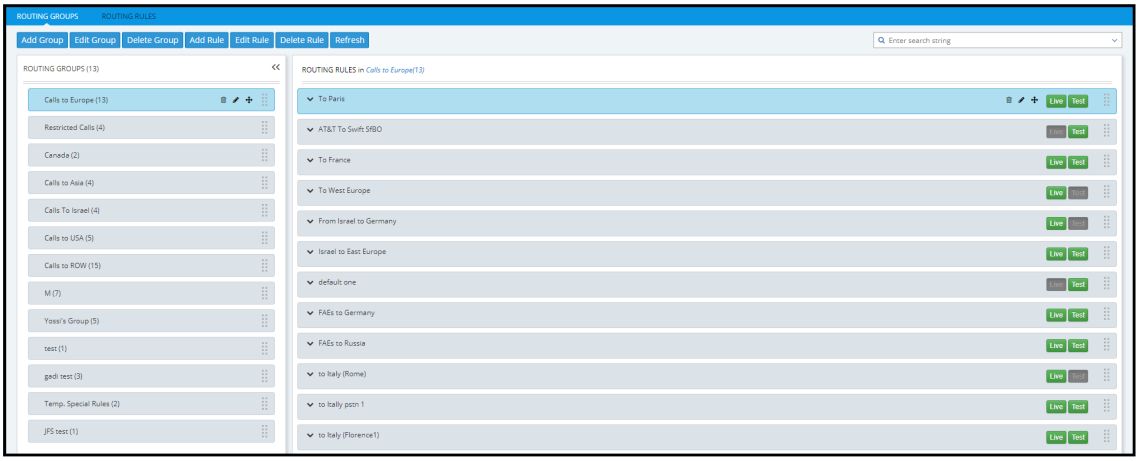
Deleting a Routing Group

You can delete a Routing Group if necessary, including rules associated with the group.

➢ To delete a Routing Group:

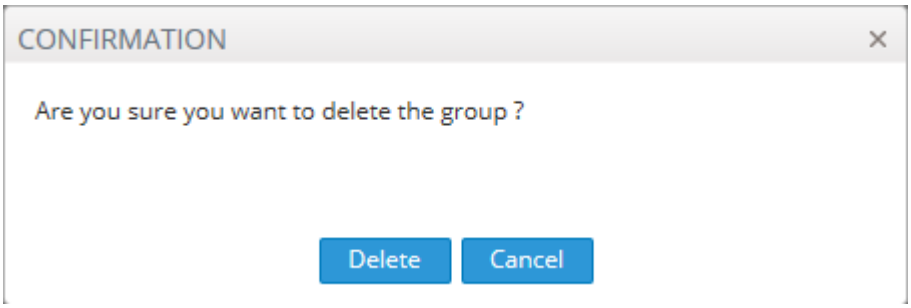
1. In the Routing page under the **Routing Group** icon, select the Routing Group to delete and then either:
   a. Click **Delete Group**:

Figure 8-8: Delete Routing Group



-or-

   b. Click the **Delete** icon in its row which is then enabled. You're prompted to confirm:



2. Click **Delete**.

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 8-9: Example of a Routing Rule

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 devices and Connections/Peer Connections 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 (Node, Peer Connection, VoIP Peer), if available.
- ARM attempts to build an alternative action (Node, Peer Connection, VoIP Peer), if available, for this call, in the order that actions are listed in the Routing Rule.
- All routing alternatives are sorted by weighted path, cost and then by number of hops.

Load Balancing

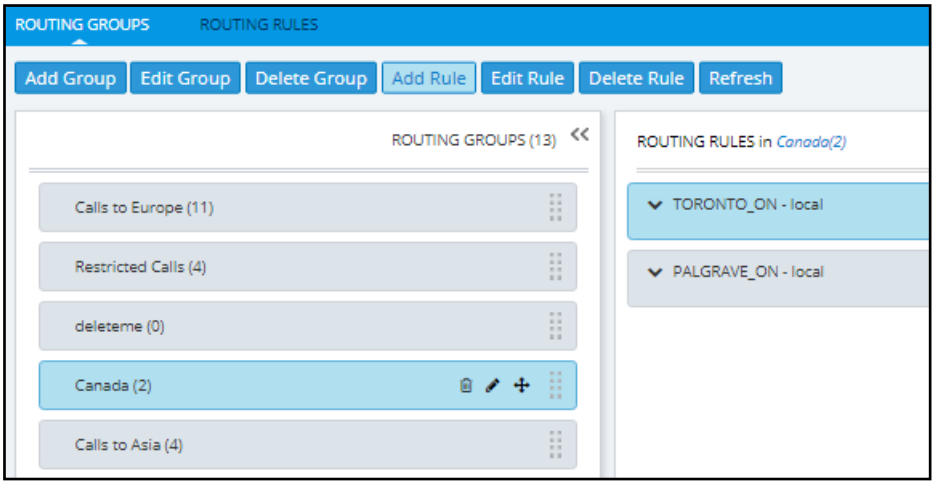
The ARM can balance call traffic between multiple destinations of the same Action. Call traffic can be distributed equally between destinations, or the distribution can be defined by the operator. Multiple routing attempts can be configured. Default: 1. Max: 3. The max can't exceed the number of destinations 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.

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:

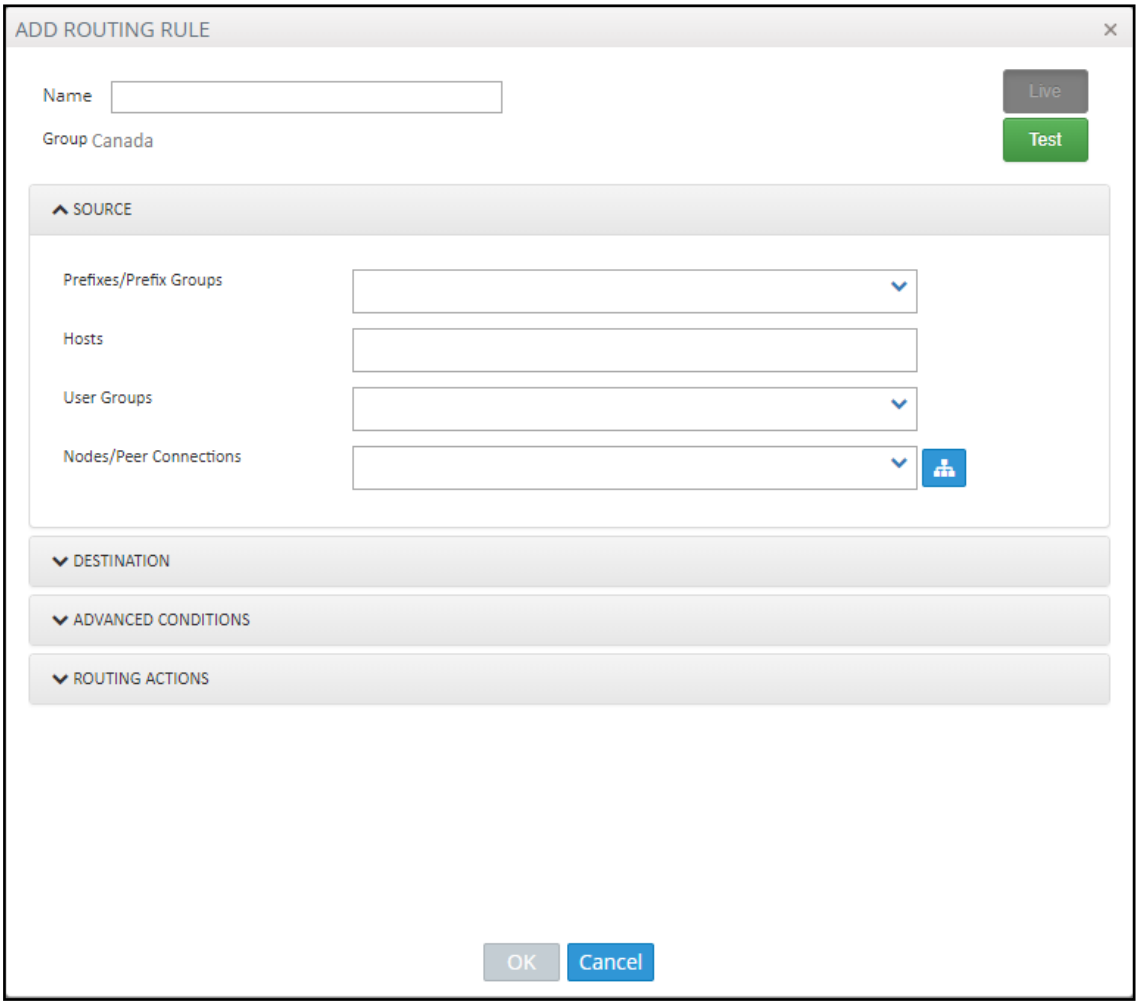
1. In the Routing Groups page under the **Routing Groups** tab, select the Routing Group with which to associate the rule, and then click **Add Rule**.

Figure 8-10: Add Rule



This screen opens:

Figure 8-11: Add Routing Rule



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 1-999 characters.
3. Enable **Live** and/or **Test** mode. See Testing a Route on page 47.
   - **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

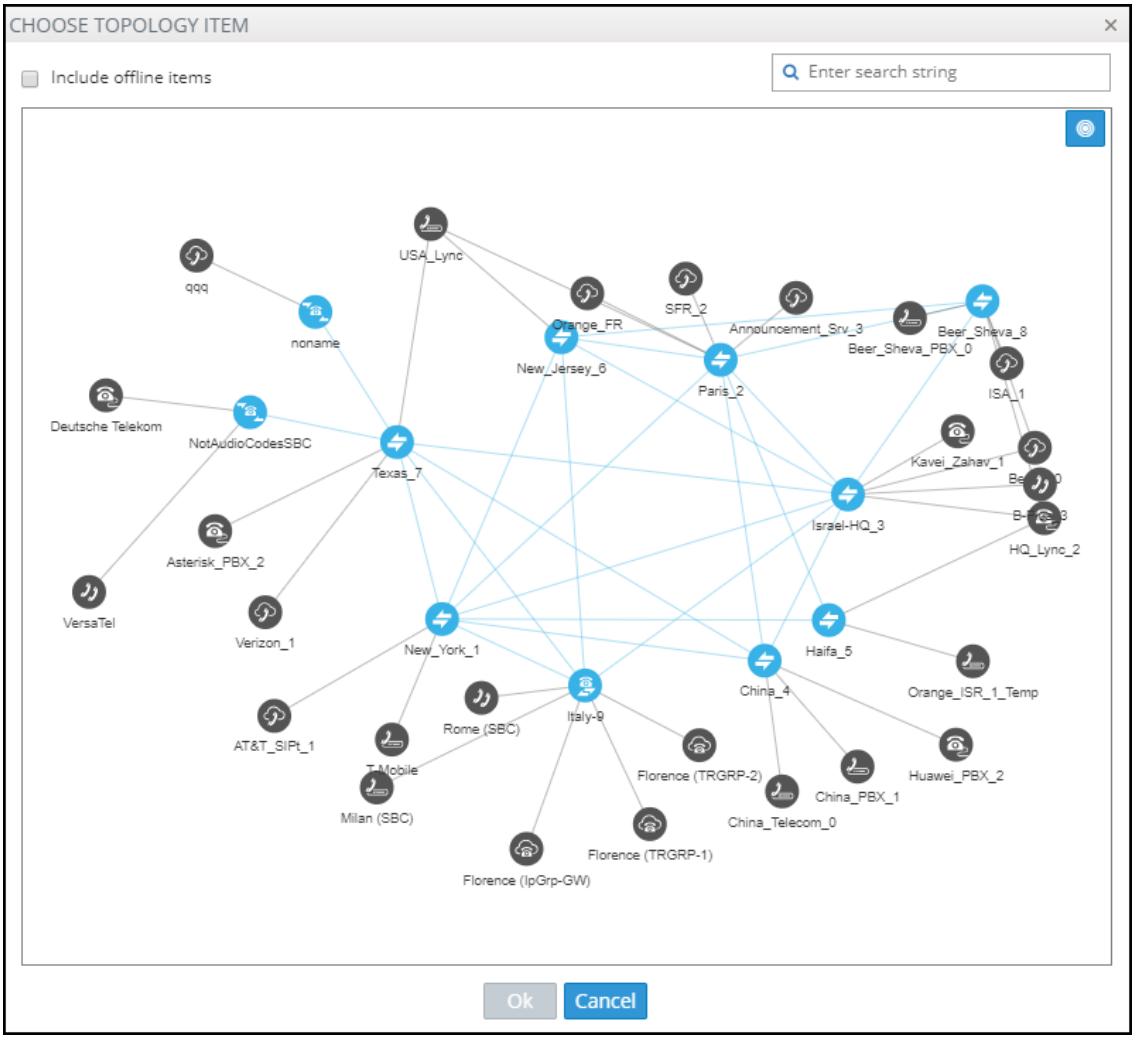
Live | Test Combination	Explanation
Live is enabled | Test is enabled	The rule will be considered for *both test and live traffic*.
Live is enabled | Test is disabled	The rule will be considered only for *live traffic*. Test mode won't be impacted. Select this option to simulate rule removal.
Live is disabled | Test is enabled	The rule will only be considered only for *test mode*. 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 *for test nor live traffic*. 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

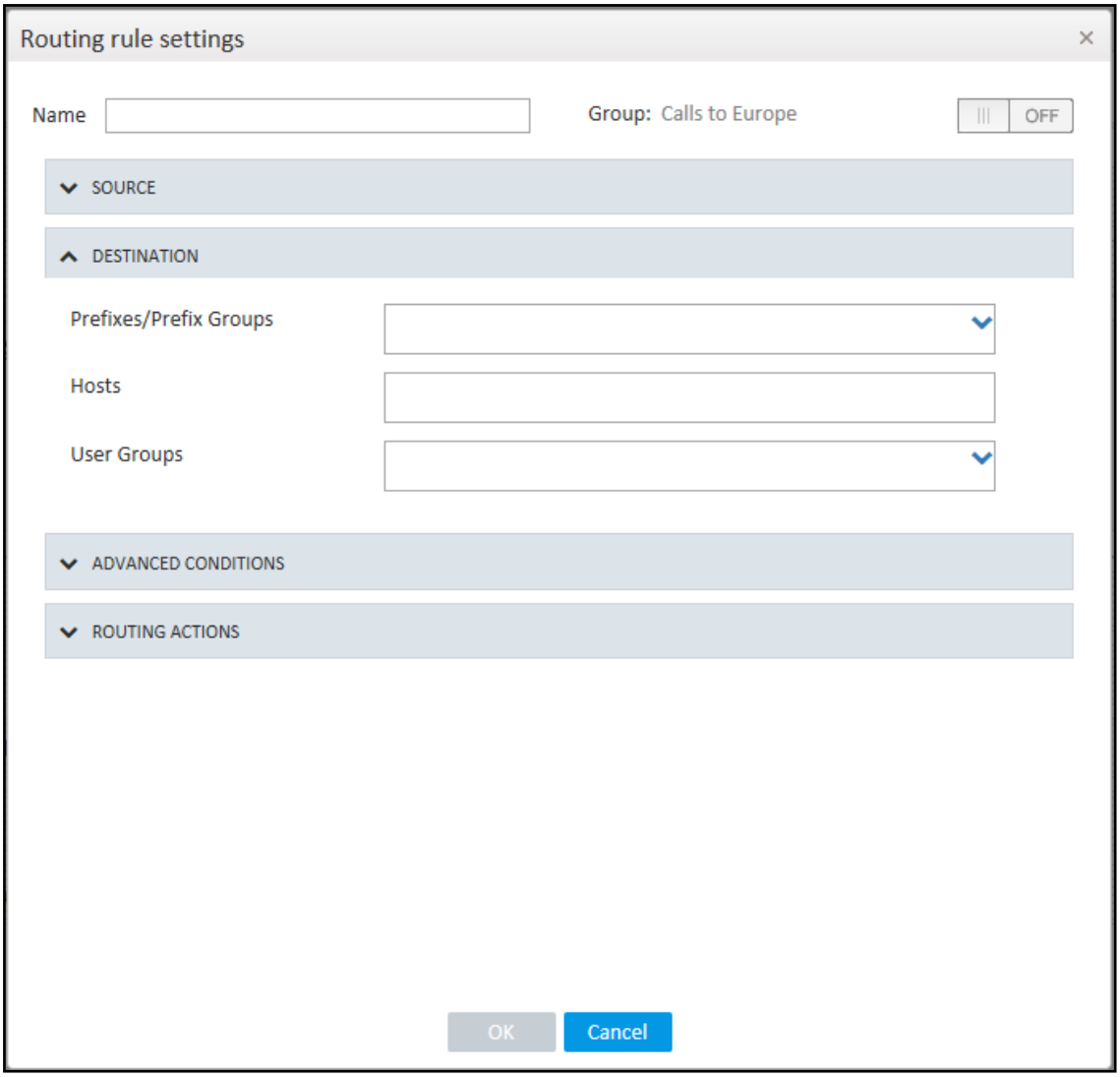
Setting	Description
Prefixes/Prefix Groups	Enter a source number prefix, or list of prefixes. You can also enter the name of a prefix group, or from the drop-down menu select a prefix group or list of prefix groups.
Hosts	Enter a source hostname, or list of hostnames.
User Groups	Enter the name of a 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 63.
Nodes/Peer Connections	Enter names of source nodes or peer connections, or a list of nodes or peer connections, or select nodes or peer connections from the drop-down menu, or click the icon  and visually and easily select the element from the Choose Topology Item screen shown in the figure following this table. This setting is mandatory if you want to define a routing rule applicable to *specific call sources* rather than (globally) to the entire network.

Figure 8-12: Choose Topology Item



5. In the Routing Rule Settings screen, click **Destination**.

Figure 8-13: Destination



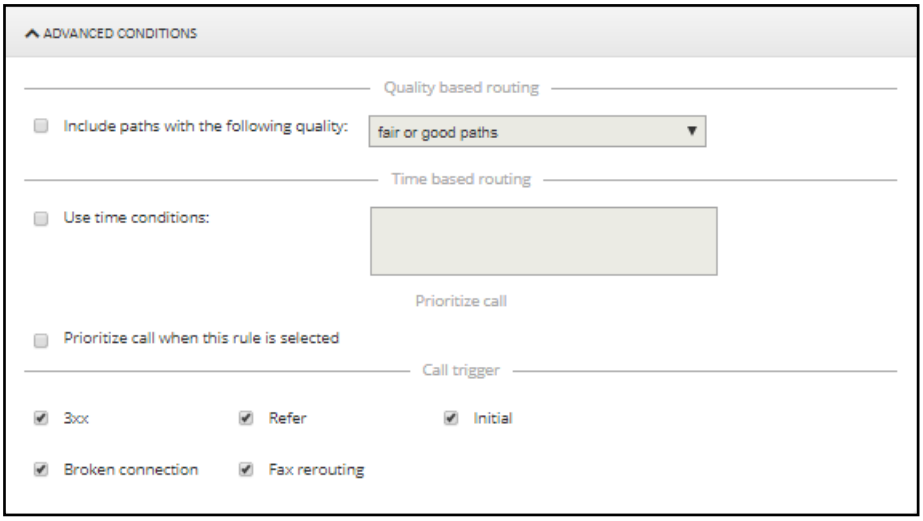
6. Configure the 'Destination' settings using the following table as reference.

