User's Manual

AudioCodes One Voice Operations Center

AudioCodes Routing Manager (ARM)

Version 10.0.100

AudioCodes Routing Manager

audiocodes

Notice

Date Published: November-27-2024

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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 Release Notes
ARM Installation Manual

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

Document Revision Record

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

LTRT	Description
	integration with Azure AD. Appending | deleting Prefixes in a Prefix Group via the REST API. VoIP Peers page. Customized ARM Connection (IP Group Name, user-defined IP Profile & Media Realm. Authentication order.
41896	Calls Details - RegEx, CSV. Centos Stream 8. Server Certificates (Configurator, Routers). Examples of Unselected Rules Reasons. No answer timeout. SecureLogix Orchestra One CAS (Call Authentication Service). Number of standard security queries (per month); Number of advanced security queries (per month). License Details. Statistics Thresholds Based Alarms. Manipulation before route; Manipulation after route. Max # of Unselected Rules in calls. Global Routing Settings (Unselected Rules). Adding Node Info to Call Details. Alternative Routing SIP Reasons.
41897	Device Location.
41898	Google Material Design. Dashboard. Dynamic Blacklist. Statistics Retention Policy. Request for Authentication: Register Sequence - Configuring IP-to-IP Routing in SBC Web interface. Upgrade Sequence. Enable Parallel Connections (Multiple Sockets). Increased capacity. Capacity enforcement. 300 Nodes; 30000 Peer Connections; 150 ARM Routers. New Platforms: KVM and OpenStack. Save AudioCodes Device INI File from ARM GUI. Edges Status. New 'Description' Field in 'Add | Edit Normalization Group'.
41899	Security Features: Security Policies (Adding | Customizing a Security Policy, Customized Security Policy Example, Updating a Security Policy, Attaching a Security Policy to an Operator). Operators can Change their Own Password. Using Network Access Server (NAS) with RADIUS Authentication. Sending Journal Events to OVOC. Routing Features: SIP Conditions and Manipulations for SIP Header Fields. Routing Rules: Preventing Source Loopback, Improved UX for Selected/Unselected Routing Rules. User Management Features: File Repository Supports Uploading CSV File with 'UTF-8' Encoding.
43000	Updated to Ver. 9.8.200. Custom REST API Request. New Actions in File Repository. UMP Server.
43001	Version 10.0. Rocky Linux 8.9.
43002	Updated to Version 10.0.100. WebSocket Tunnel. Live. Advanced LDAP Settings - Enable Referrals. Opening Firewall Ports. Operator Status (Active Block).

Table of Contents

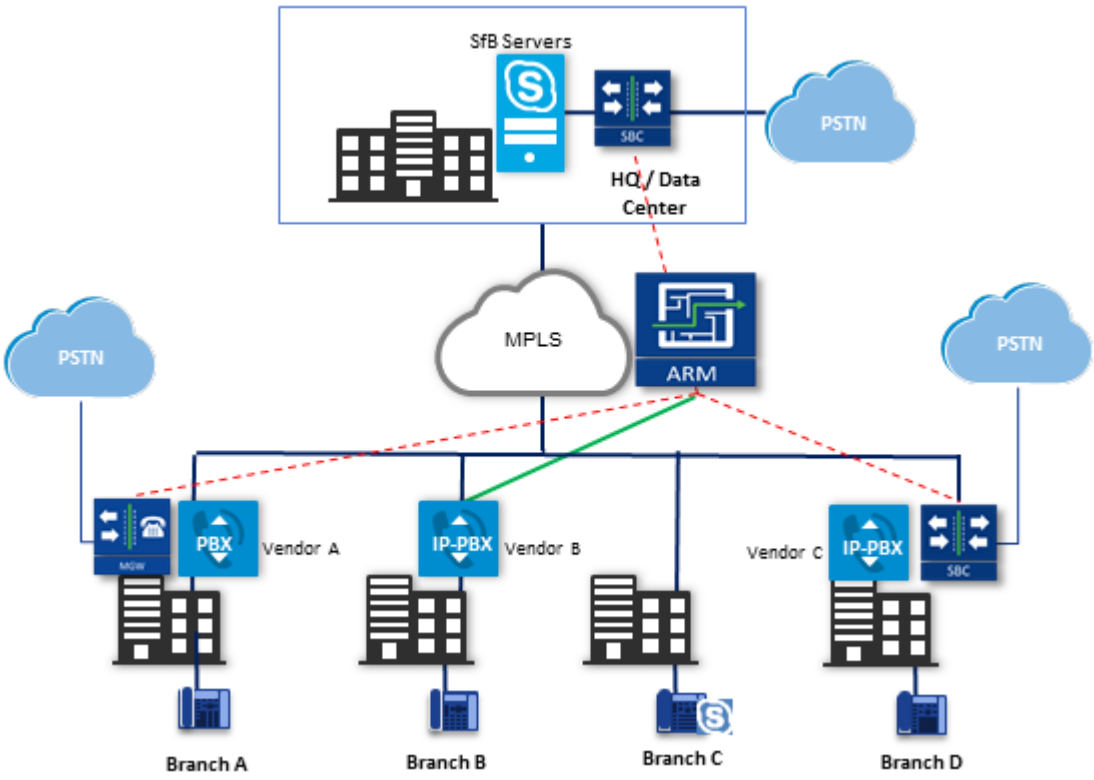
1 Overview

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

The ARM supports the following features:

- 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 IP telephony network operators 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
- Customized topology network
  - Configuring a connection is as simple as drawing a line
  - Modify by adding, deleting and changing connections
- ARM connects to user data base

ARM-Routed Devices

The following devices can be routed by the ARM:

- Mediant 9000 SBC
- Mediant 4000 SBC
- Mediant 2600 SBC
- Mediant SE/VE SBC
- Mediant 1000B Gateway and E-SBC
- Mediant 800B Gateway and E-SBC
- Mediant 800C
- Mediant 500 E-SBC
- Mediant 500L SBC
- Mediant SBC CE (Cloud Edition)
- Mediant 3000 Gateway only
- Mediant 3100 SBC, Gateway or Hybrid
- MP-1288 Media Gateway

Third-Party Open-Source Software

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

- Apache Commons - Apache License 2.0
- JSON.simple by Google – Apache License 2.0
- Json-path - Apache License 2.0
- Caffeine - Apache License 2.0
- TinyRadius – LGPL
- MongoDB - Apache License 2.0
- Rocky Linux 8.9 operating system
- Spring Framework - Apache License 2.0
- MariaDB - LGPL-2.1
- ActiveMQ - Apache License 2.0
- HiberNate - LGPL-2.1
- Log4J - Apache License 2.0
- Guava (Google core libraries) - Apache License 2.0
- Jackson - Apache License 2.0
- HttpClient5 - Apache License 2.0
- Jersey client - Apache License 2.0, MIT, EPL 2.0
- Joda-Time - Apache License 2.0
- Json - Apache License 2.0
- Junit - Common Public License Version 1.0
- HikariCP - Apache License 2.0
- Aspectj™ extension to Java -Eclipse Public License - v 1.0
- SNMP4J - Apache License 2.0
- Mockito - MIT
- Tomcat 9 - Apache License 2.0
- Angular 8 - MIT
- Microsoft Graph SDK for Java - MIT
- AZURE SDK for Java – MIT
- Failsafe - Apache License 2.0
- Fastcsv - Apache License 2.0

- Gson - Apache License 2.0
- Lettuce - Apache License 2.0
- Jdbc - LGPL-2.1
- Micrometer - Apache License 2.0
- Msal4j - MIT
- Disruptor - Apache License 2.0
- OkHttp - Apache License 2.0
- Slf4j- MIT
- Sslcontext-kickstart - Apache License 2.0
- Zip4j - Apache License 2.0

2 Getting Started with the ARM

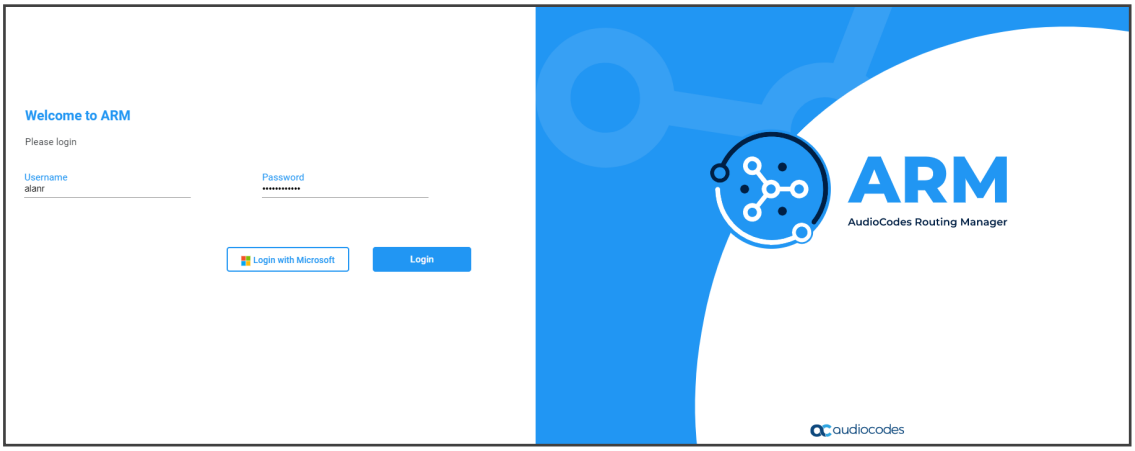
After installing the ARM and performing initial configuration (see the *ARM Installation Manual*), you can get started managing routing with the ARM.

Logging in

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

➢ **To log in:**

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



2. In the Login to ARM screen, log in using the default **Operator** and **Operator** username and password. It's advisable to change these as soon as possible (see Provisioning Operators on page 194 for instructions on how to change them).
3. Click the **Sign in with Microsoft** button if you're operating with Azure Active Directory. See Authenticating Operator Login Using Azure AD on page 220 for more information.

The ARM opens on the Dashboard page by default in your browser.

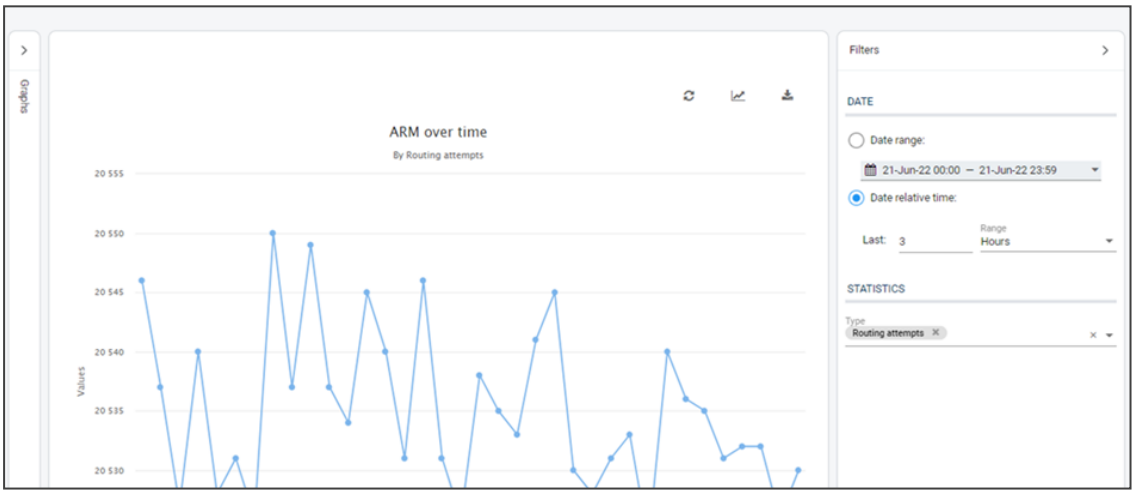
Getting Acquainted with the ARM GUI

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.

AudioCodes' clean and modern ARM GUI design uses Google Material Design's basic components and principles, making it intuitive and clear for network operators. All ARM pages and GUI functionalities are designed in this style. The following generic principles are common in the new design:

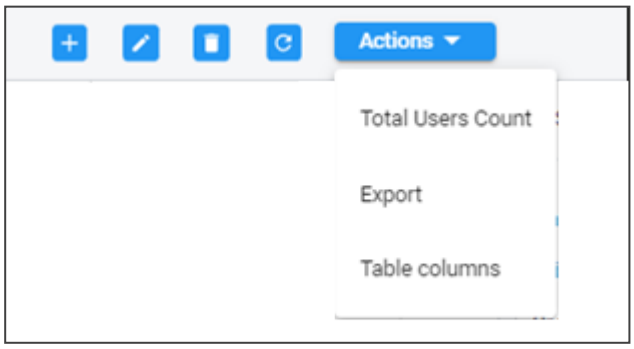
Side pane

All ARM pages have at least one side pane. Sometimes there are two, on the left and the right side of the page's main pane. Network operators can easily collapse a side pane to provide more space for the page's main pane. In the following example, the left pane is collapsed (operators can view its name: 'Graphs') while the right pane is expanded:



Actions buttons

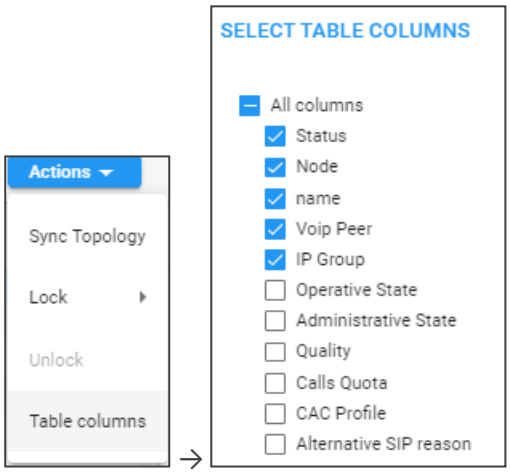
Pointing the mouse over the intuitive actions icons available on each page displays a tooltip. The icons include 'Add', 'Edit', 'Delete' and 'Refresh'. All other actions (specific per page) can be selected from the **Actions** drop-down.



'Tables' pages: GUI principles

The majority of the ARM's provisioning screens are in tabular format. All ARM pages that display 'tables' such as the Nodes page, the Peer Connections page, the Users page as well as other pages such as the VoIP Peers page, the Connections page, the Resource Groups page, the IP Profiles page and the Customers page, feature the following structural elements:

- A Summary pane on the right side of the page summarizes information related to the row selected in the 'table'.
- A 'Search' field and an 'Advanced Search' link allow network operators to filter each page by specific criteria to remove unwanted information from the page, display only required information, unclutter the page and thereby facilitate effective management.
- Columns in the 'tables' can be widened or narrowed according to the requirements and preferences of the network operators, by selecting **Table columns** from the **Actions** drop-down:



Here's the Peer Connections page displaying these configured columns:

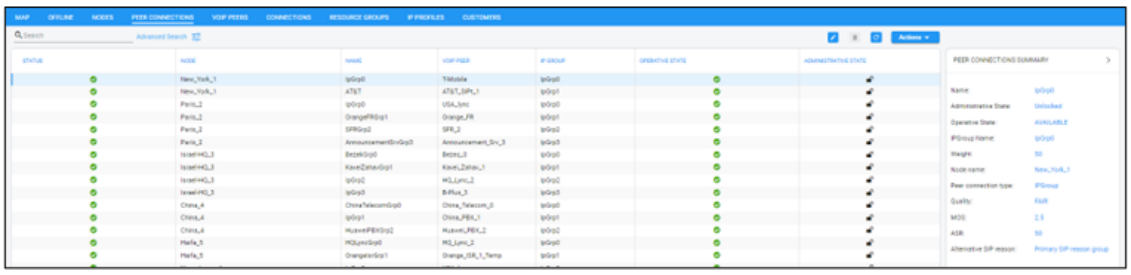
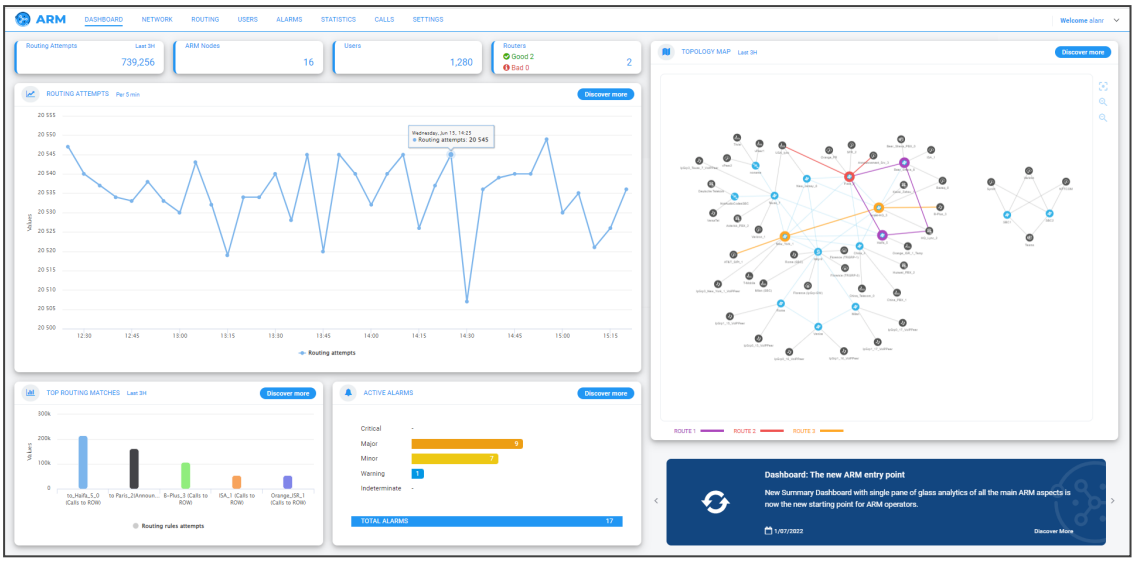


Figure 2-1: Dashboard

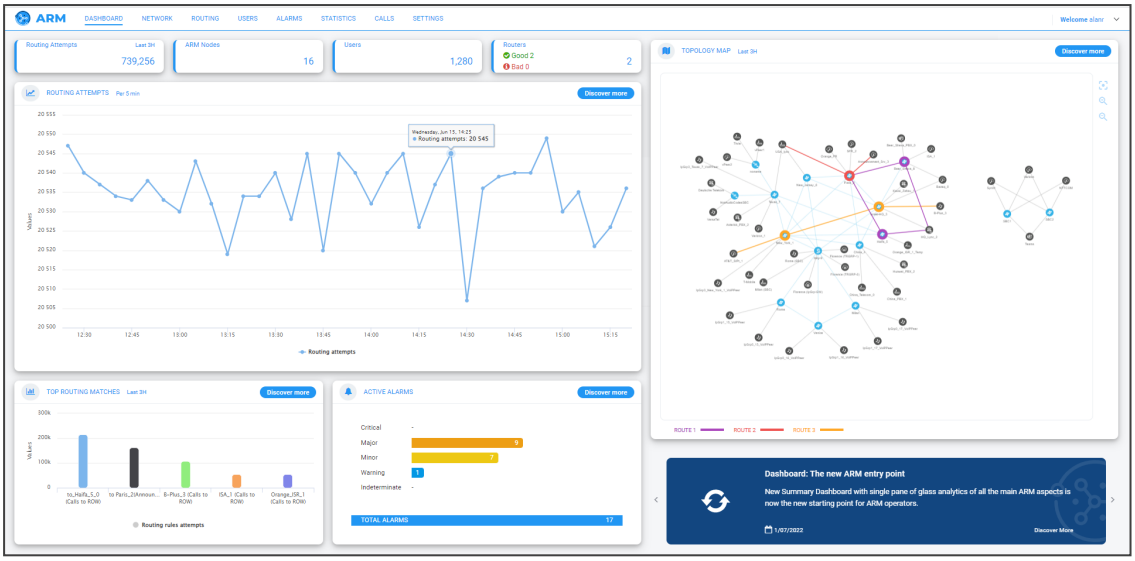


The Dashboard shows (L-R):

- Routing Attempts pane. Click **Discover more** to access the Routing Attempts graph under the **Statistics** menu (see Viewing Statistics and Reports on page 116 for more information). In the pane, operators can also immediately see:
  - the # of ARM nodes in the managed network
  - the # of users in the managed network
  - the # of good routers and bad routers in the managed network
- Top Routing Matches pane allowing network operators to determine at a glance the top routing matches that were made in a time frame in their IP telephony network. Click **Discover more** to directly access the Top Routing Rules graph under the **Statistics** menu (see under Viewing Statistics and Reports on page 116 for more information).
- Active Alarms pane, allowing network operators to determine at a glance the active alarms in the network. Click **Discover more** to access the Active Alarms page under the **Alarms** menu (see Active Alarms | History Alarms on page 372 for more information).
- Updates pane. Constantly provides operators new updates and features from the ARM server. To view each new update | feature, click > displayed on the right. To go back, click < then displayed on the left. To access an update | feature, click the **Discover More** link. To receive dynamic updates, the ARM Web client must have access to AudioCodes' portal. If this is not possible, customers are presented with the latest features released in the version they currently have.
- Network Map page: an uncluttered, operator-friendly summary of the entire IP telephony network. Click **Discover more** (or navigate to **Network** > **Map**) to open the Network Map page. By default, the Network Map page displays all VoIP entities managed in the network.

Getting Acquainted with the Dashboard

After logging in, the Dashboard opens by default.



The Dashboard shows (L-R):

- Routing Attempts pane. Click **Discover more** to access the Routing Attempts graph under the **Statistics** menu (see Viewing Statistics and Reports on page 116 for more information). In the pane, operators can also immediately see:
  - the # of ARM nodes in the managed network
  - the # of users in the managed network
  - the # of good routers and bad routers in the managed network
- Top Routing Matches pane allowing network operators to determine at a glance the top routing matches that were made in a time frame in their IP telephony network. Click **Discover more** to directly access the Top Routing Rules graph under the **Statistics** menu (see under Viewing Statistics and Reports on page 116 for more information).
- Active Alarms pane, allowing network operators to determine at a glance the active alarms in the network. Click **Discover more** to access the Active Alarms page under the **Alarms** menu (see Active Alarms | History Alarms on page 372 for more information).
- Updates pane. Constantly provides operators new updates and features from the ARM server. To view each new update | feature, click > displayed on the right. To go back, click < then displayed on the left. To access an update | feature, click the **Discover More** link. To receive dynamic updates, the ARM Web client must have access to AudioCodes' portal. If this is not possible, customers are presented with the latest features released in the version they currently have.
- Network Map page: an uncluttered, operator-friendly summary of the entire IP telephony network. Click **Discover more** (or navigate to **Network** > **Map**) to open the Network Map page. By default, the Network Map page displays all VoIP entities managed in the network.

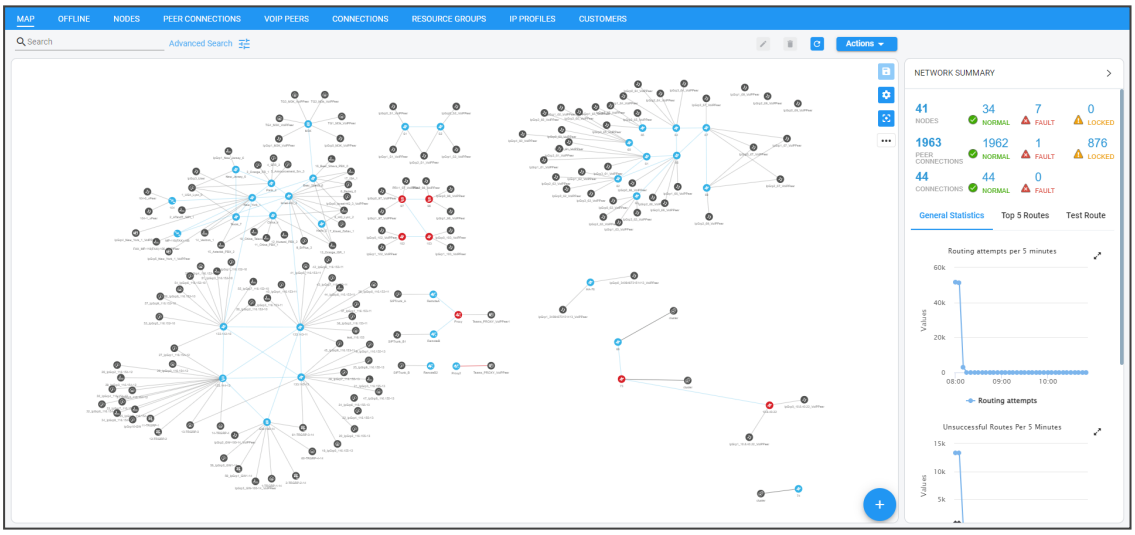
Getting Acquainted with the Network Map

The ARM's Network Map page provides an uncluttered, operator-friendly summary of the entire IP telephony network. By default, the page displays all VoIP entities managed in the telephony network. In the page, you can view node information and perform network map actions. The page shows the four main network entities that comprise the network topology (see here for an explanation of each):

- Node
- VoIP Peer
- Peer Connection
- Connection

➢ To open the Network Map page:

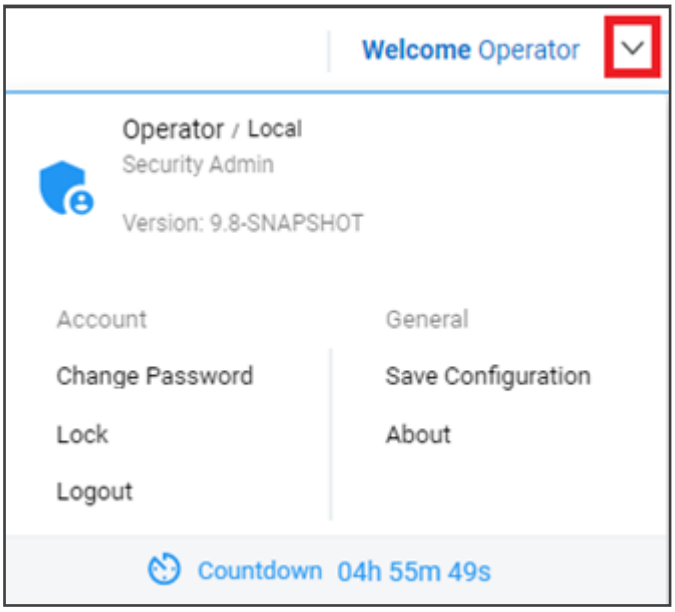
1. In the Dashboard, click **Discover more**, or navigate to **Network** > **Map**; by default, the Network Map page displays all VoIP entities managed in the network.

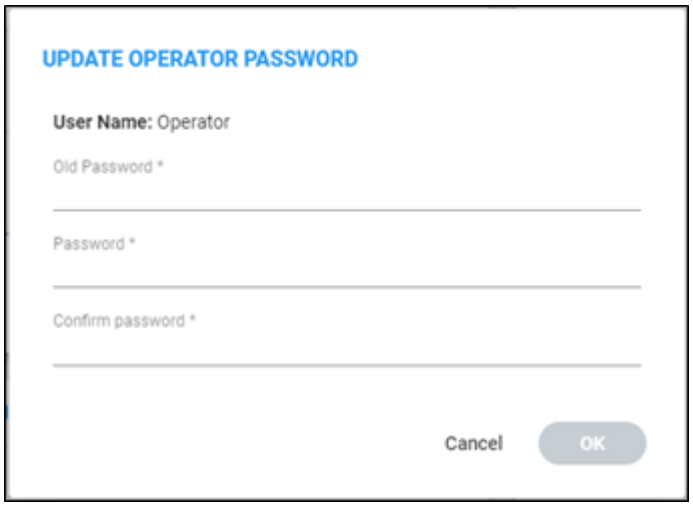


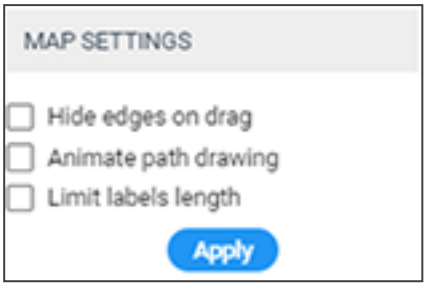
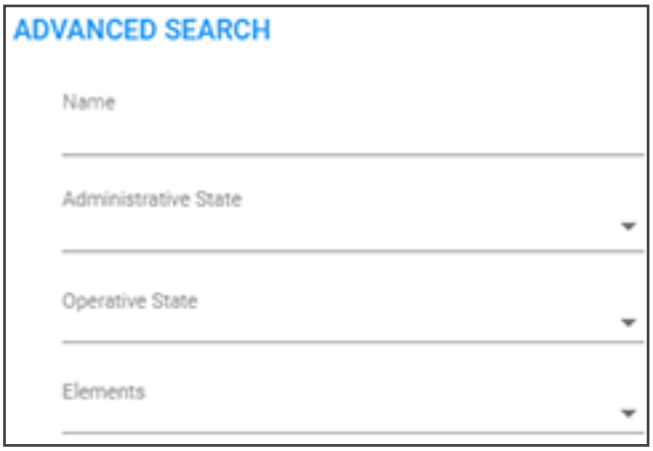
2. Use the following legend as a reference to the preceding figure.

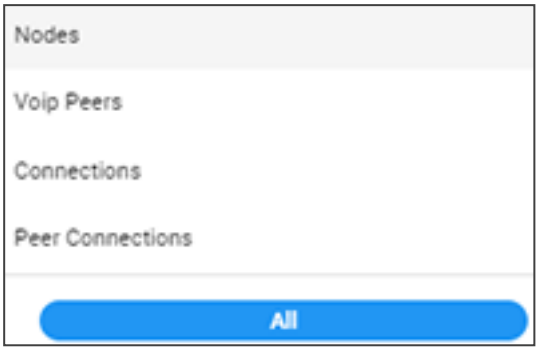
Table 2-1: Network Map page

GUI Area	Description
Actions	Click to select an action:

GUI Area	Description
	
	Click to select a Layer by which to filter the Network Map page: ✓ topology ✓ quality ✓ quota ✓ CAC See also Getting Acquainted with Network Map Layers on page 31
Toolbar	Toolbar icons let you navigate to the following ARM pages: DASHBOARD, NETWORK, ROUTING, USERS, ALARMS, STATISTICS, CALLS 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

GUI Area	Description
	Level defined in a Security Policy ■ Change Password: Operators *who were defined in the ARM* can change password. If **Operator / Local** is indicated as in the preceding figure, the logged-in operator can change their own password. If you logged in externally via LDAP or Azure, for example, you cannot change password. The 'Update Operator Password' screen then opens:  ■ Lock (Terminates user's ARM GUI session) ■ Save Configuration: The ARM_Configuration.zip file (ARM database) is saved locally in the client's 'Downloads' directory. You can send it to AudioCodes for troubleshooting. In parallel, basic ARM backup is performed and the backup file is stored in the configurator's /home/backup directory. You can use it to restore the configuration on the same machine using standard ARM restore procedure. ■ Logout ■ About: Displays the ARM version ■ Countdown: Displays how much time remains before the session terminates
	Saves entities' positions in the Network Map after they're moved.
	Map settings (opens the Map Settings pop-up menu):

GUI Area	Description
	 ■ For more information about **Hide edges on drag**, see Repositioning Elements in the Network Map Page on page 54 ■ Select **Animate path drawing** for animated visualizations of Test Route and Top Route actions. ■ Select **Limit labels length** to limit the lengths of the labels of the displayed Nodes and VoIP Peers to a predefined number of characters, useful with large networks and long Node and / or VoIP Peer names which clutter the Network Map. If selected, the parameter 'Max label length' is displayed in which the maximum number of characters allowed is defined.
	Center map; centers the Network Map in the middle of the page.
	Enables you to locate specific information in the Network Map page, Routing page, Users page, Alarms page and Settings pages. 1. Click **Advanced Search**.  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 useful functionality in very large deployments with high numbers of Nodes.

GUI Area	Description
	4. Click the 'Elements' drop-down and optionally filter for these: 
Main Screen	The Network page displays a Map view of network entities.
Summary Panes	The Network Map page 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

3. Use the following table as reference to each of the network entities that comprise the network topology.

Table 2-2: 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

Network Entity	Icon	Explanation
	 	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 (such as Teams) communicating with the ARM. It's part of the ARM network topology.
VoIP Peer		Indicates a non-AudioCodes device or entity that is also part of the ARM network topology: Teams, PBXs, SIP trunks, other vendors' SBCs / gateways. These devices participate in processing ARM network calls and are connected to Nodes by 'Peer Connections'. The ARM operator can configure one of six VoIP Peer types.
		Teams
		SIP trunk

Network Entity	Icon	Explanation	
			PSTN
			IP phones
			IP PBX
			Legacy PBX
Connection		Indicated by a blue line (available) or a red line (unavailable). Joins two Nodes. Calls can be routed between two Nodes only if there is a Connection between them. Defined by adding an IP Group (at Node level). From AudioCodes' gateway/SBC perspective, a 'Connection' is an 'IP Group'. Connections between Nodes are added by the ARM operator.	
Peer Connection		Indicated by a black line between a Node and a VoIP Peer. Represents a group of routing destinations/sources (connections to a VoIP Peer), 'last mile' connectivity. From AudioCodes' gateway/SBC perspective, a Peer Connection is a 'PSTN Trunk Group' or 'IP Group'. Red line = administrative state is unlocked / operative state is unavailable (no connection between the 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 Operators can lock / unlock a Peer Connection as well as select a *directional based* lock / unlock which allows for example stopping *only traffic towards* a specific VoIP Peer (for example, a specific IVR) while *calls coming from* this VoIP Peer will still be routed to their destination. The feature can be used to perform a graceful stoppage of traffic for maintenance reasons (for example). The feature is essential for IVR VoIP Peers when there are always calls in a queue that are not yet connected to an agent. From the IVR's perspective, the connection to the agent is outbound calls; without the uni-directional lock feature, calls fail. The Map page and Peer Connections page	

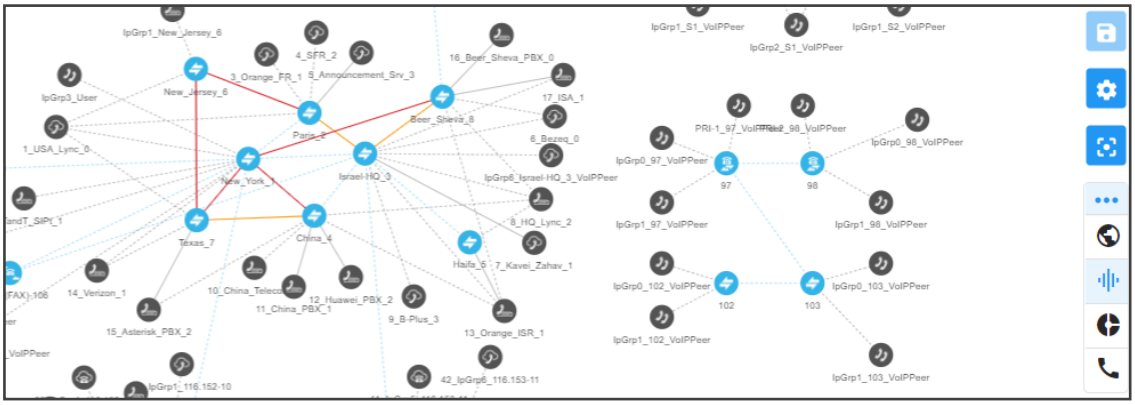
Network Entity	Icon	Explanation
		indicate a Peer Connection's directional lock.

Getting Acquainted with Network Map Layers

A **Layers** filter in the Network Map page allows the operator to filter the Network Map by:

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

Figure 2-2: Quality Layer



Select the icon of the layer to filter by; the icon changes color, from black to blue. In the preceding figure, the **quality** layer is displayed, showing the quality status of network Connections and Peer Connections.

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

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

The table below describes the different quality color codes.

Table 2-3: Quality Color Codes

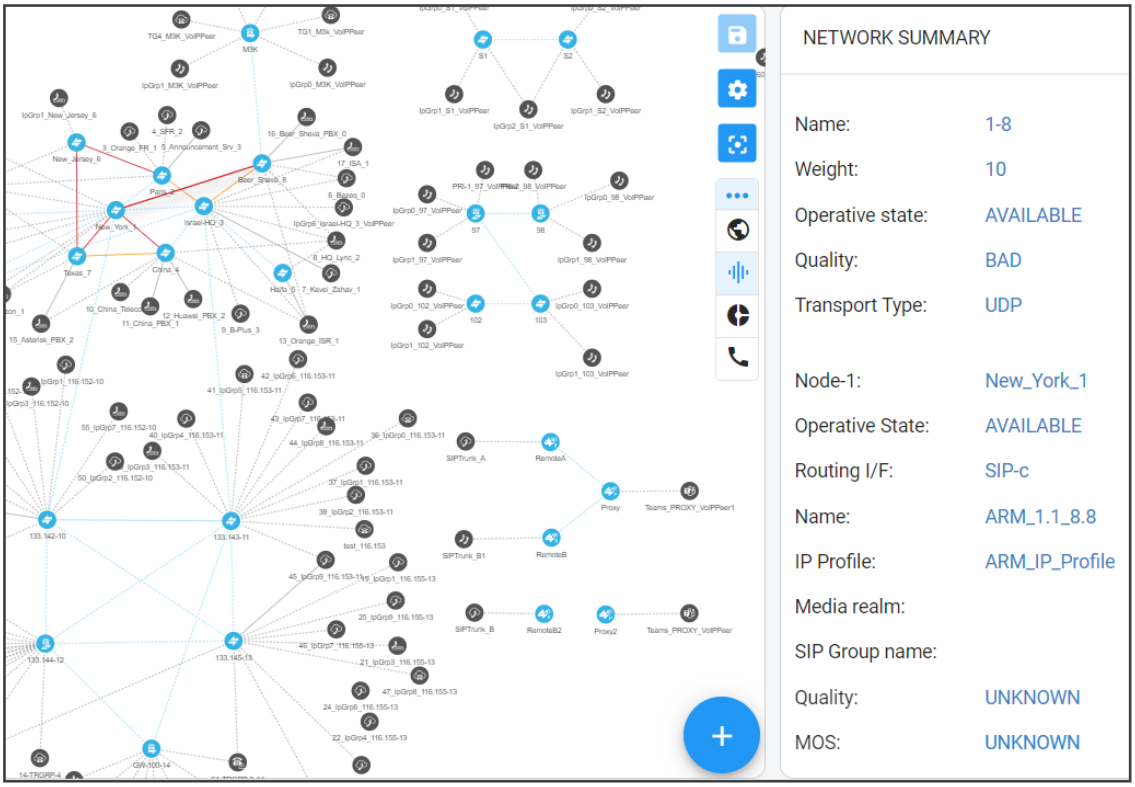
Color	Description
Blue	GOOD quality Connection
Grey	GOOD quality Peer Connection
Orange	FAIR quality Connection / Peer Connection
Red	BAD quality Connection / Peer Connection
Dotted gray	UNKNOWN quality, i.e., there is insufficient data to determine quality statistics. After enough calls are routed by 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 2-3: Summary Including Quality

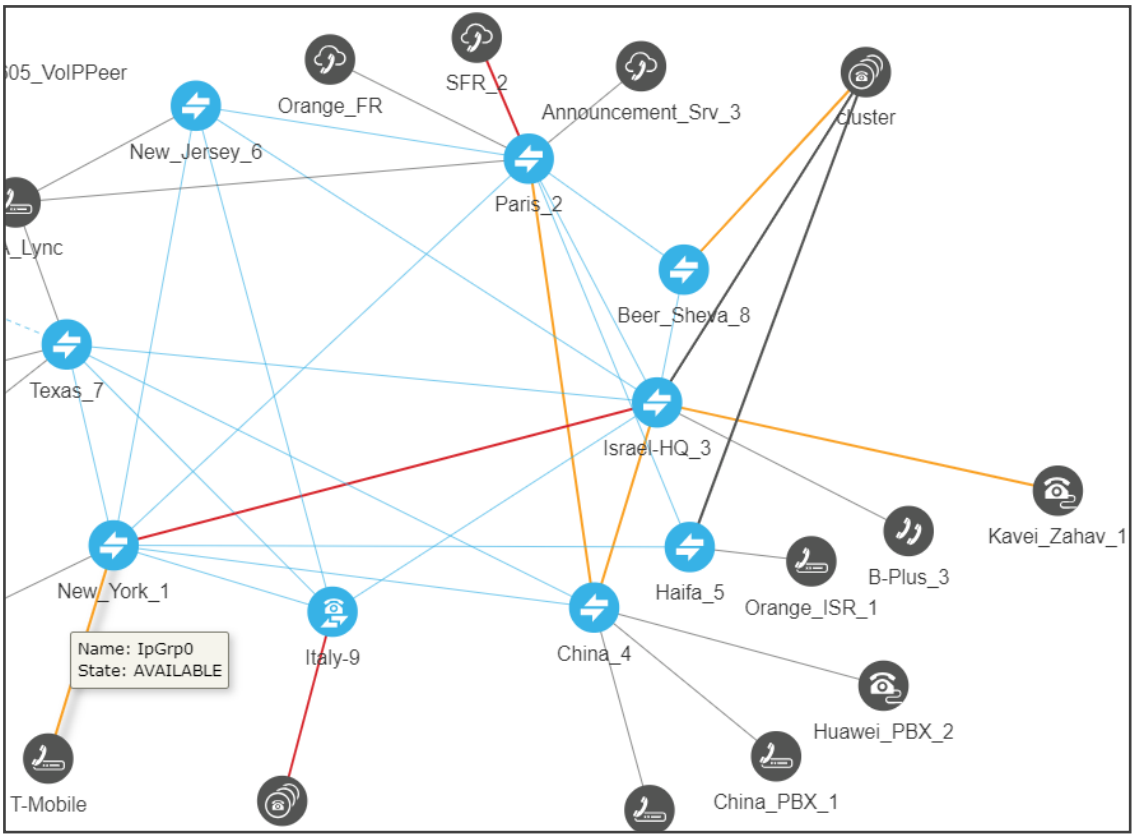


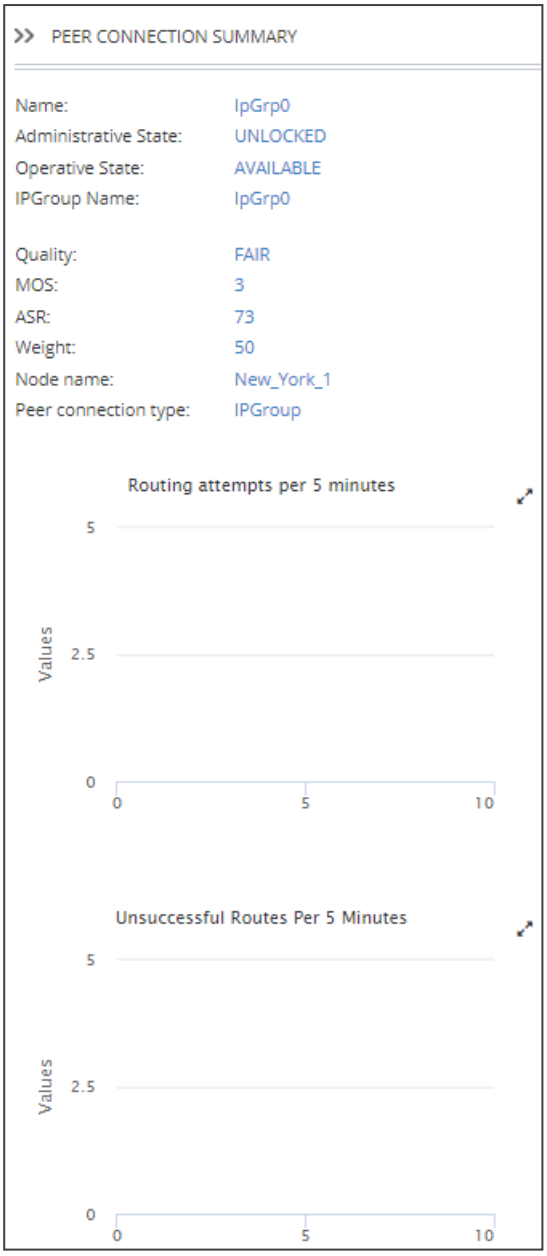
2. View a summary of the connection in the Connection Summary pane on the right side of the Network Map page. The figure above shows the Connection Summary pane for the Connection between the node **New_York_1** and **Beer_Sheva_8**. The 'Quality' parameter for both nodes is 'BAD'.
3. Use each direction's 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 2-4: Quality Layer - Peer Connection



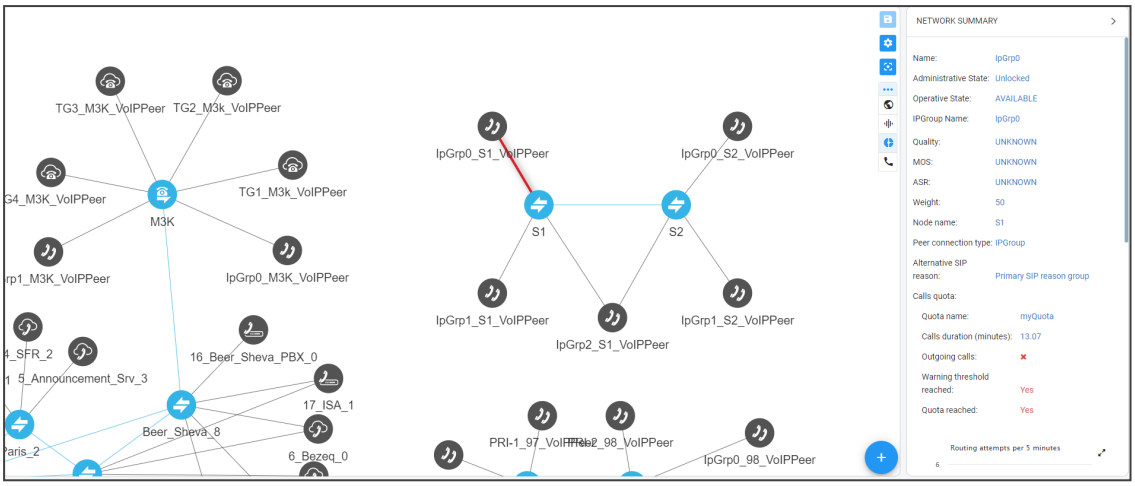


2. In the Peer Connection Summary pane on the right side of the Network Map page, view the Peer Connection Summary for the Peer Connection you clicked (selected). The figure above shows the Peer Connection whose name is 'IpGrp0'. The 'Quality' parameter is 'FAIR'.
3. Use each direction's MOS and ASR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

➢ To view the Quota status of the network:

1. Select the **quota** layer in the Network Map page.

Figure 2-5: Quota Layer



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

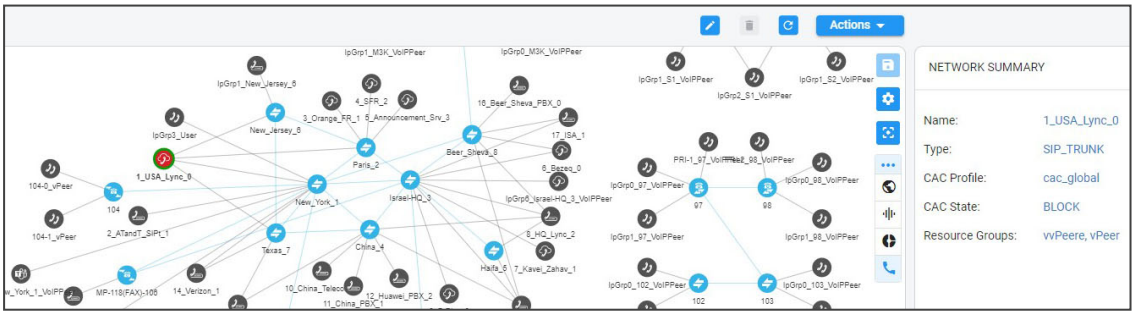
- The Quota layer can be combined with other layers in the customer's network.
- If a Peer Connection is attached to a Resource Group with a Quota, the ARM shows the Resource Group name in the Peer Connection summary; the ARM doesn't show the Quota information.

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

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

1. Select the **CAC** layer icon in the Network Map page.

Figure 2-6: CAC Layer



2. View in the Network Map status information related to the CAC Profile of the VoIP Peer. Review which VoIP Peer is blocked due to the CAC being reached. Blocked entities due to CAC are shown red. You'll also view an indication of direction, if relevant.

- The CAC layer filter can be combined with other layer filters.
- Make sure that a red color in the Network Map page is not due to Quality (for example).
- To correctly correlate colors, make sure which layer - or layers - you selected.

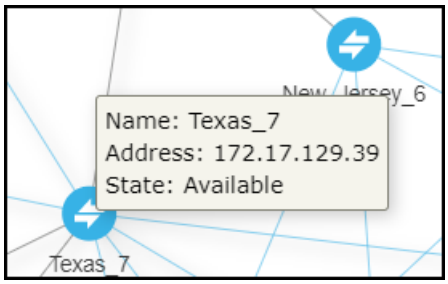
Getting Acquainted with Network Map Page Actions

Node Information and Actions

The Network Map page lets network operators view node information and perform node actions.

➢ **To view node information:**

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

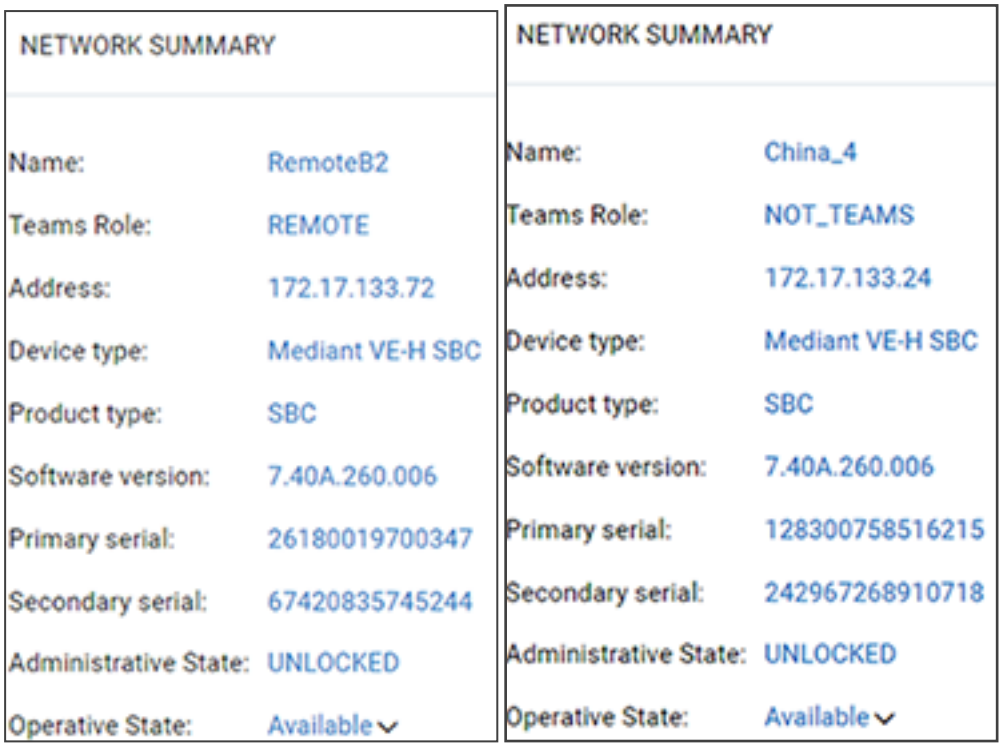


2. Use the following table as reference.

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.

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

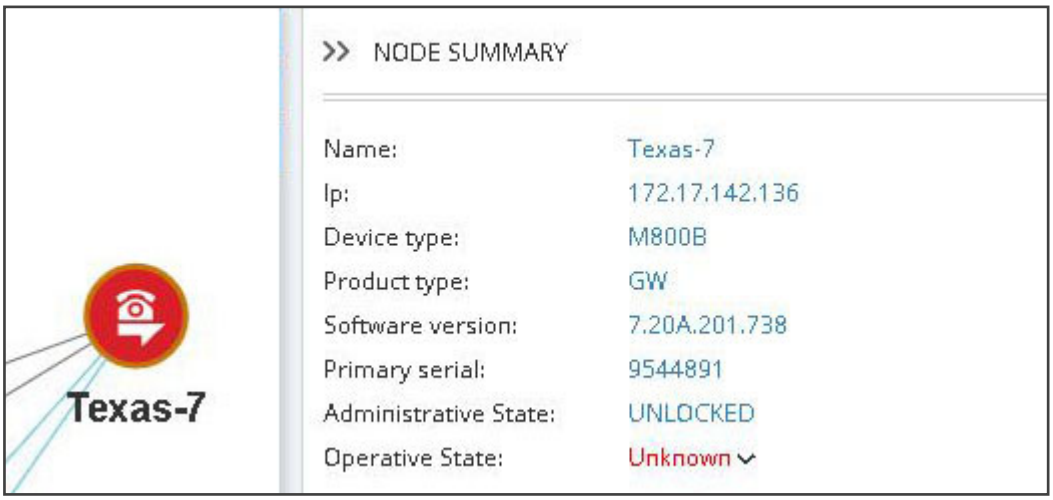


The preceding figure above left shows the Node Summary of an entity whose Teams Role is REMOTE.

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

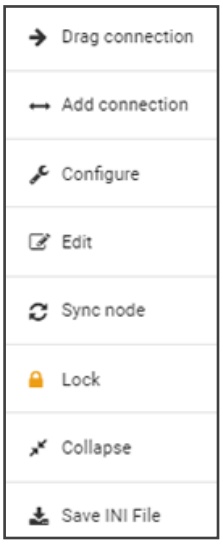
The example below shows a node's 'Operative State' as **Unknown** when the ARM Configurator is unable to access the SBC 'Texas-7'. Note that in this state, call routing requests coming from this node to the ARM Routers will be served.

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



➢ To perform an action on a node:

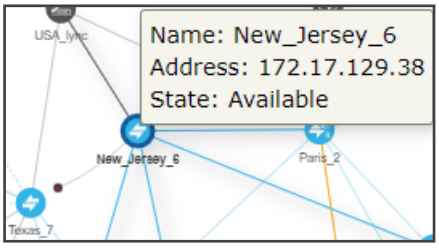
1. Right-click the node on which to perform an action.



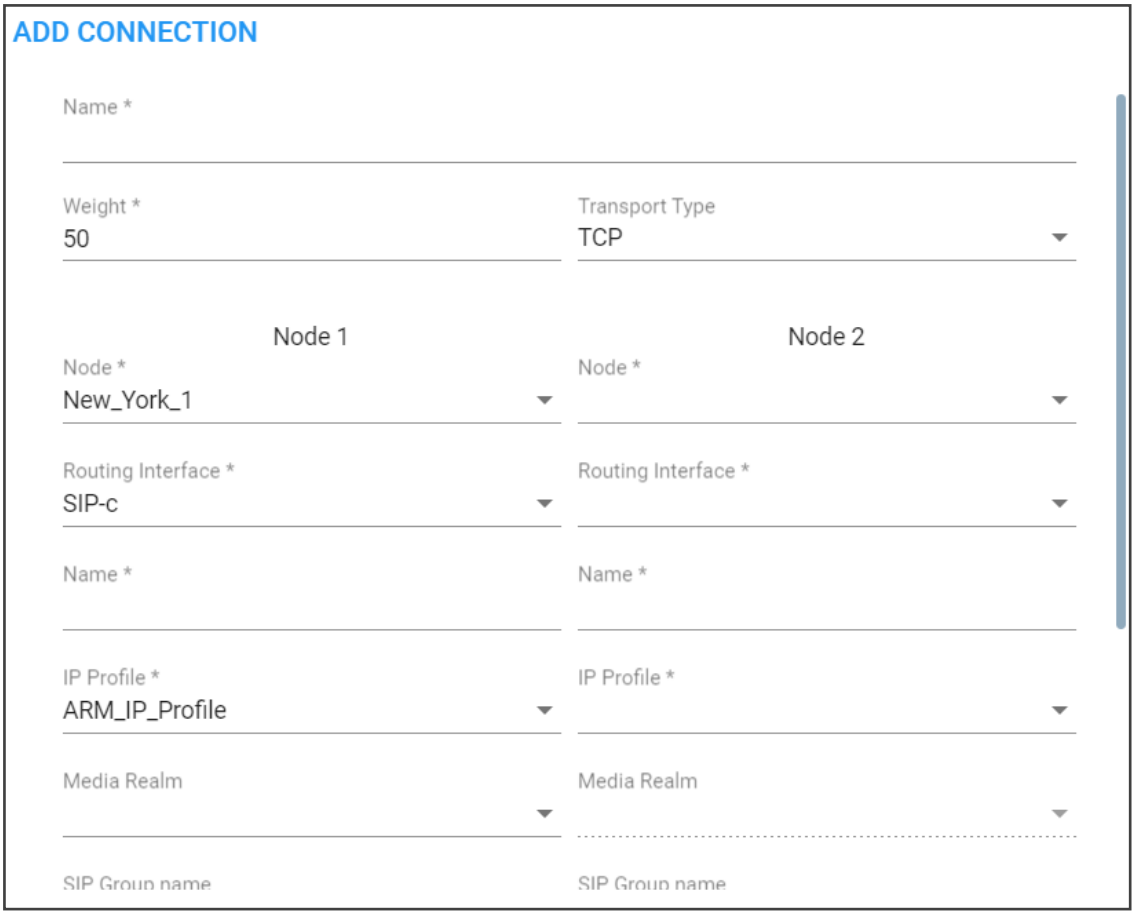
2. From the popup, choose:

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

Figure 2-8: Drag Connection

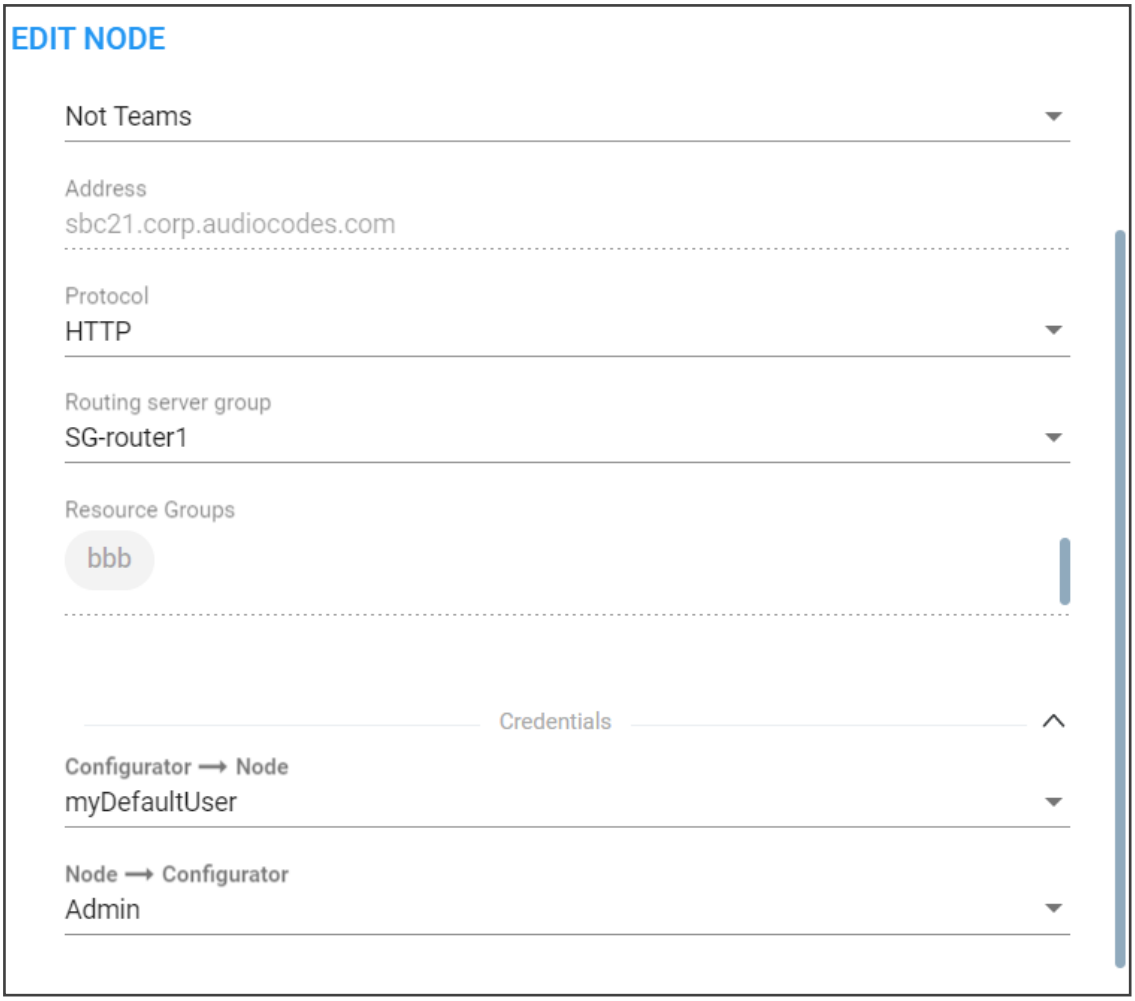


   - **Add Connection** [also available by selecting a node and then clicking the **Add Connection** button]



- 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 82 for more information.

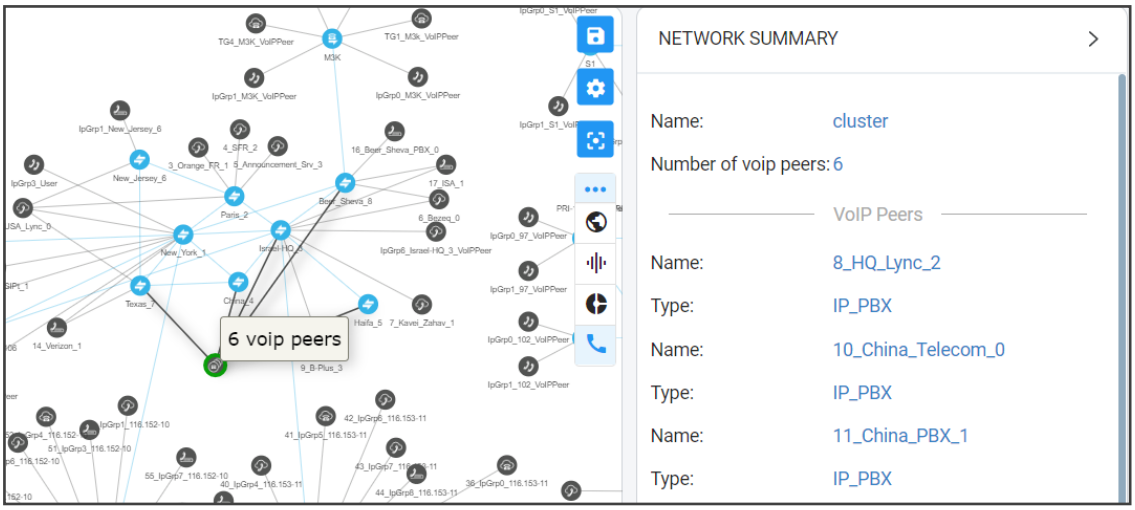
- **Configure**. Lets you directly configure a node (or SIP module) in the node's Web interface without needing to provide the node's credentials (Single Sign-on). See the AudioCodes device's *User's Manual* for detailed information. Nodes version 7.2.150 and later are supported. Earlier node versions 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.
- **Edit** [also available by right-clicking the node and then selecting **Edit**]
  - In the Edit Node dialog that opens - see the following figure - update the credentials of the device if necessary.



- 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 318.

- **Sync Node**
- **Lock/Unlock**
- **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:
  - In the Network Map page, right-click the node and select **Collapse** from the pop-up; all VoIP Peers associated with the node collapse. To undo, click  ; the Network Map page is refreshed.

Figure 2-9: Collapsed VoIP Peers

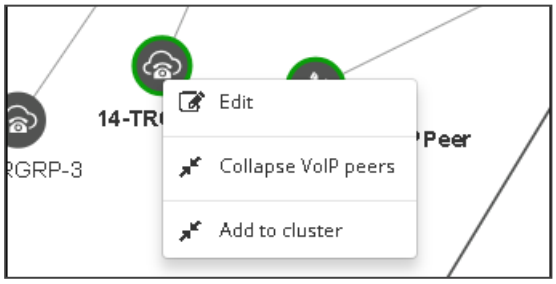


- [Refer to the preceding figure] The cluster's tooltip in the Network Map as well as the summary in the right pane indicate the number of collapsed VoIP Peers / Peer Connections in the cluster.
- [Refer to the figure following] The summary can also indicate the aggregated number of collapsed VoIP Peers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

Figure 2-10: Peer Connection Aggregation Summary

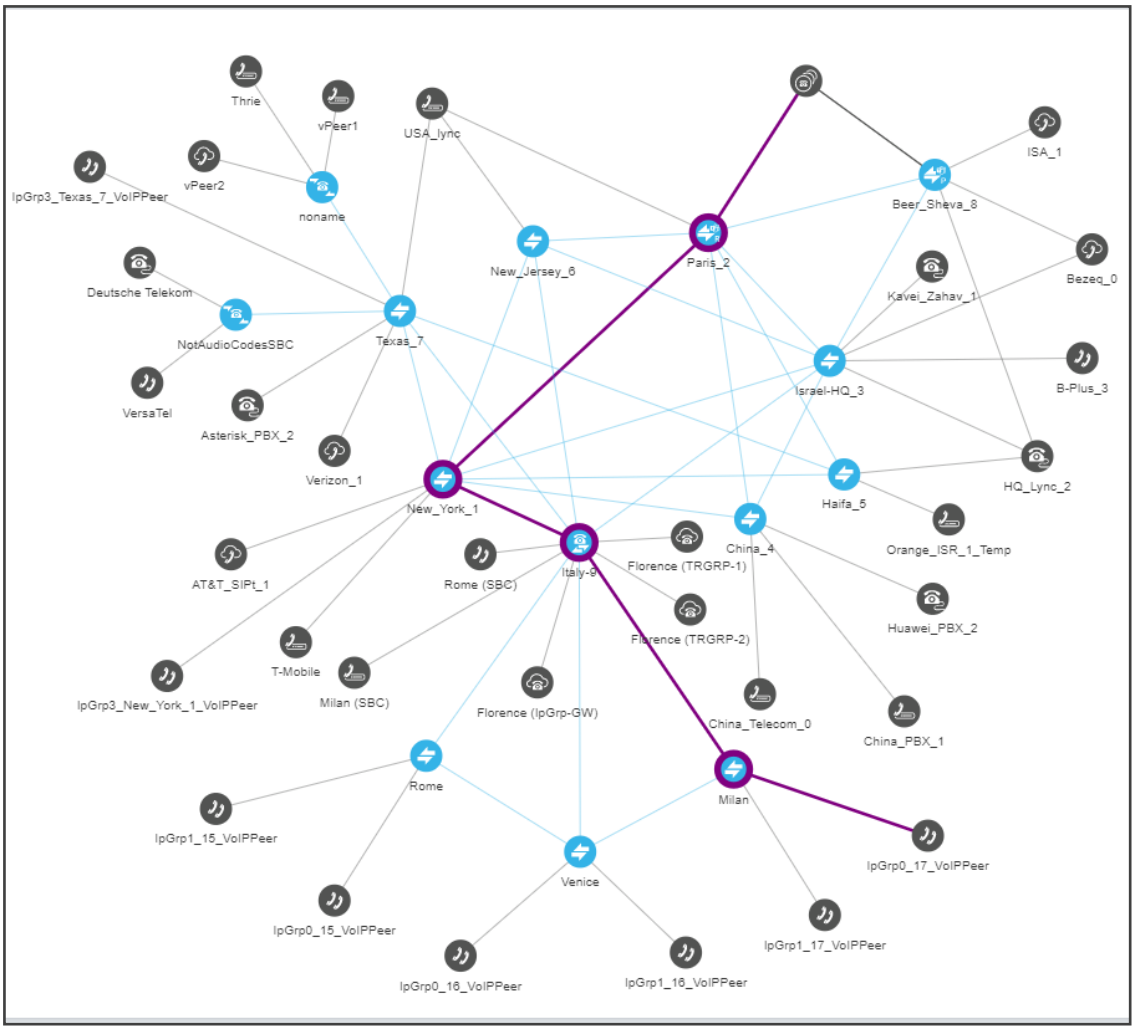
- **Add to cluster**. You can add an additional VoIP Peer or multiple VoIP Peers to an existing cluster: (1) Select the target cluster to which to add (2) press the **Ctrl** key click one or multiple VoIP Peers to add to the target cluster (3) right-click and from the pop-up menu select the action **Add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

Figure 2-11: Add to cluster



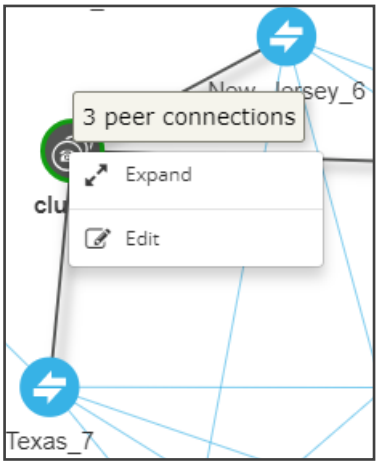
- VoIP Peers associated with more than one node are included in the collapsed cluster. If a test route is performed that terminates on a collapsed VoIP Peer, the VoIP Peer will not be expanded automatically and the path displayed in the GUI will terminate on the cluster icon.

Figure 2-12: Test Route Path Terminates on Collapsed VoIP Peer



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

Figure 2-13: Expand Cluster of VoIP Peers



- **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.

- **Save INI File**. Lets you save the AudioCodes device's INI file directly from the ARM without needing to SSO into the device, thereby making debugging and log collection easier. The action can also be performed in the Nodes page by selecting the **Save INI File** option from the **Actions** drop-down.

VoIP Peer Information and Actions

The Network Map page lets network operators view information about VoIP Peers 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 2-14: SIP Trunk

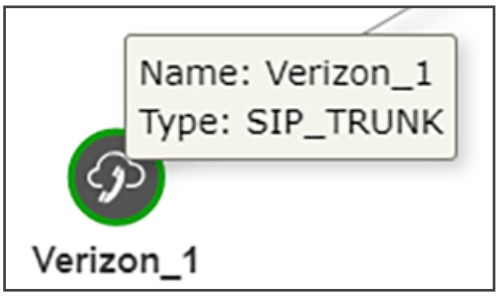
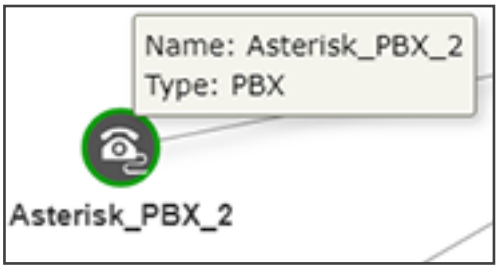


Figure 2-15: PBX | IP PBX



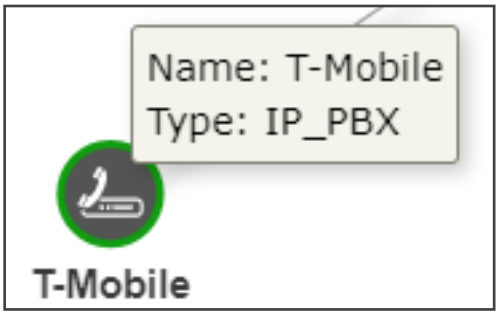


Figure 2-16: PSTN

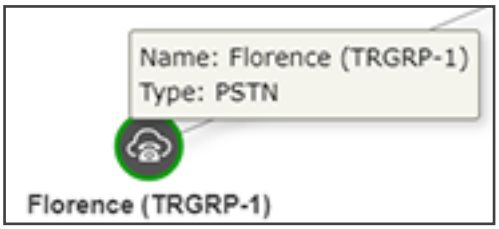
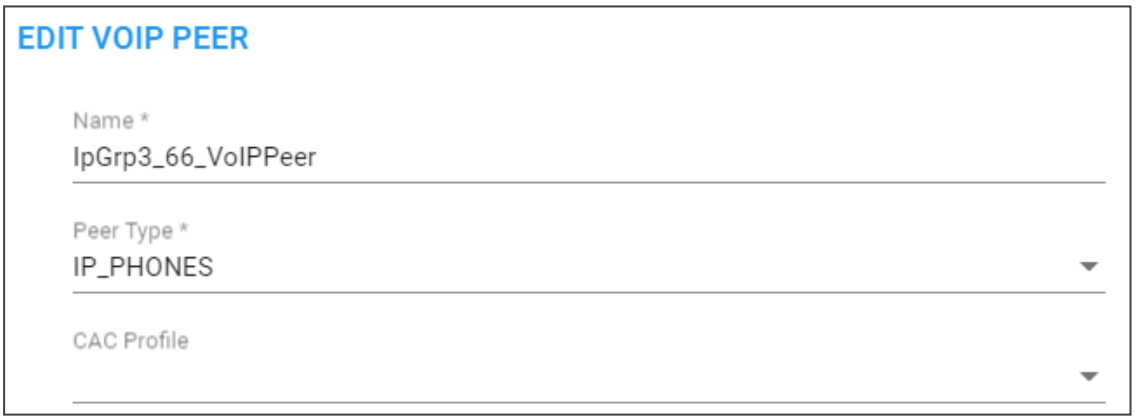


Figure 2-17: IP Phone

➢ **To edit a VoIP Peer:**

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



  - 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.

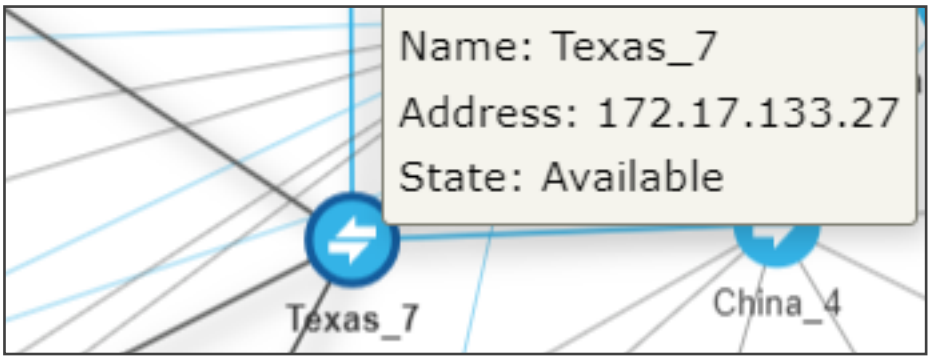
Connection Information and Actions

The Network Map page lets network operators view information about connections and perform connection actions.

➢ To view connection information:

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

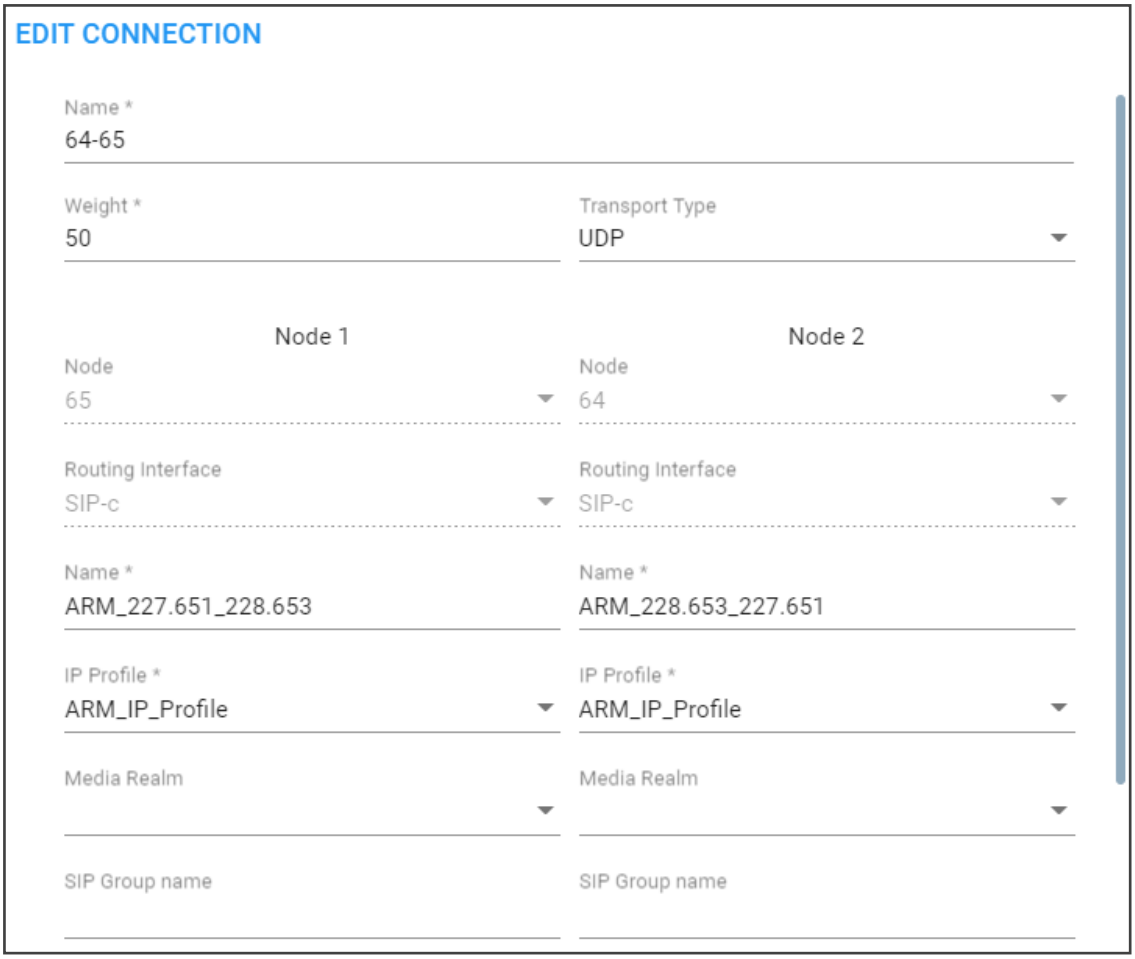
Figure 2-18: Connection Information



2. View in the tooltip the Name of the connection, its IP Address and its State.

➢ To perform an action on a connection:

1. Right-click the connection and from the popup, select **Edit**. [**Edit** is also available as an icon, and as an option in the **Actions** menu; **Delete** is available as an icon; **Add connection** is available as an option in the **Actions** menu].



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

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

4. Leave the option **use global quality definitions** at its default for quality-based routing to be applied using global (ARM level) settings. Select **use specific quality definitions** to overwrite the global settings of quality-based routing condition for a specific connection, and then select the enabled 'MOS' and/or 'ASR' option (see Routing Settings on page 289 for related information).

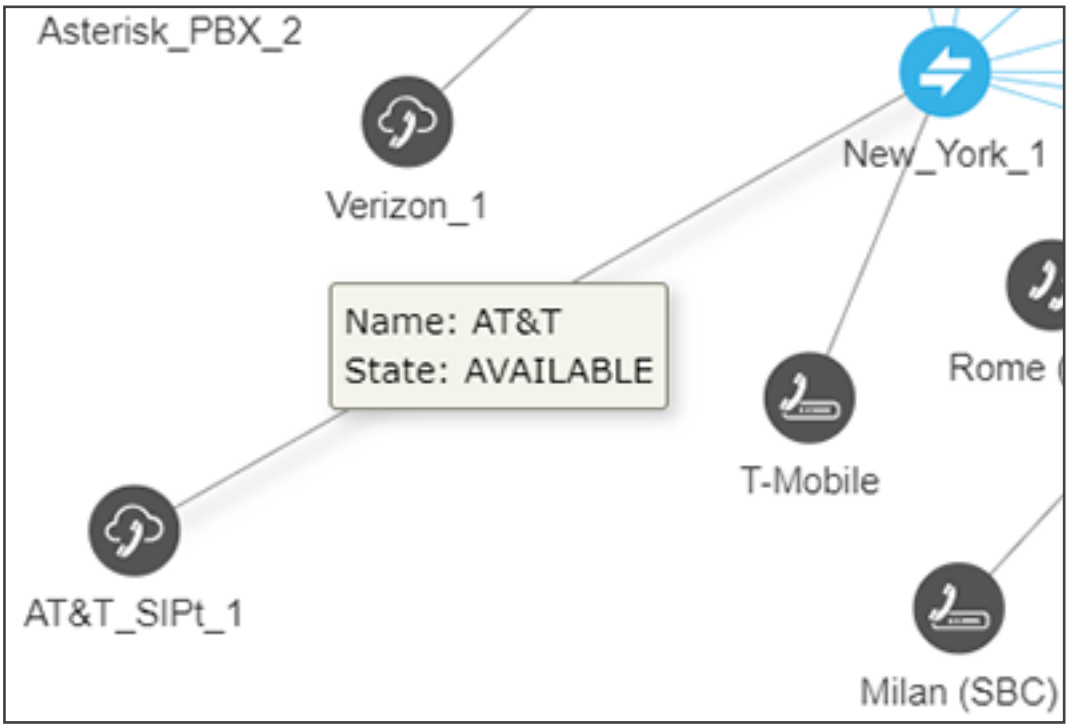
Peer Connection Information and Actions

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

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

➢ **To view Peer Connection information:**

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

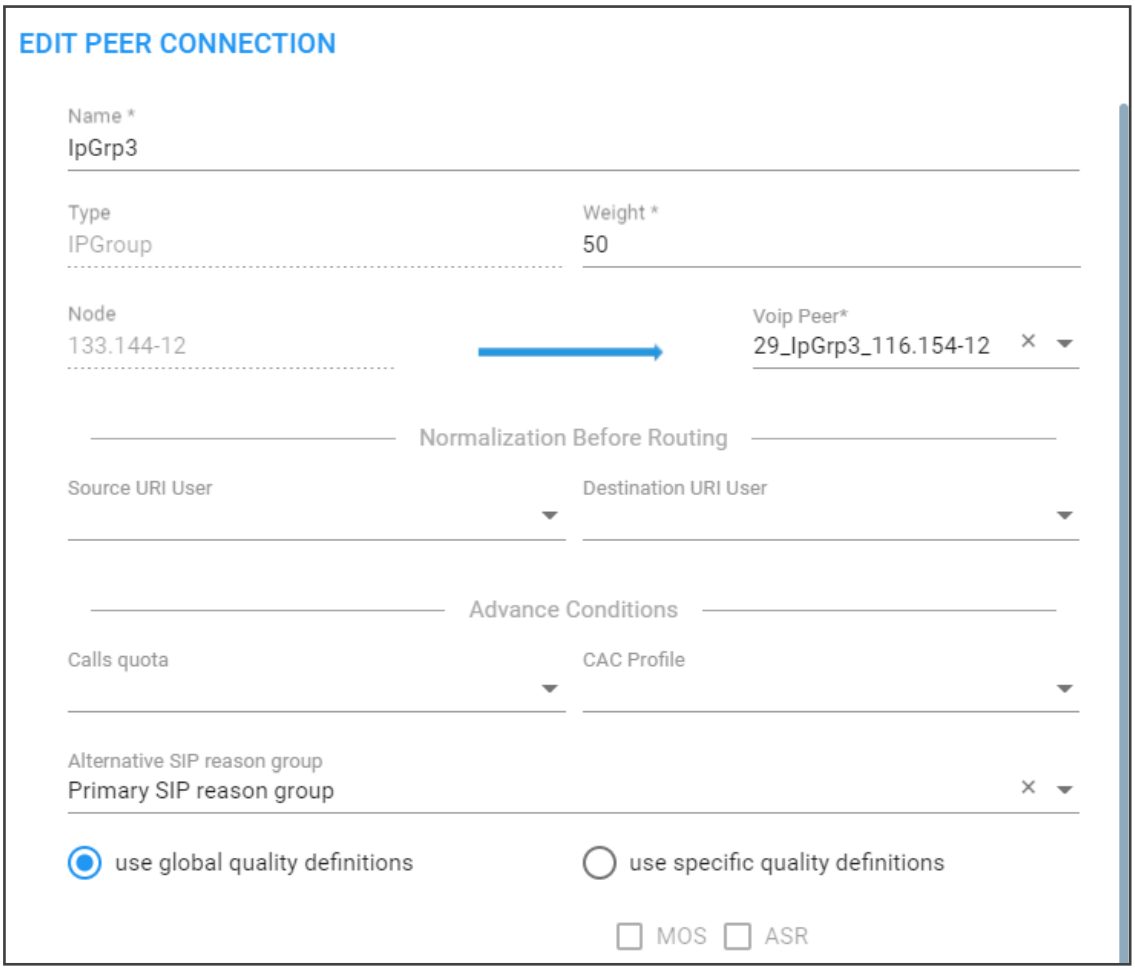


2. View the Peer Connection's Name and State.

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

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

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



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.

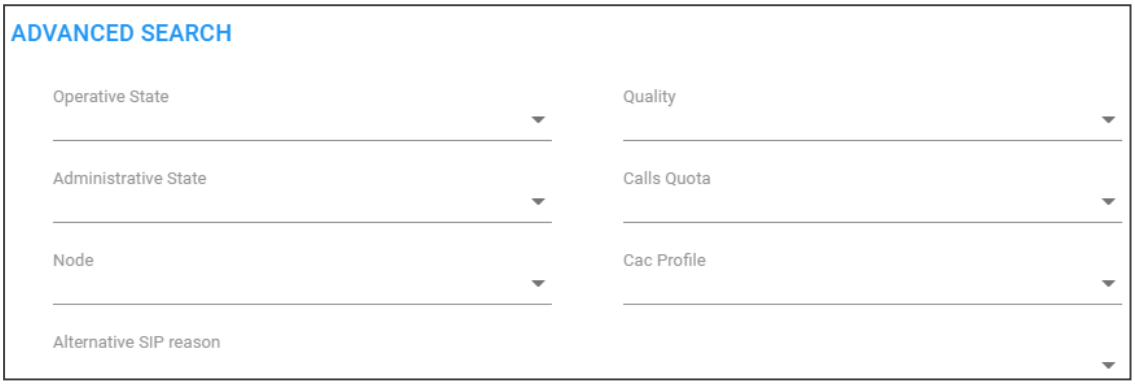
c. From the drop-down menus, select the Normalization Rule for Source and Destination URI User if pre-routing manipulation is required for a specific Peer Connection (configured as shown in Adding a Normalization Group on page 238).

d. Attach a Calls Quota to the Peer Connection (or to a group of Peer Connections gathered in a Resource Group of type 'Peer Connection'). The same quota can be

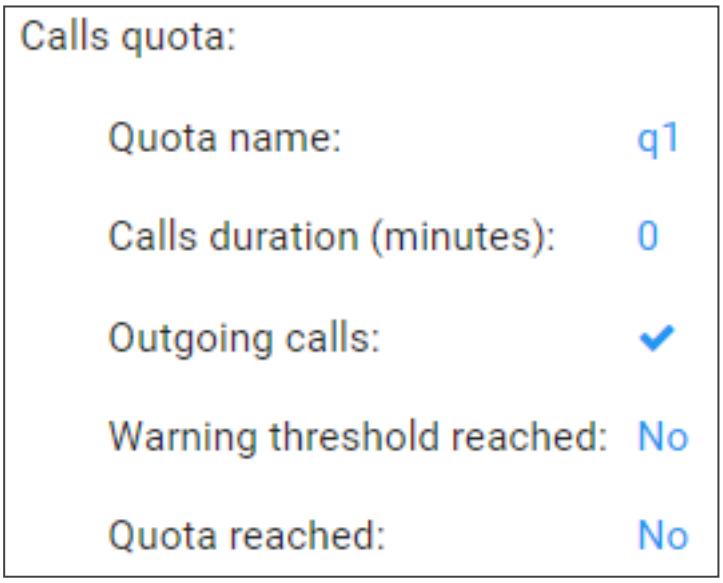
attached multiple times (reused for multiple Peer Connections or Resource Groups). From the 'Calls quota' drop-down, select a quota (defined as shown in Calls Quota on page 304). In the Peer Connections page (**Network** > **Peer Connections**), the quota is shown in the 'Calls Quota' column.

STATUS	NODE	NAME	VOIP PEER	IP GROUP	OPERATIVE STATE	ADMINISTRATIVE STATE	QUALITY	CALLS QUOTA
✔	New_York_1	IpGrp0	1_USA_Lync_0	IpGrp0	✔	🔓	UNKNOWN	
✔	New_York_1	IpGrp1	2_ATandT_SIPt_1	IpGrp1	✔	🔓	UNKNOWN	q1

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

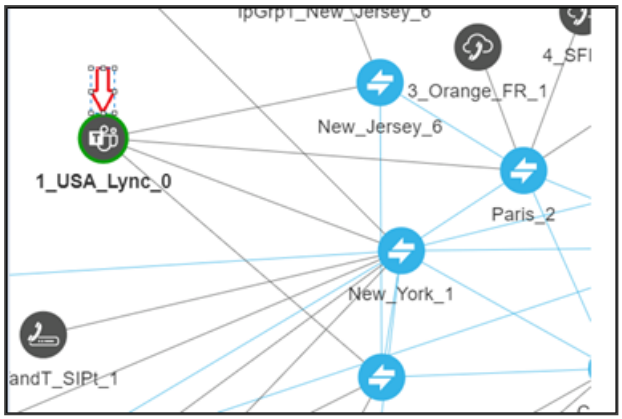


When selecting a Peer Connection with an attached quota, the following information related to quota counting is displayed:

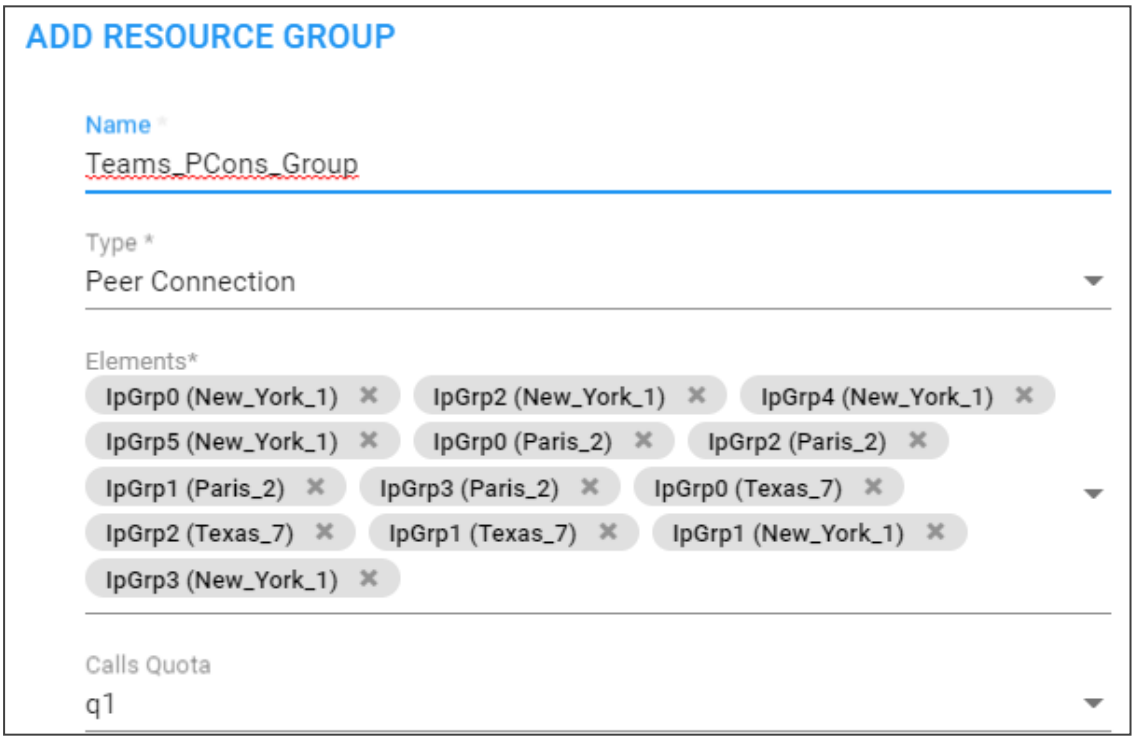


The Calls Quota can also be attached to several Peer Connections grouped in the same Resource Group. Note that only a Resource Group of type 'Peer Connection' can be associated with a Calls Quota. In this case, the calls balance, in minutes (defined by the Quota), is shared by all Peer Connections in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

that, the Quota can be attached to this Resource Group. In the following Network Topology, for example, Peer Connections come from four different SBCs to Teams:



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

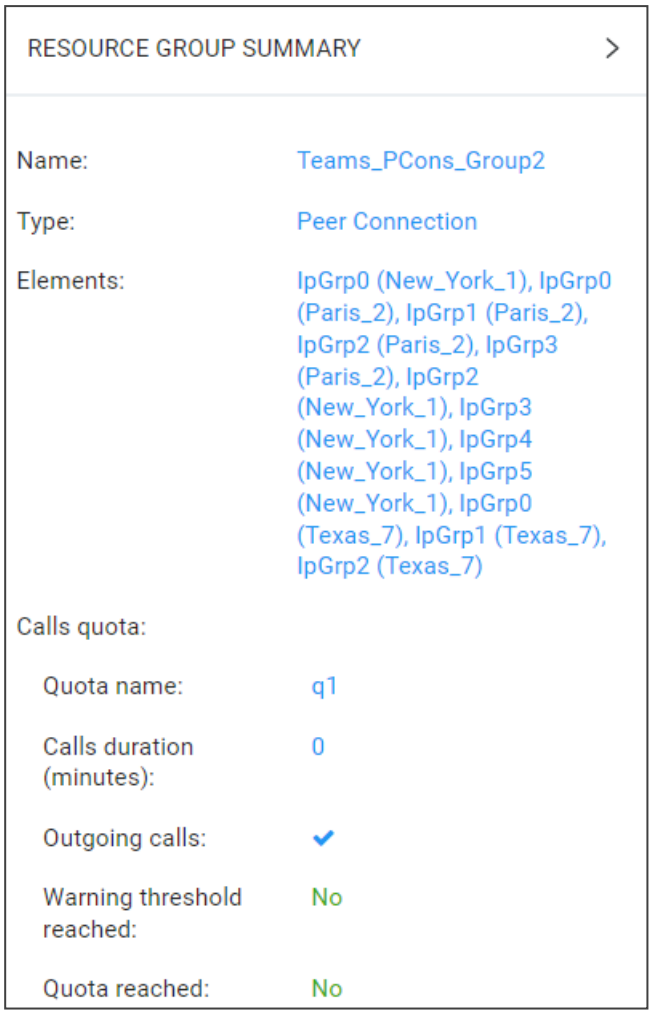


The ability to select a 'Calls Quota' becomes available only when you select 'Resource Group type' to be **Peer Connection**.

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

NAME	TYPE	ELEMENTS	CALLS QUOTA
Teams_PCons_Group2	Peer Connection	IpGrp0 (New_York_1), IpGrp0 (Paris_2), IpGrp1 ...	q1

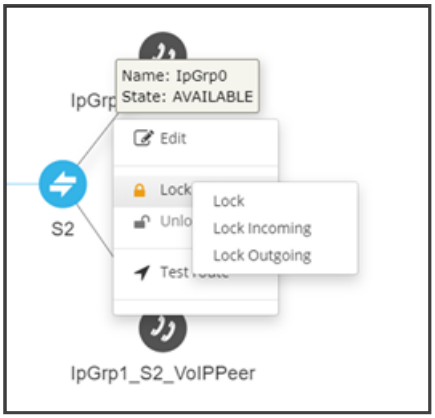
When a Resource Group with an attached Quota is selected, relevant information about the Calls Quota status is displayed on the right side of the page:



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

e. Leave **use global quality definitions** selected (default) for this Peer Connection to use the global quality profile configured as shown in Configuring Criteria for a Quality Profile on page 290.
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 290.

2. In the Network Map page, right-click the Peer Connection and choose **Lock** / **Unlock** from the popup menu as shown in the figure below. Alternatively, select the Peer Connection and then click the **edit** icon.

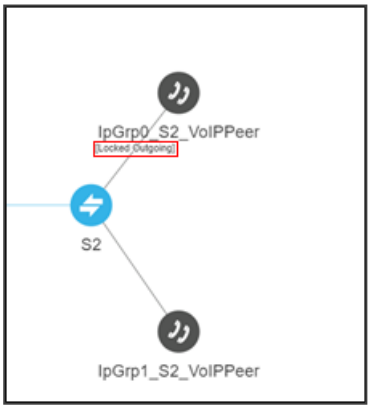


> The **Lock** / **Unlock** action is also available in the Peer Connections page (**Network** > **Peer Connections**); select the Peer Connection and then click the **edit** icon.

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

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

Figure 2-19: Locked / Unlocked Peer Connection in Map page (L) and in Peer Connections page (R)



3. In the Network Map page, right-click the Peer Connection and choose **Test Route** from the popup menu (see Testing a Route on page 96 for more information).
4. Optionally, you can **Delete** the Peer Connection. Only Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule, can be deleted.

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

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

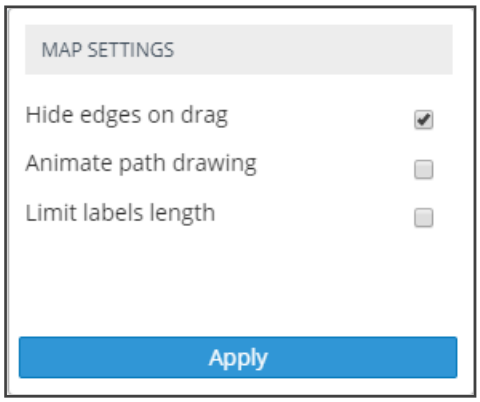
Repositioning Elements in the Network Map Page

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

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

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

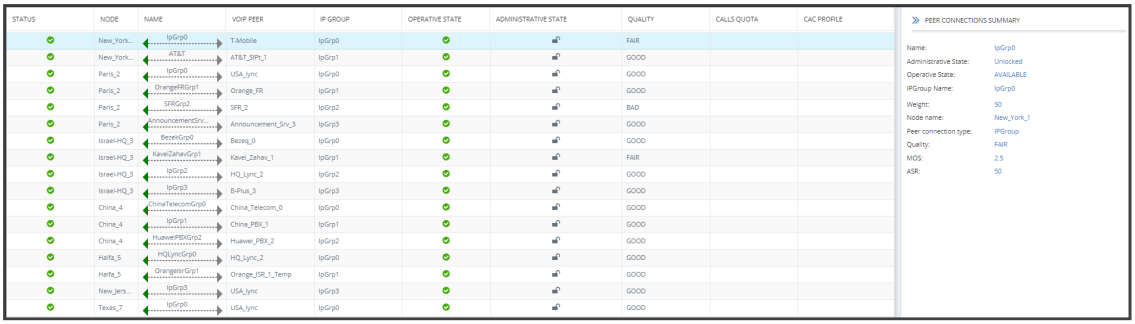
When moving / repositioning elements in the page, you can also use the **hide edges on drag** option available from the 'Diagram Configurations' icon.



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

The Peer Connections page (**Network** > **Peer Connections**) allows operators to view the Peer Connections in the IP telephony network. The maximum number of allowed Peer Connections in the ARM is 30000. This number is enforced; an alarm is generated if the threshold is crossed, and new Peer Connections are not allowed to be added to the ARM.



The following information on each Peer Connection is displayed:

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

The information displayed in the Peer Connections page is identical to that displayed in the Network Map page described under Peer Connection Information and Actions on page 48. You can search for the name of a node associated with the Peer Connection, the name of a Peer Connection, or a VoIP Peer name. It's useful to find, for example, all Peer Connections of a specific node.

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

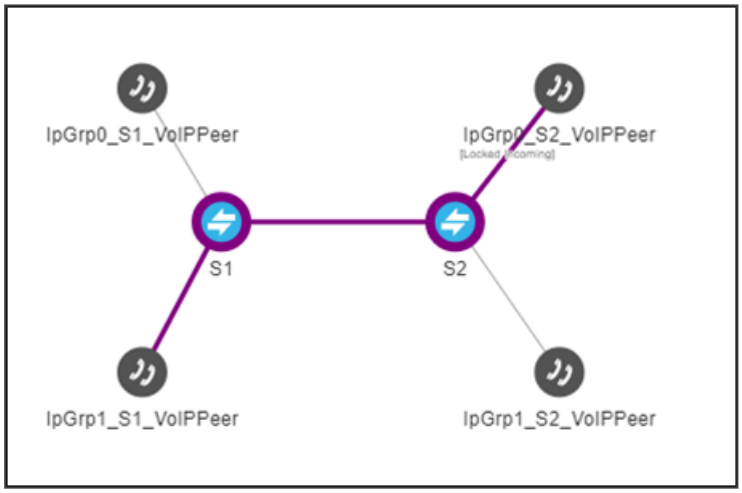
- **Sync Topology** available from the **Actions** drop-down.
- **Edit** after selecting the row of the Peer Connection to edit. For more information, see under Peer Connection Information and Actions on page 48.
- **Delete** after selecting the row of the Peer Connection to delete. Note that the **Delete** option is displayed only for Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule. for related information, see under Peer Connection Information and Actions on page 48.
- **Lock/Unlock** available from the **Actions** drop-down after selecting the row of the Peer Connection to lock/unlock. For more information, see under Peer Connection Information and Actions on page 48.

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

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

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

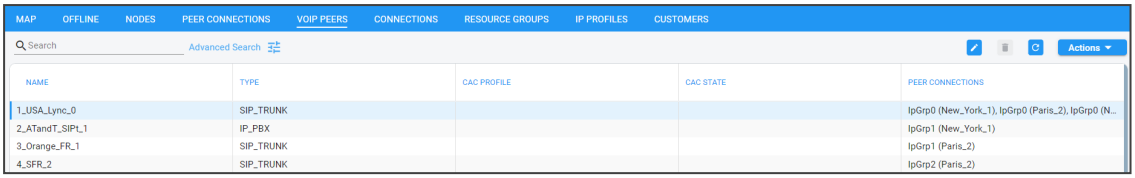
Figure 2-20: Test Route Activated for Outgoing Calls even though the Peer Connection is Locked for Incoming Calls



- Multiple rows can be selected; multiple actions (delete, lock/unlock, etc.) are supported.
- For more information about **Sync Topology**, see Synchronizing Topology on page 95.
- For more information about the **Edit**, **Delete** and **Lock**/**Unlock** actions, see under Peer Connection Information and Actions on page 48.

VoIP Peers Page Actions

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



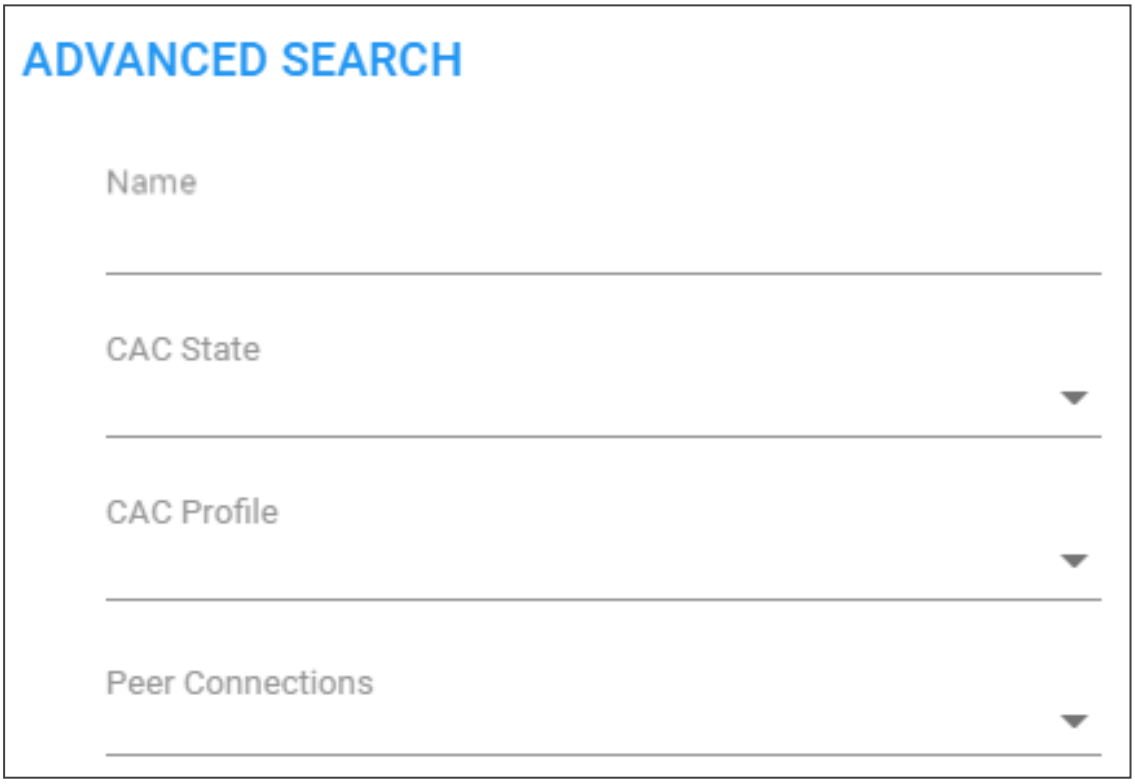
The page allows operators to manage associating a Network Topology element with a CAC Profile. When you attach a CAC Profile to a VoIP Peer (for example), the VoIP Peers page facilitates easy and effective management of the operation.

The page allows operators to apply **edit**, **delete** or **refresh** actions through the icons upper right.

The following information displayed in the page's columns is available per VoIP Peer:

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

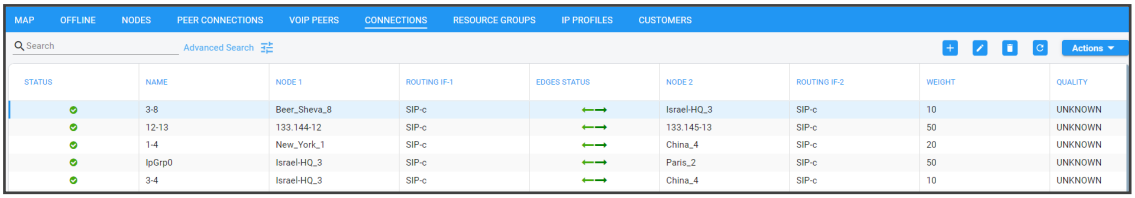
Click the **Advanced Search** link in the page:



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

Connections Page Actions

The Connections page (**Network** > **Connections**) allows operators to view the connections defined in the network.



View the following information about each connection:

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

The 'Edges Status' column displays the administrative status of each edge of every connection that was made between two nodes (node 1 and 2). Each connection between nodes comprises two (directional) IP Groups on each side. When the operator creates a connection between two nodes, the ARM defines an IP Group (edge) on each node. In this way, the connection comprises two edges and the connection status *aggregates* the statuses of both edges. The column consequently allows a better understanding of each connection's aggregated status, as each connection is affected by both directional edges.

Green = AVAILABLE

Red = UNAVAILABLE

In the example shown in the preceding figure:

- the administrative status of *both* edges (node 1 and node 2) of the connection **remote_proxy_con** is AVAILABLE ←→
- the administrative status of the node 1 edge of the connection **remoteB_proxy_con** is UNAVAILABLE while the administrative status of the node 2 edge is AVAILABLE ←→

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

Information displayed in the Connections page is identical to that displayed in the Network Map page - see under Connection Information and Actions on page 46.

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 95. For more information about the Add, Edit and Delete Connection, see under Connection Information and Actions on page 46.

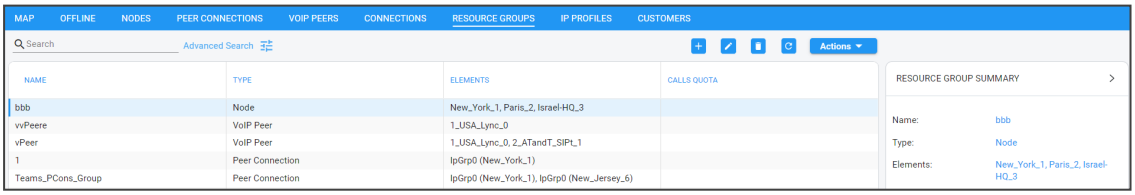
> **Do not modify the SBC-level / gateway-level configuration of the connections created by the ARM. It will disrupt routing decisions / performance.**

Resource Groups Page Actions

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

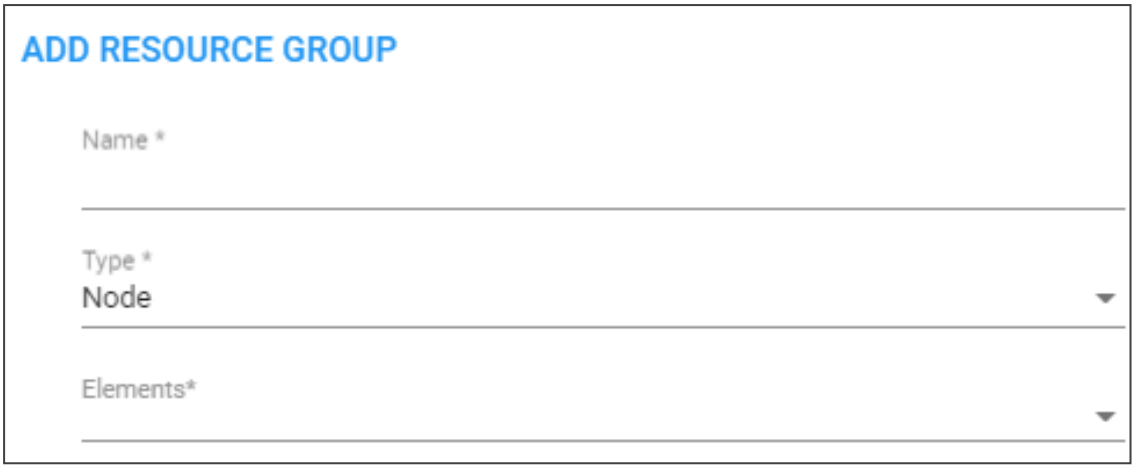
Operators can use

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



➢ To add a Resource Group:

1. In the Resource Groups page, click the **add +** icon.



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

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

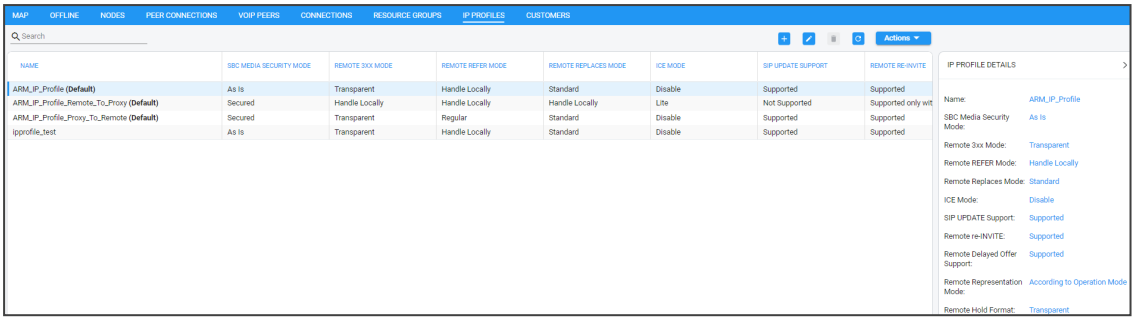
IP Profiles Page

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

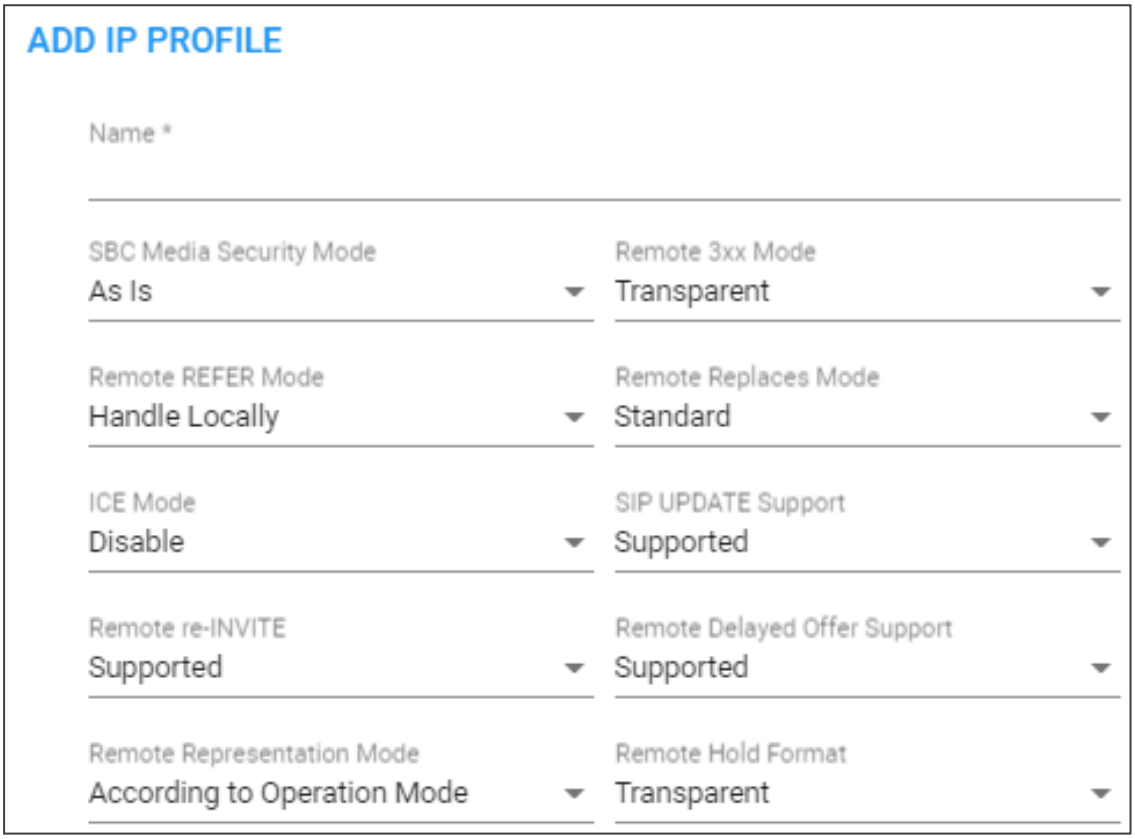
- Regular connections ('ARM_IP_Profile')
- Connections of Teams Remote to Teams Proxy devices ('ARM_IP_Profile_Remote_to_Proxy')
- Connections between Teams Proxy and Teams Remote devices ('ARM_IP_Profile_Proxy_to_Remote).

➢ **To add a new IP Profile:**

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



2. In the page, click the **add +** icon.



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

Table 2-5: IP Profile Parameters

Parameter	Description
Name	Configure an intuitive name for the IP Profile, to facilitate effective management later.
SBC Media Security Mode	Select either: ■ **Not secured** [SBC legs negotiate only SRTP/MSRPS media lines and RTP/MSRP media lines are removed from the incoming SDP offer-answer]

Parameter	Description
	■ **Secured** [SBC legs negotiate only RTP/MSRP media lines and SRTP/MSRPS media lines are removed from the incoming offer-answer] ■ **As is** (default) [No special handling for RTP/SRTP and MSRP/MSRPS is done] ■ **Both** [Each offer-answer is extended (if it isn't already) to two media lines - one RTP/MSRP and the other SRTP/MSRPS] For more information, see the device *User's Manual* available from AudioCodes.
Remote 3xx Mode	Select either: ■ **Handle Locally** [The device handles SIP 3xx responses on behalf of the dialog-initiating UA and retries the request (e.g., INVITE) using one or more alternative URIs included in the 3xx response. The device sends the new request to the alternative destination according to the IP-to-IP Routing table (the 'Call Trigger' field must be set to 3xx).] ■ **Local Host** [The device changes the host part of the Contact header in the 3xx response before forwarding the 3xx response to the dialog-initiating UA. If the 'Local Host Name' parameter of the IP Group of the dialoginitiating UA is configured with a non-empty value, the device changes the host part of the Contact header to this value. If the 'Local Host Name' is empty, the device changes the host part to the device's IP address (the same IP address used in the SIP Via and Contact headers of messages sent to the IP Group).] ■ **IP Group Name** [If the 'SIP Group Name' parameter of the IP Group of the dialog-initiating UA is configured with a non-empty value, the device changes the host part of the Contact header in the 3xx response to this value, before forwarding the 3xx response to the dialog-initiating UA.]

Parameter	Description
	■ **Database URL** [The device changes the Contact header so that the re-route request is sent through the device. The device changes the URI in the Contact header of the received SIP 3xx response to its own URI and adds a special user prefix ("T~&R_"), which is then sent to the FEU. The FEU then sends a new INVITE to the device, which the device then sends to the correct destination.] ■ **Transparent** (default) [The device forwards the received SIP 3xx response as is, without changing the Contact header (i.e., transparent handling)] For more information, see the device *User's Manual* available from AudioCodes.
Remote REFER Mode	Select either: ■ **Handle Locally** (default) [Handles the incoming REFER request itself without forwarding the REFER. The device generates a new INVITE to the alternative destination (transfer target) according to the rules in the IP-to-IP Routing table (the 'Call Trigger' parameter must be set to REFER).] ■ **Local Host** [In the REFER message received from the transferor, the device replaces the Refer-To header value (URL) with the IP address of the device or with the 'Local Host Name' parameter value configured for the IP Group (transferee) to where the device forwards the REFER message. This ensures that the transferee sends the re-routed INVITE back to the device which then sends the call to the transfer target.] ■ **IP Group Name** [Changes the host part in the REFER message to the name configured for the IP Group (in the IP Groups table).] ■ **Database URL** [SIP Refer-To header value is changed so that the re-routed INVITE is sent through the device:

Parameter	Description
	✓ Before forwarding the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T~&R_") to the Contact user part. ✓ The incoming INVITE is identified as a REFER-resultant INVITE according to this special prefix. ✓ The device replaces the host part in the Request- URI with the host from the REFER contact. The special prefix remains in the user part for regular classification, manipulation, and routing. The special prefix can also be used for specific routing rules for REFER-resultant INVITEs. ✓ The special prefix is removed before the resultant INVITE is sent to the destination ((transfer target).] ■ **Keep URI (user@host)** [The device forwards the REFER message without changing the URI (user@host) in the SIP Refer-To header. If you configure the 'Remote Replaces Mode' parameter (see below) to any value other than Keep as is, the devicemay modify the 'replaces' parameter of the Refer-To header to reflect the call identifiers of the leg. This applies to all types of call transfers (e.g., blind and attendant transfer).] ■ **Regular** [SIP Refer-To header value is unchanged and the device forwards the REFER message as is. However, if you configure the 'Remote Replaces Mode' parameter (see next) to any value other than (keep) **As is**, the device may modify the URI of the Refer-To header to reflect the call identifiers of the leg.] For more information, see the device *User's Manual* available from AudioCodes.
Remote Replaces Mode	Select either:

Parameter	Description
	■ **Standard** (default) [The SIP UA supports INVITE messages containing Replaces headers. The device forwards the INVITE message containing the Replaces header to the SIP UA. The device may change the value of the Replaces header to reflect the call identifiers of the leg.] ■ **Handle Locally** [The SIP UA does not support INVITE messages containing Replaces headers. The device terminates the received INVITE containing the Replaces header and establishes a new call between the SIP UA and the new call party. It then disconnects the call with the initial call party, by sending it a SIP BYE request.] ■ **As is** [The SIP UA supports INVITE messages containing Replaces headers. The device forwards the Replaces header as is in incoming REFER and outgoing INVITE messages from/to the SIP UA (i.e., Replaces header's value is unchanged).] For more information, see the device *User's Manual* available from AudioCodes.
ICE Mode	Enables Interactive Connectivity Establishment (ICE) Lite for the SIP UA associated with the IP Profile. ICE is a methodology for NAT traversal, employing the Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols to provide a peer with a public IP address and port that can be used to connect to a remote peer. For example, (ICE) **Lite** is required when the device operates in Microsoft Teams Direct Routing (media bypass) environments. Select either: ■ **Disable** (default) ■ **Lite** For more information, see the device *User's Manual* available from AudioCodes.

Parameter	Description
SIP Update Support	Select either: ■ **Supported Only After Connect** [The UA supports receipt of UPDATE messages, but only after the call is connected.] ■ **Not Supported** [The UA doesn't support receipt of UPDATE messages.] ■ **According Remote Allow** [For refreshing the timer of currently active SIP sessions, the device sends session refreshes using SIP UPDATE messages only if the SIP Allow header in the last SIP message received from the user contains the value "UPDATE". If the Allow header does not contain the "UPDATE" value (or if the parameter is not configured to this option), the device uses INVITE messages for session refreshes.] ■ **Supported** (default) [The UA supports receipt of UPDATE messages during call setup and after call establishment.] For more information, see the SBC *User's Manual* available from AudioCodes.
Remote re-INVITE	Defines if the SIP UA associated with this IP Profile supports receipt of SIP re-INVITE messages. Select either: ■ **Not Supported** [The UA doesn't support receipt of re-INVITE messages. If the device receives a re-INVITE from another UA that is destined to this UA, the device "terminates" the re-INVITE and sends a SIP response to the UA that sent it, which can be a success or a failure, depending on whether the device can bridge the media between the UAs.] ■ **Supported only with SDP** [The UA supports receipt of re-INVITE messages, but only if they contain an SDP body. If the incoming re-INVITE from another UA doesn't contain SDP, the device creates and adds an SDP body to the re-INVITE that it forwards to the UA.]

