Release Notes

AudioCodes One Voice™ Operations Center

AudioCodes Routing Manager (ARM)

Version 8.8

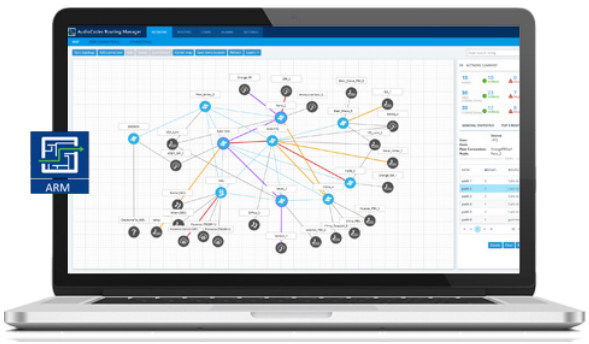


Table of Contents

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: Oct-27-2019

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

These *Release Notes* describe the new features and known issues in version 8.8 of the AudioCodes Routing Manager (ARM).

1.1 Managed AudioCodes Devices

ARM 8.8 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 8.8

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 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 8.8

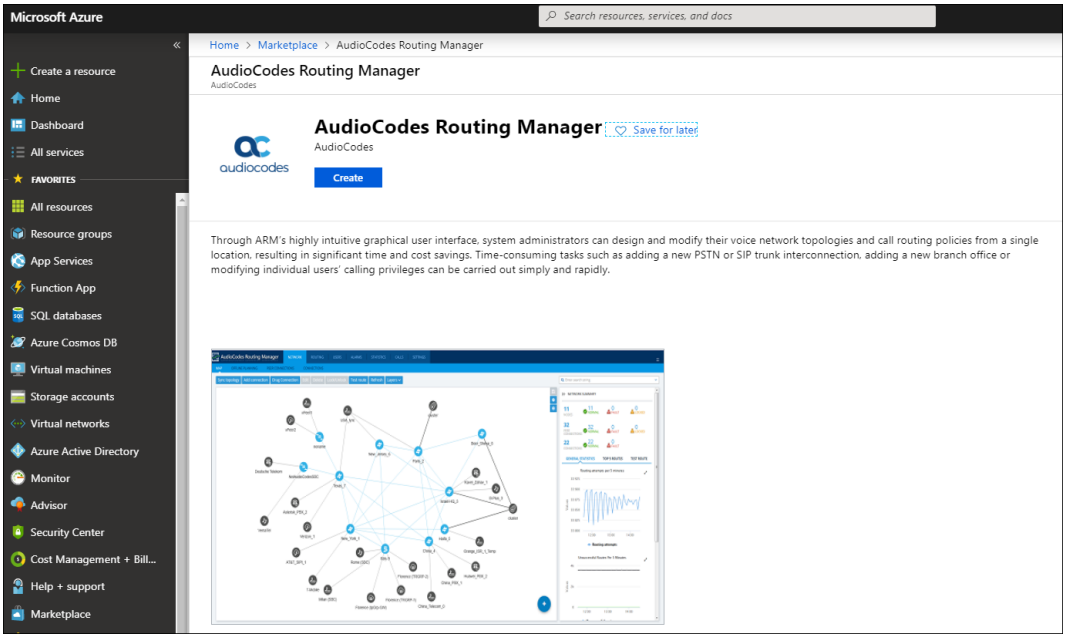
This section describes the new features and capabilities introduced in ARM 8.8.

2.1 Availability from Microsoft's Azure Marketplace

ARM 8.8 supports Microsoft's Azure Marketplace solution which includes ARM Configurator and two ARM Routers. The solution (Configurator and Routers) is deployed automatically in one Azure region, selected by the customer. AudioCodes also provides a GUI for creating a solution that includes multiple Virtual Machines.

Both ARM Routers are created in the same Azure Availability Set. This means that Azure will not instantiate them on the same rack.

Figure 2-1: ARM 8.8 Availability from Microsoft's Azure Marketplace



Note that when upgrading from 8.6 (ARM 8.6.19) to the next major version (ARM 8.8) in Azure, the ssh root user must be enabled as follows:

1. Change to root user: Run the command "sudo -i".
2. Edit the file "/etc/ssh/sshd_config". Change the line containing PermitRootLogin to "PermitRootLogin yes".
3. Run the command "service sshd restart".

After the upgrade is finished, it's recommended to:

- Change the root user's default password (on the ARM Configurator and on all Routers)
- Block the user ssh root login again

2.2 Support for Distributed Registered Users at the Network Level

ARM 8.8 supports network wide management of registered users in a customer's network. Registered users can be added to the ARM 8.8 for the ARM to then be capable of performing (for example) call routing based on SBC user registrations.

AudioCodes SBCs have long supported IP Groups of type 'User' with capabilities to store locally (at SBC level) information about registered users. This information is stored in the SBC's local database. The SBC has been able to route calls to the locally registered users even if disconnected from the registrar.

Now, when ARM 8.8 supports registered users and treats SBC-level IP groups of type 'User' as regular ARM 'Peer Connection', the registered users information is handled by the ARM and stored in the ARM database. This information is dynamically synchronized between network SBCs | Media Gateways and the ARM. The ARM provides a centralized place for storing all the registered users information distributed among several Nodes and several Peer Connections. The registered users information is dynamic and is updated dynamically at ARM level by getting updates from SBCs and synchronization with SBCs data.

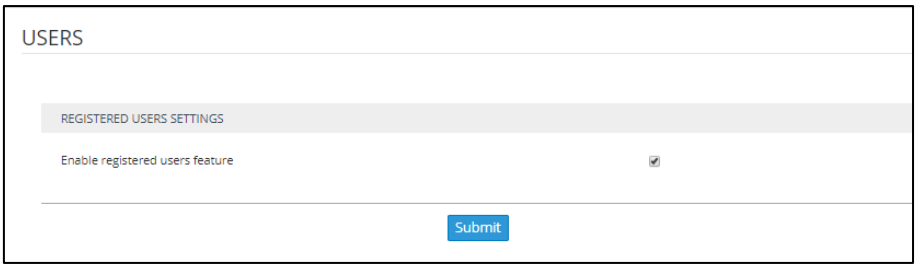
Centralized management and storage of registered users allows the ARM to route calls *at the network level* to a specific SBC and a specific Peer Connection (IP Group of type 'User').

