

AudioCodes Routing Manager (ARM)

Version 8.6

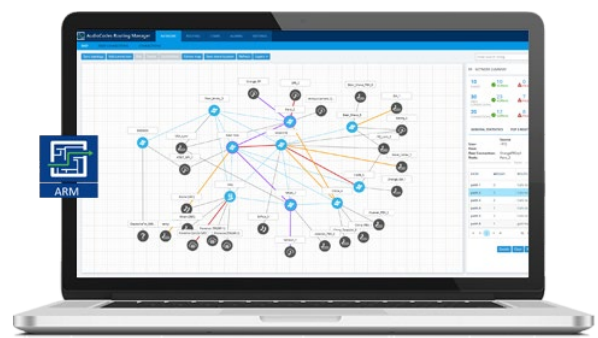


Table of Contents

1	Overview	7
1.1	Managed AudioCodes Devices	7
2	What's New in Version 8.6	9
2.1	Call-Detail Records (CDRs)	9
2.1.1	Calls Information	9
2.1.2	Call Details	11
2.1.3	Disabling Limiting the Number of CDRs	14
2.2	Routing Servers Groups with Internal and External Priorities	15
2.3	Customer Certificates with FQDN / Hostname	19
2.3.1	Using FQDN / Hostname instead of IP Address	19
2.3.1.1	Adding a Node using FQDN / Hostname	19
2.3.1.2	Adding FQDN / Hostname to a Node	20
2.3.1.3	Adding ARM with FQDN	20
2.3.2	Certificates Validation	22
2.3.2.1	Client Side Certificate Verification	22
2.3.2.2	Certificate Subject Name Verification	23
2.4	Calls Forking	24
2.5	Routing Based on any SIP Invite Header Value	25
2.5.1	SBC-Level Configuration	25
2.5.2	ARM-Level Configuration	26
2.6	Authenticating Operator Login using Open LDAP	27
2.7	ARM in the Amazon Web Services Cloud	28
2.8	Improved ARM Tolerance when Upgrading ARM Routers	28
2.9	ARM Machine OS Upgraded with Latest CentOS6.10 Security Patches	28
2.10	New Alarm for ARM Routers Unavailability	29
3	New Machine Requirements for ARM Configurator	31
4	Supported Platforms	33
5	Earliest Node Software Versions Supported by ARM Features	35
6	Known Limitations and Workarounds	37

List of Tables

Table 1-1: AudioCodes Devices Supported by ARM Version 8.6	7
Table 4-1: ARM Version 8.6 Supported Platforms	33
Table 5-1: ARM Features Supported by the Earliest Node Software	35
Table 6-1: Known Limitations and Workarounds	37

Notice

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

This document is subject to change without notice.

Date Published: March-07-2019

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

Related Documentation

Manual Name
ARM Installation Manual
ARM User's Manual
Mediant 9000 SBC User's Manual
Mediant 4000 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

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>.

1 Overview

This document describes the new features and known issues in Version 8.6 of the AudioCodes Routing Manager (ARM).

1.1 Managed AudioCodes Devices

ARM version 8.6 supports the following AudioCodes devices (Gateways and SBCs) referred to in the ARM GUI as *nodes*:

Table 1-1: AudioCodes Devices Supported by ARM Version 8.6

Device	Major Versions
Mediant 9000 SBC	7.2.158 and later
Mediant 4000 SBC	7.2.158 and later
Mediant 2600 SBC	7.2.158 and later
Mediant SE/VE SBC	7.2.158 and later
Mediant 1000B Gateway and E-SBC	7.2.158 and later
Mediant 800B Gateway and E-SBC	7.2.158 and later
Mediant 800C	7.2.158 and later
Mediant 500 E-SBC	7.2.158 and later
Mediant 500 L - SBC	7.2.158 and later
Mediant SBC CE (Cloud Edition)	7.2.250 and later
Mediant 3000 Gateway only	7.00A.129.004 and later



Note:

- Customers are strongly recommended to upgrade their devices to version 7.2.158 or later as issues were encountered with device version releases earlier than 7.2.158.
- See also Section 5 for the earliest device version supported by the ARM, *per ARM feature*.

This page is intentionally left blank.

2 What's New in Version 8.6

This section describes the new features and capabilities introduced in ARM version 8.6.

2.1 Call-Detail Records (CDRs)

ARM version 8.6 features new capability to store calls information and call-detail records (CDRs).

2.1.1 Calls Information

A new Calls List page displays ARM-routed calls information. A new **Calls** tab on the ARM's menu bar lets operators access the Calls List.

Figure 2-1: Calls List

SOURCE	DESTINATION	DATE	INCOMING NODE	INCOMING PCON	OUTGOING NODE	OUTGOING PCON	ROUTING RULE	SIP REASON	SESSION ID
114517@172.17.133.5	b420027938@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	2e05b6b81e0a81b9
115254@172.17.133.5	b4200590@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	1e6876ee7052e57f
122513@172.17.133.5	b42007547@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	6c9329b64a4a9925
127515@172.17.133.5	b72006653@172.17.133.24	24-Feb-19 17:06:08	Texas_7	IpGrp0	Texas_7	IpGrp2	toTexas_7(Asterisk_PBX...	BYE	3b65e461916a9d
120879@172.17.133.5	b610021978@172.17.133.24	24-Feb-19 17:06:08	Israel-HQ_3	IpGrp0	Beer_Sheva_8	IpGrp0	ISA_1	BYE	3d14fcca95c0f0f
124753@172.17.133.5	b42009990@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	5c2c3d382e8e0f6c
113774@172.17.133.5	b2333332807@172.17.133.24	24-Feb-19 17:06:08	Paris_2	IpGrp0	Paris_2	AnnouncementSrvGrp3	to Paris_2Announceme...	BYE	562bea86313c6766
1@172.17.133.5	b10511@172.17.133.142	24-Feb-19 17:06:08	133.142-10	IpGrp6	133.142-10	IpGrp5	to 1521010-5	BYE	37b632313d9609de
115551@172.17.133.5	b420023483@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	1c9b10b171474e93
18775@172.17.133.5	b720029967@172.17.133.24	24-Feb-19 17:06:08	Texas_7	IpGrp0	Texas_7	IpGrp2	toTexas_7(Asterisk_PBX...	BYE	39270ca513ee6f7e
128005@172.17.133.5	b31124164@172.17.133.24	24-Feb-19 17:06:08	Paris_2	SFRGrp2	Israel-HQ_3	IpGrp1	Kavei_Zahav_1	BYE	7b6dbdb15b655960
125894@172.17.133.5	b420083138@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	22030774199308c
115864@172.17.133.5	b420012034@172.17.133.24	24-Feb-19 17:06:08	Israel-HQ_3	IpGrp2	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	5c3e406525946bbe
125938@172.17.133.5	b42005930@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	143bcb02d1999f7d
112559@172.17.133.5	b13522223019@172.17.133.24	24-Feb-19 17:06:08	133.145-13	IpGrp6	133.145-13	IpGrp5	to 155-5(13-5)	BYE	7b3ecbb6925e22ef
1@172.17.133.5	b5100@172.17.133.26	24-Feb-19 17:06:08	New_Jersey_6	IpGrp0	Haifa_5	IpGrp1	Orange_ISR_1	BYE	615a3f940bcd385f
120809@172.17.133.5	b610017447@172.17.133.24	24-Feb-19 17:06:08	Israel-HQ_3	IpGrp0	Beer_Sheva_8	IpGrp0	ISA_1	BYE	0e9e5d4f000c153
119241@172.17.133.5	b42006482@172.17.133.24	24-Feb-19 17:06:08	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	3ed234e34ee6e6
118071@172.17.133.5	b720024105@172.17.133.24	24-Feb-19 17:06:08	Texas_7	IpGrp2	Texas_7	IpGrp2	toTexas_7(Asterisk_PBX...	BYE	570ea5c6725d27f
118310@172.17.133.5	b42001826@172.17.133.24	24-Feb-19 17:06:07	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	3618f4a80ba2a713
121934@172.17.133.5	b411116158@172.17.133.24	24-Feb-19 17:06:07	Texas_7	VerizonGrp1	China_4	IpGrp1	toChinaPBX-1	BYE	0888292d058a3e3c
13533@172.17.133.5	b4200911@172.17.133.24	24-Feb-19 17:06:07	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	3b2e56fe1d4e5723
13110@172.17.133.5	b4200427@172.17.133.23	24-Feb-19 17:06:07	Israel-HQ_3	IpGrp2	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	13760e58d9f02c9
14645@172.17.133.5	b720027938@172.17.133.24	24-Feb-19 17:06:07	Texas_7	IpGrp0	Texas_7	IpGrp2	toTexas_7(Asterisk_PBX...	BYE	0ee1140205d678b
110358@172.17.133.5	b420020932@172.17.133.24	24-Feb-19 17:06:07	China_4	IpGrp0	China_4	HuaweiPBXGrp2	TO HuaweiPBXGrp2	BYE	3d758c25003101f8

Each row in the page represents an ARM-routed end-to-end call which can pass multiple nodes (SBCs or Gateways) and multiple Connections and Peer Connections. Information on a call is collected by the ARM Configurator from ARM Routers, and then correlated to display a single call record.