Parameter	Description
	■ **Supported** (default) [The UA supports receipt of re-INVITE messages with or without SDP.] For more information, see the SBC *User's Manual* available from AudioCodes.
Remote Delayed Offer Support	Defines if the remote UA supports delayed offer (i.e., initial INVITE requests without an SDP offer). Select either: ■ **Not Supported** ■ **Supported** (default) For more information, see the SBC *User's Manual* available from AudioCodes.
Remote Representation Mode	Select either: ■ **According to Operation Mode** (default) [Depends on the setting of the 'Operation Mode' parameter in the IP Groups or SRDs table: ✓ **B2BUA**: Device operates as if the parameter is set to **Replace Contact**. ✓ **Call State-full Proxy**: Device operates as if the parameter is set to **Add Routing Headers**.] ■ **Replace Contact** [The URI host part in the Contact header of the received message (from the other side) is replaced with the device's address or with the value of the 'SIP Group Name' parameter (configured in the IP Groups table) in the outgoing message sent to the SIP UA.] ■ **Add Routing Headers** [Device adds a Record-Route header for itself to outgoing messages (requests\responses) sent to the SIP UA in dialog-setup transactions. The Contact header remains unchanged.] ■ **Transparent** [Device doesn't change the Contact header and doesn't add a Record-Route header for itself. Instead, it relies on

Parameter	Description
	its' own inherent mechanism to remain in the route of future requests in the dialog (for example, relying on the way the endpoints are set up or on TLS as the transport type).] For more information, see the SBC *User's Manual* available from AudioCodes.
Remote Hold Format	Defines the format of the SDP in the SIP re-INVITE (or UPDATE) for call hold that the device sends to the held party. Select either: ■ **Hold and Retrieve Not Supported** [This option can be used when the remote side does not support call hold and retrieve (resume). The device terminates call hold and call retrieve requests received on the leg interfacing with the initiator of the call hold/retrieve, and replies to this initiator with a SIP 200 OK response. Therefore, the device does not forward call hold and/or retrieve requests to the remote side.] ■ **Inactive** [Device sends SDP with 'a=inactive'] ■ **Send Only** [Device sends SDP with 'a=sendonly] ■ **Not Supported** [This option can be used when the remote side does not support call hold. The device terminates call hold requests received on the leg interfacing with the initiator of the call hold, and replies to this initiator with a SIP 200 OK response. However, call retrieve (resume) requests received from the initiator are forwarded to the remote side. The device can play a held tone to the held party if the 'Play Held Tone' parameter is set to Internal.] ■ **Inactive Zero IP** [Device sends SDP with 'a=inactive' and 'c=0.0.0.0'.] ■ **Send Only Zero IP** [Device sends SDP with 'a=sendonly' and 'c=0.0.0.0']

Parameter	Description
	■ **Transparent** (default) [Device forwards SDP as is] For more information, see the device *User's Manual* available from AudioCodes.

4. Click **OK**.

- The new IP Profile is synchronized with all nodes in the deployment.
- Operators can use the IP Profile to define connections in the ARM (see Configuring a Microsoft Teams LMO Topology on page 91).

Customers Page

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

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

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

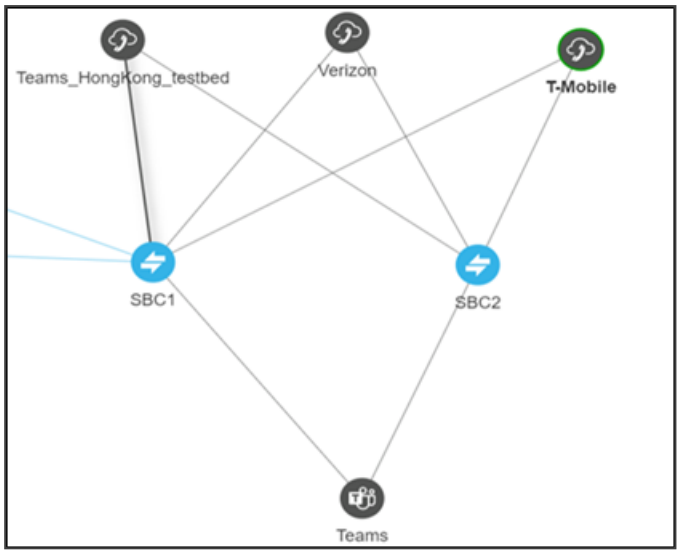
ARM Routing capabilities support the 'customer' entity as a routing condition (specific 'customer' entities or all 'customer' entities). This also includes SIP header manipulations, required by Teams multi-tenancy, that can now easily be performed by the ARM (SIP 'Contact' header).

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

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

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

Figure 2-21: CAC Capabilities - Use Case



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

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

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

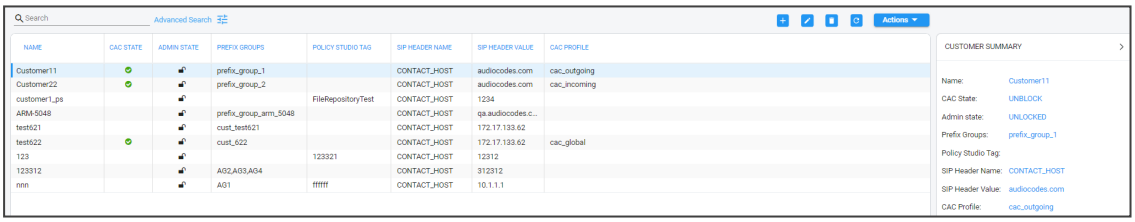
Viewing the Customers Page

The Customers page (**Network** > **Customers**) provides operators the capability to view all provisioned 'customer' entities (Teams tenants) in a table (one row per 'customer' entity). In addition to the information configured per 'customer' entity (provided by the operator in the

add + / **edit** action), the following two columns are shown in the table for each 'customer' entity:

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

Figure 2-22: Customer Page Columns



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

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

Defining a 'Customer' Entity (Teams Tenant)

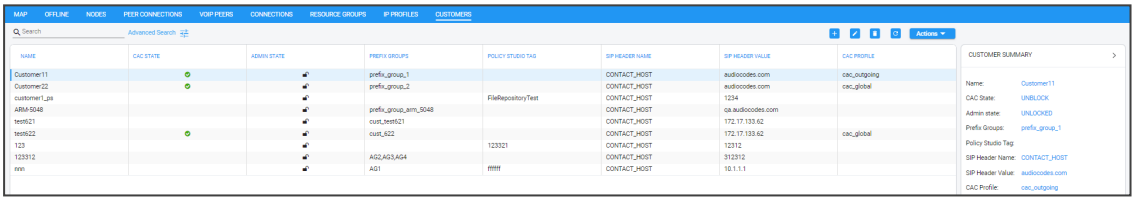
Network operators can add a logical 'customer' entity (Teams tenant) to the ARM GUI in the Customers page. The page allows **add +**, **edit**, **delete**, **Lock/Unlock** and **Refresh** actions for each 'customer' entity.

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

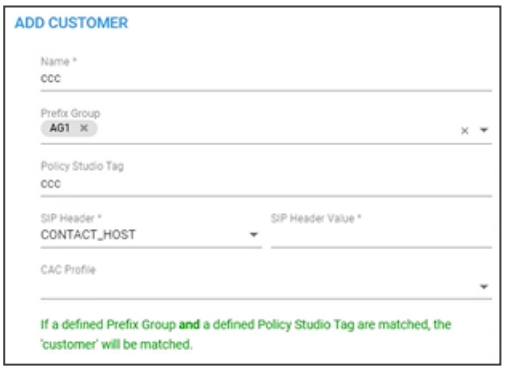
For more information and a use-case for each 'customer' definition method (either with Prefix Group or with Users), see Defining 'Customer' Entities using ARM Users & Policy Studio on page 75.

➢ To add a new 'customer' entity':

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



2. Click **add +**.

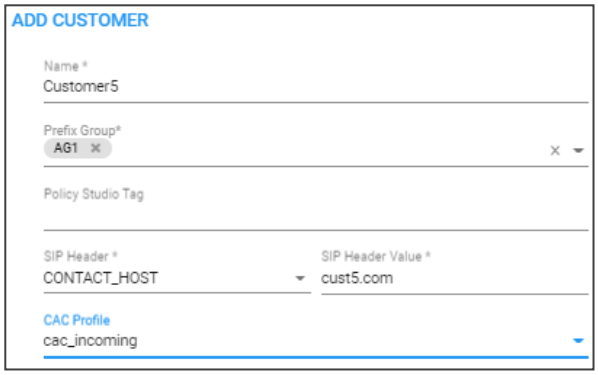
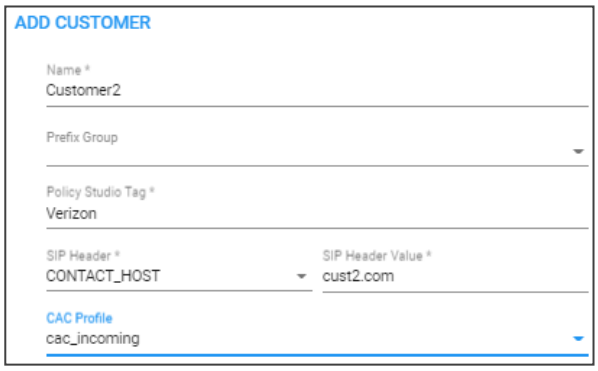


3. Configure the parameters using the following table as reference.

Table 2-6: Add Customer

Parameter	Description
Name	Mandatory. Unique name of the 'customer' entity. Configure an intuitive name to facilitate effective management later.
Prefix Group	Used if the operator chooses to identify a 'customer' entity with Prefix Groups. The

Parameter	Description
	operator can select a Prefix Group or several Prefix Groups previously defined (**Settings** > **Call Flow** > **Prefix Group**). Multiple Prefix Groups are treated as 'or' in terms of 'customer' entity definition (DIDs and ranges from all the selected Prefix Groups are considered to belong to the 'customer' entity). A Prefix Group can include not only full DIDs but also ranges. Note that the same Prefix Group cannot be used for several 'customer' entities as it uniquely identifies 'customer' entity DIDs. However, the ARM does not prevent a collision between the ranges of Prefix Groups; it's the operator's responsibility to prevent a collision of ranges between 'customer' entities.
Policy Studio Tag	Used if the operator chooses to manage 'customer' DIDs in the ARM Users page and thereby benefit from ARM Users capabilities (such as Policy Studio with pre-routing manipulations or Users Groups). The Policy Studio Tag should be provided in the Policy Studio (for incoming and outgoing calls) and is used by the ARM mainly for CAC counting and enforcement for specific 'customer' entities / Teams tenants. The extension for this Tag in a Policy Studio action is described under Customers Page on page 69.
SIP header	Each unique 'customer'/Teams tenant making outbound calls is identified/marked by Teams with the FQDN in the 'Contact' or 'From' header. A call in the direction 'to Teams' should have this 'Contact' header identification as well. From Teams' perspective, this is the way to identify and distinguish between 'customer' entities / tenants. The ARM provides an easy way to put the predefined string (the one used by Teams to identify a tenant) in the 'Contact' header for calls toward Teams (for more information about this option, see under Customers Page on page 69. The SIP header attribute allows the operator to provide a string to be used for the 'Contact'

Parameter	Description
	header. Note that it should be coordinated with the Teams settings for the ARM 'customer' entity / Teams tenant.
CAC profile	Can optionally be attached per 'customer' entity. For a description of a CAC profile and its capabilities, see CAC Profiles on page 311). The operator can attach a CAC profile to a 'customer' entity with both directions or a one-direction sessions limitation (defined under **Settings** > **Routing** > **CAC profiles**). Operators can reuse the same CAC Profile for multiple 'customer' entities.  

Editing a 'Customer' Entity

The option to edit a 'customer' entity allows the operator to modify all the attributes provided in the **add +** 'customer' entity action (including 'Name').

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

Deleting a 'Customer' Entity

The action of deleting a 'customer' entity should be used to delete an 'existing' 'customer' entity. The operator is prompted to confirm the delete before the action is applied.

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

Locking-Unlocking a 'Customer' Entity

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

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

A 'customer' entity's Lock / Unlock status is reflected in the Customers page in the 'Admin State' column.

Defining 'Customer' Entities using ARM Users & Policy Studio

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

Figure 2-23: Users page to define DIDs of 'Customer' entities

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

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

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

Viewing Network Summary Panes

Network Summary panes viewed in the right margin of the Network Map page can inform network operators how to optimize call routing in the network. Operators 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 Displaying a Specific Entity's Statistics on page 80.

Overall Network Statistics

The 'Network Summary' pane on the right side of the Network Map page by default displays statistics related to the *entire* network; by default, no entity in the Network Map page is selected. The 'Network Summary' pane's contents change after an entity is selected.

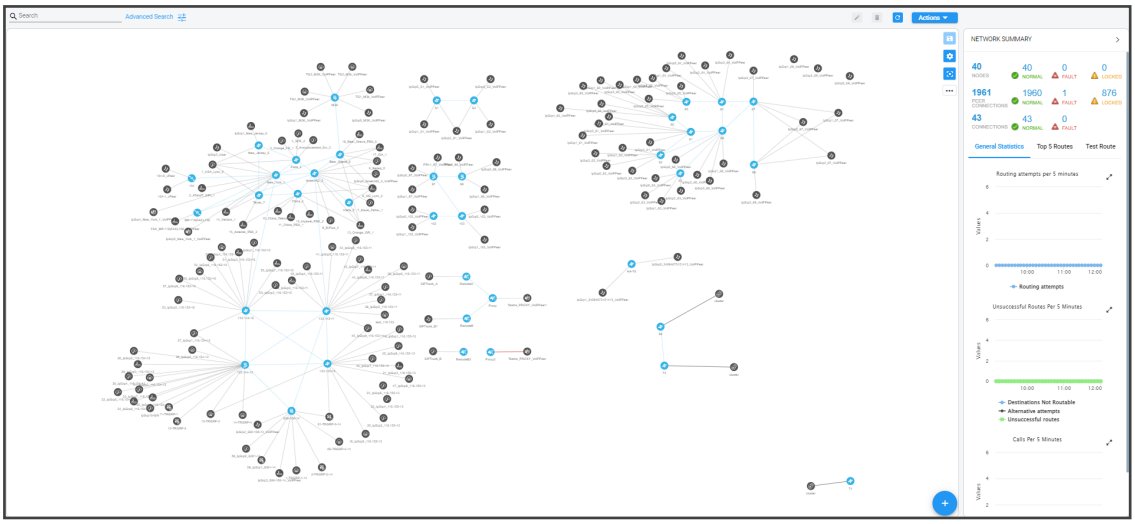
The pane displays four sections:

- Network Summary (see Network Summary below)
- General Statistics (see General Statistics on the next page)
- Top 5 Routes (see Top 5 Routes Pane on page 79)
- Test Route (see Test Route on page 80)

Network Summary

The 'Network Summary' pane on the right side of the Network Map page 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 2-24: Network Summary



The pane displays statuses of the following network entities (from left to right):

- The total # of nodes/Peer Connections/Connections in the network
- The # of nodes/Peer Connections/Connections whose status is 'Normal', i.e., available
- The # of nodes/Peer Connections/Connections whose status is 'Fault', i.e., unavailable
- The # of nodes/Peer Connections that are 'locked' (Connections cannot be locked/unlocked) and the # of nodes/Peer Connections/Connections that are unlocked and available, i.e., 'normal'

If a **Quality Layer** is selected (from the vertical ellipsis 'Layers' icon, the **Quality** icon is selected), '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.

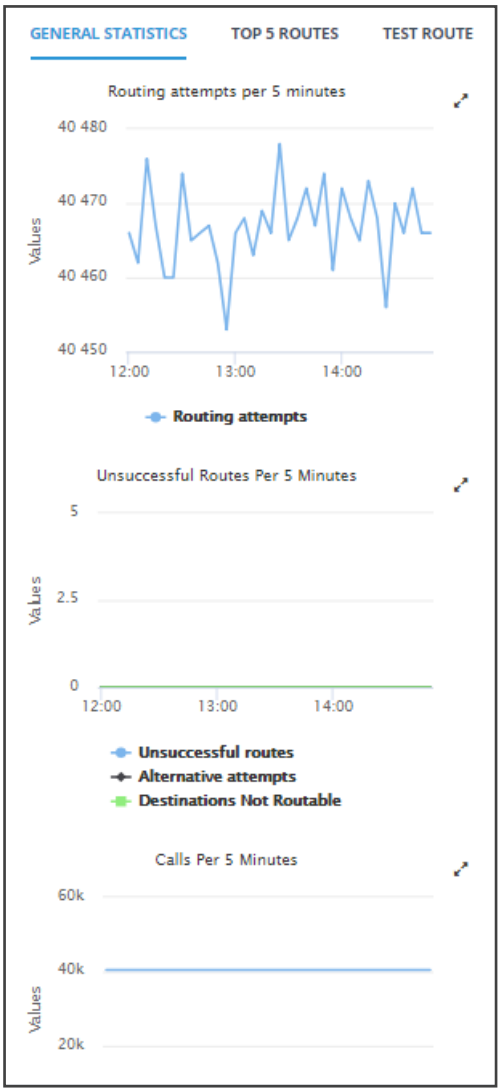
General Statistics

General statistics related to the entire network can be displayed.

➢ **To display general statistics related to the entire network:**

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

Figure 2-25: General Statistics



Three graphs are displayed (top to bottom):

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

➢ **To facilitate your analysis:**

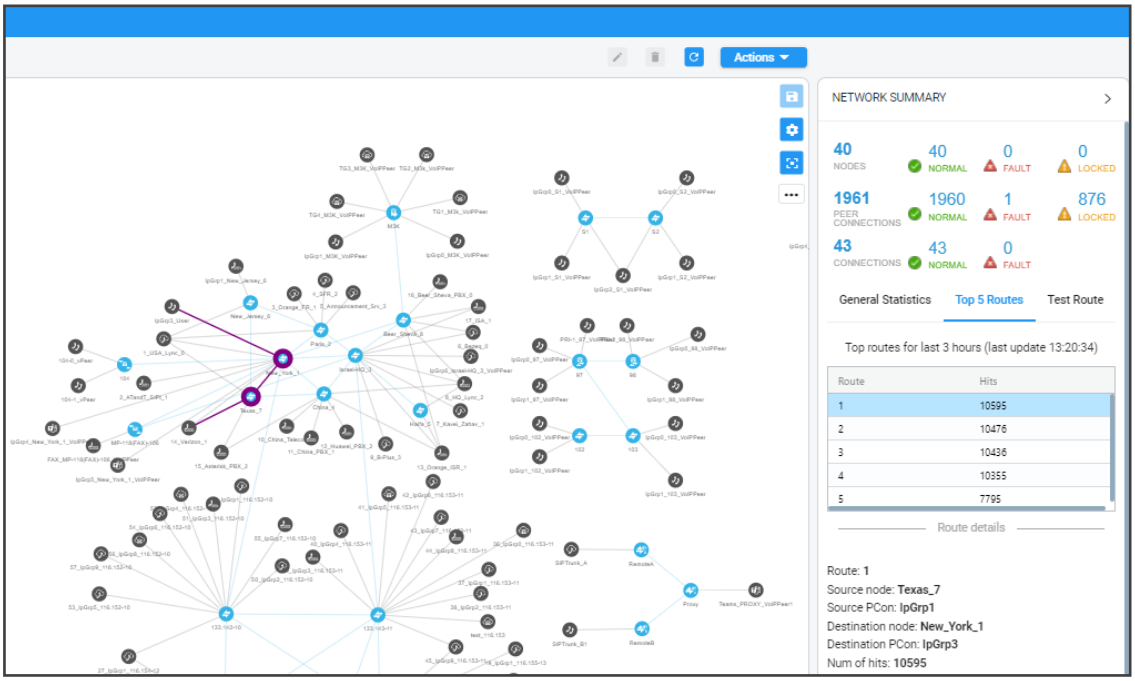
- Click the expand icon next to any of the three graphs to project a zoomed-in graph to the front.

Figure 2-26: Projecting a Zoomed-in Graph to the Front

Top 5 Routes Pane

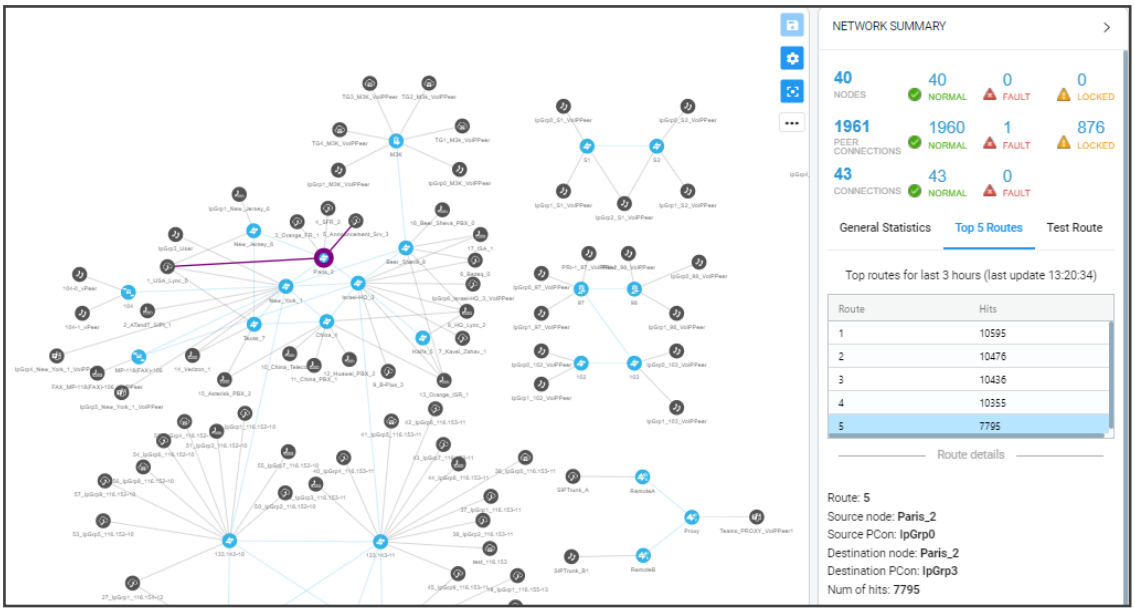
The 'Top 5 Routes' pane under the **Top 5 Routes** tab in the 'Network Summary' pane gives operators visibility into the five most frequently used routes over the last three hours.

Figure 2-27: 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 next figure, Route 5 is selected. Details displayed include Source Node / Peer Connection and Destination Node / Peer Connection.

Figure 2-28: Top 5 Routes – Details of Route 5



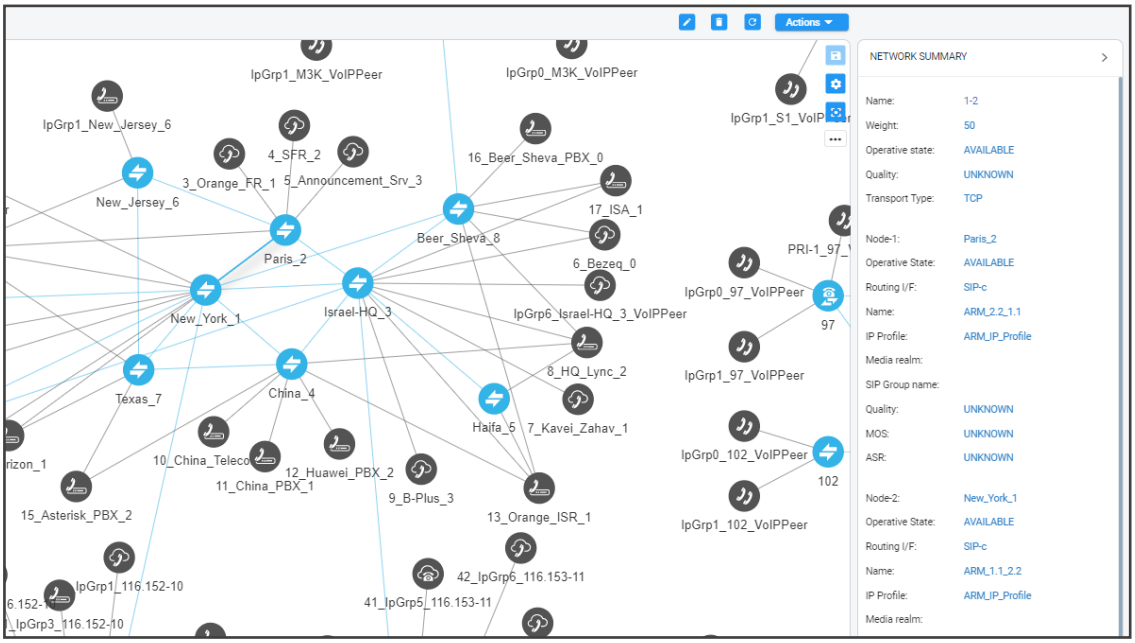
Selecting Route 1-5 (one of the top five routes) visualizes the path in **bold purple** in the Network Map as shown in the preceding two figures.

Test Route

See Testing a Route on page 96 for detailed information.

Displaying a Specific Entity's Statistics

If an entity or a connection is selected in the Network Map page, the 'Network Summary' pane on the right displays statistics related to that selected entity or connection.



In the figure above, the entity selected, i.e., the connection between **Paris_2** and **New_York_1**, is shaded. Information about this connection is displayed in the 'Network 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 page.

Other entities must be provisioned by the network operator.

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

- mandatory fields are marked with an asterix *
- a field with missing or incomplete information is outlined red

Adding an AudioCodes Node to the ARM

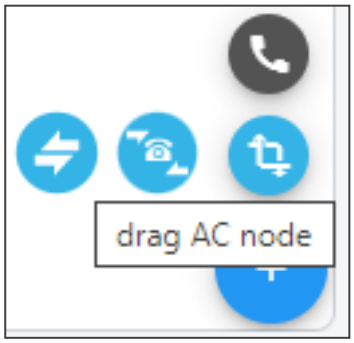
AudioCodes nodes (SBCs and gateways) are automatically detected and displayed in the ARM's Network Map page, allowing you to begin configuring actions immediately after auto-detection. However, to prevent potential provisioning mistakes at the node (SBC or Gateway) level, it's preferable to add nodes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

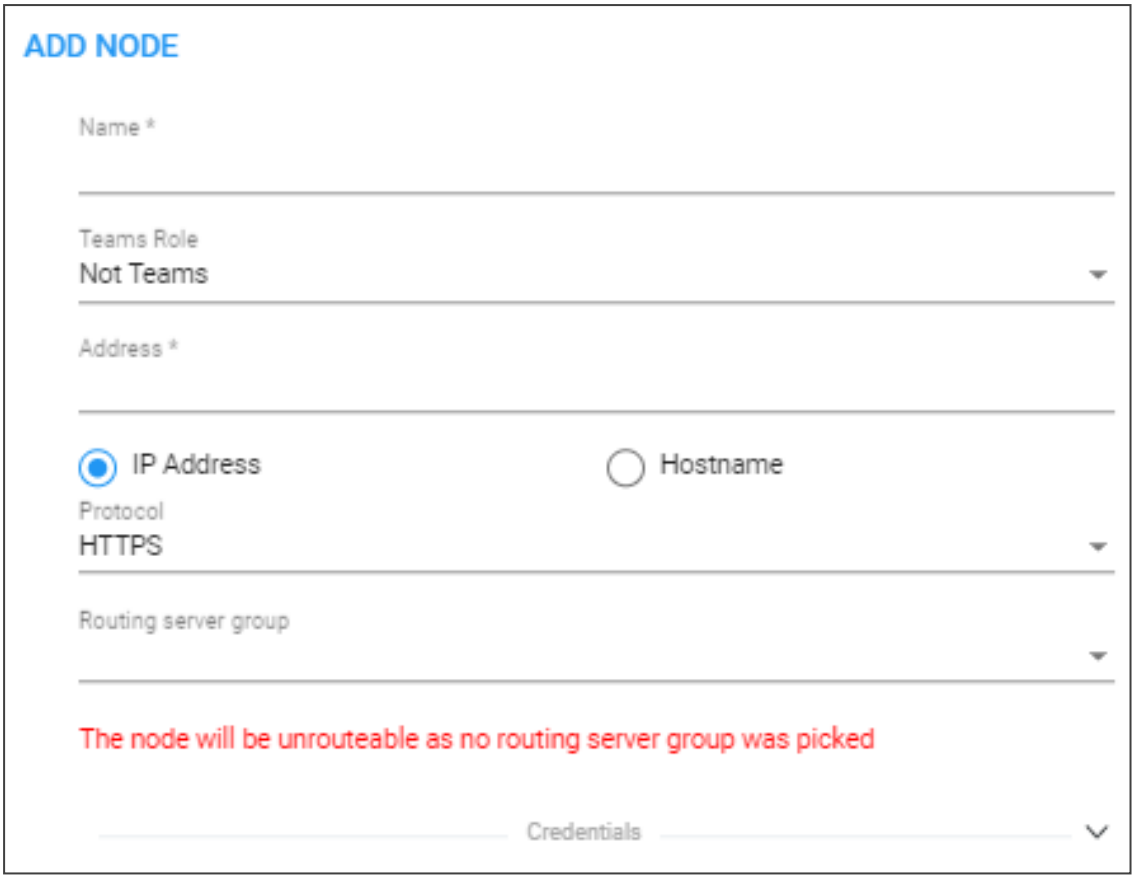
When a new node is added either by auto-detection or manually to the ARM, the ARM automatically detects Peer Connections and Routing interfaces associated with the node.

- The maximum number of allowed nodes in the ARM is 300.
- A larger machine is required for the ARM Configurator when more than 150 nodes are deployed. The ARM Configurator should have 8 CPUs and 32 GB memory.
- The maximum number of allowed nodes is enforced; an alarm is generated if the 300 threshold is crossed, and new nodes are not allowed to be added.

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

1. Click the icon, navigate to the AudioCodes node icon and then drag and drop it into the Network Map; as it drops, the Add Node screen opens.

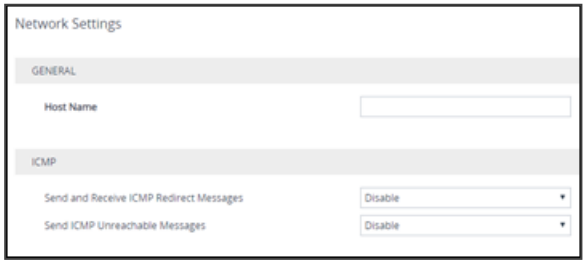




2. Provide a name, IP address or Hostname (FQDN), and protocol. The option to use Hostname (FQDN) rather than a hard-coded IP address gives you added flexibility when designing your telephony network.
3. From the 'Routing server group' drop-down, select a Routing Server Group (for more information, see Adding a Routing Servers Group with Internal and External Priorities).
4. Hostname (FQDN) can be configured for an existing node in the node's Web interface, Network Settings page. The page is opened by right-clicking the node in the ARM's Network Map page and then selecting **Configure** from the popup menu, logging in to the device's Web interface, selecting the **IP Network** menu, opening the **Advanced** tab and then selecting the **Network Settings** tab.

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

Figure 3-1: Host Name (FQDN) in the 'Network Settings' page in the node's Web Interface



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

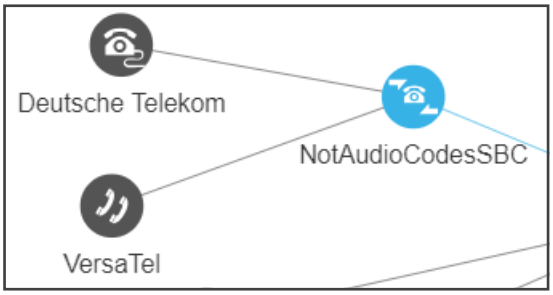
5. View the added AudioCodes node in the Topology Map; all elements associated with the node are automatically provisioned and displayed in the Network Map.

- Peer Connections are displayed in Locked state; you need to perform an unlock for them to provide a service.
- Node provisioning by auto-detection is described in Migrating Device Routing to the ARM on page 379.

Adding a Third-Party Node to the ARM

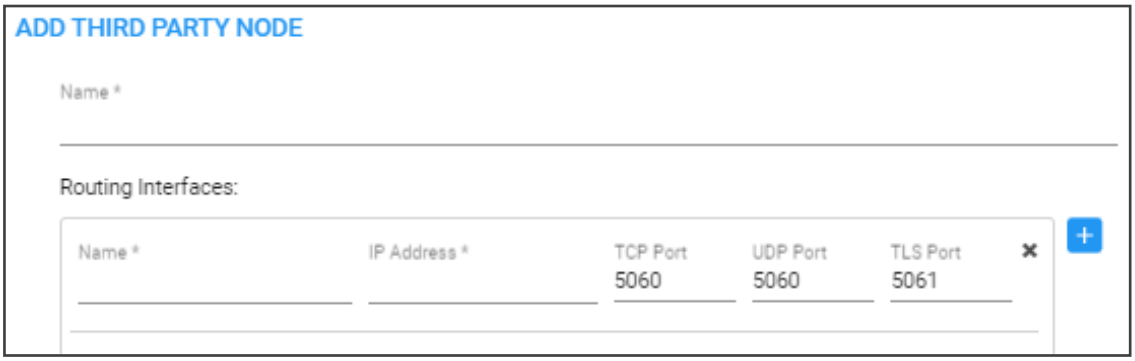
The ARM allows you to add third-party non-AudioCodes nodes (SBCs and Media Gateways) to the Network Map page so that the ARM can be used for call routing in heterogeneous environments with a mix of AudioCodes and non-AudioCodes nodes as part of your network.

Figure 3-2: Third-party device in Network Map page



➢ **To add a third-party node:**

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



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

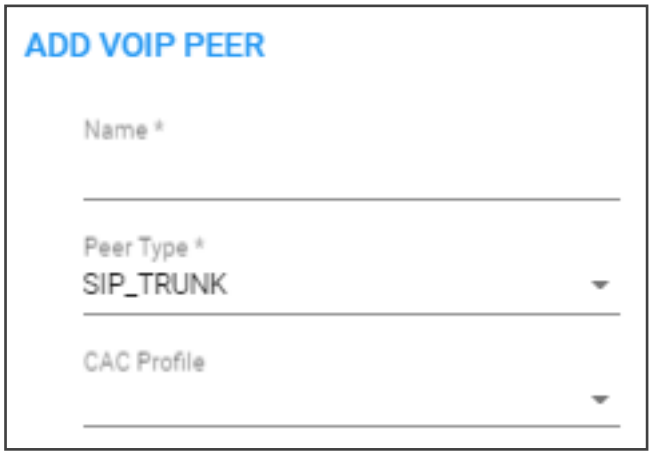
Adding a VoIP Peer

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

➢ **To add a VoIP Peer:**

1. In the Network Map page, click the  icon and then click the  icon to view the VoIP Peer types displayed.

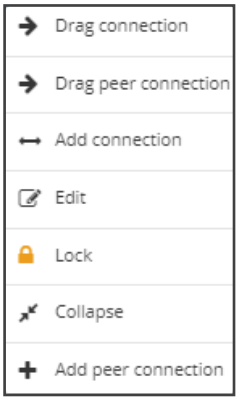
2. Drag the VoIP Peer type you require, e.g., IP PBX or SIP Trunk (you can determine the type from the tooltip displayed when pointing your cursor over it), and then drop it in the Network Map page; the 'Add VoIP Peer' screen opens. Use the preceding and following figure as references.



3. Enter a name for the VoIP Peer.
4. Verify that the 'Peer Type' displayed is the same VoIP Peer type you selected, dragged and dropped into the page.
5. From the 'CAC Profile' drop-down, select a profile. For information about CAC Profiles, see under CAC Profiles on page 311
6. Click **OK**.

➢ **To connect a third-party non-AudioCodes node with a VoIP Peer:**

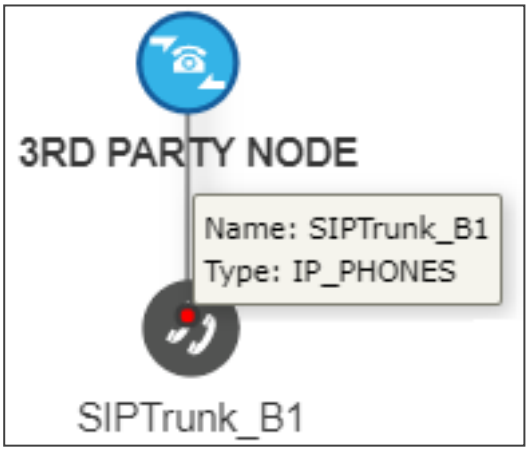
1. In the Network Map page, right-click the third-party non-AudioCodes node and from the pop-up menu, select the →**Drag connection**.



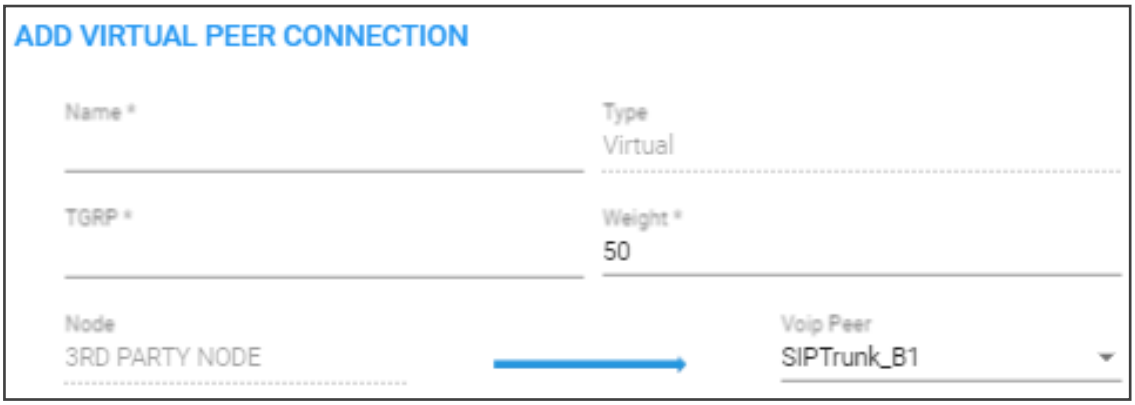
> The action 'Drag peer connection' is available only to third-party non-AudioCodes SBCs or Media Gateways. It's not applicable to AudioCodes SBCs or AudioCodes Media Gateways.

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

Figure 3-3: Drag mouse from Node to VoIP Peer



3. Release the mouse.



4. In the Add Virtual Peer Connection screen that then opens, connect the third-party node to the ARM topology - to an AudioCodes node or to a SIP module - for end-to-end routing capabilities.

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

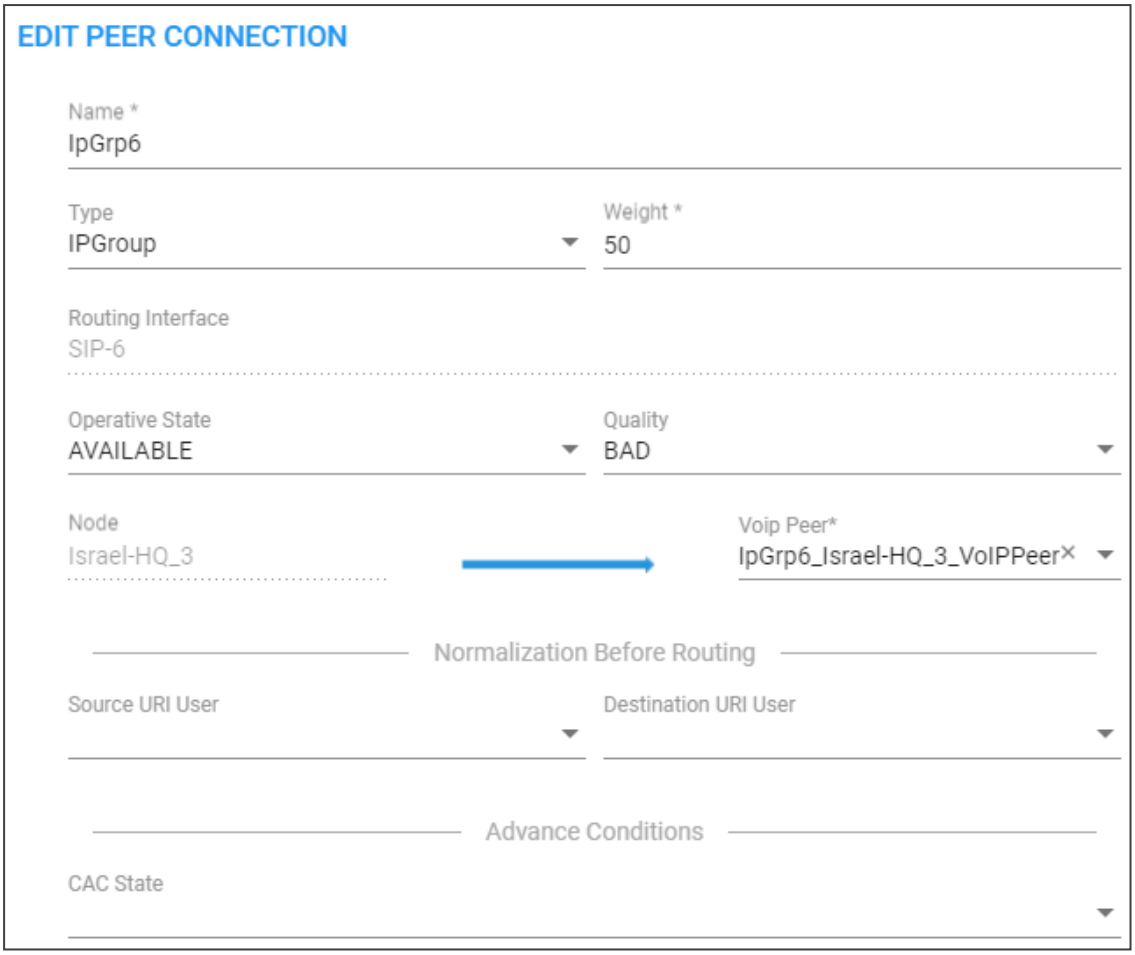
The ARM will then perform routing to Peer Connections attached to third-party nodes. In Routing Rules, choose the Peer Connection or VoIP Peer associated with the third-party node and in this way, achieve end-to-end routing in a heterogeneous network.

Attaching a CAC Profile to a Peer Connection

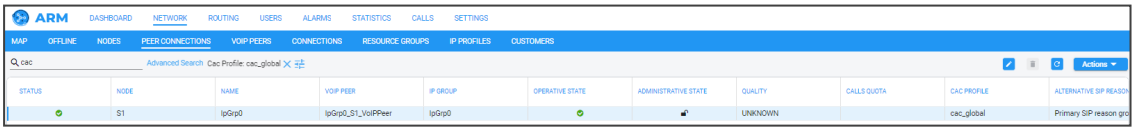
A Call Admission Control (CAC) Profile can be attached to a Peer Connection. The same CAC Profile can be reused for multiple Peer Connections. Implementing a CAC Profile enables network operators *to regulate the volume of voice traffic* handled by the device.

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

1. In the Network Map page (**Network** > **Map**) or in the Peer Connections page (**Network** > **Peer Connections**), select and **edit** a Peer Connection.

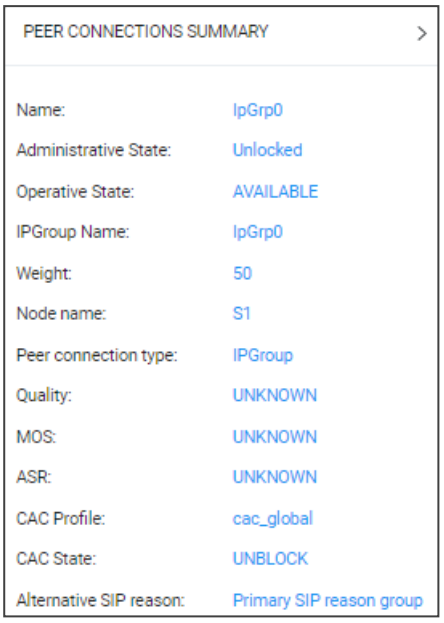


2. From the 'CAC Profile' drop-down, select one of the previously defined CAC profiles and click **OK**.
3. View in the Peer Connections page the CAC Profile in the 'CAC Profile' column. In the page, optionally filter all Peer Connections using CAC Profile.



4. Optionally click **Advanced Search** to further filter the page.

5. In the page, select a Peer Connection with an attached CAC Profile to display information about the status of the CAC in the 'Peer Connection Summary' pane on the right side of the page.



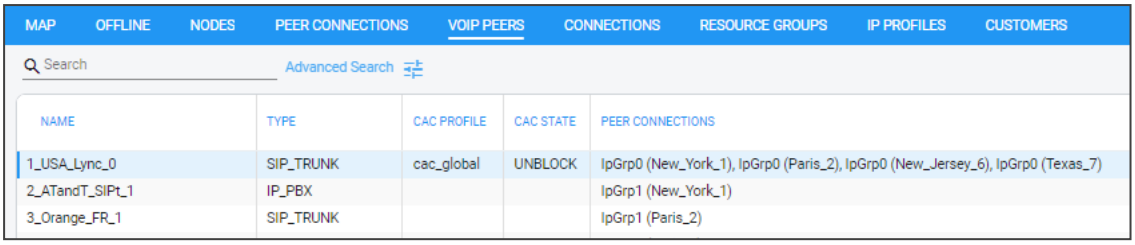
Attaching a CAC Profile to a VoIP Peer

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

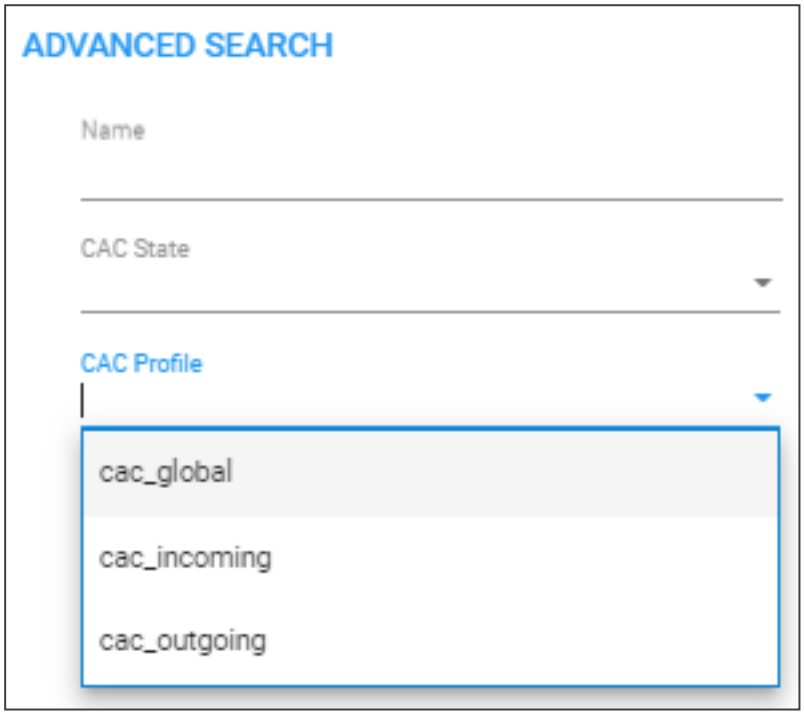
➢ To attach a CAC profile to a VoIP Peer:

1. From the Network Topology Map page (**Network** > **Map**) or from the VoIP Peers page (**Network** > **Peer Peers**), select and **edit** the VoIP Peer.

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



4. In the VoIP Peers page, you can (optionally) click **Advanced Search** to filter all VoIP Peers by CAC Profile.



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

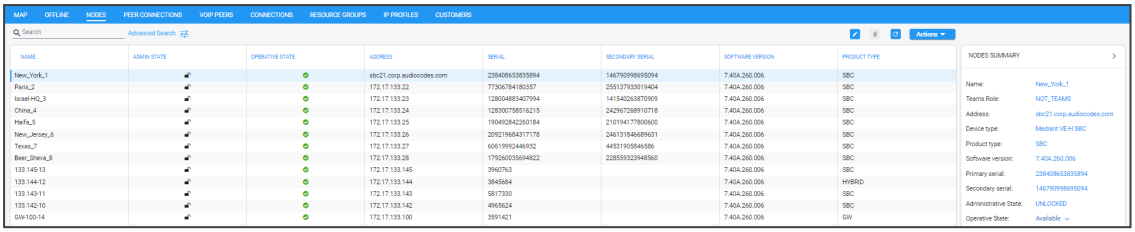
Warning – generated for VoIP Peers when the number of sessions reaches the threshold limit (as a percentage) defined in **Settings** > **Routing** > **CAC Profiles**.

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

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

Using the Nodes Page

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



Up to 300 Session Border Controllers (SBCs) and/or Media Gateways (nodes) are supported in ARM Topology and Routing, necessitated by product popularity and extensive global deployments. A number of distributed enterprises with multiple branches have required more than 100 nodes to be supported in their deployments.

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

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

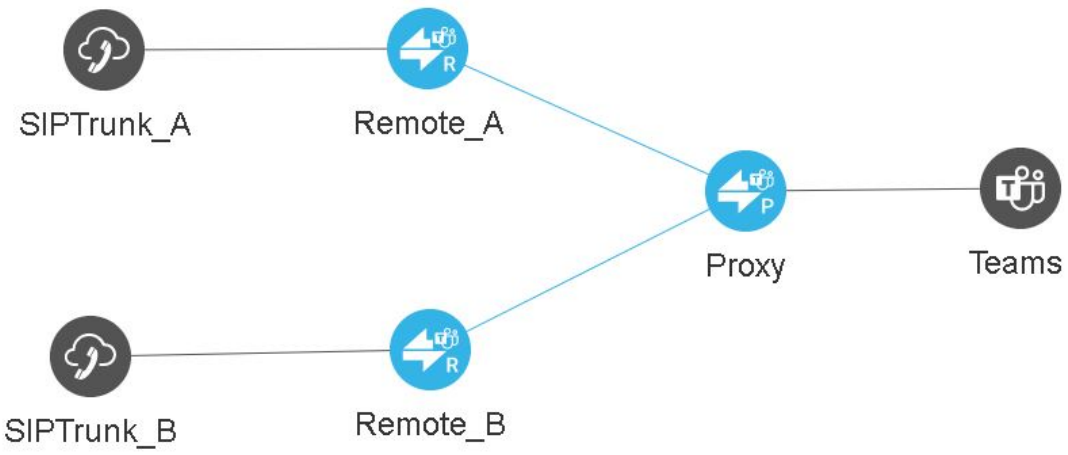
Configuring a Microsoft Teams LMO Topology

Microsoft Teams Local Media Optimization (LMO) is an important feature for enterprise telephone networks seeking to utilize Microsoft Cloud. For detailed information about LMO, see here.

Two node roles feature in the topology:

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

Figure 3-4: Typical Microsoft Teams LMO Topology

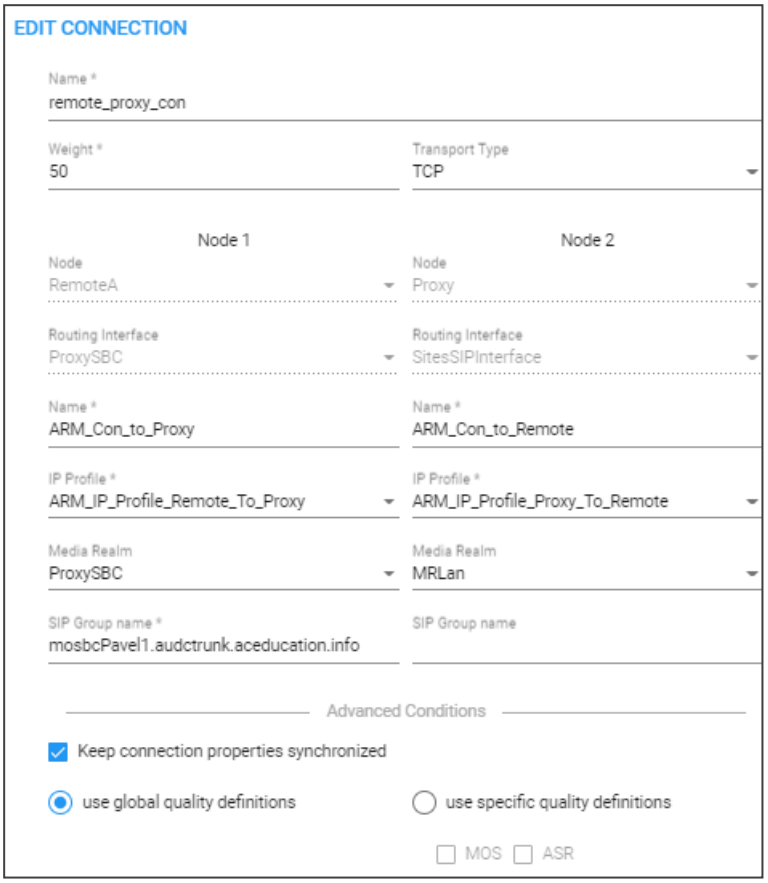


➢ To configure a Microsoft Teams LMO topology:

1. When defining the connection between the Proxy and the Remote, configure each side to support LMO by predefining the default values for IP Profiles (see IP Profiles Page on

page 60) and the connection itself (IP Group); mandatory fields are indicated with an asterisk *; fields that can be left undefined are not indicated with an asterisk.

2. After selecting the node per Teams role, define a connection between them (by clicking **Drag Connection** and then dragging a line or by clicking **Add connection** and defining a line); when the ARM detects that the connection is between Remote and Proxy, fields will be predefined with correct defaults. For example:



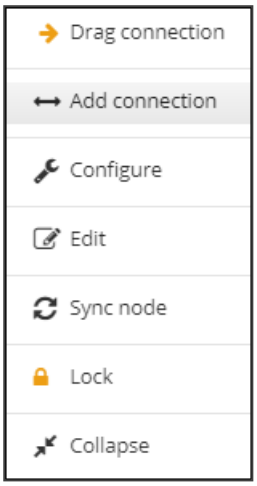
- Media Realms are synchronized from each node (the ARM Configurator determines Media Realms that are selected as used by the Routing Server).
- IP Profiles are configured in the ARM (see IP Profiles Page on page 60).

Adding Connections

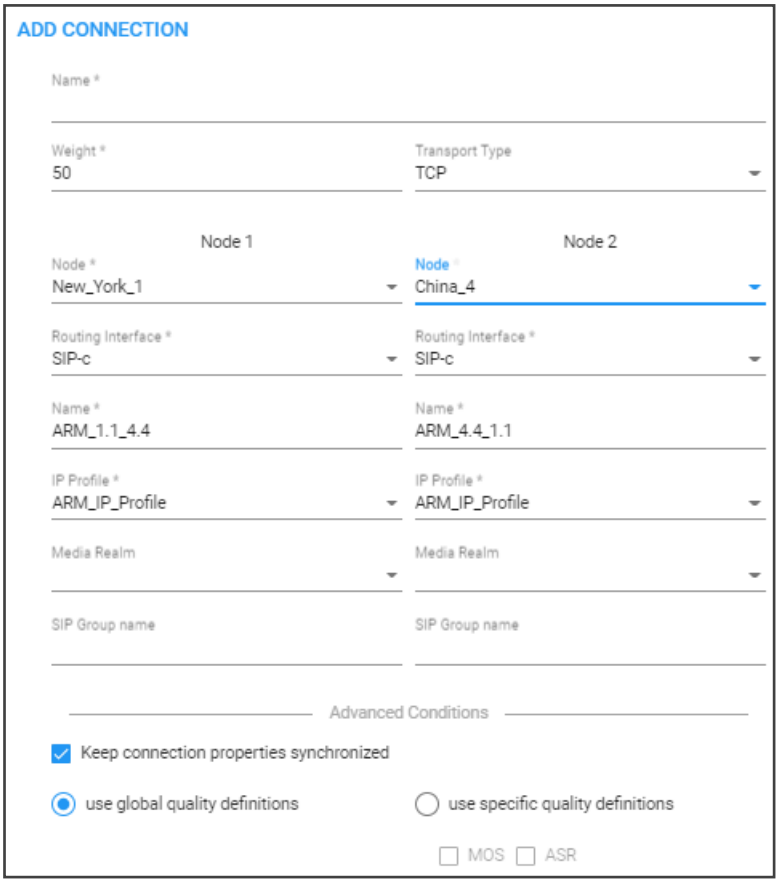
The ARM enables network operators to configure connections between nodes.

➢ **To connect two nodes:**

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



Alternatively, select the **Drag connection** option, or from the **Actions** drop-down, select **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. Select and configure a corresponding name of an IP Group for each node. Default 'Name' options are taken from the SOURCE and DESTINATION interface IDs, for example, **ARM_4.4_1.1**, as displayed in the preceding figure.
8. From the 'IP Profile' drop-down | 'Media realm' drop-down, select an element that is used by or created by the Routing Server in the SBC.

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

9. To define Advanced Conditions (quality-based routing), see Routing Settings on page 289.

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

Synchronizing Topology

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

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

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

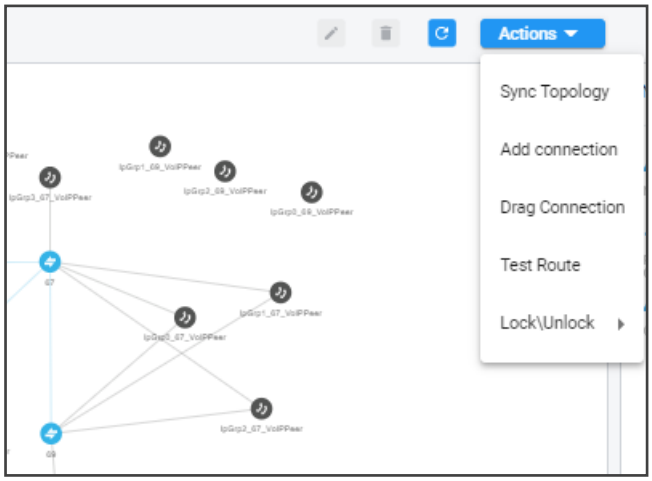
The ARM auto-discovers all network entities such as Nodes, Peer Connection and VoIP Peers, associates a VoIP peer with each Peer Connection, and displays them in the Network Map view.

The ARM detects activity originating from a node and puts the node on the map (peer collection). The ARM recognizes a newly added node and extracts all IP groups (i.e., Peer Connections). Users must add connections between nodes and change the VoIP peer types (see under Adding Connections on page 93).

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 topology:**

- In the Network Map page, Peer Connections page or Connections page, click the **Sync Topology** option in the **Actions** drop-down.



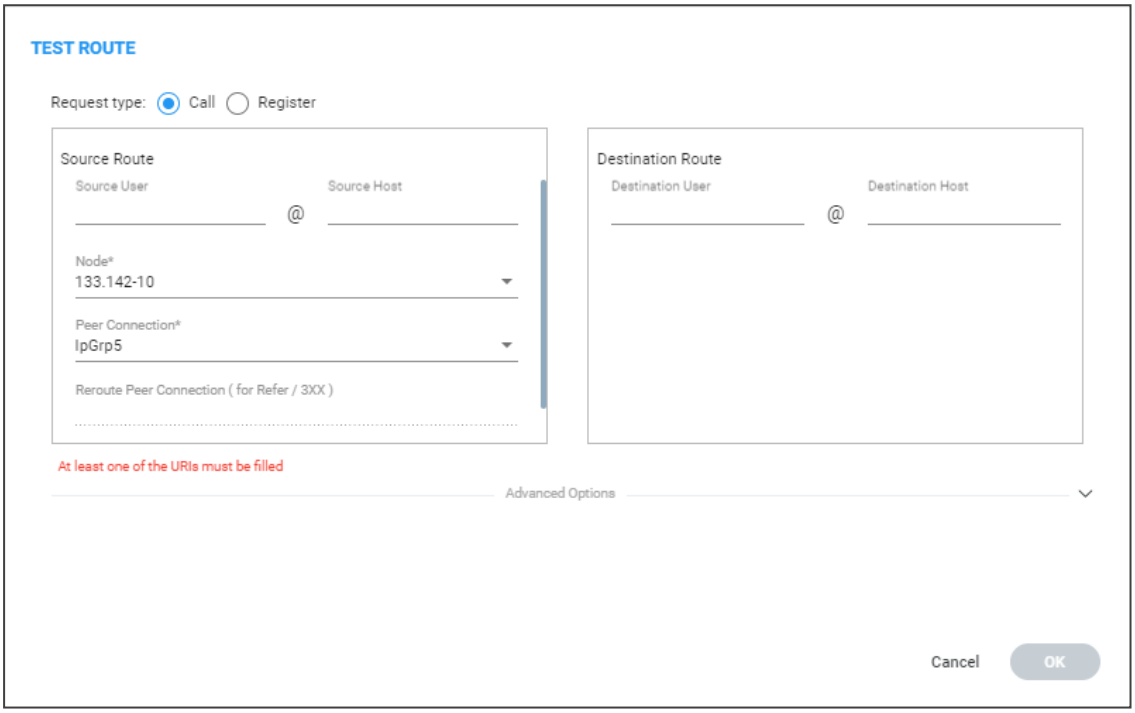
Global synchronization of the entire IP telephony network is performed.

Testing a Route

Network operators 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 page, right-click the connection between a node and a VoIP Peer (Peer Connection) and then from the popup menu, click the **Test Route** option.



2. [Optional] Enter the Source and Destination Route. From the drop-down menus, select the **Node**, **Peer Connection**, **Reroute Peer Connection** (only for **REFER/3XX**).
3. Under 'Advanced Options', select the routing rules mode:
   - **Live**. When a new call destination is calculated, the Routing Rule is taken into consideration and live traffic may be impacted.
   - **Test**. Tests the Routing Rule or Dial Plan *offline* without impacting or disrupting live calls traffic.
   - **Live** *and* **Test** selected together. The Routing Rule is considered when:
     - calculating the live routing path -and-
     - testing a route in the live topology map *and* in the offline planning page

   Each routing rule can be enabled or disabled separately for **Live** mode and / or **Test** mode (see also under Adding a New Routing Rule on page 328).

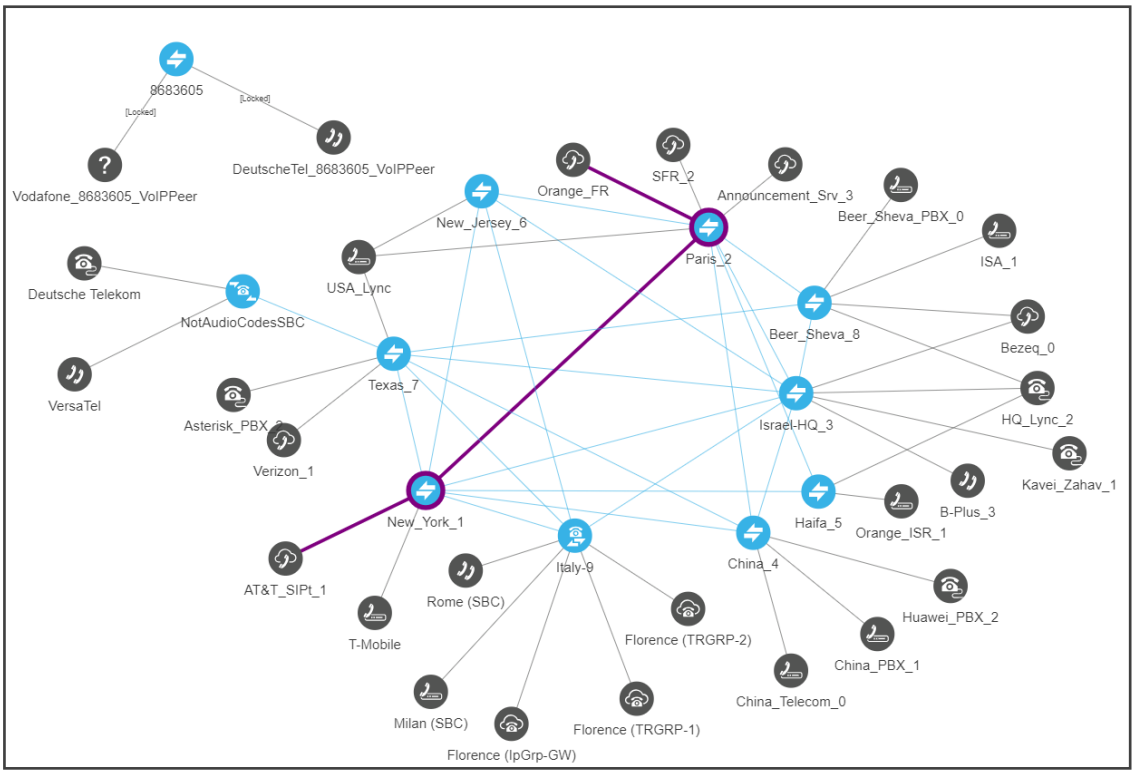
4. Under 'Advanced Options', select the call trigger. By default, the **Initial** option is enabled. See step 11 under Adding a New Routing Rule on page 328 for more information about call triggers.

5. Optionally, test the route with a specific ARM Router (also supported in 'Test Route' activated from 'Offline Planning'): Under 'Advanced Options', select from the 'Router' drop-down:

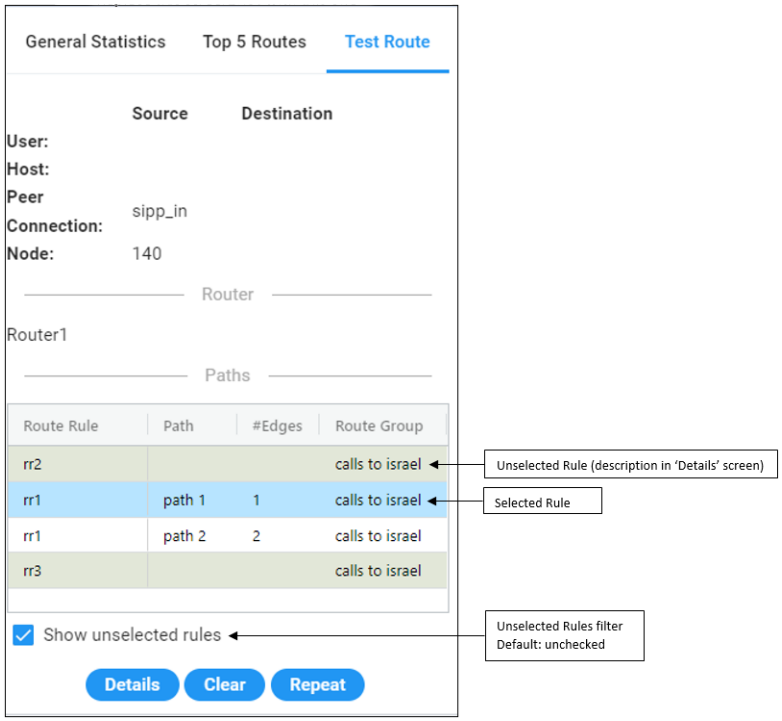
   - Any (default) = the ARM Configurator contacts any ARM Router to perform a 'Test Route' and get the results; the ARM Router is chosen randomly.
   - Select a specific ARM Router for a test call.

   Use this feature for debugging and locating potential issues.

6. 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 'Network Summary' pane on the right of the Network Map page displays detailed information under 'Paths'.



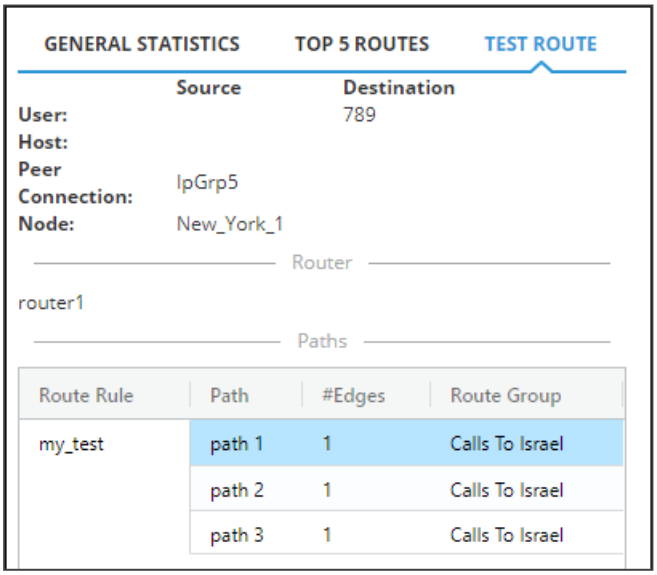
Gray = Unselected Rule

White = Selected Rule

Blue = selected row

if we have unselected rules they'll be grayed.

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



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

Figure 3-5: Forking Path 1

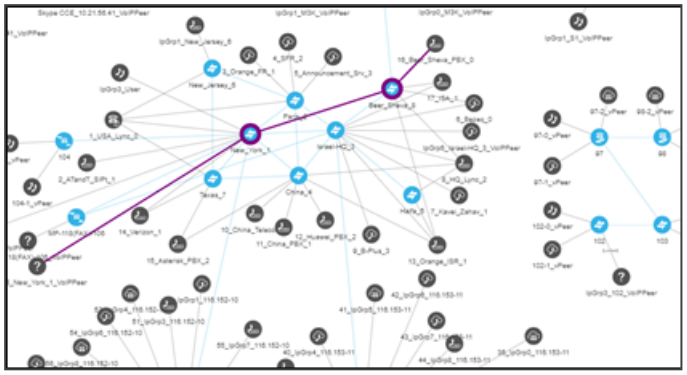


Figure 3-6: Forking Path 2

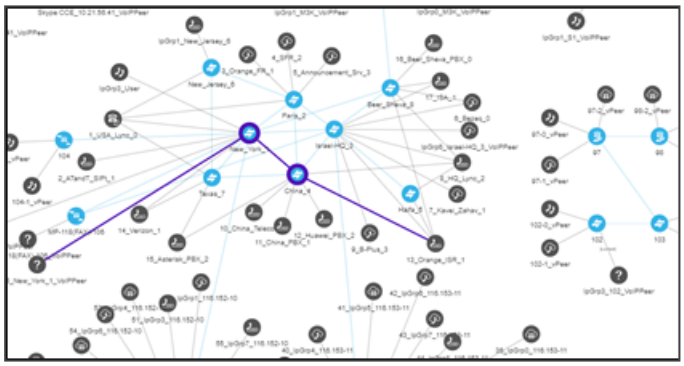
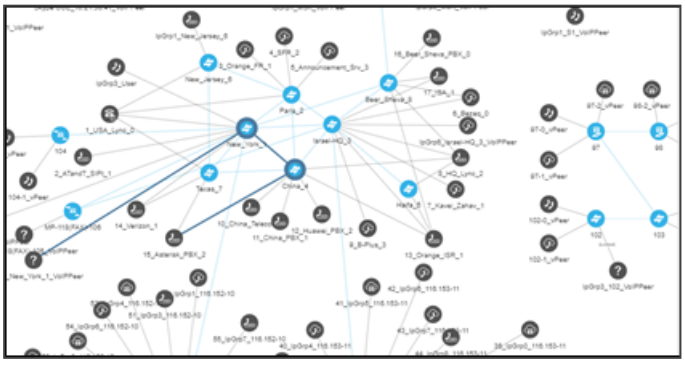
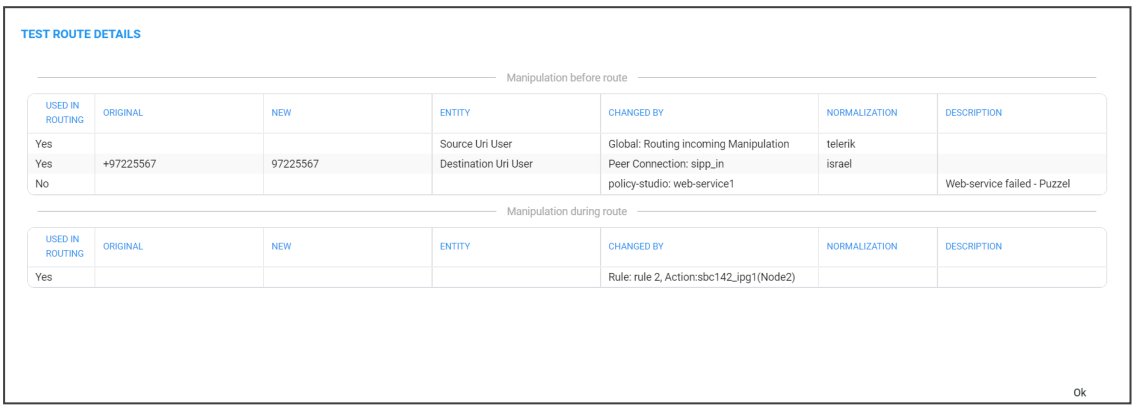


Figure 3-7: Forking Path 3



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

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



9. In the above example of the Test Route Details screen:

- Compare the column ORIGINAL to the column NEW; the number changes if a normalization rule was applied. The normalization rule is configured in the Normalization Group rules attached to the Peer Connection. For related information, see also under Peer Connections Page Actions on page 54 and Examples of Normalization Rules on page 399.
- The screen example indicates *when* manipulation was performed:
  - Manipulation *before* route (upper screen section)
  - Manipulation *during* route (lower screen section)

  In the screen example, manipulation was performed *before and during* route.
- Column ENTITY indicates which part of the SIP Request was manipulated.
  - Possible values: Source URI User, Source URI Host, Destination URI User, Destination URI Host, Destination IP Address, Destination Port, Destination Protocol, User Credential User Name, User Credential Password
- The column CHANGED BY (use the previous figure as reference):
  - the first row indicates by global Normalization Group – see under Adding a Normalization Group on page 238 and Normalization Before Routing on page 245 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 48 for detailed information

- the 'No' in the third row under the column USED IN ROUTING indicates an unselected Policy Studio that was *not* applied (see step 8 under Web-based Services on page 269)
- also under 'Manipulation during route', the Yes/No in the first row under the column USED IN ROUTING indicates the selected/unselected Test Route path.

- The column NORMALIZATION indicates which 'Manipulation Group' the entity passed through, according to which regular expression the entity was changed.
- The column DESCRIPTION indicates the reason why the Policy Studio / Routing Rule is unselected. For more information, see under Examples of Unselected Rules Reasons on page 106

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

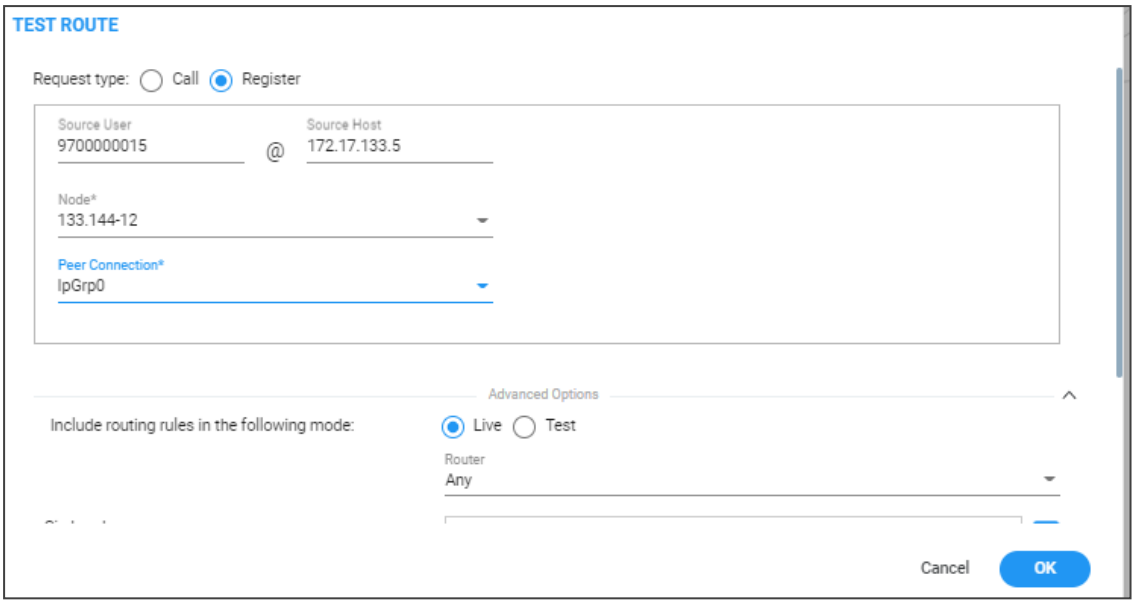
Testing a Route for Registration Messages

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

➢ **To test a route for registration messages:**

- In the Network Map page, click the **Actions** drop-down and select the **Test Route** option; in the Test Route screen that opens, select the 'Request type' to be tested. Select **Register** for testing registration messages routing. The default is **Call** (for testing call routing).

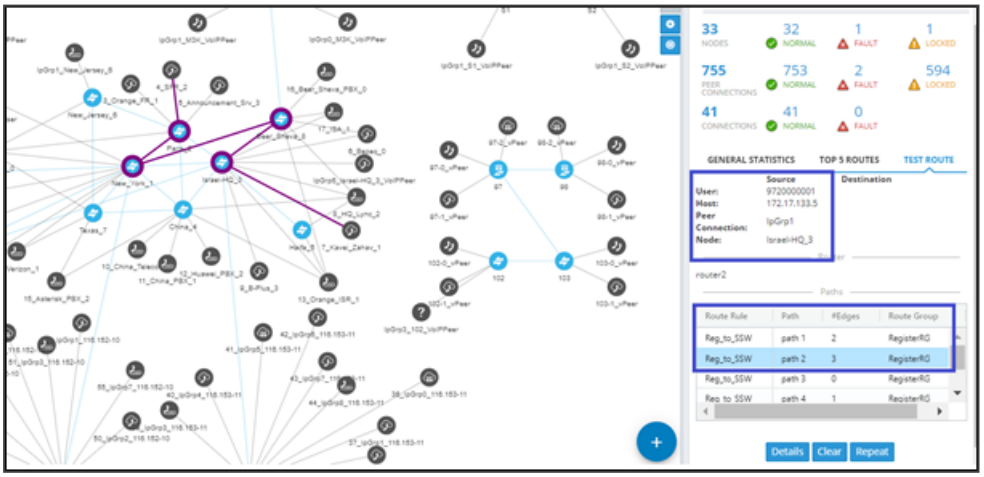
Figure 3-8: Include routing rules in the following mode: Live



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

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

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



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

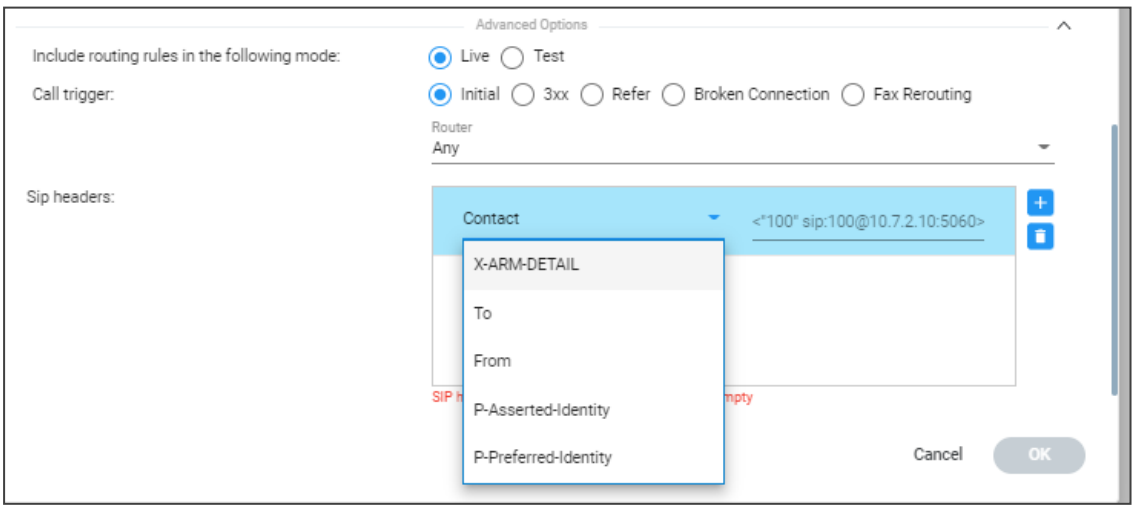
Testing Call Routing Simulation with a Specific SIP Header

The Test Route feature includes the capability to simulate a call with a specific SIP header's value. Before testing call routing simulation with a specific SIP header, you need to configure the manipulation of a specific Source URI header as described in Adding a New Routing Rule on page 328.

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

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

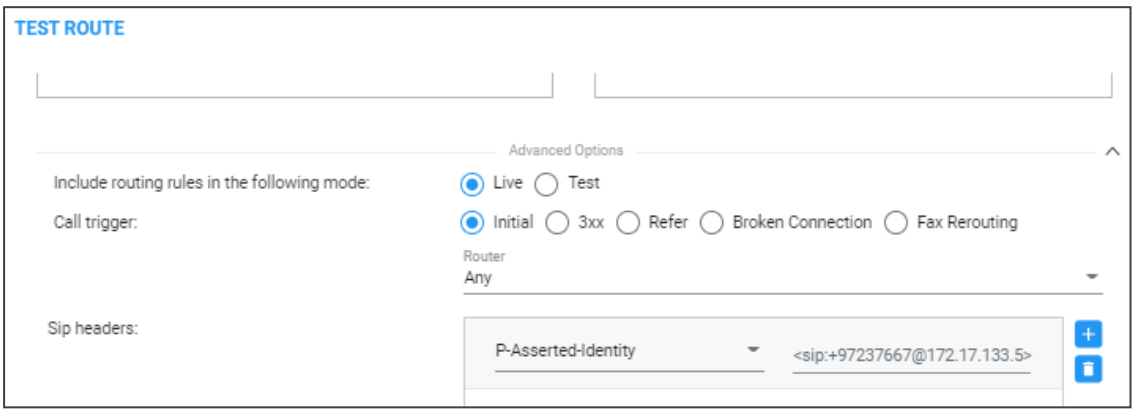
Figure 3-9: Test Route on multiple SIP headers simulation



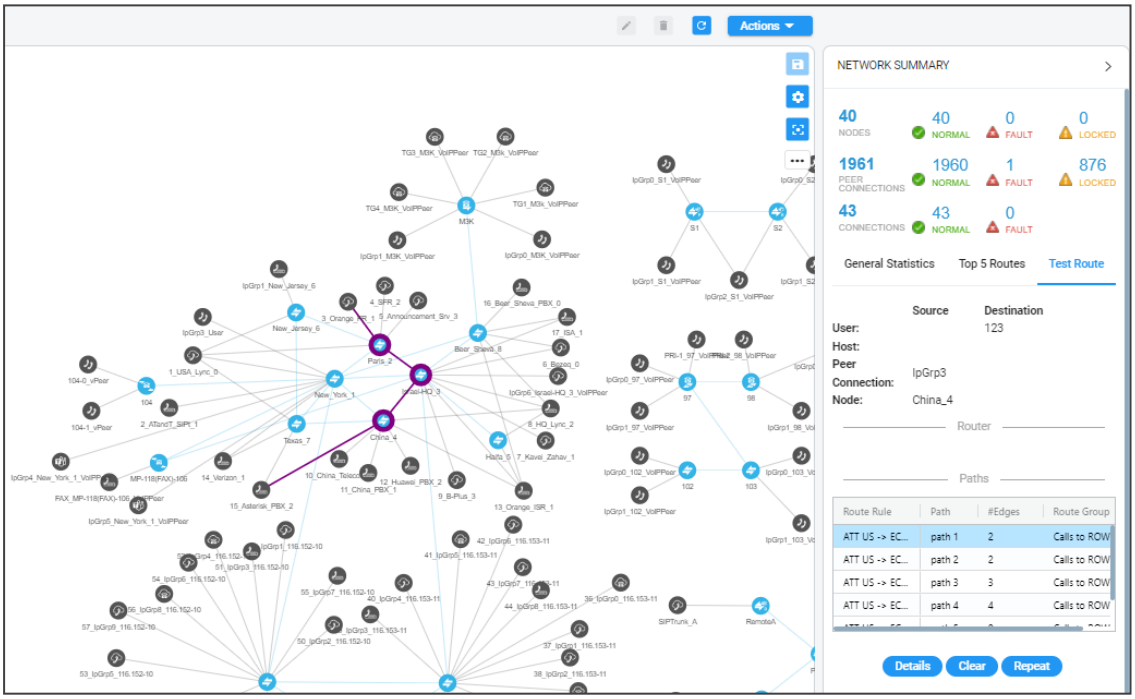
3. View the manipulated value, including the reason for the manipulation and the normalization rule that was applied, in the Test Route result in the details of the selected path.

4. Perform a Test Route with a P-Asserted-identity value simulation (for example).

Figure 3-10: Testing a route with a P-Asserted-identity value simulation



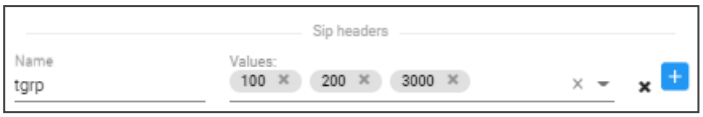
5. Click **OK** and view the Test Route results.



6. Under 'Paths', select the path and click **Details** to view its details showing the manipulation performed on P-Asserted-Identity.

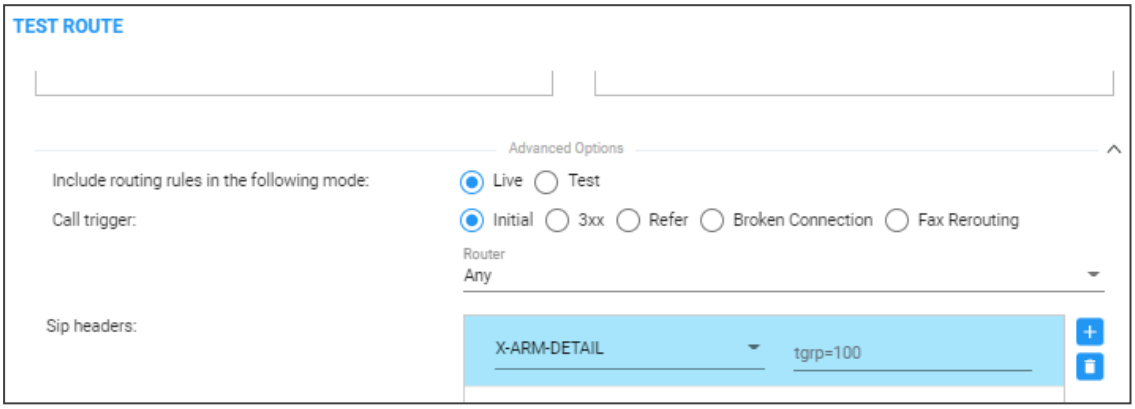
7. Following is an example of manipulation of X-ARM-DETAIL and its testing. In the Routing Rule, under ‘SIP headers’ under ‘Advanced Conditions’, add the header name and its value:

Figure 3-11: SIP Headers



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

Figure 3-12: Test Route with X-ARM-DETAIL value simulation



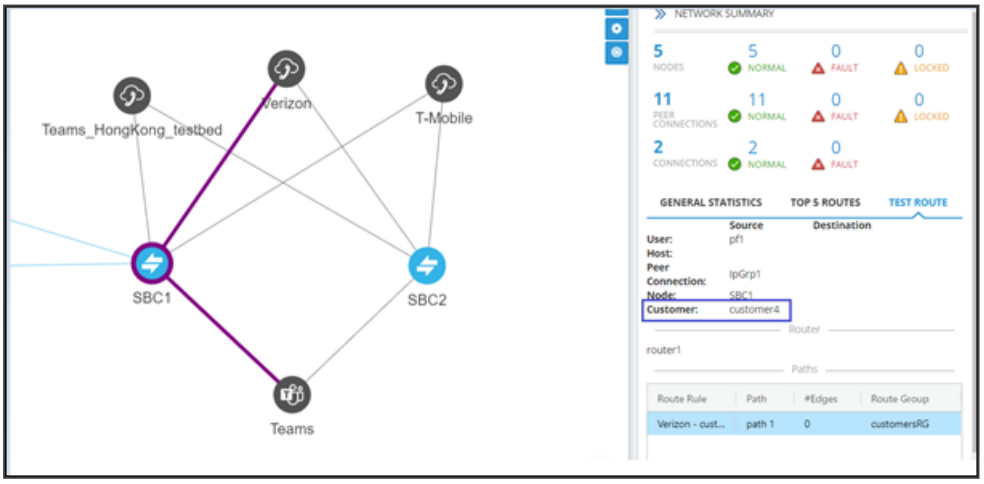
9. View the Test Route results.

Testing 'Customer' Entity

The 'Customer' entity is supported by the ARM's Test Route. For detailed information about the 'Customer' entity, see under Customers Page on page 69 and under Defining a 'Customer' Entity (Teams Tenant) on page 72

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

Figure 3-13: Testing a Route from a 'Customer' Entity



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

Examples of Unselected Rules Reasons

Examples of unselected rules reasons fall into two categories:

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

During Route – Unselected Rules

Node state is invalid

Peer Connection state is invalid

Peer Connection quality is invalid for the current action

Trunk is invalid for Request URI action

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

Registered user not found

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

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

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

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

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

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

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

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

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

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

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

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

Outgoing Peer Connection CAC limit has been reached

Outgoing VoIP Peer CAC limit has been reached

Outgoing Peer Connection Quota limit has been reached

Outgoing Topology Group Quota limit has been reached

Outgoing customer CAC limit has been reached

Incoming customer CAC limit has been reached

Incoming VoIP Peer CAC limit has been reached

Incoming Peer Connection CAC limit has been reached

Prevent source Node loopback

Prevent source Peer Connection loopback

Prevent source VoIP Peer loopback

Before Route (Policy Studio) - Unselected Rules

Web service failed – with proper reason

4 Designing a Network Topology in the Offline Page

The ARM provides network operators an add-on to design an IP network in the Offline page (**Network** > **Offline**), starting from the beginning.

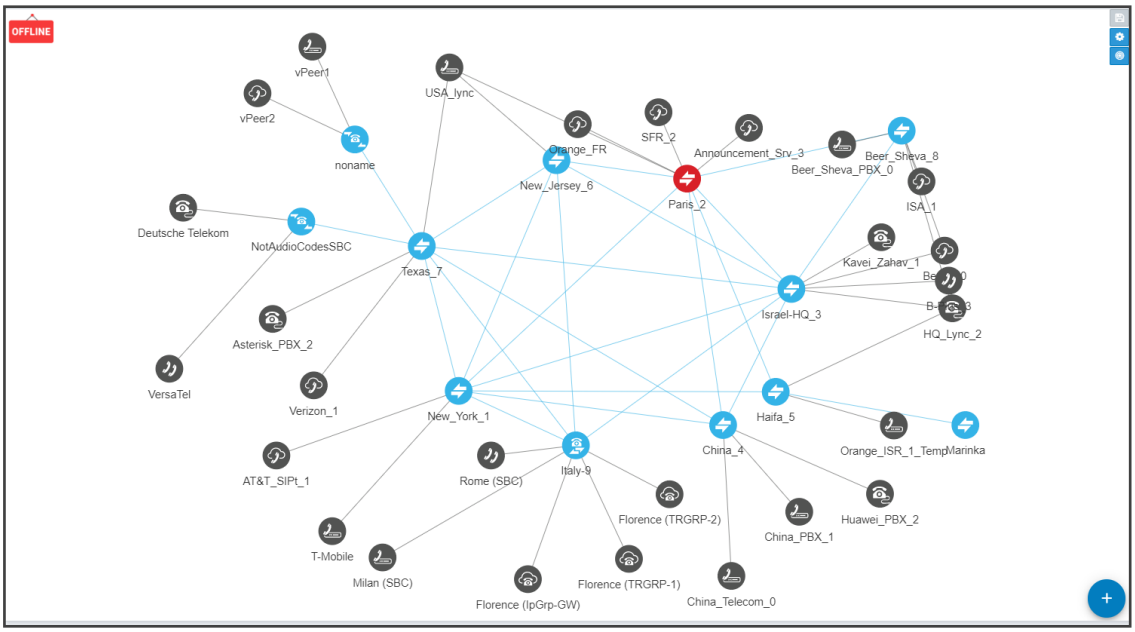
Operators can alternatively import an existing live topology into the page, make changes to entities' configuration and statuses, and test how the changes impact network functionality.

Feature benefits:

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

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

Figure 4-1: Offline page



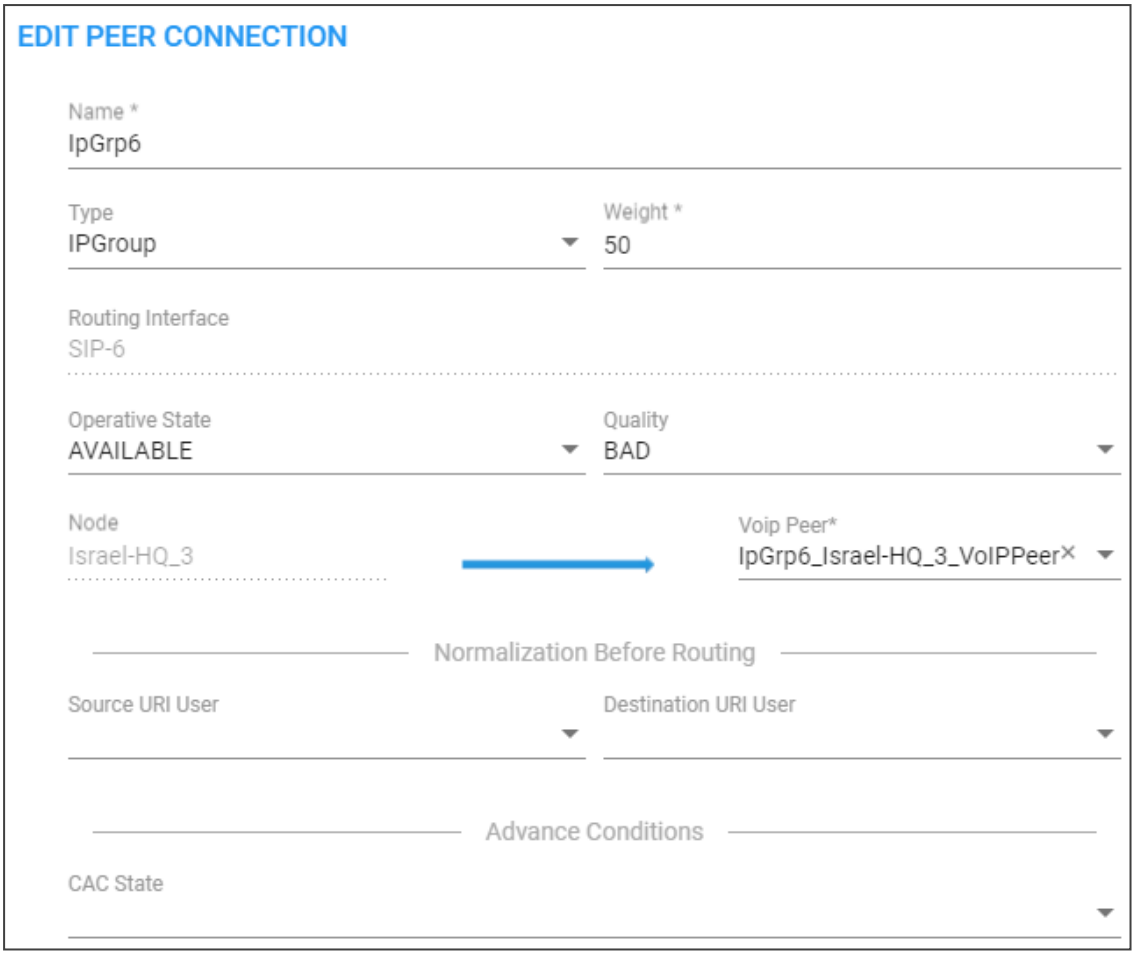
In the page, operators can create virtual nodes, Peer Connections, VoIP Peers, and Connections. Operators can import a full, currently-used topology, or part of one, e.g., a specific node, for making changes and testing offline.

Operators 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 page, they can be used in Routing Rules in testing mode; live network traffic is not 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, Quality and CAC State per Peer Connection.



After designing virtual VoIP network entities in the Offline page, 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 Page

In the ARM's Offline page (**Network** > **Offline**), network operators can:

- Add a virtual entity
- 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 page:

- Nodes
- VoIP Peers

➢ **To add a virtual node:**

1. In the Offline 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.

Icon	Used to
	Drag and drop a *SIP Trunk* onto the Offline Planning page.
	Drag and drop an *IP phone* onto the Offline Planning page.

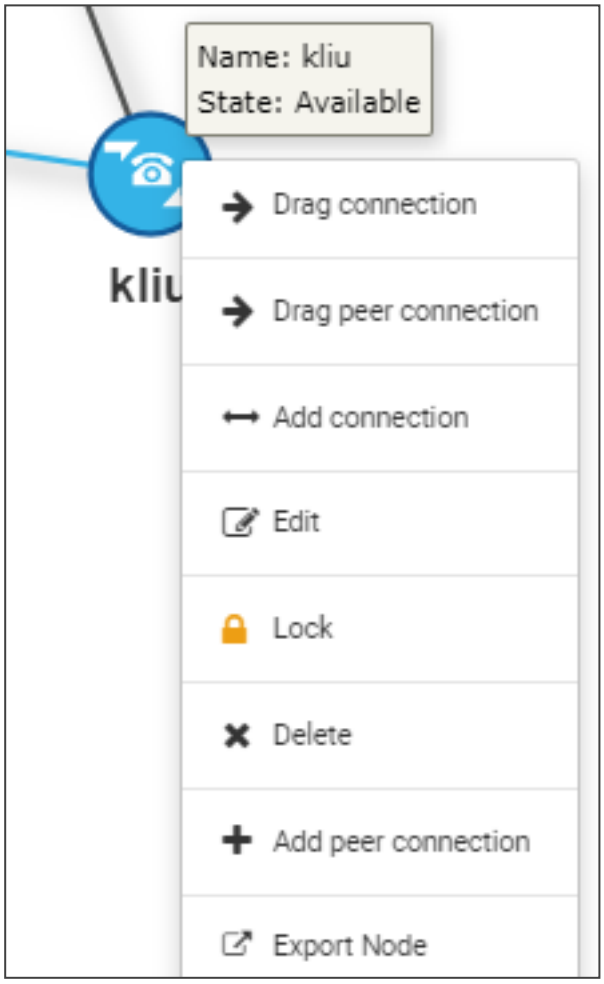
2. Drag the icon to the map and configure the name of the VoIP Peer.

Adding a Virtual Peer Connection to the Offline Page

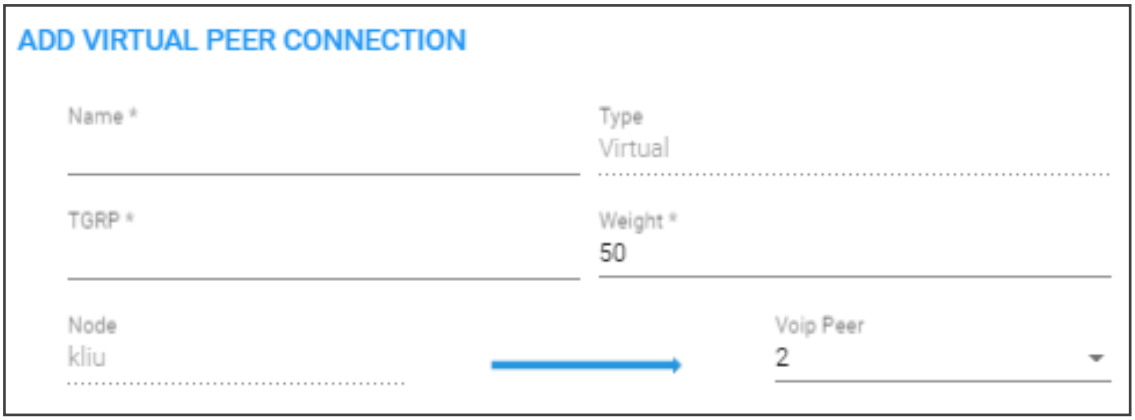
Network operators can add a virtual Peer Connection or a Peer Connection to the Offline page.

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

1. In the Offline page (**Network** > **Offline**), right-click the node from which to add a Virtual Peer Connection and then from the popup menu, select the **Drag peer connection** option.



2. Drag a line from the inside of the node to the VoIP Peer to which to connect.



3. Configure the connection. See also Adding a VoIP Peer on page 85 for more information.

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

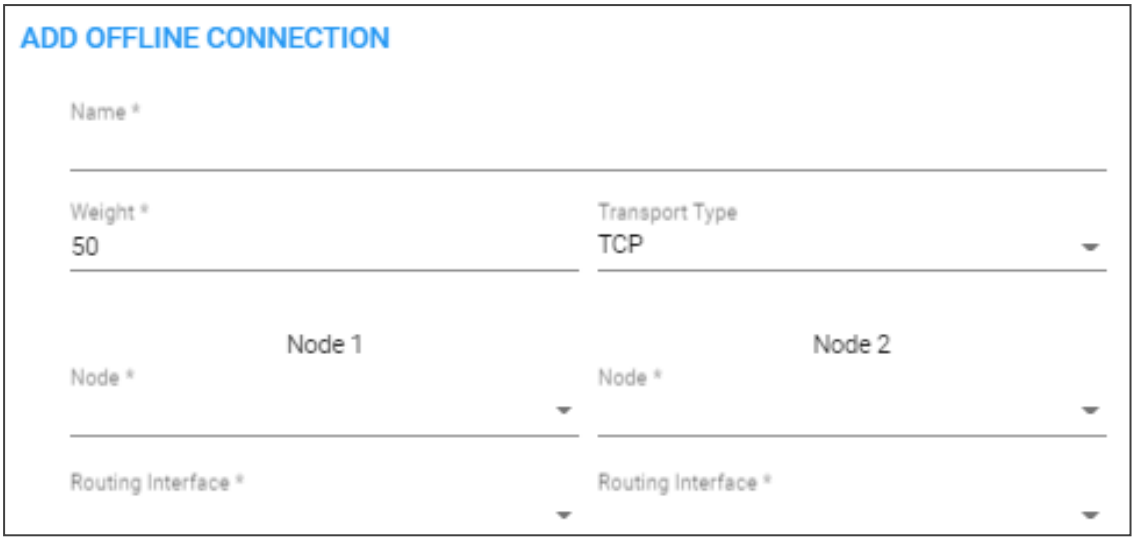
Adding a Virtual Connection

A virtual connection between two offline nodes can be added in the Offline page.

➢ **To add a virtual connection in the Offline page:**

1. Click the **Actions** drop-down and then select **Add connection**.

2. View the same screen as the 'Add Connection' screen shown in the live topology.



3. Perform the same procedure as when in the live topology (see Adding Connections on page 93).

Importing a Full Topology

The network operator can import a full topology from the live topology map to the Offline page.

➢ **To import a full topology:**

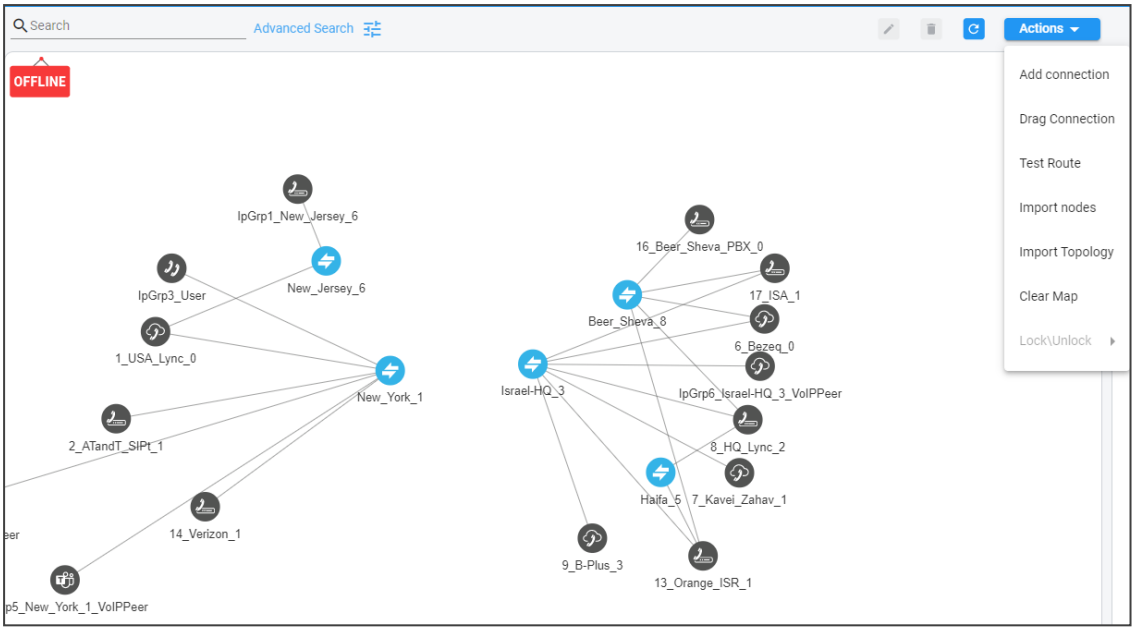
- In the Offline page, select from the **Actions** drop-down the **Import Topology** option; all network entities in the live topology including nodes, VoIP Peers, Peer Connections and Connections are imported.

Importing a Node from the Live Topology

A node (SBC / Media Gateway) can be imported from the live topology to the Offline page.

➢ **To import a node from the live topology to the Offline page:**

1. Click the **Actions** drop-down button and select the **Import nodes** option.



2. From the list that pops up, select the node to import; the node will be added to the Offline page together with Peer Connections and VoIP Peers associated with that node.

Deleting a Virtual Entity

A virtual entity can be deleted from the Offline page as part of the process of planning and designing the topology.

➢ **To delete a virtual entity from the Offline page:**

- In the Offline page, select the entity to delete and then click the delete icon .
- From the **Actions** drop-down, select the **Clear Map** option to delete all entities from the page.

Testing a Route

Network operators can test a route in the Offline 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 96). Testing a route in the Offline page factors in all entities configured in the Offline page and their status and voice quality.

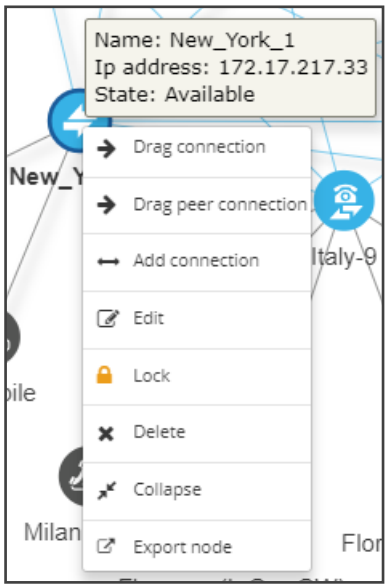
Exporting a Node from the Offline Page to the Live Topology

A node can be added to the Offline page and then exported from there 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 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 page, right-click the node and from the popup, select **Export node**.

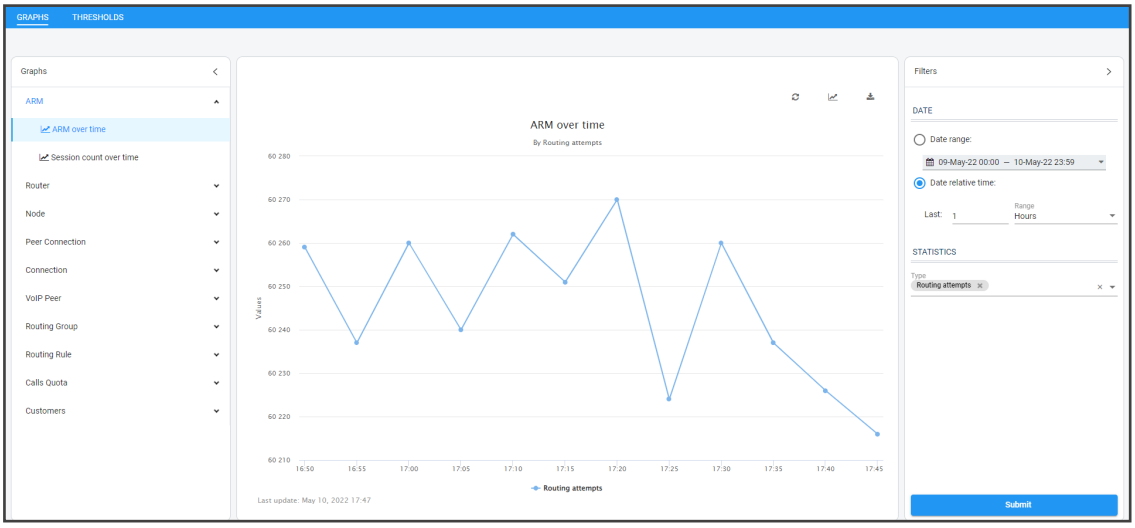


5 Viewing Statistics and Reports

The ARM provides a Statistics Graphs page and ARM-embedded statistics reports, allowing operators to debug, monitor and optimize their 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**).



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* and are collected at an interval of every five minutes. Select either: ■ ARM (ARM over time, Session count over time) ■ Router (Routers over time, Top routers, Top routers over time) ■ Node (Nodes over time, Top nodes, Top nodes over time, Nodes by peer connections, Top nodes by peer connections) ■ Peer Connection (Peer connections over time, Top peer connections, Top	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	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
peer connections over time, Peer connection sessions over time)** ■ Connection (Connections over time, Top connections, Top connections over time) ■ VoIP Peer (VoIP Peer sessions over time) ■ 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) ■ Calls Quota (Quota over time, Peer Connection over time, Resource group over time, Resource group by peer connection)*** ■ Customers (Customer sessions over time)****	attempts ✓ Unsuccessful routes ✓ Destinations Not Routable ✓ Destination calls ✓ 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	

Element	Filters	Graphical Representation
	✓ Routing third match ✓ Routing rules failures	

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

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

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

Unsuccessful routes: The call was dropped with some termination reason

Drop routing request: Discard action was triggered

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

Destination calls: Each time a call reached its destination

No match rules: No matching rule

Transient calls:

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

Registration routed: REGISTER call was routed

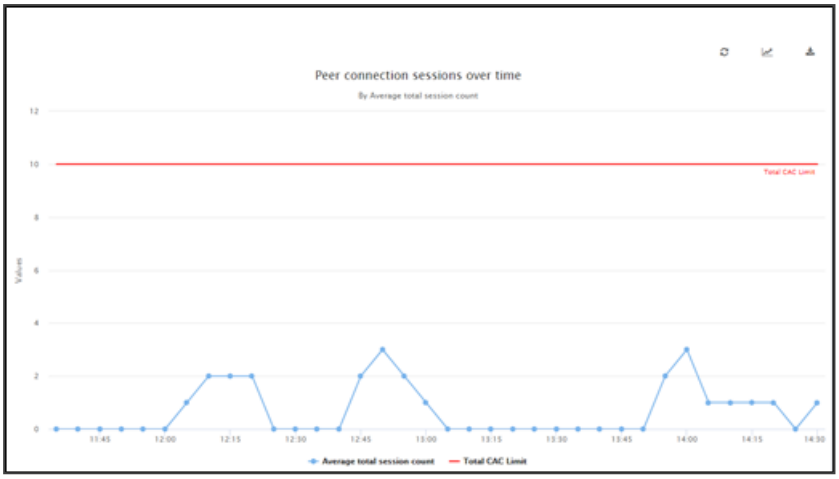
Registration unrouted: REGISTER call was not routed

Registration blocked: REGISTER call was discarded

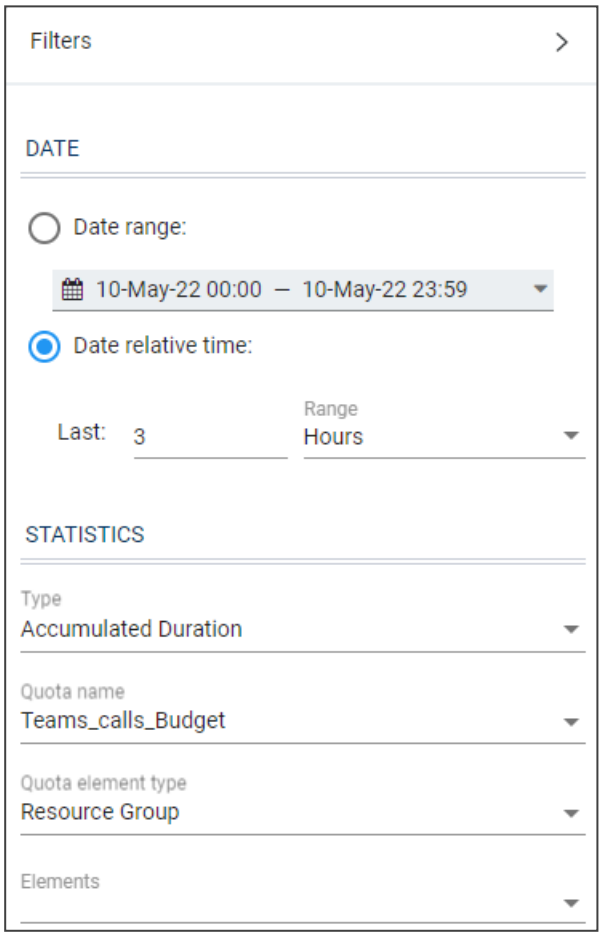
Average session count: The session count in a bucket of five minutes / 300 sec (average session count per second in a bucket of five minutes)

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

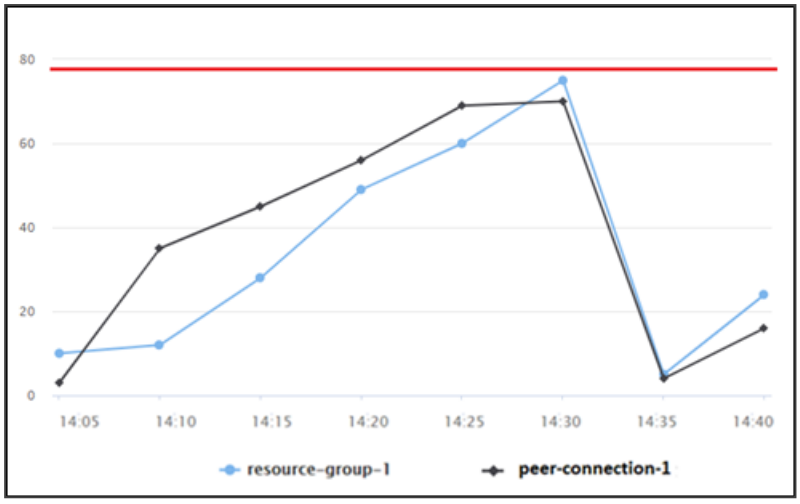
** If you select the 'Peer Connection' tab and then 'Peer Connection sessions over time', you'll view the screen shown in the following example. Notice the Total CAC Limit which is only present if a CAC was attached to the element.



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



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

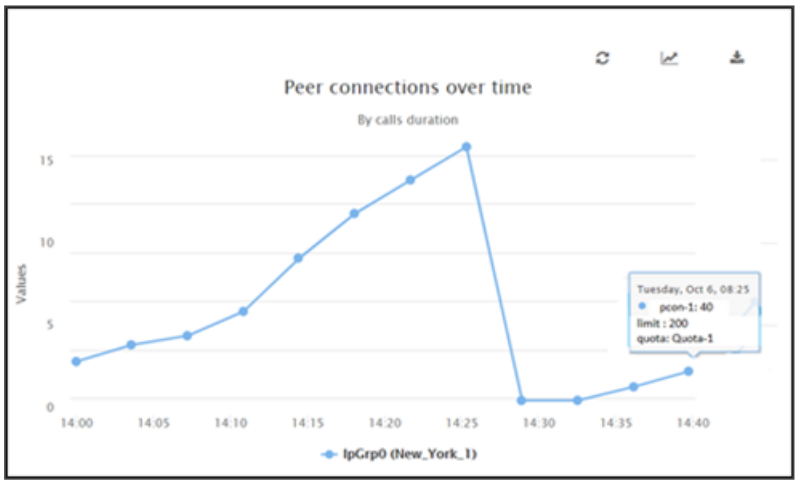


If a call starts before the quota is reached:

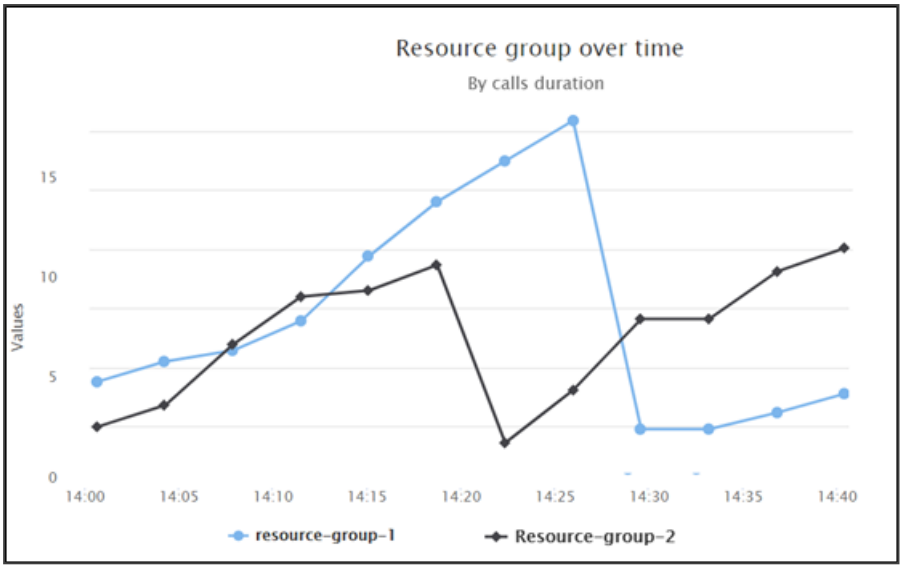
- the ARM will not drop the call
- the call will be calculated

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

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

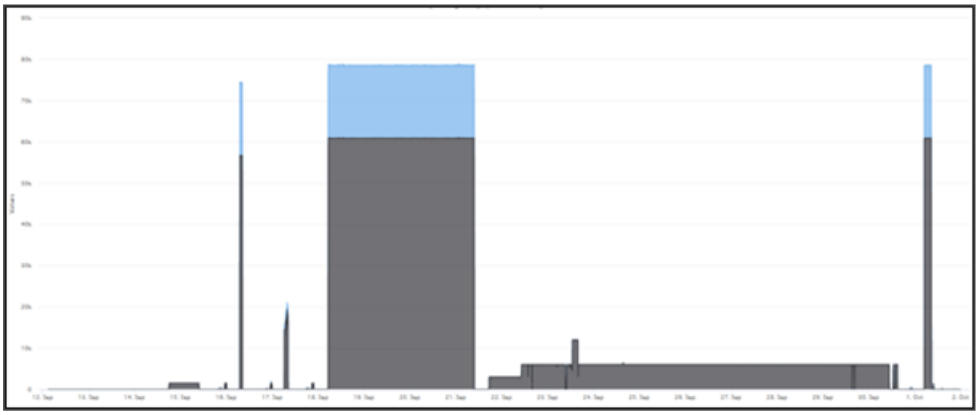


If you select the 'Quota' tab and then 'Resource group over time', you can then select a specific Resource Group (or multiple Resource Groups where each can have a different quota) and view the calls time (in minutes) over a timeline per Resource Group (the accumulated value for all Peer Connections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

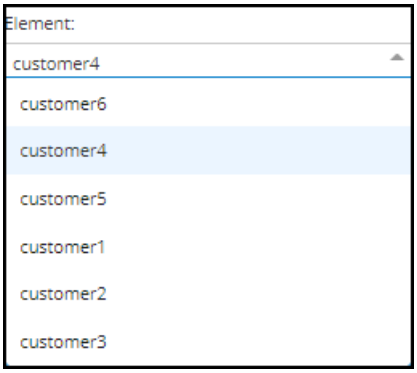


Only Resource Groups of type 'Peer Connection' can be selected. A tooltip displays for each graph the name of the quota associated with the Resource Group, and the limit (the number of minutes defined in the quota balance).