Moreover, it provides a single point from which to view, select and manage registered users.

Note: This feature is available only for Nodes Version 7.20A.254.353 or later.

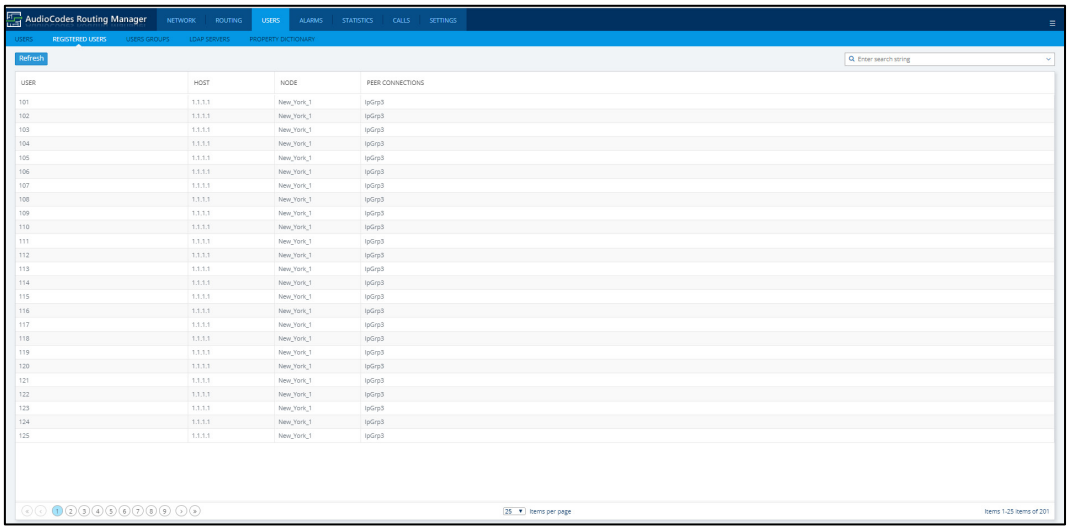
To enable management of registered users in the ARM and routing to distributed registered users, the network administrator must first enable the feature in the new Registered Users Settings screen (Settings > Administration > Users).

Figure 2-2: Registered Users Settings – Enable Registered Users Feature



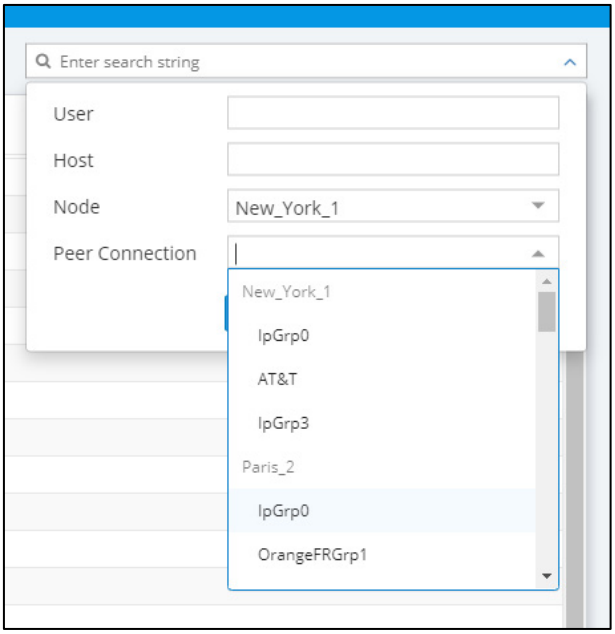
ARM 8.8 features a new Registered Users page (Users > Registered Users) shown in the next figure. The page lists all the registered users from several SBCs and several associated Peer Connections (corresponding IP Groups of type 'User'). The information stored in the ARM includes the User, Host (of the corresponding Node where the user is registered), Node name and Peer Connection name. This information is used by the ARM for further routing.

Figure 2-3: Registered Users Page



To view registered users from a specific Node or a specific Peer Connection, the 'Enter search string' filter can be used.

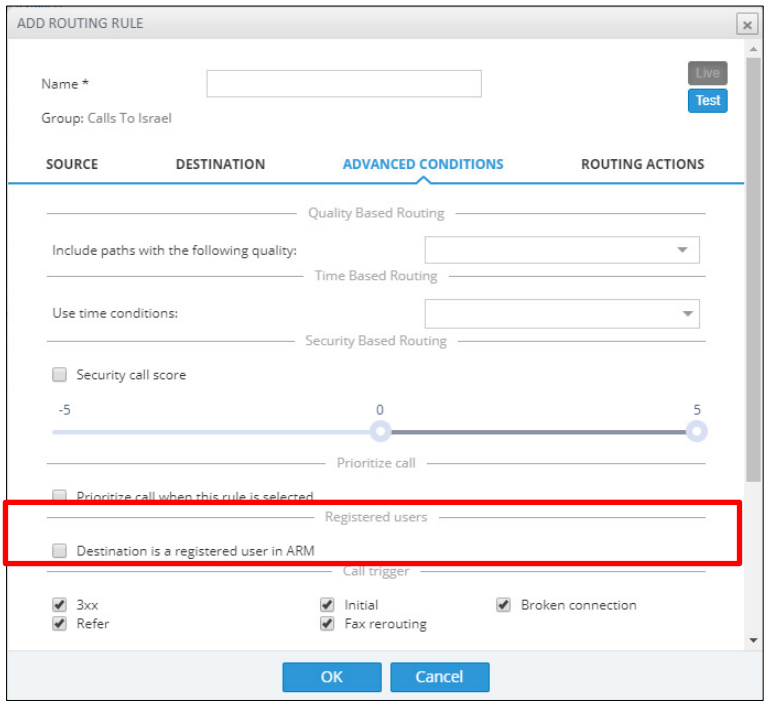
Figure 2-4: Filter



2.2.1 Definition of Routing Rules for Distributed Registered Users Routing

The feature can be applied when adding a new Routing Rule. The Add Routing Rule page features a new option **Destination is a registered user in ARM** under the tab **Advanced Conditions**. The ARM will route a call only if the destination number is the number of a registered user in the ARM (listed in the Registered Users table) and the Routing Rule is matched.