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.

7. In the Routing Rule Settings screen, click **Advanced Conditions**.

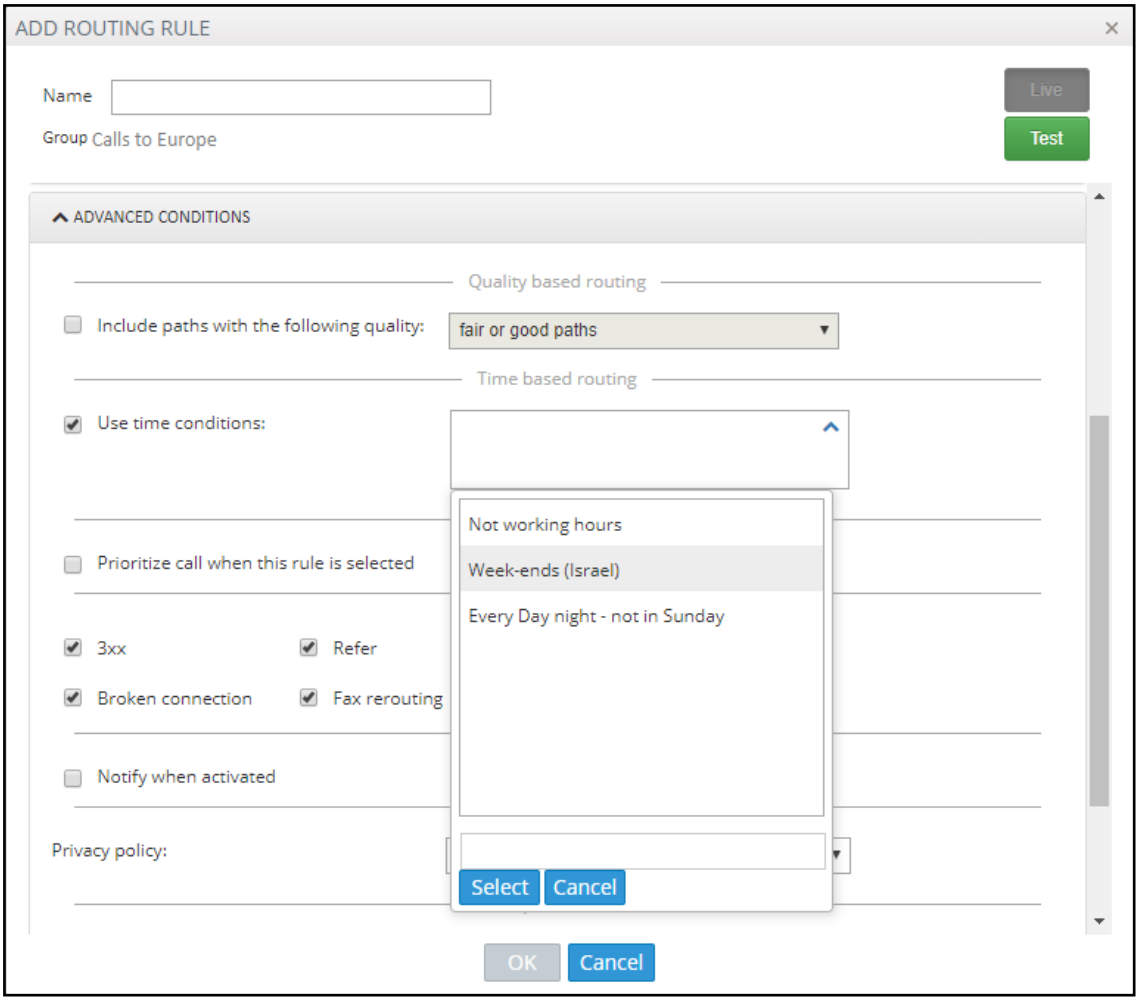
Figure 8-14: Advanced Conditions



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 114. 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 the option **use time conditions**; the pane becomes available. From the drop-down menu, select the time on which routing will be based, configured under **Settings** > **Routing** > **Time Based Routing** (see Routing Settings on page 114 for information about configuring a time range).

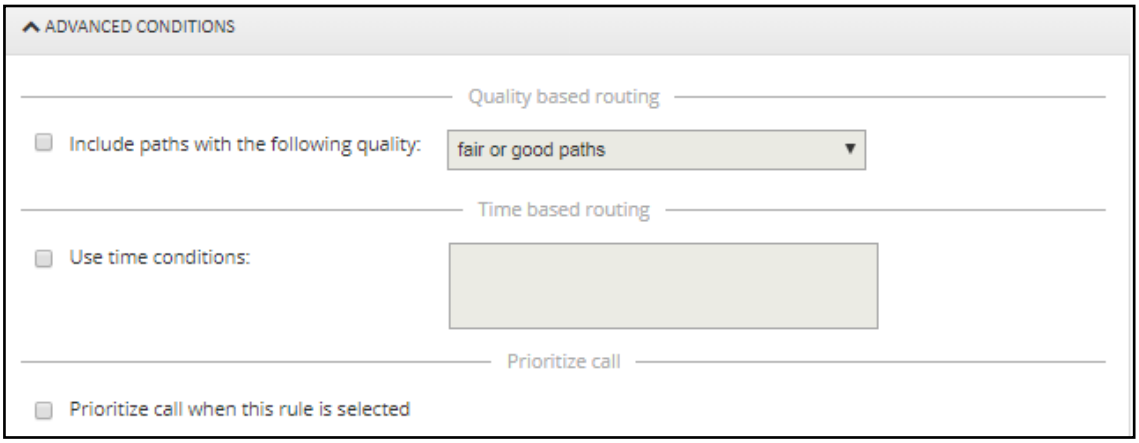
- More than one Time Condition can be associated with the same Routing Rule. Activation of the Routing Rule is then performed in 'or' between Time Conditions.
- A Time Condition can be attached to a Routing Rule which belongs to a Routing Group with an already-associated period; the ARM's calculation 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.

Figure 8-15: Advanced Conditions - Use Time Condition



10. 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 Routing Rule Settings screen.

Figure 8-16: Advanced Conditions – Prioritize call when this rule is selected

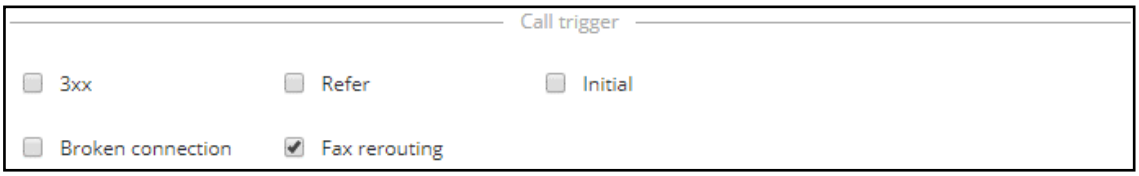


11. Under 'Advanced Conditions', select a **Call Trigger** to activate the rule for a specific Invite reason (i.e., alternative routing). By default, all 'Call Trigger' options are selected, so routing by default is based on all Call Triggers. At least one must be selected. The node applies to the ARM 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.

12. 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



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).

13. Under 'Rule Match' , select **Notify when activated** to enable a notification on a call (for example, a 911 emergency call) if the call matches a specific rule.

Figure 8-18: Rule Match: Notify when activated

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.

14. 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 8-19: 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	■ 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	■ If a regular call, stay as is ■ If anonymous, make it exposed in the SIP 'From' header

15. 15. [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.
16. 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.

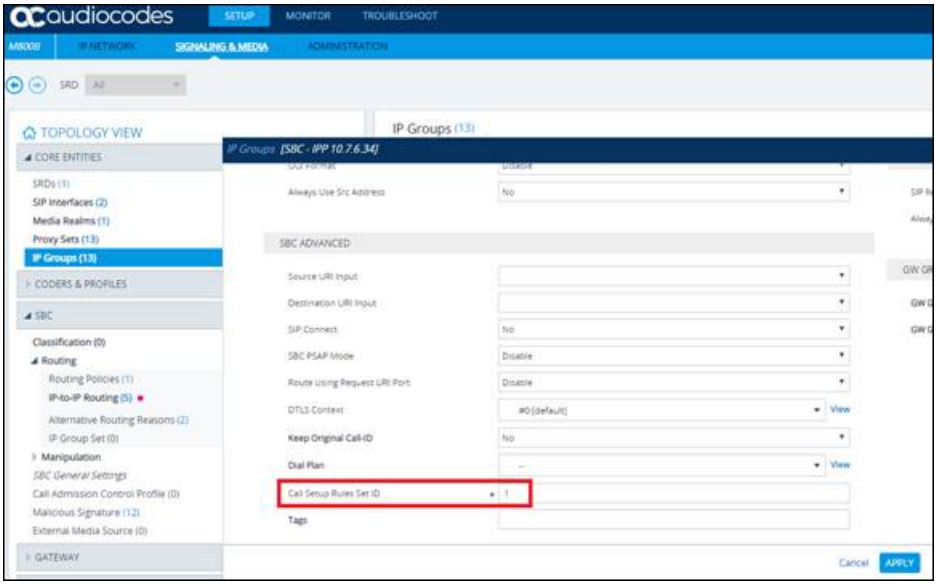
17. [SBC-Level Configuration] To send a parsed information request, add a new header with name "X-ARM-DETAIL-1", "X-ARM-DETAIL-2"… "X-ARM-DETAIL-N" and with information inside taken from the SDP or any other SIP header. X-ARM-DETAIL-X format is "X-ARM-DETAIL-1:<name=value>"

For example:

- X-ARM-DETAIL-1: "tgrp=100"
- X-ARM-DETAIL-2: "coder=711"

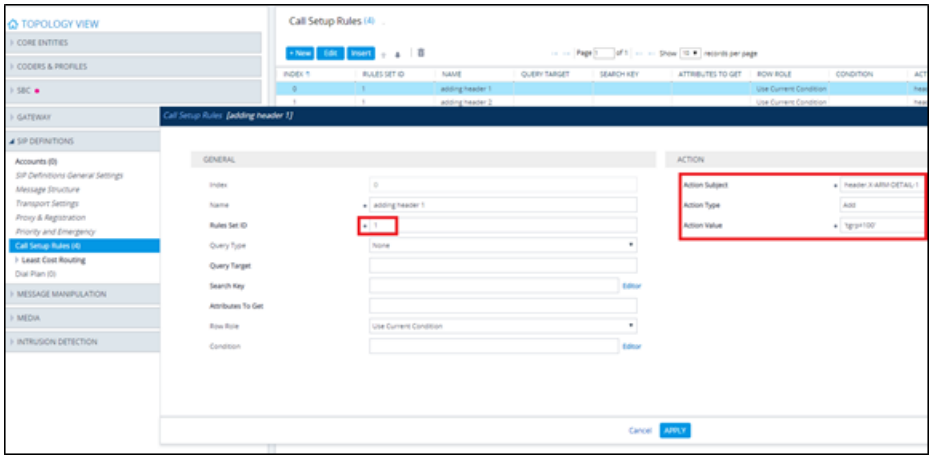
To create a new header in the SBC, add a new 'Call Setup Rules Set ID' in 'IPGroup' or in 'SIP Interface' in the device's Web interface. The figure below shows 'IPGroup'.

Figure 8-20: [Web Interface] Call Setup Rules Set ID



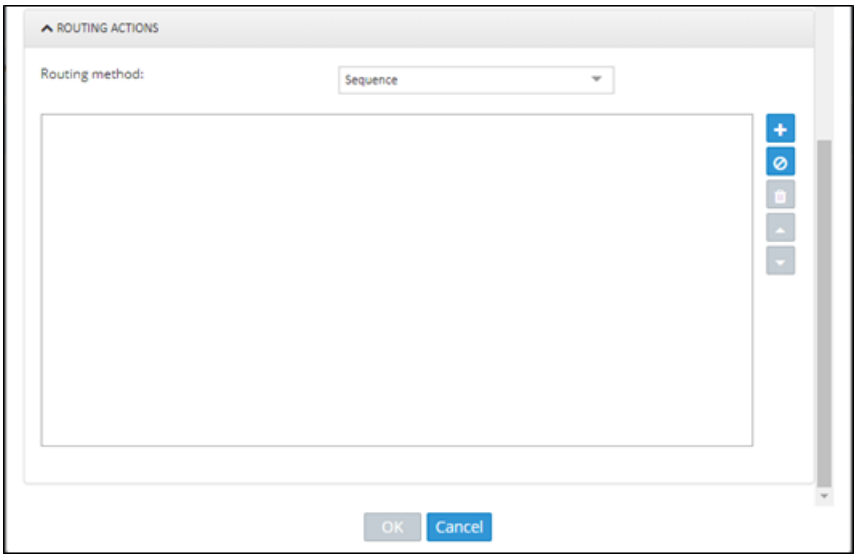
Setup rules can then be associated with the same Set ID. In the following figure, the manipulation added is 'tgrp=100'. In general, you can use a condition with RegEx and take the attributes into the Action Value.

Figure 8-21: [Web Interface] Viewing SBC Call Setup Rules Configuration



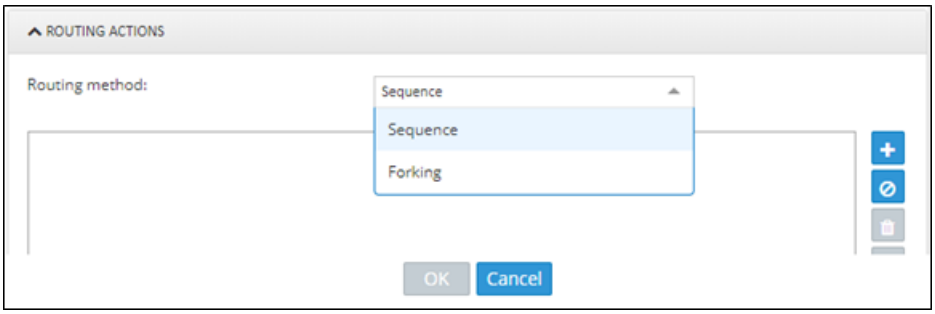
18. In the ARM's Add Routing Rule screen, click **Routing Actions**.

Figure 8-22: Routing Actions



- From the 'Routing method' drop-down, select **Sequence** or **Forking**.

Figure 8-23: Routing Actions – Routing Method



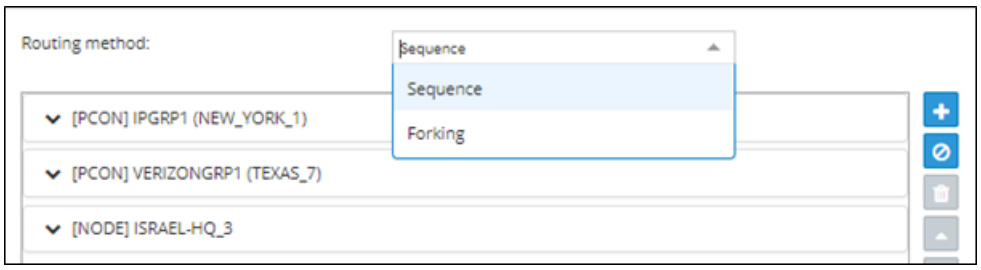
The parameter 'Routing method' is configured by default to Sequence; Routing Rule Actions are applied sequentially (the only option in ARM versions earlier than 8.6).

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.

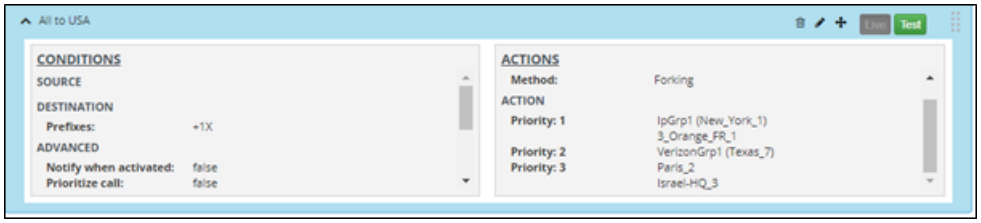
Forking implementation in ARM utilizes SBC forking capabilities. When a call matches an ARM routing rule condition with forking, the ARM instructs the SBC to perform forking per the actions configured in ARM Routing Rule.

Figure 8-24: Calls Forking – Routing method



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 8-25: Calls Forking Routing Rule

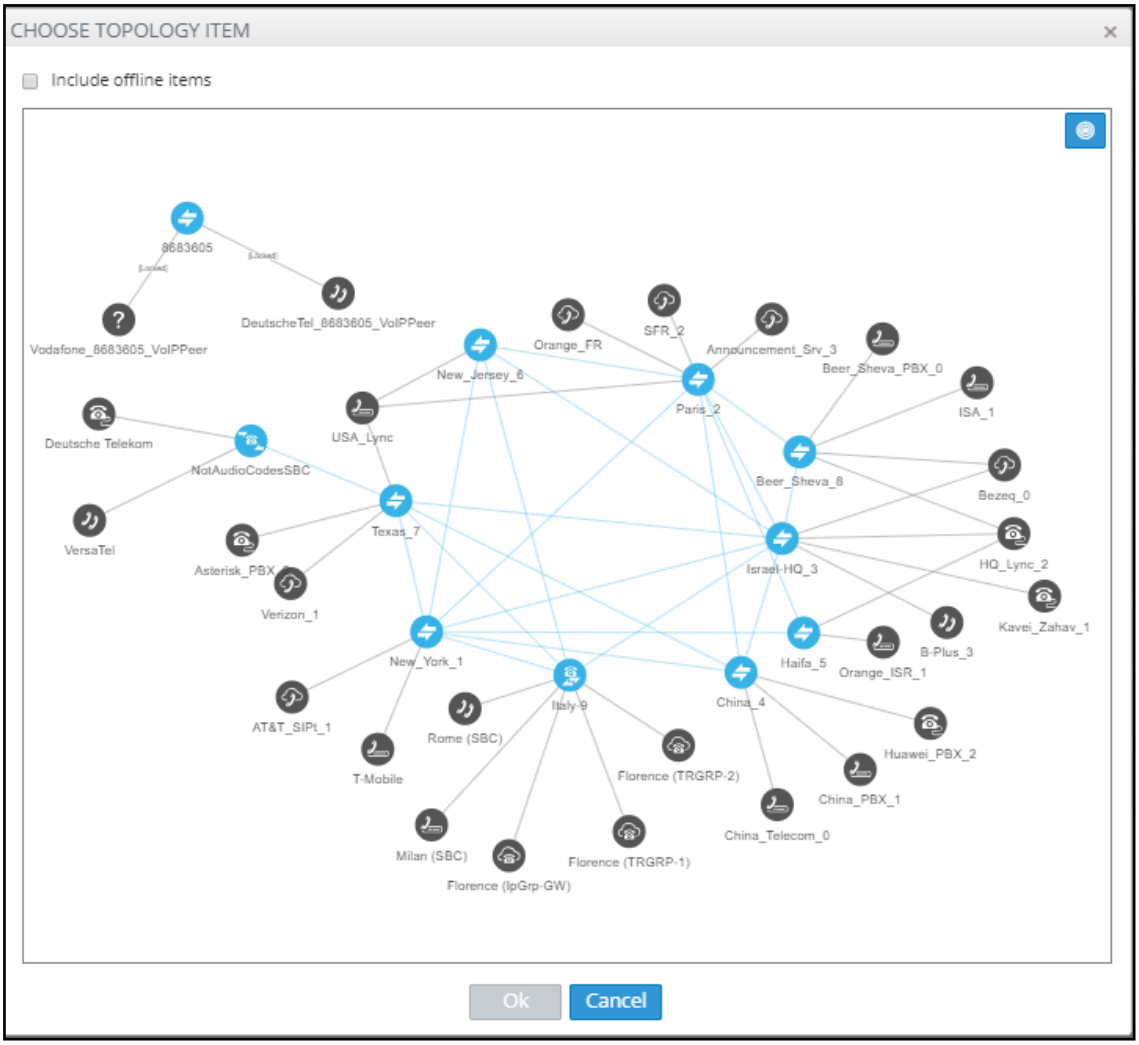


During the upgrade to ARM version 8.6, all Routing Rules are translated with the Sequence routing method (the default).