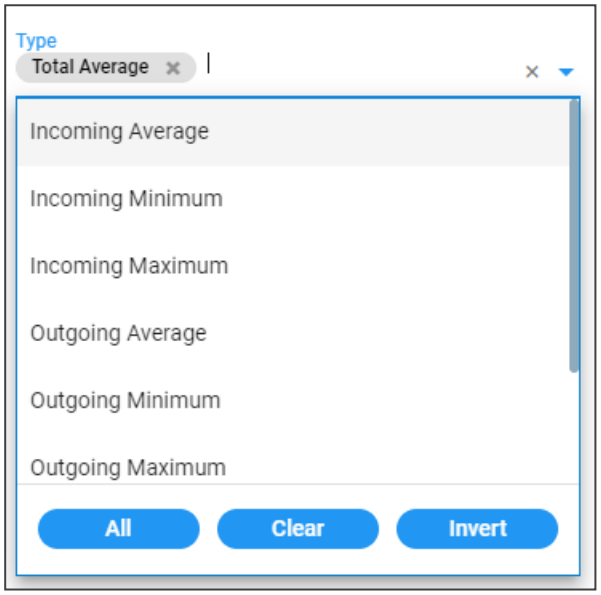
If you select the 'Quota' tab and then 'Resource group by peer connection', you'll view a stacked area (by default) showing consumption of calls minutes per Peer Connection in a specific Resource Group with an attached quota. You'll see, for example, that a quota allocated to a Resource Group connecting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



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



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



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

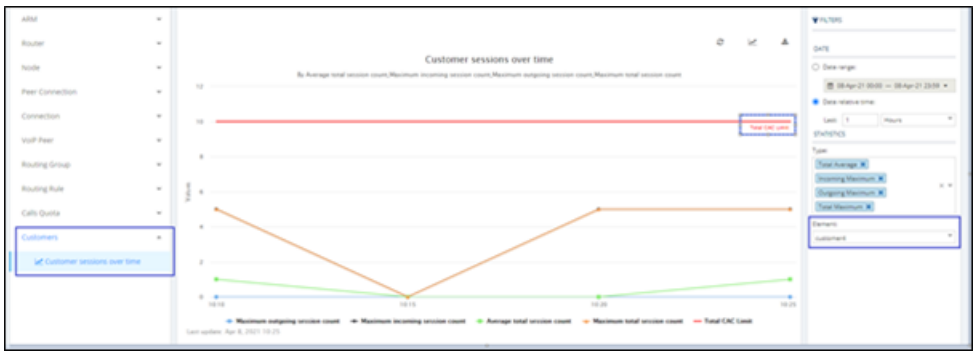
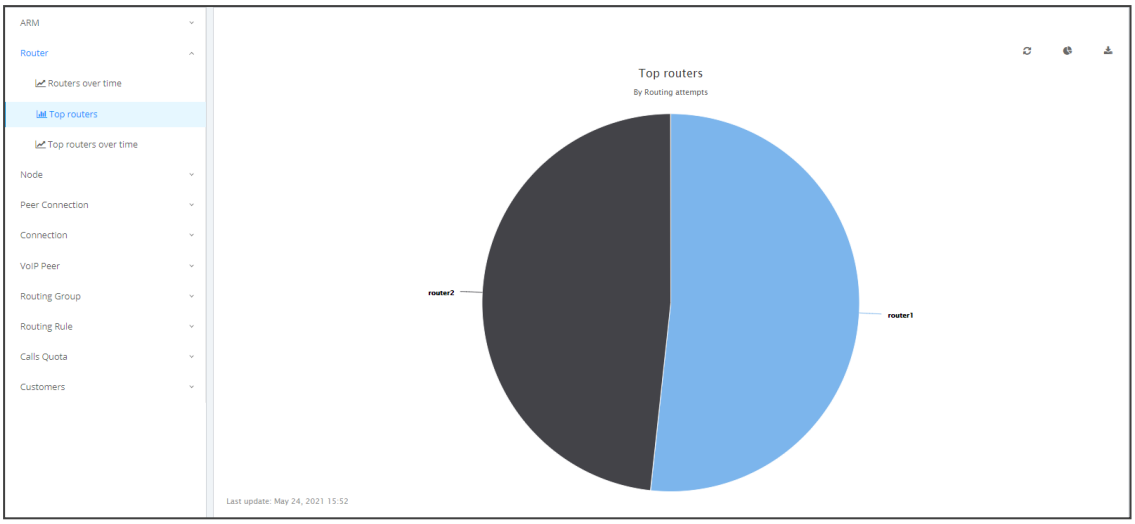
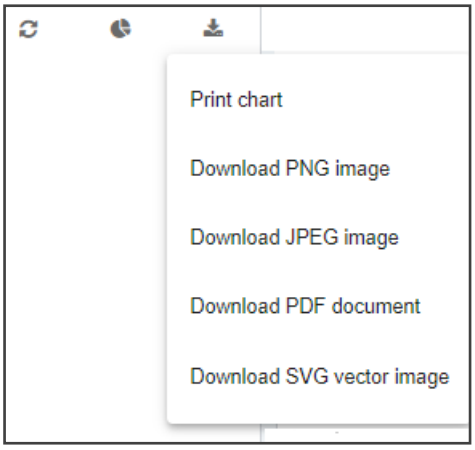


Figure 5-1: Top Routers filtered by Routing Attempts, displayed as a Pie Chart

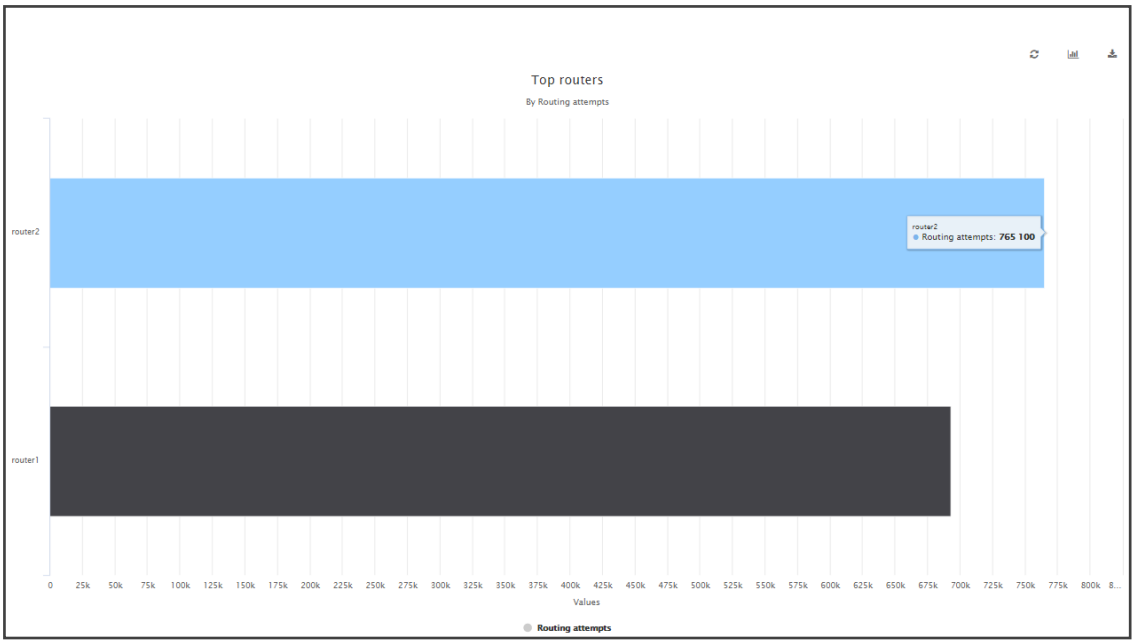


- A glance at the chart immediately reveals the top router. Point your cursor over a segment to display the number of routing attempts attempted by that router.
- You can print the chart or download the statistics in a format of your choice.

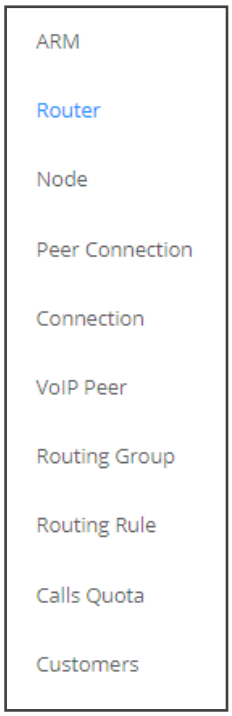


- You can select your preferred graphical representation – bar chart, column chart or pie chart. An icon 'Select chart type' allows you to present statistics according to your preferred graphical representation.

Figure 5-2: Top Routers filtered by Routing Attempts, displayed as a Bar Chart

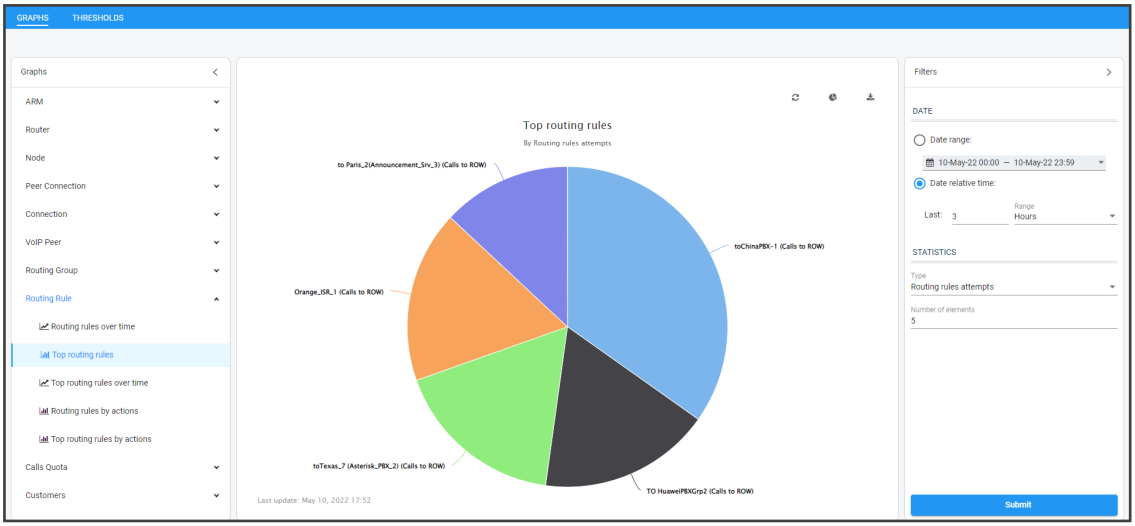


- A glance at this chart also immediately reveals the top router. Point the cursor over a bar to display the number of routing attempts attempted by that router. The following figure shows the elements that hold statistics information.



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

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



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

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

Configuring Statistics Thresholds Based Alarms

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

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

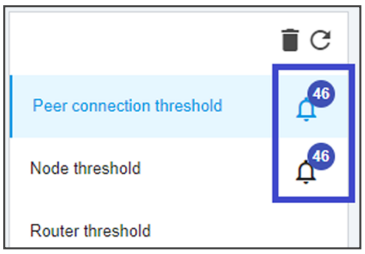
More than one alarm can be issued for the same threshold rule; an alarm is issued per element and statistic type.

The Statistics page displays a **Thresholds** tab (**Statistics** > **Thresholds**) under which thresholds are configured.

In the page's left pane:

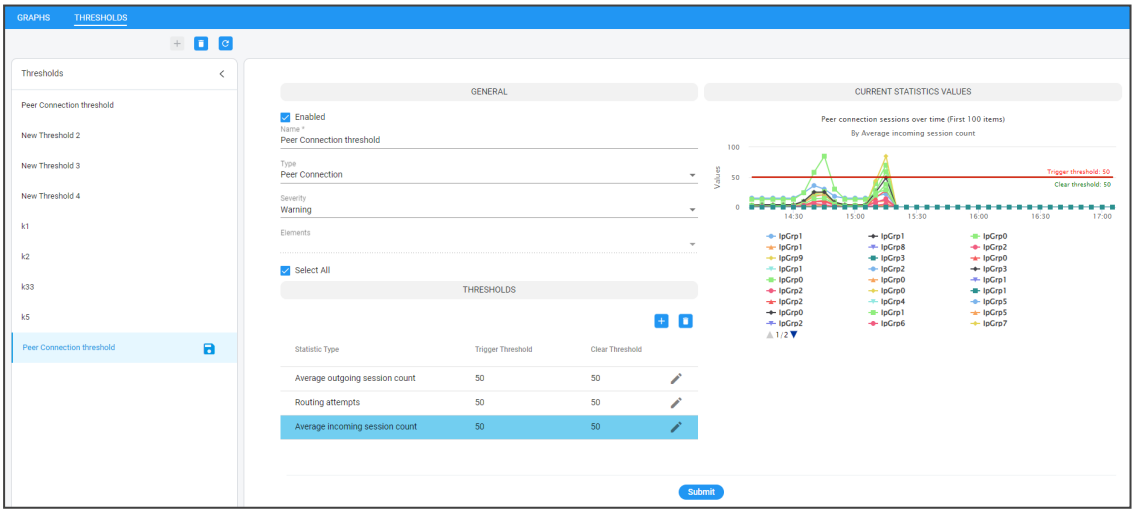
- add a new threshold by clicking the **+** icon (see also Adding a Statistics Threshold below)
- delete an existing threshold by selecting the relevant threshold rule and then clicking the trash icon (see also Deleting a Statistics Threshold on page 130)
- refresh all thresholds by clicking the refresh icon
- edit an existing threshold by clicking a specific threshold, editing it, and then clicking the **Submit** button (see also Editing a Statistics Threshold on page 129); if there are alarms related to the threshold, an icon displaying the alarms count is shown.

Figure 5-3: # of Alarms per Statistics Threshold



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

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

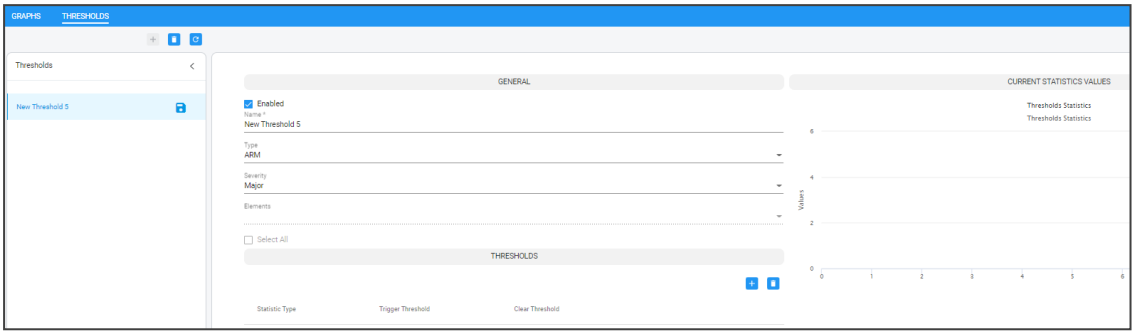


Adding a Statistics Threshold

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

➢ To add a new statistics threshold:

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

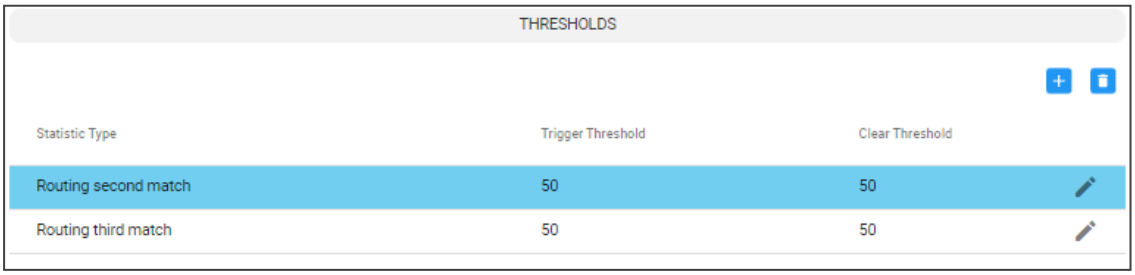


2. Click the **Submit** button to save the changes after defining the threshold.
3. Provide the following information:

   Under the 'General' section of the page:

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

Figure 5-4: Add | Edit Threshold



Under the 'Thresholds' section of the page shown in the preceding figure:

- Click the **+** icon to add a new entry with default values.
- To edit a new entry's default value, click the adjacent edit icon  .

For each threshold, provide the following information:

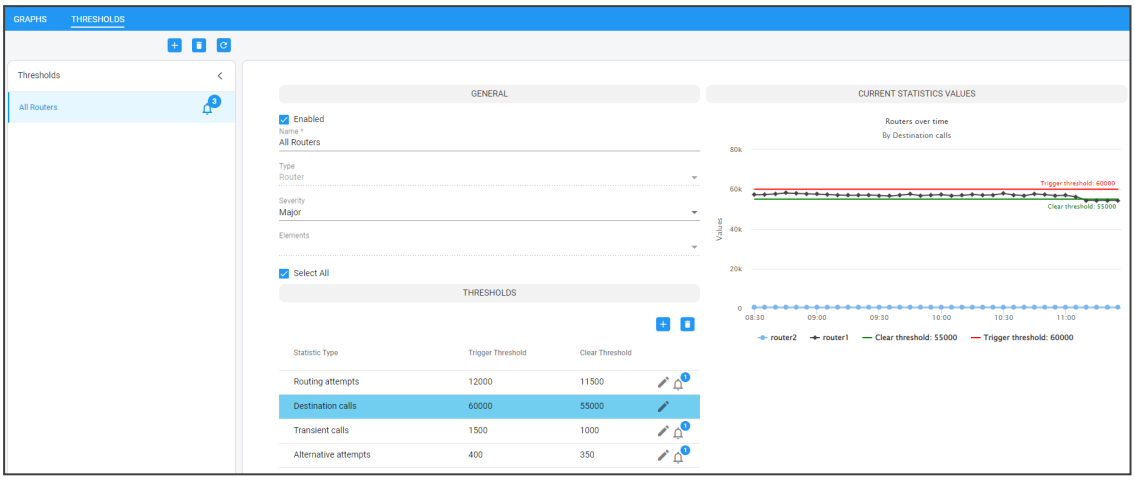
- **Statistic type**. The Statistics option depends on the element type selected above.
  - **ARM Statistics**. Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, transient calls, no match rules, maximum session count, average session count, registration routed, registration unrouted, registration blocked.
  - **Router Statistics**. Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, transient calls, no match rules, maximum session count, average session count, registration routed, registration unrouted, registration blocked.
  - **Node Statistics**. Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, transient calls, no match rules.
  - **Peer Connection Statistics**. Routing attempts, alternative attempts, unsuccessful routes, destination not routable, destination calls, drop routing requests, no match rules, maximum incoming session count, maximum outgoing session count, maximum total session count, average incoming session count, average outgoing session count, average total session count.
  - **Connection Statistics**. Transient calls.
  - **Routing Rule Statistics**. Routing rules attempts, routing rules failures, routing first match, routing second match, routing third match.
  - **Routing Group Statistics**. Routing rules attempts, routing rules failures, routing first match, routing second match, routing third match.
  - **Customer Statistics**. Maximum incoming session count, maximum outgoing session count, maximum total session count, average incoming session count, average outgoing session count, average total session count.
  - **VoIP Peer Statistics**. Maximum incoming session count, maximum outgoing session count, maximum total session count, average incoming session count, average outgoing session count, average total session count.
- **Trigger threshold**. Exceeding this value causes an alarm to be issued.
- **Clear threshold**. If the statistic value drops below this number, existing alarms will be cleared.

Viewing Statistics Thresholds Based Alarms

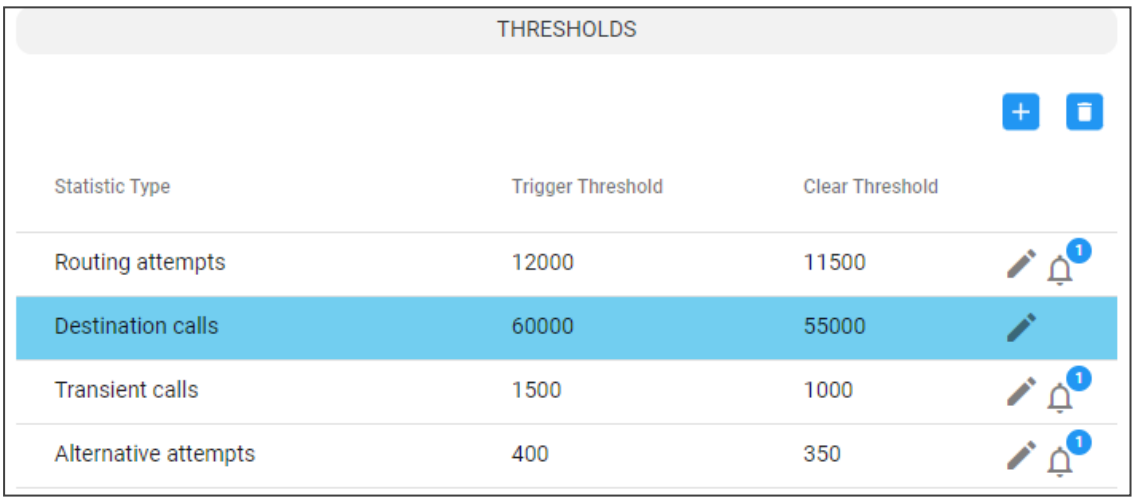
The instructions here show how to view statistics thresholds based alarms.

➢ **To view statistics thresholds based alarms:**

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



2. View in the 'Thresholds' section how many alarms exist for each statistics type.



In the example shown in the preceding figure, there's *one alarm* for 'Routing attempts', *one alarm* for 'Transient calls' and *one alarm* for 'Alternative attempts', and *no alarms* for 'Destination calls'.

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

Editing a Statistics Threshold

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

➢ **To edit a statistics threshold:**

■ Click the relevant statistics threshold, edit it, and then click **Submit**.

If during the edit

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

Deleting a Statistics Threshold

The trash icon  enables the network operator to delete a statistics threshold.

- The ARM prompts for confirmation before the delete action.
- Alarms related to the deleted threshold rule are cleared.

Accessing the ARM's Analytics API

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

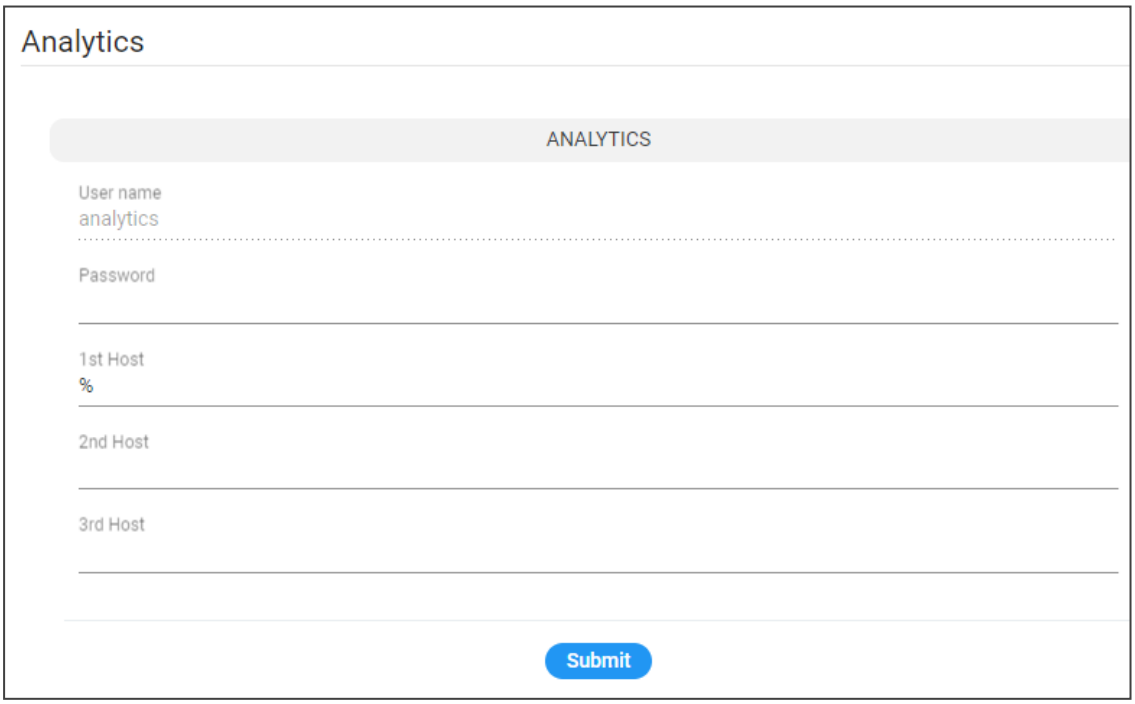
➢ **To access the ARM Analytics API:**

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

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

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

Figure 5-6: Analytics

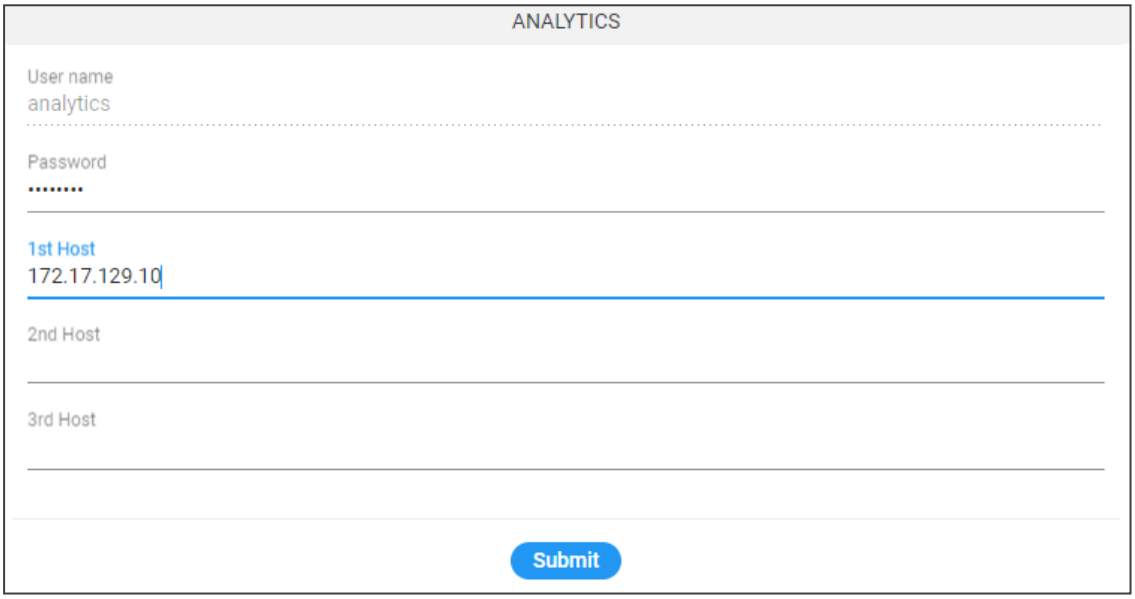


3. Make sure parameter 'User name' is set to **analytics** (read-only); access to data is allowed using this default user.

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

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

Figure 5-7: Analytics - Password and 1st Host



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

- **Nodes view**. Predefined view reflecting data from the APM nodes table with Nodes related essential information (such as ID, Serial Number, Name, Admin and Operative State, Software version, etc.)
- **Peer connection view**. Predefined view reflecting data from the Peer Connection table with information such as ID, Peer Connection Name, Admin state, related Node ID, etc.
- **Connection view**. Predefined view reflecting data from the Connection table with information such as Connection ID, Source and Destination Nodes ID and Operative State, etc.
- **VoIP Peer view**. Predefined view reflecting data from the VoIP Peers table with information such as ID, name and type.
- **Routing rules view**. Predefined view reflecting data from the Routing Rules table (ID, Name, Admin state and Routing Group reference).
- **Routing groups view**. Predefined view reflecting data from the Routing Group table (ID and Name of Routing Group)

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

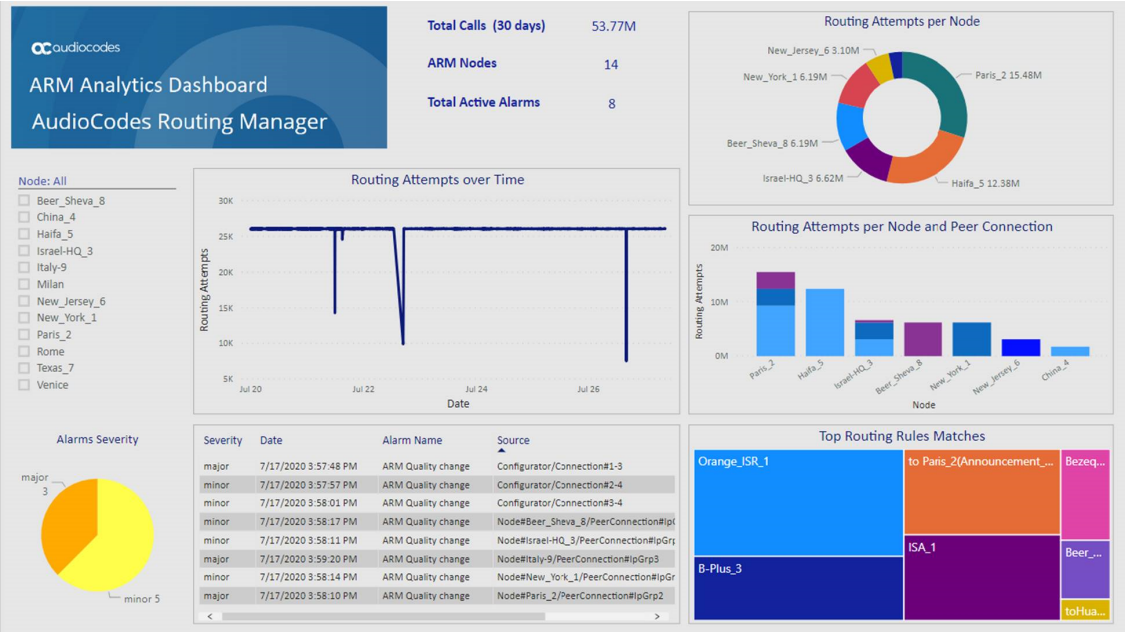
Examples of ARM Dashboard that can be Achieved using Analytics

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

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

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

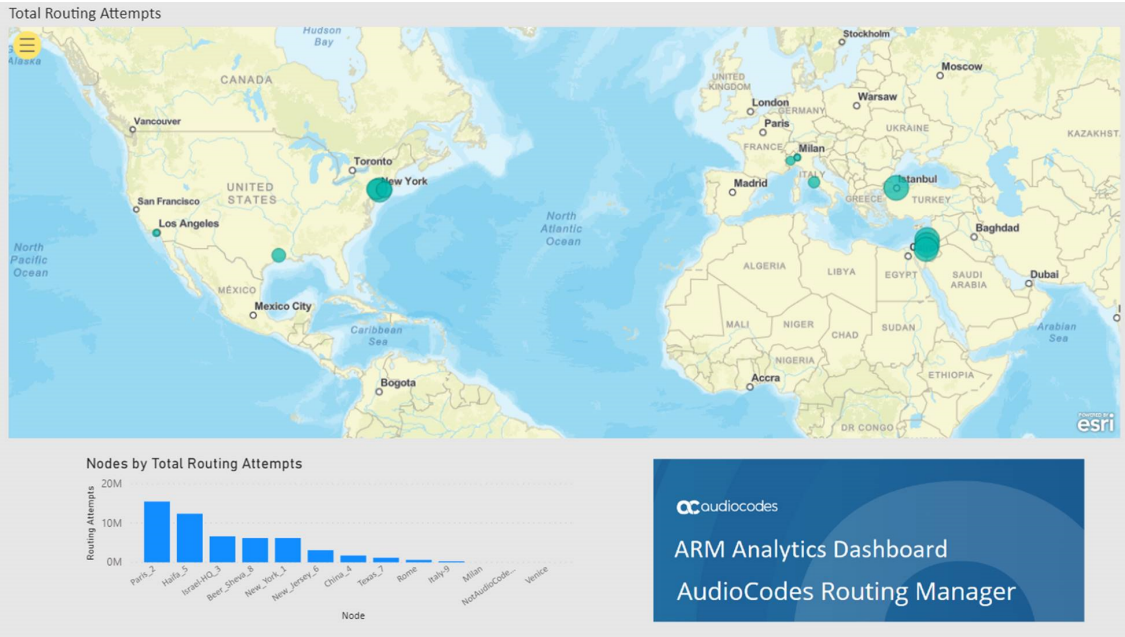
Figure 5-8: Dashboard Example 1



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

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

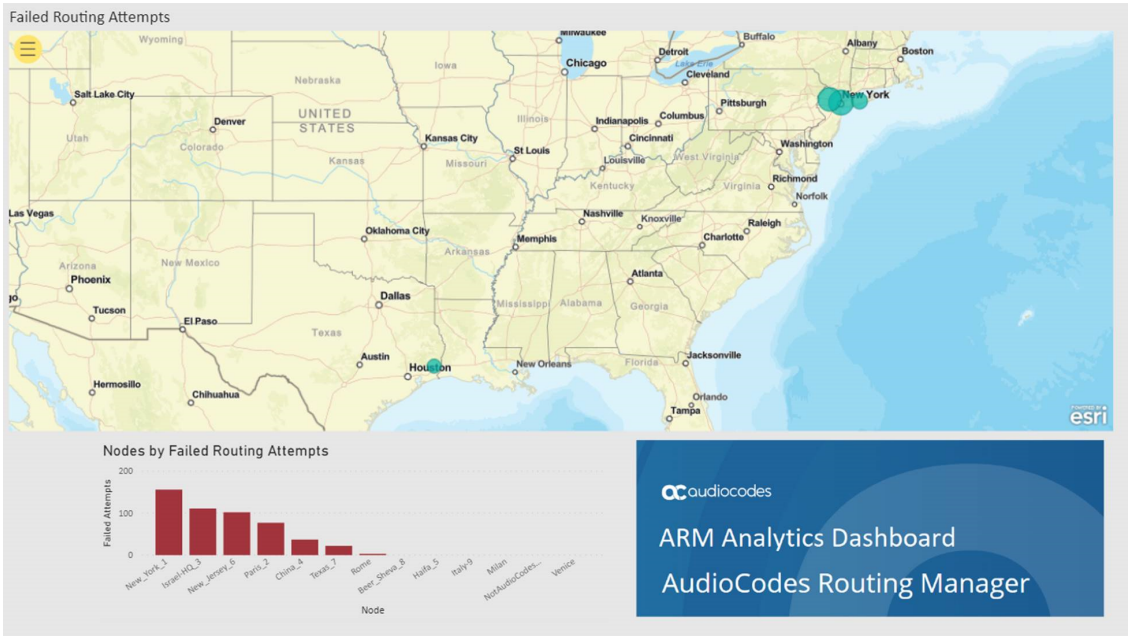
Figure 5-9: Dashboard Example 2



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

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

Figure 5-10: Dashboard Example 3



6 Performing User-Related Administration

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

- Add users to the ARM (see Adding a User Not Listed in an AD to the ARM on the next page)
- Incorporate users into the ARM from a File Repository (see Incorporating Users into the ARM from a File Repository on page 142)
- Add Users Groups to the ARM (see Adding Users Groups to the ARM on page 153)
- Determining the total number of users (see Determining Total Users Count on page 139
- Exporting ARM users to csv (see Exporting ARM Users to CSV File on page 140)
- Add an LDAP Server to the ARM (see Adding LDAP Server to ARM on page 156)
- Add an Azure AD Server to the ARM (see Azure AD as a Source for Users in the ARM on page 166)
- Add a Property Dictionary to the ARM (see Adding a Property Dictionary to the ARM on page 172)

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

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

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

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

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

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

Adding a User Not Listed in an AD to the ARM

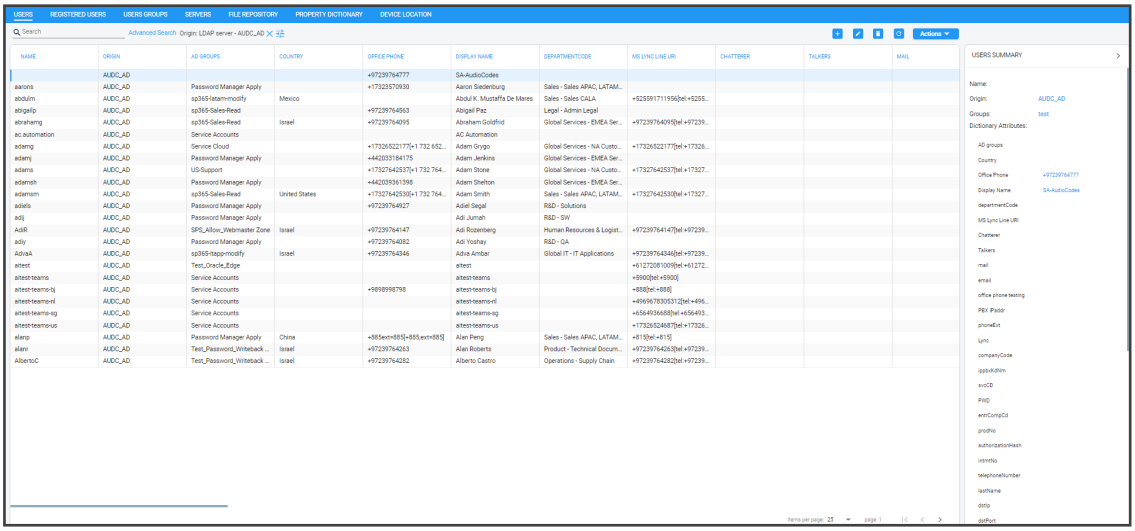
Enterprises have databases in which employee information is stored. Enterprises generally store information related to employees on Microsoft's Active Directory (AD) server. The ARM supports multiple ADs. The ARM's user administration feature can connect to an AD and import user calls routing related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

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

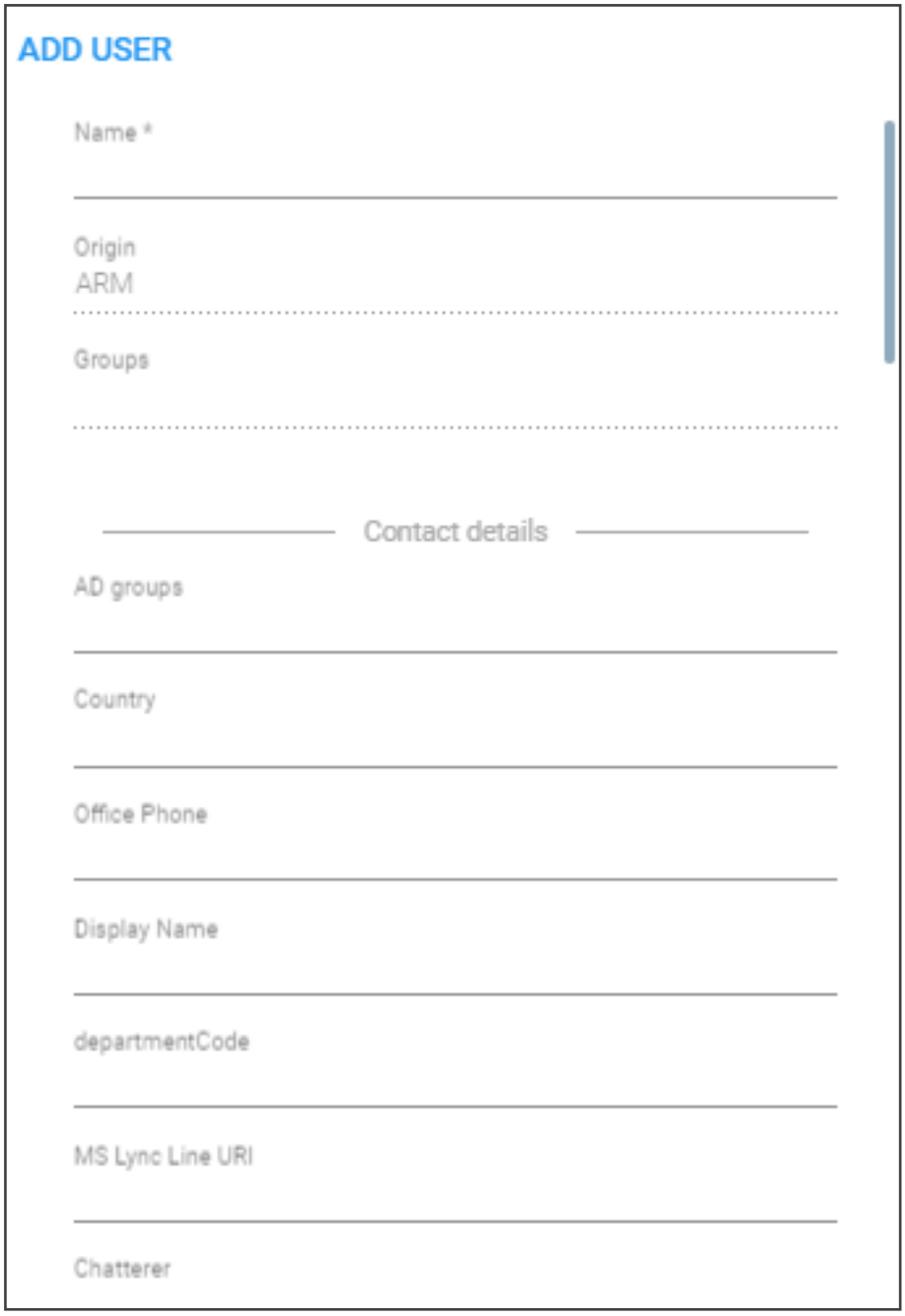
To view the users listed in the AD database and their AD attributes, you need to provision the LDAP server as shown under Adding LDAP Server to ARM on page 156.

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

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



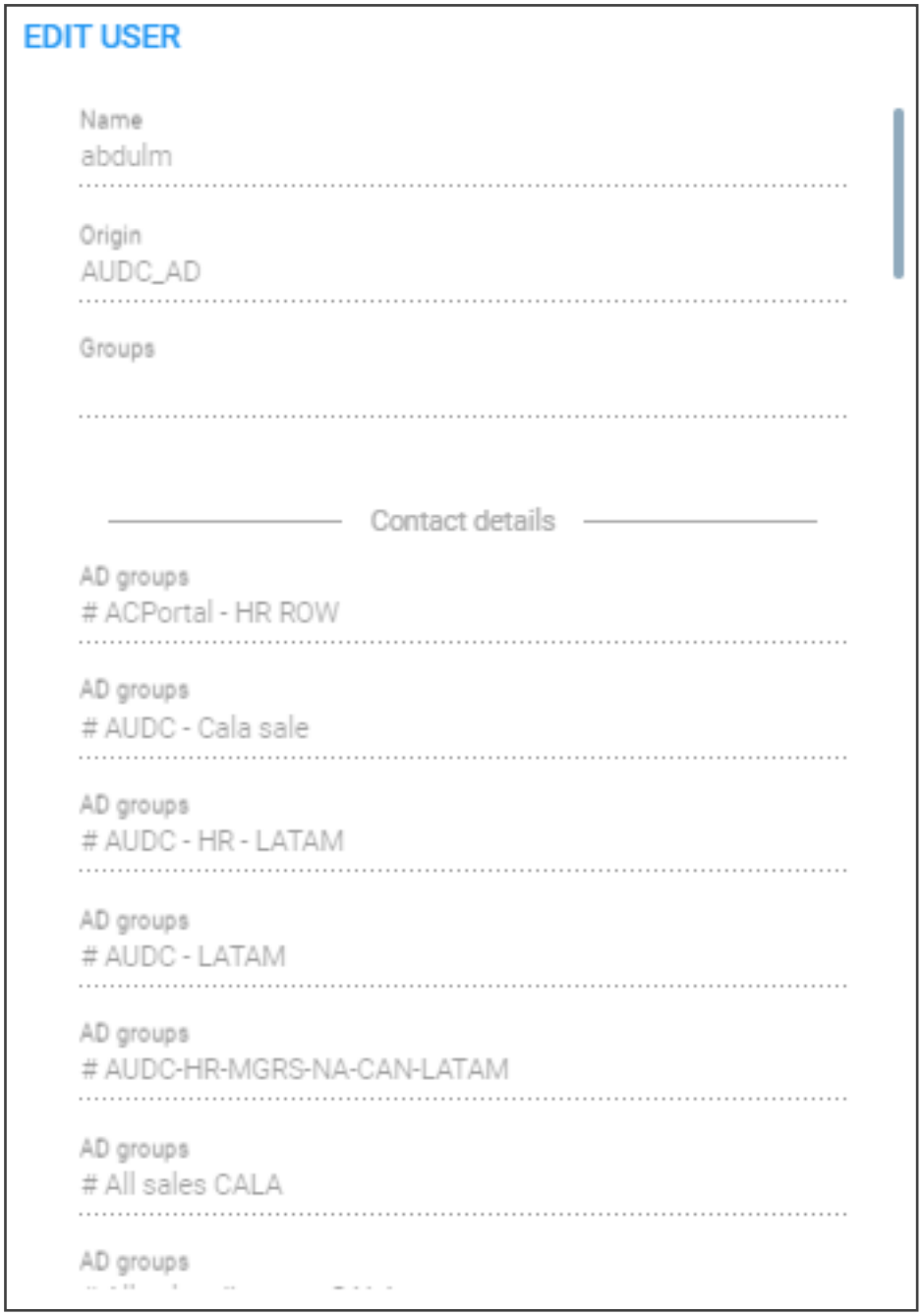
2. Click the **add** icon.



Contact 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 172.

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.

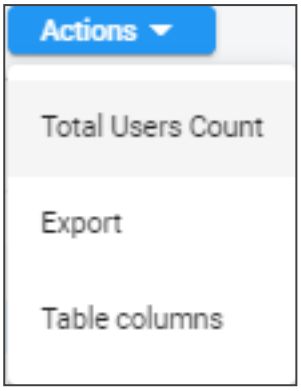
3. Click **OK**; the user is added and displayed in the Users page. To view and / or edit, select the user's row and click the **edit** icon.



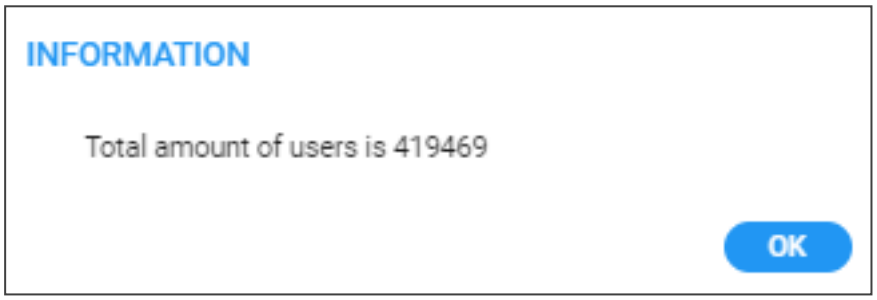
- Grayed fields indicate that the origin of this user isn't ARM and cannot be edited.
- Non-grayed fields indicate that the origin of the user is ARM and can be edited.

Determining Total Users Count

From the **Actions** drop-down in the Users page, network operators can select the **Total Users Count** option to display the overall number of users in the ARM.



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



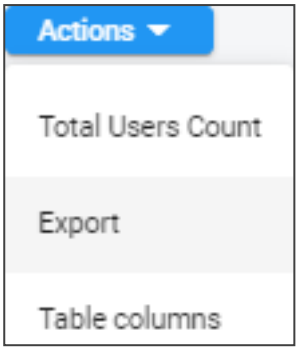
Exporting ARM Users to CSV File

The ARM provides network operators with the capability to export users to a Comma-Separated Values (CSV) file. The action is accessible in the Users page and in the Users Groups page, from the **Actions** drop-down. The operator can optionally:

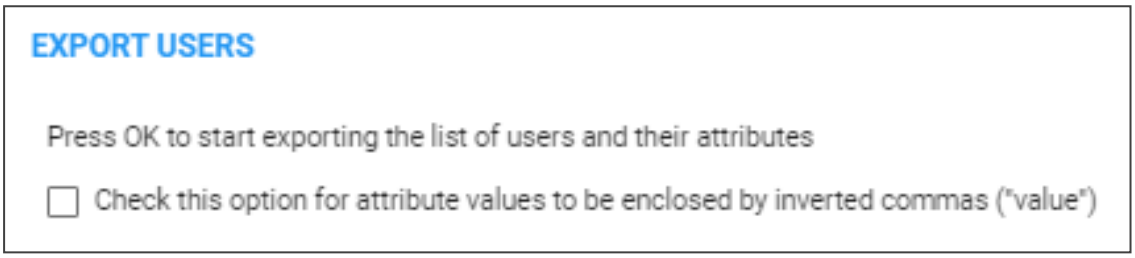
- export *all users* in the Users page (**Users** > **Users**) -OR-
- filter the Users page (**Users** > **Users**) using the 'Search' field and / or the **Advanced Search** link and then export *only those filtered users* -OR-
- export (users belonging to) a *Users Group* from the Users Groups page (**Users** > **Users Groups**)

➢ To export all users:

1. In the Users page, clear the 'Search' field, click the **Actions** drop-down and then select the **Export** option.



2. View the following prompt:



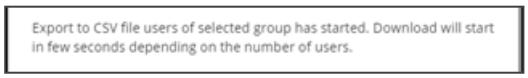
3. In the prompt, click **OK** and then view the CSV file in the lowermost left corner of the screen.

➢ To export filtered users:

1. In the Users page, filter users using the 'Search' field or 'Advanced Search' link, click the **Actions** drop-down and then select the **Export** option.
2. In the 'Export Users' prompt, click **OK** and then view the CSV file in the lowermost left corner of the screen.
3. Open the CSV file and view the subset of users filtered by name, Origin or text search filter.

➢ To export a Users Group:

1. In the Users Groups page (**Users** > **Users Groups**) select the group to export, click the **Actions** drop-down and select the **Export Users** option.
2. In the 'Export Users' prompt, click **OK**; export of users is performed in the background, as indicated by the following notification displayed:

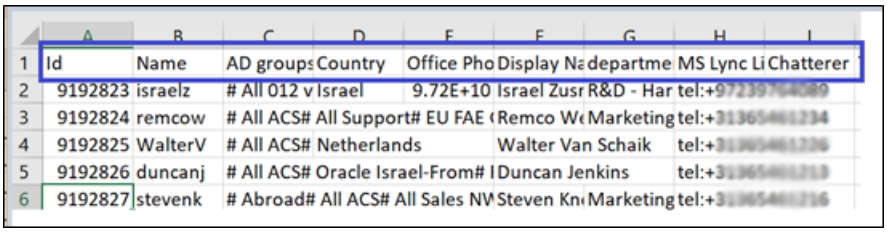


3. View the CSV file in the lowermost left corner of the screen.
4. Open the CSV file and view the users belonging to the group you exported.

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

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

Figure 6-1: CSV file



	A	B	C	D	E	F	G	H	I
1	Id	Name	AD groups	Country	Office Pho	Display Na	departme	MS Lync Li	Chatterer
2	9192823	israelz	# All 012 v	Israel	9.72E+10	Israel Zusr	R&D - Har	tel:+9723	
3	9192824	remcow	# All ACS#	All Support	# EU FAE (	Remco W(	Marketing	tel:+3136	
4	9192825	WalterV	# All ACS#	Netherlands		Walter Van Schaik		tel:+3136	
5	9192826	duncanj	# All ACS#	Oracle Israel-From	# I	Duncan Jenkins		tel:+3136	
6	9192827	stevenk	# Abroad#	All ACS# All Sales NV		Steven Kn(	Marketing	tel:+3136	

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

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

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

Incorporating Users into the ARM from a File Repository

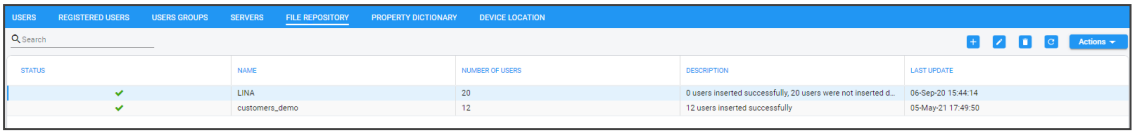
Operators can incorporate users into the ARM from a File Repository.

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

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

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

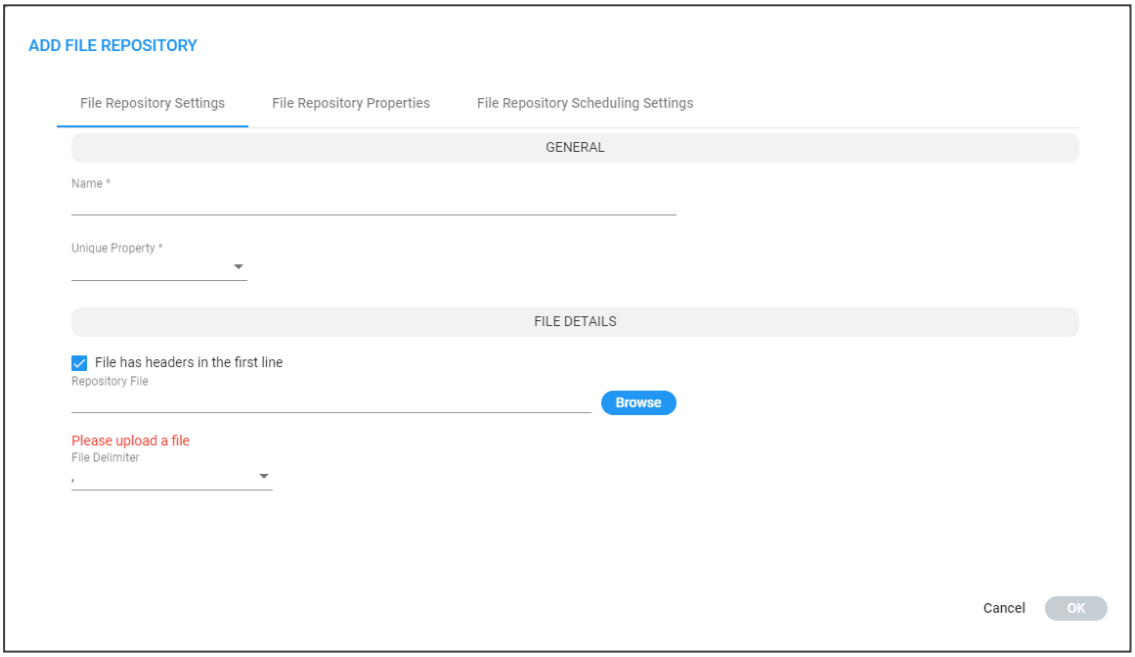
1. Open the File Repository page (**Users** > **File Repository**).



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

➢ To add a new File Repository:

1. In the File Repository page, click the add **+** icon.



2. Configure the File Repository Settings screen as follows:

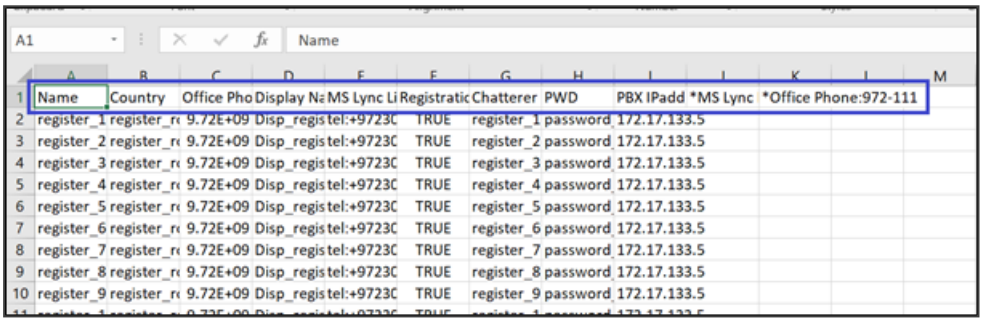
   - **Name**. Mandatory identification of the File Repository within the ARM.
   - **Unique Property**. One of the properties of the users dictionary defined in the ARM which can be treated as unique and can be seen as key for a user sourced by a specific Repository. Note that the ARM software validates this field uniqueness and will not allow duplicated entries. When adding a new File Repository, the operator is allowed to choose one of the user dictionary attributes to be treated as a unique property. Typically, the 'Name' setting is used.
   - **Field delimiter**. The delimiter used in the source CSV (can be ',', ';' or '|').
   - **File has headers in the first line**.

- If the CSV file has headers in the first line, check (select) this option. In this case, the first line will be taken so you can map the attributes by the column names as defined in the first line of the file.
- If the CSV file *does not have* headers in the first line, clear (deselect) this option. In this case, you can map the properties by the columns location - 'column 1', 'column 2'.

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

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

Figure 6-2: CSV file with defined headers in the first line

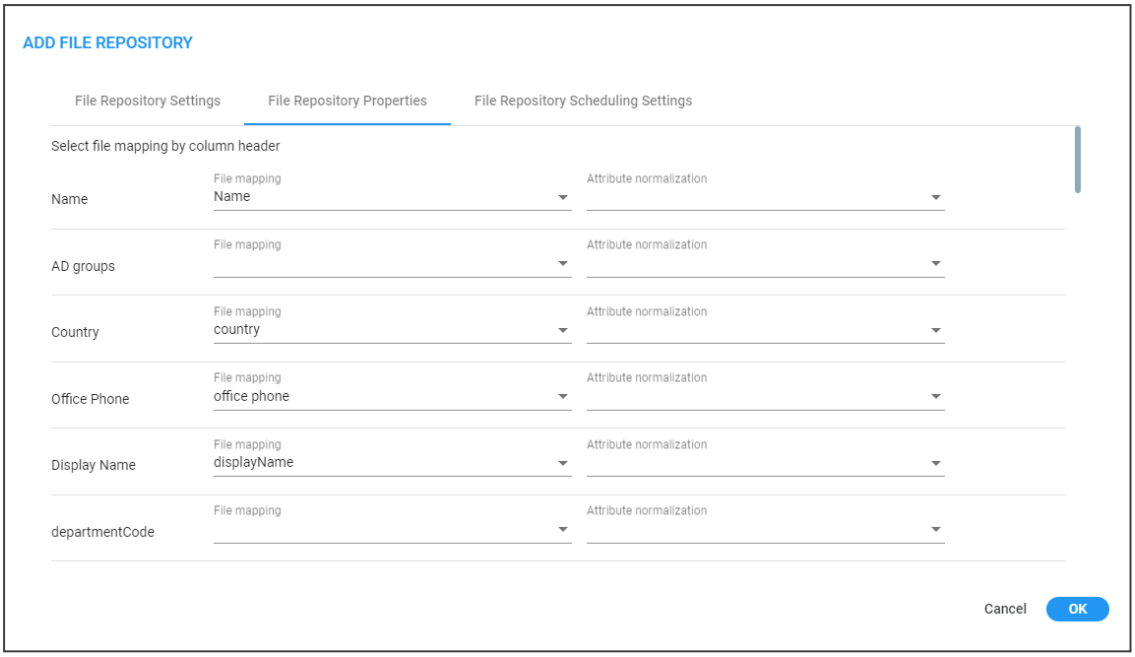


	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Country	Office Pho	Display Na	MS Lync Li	Registratic	Chatterer	PWD	PBX IPadd	*MS Lync	*Office Phone:972-111		
2	register_1	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_1	password	172.17.133.5				
3	register_2	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_2	password	172.17.133.5				
4	register_3	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_3	password	172.17.133.5				
5	register_4	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_4	password	172.17.133.5				
6	register_5	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_5	password	172.17.133.5				
7	register_6	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_6	password	172.17.133.5				
8	register_7	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_7	password	172.17.133.5				
9	register_8	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_8	password	172.17.133.5				
10	register_9	register_r	9.72E+09	Disp_regis	tel:+9723(	TRUE	register_9	password	172.17.133.5				

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

- The CSV file must not exceed 1 GB in size.
- Only upload files with UTF-8 encoding; uploading files which are not encoded in UTF-8 is possible but it is not advised as the mapping of the file might be faulty.

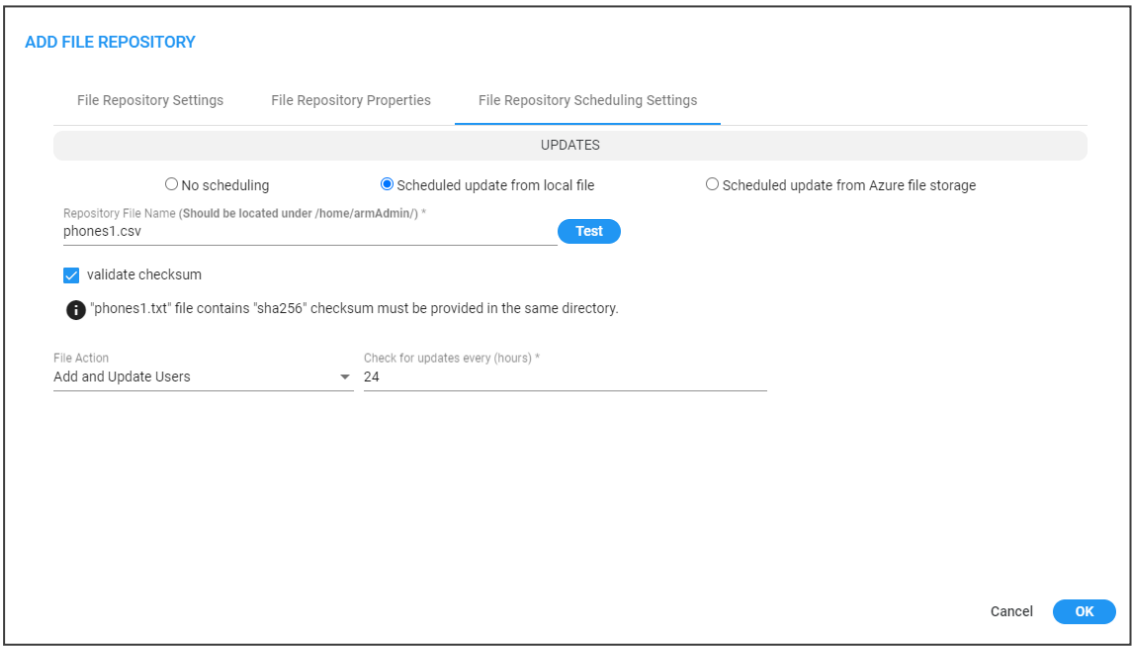
3. Configure the 'File Repository Properties' screen (similar to the parallel tab of LDAP Properties mapping) as follows:



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

4. Open the 'File Repository Scheduling Settings' tab (Default: **No scheduling**).

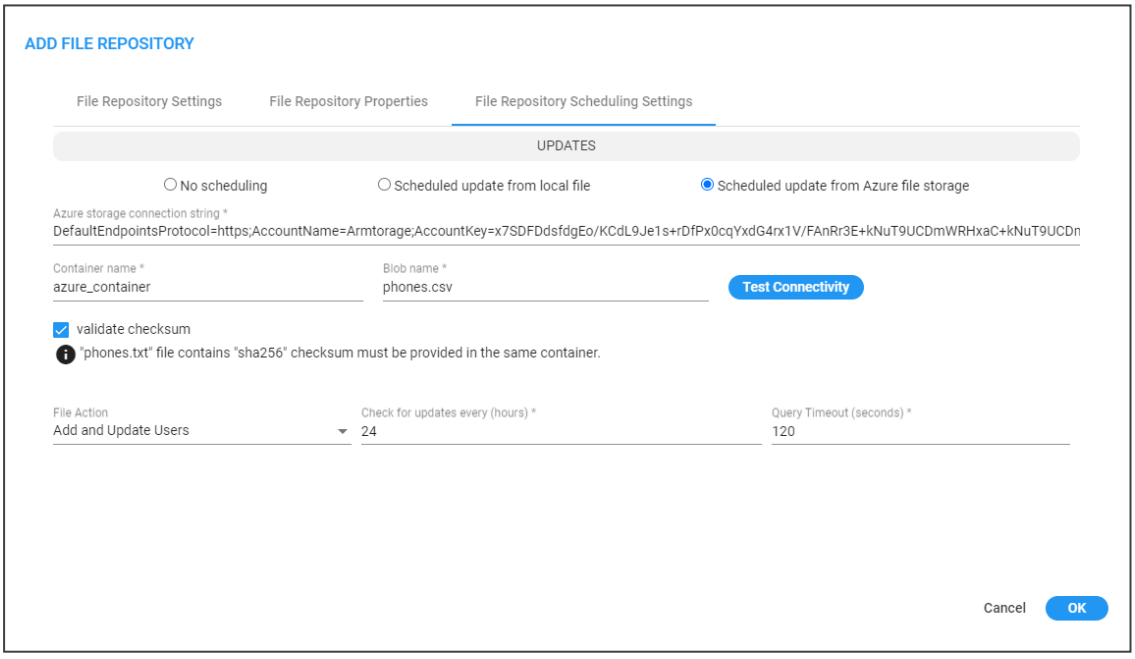
5. Select the **Scheduled update from local file** option. Use the figure below and the table below it as reference to configure an update schedule. The option enables scheduling synchronization for the selected File Repository.



Setting	Description
Repository File Name	■ The name must include file format .csv ■ The file must be located under the '/home/armAdmin/' directory (Configurator machine).
Validate checksum	If this option is selected, a .txt file with checksum must also be provided, in addition to the .csv file. See explanation If the 'Validate

Setting	Description
	checksum' option is selected, supply a .txt file with the same name of the Repository File that contains the 'sha256' checksum of the Repository File. For example, two files will be provided to ARM: on page 148.
File action	From the drop-down, select either: ■ **Add and Update Users** ■ **Delete Users** ■ **Full Sync All Users**
Update frequency (hours)	Configure 1 hour *minimum;* increments of 1 hour are supported.

6. Select the **Scheduled update from Azure file storage** option. Use the figure below and the table below it as reference to configuring an update schedule. The option enables scheduling synchronization for the selected File Repository.



Setting	Description
Azure Storage connection string	See Azure documentation for more information.
Container name	See Azure documentation for more information.
Blob name	The name must include file format .csv

Setting	Description
Validate checksum	If this option is selected, a .txt file with checksum must also be provided, in addition to the .csv file. See explanation If the 'Validate checksum' option is selected, supply a .txt file with the same name of the Repository File that contains the 'sha256' checksum of the Repository File. For example, two files will be provided to ARM: below.
File action	From the drop-down, select either: ■ **Add and Update Users** ■ **Delete Users** ■ **Full Sync All Users**
Update frequency (hours)	Configure 1 hour *minimum*; increments of 1 hour are supported.
Query Timeout (seconds)	Range: 1-6000 seconds

- If the 'Validate checksum' option is selected, supply a .txt file with the same name of the Repository File that contains the 'sha256' checksum of the Repository File. For example, two files will be provided to ARM:
  - Users.csv (Repository File)
  - Users.txt (contains sha256 of the 'Users.csv' file)

  After the sync is completed, the Repository File and the Checksum File (if one exists) are removed from the Azure storage/local machine.
- The synchronized file must include the same headers as the initial File Repository.

Limitations are the same as when manually uploading File Repository, namely:
- 1 GB max file size
- .csv file format
- Utf-8 encoding

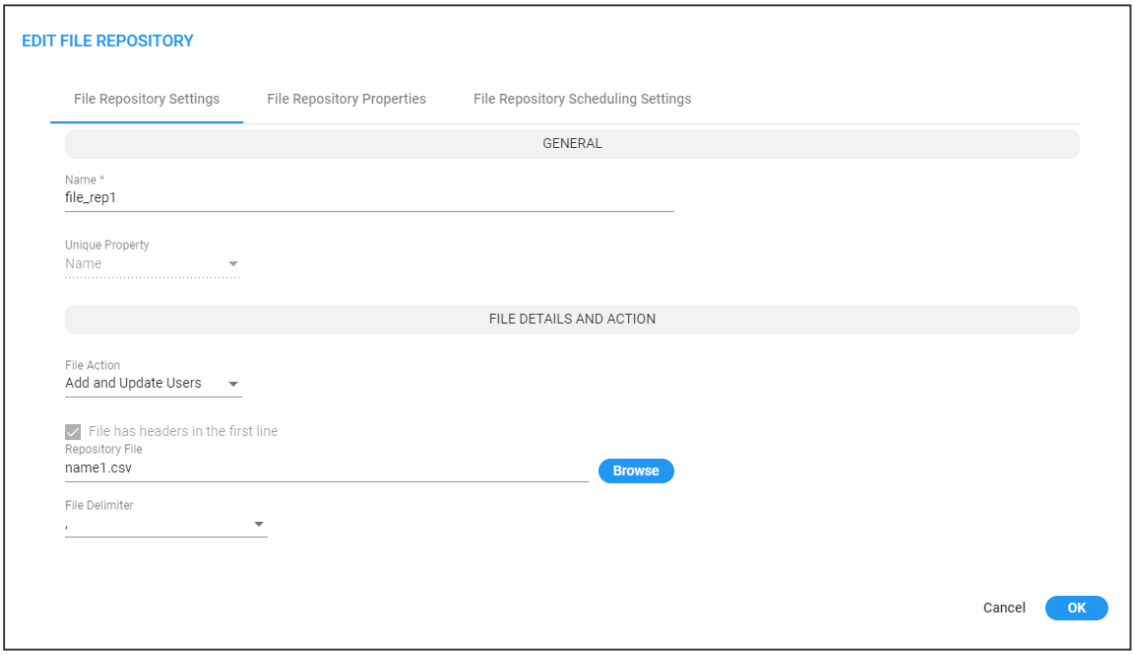
➢ To edit a File Repository:

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

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

Four actions are supported by edit a File Repository:

- Add and Update Users – adding new users and updating existing users.
- Delete Users – deleting existing users.
- Full Sync All Users - adding new users, updating existing users and deleting existing users that are not in the File Repository.
- File Repository Scheduling Settings - can be changed while editing the File Repository.



➢ To delete the File Repository:

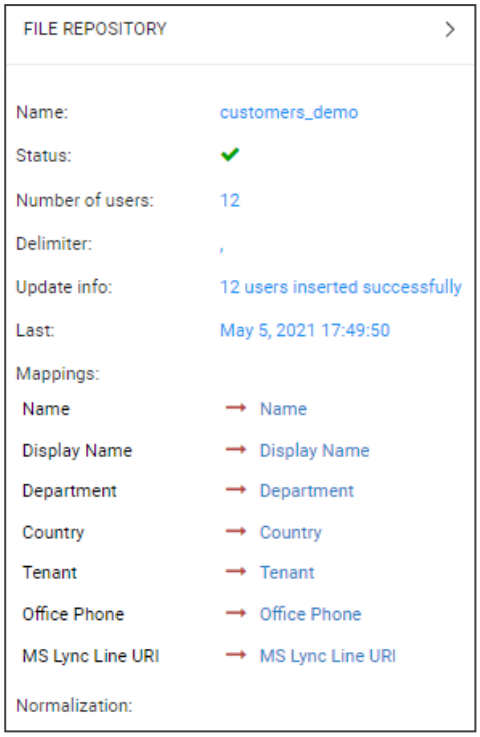
Deleting the File Repository causes all users related to it to be deleted. The ARM GUI displays a confirmation prompt indicating that all users related to this repository will be deleted.

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

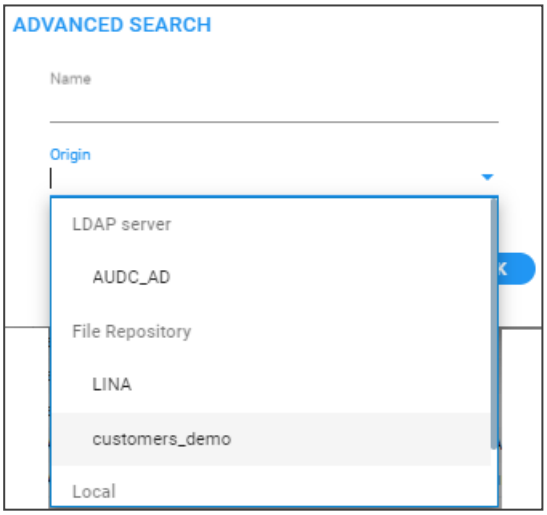
The File Repositories page displays the following information for each File Repository:

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

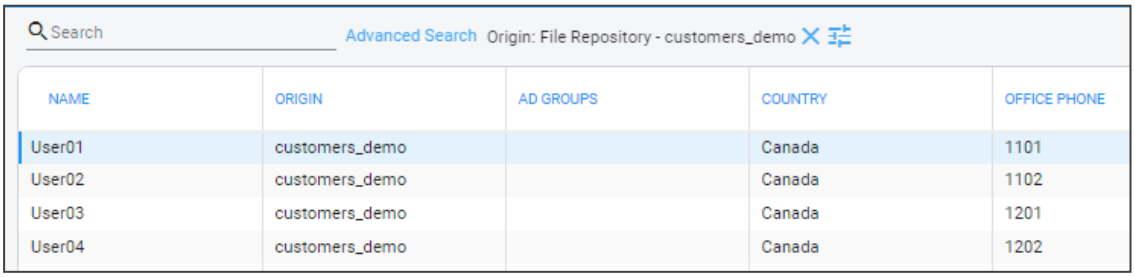
When a File Repository is selected in the File Repository page, the basic information summary for this repository is displayed on the right side of the page:

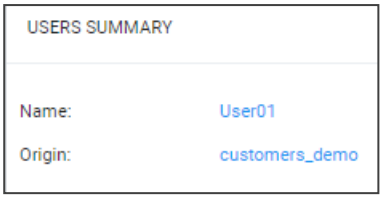


In the Users page (**Users** > **Users**), you can filter users sourced from a specific File Repository (in same way as with the LDAP). Click **Advanced Search**. and from the 'Origin' drop-down, navigate to and select the File Repository to filter by.



The indication of a specific File Repository as the source of the user information is displayed in the User's page in the 'Origin' column and in the Users Summary pane:



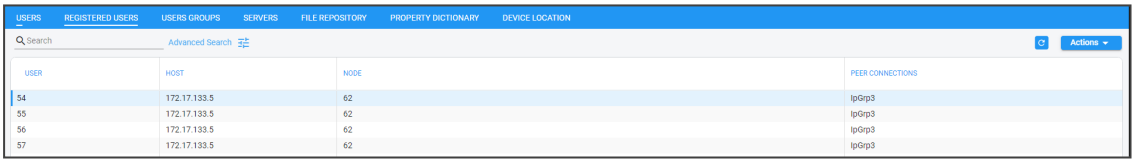


Viewing Registered Users in the ARM

The Registered Users page lets operators view the SBC registered users that were added to the ARM as shown in Adding Registered Users to the ARM on page 224. After SBC registered users are added to the ARM, the ARM will be capable of performing call routing based on SBC user registrations. When defining a Routing Rule, operators will be able to route calls to SBC registered users (see Adding a New Routing Rule on page 328). The destination to which to route the call will depend on where - which SBC - the user performed the registration. In the Routing Rule definition, operators will select the appropriate routing condition, namely, that the call destination is an SBC registered user.

➢ To view SBC registered users added to the ARM:

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



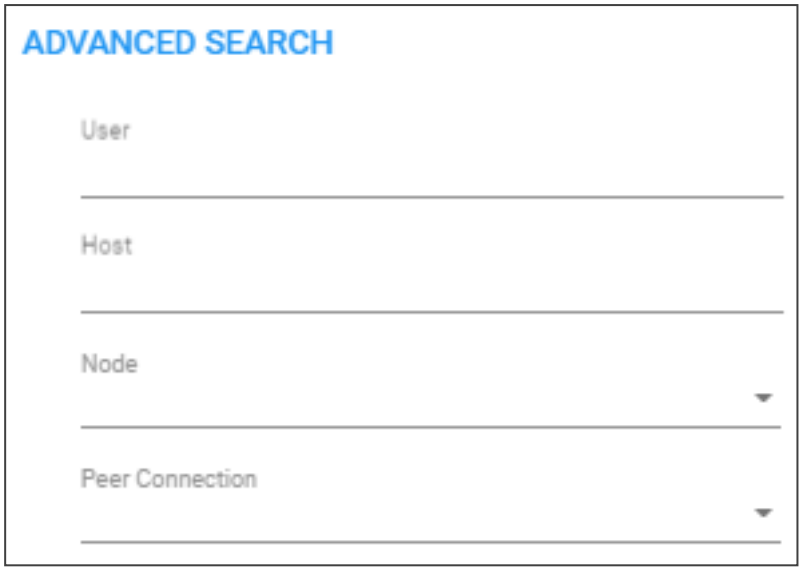
2. Click the refresh icon 

3. Use the following table as reference:

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

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

- In the Registered Users page, click the **Advanced Search** icon.



- From the 'Node' drop-down, select a specific node (SBC / Gateway) to view only registered users associated with that node.
- From the 'Peer Connection' drop-down, select a Peer Connection (IP Group) to view only registered users associated with that Peer Connection.

  The feature facilitates quick access to information by excluding unwanted information from the page.

Adding Users Groups to the ARM

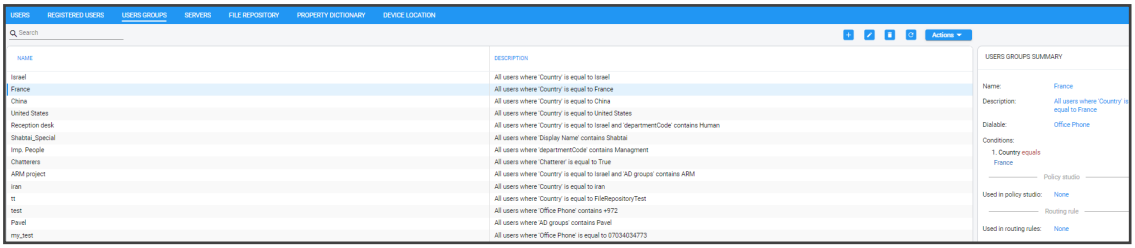
Network operators can define a Users Group by defining a set of criteria in the user properties. The ARM automatically associates users with the defined Users Group, based on the defined conditions. You can then use the Users Group in your Routing Rules as match conditions. Each Users Group has one 'Dialable 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.

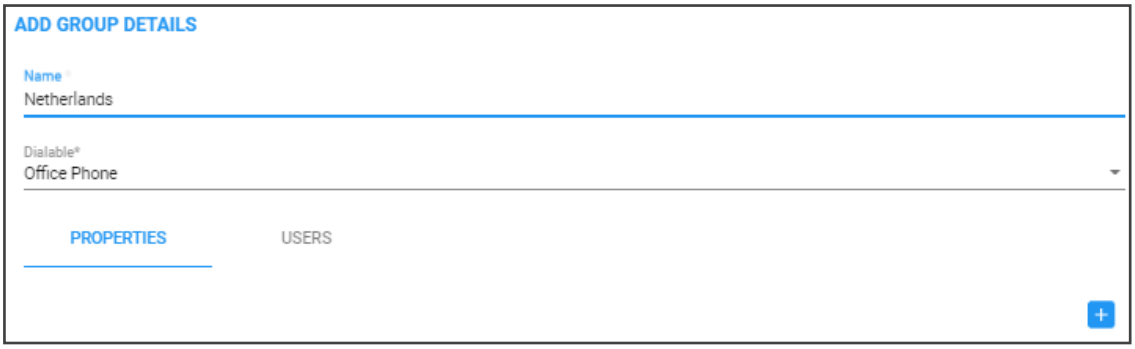
Example: A Users Group can be defined where the 'Dialable Number' attribute is **Mobile phone number** and the conditions are **Country** equals **Germany** and **Department** equals **Marketing** or **Sales**.

➢ **To add a Users Group:**

1. Open the Users Groups page (**Users** > **Users Groups**).

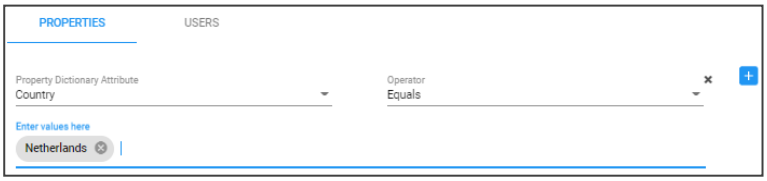


2. Click the add icon **+**.



3. Configure the group details using this table as reference.

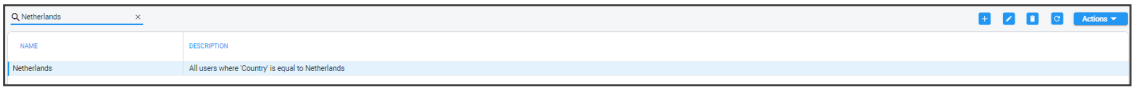
Table 6-1: User Group Details

Setting	Description
Name	Enter a name for the group for intuitive future reference.
Dialable	From the drop-down menu, select one of the Dialable Number properties. This is the user's property that is compared to the received source or destination URI to determine if the route request is from/to one of the users in this User Group. Example: **Office Phone**.
Property Dictionary Attribute	Under the **Properties** tab, click   From the drop-down, select a user attribute according to which the user will be associated with the group. Example: **Country**.
equals / not equals contains / not contains	From the 'Operator' drop-down, select the operation to be used to define the criterion.
Enter values here	Enter a value for the attribute, according to which the user will be associated with the group. Example: **Netherlands**. Press enter to add another value. At least one of the values must

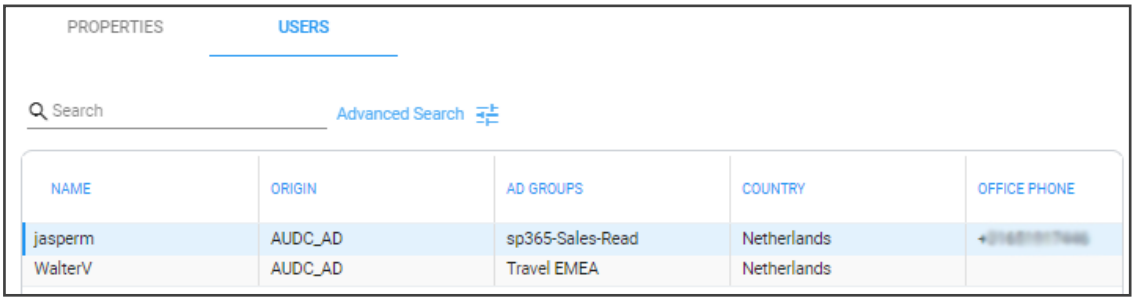
Setting	Description
	match for the attribute to be considered a match.

➢ To edit a Users Group:

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



2. Edit using the preceding table as reference and then click the **Users** tab.

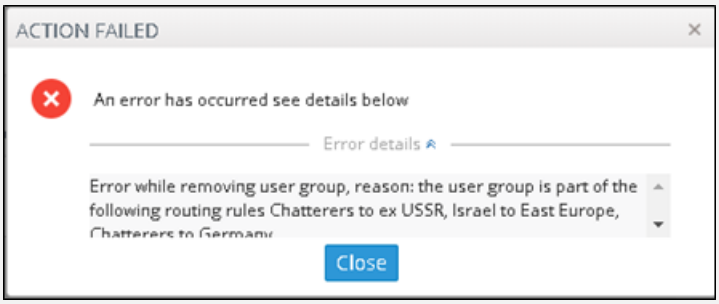


3. View the users who are associated with the group.

➢ To delete a Users Group:

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

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



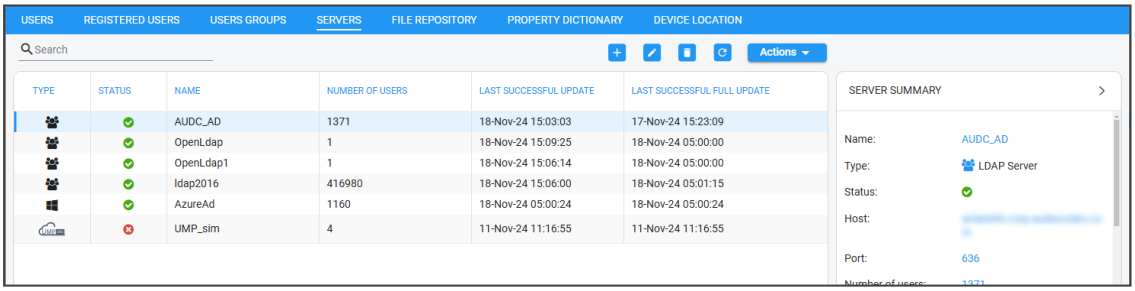
The message indicates the names of the routing rule/s associated with the group so it's easy to find and remove them before deleting the group.

Adding LDAP Server to ARM

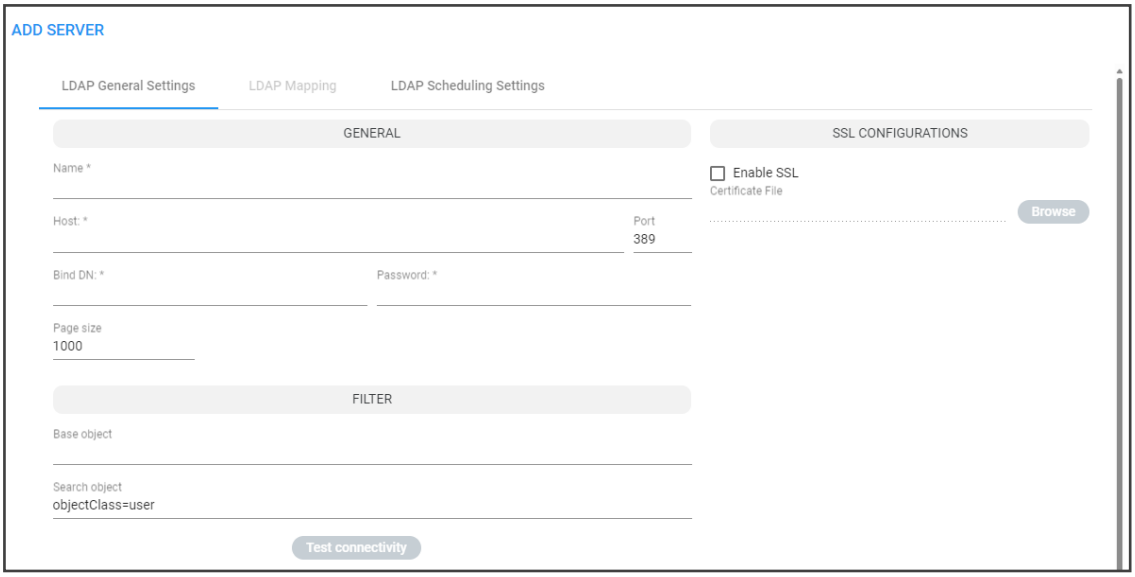
Multiple Active Directories (ADs) can be added to the ARM database using LDAP protocol, useful for consolidating information in the enterprise. All the different lists of users in the enterprise, for example, can be consolidated into one LDAP directory that can be queried by any LDAP-enabled application requiring the information.

➢ To add an LDAP server:

1. Open the Servers page (**Users** > **Servers**).



2. Click the add **+** icon, and then from the drop-down menu, select **LDAP server**.



3. Configure the LDAP General Settings using this table as reference.

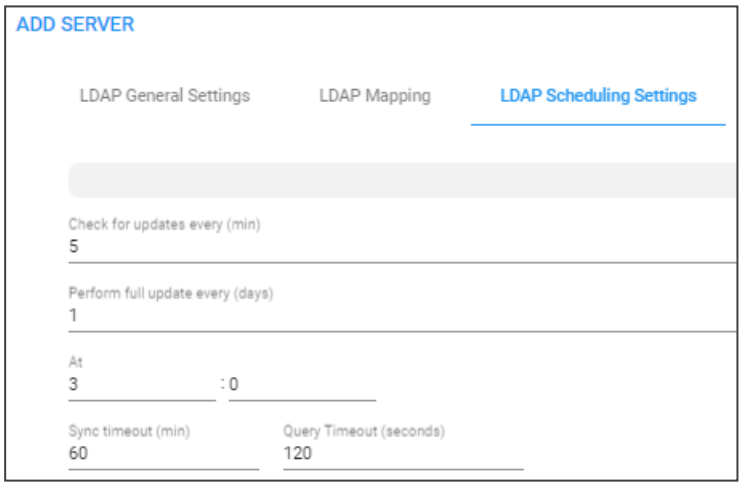
Setting	Description
Name	Enter an intuitive name for the LDAP server.
Host	IP address or DNS name of the LDAP server on which the AD is located.
Port	The LDAP port. Default: 389
Bind DN	The DN (distinguished name) or username of the user used to bind to the LDAP server. For example: ldap@audiocodes.com
Password	Defines the LDAP password used to connect.
Page size	The ARM allows operators to control the page size retrieved from the LDAP server. This may help to reduce some of the strain from the ARM or from the LDAP server. It may also help in some cases where the LDAP server doesn't return all the users defined in it. Note the final value is controlled by the LDAP server itself and cannot be defined above the value configured in the LDAP server. Configure a value in the range 1-10000. Default: 1000.
Filter	
Base Object	Consult the IT manager responsible for the Active Directory in the 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=as;dc=corp;dc=as;dc=com

Setting	Description
	The DN path is defined by the LDAP names OU (organizational unit) and DC (domain component).
Search object	An LDAP search filter used when fetching the users from the LDAP server under the base DN. The default is 'objectClass=user'.
SSL Configurations	
Enable SSL	Enables or disables the connection over SSL. Default: Disable. When disabled, communications with the AD server will be open, i.e., unencoded/unencrypted. When left unchanged at the default; the **Browse** button adjacent to 'Certificate File to Upload' will be unavailable; when enabled, the **Browse** button becomes available.
Certificate file	Enables verification that it is the AD server and no other entity that is communicating with the ARM server. Allows you to browse for a root certificate. When the AD server then sends a certificate, the ARM server uses the root certificate to verify that it is the AD server and no other entity on the other side. Following verification, communications are SSL-encoded.

4. Click **Test Connectivity** to test the connectivity between the ARM server and the AD server.
5. Click the **LDAP Mapping** tab.

- Property fields that display LDAP mappings are synced from the LDAP server
  - ✓ Under **LDAP Mapping** click a field to select the property to map to the LDAP server -OR- enter the first letter or number in the field and if necessary, enter the second as well; the field is automatically populated (filled). LDAP schema typically include multiple attributes so this feature makes it easy for network operators to find an attribute.
- Property fields not displaying LDAP mappings can be mapped locally, in the ARM:
  - ✓ Leave the property field empty and then in the Users page (**Users** > **Users**) open a user's User Details screen and edit the property there according to requirements (see Adding a User Not Listed in an AD to the ARM on page 137)
- In the Property Dictionary page you can define a new property or edit an already defined property (see Adding a Property Dictionary to the ARM on page 172)
- Each dialable Dictionary property has a default normalization which is performed on top of the defined normalization, if a defined normalization exists. This default normalization removes white spaces, minuses, semicolons and parentheses. The default normalization can be changed if needed. Contact your AudioCodes representative if you need to change it.

6. Click the **LDAP Scheduling Settings** tab.



7. Configure the LDAP Scheduling Settings using this table as reference.

Setting	Description
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). Default: Every 5 minutes
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). Default: Every day

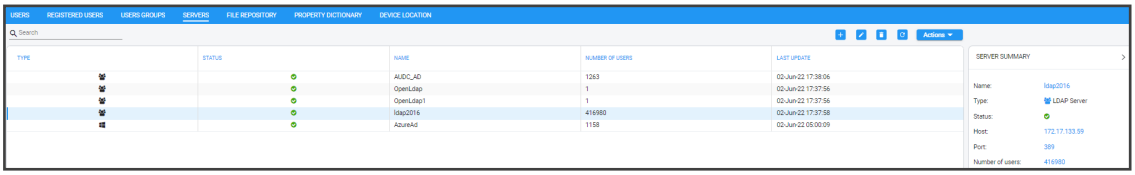
Setting	Description
At	At what time of day the full synchronization (in which the ARM server performs a full update from the AD server) will occur. Default: 0:0, i.e., midnight. Use the arrows to navigate to and select a time. In the preceding figure, the sync will occur every 10 days (frequency) at 00:00 hours (midnight). Default: 03:00 a.m.
Sync timeout (min)	If the AD server doesn't answer within the period configured, the ARM server determines that the AD server is disconnected and a refresh is sent. Default: 60 minutes.
Query Timeout (seconds)	Default: 120 seconds.

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

1. Select the row of the LDAP property to which to attach a Normalization Group.
2. In the property's **Attribute Normalization** field, select a Normalization Group. See Adding a Normalization Group on page 238 for information on how to configure a Normalization Group.
3. Click **OK**.

➢ To view the AD summary:

1. Open the Servers page (**Users** > **Servers**).



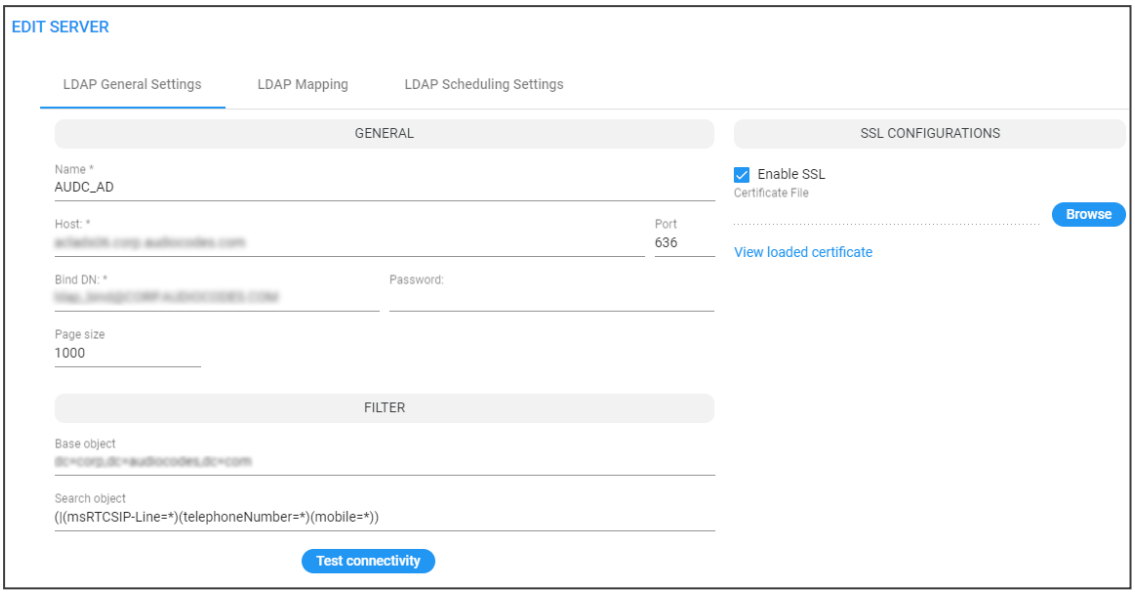
2. Select the AD whose summary you want to view.
3. Use the table as reference to the server's synchronization schedule.

Table 6-2: Server Summary

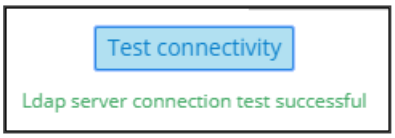
Sync every	ARM and AD databases synchronization schedule. Displays the synchronization frequency: 1-48, i.e., between once every hour (most frequent) to once every two days (most infrequent).
Full Sync at	Displays the time (hour and minute) at which to start a full synchronization. Also displays the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

➢ To edit an LDAP server:

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



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



3. Click the **LDAP Mapping** tab; the same screen that opens when *adding* an LDAP server, shown previously, is displayed. Use as reference the same parameter descriptions as when *adding* an LDAP server.
   - For each LDAP property's LDAP Mapping drop-down menu, select a mapping. Properties that have LDAP mappings are synced from the LDAP server. Properties that do not have LDAP mappings are empty and can be configured locally.
   - Select the LDAP property to which to attach a Normalization Attribute and then from the property's Attribute Normalization drop-down menu, select a Normalization Group. See Adding a Normalization Group on page 238 for information about how to configure a Normalization Group.
4. Click **OK**.

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

Operating with Azure AD

The ARM supports Microsoft Azure AD (in addition to LDAP and Microsoft Azure AD (Active Directory) on-premises) in compliance with the requirements of customers who operate fully in

an Azure cloud environment and who want to utilize Azure AD based on the Graph REST API (rather than LDAP).

The feature covers two aspects:

- Azure AD as source for users in the ARM (see Azure AD as a Source for Users in the ARM on page 166)
- Azure AD for operator authentication (see Azure AD for REST Requests Authentication on page 221)

Configuring the ARM in the Azure Portal

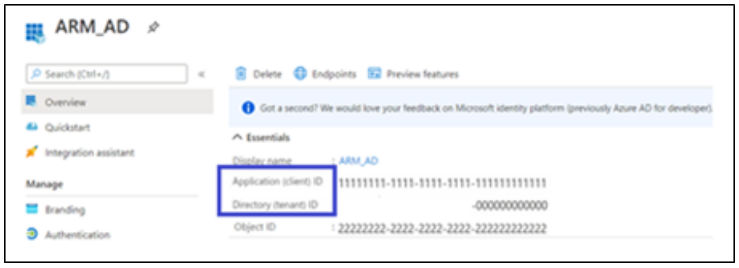
The following is relevant to both Azure AD authentication and Azure AD users. To add Azure AD to the ARM, first register the ARM as an application and provide the ARM with:

- Tenant ID
- Client ID
- Client secret

➢ To configure the ARM in the Azure Portal:

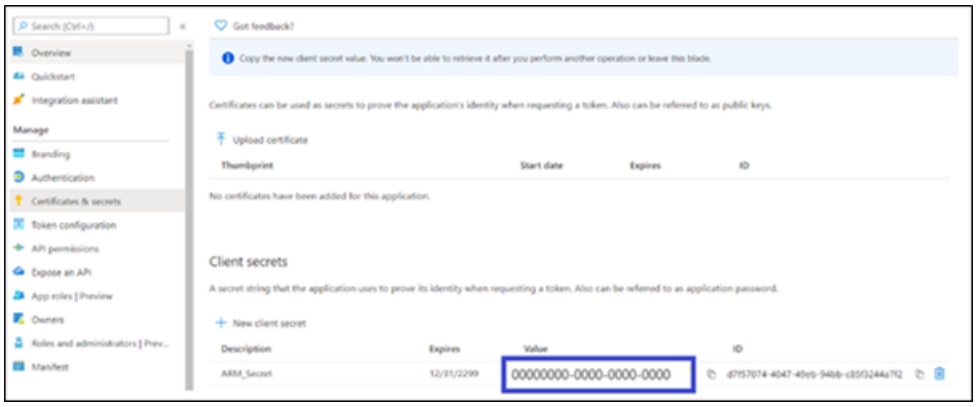
1. Register the ARM as an application; see instructions here.
2. Retrieve the **Client ID** and the **Tenant ID**.
3. When registration finishes, provide the **Client ID** and **Tenant ID** displayed in the app registration's 'Overview' pane.

Figure 6-3: Azure Portal



4. **Client secret**
   a. Create a client secret by clicking **New client secret**.
   b. Copy the client secret value (not the ID) to a safe location; it becomes visible immediately after creation; only then can it be copied; later, it's displayed with stars, e.g., **hsjfhj**********k** and cannot be copied.

Figure 6-4: Client secret



5. **Add Redirect URL**

[Relevant for Azure AD authentication and not for Azure AD users]

Enter the ARM Redirect URL to the registered application in the Azure portal.

In your Azure AD:

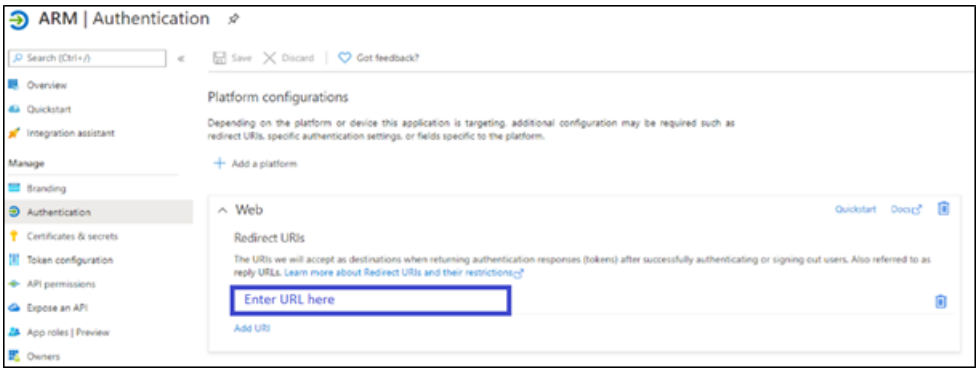
a. Under Manage: Authentication, click **add platform**.

b. Choose **Web**.

c. In 'Redirect URIs', enter the URL.

d. Click **Configure**.

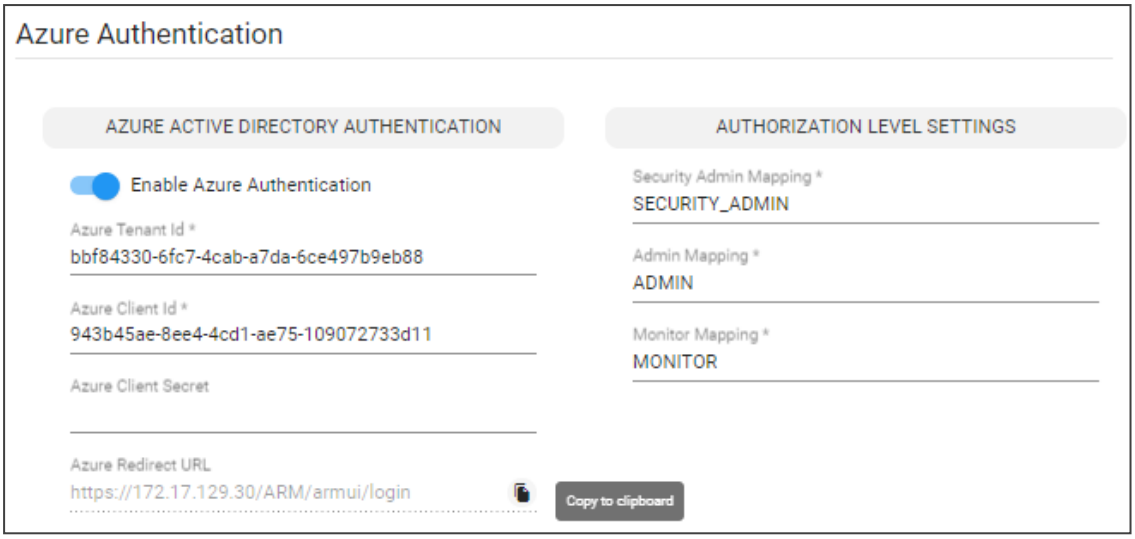
Figure 6-5: Redirect URIs



Make sure the format is **https://{{IP address/Hostname}}/ARM/armui/login**

The selected communication method (IP address or hostname) must match the 'Communication method' configured in the ARM (under **Settings** > **Administration** > **Security** tab).

For simplicity, copy the Redirect URL from the **Settings** > **Administration** > **Azure Authentication** tab.



Any change made to the 'Communication method' setting (**Settings** > **Administration** > **Security**) is automatically reflected in the Azure Redirect URL link. Make sure that the same is configured in the Azure AD.

6. API Permissions

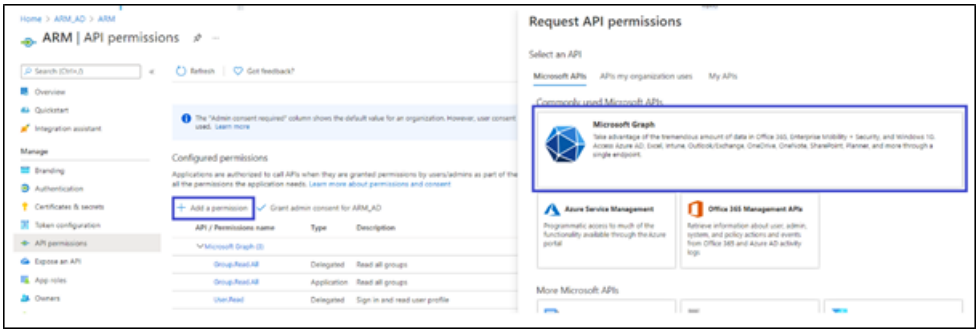
The ARM uses Microsoft's Graph API v.1.0 to retrieve a user's information and app roles. In your Azure AD, go to the **API permissions** tab and add the following permissions (of Microsoft Graph):

- **User.Read (Delegated)** – allows the ARM to sign in on behalf of the user and read the user profile.
- **Application.Read.All** (Application) – allows the ARM to retrieve all app roles in the Azure AD for the purpose of testing connectivity.

For AD users, operators must also add the following permission:

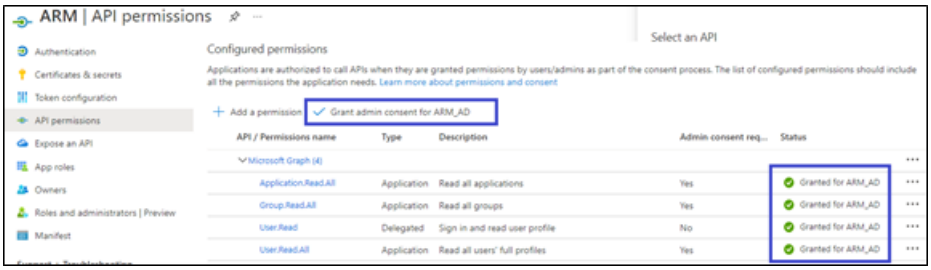
- **User.Read.All** (Application) - allows the ARM to retrieve all the users and their properties from Azure AD.
- **Group.Read.All** (Application) – allows the ARM to retrieve the user's membership groups.

Figure 6-6: API Permissions



- Click **Grant admin consent** to enable these permissions.

Figure 6-7: Grant admin consent



7. Add app roles

Create app roles that will be mapped to ARM access roles – Security Admin, Admin and Monitor. In Azure Active Directory, under **Manage**, select **App registrations** and select the application you defined in the first step.

Select **App roles** | **Preview** and then select **Create app role**.

In the **Create app role** pane, enter the settings for the role.

- **Allowed member types** - Specifies whether this app role can be assigned to users, applications, or both. To support authentication via the REST API, both (**Users/Groups** + **Applications**) options should be selected, else select **Users/Groups**. AudioCodes recommends selecting the **Both** option which supports authentication of both the REST API and the GUI.
- **Value** - Specifies the value of the roles claim that the application should expect in the token. This value should match the roles mapping in **Authorization level settings** in the ARM.

Figure 6-8: Authorization level settings

8. Assign users / groups to roles.

After you add app roles in your application, you can assign users and groups to the roles.

a. In **Azure Active Directory** under **Manage**, select **Enterprise applications** in the left-hand navigation menu.

b. Select **All applications** to view a list of all your applications and then select the application in which you want to assign users or a security group to roles.

c. Under **Manage**, select **Users and groups**.

d. Select **Add user/group** to open the **Add Assignment** pane.

e. Select the **Users** or **groups** selector from the **Add Assignment** pane; a list of users and security groups is displayed.

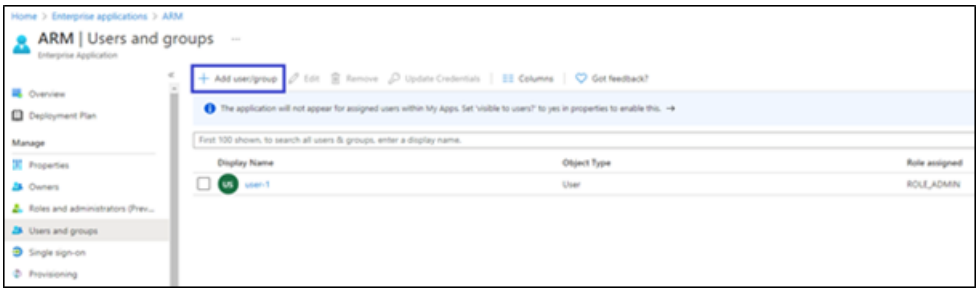
f. After you have selected users and groups, select the **Select** button to proceed.

g. Select **Select a role** in the **Add assignment** pane; all the roles you defined for the application are displayed.

h. Choose a role and select the **Select** button.

i. Select the **Assign** button to finish the assignment of users and groups to the app.

Figure 6-9: Assign



- If you're using Azure B2C, adding app roles and assigning users / groups to roles is performed differently.
- Customers without Azure AD Premium cannot assign app roles to security groups. For these customers, app role assignment to users must be done individually by the administrator or an owner of the app.

More information about the app roles configuration and assignment is available here.

Azure AD as a Source for Users in the ARM

The ARM allows you to access Azure AD natively and to add users from it. 'Azure AD Domain Services' is used as the interface between Azure AD and regular LDAP protocol to access users from Azure AD (without interfacing Azure AD with the REST API).

Microsoft's Graph API v.1.0 is used to retrieve users and the groups in which they're members. These users are treated as regular users in the ARM and can be used for regular operations - such as Users Groups.

The ARM supports most Azure AD flavors such as B2C and to a certain extent B2B (due to limitations in Microsoft's Graph API, for example, B2C doesn't support mapping of the "memberOf" attribute).

Operators cannot map Teams / Skype for Business properties such as EnterpriseVoiceEnabled, OnPremLineURI, HostedVoiceMail, VoiceRoutingPolicy as they're currently not retrievable by Microsoft's Graph API.

➢ To add the Azure AD to ARM:

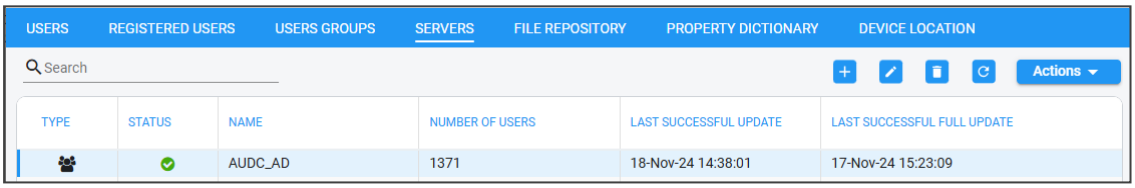
1. Register the ARM as an application and provide the ARM with the following information (as described previously):

   - Tenant ID
   - Client ID
   - Client secret

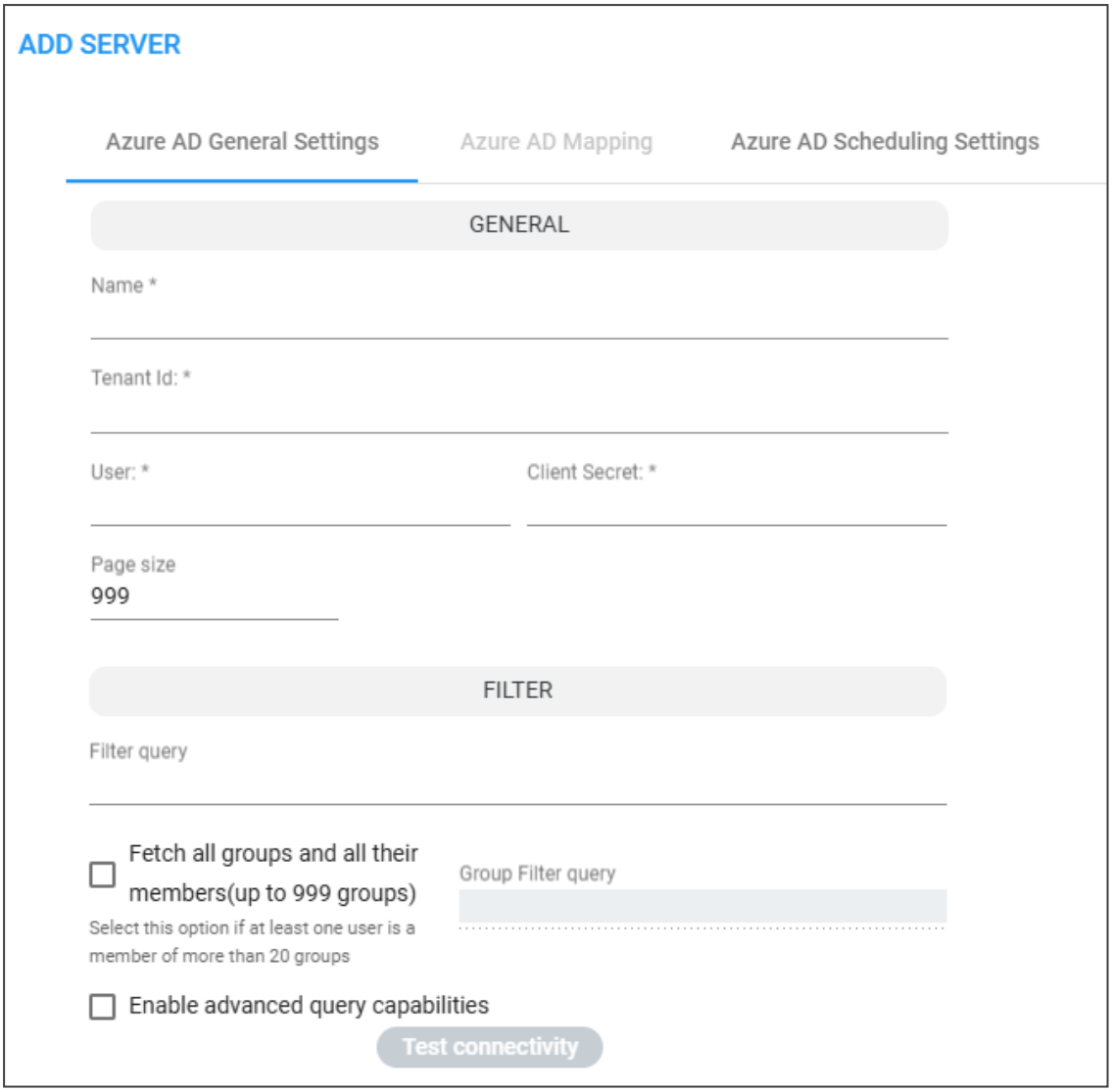
   You can also define parameters such as the frequency (in days) and the time, for the synchronization process.

> ⚠ Due to limitations in Microsoft's Graph API, the ARM doesn't support regular synchronization (Delta) against Azure AD; only full synchronization is supported.

2. Open the Servers page (**Users** > **Servers**).



3. Click the add icon **+** and from the drop-down, select **Azure AD**.



4. Provide information from Azure as shown Configuring the ARM in the Azure Portal on page 162 and then perform **Test connectivity** to test the connection. Optionally, use the search filters under the **Filter** group ('Filter query', 'Fetch all groups ...', 'Group Filter query', and 'Enable advanced query capabilities') according to Microsoft Graph-API guidelines. The parameters under **Azure AD Scheduling Settings** (under 'Updates') are related only to *full synchronization*.

5. After successfully connecting to Azure AD, map the local properties to the values from Azure AD; the 'Azure AD Mapping' drop-down fields display the relevant attributes from the Azure AD.

Figure 6-10: Azure AD Mapping

- Most fields of the type 'User' resource are available for mapping.
- See the list in Microsoft's documentation here.

Authenticating Operator Login

See Authenticating Operator Login Using Azure AD on page 220 for details.

Revoking Azure User Tokens

Network operators with a security level of 'Security Admin' can revoke all tokens created for Azure AD users.

➢ **To revoke all tokens:**

- Send the following REST request:

```
DELETE <ARM_Configurator_IP>/ARM/v1/security/authentication/token/revoke
```

Operating with UMP Server

ARM users can be learned from the UMP (User Management Pack) server. AudioCodes' UMP 365 SP Edition is a software application that automates customer onboarding and simplifies user lifecycle and identity management for hosted Microsoft Teams deployments.

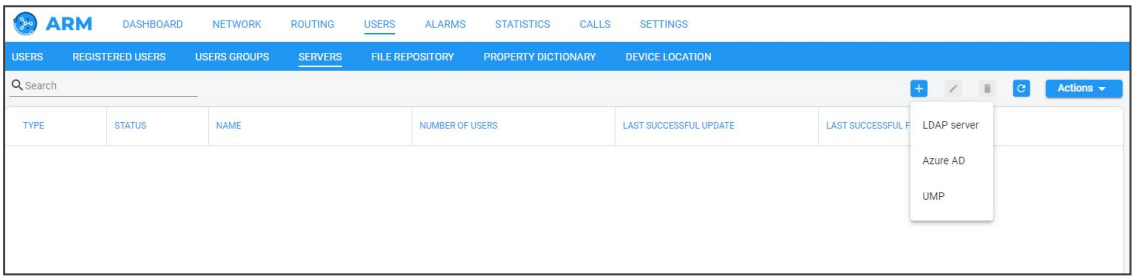
Adding UMP Server to ARM

The Servers page in the ARM enables operators to add a User Management Pack (UMP) server for retrieving user data. Follow the instructions shown below to add a UMP server to the ARM.

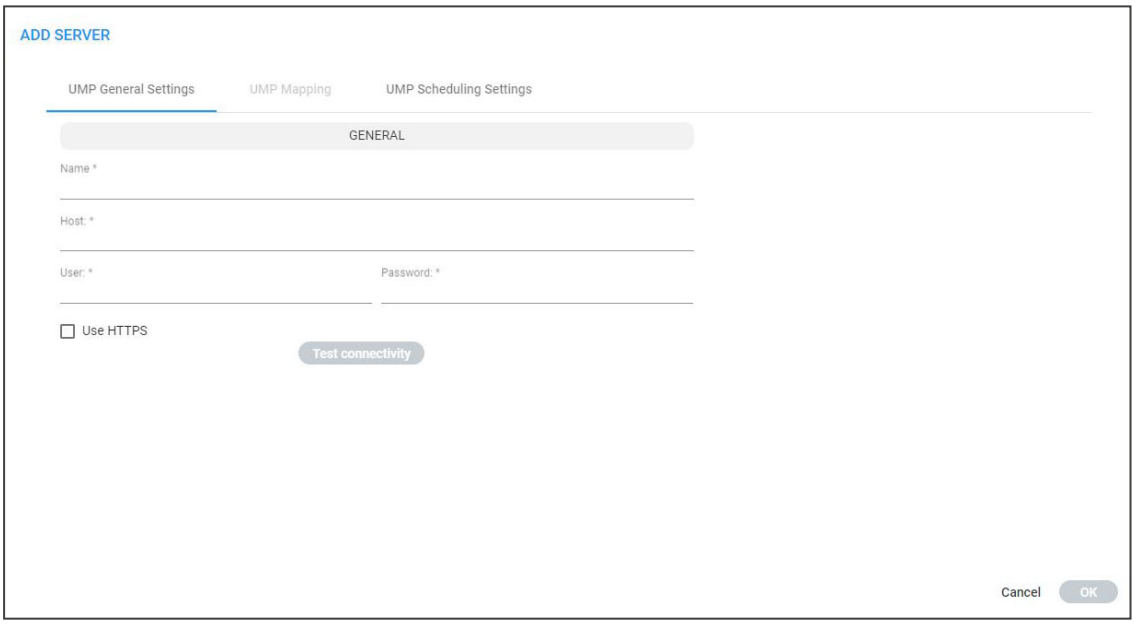
By configuring a UMP server, the ARM can retrieve users with their Teams/Lync attributes, solving a limitation using the Azure AD sever; Microsoft Graph API (REST web API enabling accessing Microsoft Cloud service resources) doesn't support retrieving Teams/Lync attributes such as 'EnterpriseVoiceEnabled' or 'OnPremLineURI' which are needed for routing.

