Release Notes

AudioCodes One Voice™ Operations Center

AudioCodes Routing Manager (ARM)

Version 9.6

Table of Contents

List of Tables

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: September-14-2021

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
ARM REST API Developer’s Guide
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

These *Release Notes* describe the new features and known issues in version 9.6 of the AudioCodes Routing Manager (ARM).

1.1 Managed AudioCodes Devices

ARM 9.6 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 9.6

Device	Major Versions
Mediant 9000 SBC	7.20A.258 and later
Mediant 4000 SBC	7.20A.258 and later
Mediant 2600 SBC	7.20A.258 and later
Mediant SE/VE SBC	7.20A.258 and later
Mediant 1000B Gateway and E-SBC	7.20A.258 and later
Mediant 800B Gateway and E-SBC	7.20A.258 and later
Mediant 800C	7.20A.258 and later
Mediant 500 E-SBC	7.20A.258 and later
Mediant 500L - SBC	7.20A.258 and later
Mediant SBC CE (Cloud Edition)	7.20A.258 and later
Mediant 3000 Gateway only	7.00A.142.001 and later
Mediant 3100 SBC, Gateway or Hybrid	7.40M3.002.084 and later

Note: See also Section 4 for the earliest device version supported by the ARM *per ARM feature*.

This page is intentionally left blank.

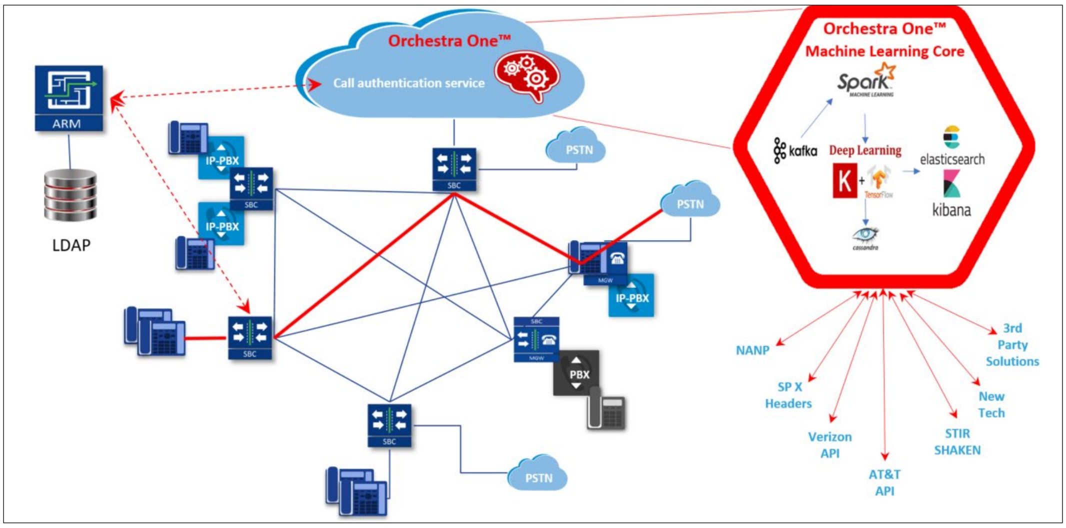
2 What's New in Version 9.6

This section covers the new features and capabilities introduced in ARM 9.6.

2.1 Security-Based Routing

ARM 9.6 supports security-based routing through integration with SecureLogix's Orchestra One™ CAS (Call Authentication Service). The ARM has supported security-based routing since ARM 8.8.

Figure 2-1: Security-Based Routing through Integration with SecureLogix's Orchestra One



The combined solution involves pre-routing consultation with Orchestra One performed by the ARM for predefined calls.

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'.

When configuring a Routing Rule in ARM 9.6, a new 'Security call score' option is available (when SecureLogix is used) under the 'Security Based Routing' section under the **Advanced Conditions** tab of the Add Routing Rule screen.

Note: Using security-based routing requires purchasing SecureLogix's license in addition to the ARM license and must be coordinated with AudioCodes.

In contrast to ARM 8.8, ARM 9.6 features two strategy modes:

- **Standard mode**. Checks for basic security verification strategy. Strategy 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'.
  - 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.

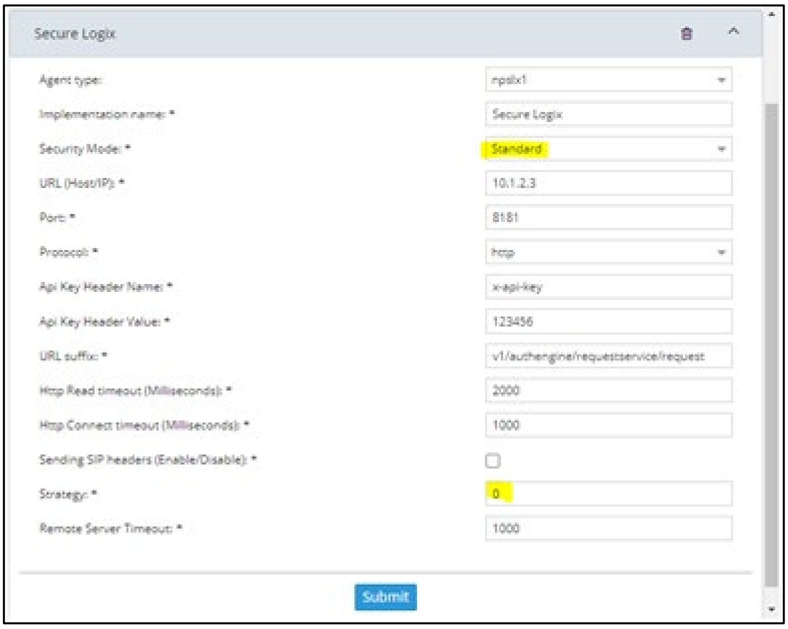
The License Key has been separated into two different license details fields:

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

2.1.1 Using an External Web Service for Pre-Routing Call Security Score Consultation

Network administrators must first define the Web Server for communication with SecureLogix's Orchestra One call authentication service, with Agent type 'npslx1'. This plugin in the ARM includes the REST API for ARM communication with Orchestra One.

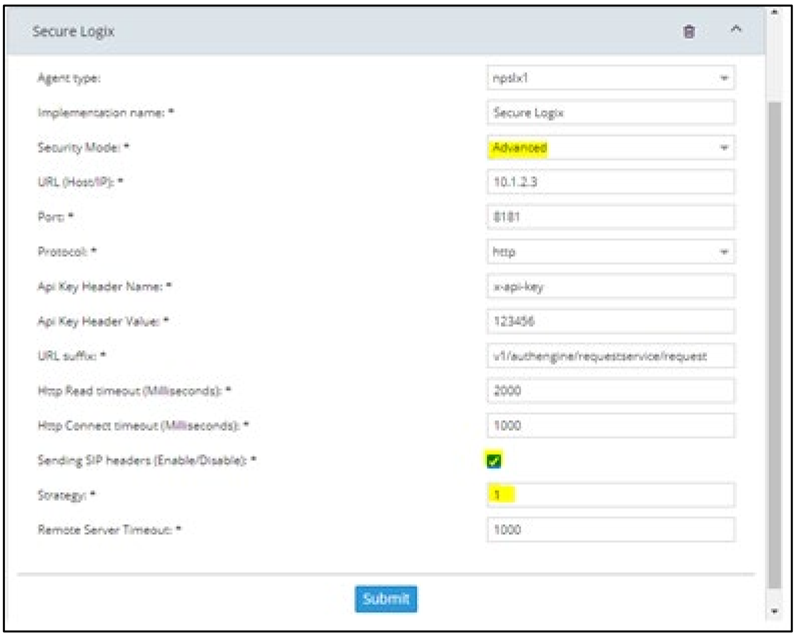
SecureLogix – Standard Mode



Secure Logix

Agent type:	npslx1
Implementation name: *	Secure Logix
Security Mode: *	Standard
URL (Host/IP): *	10.1.2.3
Port: *	8181
Protocol: *	http
Api Key Header Name: *	x-api-key
Api Key Header Value: *	123456
URL suffix: *	v1/authengine/requestservice/request
Http Read timeout (Milliseconds): *	2000
Http Connect timeout (Milliseconds): *	1000
Sending SIP headers (Enable/Disable): *	□
Strategy: *	0
Remote Server Timeout: *	1000

SecureLogix – Advanced Mode



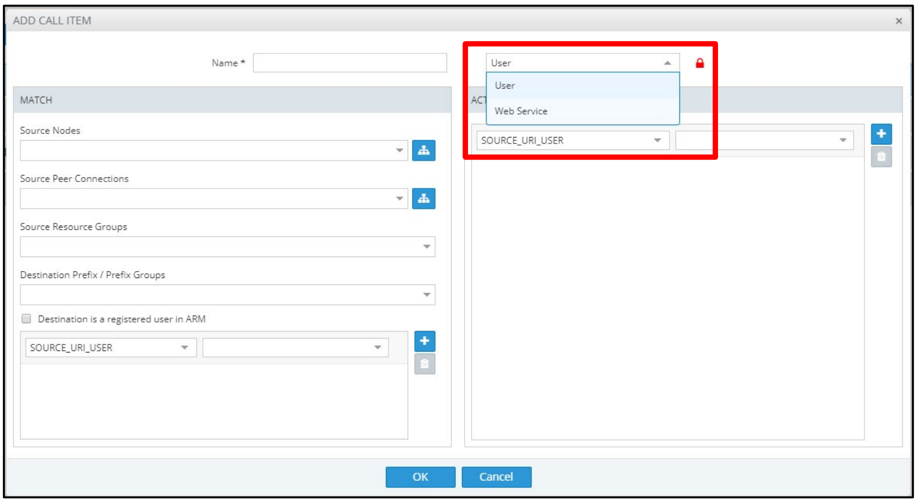
Secure Logix

Agent type:	npslx1
Implementation name: *	Secure Logix
Security Mode: *	Advanced
URL (Host/IP): *	10.1.2.3
Port: *	8181
Protocol: *	http
Api Key Header Name: *	x-api-key
Api Key Header Value: *	123456
URL suffix: *	v1/authengine/requestservice/request
Http Read timeout (Milliseconds): *	2000
Http Connect timeout (Milliseconds): *	1000
Sending SIP headers (Enable/Disable): *	☑
Strategy: *	1
Remote Server Timeout: *	1000

The newly-defined Web Server must then be assigned in the ARM's Policy Studio for pre-routing processing and consultation with SecureLogix's Orchestra One.

In addition to the default **User** usage, Policy Studio 9.6 consequently supports the following new usage: **Web Service**.

Figure 2-2: Policy Studio: Web Service

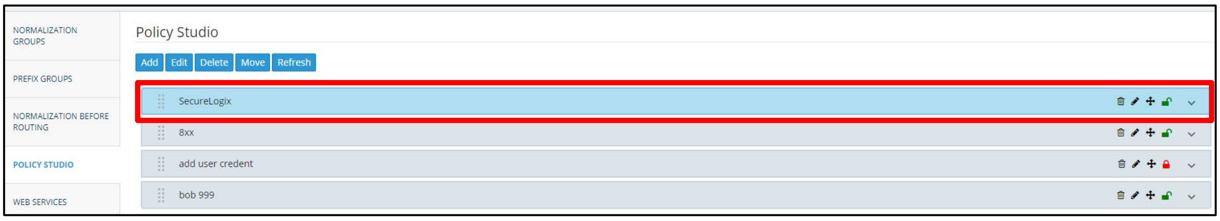


Previously, network administrators were limited to using Policy Studio based on information taken from ARM Users Data (the default **User** option).

Network administrators can now select a new option to use an external Web Service for pre-routing manipulation, for example, SecureLogix (to apply security-based routing).

Note that by correctly using a Policy Studio rule's 'condition' feature, the network administrator 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.

Figure 2-3: External Web Service 'SecureLogix' Configured in Policy Studio



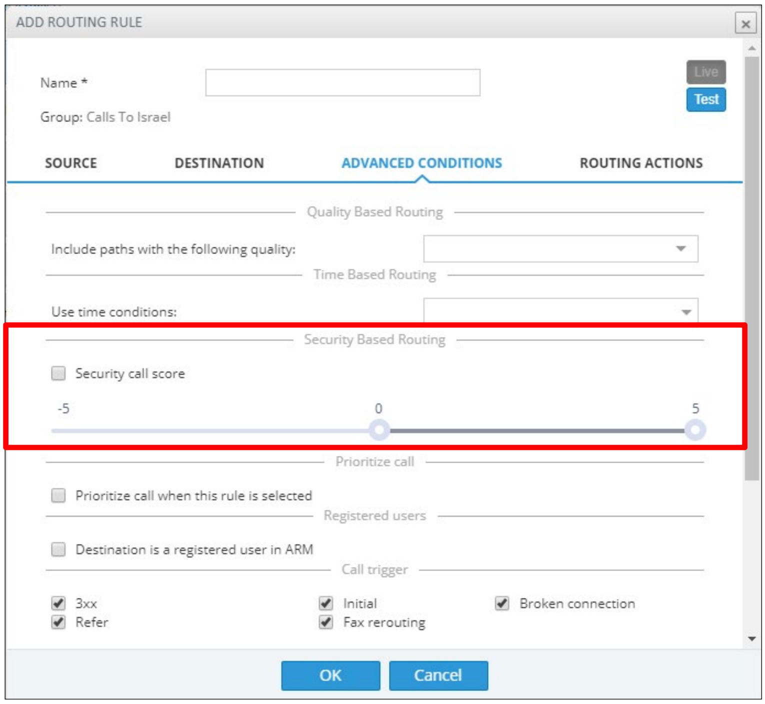
2.1.2 Using a Call's Security Score for a Routing Decision

Security-based routing can be applied to calls that receive a score from SecureLogix's Orchestra One as part of the pre-routing process.

Security-based routing is applied as part of the ARM Routing Rule and must first be enabled when editing the Routing Rule in the 'Advanced Conditions' tab settings.

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**.