- In ARM version 8.6, 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'.

19. In the main pane under 'Routing Actions' (**Add Routing Rule** screen > **Advanced Conditions**), select an action or set of actions to be taken if the Routing Rule matches; click the **+** icon (recommended). [Alternatively, select an action from the drop-down menu]. The 'Choose Topology Item' screen opens.

Figure 8-26: Choose Topology Item



- In the 'Choose Topology Item' screen, select the VoIP Peer, Peer Connection or Node to serve as the Action in the Routing Rule, and then click **OK**. This is an easy, visual way of selecting the correct topology element, especially in large networks with high numbers of topology elements where human error can easily occur.
- Use the following table as reference.

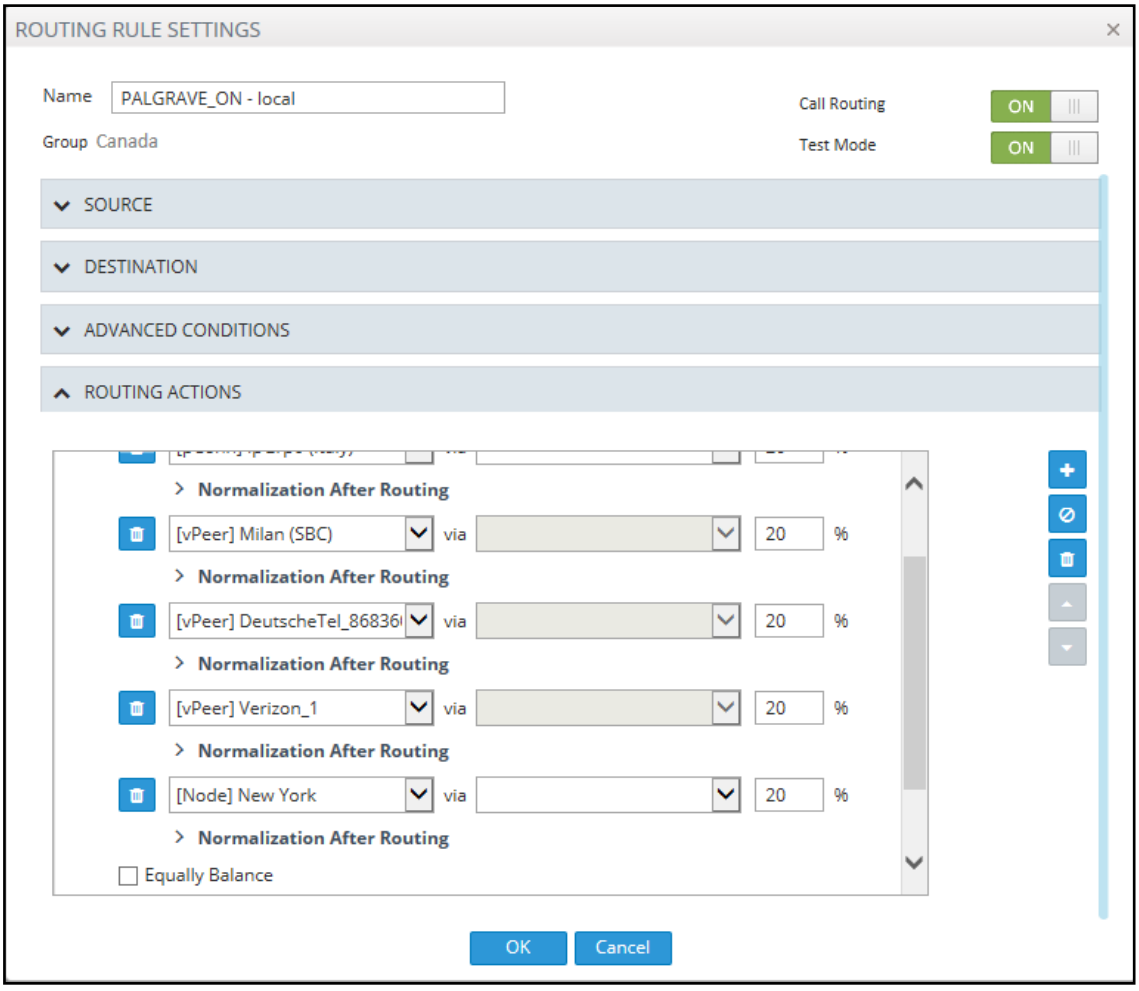
Table 8-5: Routing Actions

Setting	Description
[Action] left drop-down menu field	Select from the drop-down menu the Peer Connection, VoIP Peer or Node to which the call will be routed. In the figure above, the Peer Connection **IpGrp1 (Italy)** is selected.
[Via] right drop-down menu field	[Optional] Select from the drop-down menu the Node that the call must pass through. In the figure above, the Node **Paris_2** is selected. Only a single Node can be added in Via.
> Normalization groups	Click **>** to open post routing (after routing) normalization.

Setting	Description
Source normalization group	Select a normalization group (see Adding a Normalization Group on page 103) to manipulate the source number in the outgoing call to the peer connection. The source normalization group can only be connected to an IP Group or VoIP Peer. It cannot be connected to a Node.
Destination normalization group	Select a normalization group (see Adding a Normalization Group on page 103) 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.

20. Click **Add loading balancing**.

Figure 8-27: Routing Actions – Load Balancing - Equally Balanced (Default)

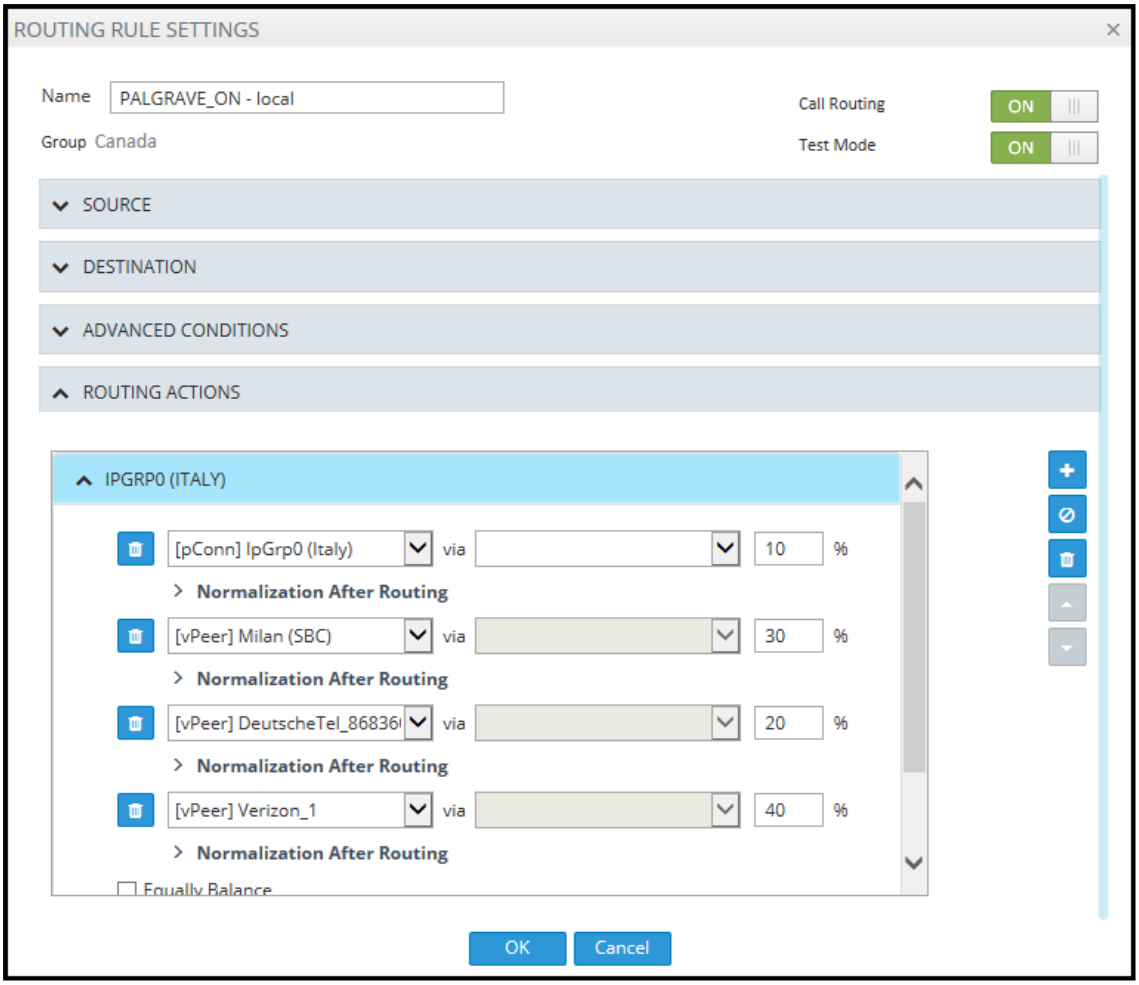


Load balancing is added between more than one Peer Connection, Node or VoIP Peer. By default, these are equally balanced, i.e., the same percentage is assigned for each option, as shown in the figure above.

You can optionally define your own percentage by clearing the 'Equally Balance' option. 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 using the Add load balancing button shown in the figure 'Routing Actions' following.

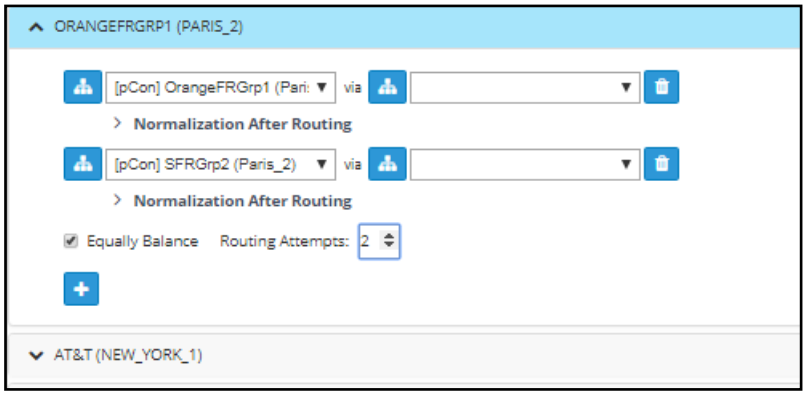
21. Enter the percentage of routes that will take this action when load balancing is configured and **Equally Balance** is cleared. Make sure you have 100% in the Action's calls destinations summary else you won't be allowed to enable the action.

Figure 8-28: Routing Actions – Load Balancing - Defining Your Own Percentages



22. 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 ORANGEFRGRP1 (PARIS_2) in the following figure).

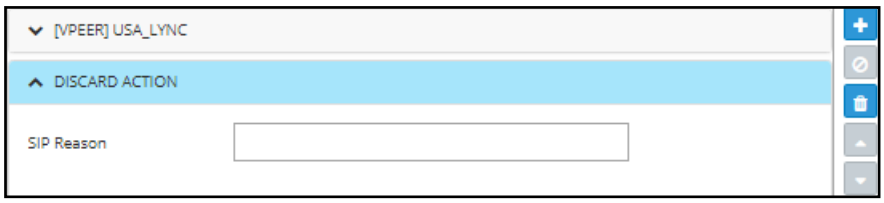
Figure 8-29: Equally Balance: Routing Attempts = 2



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.

23. Click the Call Discard action icon.

Figure 8-30: Routing Actions – Call Discard



24. Configure using the following table as reference

Table 8-6: Routing Actions – Call Discard

Setting	Description
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 **Discard call** routing 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. You can provide a specific SIP reason for 'Discard Call' as well as use the last SIP reason received from the SBC or the Gateway.
SIP Reason	Enter the 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/Nodes/Peer Connections), the rule will not check it.

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 now-enabled **Move** icon; the Move Routing Rule dialog is displayed.

Figure 8-31: Move icon

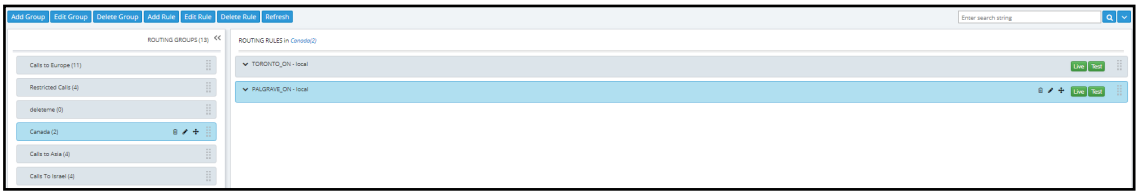
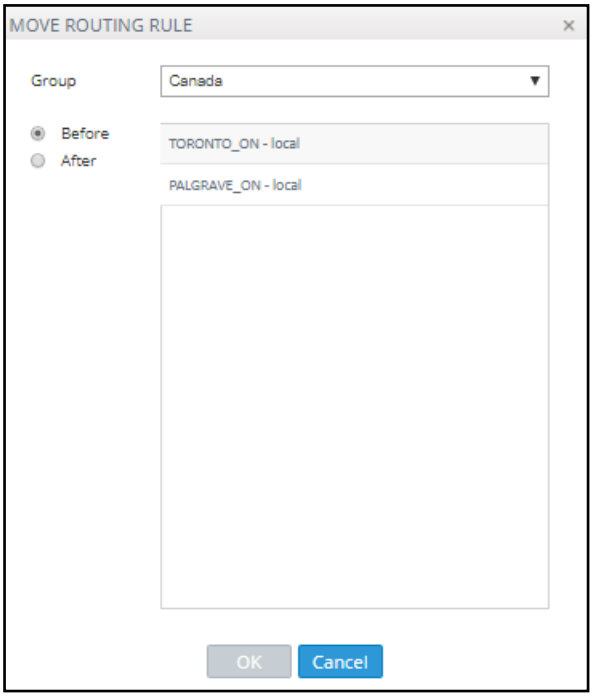


Figure 8-32: Move Routing Rule



2. From the 'Group' drop-down menu, select the group to which to move the rule.
3. Select either **Before** (default) or **After** and then select the rule before which or after which you want to move the rule.
4. Click **OK**; the rule is moved to the location you defined.

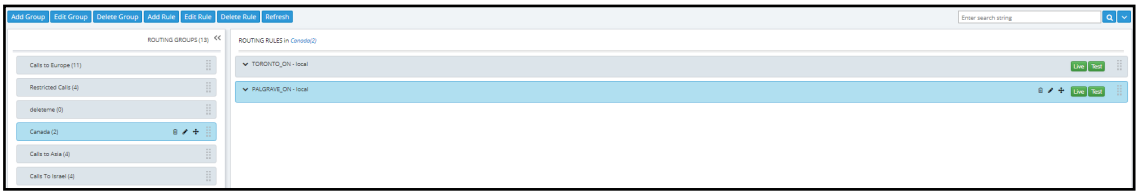
Deleting a Rule

You can delete a rule if necessary.

➢ **To delete a rule:**

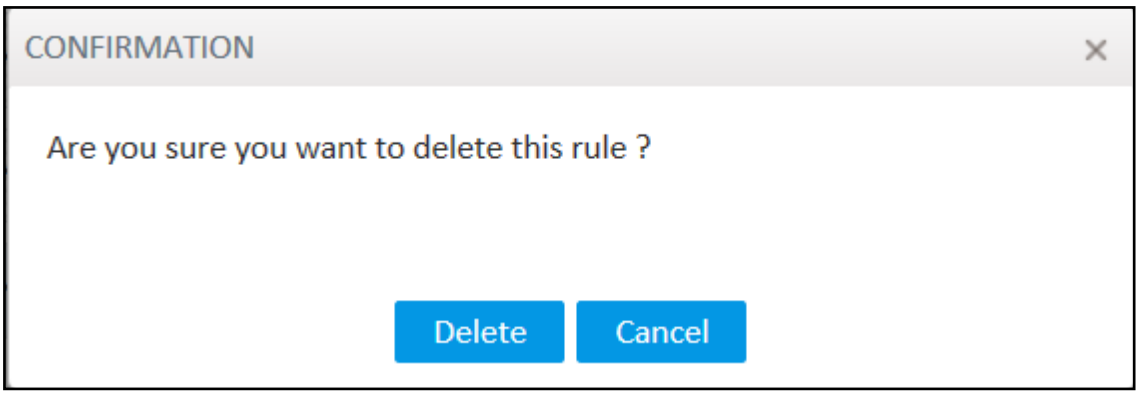
1. Click the group under which the rule is defined and then adjacent to the defined rule that you want to delete, click the now-enabled **Delete** icon shown in the following figure – OR- click the now enabled **Delete Route** button also shown in the following figure.

Figure 8-33: Delete Icon



2. In the Confirmation prompt 'Are you sure you want to delete this rule?' shown in the following figure, click **Delete**.

Figure 8-34: Delete Icon



The rule is deleted.

Testing a Route

You can test a route to make sure it performs according to expectations. See Testing a Route on page 47 for more information.

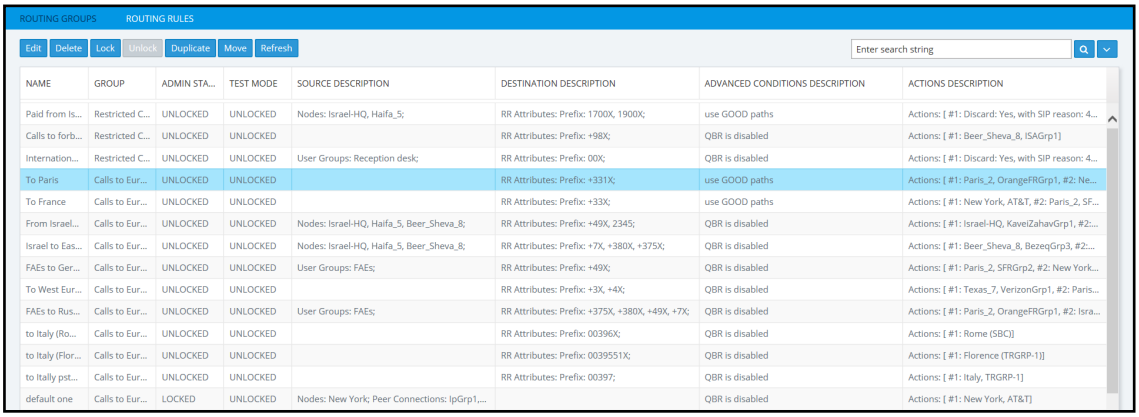
Using the Routing Rules Table View Page

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 8-35: Routing Rules Table View Page



2. Select a rule or select multiple rules; the actions buttons are activated. Administrators can:
   - Edit a rule
   - Delete rules
   - Lock / Unlock rules
   - 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.