During call processing, each ARM Router periodically sends a bulk of call information (CDRs) to the Configurator for processing. The received CDRs are processed and transformed / correlated into a single call record for each ARM end-to-end call. These records are stored in the ARM Configurator's database (MongoDB).

The 'Calls List' page significantly 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.

The page is divided into:

- Filters on the left side of the page [to narrow the search and allow operators access a specific call]
- Calls List to the right of the filters, with a predefined call digest (information)

The following filters are available to facilitate searching for calls and to exclude unwanted calls from the Calls List:

- **Source** [URI before manipulation]

- **Destination** [URI before manipulation]
- **Session ID** [Unique Session ID identifying a specific call]
- **Incoming Node** [the node from where a call was initiated; selected from the drop-down menu]
- **Incoming Peer Connection** [the Peer Connection from where the call was initiated; selected from the drop-down menu. If an incoming node is selected, the incoming Peer Connection option in the filter will include only relevant Peer Connections, associated with the selected node].
- **Outgoing Node** [the node from where the call exited the ARM network (terminated); selected from the drop-down menu]
- **Outgoing Peer Connection** [selected from the drop-down menu; if **Outgoing Node** is selected, the **Outgoing Peer Connection** option in the filter will include only relevant Peer Connections associated with the selected node]
- **Routing rule** [the name of the Routing Rule matches the call and is used for its routing]; selected from drop-down menu and organized per the Routing Groups]
- **SIP reason** [the SIP reason for why the call was terminated]
- **Date range** [the Calls List page will only list calls routed within the range of dates specified]

As the operator starts entering a filter name in a drop-down filter field (e.g., routing rule or incoming node), matching options are auto populated.

The operator can remove a filter by clicking **x**.

Figure 2-2: Calls List Filters

The following columns (call digest) is shown for CDRs / Calls in the Calls List:

- Source
- Destination
- Date
- Incoming node
- Incoming Peer connection
- Outgoing node
- Outgoing Peer Connection
- Routing rule
- SIP reason
- Session ID

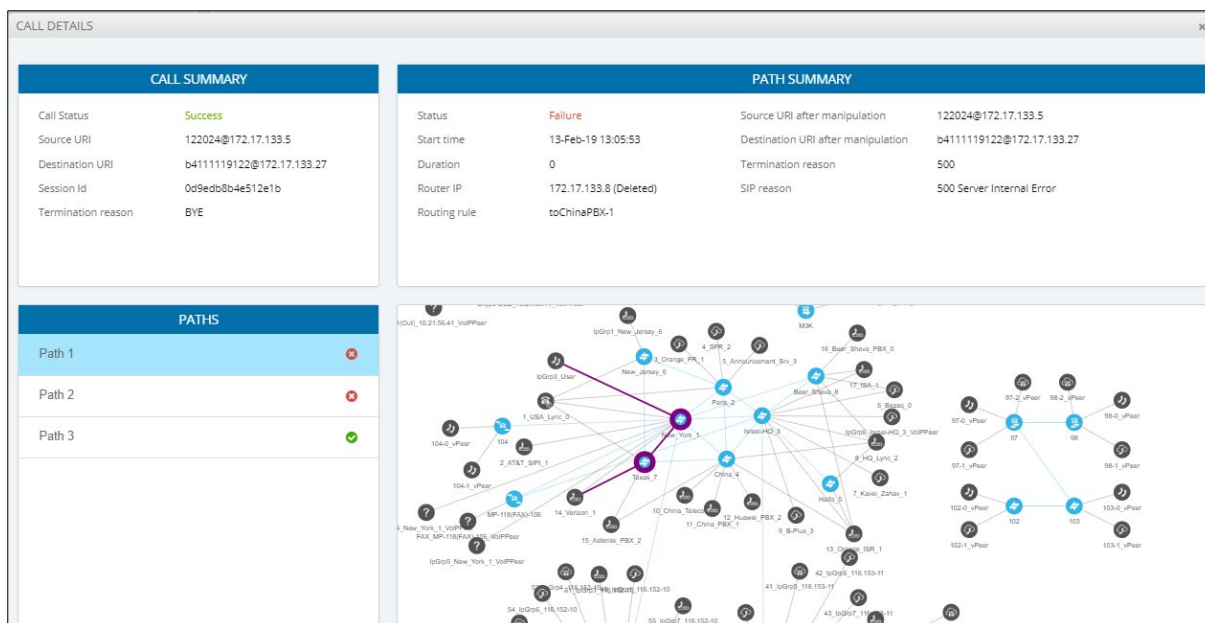
Figure 2-3: Call Columns in the Calls List

SOURCE	DESTINATION	DATE	INCOMING NODE	INCOMING PCON	OUTGOING NODE	OUTGOING PCON	ROUTING RULE	SIP REASON	SESSION ID
16066@172.17.13...	b411119406@172...	13-Feb-19 13:05:58	Texas_7	VerizonGrp1	China_4	IpGrp1	toChinaPBX-1	BYE	4acfd39e44...
18727@172.17.13...	b41111845@172...	13-Feb-19 13:05:57	Texas_7	VerizonGrp1	China_4	IpGrp1	toChinaPBX-1	BYE	370896854...

2.1.2 Call Details

Operators can view the details of a specific call. In the Calls List, the operator can filter the list and then double-click a specific call for the Call Details page to open.

Figure 2-4: Call Details



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

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

Figure 2-5: ‘Call Summary’ Pane

CALL SUMMARY	
Call Status	Success
Source URI	122024@172.17.133.5
Destination URI	b4111119122@172.17.133.27
Session Id	0d9edb8b4e512e1b
Termination reason	BYE

- Call Status
- Source URI
- Destination URI
- Session ID
- Termination reason

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

Figure 2-6: 'Paths' Pane

PATHS	
Path 1	✖
Path 2	✖
Path 3	✔

Selecting a path (routing attempt) enables the operator to view detailed information about that path. After selection, the path is highlighted in the ARM Topology map. The page's Path Summary pane (shown below) changes per the selected path.

Figure 2-7: 'Path Summary' Pane

PATH SUMMARY	
Status: Success	Source URI after manipulation: 8777777778832061@172.17.133.5
Start time: 04-Mar-19 08:55:11	Destination URI after manipulation: b153555564@172.17.133.142
Duration: 0.205 Sec	Termination reason: BYE
Router IP: 172.17.133.8 (Deleted)	SIP reason: BYE
Routing rule: to 153-5 (manipulation)	
▼ More	

The following information is displayed:

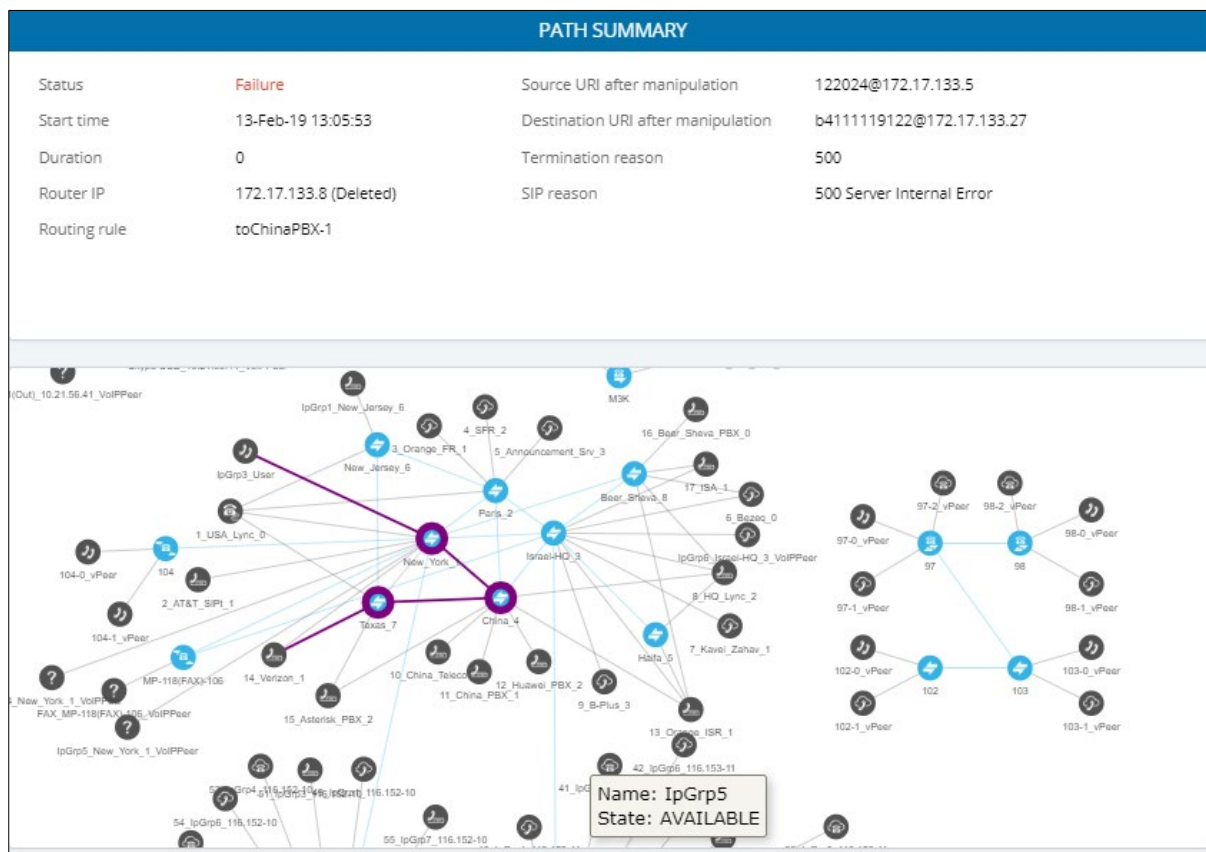
- **Status** [success or failure]
- **Start time** [ARM setup time]
- **Duration** [call duration; non-zero if 'Status' is **Success**]
- **Router IP** [the Router which handled the initial Routing request]
- **Routing rule** [call matching Routing rule used by the ARM to apply a specific routing path]
- **Source URI after manipulation**
- **Destination URI after manipulation**
- **Termination reason** [the reason why the specific path was terminated]
- **SIP reason** [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 **More** option displayed in the path's Summary Details pane. The pane's **More** option allows operators to review the details of the applied manipulation rules.

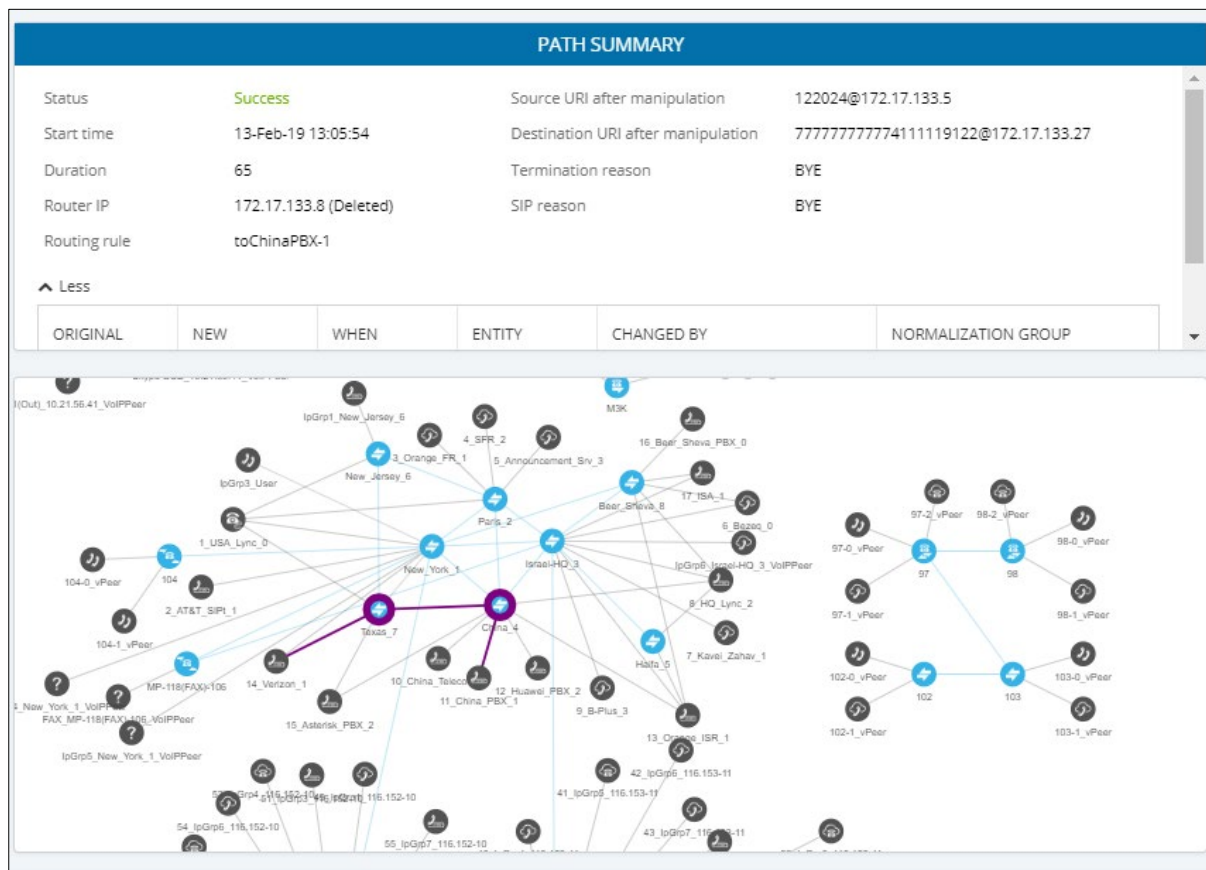
Figure 2-8: 'More' Pane Displaying Details of Applied Manipulation Rules

▲ Less					
ORIGINAL	NEW	WHEN	ENTITY	CHANGED BY	NORMALIZATION GROUP
122024	122024	After route	Source Uri User	toChinaPBX-1 (RR Action)	source1
b4111119122	7777777774...	After route	Destination Uri...	toChinaPBX-1 (RR Action)	RR-dest

This figure shows the path of a call's routing attempt whose status was **Failure**:



This figure shows the path of a routing attempt of the same call, whose status was **Success**:



2.1.3 Disabling | Limiting the Number of CDRs

ARM version 8.6 supports call-detail records (CDRs) of up to 10 million routed calls. The feature is enabled by default. Customers can optionally disable the feature in the Calls Settings section of the Calls screen (Settings > Network Services > Calls) shown below. In the same screen, customers can optionally limit the number of CDRs.

Figure 2-9: Disabling CDRs | Limiting the Number of CDRs

SYSLOGS	<div>CALLS</div> <div>CALLS SETTINGS</div> <div> <div>Enable CDR calls <input checked="" type="checkbox"/></div> <div>Keep raw CDRs for calls with partial data <input type="checkbox"/></div> <div>Keep raw CDRs for calls with full data <input type="checkbox"/></div> <div>Limit number of CDR calls to <input type="text" value="10000000"/></div> <div>Calls cleanup frequency (in minutes, change will take place after restart) <input type="text" value="10"/></div> <div>Submit</div> </div>
NTP SERVERS	
QoS	
CDR	
CALLS	



Note:

- ARM Configurator VM memory requirements have increased to 16 GB in ARM version 8.6 due to calls information and CDRs processing.
- ARM 8.6 supports up to 10 million CDRs but operators can limit the number using the setting 'Limit number of CDR calls to'.
- If running more than 150 CAPS traffic, operators are recommended to disable CDRs.

