



AI Ops / Alite

AMELIA's Autonomic IT Management Platform

Release Notes 3.10.0 (Document Version 1.0)

This AMELIA® documentation is copyright © 2025 Soundhound AI Amelia and their affiliated companies. All rights reserved.

This document is considered the confidential information of Soundhound AI Amelia and its affiliates. Disclosure to other parties is prohibited unless agreed to in a license or confidentiality agreement.

Trademarks, including AMELIA® and the AMELIA logo, are the intellectual property of Soundhound AI Amelia and its affiliated companies. Any other marks or intellectual property remain the property of their respective licensors or owners.

Table of Contents

1. RELEASE 3.10.0 3

1.1 RELEASE HIGHLIGHTS 3

1.2 BUGS 3

1.3 EPIC 3

1.4 STORY 4

1.5 TASKS..... 4

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	March 4, 2025	Added tickets for 3.10.0 release notes	Yes

1. Release 3.10.0

This section briefly lists changes to AIOps ALite for this release.

1.1 RELEASE HIGHLIGHTS

None with this release.

1.2 BUGS

- **Enhancement to Automations HTTP Client for Redirect Handling.** The Automations HTTP client was modified to follow HTTP 301 redirects automatically, aligning its behavior with common HTTP client standards and expectations. The change does not directly affect the UI as it pertains to the backend behavior of the Automations HTTP client component. The purpose of this change was to ensure that the HTTP client correctly follows redirect responses (such as HTTP 301), thereby completing requests and returning the redirected content as expected. This improvement resolves issues where the client previously would not follow redirects, potentially leading to incomplete data retrieval or errors. This change affects backend operations, improving the reliability and functionality of automated tasks that depend on HTTP requests handling redirects seamlessly. Users involved in automation setup and backend processes are indirectly affected by the improved capabilities of the system. (AP-30697)
- **Fixed Class/Type Errors in Automation Following HTTP State.** This ticket addresses and fixes the issue where automation states intermittently failed with class/type related errors when executed following an HTTP state. The change is not directly visible in the UI as it pertains to backend processing of automation sequences that include HTTP states. The purpose of this change was to resolve intermittent failures due to class/type errors, ensuring smoother execution and reliability of automation sequences that include HTTP states. This change primarily affects backend processes, particularly developers and system administrators managing automation sequences. It indirectly enhances the reliability of systems for end-users relying on these automations. (AP-30703)
- **Resolved Connection Issue with Long SQL Command Execution.** A connection failure issue that caused SQL command execution to be interrupted with a Connection refused error has been resolved. There was likely no direct change in the user interface; instead, the issue was addressed in the underlying processes handling SQL command executions. The purpose of this change was to ensure that SQL commands, regardless of their length, can execute without encountering connection issues, thereby improving system reliability and performance. This change primarily affects backend processes but indirectly benefits end-users by eliminating disruptions related to SQL command executions. (AP-30715)

1.3 EPIC

None in this release.

1.4 STORY

- **Enhancements for Configurable Retry Mechanism in Automation Engine's HTTP Request State.** A configurable retry mechanism was introduced for the HTTP Request State in the automation engine. This includes setting options for retry count, retry timer, and request timeout. These features ensure stable and robust automated workflows by handling transient errors more efficiently. The changes can be configured in both the Automation Settings view and Automation Workplace. These interfaces now allow administrators and automation developers to set default values and override retry settings for HTTP requests. The purpose of these changes is to increase the reliability and effectiveness of automated workflows by allowing them to manage transient errors through configurable retry attempts with specified timeouts and delay strategies, including exponential backoff between retries. This change primarily affects backend processes and is designed with backend users in mind, including administrators and automation developers who configure and manage automation workflows. It ultimately benefits end-users by improving the stability of automated processes. (AP-29448)

1.5 TASKS

- **Upgraded Libraries to Address Security Vulnerabilities in IPautomataLite.** The libcrypto library was upgraded from version 3.3.2-r1 to 3.3.3-r0 to address vulnerabilities CVE-2024-13176 and CVE-2024-12797. Additionally, the netty library was upgraded from version 4.1.115.Final to 4.1.118.Final to remediate CVE-2025-24970. This change is not reflected in the UI as it pertains to backend library upgrades targeting security vulnerabilities. The purpose of this change was to enhance the security of the IPautomataLite component by patching known vulnerabilities in the library dependencies, ensuring the system's integrity and protection against potential security threats. This change affected the backend of the system, primarily targeting developers and system administrators responsible for maintaining system security. It is not directly customer-facing but enhances the overall security of systems users may interact with. (AP-30662)