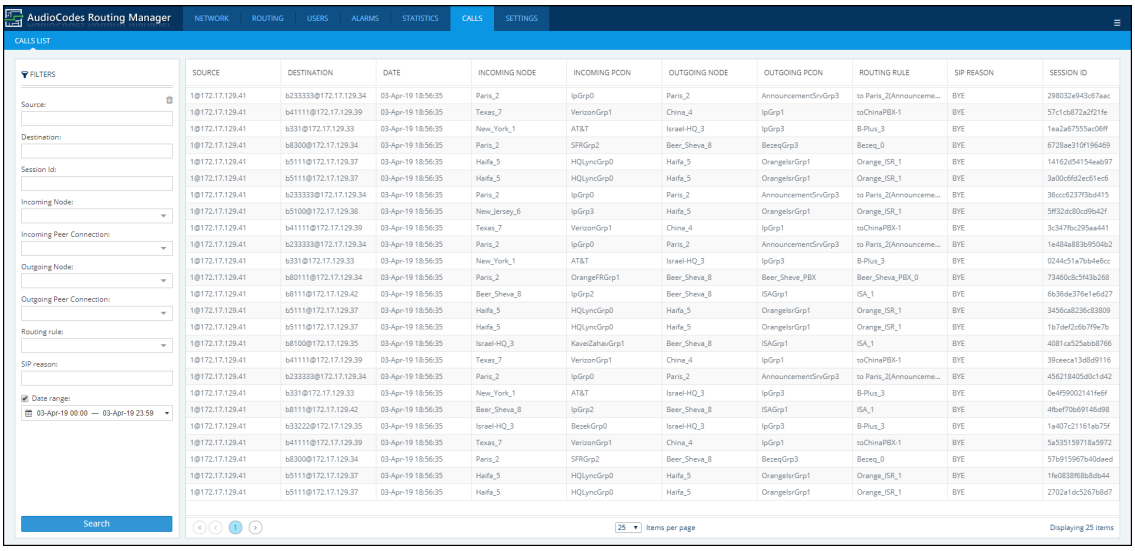
9 Viewing CDRs and Call Details

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



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

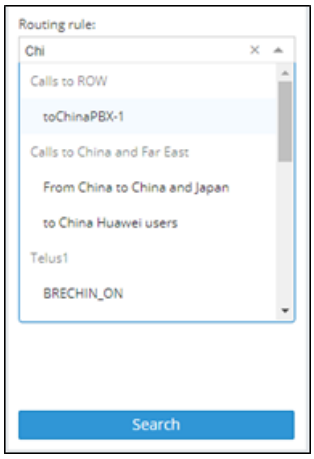
Filter	Description
Source	Enables filtering the Calls List per URI before manipulation.
Destination	Enables filtering the Calls List per URI before manipulation.
Session ID	Enables filtering the Calls List per Unique Session ID identifying a specific call.

Filter	Description
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.
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.
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



The following columns (call digest) is 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

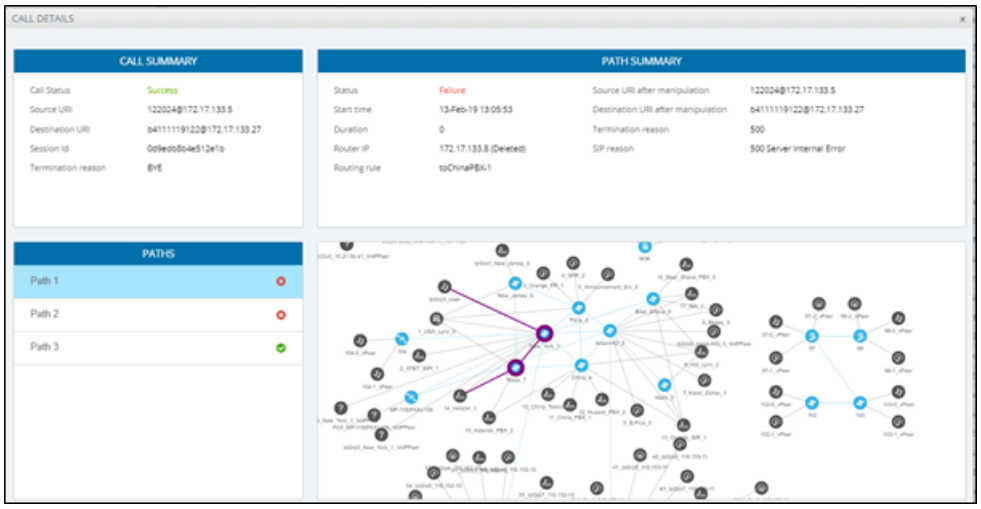
- Session ID

Figure 9-3: Call Columns in the Calls List

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.

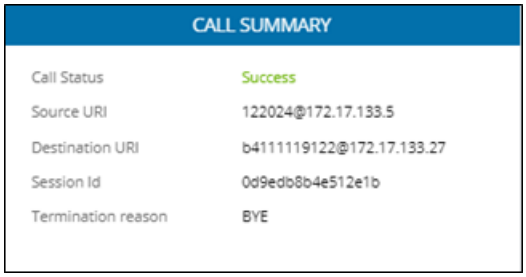
Figure 9-4: Call Details



The page displays detailed information on most routing aspects of the call and shows each routing path the ARM attempted.

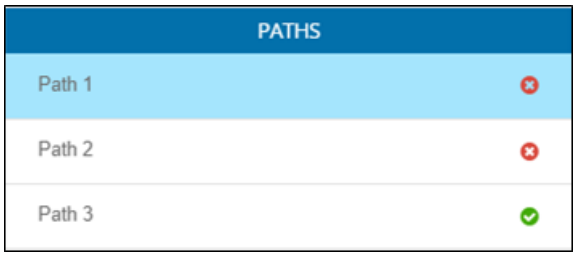
The Call Summary pane displays the following routing information about the call:

Figure 9-5: 'Call Summary' Pane



The Paths pane displays the list of paths the ARM attempted when routing the call.

Figure 9-6: 'Paths' Pane



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 9-7: 'Path Summary' Pane

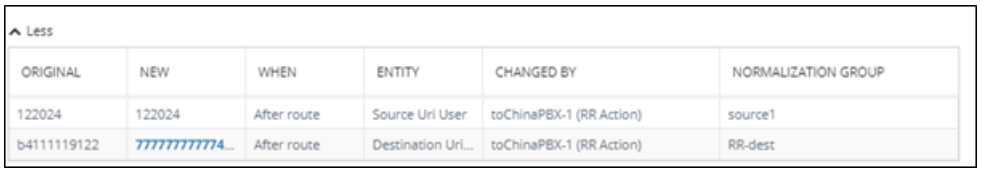
Use the table as reference to the Path Summary.

Table 9-2: Path Summary

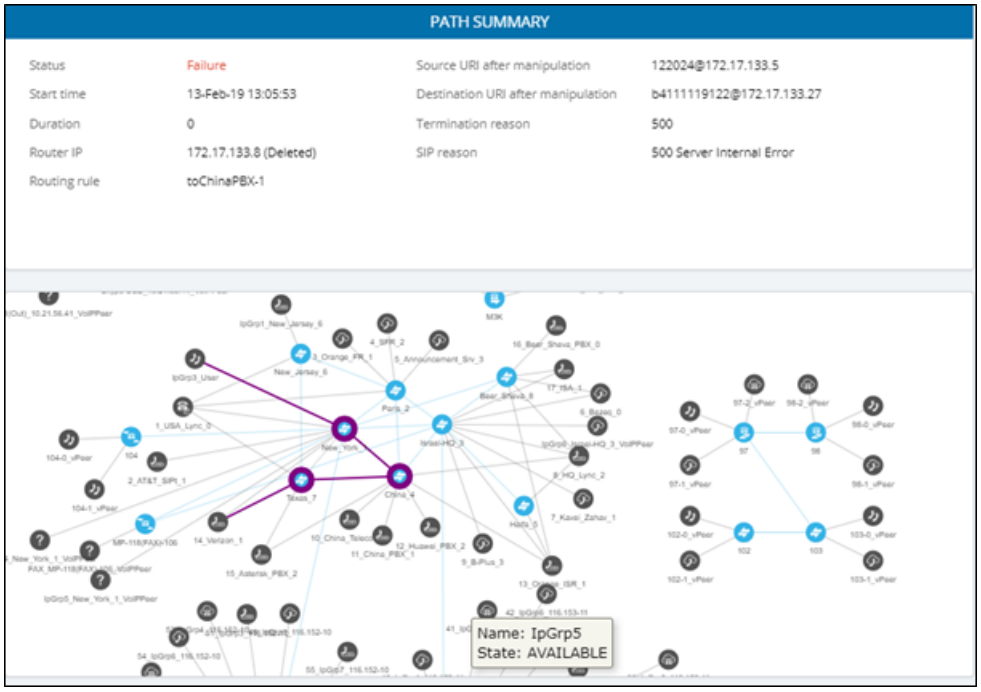
Setting	Description
Status	Displays whether the path was Success or Failure.
Start time	Displays the ARM setup time.
Duration	Displays the call duration; non-zero if 'Status' is Success.
Router IP	Displays the IP of the Router which handled the initial Routing request.
Routing rule	Displays the call 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.

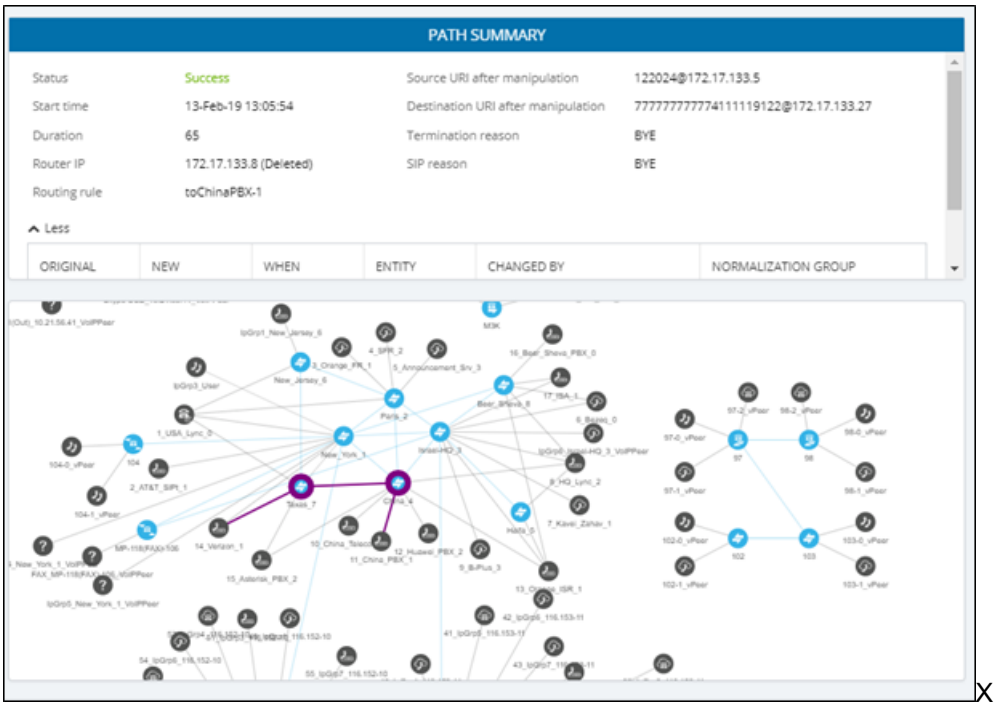
Figure 9-8: 'More' Pane Displaying Details of Applied Manipulation Rules



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:



X

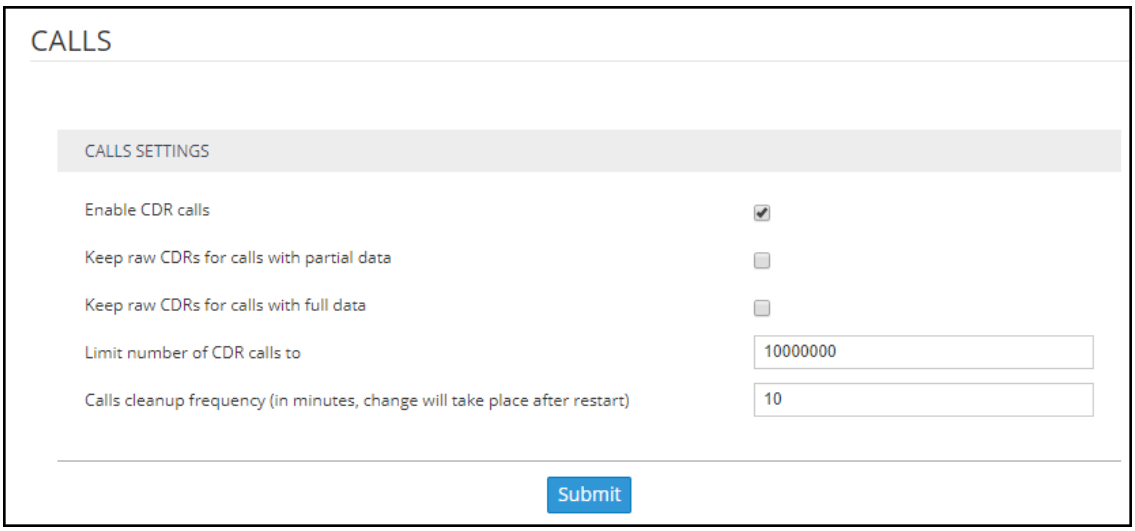
Disabling, Limiting the Number of CDRs

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** > **Network Services** > **Calls**).

Figure 9-9: 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). If you're running more than 150 CAPS traffic, it's recommended to disable CDRs.
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. If you're running more than 150 CAPS traffic, it's recommended to disable CDRs.
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.

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

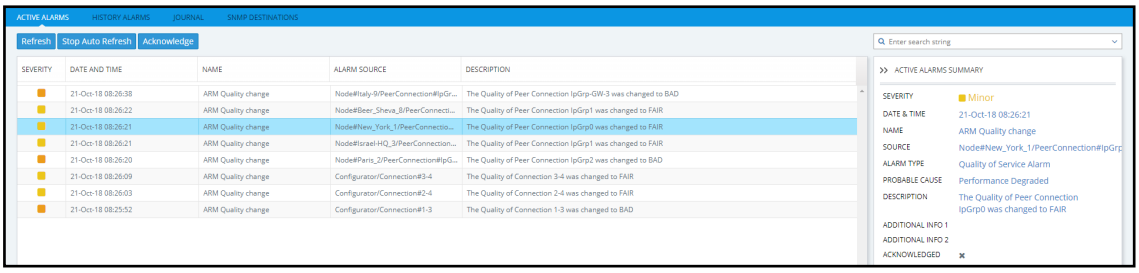
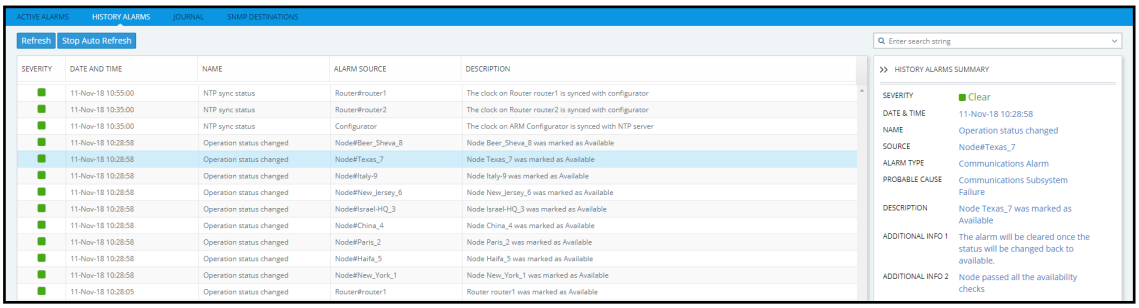


Figure 10-2: Alarms – History Alarms



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 page 159 below).
- **Refresh** the page / **Stop Auto Refresh**

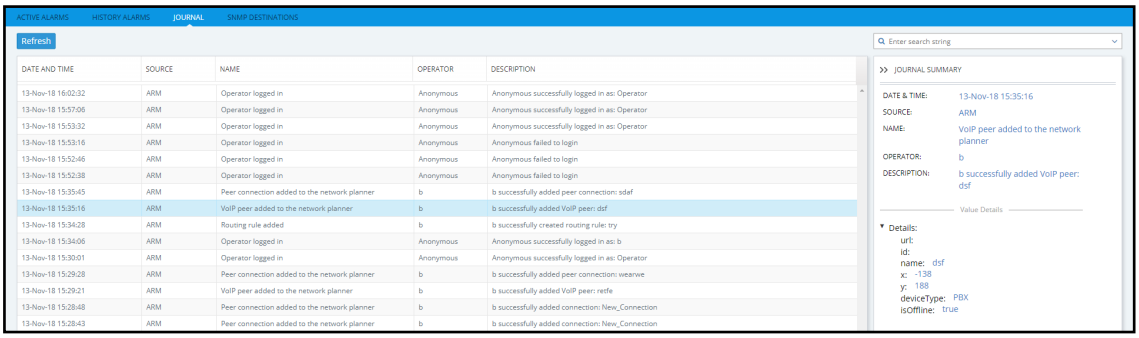
- **Acknowledge Alarm** [Applies only to the Active Alarms page] Click the button to clear a selected alarm from the page. Note that after acknowledging it, the alarm can be still viewed in the History Alarms page.

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



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.