➢ To add a UMP server:

1. Open the Servers page (**Users** > **Servers**).



2. Click the **+** icon and from the drop-down menu, select the **UMP** option.

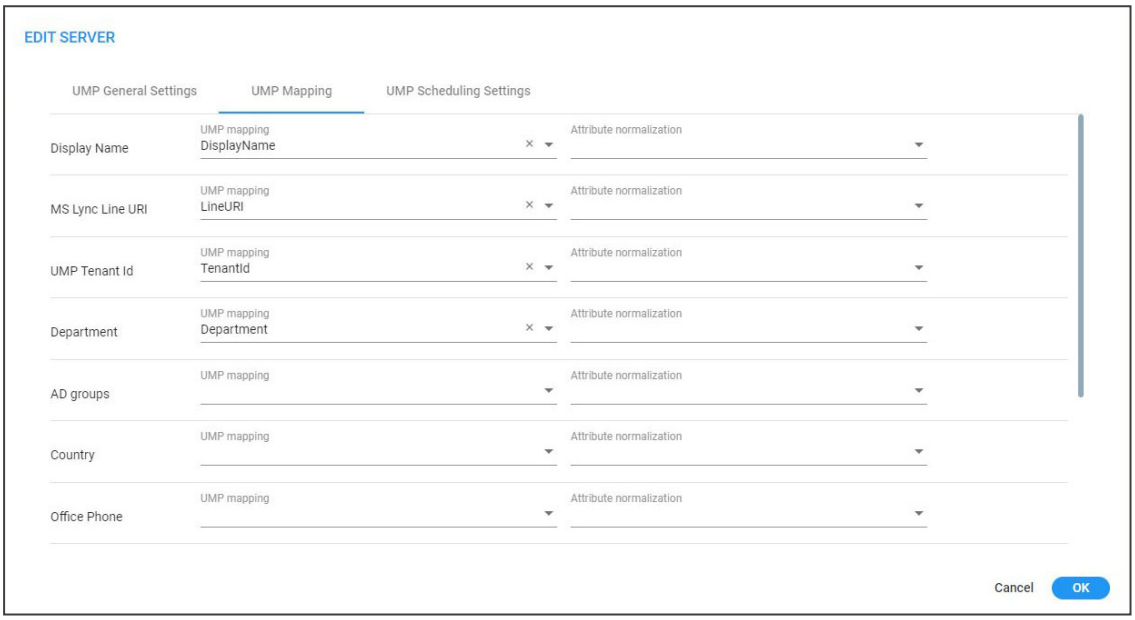


3. Configure the settings under the **UMP General Settings** tab using this table as reference.

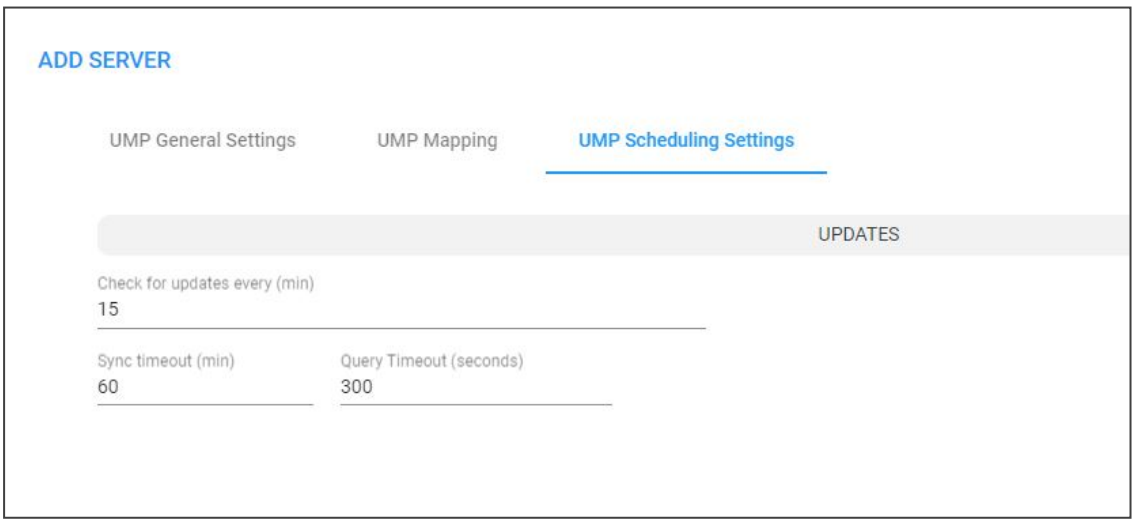
Setting	Description
Name	Enter an intuitive name for the UMP server to facilitate management later.
Host	IP address or DNS name of the UMP server.
User	Defines the UMP user used to connect.

Setting	Description
Password	Defines the UMP password used to connect.
Use HTTPS	Enables or disables the secure HTTP connection with the UMP server.

4. Optionally, perform Test connectivity.
5. Click the **UMP Mapping** tab and map the local properties to the values from the UMP server.



6. Click the **UMP Scheduling Settings** tab.



7. Configure the settings using this table as reference.

Setting	Description
Check for	Defines how frequently the ARM server checks the UMP server for

Setting	Description
updates every (minutes)	updates. Default: 15 minutes
Sync timeout (minutes)	If the UMP server doesn't answer within the period configured, the ARM server determines that the UMP server is disconnected and a refresh is sent. Default: 60 minutes.
Query Timeout (seconds)	Default: 120 seconds.

Configuring ARM in UMP Server

Contact AudioCodes support to configure the ARM IP address in the UMP server.

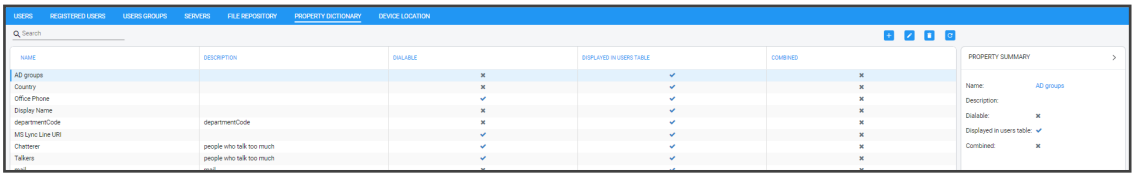
Adding a Property Dictionary to the ARM

The Property Dictionary page lets network operators manage a Property Dictionary, a set of all the properties that a user can have.

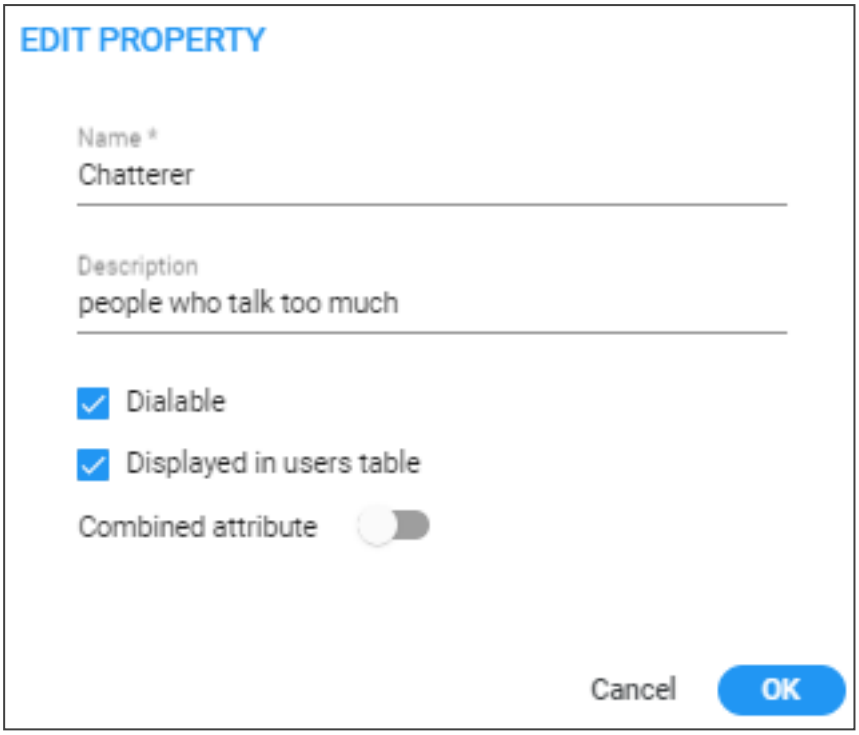
After adding a property to the dictionary, you can add it to some or all your LDAP servers. Properties added to an LDAP server will automatically be read from the LDAP server. Properties not added can be set locally in the ARM for each user. The Properties from the dictionary can then be used as User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

➢ To add / edit a property:

1. Open the Property Dictionary page (**Users** > **Property Dictionary**).



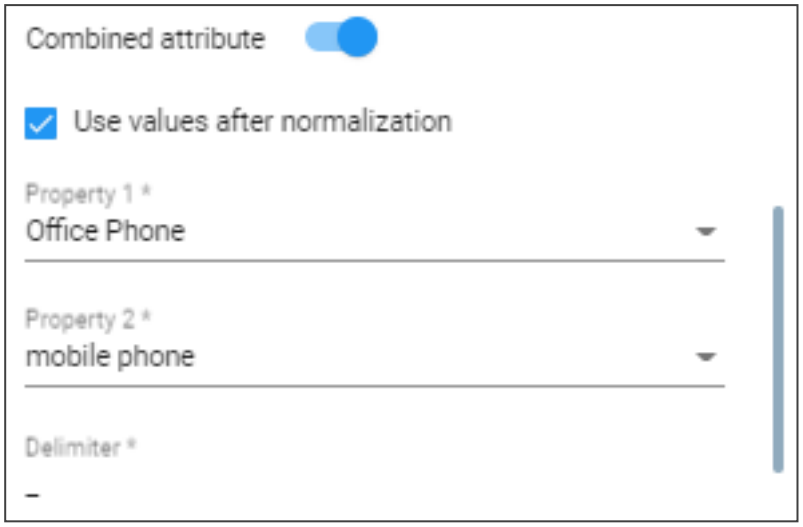
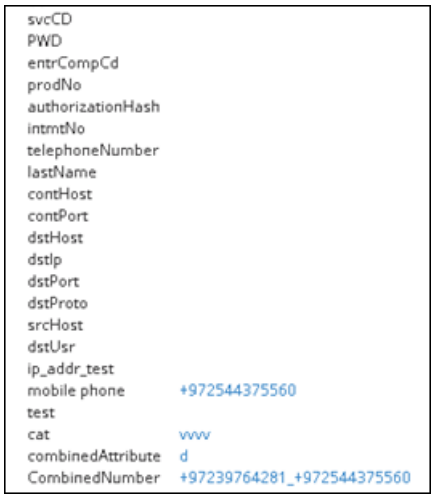
2. Click add **+** or after selecting an existing property, click the edit icon .

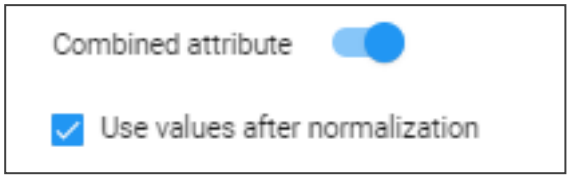


3. Use the following table as reference.

Table 6-3: 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. 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	Enable this option to add a combined attribute, i.e., combining two properties in the Property Dictionary with a predefined delimiter; if any of the properties that the new attribute is combined of changes, the new attribute will change.

Setting	Description
	 In the preceding figure, the new attribute will combine the existing properties Office Phone (Property 1) and mobile phone (Property 1), with the delimiter '_'. A change to the value of any of the comprising properties will trigger a change. The combined attribute will automatically be created for each user.  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.
Use values after normalization	Select this option to apply normalization to a user property combined of two other properties. The combined property can be applied *before or after* normalization. 1. Add a new combined property to the Property Dictionary (**Users** > **Property Dictionary** > click **Add >** select **Combined attribute**

Setting	Description
	2. Select or clear **Use values after normalization**: 

Configuring ARM to Provide Information about Device Location

The ARM can be configured to provide information about the location from where emergency calls are made. The information source is the OVOC. The ARM Configurator periodically synchronizes with the OVOC on location information via the designated REST API. Full sync of data is performed, not just the delta.

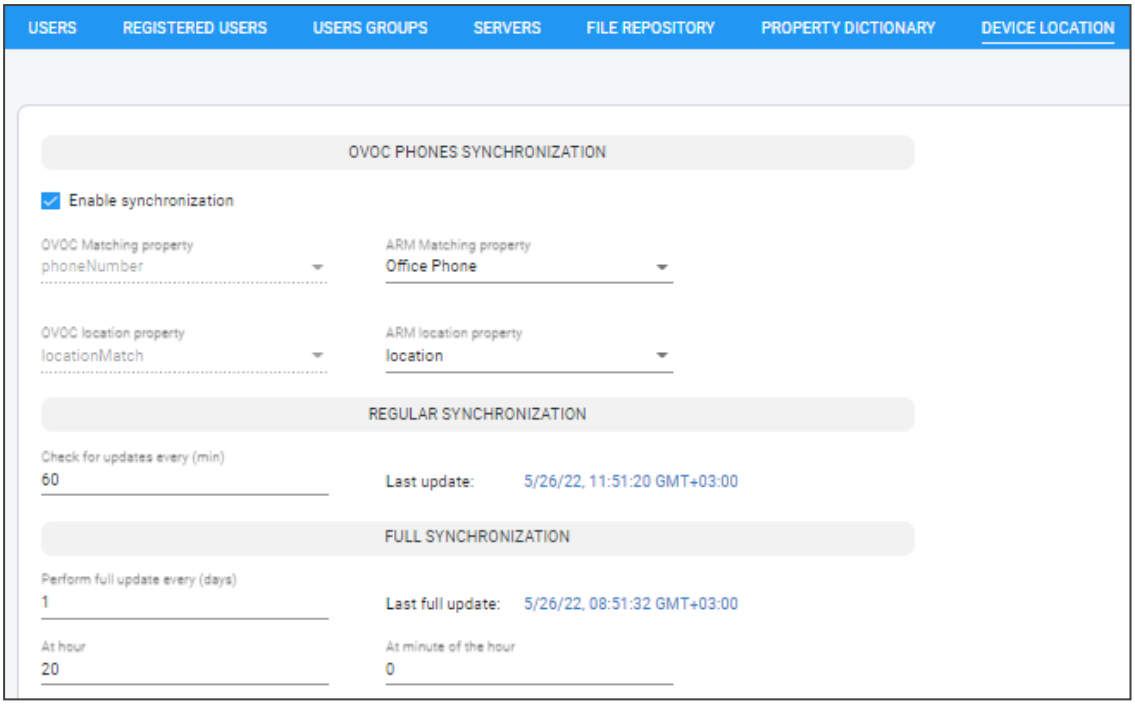
In the OVOC, location information is stored per device. Each OVOC device corresponds to an ARM user. The unique property for matching an OVOC device with an ARM user is the number of the user's device.

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

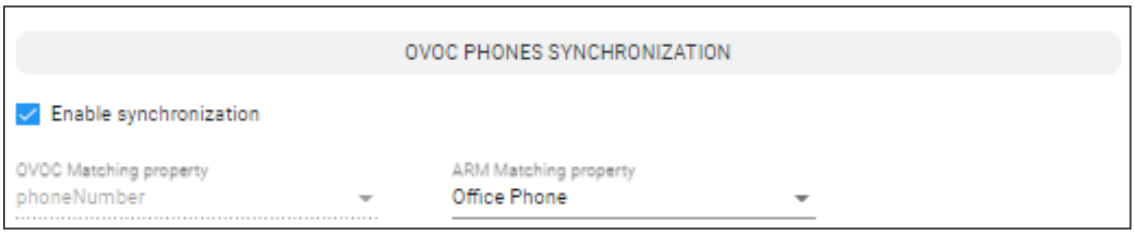
➢ **To enable device location in the ARM:**

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

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



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



Office Phone (for example) is a property that must be defined in the ARM Property Dictionary before this step. See Adding a Property Dictionary to the ARM on page 172 for information about how to define a property in the Property Dictionary.

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

Location (for example) is a property defined in the ARM Property Dictionary. See Adding a Property Dictionary to the ARM on page 172 for more information about how to define a property in the Property Dictionary.

5. In the 'Check for updates every (min)' field under screen section UPDATES, define a regular synchronization time. Default: 60 (minutes). If left at the default, the ARM checks for updates every hour.

6. Define 'Perform full update every (days)'. Default: 1 (day). If left at the default, the ARM performs a full update once a day.
7. In the 'At:' field, enter the time at which the full update will be performed. Default: 20:00. If left at the default, the ARM performs a full update at 8 pm.
8. Click **Submit**.

After configuring and submitting the Device Location settings shown here, you need to define a Policy Studio rule with Action **X_ARM_INFO_1: Location** (for example). See under Policy Studio on page 246 for more information. Once you complete this step, all configuration related to providing Device Location is complete.

7 Configuring Settings

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

- Administration
  - License (see Activating Your License on the next page)
  - Security (see Securing the ARM on page 182)
  - Operators (see Provisioning Operators on page 194)
  - Node Credentials (see Node Credentials on page 201)
  - Router Credentials (see Router Credentials on page 204)
  - Configurator Credentials (see Configurator Credentials on page 206)
  - LDAP Authentication (see Provisioning Operators using an LDAP Server on page 209)
  - RADIUS Authentication (see Provisioning Operators using a RADIUS Server on page 215)
  - Remote Manager (see Remote Manager on page 223)
  - Certificates (see Uploading Trusted Certificates on page 191)
  - Analytics (see Accessing the ARM's Analytics API on page 130)
- Network Services
  - Syslogs (see Editing a Syslog Server on page 226)
  - NTP (see Adding / Editing an NTP Server on page 228)
  - QoS (see Prioritizing Traffic Per Class of Service on page 229)
  - CDR (see Enabling CDRs on page 231)
  - Enabling WebSocket Tunnel (see Enabling WebSocket Tunnel on page 232)
- Call Flow Configurations
  - Normalization Groups (see Adding a Normalization Group on page 238)
  - Normalization Before Routing (see Normalization Before Routing on page 245)
  - Prefix Groups (see Adding a Prefix Group on page 240)
  - Policy Studio (see Policy Studio on page 246)
  - Web Services (see Web-based Services on page 269)
- Routing
  - Configuring a Quality Based Routing Condition (see Configuring Criteria for a Quality Profile on page 290)
  - Configuring a Time-Based Routing Condition (see Configuring a Time-Based Routing Condition on page 291)

- Configuring SIP Alternative Route Reason (see Configuring Alternative Routing SIP Reasons on page 293)
- Configuring Global Routing Settings (see Configuring Global Routing Settings on page 300)
- Configuring Registration Routing Settings (see Registration Routing Settings on page 302)
- Configuring Calls Quota (see Calls Quota on page 304)
- Configuring CAC Profiles (see CAC Profiles on page 311)

- Routing Servers
  - Servers
    - Adding a Routing Server (see Adding a Routing Server on page 314)
    - Editing a Routing Server (see Editing a Routing Server on page 316)
    - Locking / Unlocking a Routing Server (see Locking / Unlocking a Routing Server on page 318)
  - Groups
    - Adding a Routing Server Group (see Adding a Routing Server Group with Internal and External Priorities on page 318)
- Advanced
  - Calls (Disabling, Limiting the Number of CDRs on page 365)
  - Users (see Adding Registered Users to the ARM on page 224)
  - Statistics (Defining a Statistics Retention Policy on page 225)

Administration Settings

The ARM enables the following administrative tasks to be performed:

- Configure a software license (see Activating Your License below)
- Manage security (see Securing the ARM on page 182)
- Add an operator (see Provisioning Operators on page 194)

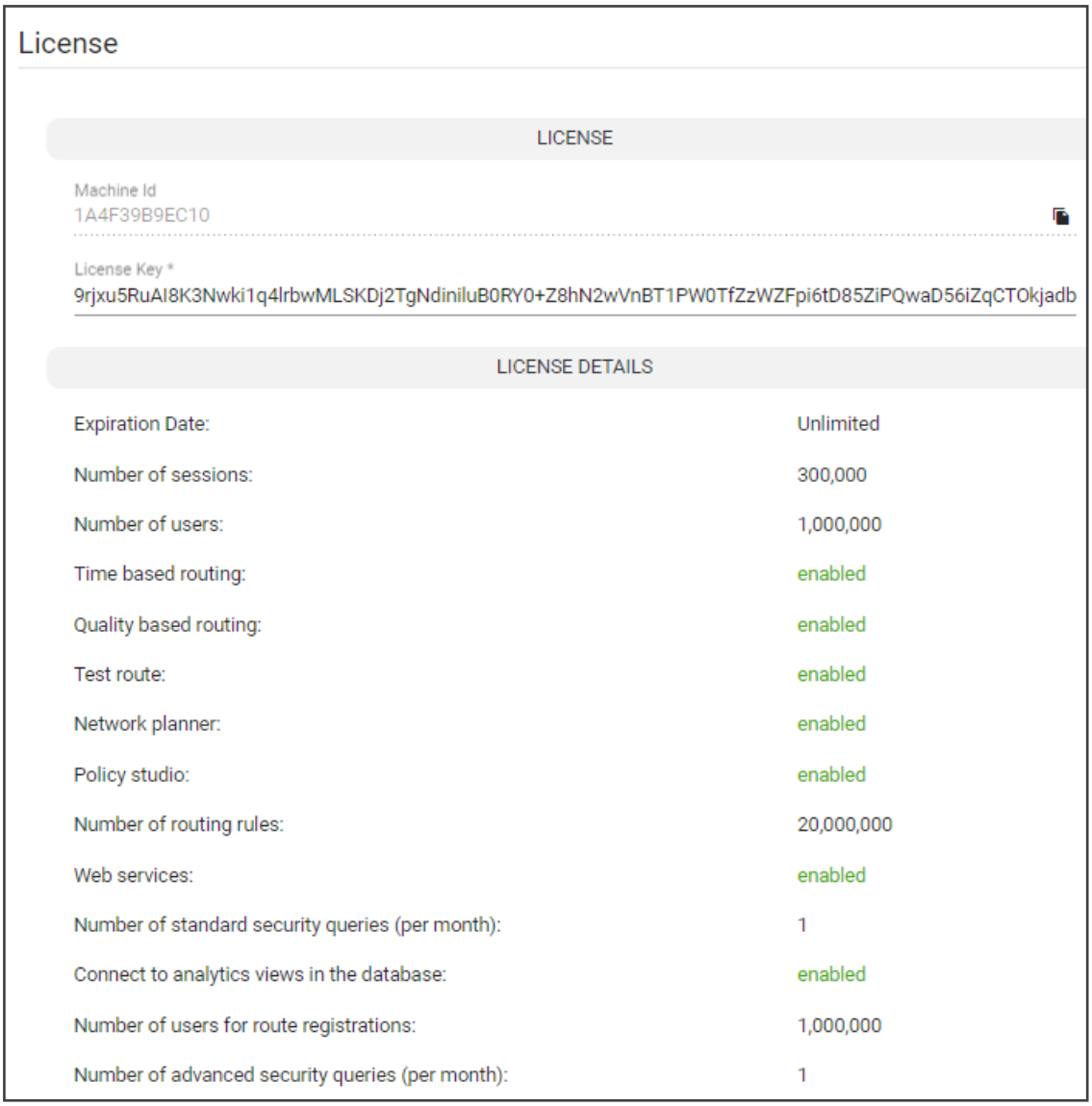
Activating Your License

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

➢ **To activate your license:**

1. After your ARM order is placed and approved, you'll receive from AudioCodes an email with the ARM's 'Product ID'.

2. After installing the ARM, retrieve the Machine ID: In the ARM, open the License page (**Settings** > **Administration** > **License**).



3. Adjacent to 'Machine ID', click the **Copy to clipboard** icon.
4. Access the Software License Activation page at www.audiocodes.com/swactivation and enter the 'Product ID' received from AudioCodes and the (Server) Machine ID that was generated as a result of your installation.
5. Click **Submit**; the ARM license is activated.
6. Make sure under LICENSE DETAILS that the number of sessions purchased and the license's expiry date match those that you purchased.

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

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

For more information about standard vs. advanced security, see step 10 'Security Based Routing', under Adding a New Routing Rule on page 328 and step 6 under Web-based Services on page 269).

Viewing License Details

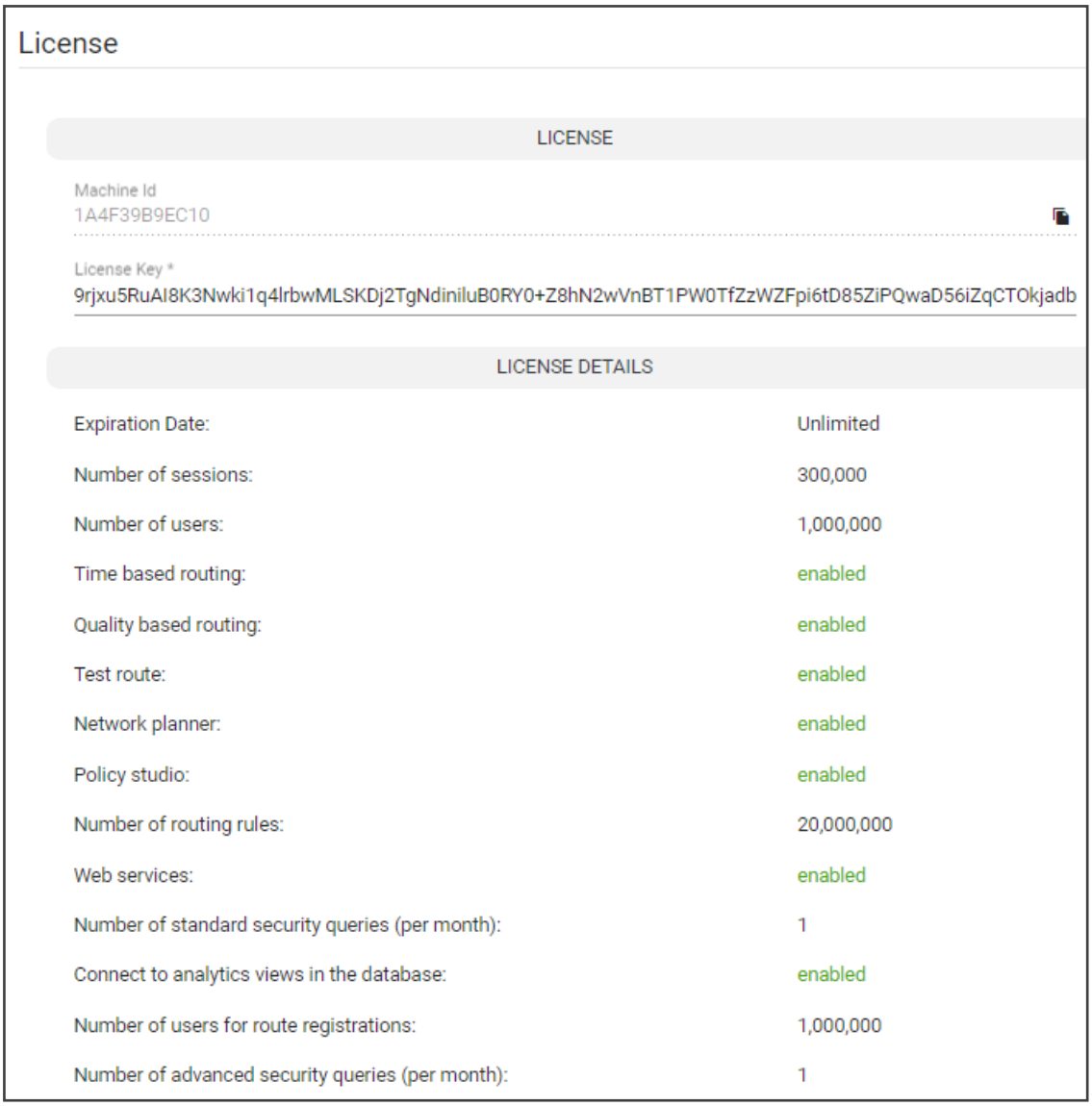
License policy is based on the following aspects of ARM functionality and capacity:

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

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

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

Figure 7-1: License Details



Securing the ARM

This ARM enables operators to secure routing management.

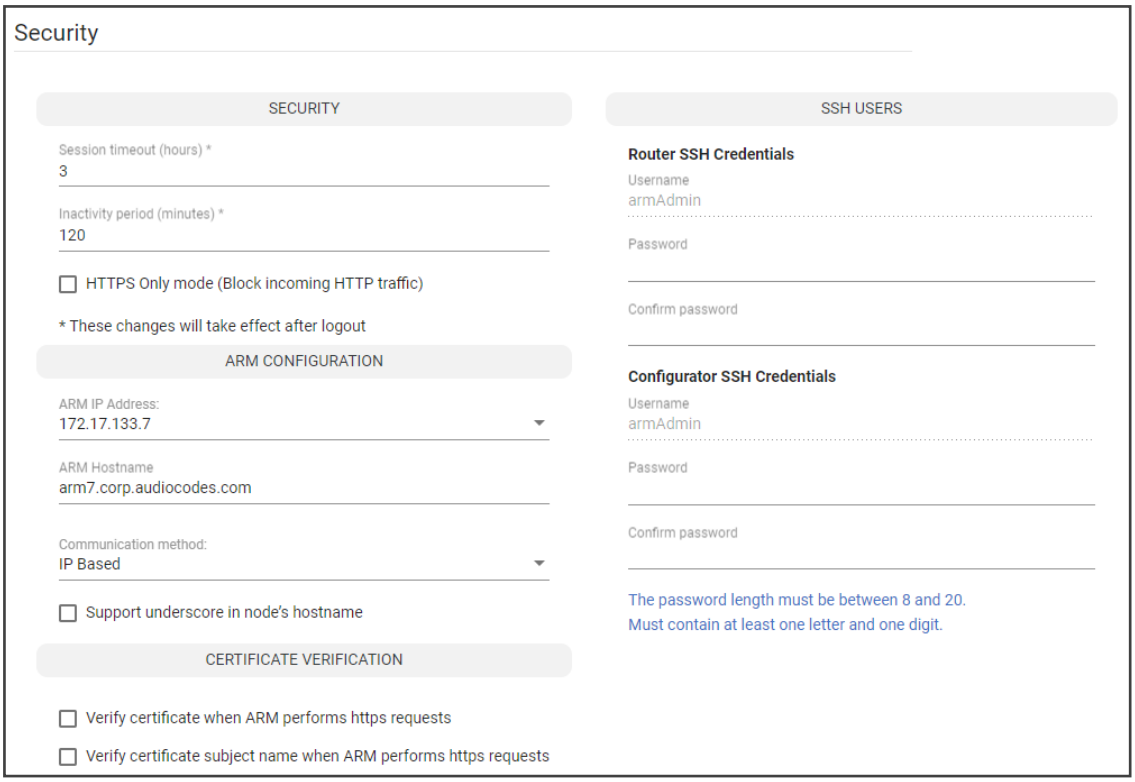
HTTPS, for example, protects users against man-in-the-middle (MitM) attacks launched from compromised networks; with MitM attacks, hackers can steal sensitive enterprise information.

SSH, for example, uses encryption to secure transfer of information between client-server; it allows users to execute shell commands on a remote device with the same level of security as if working in the accessed device.

➢ To secure the ARM:

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

Figure 7-2: Security Page



2. Use the following table as reference.

Table 7-1: Security Settings

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

3. See Enabling Client Side Certificate Validation on page 192 and Enabling Certificate Subject Name Verification on page 192 and click **Submit**.

Configuring Certificates

The ARM GUI simplifies the legacy procedure operators had to perform to change the default certificates. To change the default certificates, operators had to use Java Keytool and other

tools such as OpenSSL, and had to perform the same procedure in both the Configurator and the Routers.

- To change the server certificates of the **Configurator** using the ARM GUI, see Configuring a Configurator Certificate below
- To change the server certificates of the **Routers** using the ARM GUI, see Configuring a Router Certificate on page 189

Configuring Server Certificates

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

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

To change the server certificates of the

- **Configurator**. See Configuring a Configurator Certificate below
- **Routers**. See Configuring a Router Certificate on page 189

Configuring a Configurator Certificate

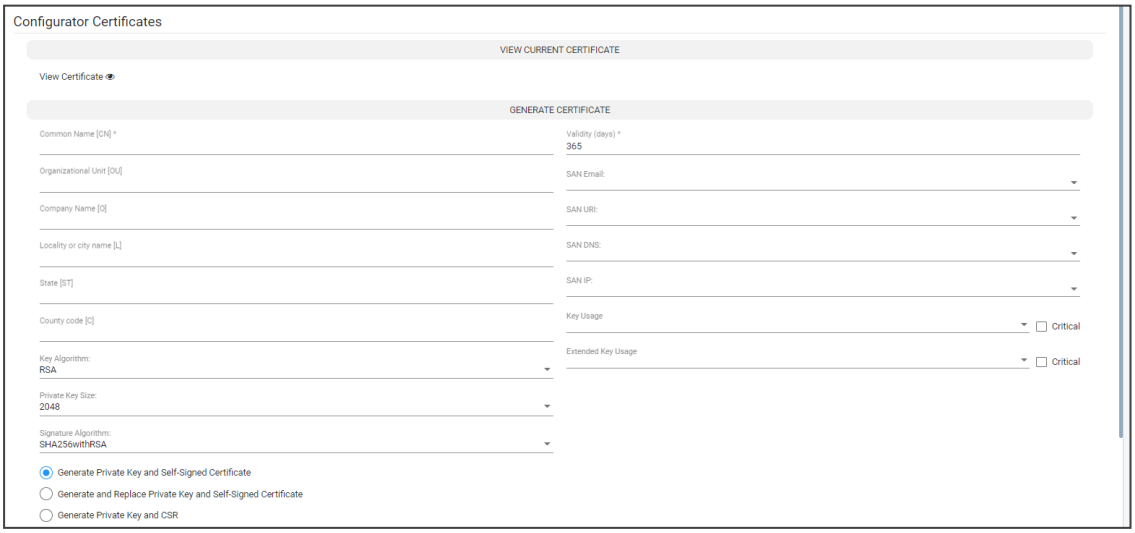
The Configurator certificate can be viewed, generated, or uploaded in the new Configurator screen (**Settings** > **Administration** > **Configurator Certificates**).

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

➢ **To view a certificate:**

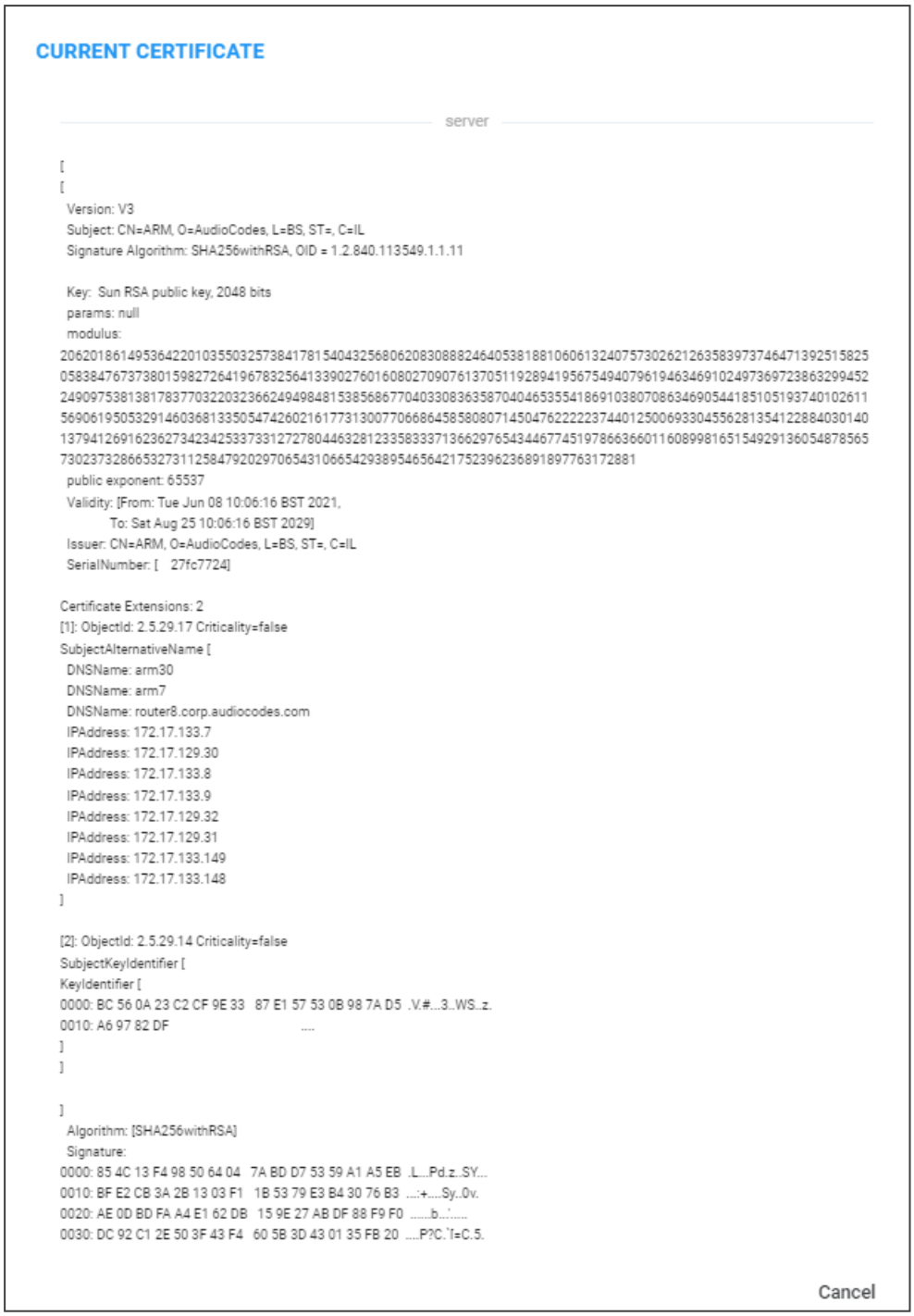
1. Open the Configurator Certificates screen (**Settings** > **Administration** > **Configurator Certificates**).

Figure 7-3: Configurator Certificates



2. Click **View Certificate**.

Figure 7-4: Current Certificate



3. Download or copy the PEM formatted certificate by pressing one of the icons in the Current Certificate view, as shown in the preceding figure.

4. Generate a self-signed certificate: In the Configurator Certificates page, select the **Generate Private Key and Self-Signed Certificate** option; you can generate and download a Java KeyStore (JKS) file which holds the private key and the self-signed certificate. This file can later be uploaded to the ARM as the Configurator or the Router certificate.

5. Configure the fields using the following descriptions as reference (common for all three operations):

   - **Common name**. The only mandatory field. CN field of the certificate. Typically holds the server hostname or IP address.

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

   - **Organization unit**, **Company name**, **Locality or city name**, **State**, **Country code**.
   - **Key Algorithm**. Allows you to control whether the private / public key is RSA or EC (Elliptic curve); the default is RSA
   - **Private key size**. Allows you to control the private key size. For RSA, one of the following values can be chosen: 2048, 3072, 4096. The default value is 2048. For EC, one of the following values can be chosen: 256, 384, or 521. The default is 256.
   - **Signature algorithm**. Allows you to control the signature algorithm for RSA. One of the following can be chosen: SHA256-With-RSA, SHA384-With-RSA, or SHA512-With-RSA. The default is SHA256-With-RSA. For EC, one of the following can be chosen: SHA256-With-ECDSA, SHA384-With-ECDSA, or SHA512-With-ECDSA. The default value is SHA256-With-ECDSA.
   - **Validity**. The number of days for which the certificate will be valid. The default value is 365.
   - **SAN** (Subject Alternative Name) fields. As the common name can hold only one value, operators can use the SAN fields to reuse the certificate (while keeping it valid) for other hostnames (SAN DNS) or for other IP addresses (SAN IP). This option allows operators to create one certificate for the entire ARM network (Configurator and Routers) with valid hostnames and IP addresses. Other SAN fields can be used (though they are less useful for the ARM) such as Email and URI.
   - **Key Usage** (KUEs). Allows you to control the purpose of the generated certificate to allow more tightly controlled usage of it. The following values can be used:
     - digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, and decipherOnly.
   - **Extended Key Usage** (EKUs). An additional key usage option which operators can use to control serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning, or Empty. The default value is Empty, meaning the certificate can be used for any operation.

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

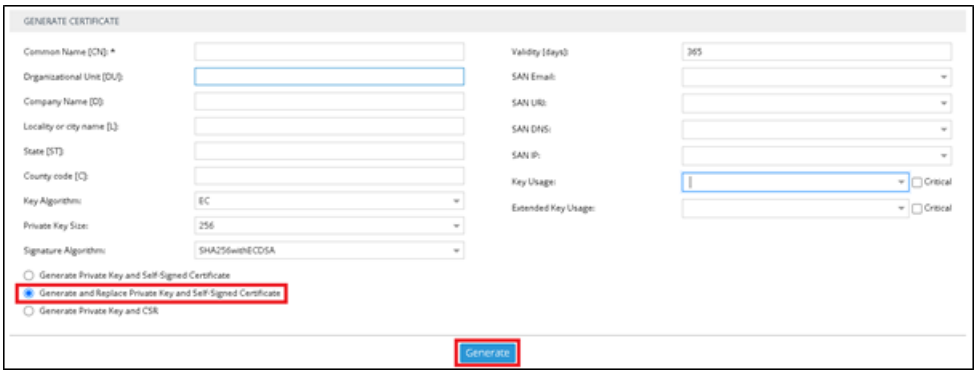
Generating and Replacing a Private Key and Self-Signed Certificate

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

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

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

Figure 7-5: Generate Certificate



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

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

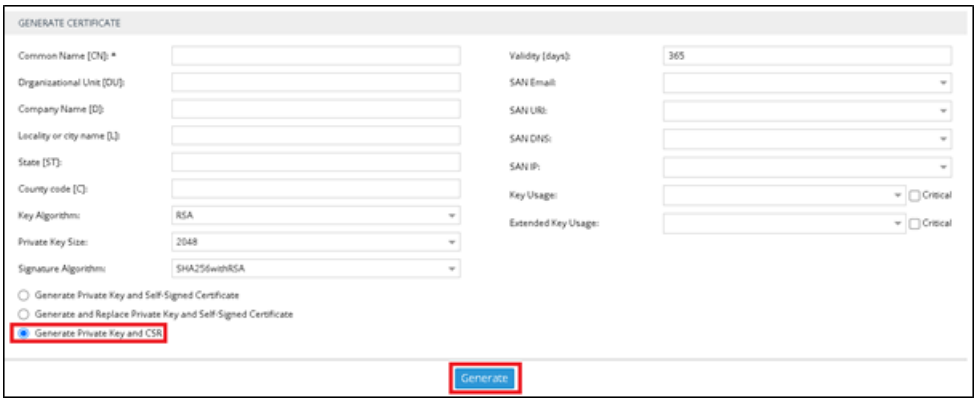
Generating a Private Key, Self-Signed Certificate and CSR

Operators can generate and download a ZIP file which holds a JKS (Java KeyStore file) of the private key and the self-signed certificate, and a text file with the CSR which can be sent to a Certificate Authority (CA) for signing. The JKS file and the signed certificate can later be uploaded to ARM (Configurator and Routers), to replace the loaded certificate.

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

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

Figure 7-6: Generate Certificate

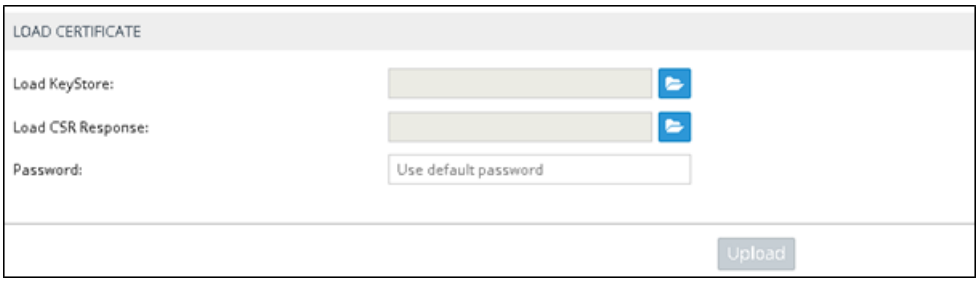


2. Select the **Generate Private Key and CSR** option and click **Generate**.

Loading a Certificate

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

Figure 7-7: Load Certificate



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

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

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

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

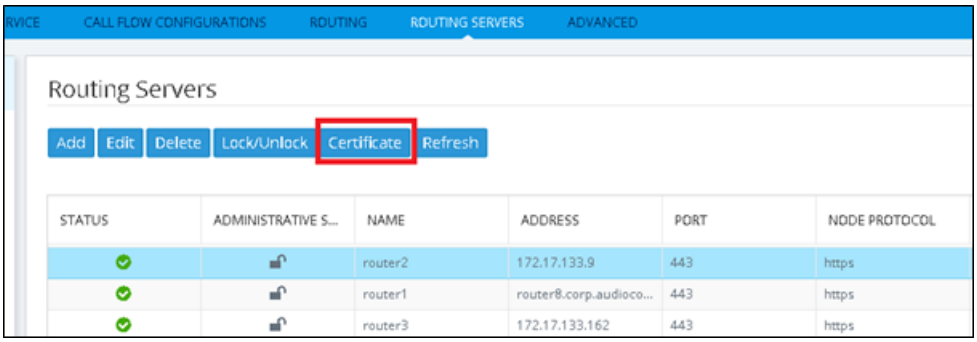
Configuring a Router Certificate

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

➢ To configure a Router Certificate:

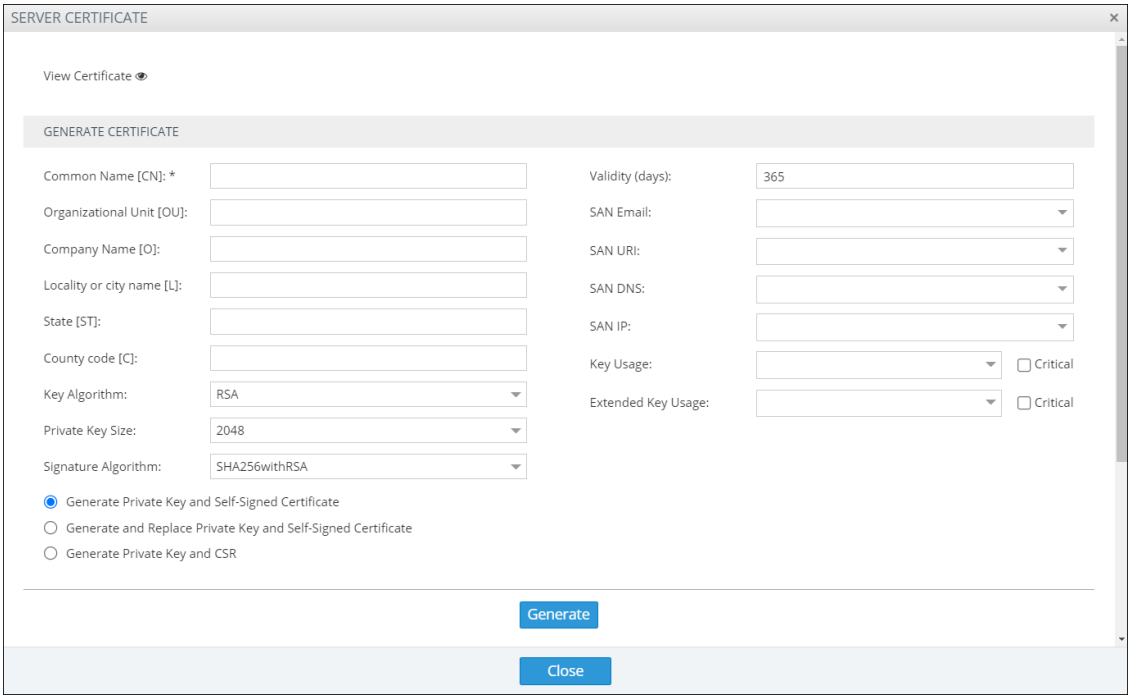
1. Open the Routing Servers page (**Settings** > **Routing Servers** > **Servers**).

Figure 7-8: Routing Servers page



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

Figure 7-9: Server Certificate



3. Configure the parameters using the options described under Configuring a Configurator Certificate on page 184; they're the same.

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

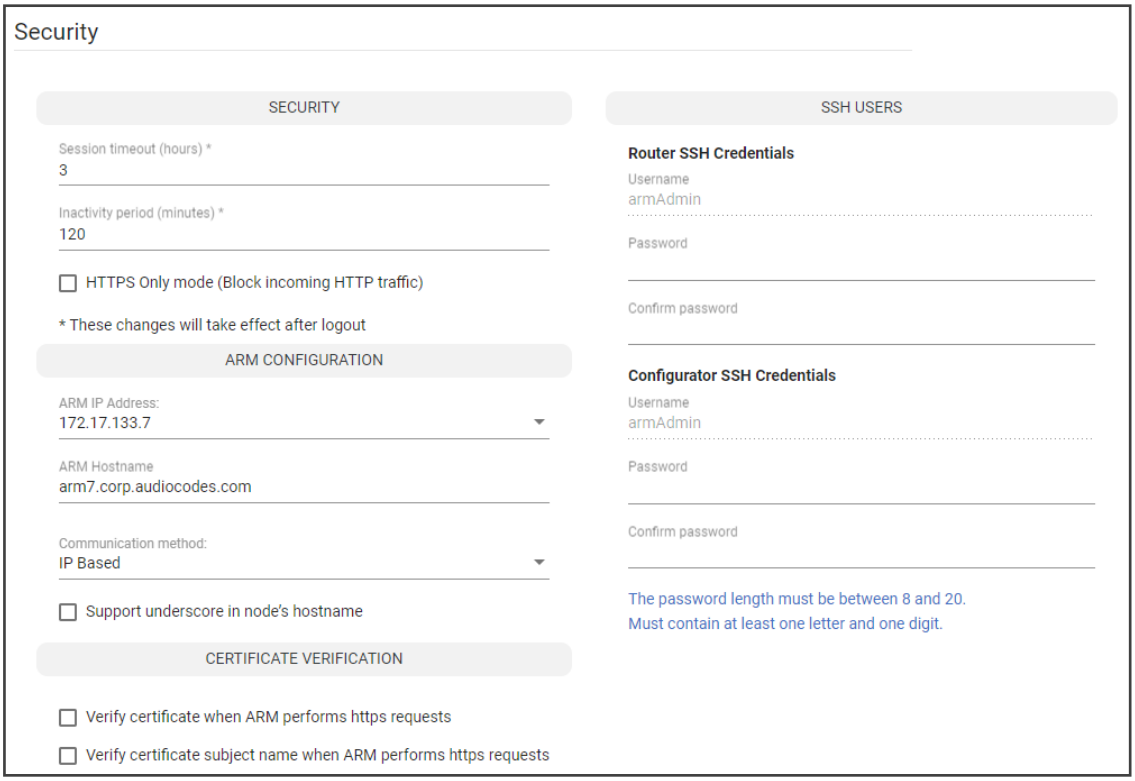
Determining ARM Communications with Other Entities

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

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

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

Figure 7-10: Security



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

- Support underscore in node's hostname [check this option for an underscore in Hostname (FQDN) to be supported]

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

See also Strengthening Security: Certificate Validation below

Strengthening Security: Certificate Validation

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

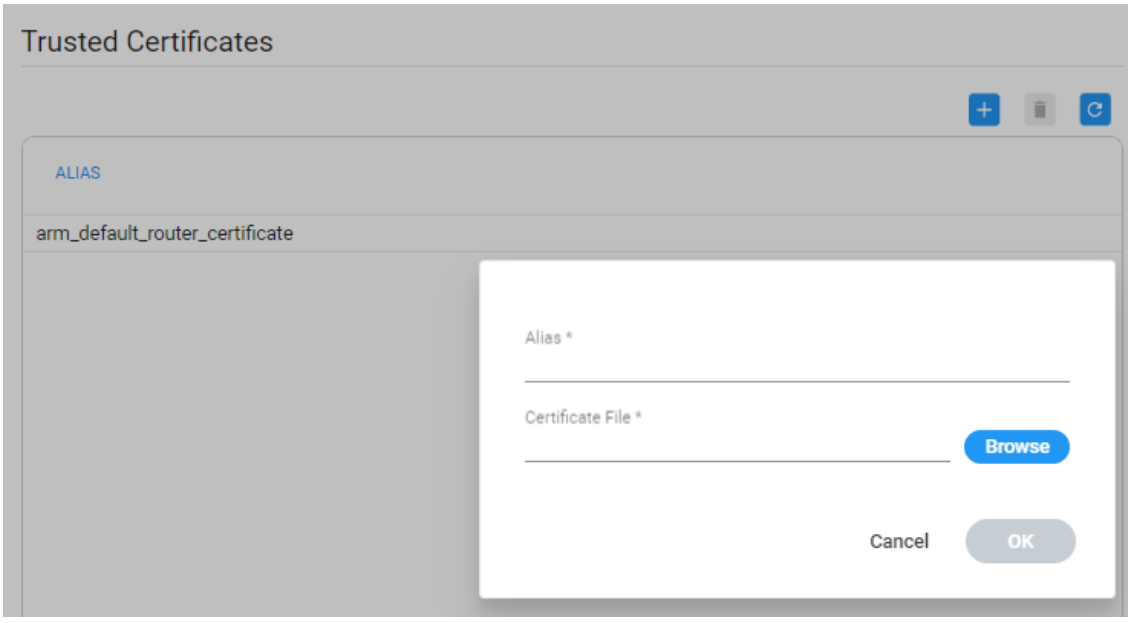
Uploading Trusted Certificates

Operators must first upload trusted certificates to the ARM.

➢ **To upload trusted certificates:**

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

Figure 7-11: Add Trusted Certificate



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

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

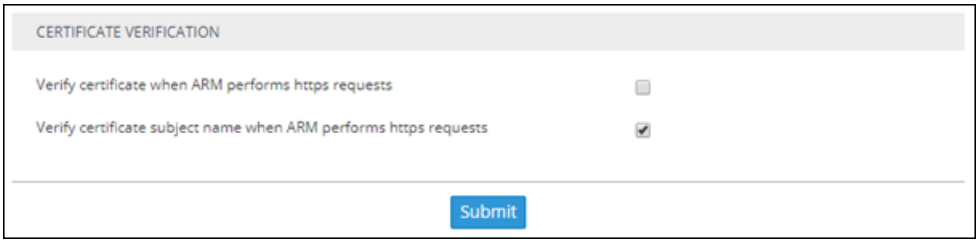
Enabling Certificate Subject Name Verification

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

➢ **To enable certificate subject name verification:**

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

Figure 7-12: 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.

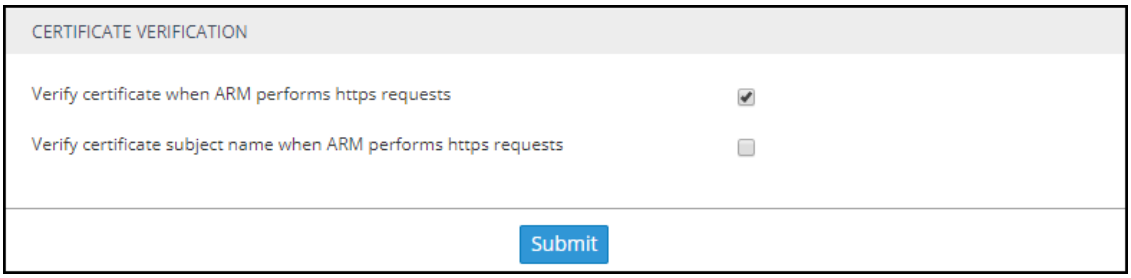
Enabling Client Side Certificate Validation

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 7-13: Certificate Verification



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

Enhancing SSH Users Management for Security

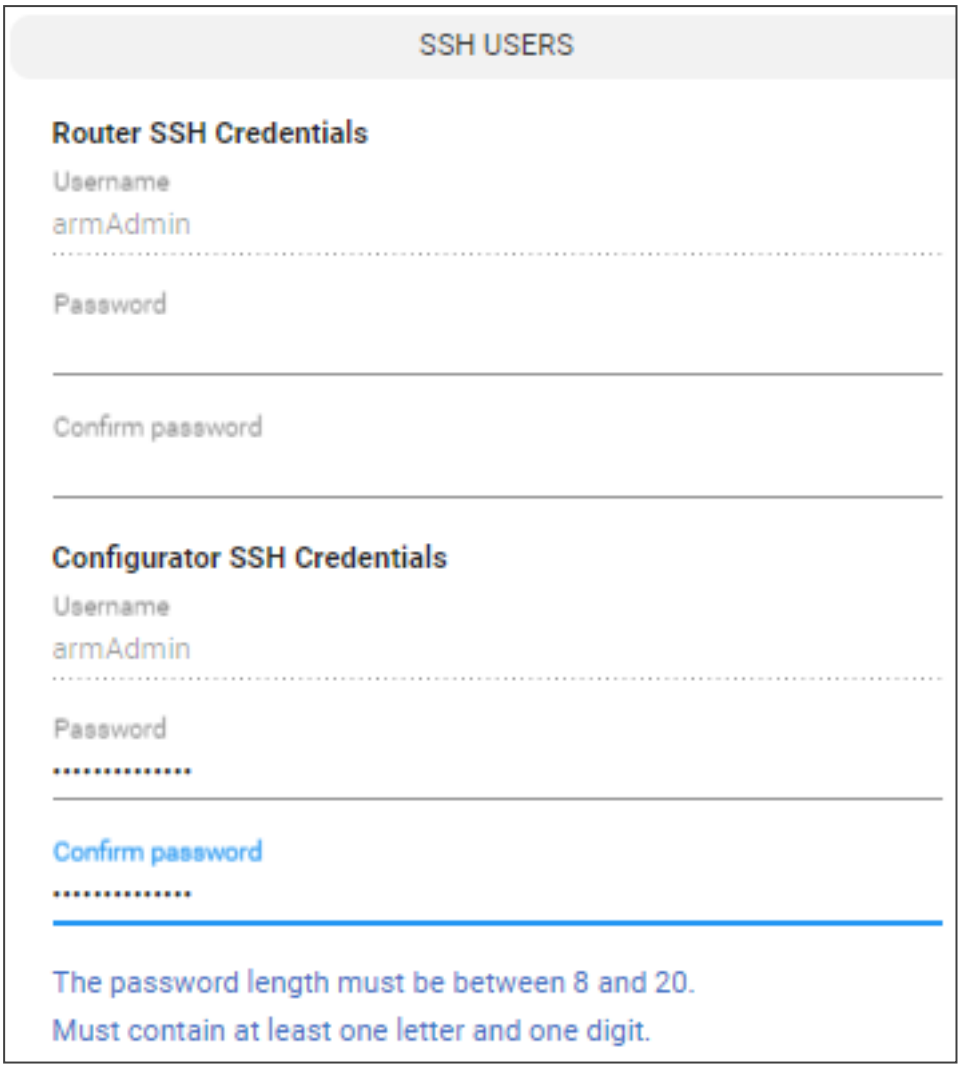
For security reasons, the ARM blocks remote **root** login into ARM VM Linux machines for both ARM Configurator and ARM Router. The feature prevents accidental damage of ARM system files available for the **root** user. External hackers typically attack the **root** user because the **root** account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

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

➢ **To configure enhanced SSH users management for security:**

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

Figure 7-14: SSH Users



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

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

See the *ARM Installation Manual* for more information.

Provisioning Operators

The credentials of operators, i.e., network administrators or IT managers, can be provisioned in four ways:

- Using the ARM's Operators page – see Manually Provisioning an Operator in the ARM's Operators Page on page 199
- Using the enterprise's LDAP authentication server – see Provisioning Operators using an LDAP Server on page 209
- Using the enterprise's RADIUS authentication server – see Provisioning Operators using a RADIUS Server on page 215
- Using the enterprise's Open LDAP authentication server – see Authenticating Operator Login using Open LDAP on page 213
- Using Azure AD - see Authenticating Operator Login Using Azure AD on page 220

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.

Customizing Security Policies

The ARM enables operators to fine-tune the Security Level of each operator by attaching one or more ‘Security Policy’ entities to each operator.

A 'Security Policy' defines operator Security Level.

The feature allows a ‘Security Admin’ to define a stricter write (Add or Edit) Security Level of ‘Monitor’ operators to a subset of ARM actions:

- Routing - Routing Groups *and* Routing Rules
- User Groups
- User Management - Adding, updating, or removing LDAP servers, Azure AD, file repository, or any local user.
- Normalization Groups
- Prefix Groups
- Policy Studio

For example, attaching a Security Policy to an operator with routing permissions allows that operator to exclusively make basic edits/changes to Routing Rules.

The default behavior remains the same.

Three default Security Policies are available, one for each Security Level:

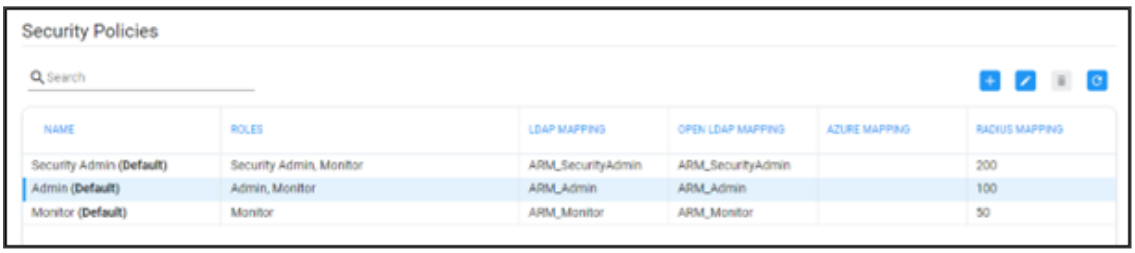
- **Security Admin**
- **Admin**
- **Monitor** (without any write access)

These default Security Polices are attached to the default 'Operator' shipped with the ARM.

- 'Monitor' Security Policy allows 'Read All' access to any ARM action (excluding security and license settings).
- Security Policy adds 'Write' access to some ARM actions.
- 'Monitor' is the base Security Policy in the ARM. Always customize a Security Policy based on 'Monitor'.

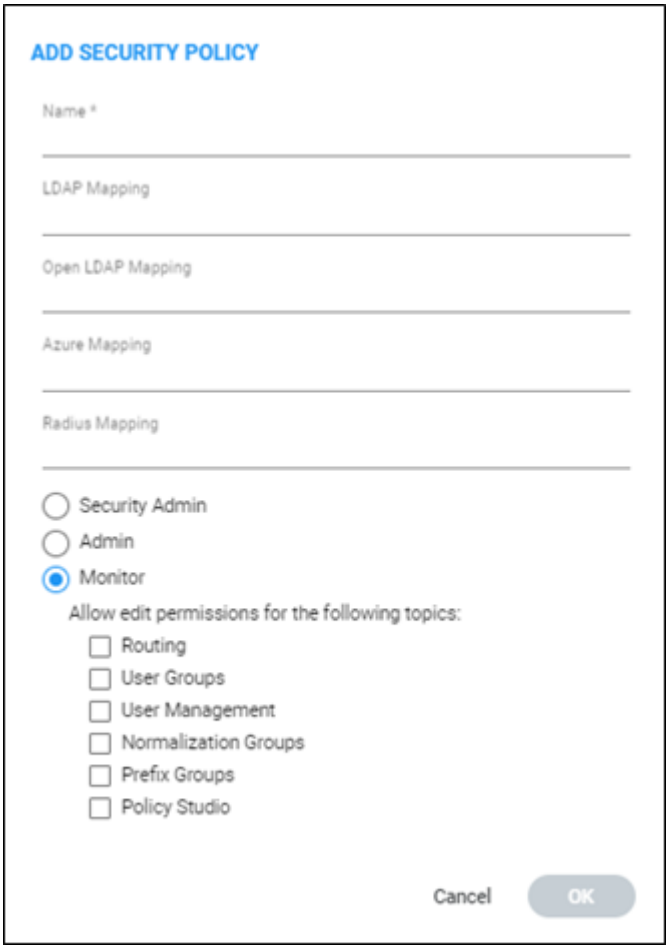
Adding | Customizing a Security Policy

Operators can view, add, customize, or edit Security Policies in the newly added Security Policies page (**Settings** > **Administration** > **Security Policies**).



➢ To add a new Security Policy:

1. Click the **+** icon; the Add Security Policy screen opens.



The Edit Security Policy screen which opens when modifying an existing Security Policy, is identical to the Add Security Policy screen.

- **Security Admin** is the default Security Policy.
- **Monitor** is the base Security Policy in the ARM.

2. Always customize a Security Policy based on **Monitor**. Use the table below as reference to the preceding figure.

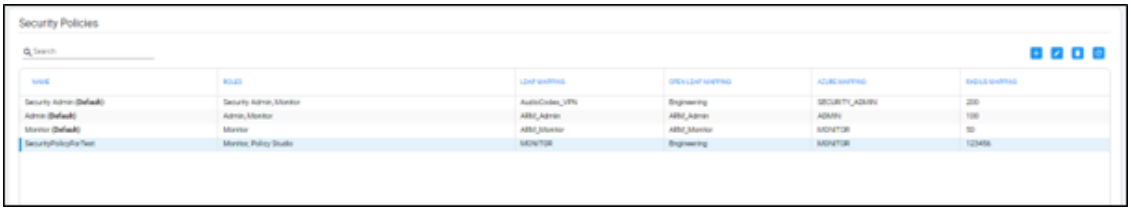
Parameter	Description
Name	The name of the policy. Saved as the identifier when attaching the policy to an operator.
LDAP Mapping	The value that is checked against the value of the defined **permission attribute** in the LDAP Authentication to match this Security Policy.
Open LDAP Mapping	The value which that is checked against the value of the defined **permission attribute** in the Open LDAP Authentication to match this Security policy.
Azure	The value that is checked against one of the roles defined for Azure

Parameter	Description
Mapping	authentication.
RADIUS Mapping	The value that is checked against the value of ACLAuthLevelAttribute of the RADIUS server. The following values can be used if the default AudioCodes values are used: ■ Security admin - 200 ■ Admin - 100 ■ Monitor - 50

3. Choose one of the following default Security Levels for the Security Policy:
   - ✓ **Security Admin** – 'Read and Write' access to anything in the ARM.
   - ✓ **Admin** – 'Read and Write' access to anything besides the security properties of the ARM and operator credentials.
   - ✓ **Monitor** – 'Read' access to anything besides the security properties of the ARM (including other operators)
4. If **Monitor** is chosen, you can add a 'Write' permission to one or more of the following actions:
   - ✓ Routing - Routing Groups and Routing Rules
   - ✓ User Groups
   - ✓ User Management - Adding, updating or removing LDAP servers, Azure AD, file repository or any local user.
   - ✓ Normalization Groups
   - ✓ Prefix Groups
   - ✓ Policy Studio

Customized Security Policy Example

A customized Security Policy named 'SecurityPolicyForTest' is shown in the Security Policies page in the figure below.



The policy can be attached to an operator in the Add | Edit Operator screen described in Manually Provisioning an Operator in the ARM's Operators Page on the next page. This allows that operator to not only monitor the ARM but also to add/edit Policy Studio rules.

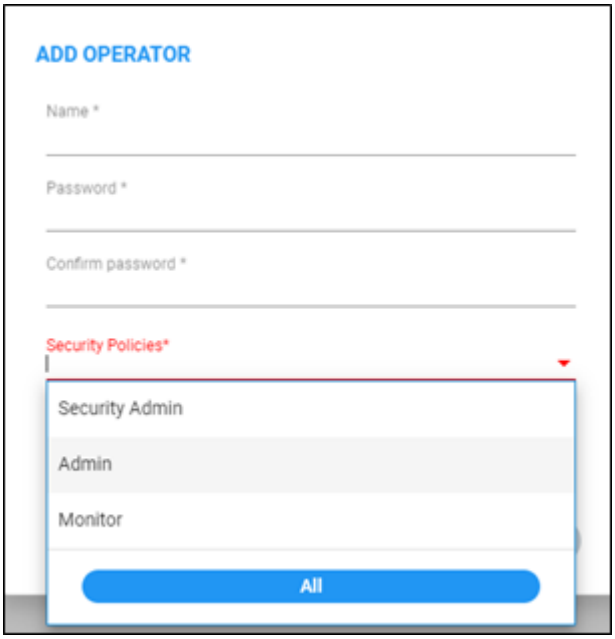
Updating a Security Policy

Operators can update any of the Security Policy properties besides the three default ones, which are indicated by a **Default** indication. For these, operators can only change the various mappings.

Attaching a Security Policy to an Operator

Operators must attach at least one Security Policy to an operator. If multiple Security Policies are attached, the ARM will unify all the roles (actions) of the attached Security Policies.

The Security Policy is attached to the operator in the Add Operator / Edit Operator screen described under Manually Provisioning an Operator in the ARM's Operators Page below.

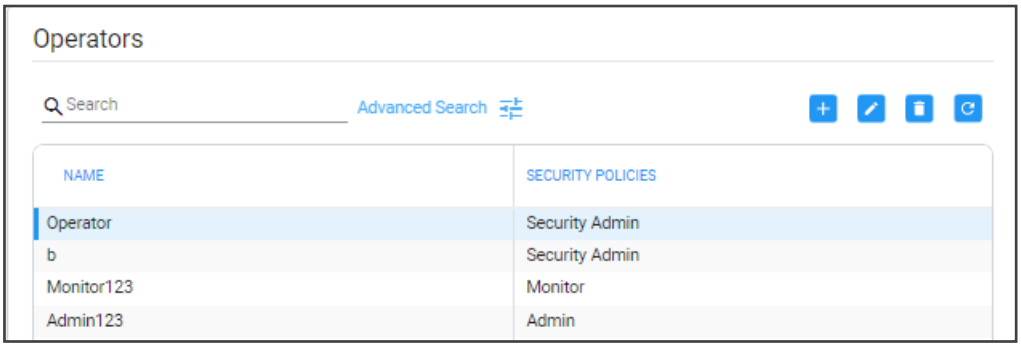


Manually Provisioning an Operator in the ARM's Operators Page

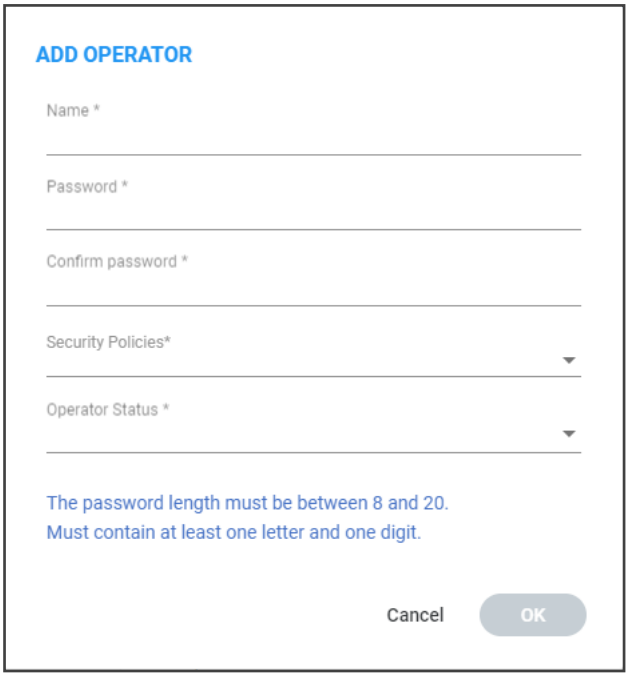
Operators can be manually provisioned using ARM's Operators Page.

➢ **To manually add an operator:**

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



2. Click the add icon **+**.



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

Table 7-2: Add Operator

Parameter	Description
Name	Enter a name for the operator to log in with.
Password	Enter a password for the operator to log in with.
Confirm Password	Confirm the password.
Security Policies	Select one of the following three default 'Security Policies' or select a customized Security Policy you made in the Security Policies page as shown in Customizing Security Policies on page 195. ■ **Admin** can perform any action and provisioning but cannot define new operators. ■ **Security admin** can perform any action, perform provisioning and define a new operator of any permission level. Only 'Security admin' can make changes to any ARM credentials such as node credentials or ARM Router/Configurator credentials. ■ **Monitor** (read-only) cannot perform provisioning or apply any actions. They cannot, moreover, view information under **Settings** >

Parameter	Description
	Administration. License, Security, Certificates, Authentication and Credentials information is only available for viewing and editing to the operator with **Security Admin** or **Admin** privileges. Access to view this information by the operator whose security level is **Monitor** is restricted using the REST API as well. Note that a Security Policy defines the operator's Security Level. For more information about Security Policies, see Customizing Security Policies on page 195.
Operator Status	Select one of the following options to allow or block the operator from logging in to ARM: ■ **Active:** Allows the operator to log in to ARM. ■ **Blocked:** Blocks the operator from logging in to ARM for a specific lockout duration. ■ **Permanent Blocked:** Permanently blocks access to ARM. This option can't be selected. **Note:** ■ This field is displayed only if your admin has enabled the Login Security feature. ■ After 5 consecutive failed ARM login attempts, the operator is blocked for 180 minutes (3 hours). You can view the status of an existing operator, by selecting the operator in the list, and then clicking the Edit icon. If the operator is currently blocked, you can (as Security Admin) unblock (release) the operator by selecting **Active** from the 'Operator Status' drop-down list.

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

Node Credentials

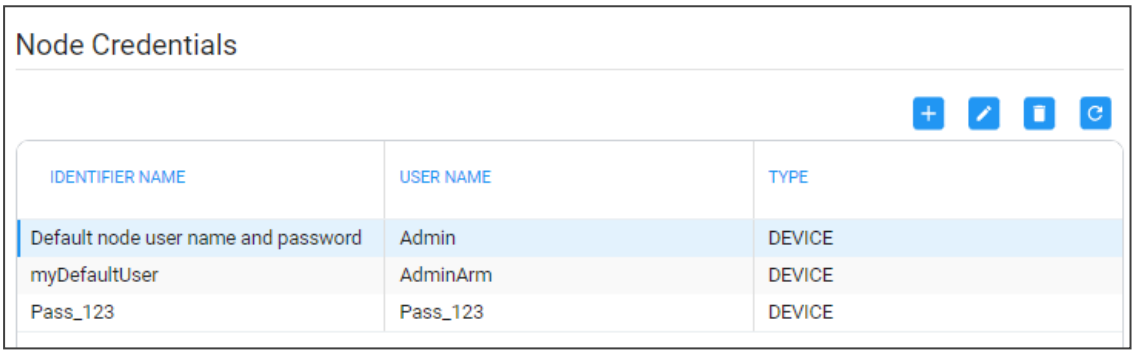
Operators can apply credentials *per Node* for ARM Configurator-Node communications.

- 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:**

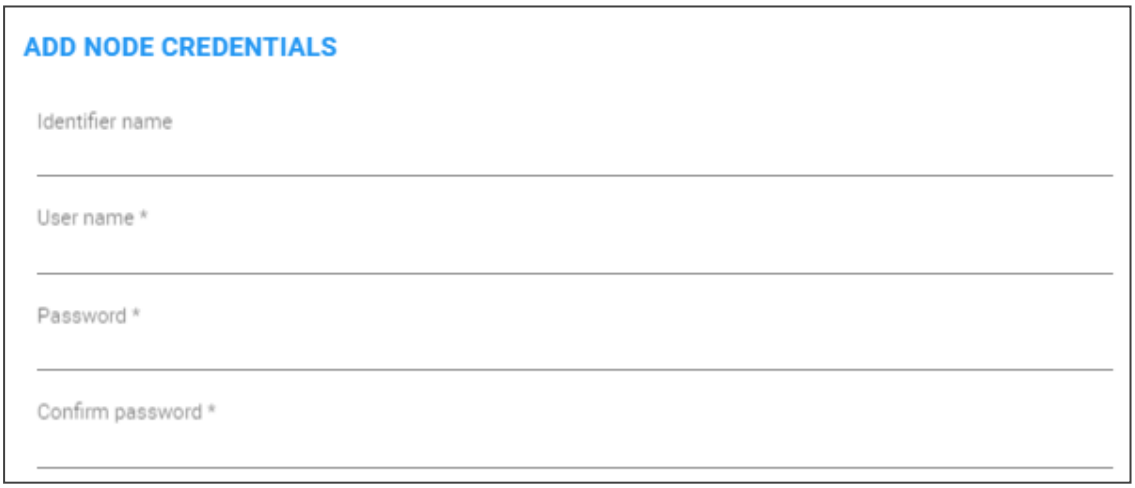
1. Open the Node Credentials page (**Settings** > **Administration** > **Node Credentials**).

Figure 7-15: Node Credentials



2. Click **Add**.

Figure 7-16: Add Node Credentials



3. Configure the fields using the table as reference.

Table 7-3: Add Node Credentials

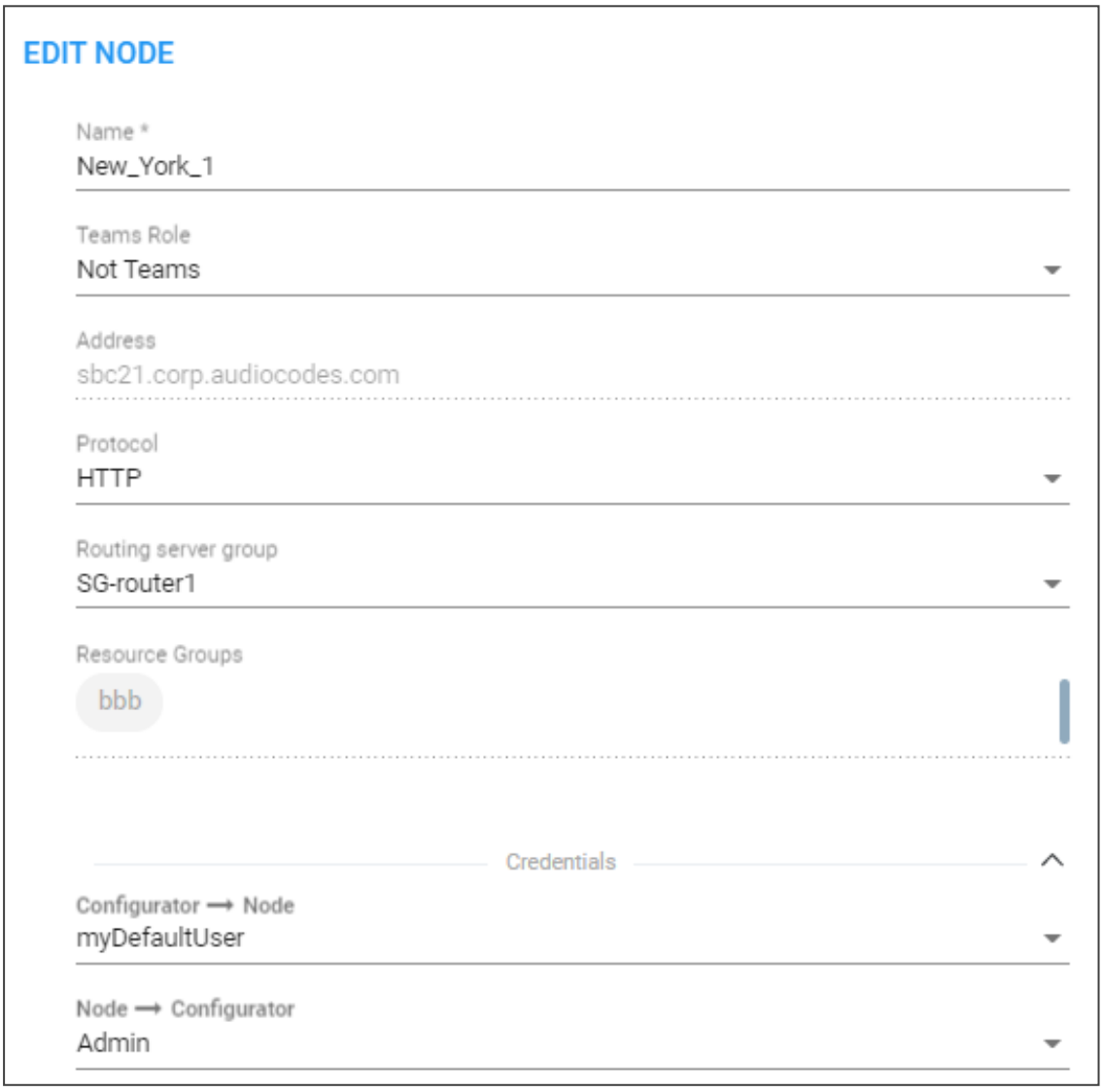
Setting	Description
Identifier name	Enter a name to identify this set of device credentials.
User name	Enter the user name.
Password	Enter the password.

Setting	Description
Password confirm	Re-enter the password.

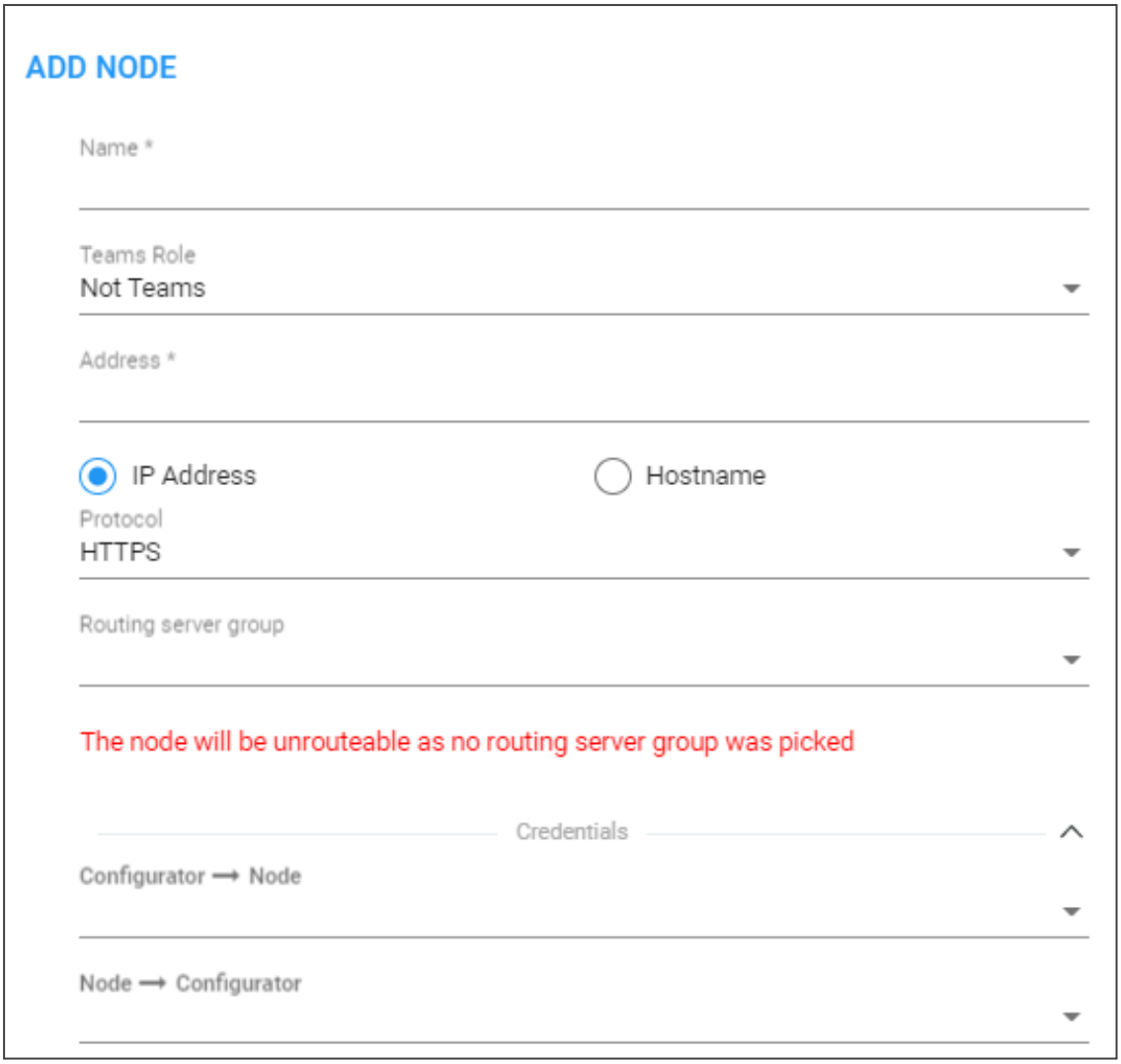
4. Click **OK**.

- After adding credentials you can Edit or Delete.
- 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 7-17: Edit Node - Credentials - Configurator > Node



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



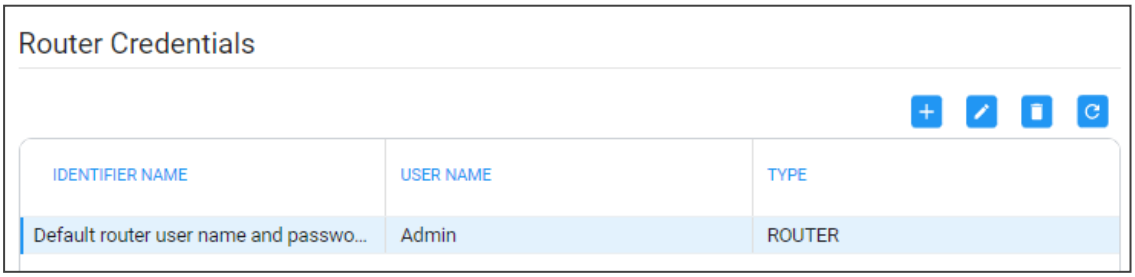
Router Credentials

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 7-18: Router Credentials



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

2. Click the add icon **+**.

Figure 7-19: Add Router Credentials

3. Configure the fields using the table as reference.

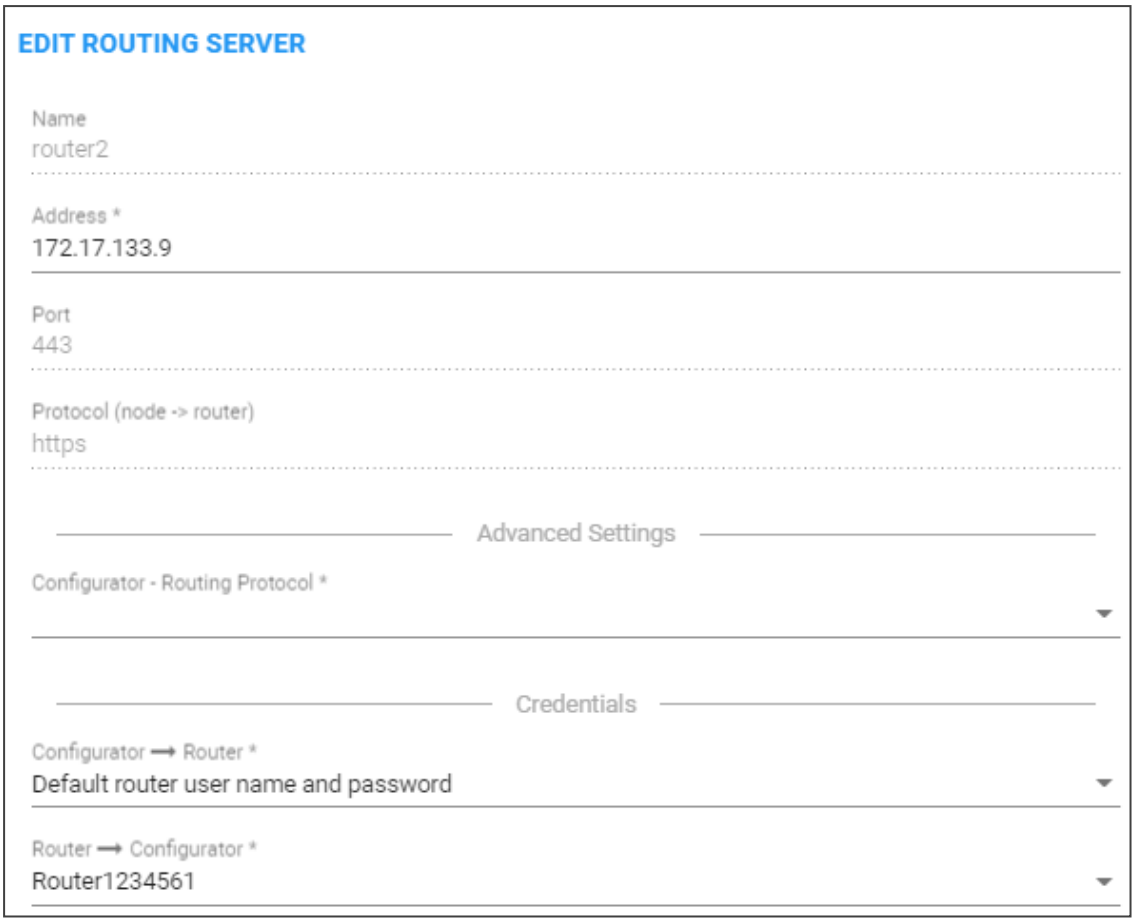
Table 7-4: Add Router Credentials

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 7-20: Edit Routing Server



Configurator Credentials

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

- **Node - ARM Configurator**

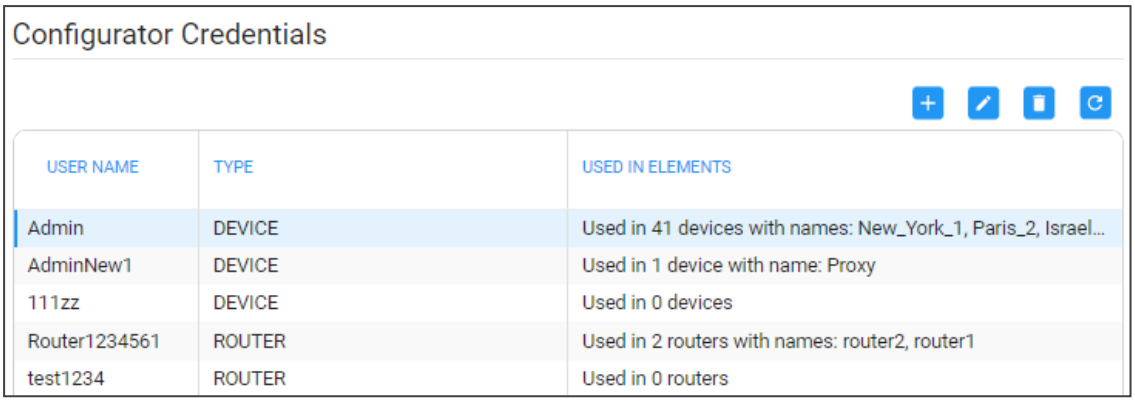
  and

- **ARM Router - ARM Configurator**

➢ **To configure new credentials:**

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

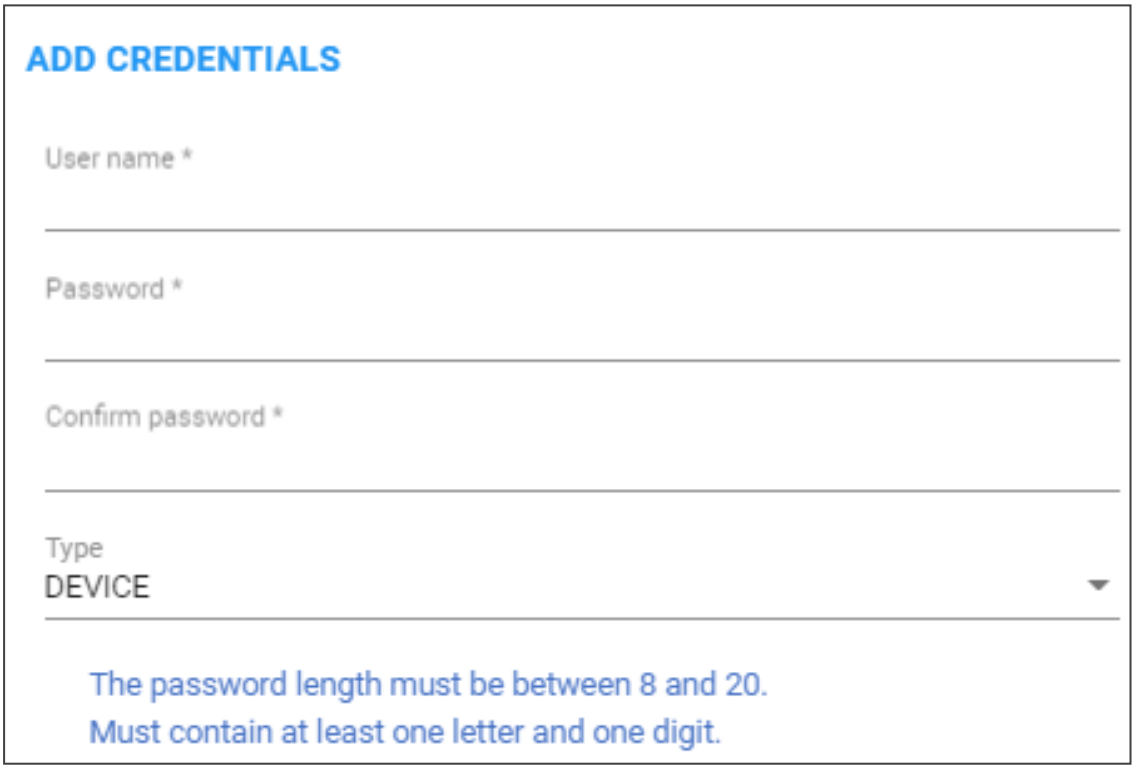
Figure 7-21: Configurator Credentials



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

2. Click the add icon **+**.

Figure 7-22: 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**.

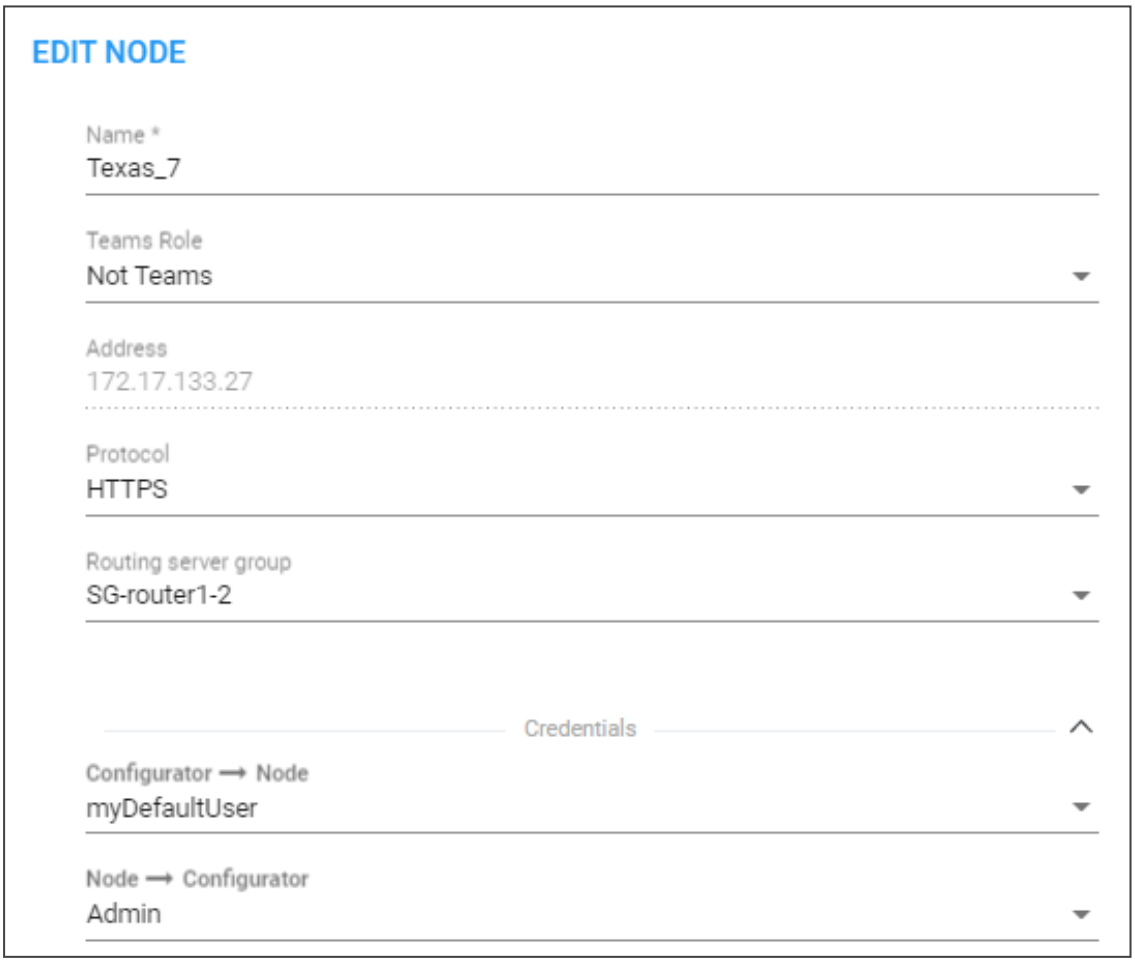
3. Configure the fields using the table as reference.

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**.

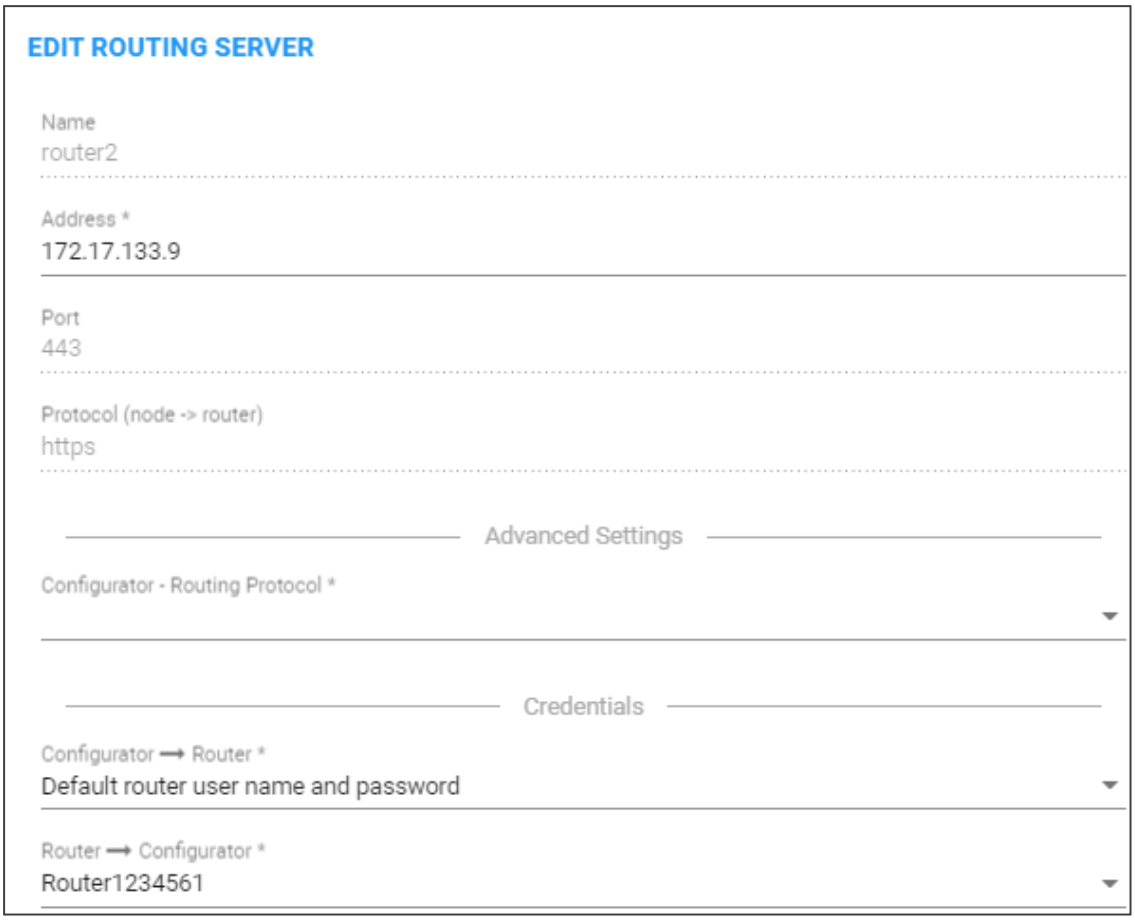
4. Click **OK**.
5. [Optionally] Apply one of the previously defined settings to a specific
   - **Node** (or use the default Node): Open the Edit Node screen (**Network** > **Map** > <right-click the node> > **Edit**) and expand 'Credentials'.

Figure 7-23: Edit Node



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

- **Router**: Open the Routing Servers page (**Settings** > **Routing Servers**), click the add **+** or the edit icon for the specific ARM Routing Server, 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.

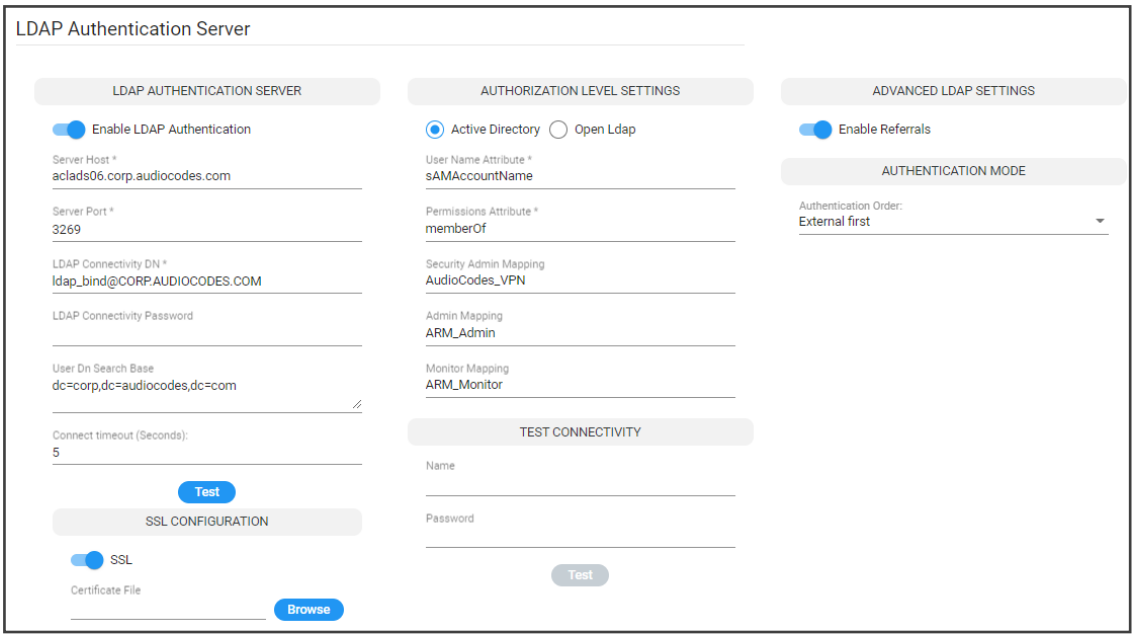
Provisioning Operators using an LDAP Server

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 199.

➢ **To add an LDAP operator login authentication server:**

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

Figure 7-24: LDAP Authentication Server



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	Switch this option on or off to enable or disable operator login authentication using an LDAP-compliant authentication server.
Server Host	Enter the IP address of the LDAP server's host.
Server Port	Enter the LDAP server's port number. Default: 389
LDAP Connectivity DN	Configure the 'LDAP Connectivity DN' parameter as required.
LDAP Connectivity Password	Configure the 'LDAP Connectivity Password' as required.
User DN Search Base	Configure the 'User DN Search Base' as required.
Connect timeout (seconds)	Configure the operator login authentication timeout. Default: 5 seconds.

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

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

Table 7-7: SSL Parameters

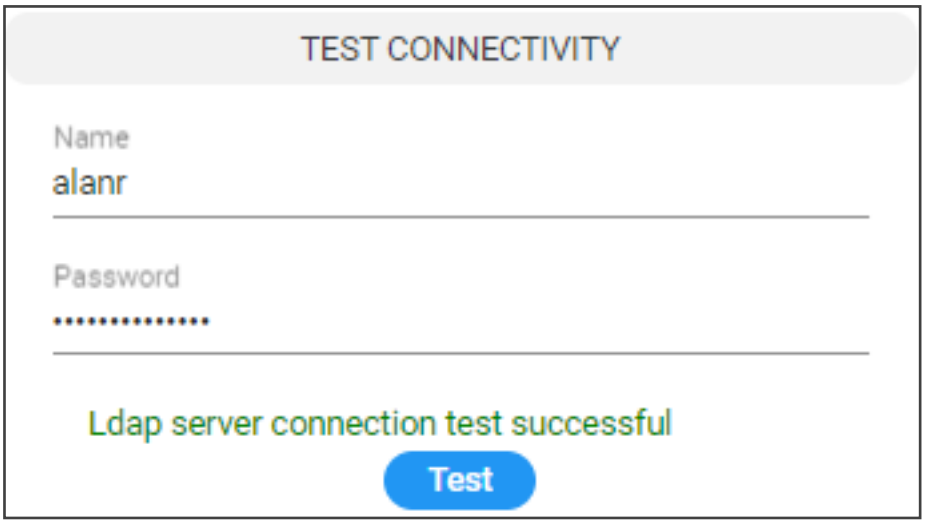
Parameter	Description
SSL	Enable the 'SSL' option to secure the connection with the LDAP server over SSL. If disabled, the connection with the LDAP server will be non-secured.
Certificate file	Click the **Browse** button to browse to and select the certificate file that you want to use to secure the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

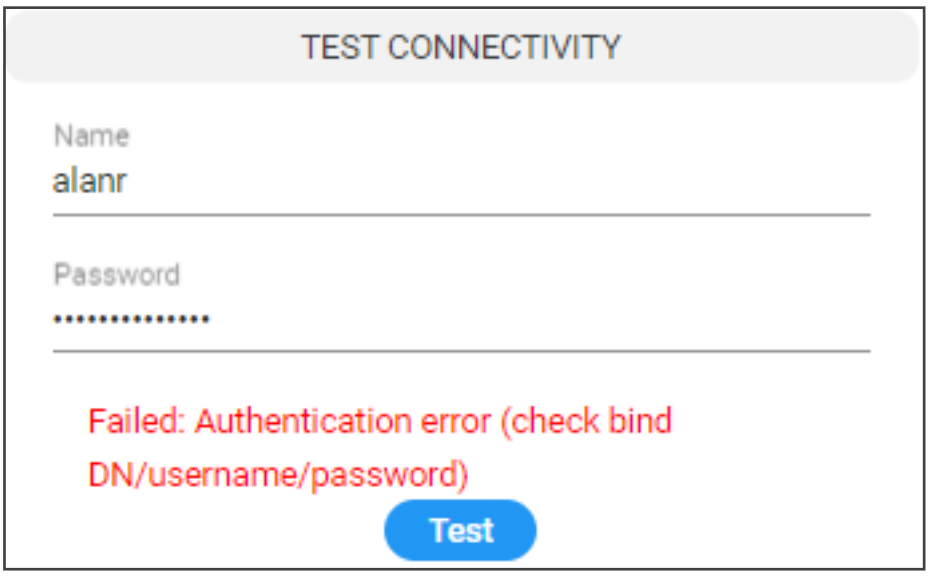
4. Configure the Test Connectivity parameters to test the connection to the LDAP server. Use the following table as reference.

Table 7-8: Test Connectivity

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

Figure 7-25: LDAP Connectivity Test Result





5. View the result of the LDAP server connectivity test; the figure at left shows a successful connection while the figure at right shows a failed test.
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: Authorization Level Settings

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,

Parameter	Description
	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**.

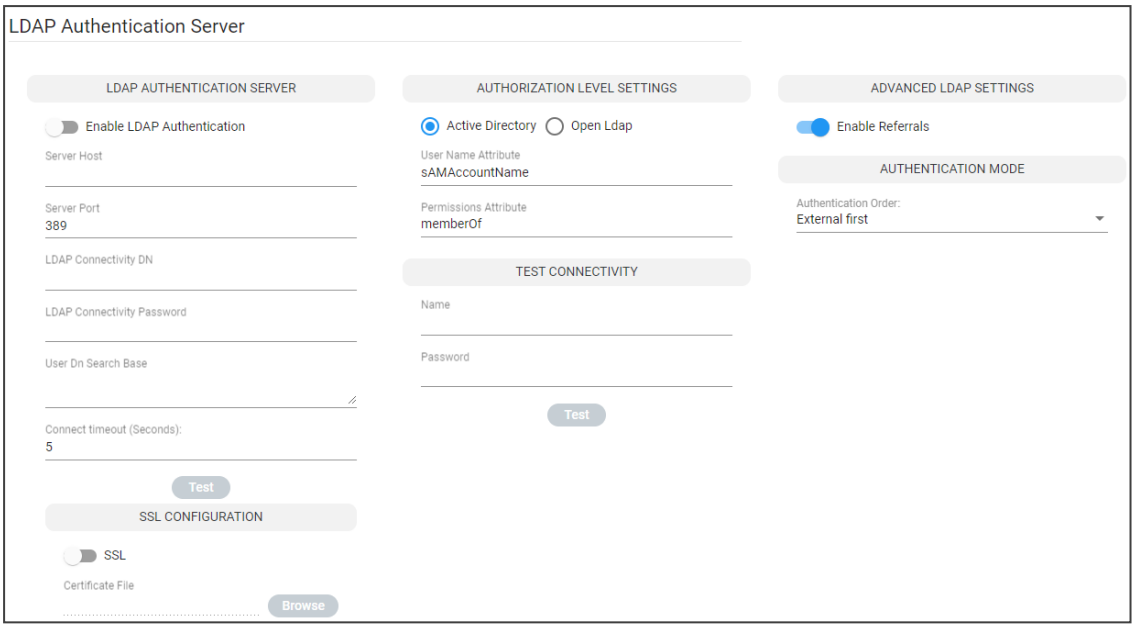
Authenticating Operator Login using Open LDAP

Operator login can optionally be authenticated using Open LDAP.

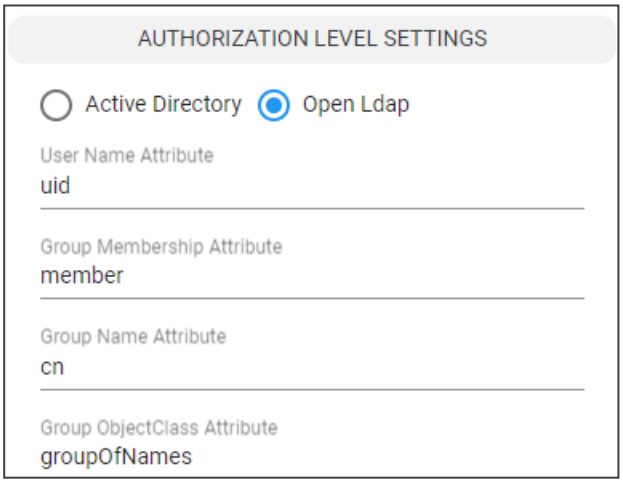
➢ **To configure operator login authentication using Open LDAP:**

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

Figure 7-26: Authenticating Operator Login using Open LDAP



2. Configure the Authorization Level Settings. When **Active Directory** is selected (default), configure:
   a. User Name Attribute [the LDAP attribute used to identify the username]
   b. Permissions Attribute [the LDAP attribute used to identify the user permissions]
3. Select **Open LDAP**.



4. Configure:
   a. User Name Attribute [the LDAP attribute used to identify the username]
   b. Group Membership Attribute [The LDAP attribute used to list the members of the LDAP group]
   c. Group Name Attribute [The LDAP attribute used to identify the LDAP group name]
   d. Group ObjectClass Attribute [The value of the ObjectClass attribute that identifies a user group LDAP object]

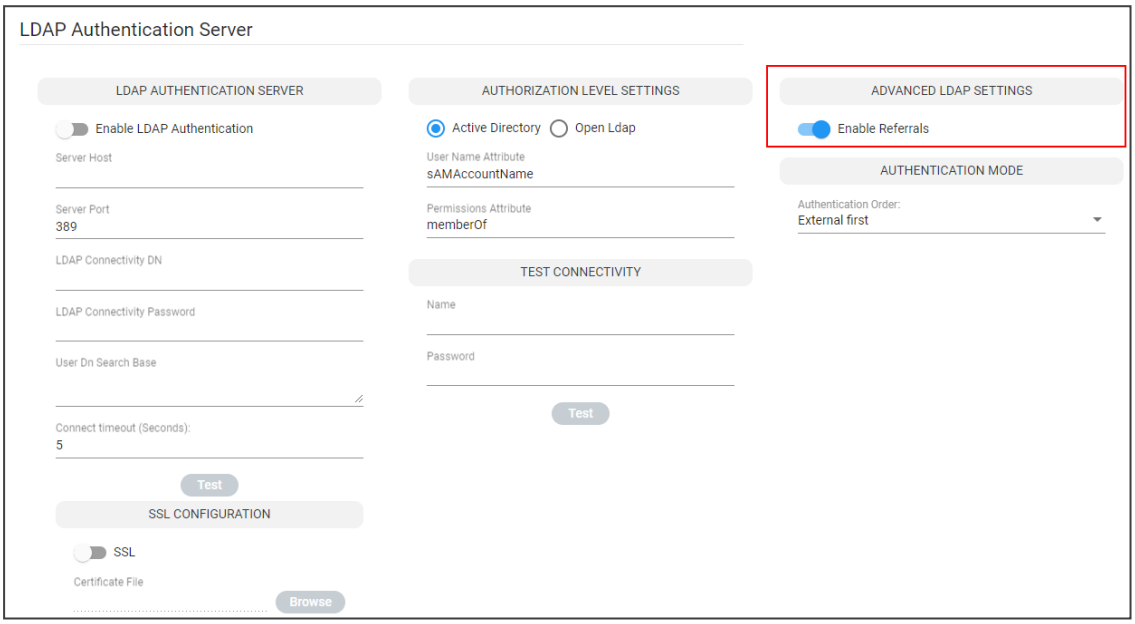
See also Adding LDAP Server to ARM on page 156

See also Advanced LDAP Settings - Enable Referrals below

See also Managing Authentication Order on page 220

Advanced LDAP Settings - Enable Referrals

The LDAP Authentication Server page displays the **Enable Referrals** feature under Advanced LDAP Settings as shown in the figure below.



Enable Referrals is by default enabled.

Applies only to a distributed environment in which directory data is spread across multiple LDAP servers.

- **Enabled** = referrals will be used to direct the LDAP client to another LDAP server or service when the current LDAP server is unable to fulfill a request. When the LDAP server receives a request for data it doesn't have, it will refer the client to another LDAP server that might have that data.
- **Disabled** = referrals will **not** be used to direct the LDAP client to another LDAP server or service when the current LDAP server is unable to fulfill a request. If the LDAP server receives a request for data it doesn't have, it will **not** refer the client to another LDAP server that might have that data.

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 199. 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**).

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

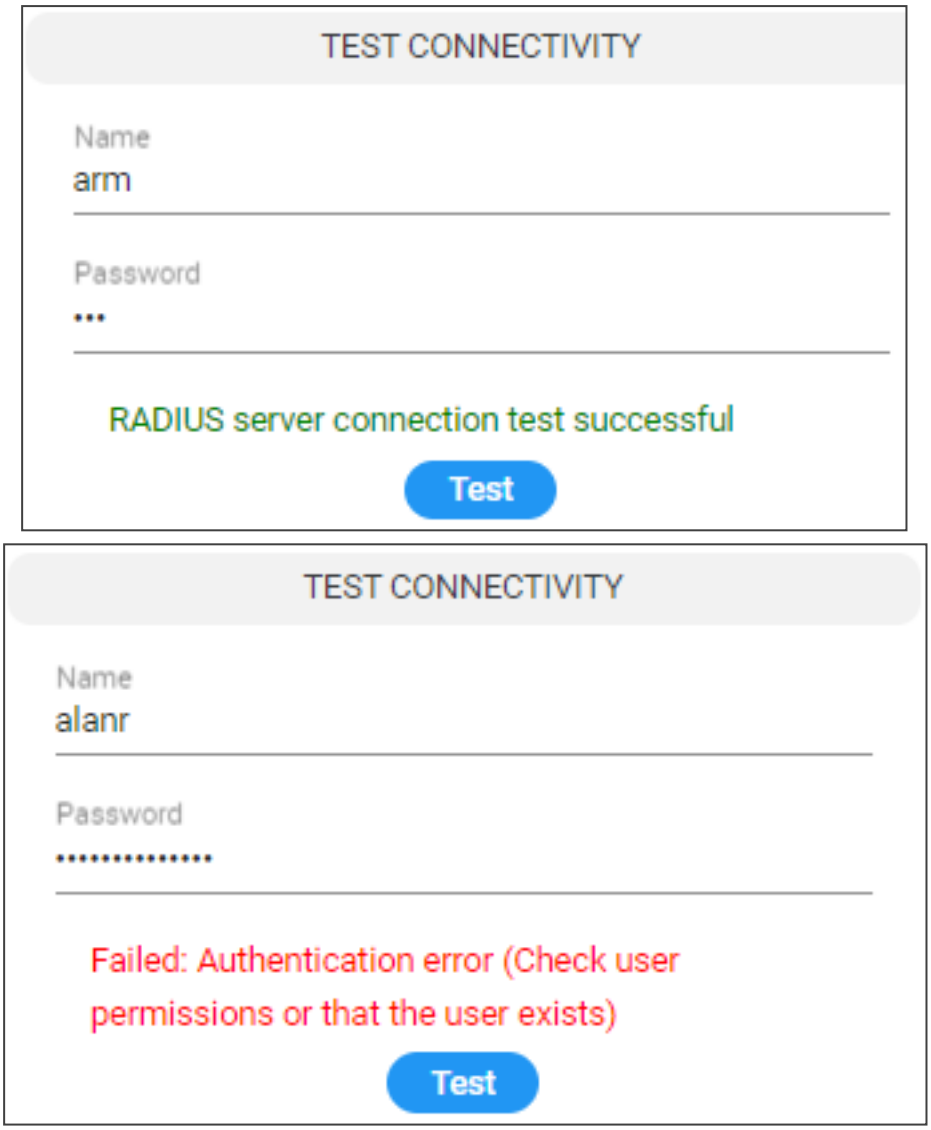
Parameter	Description
	the RADIUS server (i.e., message integrity). By default, no value is defined.
RADIUS retransmit timeout (msec)	If no response is received from the RADIUS authentication server, the ARM Configurator can be configured to *resend packets* to it. Enter the time (in milliseconds) the 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 Security Policy	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]
NAS IP Address	Indicates the IP address of a network access server (NAS). A NAS can be used in the RADIUS authentication process. The NAS acts as the gateway between the user and the wider network. When a user attempts to obtain network access, the NAS passes authentication information (for example, user name and password) between the user and the RADIUS server.
NAS Port	Indicates the physical port number of the network access server.
NAS Identifier	A specific string that identifies the specific NAS server.
Additional attribute name	Option to add another attribute in the RADIUS authentication process. To use this option, enter properties in the field.
Additional attribute value	Option to add another attribute in the RADIUS authentication process. To use this option, enter properties in the field.
Test	Click this **Test** button to test *general connectivity*.

3. Connectivity with the RADIUS authentication server can also be tested for *specific credentials* by clicking the **Test** button located under the screen section 'Test Connectivity', after configuring the Test Connectivity parameters described in the following table.

Table 7-11: Test Connectivity for Specific Credentials

Parameter	Description
Name	If 'Name' is undefined (empty), the connectivity test checks if the RADIUS authentication server can be logged into per the values defined under the 'RADIUS Authentication Server' parameters. If you enter a user name, the connectivity test checks that it's valid for logging into the ARM. Enter the user name assigned to the RADIUS server.
Password	If 'Password' is undefined (empty), the connectivity test checks if the RADIUS authentication server can be logged into per the values defined under the 'RADIUS Authentication Server' parameters. If you enter a user password, the connectivity test checks that it's valid for logging into the ARM. Enter the password required for accessing the RADIUS server.

Figure 7-27: RADIUS Connectivity Test Result



4. View the result of the RADIUS server connectivity test; the figure on the left shows a successful test while the figure on the right shows a failed test.

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

   - RADIUS
   - Local storage (Database)

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

5. Configure authentication order. For more information, see Managing Authentication Order on the next page.

6. Click **Submit**.

Managing Authentication Order

The ARM lets you manage the authentication order for LDAP | RADIUS authentication.

You can define whether the ARM will first check the external service (LDAP | RADIUS), or the local database (the Operators page); the default behavior is to first check the external service.

Change can be applied for each authentication method, depending on which one is used, by navigating in the ARM GUI to:

Settings > **Administration** > **LDAP Authentication**

Settings > **Administration** > **RADIUS Authentication**

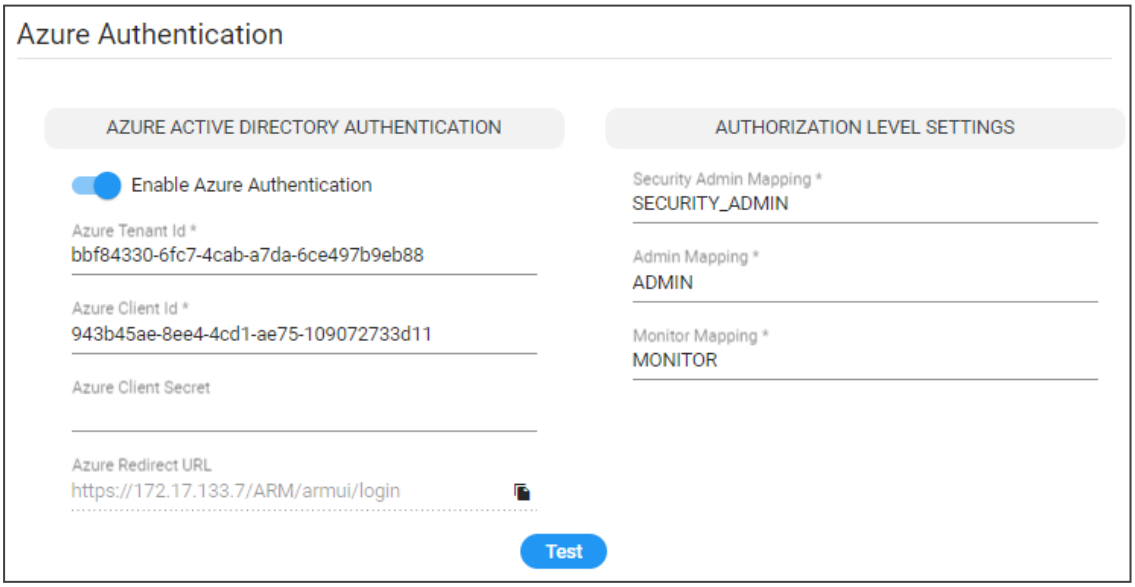
Figure 7-28: Authentication Order

Authenticating Operator Login Using Azure AD

The ARM supports Azure AD for operator login authentication (in addition to support for Azure AD as a source of ARM users). The feature augments local operator login authentication and comes in addition to LDAP and RADIUS authentication.