Figure 2-5: Destination is a registered user in ARM



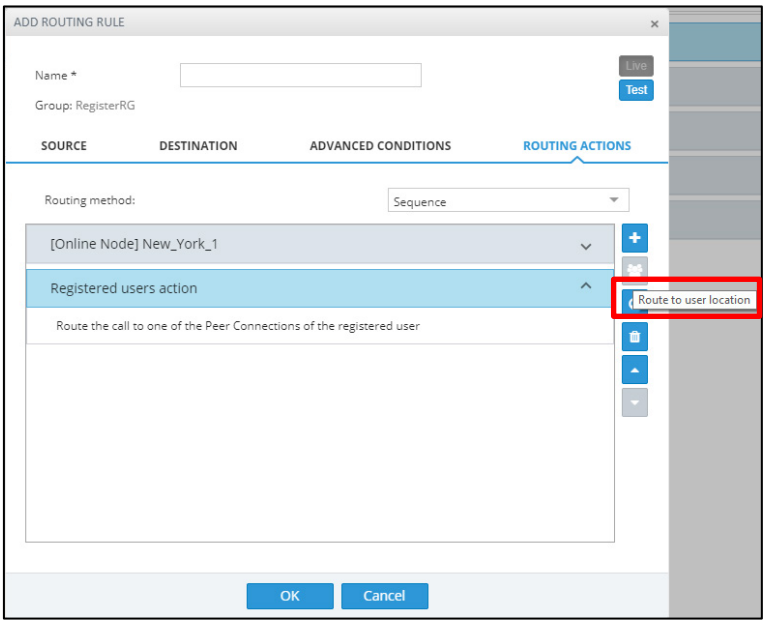
The Add Routing Rule screen in ARM 8.8 shown in the figure above features a new option **Destination is a registered user in ARM** under a new section 'Registered users' under the **Advanced Conditions** tab.

If network administrators select this option, the Routing Rule will be matched only if the destination number is a registered user number (listed in the Registered Users table).

The feature can also be applied in Policy Studio which features a new option **Destination is a registered user in ARM**. If selected, the Policy Studio rule will be matched only if the destination number is a registered user's number (listed in the Registered Users table).

ARM 8.8 features a new Routing Rule action: **Route to user location**.

Figure 2-6: Route to User Location



If the action is selected, the ARM will attempt to route the call to the location of the registered user (the destination number is used as the key by which to search for the location).

2.3 Resource Groups

ARM 8.8 features a new Resource Groups page (Network > Resource Groups) that allows network administrators to add and view a group of ARM topology resources. The group of resources can contain topology elements of the same type, like Nodes, Peer Connections or VoIP Peers, for further use in ARM-related definitions.

Figure 2-7: Add Resource Group

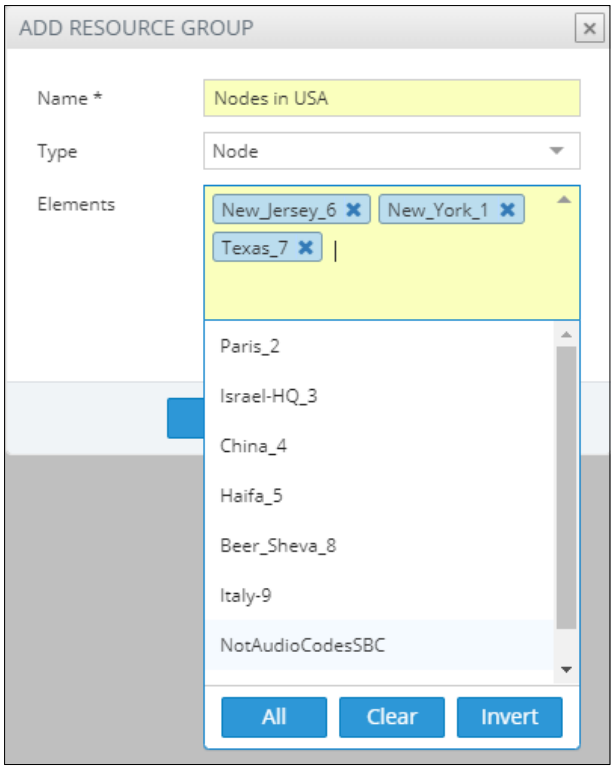
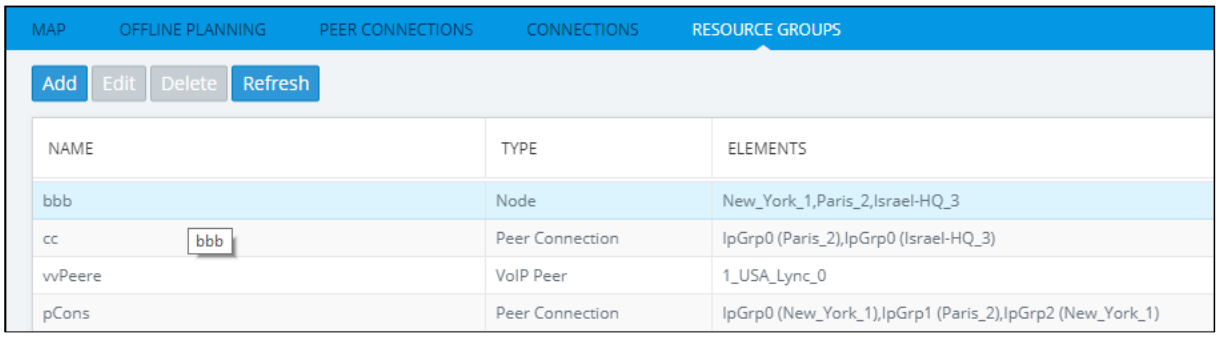


Figure 2-8: Resource Groups



Network administrators can determine at a glance the elements defined in each Resource Group. The page also allows network administrators to edit and delete Resource Groups.