2.2 Routing Servers Groups with Internal and External Priorities

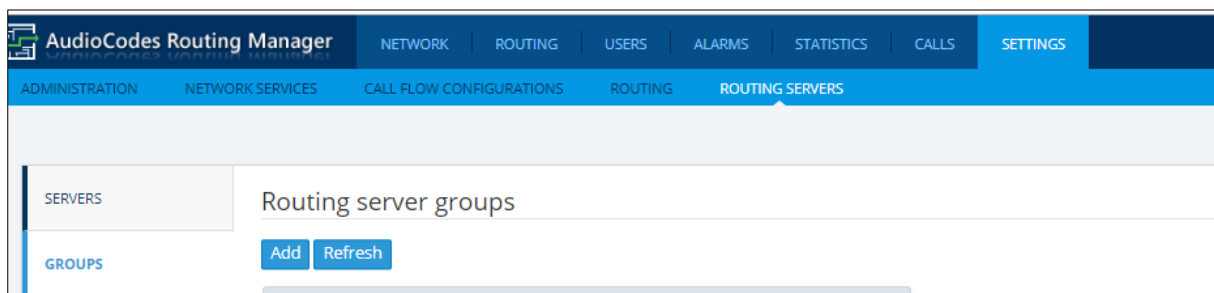
In versions prior to ARM version 8.6, the ARM allowed multiple ARM Routers to be attached to a node (SBC or Gateway), with one policy selected (Round Robin policy, by default).

When an ARM deployment is geographically distributed, however, the necessity arises for multiple groups of ARM Routers with a policy between them. 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).

ARM version 8.6 supports this new functionality: Customers can now configure an ARM Routing Servers Group with internal policies (within a group) and external policies (between groups).

To apply this feature operators must first configure a Routing Server Group in the 'Routing server groups' page (Settings > Routing Servers > Groups).

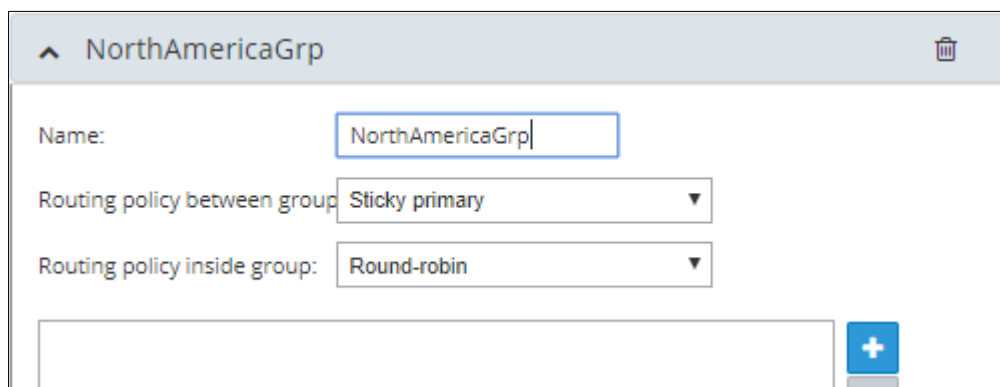
Figure 2-10: Routing Server Groups



When adding a new ARM Routers Group, the operator is prompted to configure the:

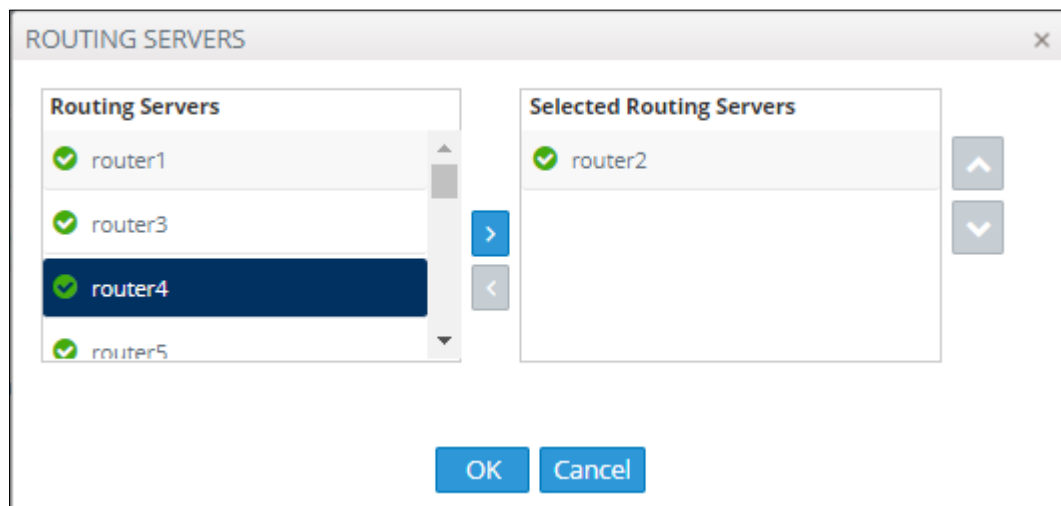
- Name of the group to be attached to a node or to multiple nodes
- Routing Policy to be applied between groups; 'Sticky primary' is the default. Two routing policies between Routing Groups are available:
 - 'Sticky primary' [the node reverts to the primary group when at least one ARM Router is available]
 - 'Sticky Last' [after a node switches to the next Routing Group, it uses its ARM Routers while at least one of them is available]
- Routing Policy to be applied between the ARM Routers inside the Routing Group ('Round Robin' is the default). Three routing policies are available: Round Robin, Sticky Primary and Sticky Last.

Figure 2-11: Routing Policy Options



Operators must then attach one or more ARM Routing Servers to the Routing Group.

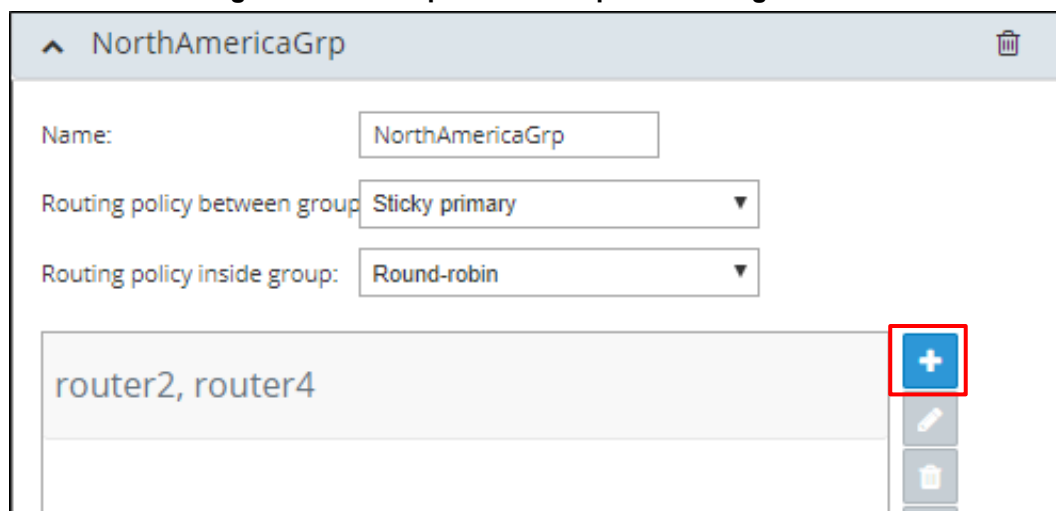
Figure 2-12: Attaching Routing Server/s to Routing Group



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.

