SoundHound AI AMELIA

Autonomics

AMELIA's Autonomic IT Management Platform

Release Notes 3.13.0

(Document Version 1.0)

Table of Contents

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	June 4, 2025	Added tickets for 3.13.0 release	Yes

1. Release 3.13.0

This section briefly lists changes to Autonomics for this release.

1.1 Release Highlights

1.1.1 Rollback to a previous version

Database schema is not compatible with previous releases. Once updated, it is not possible to rollback to the previous version without restoring from the backup.

1.1.2 MID-server Endpoint Proxy Support for Events and Metrics

ALite has been updated to function as an Integration Endpoint Proxy. As a result, it now starts a web server that listens on port 8443 by default. This can be changed using the following property:

```
server.port=8443
```

By default, a self-signed certificate for localhost is used. However, it is recommended to configure a valid certificate instead. The relevant properties are:

```
server.ssl.key-store=/full/path/to/file
server.ssl.key-store-password=
server.ssl.key-alias=
server.ssl.key-store-type=
```

1.1.3 HashiVault Certificate Authentication

HashiVault authentication using client certificates has been introduced. Certificates can be stored either in Locksmith or on the ALite file system.

To use certificates stored in Locksmith, define the **HashiVault Certificate Locksmith Element** on the connection and point it to the corresponding Locksmith entry.

To use certificates stored on the ALite file system, configure the following absolute paths on the connection:

- **HashiCorp Vault TLS Certificate Path** (required)
- **HashiCorp Vault TLS Private Key Path** (required)
- **HashiCorp Vault CA Certificate Path** (optional if the server uses a certificate signed by a CA that is already trusted by system's trust store)

1.1.4 Payload-Level Authentication for Event Ingestion

Native event and metric integrations have been enhanced to support authentication details within the event payload.

When **Enable payload-based authentication** is activated, an additional attribute should be included to carry the Platform token.

```
"attributes": {
    "${authFieldKey}": "<integration_platform_token>"
}
```

The name of this attribute is specified by the new field, "Authentication field key."

1.2 BUGS

- **Resolved Dry Run Import Error for Linked Automations in Content Packs.** A dry run import error that occurred due to linked automations in content packs has been addressed and resolved. The change occurred within the content pack upload/import functionality on the Autonomics platform under the client SH Enterprise backups. The purpose of this change was to fix a dry run import error where linked automatons, specifically between parent and child automations, resulted in an internal server error preventing proper validation during the import process. This change affects the backend system handling the import processes and may indirectly affect users attempting to import content packs containing linked automations. (AP-31026)

- **Corrected Error Message for Empty or Unknown Client in Automation Create Task Block.** The error message that appears when a Create Task block in an automation has no client or an unknown client has been updated to provide a clearer and more specific message. The change impacts the error message displayed in the workflow logs within the automation tool interface. The original error message was vague and did not clearly indicate the issue's cause. The new error message provides explicit information about the absence or invalidity of a client ID, aiding troubleshooting efforts. This change affects backend processes, specifically those involved in workflow automation error logging and diagnostics. (AP-31202)

- **Restore Scroll Bar Functionality for Workflow Options in Change Requests.** A scroll bar has been reinstated for the workflow options list in the Change Request tickets. Previously, if a user from any of the selected approval groups attempted to approve a change, the list would become truncated, cutting off some options and causing usability issues. The change was made in the workflow options button within the Change Request tickets section of the Autonomics interface. The purpose of this change was to resolve a UI issue encountered by users where the workflow options list was getting truncated without a scroll option, particularly when all 4 approval groups were selected. Reintroducing the scroll bar enhances user experience by allowing all options to be accessible regardless of screen resolution. This change is customer-facing, as it directly affects the user interface experience for end-users working with Change Request tickets on the Autonomics platform. (AP-31204)