Figure 2-4: Security Based Routing - Security Call Score



ADD ROUTING RULE

Name *

Group: Calls To Israel

Quality Based Routing

Include paths with the following quality:

Time Based Routing

Use time conditions:

Security Based Routing

□ Security call score

-5 0 5

Prioritize call

□ Prioritize call when this rule is selected

Registered users

□ Destination is a registered user in ARM

Call trigger

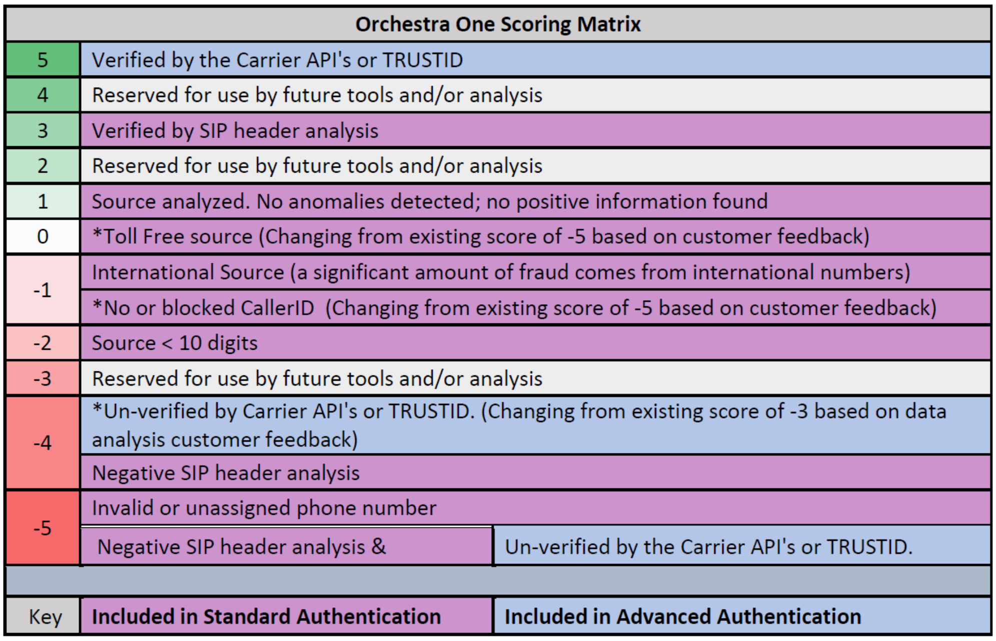
☑ 3xx ☑ Initial ☑ Broken connection

☑ Refer ☑ Fax rerouting

When enabled, the Routing Rule uses the score returned from SecureLogix's Orchestra One as part of the match. The slider is used to control the score threshold. If no score is returned from Orchestra One or the score doesn't match the threshold, the rule won't be matched. In this way, ARM administrators may use the call's security score as part of the routing decision. For example, calls to a specific (security-sensitive) destination with a score of less than **4** can be dropped, while calls to other destinations with a score of **4** can still be routed normally.

The administrator 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.

2.2 Viewing Unselected Rules

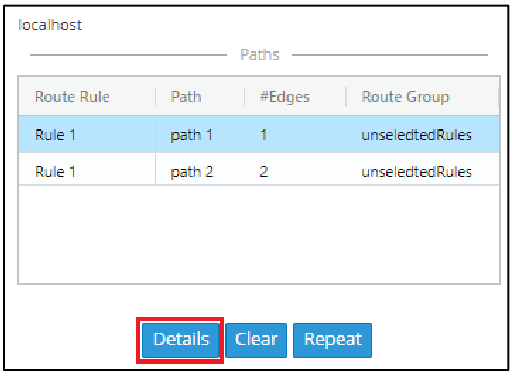
ARM 9.6 provides the capability to view more information about the path selection process. Unselected rules can be viewed both before route and during route.

- Before route: Web services that have been activated but have experienced a problem, an unselected rule will be presented (shown in every Path Details screen (as the pre-manipulations until the current version).
- During route: Appropriate Routing Rules, which were not selected for certain reasons (to be mentioned later), will be presented as unselected rules (shown in the Details window of the next path).

Unselected rules can be viewed in both Test Routes and Calls.

2.2.1 Viewing Unselected Rules in Test-Route

After pressing a path's **Details** button, the Test Route Details screen opens.

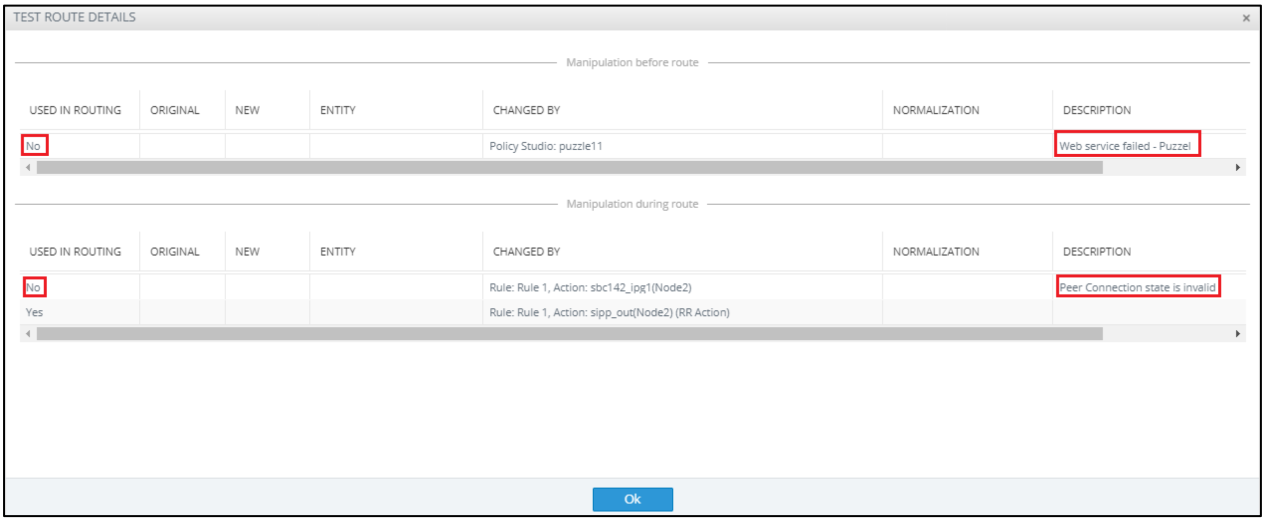


localhost

Paths

Route Rule	Path	#Edges	Route Group
Rule 1	path 1	1	unseledtedRules
Rule 1	path 2	2	unseledtedRules

- Under the 'Manipulation before route' label, unselected rules were added.
- Under the 'Manupulation during route' label, unselected Rules were added.
    - Each path details window shows the Unselected Rules that were 'unselected' until the chosen path.
    - The last line presents the selected path.
- Each Unselected Rule line has a description and is marked with the USED IN ROUTING column ('No').



TEST ROUTE DETAILS

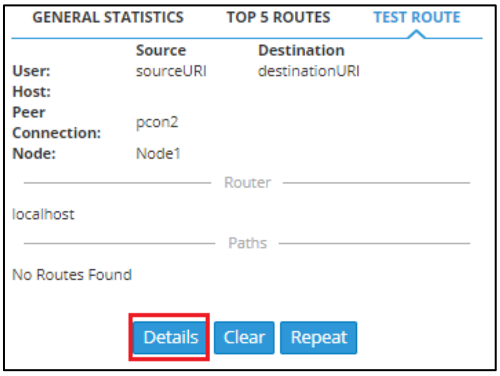
Manipulation before route

USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZATION	DESCRIPTION
No				Policy Studio: puzzle11		Web service failed - Puzzel

Manipulation during route

USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZATION	DESCRIPTION
No				Rule: Rule 1, Action: sbc142_ipg1(Node2)		Peer Connection state is invalid
Yes				Rule: Rule 1, Action: sipp_out(Node2) (RR Action)		

Note: If there are no paths, the **Details** button will be shown, and the Details screen will show all the Unselected Rules with descriptions.



	Source	Destination
User:	sourceURI	destinationURI
Host:		
Peer Connection:	pcon2	
Node:	Node1	

Router

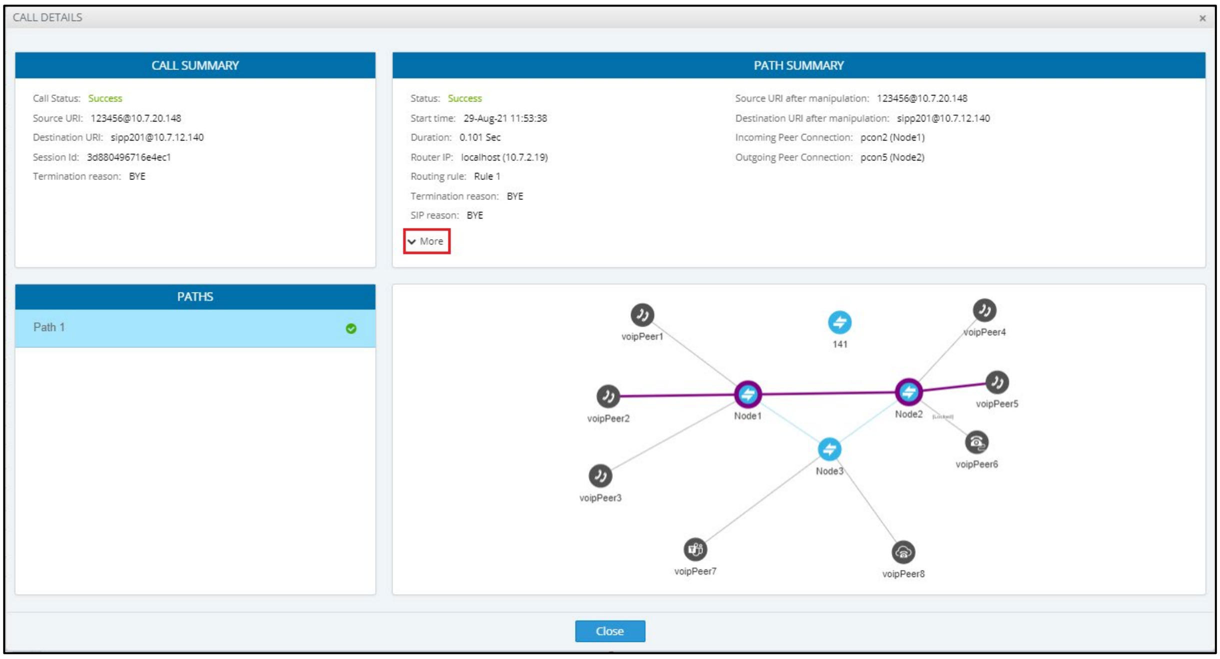
localhost

Paths

No Routes Found

2.2.2 Viewing Unselected Rules in Calls

In the Call Details screen, pressing the **More** button shows the manipulations, including the Unselected Rules.



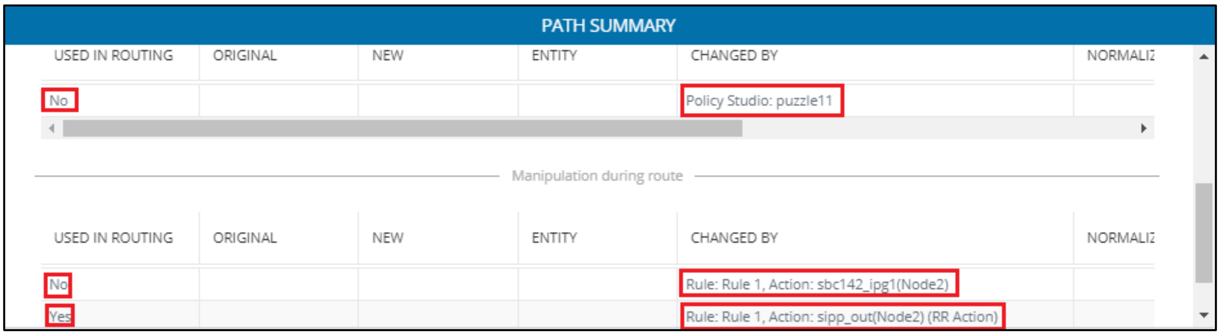
CALL SUMMARY

Call Status: Success
Source URI: 123456@10.7.20.148
Destination URI: sipp201@10.7.12.140
Session Id: 3d880496716e4ec1
Termination reason: BYE

PATH SUMMARY

Status: Success
Start time: 29-Aug-21 11:53:38
Duration: 0.101 Sec
Router IP: localhost (10.7.2.19)
Routing rule: Rule 1
Termination reason: BYE
SIP reason: BYE
More

Source URI after manipulation: 123456@10.7.20.148
Destination URI after manipulation: sipp201@10.7.12.140
Incoming Peer Connection: pcon2 (Node1)
Outgoing Peer Connection: pcon5 (Node2)



PATH SUMMARY

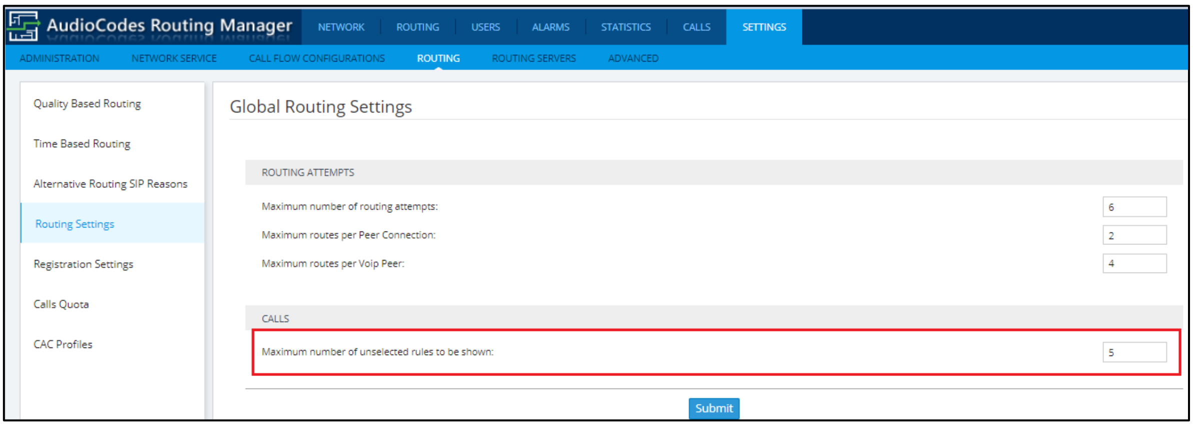
USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZ
No				Policy Studio: puzzle11	

Manipulation during route

USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZ
No				Rule: Rule 1, Action: sbc142_ipg1(Node2)	
Yes				Rule: Rule 1, Action: sipp_out(Node2) (RR Action)	

2.2.3 Configuring Maximum Unselected Rules for Calls

For calls, it’s possible to configure a maximum number of Unselected Rules/Policies. The default value is 5, limited to 25 per call. For **Test Route** the limitation is 100 and not configurable in the ARM GUI.



Global Routing Settings

ROUTING ATTEMPTS

Maximum number of routing attempts: 6

Maximum routes per Peer Connection: 2

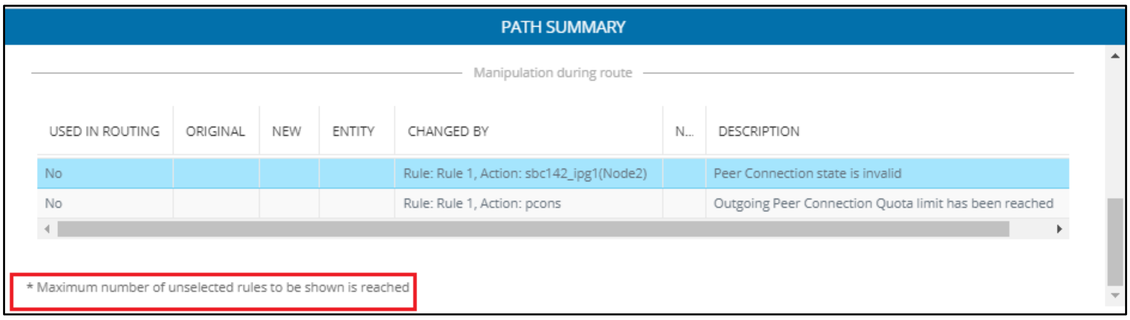
Maximum routes per Voip Peer: 4

CALLS

Maximum number of unselected rules to be shown: 5

2.2.4 Call Details Screen Unselected Rules Additional Information

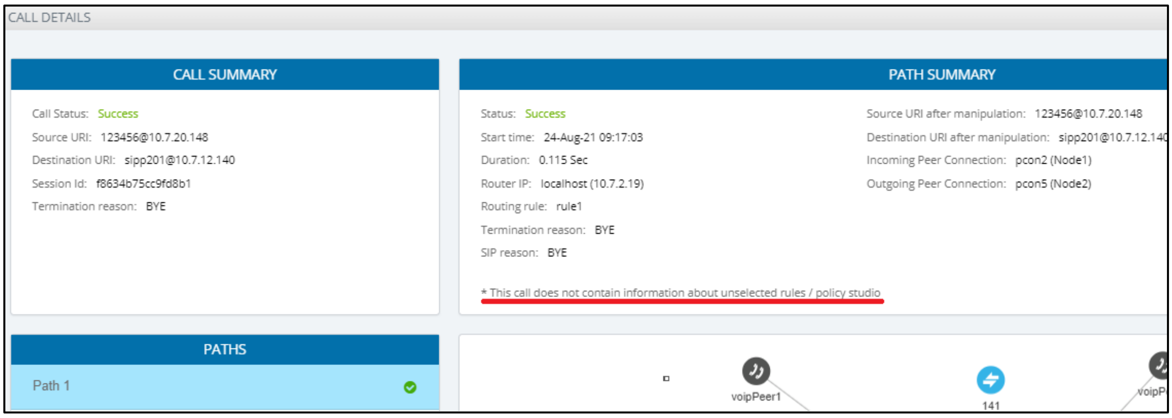
Due to the limitation on the number of Unselected Rules in calls, an indication is shown if the Unselected Rules list is cut and there are more Unselected Rules that are not shown.