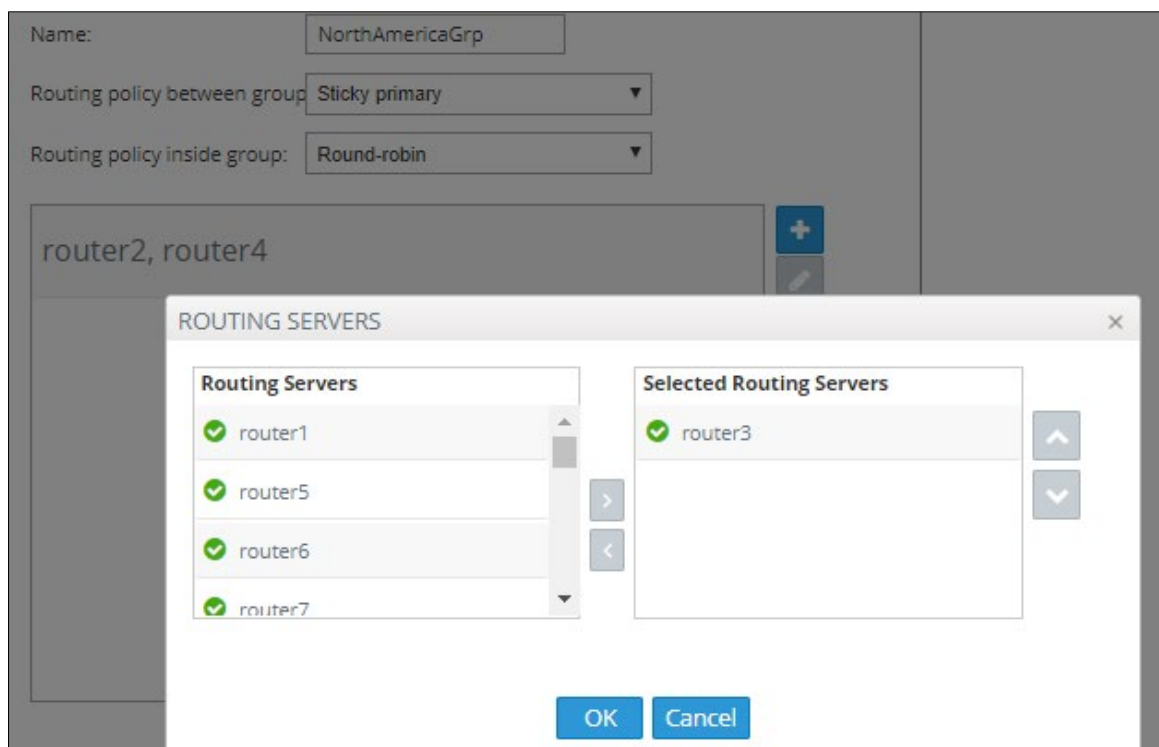
When providing multiple sub-groups of Routing Servers, operators must click +.

Figure 2-13: Multiple Sub-Groups of Routing Servers



The new sub-group of routers with the same Routing Policy inside the group can then be configured.

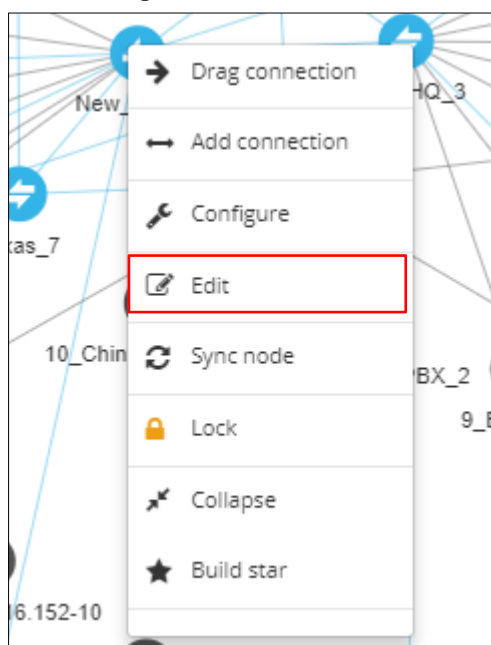
Figure 2-14: Sub-Group of Routing Server with the Same Routing Policy



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

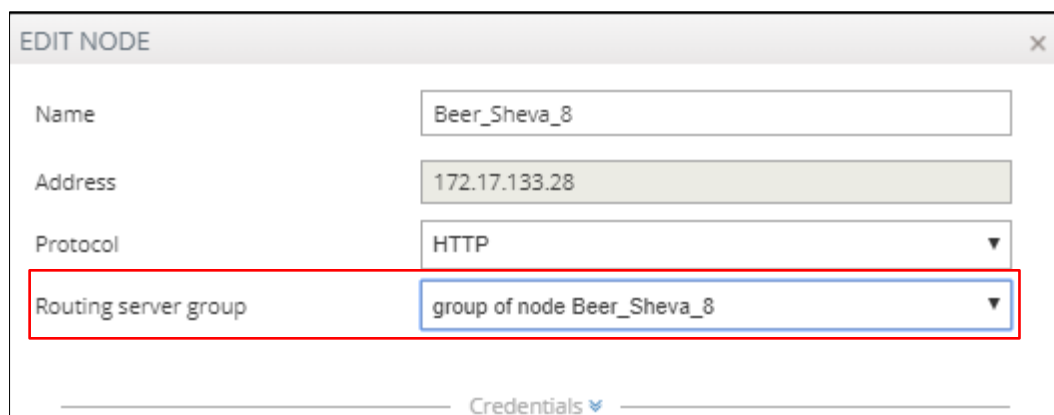
When the ARM Routing Servers group is created, it can be attached to a single node or to multiple nodes (SBCs or Gateways). To do this, operators must apply an Edit action on a specific node.

Figure 2-15: Edit Node



The Routing Server Group can be selected from the drop-down (one of the previously configured).

Figure 2-16: Edit Node – Selecting Routing Server Group



The screenshot shows a window titled "EDIT NODE" with a close button (X) in the top right corner. It contains several input fields: "Name" with the value "Beer_Sheva_8", "Address" with the value "172.17.133.28", "Protocol" with a dropdown menu showing "HTTP", and "Routing server group" with a dropdown menu showing "group of node Beer_Sheva_8". The "Routing server group" field is highlighted with a red rectangular box. At the bottom of the window, there is a "Credentials" section with a small blue icon.

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.



Note: Support for Routing Server Groups is available from node software version 7.20A.240. If a customer's deployment includes nodes whose software version is earlier than 7.20A.240, the ARM provides a backward-compatible configuration with one (default) Routing Server Group and a policy between its Routers.

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.

2.3 Customer Certificates with FQDN / Hostname

FQDN / Hostname is supported in ARM version 8.6 (and on nodes whose software version is 7.252 and later):

- Nodes can be added to the ARM using FQDN / Hostname
- ARM can be defined in the node's Web interface using ARM's FQDN / Hostname

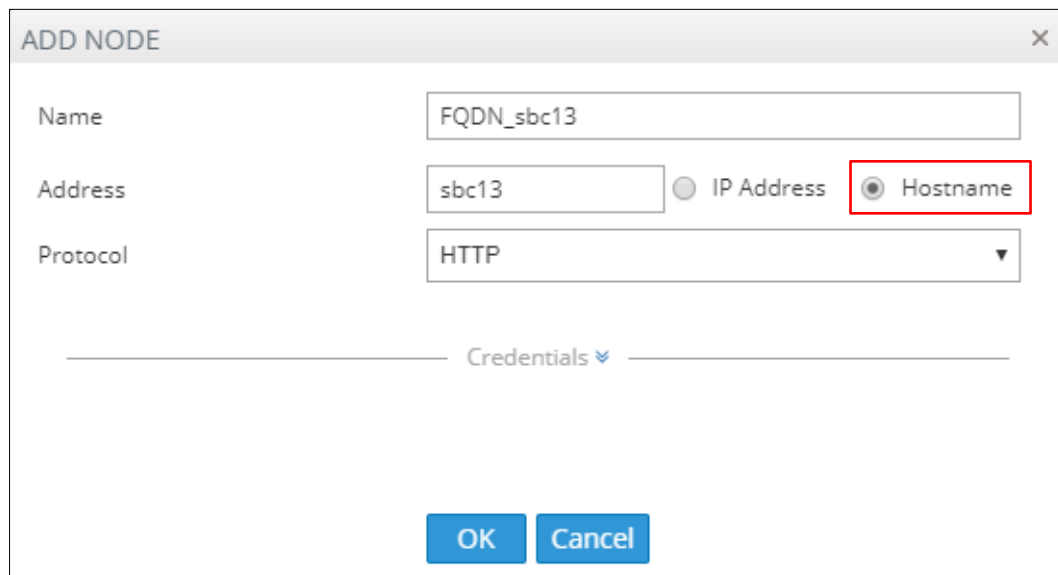
The feature gives operators more flexibility when designing their telephony networks because they're no longer limited to using hard-coded IP addresses.

2.3.1 Using FQDN / Hostname instead of IP Address

2.3.1.1 Adding a Node using FQDN / Hostname

A new **Hostname** option in the Add Node screen shown below allows operators to add a node to the ARM using FQDN / Hostname instead of IP address.