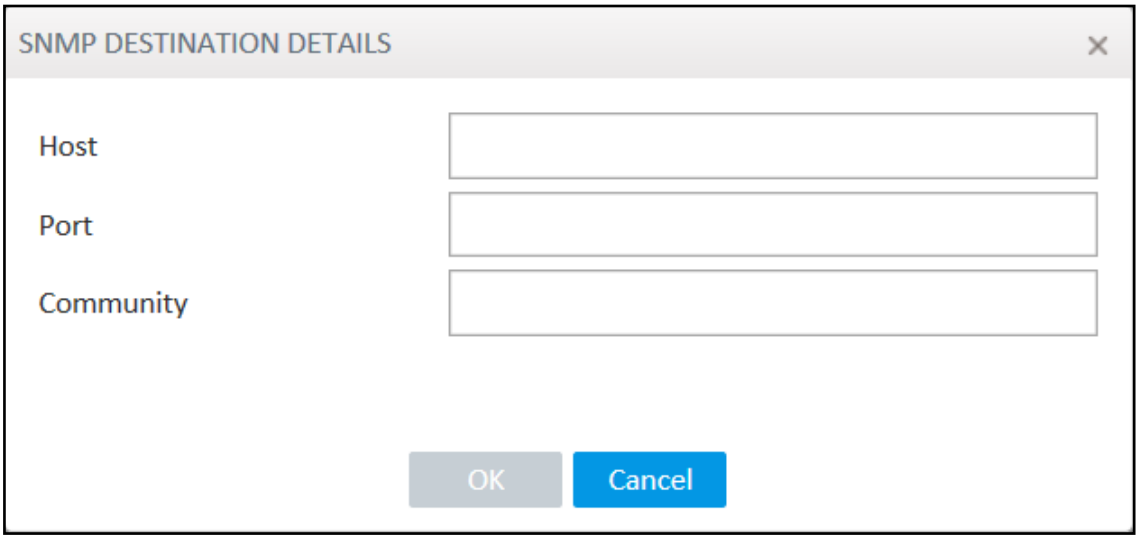
Collecting Info via SNMP to Enhance IP Network Telephony Performance

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



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

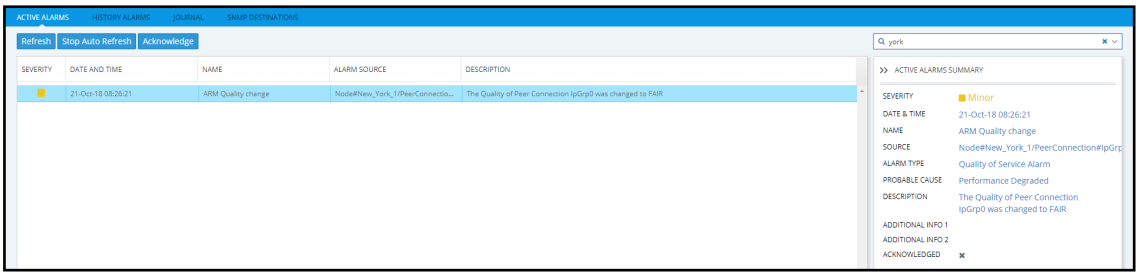
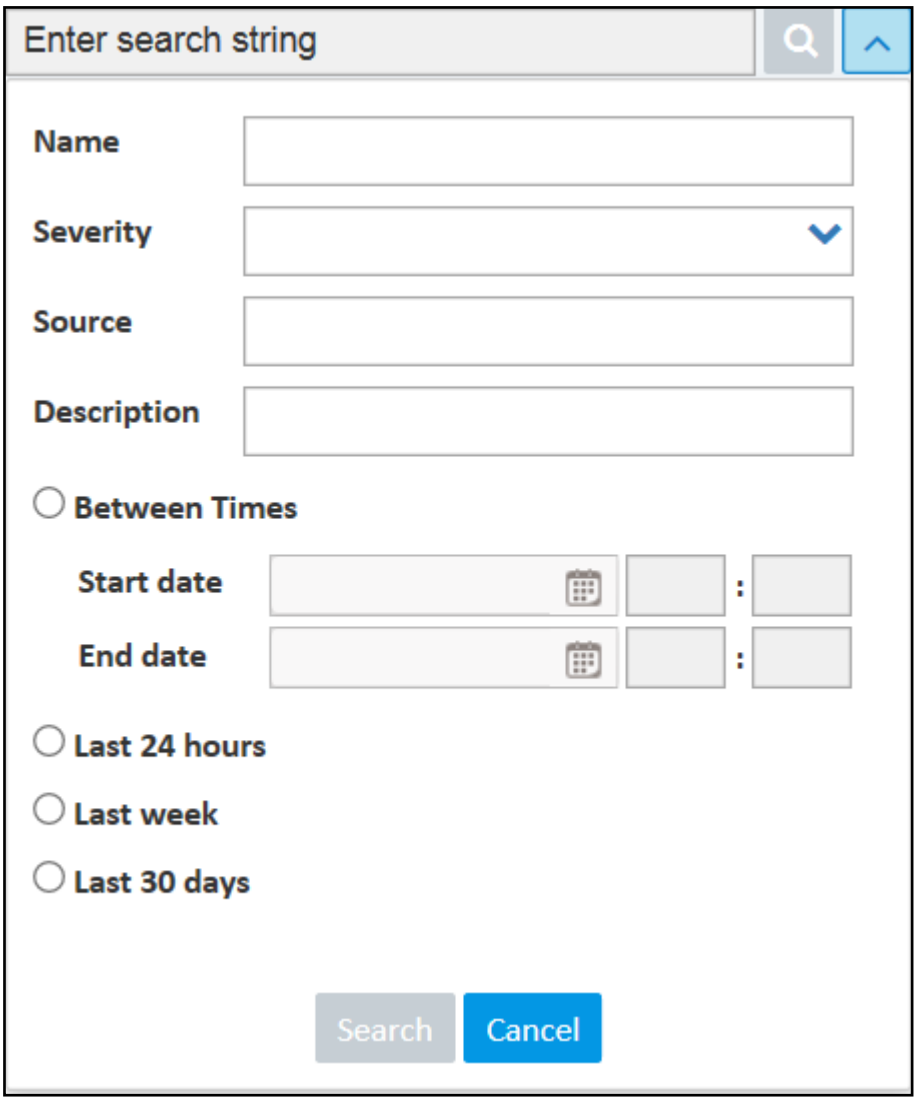


Figure 10-6: Searching for a Specific Alarm



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.
   - 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**.

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 Getaway 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 166.

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 on the previous page, respectively.

See Migrating Hybrid Routing to the ARM on page 171 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.

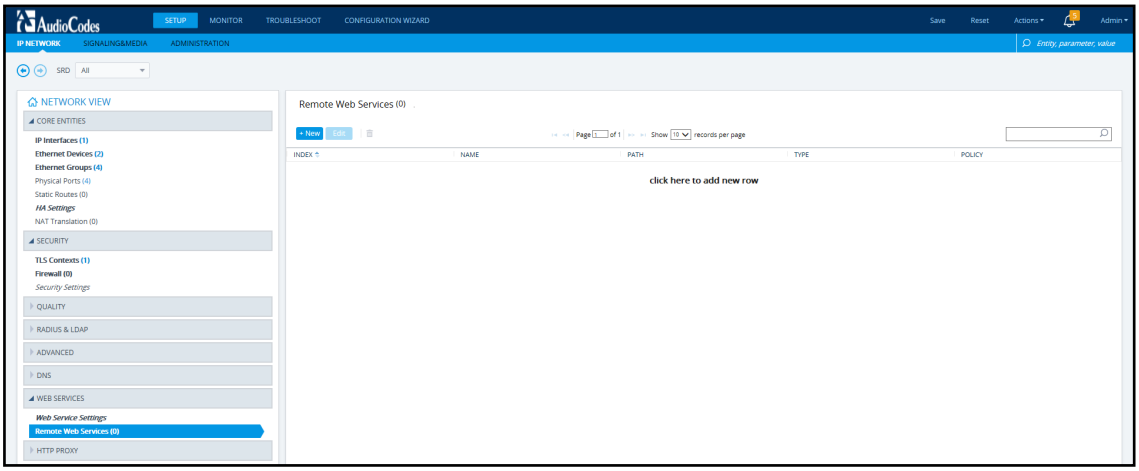
AudioCodes recommends starting a migration by manually adding a device in the ARM Network page as shown in Adding an AudioCodes Node to the ARM on page 40.

For auto-discovery provisioning, take the steps below to connect the device to the ARM network.

➢ To connect the device:

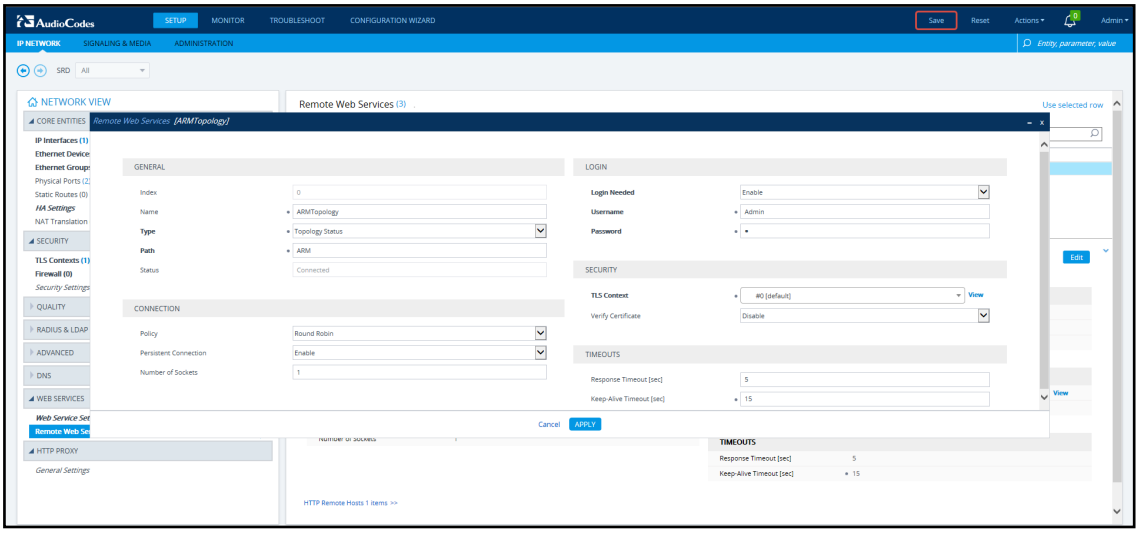
1. In your internet browser, enter the device's IP address in the Address bar, and then in the login page that opens, enter the User Name and Password (**Admin**, **Admin** are the defaults).
2. In the device's Web interface that opens, check the **Setup** menu and then navigate to the HTTP Remote Services page (**IP Network** > **Web Services** > **Remote Web Services**).

Figure 11-1: Services



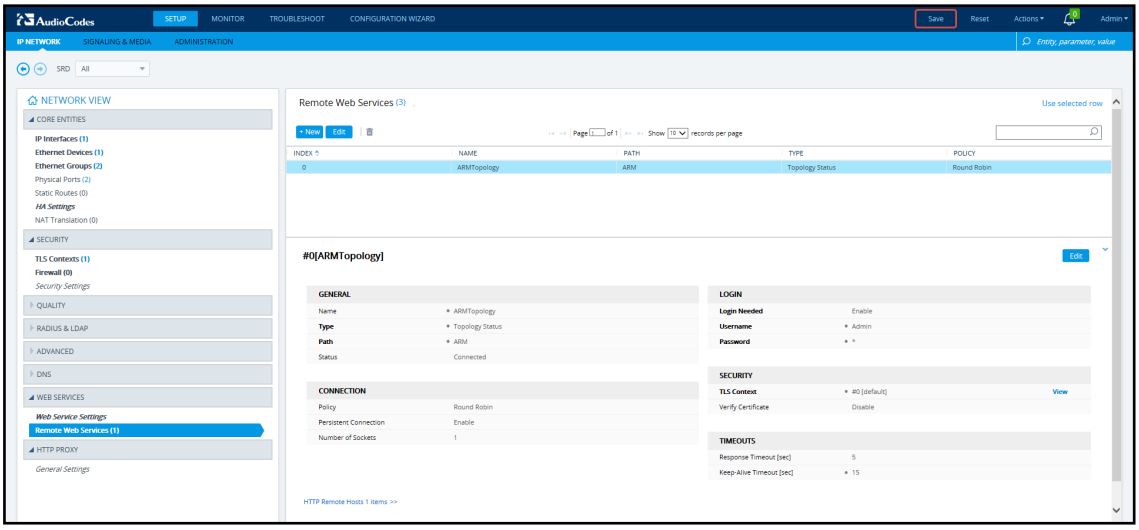
3. Click **+New** or **click here to add new row**.

Figure 11-2: Web Interface - HTTP Remote Services – Add Row



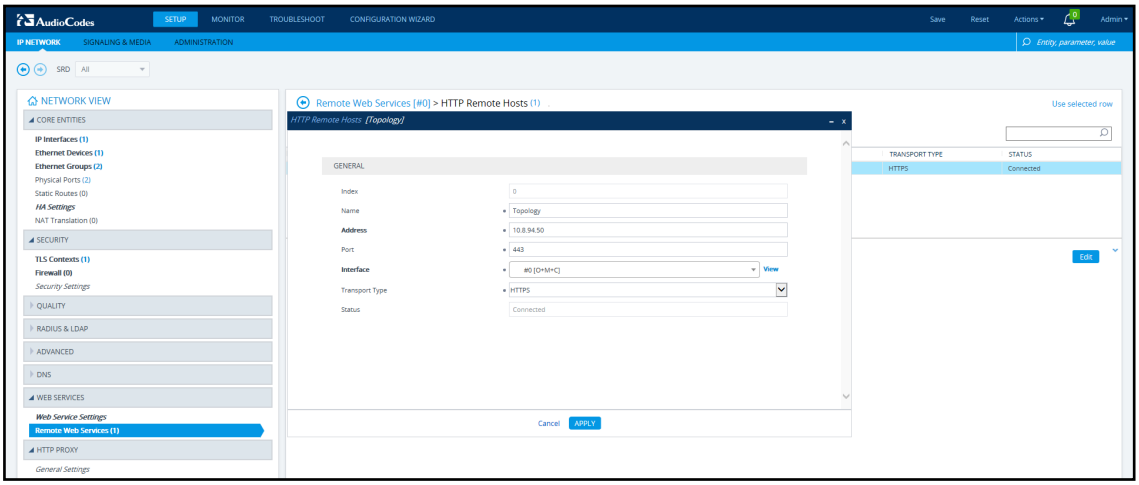
4. Configure the dialog using the figure above as reference, and click **Apply**.

Figure 11-3: Web Interface - Remote Web Services – HTTP Remote Hosts



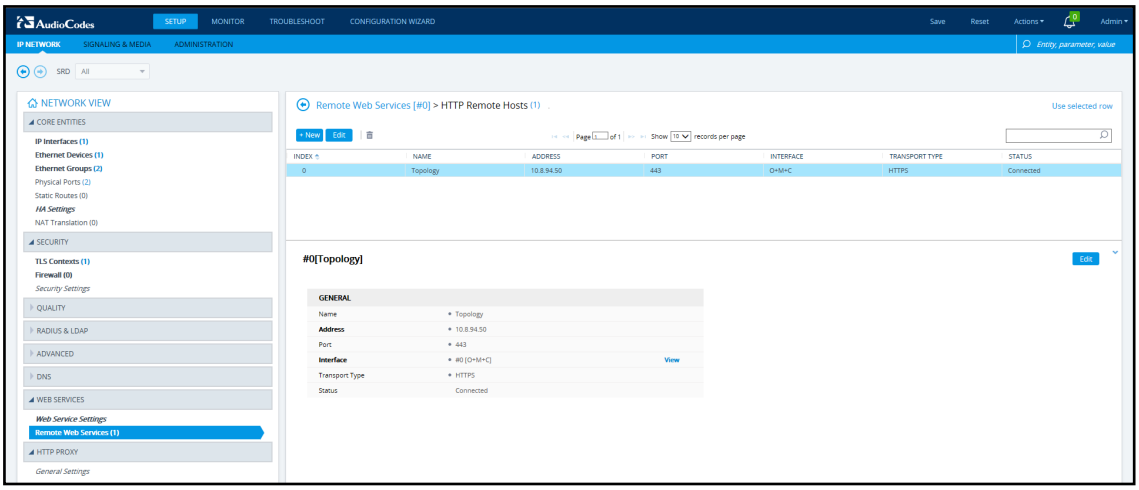
5. Click the **HTTP Remote Hosts** link shown in the figure above.
6. In the HTTP Remote Hosts page that opens, click the **Add** tab.

Figure 11-4: Web Interface - Remote Web Services - HTTP Remote Hosts - Add



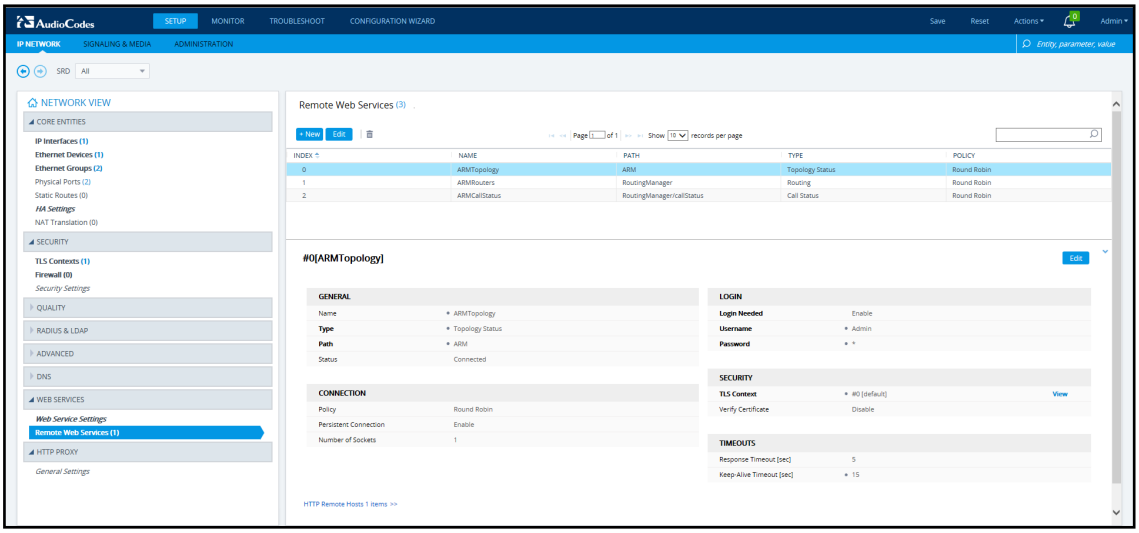
7. Define the IP Address of the ARM Topology Server to which you want to point the device and define the ARM Topology Server settings, and then click **Save**; wait until connected.

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.

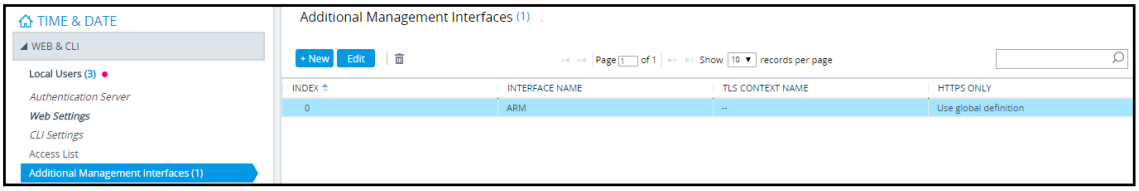
Defining a dedicated IP interface on the device for ARM traffic allows keeping ARM traffic internal, if required, separating ARM traffic from other device management traffic such as Web, SNMP and NTP.