1. Configure the Azure portal to allow the ARM as a valid application (see Configuring the ARM in the Azure Portal on page 162); Azure AD is added to the ARM in the Azure Authentication page (**Settings** > **Administration** > **Azure Authentication**).

Figure 7-29: Azure Authentication



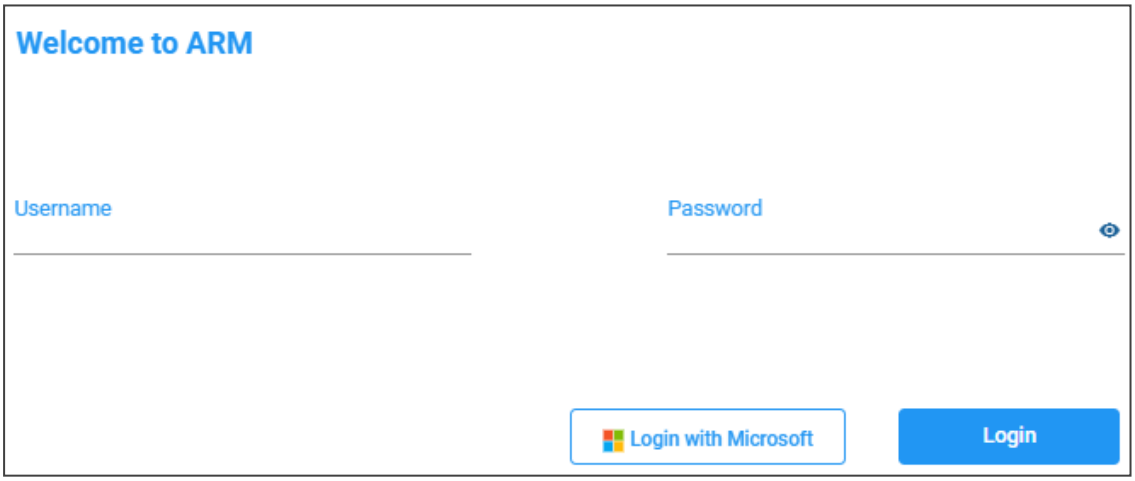
Only operators with a security level of 'Security Admin' can edit Azure Authentication attributes.

2. Test connectivity with Azure AD. Use the **Test** button shown in the preceding figure (available for operators whose security level is 'Admin' or 'Secure Admin').

In the connectivity test, the ARM also validates the Authorization-level mappings; if an Azure AD membership group does not contain the authorization mappings, a warning message is displayed.

3. Under the section 'Authorization Level Settings', map the ARM's access roles ('Security Admin', 'Admin' and 'Monitor') with the Azure AD's app roles.
4. After Azure authentication is enabled, the **Login with Microsoft** button is displayed in the login screen:

Figure 7-30: Login with Microsoft



5. Select **Login with Microsoft**; the browser redirects to the Microsoft login page and after authentication with Microsoft, it redirects back to the ARM GUI. See also Logging in on page 18.

Azure AD for REST Requests Authentication

Operators who operate the ARM using the official ARM REST API can also use Azure AD for authentication.

➢ **To use the ARM REST API with an Azure AD user:**

1. Configuration in Azure portal:

In Azure Active Directory under **Manage** select **App registrations**, select the default ARM application. Under **Manage**, select **Expose an API**:

a. Click **Add a scope**

b. Click **Save and continue**; the default value is created: “api://{client-id}”.

Register your own REST application for REST authentication.

In the **Azure Active Directory** pane, click **App registrations** and choose **New registration**.

In the new application:

c. Create a client secret – as described previously.

d. Add permission to access the default ARM application:

Under **API permissions** click **Add permission**.

Select **my APIs**, select **application** and then select the exposed API previously defined in the app and select the role for the REST authentication (from the app roles defined previously in the application).

Click **Grant admin consent**.

2. Acquire an access token from Microsoft. To acquire access token from Microsoft using REST client:

Send a request to Microsoft Identity platform’s token endpoint, as follows:

```
POST
https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token
```

Using **x-www-form-urlencoded** as ‘Body content type’ and the following ‘Body’ content:

```
grant_type=client_credentials&
client_id=<rest-app-client-id>&
client_secret=<rest-app-client-secret>&
scope = api://<client-id>/.default
```

Replace **tenant-id** and **client-id** with **tenant id** and **client id** of the default ARM application.

Replace **rest-app-client-id** and **rest-app-client-secret** with the **client id** and **client secret** of your own REST application.

A successful response will contain an access token:

```
{
"token_type": "Bearer",
"expires_in": 3599,
"ext_expires_in": 3599,
"access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsI…"
}
```

3. Access ARM’s REST API using the access token:

To access ARM's REST API using the access token, send a Post request with the token received from Microsoft to:

```
POST <ARM_Configurator_IP>/ARM/v1/login/microsoft/authentication/token
```

with the following body:

```
{
accessToken: String,
authenticationType: ACCESS_TOKEN
}
```

The ARM validates the Microsoft access token and generates an ARM token with the received role.

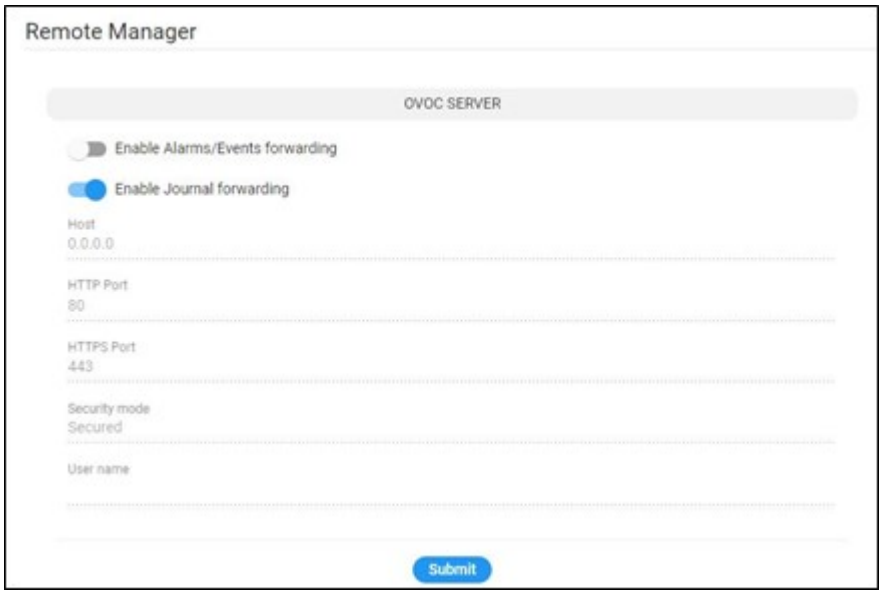
4. In any REST Request to the ARM, use the received token in the authorization Header like this:

Figure 7-31: Authorization Header

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**).



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**.

  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.

In addition to the option to send alarms to the OVOC, the ARM also supports the option to send all Journal data to the OVOC.

➢ **To enable Journal data to be sent to the OVOC:**

- Drag the **Enable Alarms/Events forwarding** slider to the 'on' position and click **Submit** as shown in the preceding figure.

> As with sending alarms/events, the OVOC must be configured to get Journal data from ARM.

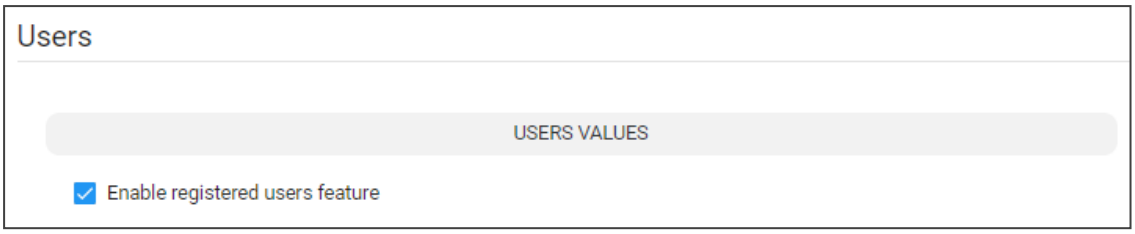
Adding Registered Users to the ARM

SBC registered users can be added to the ARM for the ARM to then be capable of performing call routing based on SBC user registrations. Each SBC has its own registered users. The added SBC registered users and their related information will be viewable in the ARM's Registered Users page shown in Viewing Registered Users in the ARM on page 152. To add registered SBC users to the ARM, operators need to first enable the feature as shown below. After the feature is enabled, the SBC registered users and their related information are taken from the SBC and added to the ARM. Later, when defining a Routing Rule, for example, operators can then route calls to SBC registered users (see Adding a New Routing Rule on page 328). The destination to which to route the call will depend on where - which SBC - the user performed the registration. In the Routing Rule definition, operators will select the appropriate routing condition, namely, that the call destination is an SBC registered user.

➢ **To add SBC registered users to the ARM:**

1. Open the Users page (**Settings** > **Advanced** > **Users**).

Figure 7-32: Users



2. Make sure the 'Enable registered users feature' option is selected and then click the **Submit** button.

Defining a Statistics Retention Policy

The ARM allows operators to store statistics for up to a maximum of one year (365 days). The statistics are collected every five minutes per Network Topology element and are displayed in the ARM GUI by graphs which help operators analyze network routing.

The statistics are collected by the Routers. The Configurator samples them every five minutes. Session statistics are calculated by the Configurator itself.

➢ **To define how long statistics will be stored:**

1. Open the Statistics page (**Settings** > **Advanced** > **Statistics**).

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

Table 7-12: Statistics

Parameter	Description
Number of days to keep calls quotas statistics	Allows the network operator whose security level is 'Administrator' to configure how long the ARM will store calls quotas statistics, in days. The value can be changed to a value in the range of 90-365. The default is 365 days.
Number of days to keep statistics	Allows the network operator whose security level is 'Administrator' to configure how long the ARM will store statistics records, in days. The value can be changed to a value in the range of 31-365. The default is 365 days.

The maximum number of days the statistics graph can be displayed is 31 days.

Network Services Settings

The Syslog Server configuration settings can be edited as shown in Editing a Syslog Server below.

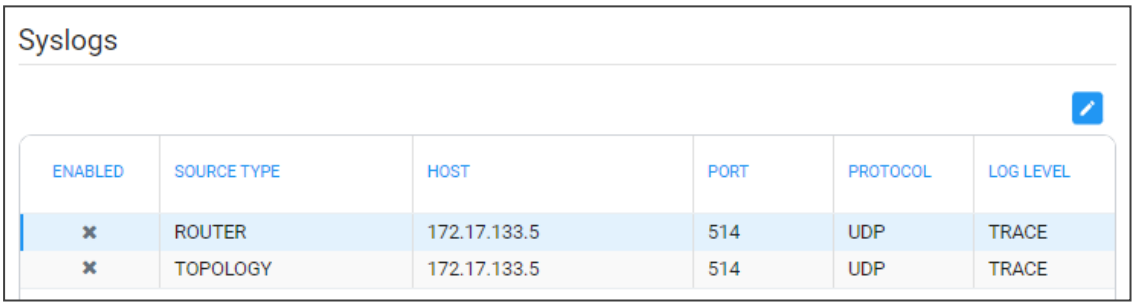
An NTP server can be added and its configuration settings edited as shown in Adding / Editing an NTP Server on page 228.

Editing a Syslog Server

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

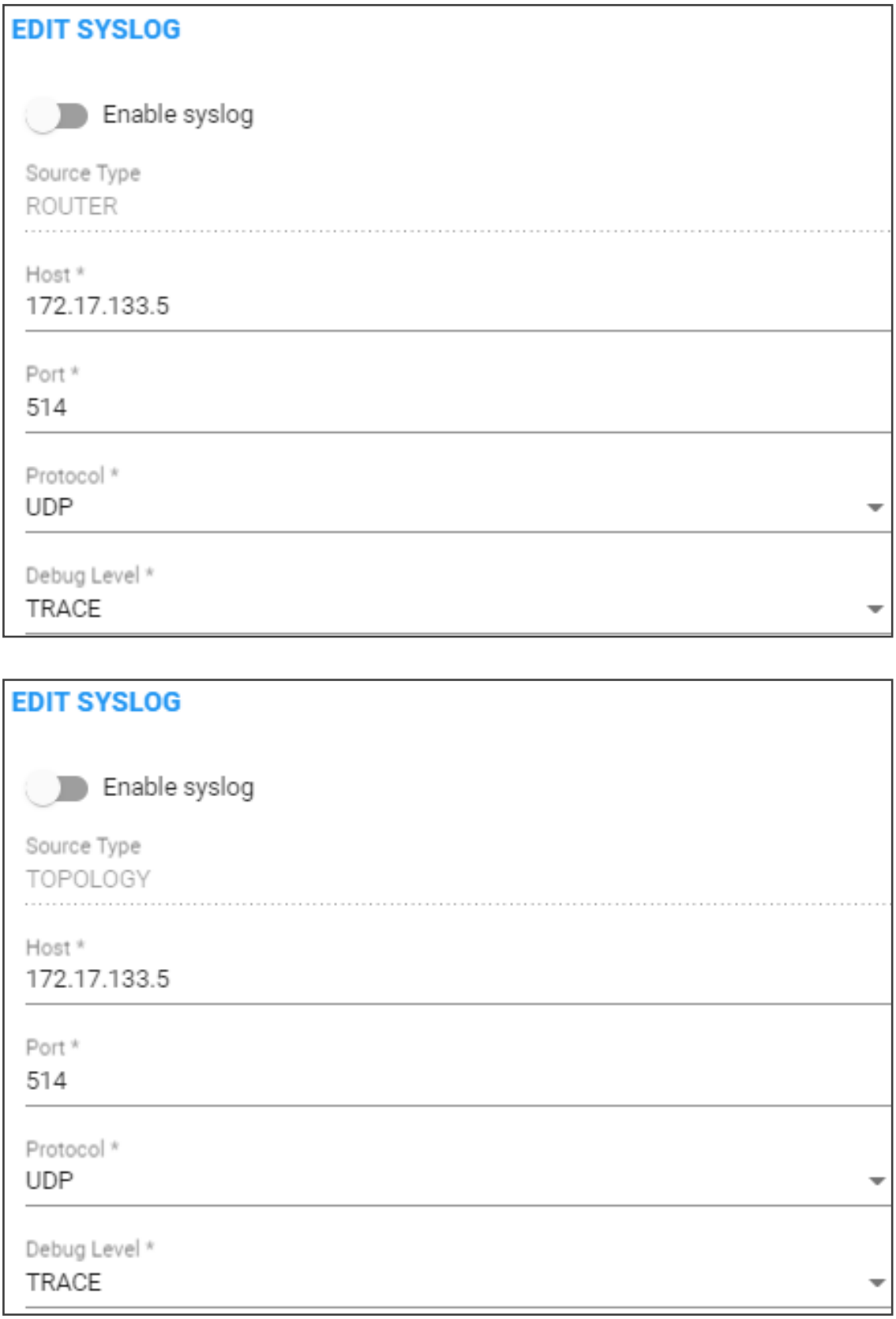
➢ **To edit a Syslog Server:**

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



2. Select the Router or Topology row and then click the **edit** icon.

Figure 7-33: Edit Syslog



3. Use this table as reference.

Table 7-13: Edit Syslog

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) ■ INFO ■ WARN ■ ERROR

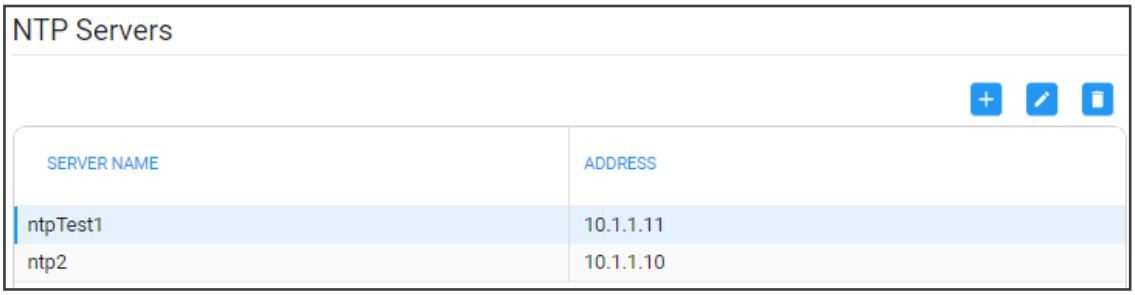
When enabling syslog for a Router, there's a single syslog server for all Routing servers in the ARM. All ARM Routers send their syslog to this syslog server (at the same 'Debug Level'). This is necessary for proper calls debugging, as a single call can be processed by several different ARM Routers (they are state-less). For the ARM Configurator, however, you can assign a different syslog server.

Adding / Editing an NTP Server

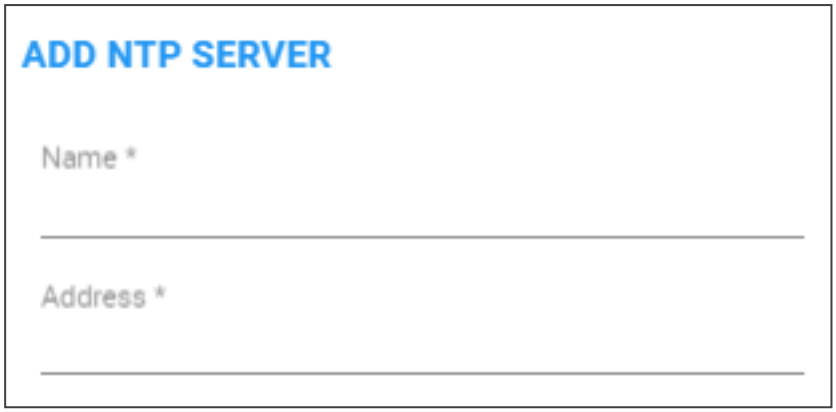
An NTP server can be added to the ARM and its configuration settings can be edited.

➢ **To add an NTP server:**

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



2. Click the add **+** icon.



3. Configure the NTP server settings using the following table as reference. The same settings are displayed when editing the server.

Table 7-14: Add NTP Server

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 7-15: Protocols Mapped to Class of Service

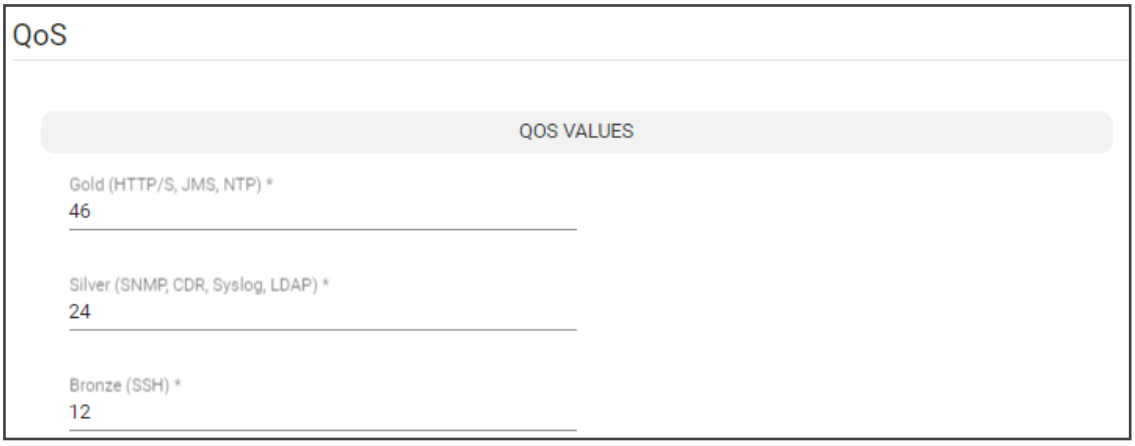
Application Protocol	Class of Service (Priority)	Traffic Type
HTTP/HTTPs	Gold	■ Signaling/Control ■ Communication between node and ARM Configurator, node and ARM Configurators ■ Some communication between ARM Routers and ARM Configurator
JMS	Gold	Management affecting signaling. Critical communication

Application Protocol	Class of Service (Priority)	Traffic Type
		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 7-34: QoS



2. Configure QoS values using this table as reference.

Table 7-16: QoS Settings

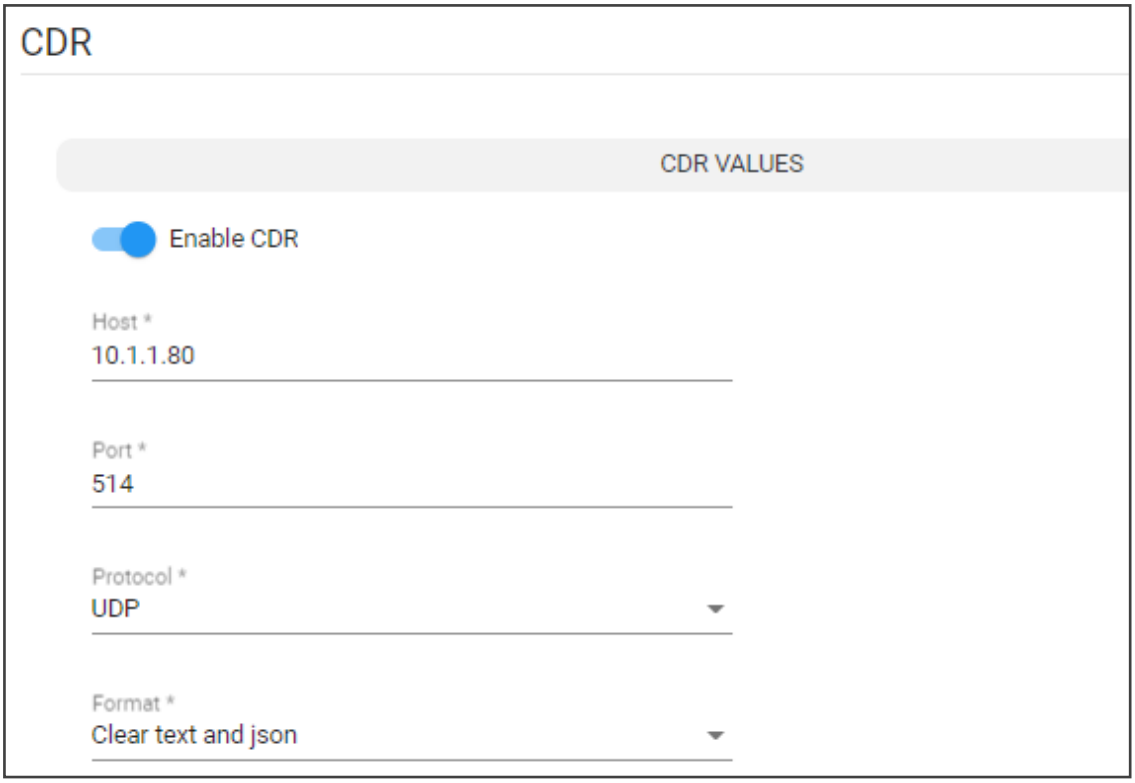
Setting	Description
Gold	[Application protocol: HTTP/S, JMS, NTP] You can change the default value of 46 to suit the requirements of your IP network. As part of IP network planning and optimization, the value can be changed to a value in the range between 0-63. The value determines priority of IP packets 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**).



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

Table 7-17: 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.

Enabling WebSocket Tunnel

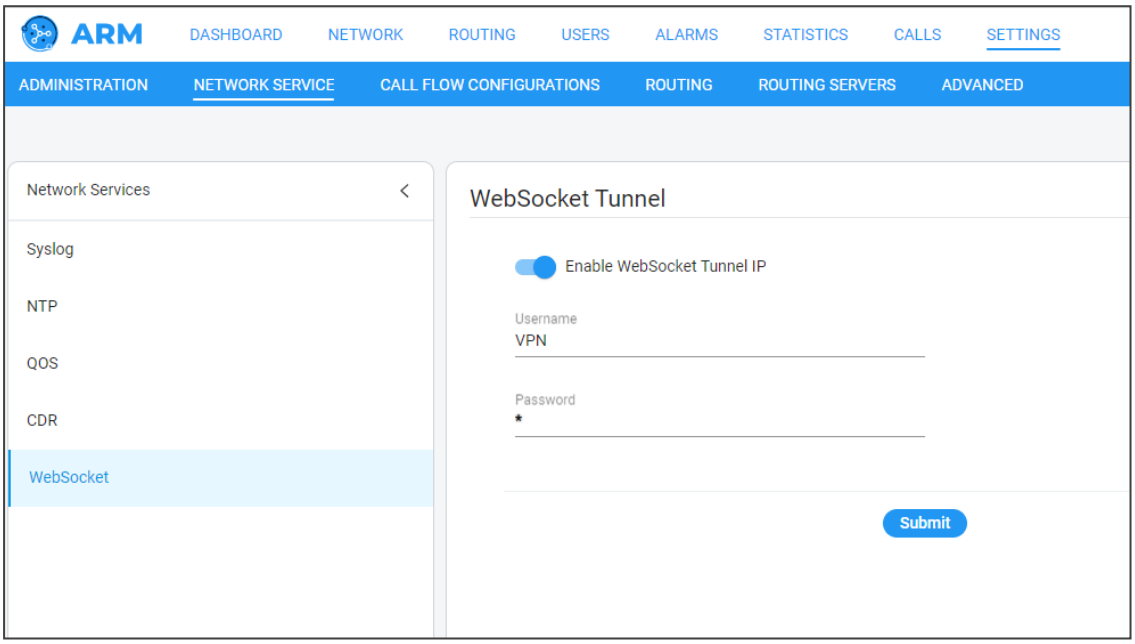
Communication between the ARM Router and the ARM Configurator may optionally be configured to use WebSocket Tunnel (VPN). This will enable deployment of Router instances in a Network Address Translation (NAT) environment. The Configurator and Routers will establish a new "overlay network". The address range known as "link local address" range, 169.254.0.0/18, will be used by this network. While every ARM Router in this network will have a unique address, the ARM Configurator will always be allocated 169.254.0.1.

➢ To enable WebSocket Tunnel:

> WebSocket Tunnel needs to be enabled in both the Configurator and the Router. It's accomplished through the UI on the Configurator side and a script on the Router side.

➢ To enable WebSocket Tunnel in the Configurator:

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



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

Setting	Description
Enabled	Select or clear the option to enable or disable WebSocket Tunnel.
Username	Enter the WebSocket Tunnel username.
Password	Enter the WebSocket Tunnel password.

➢ To enable WebSocket Tunnel in the Router

> It's possible to enable WebSocket Tunnel on both new and existing Routers. Regarding a new Router, the new Router will be added by the Configurator once the WebSocket Tunnel has been established.

1. Log into the Router using SSH.
2. Switch user to root by "su –"
3. Enter the root password.

4. Validate the activity of the Router by using the following command:

```
systemctl is-active tomcat.service
```

5. If the Router isn't active, execute the following command:

```
systemctl start tomcat.service
```

6. To run the WebSocket Tunnel script, execute the following command:

```
websocket_arm --start
```

7. Answer **y** to enable WebSocket Tunnel or **n** to quit.
8. Enter the IP address of the ARM Configurator.
9. Enter the username to match the WebSocket Tunnel username configured on the ARM Configurator. The default username is "VPN" (without quotation marks).
10. Enter the password to match the WebSocket Tunnel password configured on the ARM Configurator. The default password is "123456" (without quotation marks).
11. Enter the REST username to match the Configurator Credential username (Router type) configured on the ARM Configurator.
12. Enter the REST password to match the Configurator Credential password (Router type) configured on the ARM Configurator.
13. Enter the IP address of the Router itself.

```
[root@router ~]#
[root@router ~]# websocket_arm --start
Starting
Do you want to enable WebSocket Tunnel? ([y]/n): y
Enable WebSocket Tunnel for ARM Live
Enter the Configurator host []: 172.17.133.163
Enter the username of the web_socket [default username]: VPN
Enter the password of the web_socket [default password]: 123456
Enter the Configurator HTTP user name [Router]: Router
Enter the Configurator password [default password]: Pass_1234
Enter the Router host []: 172.17.133.166
 Enabling tun-ws-client service
 Starting tun-ws-client service
 WebSocket connected (169.254.0.6)
End
[root@router ~]#
```

14. Check the WebSocket Tunnel Router status:
    - Execute the following command:

```
websocket_arm --status
```

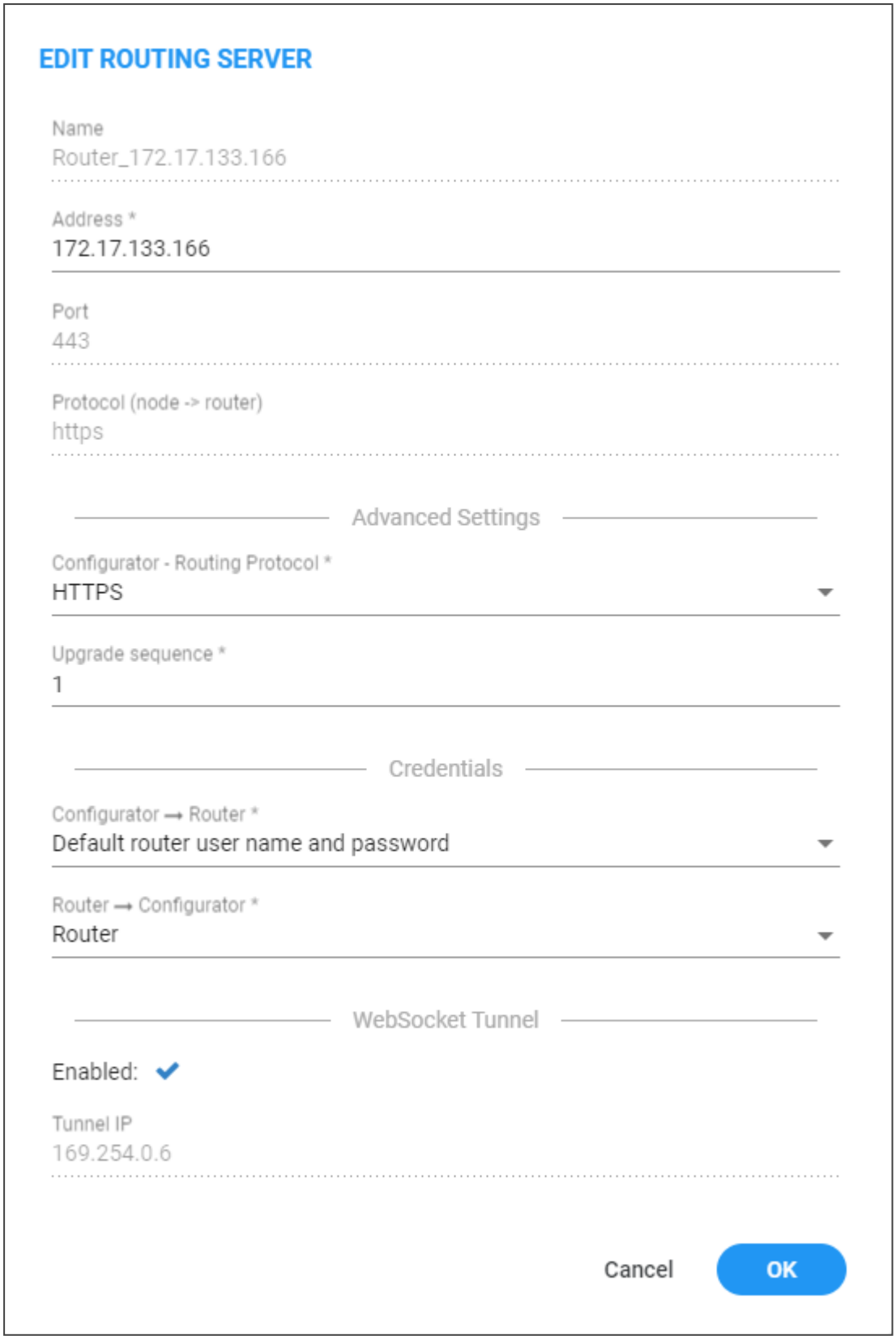
```
[root@router ~]#
[root@router ~]# websocket_arm --status
WebSocket Tunnel Status:
 Enabled: true
 Connected: True
 Ip Address: 169.254.0.6
[root@router ~]#
[root@router ~]#
```

15. Check the WebSocket Tunnel Router status in the Configurator:

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

    b. Select the Router configured to WebSocket Tunnel and then click the edit icon.

    c. Make sure the WebSocket Tunnel is enabled and the Router has a Tunnel IP Address.



➢ **To disable WebSocket Tunnel in the Router:**

1. Log into the Router using SSH.
2. Switch user to root by "su –"

3. Enter the root password.
4. Validate the activity of the Router using the following command:

```
systemctl is-active tomcat.service
```

5. If the Router isn't active, execute the following command:

```
systemctl start tomcat.service
```

6. To run the WebSocket Tunnel script, execute the following command:

```
websocket_arm --stop
```

7. Answer **y** to disable WebSocket Tunnel or **n** to quit.

```
[root@router ~]#
[root@router ~]# websocket_arm --stop
Starting
You are going to disable WebSocket Tunnel. Are you sure? (y/[n]): y
Disable WebSocket Tunnel
 Disabling tun-ws-client service
 Stoping tun-ws-client service
End
[root@router ~]#
```

8. Check the WebSocket Tunnel Router status in the Configurator:
   a. Open the Routing Servers page (**Settings** > **Routing Servers** > **Servers**).
   b. Make sure the WebSocket Tunnel is disabled for that Router and that its status is enabled.

➢ **To disable WebSocket Tunnel in the Configurator:**

1. Open the Routing Servers page (**Settings** > **Routing Servers** > **Servers**) and make sure there are no Routers configured to WebSocket Tunnel.
2. Open the WebSocket page (**Settings** > **Network Services** > **WebSocket**) and turn off the 'Enable WebSocket Tunnel IP' parameter.

Call Flow Configurations

The ARM's **Call Flow Configurations** tab under the Settings menu allows operators to configure

- Normalization Groups (see Adding a Normalization Group on the next page)
- Prefix Groups (see Adding a Prefix Group on page 240)
- Normalization before Routing (see Normalization Before Routing on page 245)
- Policy Studio (see Policy Studio on page 246)

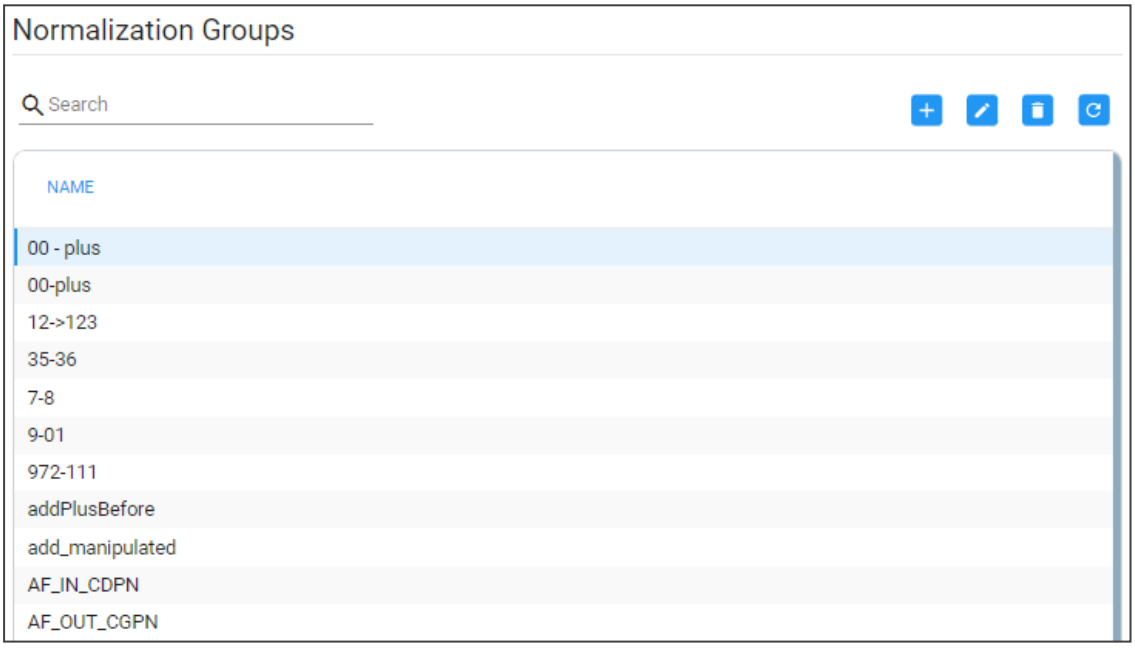
- Web Services (see Web-based Services on page 269)
- SIP Condition Group (seeAdding a SIP Condition Group on page 283)
- SIP Manipulation Group (see Adding a SIP Manipulation Group on page 286)

Adding a Normalization Group

Network administrators 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** > **Call Flow Configurations** > **Normalization Groups**).



2. Click the add **+** icon.

3. Click the **+** icon.

4. Use the following table as reference.

Table 7-18: Normalization Groups

Setting	Description
Name	Enter a group Name for intuitive future reference.
Regular Expression / Replace By / Description	1. Click the **+** icon 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 399. 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 inform-

Setting	Description
	ation. 4. Enter a description for the convenience of operators managing the network.
Test string	Use this feature 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 under 'Simulation Result'.

After a Normalization Group is defined, you can attach it to a:
- Peer connection (see Peer Connection Information and Actions on page 48).
- Globally (see Normalization Before Routing on page 245)
- Routing Rule action (see Adding a New Routing Rule on page 328)
- LDAP attribute (see Adding LDAP Server to ARM on page 156)

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 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 328 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.

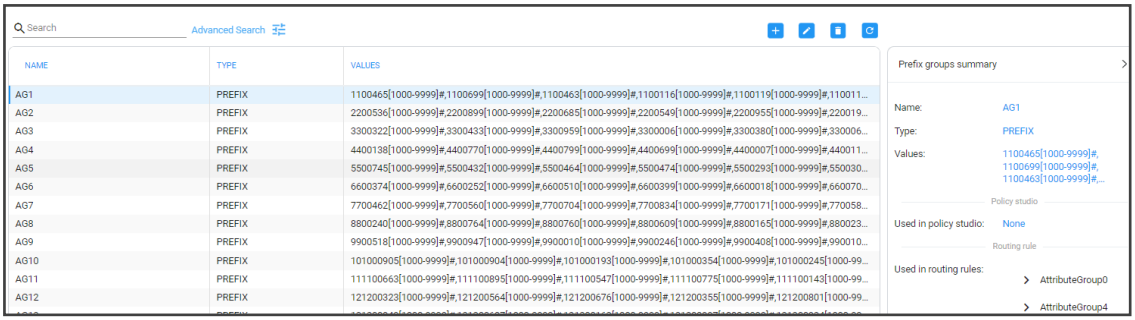
To develop a customer-specific Dial Plan into an ARM Prefix Group, the REST API is available. This can significantly facilitate ARM provisioning.

Adding a Prefix Group

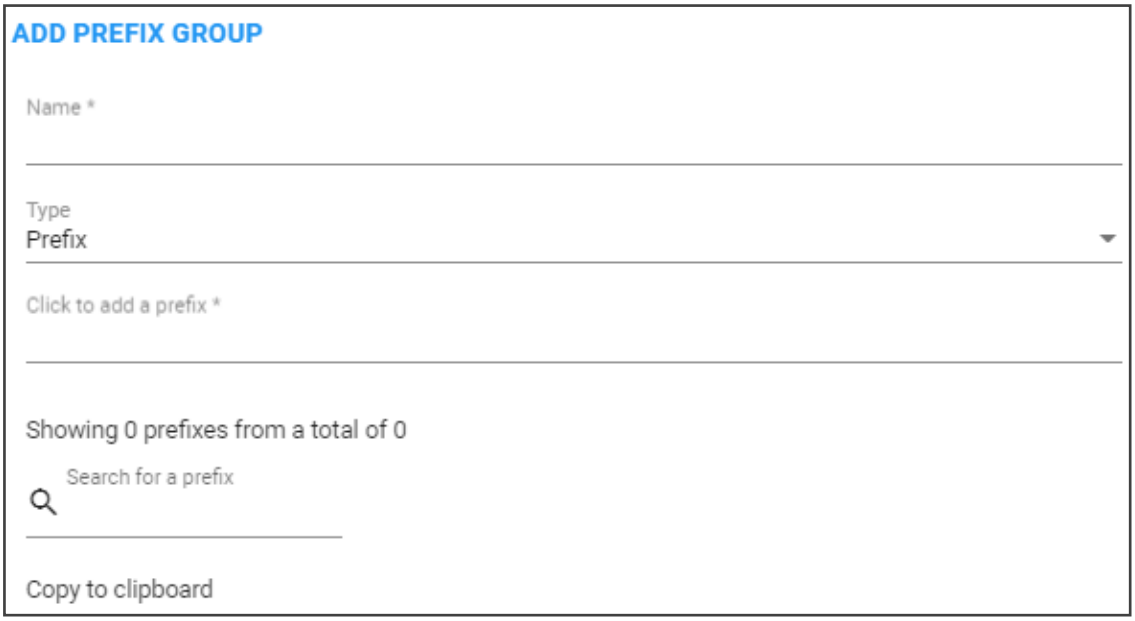
The ARM conveniently allows network operators to add a Prefix Group.

➢ **To add a Prefix Group:**

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



2. Click the add **+** icon.



3. Define a Prefix Group using the following table as reference.

Table 7-19: Add Prefix Group

Setting	Description
Name	Enter a name for the prefix group; the **OK** button is activated.
Type	Filter; from the drop-down select **Prefix** or **Pool of Numbers**. ■ **Pool of Numbers**: DID and emergency calls ■ **Prefix**: All the rest
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 398 for more information). ✓ Multiple prefixes can be copied from an external file and pasted into this field.

Setting	Description
	✓ Using the 'Copy to clipboard' feature, you can copy multiple existing prefixes in this field to the clipboard and then paste into an external file where you can view (for example) all prefix strings at once or count (for example) how many prefixes exist in the group.

4. Click **OK**; the Prefixes Group is created.
   - Associate the group with a rule's condition in the Routing page
   - The group can be associated with Source, Destination or both.

Searching for a Prefix Group

The telephony network may include dozens of prefix groups and multiple prefixes within each group. The 'Enter search string' field in the Prefix Groups page allows the operator to quickly locate a group. After locating a group, the operator can view it and/or edit it.

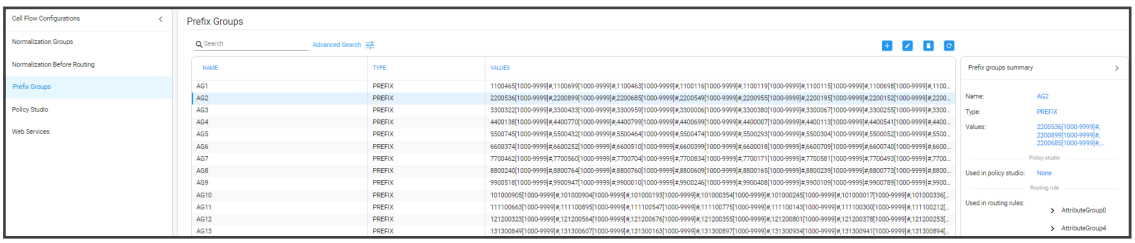
See also Validating Prefix or DID Uniqueness on page 244.

Searching for a Specific Prefix within a Prefix Group

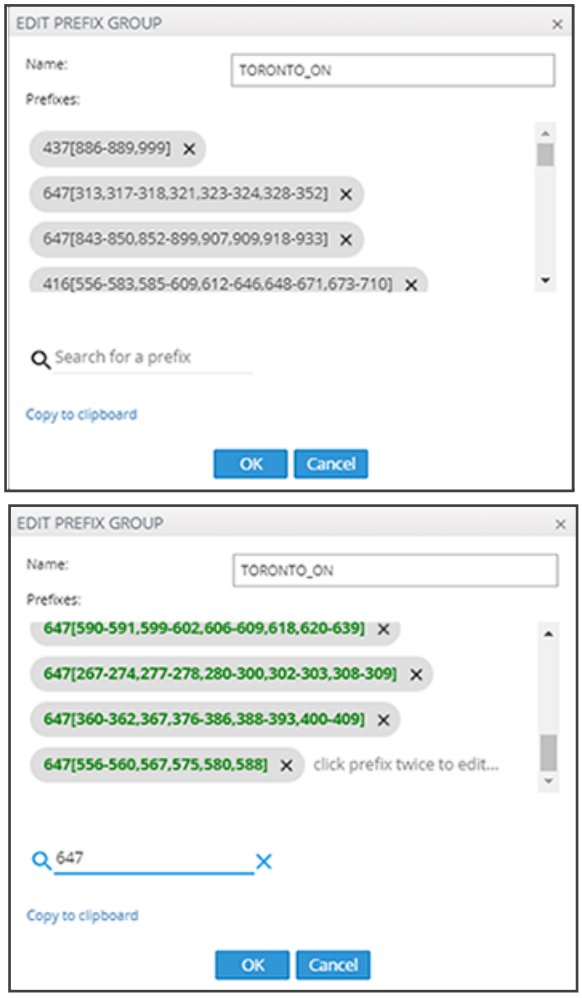
After locating a group in the Prefix Groups page using the 'Enter search string' field (for example), the operator can conveniently search in that group for a specific prefix (string).

➢ To search for a specific prefix in a group:

1. In the Prefix Groups page (**Settings** > **Call Flow Configurations** > **Prefix Groups**), select the group to search in.



2. Click the edit icon.



3. In the 'Search for a prefix' field, define the string to search for and then 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 398 for more information.

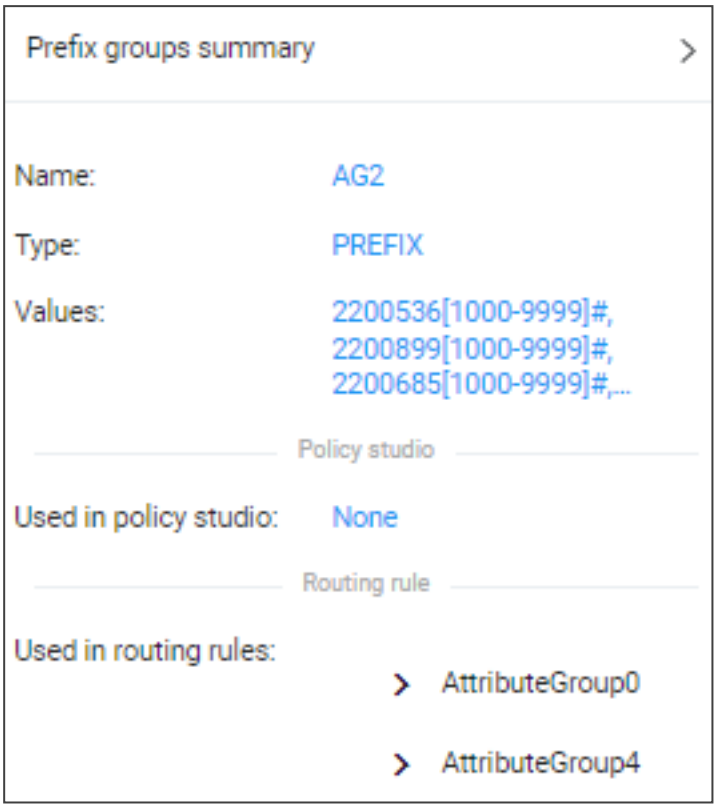
Viewing the Details of the Prefix Group Used for Routing

The ARM helps you determine what Prefix Group is used for routing. As deployment of the ARM has expanded, customer-managed dialing plans have grown more and more extensive (many Prefix Groups are being used in hundreds of Routing Rules and Policy Studio definitions). Sometimes, it's difficult to understand why a specific Routing Rule was selected by the ARM for Call Routing and where a specific Prefix Group is being used.

For this reason, in addition to the **Exact Match** DID search described in Validating Prefix or DID Uniqueness on the next page, the ARM gives operators a detailed description of the selected

Prefix Group used in ARM routing. It covers both Policy Studio (pre-routing mechanism) and Routing Groups/Routing Rules.

When a Prefix Group is selected, its summary is displayed on the right side of the page:



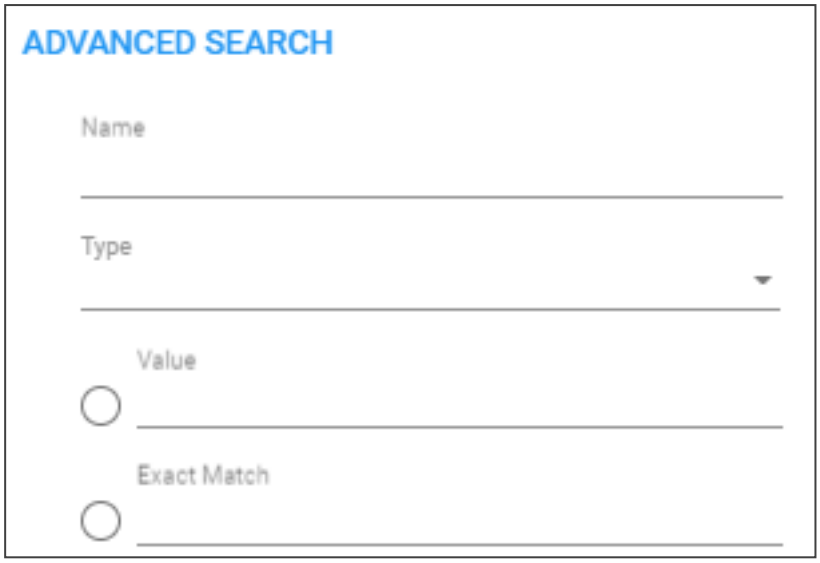
If the selected Prefix Group is not used in Policy Studio, Policy Studio will be indicated as 'None'. The same applies to Routing Groups. If a Prefix Group is used in multiple Routing Groups, all of them will be listed.

Validating Prefix or DID Uniqueness

The ARM helps validate a prefix or a specific DID. As deployment of the ARM has expanded, customer-managed dialing plans have grown more and more extensive (many Prefix Groups with hundreds of prefixes, or complete phone numbers in a single group). Sometimes, it's difficult to preserve the uniqueness of a specific DID (or prefix) definition so you may sometimes erroneously define Routing Rules with a specific prefix (or DID) but the same prefix (or DID) matches a different Prefix Group / Routing Rule.

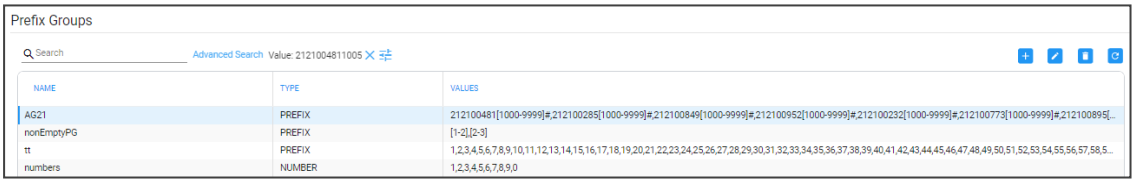
➢ **To validate if a specific DID (phone number) is part of an existing Prefix Group:**

1. Open the Prefix Groups page (**Settings** > **Call Flow Configurations** > **Prefix Groups**).
2. Search for the 'Name' of a Prefix Group, filter its 'Type' and search for an exact string ('Value') if it appeared as part of the Prefix Group.
3. Click the Advanced Search link, select the **Exact Match** option to find all Prefix Groups that match the exact phone number.



The **Exact Match** option finds a number even if it fits a 'range' or another pattern in the Prefix Group. In the following example, an **Exact Match** search was applied for DID **2121004811005** and was found as part of Prefix Group **AG21** (for example) because it's in the range **212100481[1000-9999]#**.

Figure 7-35: Advanced Search Results



Normalization Before Routing

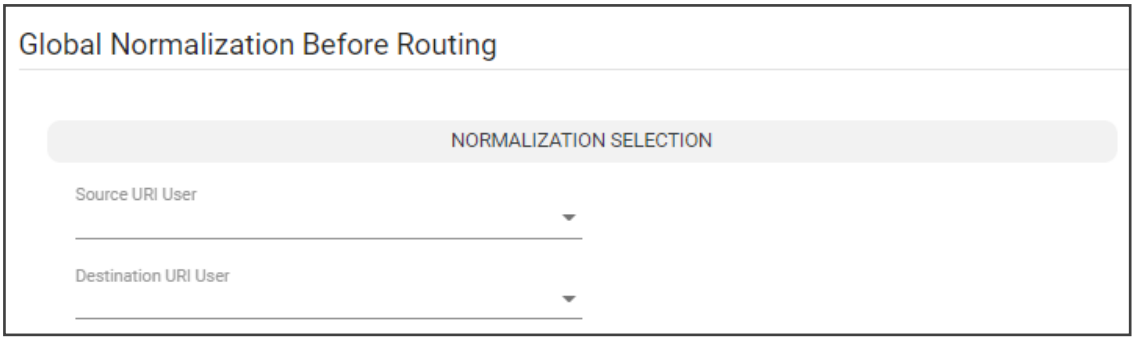
A normalization rules group can be applied to a routing request's source user part and to a routing request's destination user part. See Adding a Normalization Group on page 238 for information on how to add a normalization rules group.

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 48).

➢ **To attach a normalization rules group globally before routing:**

1. Open the Normalization Before Routing page (**Settings** > **Call Flow Configurations** > **Normalization Before Routing**).



2. Use the following table as reference.

Table 7-20: Normalization Before Routing

Setting	Description
Source URI User	From the drop-down menu, select the normalization rules group. This will be the normalization on the Source URI User field.
Destination URI User	From the drop-down menu, select the normalization rules group. This will be the normalization on the Destination URI User field.

3. Click **Submit**.

Policy Studio

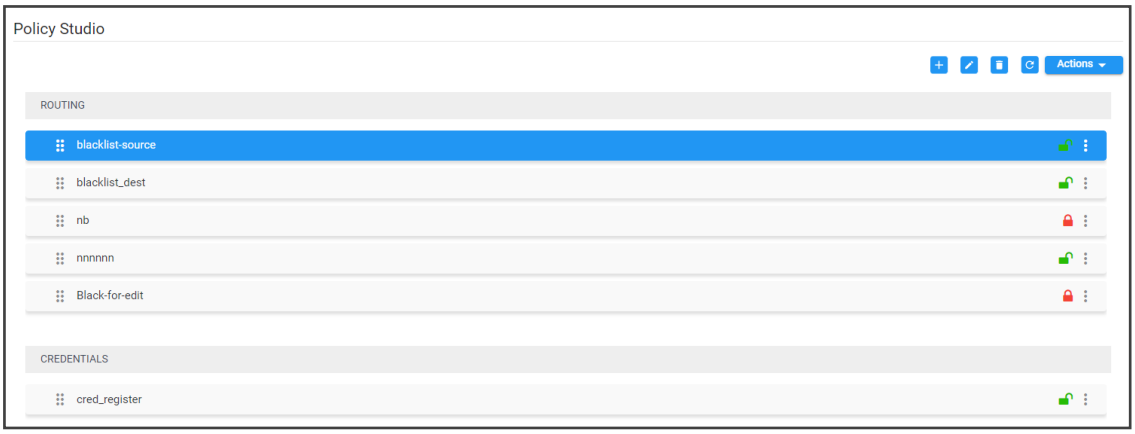
This feature allows adding to route requests information that is not contained in the route requests but which is taken from the Users page. To accomplish this with legacy products without ARM, the LDAP server must be queried for every call using complex query rules, creating delays and straining the server. In the ARM, the Users page is loaded to memory and information gathering is handled internally in real time. Policy Studio Use Examples:

- Each user has an internal 4-digit extension and an unrelated external phone number. When a user makes a call outside the enterprise, the source number, i.e., the user's extension, must be replaced with their external number. When a call comes in from outside, the external number must be replaced with the user's extension.
- Same as the previous example but, in addition, there can be more than one user with the same extension, and what differentiates them is their hostname. The ARM can locate the user based on a combination of the extension and hostname attributes.

Policy Studio is a set of rules. Each rule contains a match condition and an action. The match condition is a set of route request fields to be compared, and a set of user properties to be compared to. The match condition also has a source node or Peer Connection or set of source nodes or Peer Connections. The action is a set of route request or response fields to be replaced, and a set of user fields to replace them with. For every route request received, the ARM processes all the rules from top to bottom. For each, the ARM searches in the users table for a user that matches all the fields. If a user is not found, the ARM proceeds to the next rule. If a user is found, the ARM stops parsing the rules and performs the action in this rule. The action is to replace all the listed fields with the properties of the user, as configured.

➢ To add a Policy Studio rule:

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



2. Click the add icon **+** and from the 'Type' drop-down, select **User**, **Web Service**, **Credentials**, **Blacklist** or **DIDs Count**:

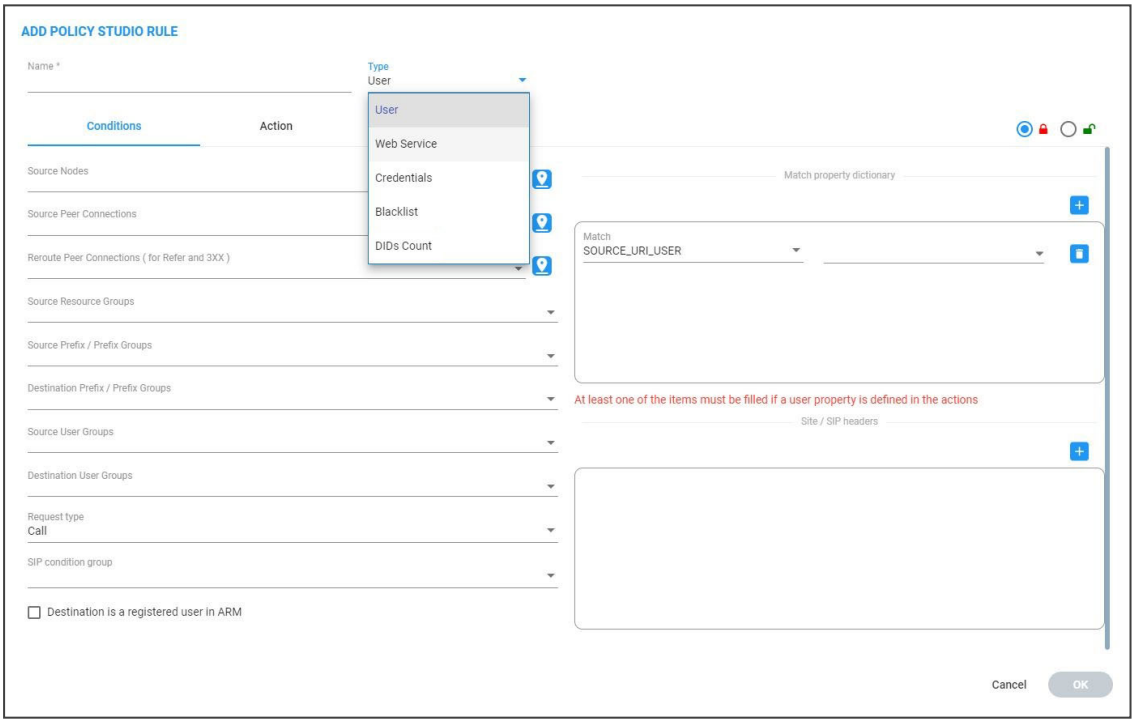


Figure 7-36: Web Service

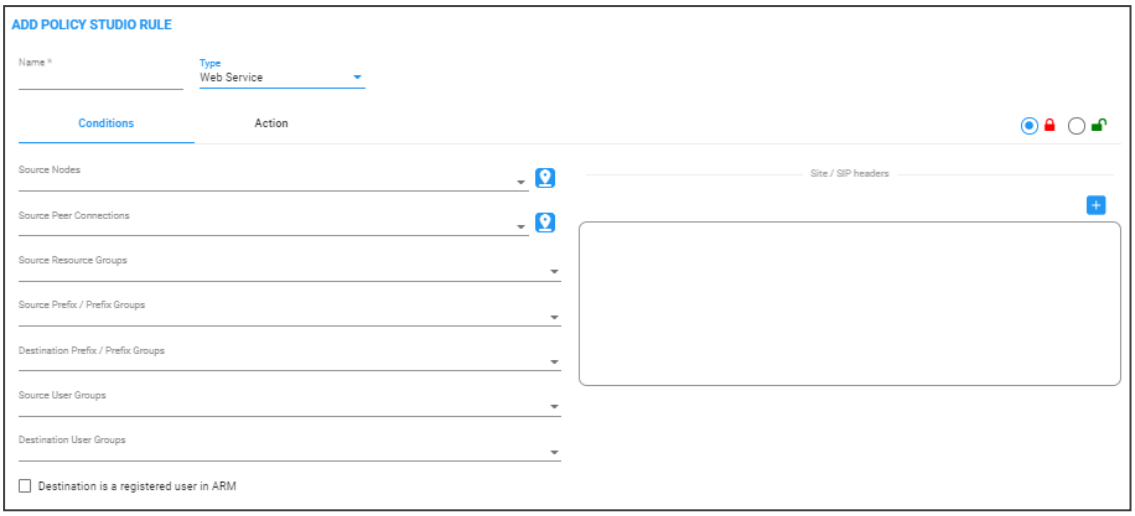


Figure 7-37: Credentials

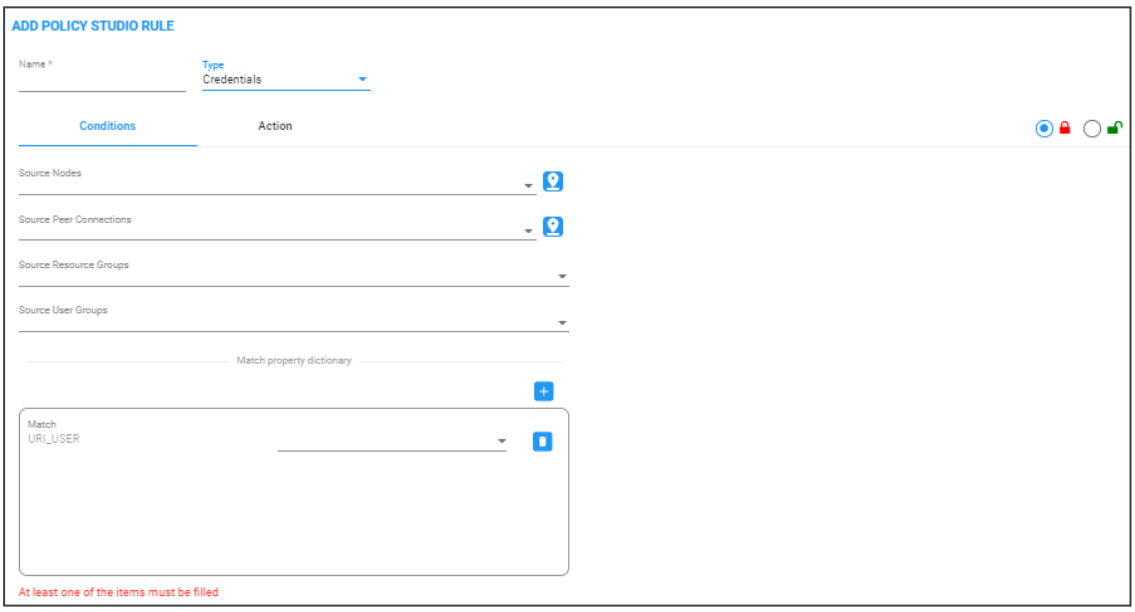


Figure 7-38: Black List

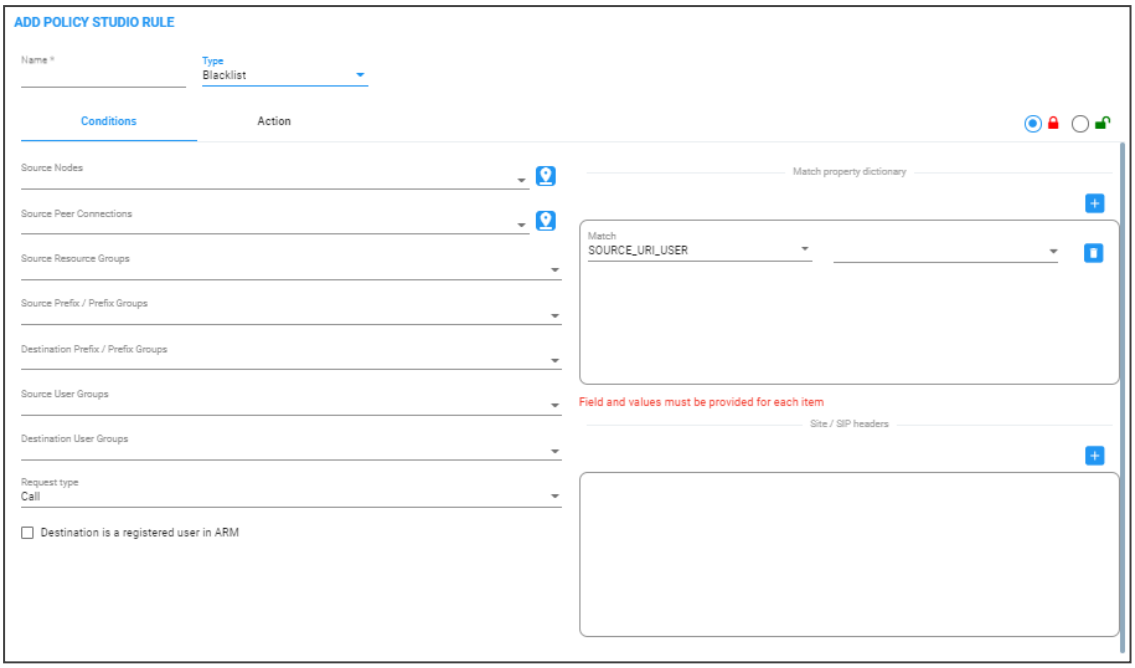
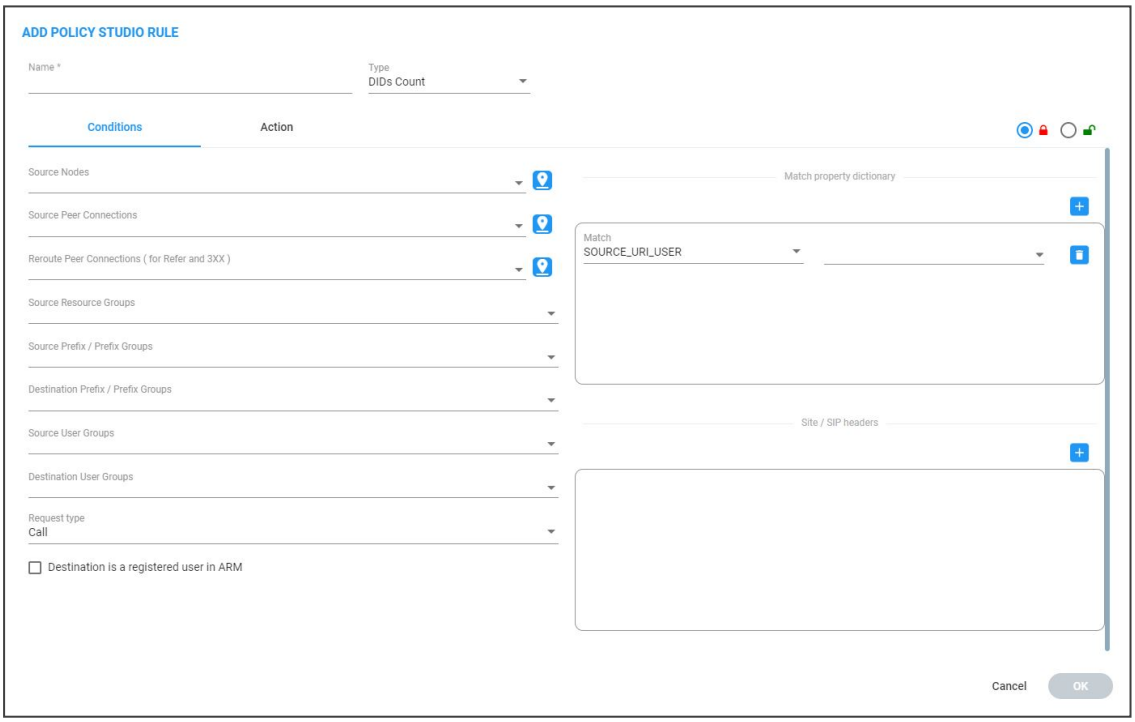


Figure 7-39: DIDs Count



3. Configure the settings using the following table as reference.

Table 7-21: Policy Studio Settings

Setting	Description
Name	Defines the name of the Policy Studio rule to add, to facilitate management of the feature.

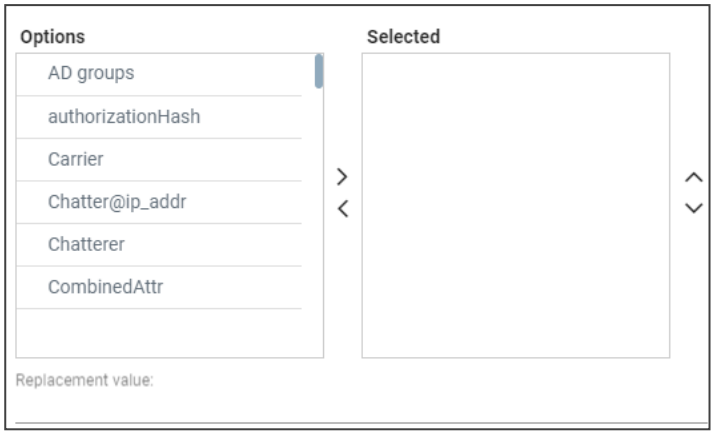
Setting	Description
Type	Policy Studio supports five rule types, as shown in the preceding figures: ■ **User** (default). Select this to use Policy Studio based on information taken from ARM Users Data. ■ **Web Service**. Select this to use an external web service for pre-routing manipulation. See also Web-based Services on page 269. ■ **Credentials**. Select this for the SBC to function as authentication server for SIP messages requests and for the ARM to centrally manage the user credentials of all SIP phones in the global network. See Adding a Policy Studio Rule for Users Credentials Information on page 258 for more information. ■ **Blacklist**. Select this to add into a blacklist a phone number of a caller/ callee if it is called more than a defined number of times within a defined time period. See Managing a Dynamic Blacklist on page 366 for more information. ■ **DIDs Count**. Select this to indicate a phone number of a caller/ callee if it is called more than a defined number of times. See Configuring DIDs Count for more information.
MATCH	The set of match conditions for finding a user from the Users table. Click **+** to add more conditions.
Source Nodes	From the drop-down, select a Node or set of Nodes for which this rule will be used. Alternatively, click the adjacent  button to select a Node or set of Nodes from the Topology Map. If left empty, the rule is used regardless of the origin of the call. **Note**: To select multiple elements in the Choose Topology Item screen, press **Ctrl** and click the elements.
Source Peer Connections	Select a Peer Connection or set of Peer Connections for which this rule will be used. Alternatively, click the adjacent  button to select a Peer Connection or set of Peer Connections from the Topology Map. If left empty, the rule is used regardless of the origin of the call.

Setting	Description
	Note: To select multiple elements in the Choose Topology Item screen, press **Ctrl** and click the elements.
Source Resource Groups	Select a set of Nodes or a set of Peer Connections for which this rule will be used. If left empty, the rule is used regardless of the origin of the call.
Source Prefix / Prefix Groups	Allows a Prefix or a Prefix Group to be configured as the 'Source' in a Policy Studio condition. Optionally add the condition for users' information-based pre-routing.
Destination Prefix / Prefix Groups	Allows a Prefix or a Prefix Group to be configured as the 'Destination' in a Policy Studio condition. Optionally add the condition for users' information-based pre-routing.
Destination is a registered user in ARM	If this option is selected, the Policy Studio rule will be matched *only* if the destination number is a registered user's number (listed in the Registered Users table).
Request type	This condition in a Policy Studio rule of type 'User' allows differentiation between a Policy Studio rule to be used for call setup and a Policy Studio rule to be used for routing registration messages. Default: **Call**. Switch the 'Request type' to **Register** if you want to use the Policy Studio rule for registration messages manipulations / prerouting manipulation. The following example applies pre-routing tagging to all registration messages based on value **Country** of the Users table, which can later be used for Tag-based routing. For example, route users registration to different SoftSwitches based on the value of **Country**.
SIP Header	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 (default) ■ SOURCE_URI_HOST ■ DEST_URI_USER ■ DEST_URI_HOST ■ CONTACT_URI_USER

Setting	Description
	■ CONTACT_URI_HOST ■ CONTACT_URI_PORT ■ P_ASSERTED_IDENTITY_DISPLAY_NAME ■ P_ASSERTED_IDENTITY_USER ■ P_ASSERTED_IDENTITY_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 page 257.
Site	Allows configuring a 'Site' condition as a matching criterion. This is necessary for DID masking in the case of an E911 (Teams emergency call and call-back). See also DID Masking on page 273. The matching criterion is needed to provide a separate range of DID numbers for Teams emergency calls on a per-site basis. Teams uses a proprietary LMO (Local Media Optimization) header to indicate the user's current site: **X-MS-UserSite**, shown in the next figure. See also Configuring a Microsoft Teams LMO Topology on page 91.  A DID masking Policy Studio rule matching this attribute enables you to manage emergency numbers with a separate pool of numbers for each site (coordinated with Teams definitions). In the example shown in the preceding figure, the SIP field **X-MS-UserSite** is set to **Boston**; emergency calls with a call-back Policy Studio rule will consequently only be applied to calls from the 'Boston' site. Note that this field allows multiple values to be set; the same rule will then be applied to multiple sites.
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

Setting	Description
	properties): ■ SOURCE_URI_USER ■ SOURCE_URI_HOST ■ DEST_URI_USER ■ DEST_URI_HOST ■ DEST_IP_ADDR ■ DEST_PORT ■ DEST_PROTOCOL ■ USER_CREDENTIALS_USER_NAME ■ USER_CREDENTIALS_PASSWORD ■ P_ASSERTED_IDENTITY_DISPLAY_NAME ■ P_ASSERTED_IDENTITY_USER ■ P_ASSERTED_IDENTITY_HOST ■ TAG_1 (see here for more information) ■ TAG_2 (see here for more information) ■ TAG_3 (see here for more information) ■ INCOMING_CUSTOMER_TAG ■ OUTGOING_CUSTOMER_TAG ■ X_ARM_INFO_1 ■ X_ARM_INFO_2 ■ X_ARM_INFO_3 Multiple actions can be defined. Click **+** to define another action. **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 on page 257.
Source or Destination Number	[Applies to a Policy Studio Rule whose 'Type' is **Black List** or **DIDs Count**]. Select Source Number for the caller's phone number or Destination Number for the callee's phone number.

Setting	Description
	See Managing a Dynamic Blacklist on page 366. See Configuring DIDs Count.
Conditions	[Applies to a Policy Studio Rule whose 'Type' is **Black List**]. Call time range (seconds). Default: 60. Number of calls during time range criteria. Default: 5. See Managing a Dynamic Blacklist on page 366. [Applies to a Policy Studio Rule whose 'Type' is **DIDs Count**] Number of calls from first hit. Default: 5 See Configuring DIDs Count.
Action	[Applies to a Policy Studio Rule whose 'Type' is **Black List**]. Blocking number time period (minutes). Default: 60 minutes. See Managing a Dynamic Blacklist on page 366. [Applies to a Policy Studio Rule whose 'Type' is **DIDs Count**] ■ Select the **Clear DID count timer from the first hit** option and then configure the **Block Number Duration** (in minutes). Default: 60. ■ Select the **Clear DID count at** option to clear the counting every day at a specific time. See Configuring DIDs Count.
Match	[Applies to a Policy Studio Rule whose 'Type' is **Black List** or **DIDs Count**]. From the drop-down, select a tag: ■ TAG_1 ■ TAG_2 ■ TAG_3 See here for more information. Click the drop-down arrow on the right:

Setting	Description
	 Select the option you require and then click **Apply**.
White List	[Applies to a Policy Studio Rule whose 'Type' is **Black List**]. Click the drop-down arrow and select a list of numbers that will never be blocked.
Generate alarm when number is blocked	[Applies to a Policy Studio Rule whose 'Type' is **Black List**]. Select this option for an alarm to be generated when a number is blocked. See also Active Alarms | History Alarms on page 372.
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.
Flow	Allows operators to exercise an option to control the action to be executed after a Policy Studio rule is matched. Use the following as reference when configuring 'Flow': ■ **Stop**. This is the default action. When the rule is matched, the ARM stops and continues to Routing Rule matching. ■ **Continue**. The ARM continues to the next matching

Setting	Description
	Policy Studio rule. ■ **Continue to policy studio rule**. The ARM continues to the next matching Policy Studio rule from a specific Policy Studio rule. This essentially triggers execution of the rule.

Fields such as 'Source Nodes' and 'Source Peer Connections' in Policy Studio's Add Call Item screen and Edit Call Item screen feature filters in which network administrators can select multiple elements and then *invert the selection*. The feature improves usability and user experience especially in large networks with high numbers of elements. The feature allows network administrators to

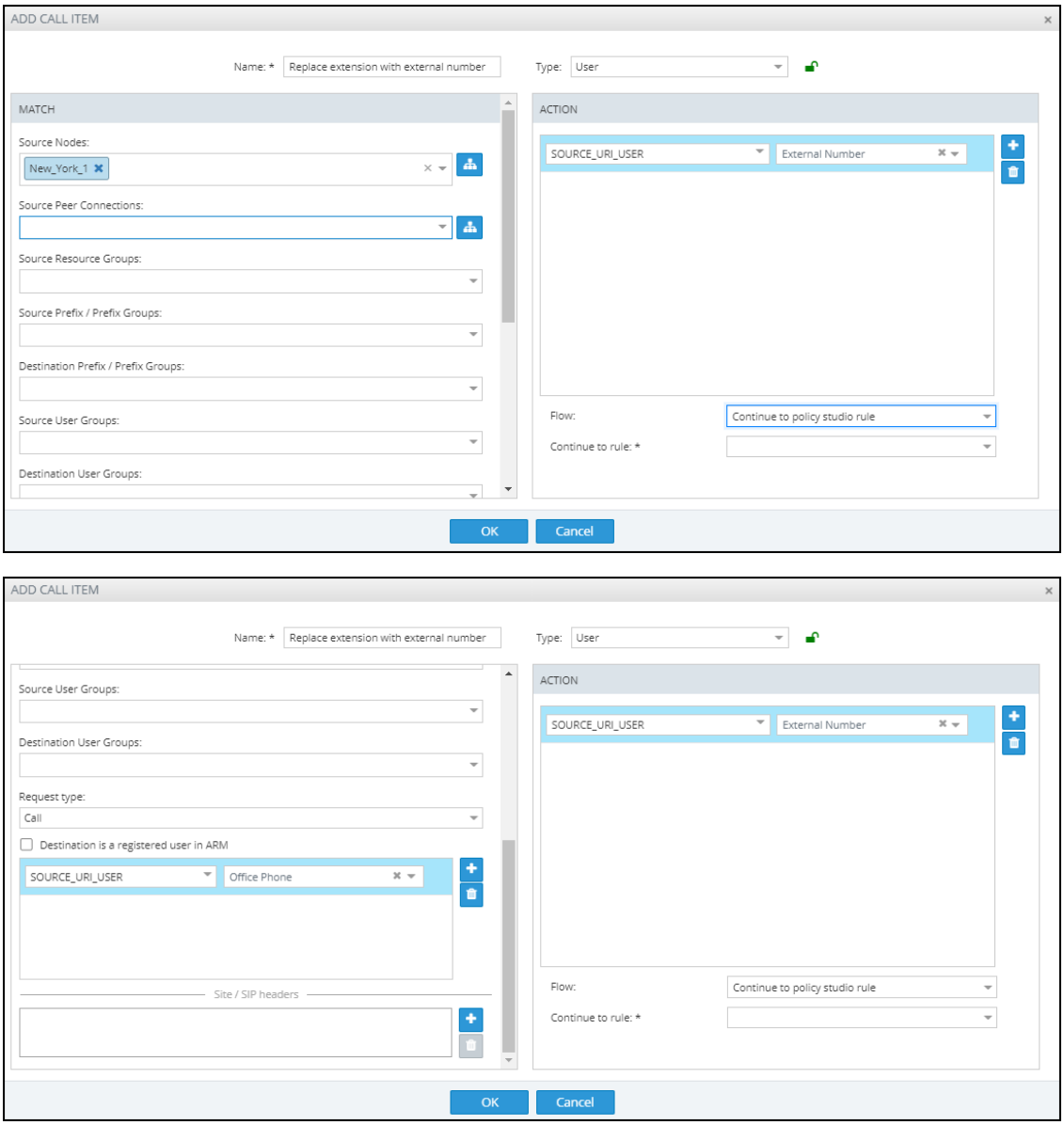
- Select a single element
- Delete a single element (x)
- Select All elements
- Clear all selected elements
- Select All and delete a few (x)
- Select All, delete a few (x) and then invert the selection; the elements deleted will be in the selection
- Select a few elements and then invert the selection;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

Example 1 of a Policy Studio Rule

Refer to the defined Policy Studio rule shown in the figure depicting the Call Item Settings screen:

- For every route request coming from node New_York_1, the ARM will search for a user whose *office phone* property is equal to the value of the SOURCE_URI_USER field.
- ARM will then replace the SOURCE_URI_USER field with the value of the found user's *External Number* property.

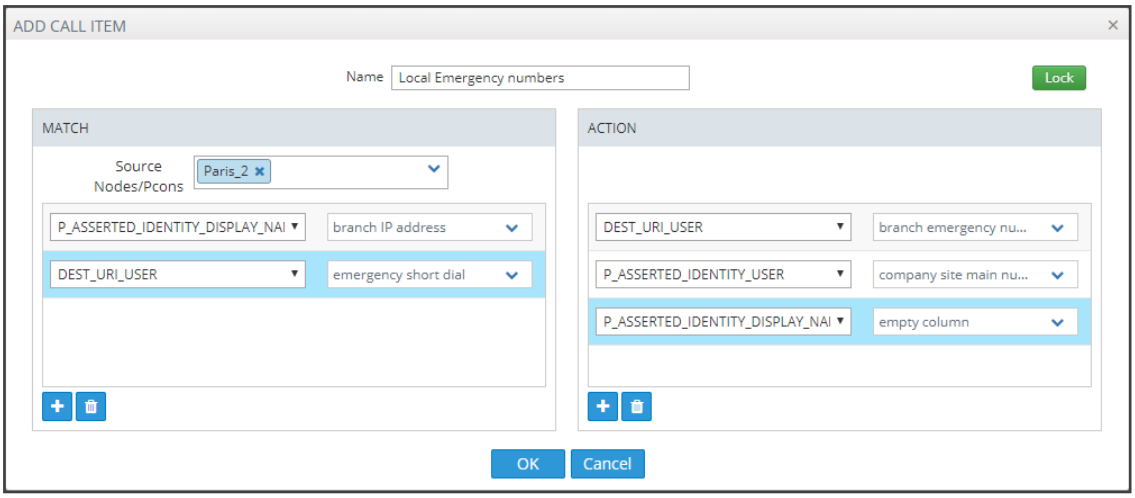
Figure 7-40: Policy Studio Rule Example 1



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 7-41: Policy Studio Rule Example 2



In the rule above.

- The node sends a route request to the ARM. The request includes the two fields under MATCH and the values configured for them; if one and/or the other exists and their values are those configured, then the manipulations configured under ACTION will be used in response to the route request:
  - DEST_URI_USER will be replaced by *branch emergency number*
  - P-ASSERTED_IDENTITY_USER will be replaced by *company site main number*
  - P-ASSERTED_IDENTITY_DISPLAY_NAME will be replaced by *empty column*

Adding a Policy Studio Rule for Users Credentials Information

The SBC can function as authentication server for SIP messages requests. The SBC is used to store the users (SIP phones) credentials information. Irrespective of under which local SBC in the network the phone is located, the ARM provides a centralized point for global credentials management of all SIP phones in a network. The SBC requests the ARM to provide credentials for specific users. This information is stored in the ARM users database. When the SBC needs to authenticate a user, it sends a REST request to the ARM to obtain the credentials for that user and then sends the 'challenge' for credentials back to the client. The client then resends the request with an Authorization header (containing a response to the 'challenge') and the authentication process continues regularly. Request for authentication is relevant for INVITE and for REGISTER requests coming from a SIP phone. The following figures show the flows:

Figure 7-42: Request for Authentication: Invite Sequence

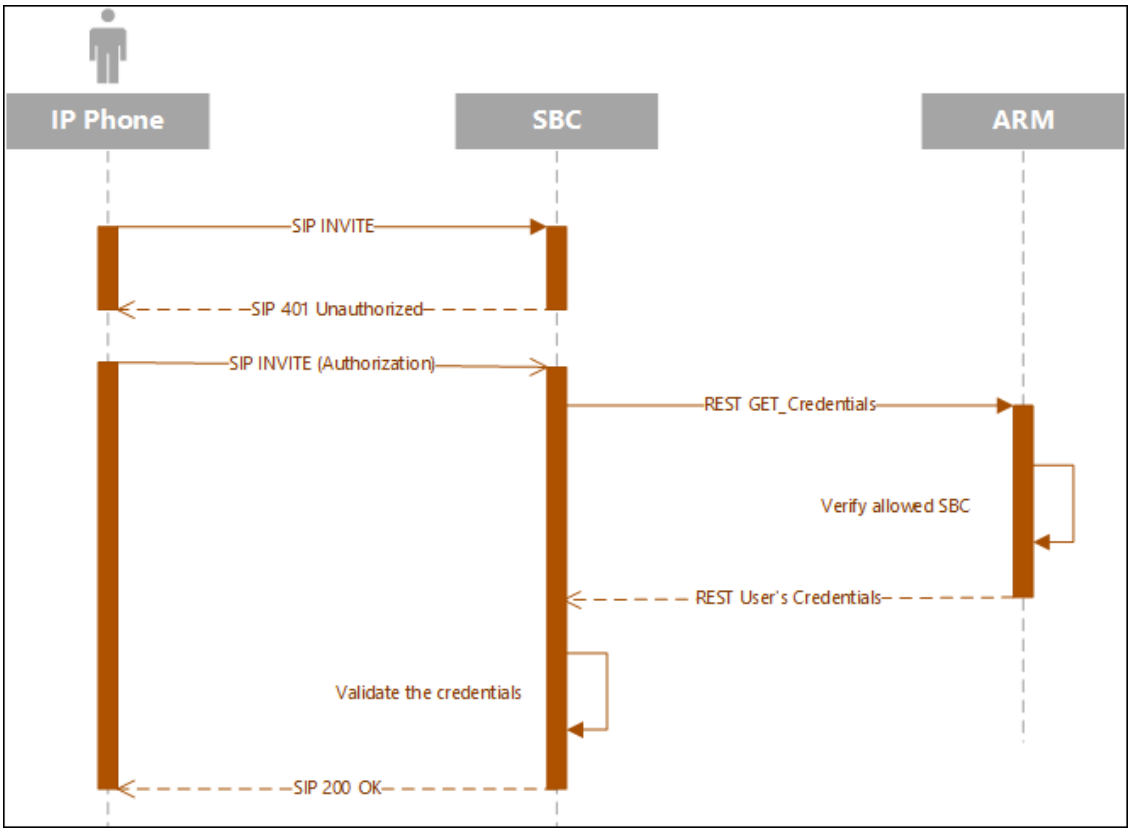
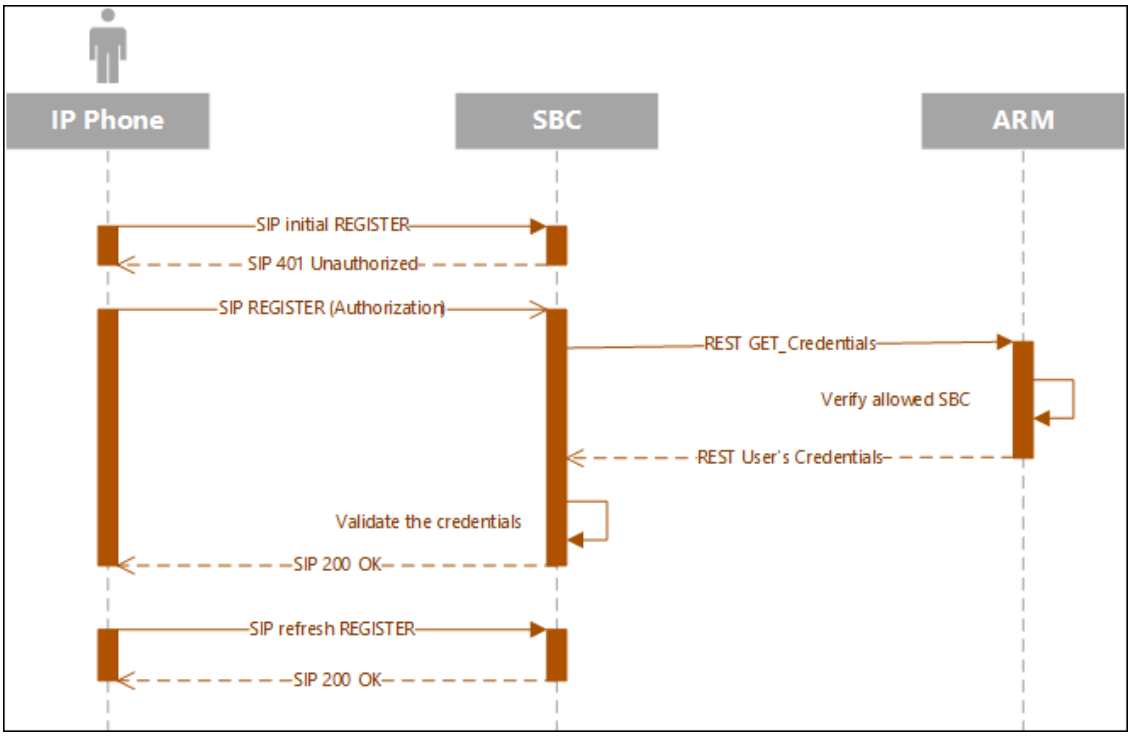


Figure 7-43: Request for Authentication: Register Sequence



> To configure the SBC to send the above REST API to the ARM, you need to configure an IP Group with specific settings in the SBC's Web interface. For more information, see Configuring the SBC to Send the REST API on page 263.

The operator should prepare credentials information to be provided to the SBC upon credentials requests. The information should be part of the ARM users database. The operator must define a dedicated dictionary attribute where the credentials will be stored for each authorized SIP phone. The information is provided by the ARM using the Policy Studio matching feature. Policy Studio is divided into two types of rules: (1) Policy Studio Rules designated for Routing and (2) Policy Studio Rules designated for Credentials. The operator who does not source ARM credentials information does not need to define Credentials Policy rules and can use the regular functionality of Policy Studio for Calls and Registrations pre-routing smart manipulations.

➢ To add a Policy Studio rule for credentials information:

1. Add a rule and select **Credentials** from the rule's 'Type' drop-down. The newly created rule will automatically be placed in the 'Credentials' section in the Policy Studio screen to distinguish it from Routing related rules.

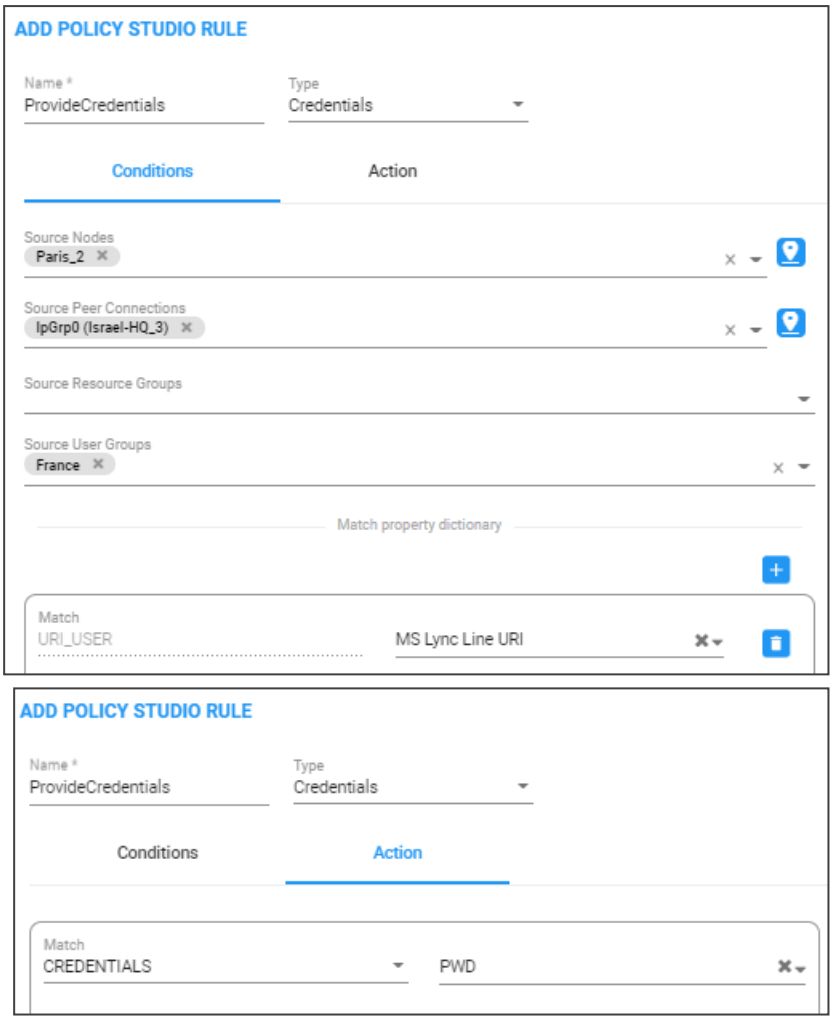
Figure 7-44: Credentials

2. The matching criteria for Policy Studio of type **Credentials** must be **User_URI** and (optionally) **HOST_URI**. This information is used as a unique identifier to find the correct entry in the Users page to retrieve requested credentials information.

> These are the only properties that can be used for matching of the credentials request.

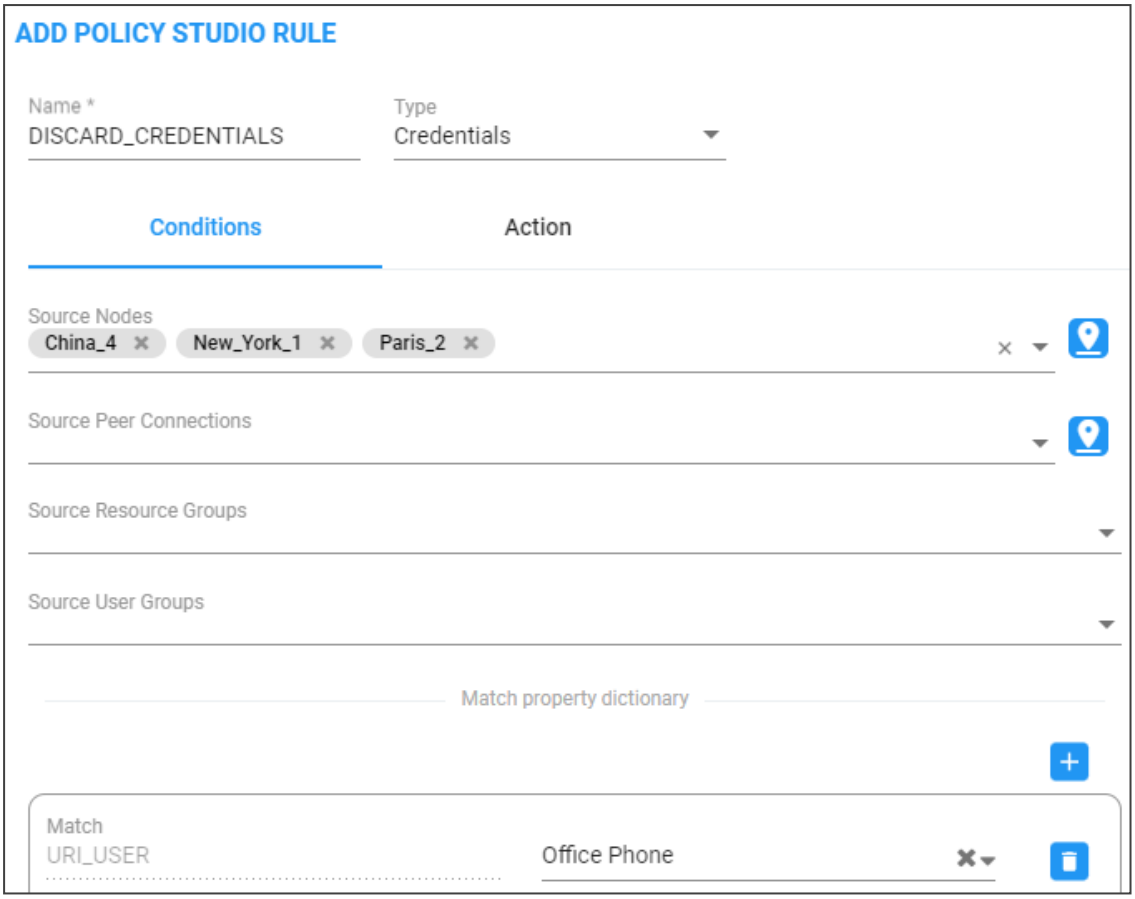
3. Optionally apply the following matching criteria to narrow the group of users to whom this service (of supplying credentials by the ARM) is provided:
   - Source Node
   - Source Peer Connection
   - Source Resources group
   - Source users group

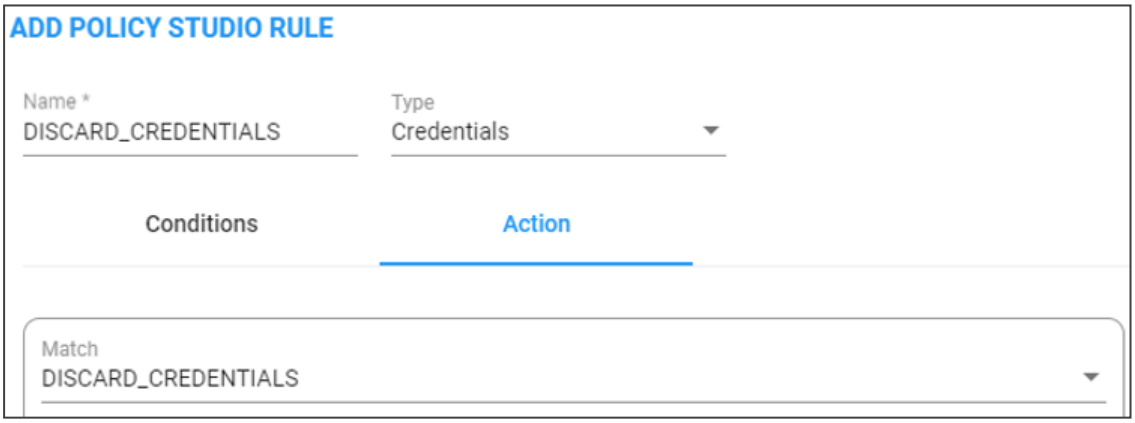
Figure 7-45: Add Policy Studio Rule - Type 'Credentials'

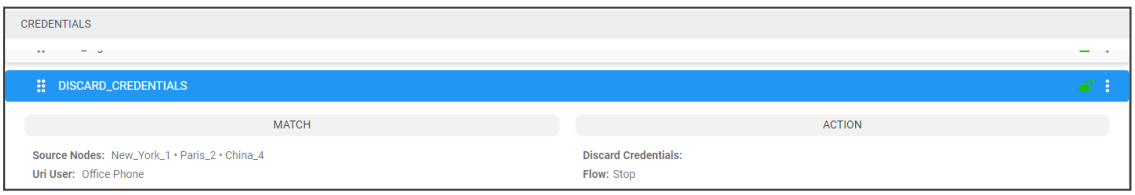


If the ARM does not find in the users database a match for a specific URI_USER and (optional) URI_HOST, it will return a 404 (not found) HTTP response to the SBC (and consequentially, to the SIP phone). If you want to have a configuration in which every user (SIP phone) is allowed to register only upon specific conditions (for example, only from certain IP Group/Peer Connection or Group of Peer Connections or Nodes, etc.), it can be done by a combination of Match (condition) part of the Credential Policy Studio rule and a specific action named **Discard_Credentials** relevant for credentials rules only. In this case, although the user is found but is not authorized for the specified IP group or SBC, the ARM will respond with a 403 HTTP response (forbidden).

For example, the following rule of type **Credentials** named **DiscardUnauthorizedCredentialRequests** will not provide credentials for a request coming from node 'China' for users who are part of the 'United States' users group; the ARM will respond with a 403 HTTP response (forbidden).







The order (priority) of the rules in Policy Studio is important. For example, if an operator added 'Discard Credentials' but there is a higher rule with the same match criteria, all users in the 'Discard Credentials' rule will be authorized (the higher rule will be applied).

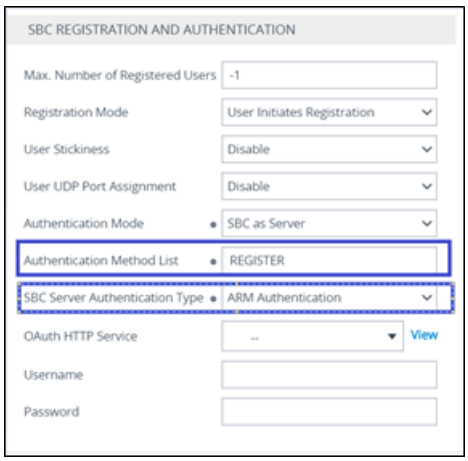
Configuring the SBC to Send the REST API

The SBC must be configured to send the REST API to the ARM as described in Adding a Policy Studio Rule for Users Credentials Information on page 258.

➢ To configure the SBC to send the REST API to the ARM:

- In the SBC's Web interface, configure an IP Group with specific settings.
  - For **REGISTER** messages: In the SBC's Web interface in IP Group settings, under the 'SBC Registration and Authentication' section, configure parameter 'Authentication Method List' to **REGISTER** and from the 'SBC Server Authentication Type' drop-down, select **ARM Authentication**.

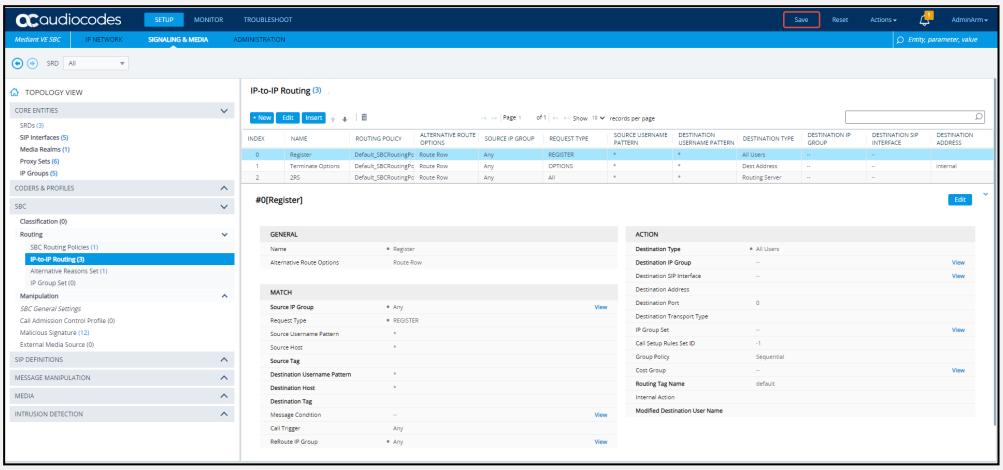
Figure 7-46: SBC Web interface - SBC Registration and Authentication - REGISTER



➢ **To configure IP-to-IP Routing (referred from Adding a Policy Studio Rule for Users Credentials Information on page 258):**

1. In the SBC's Web interface, open the IP-to-IP Routing page (**Setup** > **Signaling & Media** > **SBC** > **Routing** > **IP-to-IP Routing**).

Figure 7-47: IP-to-IP Routing page in SBC's Web interface

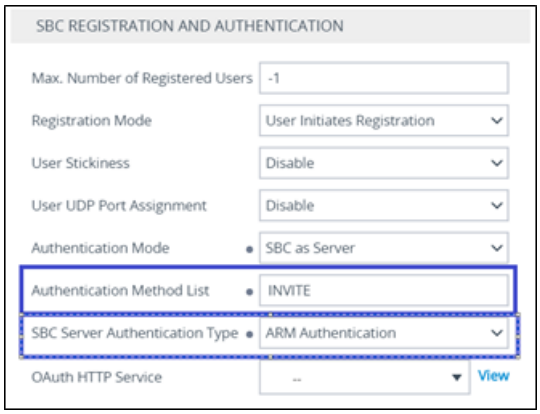


2. [Use the preceding figure as reference] Define an IP-to-IP Routing Rule with a 'Request Type' of **Register**.
3. Define its 'Destination Type' as **All Users**.
4. Make sure this Routing Rule is located in the IP-to-IP Routing page *before* the IP-to-IP Routing Rule whose 'Destination Type' is defined as **Routing Server**.

- For **INVITE** messages: In the SBC's Web interface in IP Group settings, under the 'SBC Registration and Authentication' section, configure parameter 'Authentication Method List' to **INVITE** and from the 'SBC Server Authentication Type' drop-down, select **ARM Authentication**.

- The INVITE/REGISTER is received in the incoming Pcon.
- To configure INVITE or REGISTER to the same incoming Pcon, configure parameter 'Authentication Method List' to **INVITE|REGISTER**.

Figure 7-48: SBC Web interface - SBC Registration and Authentication - INVITE



- The feature involves changes in the SBC ↔ ARM REST internal REST API
- The feature is supported starting from SBC version 7.20A.259.031

Tag-based Routing

The ARM increases flexibility in the flavors of the routing criteria by adding 'Tag-based routing' as a routing method. This routing method allows operators to assign Tags to the messages to be routed by the ARM, and to use these Tags' values as routing criteria. The feature can be applied for the routing of both call and registration messages. Multiple Tags can be assigned to a single message (up to three) and all these Tags' values can be used for routing matching.

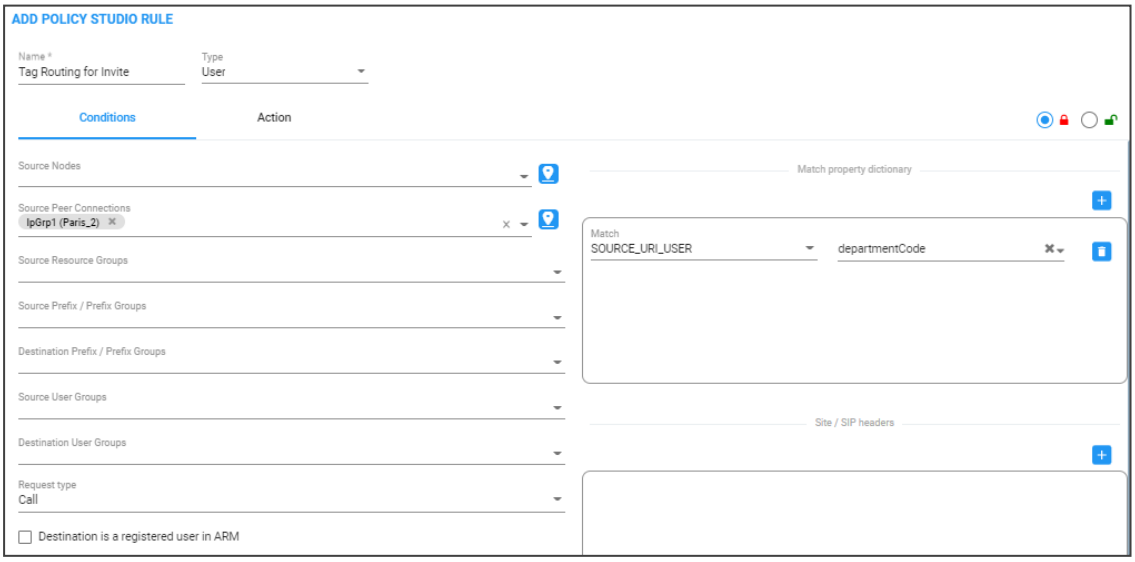
Here's how to assign Tags in Policy Studio rules. The Tag value can be assigned using Policy Studio capabilities (ARM pre-routing functionality engine). The Tag value can be taken from any field of the user's Property Dictionary the operator would like to use for further routing. This capability can only be applied to the Policy Studio rule whose 'Type' parameter is configured to **User**. The regular matching criteria with all the available parameters applies to Tag assigning as well.

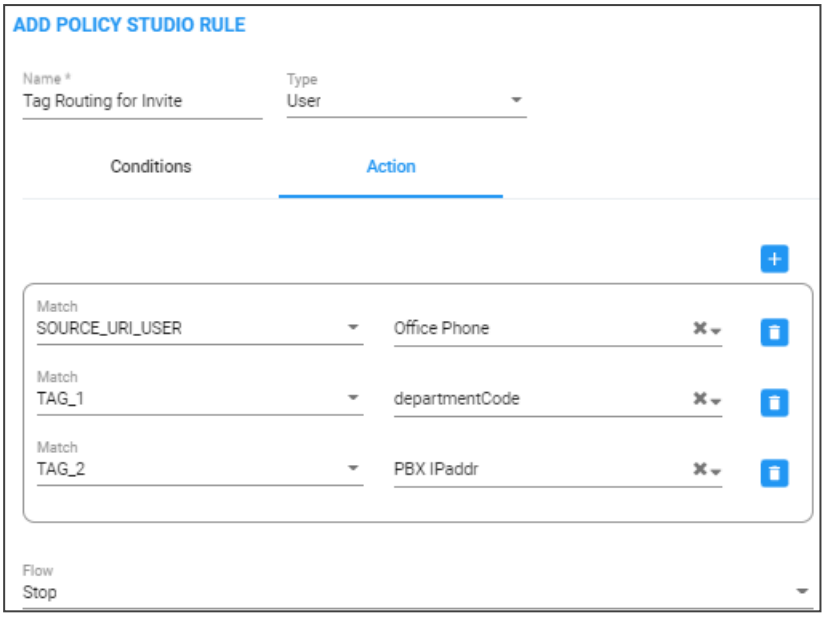
➢ To assign a Tag

- Under the 'Action' section in the 'Add Call Item' screen that opens when adding a Policy Studio rule, select one or more Tags (TAG_1, TAG_2, TAG_3) and assign it with one or more attributes from the Property Dictionary. The value of this Property Dictionary for matching the user will be factored in for the corresponding TAG value and will be used for further routing.

  The following example shows a Policy Studio rule named 'Tag Routing for Invite' applicable for calls setup routing coming from a specific Peer Connection to the user's office phone. This Policy Studio rule will assign the value **DepartmentCode** of the user to TAG_1 and **PBXIPaddr** to TAG_2. Both Tags can later be used in Routing Rules.

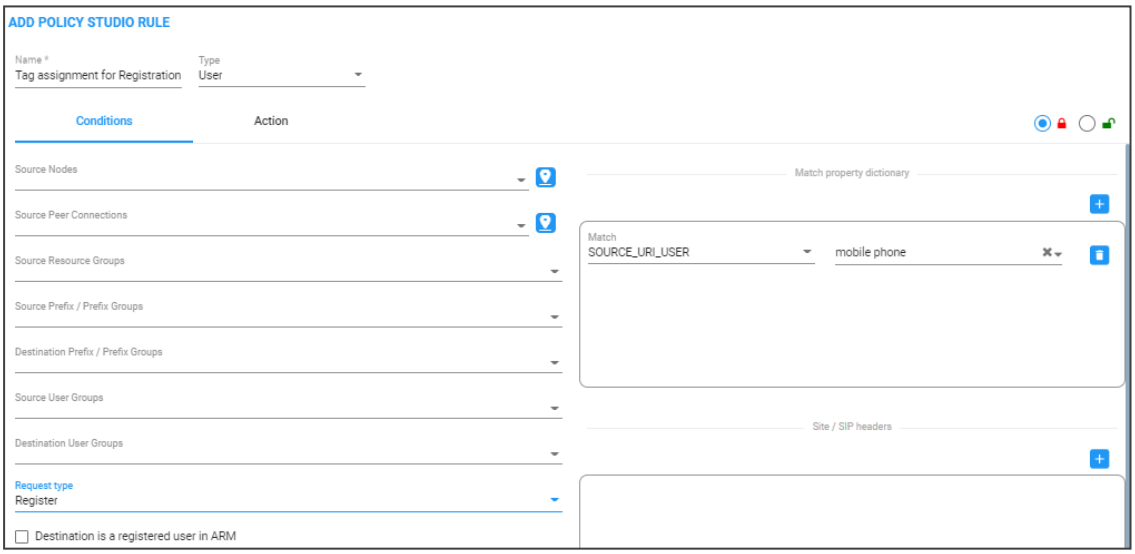
Figure 7-49: Values assigned to Tags in Policy Studio rule

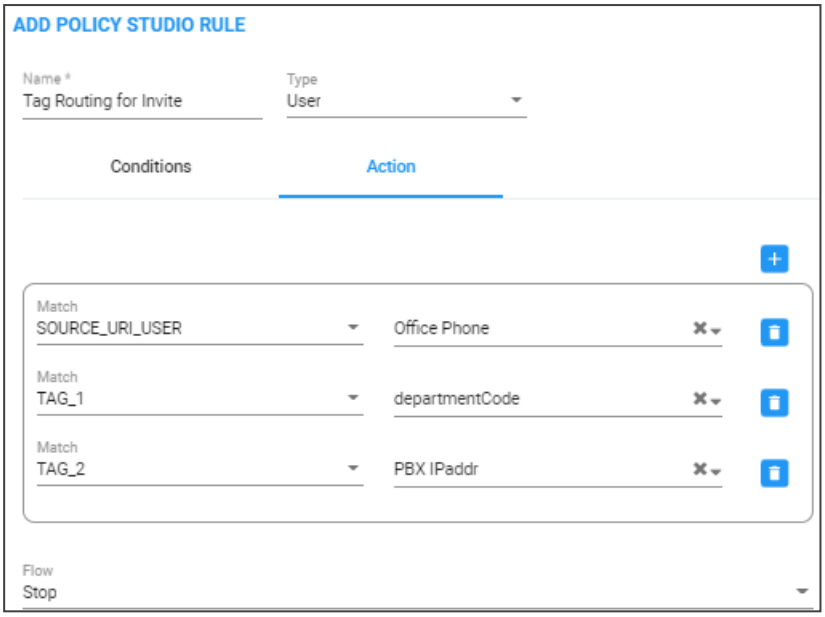




The next example uses Policy Studio to assign a Tag value for registration messages (rule named 'Tag assignment for registration'. TAG_1 gets the value from the **PBX IPaddr** attribute of the user matching the user's mobile phone.

Figure 7-50: Value assigned to Tag for registration messages in Policy Studio rule





Tag values assigned to a routing request in Policy Studio can be further used as matching criteria in Routing Rules. Tag-based Routing Rules can be applied when 'Request type' is configured to **Calls** or **Register**. Tag matching criteria are available in ARM Routing Rules under the **Advanced Conditions** tab.

➢ To apply a Tag-based Routing Rule:

- In the Add Routing Rule screen (**Routing** > **Routing Groups** > click the **Add Rule** button) under the **Advanced Conditions** tab under the 'Tags' section, add a row by clicking the **+** icon and then select Tag 1, Tag 2 or Tag 3 (according to which Tag was assigned to the routing request in Policy Studio (TAG_1, TAG_2 or TAG_3). Note that it's important that the same Tags in Policy Studio are assigned with values for future matching criteria in Routing Rules. One Routing Rule can have a Tag-matching condition involving multiple values of the same Tag and involving more than one Tag in the same condition. In this case, matching is calculated as follows:

  - Several values for the same Tag are treated as 'or'
  - Several Tags in the condition are treated as 'and'

  In the following example, the rule named 'RouteCallBased Tagging' has a Tag-based condition as routing criteria. It will be matched if Tag 1's value is either **RandD** or **Sales**. Assuming that Tag1 got its value of **Department IP** in Policy Studio, this Routing Rule allows routing based on this value.

Figure 7-51: Value assigned to Tag in 'Add Routing Rule' screen

In some cases , the same functionality for routing can be achieved using a Users Group or Tag-based routing. You can use either method of implementation but in the case of a high

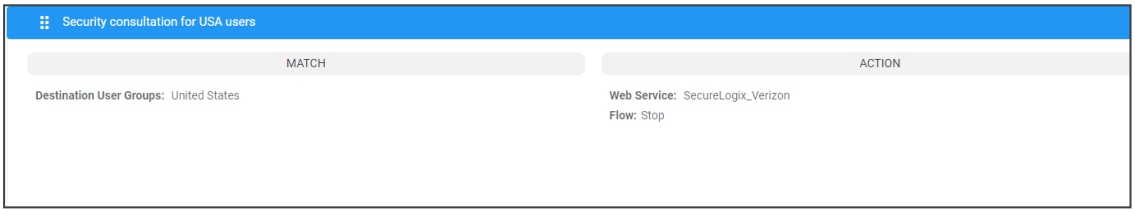
number of users (more than 1 million), using Tag-based routing is more efficient and preferable.

Users Group as Matching Criterion

The ARM allows using a Users Group (or multiple Users Groups) as a matching criterion in the Policy Studio. You can specify a User Group (or Groups) as source ('Source User Group') and / or destination ('Destination User Groups') matching criteria. This criterion can be applied for all types of Policy Studio rules.

For Web services, this feature allows narrowing the criteria for accessing the external Web service, which can be very expensive (as in the case of security-based routing consultations). In the following example, it will attempt accessing security services only for United States users:

Figure 7-52: Users Group as matching criterion



This criterion allows you to perform, for example, different manipulations for users of a certain country, with the ability to differentiate them in 'From' and 'To':

Figure 7-53: Users Group as matching criterion - Conditions tab

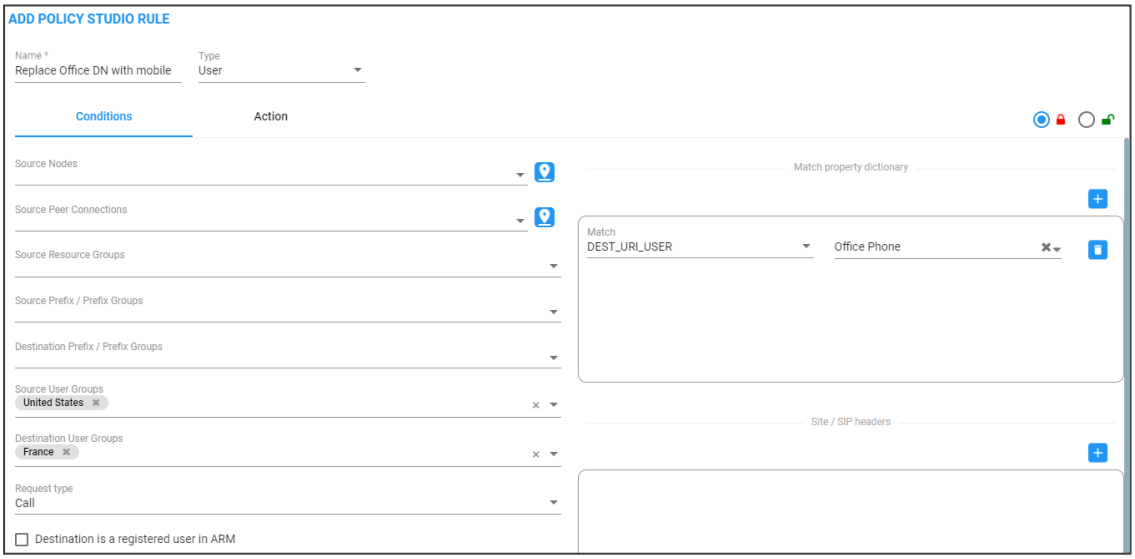


Figure 7-54: Users Group as matching criterion - Action tab

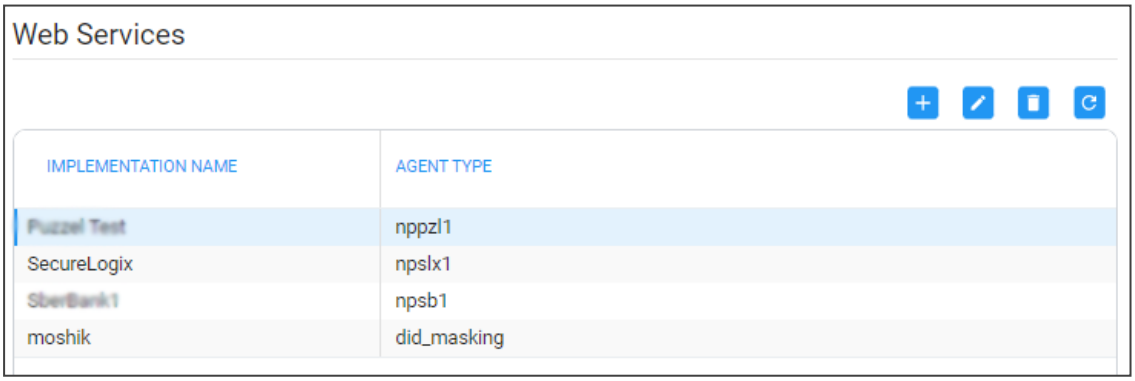
Web-based Services

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**)



2. Click the add **+** icon.

3. In the Add Web Service screen, configure the Web service you require.

- Parameters in the screen are *per customer* and therefore differ from one customer to the next. Contact your AudioCodes representative if necessary for clarifications.
- 'Custom_Http_Client' agent type can be used by all customers; it's used from SIP Manipulation Groups and not through Policy Studio like the other web services.