USED IN ROUTING	ORIGINAL	NEW	ENTITY	CHANGED BY	N...	DESCRIPTION
No				Rule: Rule 1, Action: sbc142_ipg1(Node2)		Peer Connection state is invalid
No				Rule: Rule 1, Action: pcons		Outgoing Peer Connection Quota limit has been reached

* Maximum number of unselected rules to be shown is reached

For old calls that don’t have the Unselected Rule information, an appropriate message is presented.



Call Status: Success

Source URI: 123456@10.7.20.148

Destination URI: sipp201@10.7.12.140

Session Id: f8634b75cc9fd8b1

Termination reason: BYE

Status: Success

Start time: 24-Aug-21 09:17:03

Duration: 0.115 Sec

Router IP: localhost (10.7.2.19)

Routing rule: rule1

Termination reason: BYE

SIP reason: BYE

* This call does not contain information about unselected rules / policy studio

Source URI after manipulation: 123456@10.7.20.148

Destination URI after manipulation: sipp201@10.7.12.140

Incoming Peer Connection: pcon2 (Node1)

Outgoing Peer Connection: pcon5 (Node2)

2.2.5 Examples of Unselected Rules Reasons

2.2.5.1 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"

2.2.5.2 Before Route (Policy Studio) - Unselected Rules

Web service failed – with proper reason.

2.3 Enhanced Calls View Page Capabilities

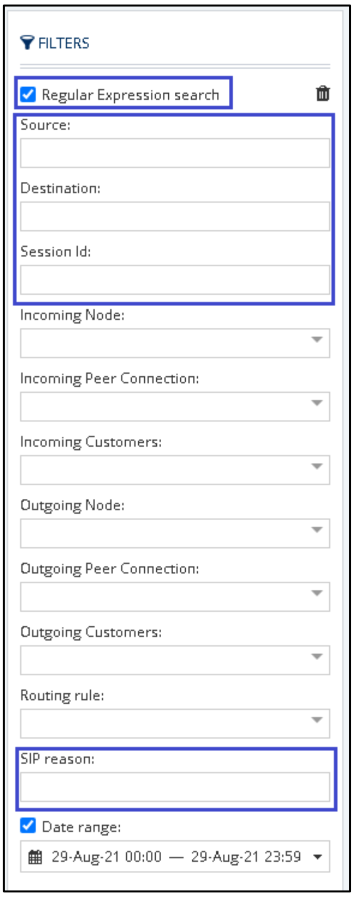
The Calls View page in ARM 9.6 features two new capabilities:

- Some fields allow regular expression which operators can use to further narrow down the search
- Export up to 10000 of the filtered calls to a CSV file

2.3.1 Filtering Calls Using Regular Expression

By selecting the **Regular Expression search** option, operators can use any valid regular express pattern to search the following fields:

- Source
- Destination
- Session ID
- SIP reason



FILTERS

☑ Regular Expression search

Source:

Destination:

Session Id:

Incoming Node:

Incoming Peer Connection:

Incoming Customers:

Outgoing Node:

Outgoing Peer Connection:

Outgoing Customers:

Routing rule:

SIP reason:

☑ Date range:

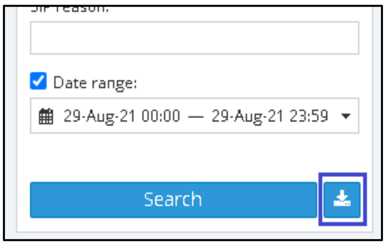
29-Aug-21 00:00 — 29-Aug-21 23:59

Note: Performing a search using regular expression can be extremely slow as a non-prefix (^) search cannot take advantage of the database indexes. The speed depends on the expression and the number of results.

2.3.2 Export Calls to CSV File

Operators can export calls which match the search criteria, by pressing the button adjacent to the **Search** option.

The maximum number of calls which will be exported is 10000.



The CSV file consists of the following columns:

- Session id
- Setup time
- Release time
- Source URI
- Destination URI
- Incoming node
- Incoming peer connection
- Outgoing node
- Outgoing peer connection
- Incoming customer
- Outgoing customer
- Routing rule
- SIP termination reason
- Voice duration (In milliseconds)

2.4 Statistics Thresholding and Alarming

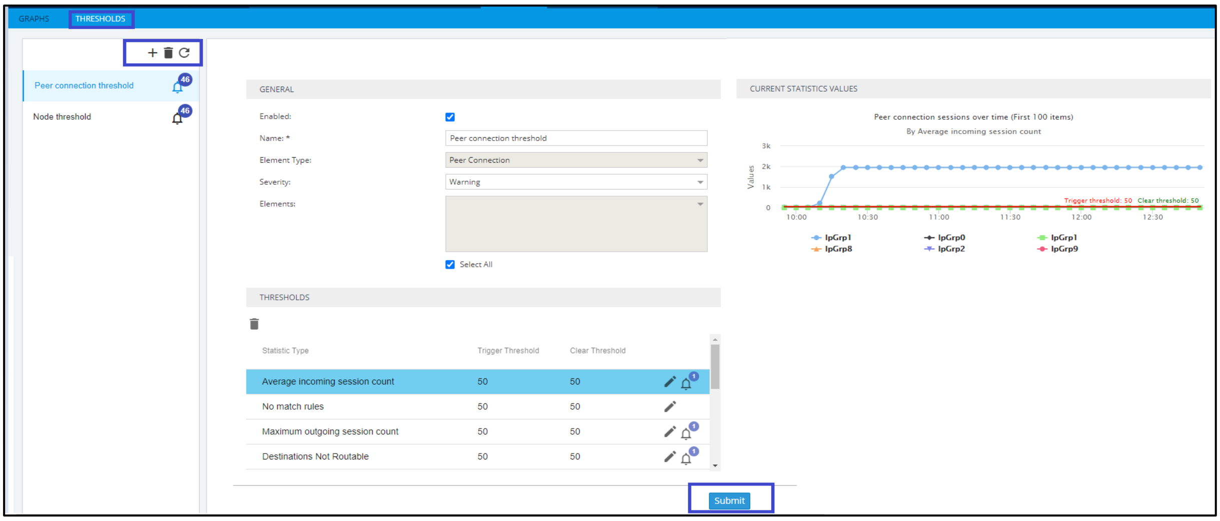
ARM 9.6 provides the capability to define threshold-based alarms based on ARM statistics. Every five minutes, the ARM analyzes defined threshold rules and checks whether the defined thresholds were exceeded every 5 minutes, starting at x2/x7, the last 5 minutes bucket is analyzed, a bucket being a period 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.

2.4.1 Viewing the Threshold Rules Page

A **Thresholds** tab has been added to the Statistics page in the ARM GUI (**Statistics** > **Thresholds**).



GENERAL

Enabled: ☑

Name: * Peer connection threshold

Element Type: Peer Connection

Severity: Warning

Elements:

☑ Select All

THRESHOLDS

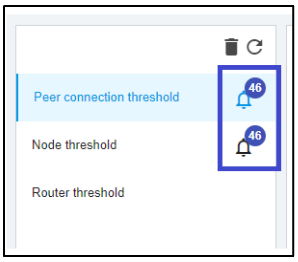
Statistic Type	Trigger Threshold	Clear Threshold
Average incoming session count	50	50
No match rules	50	50
Maximum outgoing session count	50	50
Destinations Not Routable	50	50

The page allows **Add**, **Edit**, **Delete** and **Refresh** actions.

In the left pane, operators can add a new threshold **(**by clicking the **+** icon), delete an existing threshold (by selecting the relevant threshold rule and then clicking the trash icon) or refresh all thresholds (by clicking the refresh icon).

To edit an existing threshold, operators click a specific threshold, edit it, and then click the **Submit** button.

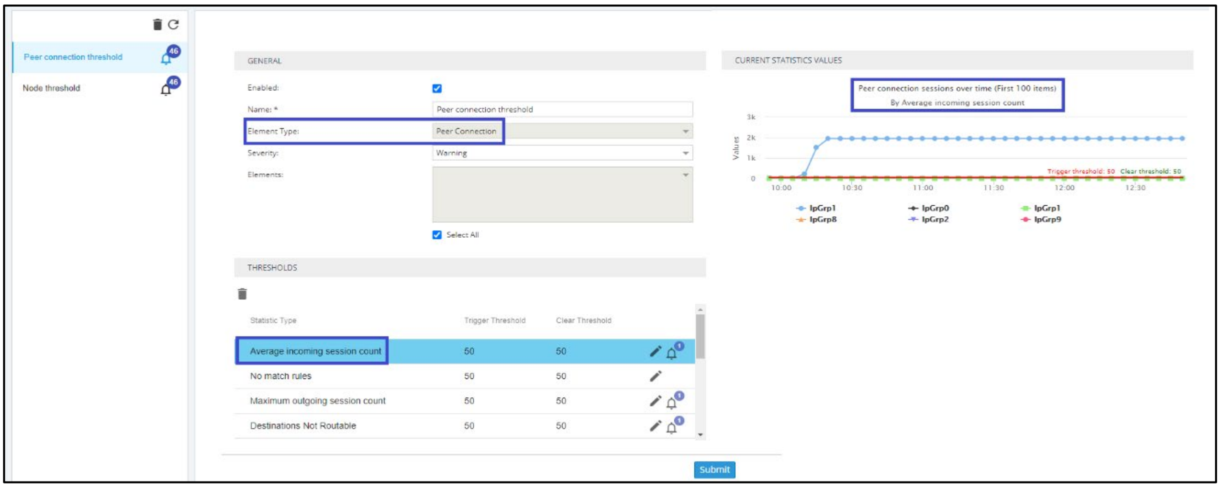
If there are alarms related to the threshold rule, an icon displaying the alarms count is shown.



In the example shown in the preceding figure, there are currently 46 alarms related to ‘Peer connection threshold’ and ‘Node threshold’, and no alarms related to ‘Router threshold’.

In the right pane, operators can 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 example shown in the following figure, the chart represents Peer Connections by average incoming session count for the last three hours.



GENERAL

Enabled: ☑

Name: * Peer connection threshold

Element Type: Peer Connection

Severity: Warning

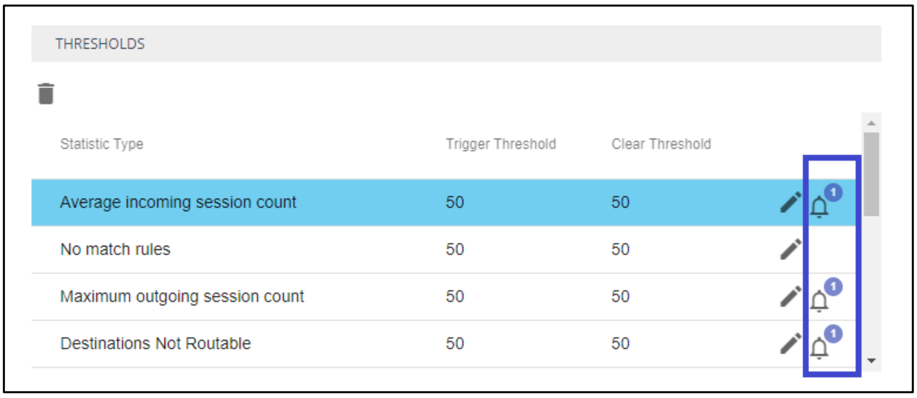
Elements:

☑ Select All

THRESHOLDS

Statistic Type	Trigger Threshold	Clear Threshold	
Average incoming session count	50	50	1
No match rules	50	50	
Maximum outgoing session count	50	50	1
Destinations Not Routable	50	50	1

In the ‘Thresholds’ section, the operator can see how many alarms exist for each statistic type.

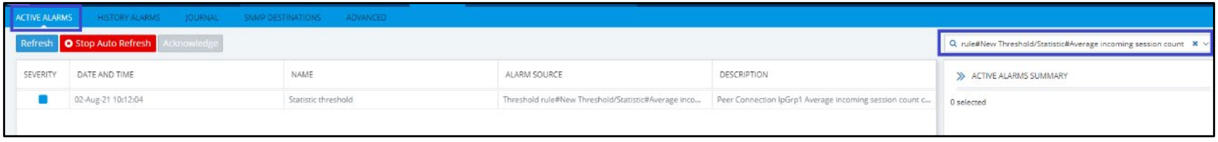


THRESHOLDS

Statistic Type	Trigger Threshold	Clear Threshold	
Average incoming session count	50	50	1
No match rules	50	50	
Maximum outgoing session count	50	50	1
Destinations Not Routable	50	50	1

In the example here, there is one alarm for ‘Average incoming session count’ and zero alarms for ‘No match rules’.