- **Resolved Overlapping Issue in Settings Tab for Themes and Virtual Hosts.** The ticket addressed the overlapping issue in the Settings tab where the Themes and Virtual Hosts sections were overlapping

with each other, resulting in a requirement to zoom out to 80% for proper viewing. This issue has been resolved. The change took place in the Settings tab of the UI where the Themes and Virtual Hosts sections are displayed. The layout was adjusted to accommodate both sections without overlapping. This change enhances the user interface by ensuring the Themes and Virtual Hosts sections are clearly visible without the need for users to adjust the zoom level. This improves the user experience and interaction within the Settings tab. This change is customer-facing, as it impacts users interacting with the Settings tab in the UI. (AP-31209)

- **Fix for JDBC Driver Class Loading Error in Automata Execution.** The issue with the JDBC driver class not being loaded, resulting in execution failures for SQL, MySQL, and PostgreSQL jobs in Automata, has been resolved. This change ensures that JDBC driver classes are correctly identified and loaded during the execution of automatic jobs. There was no direct change in the UI, as this fix pertains to backend operations involving the execution of automatic jobs using JDBC connections. The purpose of this change was to rectify a connectivity issue caused by the failure to load the JDBC driver classes. This was essential to allow successful execution of automation jobs that interact with SQL databases, thus restoring the normal operation of these processes. This change primarily impacted the backend, specifically affecting developers and system administrators who rely on Automata for executing database-related jobs. It indirectly benefits end users who depend on these backend processes. (AP-31217)

- **Resolution of Field Mismatches in Reporting and Workspace Views for Autonomics Tasks.** This ticket addresses the issue of mismatching field values, specifically the Owner and Owner email fields, between task details and the views offered in Reporting and Workspace. The system has been updated to ensure consistency across these fields post an upgrade. The change specifically took place in the Workspace and Reporting views of the Autonomics platform, ensuring that the information displayed matches the detailed information seen within individual ticket details. The purpose of this change was to correct discrepancies in data presentation across different views within the Autonomics platform. These mismatches were reported by the client, Chemours, as they led to confusion and possible errors in task management and reporting.This change primarily affected customer-facing aspects of the platform. It ensures that the Chemours team, utilizing the Autonomics platform, sees consistent data across all parts of their interface. The backend work was done to fix these inconsistencies, enhancing the reliability of user-facing components. (AP-31244)

- **Resolve Empty Client Field in Clients Drop-Down After Login.** The issue of the client field being empty in the Clients drop-down menu after a user successfully logs into the instance has been addressed and resolved. The change occurred in the Clients drop-down menu within the application's user interface, which is accessed after the user logs into their account. The purpose of this change was to fix a defect where the client field appeared empty, improving the user experience by ensuring that necessary client information is displayed correctly upon login. This change primarily affected the customer-facing side of the application, as it relates to the user interface that customers interact with during the login process. (AP-31249)

- **Resolve Task Creation Failure in Zabbix Integration for Autonomics v3.** This ticket addresses the issue where the Zabbix integration (pat_zabbix) is not successfully creating tasks in Autonomics version 3.5.1, although it was working as expected in version 2. The debugging has revealed that while data retrieval

appears correct, task creation fails. The change impacts the backend integration flow of Autonomics with Zabbix, specifically around the task creation process which might not directly reflect in the UI, but would affect the outcomes and alerts managed within the Autonomics platform. The purpose is to ensure that the integration between Autonomics v3 and Zabbix creates tasks successfully. The failure in task creation despite successful data retrieval needs to be resolved to maintain consistent alert processing and workflow automation. This change affects the backend processing of tasks and is crucial for teams relying on automated task creation through integrations in Autonomics, such as IT operations and system administrators. (AP-31253)

- **Improved User Feedback for Failed Deletion in Authentication System.** The system now provides a more user-friendly error message when an attempt to delete the IPsoft LDAP authentication system fails due to a database foreign key constraint violation. The change is reflected in the error messaging dialog that appears when a deletion attempt of an authentication system is unsuccessful. The purpose of this change was to offer clearer, more understandable feedback to users when they encounter a failure due to database constraints, improving the overall user experience by reducing confusion and aiding in troubleshooting. This change affects customer-facing aspects of the user interface, particularly users (e.g., administrators) attempting to manage authentication systems within the platform. Backend processes were not directly altered. (AP-31268)