4. If you're using the SecureLogix's Orchestra One call authentication service plugin for security based routing, define the Web Server as Agent type **npslx1** for communication with SecureLogix's Orchestra One call authentication service, as shown in the figures below. This plugin includes the REST API for ARM communication with Orchestra One.
5. In the field 'Implementation name', define the name of the web server; the name will be used in the ARM's Policy Studio.
6. In the 'Security Mode' field, define **Standard** or **Advanced** and in the 'Strategy' field define **0** or **1** as shown in the next figures.

Figure 7-55: SecureLogix - Standard Mode

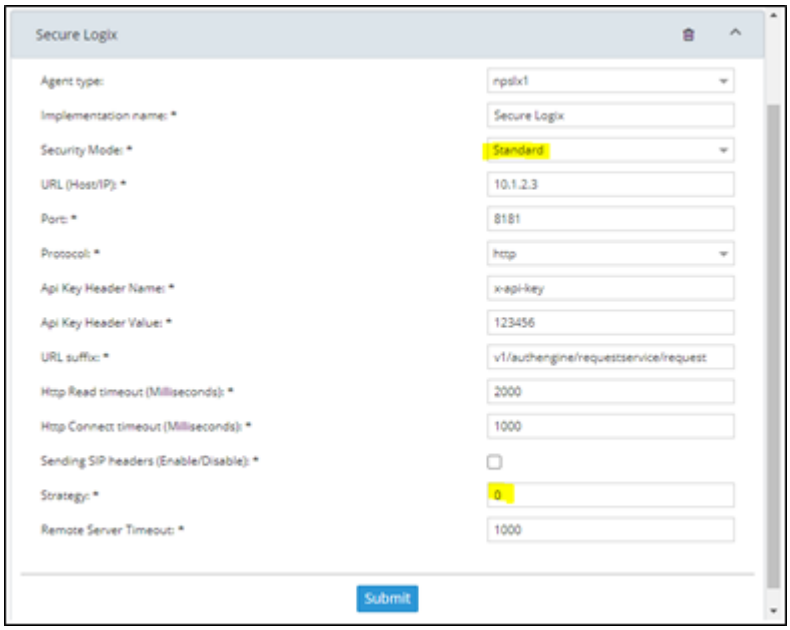
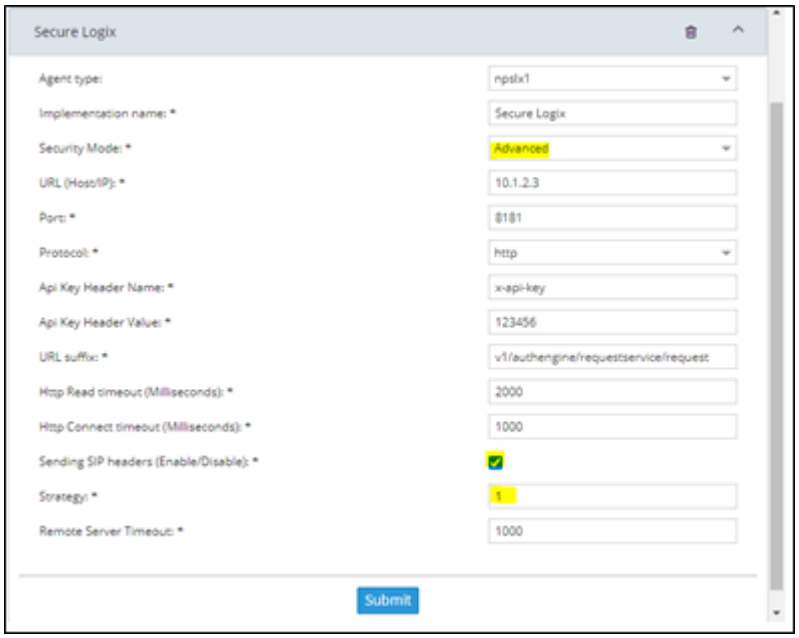


Figure 7-56: SecureLogix - Advanced Mode

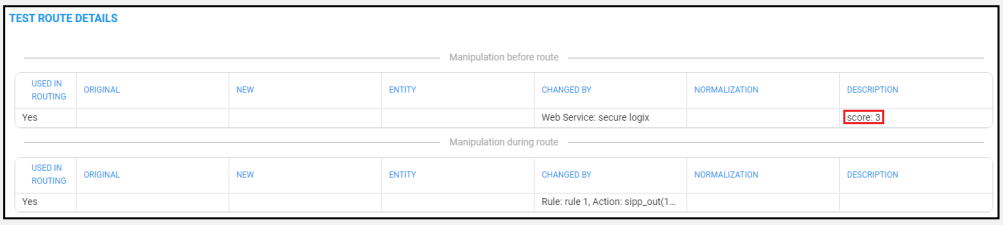


- **Standard mode**. Checks for *basic security verification strategy*. The 'Strategy' field is set to **0** and read-only.
- **Advanced**. Calls are verified with the Orchestra One server. For example:
  - For 'Strategy' value **1**, Orchestra One will 'Authenticate using the Verizon Call Verification Service (VCVS) when applicable'.
  - When 'Strategy' is set to **1**, operators will be able to set it to **1** or higher. For **Advanced** mode, it's typically necessary to enable the 'Sending SIP headers' option.

7. Click **Submit**.

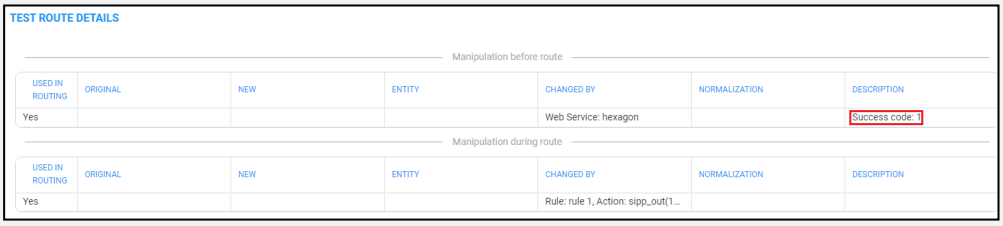
If you're using the SecureLogix plugin for security based routing:

- The newly-defined Web Server must then be assigned in Policy Studio for pre-routing processing and consultation with SecureLogix's Orchestra One. See step 8 below for more information, as well as Policy Studio on page 246.
- When adding a new Routing Rule, the **Security call score** option under Security Based Routing must be selected. See Adding a New Routing Rule on page 328, step 10 for more information.
- The returned score given by SecureLogix is indicated under 'Manipulation before route' in the Test Route Details screen (and in the Call Details screen).



If you're using the Hexagon Fraud Management Solution plugin for security based routing:

- Hexagon gives an "OK" to route a call
- Hexagon blocks an illegal call from entering the enterprise
- Hexagon is sent a "Notify" for a call from the enterprise
- The returned code given by Hexagon is indicated (for example) under the 'Manipulation before route' in the Test Route Details screen (and in the Call Details screen).



8. Apply the service: In Policy Studio (**Settings** > **Call Flow Configurations** > **Policy Studio**), click + to add a new Policy Studio rule and then after selecting **Web Service** from the 'Type' drop-down, click **Action**.

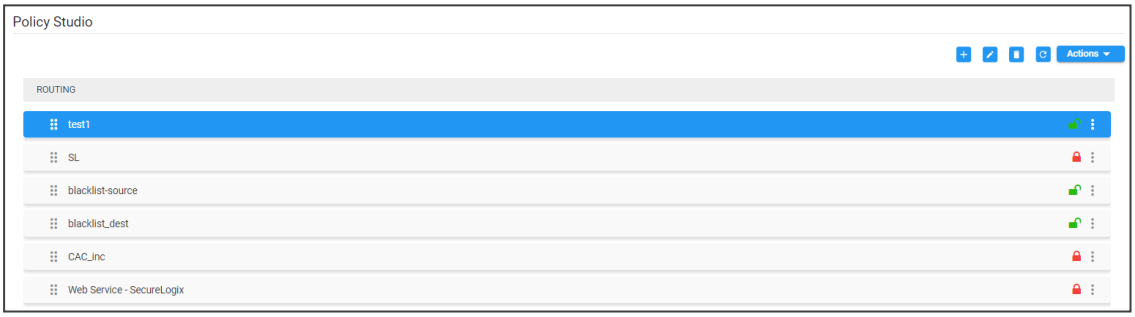
Figure 7-57: Policy Studio - Add Call Item

9. Select number portability as shown in the preceding figure. The default is **User** to preserve the existing functionality of Policy Studio. Previously, operators were limited to using Policy Studio based on information taken from ARM Users Data (the default **User** option) but can

now select the option to use (an external) **Web Service** for pre-routing manipulation, for example, SecureLogix's Orchestra One (to apply security-based routing). Using the Policy Studio rule's 'condition' feature, operators can reduce the number of consultations that will be made with SecureLogix's Orchestra One. The ARM will perform the consultation only for calls matching the rule criteria. In this way, customers can perform consultations only for calls coming from a specific node (or group of nodes), or from specific Peer Connections or from specific Resource Groups. The destination Prefix (or Prefix Group) also can be used as call matching criteria.

10. Policy Studio can be applied to a specific condition (see under MATCH in the preceding figure):
    - Source Nodes and / or Peer Connections and / or Source Resource groups
    - Destination Prefix and / or Prefix groups
    - Applicable for ARM registered users
11. View the external Web Service (SecureLogix, for example) configured in Policy Studio:

Figure 7-58: External Web Service 'SecureLogix' Configured in Policy Studio



DID Masking

Network administrators can assign Direct Inward Dialing numbers to AudioCodes' media gateway so that PSTN network users can *directly reach* VoIP network users. The gateway connects the PSTN network to the VoIP network, routing and translating calls between the two. A call from a PSTN user is directed to the VoIP user who holds the corresponding DID number.

The feature has two main applications:

- It masks the enterprise's internal phone numbers while allowing return calls to the original caller. A bank, for example, can use the feature to change an employee's phone number to the bank's global number so that when a customer calls the global number back, they'll directly call the same employee who originated the call.
- It changes the outgoing phone number to a local phone number of the destination location from a predefined pool of numbers while allowing return calls to the original number which is in a different location; this opens a private use case.

The feature supports calling an emergency service (E911) using the local number of a user who is not located in that country / region and also supports receiving a return call from the emergency service. For example, an employee visiting a different office branch must call an

emergency service. The call in this case is originated with the telephone number of the branch and when the emergency service operator calls back, they'll get to the employee who called.

The capability is achieved by saving the mapping between the original source number, the destination number and the number used to hide the original caller. This mapping is shared across all the ARM Routers so no matter which ARM Router received the return call, it will be routed to the original caller.

The mapping is saved in a Redis database which operates in a master-slave mode. By default, the master is in the ARM Conifigurator and the slaves are in the ARM Routers. Each Router has its own Redis instance. The mapping of the outgoing call is saved in the master Redis instance which is replicated to each ARM Router. The incoming call is first looked up in the local Redis instance before going to the master Redis instance. This reduces delay and network traffic.

The default master location can be changed. This should be done mainly for large enterprises whose CPS is high enough to put a high load on the ARM Configurator.

The default behavior is to add the original caller phone number as an X-Header and not manipulate the destination number directly.

➢ To enable DID in the ARM:

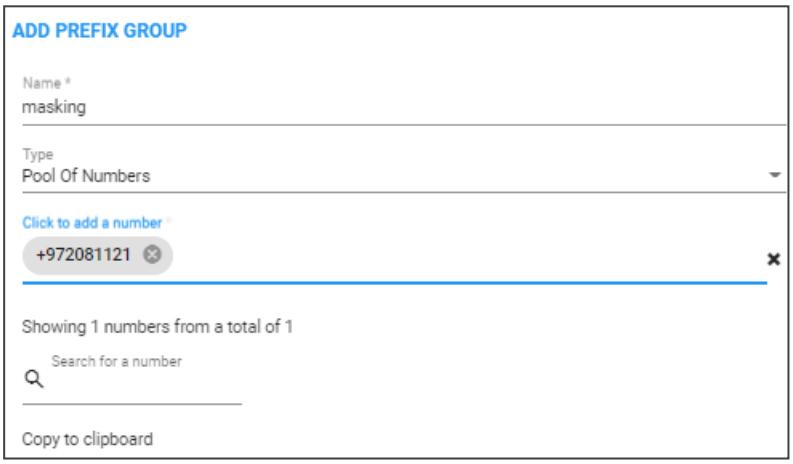
1. In the ARM GUI's Web Services page (**Settings** > **Call Flow Configurations** > **Web Services**), add a new Web Service.

2. Define 'Agent type' (the type of web service for the DID masking feature); in the preceding figure it is defined as **did_masking**.
3. Define the service's parameters using the following as a reference:
   - **Implementation name**: The name of the web service; the name will be used in the ARM's Policy Studio.
   - **Query Timeout**: The timeout of the lookup for a call, in milliseconds.

- **Connect timeout**: The master Redis instance's timeout. After the time expires the master is indicated as unavailable from the ARM Router's perspective. The time is in milliseconds.
- **Password**: The password of the master Redis instance
- **Use Configurator as master**: By default, this option is selected; the ARM Configurator is by default used as the master of the Redis instance. If the option is cleared, a new option is displayed for the host and the port of the new master.
- **Redis debug level enabled**: By default, this option is cleared. The option enables more detailed logging in the Redis.

4. After you **Submit**, add a Prefix Group of a new type 'Pool of Numbers' and then define a pool of numbers that will be used as the DID masking numbers, as shown in the next figure:

Figure 7-59: Add a Prefix Group of New Type 'Pool of Numbers'



5. Define the group's parameters using the following as a reference:
   - 'Type': Must be set to **Pool of Numbers**. When the Prefix Group is of this type, the numbers inside will be handled as full numbers (as if they ended in a #).
   - 'Numbers': Defines the numbers inside the pool.
6. Define a new Policy Studio of action type 'Web Service'. Select the DID masking web service and then configure:
   a. a condition for when to perform masking (under 'Match')
   b. the direction of the call, either outgoing or incoming, *per the matching condition* because the ARM doesn't have the capability to 'find' the direction of a call.
   c. Source and Destination normalization for the lookup operation; this only manipulates the URIs for the Redis and has no effect on the URI for the routing operation.

      If the direction of the call is *outgoing*, the following must be configured:

   d. Pool of numbers from which the manipulated number will be picked. The field can remain empty. If left empty, the ARM will not perform any manipulation but will simply save the destination and source number mapping which is useful in cases when the manipulation itself is performed after the ARM routing.

e. Call expiration time

f. The flow of the Policy Studio

After creating an outgoing Policy Studio rule, the ARM automatically creates an incoming Policy Studio rule above the outgoing rule. The name of the rule will be 'Callback of Outgoing rule name'. Most attributes will automatically be defined. The rule can be updated to give the operator more control over how the callback is executed.

If the direction of the call is incoming, the following must be configured:

g. How ARM Routers should look up the incoming call in the Redis:

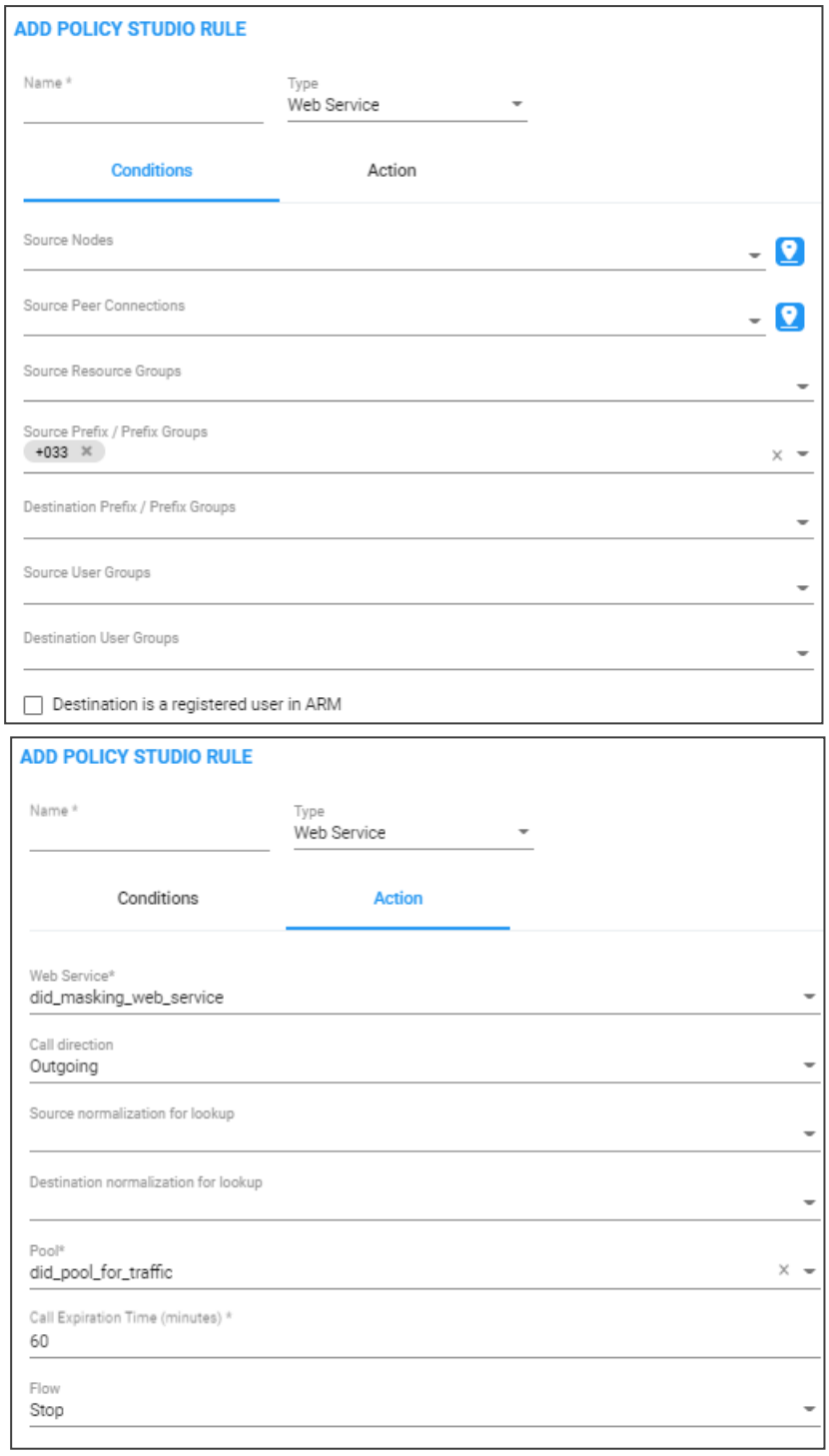
i. Source and Destination number

ii. Only the Source number -or-

iii. Only the Destination number

Make your selection per your network requirements. For example, if some sort of normalization was performed prior to the ARM routing (e.g., the same destination number for all calls).

Figure 7-60: Add Call Item - How ARM Routers should look up the incoming call in the Redis



7. Configure using the following as reference:

- **Web Service**: The web service that will be used for the action manipulation.
- **Call direction**: The direction of the matched call: Outgoing or Incoming.
- **Source normalization for lookup**: Normalization to perform on the Source URI before the operation in the Redis. The normalization has no effect on the URI itself. It's useful when the Source number changes in one of the directions.

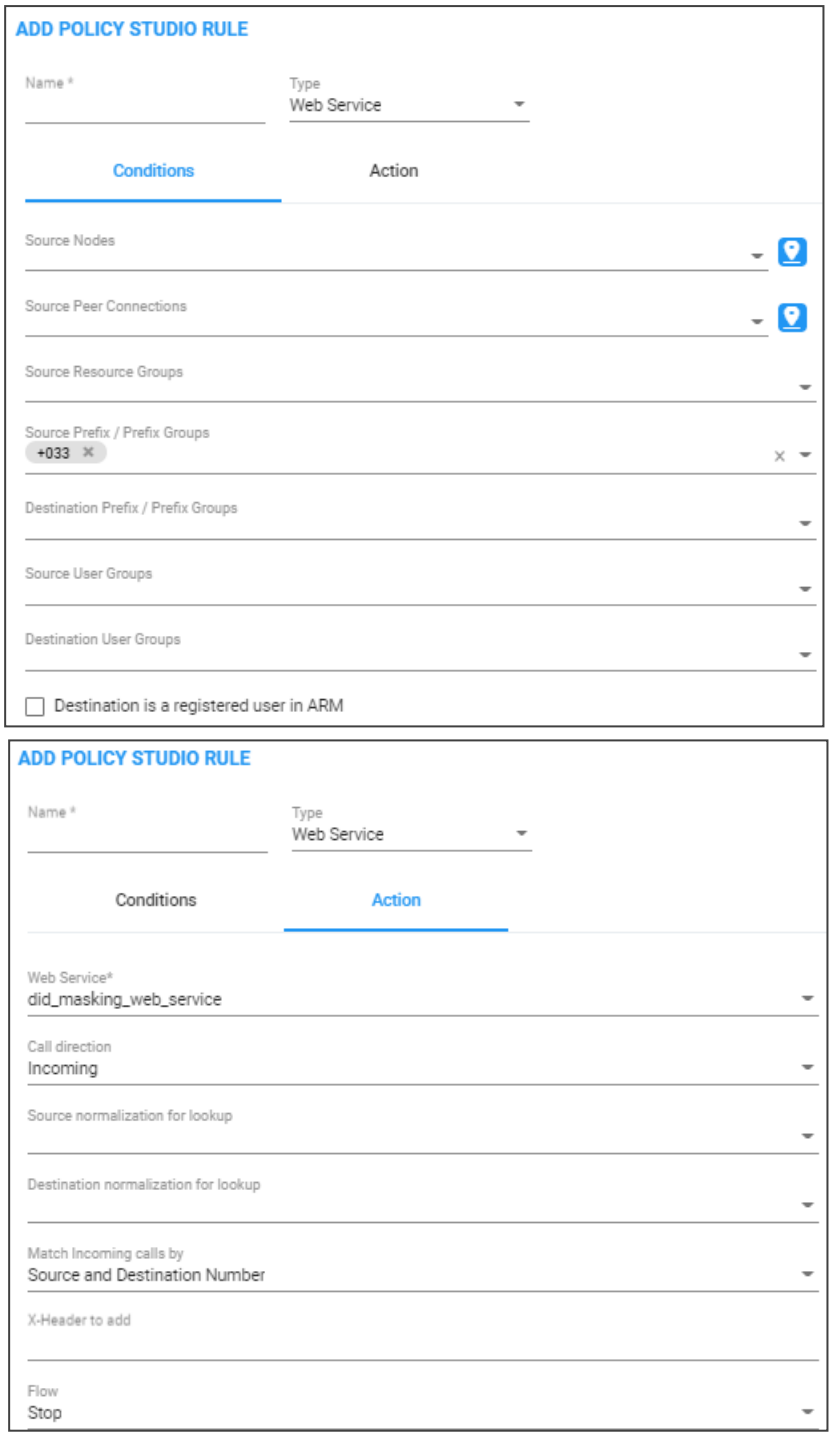
- **Destination normalization for lookup**: Normalization to perform on the Destination URI before the operation in the Redis. The normalization has no effect on the URI itself. It's useful if the Destination number changes in one of the directions.

  For *outgoing* calls:

  - **Pool**: The pool of numbers from which the ARM will pick the manipulated number. If this field is empty, the ARM will not perform manipulation and will only save the Source to Destination number mapping.
  - **Call Expiration time**: The time a call is saved in the database. Defines the length of time ARM allows a return call before discarding the mapping.
  - **Flow**: Defines what the ARM should do after this Policy Studio rule is matched

  For *incoming* calls:

Figure 7-61: Incoming Calls



8. Configure using the following as reference:

- **Match incoming calls by**: Defines how the ARM looks up a return call that was masked.
  - **Source and Destination number**. ARM performs the lookup using a combination of both the caller's number and the masked number. The original caller will be retrieved only if the return call came from the same destination number that was originally called.

- **Destination**. This is a looser lookup option. The ARM performs it using the masked number. The last number masked to the number is retrieved, allowing a return call from any calling number to the number from the pool. It's typically used for E911 scenarios in which the E911 operator's source number doesn't have to be the E911 number.
- **Source**. ARM performs the lookup by the Source number. This option is useful when the Destination number is a static number (like E911) and identification of the call can only be performed using the Source number. The latest number mapped to the number is retrieved.

  In the preceding figure, for example, the Policy Studio rule will mask all outgoing calls from **prefix '+033'** with numbers from the pool **'pool for DID traffic'** and save the mapping for the return call for one hour.

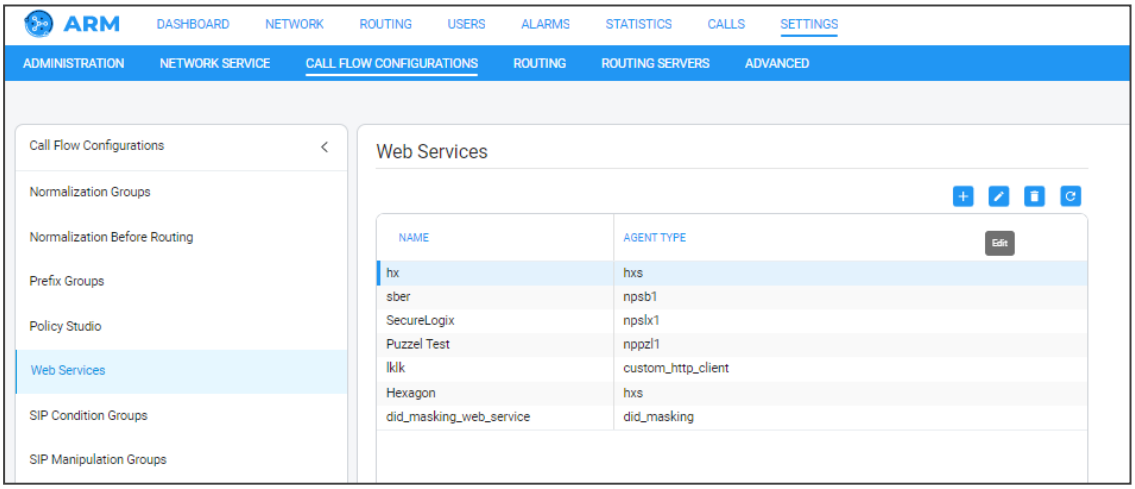
  When an incoming call matches any number in the pool, the ARM retrieves the original number that initially called and replaces the destination with the original number.

Customizing a Web Service

The ARM enables operators to customize a web service.

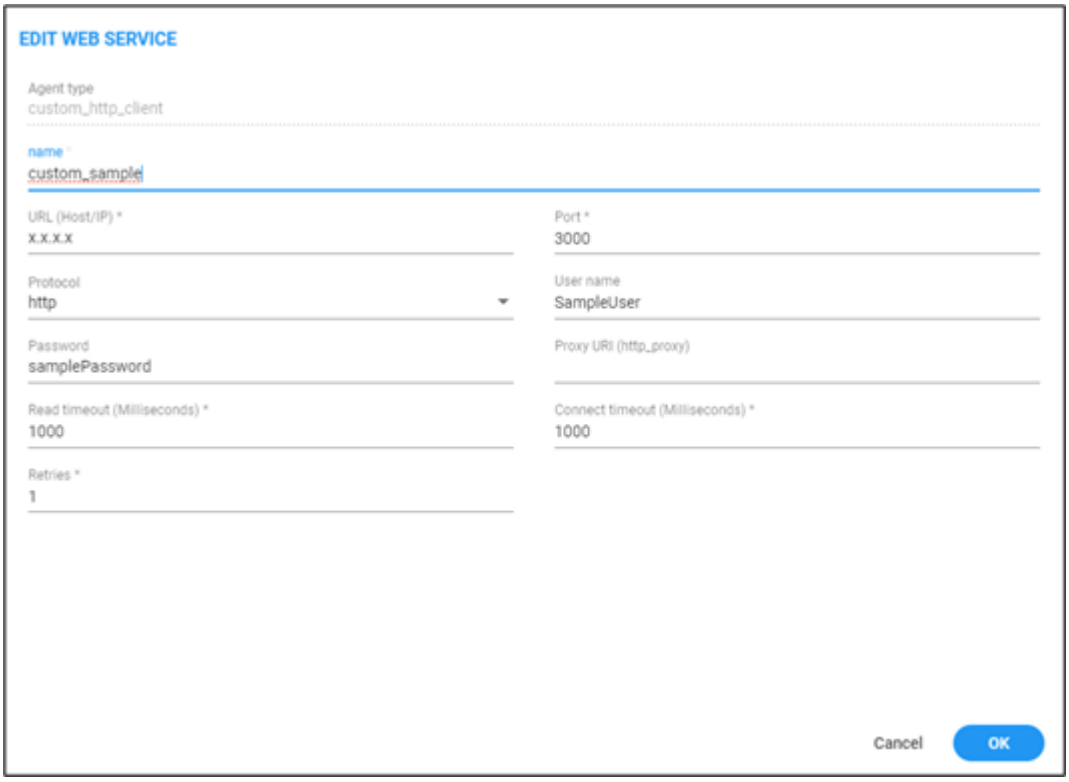
➢ To customize a web service:

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

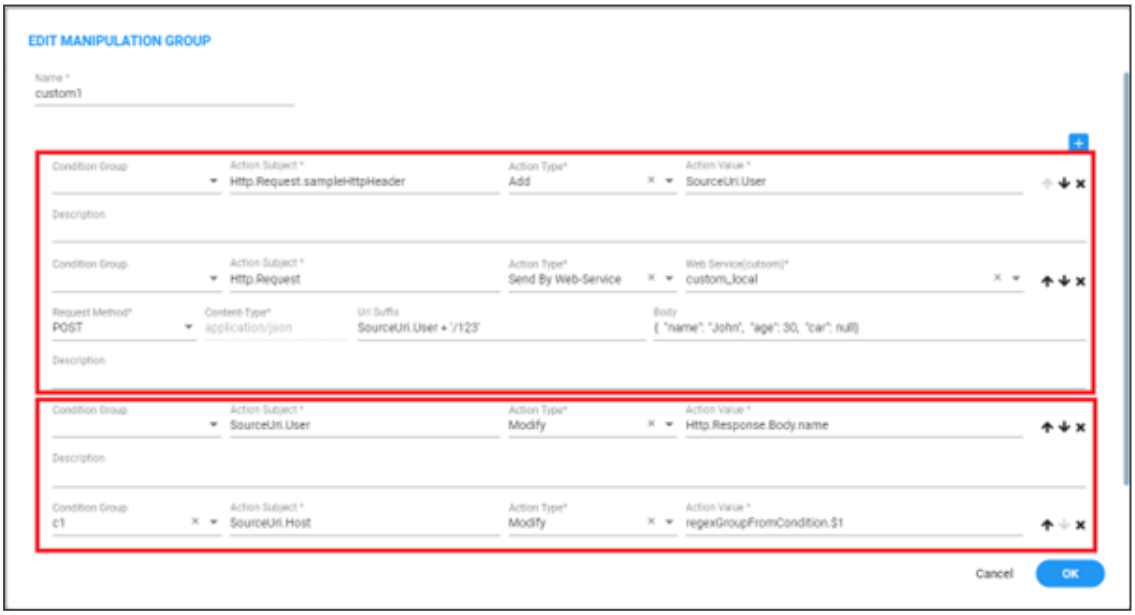


With the help of a SIP Manipulation Group, you can use a 'custom' web service and send a GET/POST/PUT/PATCH REST API request.

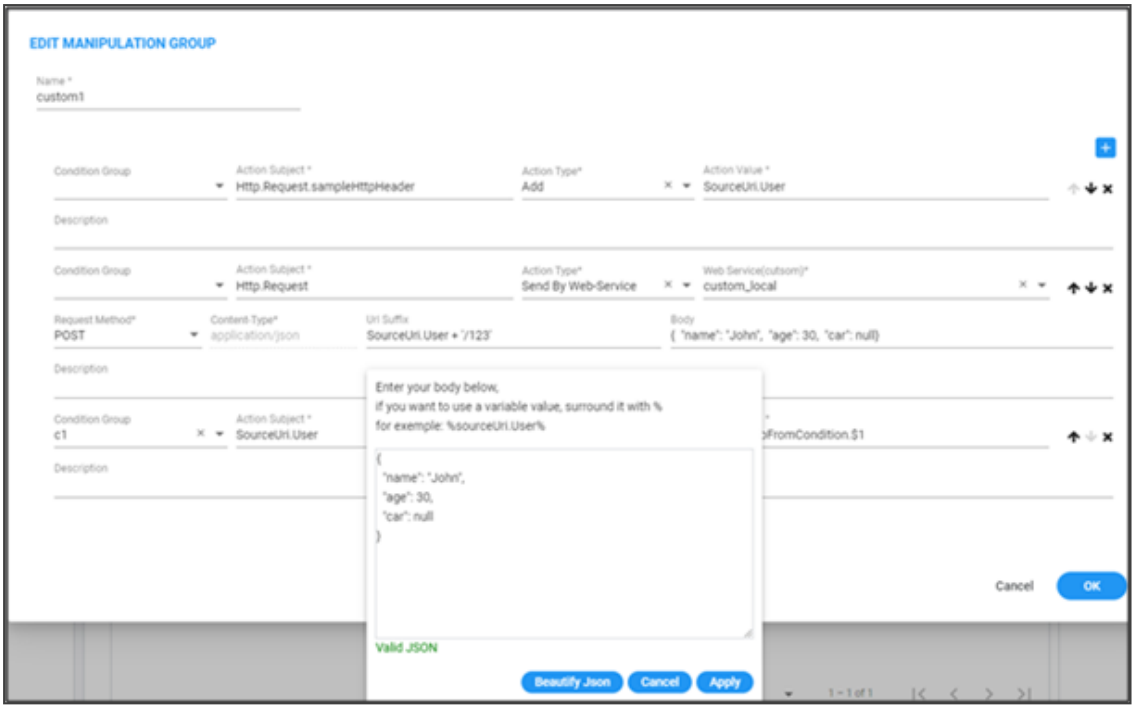
2. Click **+** to add a new web service -OR- select an already configured service and then click the 'edit' icon.



3. Use the preceding screen to add | edit a 'custom' web service.
4. Customize the web service in the 'SIP Manipulation Groups' page:
   - The uppermost screen section indicated in the figure below enables operators to prepare the request and its sending.
   - The lowermost screen section indicated in the figure below enables operators to use the response.

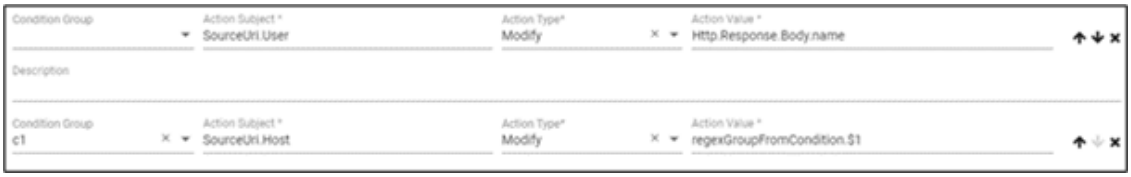


5. Prepare and send the request:



- In the first rule, an HTTP header is added to the request
  - ✓ Its key will be 'sampleHttpHeader'
  - ✓ It will receive its value from 'SourceUri.User'
- In the second rule, a POST request will be sent by 'custom_local' web-service.
  - ✓ The URL suffix can be built in a similar way to 'action value' field.
  - ✓ The body of the request is built by writing full and valid JSON. Inside the JSON it is possible to combine values from the system/headers by wrapping them with the '%' character, as shown in the figure.

6. Add rules after the request (in the same Manipulation Group) and in these rules, use the response values, for example:



- [Refer to the preceding figure] In the first rule, in the 'sourceUri.User' field, the 'name' field will be applied if it exists in the body of the received response (currently, first-level JSON search is supported).
- In the second rule, note that first a condition-group (built separately) is called. Two new related options are available:
  - ✓ If inside condition-group regex matched, you can use its groups in the same condition-group or in linked manipulation-group window (in the preceding figure, see 'regexGroupFromCondition.$1')
  - ✓ If a condition group is linked to a manipulation group like here, the operator is able to use the 'Http.Response…' values also in the linked condition-group.

7. View the linked condition-group as exemplified in the following figure.

- [Refer to the preceding figure] In the first rule, a regex is performed on the body of the HTTP Response (possible if this Condition-Group is called from a Manipulation-Group).
- In the second rule, a test is made on the first group found in the last regex (if found).

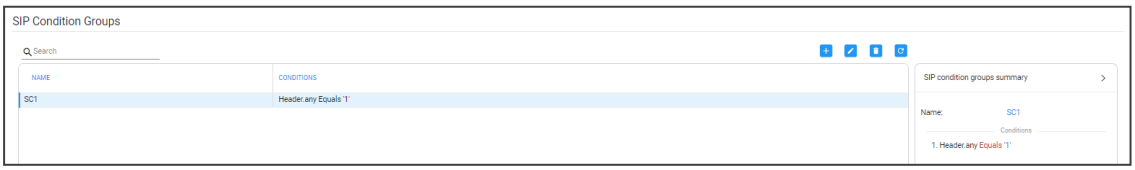
Adding a SIP Condition Group

A SIP Condition is used to test specific parts of SIP headers fields from the incoming Get-Route request message, with specified values. The routing flow of the call will be dependent on the outcome of the SIP Condition.

Network administrators can add a SIP Condition Group. A SIP Condition Group can comprise one condition or multiple conditions. If there are conditions rules in a group, they're performed in the order they're listed. Each condition has an operator ('AND' or 'OR') for logical operating with the next condition.

➢ To add a SIP Condition Group:

1. Open the SIP Condition Groups page (**Settings** > **Call Flow Configurations** > **SIP Condition Groups**).



2. Click the **Add +** icon.

3. Use the following table as reference:

Parameter	Description
Name	Enter an intuitive SIP Condition Group name.
Subject	Define the message component to compare with. You can use the built-in syntax editor to help you configure the field. See also SIP Condition Syntax on page 402 for information about the syntax to use.
Operator	The comparing type such as equals, exists, etc. ■ Equal - Returns 'true' if the subject equals the value. ■ Doesn’t equal - Returns 'true' if the subject does not equal the value. ■ >= - Performs a character-by-character compare. Returns 'true' if the ASCII value of the subject is greater than or equal to that in the value. ■ <= - Performs a character-by-character compare. Returns 'true' if the ASCII value of the subject is less than or equal to that in the value. ■ > - Performs a character-by-character compare. Returns 'true' if the ASCII value of the subject is greater than that in the value. ■ < - Performs a character-by-character compare. Returns 'true' if the ASCII value of the subject is less than that in the value. ■ Contains - Returns 'true' if the value is found in the subject. ■ Doesn’t contain - Returns 'true' if the value is not found in the subject. ■ Suffix - Returns 'true' if the subject has Value as suffix. ■ Prefix - Returns 'true' if the subject has Value as prefix. ■ Len greater Than - Returns 'true' if subject length is greater than the value (a number). ■ Len Less Than - Returns 'true' if the subject length is less than the value (a number). ■ Len equal to - Returns 'true' if the subject length is equal to the value (a number). ■ Regex - Returns 'true' if the subject matches the given regular expression.

Parameter	Description
	■ Exists - Returns 'true' if the subject exists. ■ Doesn’t exist - Returns 'true' if the subject doesn’t exist. ■ Prefix Group - Returns 'true' if the subject belongs to a specific prefix group (only for users).
Values	The strings to be compared with the subject. Each string value must be enclosed by a single quotation mark ('...'). To concatenate values, use the plus “+” operator. The condition is 'true' if the subject meets at least one of the values. Use the built-in syntax editor to help you configure the field. See also SIP Condition Syntax on page 402.
Description	Enter a brief description of the SIP Condition Group.

➢ To add a SIP Condition to a SIP Condition Group:

1. Click the **Add +** icon.
2. Define the previous SIP Condition's field ‘Operator with next line’ as shown in the next figure.

   If there are more than two SIP Conditions, the logical Expression is evaluated from left to right. For example:

   - "A AND B OR C" is calculated as (A AND B) OR C.
   - "A OR B AND C" is calculated as (A OR B) AND C.
   - “A OR B AND C OR D” is calculated as ((A OR B) AND C) OR D.

3. Define the fields of the new SIP Condition according to the parameter descriptions in the previous table.

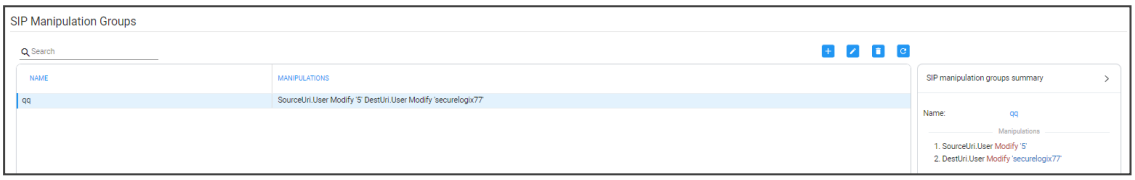
After a SIP Condition Group is defined, you can attach it to a:
- Policy Studio (User type) > Conditions
- Routing Rule > Advanced Conditions
- SIP Manipulation Group

Adding a SIP Manipulation Group

The SIP Manipulation feature enables the manipulation of SIP headers fields from the incoming Get-Route request message. A SIP Manipulation Group can comprise one manipulation or multiple manipulations. If there are manipulation rules in a group, they're performed in the order they're listed.

➢ To add a SIP Manipulation Group:

1. Open the SIP Manipulation Groups page (**Settings** > **Call Flow Configurations** > **SIP Manipulation Groups**).



2. Click the **Add +** icon.

3. Use the following table as reference:

Parameter	Description
Name	Enter an intuitive SIP Manipulation Group name.
Condition Group	Select a predefined SIP Condition Group that must exist for the manipulation rule to be applied.
Action Subject	Define the message component on which the manipulation is performed. You can use the built-in syntax editor to help you configure the field. See also SIP Manipulation Syntax on page 408 for information about the syntax to use.
Action Type	Define the type of the action: ■ Add – Add a new Action Subject with the Action Value. ■ Remove - Deletes the Action Subject. ■ Modify - Sets the Action Subject to an Action Value. ■ Add Prefix - Adds the Action Value to the beginning of the Action Subject.

Parameter	Description
	■ Add Suffix - Adds the Action Value to the end of the Action Subject. ■ Remove Prefix - Remove the Action Value from the beginning of the Action Subject. ■ Remove Suffix - Remove the Action Value from the end of the Action Subject. ■ Normalization - Run a Normalization Group on the Action Subject. ■ Random From Pool – Replace the Action Subject with a number from a pool (only for users). ■ Send By Web-Service - Can be activated with 'Http.Request'; as soon as it is selected and a web-service is selected, a new line is opened for sending the request. The 'Add' action is performed only if the Action Subject doesn't exist in the incoming SIP headers. For example, you cannot add Header.From.Name to "bob <sip:1000@1.1.1.1:5600>" TO header. Use Modify action instead. The Modify action is performed only if the Action Subject exists in the incoming SIP headers. For example, you cannot Modify Header.From.Name on "<sip:1000@1.1.1.1:5600>" TO header. Use Add action instead.
Action Value	Defines a value that you want to use in the manipulation. Each string value must be enclosed by a single quotation mark ('...'). To concatenate values, use the plus "+" operator. You can use the built-in syntax editor to help you configure the field.
Description	Enter a brief description of the SIP Manipulation Group.

➢ To add a SIP Manipulation to a SIP Manipulation Group:

1. In the SIP Manipulation Groups page, click the **Add +** icon.

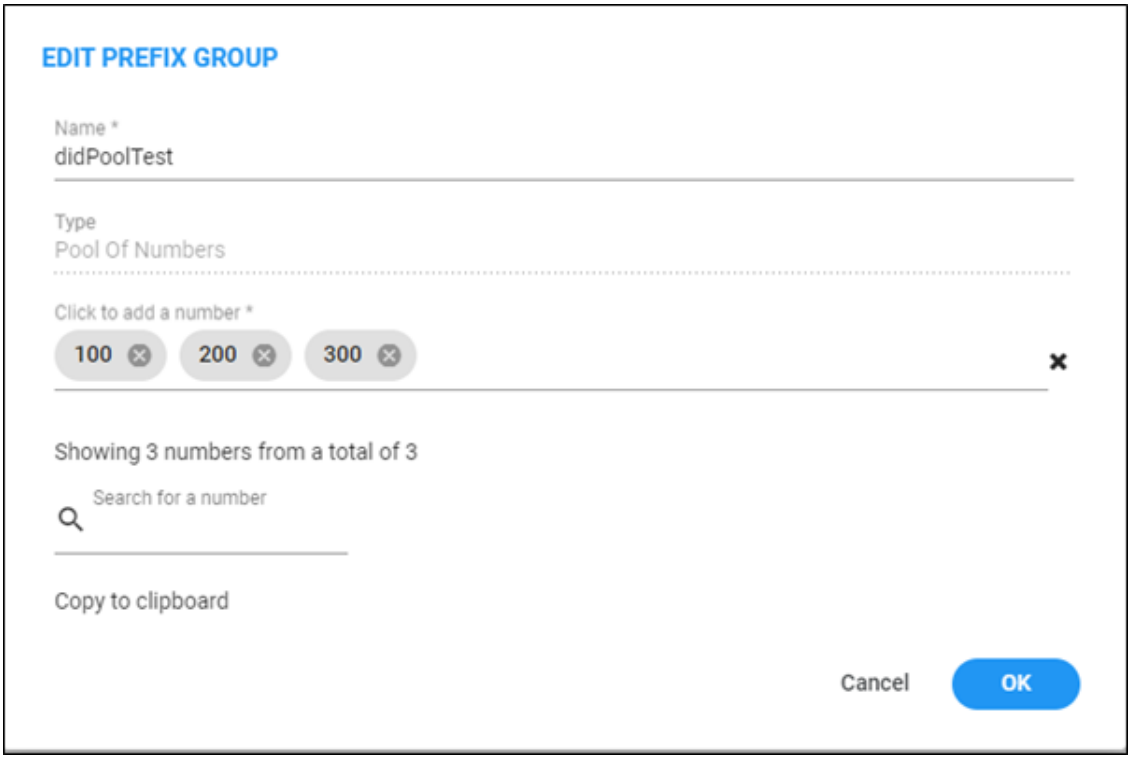
2. Define the fields of the new SIP Manipulation according to the parameter descriptions in the preceding table. The preceding figure shows two SIP Manipulations in a SIP Manipulation Group.

> After a SIP Manipulation Group is defined, you can attach it to a:
> - Policy Studio (User type) > Action
> - Routing Rule > Action
>
> While a Policy Studio rule performs SIP Manipulation Group, the manipulated values are updated for all routes. A SIP Manipulation Group that calls from a Routing Rule Action affects only the current route.

The ARM GUI displays the manipulation in the Calls Details page.

Manipulating User Part of Header by Randomly Picking Number from Pool

ARM provides the ability to manipulate a user part of a header by picking a number from a pool of numbers. The pool of numbers is defined in a Prefix Group.



The Prefix Group shown in the preceding figure is a pool of the numbers: 100,200,300. Range (such as 400-450) is not supported.

Operators can manipulate the user part of the SIP header by replacing it with a random number from a predefined pool of numbers. The SIP Manipulation shown in the figure below replaces the Source URI User with a random number from the 'didPoolTest' pool:

The feature is part of the SIP Manipulation feature and therefore can be used from Policy Studio Action and from Routing Rule Action.

Routing Settings

These are the Routing Settings that network administrators can configure:

- Criteria for a Quality Profile (see Configuring Criteria for a Quality Profile)
- Time-Based Routing Condition (see Configuring a Time-Based Routing Condition)
- Alternative Routing SIP Reasons (see Configuring Alternative Routing SIP Reasons)
- Global Routing Settings (see Configuring Global Routing Settings)

- Registration Routing Settings (see Registration Routing Settings)
- Calls Quota (see Calls Quota)
- CAC Profiles (see CAC Profiles)

Configuring Criteria for a Quality Profile

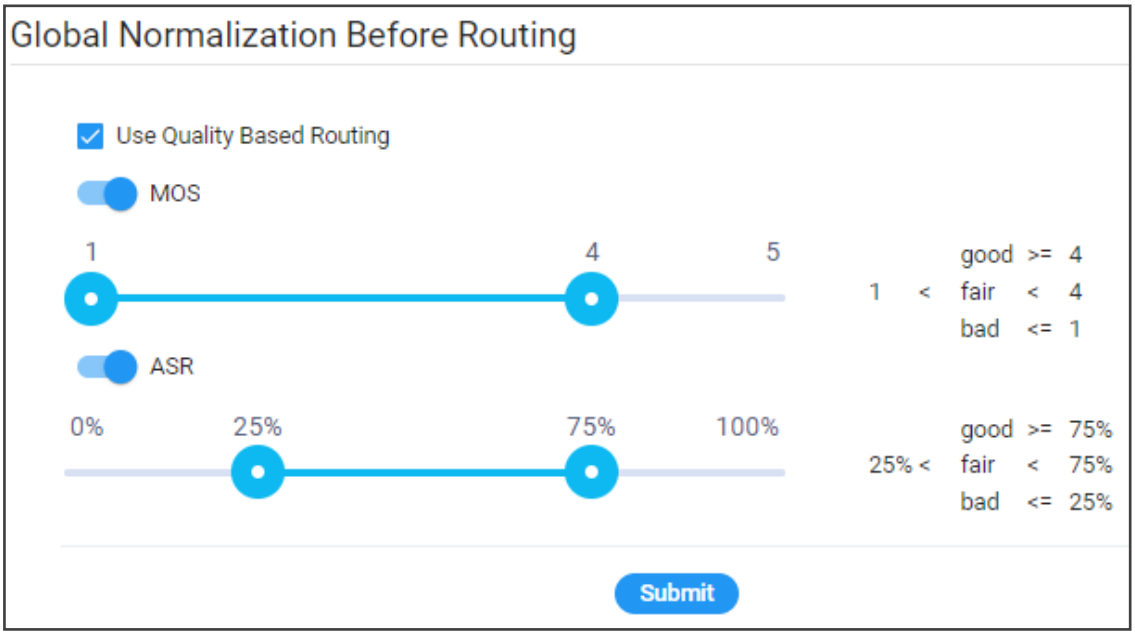
You can configure criteria for a quality profile for bad, fair or good call paths based on the calculation of MOS and ASR. You can configure a specific Peer Connection to exclude either the MOS or the ASR criterion (see Peer Connection Information and Actions on page 48). After enabling 'Use Quality 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 328) 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 Global Normalization Before Routing screen (**Settings** > **Routing** > **Quality Based Routing**). By default, **Use Quality Based Routing** is selected. If it isn't, select it.

Figure 7-62: 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 7-22: 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 328).

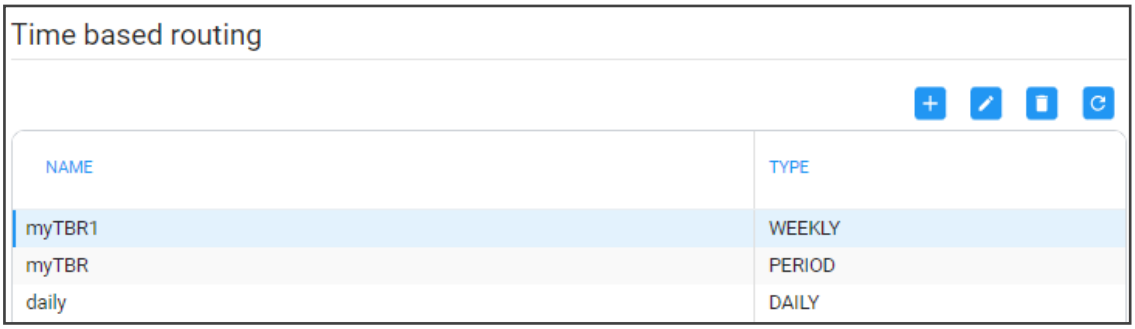
Configuring a Time-Based Routing Condition

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 328 under 'Advanced Conditions').

➢ **To configure a time-based routing condition:**

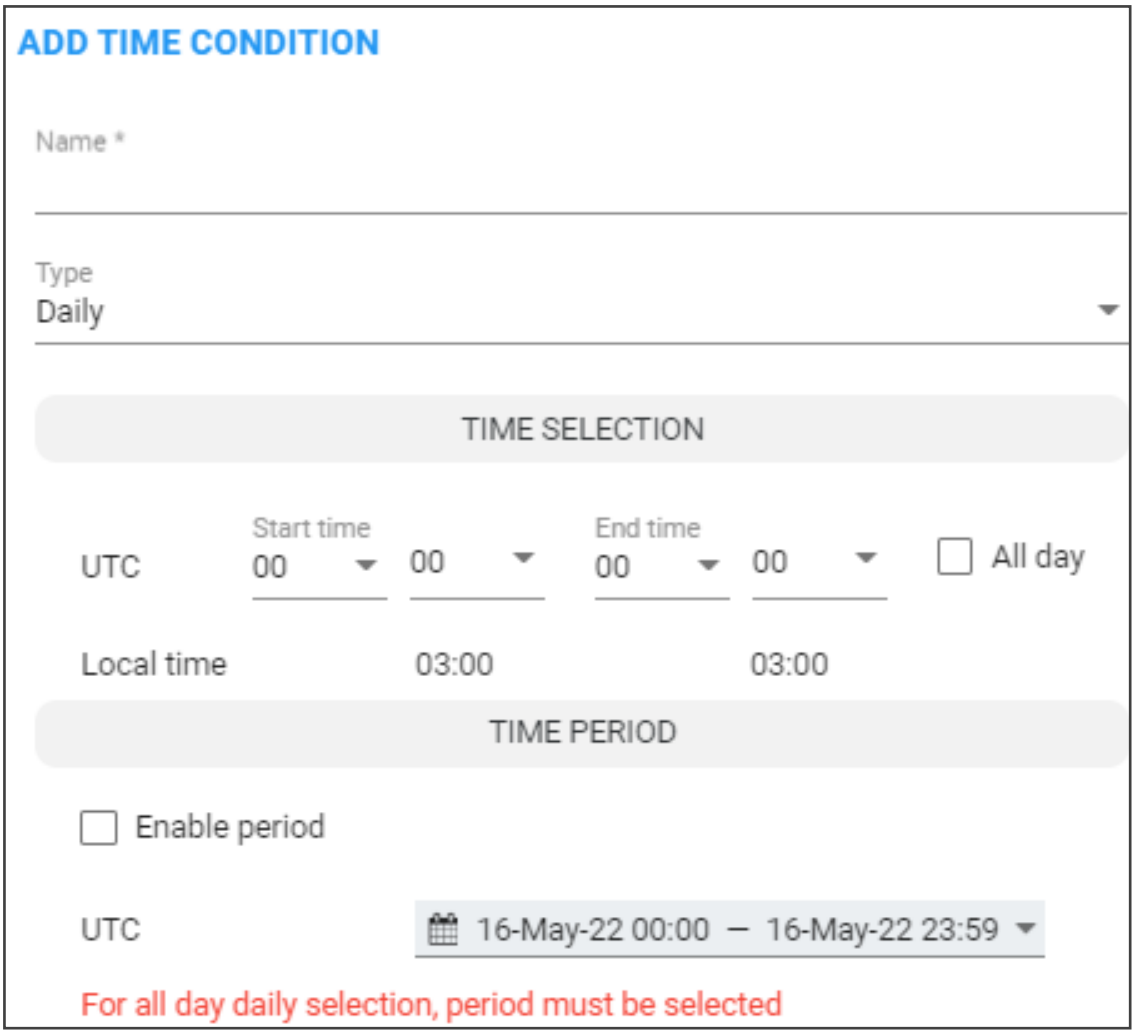
1. Open the Time-Based Routing screen (**Settings** > **Routing** > **Time Based Routing**).

Figure 7-63: Time based routing



2. Add a time-based routing condition: Click the **add +** icon.

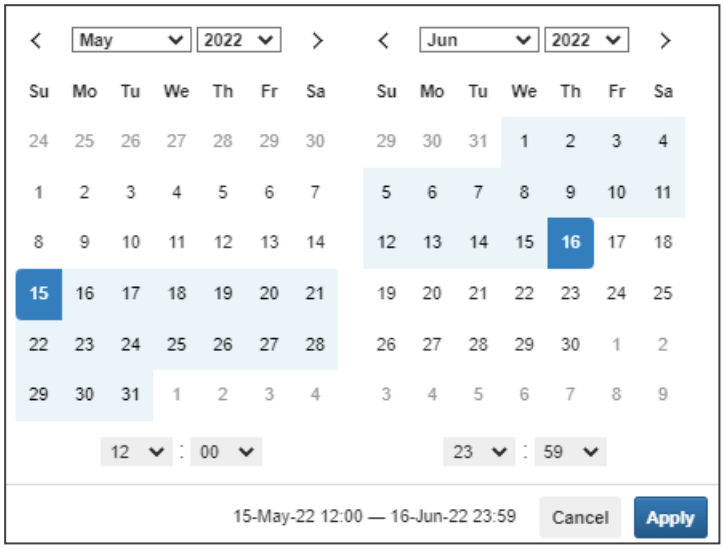
Figure 7-64: Add Time Condition



3. Configure a time-based routing condition. Use the following table as reference.

Table 7-23: Time Condition Settings

Setting	Description
Name	Enter an intuitive name to later easily identify the condition.
Type	Select either **Daily** or **Weekly**. ■ Daily - This is a daily recurring period. ■ Weekly - This is a period recurring on given days of the week.
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.

Setting	Description
Enable period	Select this option to base the routing condition on a period.
Start of period End of period	Click the calendar icon and select the date on which the period will *start*; from the drop-downs, select the hour and the minutes past the hour.  Select the date on which the period will *end*; from the drop-downs, select the hour and the minutes past the hour and then click **Apply**.

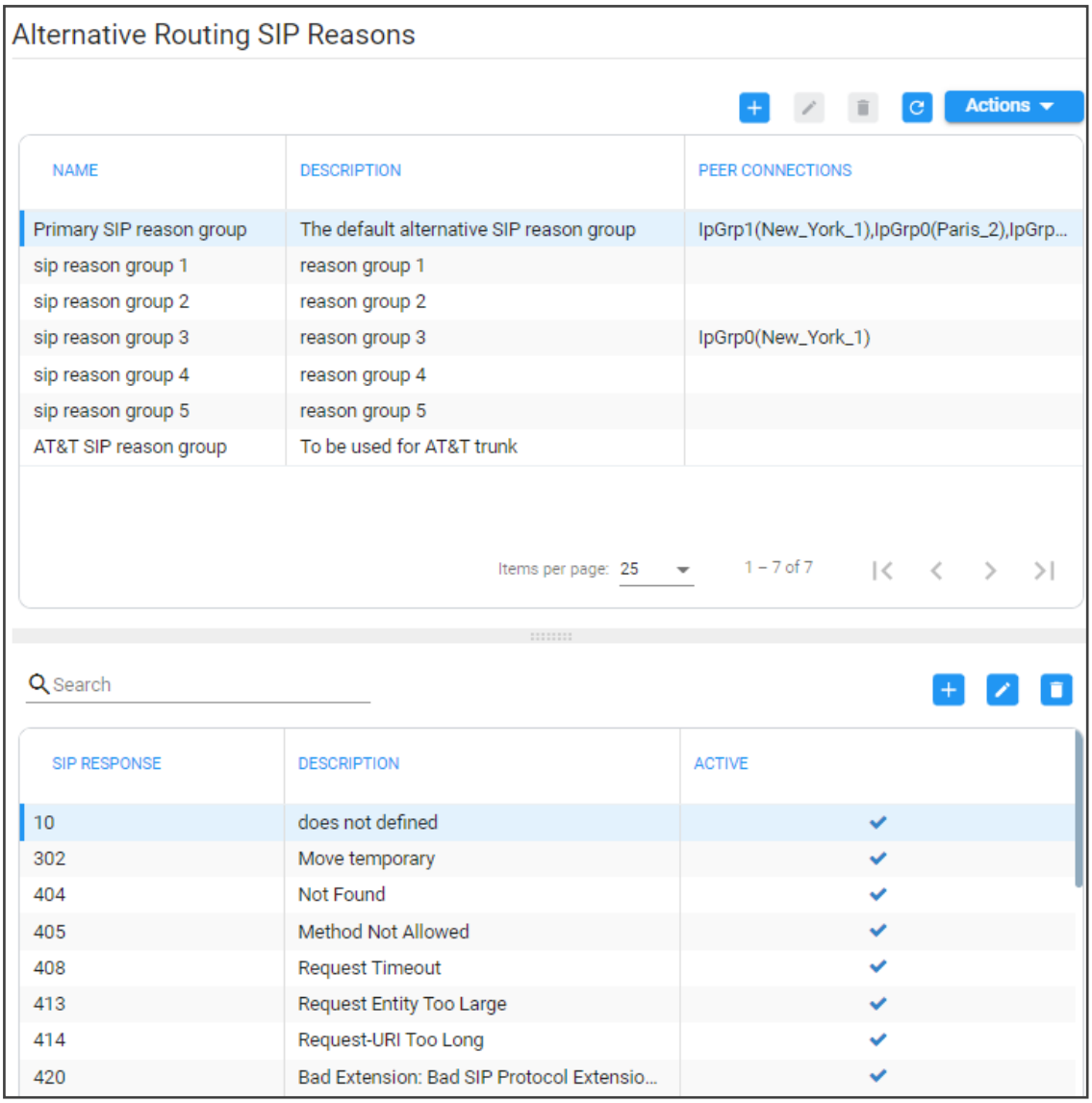
4. Click **OK**.

- A profile is now generated which you can associate with a Routing Rule (see Adding a New Routing Rule on page 328 under 'Advanced Conditions').
- Also, the configured time condition can be associated with a Routing Group. In this case, it will apply to *all* Routing Rules in the Group.
- The same time condition profile can be reused multiple times.

Configuring Alternative Routing SIP Reasons

Operators can configure SIP responses in the Alternative Routing SIP Reasons page (**Settings** > **Routing** > **Alternative Routing SIP Reasons**), in the SIP RESPONSE section; the ARM will then apply alternative routing paths if available. SIP reasons for call re-routing are globally configured here. If a SIP reason in this section is activated, the ARM tries to perform alternative routing if this SIP reason is returned at the initial routing failure.

Figure 7-65: Alternative Routing SIP Reasons



Operators, however, sometimes need to apply different *sets* of SIP reasons for alternative routing, *per Peer Connection*, mainly due to the different flavors in the handling of alternative routing with PBXs or specific SIP trunks and Service Providers. The upper section of the page provides this functionality. So in addition to the global (default) settings in the lower section of the page under SIP RESPONSE, operators can provide a different *set* of SIP reasons for alternative routing *per Peer Connection*.

Operators can define several 'SIP reasons groups' in the upper section of the page. See Configuring a SIP Reason Group on page 296 for more information. By default, there is a 'Primary SIP reason group' attached and activated for the entire ARM (for all ARM Peer Connections).

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

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

➢ To configure an Alternative Routing SIP Reason:

1. In the lower section of the Alternative Routing SIP Reasons page (**Settings** > **Routing** > **Alternative Routing SIP Reasons**), under SIP RESPONSE, click the **add +** icon.

Figure 7-66: Adding an Alternative Routing SIP Reason

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

➢ 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 the **edit** icon.

Figure 7-67: Editing an Alternative Routing SIP Reason

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

> By clearing the 'Active' option, the operator can 'deactivate' a SIP reason without deleting its row in the table. If a SIP reason is 'deactivated', the ARM will not apply an alternative route. The ARM will function as if there is no row at all. The 'deactivated' row, however, remains in the table, and if the operator re-decides, it can be 'reactivated' by selecting the 'Active' option.

➢ **To delete an Alternative Routing SIP Reason:**

- In the Alternative Routing SIP Reasons screen, select the SIP response to delete and then click the **delete** icon.

Configuring a SIP Reason Group

Operators can define several 'SIP reasons groups' in the upper section of the Alternative Routing SIP Reasons page (**Settings** > **Routing** > **Alternative Routing SIP Reasons**). By default, there is a 'Primary SIP reason group' attached and activated for the entire ARM (for all ARM Peer Connections). Additional groups can be defined, either from scratch or duplicated from an existing group, and later attached to a specific Peer Connection (or several Peer Connections). Operators can:

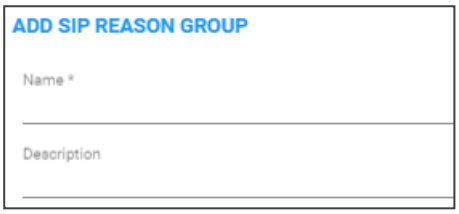
- Add a new group (with an empty SIP reasons table)
- Duplicate group
  - Change the name of the group.
  - View the SIP reasons section and select/unselect the values.
- Edit group
  - Edit the name and description of the group.
  - Delete group (the default 'SIP reason group' cannot be deleted)
  - Refresh

Each 'SIP reason group' has the following properties:

- Name
- Description
- Peer Connection that contains the 'SIP reason group'.

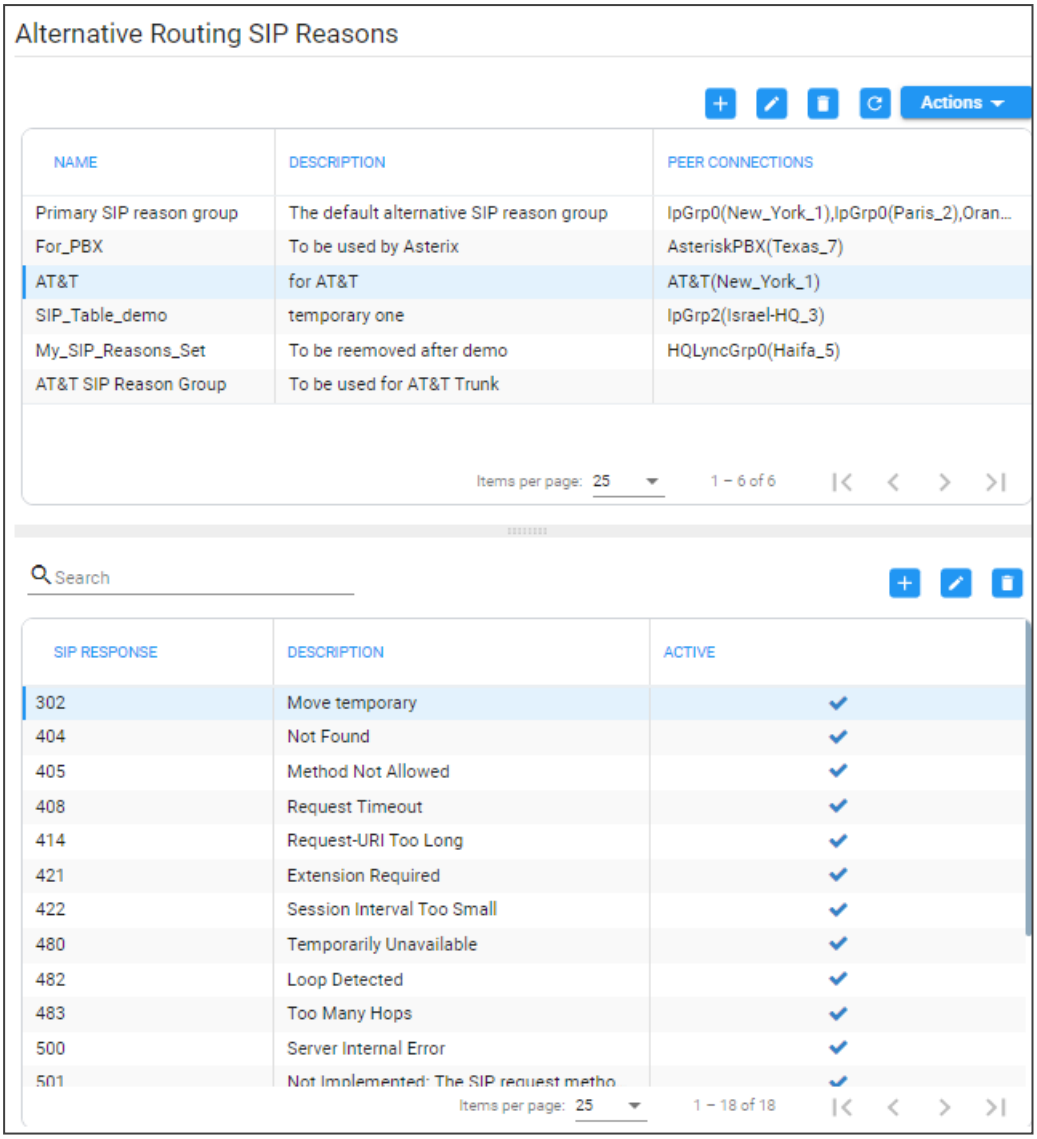
➢ To add a SIP Reason Group:

1. In the upper section of the Alternative Routing SIP Reasons page (**Settings** > **Routing** > **Alternative Routing SIP Reasons**), click **Add**.



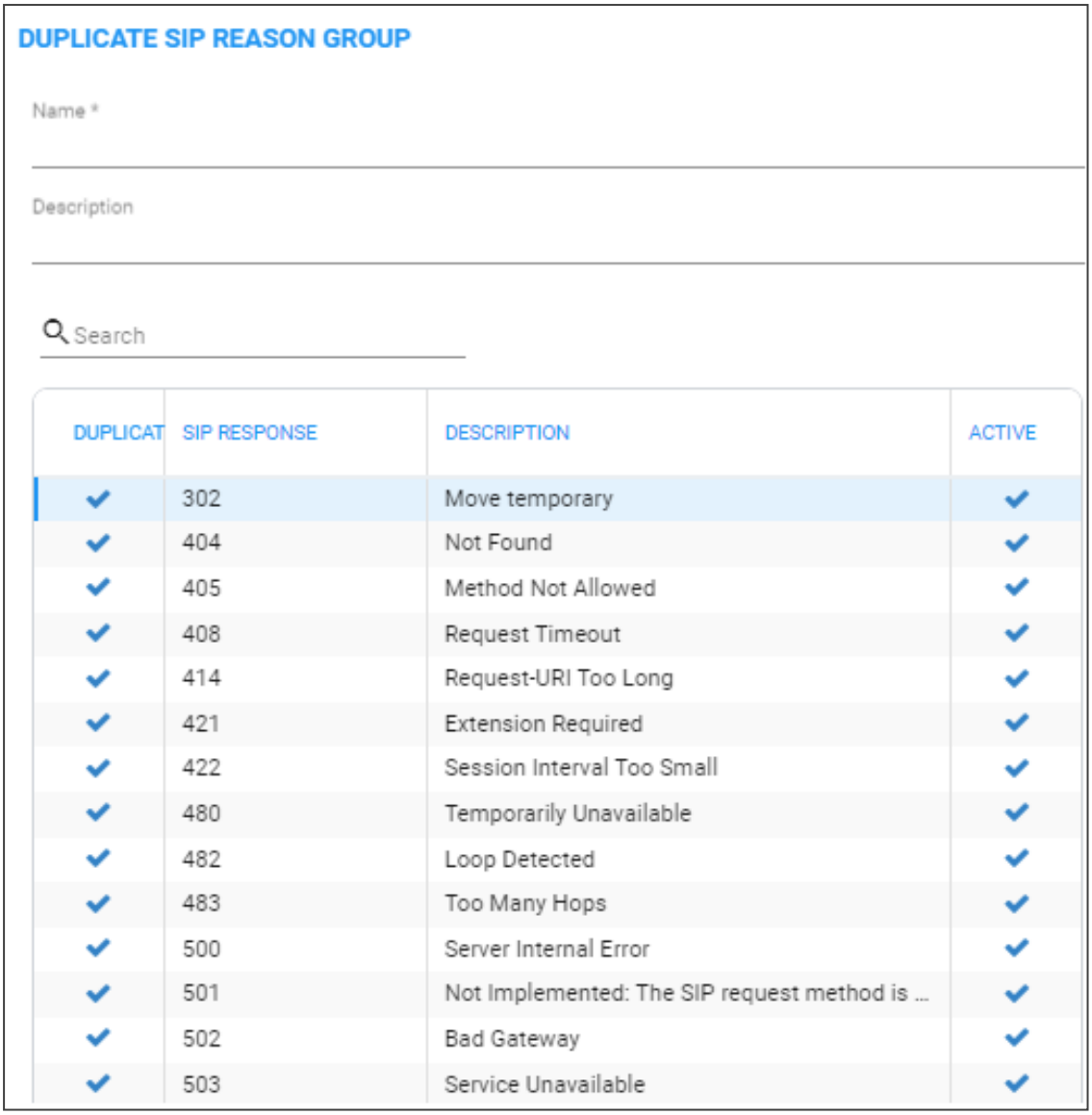
2. When adding (or editing) a group, provide a name for the group and an optional description.

3. Select a group and then select a SIP Response.



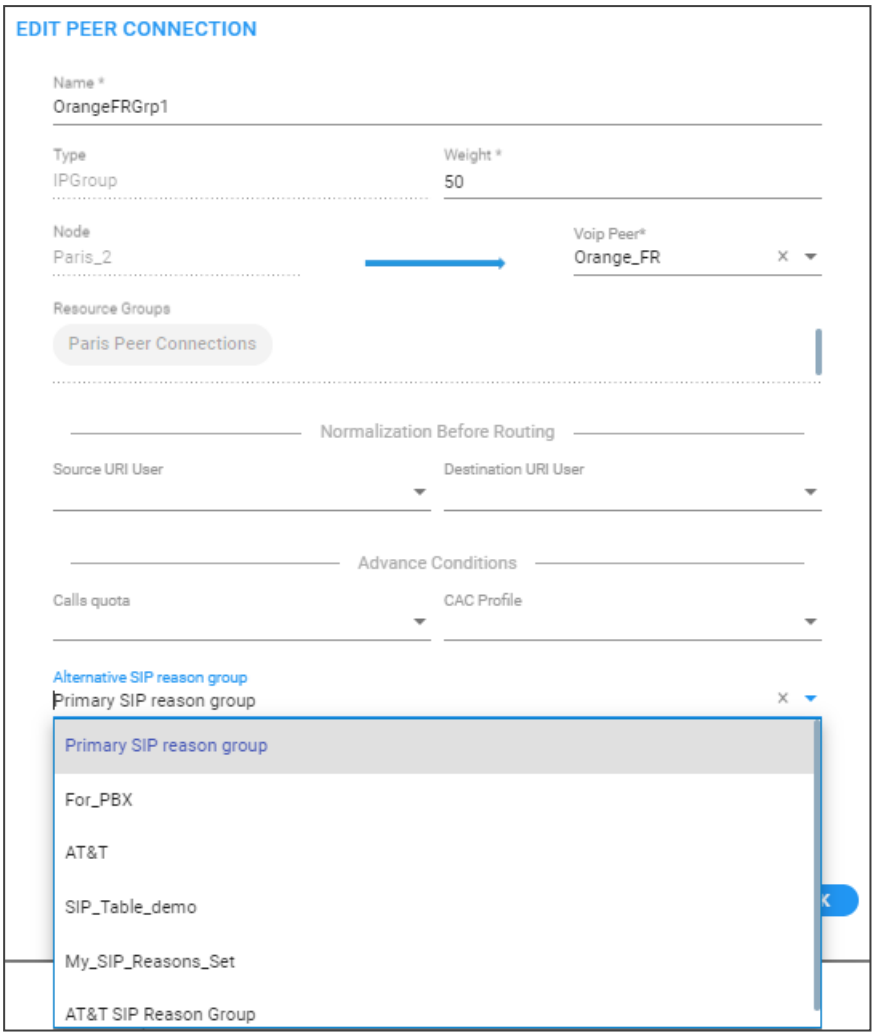
4. Click the edit icon to view and edit the group's SIP reason that is then displayed.

5. To duplicate an existing SIP Reason Group, select the group to duplicate and from the 'Actions' drop-down, select **Duplicate**.



6. Provide a new unique name and an optional description to facilitate effective management later.
7. Attach a newly-defined SIP reason group to one or more Peer Connections (using both Add and Edit screens), either in the Network Map page or from the Peer Connections page:

Figure 7-68: Attach a SIP Reason Group to Peer Connection/s



8. View the 'SIP reason group' in the Peer Connections Summary in the Peer Connections page (**Network** > **Peer Connections**). The indication of Peer Connection associated with the group is shown in the 'Alternative SIP Reason' column.

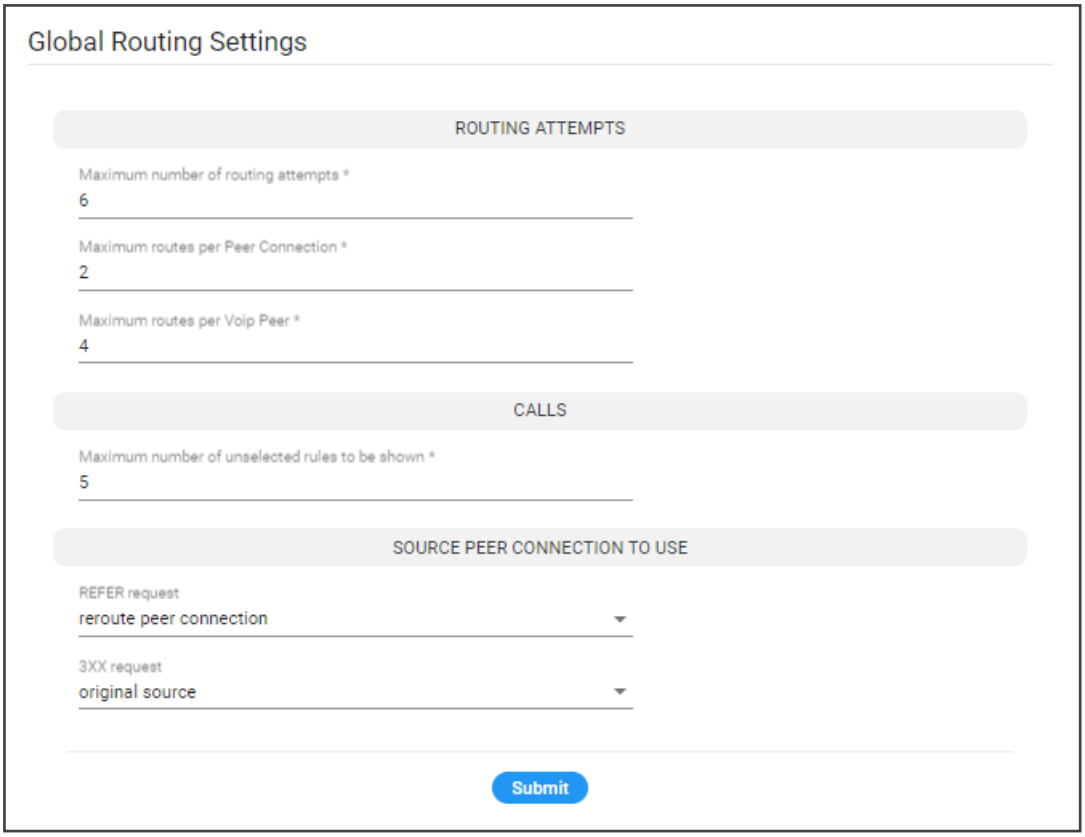
> By default, all Peer Connections are associated with the default 'Primary SIP reason group'.

Configuring Global Routing Settings

The ARM enables network operators to configure routing settings that take effect globally.

➢ **To configure global routing settings:**

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



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

Table 7-24: Global 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 routes per Peer Connection	Defines the maximum number of routing attempts per Peer Connection. If the maximum number of routing attempts has not yet been reached, the ARM tries to re-route the call to a preferable Peer Connection. Default: 2 attempts.
Maximum routes per VoIP Peer	Allows operators to determine the maximum number of routing attempts per VoIP Peer for a specific call. Default: 4.
Maximum number of unselected rules to be shown	Allows configuring for calls a maximum number of unselected Routing Rules / Policies. The default value is 5, limited to a maximum of 25 unselected rules per call.

Setting	Description
REFER request	Configure the value of the source Peer Connection for REFER requests: ■ Original Peer Connection ■ Reroute Peer Connection
3XX request	Configure the value of the source Peer Connection for 3XX requests: ■ Original Peer Connection ■ Reroute Peer Connection

3. Click **Submit**.

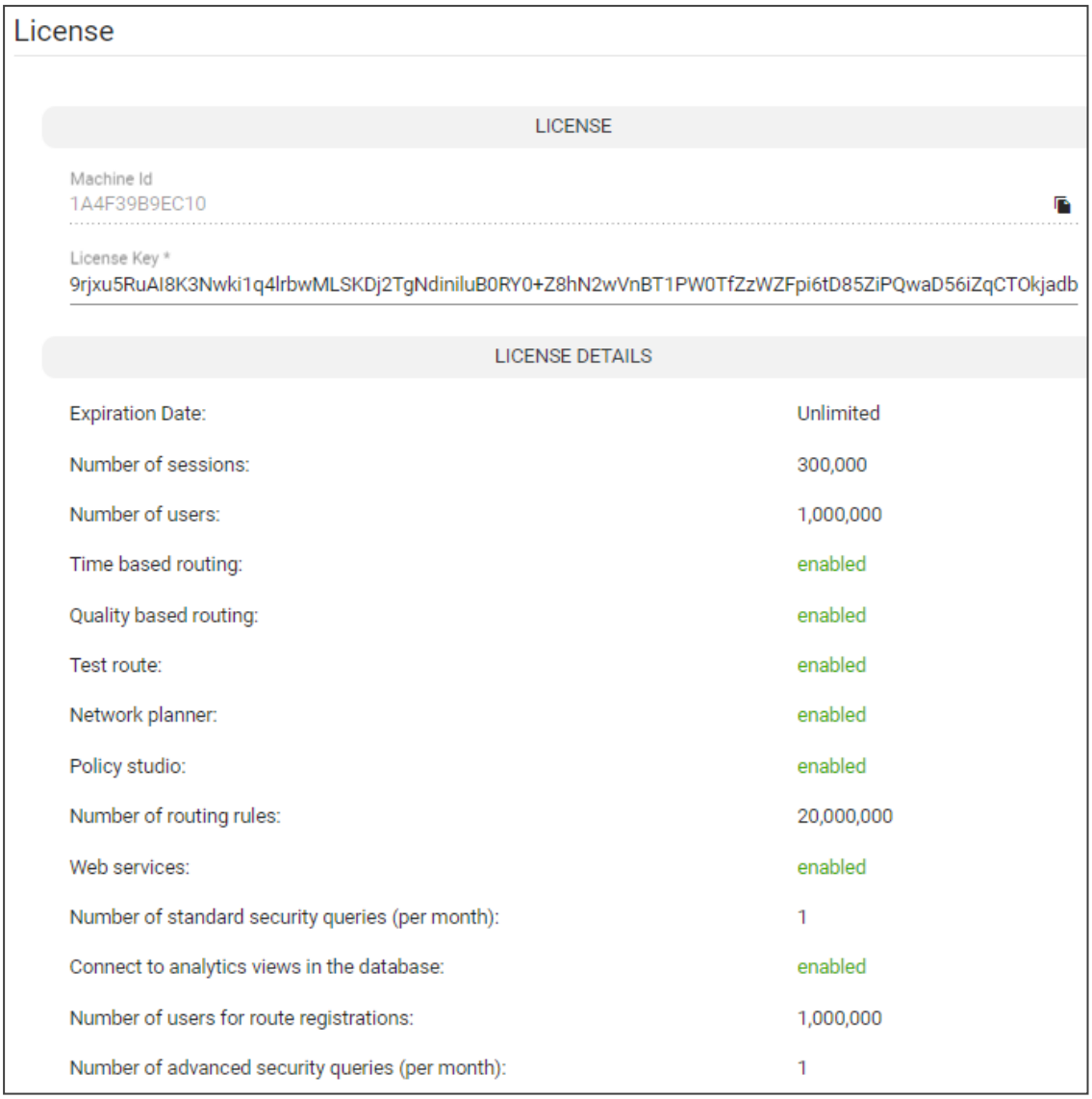
Registration Routing Settings

The ARM allows operators to route registration messages using any Dictionary Property mapped to a value of **True** / **False**.

➢ **To perform registration routing:**

1. In the License page (**Settings** > **Administration** > **License**), make sure the number of registered users (telephones) you require is configured for the parameter 'Number of users for route registrations'.

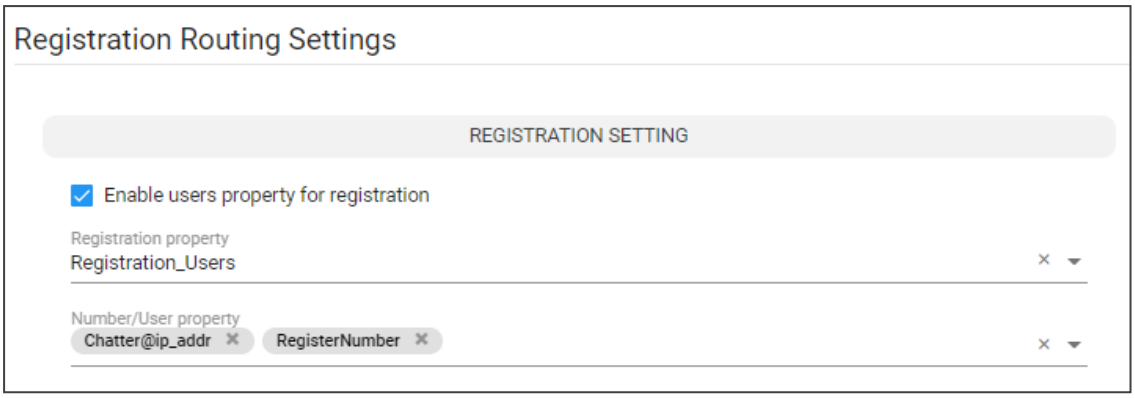
Figure 7-69: Number of users for route registrations



Make sure the number defined for 'Number of users for route registrations' does not exceed the number defined for 'Number of users' (see the preceding figure). The number defined for ‘Number of users for route registration’ will only be displayed after you purchase the number of users (telephones) for registrations routing you require. If there is no license for ‘Number of users for route registration’, the settings described below will not be relevant.

2. Open the Registration Settings page (**Settings** > **Routing** > **Registration Settings**).

Figure 7-70: Registration Routing Settings



3. Use the table below as reference when defining the settings for routing registration messages in the ARM.

Table 7-25: Registration Routing Settings

Setting	Description
Enable users property for registration	Must be switched on for enabling the Registrations routing feature.
Registration property	This property determines whether the user (phone / host) will be used for routing the registration message. It can be any Dictionary Property mapped to a value of **True** / **False**.
Number/User property	This property is used by the ARM to identify a specific user/telephone registration for Registration routing. It's usually a combined attribute comprising User@Host attributes. Note that this is the identification information ARM gets from SBCs for Registration routing. Note also that more than one property can be selected from the user dictionary. In this case, the ARM will route the Registration message if there is a match with any of them.

Changes to users are not reflected instantly in the Router. The Router is updated periodically (every 30 minutes) so if there is any change to a user's registration property, number or user property, it will not be reflected immediately.

Calls Quota

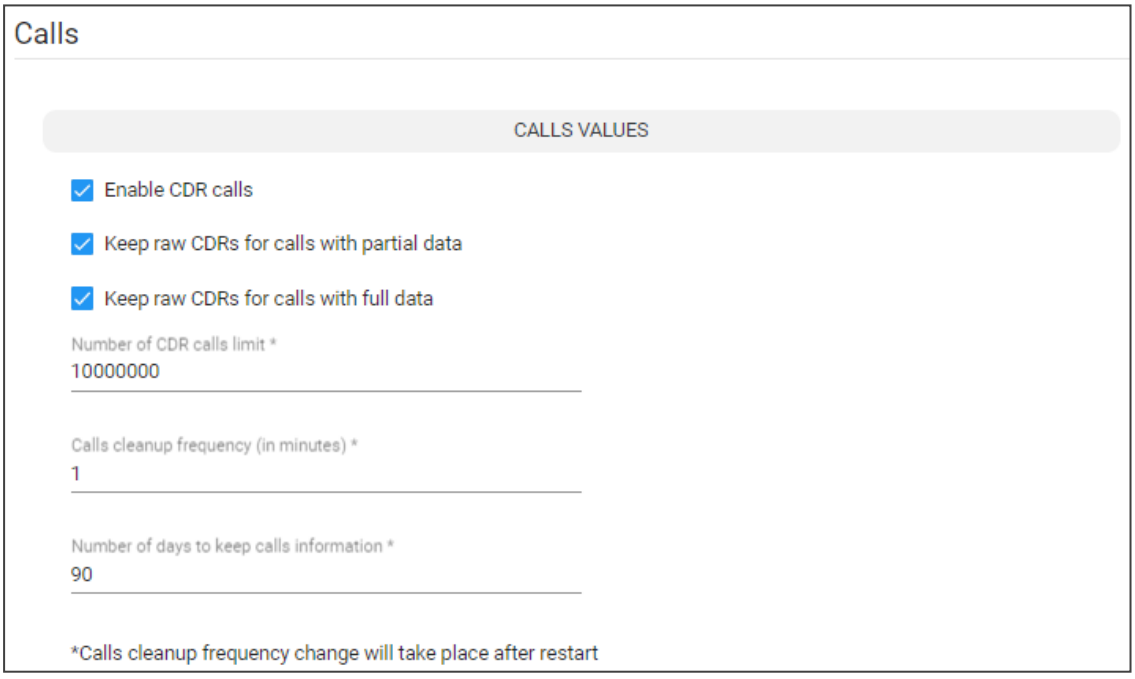
The ARM allows you to put a quota on calls duration in minutes, on either a single Peer Connection or on a group of Peer Connections.

Using the ARM GUI or northbound REST API, you can define a time limit on calls, in minutes, and periodicity. Based on these definitions, you can define an action to block outgoing calls if

the quota (limit) is reached, to be automatically applied by the ARM. An alarm is always generated if the limit is reached.

When applying the feature:

- The quota can be attached to either a single Peer Connection or to a group of Peer Connections gathered in a Resource Group of type 'Peer Connection'.
- The ARM counts only outgoing calls time (outgoing Peer Connections).
- You can define an alternative route (an Action in a Routing Rule) with an alternative Peer Connection if they want to handle a call when the primary Peer Connection is blocked due to the quota being reached.
- The ARM starts counting calls minutes from the moment the quota is attached to the Peer Connection or set of Peer Connections (and not from the beginning of the interval).
- Emergency calls are allowed regardless of the quota (even if the resource is blocked).
- If a customer wants to reset the quota, they can detach the quota from the entity or edit an existing one (increase the numbers, for example).
- The 'CDR calls' feature must be enabled in the ARM (**Settings** > **Advanced** > **Calls** and then select the option **Enable CDR calls**).

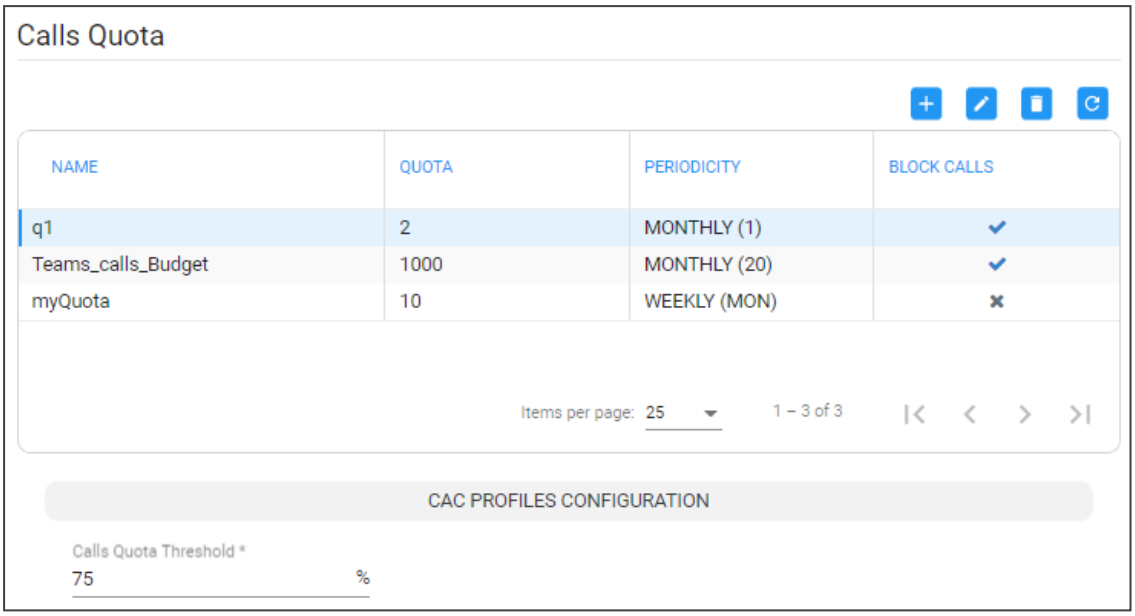


The ARM uses calls information to get every call's duration and calculates the accumulated minutes of all calls per Peer Connection.

In rare cases, a call duration might go missing (if a specific call is not present in the CDRs for some reason).

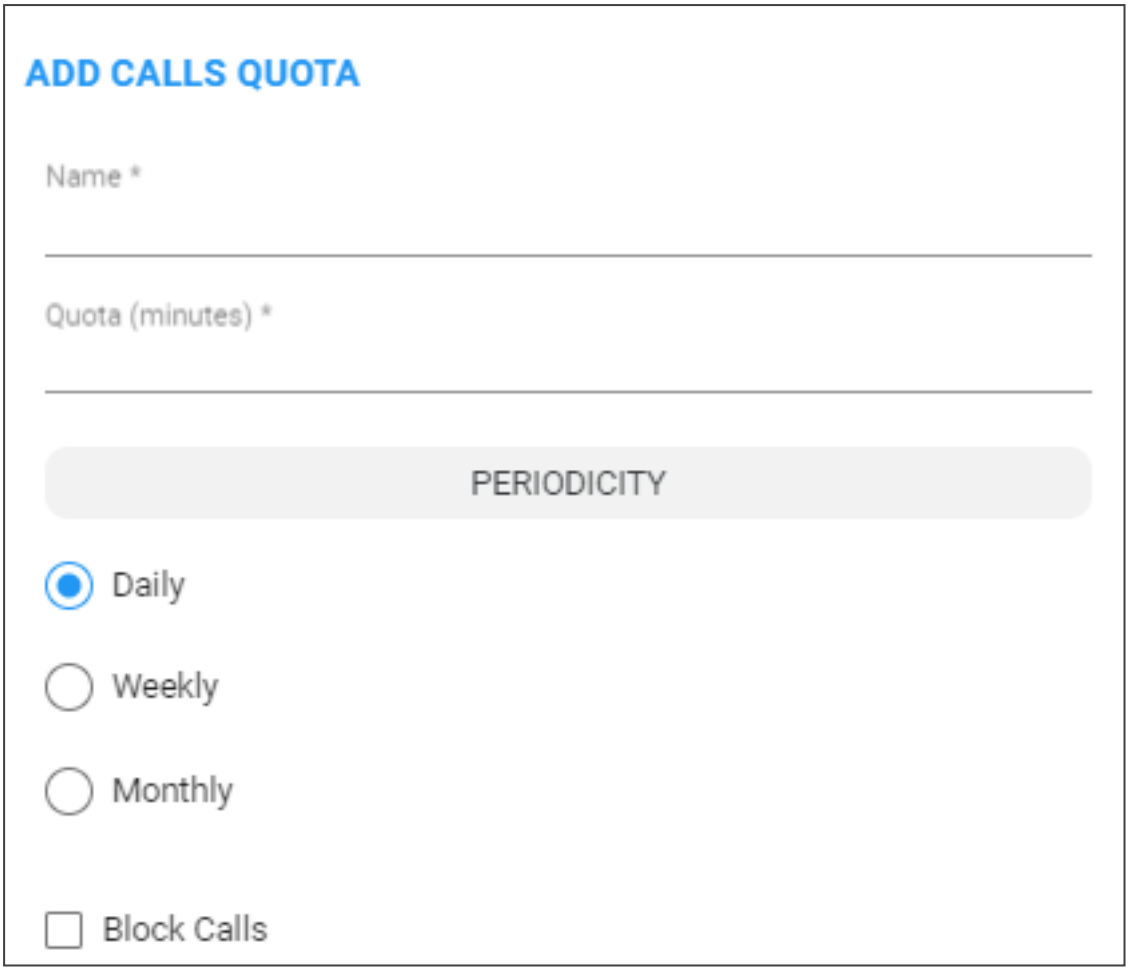
➢ To add a quota:

1. Open the Calls Quota page (**Settings** > **Routing** > **Calls Quota**).



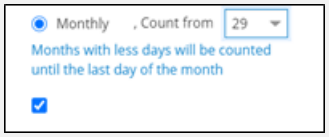
The Calls Quota page summarizes all defined quota information. The following options are available after selecting an already defined quota: **+** to add a new Quota (row); edit to edit an existing Quota's settings; delete ; and refresh .

2. Click **+**.

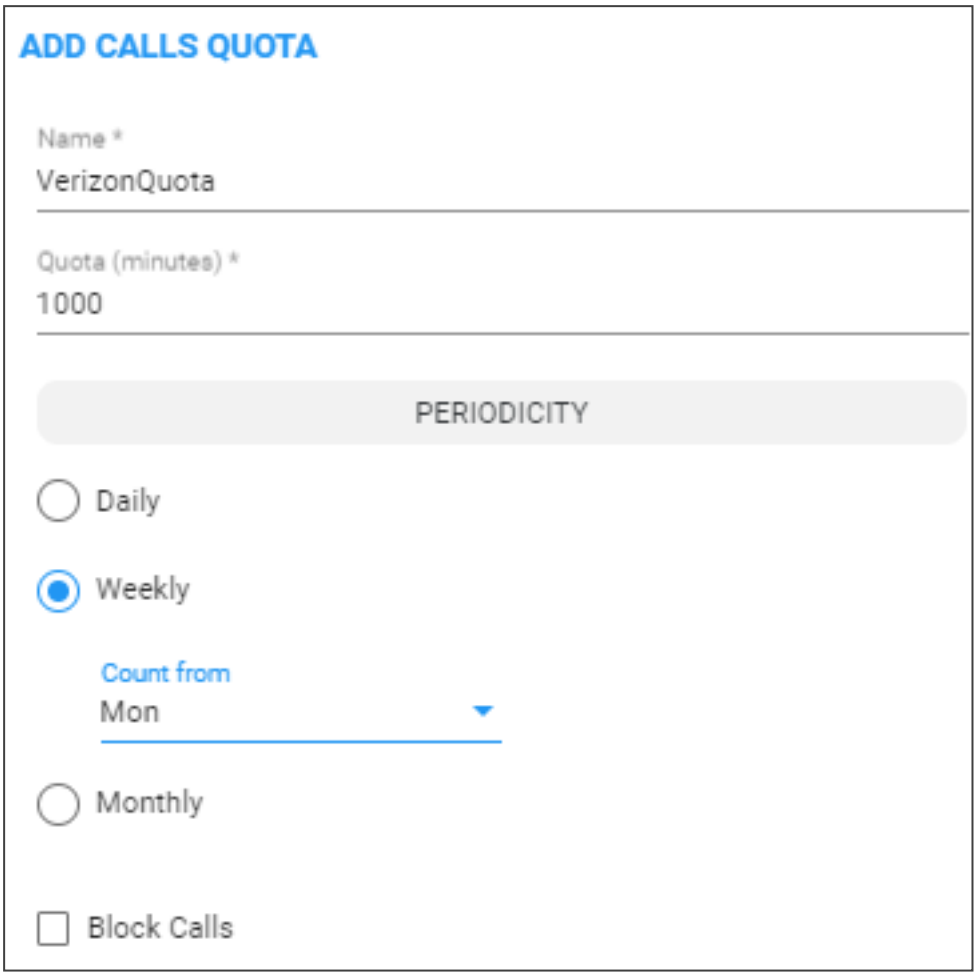


3. Define an intuitive unique 'Name' for the quota (mandatory).
4. Define 'Quota (minutes)' (mandatory); this defines the number of minutes allowed in the selected period.
5. Define 'Periodicity', i.e., the period for the quota to be applied:
   - **Daily** – the quota count, in minutes, will be reset daily (00:00-23:59).
   - **Weekly** – the quota count, in minutes, will be reset weekly. In this case, the operator must select from which day in the week counting should start and be reset (Example: Monday).
   - **Monthly** – the quota count, in minutes, will be allocated monthly. In this case, operators must select the day in the month from which counting of the minutes starts (Example: 5 days of each month).

If you select the start day to be after the 28th of the month, you'll receive the following warning:

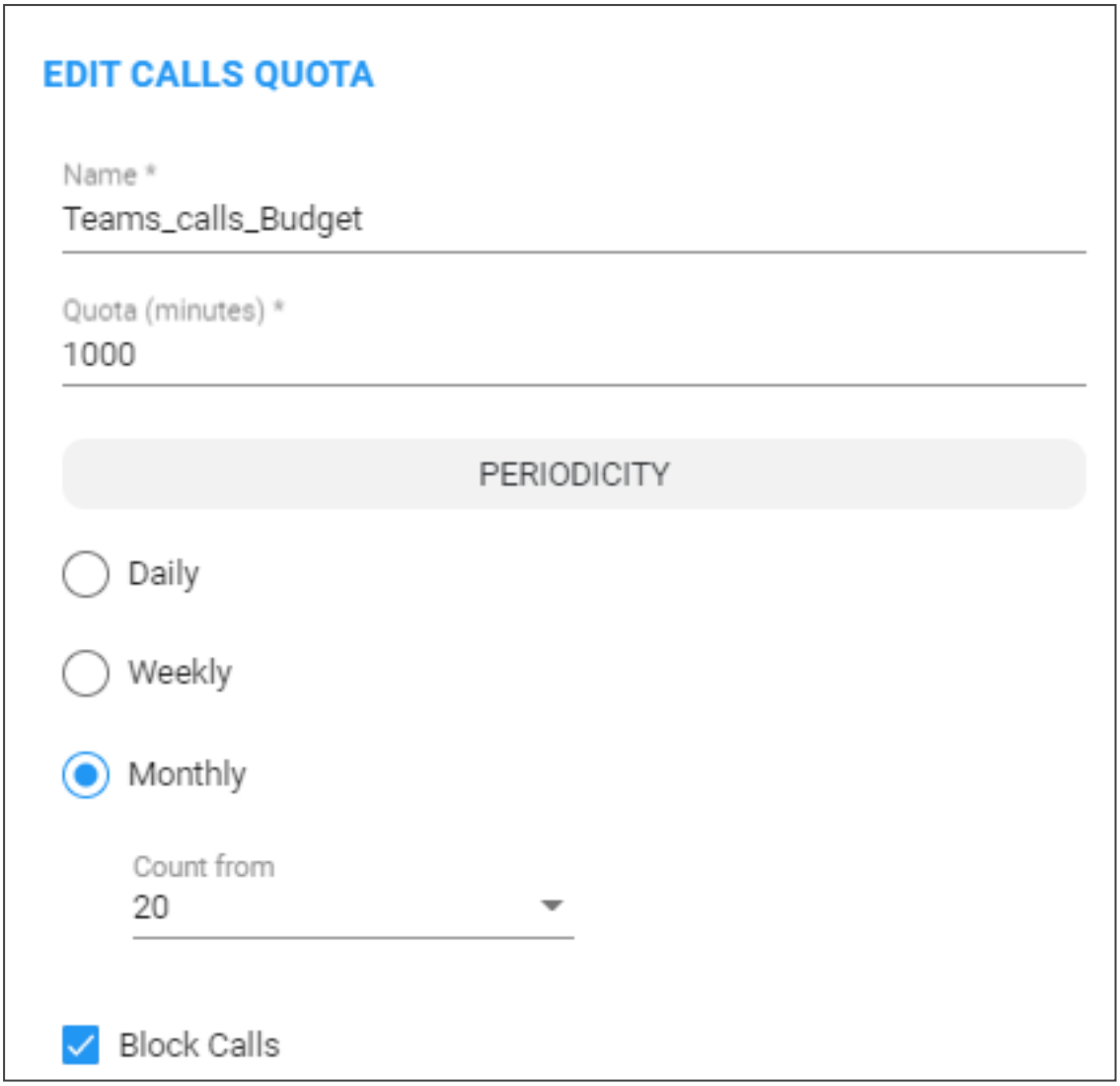


- **Block calls** – an action to be taken if the quota is reached during the specified period. If you select this option, the Peer Connection's outgoing calls - except for emergency calls - will be blocked when the calls quota is reached. Note that an alarm is always generated when a quota is reached; you cannot disable the alarm.

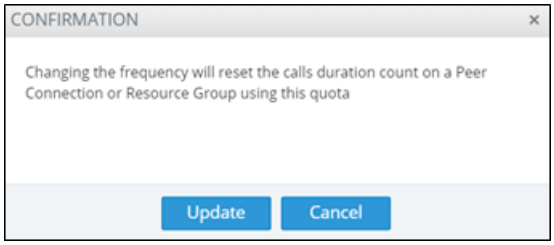


➢ **To edit an existing quota**

1. In the Calls Quota page, select the row (quota) and then click the edit icon.



All settings can be edited and reapplied. If operators change the frequency of the period when editing a quota, they must take the following into consideration:



➢ To delete an existing quota

- Click the delete icon.

> ⚠ A quota cannot be deleted while it is attached to a Peer Connection or a Resource Group. If you attempt to delete it, an error message is displayed along with the names of the specific topology elements currently using the quota.

➢ To define a Calls Quota Threshold:

- In the Calls Quota page, locate the 'Calls Quota Threshold' setting lowermost in the page and enter a percentage.

- The ARM can generate two alarms: One on hitting the Quota threshold and the other on crossing the Quota value. The ARM always generates Quota-related alarms regardless of the operator's setting to block (or not to block) a Peer Connection if the Quota is reached.
- The same threshold value (as a percentage) applies to all quotas defined in the ARM.

You can choose whether to block the Peer Connection when the Quota is reached, or not, but the ARM always generates Quota-related alarms regardless of the operator's setting to block (or not to block) a Peer Connection if the Quota balance is reached.

The following severities are supported for Quota-related alarms:

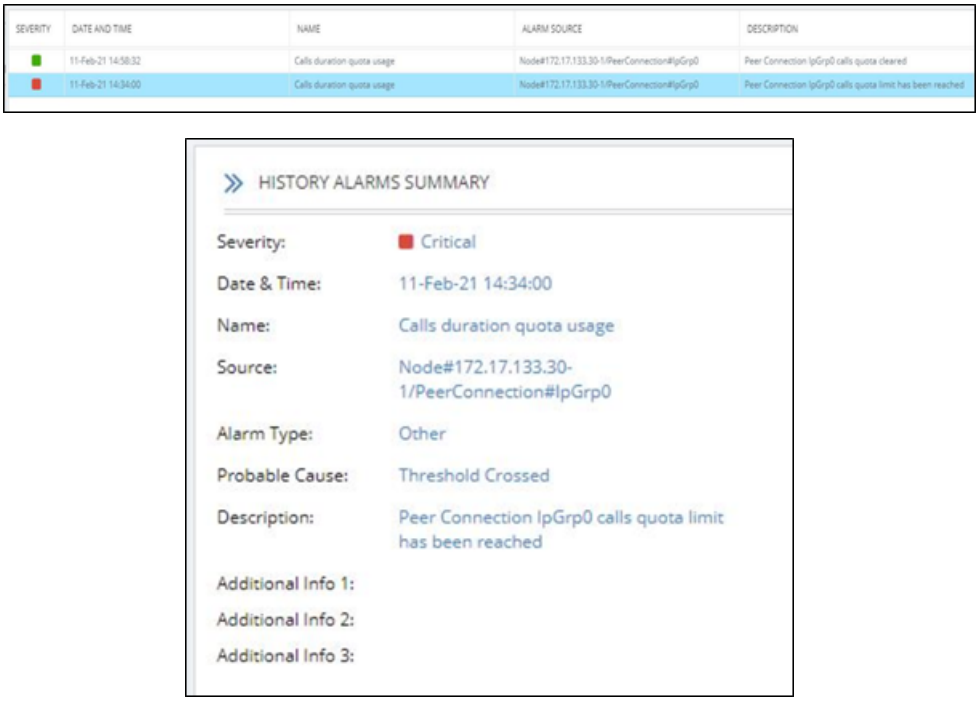
Warning – generated for a Network Topology element when the time spent by a specific Peer Connection (or Resource Group) reaches the Threshold limit (as a percentage) defined in **Settings** > **Routing** > **Calls Quota**.

Critical – generated when the Quota is reached for a specific Network Topology element (Peer Connection or Resource Group).

Clear – generated when the end of the period resets the quota for the relevant Network Topology element. The quota alarm also can be cleared when the quota is deleted from the Peer Connection or Resource Group, or when the limit or periodicity of a quota is changed.

The figure below exemplifies a generated alarm and its fields:

Figure 7-71: Quota Threshold Alarm



CAC Profiles

Call Admission Control (CAC) is the practice or process of regulating traffic volume in voice communications, usually reflected by a maximum number of allowed simultaneous sessions in the network.

The ARM allows you to define CAC Profiles that can later be attached to 'customer' entities (Teams Super Trunk tenants), Peer Connections and VoIP Peers, giving you another way to balance and control the number of sessions throughout the entire network and to prevent oversubscription.

The CAC Profiles page enables operators to optionally add a CAC profile to be later attached (for example) per 'customer' entity (see also Defining a 'Customer' Entity (Teams Tenant) on page 72).

You can limit the

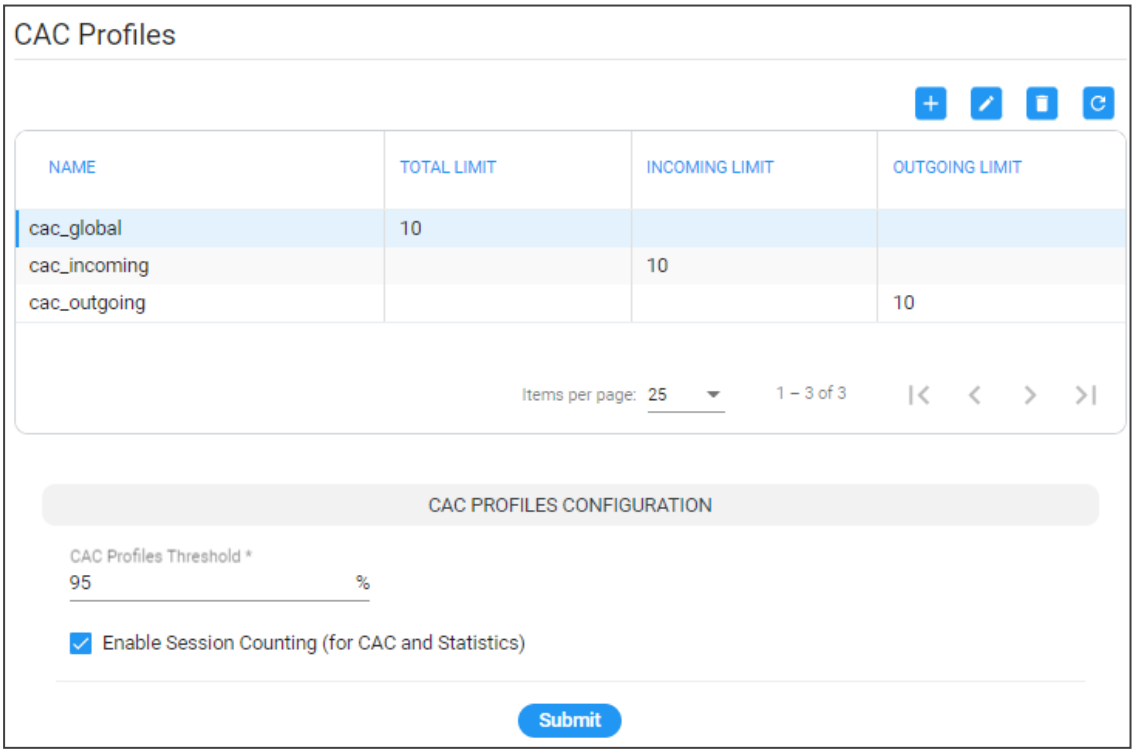
- incoming Peer Connection / Customer or the connected VoIP Peer
- outgoing Peer Connection / Customer or the connected VoIP Peer
- total session

You can also

- control the threshold of the warning alarm
- disable the entire CAC feature

➢ To add a CAC profile:

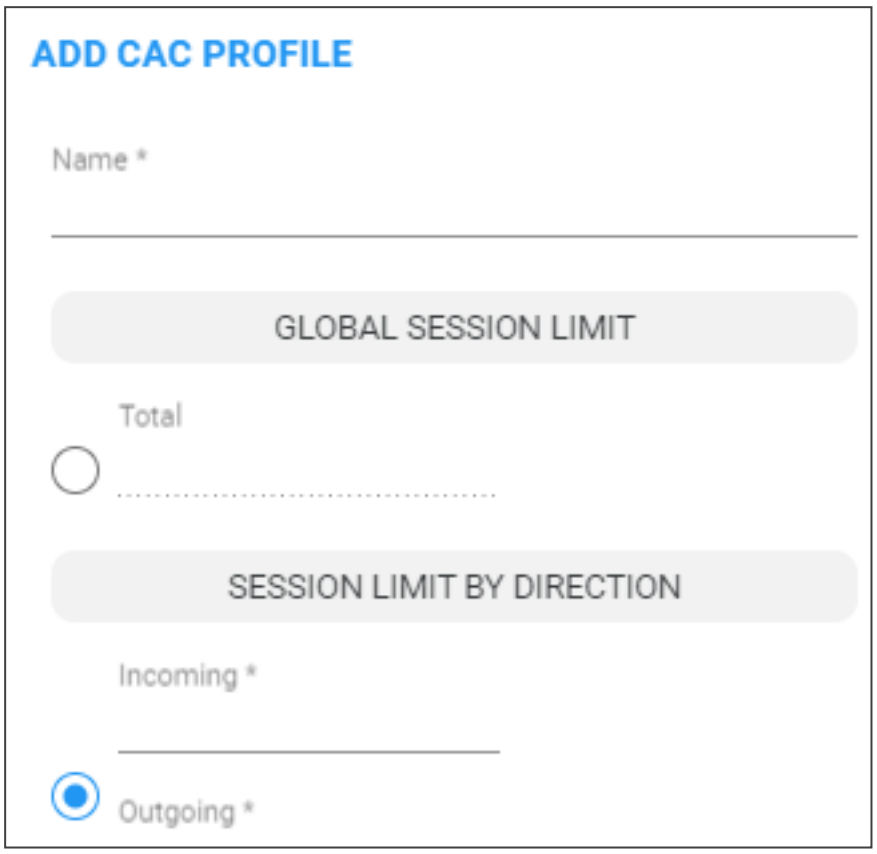
1. Open the CAC Profiles page (**Settings** > **Routing** > **CAC profiles**).



After selecting a profile (row), the actions **add +**, **edit**, **delete** and **refresh** will become available.

2. Click the **add +** icon.

Table 7-26: CAC Profiles



3. Define an intuitive, unique 'Name' for the CAC Profile (mandatory).
4. Define one of the following:
   - **Global Session Limit** – the limit on the total count of outgoing and incoming sessions

     -or-
   - **Session Limit by Direction** – limit by either or by both:
     - Incoming – Limit by the incoming sessions
     - Outgoing – Limit by the outgoing sessions

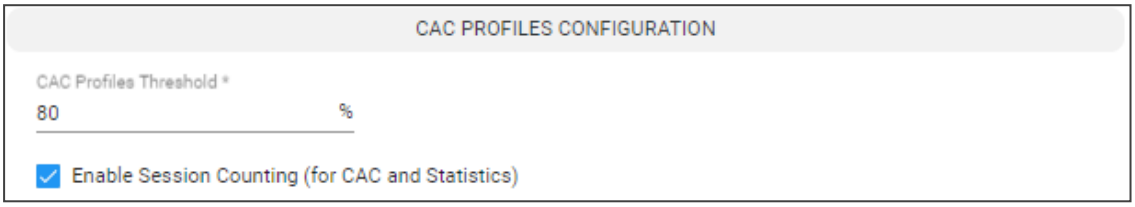
- Operators can reuse the same CAC Profile for multiple 'customer' entities.
- In the CAC Profiles page, the selected row (CAC Profile) can be edited using the **Edit** button; all settings can be edited and reapplied.
- If a CAC profile is edited (changed), the status of the network elements to which it is attached will be recalculated and appropriate alarms will be raised or cleared.

Defining a CAC Profile Threshold

The ARM lets network operators adjust the threshold for generating a warning alarm.

➢ To adjust the threshold for generating a warning alarm:

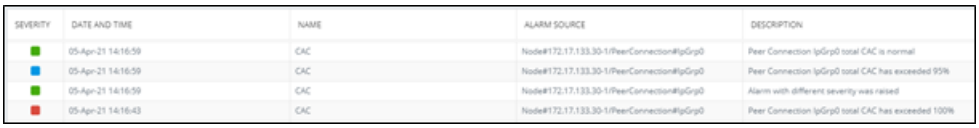
- Open the CAC Profiles page (**Settings** > **Routing** > **CAC Profiles**) and locate the screen section 'CAC Profiles Configuration' (the lowermost section of the screen).



The same CAC Profiles Threshold (percentage) value is applicable for all CAC Profiles defined in the ARM. To change the CAC profile, click **Submit**.

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

- **Warning** – generated for a Peer Connection when the number of sessions reaches the threshold limit (as a percentage) defined under **Settings** > **Routing** > **CAC Profiles**.
- **Critical** – generated when the number of sessions reaches the defined session limit.
- **Clear** – Generated to clear 'set' alarms when the number of sessions drops under the defined limit or when the CAC Profile is detached.

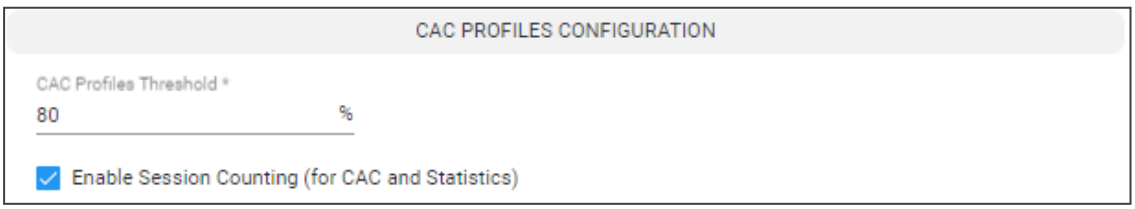


Disabling CAC and Session Counting

The ARM GUI lets operators disable CAC and Session Counting.

➢ To disable CAC and Session Counting:

1. Open the CAC Profiles page (**Settings** > **Routing** > **CAC Profiles**) and locate the screen section 'CAC Profiles Configuration' (the lowermost section of the screen) as shown previously.