Note:

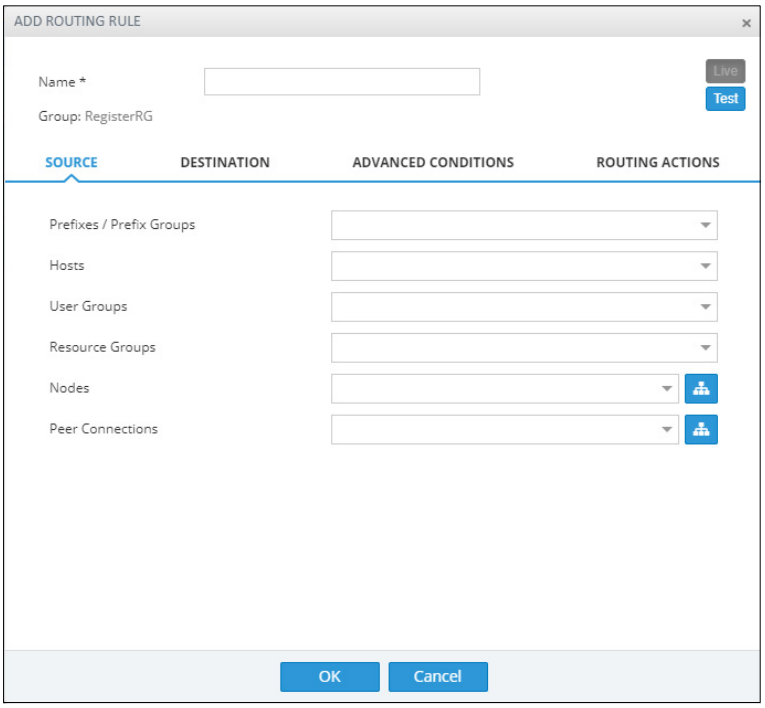
- Network administrators can use a Resource Group comprising Nodes or Peer Connections as *the source of a call* in a Routing Rule and/or as *the source Resource Group* in a Policy Studio rule.
- Any Resource Group can be used as the action in a Routing Rule..

2.4 Improved Usability and User Experience

2.4.1 'Add Routing Rule' Screen

The Add Routing Rule screen has been re-conceptualized and redesigned for an improved look and feel and for improved usability and user experience - where 'user' is the network administrator.

Figure 2-9: Add Routing Rule

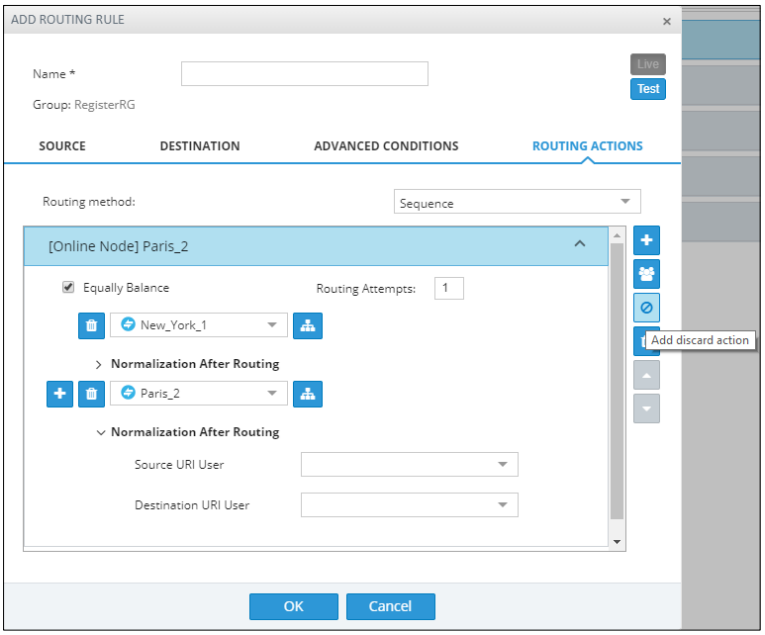


The tabs **Source**, **Destination**, **Advanced Conditions** and **Routing Actions** are now laid out horizontally across the screen. The default screen tab is **Source** as shown in the preceding figure. Network administrators click a tab to display its screen.

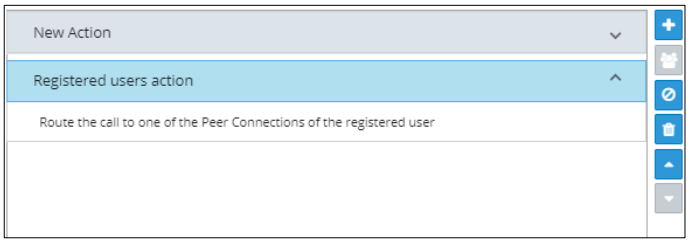
Previously, the tabs were listed vertically, one under the other. Network administrators clicked a tab to display the parameters under it and parameters were displayed in list format more than in a dedicated parameters screen.

The **Routing Actions** tab's screen has been reconceptualized and redesigned for an improved look and feel and for enhanced usability, as shown in the next figure.

Figure 2-10: Add Routing Rule – Routing Actions



Here's how the Routing Actions are now laid out:

	[Located upper right] Allows the network administrator to 'Add an action'
	[Located upper right] Allows the network administrator to 'Route to user location'. This functionality is new in Version 8.8. If selected, the ARM attempts to route the call to the location of the registered user (the destination number is used as the key to search for the location). *The ARM will only be able to route the call if the destination number is the number of a registered user in the ARM (listed in the Registered Users table) and the Routing Rule is matched*. 
	[Located upper right] Allows the network administrator to 'Add a discard action'
	[Located adjacent to the action field] Allows the network administrator to 'Add load balancing'
	[Located adjacent to the action field] Allows the network administrator to 'Choose a Topology item'

Note:

- The redesigned ARM 8.8 Add Routing Rule – Routing Actions screen does not feature the 'via' action as previous versions did.
- Customers *upgrading from a previous version* will still view the action but are advised to exclude it from routing definitions.
- The feature was omitted from ARM 8.8 as part of the need to improve usability and user experience. In future, the feature will be redesigned and reincorporated for a friendlier user experience.

