Version Description Document (VDD)
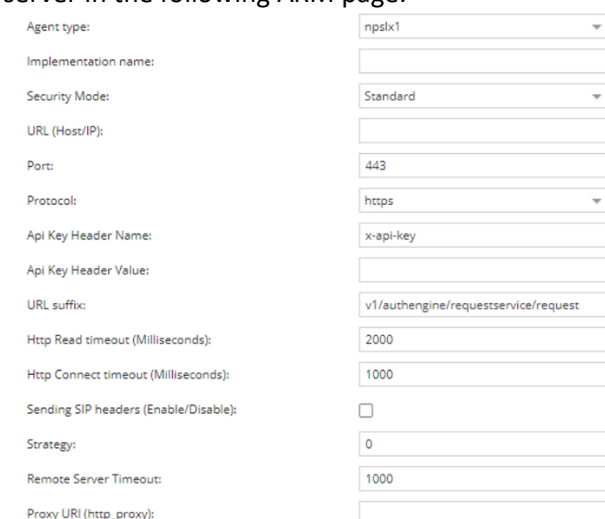
Patch Release Ver. 9.6.24 (ARM 9.6 Fix 3)

This document serves as the Version Description Document (VDD) for AudioCodes Routing Manager (ARM).

Version Summary

Components	Description
Version Identifier	ARM 9.6.24 (ARM 9.6 Fix3)
Date	April 7, 2022
Version Objectives	Bug fixes; security vulnerabilities fixes; HTTP proxy support for SecureLogix Web service.
Basic Release Notes Document	This VDD is based on the ARM 9.6 Release Notes and ARM 9.6 Fix 2 VDD
Media DVDs Checksums	

Features

Incident Index	Incident Description
ARM-5519 BR-2780	Added the capability to define HTTP proxy URI for communication with SecureLogix (OrchestraOne) Web service. This capability was also added to the configuration of the web server in the following ARM page:

Agent type: npslx1

Implementation name:

Security Mode: Standard

URL (Host/IP):

Port: 443

Protocol: https

Api Key Header Name: x-api-key

Api Key Header Value:

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

Proxy URI (http_proxy):

Bug Fixes

Incident Index	Incident Description
ARM-5439	If an alternative route exists in a call from/to a customer, the ARM Router sends call-info via the third alternative route even though it's not relevant to 'customers' (does not have 'customer' as a routing rule condition, but only matches other call criteria).
ARM-5440	When collecting logs from the ARM Router, the dump command results in an error message with no database output.
ARM-5447	RADIUS authentication doesn't allow a password of more than 16 characters; RADIUS 2.0, which allows more characters, is not yet supported.
ARM-5460	An operator with a security level of 'Admin' cannot change their own password. An operator of security level 'Security Admin *can* change their own password but configuring the operator with this security level is not an option when the customer wants to prevent the operator from changing/deleting/creating other accounts.
ARM-5537	Urgent fix for active exploitation of a vulnerability in the Spring Framework designated as CVE-2022-22965 that allows malicious actors to download malware.
ARM-5372	The ARM's sessions count steadily increases over time and does not decrease, even at midnight after users have left work and no calls are made. The high session count triggers CAC, forcing the operator to set the CAC limit artificially higher (the operator has a single customer which they divided into two 'Customers' in the ARM with different CAC policies for each).
ARM-5436	A possible issue with CAC calculation and customer session reporting was encountered in ARM 9.6.19. In their deployment, the customer defined CAC profiles and a 'Customer' based on Prefix Groups. CAC alarms occurred and it was observed that the status of the defined 'Customer' was blocked, even though traffic was light, raising suspicions of an issue.
ARM-5535 (partially fixed)	Azure AD connectivity issues were encountered by a customer whose users were defined with directoryRoles (memberOf).
ARM-5442	The customer's security department has flagged vulnerability to Log4j even after applying the 'AudioCodes Response to Security Vulnerability – Apache Log4j 2 (CVE-2021-44228)' in compliance with 'Product Notice #0449' and updating to ARM 9.6.21. Only an ARM Router is getting flagged, not the ARM Configurator or the other routers.

Known Limitations and Workarounds

Index	Limitation and Workaround
1	Refer to the limitation in the document ARM 9.6 Release Notes

Documentation

- N/A

Special Instructions

- Clean Install is supported on all ARM supported platforms
- Upgrade is supported from 8.8.xx, 9.0.xx, 9.2.xx, 9.4.xx and 9.6.xx versions on all supported ARM platforms