- **Improved Error Messaging for Invalid SAML Login Script.** The error messaging for invalid SAML login scripts has been enhanced to provide more informative feedback. The error message now explains the issue more specifically and includes an Audit Log Entity ID for reference. The change occurs in the error message dialog box that is displayed to users when an invalid SAML login script is encountered. Additionally, users can view the script error by clicking on the Note field in the audit record. The purpose of this change is to enhance the troubleshooting process for users who encounter an invalid SAML login script error. By providing more detailed error messages, users can understand the issue better and reference the Audit Log Entity ID when seeking support. This change is customer-facing as it directly impacts users who interact with the system's login functionality and receive error messages when issues arise with the SAML login script. (AP-31276)

- **Refined LDAP Group Sync to Extract CN Values Correctly.** The LDAP group extraction process has been modified to correctly extract the CN (Common Name) value from the `memberOf` attribute, rather than using the entire string for group synchronization. There was no change in the user interface (UI) as this modification pertains to backend processing. The purpose of this change is to improve the accuracy of group synchronization by ensuring only the CN value is used as the Login Group code, in accordance with expected behavior. This prevents potential issues caused by using the entire `memberOf` attribute string. This change affects the backend, specifically the mechanism for LDAP group synchronization. It is not directly customer-facing, but enhances internal processes that can impact user management indirectly. (AP-31313)

- **Fixed Redirect Loop Issue on Login Page After Session Expiry.** The issue causing the redirect loop on the login page after a session expiry was fixed. Additionally, the problem with the API endpoint not returning data and resulting in an HTTP 204 status was addressed. The change impacted the login page experience, specifically addressing the redirect loop scenario users encountered upon session expiry. The change was implemented to resolve the user experience issue where users could not access the

login page after their session expired, due to an infinite redirect loop. This fix also aimed to correct the API behavior, which was improperly providing an HTTP 204 status without returning data. This change affected both backend processes and the customer-facing login experience. The backend API behavior correction and frontend redirect loop fix are parts of the solution. (AP-31325)

- **Session Timeout Compliance Issue on Password Policies.** The session timeout behavior was modified to ensure that user sessions are logged out according to the timeout value specified on the Password Policies page. The discrepancy between the intended and actual session expiration times was fixed. The change affects the backend functionality related to user session management, specifically tied to the configurations set on the Password Policies page. There is no direct visible change in the UI, but the session handling logic was adjusted to adhere to the policy settings. The purpose of the change was to correct the session timeout mechanism, ensuring that sessions expire precisely according to the duration defined by administrators in the Password Policies page. This fixes the previous inconsistency where the session was not expiring as expected, leading to potential security concerns. This change primarily affects internal backend processes and indirectly benefits all users by enforcing more accurate session timeout policies. There is no direct impact on the visible UI for end-users, but system administrators and security teams benefit from improved compliance to configured security settings. (AP-31328)

1.3 EPIC

None in this release.

1.4 STORY

- **Enhancement for Date Management in Workflow Variables.** A feature was added to workflow variables of type Date, allowing users to set restrictions and options for date entries. This includes allowing users to specify whether dates should only be in the future or if dates from the past are also acceptable. Additionally, users can set default dates to the current time or an offset future date/time. The change was implemented in the workflow variable settings interface of the IPworkflow component, where users define and manage date variables. It includes the ability to set restrictions, choose default values based on creation or start times, and view validation messages. The purpose of this change was to provide users with greater control and flexibility over date variables in workflows. This allows for better date management and provides users feedback on invalid entries, ensuring workflows adhere to specific temporal criteria set by the users. This change is primarily backend-focused but affects end-users who create or manage workflows involving date variables. It enhances the user experience by adding more customizable options and clear validation feedback within the workflow system. (AP-29601, AP-30083)