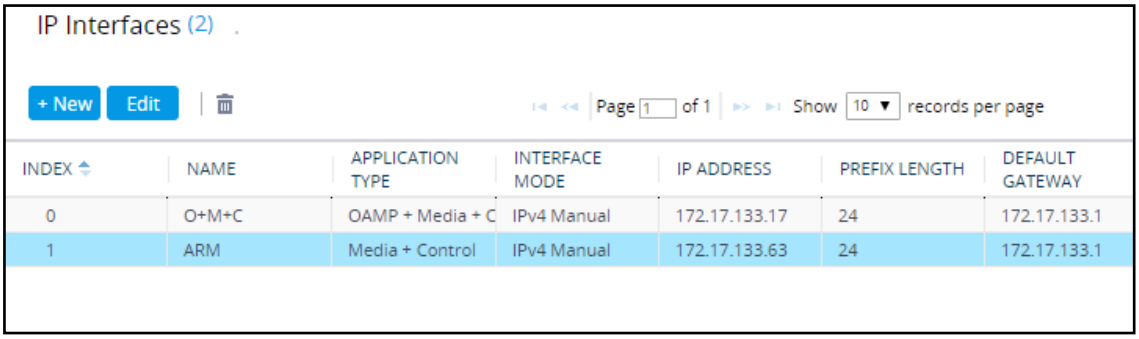
When defining ARM on the node, you must assign an IP interface to the remote host (ARM) and a TLS context for the HTTP Service. The ARM automatically adds its routers to all nodes. When the ARM does this, it uses the same IP interface and TLS context that you defined for the ARM Configurator HTTP Service. 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





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

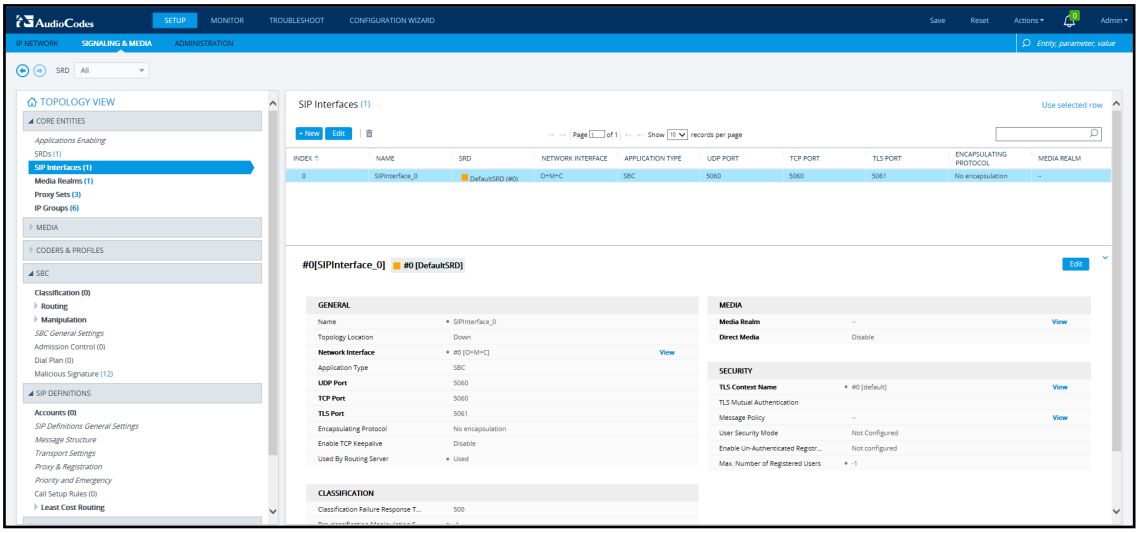
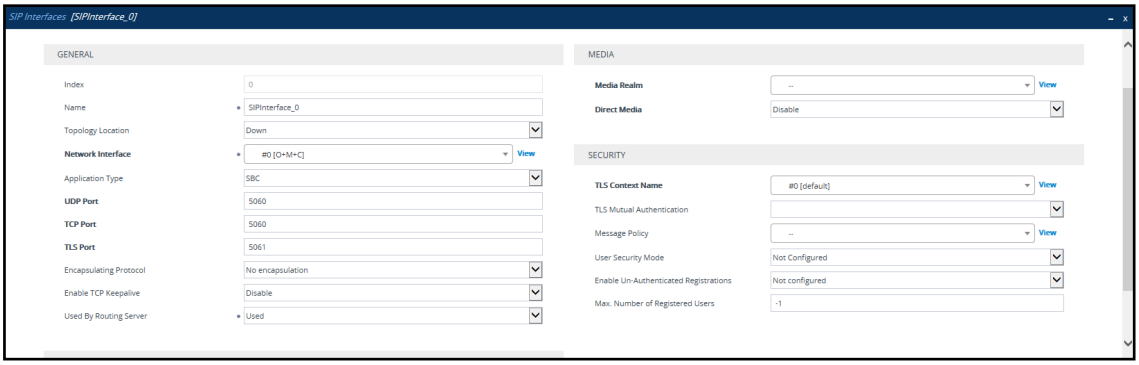


Figure 11-9: Web Interface – SIP Interfaces Table - Configuring a SIP Interface



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 175.
- '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

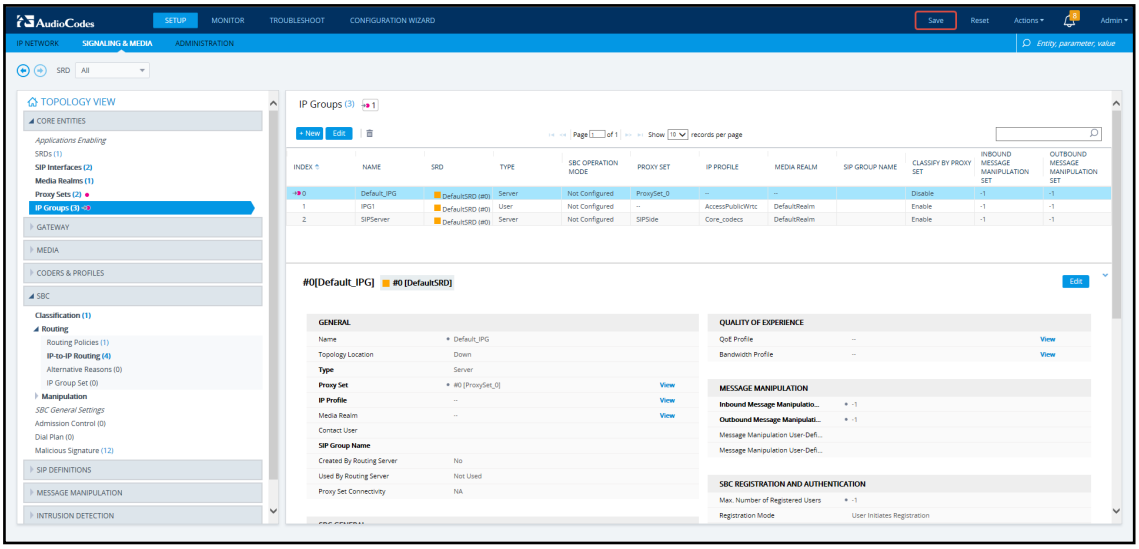
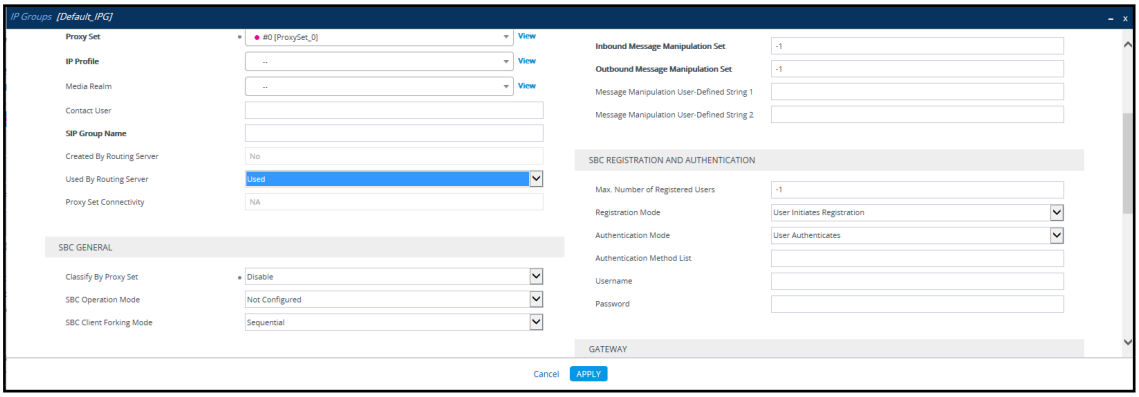


Figure 11-11: Web Interface – IP Groups - Configuring an IP Group



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 27).

> 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

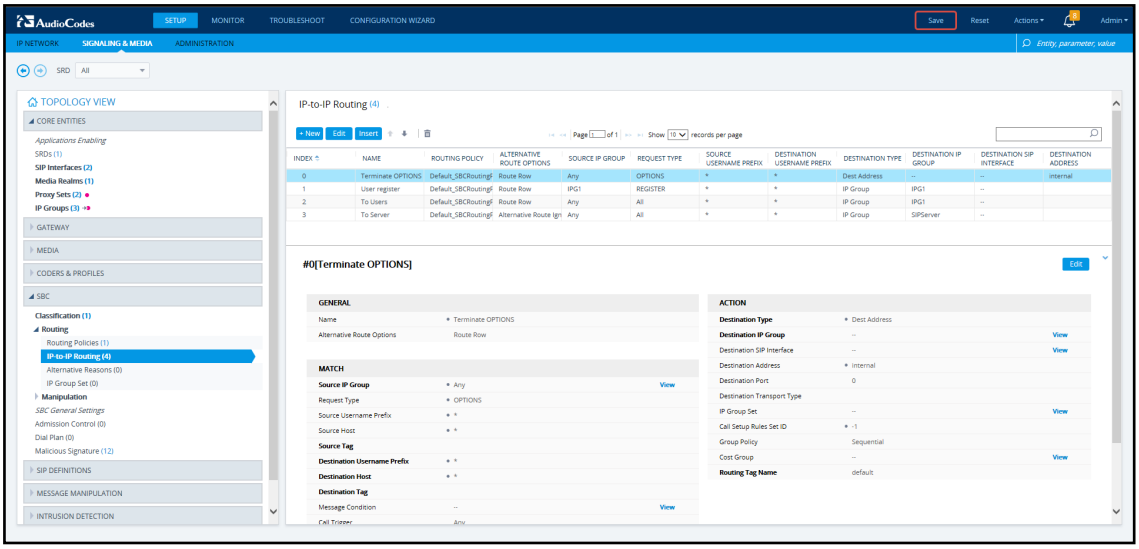
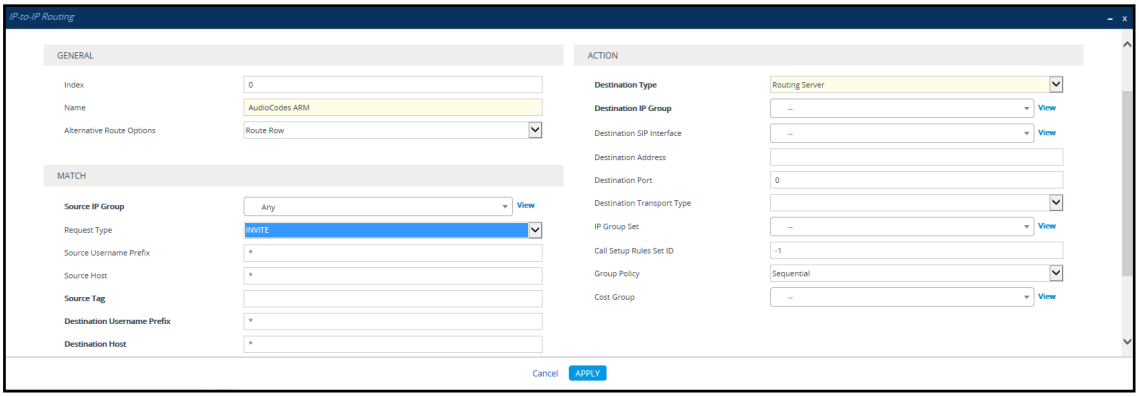


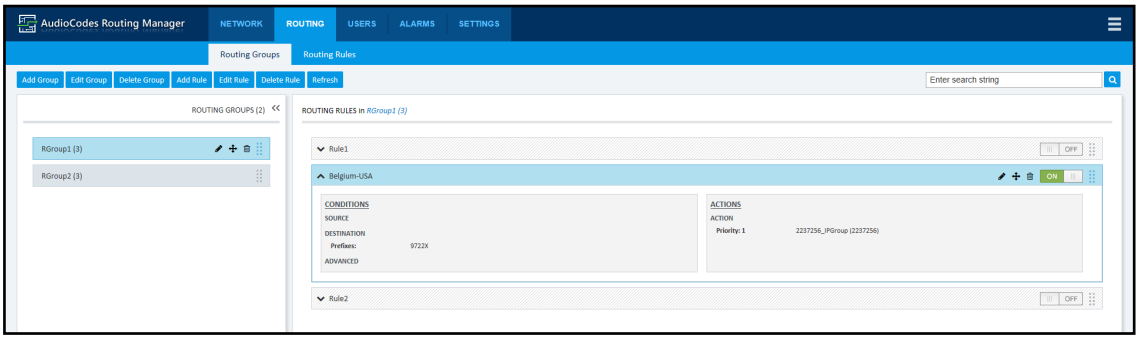
Figure 11-13: Web Interface – IP-to-IP Routing Table – Add Row – Rule tab



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 183 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 128).

Figure 11-14: Configuring a Routing Rule in the ARM



12. In the ARM GUI, switch **ON** 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 150 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 175.

Migrating Media Gateway Routing to the ARM

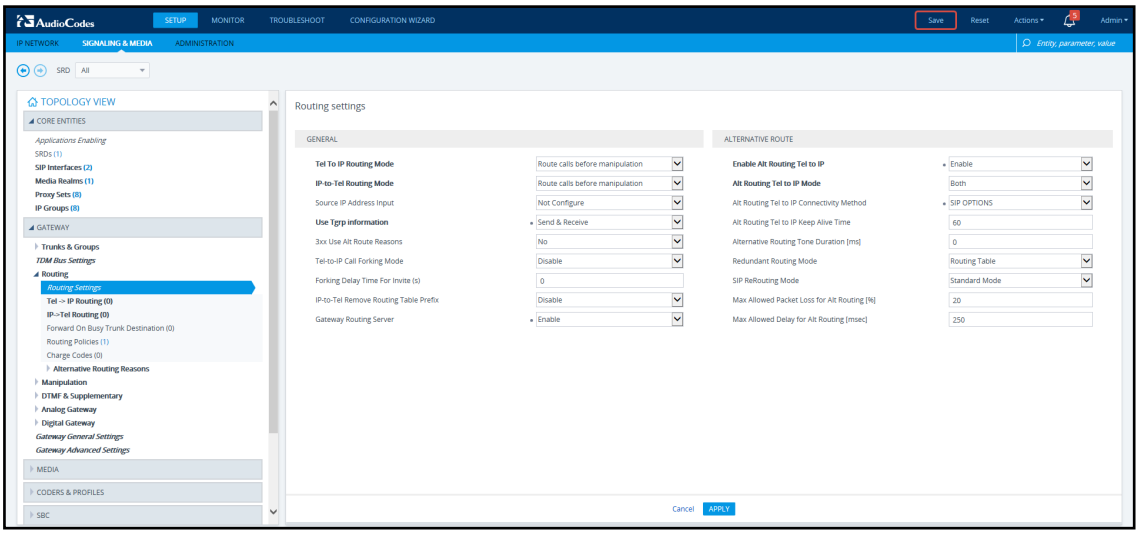
After making sure that the device (the gateway in this case) is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing rules from those defined in the Web interface to the ARM. Screenshots are for illustrative purposes.

'Trunk Group' and 'IP Group' in the Web are called 'Peer Connection' in the ARM.

➢ To migrate gateway routing rules to the ARM:

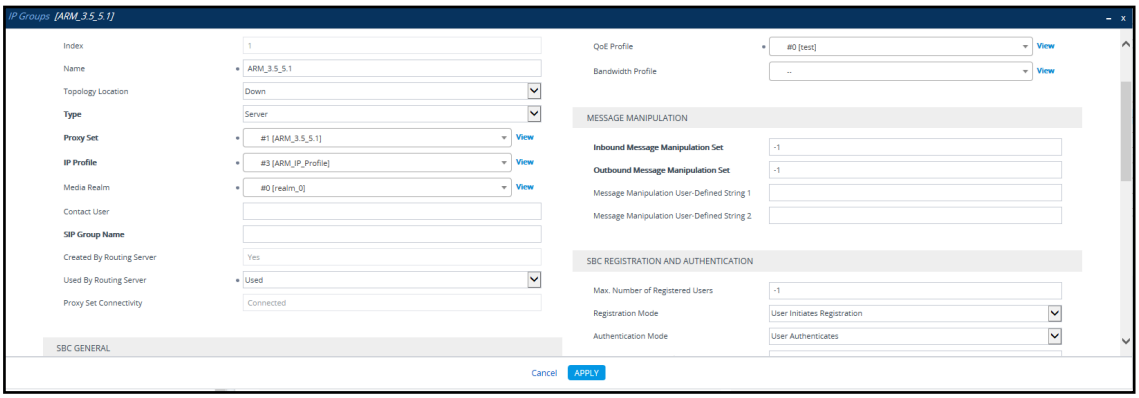
1. In the Web interface, navigate to the Routing Settings page, and set the parameter 'Gateway Routing Server' to **Enable**.

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**.

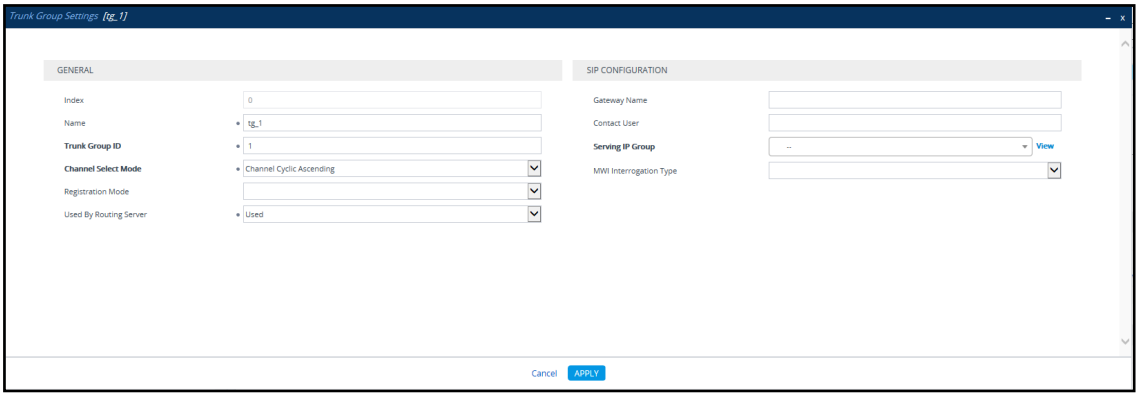
Figure 11-16: Web Interface - IP Groups Page



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.