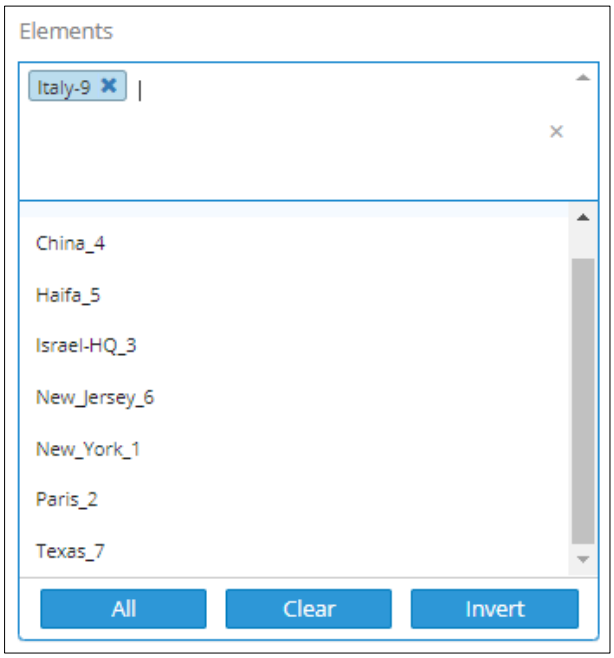
2.4.2 Select Multiple Elements and Invert the Selection

ARM 8.8 pages feature filters in which the network administrator can select multiple elements and then *invert the selection*. The feature improves usability and user experience especially in large networks with high numbers of elements.

The Statistics pages, for example, as well as the Add | Edit Routing Rule screens (the 'Nodes', 'Peer Connections' and 'User Groups' fields under the **Source** tab) and the Policy Studio's Add Call Item screen (the 'Source Nodes' and 'Source Peer Connections' fields) feature filters like these.

The figure below shows the filter in the Statistics page's 'Nodes by peer connections' graph.

Figure 2-11: Select Multiple Elements and Invert the Selection



The feature allows network administrators to

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

2.4.3 'LDAP Server Settings' Screen

The LDAP Server Settings screen has been moderately reconceptualized and redesigned for an improved look and feel and for improved usability and user experience (where 'user' is the network administrator).

Figure 2-12: LDAP Server Settings – LDAP Settings

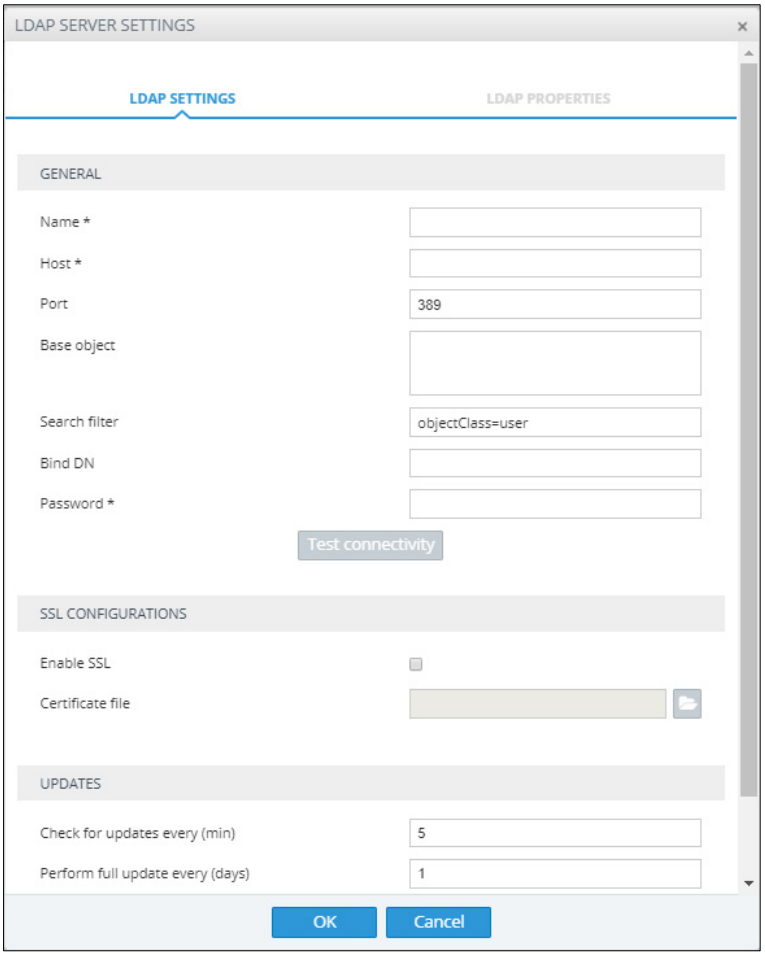
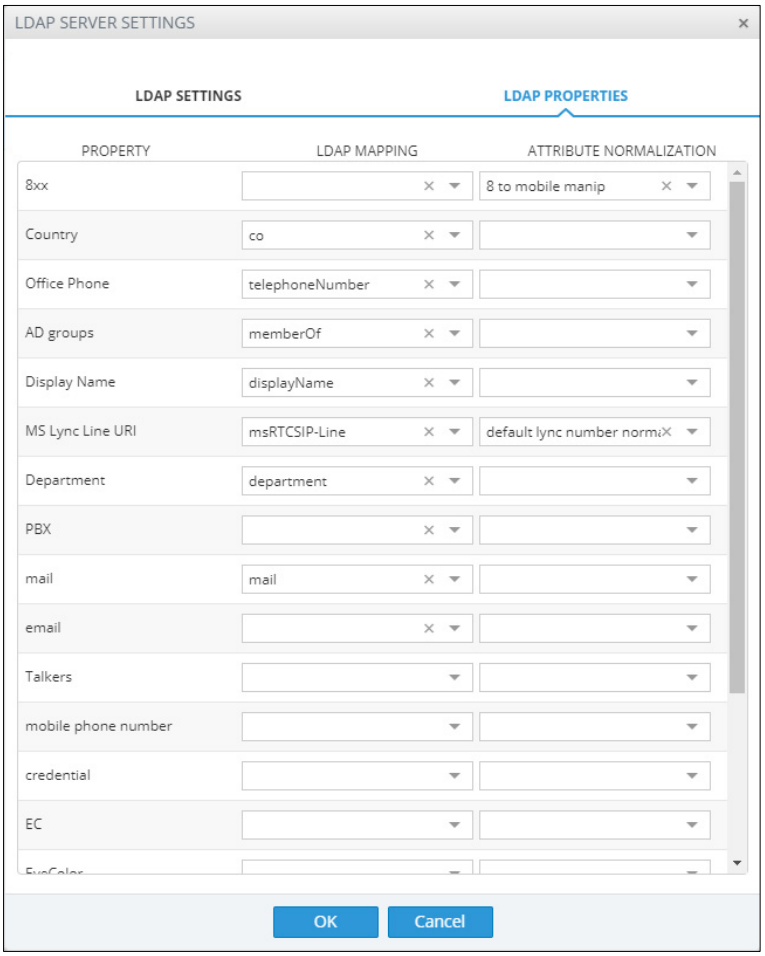


Figure 2-13: LDAP Server Settings – LDAP Properties



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

ARM 8.8 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 8.8. The changes in the upgrade procedure are described in the *ARM Installation Manual*.