Clicking the icon enables operators to navigate to the **Alarms** page filtered by the relevant alarms.



rule#New Threshold/Statistic#Average incoming session count

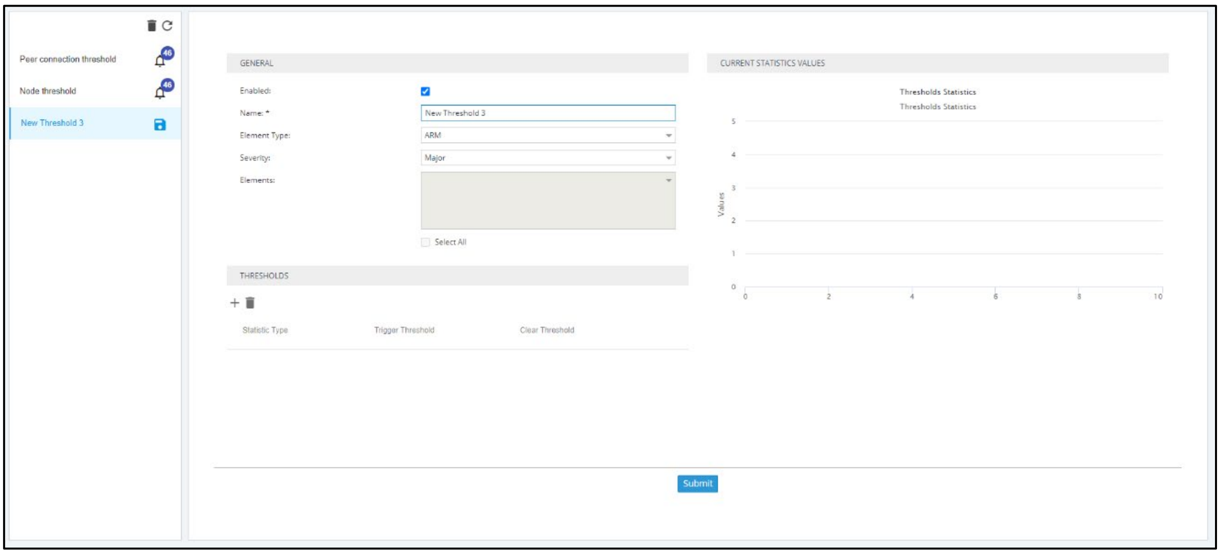
SEVERITY	DATE AND TIME	NAME	ALARM SOURCE	DESCRIPTION
■	02-Aug-21 10:12:04	Statistic threshold	Threshold rule#New Threshold/Statistic#Average inco...	Peer Connection IpGrp1 Average incoming session count c...

ACTIVE ALARMS SUMMARY

0 selected

2.4.2 Adding a New Threshold Rule

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



Peer connection threshold 46

Node threshold 46

New Threshold 3

GENERAL

Enabled: ☑

Name: * New Threshold 3

Element Type: ARM

Severity: Major

Elements:

□ Select All

THRESHOLDS

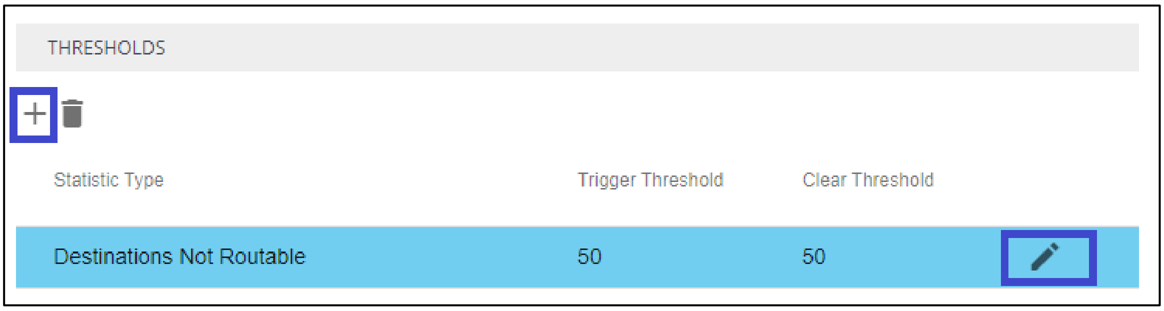
Statistic Type	Trigger Threshold	Clear Threshold

To save the changes after defining the threshold, the operator must click the **Submit** button in the right pane.

Operators must provide the following information:

Under the 'General' section of the page:

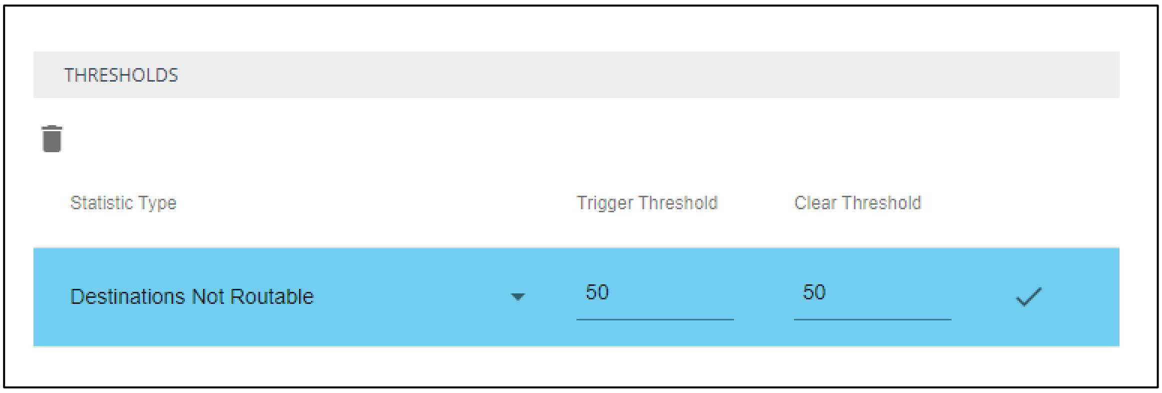
- **Enabled**. If unchecked, no alarms will be triggered, and the rule will be ignored.
- **Name**. Mandatory. Unique name of the 'threshold'.
- **Element type**. Can be:
  - ARM
  - Router
  - Node
  - Connection
  - Peer Connection
  - Routing Rule
  - Routing Group
  - Customer
  - VoIP Peer
- **Severity**.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


THRESHOLDS

Statistic Type	Trigger Threshold	Clear Threshold
Destinations Not Routable	50	50

Under the ‘Thresholds’ section of the page:

Clicking the **+** icon adds a new entry with default values. To edit the values, the operator clicks the edit icon.


THRESHOLDS

Statistic Type	Trigger Threshold	Clear Threshold	
Destinations Not Routable	50	50	✓

For each threshold, operators must 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.

2.4.3 Editing a Threshold Rule

The option to edit a ‘Threshold rule’ entity allows the operator to change the same attributes that are provided in the **Add Threshold** action, excluding element type.

To edit a threshold rule, the operator clicks the relevant rule, edits it, and then clicks **Submit**.

If during **Edit** the operator disables the threshold, related alarms will be cleared, and this threshold rule will be unchecked until it will be changed back to enable.

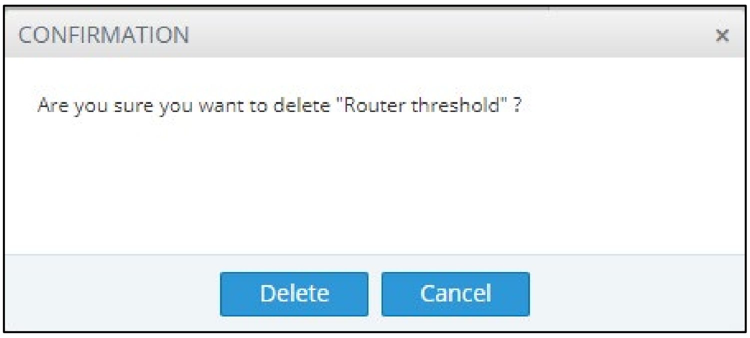
If during **Edit** the operator deletes a statistic threshold, related alarms will be cleared.

If during **Edit** the operator edits the ‘trigger threshold’ or ‘clear threshold’ of statistic threshold, alarms will be raised / cleared in the next ARM checking time.

If during **Edit** the operator deletes elements, alarms related to the deleted elements will be cleared.

2.4.4 Deleting a Threshold Rule

The action to **Delete** a ‘Threshold rule’ (indicated by the trash icon) is used to delete an existing ‘Threshold rule’. The operator is prompted for confirmation before the delete action:



CONFIRMATION

Are you sure you want to delete "Router threshold" ?

Alarms related to the deleted threshold rule are cleared.

2.5 Configuring Certificates

2.5.1 Configuring Server Certificates

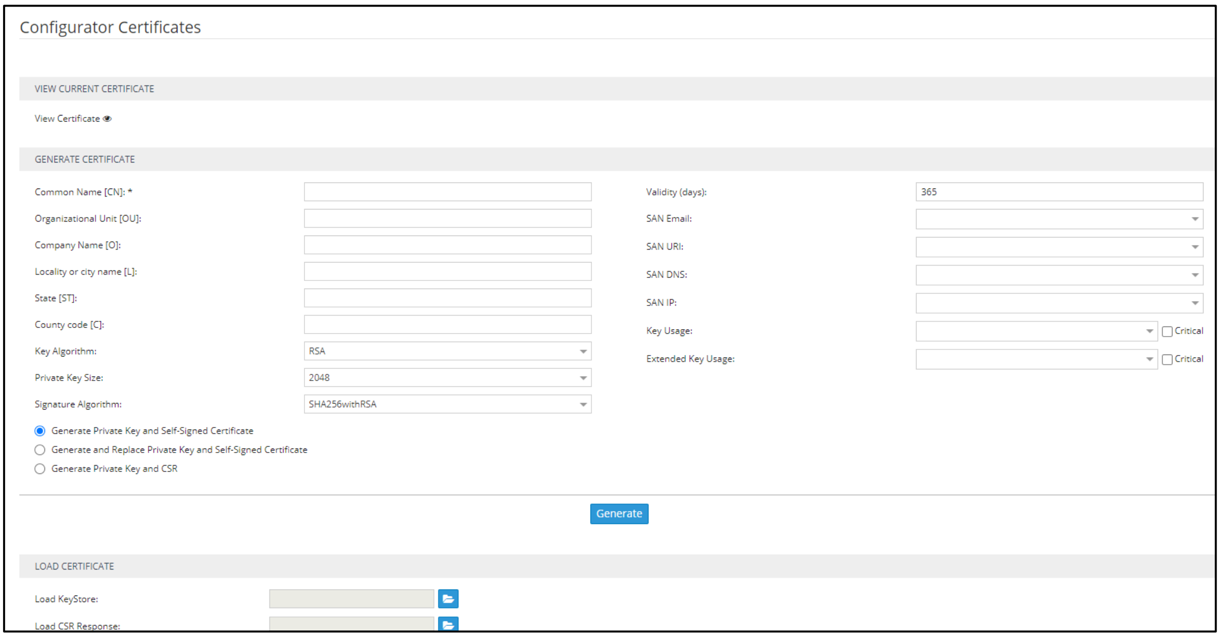
Before ARM 9.6, operators needed to manually run a procedure that required using Java Keytool and other tools such as OpenSSL, to change the default certificates. Operators needed to perform the same process, moreover, in both the Configurator and the Routers. In ARM 9.6, this process is simplified; operators can now change the server certificates of both the Configurator and the Routers from the ARM GUI.

2.5.2 Configuring a Configurator Certificate

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

2.5.2.1 Viewing a Certificate

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



Configurator Certificates

VIEW CURRENT CERTIFICATE

View Certificate

GENERATE CERTIFICATE

Common Name [CN]: *

Organizational Unit [OU]:

Company Name [O]:

Locality or city name [L]:

State [ST]:

County code [C]:

Key Algorithm: RSA

Private Key Size: 2048

Signature Algorithm: SHA256withRSA

Validity (days): 365

SAN Email:

SAN URI:

SAN DNS:

SAN IP:

Key Usage: □ Critical

Extended Key Usage: □ Critical

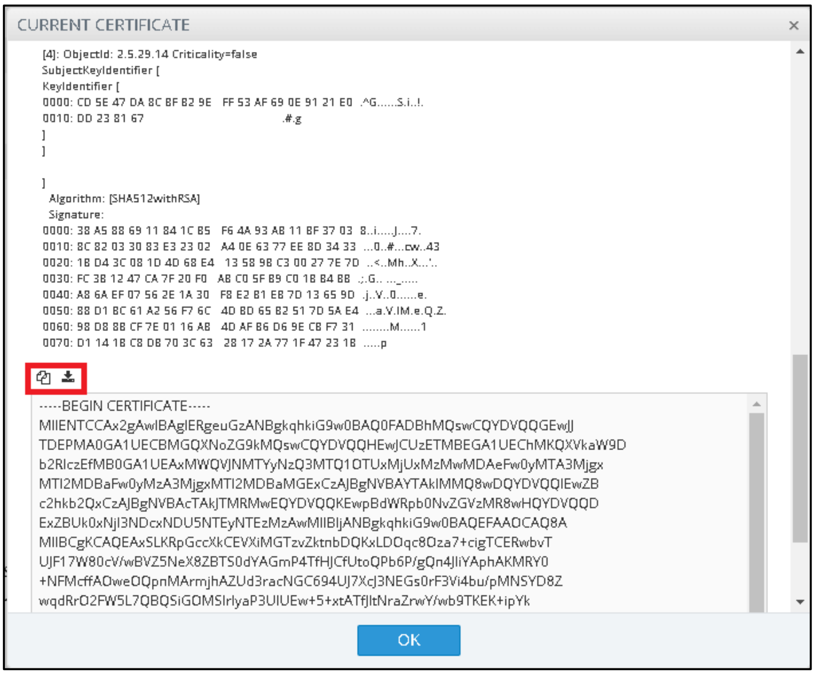
● Generate Private Key and Self-Signed Certificate
○ Generate and Replace Private Key and Self-Signed Certificate
○ Generate Private Key and CSR

LOAD CERTIFICATE

Load KeyStore:

Load CSR Response:

Operators can download or copy the PEM formatted certificate by pressing one of the icons in the Current Certificate view.



```
[4]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: CD 5E 47 DA 8C BF B2 9E   FF 53 AF 69 0E 91 21 E0  .^G......S.i..!.
0010: DD 23 81 67                                        .#.g
]
]

]
  Algorithm: [SHA512withRSA]
  Signature:
0000: 38 A5 88 69 11 84 1C B5   F6 4A 93 AB 11 BF 37 03  8..i.....J....7.
0010: 8C 82 03 30 83 E3 23 02   A4 0E 63 77 EE 8D 34 33  ...0..#...cw..43
0020: 1B D4 3C 08 1D 4D 68 E4   13 58 9B C3 00 27 7E 7D  ..<..Mh..X...'..
0030: FC 3B 12 47 CA 7F 20 F0   AB C0 5F B9 C0 1B B4 BB  .;.G.. ..._.....
0040: A8 6A EF 07 56 2E 1A 30   F8 E2 B1 EB 7D 13 65 9D  .j..V..0......e.
0050: 88 D1 BC 61 A2 56 F7 6C   4D BD 65 B2 51 7D 5A E4  ...a.V.lM.e.Q.Z.
0060: 98 D8 8B CF 7E 01 16 AB   4D AF B6 D6 9E CB F7 31  ........M......1
0070: D1 14 1B C8 DB 70 3C 63   28 17 2A 77 1F 47 23 1B  .....p
```

-----BEGIN CERTIFICATE-----
MIIENTCCAx2gAwIBAgIERgeuGzANBgkqhkiG9w0BAQ0FADBhMQswCQYDVQQGEwJJ
TDEPMA0GA1UECBMGQXNoZG9kMQswCQYDVQQHEwJCUzETMBEGA1UEChMKQXVkaW9D
b2RlczEfMB0GA1UEAxMWQVJNMTYyNzQ3MTQ1OTUxMjUxMzMwMDAeFw0yMTA3Mjgx
MTI2MDBaFw0yMzA3MjgxMTI2MDBaMGExCzAJBgNVBAYTAkIMMQ8wDQYDVQQIEwZB
c2hkb2QxCzAJBgNVBAcTAkJTMRMwEQYDVQQKEwpBdWRpb0NvZGVzMR8wHQYDVQQD
ExZBUk0xNjI3NDcxNDU5NTEyNTEzMzAwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAxSLKRpGccXkCEVXiMGTzvZktnbDQKxLDOqc8Oza7+cigTCERwbvT
UJF17W80cV/wBVZ5NeX8ZBTS0dYAGmP4TfHJCfUtoQPb6P/gQn4JliYAphAKMRY0
+NFMcffAOweOQpnMArmjhAZUd3racNGC694UJ7XcJ3NEGs0rF3Vi4bu/pMNSYD8Z
wqdRrO2FW5L7QBQSiGOMSIrlyaP3UlUEw+5+xtATfJltNraZrwY/wb9TKEK+ipYk

2.5.2.2 Generating a Self-Signed Certificate

By selecting the **Generate Private Key and Self-Signed Certificate** option, operators 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.