2. Clear the option **Enable Session Counting (for CAC and Statistics)** and click **Submit**.

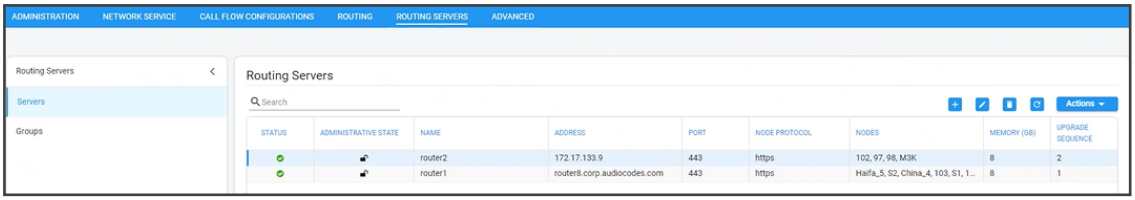
Adding a Routing Server

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

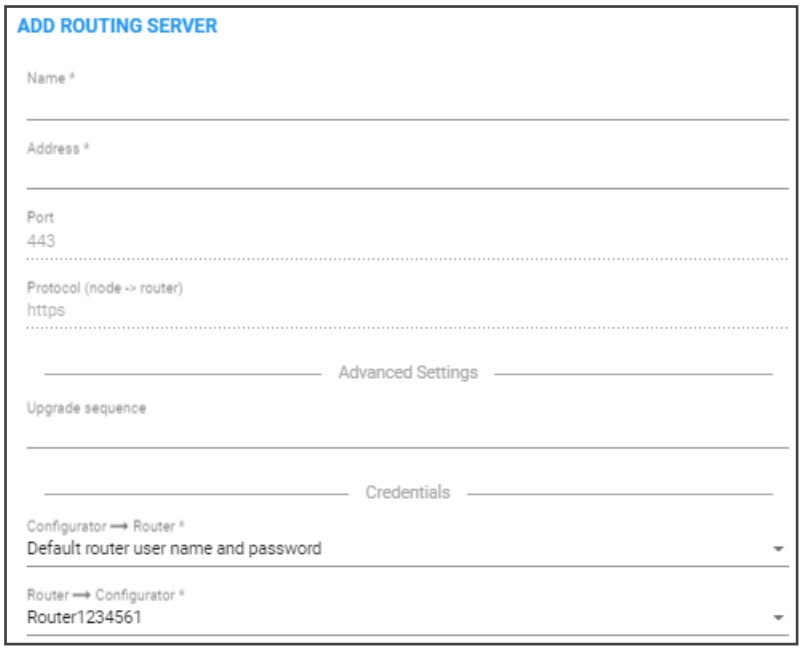
- ARM Version 8.4 supports up to 40 Routing Servers - a necessary feature in *very large* ARM deployments of almost unlimited scale.
- ARM Version 8.2 and earlier supported up to 10 Routing Servers.
- ARM Version 10.0 supports up to 150 Routing Servers for globally distributed IP telephony deployments with multiple branches. Moreover, some deployments need at least two ARM Routers per site to provide ARM Routers redundancy. These deployments required a high number of ARM Routers. The ARM still supports synchronization and smooth operation with these high numbers.
- 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 37 for more information) and to provide the adjacent Routing Server as the priority for handling the Node's routing requests.
- ARM Router 'survivability' is supported. When the ARM Configurator is reconnected to ARM Routers after the ARM Routers have been in 'survivability' mode, *full configuration synchronization is performed*; the ARM Routers get a new snapshot of all data from the ARM Configurator.
  - ✓ ARM Routers don't have a database; all data is stored in cache memory optimized to provide fast replies to SBCs routing requests. ARM Routers don't restart; they get the data from the ARM Configurator and build a new data cache ('map' and 'locator'). During the rebuild, the ARM Routers still use the old cache. Only after the new 'map' and 'locator' is built, the ARM Router switches to use it. *There is no service interruption at any point in this process*.
  - ✓ When an ARM Router is in 'survivability' mode (disconnected from ARM Configurator), it stores the 'cache snapshot' in the local disc so if the ARM Router restarts and needs to continue operating while the ARM Configurator is still unavailable, it will come with locally-stored data and continue to route calls (i.e., continue to operate in 'survivability' mode). ARM Routers can operate in this mode for months without any interruption to service.
  - ✓ If a Node (SBC or Gateway) is unavailable or unroutable per the last configuration received from the ARM Configurator and it starts sending a Routing Request, the disconnected ARM Router will determine it to be 'available', update the local configuration and serve it.

➢ **To add a Routing Server to the ARM:**

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



2. Click the add icon **+**.



Adding a Routing Server without adding it to a Routing Server Group will have no effect as Routing Servers are as of ARM Version 8.6 not attached directly to nodes (see under Adding a Routing Servers Group with Internal and External Priorities).

3. Configure the routing server using the following table as reference.

Table 7-27: Routing Server Details

Setting	Description
Name	Enter a name for the ARM Router (routing server).
Address	Enter the IP address or host name for the ARM Router (routing server).
Port	[Read only] ARM Router (routing server) port number. Default: 443
Protocol	[Read only] HTTPS
Upgrade Sequence	Network operators can group ARM Routers so that *multiple ARM Routers* can be upgraded simultaneously, reducing the time required for ARM software upgrade. **It is the network operator's responsibility to group ARM Routers in a way that no service outage will occur.**

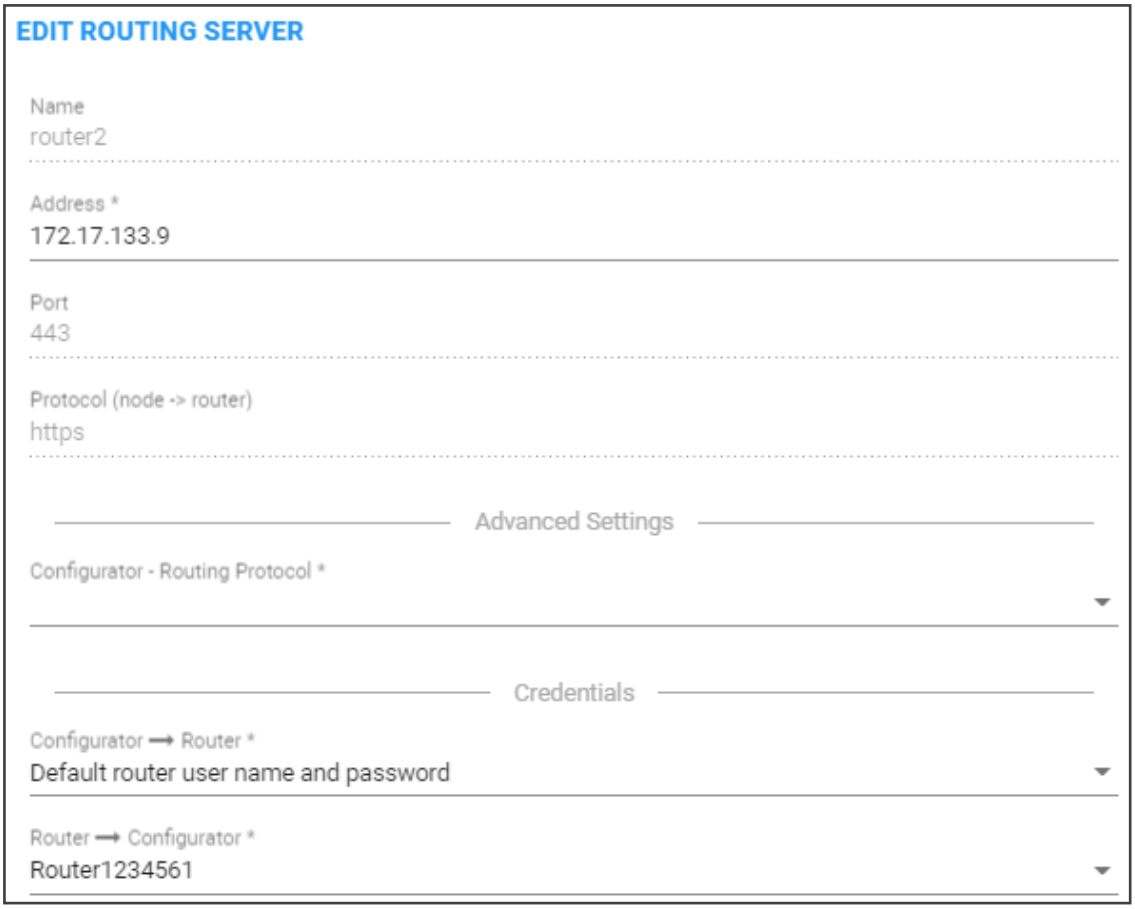
Setting	Description
	By default, the ARM Routers undergo upgrade one by one. This is the preferred way for customers with 2-6 ARM Routers to upgrade. ➢ **To apply the 'Upgrade Sequence' feature:** ■ In the Routing Servers page (**Settings** > **Routing Servers** > **Servers**), add Routing Servers to the ARM as shown before and then in the 'Upgrade Sequence' field of each, enter a value. ✓ The Routing Server with the *lowest* 'Upgrade Sequence' value is upgraded *first*. ✓ Routing Servers defined with the *same* 'Upgrade Sequence' value are upgraded *at the same time*. ✓ Include in each 'group' i.e., Routing Servers defined with the same 'Upgrade Sequence' value, Routing Servers whose simultaneous upgrade *won't impact calls routing*. ⚠ The feature is recommended *only if you have a high number of Routing Servers* in your deployment.
Credentials	Allows you to specify the credentials which the Configurator will use to communicate with the router and vice versa.

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** > **Servers**) as shown previously.
2. Select the row of the routing server to edit, and then click the edit icon .



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

Table 7-28: Edit Routing 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 Settings	
Configurator – Routing Protocol	To display this parameter, click the drop-down arrow adjacent to Advanced Settings 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.

Setting	Description
Credentials	
Configurator > Router	To display this parameter, click the drop-down arrow 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 the drop-down arrow 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 network operators 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 (SBCs / Media Gateways) 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**) as shown previously.
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

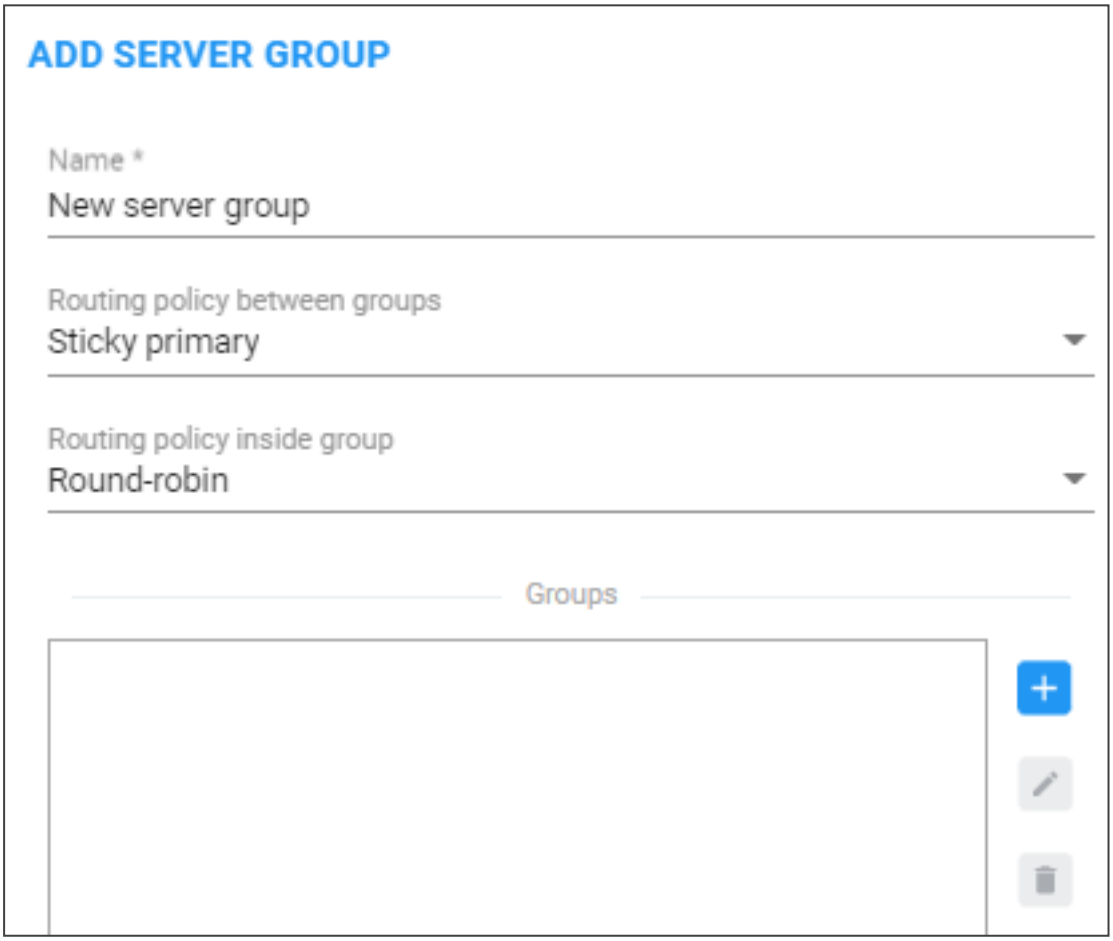
The ARM allows adding a single group of Routing Servers. The ARM also allows you to add multiple groups of ARM Routers with a policy between them. This may be necessary when an ARM deployment is geographically distributed. ARM customers in circumstances like this prefer

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**).

2. Click the add icon **+**.

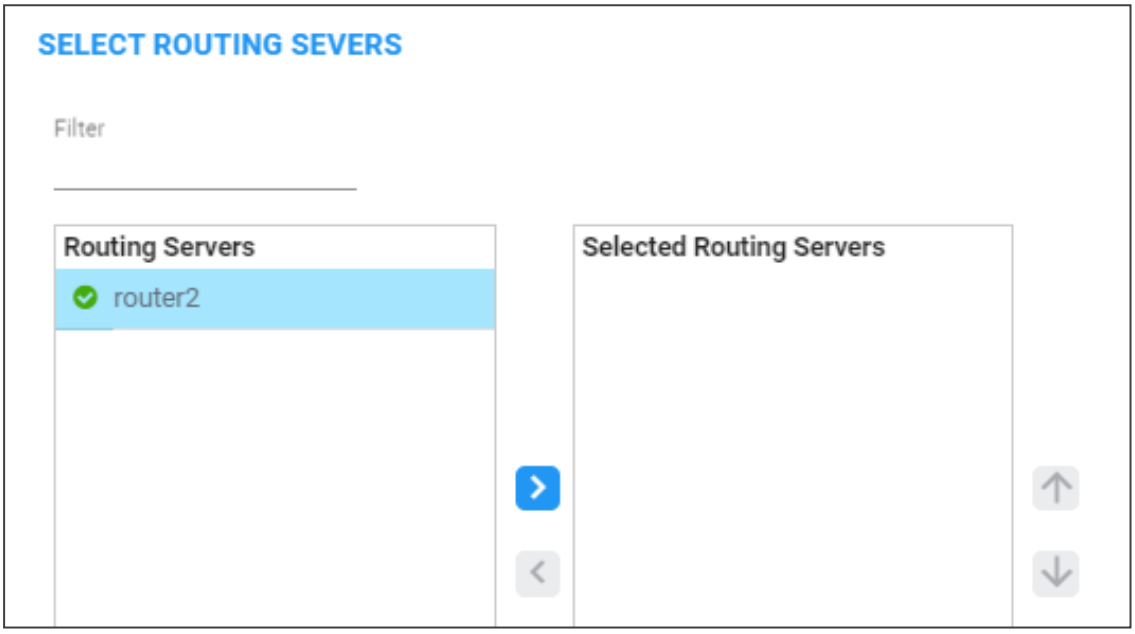


- Configure the 'Name' of the new server group to be attached to a node or to multiple nodes.
- Configure the 'Routing policy between groups'; 'Sticky primary' is the default. Two routing policies between Routing Groups are available:

- ‘Sticky primary’ [the node reverts to the primary group when at least one ARM Router is available]
- ‘Sticky last available’ [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 Available.
4. In the 'Groups' pane, click **+** to attach one or more ARM Routing Servers to the Routing Group.

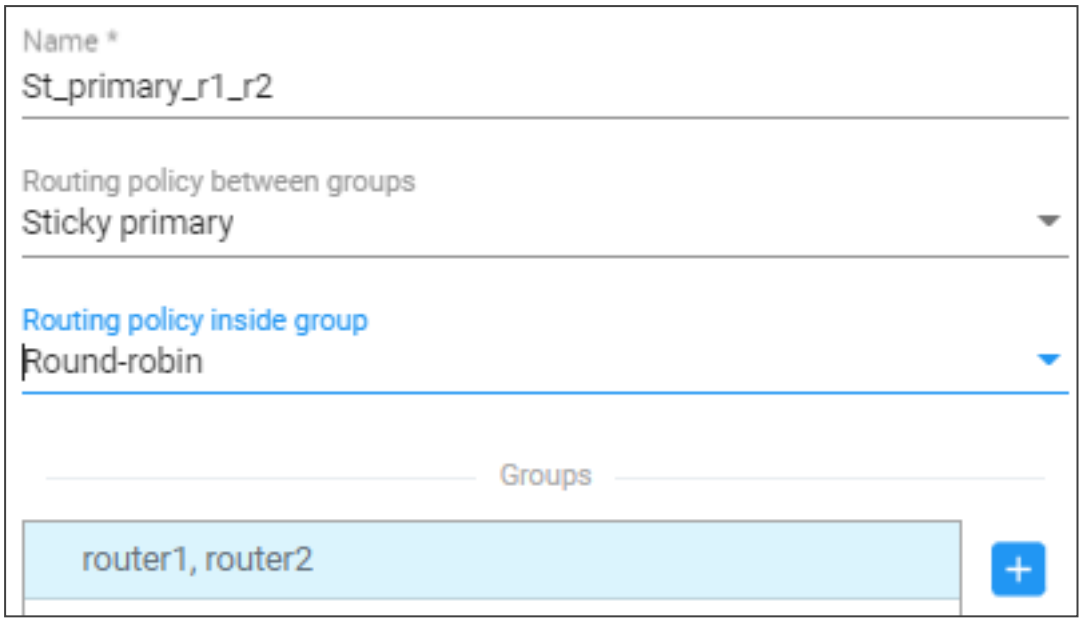
Figure 7-72: Attaching Routing Server to a Routing Group



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 **+** again.

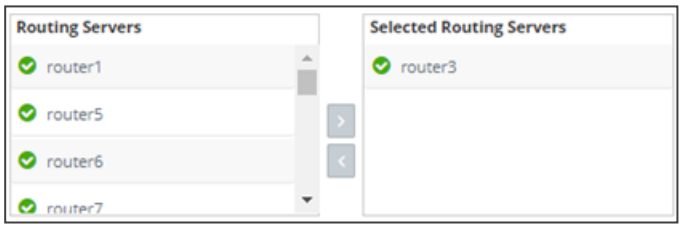
The maximum number of routing servers allowed for the entire server group is 10, so if you have five sub-groups, each can have up to two routing servers inside).

Figure 7-73: Multiple Sub-Groups of Routing Servers



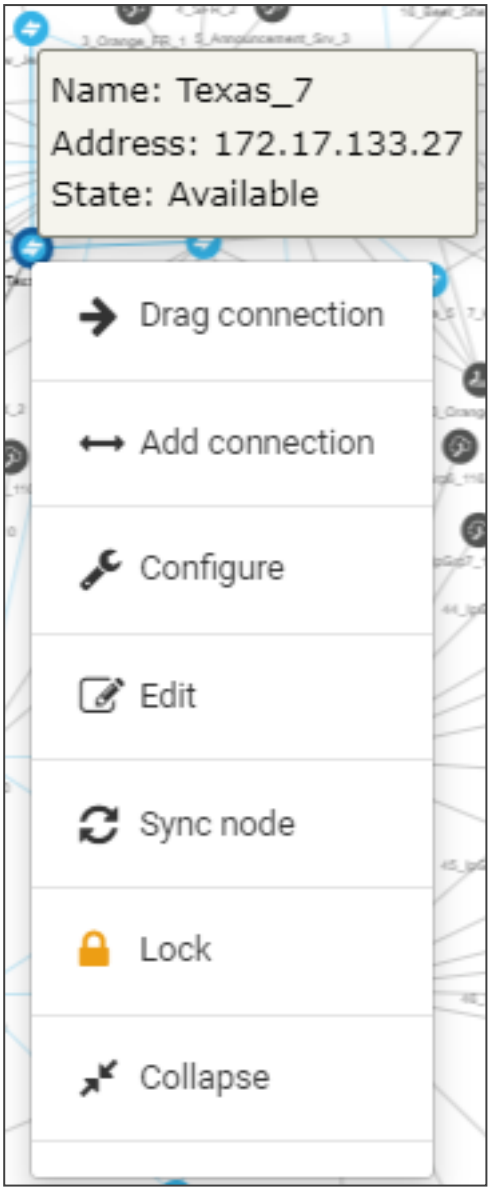
6. Configure a new sub-group of routers with the same Routing Policy inside the group.

Figure 7-74: 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, right-click the node in the Network Map page and select **Edit**.



8. In the Edit Node screen that opens (shown in the next figure), select one of the previously configured groups from the 'Routing server group' drop-down.

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.

9. Under the 'Advanced' section of the Add Server Group screen, optionally select **Enable parallel connections (multiple sockets)**.

SBC version 3.4.300 and later supports this feature.

Before ARM 9.8, a node always opened one socket towards each provisioned ARM Router for Node ↔ ARM Router communication. In some cases, this led to problems of blocking if heavy traffic or a delay in ARM → SBC responses to routing requests (usually due to external web services) occurred.

ARM 9.8 and later, combined with SBC 7.4.300, enables opening a number of connections in the direction of the ARM Router. When the connections are open, any delay resulting from handling are minimal because connections opened in parallel allow much quicker handling than connections opened consecutively.

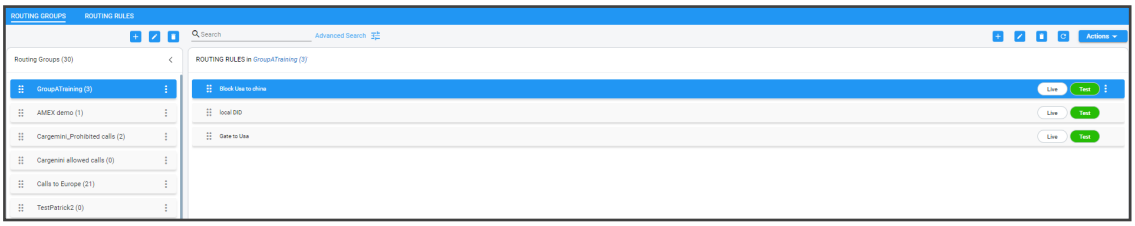
Supporting multiple sockets for the Routing Server solves the problem of head-of-line blocking; the first sent message would previously take time to answer and would block all the others.

8 Defining Calls Routing

The ARM lets network administrators responsible for enterprise VoIP define call routing. ARM routing provides a comprehensive call routing solution for an IP telephony network.

➢ **To define calls routing:**

- Open the Routing Groups page (**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 328)
3. Test the route (see Testing a Route on page 96)

Adding a Routing Group

Before adding a rule, you must add a Routing Group. Routing Groups help present rules in the GUI in an organized fashion, enhancing user experience. Routing Groups also allow you to move a group of Routing Rules, collectively changing their routing priority.

➢ **To add a Routing Group:**

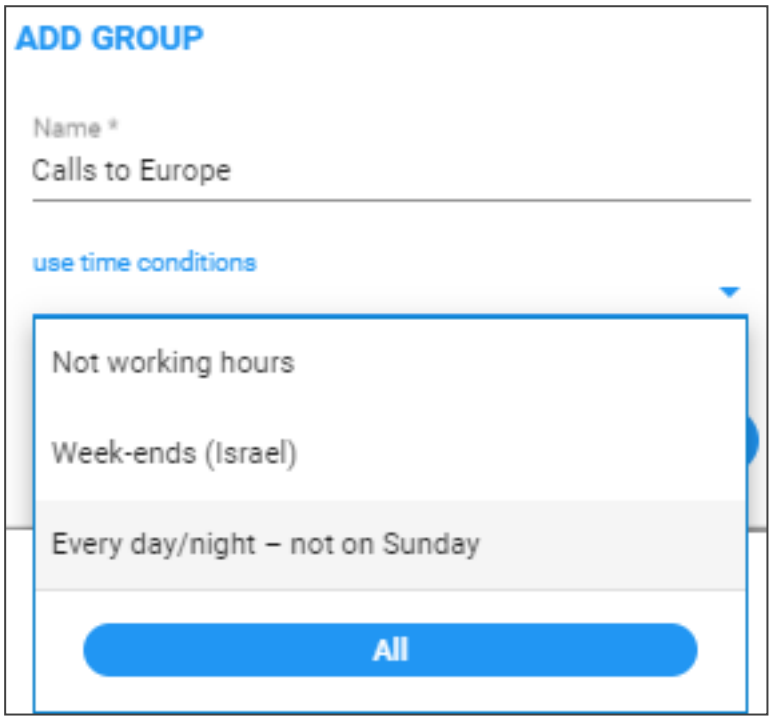
1. In the Routing Groups page (**Routing** > **Routing Groups**) shown previously, click the Add Group **+** icon above the *left* window in the page. (In the *right* window in the page you'll later add *Routing Rules*).

2. Define a name for the Routing Group to be added. Define a user-friendly name to facilitate intuitive management by administrators. Some example of groups you can add are 'Restricted Calls', 'Calls to Europe', 'Calls to Far East', 'Calls to ROW', etc.

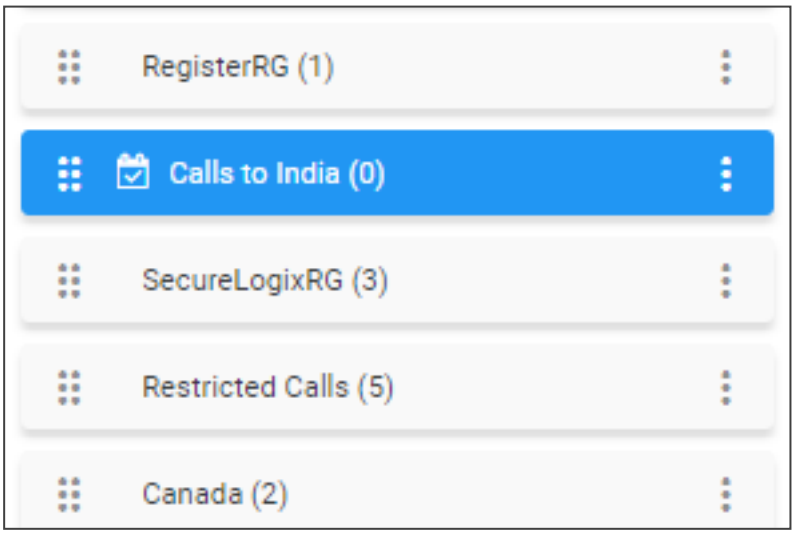
The routing group's name must be distinct from names of other routing group names, and must be between 1-255 characters.

3. From the drop-down, select the **use time conditions** option to attach a time condition to the Routing Group. See Configuring a Time-Based Routing Condition on page 291 for related information on how to attach a time condition to a Routing Rule. You can attach multiple time conditions. These conditions will apply to all rules in the group.

Figure 8-1: Add Group with Time Condition



4. Click **OK**; the new Routing Group is added to the list of groups in the Routing Groups page. If you attached a time condition to the group, it's visually indicated (see the calendar icon):



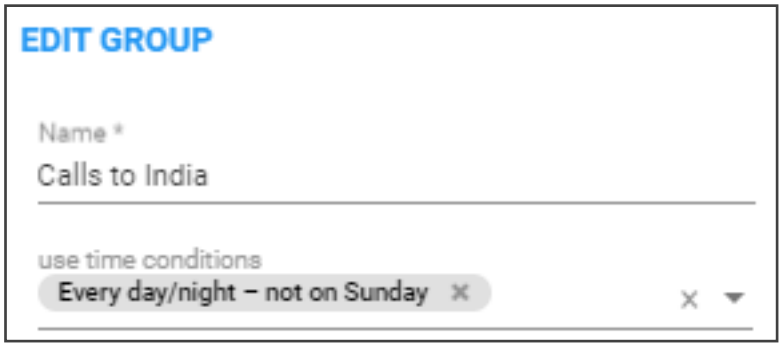
Routing Groups listed higher take precedence over those lower. Routing Groups in the list can be reordered (see Moving a Routing Group below). Priority is calculated internally, based on Previous and Next groups.

Editing a Routing Group

You can edit a Routing Group if necessary.

➢ **To edit a Routing Group:**

1. In the Routing Groups page (**Routing** > **Routing Groups**), select the Routing Group to edit, and then click the Edit Group icon (or click the adjacent vertical ellipsis and from the popup, select **Edit**).



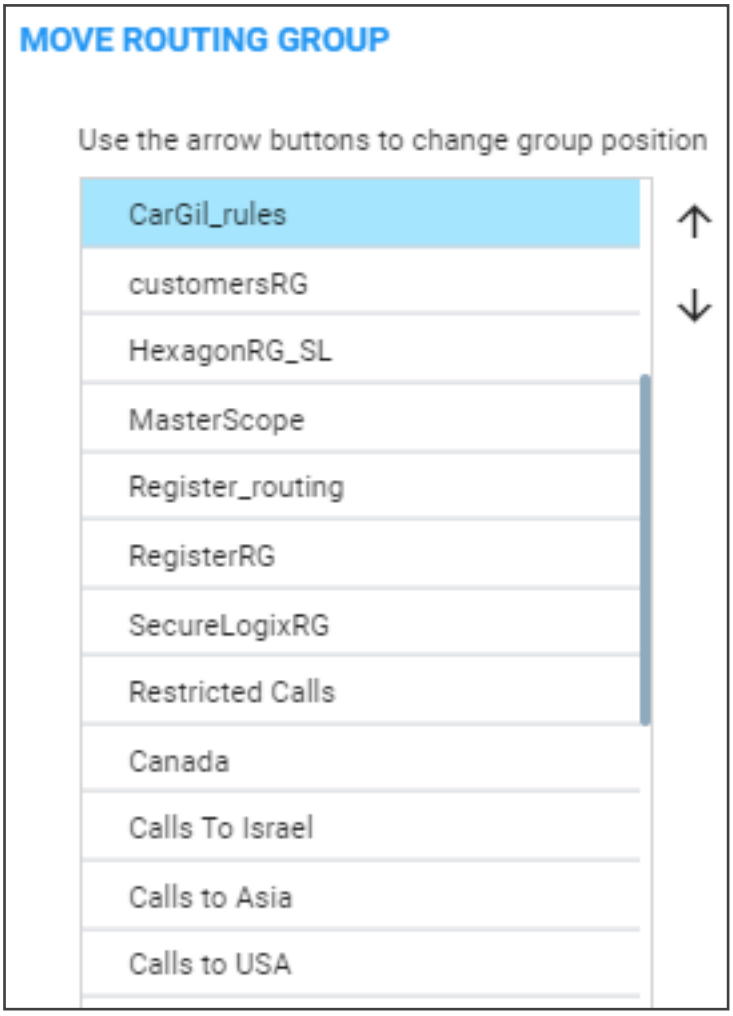
2. Edit the 'Name' field. Enter a user-friendly name to facilitate intuitive management by network administrators.
3. Edit the time condition. From the **use time conditions** drop-down, you can clear time conditions if defined. See Configuring a Time-Based Routing Condition on page 291 for related information. 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 click the adjacent vertical ellipsis and from the popup, select **Move**.



2. Select the Routing Group to promote / demote, and then click ↓ or ↑.

Deleting a Routing Group

Routing Groups can be deleted, if necessary, including the rules associated with the group if there are any.

➢ **To delete a Routing Group:**

1. In the Routing Groups page, select in the *left* window in the page the Routing Group to delete and then click the delete icon -OR- click the adjacent vertical ellipsis and from the popup, select **Delete**.
2. Confirm the action in the confirmation prompt that is then displayed.

Adding a New Routing Rule

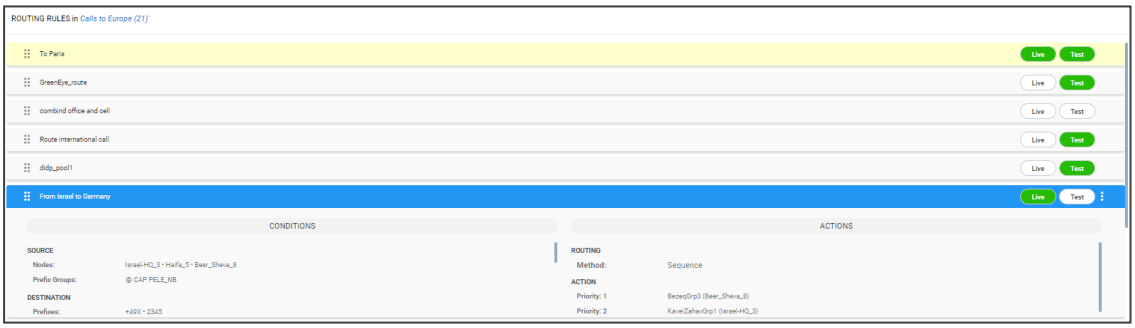
After adding a Routing Group, add a new Routing Rule to associate with the Group. Each Routing Rule is given a unique priority within the Routing Group. A rule listed higher than another, even if in the same Routing Group, takes precedence.

- 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 8-2: 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 Nodes, Connections, Peer Connections and Resource Groups are available, it sends the call to the destination configured for that rule. If it doesn't find a matching rule, it indicates that a route for the call has not been found.

Alternative Routing

The ARM performs alternative routing as follows:

- The ARM attempts to build an alternative path for the same Routing Rule action (Nodes, Peer Connections, VoIP Peers and Resource groups), if available. For more information on Resource Groups, see Resource Groups Page Actions on page 59.
- ARM attempts to build an alternative action (Nodes, Peer Connections, VoIP Peers and Resource groups), if available, for this call, in the order that actions are listed in the Routing

Rule. For more information on Resource Groups, see Resource Groups Page Actions on page 59.

- All routing alternatives are sorted by weighted path, cost and then by number of hops.

Load Balancing

The ARM can balance call traffic between multiple destinations of the same Action. Call traffic can be distributed equally between destinations, or the distribution can be defined by the operator. Multiple routing attempts can be configured. Default: 1. Max: 3. The max can't exceed the number of destinations in the load balancing action. If a call to a destination configured in a load balancing action fails, the ARM will try to route it to one of the destinations configured in load balancing before searching for a new rule or action for it.

Registered users

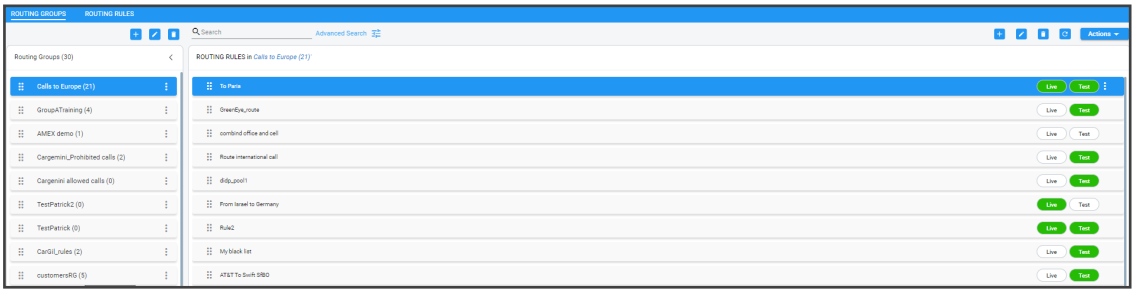
The ARM can route a call only if *the destination number is the number of a registered user in ARM* (listed in the Registered Users table) and the Routing Rule is then matched.

Discard Call

The ARM can be configured to discard calls matching specific conditions as a single action, or as the last action of a rule if previous destinations were unavailable.

➢ To add a new Routing Rule to a Routing Group:

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



This screen opens:

2. Enter a name for the routing rule that is distinct from the names of the other routing rules in the same group. Define a user-friendly name to facilitate intuitive management by network administrators. The name can be between 1-255 characters.

3. Enable **Live** and/or **Test** mode. See Testing a Route on page 96.

   - **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:

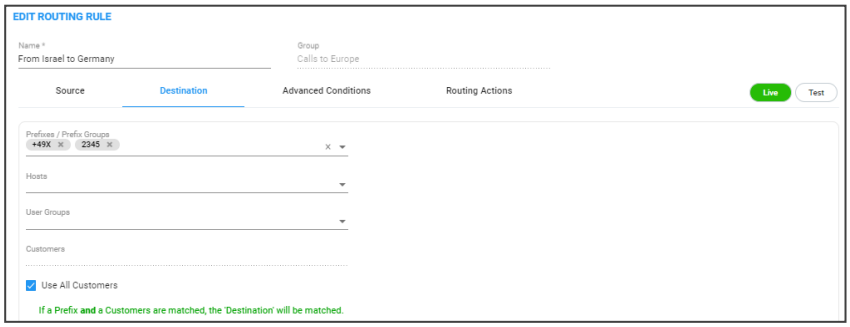
Table 8-1: Live | Test Mode Combinations

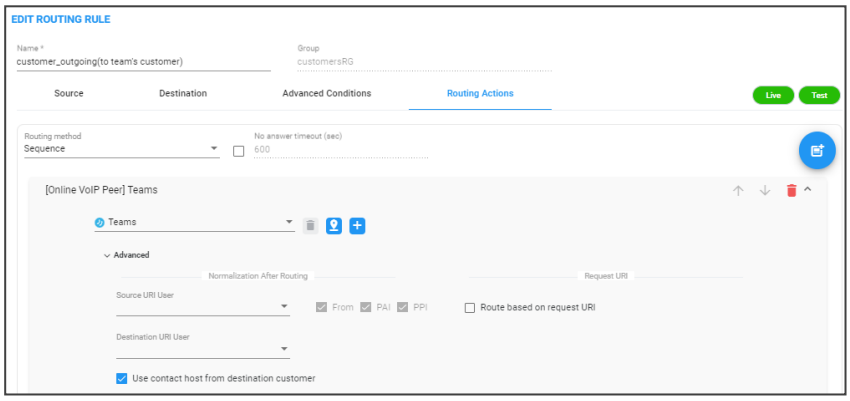
Live | Test Combination	Explanation
Live is enabled | Test is enabled	The rule will be considered for *both test and live traffic*.
Live is enabled | Test is disabled	The rule will be considered only for *live traffic*. Test mode won't be impacted. Select this option to simulate rule removal.
Live is 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 | Test Combination	Explanation
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.

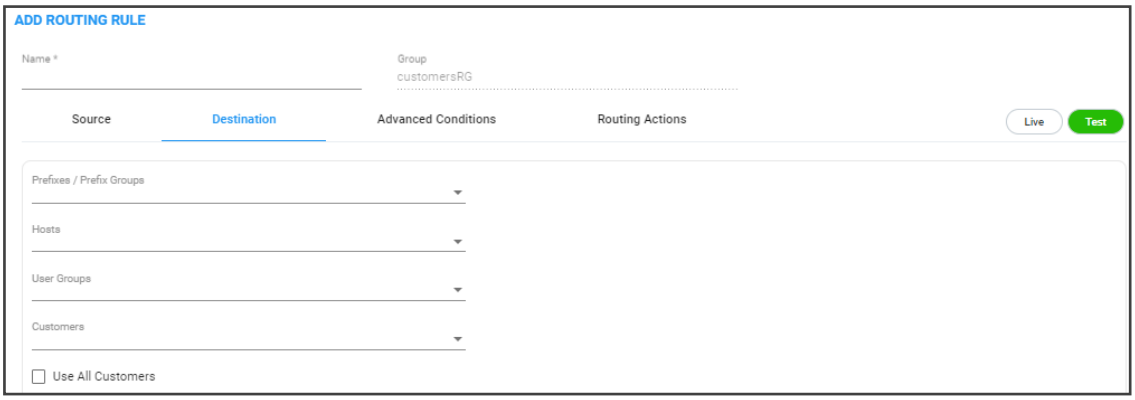
Table 8-2: Source Settings

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 153.
Customers	Allows you to select a 'customer' entity / set of 'customer' entities. From the drop-down, select a specific 'customer' entity or a set of 'customer' entities to be used to match the SOURCE field under the **Advanced Conditions** tab. Select the **Use All Customers** option for the rule to be applied to all 'customer' entitles (without selecting a specific 'customer' entity or a set of 'customer' entities). This is a very powerful functionality especially in the case of a very high number of 'customer' entities. In this way, with a single rule, you can define Calls Routing towards all the 'customer' entities with a Teams Peer VoIP Peer destination (action). This single rule will cover calls toward Teams for all 'customer' entities coming from several SBCs. Following is an example of a rule using **Use All Customers** in the Destination condition of a rule leading toward Teams.  Each 'customer' entity is identified / indicated by Teams with the

Setting	Description
	FQDN in the 'Contact' or 'From' header. The call in the direction 'to Teams' should have this 'Contact' header identification as well. The ARM provides an easy way to put the predefined string (the one used by Teams to identify the tenant) in the Contact header for calls towards Teams. In a Routing Rule's 'Routing Action', check the **Use Contact host from destination customer** option under the 'Advanced' section of a specific action; in this case, the ARM automatically installs the value (string) provisioned in the **SIP header** field of the defined 'customer' entity into **SIP Contact header** of the invite designated to reach Teams. 
Resource Groups	From the drop-down, select a Resource Group. This setting is mandatory to define a routing rule applicable to *specific call sources* rather than (globally) to the entire network. Resource Groups comprise Nodes, Peer Connections and VoIP Peers.
Nodes	From the drop-down, select a source Node or Nodes, or select the element from the topology screen . This setting is mandatory to define a routing rule applicable to *specific call sources* rather than (globally) to the entire network. **Note 1**: To select multiple elements in the topology screen, press **Ctrl** and click the elements to select. **Note 2**: If the selected 'Nodes' or 'Peer Connections' or 'Reroute Peer Connections' or Topology group matches one of the conditions specified under the **Advanced Conditions** tab, the ARM will use this rule.
Peer Connections	From the drop-down, select a source Peer Connection or Peer Connections, or select the element from the topology screen shown in the figure following this table. This setting is mandatory to define a routing rule applicable to *specific call sources* rather than (globally) to the entire network.

Setting	Description
	Note 1: To select multiple elements in the Choose Topology Item screen, press **Ctrl** and click the elements to select. **Note 2**: If the selected 'Nodes' or 'Peer Connections' or or 'Reroute Peer Connections' or Topology group matches one of the conditions specified under the **Advanced Conditions** tab, the ARM will use this rule.

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

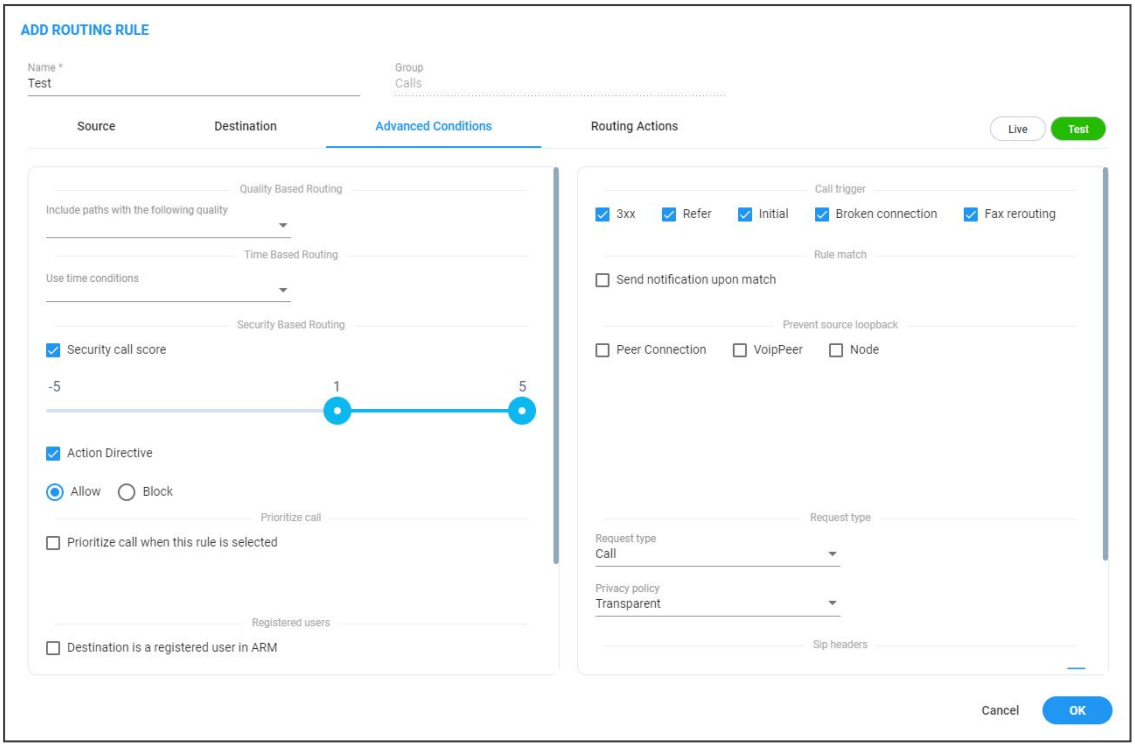


6. Configure the 'Destination' settings using the following table as reference.

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.
Customers	See Customers on page 332.

7. In the Add Routing Rule screen, click **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 289. Criteria for bad, fair and good quality, based on the calculation of MOS and ASR, can be defined. This screen lets you associate the criteria you defined with the Routing Rule.

9. Under 'Time based routing', select from the drop-down menu the time on which routing will be based, configured under **Settings** > **Routing** > **Time Based Routing** (see Routing Settings on page 289 for information about configuring a time range).

- More than one Time Condition can be associated with the same Routing Rule. Activation of the Routing Rule is then performed in ‘or’ between Time Conditions.
- A Time Condition can be attached to a Routing Rule which belongs to a Routing Group with an already-associated period; the ARM's calculation of this Routing Rule's activation will then be ‘and’; the rule will be activated during the period assigned to the Routing Group and the period assigned to the Routing Rule.

10. Under Security Based Routing, select the **Security call score** and/or **Action Directive** options only if SecureLogix's Orchestra One™ CAS (Call Authentication Service) is used. The ARM supports security-based routing through integration with SecureLogix’s Orchestra One™ CAS.

Using security-based routing requires purchasing SecureLogix’s license in addition to the ARM license and must be coordinated with AudioCodes.

Once **Security call score** is enabled, the Routing Rule will use the score returned from SecureLogix as part of the match. The slider is used to control the score threshold. If no

score is returned from SecureLogix or the score doesn't match the threshold, the rule will not be matched. Based on the score the ARM gets for a specific call, a routing decision is applied. Example:

- For low-scoring calls (bad calls), the routing action may be 'Drop call'.
- For average-scoring calls (suspicious calls), the network administrator can apply number manipulation and display the number with a '?' or with the word 'Suspicious'.

The ARM features two strategy modes:

- **Standard mode**. Calls are verified with the Orchestra One server with a low price. It checks for basic secure. Strategy is set to 0 and as read-only.
- **Advanced**. Calls are verified with the Orchestra One server with a higher price. For example:
  - For Strategy value 1, Orchestra One will 'Authenticate using the Verizon Call Verification Service (VCVS) when applicable'.
  - Strategy is set to 1 and as user will be able to set it to 1 or higher. For Advanced mode, it's typically necessary to enable the Sending SIP headers option.

A call's Security Score can be used as basis for a routing decision. Security-based routing can be applied to calls that receive a score from SecureLogix's Orchestra One as part of the pre-routing process. The Routing Rule is applied to a specific range or to a certain value of the call security score received from the ARM ↔ Orchestra One consultation. The range is from -5 to 5.

ARM administrators may use the call's security score as part of the routing decision. For example, calls to a specific (security-sensitive) destination with a score of less than 4 can be dropped, while calls to other destinations with a score of 4 can still be routed normally.

Operators can moreover apply number manipulation to the source call number and turn a source DID with a 'suspicious' security score into a question mark - which will draw the attention of the recipient of the call. The score description shown below is excerpted from the documentation of SecureLogix's Orchestra One:

Orchestra One Scoring Matrix		
5	Verified by the Carrier API's or TRUSTID	
4	Reserved for use by future tools and/or analysis	
3	Verified by SIP header analysis	
2	Reserved for use by future tools and/or analysis	
1	Source analyzed. No anomalies detected; no positive information found	
0	*Toll Free source (Changing from existing score of -5 based on customer feedback)	
-1	International Source (a significant amount of fraud comes from international numbers)	
	*No or blocked CallerID (Changing from existing score of -5 based on customer feedback)	
-2	Source < 10 digits	
-3	Reserved for use by future tools and/or analysis	
-4	*Un-verified by Carrier API's or TRUSTID. (Changing from existing score of -3 based on data analysis customer feedback)	
	Negative SIP header analysis	
-5	Invalid or unassigned phone number	
	Negative SIP header analysis &	Un-verified by the Carrier API's or TRUSTID.
Key	**Included in Standard Authentication**	**Included in Advanced Authentication**

* These scores are scheduled for update this calendar year based on customer feedback continued and data analysis.

See also:

- Web-based Services on page 269 for information on how to configure an external web-based service
- Policy Studio on page 246 for information on how to configure an external web-based service
- Activating Your License on page 179 for information related to standard vs. advanced security
- Viewing License Details on page 181 for information related to standard vs. advanced security

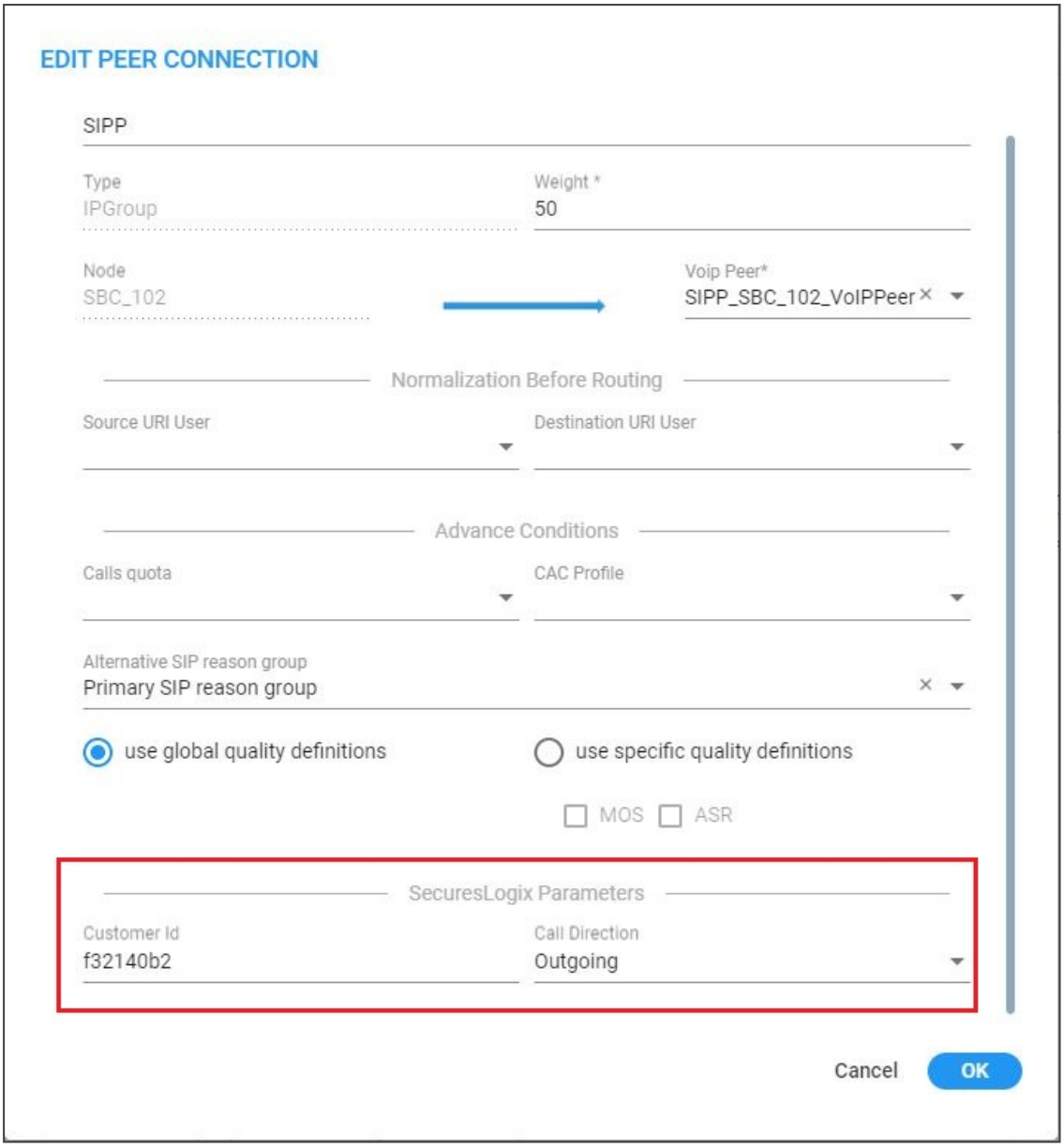
11. Under 'Action Directive', select **Allow** to enable the Routing Rule to use the ‘action directive’ value returned from SecureLogix as part of the match. If you select **Block**, define a Discard action to drop the call.

    - If no Action Directive is returned from SecureLogix or the Action Directive value doesn’t match the Action Directive selected, the rule will not be matched.
    - Alternatively, if the Action Directive value matches the Action Directive selected, the Routing Rule action will be performed.

    The SecureLogix Call Authentication Service response depends on the ARM query. For using Action Directive, ARM needs two additional attributes to be included in its query to SecureLogix’s Orchestra One:

    - Customer ID
    - Call Direction

    Configure these in the Edit Peer Connection screen. Use the figure below as reference.



Use the table below as reference.

Setting	Description
Customer ID	Customer identification string
Call Direction	Inbound (in) or outbound (out)

12. Select **Prioritize call when this rule is selected** to prioritize emergency calls over regular calls. The ARM supports emergency call preemption for SBC and gateway calls. If one of the devices is unavailable to process an emergency call because of lack of resources, a regular call will be preempted to free up resources so that the emergency call will be established. The ARM may preempt more than one active call to provide sufficient resources for processing the emergency call. Emergency calls can be identified by the matching rules parameters in the Add Routing Rule screen.

13. Under Registered Users, select **Destination is a registered user in ARM**; the routing rule will then be matched only if the destination number is a registered user number (listed in the Registered Users table).

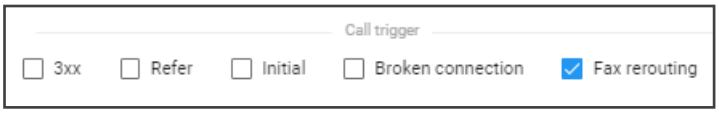
14. Under 'Advanced Conditions', select a **Call Trigger** to activate the rule for a specific Invite reason (i.e., alternative routing). By default, all 'Call Trigger' options are selected, so routing by default is based on all Call Triggers. At least one must be selected. The node applies to the ARM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

15. 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 8-3: 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).

16. Under 'Rule match' , select **Send notification upon match** to enable a notification on a call (for example, a 911 emergency call) if the call matches a specific rule.

When the ARM receives a call matching this rule condition, a notification (event) with related information is issued by the ARM Configurator. At the ARM level, the event can be sent to an SNMP target. With the ARM integrated into the OVOC, the call notification can trigger the issuance of an email by the OVOC, for example:

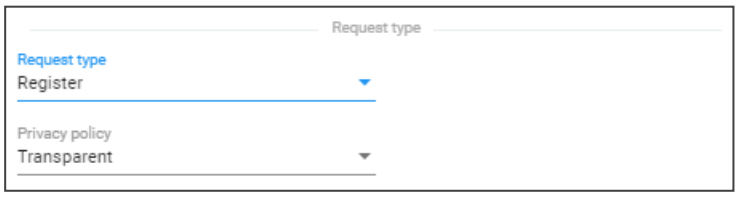
```
***** Event Info *****
Alarm Name: General Alarm
Date & Time: 09:24:16 AM September 6, 2018
Source: Router#172.17.113.23
Source Description:
Severity: info
Unique ID: 67
Alarm Type: other
Alarm Probable Cause: other
Description: Routing Rule 911 was matched
Additional Info 1:
Additional Info 2: Routing Rule "911" of Group "911" is
matched.
Call from Pcon "Pcon Pcon-1" , Node "Node 16161104" -
From number "+12345", To number "911".
Additional Info 3:
***** ARM Info *****
ARM IP Address 172.17.113.23
```

Notifications are typically required and used for 911 emergency calls, which should typically be reported via an email application or another notification application. The notification engine, however, can be used for any other matching rule.

17. Under the screen section 'Prevent source loopback', check the elements for which you want to prevent source loopback. For example, if you check the **Peer Connection** option, the call will not be routed back to the source Peer Connection.

In the case of a third-party node, the **Peer Connection** option is irrelevant.

18. Optionally use the Routing Rule for routing registration messages: Configure (switch) the 'Request type' condition from its default **Call** to **Register**.



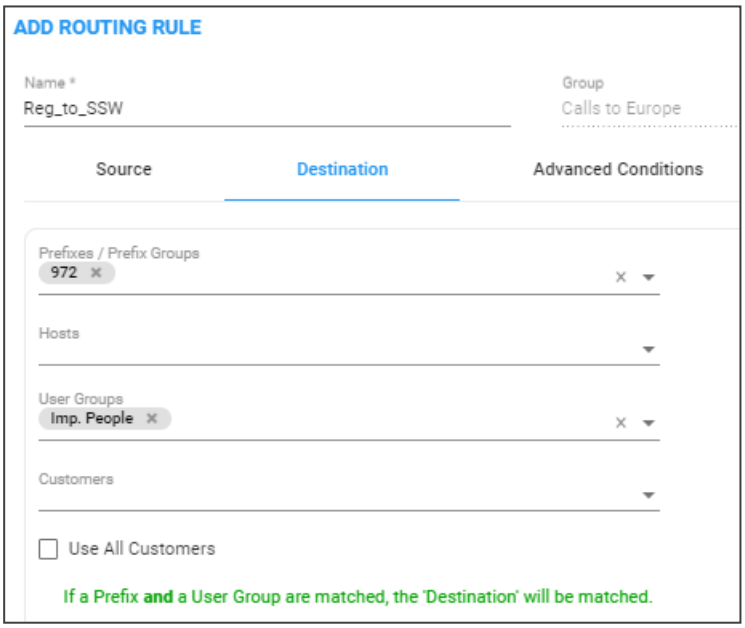
You can define a dedicated set of Routing Rules for routing registration messages. The registration messages routing rules can be grouped in a separate dedicated Routing Group (or Groups). The 'Request type' condition differentiates between a Routing Rule to be used for call setup routing and a Routing Rule to be used for registration routing.

If you don't specify any other condition in the Routing Rule but you switch 'Request type' to **Register**, this routing rule will be applied to all the users defined as **True** (enabled) in their registration property, i.e., for all users allowed to route their registration messages. The operator can define multiple Routing Rules for registration messages based on conditions such as:

- Source Node or Peer connection for registration messages coming from a specific topology element.
- Destination Prefix/Prefix group for a group of registration numbers.
- Destination User Groups for groups created with any sophisticated criteria with ARM users group facilities.
- Source URI taken from the SIP 'To' header.
- DEST URI taken from the SIP Request URI.
- Tag based. Very useful criterion. In the Policy Studio, you can assign a Tag to users based on a user's Dictionary Attribute and route registrations to different SoftSwitches based on the Tag's value.

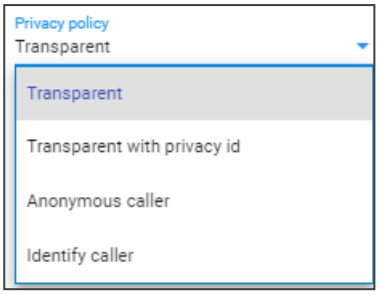
In the example below, the Routing Rule will be applied to users whose registration number starts with prefix 972 and who belong to the previously created Users Group 'Imp. People'.

Figure 8-4: Routing Rule Example



Note that not all conditions are relevant for routing of Registration messages. For example, conditions such as Source Prefix, Source Users Group or Call Trigger are not relevant.

19. 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.



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

20. [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.

21. 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.

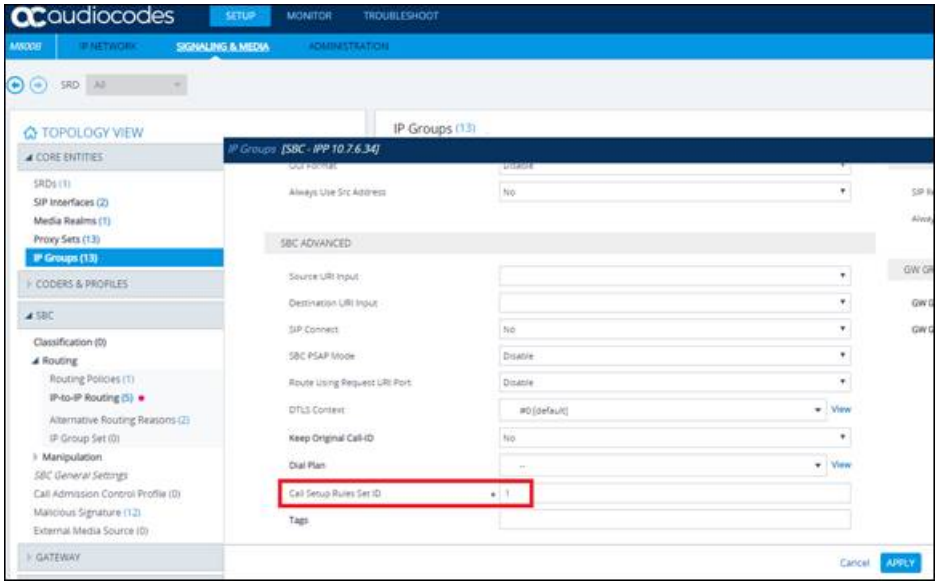
22. [SBC-Level Configuration] To send a parsed information request, add a new header with name "X-ARM-DETAIL-1", "X-ARM-DETAIL-2"… "X-ARM-DETAIL-N" and with information inside taken from the SDP or any other SIP header. X-ARM-DETAIL-X format is "X-ARM-DETAIL-1:<name=value>"

For example:

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

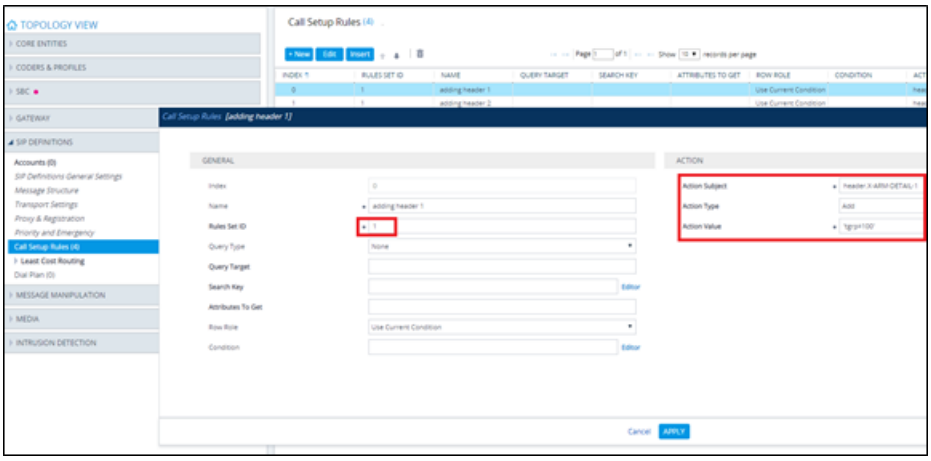
To create a new header in the SBC, add a new 'Call Setup Rules Set ID' in 'IPGroup' or in 'SIP Interface' in the device's Web interface. The figure below shows 'IPGroup'.

Figure 8-5: [Web Interface] Call Setup Rules Set ID



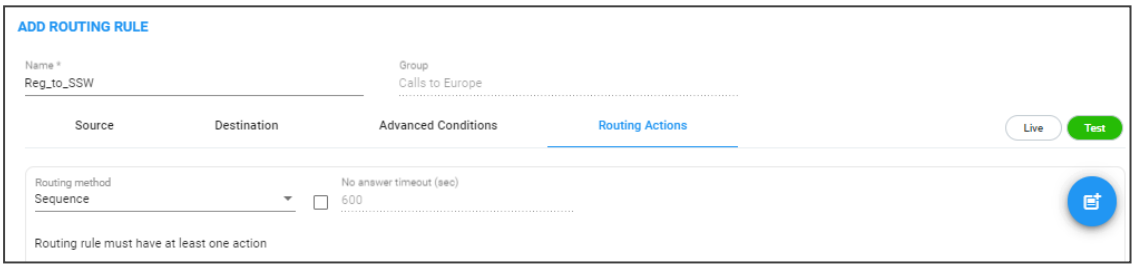
Setup rules can then be associated with the same Set ID. In the following figure, the manipulation added is 'tgrp=100'. In general, you can use a condition with RegEx and take the attributes into the Action Value.

Figure 8-6: [Web Interface] Viewing SBC Call Setup Rules Configuration



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

Figure 8-7: Routing Actions



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

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

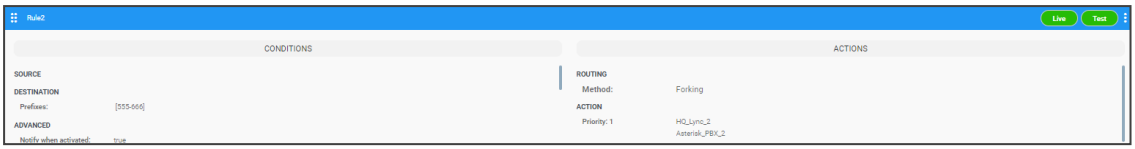
If you configure 'Routing method' to Forking, the actions are applied simultaneously and the call is split to all the destinations. The ARM supports calls forking at a network level. SIP forking refers to the process of 'forking' a single SIP call to multiple SIP endpoints. A single call can be split to many endpoints at the same time. The first extension (SIP end-point) to pick up the call receives the call; all other extensions then stop ringing.

Forking implementation in the ARM is designed to split specific calls (matching preconfigured condition) between several network-wide destinations (Peer Connections, VoIP Peers or nodes). Forking is integrated into ARM Routing Rules logic. Forking is applied if a call matches the Routing Rule condition.

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

The ARM supports up to three forking legs (different actions). If one or more of the actions with Forking Routing methods includes load balancing between multiple destinations, the load balancing (with configured percentages) will be applied to choose the correct destination of the forking leg.

Figure 8-8: Forking



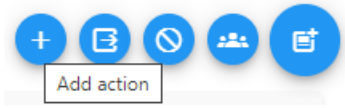
- When upgrading from an earlier ARM version than 8.6, all Routing Rules are translated with the Sequence routing method (the default).
- In the ARM, forking capabilities can only be applied to SBCs. Media Gateways aren't supported.
- Forking in the ARM is supported on SBC software 7.20.252 GA or later (release pending). For earlier SBC versions, Forking functions like 'Sequence'.

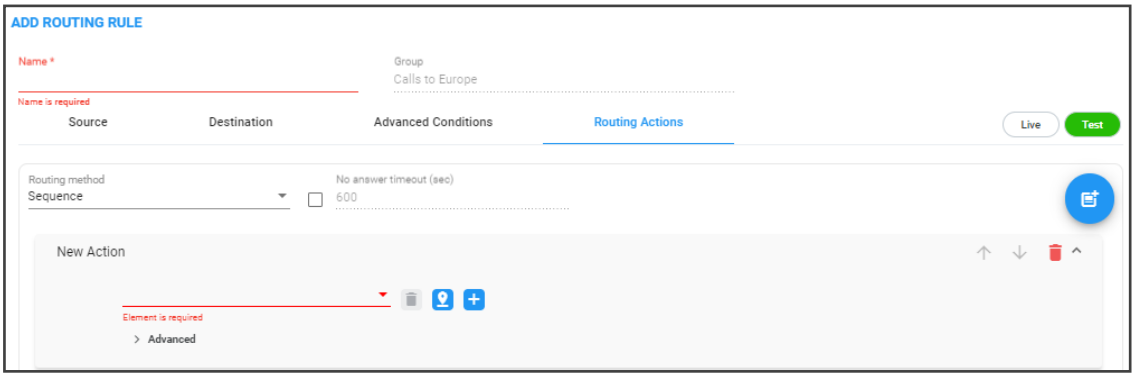
25. Select the **No answer timeout** option; if the called party does not answer a call within this given interval, the device will disconnect the session. Clear the option for the device to use the default value. The option allows management of the SBC/Gateway's timeout feature for no answer. The option controls the SBC/Gateway 'No answer timeout'.

The option is available only for the 'sequence' routing method.

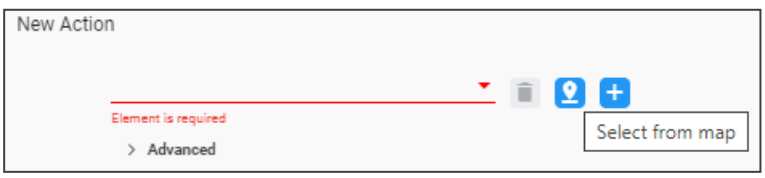
The feature gives the ARM the capability of managing delayed call forking. If the number is dialed and there is no call pickup after the configured timeout, the call is forked.

1. Under 'Routing Actions', navigate to and choose the 'Add action' **+** option.





a. Select from the drop-down menu the Peer Connection, VoIP Peer, node or Resource Group to which the call will be routed; the list is categorized; best practice is to scroll down the list to the category and then select the element.



Alternatively, click the 'Select from map' icon and in the topology screen that opens select the VoIP Peer, Peer Connection or Node. In large networks with high numbers of topology elements, this visual method of selecting the topology element may prevent human error from occurring and facilitate precise selection.

> If a Resource Group is selected for an action, a 'Resource Attempts' option is displayed.

b. Configure the number of 'Resource attempts', i.e., the number of elements the ARM will try before going to the next action. The maximum number of attempts that can be configured = the number of elements in the Resource Group.

c. Click **Advanced** to open post routing (after routing) normalization.

- From the 'Source URI User' drop-down, select the source element (see Adding a Normalization Group on page 238) 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.

  Source URI manipulation *for a specific field*, either the 'From' field, the 'PAI' field or the 'PPI' field, can be applied.

  By default, all three fields are checked when you apply a manipulation to Source URI users. Prior to ARM 9.2, this was the only available behavior. From ARM 9.2, you can check a specific field and clear the others. The functionality is valid for post-routing only. It's supported per Action.

  You can also *test a call* with a manipulation of a specific Source URI header, using the Test Route feature extension (support for a specific SIP header simulation). For more information, see Testing a Route on page 96.

- From the 'Destination URI User' drop-down, select the destination element (see Adding a Normalization Group on page 238) to manipulate the destination number in the outgoing call to the Peer Connection. The destination normalization group can only be connected to an IP Group or VoIP Peer. It cannot be connected to a Node.

2. Optionally select the **Route based on request URI** check box under the 'Request URI' section (under section 'Normalization After Routing') to enable *combined* ARM and SIP based routing decisions on a per-action basis, for when a customer (or a customer's network) provides routing instructions for a call as part of the SIP INVITE message (via REQUEST URI). The Peer Connection (the SBC's IP Group) must be specified in the action as well. SIP based routing takes place in the context of a specific SBC and IP Group. In this way,

the ARM will route a call until a specified SBC and request the SBC to use 'REQUEST URI' for further routing. The feature is available for SBCs only.

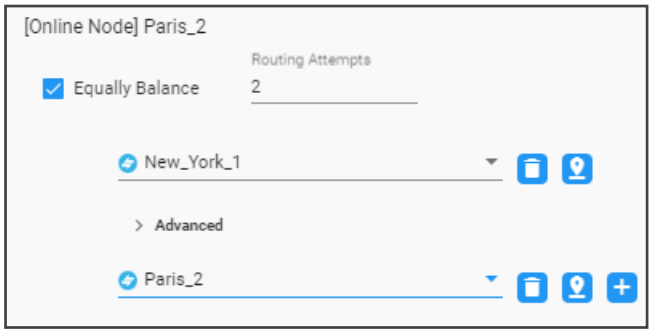
3. Click the 'Add load balancing' button; the screen adds the following items:
   - **Equally Balance** option (selected by default)
   - 'Routing Attempts' field
   - Drop-down field for selecting Peer Connection, VoIP Peer or Node with an 'Add load balancing' button located next to it

Figure 8-9: Load Balancing

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

4. (Optional) Clear the **Equally Balance** check box to define your own percentage. Any distribution can be chosen, i.e., any percentage of calls can be handled by a specific routing option. Several routing destinations (more than two) are supported by using the 'Add load balancing' button.
5. Enter the percentage of routes that will take this action when load balancing is configured and **Equally Balance** is cleared. Make sure you have 100% in the Action's calls destinations summary else you won't be allowed to enable the action.
6. Configure the parameter 'Routing Attempts' as shown in the following figure. The maximum attempts that can be configured is 3. Default: 1. The maximum number of 'Routing Attempts' can't exceed the number of destinations in the action; see for example the action [Online Node] PARIS_2 in the following figure.

Figure 8-10: Equally Balance: Routing Attempts = 2



The 'Routing Attempts' parameter determines the number of attempts that will be made within the load balancing action. If load balancing is configured within a Routing Rule's Action and a call to a destination configured in this Action fails for some reason, the ARM will try to route the call to one of the destinations configured in load balancing before searching for a new rule or action for the call.

7. Click **> Advanced** in order to apply number manipulation on the Source URI and / or the Destination URI.

- To remove a Peer Connection, Node, VoIP Peer or Resource Group, click the adjacent trash can.
- To remove an entire action, click the trash can on the right side of the screen.

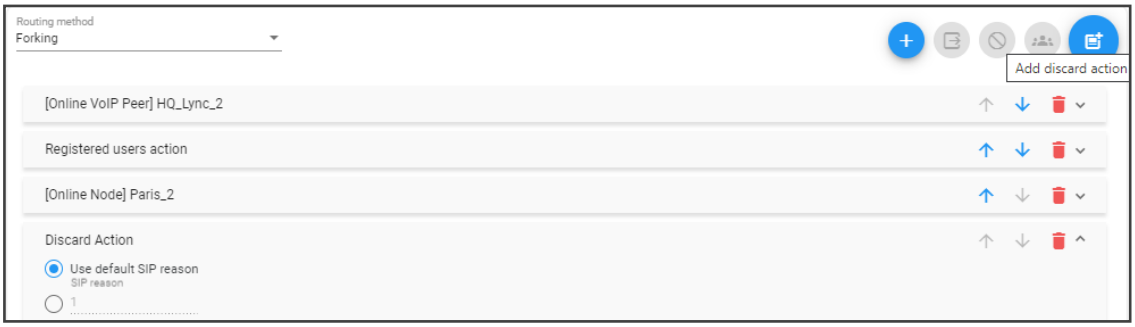
8. (Optional) Click the **Route to user location** button 

Figure 8-11: Route to user location

The ARM will now attempt to route the call to the location of the registered user (the destination number is used as the key to search for the location).

The ARM supports forking for registered users. If the Routing Rule's 'Routing Method' is set to 'Forking' and the action is set to 'Registered Users' ('Route to user location'), the ARM will attempt to apply forking if the same user is registered in multiple SBCs.

9. (Optional) Add a discard action by clicking the 'Add discard action' icon.



In a routing rule, you can apply a policy to attempt multiple routing options and to discard the call if none succeed. The action 'Discard Action' can be used - in addition to other routing actions of the same rule - as a last routing rule action or as a sole action.

10. Configure the discard action using the following as reference.

Table 8-5: Discard Action

Setting	Description
Use default SIP reason	Select the default SIP reason (the last SIP reason received from the SBC or the Gateway) or provide a specific SIP reason as shown in the next parameter description..
SIP Reason	Select this option for a specific SIP reason to be returned to the source peer connection when rejecting the call. Must be a valid SIP reason.

If any field is left empty (Prefix Group/Host/User Group/Node/Peer Connection), the rule will not check it.

11. Click the 'Add stop ARM routing action' (and continue with node's internal routing). This feature enables a combined routing decision taken by the ARM and a node (SBC only). The feature enables customers to specify that after a specific number of routing attempts configured in ARM routing, they'd like to continue with the local SBC routing table. The ARM supports the action in the Routing Rule: **Stop ARM routing**. A second action follows this: **Stop ARM routing and continue with node's internal routing table**. This action is always the last option in a Routing Rule. The feature is only available for SBC nodes.

Figure 8-12: Continue with Node's internal routing table

The feature additionally allows current AudioCodes SBC customers who want to use ARM Security-based Routing (integrated with SecureLogix) without immediately moving to the ARM. These customers can use ARM's SecureLogix integration feature but must indicate in their routing rule that the calls must be routed based on the SBC's existing routing table. ARM routing capabilities can be provisioned in future.

Fields such as 'Nodes', 'Peer Connections' and 'User Groups' in the Add Routing Rule screens and Edit Routing Rule screens feature filters in which network administrators can select multiple elements and then *invert the selection*. The feature improves usability and user experience especially in large networks with high numbers of elements. The feature allows network administrators to

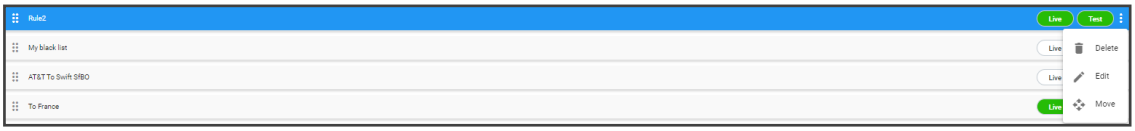
- Select a single element
- Delete a single element (x)
- Select All elements
- Clear all selected elements
- Select All and delete a few (x)
- Select All, delete a few (x) and then invert the selection; the elements deleted will be in the selection
- Select a few elements and then invert the selection;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

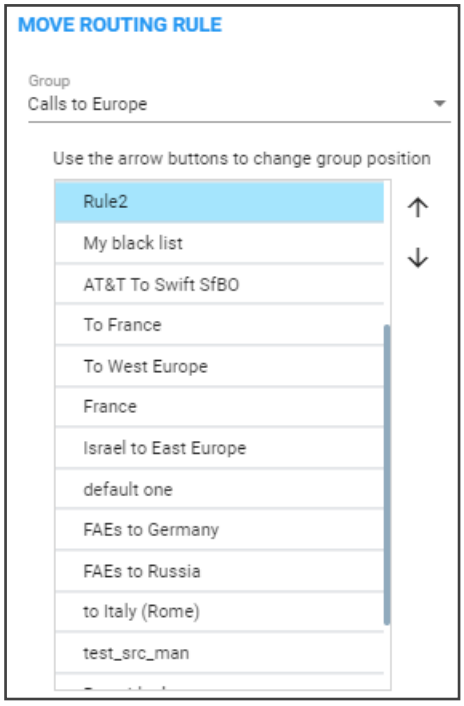
Moving a Routing Rule

You can move a rule within the group under which it is defined, or you can move it to another group, above or below a rule defined within that group.

➢ **To move a rule:**

1. Click the Routing Group under which the rule is defined and then
   - Drag and drop the rule to the Routing Group you want to move it to -OR-
   - Select the rule and then click the vertical ellipsis and select **Move**.





2. From the 'Group' drop-down menu, select the new group to which to move the rule to.
3. Click ↑ or ↓ to locate the rule within the new group's rules -OR- click a rule *above which* you want your rule to be moved.
4. Click **OK**; the rule is moved to the location you defined.

Deleting a Rule

Rules can be deleted if necessary in the *right* window of the Routing Groups page under *Routing Rules* -OR- in the Routing Rules page.

➢ **To delete a rule:**

1. In the Routing Groups page (**Routing** > **Routing Groups**) in the *right* window of the page, select the rule to delete and then click the delete rule icon -OR- click the adjacent vertical ellipsis and from the popup, select **Delete**.
2. In the Routing Rules page (**Routing** > **Routing Rules**), select the rule to delete and click the delete icon .
3. Confirm the action in the prompt.

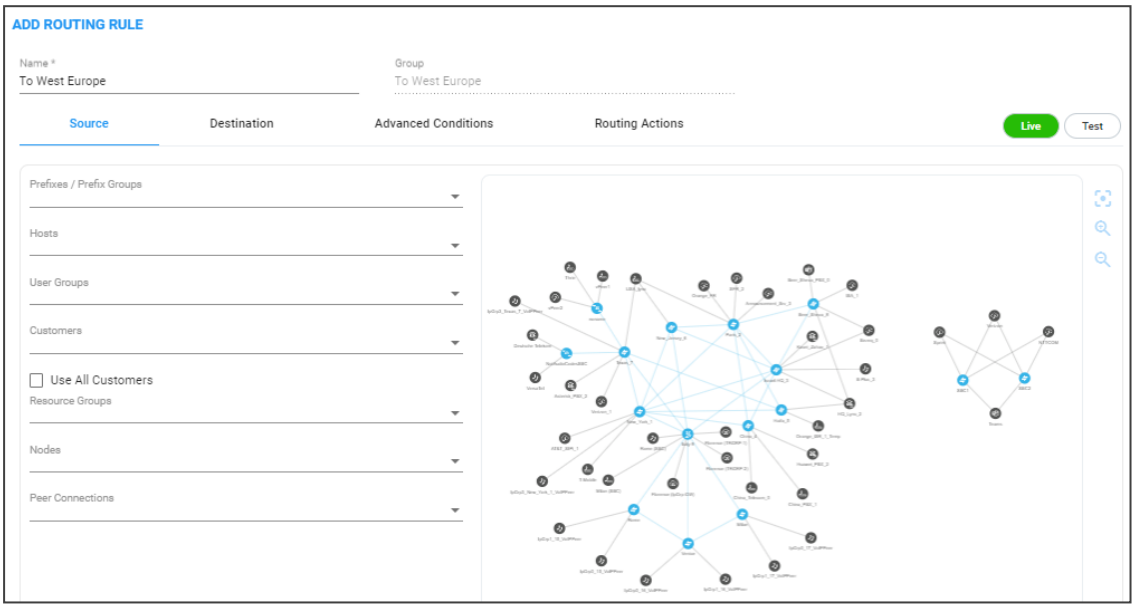
Duplicating a Routing Rule

You can duplicate a Routing Rule listed in the Routing Rules page (or in the Routing Groups page). The feature can be of particular benefit to support engineers and Field Application Engineers when they need to define *multiple* Routing Rules that are *similar* to rules already defined,

for example, a rule that will have the same actions as a previously defined rule but a different prefix and node.

➢ **To duplicate a routing rule:**

1. In the Routing Rules page (**Routing** > **Routing Rules**) , select the rule to duplicate and then from the **Actions** drop-down, choose the **Duplicate** option.



2. Modify the duplicated rule to conform to your requirements using Adding a New Routing Rule on page 328 as reference.

Testing a Route

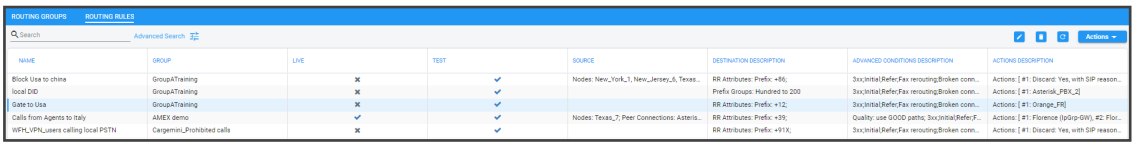
A route can be tested to make sure it performs according to expectations. See Testing a Route on page 96 for more information.

Using the Routing Rules Page

Some network administrators prefer to manage routing rules in the Routing Rules page.

➢ **To manage routing rules:**

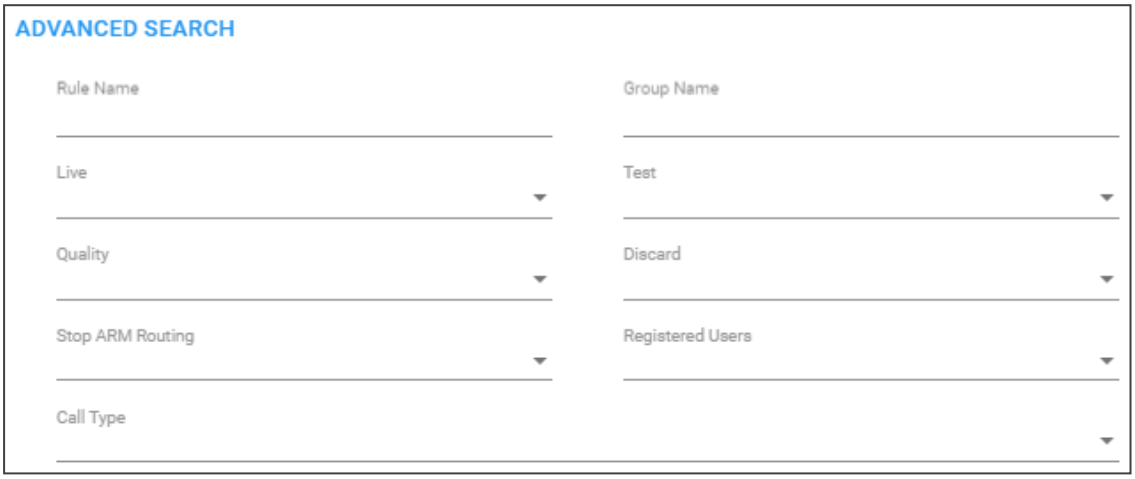
1. Open the Routing Rules page (**Routing** > **Routing Rules**).



2. In the page:
   - Edit a rule
   - Delete a rule

- Duplicate a rule (allows administrators to conveniently and easily add a rule based on an already defined rule)
- Promote or demote 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.
4. Click the **Advanced Search** link.



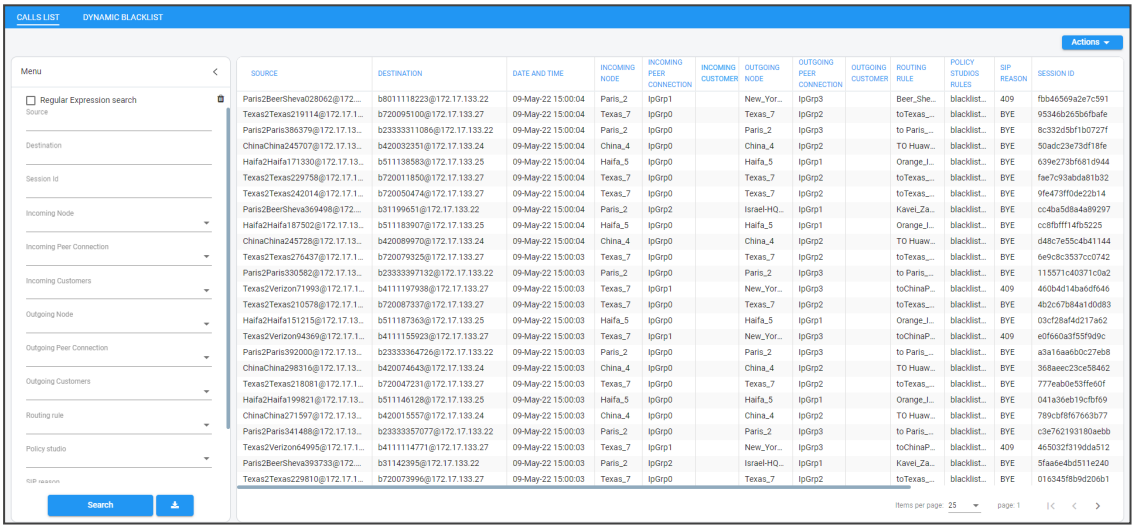
The search filters the page according to one or more parameter values chosen.

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.



Each row in the Calls List 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.

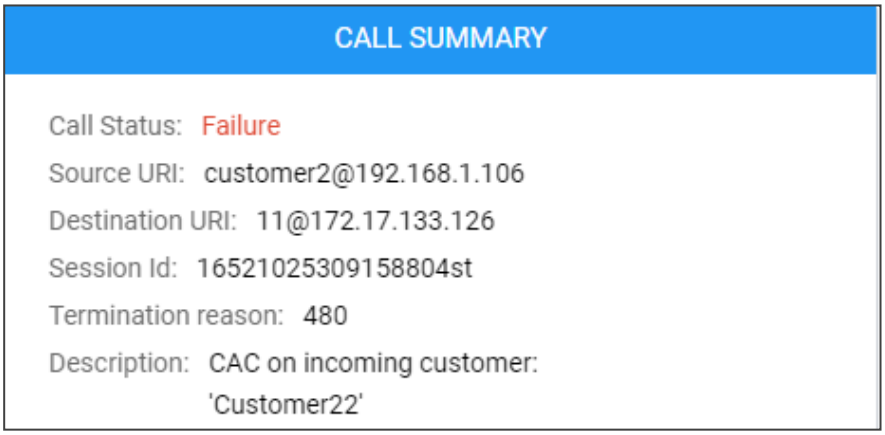
During call processing, each ARM Router periodically sends a bulk of call information (CDRs) to the ARM Configurator for processing. The received CDRs are processed and transformed / correlated into a single call record for each ARM end-to-end call. These records are stored in the ARM Configurator's database (MongoDB).

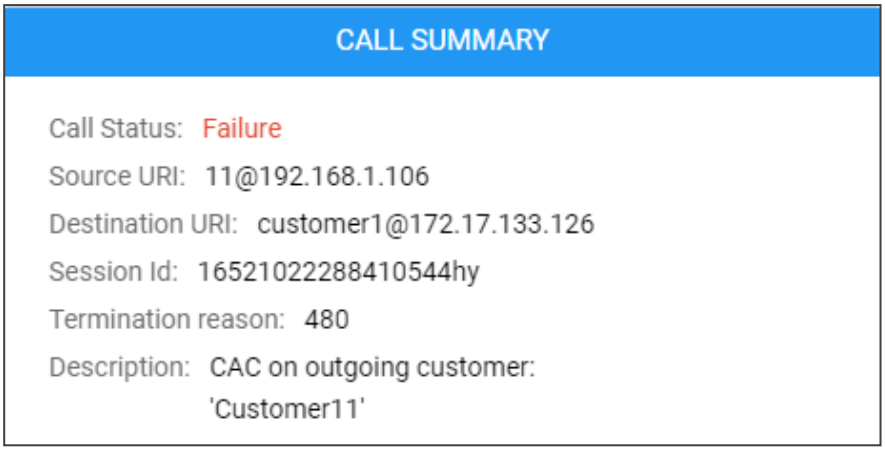
The page displays:

- Filters on the left side of the page, used to facilitate searching for calls and to exclude unwanted calls from the Calls List
- Calls List to the right of the filters, with a predefined call digest (information)

2. Use the following table as reference when using filters:

Table 9-1: Filter Descriptions

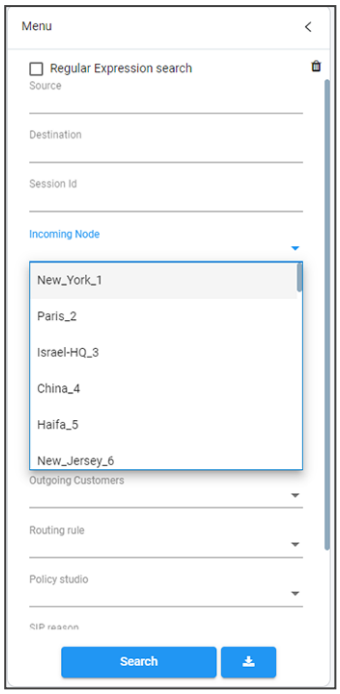
Filter	Description
Source	Enables filtering the Calls List per URI before manipulation.
Destination	Enables filtering the Calls List per URI before manipulation.
Session ID	Enables filtering the Calls List per Unique Session ID identifying a specific call.
Incoming Node	Enables filtering the Calls List per the node from where a call was initiated; selected from the drop-down menu.
Incoming Peer Connection	Enables filtering the Calls List per the Peer Connection from where the call was initiated; selected from the drop-down menu. If an incoming node is selected, the incoming Peer Connection option in the filter will include only relevant Peer Connections, associated with the selected node.
Incoming Customer	Indicates the call is classified as *from* a 'customer' entity. If a call from a 'customer' entity is dropped due to the number of simultaneous sessions (if a CAC Profile is attached to a 'customer' entity), double-click it in the Call Details page: 
Outgoing Node	Enables filtering the Calls List per the node from where the call exited the ARM network (terminated); selected from the drop-down menu.
Outgoing Peer Connection	From the drop-down menu select an Outgoing Node; the Outgoing Peer Connection option in the filter will include only relevant Peer Connections associated with the selected node.
Outgoing Customer	Indicates the call is classified as *to* a 'customer' entity. If a call to a 'customer' entity is dropped due to the number of simultaneous sessions (if a CAC Profile is attached to a 'customer' entity), double-click it in the Call Details page:

Filter	Description
	
Routing Rule	Enables filtering the Calls List per the name of the Routing Rule matching the call and used for its routing; selected from drop-down menu and organized per the Routing Groups.
Policy Studio Rules	Enables filtering the Calls List per the Policy Studio rules.
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.

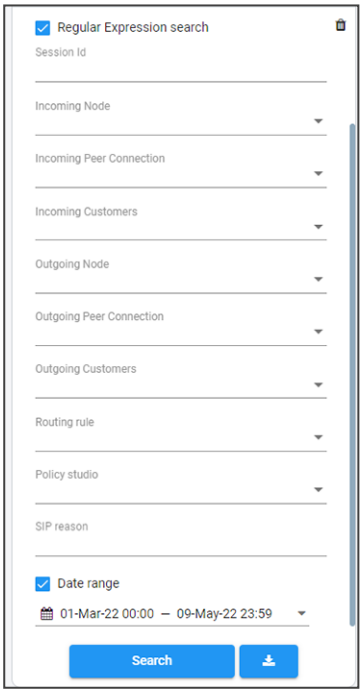
You can remove a filter by clicking **x**.

Figure 9-1: Filters



Some fields allow a regular expression which operators can use to further narrow down the search.

Figure 9-2: Regular Expression search



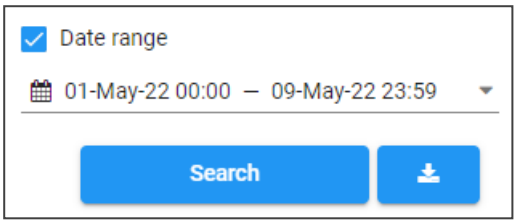
By selecting the **Regular Expression search** option, you can use any valid regular express pattern to search the following fields:

- Source
- Destination
- Session ID

- SIP reason

> **Performing a search using regular expression can be slow. The speed depends on the expression and the number of results.**

Up to 10000 of the filtered calls can be exported to a CSV file. You can export calls which match the search criteria by pressing the **Export calls to CSV** button adjacent to the **Search** button.



The CSV file consists of the following columns (same as the columns in the Calls List page):

- Session id
- Setup time
- Release time
- Source URI
- Destination URI
- Incoming node
- Incoming peer connection
- Outgoing node
- Outgoing peer connection
- Incoming customer
- Outgoing customer
- Routing rule
- Policy Studio rules
- SIP termination reason
- Voice duration (in milliseconds)

Figure 9-3: Call Columns in the Calls List

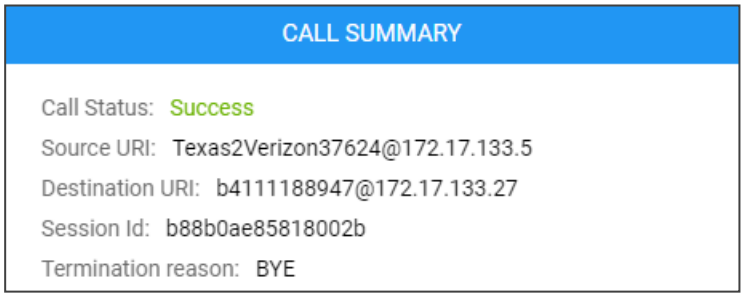
SOURCE	DESTINATION	DATE AND TIME	INCOMING NODE	INCOMING PEER CONNECTION	INCOMING CUSTOMER	OUTGOING NODE	OUTGOING PEER CONNECTION	OUTGOING CUSTOMER	ROUTING RULE	POLICY STUDIOS RULES	SIP REASON	SESSION ID
Paris2...	b801114...	09-...	Paris_2	IpGrp1		New_Y...	IpGrp3		Beer_...	black...	409	1684c763bf602c25
Texas...	b720077...	09-...	Texas_7	IpGrp0		Texas_7	IpGrp2		toTex...	black...	BYE	5058e832159982a2
Haifa...	b511134...	09-...	Haifa_5	IpGrp0		Haifa_5	IpGrp1		Orang...	black...	BYE	510e9cebf45cdc96

Call Details

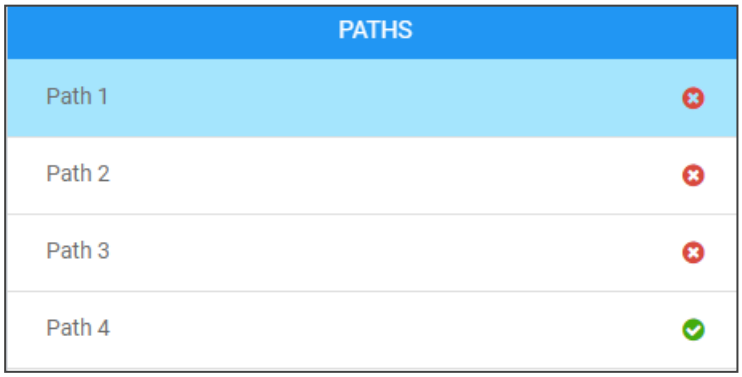
The details of a specific call can be viewed. In the Calls List page, filter the list and then double-click a specific call for the Call Details page to open.

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

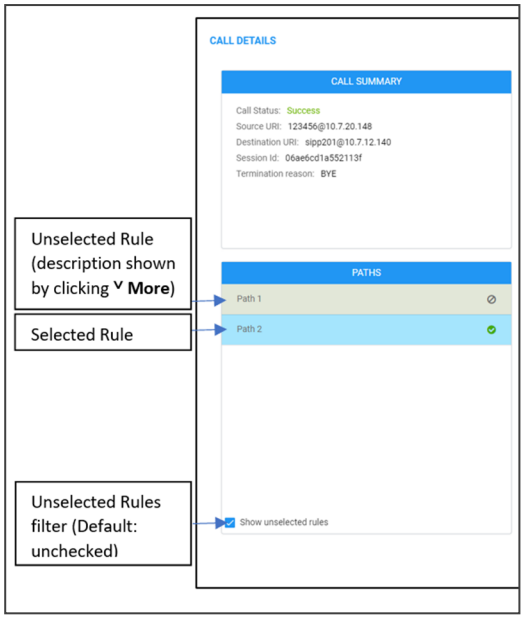
The Call Summary pane displays the following routing information about the call:



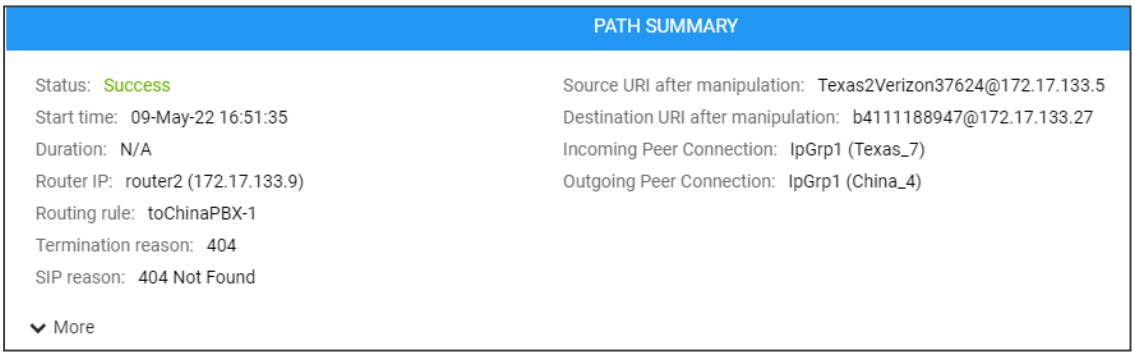
The Paths pane displays the list of paths the ARM attempted when routing the call.



Unselected paths appear also for calls:



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.



Pre-route Unselected Rules such as web-services are still displayed in the 'Details' screen of every path (viewed by clicking ˅ **More**).

Use the table as reference to the Path Summary.

Table 9-2: Path Summary

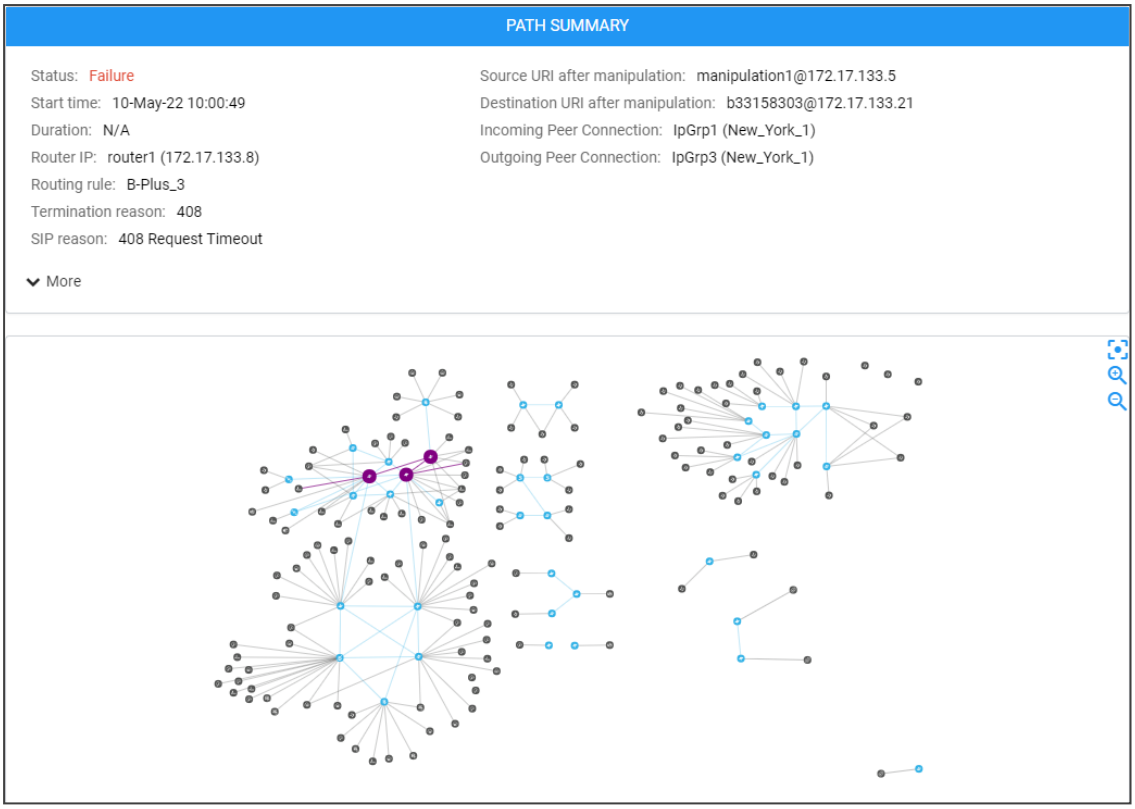
Setting	Description
Status	Displays whether the path was Success or Failure.
Start time	Displays the ARM setup time.
Duration	Displays the call duration; non-zero if 'Status' is Success.
Router IP	Displays the IP of the Router which handled the initial Routing request.

Setting	Description
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.
Incoming Peer Connection	Displays the incoming Peer Connection.
Outgoing Peer Connection	Displays the outgoing Peer Connection.
Termination reason	Displays the reason why the specific path was terminated.
SIP reason	Displays the specific path's SIP termination reason.

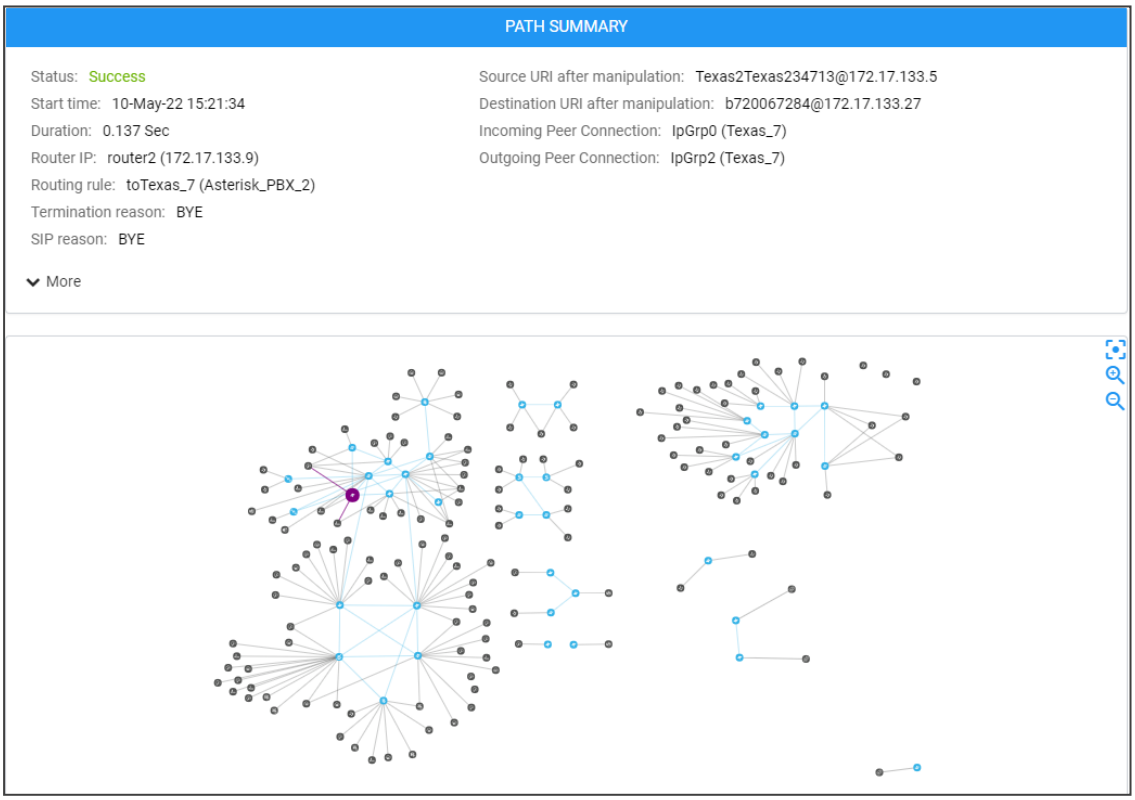
If Source or Destination URI manipulation was applied for a specific path, the manipulation information will be accessible from the displayed **More** option. The pane's **More** option allows you to review the details of the applied manipulation rules.

Figure 9-4: '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:



The maximum number of Unselected Rules in calls can be configured in the Global Routing Settings page (see Configuring Global Routing Settings on page 300). The default value is 5, limited to a maximum of 25 per call. The 'Path Summary' pane under 'Manipulation during

route' indicates (after clicking the **More** option) if the maximum number of Unselected Rules has been exceeded and if there are more Unselected Rules that are not shown:

Maximum number of unselected rules to be shown is reached.

For historical calls, the Call Details page's 'Path Summary' pane indicates if the maximum number of Unselected Rules was exceeded and if there are more Unselected Rules that were not shown:

This call does not contain information about unselected rules / policy studio.

Old calls that are not supported by this feature are indicated.

Adding Node Information to Call Details

The ARM enables customers to add information from a node to Call Details, using a variable in the node **Var.call.Src.UserDefined1**.

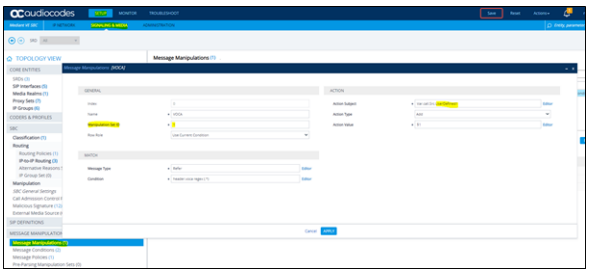
The variable can be created and assigned with a value using Message Manipulation; it's attached to the 'Inbound Message Manipulation Set' of a specific IP Group in the node.

In the example shown in the figure below:

➢ To add information from a node to Call Details:

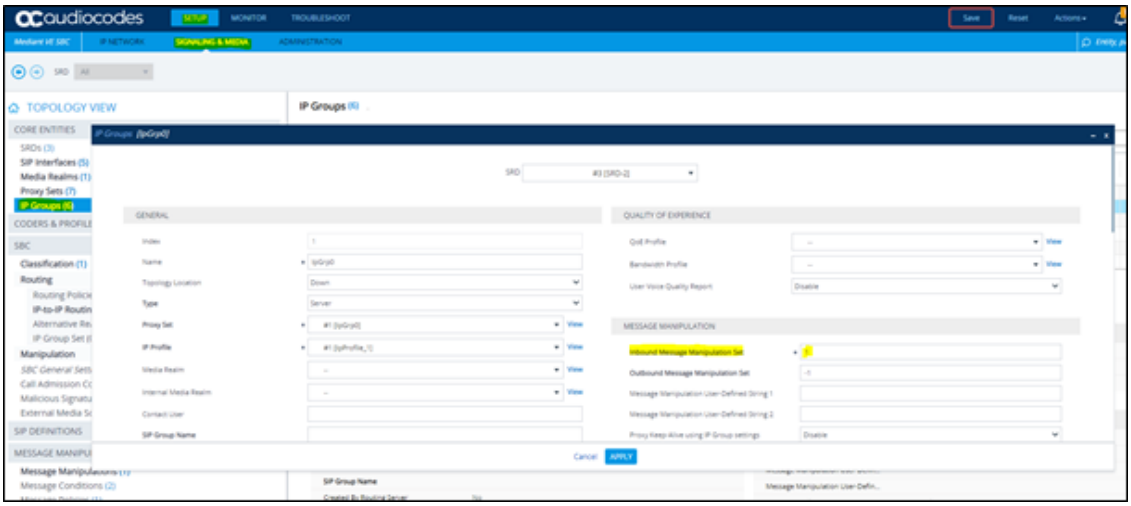
1. Take information from propriety header 'voca' and assign it to the variable **Var.call.Src.UserDefined1**.

Figure 9-5: Information from propriety header 'voca'



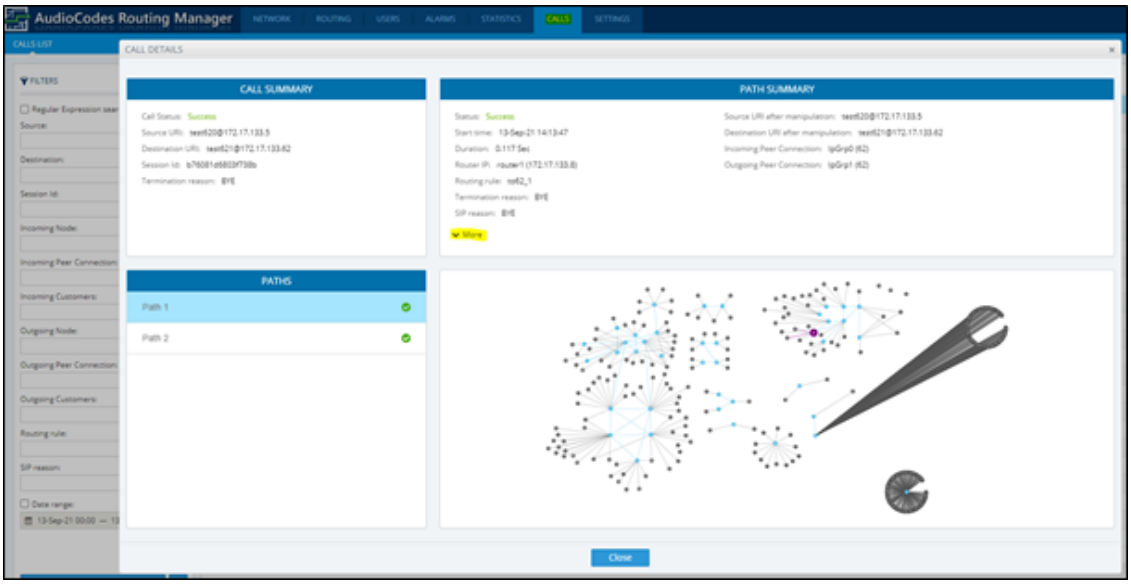
2. Assign it to the IP Group in the node:

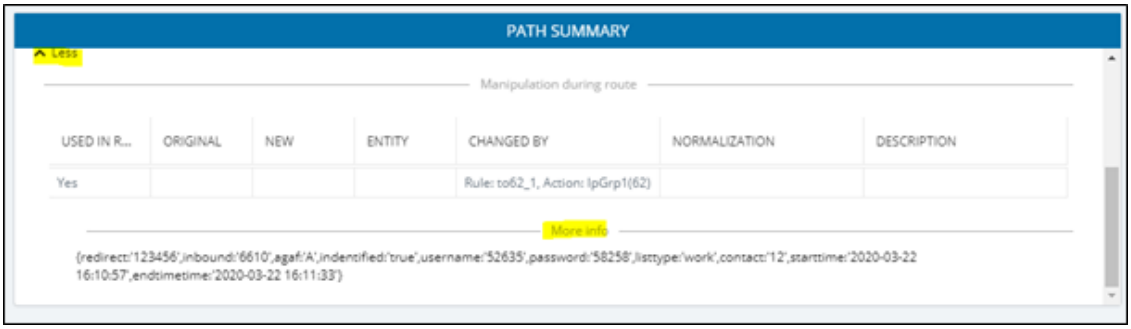
Figure 9-6: Assign info to the IP Group in the node



3. View the information by clicking the **More** option in the Call Details screen (accessed from the **Calls** menu) shown in the figure below, and then locating screen section 'More Info', shown in the figure below it. In the following example, it's a string contained by the 'voca' header.

Figure 9-7: Call Details





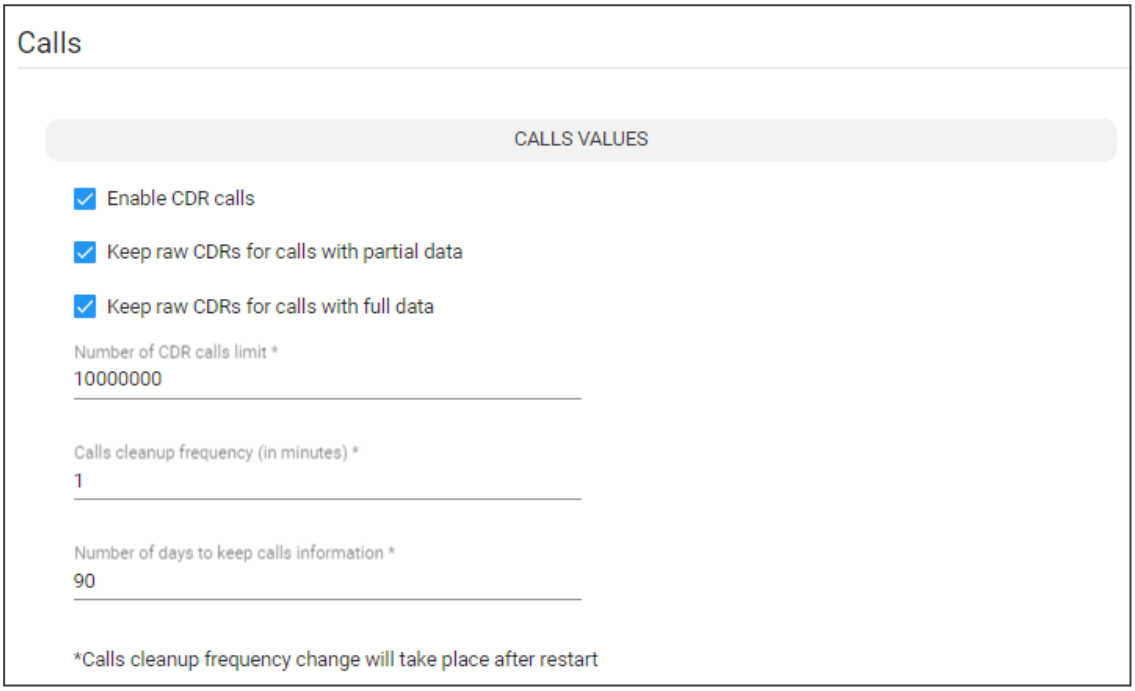
Disabling, Limiting the Number of CDRs

The Call Detail Records feature is by default enabled. You can optionally disable it. You can also control the number of records the ARM keeps in the database. The default number of records is 10 million. This is also the maximum number.

➢ **To control call records:**

1. Open the Calls screen (**Settings** > **Advanced** > **Calls**).

Figure 9-8: Calls



2. Use the following table as reference.

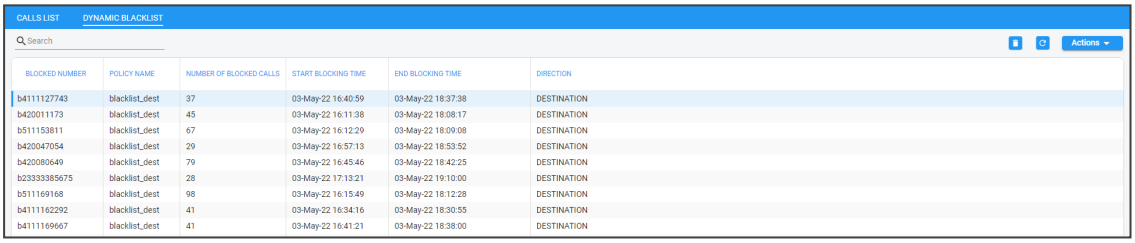
Table 9-3: Calls

Setting	Description
Enable CDR Calls	Optionally disable CDRs by clearing the selection. By default, the parameter is selected (enabled).
Keep raw CDRs for calls with partial data	If selected, the ARM saves all CDRs processed to create 'end-to-end calls' for calls terminated before all information about them was received. This parameter impacts database size so the default is unselected; you'll not be able to save 10 million calls. Enable the parameter for debugging purposes only.
Keep raw CDRs for calls with full data	If selected, the ARM saves all CDRs processed to create 'end-to-end calls' for calls terminated successfully. This parameter impacts database size so the default is unselected; you'll not be able to save 10 million calls. Enable the parameter for debugging purposes only.

Setting	Description
Limit number of CDR calls to	Enter the number of CDRs to limit the ARM to.
Calls cleanup frequency	Determines how often the ARM checks the size / number of calls. Default: Every 10 minutes. The parameter depends on the number of CAPs. After changing the parameter, restart the ARM Configurator.
Number of days to keep calls information	Determines how long calls information will be kept (in days). Gives operators the ability to manage resources more effectively. Minimum: 1 day. Maximum: 365 days.

Managing a Dynamic Blacklist

ARM supports management of a flexible automatic dynamic blacklist.



When configured, the blacklist can include either source of destination phone numbers (DIDs), calling or called with predefined frequency. The list is maintained automatically by the ARM according to customer definitions; in the ARM, operators add phone numbers to the blacklist or remove them from it.

The feature allows operators to prevent DDOS/DOS and calls flooding attacks on the enterprise. DID calling (or called) with suspicious frequency can be handled as bothersome and disruptive, and added to the blacklist.

Operators can decide how to handle blacklisted calls using the ARM's generic routing capabilities. The calls can be dropped or routed to a specific server (for example).

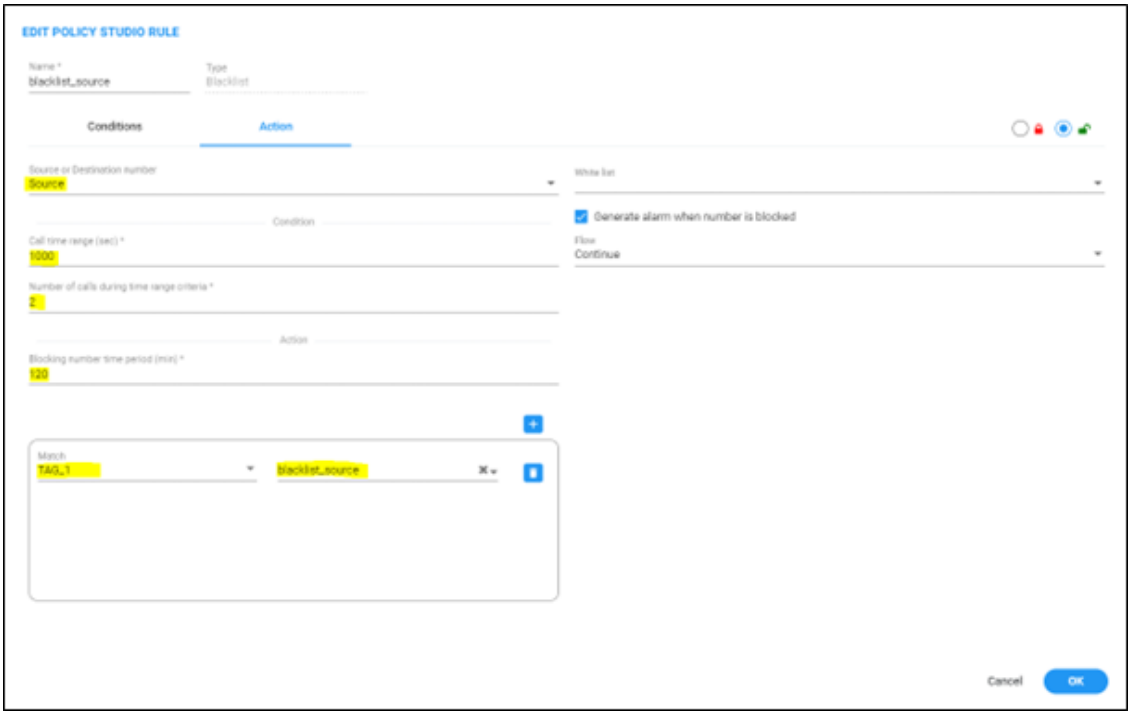
Network operators must configure a Policy Studio Rule to dynamically add a number to the blacklist or remove a number from it, with some criteria.