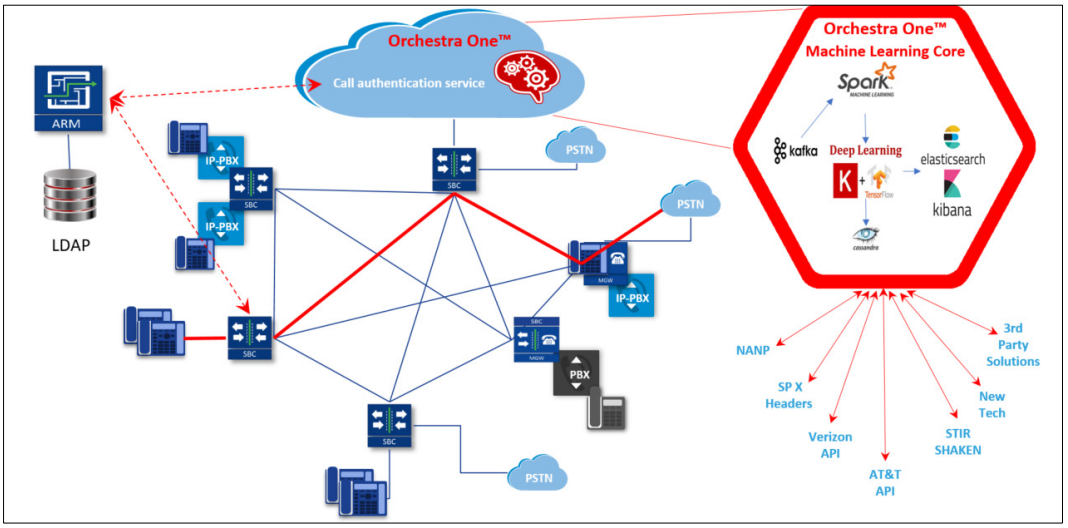
Note:

- When the upgrade is finished, best practice is to clear the GUI cache (**Ctrl**+**F5**).
- Upgrading from ARM 8.6 to ARM 8.8 does not preserve calls (CDRs) information on calls run by ARM 8.6.
- If a customer needs calls information from ARM 8.6, contact AudioCodes support (R&D) for the procedure to back up calls (CDRs) information.

2.6 Security Based Routing

ARM 8.8 supports Security Based routing through integration with SecureLogix's Orchestra One™ CAS (Call Authentication Service).

Figure 2-14: 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 8.8, a new 'Security call score' option is available under the Security Based Routing section in the Advanced Conditions tab of the Add Routing Rule screen. The option is available when SecureLogix is used.

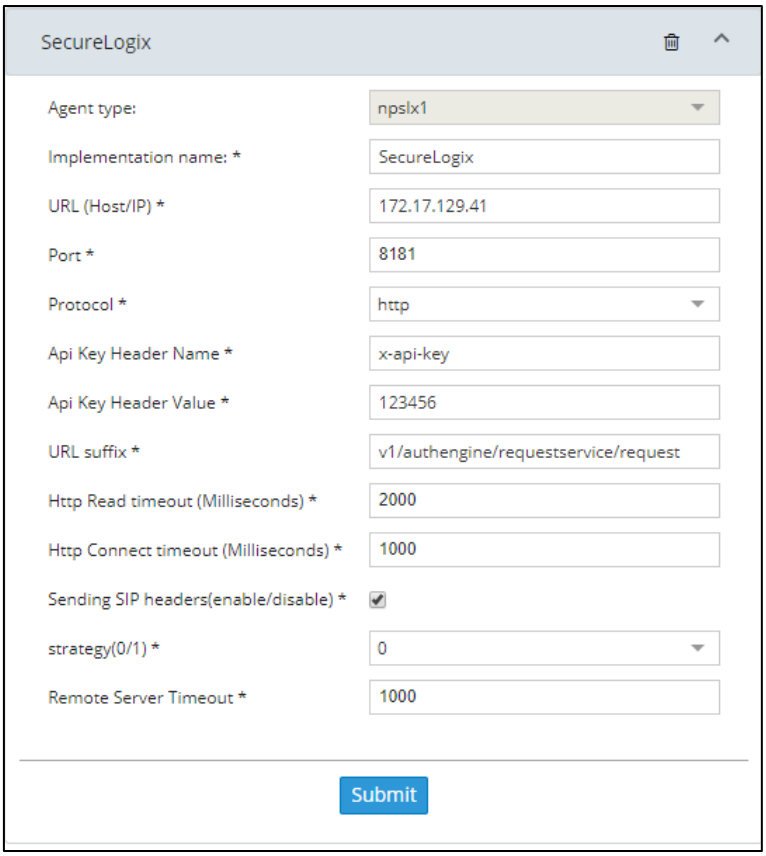
Note:

- Using security-based routing requires purchasing SecureLogix's license (in addition to the ARM license) and should be coordinated with AudioCodes.
- The feature is currently unavailable but will become available by January 2020.

2.6.1 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.