Figure 2-17: Add Node using Hostname / FQDN



The screenshot shows a dialog box titled "ADD NODE" with a close button (X) in the top right corner. The dialog contains the following fields and options:

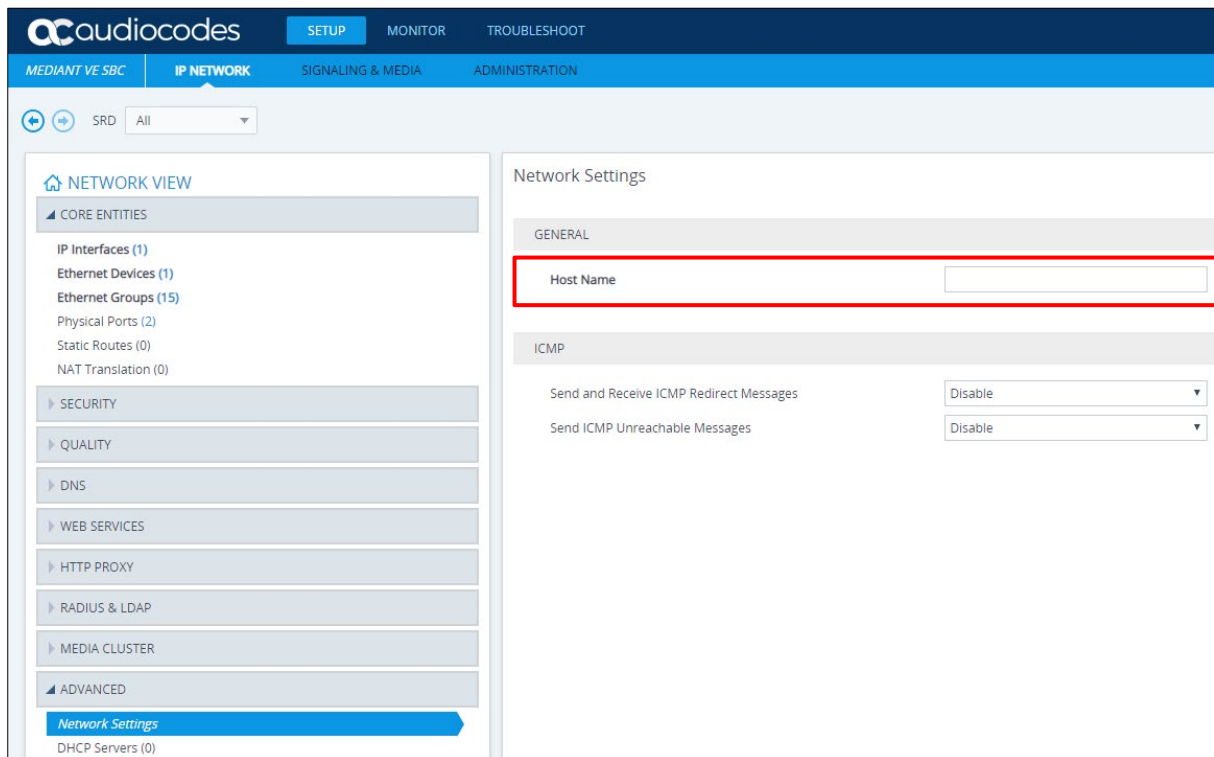
- Name:** A text input field containing "FQDN_sbc13".
- Address:** A text input field containing "sbc13". To its right are two radio buttons: "IP Address" (unselected) and "Hostname" (selected). The "Hostname" radio button and its label are highlighted with a red rectangle.
- Protocol:** A dropdown menu showing "HTTP".
- Credentials:** A section header with a small blue icon, located below a horizontal line.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

2.3.1.2 Adding FQDN / Hostname to a Node

Operators can configure FQDN / Hostname for an existing node, in the node's Web interface, Network Settings page.

The page is opened by right-clicking the node in the ARM's Network Map page to log in, selecting the **IP Network** menu, opening the **Advanced** tab and then selecting the **Network Settings** tab.

Figure 2-18: Node's Web Interface - Network Settings Page – Host Name



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 FQDN and IP address, FQDN is used. ARM version 8.6 allows operators to change the Hostname or IP address. The ARM displays all devices' IP addresses and hostnames.

2.3.1.3 Adding ARM with FQDN

Operators can change the way ARM communicates with other entities, e.g., routers and nodes. The ARM can publish either hostname or IP address when configuring other entities. The **Security** tab under the Settings menu allows operators to do this.

Figure 2-19: Security

LICENSE	Security
SECURITY	<div>SECURITY</div> <div> Session timeout (hours): <input type="text" value="2"/> </div> <div> Inactivity period (minutes): <input type="text" value="120"/> </div> <div> http/https enabled: <input checked="" type="checkbox"/> </div> <div> * These changes will take place after logout </div>
OPERATORS	
NODE CREDENTIALS	
ROUTER CREDENTIALS	
CONFIGURATOR CREDENTIALS	
LDAP AUTHENTICATION	<div>ARM CONFIGURATION</div> <div> ARM IP Address: <input type="text" value="172.17.133.7"/> </div> <div> ARM Hostname: <input type="text" value="arm7.corp.audiocodes.com"/> </div> <div> Communication method: <input type="text" value="IP Based"/> </div>

- 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 hostname or IP address for the other entities]



Note: This action may take some time depending on network size and the number of configured ARM Routers. The action will cause entities to be temporarily disconnected.

2.3.2 Certificates Validation

ARM version 8.6 adds the first phase of security enhancement.

2.3.2.1 Client Side Certificate Verification

Operators can configure trusted certificates; the ARM only accepts certificates when initiating TLS communications from the ARM. The certificate verification feature is enabled by selecting a new option **Verify certificate when ARM preforms https requests** (in Settings > Administration > Security).

Figure 2-20: Certificate Verification

LICENSE	Security
SECURITY	
OPERATORS	<p>SECURITY</p> <p>Session timeout (hours): <input type="text" value="2"/></p> <p>Inactivity period (minutes): <input type="text" value="120"/></p> <p>http/https enabled: <input checked="" type="checkbox"/></p> <p>* These changes will take place after logout</p>
NODE CREDENTIALS	
ROUTER CREDENTIALS	
CONFIGURATOR CREDENTIALS	<p>ARM CONFIGURATION</p> <p>ARM IP Address: <input type="text" value="172.17.133.7"/></p> <p>ARM Hostname: <input type="text" value="arm7.corp.audiocodes.com"/></p> <p>Communication method: <input type="text" value="IP Based"/></p>
LDAP AUTHENTICATION	
RADIUS AUTHENTICATION	
REMOTE MANAGER	<p>CERTIFICATE VERIFICATION</p> <p>Verify certificate when ARM performs https requests <input type="checkbox"/></p> <p>Verify certificate subject name when ARM performs https requests <input type="checkbox"/></p>
CERTIFICATES	<p><input type="button" value="Submit"/></p>

The Add Certificate screen (Settings > Administration > Certificates > Add) allows operators to upload trusted certificates.

Figure 2-21: Add Certificate

- **Alias** [the name of the certificate]
- **Certificate file** [any valid Base64-encoded certificate file]



Note: This setting is system wide; the operator needs to 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, the operator must reupload the changed certificate.

2.3.2.2 Certificate Subject Name Verification

A new security enhancement is supported: 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.

A new option **Verify certificate subject name when ARM performs https requests** under the Certificate Verification section of the Security page (Settings > Administration > Security) allows operators to enable the feature.

Figure 2-22: Verify certificate subject name when ARM performs https requests



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

2.4 Calls Forking

ARM version 8.6 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.

A new parameter 'Routing Method' has been added for this purpose to the Routing Rule Action part, on a per-Routing Rule basis.

Figure 2-23: Calls Forking – Routing method

The Routing Method value is set by default to **Sequence**; Routing Rule actions are applied *sequentially* (the only option in ARM versions earlier than 8.6).

If the Routing Method is set to **Forking**, the actions are applied simultaneously and the call is split to all the destinations.

ARM version 8.6 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 2-24: Calls Forking Routing Rule

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



Note:

- In ARM version 8.6, forking capabilities can only be applied to SBCs. Media Gateways aren't supported.
- Forking in the ARM is supported on SBC software 7.20.252 GA or later (release pending). For earlier SBC versions, Forking functions like 'Sequence'.

2.5 Routing Based on any SIP Invite Header Value

ARM version 8.6 provides a new capability to route a call based on any SIP Invite header value as Routing Rule matching criterion. Customers can now route a call based (for example) on a TGRP value or specific SDP information; any information present in the SIP Invite can be used as a condition in the ARM Routing Rule.

The feature is configured at SBC *and* ARM level:

- At the SBC level, the operator must apply SBC message manipulation and provide the required information in the predefined SIP header (X-Header) in a specific format.
- At the ARM level, the information can be used as a condition in an ARM Routing Rule.

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.