➢ To configure a Dynamic Blacklist:

1. Open the Policy Studio page (**Settings** > **Call Flow Configurations** > **Policy Studio**) and click the add icon **+** to configure a Policy Studio rule to dynamically add a number. See here for detailed information about Policy Studio.
2. In the Add Policy Studio Rule screen, configure 'Type' as **Blacklist**; parameters displayed under the **Conditions** tab are identical to those displayed when **User** is defined for 'Type'. See here for more information.
3. Click the **Action** tab and configure:

- Source or Destination number – to be checked and added to / removed from the list.
- Call time range (sec) – higher equals 1. Default: 60.
- Number of calls during time range criteria - higher equals 1. Default: 5.
- Blocking number period time (min) - higher equals 10. Default: 60.
- Adding tags = Tag_1/2/3. Decision of blocking in the Routing Rule using tag info.
- Whitelist – Policy Studio will ignore those Prefixes / Prefix Groups.
- Generate alarm when number is blocked – when there is at least one number in the list, an alarm will be triggered. When the list is empty, the alarm will be cleared.
- An event is generated for each new number added to the Blacklist.

  Use this example as reference:



4. Refer to the example in the figure:
   - Source or Destination number = **Source**
   - Call time range (sec) = **1000**
   - Number of calls during time range criteria = **2**
   - Blocking number period time (min) = **120**
   - Adding Tag_1 = **blacklist_source**

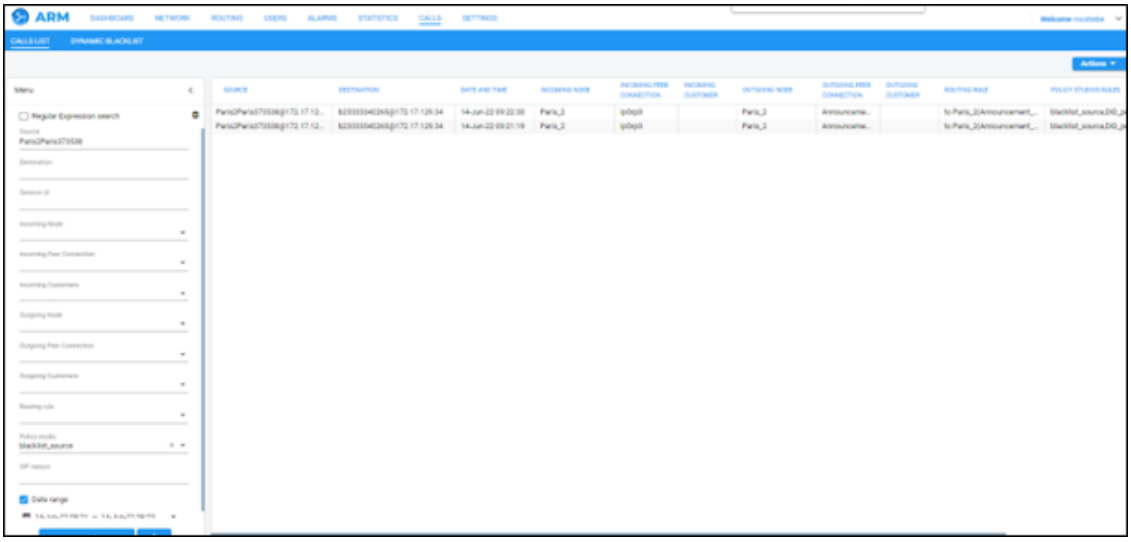
With this configuration, the following scenario occurs:

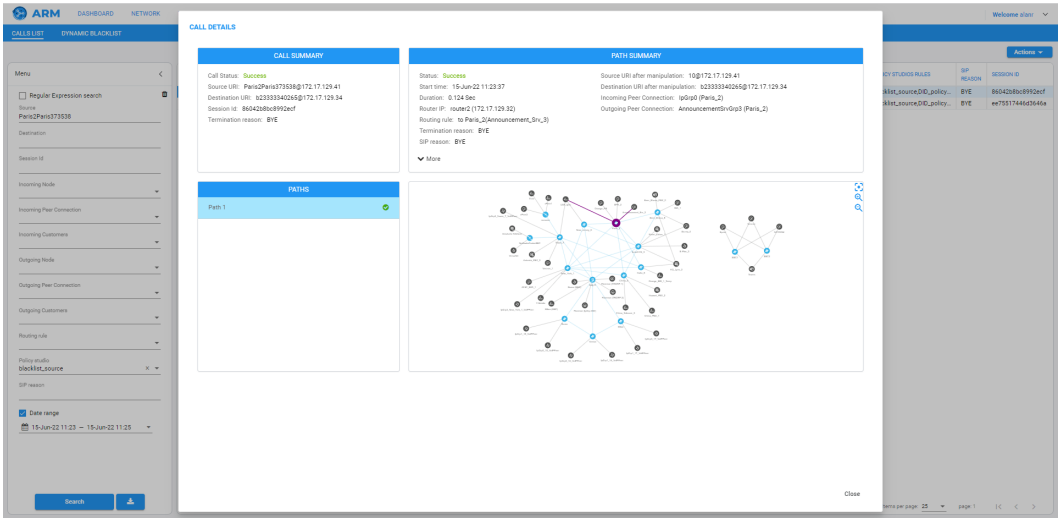
- If the **source** number calls more than **2** times in **1000** seconds, it's added to the Blacklist for **120** minutes after which it's removed.

- For each call from a source number listed in the Blacklist, Policy Studio will create TAG_1 = **blacklist_source**.
- The decision whether or not to block this tagged call is made in the Routing Rule, as shown in the following example:

➢ To view blacklisted (blocked) DIDs:

1. Open the 'Dynamic Blacklist' page (**Calls** > **Dynamic Blacklist**) to view current content as shown here; all blacklisted numbers are shown in the page, which centralizes all calls from all ARM Routers.
2. In the page:
   - **Delete** single or multiple DIDs from the list by selecting the number to delete and then clicking the delete icon . The function allows you to manually interfere with ARM decisions that are based on configuration of a 'Blacklist' in Policy Studio Rules. Multiple DIDs can be selected with 'multi-select' option.
   - **Delete all** can be selected from the **Actions** drop-down; all numbers are deleted from all Blacklists (defined in Policy Studio Rules). This action resets the lists.
   - **View calls** can be selected from the **Actions** drop-down (after selecting a row), allowing you to view details of a call with phone numbers (DIDs), as part of the Blacklist; the filtered Call Details screen from the filtered Calls List page (**Calls** > **Calls List**) opens.





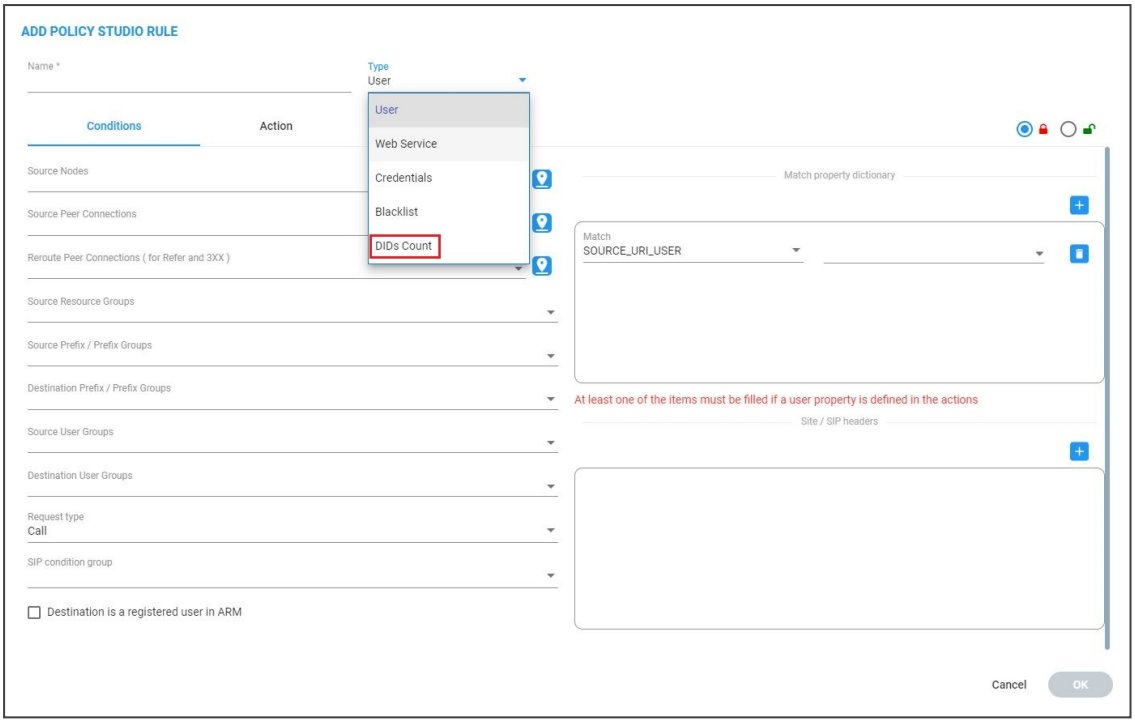
The feature allows you to view (for example) if an attack is continuing and if attempts are still being made to call from / to the restricted number.

Configuring a DIDs Count

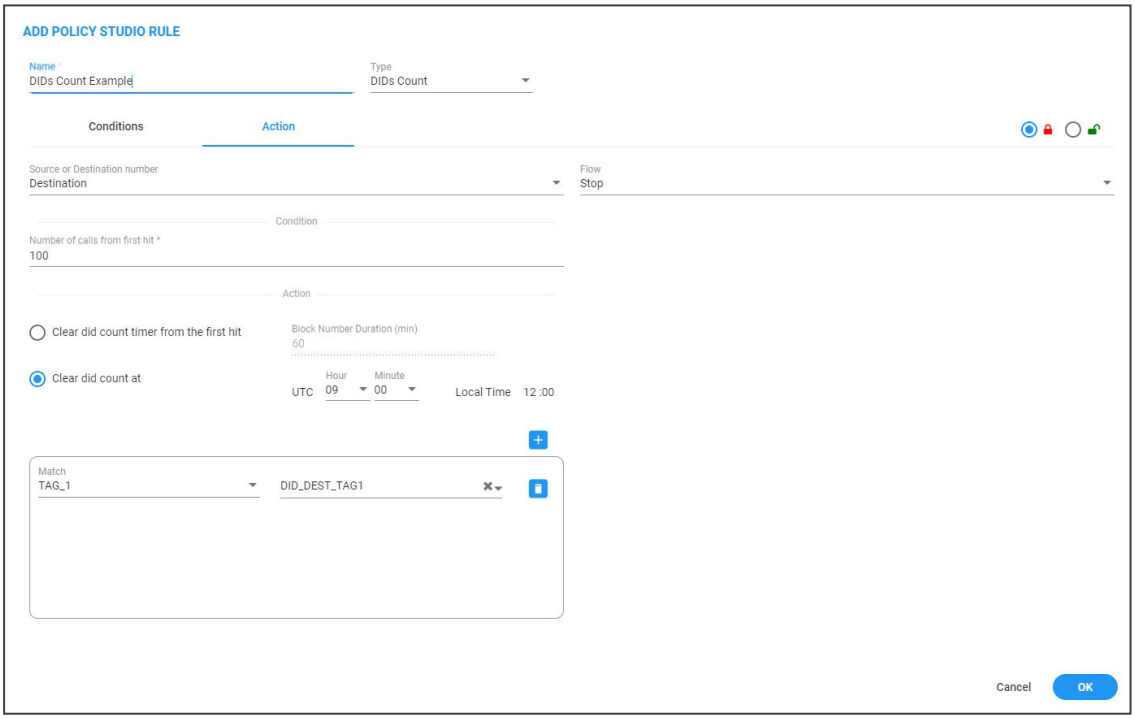
ARM supports phone numbers (DIDs) counting. The feature allows operators to prevent DDOS/DOS and calls flooding attacks on the enterprise. DID calling (or called) with suspicious frequency can be handled as bothersome and disruptive, and can be blocked by using the ARM's generic routing capabilities.

➢ **To configure a DIDs count:**

1. Open the Policy Studio page (**Settings** > **Call Flow Configurations** > **Policy Studio**) and click the add icon **+** to configure a Policy Studio rule to dynamically add a number. See here for more information.
2. In the Add Policy Studio Rule screen, configure 'Type' as **DIDs Count**; parameters displayed under the **Conditions** tab are identical to those displayed when 'Type' is defined as **User**. See here for more information.



3. Click the **Action** tab.



4. Configure:

- Source or Destination number – the phone number of the caller/callee to be counted.
- Number of calls from first hit: the number of calls from which to add the tags for this Policy Studio.
- Clear DID count timer from the first hit - the duration, in minutes, from the first hit until the count clearing.

- Clear DID count at - the specific time of day for the count clearing.
- Adding tags = Tag_1/2/3. Tag info is used in Routing Rules.

10 Viewing Alarms

The Alarms page shown in the figures in the following pages displays alarms generated in the enterprise's network topology, e.g., SBC disconnected. In the Alarms page, 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: Active Alarms

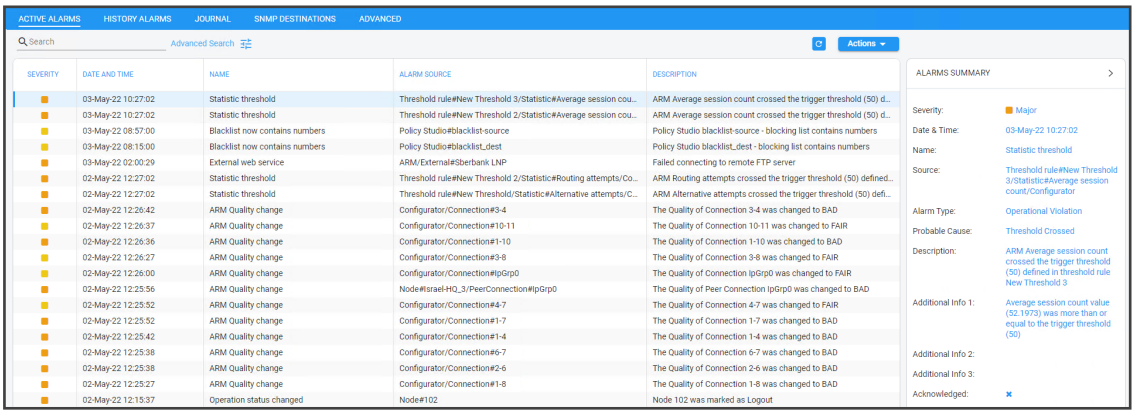
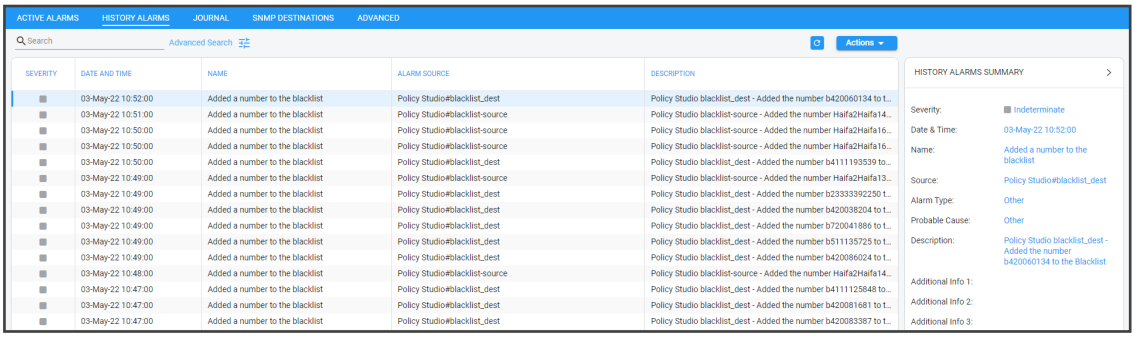


Figure 10-2: History Alarms



Click any alarm listed on any page; that alarm's ALARMS SUMMARY pane, shown in the preceding figure, displays the column information as well as:

- ALARM TYPE
- PROBABLE CAUSE
- ADDITIONAL INFO1
- ADDITIONAL INFO2
- ACKNOWLEDGED

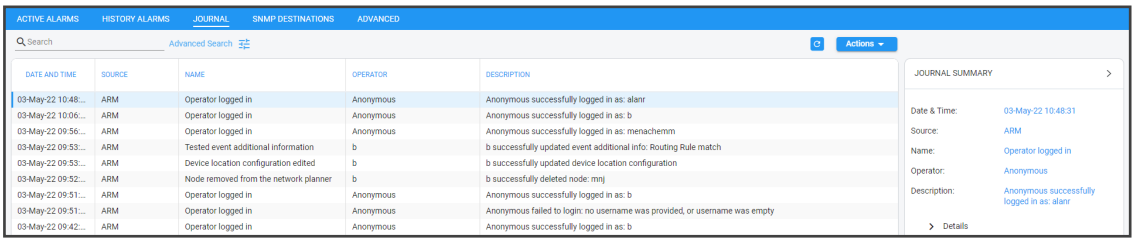
In the Active Alarms and History Alarms pages you can:

- Sort alarms, according to column header
- Use the 'Search' feature to locate specific alarms (see Locating a Specific Alarm on the next page).
- **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 viewing historical actions and activities performed in the ARM by all network operators up to the present time.

The page can help determine if another operator's action or activity may have changed network functionality and been responsible for an active alarm.



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.

In the JOURNAL SUMMARY pane, click **> Details** to view the operator's:

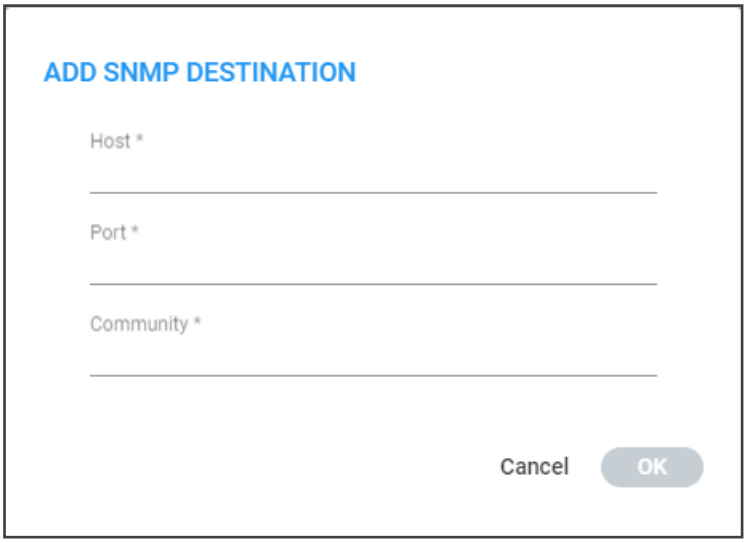
- url
- id
- userName
- password
- role
- names

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 the add icon **+**.



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.

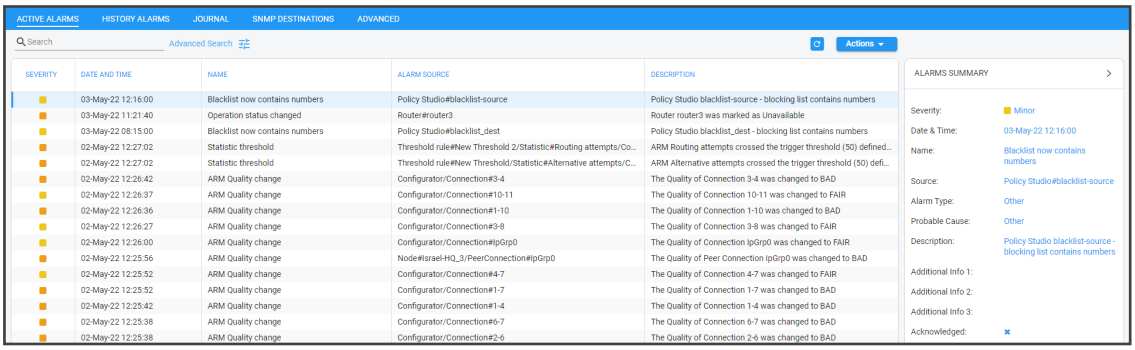
Locating a Specific Alarm

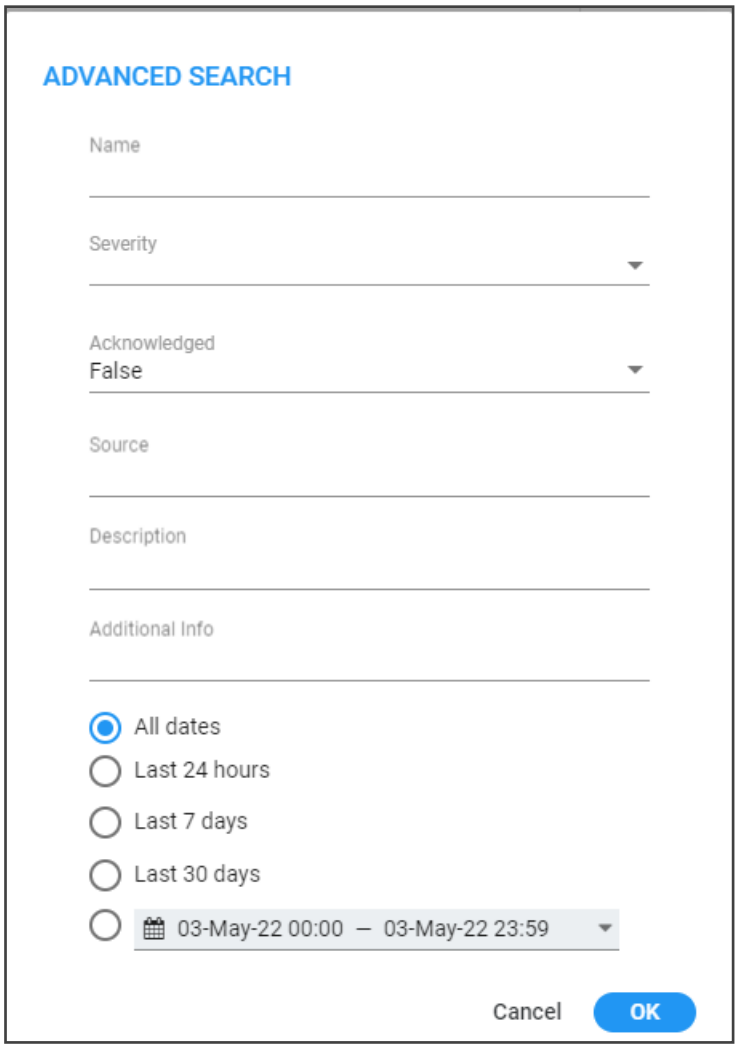
The search feature helps administrators quickly and easily locate specific alarms thereby facilitating effective management which in turn leads to improved performance of the IP telephony network.

➢ 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 **Advanced Search** icon; the figure shown after the next is displayed.

Figure 10-3: Search





2. Enter any information about the alarm you know. You must enter information in at least one field.

   - The 'Name' field is identical to the simple search string field.

- From the 'Severity' drop-down menu, select Clear, Indeterminate, Warning, Minor, Major or Critical. All alarms whose severity level match your selection will be displayed.
- From the 'Acknowledged' drop-down menu, select True (the default is False). All acknowledged alarms will be displayed.
- For the alarm 'Source', enter the node name or the Peer Connection name, if you know it. All alarms originating from that source will be displayed.
- In the 'Description' field, enter a key word used to describe the alarm.
- Select either **Between Times**, **Last 24 hours**, **Last week** or **Last 30 days**. All alarms whose timestamp matches your selection will be displayed.

3. Click **OK**.

Enriching Routing Rule Matching Notifications with ARM Information

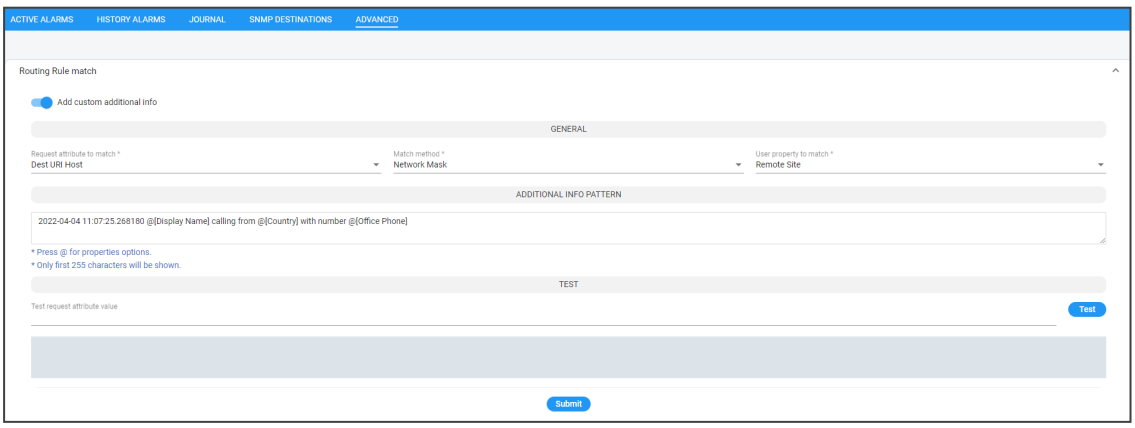
In addition to supporting notification on a call matching a specific rule, the ARM also allows operators to *customize information provided with the notification*. The feature - notification sent on a call matching a rule - is usually applied for emergency calls such as 911 calls. The notifications usually require additional information such as user name, building, floor, country or office branch name. This information is not part of the SIP INVITE message but it can be added to the ARM users database and used for additional information in notifications.

➢ **To implement the feature, follow this procedure:**

- Add the corresponding Property Dictionary property (**Users** > **Property Dictionary**) to the ARM's Users table and add the information to these columns; this data will be used as the additional information in generated notifications. See Adding a Property Dictionary to the ARM on page 172 for more information.
- Customize the notification in the 'Routing Rule match' screen (**Alarms** > **Advanced** > **Routing Rule match**) as described below.

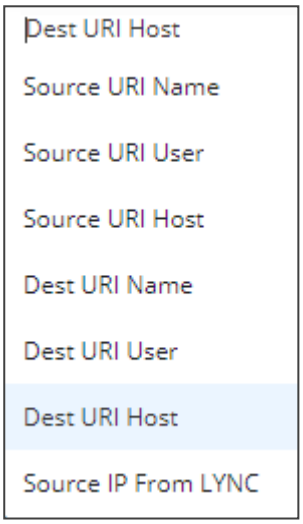
➢ **To enrich routing rule matching notifications with ARM information:**

1. Open the 'Routing Rule match' screen (**Alarms** > **Advanced**) to customize the notification.



2. Enable the feature using parameter 'Add custom additional info'.
3. Define the notification under GENERAL and under ADDITIONAL INFO PATTERN shown in the preceding figure.
   - The GENERAL section relates to matching. It is used to identify the exact row (the exact record) in the Users page to be used to extract additional information for the notification. It includes:
     - **Request attribute to match**. Defines which **SIP INVITE message** property will be used as the matching criteria. The information is taken by the ARM Router from the SIP message and used to find the corresponding row in the Users page. Operators can select from the drop-down:

Figure 10-4: Request attribute to match: SIP INVITE message properties



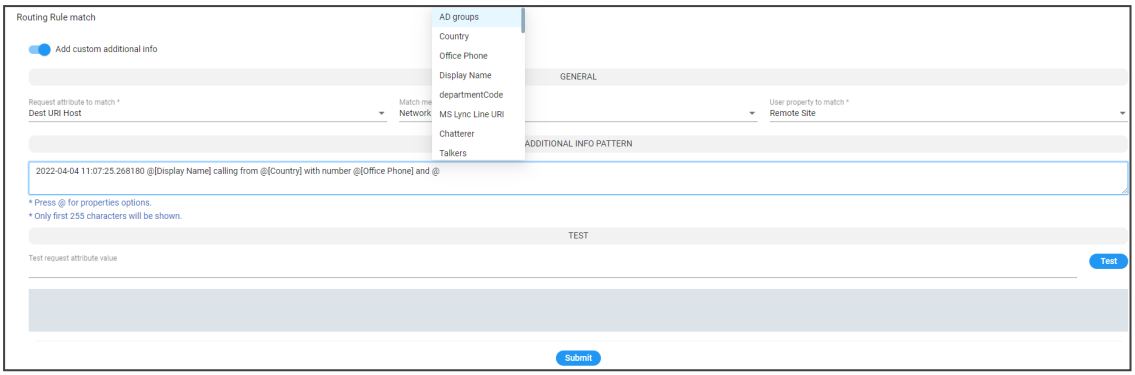
     - **Match method**. Defines how to look for the corresponding entry in the Users table. Available values are Full (for an exact match), Contains (for the Users table value to contain the SIP message field) or Network Mask (for the value of the subnet mask).
     - **User property to match**. Defines one of the properties (available in the ARM Users table) to be used for matching; the operator can select any property from the Property Dictionary.

In the preceding example, the Routing Rule match criteria are configured to make the following match:

If the IP address is taken from 'Dest URI Host' of the SIP Invite message belonging to the subnet (the matching method 'Network Mask') defined in the 'Remote Site' property of the ARM Users table, it will be considered as a match and this row in the Users table will be used for 'Additional info pattern'.

Using parameter 'Additional Info pattern', the operator defines information (and format) to be added as 'Additional Info 2' in the notification. This `information is taken from the Users page (per matching row). The information to be presented is formatted using the @ symbol after which the operator can select a specific property:

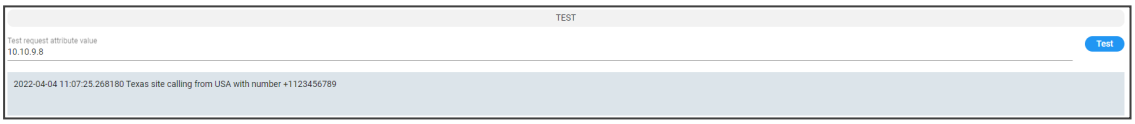
Figure 10-5: Add custom additional info



4. Use the 'Test request attribute value' field shown in the figure below to test the definition.

   - Enter any potential value for 'Request attribute to match' (that can potentially be received in the appropriate SIP header) and thereby validate the required definitions.
   - This is the pattern that will be displayed in 'Additional Info 2' in a real notification in the case of a real call.

Figure 10-6: Test request attribute value



If there is no match, the message **No user info found** is displayed.

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 385.

Gateway Routing Logic

AudioCodes' Media Gateway routes and handles IP-to-Tel, Tel-to-IP and Tel-to-Tel calls using an internal loopback IP Group.

Gateway routing logic is configured in the device's internal IP-to-Tel and Tel-to-IP tables. To migrate the gateway application's routing logic to the ARM network, you must set the routing parameter 'Gateway Routing Server' to Enable. When this configuration is applied in the gateway, all its routing goes through the ARM and internal routing configuration is ignored.

Hybrid Device Routing Logic

The ARM routes calls from the hybrid device's PSTN (gateway application) to IP (SBC application) or vice versa.

Calls cannot be routed from an IP Group (PCon in ARM) associated with a gateway application, to an IP Group associated with an SBC application on the same hybrid device.

To support a hybrid device, two internal IP Groups must be configured:

- From the SBC application to the Media Gateway application
- From the Media Gateway application to the SBC application

The ARM GUI does not display these two internal IP Groups. Routing is performed per the logic described under SBC Routing Logic on the previous page and Gateway Routing Logic above, respectively.

See Migrating Hybrid Routing to the ARM on page 391 for information about how to migrate hybrid device routing to the ARM.

Connecting the Device to the ARM Topology Server

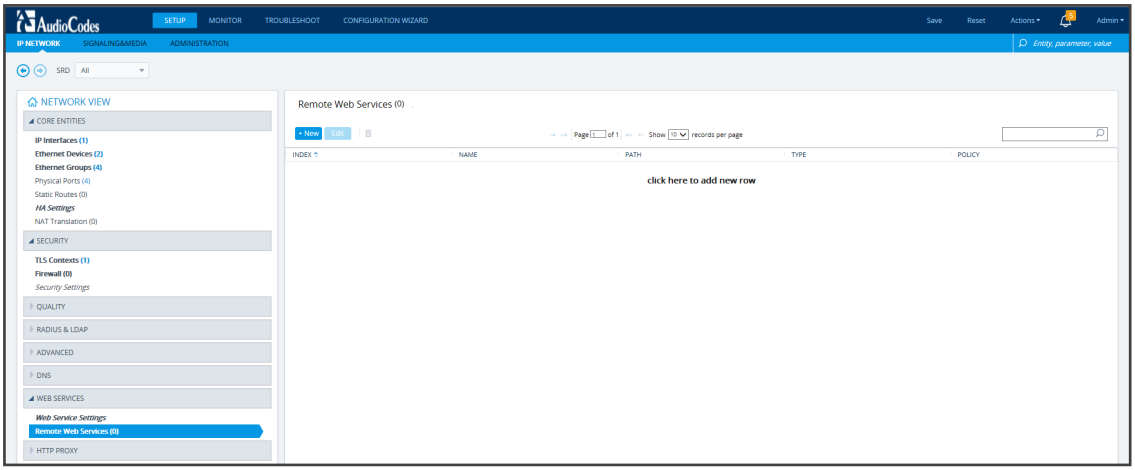
You need to connect the device to the ARM Topology Server.

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 82.

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

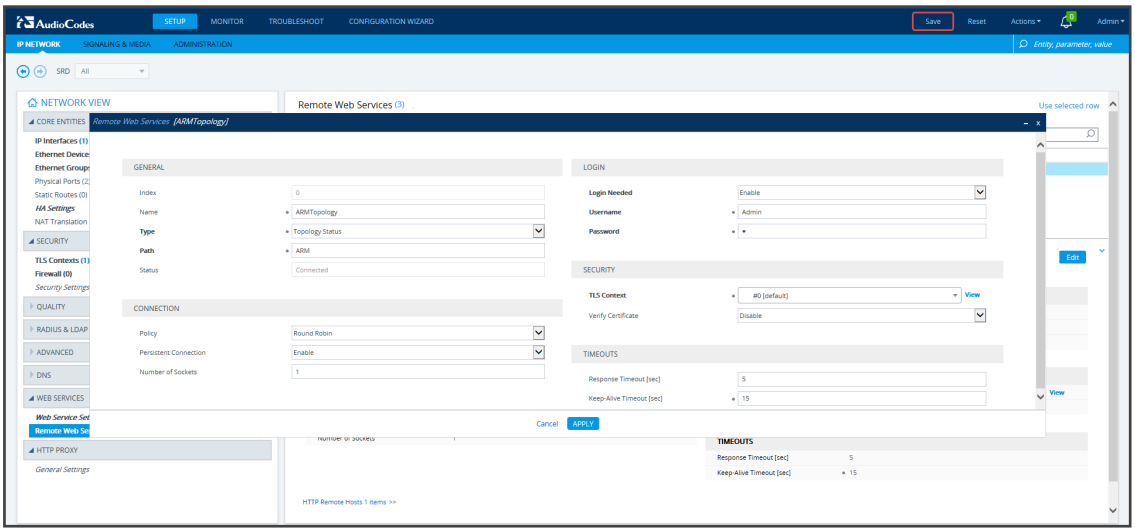
➢ **To connect the device:**

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**).



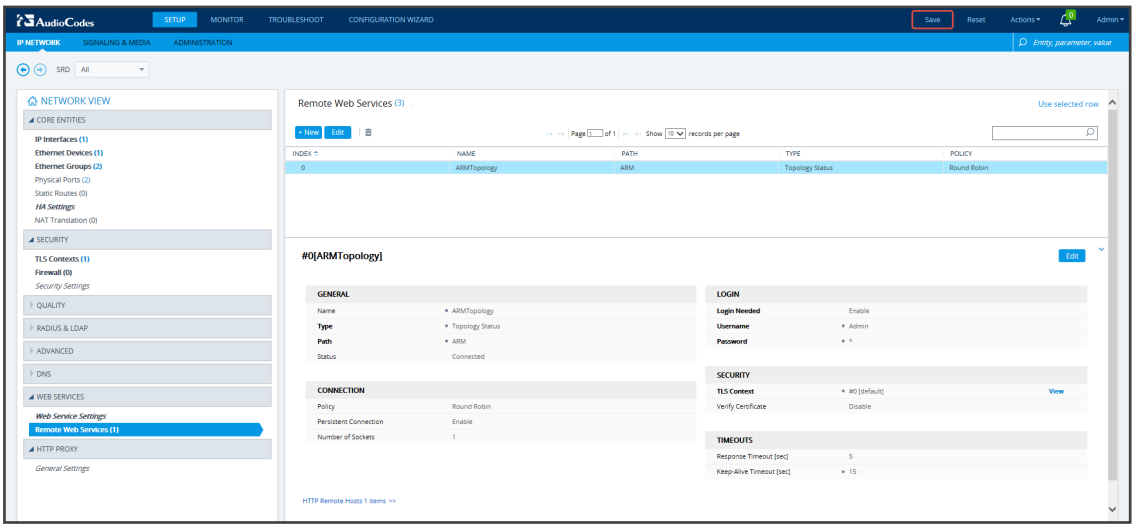
3. Click **+New** or **click here to add new row**.

Figure 11-1: Web Interface - HTTP Remote Services – Add Row



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

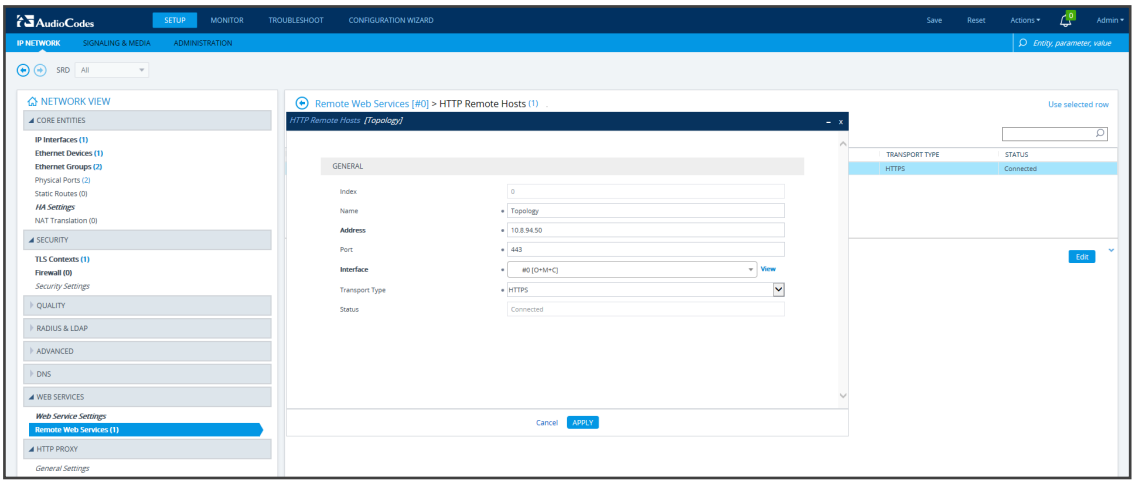
Figure 11-2: Web Interface - Remote Web Services – HTTP Remote Hosts



5. Click the **HTTP Remote Hosts** link shown in the figure above.

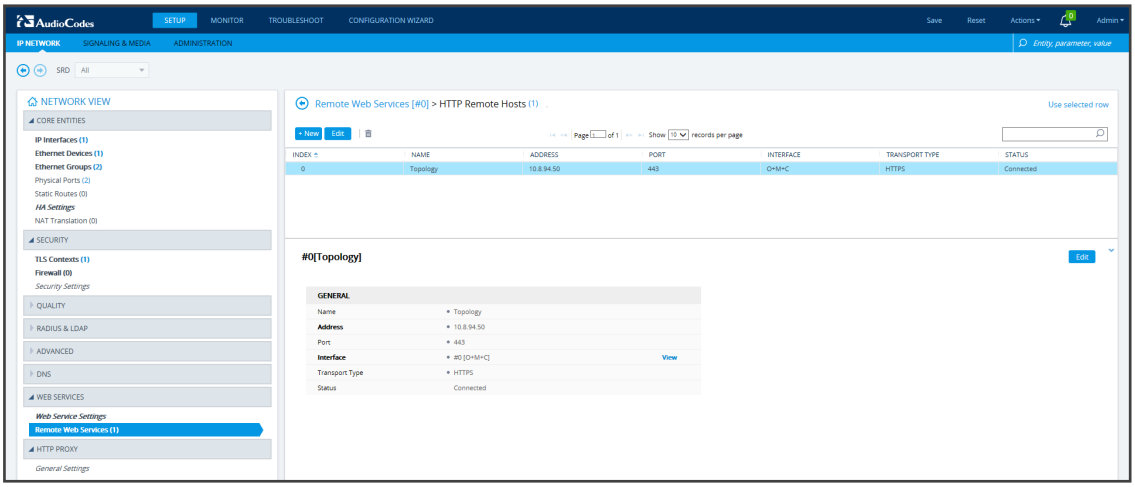
6. In the HTTP Remote Hosts page that opens, click the **Add** tab.

Figure 11-3: 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.

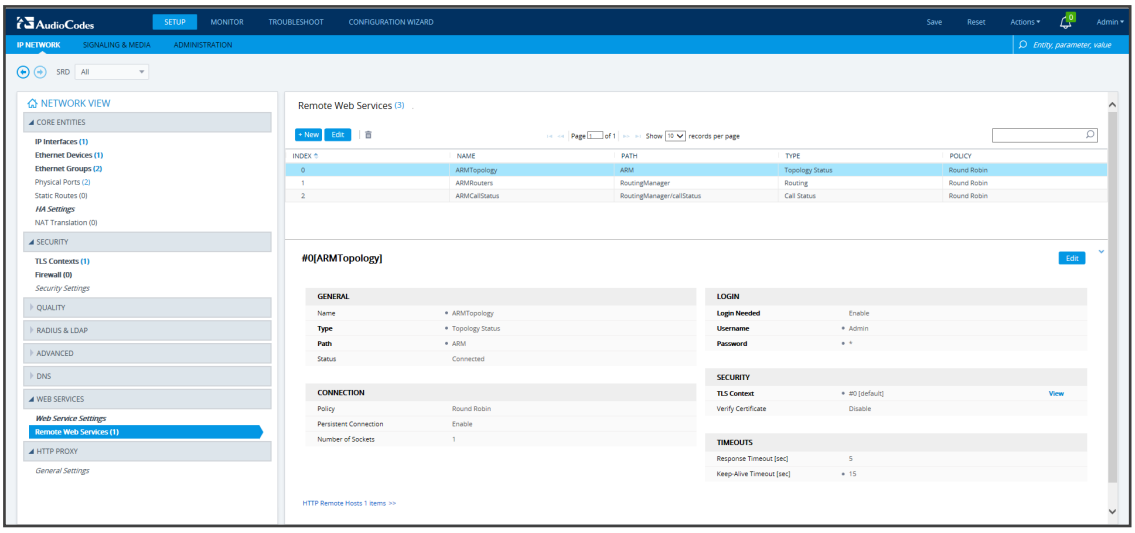
Figure 11-4: Web Interface – Device Connected to ARM Topology Server



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 11-5: 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

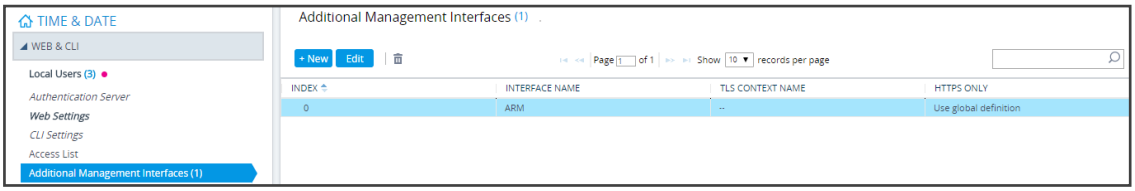
ARM version 7.8 and nodes (SBC or Gateway) version 7.20A.154.044 and later support the capability to define on AudioCodes devices additional IP interfaces for management on any application type (Media and/or Control, not OAMP) and different TLS contexts for each IP interface.

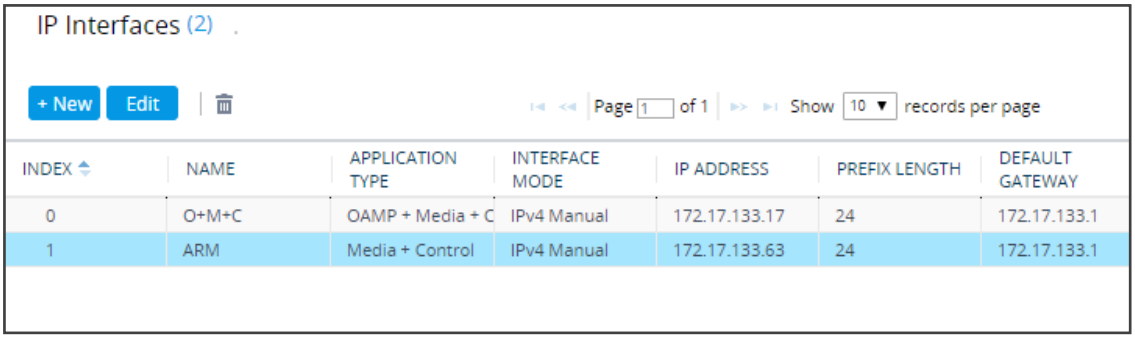
Defining a dedicated IP interface on the device for ARM traffic allows keeping ARM traffic internal, if required, separating ARM traffic from other device management traffic such as Web, SNMP and NTP.

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.





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 11-6: Web Interface – SIP Interfaces

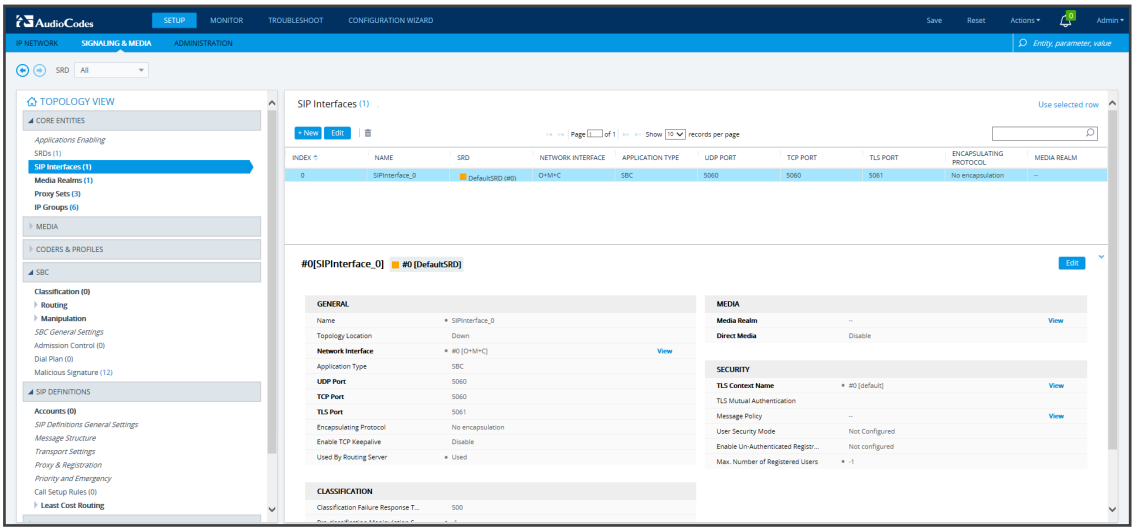
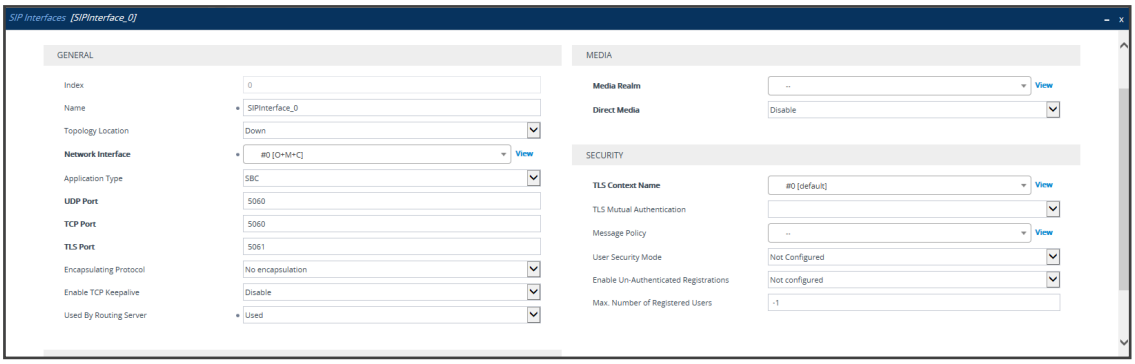


Figure 11-7: Web Interface – SIP Interfaces Table - Configuring a SIP Interface



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 395.
- '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 11-8: Web Interface – IP Groups

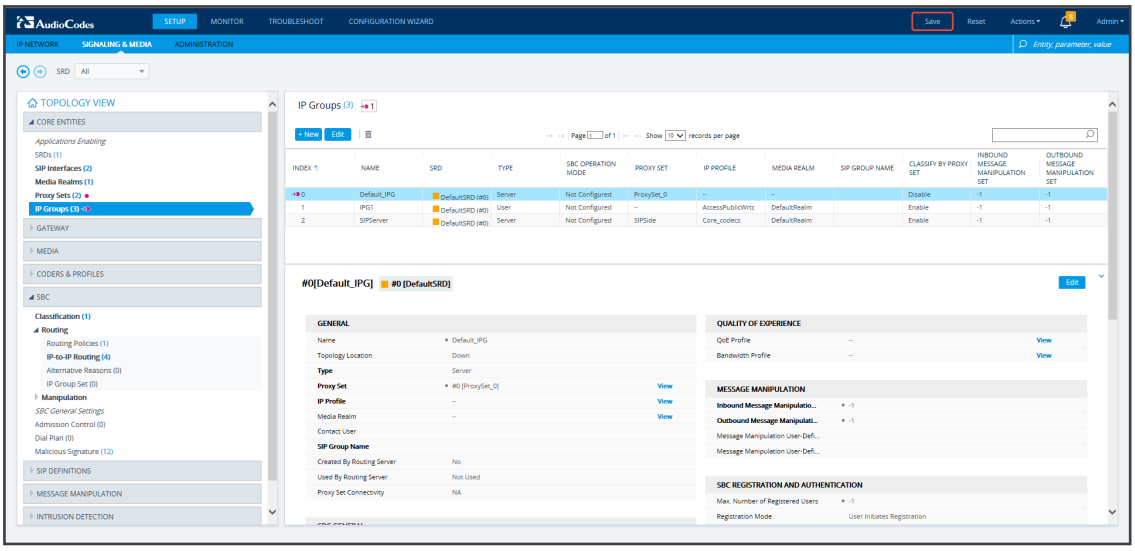
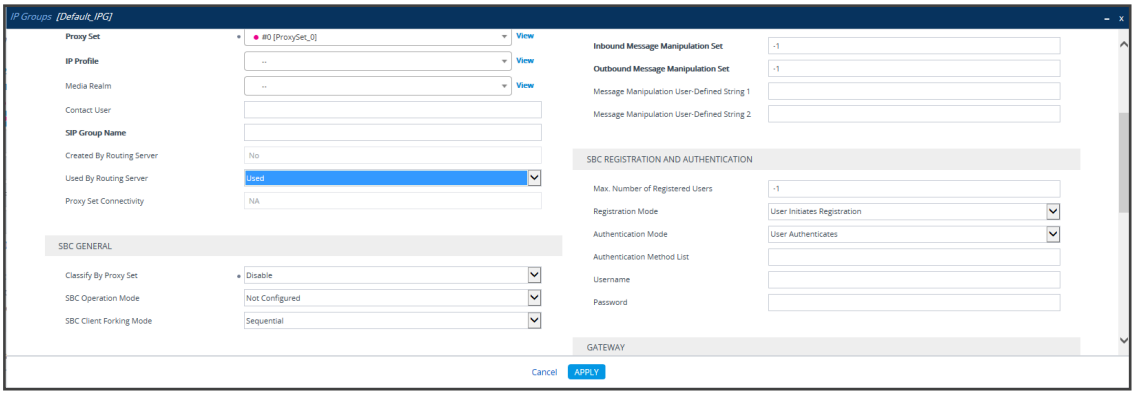


Figure 11-9: Web Interface – IP Groups - Configuring an IP Group



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 44).

> 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 11-10: Web Interface – IP-to-IP Routing

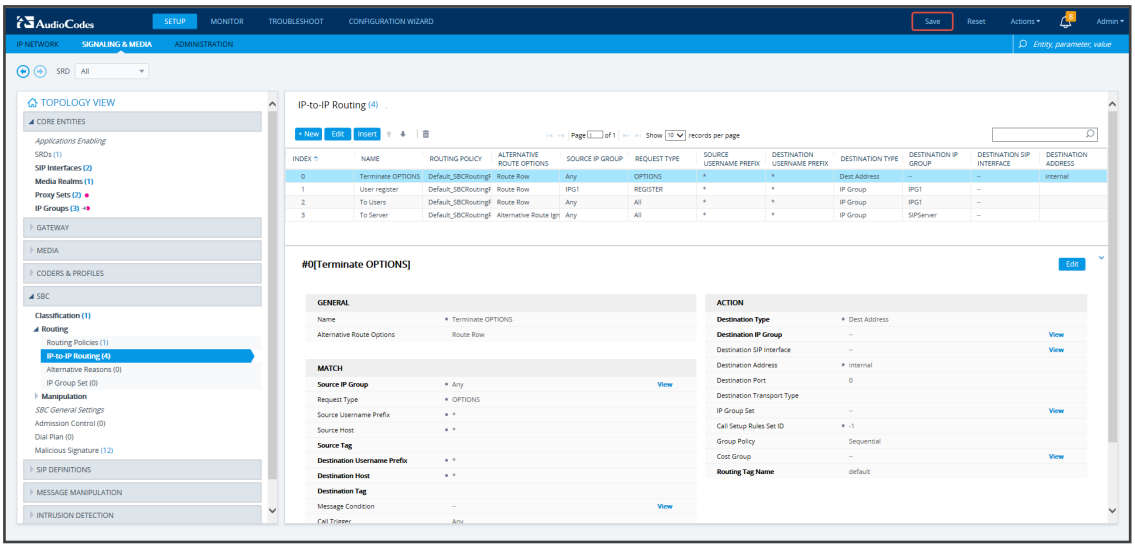
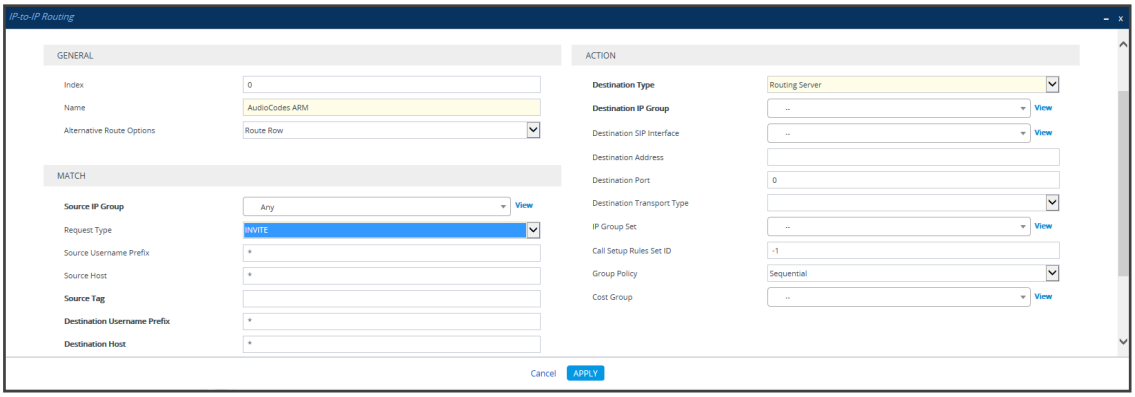


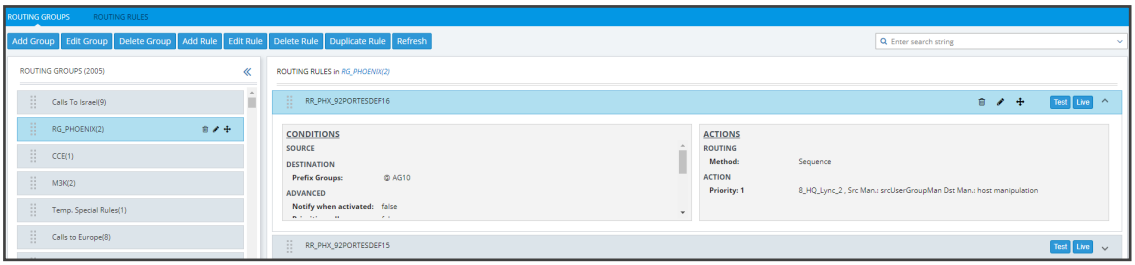
Figure 11-11: Web Interface – IP-to-IP Routing Table – Add Row – Rule tab



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 416 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 325).

Figure 11-12: Configuring a Routing Rule in the ARM



12. In the ARM GUI, switch **Live** the routing rule; rule is now activated in the ARM.
13. In the Web interface, delete the routing rule. The transition is now complete.
14. Perform a Test Route (see Testing a Route on page 352 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 395.

Migrating Media Gateway Routing to the ARM

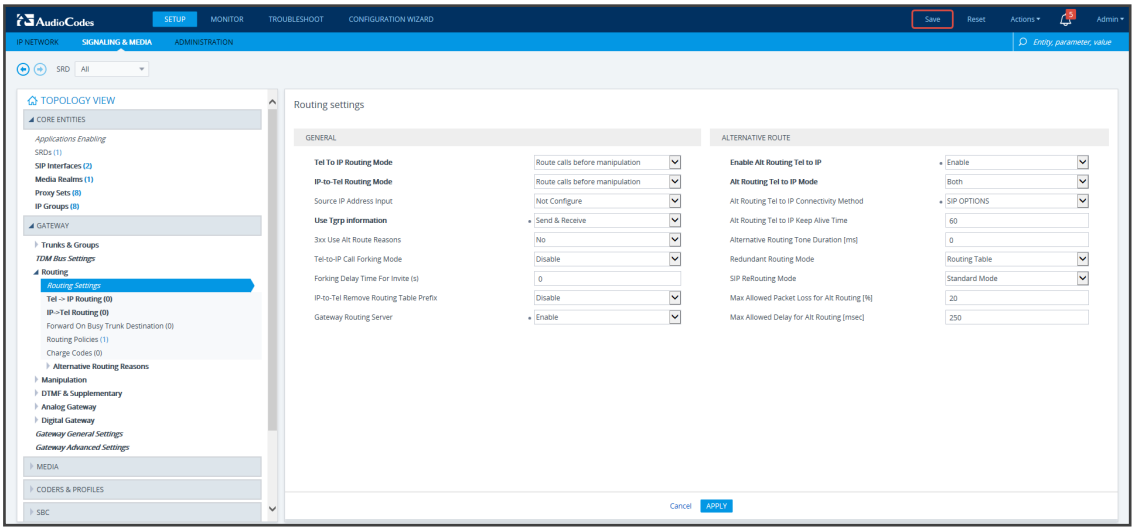
After making sure that the device (the gateway in this case) is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing rules from those defined in the Web interface to the ARM. Screenshots are for illustrative purposes.

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

➢ To migrate gateway routing rules to the ARM:

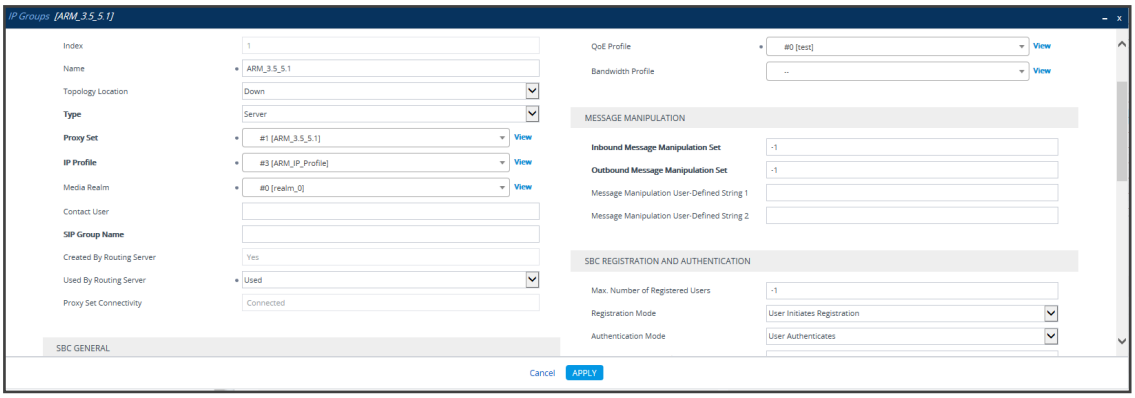
1. In the Web interface, navigate to the Routing Settings page, and set the parameter 'Gateway Routing Server' to **Enable**.

Figure 11-13: Web Interface - Routing Settings Page



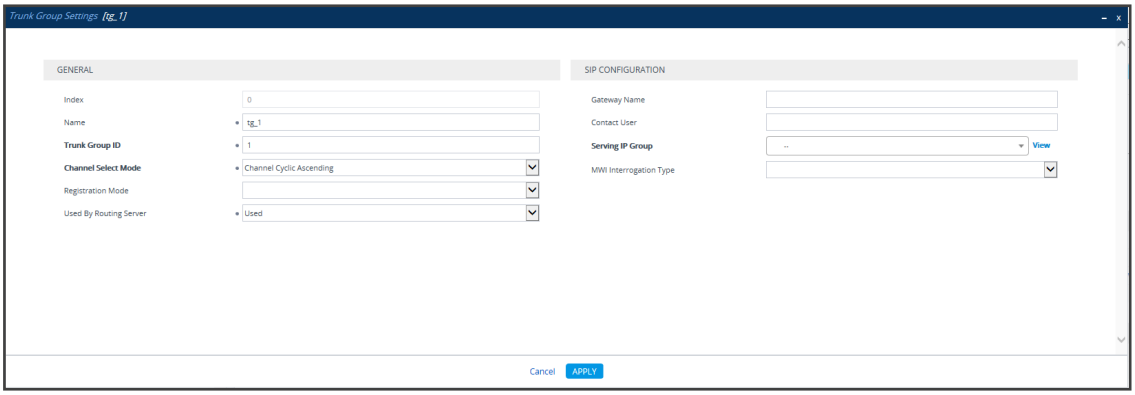
2. Navigate in the Web interface to the IP Groups page.
3. Locate the IP Group to expose the enterprise network to the ARM environment.
4. [Mandatory] Enter a unique name for the IP Group as shown in the following figure.
5. Set the 'Used by Routing Server' parameter to **Used** as shown in the following figure, and then click **Apply**.

Figure 11-14: 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 11-15: 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.

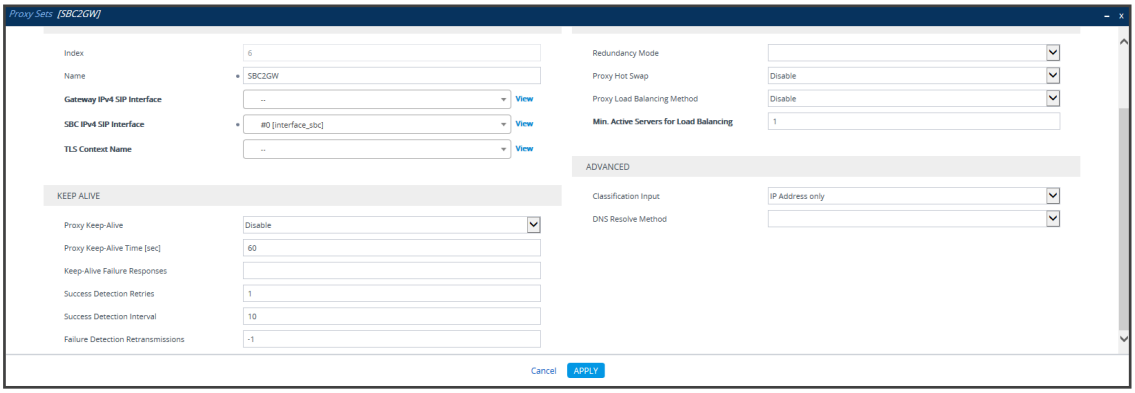
Migrating Hybrid Routing to the ARM

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:

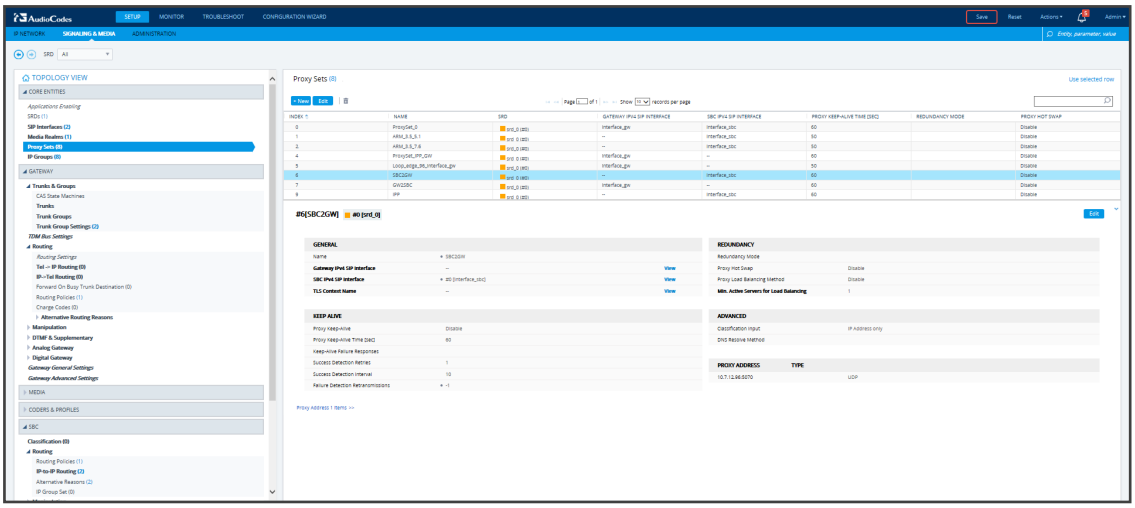
1. Perform migration of the SBC per the instructions in Migrating SBC Routing to the ARM on page 385.
2. Perform migration of the Media Gateway per the instructions in Migrating Media Gateway Routing to the ARM on page 389.
3. Open the hybrid device's Web interface.
4. Create an IP Group (Peer Connection) 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 11-16: Add Proxy Set – for SBC



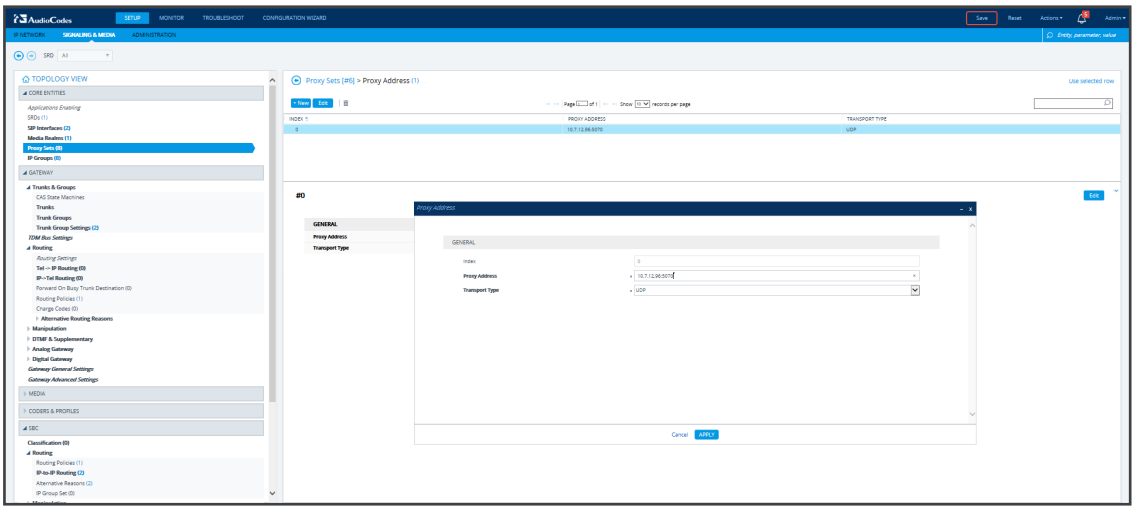
   b. From the 'SBC IPv4 SIP Interface' drop-down menu, select **SBC SIP Interface** and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

Figure 11-17: 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.

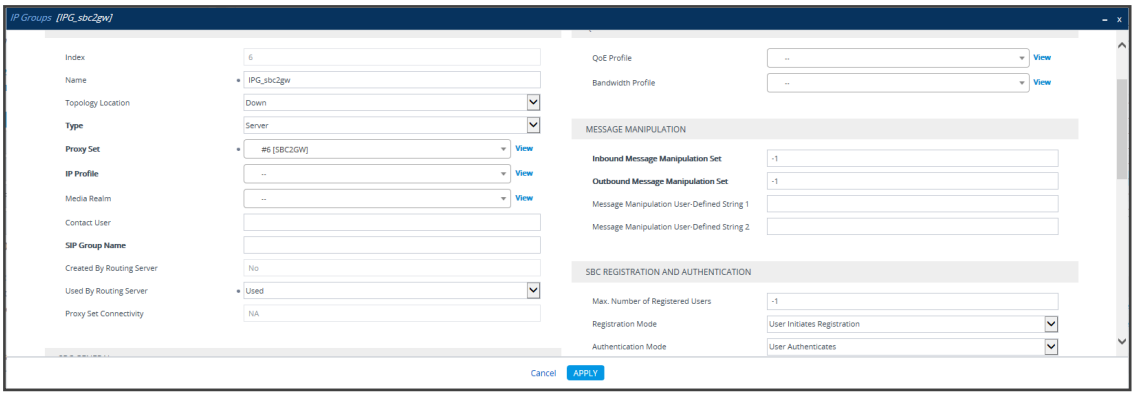
Figure 11-18: Add New Proxy Address



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.

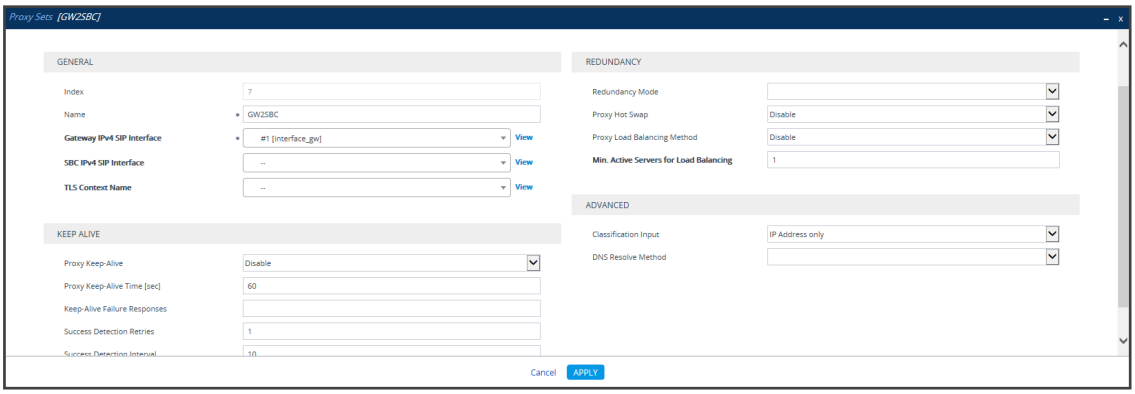
Figure 11-19: IP Group for the SBC Application



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

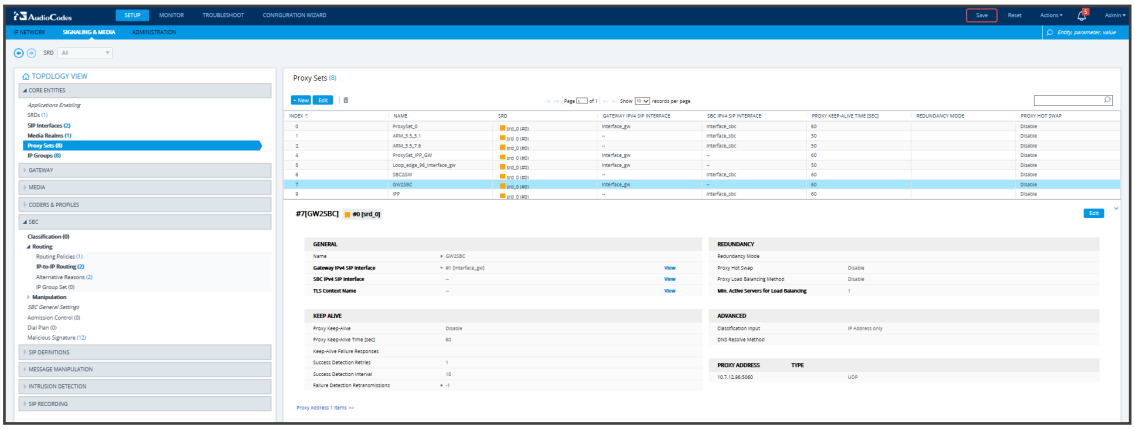
   a. Open the Proxy Sets page (**Setup** > **Signaling & Media** > **Core Entities** > **Proxy Sets**) and then add a Proxy Set (click **New**) for the Media Gateway application:

Figure 11-20: New Proxy Set for Media Gateway Application



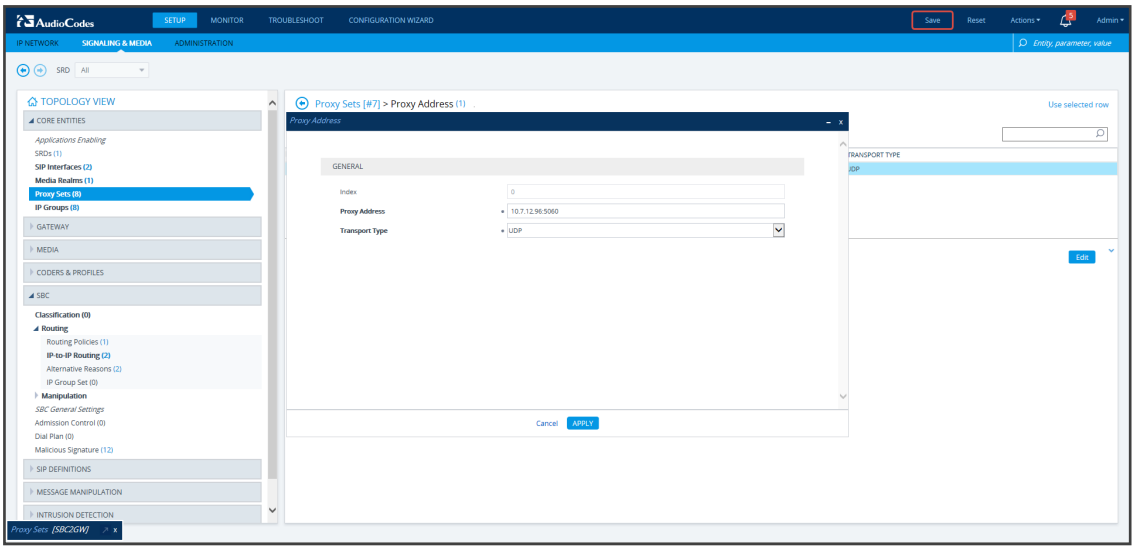
   b. Select **Gateway SIP Interface** from the 'Gateway IPv4 SIP Interface' drop-down menu and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

Figure 11-21: 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.

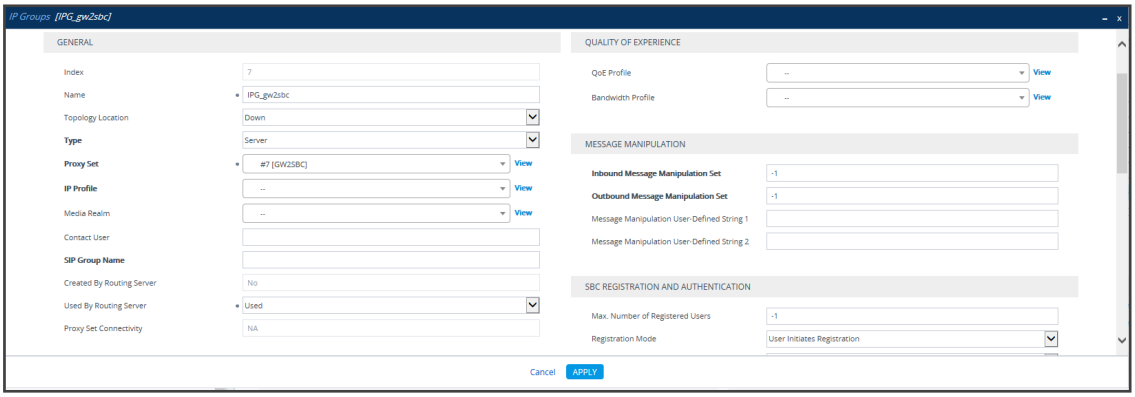
Figure 11-22: Add New Proxy Address



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 11-23: IP Group for the SBC Application



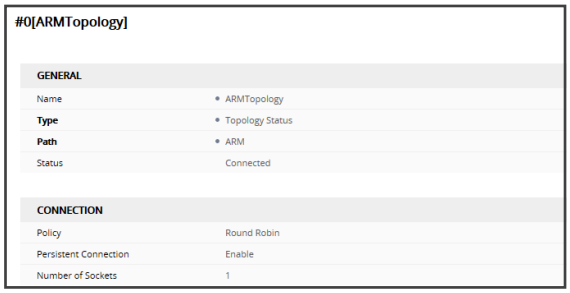
8. Click **Apply**. Check in the ARM that calls can be routed to and from the hybrid device.

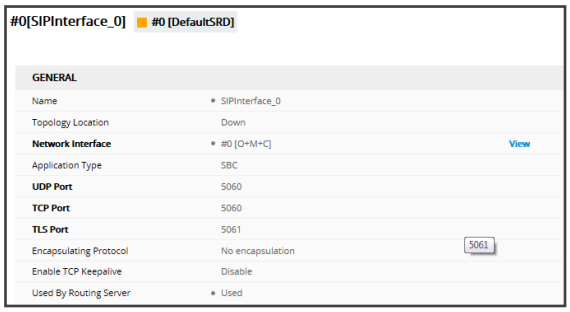
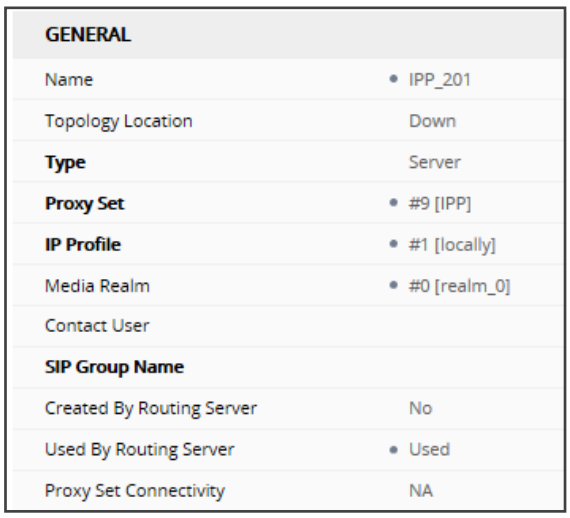
12 Checklist for Migrating SBC Routing to the ARM

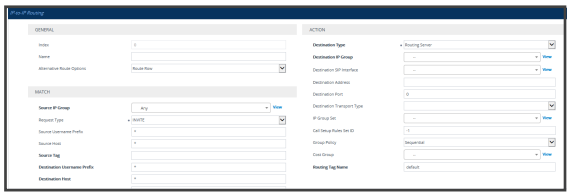
Administrators can use the checklist shown in the following table when migrating SBC routing to the ARM. Tick off the items in the list as you proceed.

> 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  ■ 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'.	You're able to select the chosen SIP Interfaces as ARM 'Routing Interfaces' for ARM

Item	SBC-Level	What should be viewed in the ARM
	■ Open the SBC Web interface (**Setup** > **Signaling & Media** > **Core Entities** > **SIP Interfaces**) 	Connections between the Nodes (SBCs)
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

Item	SBC-Level	What should be viewed in the ARM
		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**). ■ 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. 	Calls are now routed by the ARM: ■ SBC gets an INVITE ■ Sends routing Request to ARM ■ Get reply from ARM ■ 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.

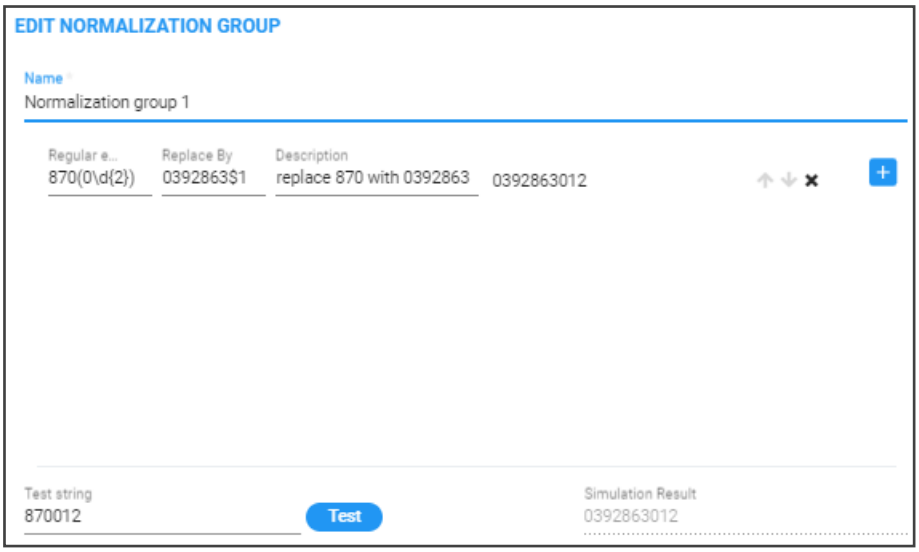
Table 13-1: Prefixes

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	

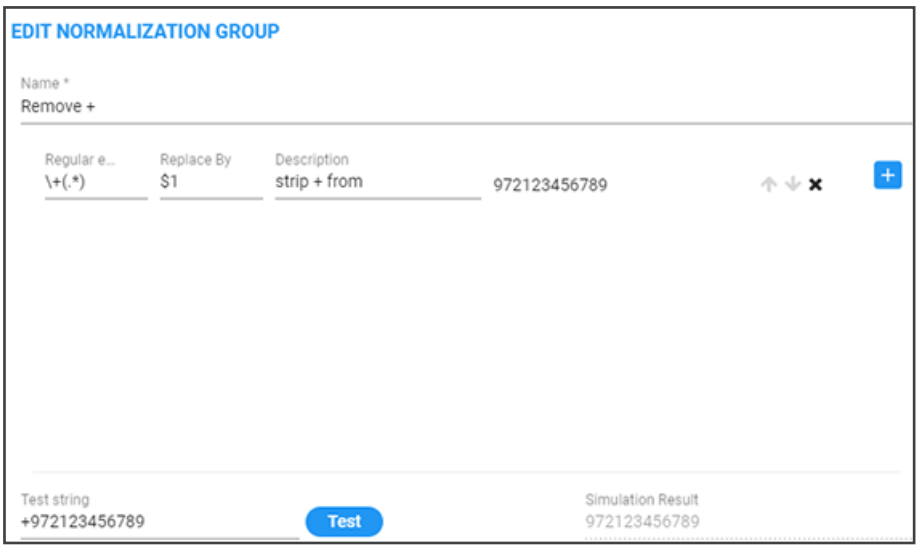
14 Examples of Normalization Rules

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

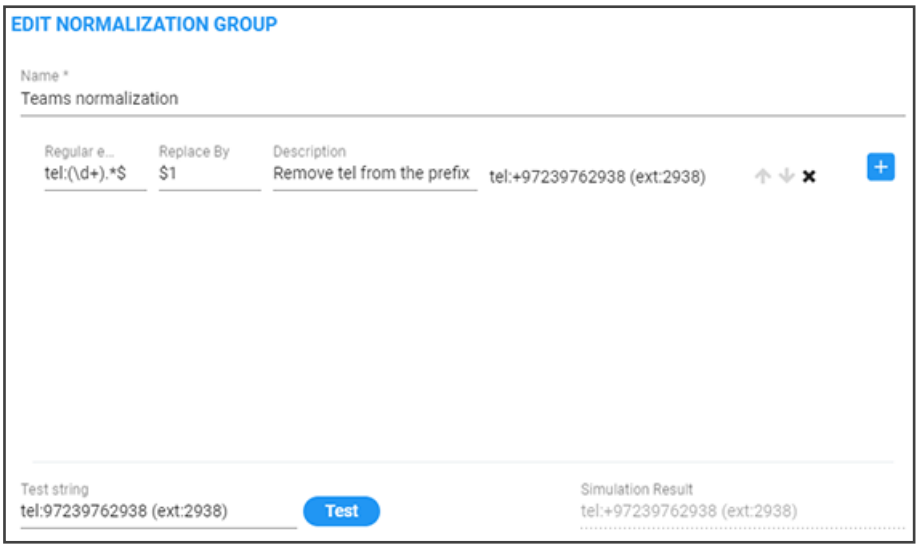
- Remove any non-number text from the prefix of the number:



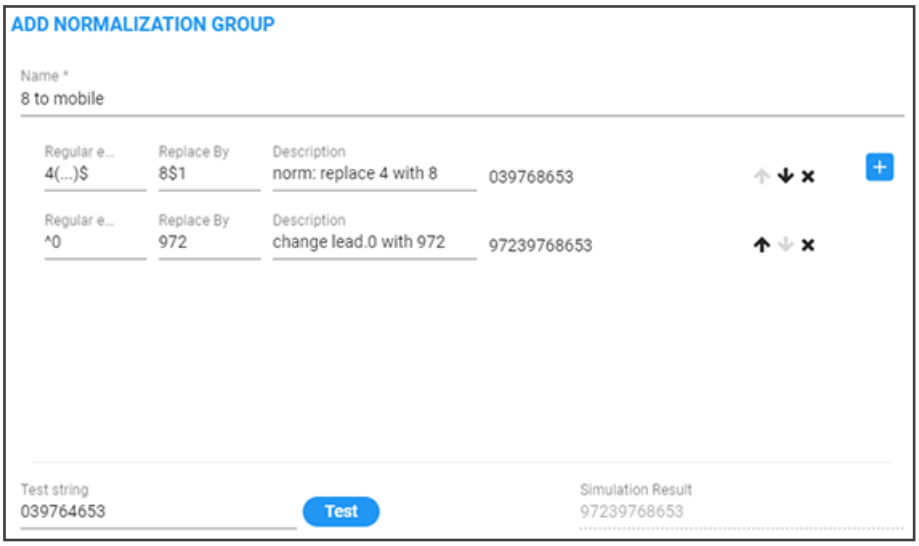
- Strip the **+** from the number.



- Teams: 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**.



15 SIP Condition and SIP Manipulation Syntax

This appendix describes the syntax to be used to define:

- SIP Condition (go to SIP Condition Syntax)
- SIP Manipulation (go to SIP Manipulation Syntax on page 408)

SIP Condition Syntax

This appendix describes the syntax to be used to define a SIP Condition. SIP Condition Rule parts are:

- Subject
- Operator
- Values
- Description

Subject

Syntax

<Header>/<Tags>/<Source URI>/<Dest URI>/<Http>/<regexGroupFromCondition>

The Condition is used to test specific parts of a SIP header / Tags / Source URI /Dest URI/<Http>/<regexGroupFromCondition>.

The string is case-insensitive.

Header

Syntax:

header.<header-name>.<attribute>

Where:

- <header-name> specifies the header name as it arrives in the message. For example: From, To, etc.
- <attribute> specifies a specific part of the message. For example: url.user, url.host, etc.

The Header can be one of the following:

- Header.From
- Header.From.URL.User
- Header.From.URL.Host
- Header.From.Name
- Header.To

- Header.To.URL.User
- Header.To.URL.Host
- Header.To.Name
- Header.P-Asserted-Identity
- Header.P-Asserted-Identity.URL.User
- Header.P-Asserted-Identity.URL.Host
- Header.P-Asserted-Identity.Name
- Header.P-Asserted-Identity.TelNumber
- Header.P-Preferred-Identity
- Header.P-Preferred-Identity.URL.User
- Header.P-Preferred-Identity.URL.Host
- Header.P-Preferred-Identity.Name
- Header.Diversion
- Header.Diversion.URL.User
- Header.Diversion.URL.Host
- Header.Diversion.Name
- Header.Referred-By
- Header.Referred-By.URL.User
- Header.Referred-By.URL.Host
- Header.Referred-By.Name
- Header.Refer-To
- Header.Refer-To.URL.User
- Header.Refer-To.URL.Host
- Header.Refer-To.Name
- Header.History-Info
- Header.Request-URI
- Header.Request-URI.URL.User
- Header.Request-URI.URL.Host

For other headers, the syntax is header.<header-name>

For example: header.my-header

Tags

Syntax:

Tags.TAG_<index>

Where:

Index values are: 1,2,3.

For example: Tags.TAG_1

Source URI

Syntax:

SourceUri .User/Host

For example: SourceUri .Host

Dest URI

Syntax:

DestUri.User/Host

For example: DestUri.User

Http

Syntax: Http.<request/response>.<attribute>

Where:

- <request/response> specifies whether it is the request or response.
- <attribute> specifies a specific part of the request/response.

  These are the available options:

  - Http.Response.Status
  - Http.Response.Body
  - Http.Response.Body.FieldName
  - Http.Request.otherHeader

regexGroupFromCondition

Syntax: regexGroupFromCondition[$1-$6]#

Where:

- [$1-$6] Specifies which group to take from the last regex operation.

Operator

The following table describes the condition operators.

Condition Operand	Description
==	Tests for equivalent values.
!=	Tests for not equivalent values.
>=	Tests for greater than or equal to values.
<=	Tests for less than or equal to values.
>	Tests for greater than values.
<	Tests for less than values.
Contains	Tests a string containing specified text.
Doesn’t contain	Tests a string not containing specified text.
suffix	Tests whether a string has a particular suffix.
prefix	Tests whether a string has a particular prefix.
len >	Tests whether the length of a string is greater than a specific value.
len <	Tests whether the length of a string is less than a specific value.
len ==	Tests whether the length of a string is equal to a specific value.
regex	Tests whether a string matches the given regular expression.
Exists	Tests whether a parameter exists.
Doesn’t exist	Tests whether a parameter does not exist.
Prefix Group	Tests whether a parameter belongs to a specific prefix group.

Values

Syntax

<Value> [+ <Value>]*|

To concatenate values, use the plus “+” operator.

For example, ‘+1’ + header.from.url.user

Value

Syntax

< Subject>/String/prefix group

Where:

String – free string. Must be enclosed by a single quotation mark ('...').

The value should be empty for exist / !exists operators.

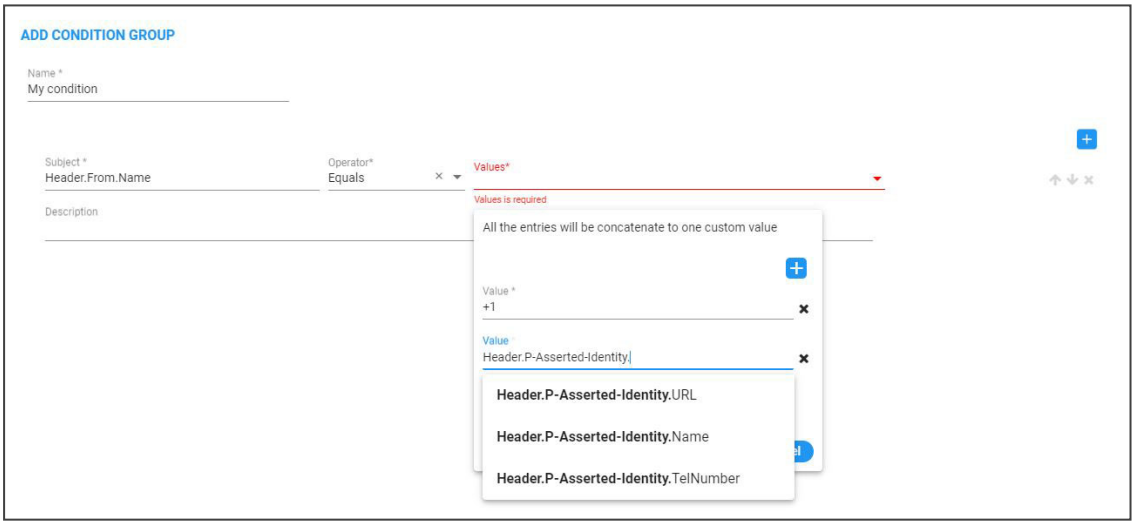
The value should be a single string format for Regex operator.

The value should be a Prefix Group for PrefixGroup operator.

The ARM UI provides an auto completion wizard to configure the SIP Condition.

Figure 15-1: Auto Completion Subject

Figure 15-2: Auto Completion Value



Example 1

The following SIP Condition returns true if the display name of To header is ‘Bob‘ or ‘Alice’:

Figure 15-3: Or Condition

Example 2

The following SIP Condition returns true if the display name of From header is 'Carol', and the display name of To header is 'Bob' or 'Alice':

Figure 15-4: And Operator Condition

Example 3

The following SIP Condition returns true if the P-Asserted-Identity header contains the concatenation of:

- User part of From header
- @
- Host part of From header

Figure 15-5: Concatenation Strings

Example 4

The following SIP Condition returns true if the 'X-My-Header' header exists:

Figure 15-6: Other Header

Example 5

The following Sip Condition does the following things:

- In the first rule, a regex is performed on the body of the HTTP Response (possible if this Condition-Group is called from a Manipulation-Group)

- In the second rule, a test is made on the first group found in the last regex (if found)

SIP Manipulation Syntax

This appendix describes the syntax to be used to define a SIP Condition. SIP Manipulation Rule parts are:

- SIP Condition group
- Action Subject - as described at Subject
- Action Type
- Action Value
- Description

If the chosen action is 'Send By Web-Service' and web-service is also selected, a new line will open that will include the following fields:

- Request Method
- Content-Type
- URL Suffix
- Body

Action Type

The 'Action Type' field specifies the type of action you want to perform on the Action Subject by the Action Value. The following table describes the manipulation actions.

Action Type	Description
Add	Add a new Action Subject with the Action Value

Action Type	Description
Remove	Deletes the Action Subject
Modify	Sets the Action Subject to Action Value
Add Prefix	Adds the Action Value to the beginning of the Action Subject
Add Suffix	Adds the Action Value to the end of the Action Subject
Remove Prefix	Remove Action Value from the beginning of the Action Subject
Remove Suffix	Remove Action Value from the end of the Action Subject
Normalization	Run Normalization group (Action Value) on the Action Subject
Random From Pool	■ Replace the Action Subject with number from the Prefix Group (Action Value). ■ The Prefix Group type should be 'Pool Of Numbers'. ■ The Action Subject suffix should be 'User'.
Send By Web-Service	Sends the configured HTTP Request via the selected Custom Web-Service.

Action Value

Syntax

<Value>/Normalization group/Prefix Group/Custom Web-Service

Where:

Value - as described at Value.

The value should be empty for 'Remove' action.

The value should be a Normalization group for 'Normalization' action.

The value should be a Prefix Group for 'Random From Pool' action.

The value should be a 'Custom' Web-Service for 'Send By Web-Service' action.

The following table describes the possible manipulation actions per subject.

Action Subject	Action Type
Header.From	Modify, Normalization
Header.From.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, RemoveS uffix, Normalization, Random From Pool

Action Subject	Action Type
Header.From.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.From.Name	Add, remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.To	
Header.To.URL.User	
Http.Request.otherHeader	Add, Remove, Modify
Header.To.URL.Host	
Header.To.Name	
Header.P-Asserted-Identity	Add, Remove, Modify, Normalization
Header.P-Asserted-Identity.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
Header.P-Asserted-Identity.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.P-Asserted-Identity.Name	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.P-Asserted-Identity.TelNumber	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.P-Preferred-Identity	Add, Remove, Modify, Normalization
Header.P-Preferred-Identity.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
Header.P-Preferred-Identity.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.P-Preferred-Identity.Name	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.Diversion	Add, Remove, Modify, Normalization
Header.Diversion.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
Header.Diversion.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove

Action Subject	Action Type
	Suffix, Normalization
Header.Diversion.Name	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.Referred-By	Add, Remove, Modify, Normalization
Header.Referred-By.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
Header.Referred-By.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.Referred-By.Name	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.Refer-To	Add, Remove, Modify, Normalization
Header.Refer-To.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
Header.Refer-To.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.Refer-To.Name	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.History-Info	Add, Remove, Modify, Normalization
Header.Request-URI	Modify, Normalization
Header.Request-URI.URL.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
Header.Request-URI.URL.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Header.otherHeader	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Tags.TAG_1	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
Tags.TAG_2	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization

Action Subject	Action Type
Tags.TAG_3	Add, Remove, Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
SourceUri.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
SourceUri.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization
DestUri.User	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization, Random From Pool
DestUri.Host	Modify, Add Prefix, Add Suffix, Remove Prefix, Remove Suffix, Normalization

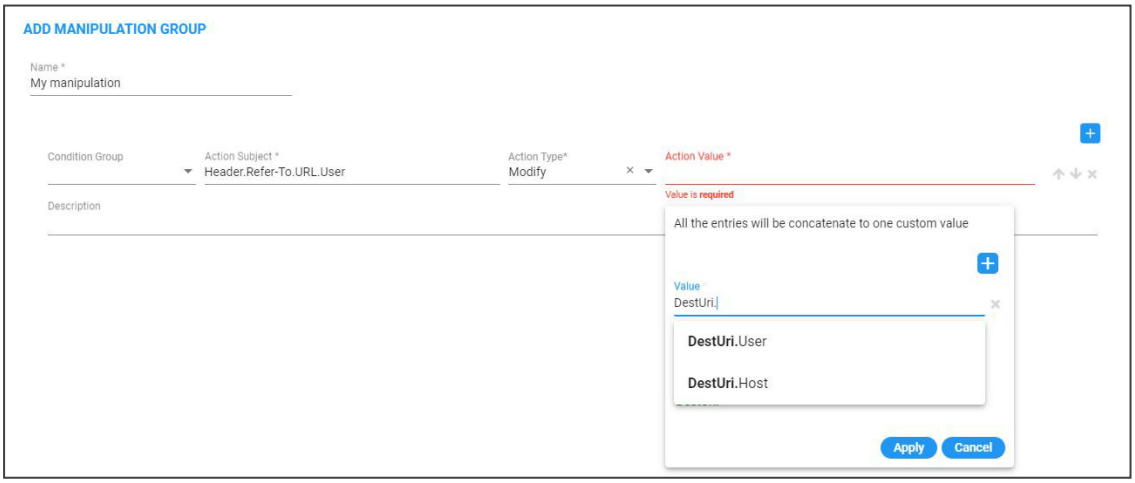
The following headers cannot be changed:

- Via
- Call-ID
- CSeq
- Contact

For example, the action Modify action is not valid for "Header.Contact" subject.

The ARM GUI provides an auto completion wizard to configure the SIP Manipulation.

Figure 15-7: Auto Completion Manipulation



Example 1

The following SIP Manipulation Adds ‘1212’ as prefix to the Tel Number of P-Asserted-Identity header:

Figure 15-8: Tel Number

Example 2

The following SIP Manipulation runs a SIP Condition before manipulating the Dest URI User.

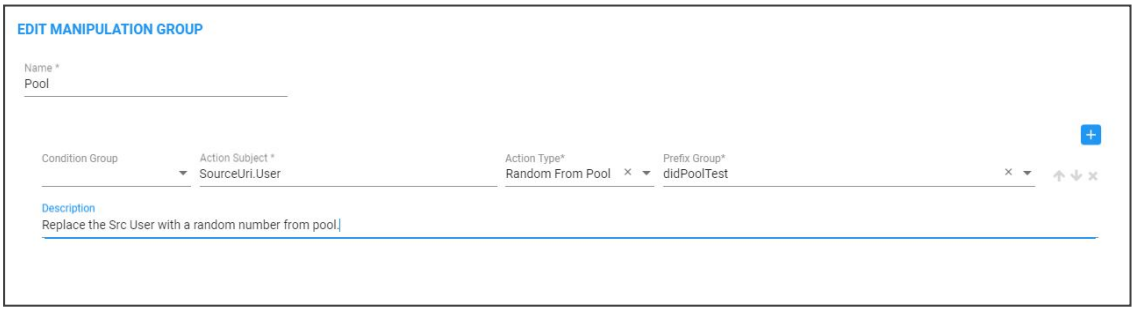
If Tag1 exists, its value will be stored in the Dest URI User.

Figure 15-9: Run Tag Condition Before Manipulation

Example 3

The following SIP Manipulation replaces the Source URI User with a random number from a Prefix Group (pool of numbers).

Figure 15-10: Pool

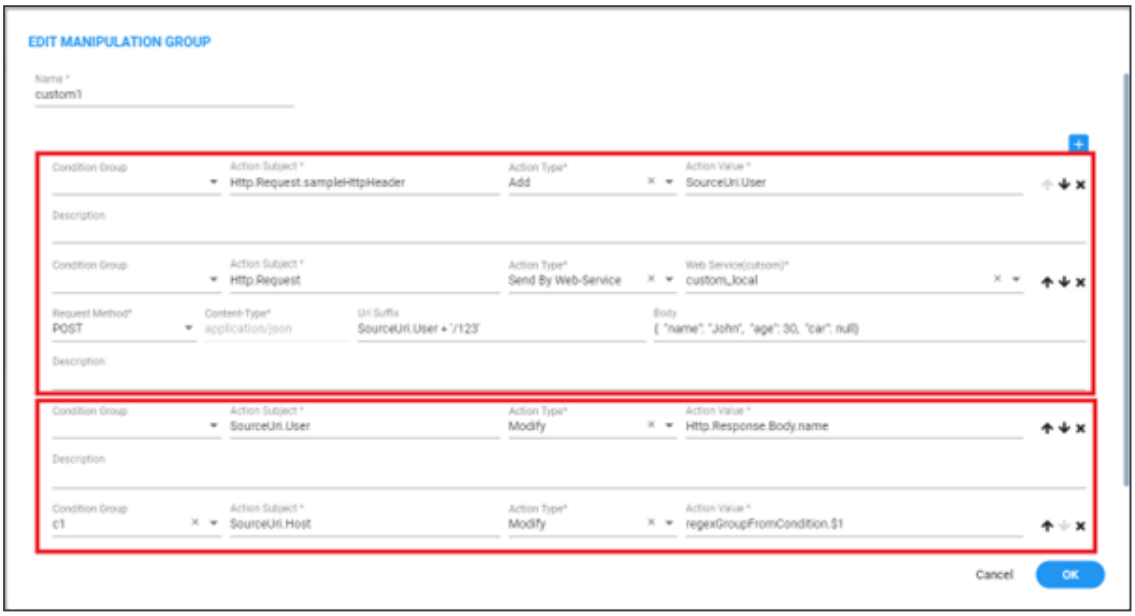


Example 4

The SIP Manipulation Group shown in the figure below:

- Prepares and sends the HTTP Request (uppermost section indicated in the figure below)
  - Sends HTTP request with the 'sampleHttpHeader' taking SourceUri.User as the value of this header.
  - Using 'custom_local' web service it sends a POST request, with the suffix and body shown in the figure below.
- Uses the HTTP response (lowermost section indicated in the figure below)

- If there is a 'name' field in the response body (first-level JSON searching is currently supported), its value will be inserted to 'SourceUri.User'
- Using the regex executed in the condition 'c1', if there was a match, take the first group and put it inside 'SourceUri.Host'



16 Call Routing

The following describes call routing:

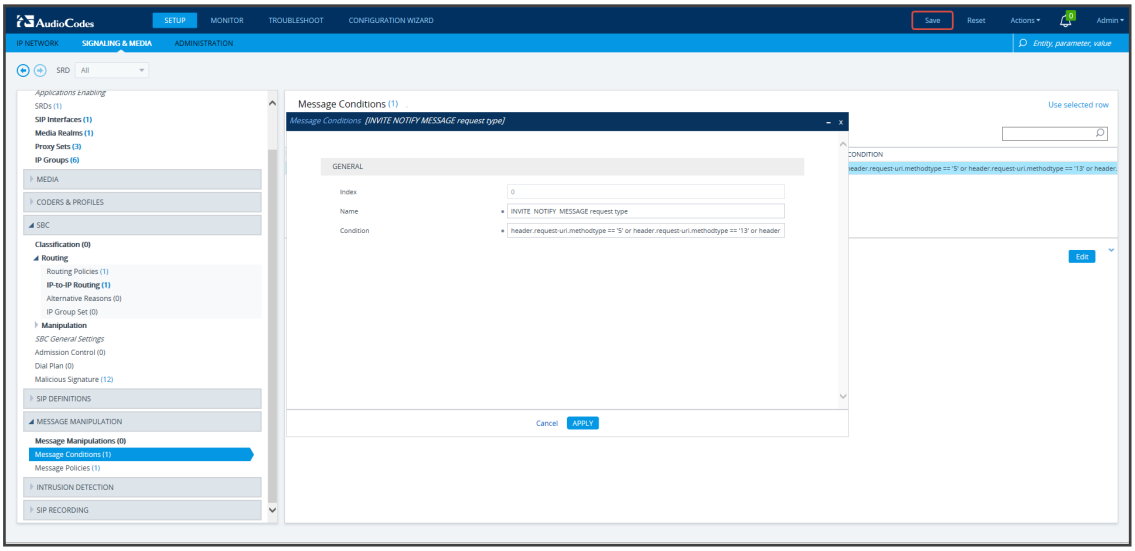
- A routing request results in an HTTP error response if no routing is available.
- A routing request from a source node which has an alternate route option returns the next alternate route option. The call route is not recalculated. If the alternate route list is empty, a 404 result is returned.
- A 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.

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

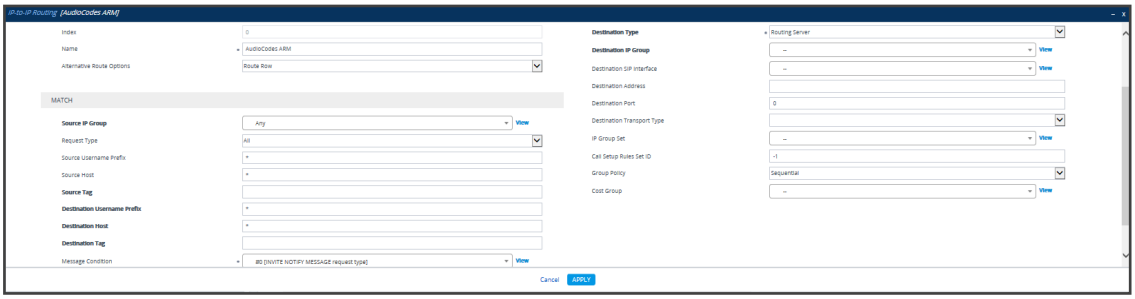
The SBC can be configured to send MESSAGE and NOTIFY SIP requests to the ARM. To get not only INVITE but also NOTIFY and MESSAGE, create a new Condition in the Condition table with the value: "header.request-uri.methodtype == '5' or header.request-uri.methodtype == '13' or header.request-uri.methodtype == '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**.



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**.



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.

18 Opening Firewall Ports for the ARM

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

Table 18-1: Opening Firewall Ports for the ARM

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
ARM and Devices (SBCs / Gateways / Hybrid nodes)					
Device ↔ ARM Configurator (REST)	TCP (HTTPS) - default	✓	443	Topology Auto-discovery, Topology Status update, Quality information, long call sessions information (for licensing)	Bi-Directional
	TCP (HTTP) – debug only	×	80	Topology Auto-discovery, Topology Status update, Quality information, long calls session information (for licensing)	Bi-directional
Device ↔ ARM Router (REST)	TCP (HTTPS) - default	✓	443	Routing requests and calls status	Bi-Directional
	TCP (HTTP) – debug only	×	80	Routing requests and calls status	Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
ARM and LDAP Active Directory Server					
ARM Configurator ↔ Active Directory LDAP server	TCP (LDAP)	×	389 (Default, can be configured at ARM)	Getting of ARM AD users and updating ARM user database	Bi-directional
	TCP (TLS - LDAPS)	✓	636 3268 for 'Global catalog' Default, can be configured at ARM)	Getting of ARM AD users and updating ARM user database LDAPS (TLS) is configured at ARM	Bi-directional
ARM GUI and North bound Interface					
UI (REST communication) → ARM Configurator	TCP (HTTPS)	✓	443	ARM component status updates, GUI, Provisioning, Alarms indications	Incoming (from ARM Configurator perspective)
Third-party application (via official REST API) → ARM Configurator	TCP (HTTPS)	✓	443	ARM component status updates, GUI, Provisioning, Alarms indications	Incoming (from ARM Configurator perspective)
ARM Configurator → SNMP Target	UDP (SNMP)	×	161, 162 or configurable	ARM generates SNMP traps/alarms toward predefined	Outgoing

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				SNMP Target.	
ARM Management / Maintenance Interfaces					
ARM Configurator ↔ NTP Server	UDP (NTP server)	×	123	ARM Configurator acts as NTP client toward external (pre-configured) NTP server. It also acts as NTP Server toward ARM Routers.	Bi-directional
ARM Router → NTP Server (ARM Configurator)	UDP (NTP)	×	123	ARM Router acts as NTP client	Outgoing
ARM Configurator ↔ Client PC (SSH)	TCP	✓	22	SSH communication between ARM Configurator and external PC initiated by client PC: For ARM maintenance	Bi-directional
ARM Router ↔ Client PC (SSH)	TCP	✓	22	SSH communication between ARM Router and external PC initiated by client PC: For ARM maintenance	Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
ARM Configurator → Syslog server	TCP	×	514 (by default) or configurable	ARM Configurator logs can be forwarded to external syslog server.	Outgoing
ARM Router → Syslog server	TCP	×	514 (by default) or configurable	ARM Routers logs can be forwarded to external syslog server.	Outgoing
ARM Inter-Components Communication (Configurator ↔ Routers)					
ARM Configurator ↔ ARM Routers	TCP (HTTPS)	✓	443	Getting call statistics from the ARM Configurator; getting call sessions information for ARM licensing	Bi-directional
	TCP (HTTP) - debug only	×	80	Getting call statistics from the ARM Configurator; getting call sessions information for ARM licensing	Bi-directional
ARM Configurator ← JMS Broker	TCP (TLS)	✓	8080	Informing ARM Routers about topology changes (including	Incoming

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				topology status and quality changes)	
ARM Router → JMS Broker	TCP (TLS)	✓	8080	Getting Topology updates from ARM	Outgoing
ARM Configurator ← Redis from Router	TCP (TLS)	✓	6379 (Router uses same 80 and 443)	Needed only if DID Masking or Dynamic Blacklist is used	Bi-directional
ARM Configurator → ARM Router (SSH)	TCP	✓	22	SSH communication between ARM Configurator and ARM Router	Outgoing

19 About CDRs Sent by ARM to CDR Server

ARM Routers send CDRs (Call Detail Records) to a CDR Server. CDR messages contain information about all calls routed by the ARM, for example, source and destination users, call duration and call path. CDR messages also provide billing details. CDRs are sent as syslog packets to a predefined IP address configured by the operator. CDR syslog messages comply with RFC 3164 and are identified by Facility 17 (local1) and Severity 6 (Informational). CDR messages are built using getRoute and CallStatus_callEnd messages, by the first node in the paths. CDR types are CALL_START and CALL_END.

Calls from an SBC node:

1. One CALL_START message is sent per route (path)
2. Two CALL_END messages are sent at the end of the call

Calls from a gateway node:

1. One CALL_START message is sent per route (path)
2. One CALL_END message is sent at the end of the call (not per route)

SessionId is identical for all CDR messages related to the same call.

The **routeSeq:**

1. Represents the route (path) the ARM attempts
2. The count starts from 0
3. For example, for an SBC call, when there are three paths to attempt, the ARM sends:
   a. First route (path): One CALL_START message and one CALL_END (outgoing leg) message. routeSeq = 0.
   b. Second route (path): One CALL_START message and one CALL_END (outgoing leg) message. routeSeq = 1.
   c. Third route (path): One CALL_START and two CALL_END (incoming and outgoing legs) messages. routeSeq = 2.

The following table describes all CDR fields.

Table 19-1: CDR Field Descriptions

CDR Field	Description	CDR Report Type	Format
RouterIp	IP address of the Router that sends the CDR.	All	String (15)
Seq	Each router sends its own sequence CDR 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.	-	String (13)

CDR Field	Description	CDR Report Type	Format
	■ "CALL_END": CDR is sent upon a CALL_ STATUS_END_CALL message from the node.		
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)
lastNodeName	Name of the last node	"CALL_START"	String (25)
lastPconId	ID of the last Peer Connection	"CALL_START"	String (10)
lastPconName	Name of the last Peer Connection	"CALL_START"	String (35)
srcUri	Source URI as actually sent (after manipulation).	All	String (50)
srcUriBeforeMap	Source before manipulation.	"CALL_START"	String (50)
from	From URI as actually sent (after manipulation).	"CALL_START"	String (50)

CDR Field	Description	CDR Report Type	Format
fromBeforeMap	From URI before manipulation.	"CALL_START"	String (50)
pai	P-Asserted-Identity URI as actually sent (after manipulation).	"CALL_START"	String (50)
paiBeforeMap	P-Asserted-Identity URI before manipulation.	"CALL_START"	String (50)
ppi	P-Preferred-Identity URI as actually sent (after manipulation).	"CALL_START"	String (50)
ppiBeforeMap	P-Preferred-Identity URI before manipulation.	"CALL_START"	String (50)
dstUri	Destination URI as actually sent (after manipulation).	All	String (50)
dstUriBeforeMap	Destination before manipulation.	"CALL_START"	String (50)
armSetupTime	ARM Router time when sending CALL_START.	"CALL_START"	String (30)
armReleaseTime	ARM Router time when sending CALL_END.	"CALL_END"	String (30)
sbcSetupTime	Gateway / SBC time when start handling Invite message.	"CALL_END"	String (40)
sbcConnectTime	Gateway / SBC time when 200 OK response (i.e., call is established)	"CALL_END"	String (40)
sbcReleaseTime	Gateway / SBC time when a BYE message (i.e., call ends)	"CALL_END"	String (40)
sbcAlertTime	Gateway / SBC time when start ringing	"CALL_END"	String (40)
alertDuration	Time of ringing in milliseconds (should be configured in the SBC /gateway to send in milliseconds)	"CALL_END"	String (13)
voiceDuration	Time of voice streamed in milliseconds (should be configured in the SBC /Gateway to send in milliseconds)	"CALL_END"	String (13)
completeDuration	Time of the whole call in milliseconds (from the first incoming Invite until ending the call)	"CALL_END"	String (16)
sipTerminationReason	SIP termination reason	"CALL_END"	String (20)
sipTerminationReasonDesc	SIP termination reason – more detailed	"CALL_END"	String (35)
routeSeq	Each route (path) of a call has a number. Starting from 0.	"CALL_START"	String (8)
sipInterface	sipInterface ID of the Connection or Peer Connection in the SBC / Gateway	"CALL_START"	String (20)
legId	Leg id of the SBC / Gateway	"CALL_END"	String (11)
routingRuleId	The Routing Rule ID of the match rule	"CALL_START"	String (13)
routingRuleName	The Routing Rule name of the match rule	"CALL_START"	String (30)
discardingByRoutingRule	The Routing Rule ID in case of discarding rule	"CALL_START"	String (24)

CDR Field	Description	CDR Report Type	Format
continueWithNodeInternalTablesByRoutingRule	Stop ARM routing and continue with node's internal routing	"CALL_ START"	String (44)
fork	Is a fork call	"CALL_ START"	String (5)
Path	String – describes the path.	"CALL_START"	String (200)

Two CDR format options are available:

- Clear text (separating each value with "|")
- As JSON

Here's an example of an ARM signaling CDR as *clear text*, sent at the end of a call (which was terminated normally):

Format:

```
|routerIp|seq|creationDate|cdrReportType|appType|sessionId|callId|direction
|pconOrConName
|nodeId|nodeName|nodeIp|pconId|conId|pconOrConType|sipInterface
|outPconId|outConId|outPconOrConType|lastPconId|lastNodeId|lastNodeName
|lastPconName|srcUri|srcUriBeforeMap|from|fromBeforeMap|pai|paiBeforeMap
|ppi|ppiBeforeMap|dstUri|dstUriBeforeMap|armSetupTime|armReleaseTime
|sbcSetupTime |sbcConnectTime|sbcReleaseTime|sbcAlertTime|alertDuration
|voiceDuration
|completeDuration|sipTerminationReason|sipTerminationReasonDesc|routeSeq
|legId|routingRuleId|routingRuleName|discardingByRoutingRule
|continueWithNodeInternalTablesByRoutingRule |fork |path
```

Value:

```
|10.7.6.102|4|2020-12-06T09:21:23.729Z|CALL_START|SBC|33a4b1cfb37733a5
|1-24960@10.7.20.148|RMT|SIPP|1|SBC_
102|10.7.12.102|70|null|IPGroup|SIPP|null
|1|IPGroup|71|3|Hybrid_96|SIPP |401@10.7.20.148
|123456@10.7.20.148||||||sipp201@10.7.12.102 |sipp201@10.7.12.102 |2020-12-
06T09:21:23.728Z|||||| |0||| |0 |-1 |47 |src_uri |-1|-1|false|IncomingLeg=
[nodeId=1,nodeName=SBC_102,pconId=70,pconOrConnectionName=SIPP],
Outgoing Leg=[nodeId=3,nodeName=Hybrid_
96,pconId=71,pconOrConnectionName=SIPP], Edges=[Edge [connSrcNode=1,
connDestNode=5, connectionId=1], Edge [connSrcNode=5, connDestNode=3,
connectionId=2]]]
```

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

```
jsonCdr={"creationDate":"2020-12-06T09:21:23.729Z","sessionKey":"1_
33a4b1cfb37733a5","routerIp":"10.7.6.102","routerId":10,"seq":4,"cdrReportType":
"CALL_
START","cdrApplicationType":"SBC","sessionId":"33a4b1cfb37733a5","callId":"1-
24960@10.7.20.148","callOrig":"RMT","pconOrConName":"SIPP","nodeId":"1",
"nodeName":"SBC102","nodeIp":"10.7.12.102","pconId":70,"conId":null,
"pconOrConType":"IPGroup","sipInterface":"SIPP","outPconId":null,"outConId":1,
"outPconOrConType":"IPGroup","lastPconId":71,"lastNodeId":3,
"lastNodeName":"Hybrid96","lastPconName":"SIPP","srcUri":"401@10.7.20.148",
"srcUriBeforeMap":"123456@10.7.20.148","from":"","fromBeforeMap":"","pai":"",
"paiBeforeMap":"","ppi":"","ppiBeforeMap":"","dstUri":"sipp201@10.7.12.102",
"dstUriBeforeMap":"sipp201@10.7.12.102","armSetupTime":"2020-12-
```

06T09:21:23.728Z",
"armReleaseTime":"","sbcSetupTime":"","sbcConnectTime":"","sbcReleaseTim
e":"",
"sbcAlertTime":"","alertDuration":"","voiceDuration":"0","completeDuration":"",
"sipTerminationReason":"","sipTerminationReasonDesc":"","routeSeq":0,"legId":-
1,"routingRuleId":47,"routingRuleName":"src_uri","path":"Incoming Leg=
[nodeId=1,nodeName=SBC_102,pconId=70,pconOrConnectionName=SIPP],
Outgoing Leg=[nodeId=3,nodeName=Hybrid_
96,pconId=71,pconOrConnectionName=SIPP], Edges=[Edge [connSrcNode=1,
connDestNode=5, connectionId=1], Edge [connSrcNode=5, connDestNode=3,
connectionId=2]]]","discardingByRoutingRule":-1,
"continueWithNodeInternalTablesByRoutingRule":-
1,"fork":false,"httpResponse":200,"description":""}

20 Supported ARM Configurator and ARM Router Cipher Suites

Listed here are the cipher suites supported by the ARM server (ARM Configurator and ARM Router). The list following this list shows the client-supported cipher suites.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Listed here are the client-supported (when the ARM interfaces SBCs) cipher suites (most of the TLS available ciphers):

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-43002