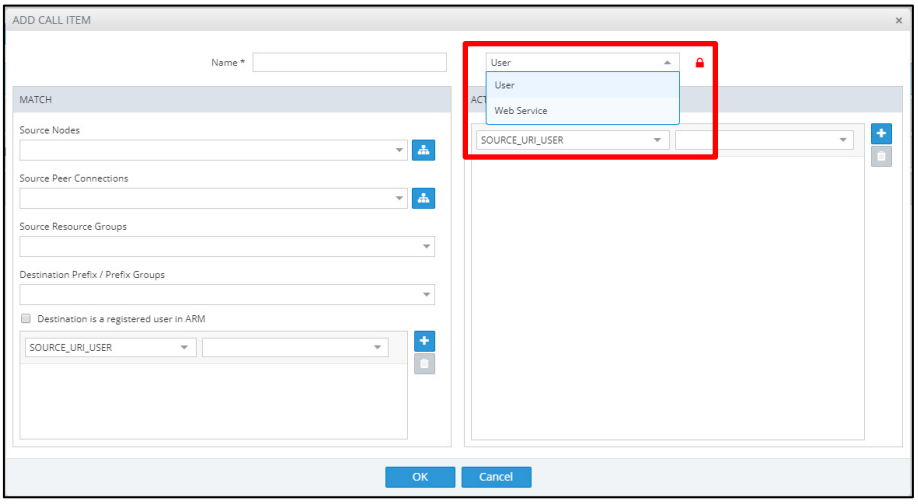
Figure 2-15: SecureLogix



The newly defined Web Server must then be assigned in Policy Studio for prerouting processing and consultation with SecureLogix's Orchestra One.

Policy Studio 8.8 consequently supports a new usage (in an addition to the default 'User' usage): **Web Service**.

Figure 2-16: Policy Studio: Web Service



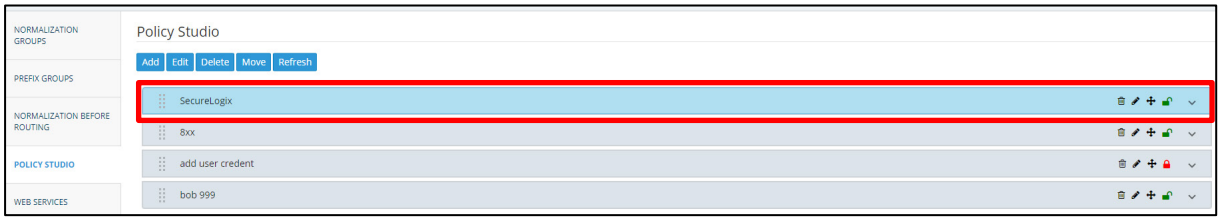
Previously, network administrators were limited to using Policy Studio based on information taken from ARM Users Data (the default 'User' option).

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 2-17: External Web Service 'SecureLogix' Configured in Policy Studio



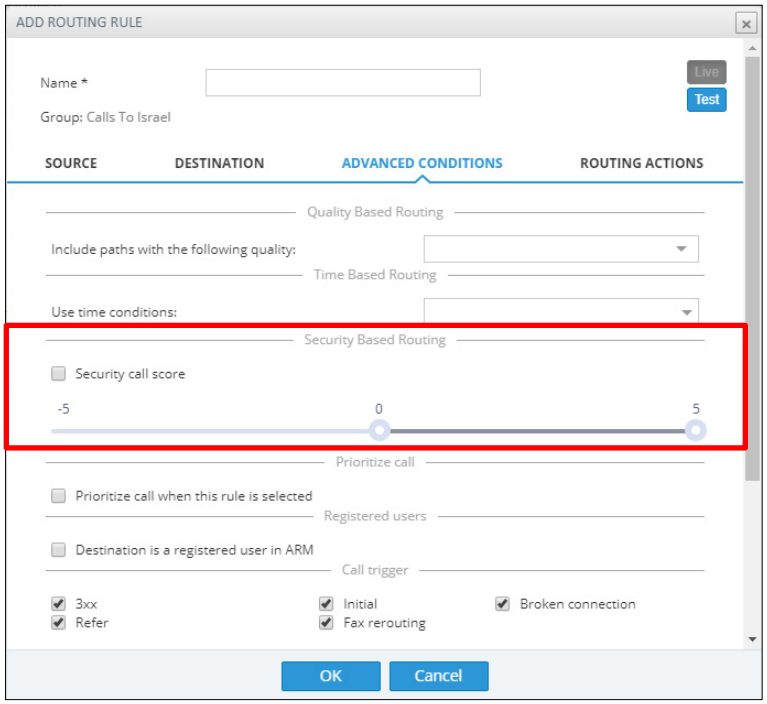
2.6.2 Using a Call's Security Score for a Routing Decision

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 2-18: Security Based Routing - Security Call Score



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.

This page is intentionally left blank.

3 Supported Platforms

ARM 8.8 supports the platforms shown in the table below.

Table 3-1: ARM 8.8 Supported Platforms

ARM	Platform	Application
GUI	Web Browser	Firefox, Chrome, Edge
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.

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	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	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	

This page is intentionally left blank.

5 Resolved Issues in ARM 8.8

The table below lists issues which were encountered by customers in previous releases but which are resolved in ARM 8.8.

Table 5-1: Resolved Issues in ARM 8.8

Incident	Problem / Limitation	Comments/Solution
ARM-2972	When editing a Routing Rule customers cannot remove some of the Peer Connections by deselecting them from the drop-down list.	The redesign of the Routing Rule includes a new component for Peer Connections editing.
ARM-2883	The ARM CDRs utility for unanswered calls incorrectly handles call records if the call duration is 0.	For unanswered calls, the ARM fills the START field when the first Invite arrives.
ARM-2812	The Connectivity alarm has a wrong description. When there is no RouterGroup attached to the Node, the Connectivity alarm makes no mention of it.	Additional information was added in the event that the Node changes to 'Unavailable' and has no Routing Server Group. Example: ADDITIONAL INFO 1: The Configurator can reach the Node, the Node can reach the Configurator, the Node cannot reach the Routers as determined by the Routers and as determined by the Node. ADDITIONAL INFO 2: The Node has no Routing Server Group attached.
ARM-2760	Unable to use # and * as the first digit in a Routing Rule. For the user to dial *42 or #31# there's no option to add these prefixes in the 'Prefixes/Prefix Groups' field in the Routing Rules.	The following functionality was added: 1 "#" can also be in the beginning, middle and end of the string. At the end = this is the last character; else handle it as a simple character (as a number or as a-zA-Z). 2 "*" - ARM handles it as a simple character (as a number or as a-zA-Z). Note that the ARM does not handle it as any number as the SBC does.
ARM-2750	Web Service timeouts. When 'Read timeout' and 'Connect timeout' in the external database connection are undefined, the ARM stops functioning completely.	ARM 8.8 does not allow the timeouts to be empty. In addition, the router's software was fixed to prevent the exception from occurring.
ARM-2745	An option is needed to allow network administrators to delete ARM users even though their source is Active Directory. The option is needed for AD users who move to another PBX. Their deletion from the AD should immediately be reflected in the ARM.	ARM 8.8 adds this option. Note that if network administrators can delete an LDAP user, they're actually deleting a user that still exists in Active Directory; this user will automatically be added again only after a 'full synch' (once a day) and not during the 'periodical synchronization' of deltas (every 15 minutes).