2.5.1 SBC-Level Configuration

To send the parsed information request, operators must add a new header with name “X-ARM-DETAIL-1”, “X-ARM-DETAIL-2”... “X-ARM-DETAIL-N” and 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:

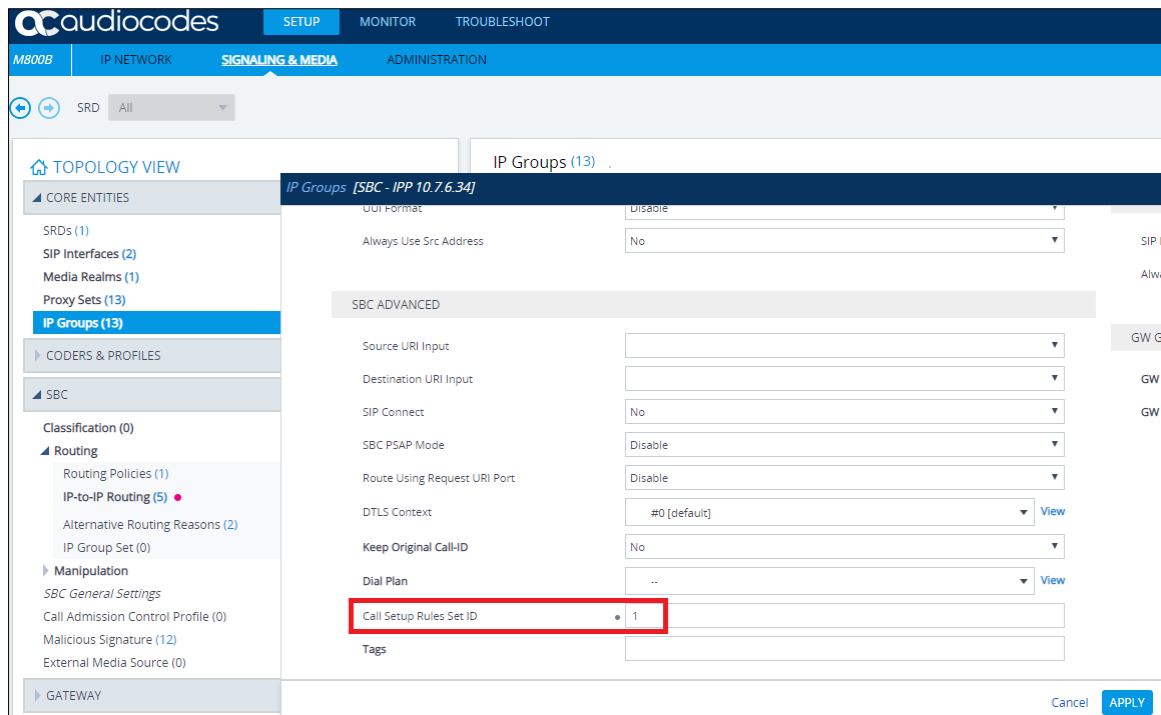
X-ARM-DETAIL-1: “tgrp=100”

X-ARM-DETAIL-2: “coder=711”

To create a new header in the SBC, operators must add a new “Call Setup Rules Set ID” in “IPGroup” or in “SIP Interface”.

Below is an example for IPGroup:

Figure 2-25: Viewing SBC IPGroup Configuration



Setup rules can then be associated with the same Set ID.

Figure 2-26: Viewing SBC Call Setup Rules Configuration

INDEX	RULES SET ID	NAME	QUERY TARGET	SEARCH KEY	ATTRIBUTES TO GET	ROW ROLE	CONDITION	ACTION
0	1	adding header 1				Use Current Condition	hea	
1	1	adding header 2				Use Current Condition	hea	

GENERAL

Index: 0

Name: adding header 1

Rules Set ID: 1

Query Type: None

Query Target:

Search Key:

Attributes To Get:

Row Role: Use Current Condition

Condition:

ACTION

Action Subject: header:X-ARM-DETAIL-1

Action Type: Add

Action Value: tgrp=100

In this example, the manipulation added is “tgrp=100”. In general, operators can use a condition with RegEx and take the attributes into the Action Value.

2.5.2 ARM-Level Configuration

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 preconfigured ‘X-ARM-DETAIL-N’ header and ready to use it for routing.

This configuration in the ARM is performed at the Routing Rule level, in the ARM Routing Rule ‘Advanced Condition’ > SIP headers.

Figure 2-27: SIP Headers

Sip headers

name: tgrp values: 100 200

name: coder values: 711 729

In the SIP headers, ‘name’ is the SIP header name and ‘values’ is 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 above 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”).

2.6 Authenticating Operator Login using Open LDAP

ARM version 8.6 adds the option to use LDAP authentication with Open LDAP. The LDAP Authentication page in the ARM allows operator authentication using Open LDAP (Settings > Administration > LDAP Authentication).

Figure 2-28: LDAP Authentication Page for Authenticating Operator Login using Open LDAP

The screenshot shows the 'LDAP Authentication' page in the AudioCodes Routing Manager. The left sidebar contains a menu with options: LICENSE, SECURITY, OPERATORS, NODE CREDENTIALS, ROUTER CREDENTIALS, CONFIGURATOR CREDENTIALS, LDAP AUTHENTICATION (selected), and RADIUS AUTHENTICATION. The main content area is titled 'LDAP Authentication' and includes a section for 'LDAP AUTHENTICATION SERVER' with fields for 'Enable LDAP Authentication' (a toggle switch), 'LDAP Authentication Server Host *' (a text field with 'aclsads01.corp.audiocodes.com'), 'LDAP Authentication Server Port' (a text field with '3268'), 'LDAP Connectivity DN' (a text field with 'ldap_bind@CORP.AUDIOCODES.COM'), 'LDAP Connectivity Password' (a text field), and 'User Dn Search Base' (a text field with 'dc=corp,dc=audiocodes,dc=com'). A 'Test' button is located below these fields. At the bottom, the 'AUTHORIZATION LEVEL SETTINGS' section is highlighted with a red box, showing two radio buttons: 'Active Directory' and 'Open Ldap'.

LDAP authentication settings previously supported LDAP authentication with Microsoft Active Directory.

LDAP Authentication Server settings for Open LDAP are the same as for Active Directory. In the Authorization Level setting, **Open Ldap** is selected and the following mapping attributes are provided:

- **User Name Attribute** [The LDAP attribute used to identify the username]
- **Group Membership Attribute** [The LDAP attribute used to list the members of the LDAP group]
- **Security Admin Group Name** [The name of the LDAP group containing operators with Admin security level access to ARM]
- **Admin Group Name** [The name of the LDAP group containing operators with Admin access to ARM]
- **Monitor Group Name** [The name of the LDAP group containing operators with Monitor access to ARM]
- **Group Name Attribute** [The LDAP attribute used to identify the LDAP group name]
- **Group ObjectClass Attribute** [The value of the ObjectClass attribute that identifies a user group LDAP object]

Figure 2-29: Authorization Level Settings

The screenshot shows the 'AUTHORIZATION LEVEL SETTINGS' section. At the top, there are two radio buttons: 'Active Directory' and 'Open Ldap', with 'Open Ldap' selected. Below this, there are seven rows of settings, each with a label on the left and a text input field on the right:

- User Name Attribute: uid
- Group Membership Attribute: member
- Security Admin Group Name: ARM_SecurityAdmin
- Admin Group Name: ARM_Admin
- Monitor Group Name: ARM_Monitor
- Group Name Attribute: cn
- Group ObjectClass Attribute: groupOfNames

2.7 ARM in the Amazon Web Services Cloud

ARM version 8.6 supports running the ARM application in the Amazon Web Services (AWS) cloud. ARM version 8.6 is published in AWS in the form of AMIs (Amazon Machine Images). Instructions for deploying ARM AMIs in AWS are provided in the *ARM Installation Manual Version 8.6*. Instructions for setting auto-recovery of ARM VMs if a hardware failure occurs are also provided.

When deploying the ARM in AWS, all VMs must be in the same virtual private cloud (VPC) and in the same subnet. All VMs must be in a security group that allows all

- outgoing traffic
- incoming traffic from inside the VPC
- incoming SSH, HTTP, HTTPS from any of the enterprise's subnets

2.8 Improved ARM Tolerance when Upgrading ARM Routers

The increased number of supported ARM Routers (up to 40 as of ARM version 8.4) raised a requirement for a more tolerant approach to ARM software upgrade when upgrading ARM Routers.


ARM version 8.6 allows customer to continue the ARM Routers upgrade process if it was previously stopped for any reason (e.g., network disconnection of the shell between the operator and the Configurator, or desynchronization of one of the Routers). Operators can now run the upgrade again and it will continue to upgrade all remaining ARM Routers (starting from the last failed ARM Router).