The following fields are common for all three operations:

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

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

Organization unit, Company name, locality, State, Country code.

Key Algorithm. Operators can control whether the private / public key is RSA or EC (Elliptic curve); the default is RSA

Private key size. Operators can 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. Operators can 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.

The SAN (Subject Alternative Name). 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.

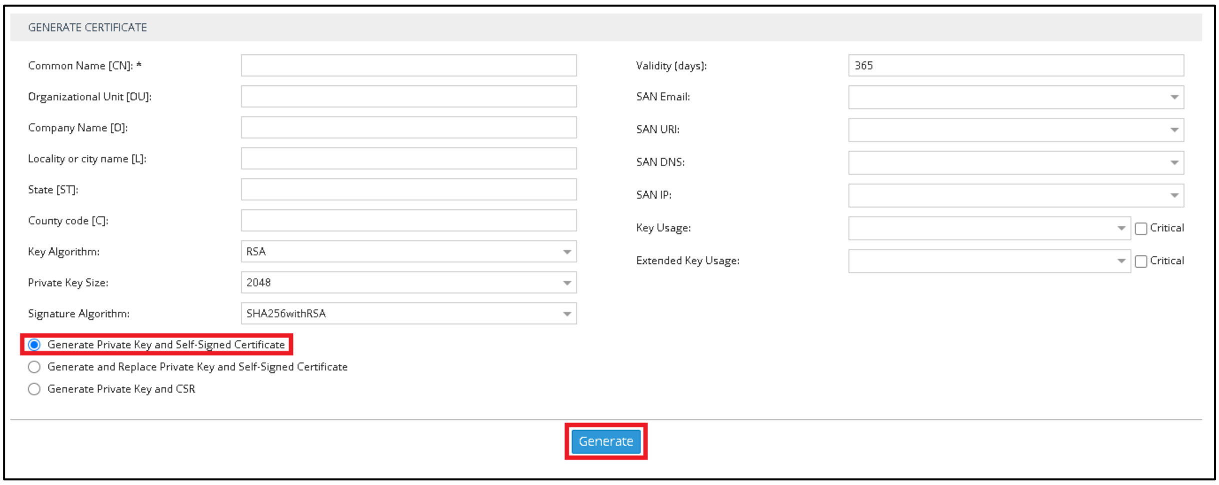
Other SAN fields can be used (though they are less useful for ARM) such as Email and URI.

Key Usage (KUEs). Operators can 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.

> **Note:** 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.



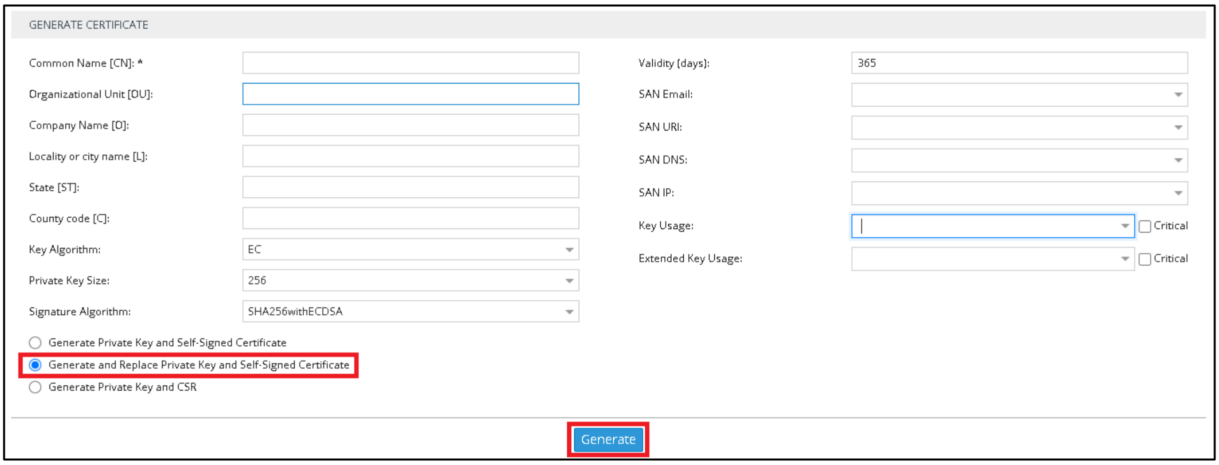
GENERATE CERTIFICATE

Common Name [CN]: *		Validity (days):	365
Organizational Unit [OU]:		SAN Email:	
Company Name [O]:		SAN URI:	
Locality or city name [L]:		SAN DNS:	
State [ST]:		SAN IP:	
County code [C]:		Key Usage:	□ Critical
Key Algorithm:	RSA	Extended Key Usage:	□ Critical
Private Key Size:	2048		
Signature Algorithm:	SHA256withRSA		

● Generate Private Key and Self-Signed Certificate
○ Generate and Replace Private Key and Self-Signed Certificate
○ Generate Private Key and CSR

2.5.2.3 Generating and Replacing a Private Key and Self-Signed Certificate

By selecting the **Generate and Replace Private Key and Self-Signed Certificate** option, operators can generate a new self-signed certificate and replace the currently loaded certificate of the Configurator. This option also triggers a reload of the Configurator's port 443 (TLS) configuration.



GENERATE CERTIFICATE

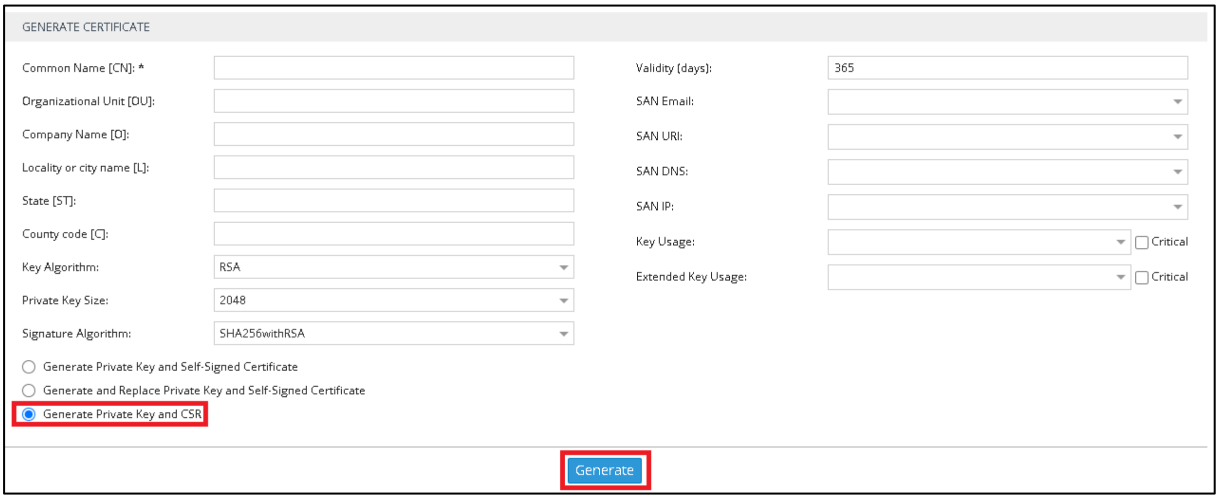
Common Name [CN]: *		Validity (days):	365
Organizational Unit [OU]:		SAN Email:	
Company Name [O]:		SAN URI:	
Locality or city name [L]:		SAN DNS:	
State [ST]:		SAN IP:	
County code [C]:		Key Usage:	□ Critical
Key Algorithm:	EC	Extended Key Usage:	□ Critical
Private Key Size:	256		
Signature Algorithm:	SHA256withECDSA		

○ Generate Private Key and Self-Signed Certificate
● Generate and Replace Private Key and Self-Signed Certificate
○ Generate Private Key and CSR

2.5.2.4 Generating a Private Key, Self-Signed Certificate and CSR

By selecting the **Generate Private Key and CSR** option, 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.



GENERATE CERTIFICATE

Common Name [CN]: *		Validity [days]:	365
Organizational Unit [OU]:		SAN Email:	
Company Name [O]:		SAN URI:	
Locality or city name [L]:		SAN DNS:	
State [ST]:		SAN IP:	
County code [C]:		Key Usage:	□ Critical
Key Algorithm:	RSA	Extended Key Usage:	□ Critical
Private Key Size:	2048		
Signature Algorithm:	SHA256withRSA		

○ Generate Private Key and Self-Signed Certificate

○ Generate and Replace Private Key and Self-Signed Certificate

● Generate Private Key and CSR

2.5.2.5 Loading a Certificate

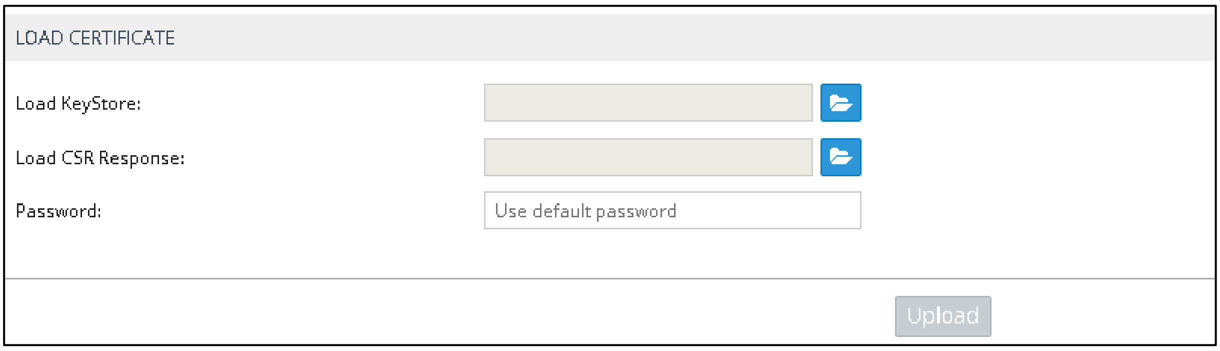
Operators can either load their own JKS (Java KeyStore) file with the private key and the certificate, or the KeyStore file which was generated using one of the options through the ARM GUI.

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

Note: 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.

Note: 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.



LOAD CERTIFICATE

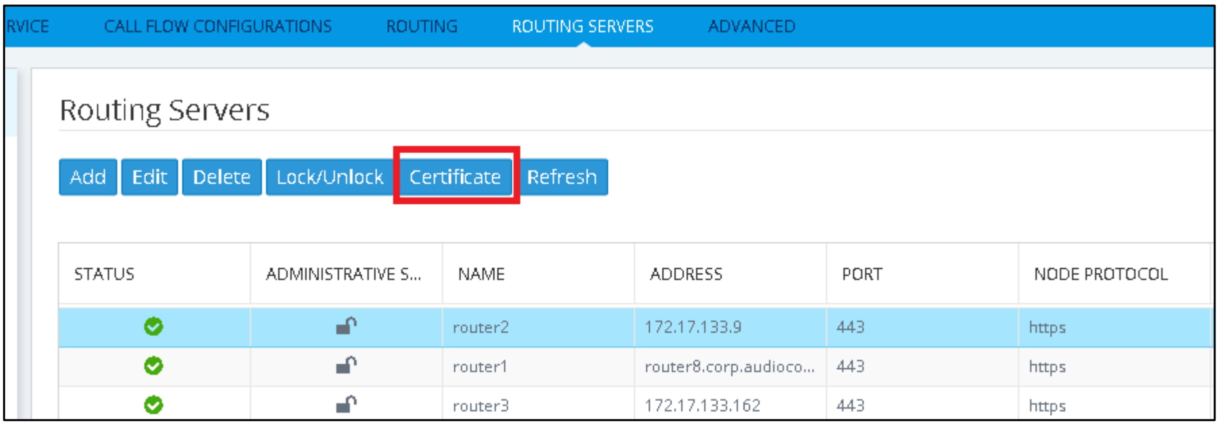
Load KeyStore:	
Load CSR Response:	
Password:	Use default password

2.5.3 Configuring a Router Certificate

To facilitate management, the same certificate operations can be performed on each Router.

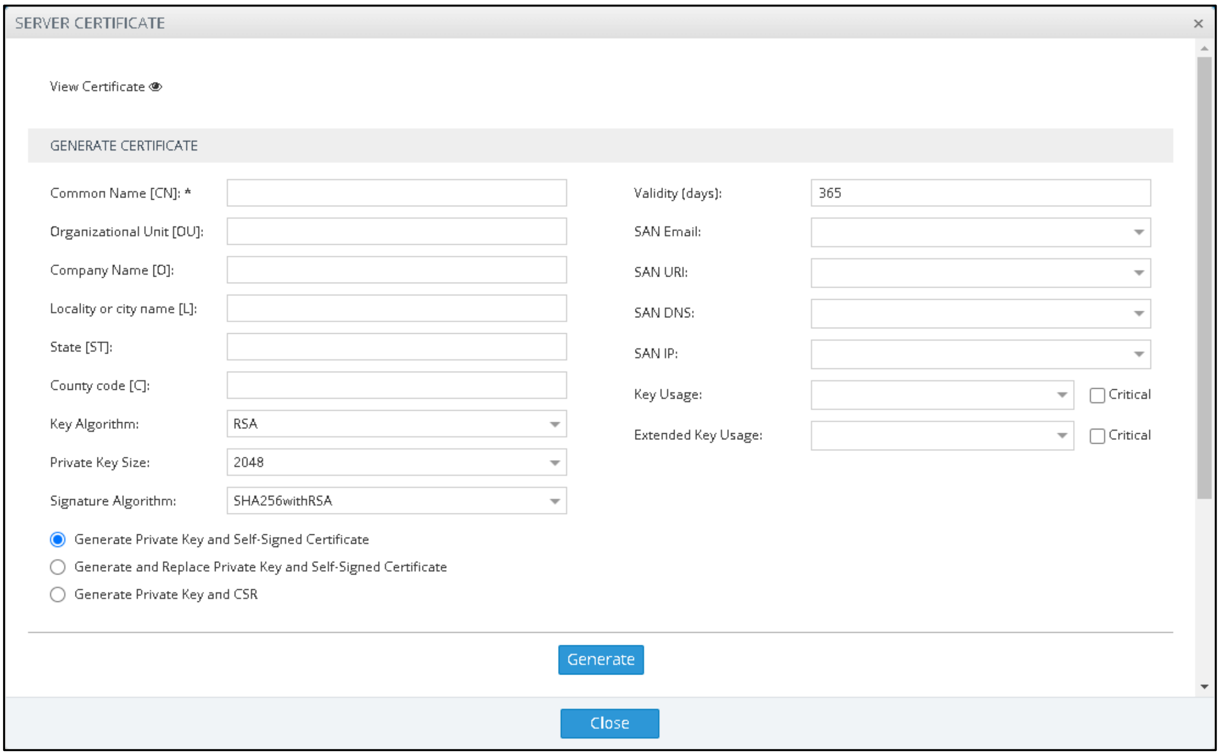
2.5.3.1 Viewing a Router Certificate

After selecting a Router in the Routing Servers page and then pressing the **Certificate** button, the Server Certificate screen opens displaying the same options described in Section 2.5.2, Configuring a Configurator Certificate.