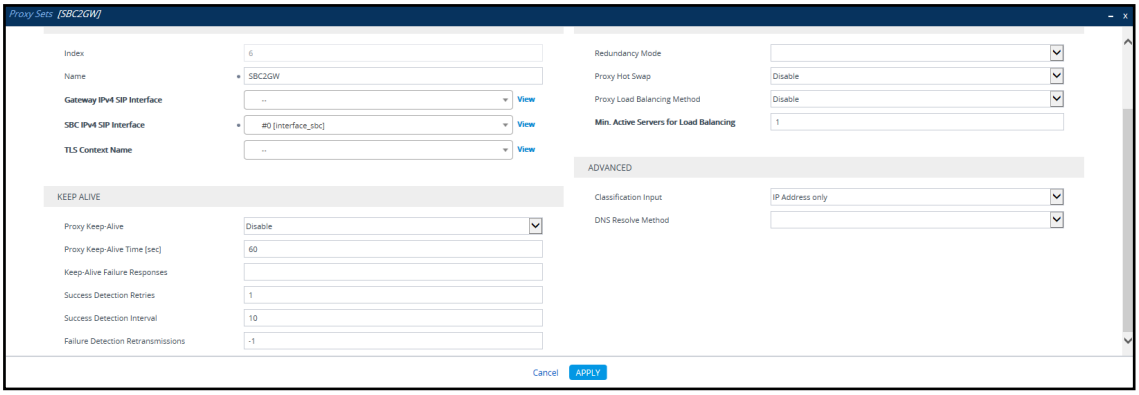
Migrating Hybrid Routing to the ARM

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:

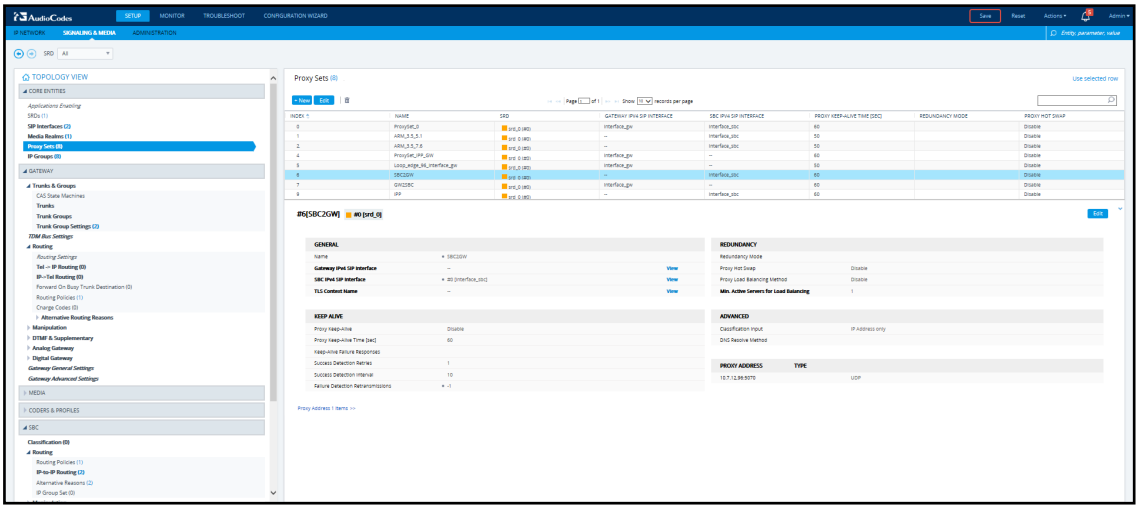
1. Perform migration of the SBC per the instructions in Migrating SBC Routing to the ARM on page 166.
2. Perform migration of the Media Gateway per the instructions in Migrating Media Gateway Routing to the ARM on the previous page.
3. Open the hybrid device's Web interface.
4. Create an IP Group (Peer 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



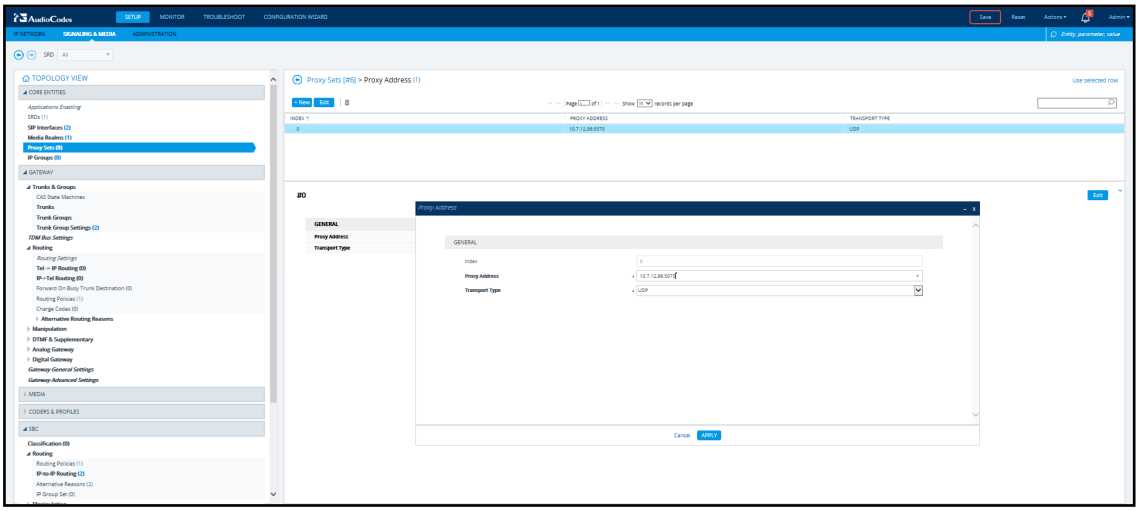
b. From the 'SBC IPv4 SIP Interface' drop-down menu, select **SBC SIP Interface** and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

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.

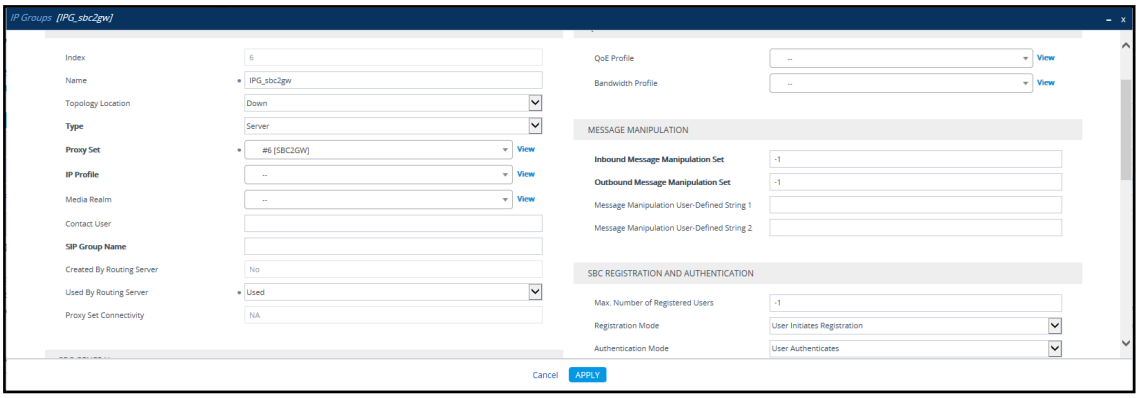
Figure 11-20: Add New Proxy Address



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.

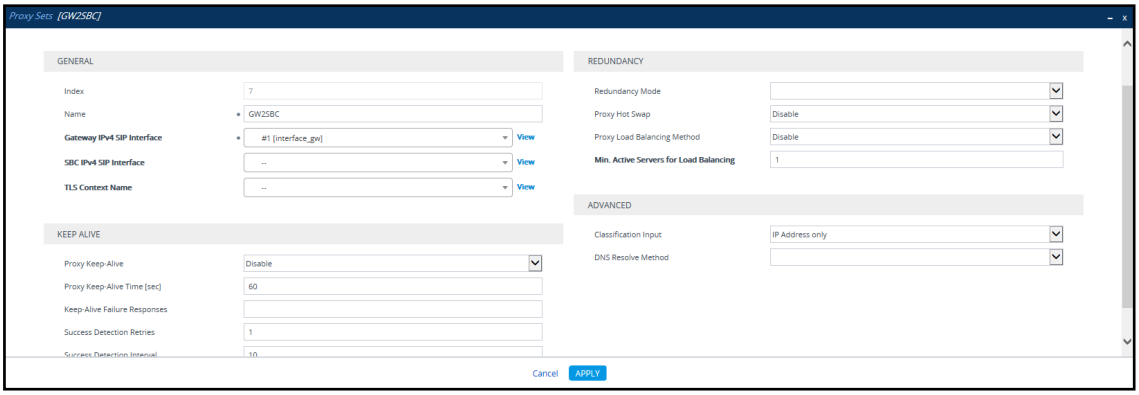
Figure 11-21: IP Group for the SBC Application



6. Create an IP Group (Peer Connection) for the *Media Gateway* application:

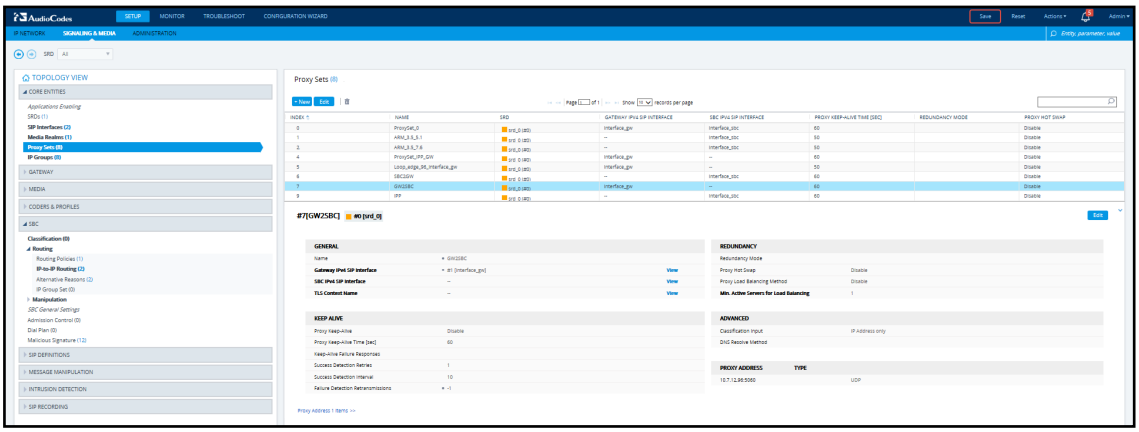
a. Open the Proxy Sets page (**Setup** > **Signaling & Media** > **Core Entities** > **Proxy Sets**) and then add a Proxy Set (click **New**) for the Media Gateway application:

Figure 11-22: New Proxy Set for Media Gateway Application



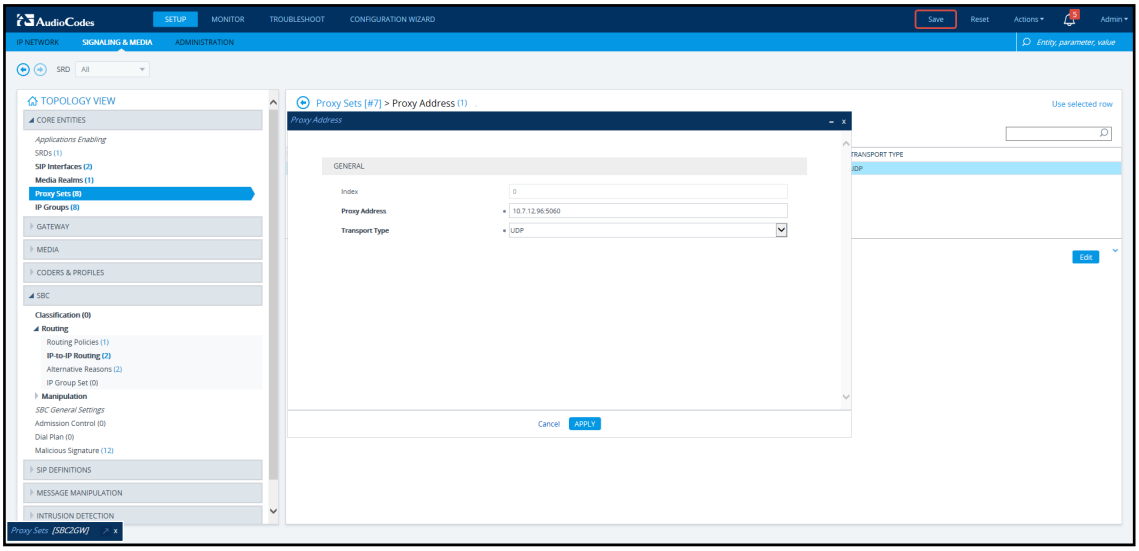
b. Select **Gateway SIP Interface** from the 'Gateway IPv4 SIP Interface' drop-down menu and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

Figure 11-23: Proxy Sets



7. From the Proxy Sets list shown in the figure above, select the proxy set you added and then click the Proxy Address link.

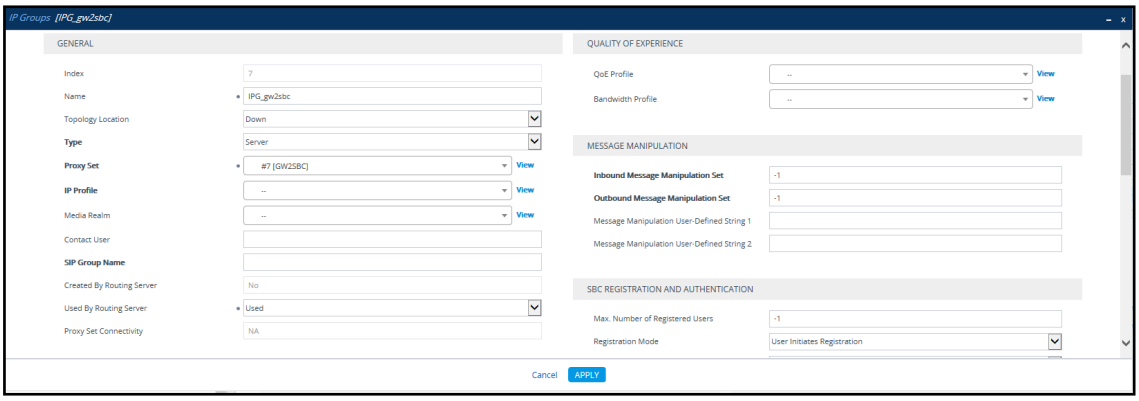
Figure 11-24: Add New Proxy Address



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



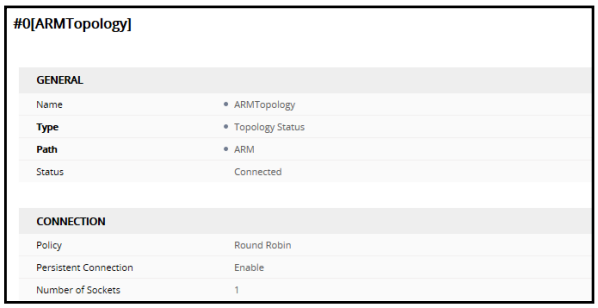
8. Click **Apply**. Check in the ARM that calls can be routed to and from the hybrid device.

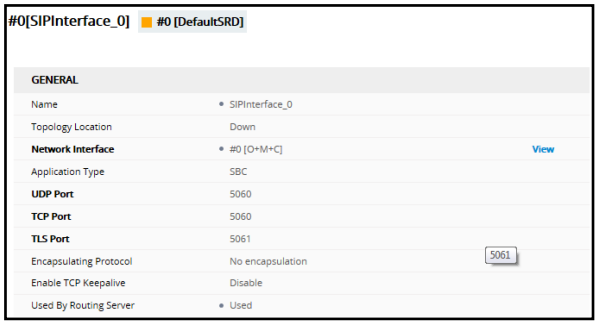
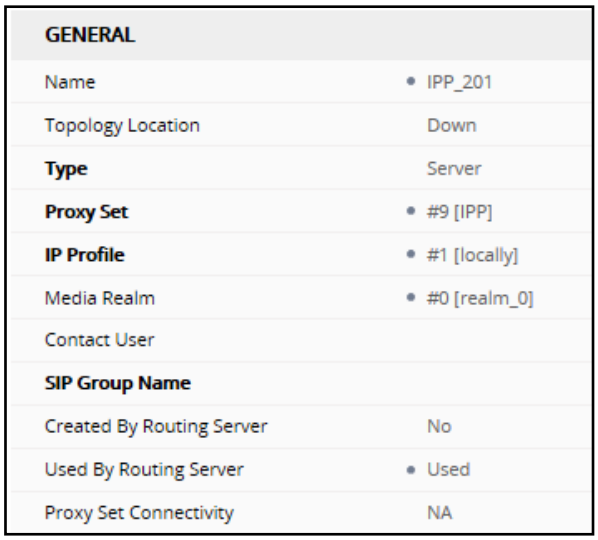
12 Checklist for Migrating SBC Routing to the ARM

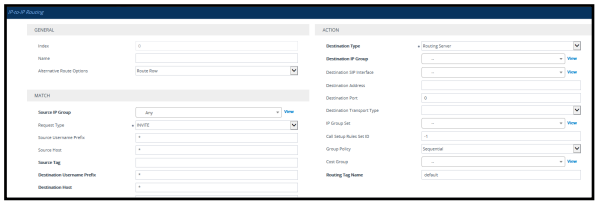
Administrators can use the checklist shown in the following table when migrating SBC routing to the ARM. Tick off the items in the list as you proceed.

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	Configure the IP address of the ARM's 'Configurator' **Note**: Do not configure Routers independently. Only configure 'Configurator' IP address and credentials: ■ Configure in the SBC's Web interface (**Setup** > **IP Network** > **Web Services** > **Remote Web Services**): ✔ IP address of the Configurator ✔ User name and Password for connecting to the Configurator. Default: Admin/Admin  #0[ARMTopology] GENERAL Name • ARMTopology Type • Topology Status Path • ARM Status Connected CONNECTION Policy Round Robin Persistent Connection Enable Number of Sockets 1 ■ Make sure the status of each ARM service is 'Connected'.	View the new Node. Make sure it becomes green-coded, indicating that it's available.
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'. ■ Open the SBC Web interface (**Setup** > **Signaling & Media** > **Core Entities** > **SIP Interfaces**)	You're able to select the chosen SIP Interfaces as ARM 'Routing Interfaces' for ARM Connections between the Nodes (SBCs)

Item	SBC-Level	What should be viewed in the ARM
		
4	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. ■ Open the IP Groups page (**Setup** > **Signaling & Media** > **Core Entities** > **IP Groups**). 	View the selected IP Groups as ARM Peer Connections and attached VoIP Peers. View their availability status (green/red). In the ARM, unlock these Peer connections.
5	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.	In the ARM you can now: ■ View and create ARM topology (connections between the Nodes) ■ Add ARM routing groups and Routing rules, manipulation groups, etc. ■ Test yourself using the ARM's 'test route'
6	Command the SBC to route calls using the ARM: ■ Open the SBC Web interface IP-to-IP Routing (**Setup** > **Signaling & Media** > **SBC** > **IP-to-IP Routing**).	Calls are now routed by the ARM: ■ SBC gets an INVITE ■ Sends routing Request to ARM ■ Get reply from ARM

Item	SBC-Level	What should be viewed in the ARM
	■ 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. 	■ Sends INVITE further according to the ARM's instructions
7	Configure manually using the ini file (or in the 'Admin' Web interface page): **SendAcSessionIDHeader** = **1**	Causes the SBC to preserve Call ID when a call passes through several SBCs.

13 Prefixes

Use the following table as reference when defining prefixes.