Incident	Problem / Limitation	Comments/Solution
ARM-2742	After performing Test Route, the 'Paths' section on the right side of the page does not show the entire name of the Route Group and Route Rule if too long.	Network administrators can view in a tooltip the entire Routing Group / Routing Rule name even if long.
ARM-2723	Impossible to remove row in prefix group. In case of a very long row in prefix group it is impossible to remove the row because the button 'remove' is out of the window	In ARM 8.8 we redesigned this component in order to fix the issue. Even when the row (prefix with ranges) is very long the 'remove' sign is still shown and the prefix is shortened wit '…' in the presentation. The entire prefix can be shown in this case using tooltip.
ARM-2722	CDR files location cannot be configured. 1 All CDR messages are collected on a syslog server in JSON format. 2 Every 15 minutes the JSON is rotated. 3 At the end of the rotation, a bash script is executed where the JSON files are converted and manipulated for populating the CDR database. In the last step (during generation), the files *DropedCdrs.json* and *UnfinishedCdrs.json* are loaded and after CDR generation, are exported with the new unfinished and dropped CDRs. Also, the log file *CdrGenerator.log* is updated with log information. Note that the files are stored in the folder in which the cdrgenerator with which the user is currently executing, resides.	In compliance with customer requests, the path of the dropped and unfinished calls' CDRs can now be defined.
ARM-2713	ARM 8.6 doesn't function with the Mediant 3000 (fix propagation).	The fix was urgently provided as a maintenance release of ARM 8.6 and it is also propagated to ARM 8.8.
ARM-2631	The reason for calls dropped by the ARM is not correctly reflected in the OVOC. The issue arises when a call is rejected by the destination with a reason that does not appear (486) in 'SIP Alt reason' in the ARM. The SBC sends the OVOC a failure with the reason of **ARM Drop** even though the real reason is 486.	ARM 8.8 does not return 'Dropped call' as it is not the ARM which determines whether to drop the call. ARM 8.8 returns 404 (not found) if the number of the reason doesn't exist in 'Alternative Routing SIP Reasons' in the ARM.
ARM-2539	Data input into Source and Destination Prefixes in the GUI is problematic. After inputting data in the 'Prefix/Prefix Group' in 'Source' or 'Destination' and then leaving the drop-down list, the data is not inputted into the list. Only pressing the **Enter** key inputs the data. When leaving all other GUI components, the data is inputted into the list and it's unnecessary to press the **Enter** key.	The Add/Edit Routing Rule screen has been redesigned. In ARM 8.8, it supports the required functionality. Even if network administrators click **OK** without pressing the **Enter** key, the data is accepted by the GUI and transferred to the server side.
ARM-2294	The ARM's Web interface sometimes freezes and network administrators need to open a new window in the browser and log in again. The issue most often reproduces when performing	Several improvements were implemented when managing networks using LDAP Authentication.

Incident	Problem / Limitation	Comments/Solution
	LDAP Authentication. When using a local username (network administrator), the issue occurs less frequently.	
ARM-2875	The SBC strips the PID after a call is routed via the ARM. The ARM changes the header flag to 'hide'.	ARM 8.8 resolves the issue in combination with a fix at the SBC level (SBC-14902). The ARM fix is to never 'hide' the PAI.

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
Number of CAPs	300 CAPs per ARM Router
Maximum number of supported ARM Routers	Tested up to 40
Maximum number of Routing Groups	Tested up to 2000
Maximum number of Routing Rules	Tested up to 5000
Maximum number of ARM Users (either local or LDAP)	250000 *
Maximum number of Nodes in ARM network	Tested up to 40
Maximum number of Peer Connections in ARM network	Tested up to 750
Maximum number of Connections in ARM network	Tested up to 40
Maximum number of Prefix Groups	Tested up to 3500
Maximum number of Prefixes in a single Prefix Group	Tested up to 2000
Maximum number of Normalization rules	Tested up to 2000

* This limit is configured in the basic ARM configuration. If necessary, it can be increased to up to 1 million.

This page is intentionally left blank.

7 Known Limitations and Workarounds

The table below lists the known limitations and workarounds in ARM 8.8.

Table 7-1: Known Limitations and Workarounds

Incident	Problem / Limitation	Comments/Workaround
-	Upgrading from version 8.2 (or earlier) directly to version 8.8 is not supported	Upgrade first to version 8.6 and then to version 8.8.
-	If the name of the ARM Router includes spaces, the ARM will not function successfully.	Change the name of the ARM Router if it includes spaces.
-	After an operator manually adds a new node to the ARM Topology, the attached Routing Server Group is not associated with the node even though it is shown in the GUI.	Edit the node's settings: Change the Routing Server Group to another value and then change it again back to the original (required) value.
-	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 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).	-
-	The redesigned ARM 8.8 Add Routing Rule – Routing Actions screen does not feature the 'via' action as previous versions did.	Customers upgrading from a previous version will still view the action but are advised to exclude it from routing definitions. In future, the feature will be redesigned and reincorporated for a friendlier user experience
-	Upgrading from ARM 8.6 to ARM 8.8 does not preserve calls (CDRs) information on calls run by ARM 8.6.	If a customer needs calls information from ARM 8.6, contact AudioCodes support (R&D) for the procedure to back up calls (CDRs) information.

Incident	Problem / Limitation	Comments/Workaround
-	Miscellaneous issues with the ARM GUI after upgrading from ARM 8.6 to ARM 8.8.	Customers are requested to clear the browser cache after performing a software upgrade (**Ctrl**+**F5**).
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 network administrator 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.
ARM - 3030	When removing or changing the user's property, which is mapped to Active Directory attribute the action does not success but the error message is not shown.	The most important thing is that the property is not changed or deleted (as Active directory hosts the information).

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/

LTRT-41949