Routing Servers

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



SERVER CERTIFICATE

GENERATE CERTIFICATE

Common Name [CN]: *		Validity (days):	365
Organizational Unit [OU]:		SAN Email:	
Company Name [O]:		SAN URI:	
Locality or city name [L]:		SAN DNS:	
State [ST]:		SAN IP:	
County code [C]:		Key Usage:	□ Critical
Key Algorithm:	RSA	Extended Key Usage:	□ Critical
Private Key Size:	2048		
Signature Algorithm:	SHA256withRSA		

● Generate Private Key and Self-Signed Certificate
○ Generate and Replace Private Key and Self-Signed Certificate
○ Generate Private Key and CSR

Note:

- 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.

2.6 Delayed Alternative Routing

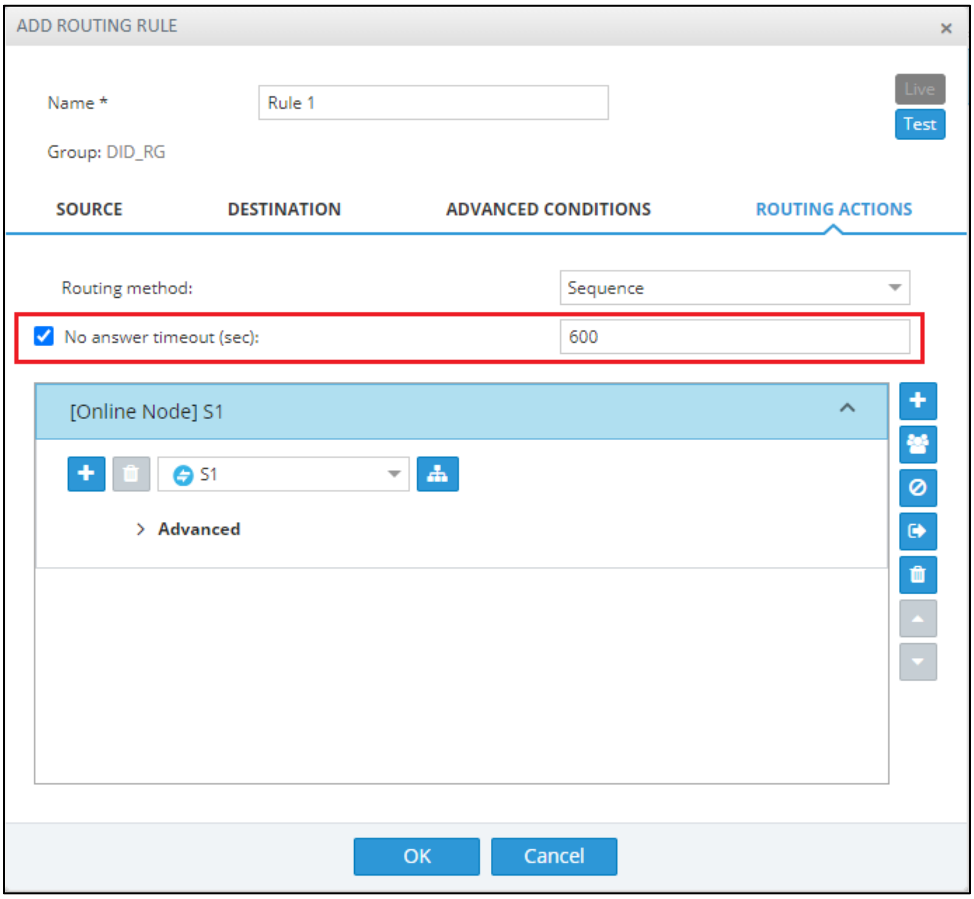
The ARM 9.6 allows management of the SBC/Gateway’s timeout feature for no answer. A new field ‘No answer timeout’ has been added to the Add/Edit Routing Rule screen (see the figure below). The new field controls the SBC/Gateway ‘No answer timeout’.

No answer timeout. If the called party does not answer the call within this given interval, the device disconnects the session.

- If the option is selected, the device will use the value defined in the field for the timeout.
- If the option is cleared, the device will use the default value.

Note: This 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.



Name * Rule 1

Group: DID_RG

Routing method: Sequence

☑ No answer timeout (sec): 600

S1

Note: If the SBC does not support the feature, the default value will be used.

2.7 Centos Stream 8

ARM 9.6 is provided with the CentOS Stream 8 operating system. All ARM elements (ARM Configurator and ARM Router) are now based on this distribution.

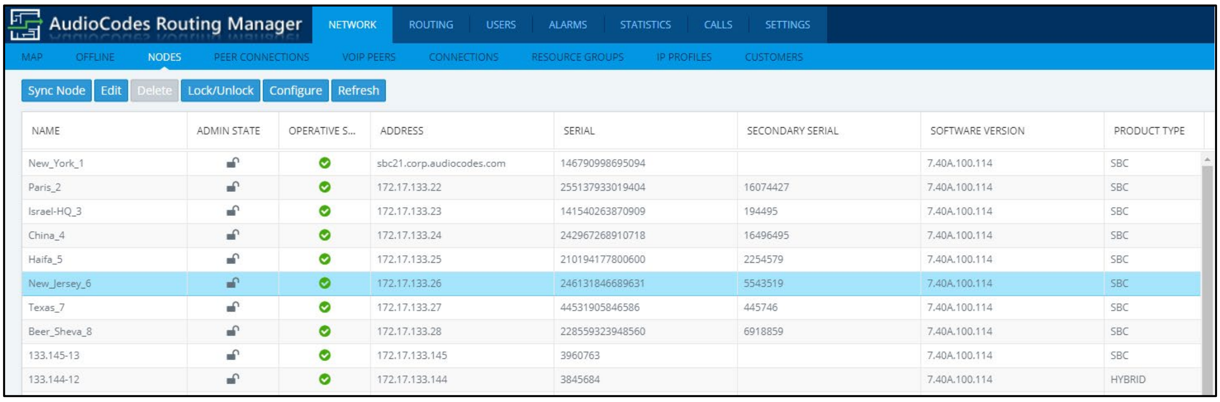
The transition to this version was due to the reason that the previous ARM version was based on CentOS 8, which becomes End of Life at the end of 2021.

The ARM upgrade process, which contains the migration to CentOS Stream 8, remains (as it was in previous versions) simple for operators.

2.8 Support for up to 150 Nodes and a Nodes Page

Product popularity and extensive global deployments necessitated support for more nodes (SBCs and Media Gateways) in ARM Topology and Routing. Some distributed enterprises with multiple branches have required more than 100 nodes to be supported in their deployments. ARM 9.6 increases the number of supported nodes to up to 150 SBCs and/or Media Gateways.

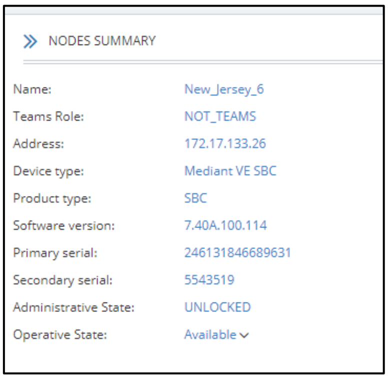
ARM 9.6 also supports a Nodes page (**Network** > **Nodes**), shown in the next figure, to facilitate more convenient management of high numbers of nodes for operators.



NAME	ADMIN STATE	OPERATIVE S...	ADDRESS	SERIAL	SECONDARY SERIAL	SOFTWARE VERSION	PRODUCT TYPE
New_York_1	🔓	✓	sbc21.corp.audiocodes.com	146790998695094		7.40A.100.114	SBC
Paris_2	🔓	✓	172.17.133.22	255137933019404	16074427	7.40A.100.114	SBC
Israel-HQ_3	🔓	✓	172.17.133.23	141540263870909	194495	7.40A.100.114	SBC
China_4	🔓	✓	172.17.133.24	242967268910718	16496495	7.40A.100.114	SBC
Haifa_5	🔓	✓	172.17.133.25	210194177800600	2254579	7.40A.100.114	SBC
New_Jersey_6	🔓	✓	172.17.133.26	246131846689631	5543519	7.40A.100.114	SBC
Texas_7	🔓	✓	172.17.133.27	44531905846586	445746	7.40A.100.114	SBC
Beer_Sheva_8	🔓	✓	172.17.133.28	228559323948560	6918859	7.40A.100.114	SBC
133.145-13	🔓	✓	172.17.133.145	3960763		7.40A.100.114	SBC
133.144-12	🔓	✓	172.17.133.144	3845684		7.40A.100.114	HYBRID

The Nodes page provides (a subset of) the relevant functionalities that already exist for nodes in the Network Map page, but in table view/format, viz., Sync Node, Edit, Delete, Lock/Unlock, and Configure.

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



Name: New_Jersey_6
Teams Role: NOT_TEAMS
Address: 172.17.133.26
Device type: Mediant VE SBC
Product type: SBC
Software version: 7.40A.100.114
Primary serial: 246131846689631
Secondary serial: 5543519
Administrative State: UNLOCKED
Operative State: Available

2.9 Sets of SIP Reasons for Alternative Routing

Before ARM 9.6, the SIP reasons for call re-routing were globally configured for all ARM-routed calls. The settings were in Settings > Routing > Alternative Routing SIP Reasons. Currently, if a certain SIP reason in this table is activated, the ARM tries to perform alternative routing if this SIP reason is returned at the initial routing failure.

However, customers 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.

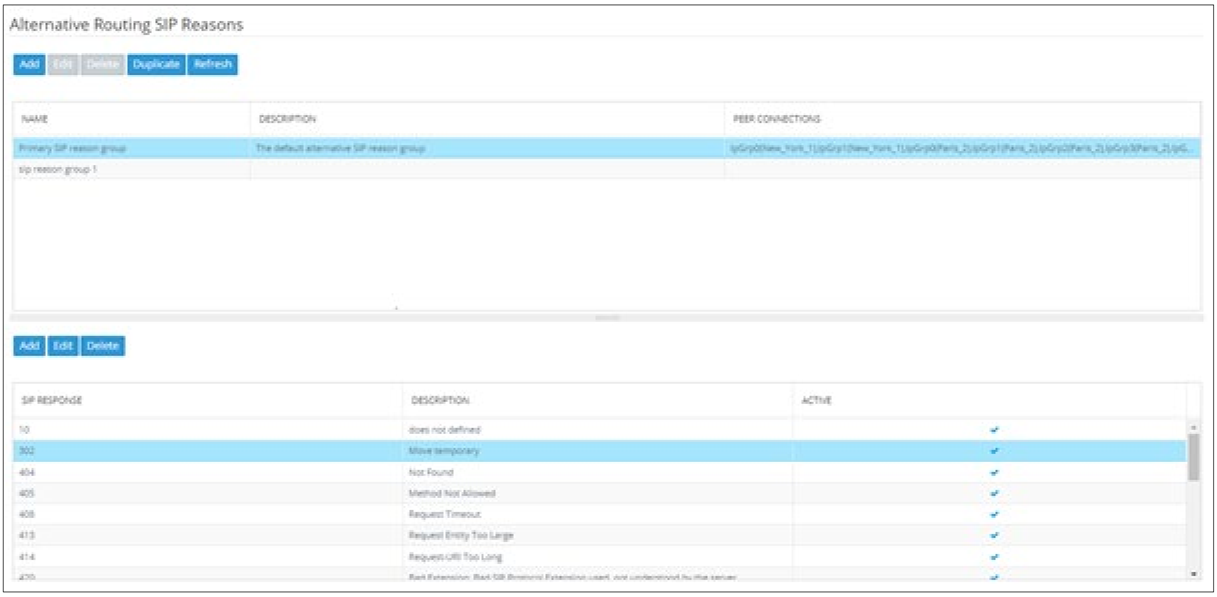
ARM 9.6 provides this functionality. Global settings (Settings > Routing > Alternative Routing SIP Reasons) are still supported and currently they provide the default behavior. Over and above this, operators can provide a different set of SIP reasons for alternative routing per Peer Connection.

The settings are provided in the same place: Settings > Routing > Alternative Routing SIP Reasons. But ARM 9.6 features a table of ‘SIP reasons groups’. Several ‘SIP reasons groups’ can be defined in the ARM. By default, there is a ‘Primary SIP reason group’ attached and activated for the entire ARM (for all ARM Peer Connections).

Each group has the following properties:

- Name
- Description
- Peer Connection that contains the ‘SIP reason group’.

The default ‘SIP reason group’ cannot be deleted. 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).



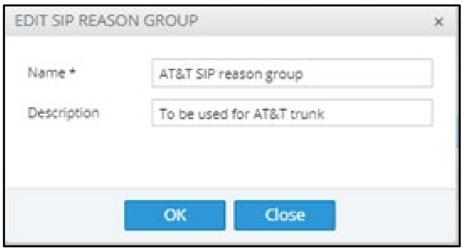
NAME	DESCRIPTION	PEER CONNECTIONS
Primary SIP reason group	The default alternative SIP reason group	IpGrp0(New_York_1);IpGrp1(New_York_1);IpGrp0(Paris_2);IpGrp1(Paris_2);IpGrp2(Paris_2);IpGrp3(Paris_2);IpG...
sip reason group 1		

SIP RESPONSE	DESCRIPTION	ACTIVE
10	does not defined	✓
302	Move temporary	✓
404	Not Found	✓
405	Method Not Allowed	✓
408	Request Timeout	✓
413	Request Entity Too Large	✓
414	Request-URI Too Long	✓
420	Bad Extension. Bad SIP Protocol Extension used, not understood by the server	✓

The operator can:

- Add a new group (with an empty SIP reasons table)
- Duplicate group
  - The operator should change the name of the group.
  - The operator can view the SIP reasons table and select/unselect the values.
- Edit group
  - The operator can edit the name and description of the group.
  - Delete group
  - Refresh