2.9 ARM Machine OS Upgraded with Latest CentOS6.10 Security Patches

ARM version 8.6 runs on the latest edition of the CentOS 6 (CentOS 6.10) operating system. The latest security patches are automatically applied during the upgrade to ARM version 8.6. The changes in the upgrade procedure are described in the *ARM Installation Manual*.


2.10 New Alarm for ARM Routers Unavailability

A new Critical alarm was added to ARM version 8.6. The alarm is sent if all preconfigured ARM Routers become unavailable or disconnected.

SEVERITY	 Critical
DATE & TIME	14-Feb-19 14:51:12
NAME	No available routers
SOURCE	Configurator
ALARM TYPE	Communications Alarm
PROBABLE CAUSE	Communications Subsystem Failure
DESCRIPTION	Currently there are no available routers in the system

The alarm is cleared when at least one ARM Router returns to service.

In the Warning alarm sent if an ARM Router fails, a new indication 'Additional Info 2' was added, specifying how many ARM Routers out of the provisioned ARM Routers are unavailable.

>> HISTORY ALARMS SUMMARY	
SEVERITY	 Warning
DATE & TIME	14-Feb-19 14:51:11
NAME	Operation status changed
SOURCE	Router#router5
ALARM TYPE	Communications Alarm
PROBABLE CAUSE	Communications Subsystem Failure
DESCRIPTION	Router router5 was marked as not synced
ADDITIONAL INFO 1	The alarm will be cleared once the status will be changed back to available.
ADDITIONAL INFO 2	(16 / 32 Routers are unavailable)

This page is intentionally left blank.

3 New Machine Requirements for ARM Configurator

ARM version 8.6 features storage in the ARM Configurator of up to 10 million CDRs as described in Section [2.1](#). To provide this feature, the ARM Configurator's requirement for RAM has increased to **16 GB**. The ARM Router still requires only **8 GB**.

The ARM Configurator requires this increased memory during ARM upgrade. See the *ARM Installation Manual* for the memory update procedure as part of the upgrade.

This page is intentionally left blank.

4 Supported Platforms

ARM version 8.6 provides support for the platforms shown in the table below.

Table 4-1: ARM Version 8.6 Supported Platforms

ARM	Platform	Application
GUI	Web Browser	Firefox, Chrome, Internet Explorer (Version 11)
Deployment	VMWare	VMware ESXI 5.5, 6.0, 6.5, 6.7
	HyperV	Windows Server 2016 Hyper-V Manager Microsoft Corporation Version: 10.0.14393.0

This page is intentionally left blank.

5 Earliest Node Software Versions Supported by ARM Features

Some ARM features are developed in coordination with nodes (AudioCodes' SBCs and Gateways). To activate and use an ARM feature, the node needs to be upgraded to the earliest software supporting that feature if it's configured with software that does not support it.

The following table displays ARM features supported by the earliest node software.

Table 5-1: ARM Features Supported by the Earliest Node Software

#	Feature	Earliest Node Software Supporting It	Comments
1	Quality-based routing	Version 7.2.158 and later	The quality-based routing feature is not supported when operating with nodes version 7.0 (for Mediant 3000).
2	Separate interface at the node level for ARM traffic	Version 7.2.158 and later	The capability to configure a separate interface at the node level for ARM traffic is not supported when operating with nodes earlier than version 7.2.154 (for Mediant 3000).
3	Call preemption	Version 7.2.158 and later	The call preemption for emergency calls feature is not supported when operating with nodes version 7.20A.154.044 or earlier (not applicable for Mediant 3000).
4	Number Privacy	Version 7.2.250 or later	The Number Privacy feature is supported as of node version 7.20A.250.
5	Support of IP Group of type User without 'dummy' IP	7.20A.250 and later	Operators who want to use a node's IP Group of type 'User' as the ARM Peer Connection can avoid configuring a dummy IP Profile if using node version 7.20A.250 and later. Customers who use ARM version 8.4 with node version earlier than 7.2.250 and who want to configure an IP Group of type 'User' as the ARM Peer Connection, must configure a dummy IP Profile (with a dummy IP address) at the node level, to be associated with this IP Group.
6	Support of ARM Routers group and policies.	Version 7.20A.240 or later	
7.	Support of ARM Routed Calls/CDRs representation	Version 7.20A.250.205 or later	
8	Support of Forking in ARM (SBC only)	Version 7.20A.252 or later.	

This page is intentionally left blank.

6 Known Limitations and Workarounds

The table below lists the known limitations and workarounds in this version release.

Table 6-1: Known Limitations and Workarounds

Incident	Problem / Limitation	Comments/Workaround
-	Attaching / detaching a user to / from an Active Directory Group is reflected in the ARM's Users page (and Users Groups page) only after performing a full update (synchronization) with the LDAP server (by default performed automatically every 24 hours).	Operators must take this into consideration
-	There is a minor bug in old versions of the VMware vSphere client application that may cause the following error message to be sent when deploying ARM Virtual Machines: 'Provided manifest file is invalid: Invalid OVF manifest entry'	Two workarounds: ✓ Upgrade the VMware environment to a newer version. ✓ Use the VMware vSphere Web client rather than the client application.
-	ARM Forking is supported for SBC only (Media Gateway is not supported).	-
ARM-2479	ARM does not support FQDN for third-party devices (non-AudioCodes SBCs or Gateways).	These devices should be added and operated with IP addresses.
-	An ARM alarms duplication issue occurs in OVOC Version 7.1.164 ARM 8.4 if the operator implements ARM alarms integrated with the OVOC. The issue is fixed in ARM Version 8.6 and OVOC Version 7.6.1000 but if duplicated alarms remain, the operator must perform a workaround.	To delete previously generated duplicated alarms if they remain, remove the ARM from the OVOC and then add it again.
GUI Incidents		
-	In the ARM Map, the 'drag' feature used to 'draw' a connection between two nodes does not complete successfully when the 'hide edges on drag' option is selected. When the option is selected, if the operator starts the 'Drag connection' action but does not end it at the node (does not complete the 'Drag Connection' action), the Map remains in a state in which edges are hidden.	Moving (repositioning) any Map element (node or VoIP Peer) fixes the situation.
-	The maximum number of aggregated Peer Connections in a VoIP Peers cluster is 99.	-
ARM-1204	After operator inactivity for a long period (days or weeks), the operator sometimes can't log in into the ARM with their regular user and password.	Apply Ctrl+F5 to refresh the ARM login screen.
ARM-2508	If an ARM Router is configured with its DNS name rather than with its IP address, the 'Router IP' parameter in the Path Summary pane of the Calls Details page for calls handled by this router incorrectly displays '(Deleted)' after the IP address.	Disregard this indication. It will be fixed in the next major release.

Incident	Problem / Limitation	Comments/Workaround
ARM-2503	<p>The 'Items per Page' function, used to determine the number of table rows to display per page, is not clickable and can't be changed from the default. Applies to the following tables:</p> <ul style="list-style-type: none"> ✓ Routing Rules (table view) [Routing > Routing Rules] ✓ Peer Connections (table view) [Network > Peer Connections] ✓ Connections (table view) [Network > Connections] ✓ Users Table [Users > Users] ✓ Property Dictionary (table) [Users > Property Dictionary] ✓ Alarms tables (including Active Alarms, History Alarms and Journal) [Alarms tab] ✓ Time Based Routing (table) [Settings > Routing > Time Based Routing] 	<p>The paging function allowing operators to go to a specific row in a table is available.</p> <p>The issue will be fixed in the next major release.</p>
ARM-2539	<p>When editing Routing Rules, if an operator enters a name in the 'Prefix/Prefix Group' field (under Source or Destination) without pressing Enter, the information will not be entered and a blue 'bubble' displaying the name will not be displayed as it should. The issue does not occur with the other Routing Rules fields.</p>	<p>Enter a Prefix or Prefix Group name in the field and then press the Enter key. Make sure the name is entered and a blue 'bubble' is displayed.</p>
ARM-2428	<p>An incorrect number of rows is displayed in the Prefix Groups page (Settings > Call Flow Configurations > Prefix Groups) irrespective of the number of rows the operator selects from the 'Items per page' drop-down. The page displays 1000 rows even if 25, 50 or 100 is selected from the drop-down.</p>	<p>Disregard the 'Items per page' drop-down.</p>

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Website: <https://www.audiocodes.com/>

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

LTRT-41947