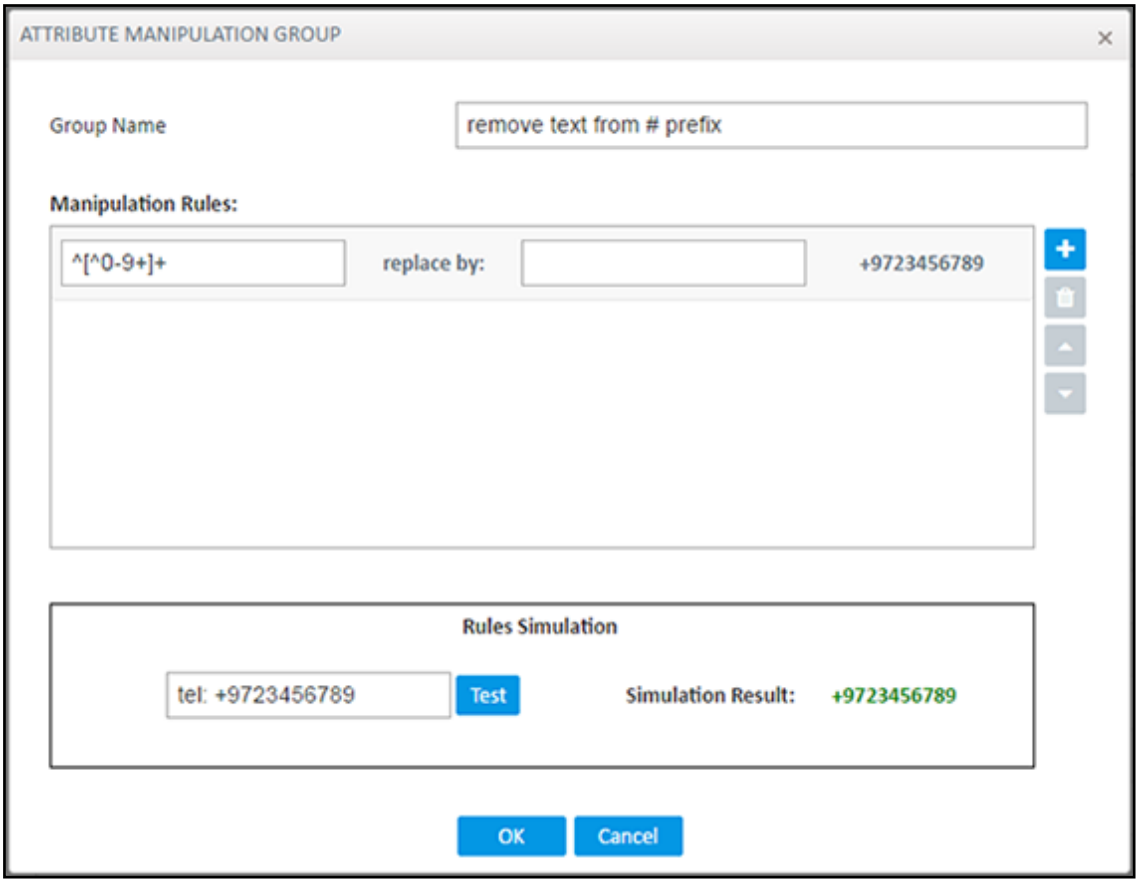
Table 13-1: Prefixes

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	

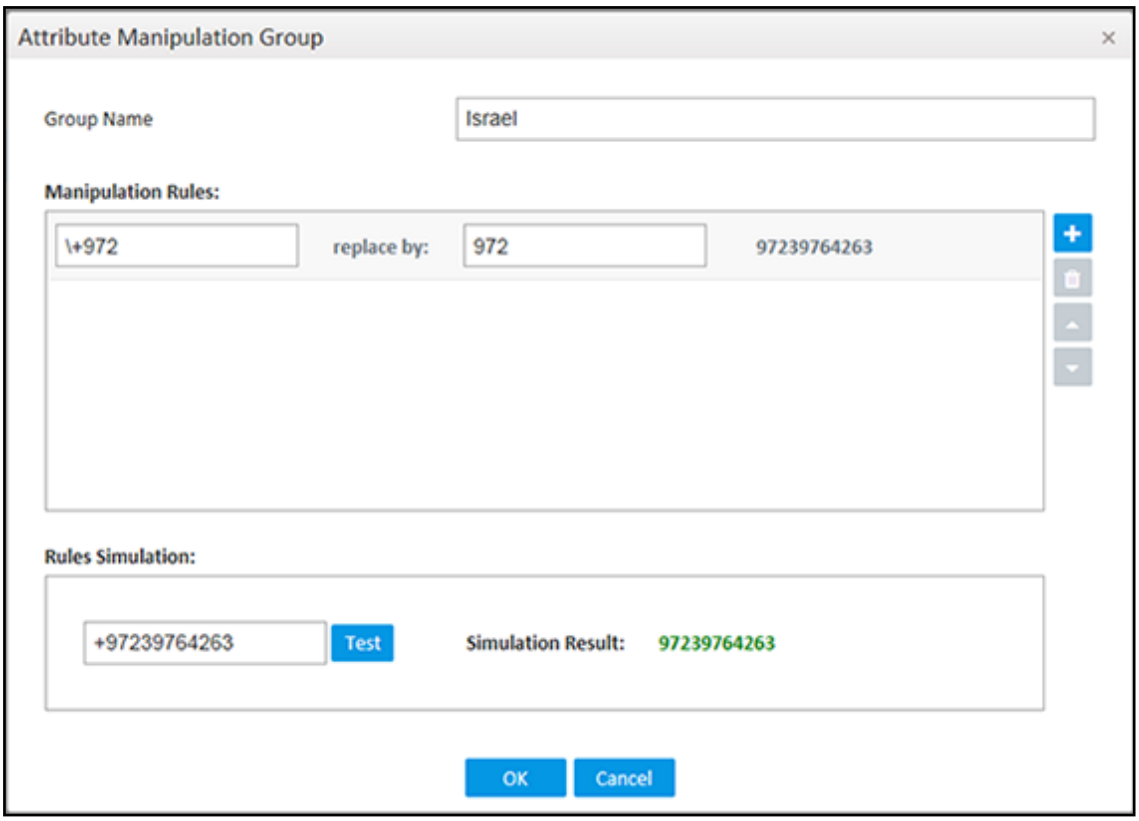
14 Examples of Normalization Rules

Here are some examples of Normalization Rules and regular expressions for your reference.

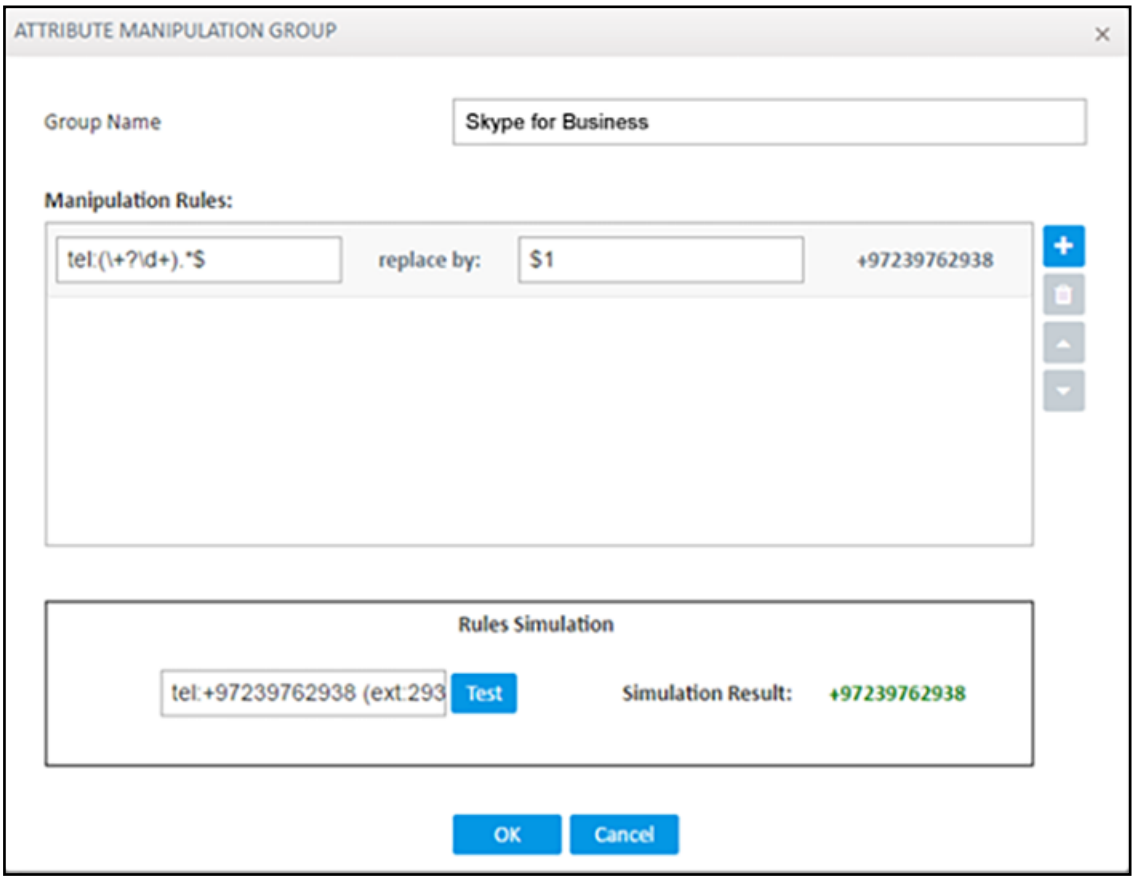
- Remove any non-number text from the prefix of the number:



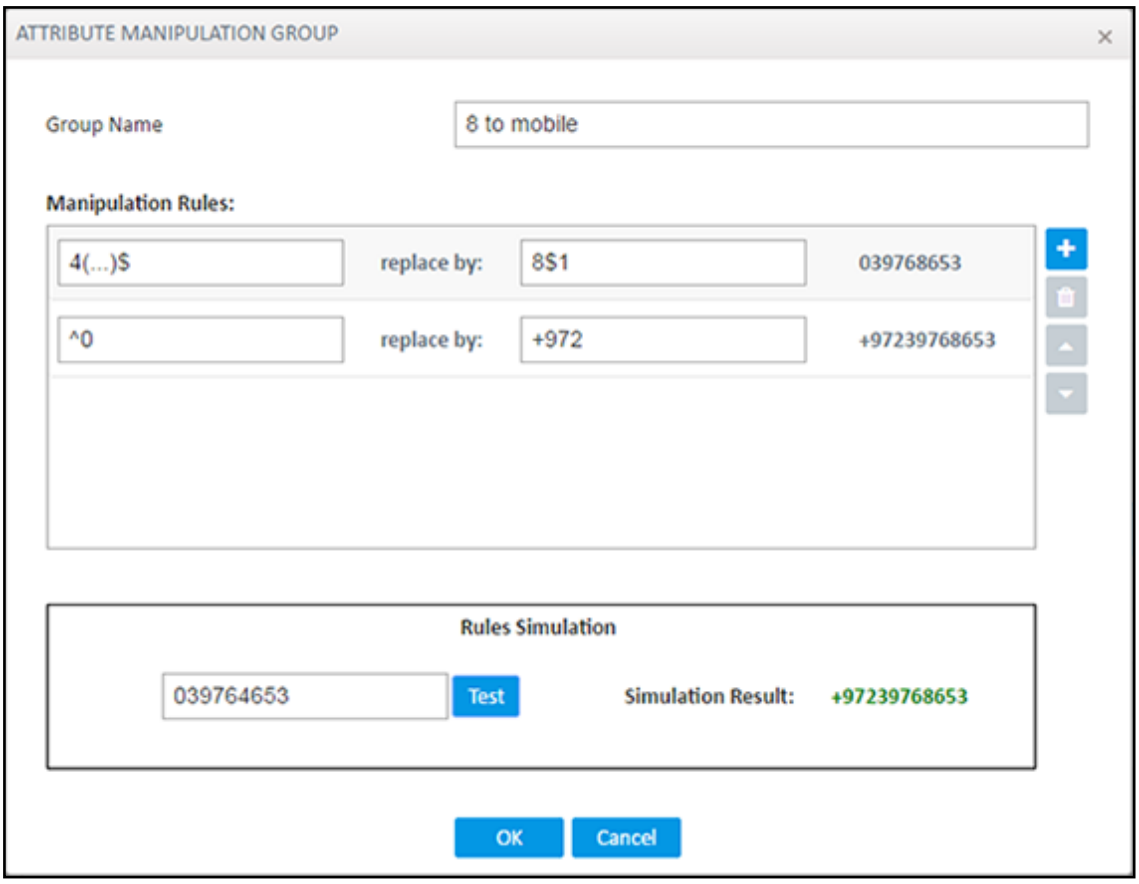
- Strip the **+** from the number.



- 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).



- If the fourth digit from the right is **4**, change it to **8**, and if the first digit is **0**, change it to **+972**.



- 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.

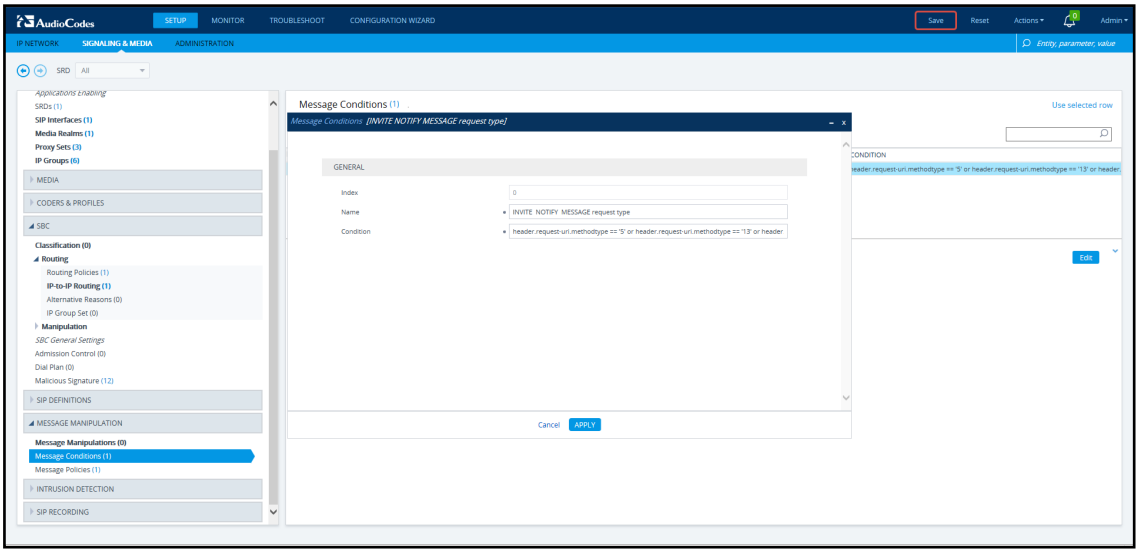
16 Configuring an SBC to Send SIP Requests other than INVITE to ARM

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:**

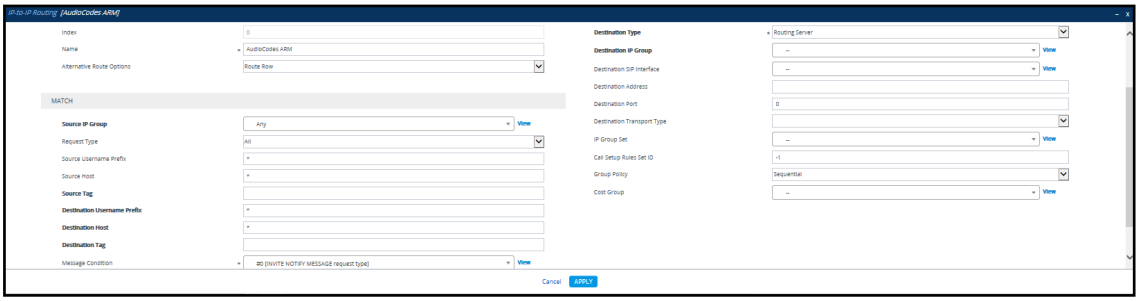
1. Open the Message Conditions page (**Setup** > **Signaling & Media** > **Message Manipulation** > **Message Conditions**) and click **Add**.

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 Opening Firewall Ports for the ARM

Ports for the ARM must be opened in the Firewall. Use the following table as reference.

Table 17-1: 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
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'	Getting of ARM AD users and updating ARM user database	Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
			Default, can be configured at ARM)	LDAPS (TLS) is configured at ARM	
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 SNMP Target.	Outgoing
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

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
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
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)					

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
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 topology status and quality changes)	Incoming
ARM Router → JMS Broker	TCP (TLS)	✓	8080	Getting Topology updates from ARM	Outgoing

18 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 18-1: 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 staring with 1.	All	String (10)
CreationDate	The creation date of the CDR.	All	String (40)
CdrReportType	Report type: ■ "CALL_START": CDR is sent upon an getRoute message on the first node. ■ "CALL_END": CDR is sent upon a CALL_STATUS_ END_CALL message from the node.	-	String (13)

CDR Field	Description	CDR Report Type	Format
AppType	Endpoint type: ■ "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)

CDR Field	Description	CDR Report Type	Format
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)
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)

CDR Field	Description	CDR Report Type	Format
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)
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 |dstUri |dstUriBeforeMap |armSetupTime
|armReleaseTime |sbcSetupTime |sbcConnectTime |sbcReleaseTime |sbcAlertTime
|alertDuration |voiceDuration |completeDuration |sipTerminationReason
|sipTerminationReasonDesc |routeSeq |legId |routingRuleId |routingRuleName
|discardingByRoutingRule |path
```

Value:

```
|10.7.6.102 | 2 | 2019-02-21T08:53:15.123Z | CALL_END | SBC | 7018782a40c69c13 |
75aed8-8802070a-13c4-55013-16cc4-7c2dd6ce-16cc4 | RMT | 102 | 4 | SBC_97 | 10.7.12.97
|null |null |IPGroup | |null |null |IPGroup |null |null |  |  |102@10.7.2.136  |  |201@10.7.12.97  | |
|2019-02-21T08:53:15.116Z |23:27:10.537  UTC Wed Feb 07 2018 |23:27:13.554  UTC Wed
Feb 07 2018 |23:27:18.842  UTC Wed Feb 07 2018 |23:27:10.837 UTC Wed Feb 07 2018
|2717 |5288 |8305  |BYE |BYE |0 |1 |-1 |  |-1  |null
```

Here's an example of an ARM signaling CDR as JSON, sent at the end of a call (that was terminated normally):

```
jsonCdr={"creationDate":"2019-02-
21T08:53:15.123Z","sessionKey":"47018782a40c69c13","routerIp":"10.7.6.102","seq":2,"c
drReportType":"CALL_
END","cdrApplicationType":"SBC","sessionId":"7018782a40c69c13","callId":"75aed8-
8802070a-13c4-55013-16cc4-7c2dd6ce-
16cc4","callOrig":"RMT","pconOrConName":"102","nodeId":"4","nodeName":"SBC_
97","nodeIp":"10.7.12.97","pconId":null,"conId":null,"pconOrConType":"IPGroup","sipInterf
ace":"","outPconId":null,"outConId":null,"outPconOrConType":"IPGroup","lastPconId":null,
"lastNodeId":null,"lastNodeName":"","lastPconName":"","srcUri":"102@10.7.2.136","srcU
riBeforeMap":"","dstUri":"201@10.7.12.97","dstUriBeforeMap":"","armSetupTime":"","arm
ReleaseTime":"2019-02-21T08:53:15.116Z","sbcSetupTime":"23:27:10.537  UTC Wed Feb
07 2018","sbcConnectTime":"23:27:13.554  UTC Wed Feb 07
2018","sbcReleaseTime":"23:27:18.842  UTC Wed Feb 07
2018","sbcAlertTime":"23:27:10.837 UTC Wed Feb 07
2018","alertDuration":"2717","voiceDuration":"5288","completeDuration":"8305","sipTermin
ationReason":"BYE","sipTerminationReasonDesc":"BYE","routeSeq":0,"legId":1,"routingR
uleId":-1,"routingRuleName":"","path":null,"discardingByRoutingRule":-
1,"httpResponse":200,"description":""}
```

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-400s0
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/

Document #: LTRT-41890