

# Autonomics / Alite

## AMELIA's Autonomic IT Management Platform

---

### Release Notes 3.14.0 (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 3.14.0 ..... 3**

1.1 RELEASE HIGHLIGHTS ..... 3

1.1.1 PAGE SIZE LIMIT ENFORCEMENT ..... 3

1.1.2 API DEPRECATION NOTICE: ATTACHMENT ENDPOINTS ..... 3

1.2 BUGS ..... 3

1.3 EPIC ..... 4

1.4 STORY ..... 4

1.5 TASKS ..... 4

## Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	July 2, 2025	Added tickets for 3.14.0 release notes	Yes

# 1. Release 3.14.0

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

## 1.1 RELEASE HIGHLIGHTS

---

### 1.1.1 Page Size Limit Enforcement

In an upcoming release, we will enforce a maximum page size limit of 100 items across all paginated REST API endpoints.

#### WHAT'S CHANGING

- Clients requesting more than 100 items per page will receive a 400 Bad Request response.
- This change improves performance, prevents timeouts, and ensures more consistent API response times.

#### RECOMMENDED ACTION

- Review your API usage and update any requests specifying pageSize > 100 to comply with the new limit.
- If your integration relies on larger payloads, consider processing results across multiple pages.

This change will be introduced in version **3.17.0** or later (exact version to be confirmed). Please plan accordingly.

### 1.1.2 API Deprecation Notice: Attachment Endpoints

The following attachment-related APIs are deprecated and will be removed in version 3.17.0 or later (exact version to be confirmed). Please update your integrations accordingly.

Deprecated Endpoints:

- POST /api/attachments  
Replaced by: POST /api/tickets/{ticketId}/attach
- GET /api/attachments/{attachmentId}/content  
Replaced by: GET /api/attachments/{attachmentId}/download

We recommend updating your implementations to use the new endpoints to ensure continued functionality.

## 1.2 BUGS

---

- **Resolved Discrepancy in ALites Connection Status Display.** The issue causing the ALites connection status to inaccurately display as Disconnected even when the ALite is functioning correctly was resolved. The change specifically impacted the area of the UI where ALites connection status is displayed to users. The purpose of

this change was to rectify the misleading status display, ensuring users can accurately monitor and manage the operational status of their ALites. This change is backend-focused but impacts the customer-facing experience by improving the accuracy of status information displayed to users. (AP-31384)

## 1.3 EPIC

---

None in this release.

## 1.4 STORY

---

- **Enhancement of Outbound SMTP Email Integration for Diverse IT Environments.** The system now supports outbound email functionality through any standard SMTP server, with options for authenticated and unauthenticated configurations. It includes support for various authentication methods (LOGIN, PLAIN) and secure connection protocols (STARTTLS, SSL). The user interface allows configuration of SMTP server details, such as hostname and custom port numbers. The change occurred in the email integration settings within the user interface, where users can now configure SMTP server details, choose between authentication options, and secure connection methods. The UI also includes settings related to hostname and port configuration. The purpose of this change is to enhance the flexibility and compatibility of the platform's email capabilities across diverse IT environments by allowing users to send automated emails through any standard SMTP server. This enhancement aligns with security best practices by securely managing credentials and supports a variety of secure transmission methods. This change is primarily customer-facing, as it enhances the options available to end-users and administrators when configuring outbound email capabilities in the platform. However, it also requires backend updates to handle the various connection protocols and authentication methods securely. (AP-31056, AP-31057)

## 1.5 TASKS

---

- **Upgrade Dependencies to Mitigate ALite Security Vulnerabilities.** Dependencies used by IPautomataLite were upgraded to their latest supported versions to address and remediate identified security vulnerabilities. This change does not affect the user interface; it involved backend dependency upgrades. The purpose of this change was to ensure the security and stability of the application by mitigating known vulnerabilities in the dependencies. This change affected the backend systems. It is not customer-facing and does not impact the user interface directly. (AP-31496)
- **Upgrade Dependencies to Mitigate ALite Security Vulnerabilities.** Dependencies were upgraded to their latest supported versions, excluding Python-related dependencies such as pip and setuptools, to address and remediate existing security vulnerabilities in the ALite component. The change does not directly impact the user interface as it involves backend dependency updates. The purpose of the change was to mitigate security vulnerabilities identified in the ALite component by updating dependent libraries and tools to ensure the system remains secure and up-to-date. This change affects the backend systems and is not directly customer-facing. It ensures enhanced security and stability within the backend infrastructure. (AP-31359)