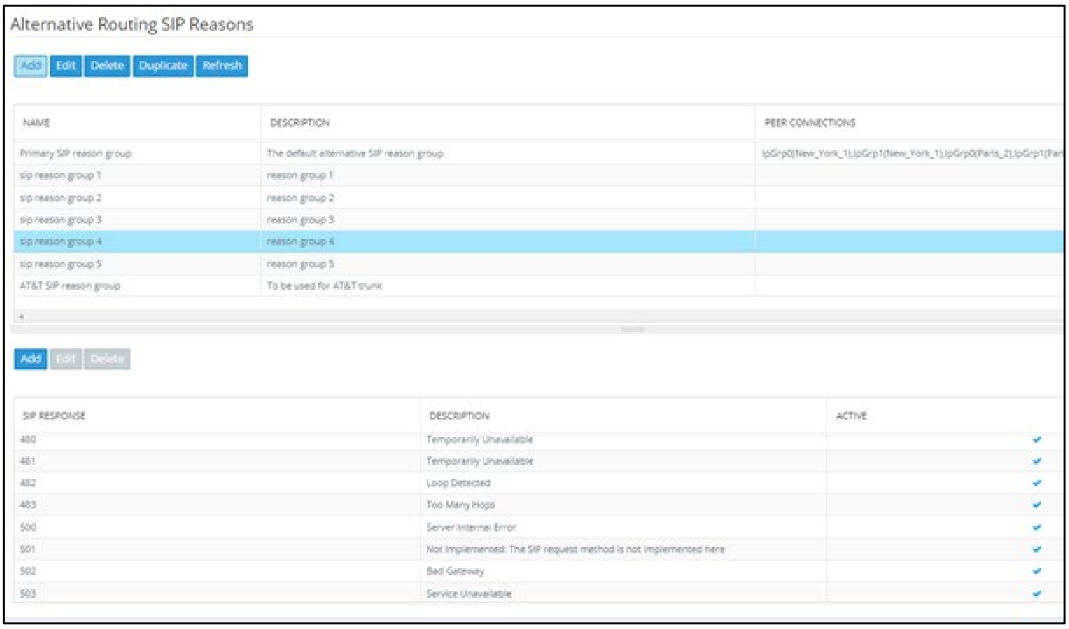
When adding/editing a new group, the operator should provide a name for the group and an optional description:



EDIT SIP REASON GROUP

Name *	AT&T SIP reason group
Description	To be used for AT&T trunk

When a specific group is selected, the group's SIP reason table is displayed and can be edited:

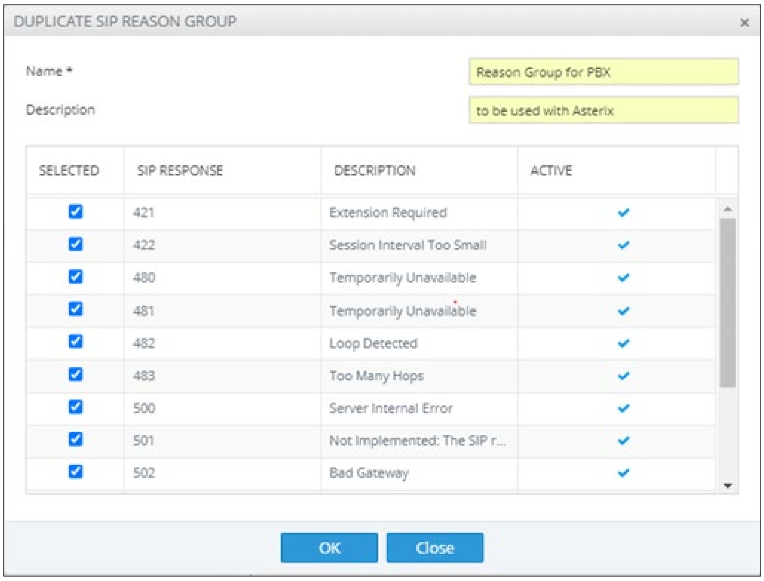


Alternative Routing SIP Reasons

NAME	DESCRIPTION	PEER CONNECTIONS
Primary SIP reason group	The default alternative SIP reason group	IpGrp0(New_York_1),IpGrp1(New_York_1),IpGrp0(Paris_2),IpGrp1(Par
sip reason group 1	reason group 1	
sip reason group 2	reason group 2	
sip reason group 3	reason group 3	
sip reason group 4	reason group 4	
sip reason group 5	reason group 5	
AT&T SIP reason group	To be used for AT&T trunk	

SIP RESPONSE	DESCRIPTION	ACTIVE
480	Temporarily Unavailable	✓
481	Temporarily Unavailable	✓
482	Loop Detected	✓
483	Too Many Hops	✓
500	Server Internal Error	✓
501	Not Implemented: The SIP request method is not implemented here	✓
502	Bad Gateway	✓
503	Service Unavailable	✓

When duplicating an existing SIP reason group, the operator must provide a new unique name and an optional description:



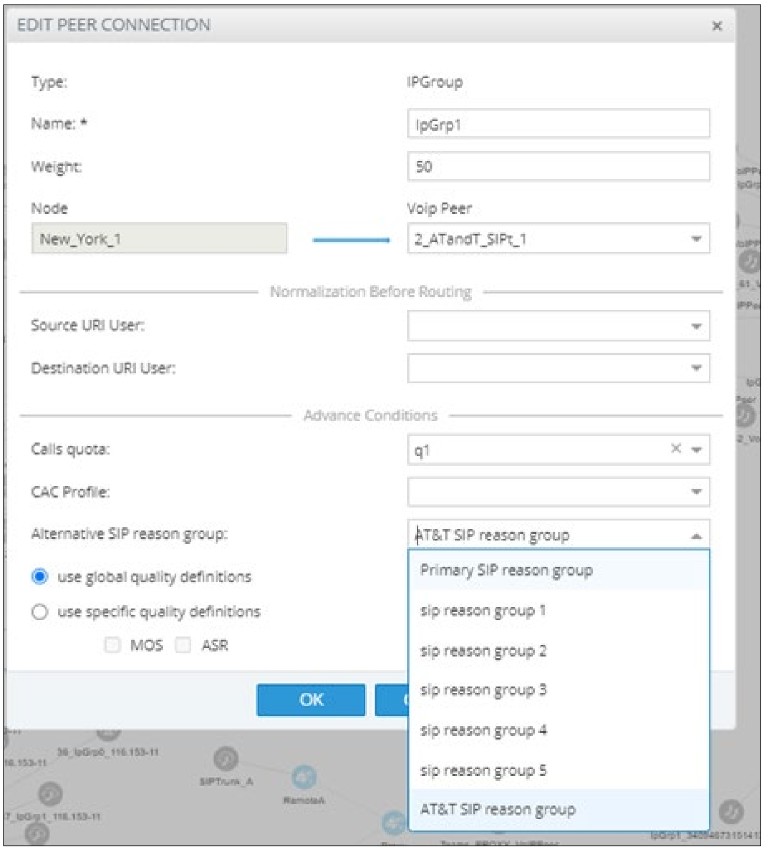
DUPLICATE SIP REASON GROUP

Name *	Reason Group for PBX
Description	to be used with Asterix

SELECTED	SIP RESPONSE	DESCRIPTION	ACTIVE
☑	421	Extension Required	✓
☑	422	Session Interval Too Small	✓
☑	480	Temporarily Unavailable	✓
☑	481	Temporarily Unavailable	✓
☑	482	Loop Detected	✓
☑	483	Too Many Hops	✓
☑	500	Server Internal Error	✓
☑	501	Not Implemented: The SIP r...	✓
☑	502	Bad Gateway	✓

Add/Edit and Delete of a specific SIP reason inside a group is performed in the same way as in versions before ARM 9.6.

A newly-defined SIP reason group can be attached to one or more Peer Connections (using both Add and Edit screens), either in the Network Map page or from the Peer Connections page:



EDIT PEER CONNECTION

Type: IPGroup

Name: * IpGrp1

Weight: 50

Node: New_York_1

Voip Peer: 2_ATandT_SIPt_1

Normalization Before Routing

Source URI User:

Destination URI User:

Advance Conditions

Calls quota: q1

CAC Profile:

Alternative SIP reason group: AT&T SIP reason group

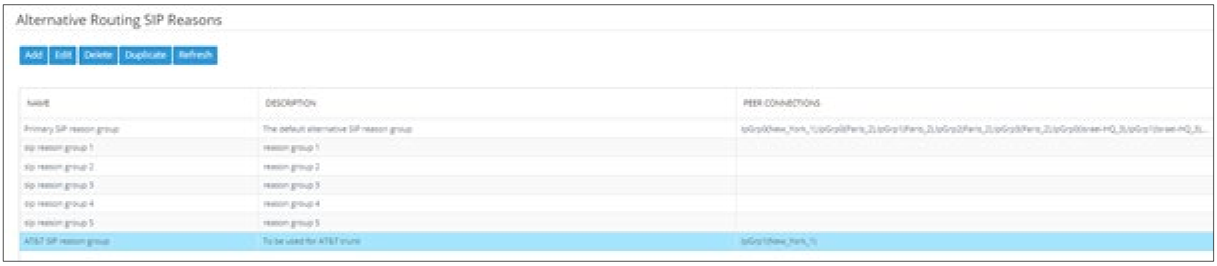
● use global quality definitions

○ use specific quality definitions

□ MOS □ ASR

The SIP reason group is displayed in the Peer Connection summary and table.

The indication of Peer Connection associated with the group is shown in the SIP reason group table:



Alternative Routing SIP Reasons

NAME	DESCRIPTION	PEER CONNECTIONS
Primary SIP reason group	The default alternative SIP reason group	IpGrp0(New_York_1),IpGrp0(Paris_2),IpGrp1(Paris_2),IpGrp2(Paris_2),IpGrp3(Paris_2),IpGrp0(Israel-HQ_3),IpGrp1(Israel-HQ_3),I...
sip reason group 1	reason group 1	
sip reason group 2	reason group 2	
sip reason group 3	reason group 3	
sip reason group 4	reason group 4	
sip reason group 5	reason group 5	
AT&T SIP reason group	To be used for AT&T trunk	IpGrp1(New_York_1)

By default, all Peer Connections are associated with the default SIP reason group.

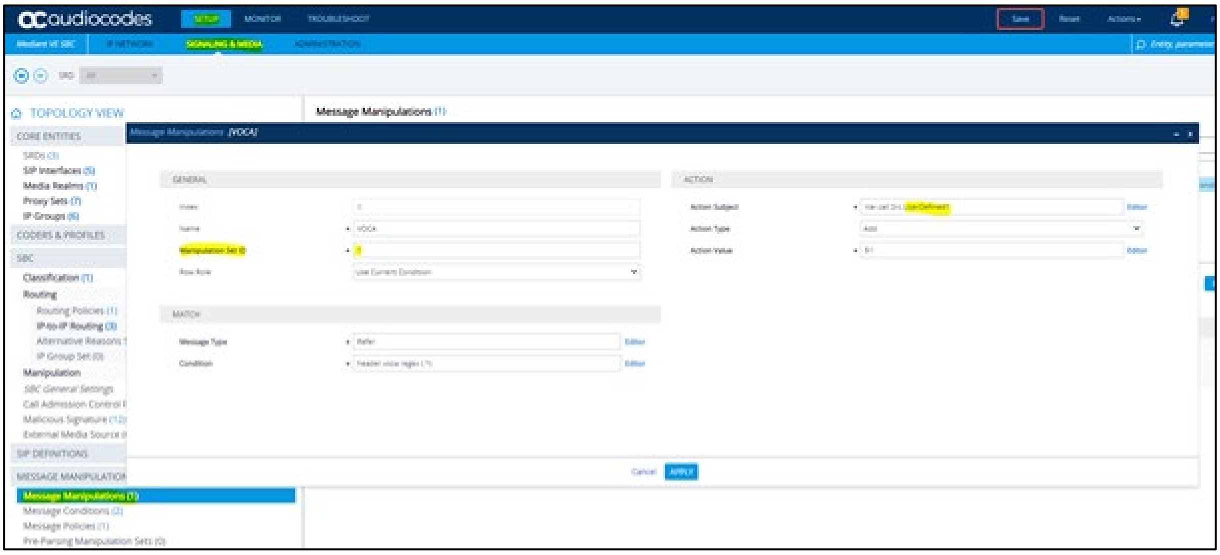
2.10 Adding Information from Node to Calls View

ARM 9.6 enables customers to add information from a node to Calls view, using a new 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:

1. Information is taken from propriety header 'voca' and assigned to the variable **Var.call.Src.UserDefined1**.



Message Manipulations [VOCA]

GENERAL

Index: 1

Name: VOCA

Manipulation Set ID: 1

Row Role: Use Current Condition

MATCH

Message Type: Refer

Condition: header.voca regex (.*)

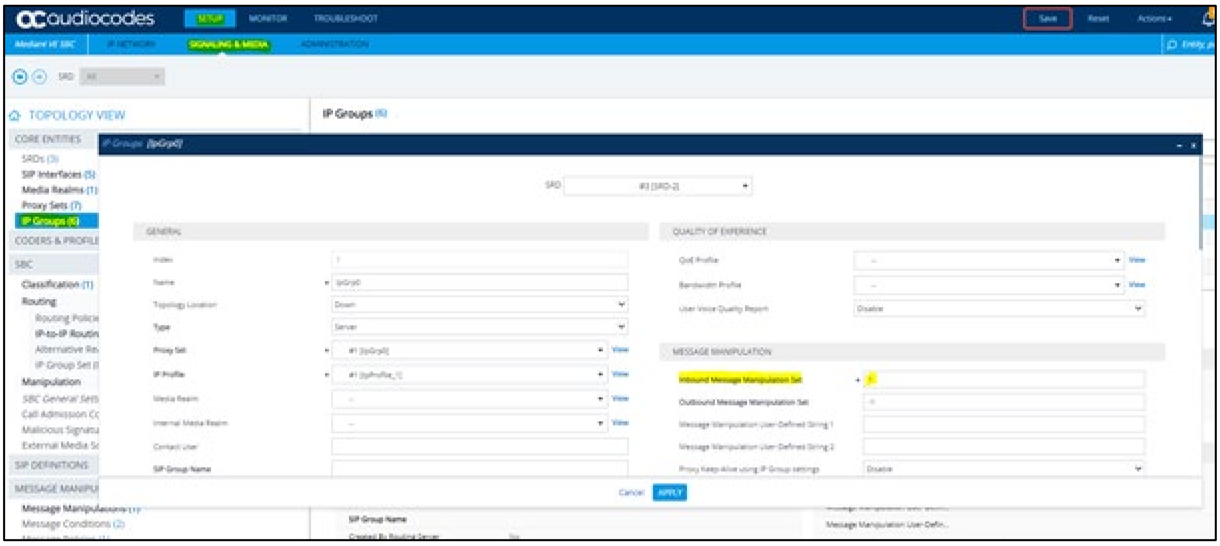
ACTION

Action Subject: var.call.Src.UserDefined1

Action Type: Add

Action Value: $1

2. It's then assigned to the IP Group in the node:



IP Groups [IpGrp0]

SRD: #3 [SRD-2]

GENERAL

Index: 1

Name: IpGrp0

Topology Location: Down

Type: Server

Proxy Set: #1 [IpGrp0]

IP Profile: #1 [IpProfile_1]

Media Realm: --

Internal Media Realm: --

Contact User:

SIP Group Name:

QUALITY OF EXPERIENCE

QoE Profile: --

Bandwidth Profile: --

User Voice Quality Report: Disable

MESSAGE MANIPULATION

Inbound Message Manipulation Set: 1

Outbound Message Manipulation Set: -1

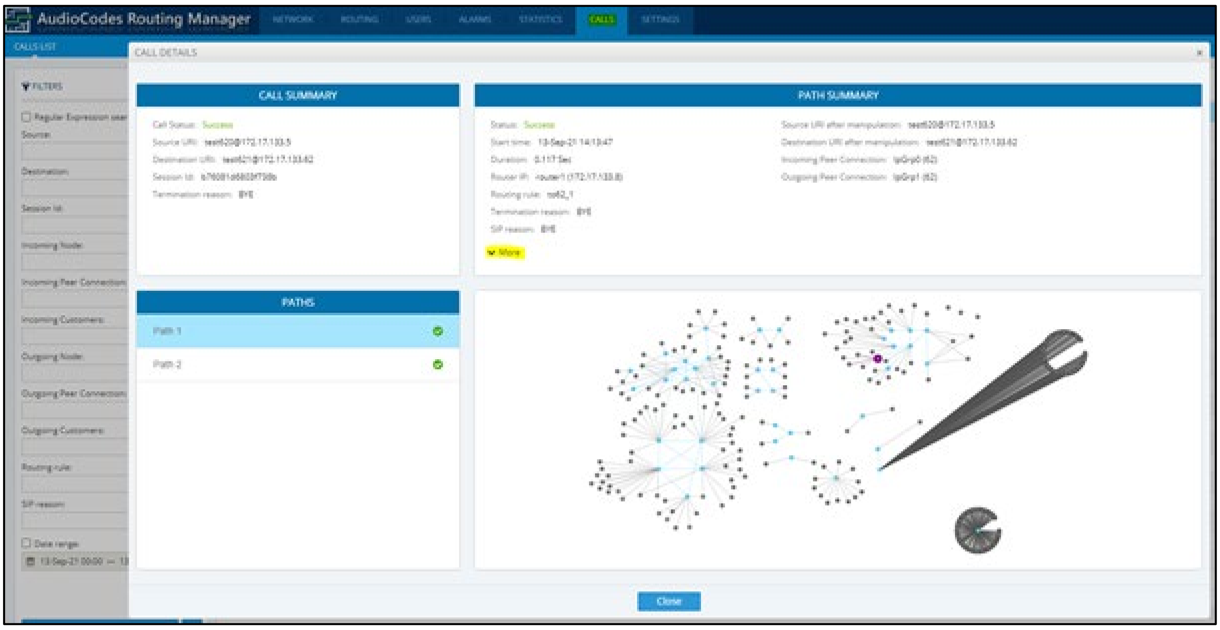
Message Manipulation User-Defined String 1:

Message Manipulation User-Defined String 2:

Proxy Keep-Alive using IP Group settings: Disable

3. The information is viewed 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.

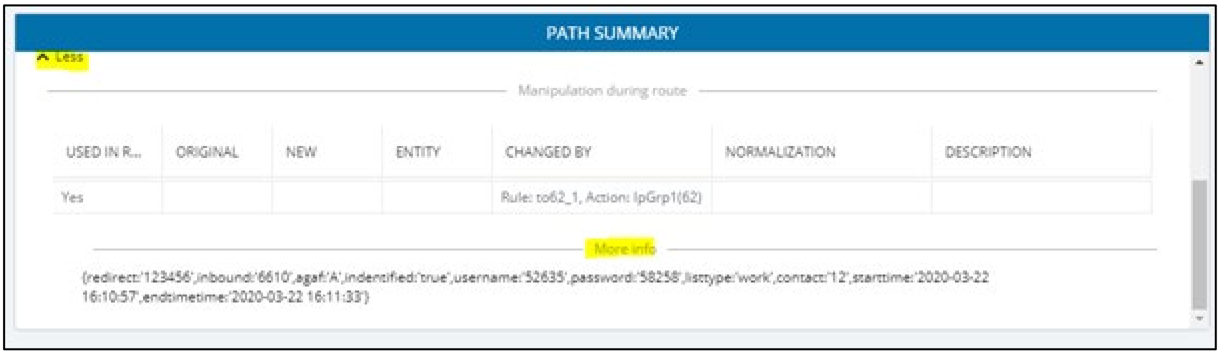
   In the following example, it’s a string contained by the ‘voca’ header.



Call Status: Success
Source URI: test620@172.17.133.5
Destination URI: test621@172.17.133.62
Session Id: b76081d6803f758b
Termination reason: BYE

Status: Success
Start time: 13-Sep-21 14:13:47
Duration: 0.117 Sec
Router IP: router1 (172.17.133.8)
Routing rule: to62_1
Termination reason: BYE
SIP reason: BYE

Source URI after manipulation: test620@172.17.133.5
Destination URI after manipulation: test621@172.17.133.62
Incoming Peer Connection: IpGrp0 (62)
Outgoing Peer Connection: IpGrp1 (62)



USED IN R...	ORIGINAL	NEW	ENTITY	CHANGED BY	NORMALIZATION	DESCRIPTION
Yes				Rule: to62_1, Action: IpGrp1(62)		

{redirect:'123456',inbound:'6610',agafi:'A',indentified:'true',username:'52635',password:'58258',listtype:'work',contact:'12',starttime:'2020-03-22 16:10:57',endtimetime:'2020-03-22 16:11:33'}

This page is intentionally left blank.

3 Supported Platforms

ARM 9.6 supports the platforms shown in the table below.

Table 3-1: ARM 9.6 Supported Platforms

ARM	Platform	Application
GUI	Web Browser	Firefox, Chrome, Edge
Deployment	VMWare	VMware ESXI 6.5, 6.7, 7.0 Update 2
	HyperV	Windows Server 2016 Hyper-V Manager Microsoft Corporation Version: 10.0.14393.0

This page is intentionally left blank.

4 Earliest SBC/GW Software Versions Supported by ARM Features

Some ARM features are developed in coordination with nodes (AudioCodes' SBCs and Media 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 4-1: 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	-
5	Support of IP Group of type User without 'dummy' IP	7.20A.250 and later	Network administrators 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	-
9	Support for Registered users in ARM	Version 7.20A.254.353 or later	-
10	Support for combined ARM and	Version 7.20A.256.391	Supported for SBC only

#	Feature	Earliest Node Software Supporting It	Comments
	SIP based Routing decision (Route based on Request URI)		
11	Support for combined ARM and SBC Routing decision	Version 7.20A.256.391	Supported for SBC only
12	ARM as an Information Source for Users Credentials	Version 7.20A.256.713	Supported for SBC only
13	Support for Microsoft Teams LMP (Local Media Optimization) and additional IP Profiles	Versions: 7.20A.258 -0313, 7.20A.260-180 7.40A.005 (official release) and later	-
14	ARM connection with ABC level defined IP Profile and Media Realm	Versions: 7.20A.258 -0313, 7.20A.260-180 7.40A.005 (official release) and later	SBC only
15	ARM 'Customer' entity (Team multi-tenancy) - support for Contact header manipulation	7.40A.005.509 or later	
16	Delayed Alternative Routing	Official build from SBC 7.4.200 stream	-
17	Story of a call: Integration with Voca. Additional information in ARM calls information.	Official build from SBC 7.4.200 stream	-
18	Support for more efficient way of synchronization of SBC IP groups with ARM	Official build from SBC 7.4.200 stream	If the customer runs earlier SBC SW, the synchronization will work in a pre-ARM 9.6 way.

5 Resolved Issues in ARM 9.6

The table below lists major issues which were encountered by customers in previous releases, but which are resolved in ARM 9.6.

Table 5-1: Resolved Issues in ARM 9.6

Incident	Problem / Limitation
ARM-4932	File Repository mapping gets lost.
ARM-4716	With Azure Cloud Edition (CE), when a switchover occurs, mismatch of SerialNum occurs. Generally, Azure CE is supported behind Load Balancer.
ARM-4711	The ARM doesn't use SBC2GW IP Group if the source node and the destination node are the same for a call from User IP Group.
ARM-4703	After switchover, a retransmit session of the login occurs. Generally, Azure CE is supported behind Load Balancer.
ARM-4676	Azure CE is supported behind Load Balancer.
ARM-4336	The ARM is not populating Calls History.
ARM-3532	Issues occur when adding a node using host name.

This page is intentionally left blank.

6 Tested ARM Capacities

Table 6-1 lists tested ARM capacities. The table presents the results of *the maximum capacities* tested. If customers require *higher capacities* tested, they should communicate this to AudioCodes.

Table 6-1: Tested ARM Capacities

Item	Maximum Capacity Tested
CAPs (assuming the average call duration is 100 seconds)	300 CAPs per ARM Router
	ARM total: 3,000 CAPs
ARM Routers	40
Routing Groups	2,000
Routing Rules per ARM	10,000
ARM Users (either local or LDAP/Azure AD)	1 million Possible extension to 4 million when ordering a special Feature Key. Requires 16 GB memory for Routers.
‘Customer’ entities (Teams tenants)	Up to 20,000
Nodes number	150
Peer Connections	Per Node: 600
	ARM total: 1,500
Connections	1000
Prefix Groups	2,000
Prefixes in a single Prefix Group	2,000
Calls history	10 million
Threshold alarms	150 threshold rules 25 elements/entities per rule
Statistics history	30 days

This page is intentionally left blank.

7 Known Limitations and Workarounds

The table below lists the known limitations and workarounds in ARM 9.6.

Table 7-1: 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).	Network administrators should take this into consideration
-	When defining a Users Group, the condition is applied to the pre-manipulated value of the property used in the condition definition (the original value taken from the Active Directory).	Network administrators should take this into consideration
-	For VMware users, after rebooting or upgrading an ARM Configurator, its clock 'drifts'. This can sometimes cause inconsistency between ARM Configurator and ARM Router data.	Make sure the clock in the machine (Host) and the VM (Guest) are the same. Both should be synchronized with the same NTP.
-	For customers who use auto-detect mode to add a new node (SBC / gateway) to the ARM, the name of the Configurator Web service configured at the node level for auto-discovery *must* be **ARMTopology** else the ARM data center recovery mechanism will not work correctly for the node; it will not be redirected to the new Configurator.	Generally, it's preferable to add a node using the ARM GUI rather than auto-detection.
-	When the ARM is used with Load Balancing CE SBC in an Azure environment, the operator should make sure to define the FQDN / IP Address as the Hostname of the LB CE SBC and add the LB CE SBC in the ARM using that Hostname.	-
Breaking changes		
-	ARM 9.6 does not support 'Build Star' and 'Build Mash' capabilities. These capabilities were removed from the GUI and REST API starting from ARM 9.4 as they are not widely used by customers and are potentially problematic.	Operators should add Connections and build the ARM Network Topology based on customer requirements.
-	For operators of the pre-9.2 ARM version: ARM 9.2 changes the REST API for ARM Users management (Add, Delete, Modify) in a way that is not backward compatible.	Customers must take this into consideration. The new REST API for users is described in the *ARM 9.2* and the *ARM 9.6 REST API Developer's Guide*. If customers develop scripts based on this REST API, these scripts should be adjusted

Incident	Problem / Limitation	Comments/Workaround
		to the new REST API when moving to ARM 9.2 or ARM 9.6.
-	Starting from ARM 9.4, the REST API for getting all VoIP Peers (VoIP Peers GET API) is changed. This non-backward compatible change was implemented to support Paging.	Customers should take this into consideration. The new REST API for getting the VoIP Peers is described in the *ARM 9.4 REST API Developer's Guide*. If customers develop scripts based on this REST API, these scripts should be adjusted to the new REST API when moving to ARM 9.4/ ARM 9.6.
-	For a two-step upgrade (for customers upgrading from ARM 8.6 or earlier): The redesigned ARM 8.8 Add Routing Rule – Routing Actions screen does not feature the 'via' action as previous versions did. The same applies to ARM 9.0, ARM 9.2, ARM 9.4 and ARM 9.6.	Customers upgrading from a previous version will still view the action but are advised to exclude it from routing definitions.
-	In ARM 9.6 (starting from ARM 9.4), when an alarm for a Routing Rule is generated, the detailed alarm information is placed in both **Additional Info 1** and **Additional Info 2**.	Operators should use information from both fields. This is done to provide detailed information about the alarm without truncation.
-	ARM 9.6 REST API is not backward compatible in the definition (Add / Edit / Delete) of 'Alternative Routing SIP Reason'. This is due to the new feature (Sets of SIP Reasons for Alternative Routing).	Customers should take this into consideration. The new REST API for managing SIP reasons will be described in *ARM 9.6 REST API Developer's Guide*. If customers develop scripts based on this REST API, these scripts should be adjusted to the new REST API when moving to ARM 9.4 ARM 9.6.
Upgrade		
-	Direct upgrade from ARM 8.6 and earlier to ARM 9.6 is not supported.	For these cases, a two-step upgrade is required: Step 1: Upgrade to ARM 9.0 or ARM 9.2 Step 2: Upgrade to ARM 9.6 **Note**: The following direct upgrades are supported: • ARM 8.8 > ARM 9.6 • ARM 9.0 > ARM 9.6 • ARM 9.2 > ARM 9.6 • ARM 9.4 > ARM 9.6
-	For pre-ARM 9.2 deployments, the upgrade to ARM 9.6 is not a regular upgrade as it upgrades the OS of all components to CentOS Stream from CentOS6. Note that for ARM 9.2 and ARM 9.4 deployments (running CentOS8), the upgrade is smooth.	Make the following preparations: • Make sure you downloaded not only the upgrade but also the installation images for the ARM Configurator and the ARM Router (not as for the usual upgrade). • Request from AudioCodes a Feature Key with all the ordered features and ordered number of sessions for the new VM in ARM 9.6.

Incident	Problem / Limitation	Comments/Workaround
		• Prepare temporary IP and VM resources required for each server upgrade. • Prepare extended storage for the ARM Configurator (the ARM Configurator allocates 80 GB in ARM 9.6 – like in ARM 9.4).
-	To upgrade to ARM 9.6 in a VMware environment, the customer must have VMware ESXI 6.5, 6.7 or 7.0 update 2 (earlier versions are not supported with CentOS Stream).	-
-	For a two-step upgrade (for customers performing an upgrade from ARM 8.6 and earlier): Upgrading from ARM 8.6 to ARM 8.8/9.0 does not preserve calls (CDRs) information on calls run by ARM 8.6. Note that upgrading from ARM 8.8/ARM 9.0, ARM 9.2, ARM 9.4 to ARM 9.6 preserves calls information during the upgrade.	If a customer needs calls information from ARM 8.6, contact AudioCodes support (R&D) for the procedure to back up calls (CDRs) information.
-	Miscellaneous issues with the ARM GUI after upgrading from previous releases.	Customers are requested to clear the browser cache after performing a software upgrade (**Ctrl**+**F5**).
GUI Incidents		
ARM-3249 ARM - 2724	Prefixes in a Prefix Group cannot be edited. Double-clicking an existing prefix to modify it doesn't work.	The customer can remove the old prefix and define a new prefix.
ARM-4528	In the **Alarms** > **Journal**, the calls Quota Name is not shown in the 'Description'.	-
ARM-5005	In the File Repository table, scrollbar and search are not supported.	This table wasn't initially supposed to support more than 20 entries. It will be fixed in the next release.
ARM-5013	In the Alarm Threshold Rules, in the graphs presentation, the names of Peer Connections are sometimes cut off.	-
ARM in Azure with SBCs behind Load Balancer		
ARM-4676	After a switchover of an SBC occurs, the node can temporally (for few seconds) switch between available and unknown state in the ARM; calls are unaffected as routing continues regularly.	The issue occurs as it takes time for the Load Balancer (usually up to 10 seconds) to switch to the secondary SBC.
ARM-4676	After a switchover of an SBC occurs, the connections to the HA SBC are indicated for a few minutes as unavailable.	The connection between the HA SBCs behind the Load Balancer and the other nodes should have **Keep connection properties synchronized** disabled. Also, the IP of the proxy set towards the node behind the Load Balancer should be configured manually (at the SBC level) with the Load Balancer's IP.

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/