- **Implement Filter for Automation Executions by Name in Execution Log.** A filter option was added to the Automation Execution view that allows users to filter automation executions by selecting a specific automation name from a dynamically populated dropdown list. The dropdown also retains the five most recently selected automation names for quicker access in the future. The change occurred in the Automation Execution view, where the new filtering functionality by automation name has been implemented. The purpose of this change is to enhance the user experience by enabling users to conveniently view and manage automation executions related to specific automations. This assists users

in focusing on relevant data and streamlines the process of finding executions for specific tasks. The change is customer-facing, affecting end-users who interact with the Automation Execution view in the application's UI. (AP-29866)

- **Automation Designer: Display Variable Default Values in Properties.** A new column labeled Default Value has been added to the Variable List in the automation designer, allowing users to view the default values of variables directly without needing to access additional menus. The change occurred in the Variable List section of the automation designer, where the new Default Value column is now present. The purpose of this change is to improve user efficiency and streamline the user experience by allowing users to quickly and easily identify default variable values. This eliminates the need for additional clicks and navigation, reducing user friction. This change is customer-facing, affecting users interacting with the automation designer interface. (AP-30435)

- **Add Certificate-Based Authentication for HashiVault Integration in Automations Lite.** Support for certificate-based authentication has been introduced for HashiVault integrations within Automations Lite. This enhancement allows for the use of client TLS certificates for secure authentication, complementing existing credentials-based methods. The changes are manifested in the configuration settings related to authentication methods within Automations Lite. Users can now choose and configure certificate-based authentication as an option for HashiVault integrations. The purpose of this change is to provide a more secure, certificate-based authentication method for environments integrating HashiVault with Automations Lite. This enhancement caters to users requiring robust identity verification to ensure the integrity and security of their credentials. This change affects both backend processes and customer-facing configurations, as it involves backend authentication mechanisms and provides an additional option for end-users administrating authentication settings in Automations Lite. (AP-30469)

- **Introduce Payload-Level Authentication for Legacy Event Integration Systems.** Native event integrations now support authentication through the event payload itself, allowing systems that can't control HTTP headers to authenticate successfully. A checkbox for Authentication in Payload and a configurable text box for specifying the authentication field name were added to the integration configuration UI. The change enables legacy systems, which lack the ability to control HTTP headers, to utilize our event integration by supporting authentication via the payload. This change affects both backend processes and customer-facing elements within the event integration setup. (AP-31017, AP-31252)

- **MID-server Webhook Proxy Support for Secure Event and Performance Metric Integration.** Support for webhook endpoints is extended to use the MID-server to enable event and performance metric data transmission, ensuring adherence to compliance and security requirements for customers that restrict infrastructure exposure. This change does not reflect directly in the end-user interface but affects how webhooks interact with the MID-server for backend processing, allowing users to configure and manage webhooks through the existing MID-server setup. The purpose of this change is to allow customers with stringent security and network policies to send event and performance metric data securely through a MID-server instead of directly exposing platform endpoints. This enables compliance with security standards while ensuring seamless data integration. This change primarily affects the backend,

specifically targeting customers who need secure data routing options via the MID-server for event and performance metric ingestion, without exposing their infrastructure externally. (AP-31066)

- **Rename Webhook Integrations to Inbound Endpoints in the UI.** The names of several webhook integrations have been updated to Inbound Endpoints to better represent their functionality. The changes will appear in the integrations section of the application interface. The purpose of this change is to enhance clarity and accuracy in how these integrations are described within the application, aligning their names more closely with their actual operations. This change is customer-facing, specifically affecting users interfacing with the UI to manage or utilize integrations. (AP-31278)

1.5 TASKS

- **Enhanced Java Integration Page with Metadata Default Values and UI Consistency.** Default values from metadata.json are now automatically populated in text fields upon uploading a fat jar, a default value is set for the platform token header, users can inquire about selecting multiple files via the Import Properties button, and the capitalization of default properties titles has been standardized. The changes are reflected on the Java Integration edit page where fat jars are uploaded, specifically in the metadata text fields, platform token header field, the Import Properties button, and in the titles of default properties. The purpose of these changes was to enhance user experience by ensuring data consistency and reducing manual input through automation of default values. Additionally, it aimed to unify UI consistency in title capitalization for better readability and improved usability. This change is customer-facing, impacting users interacting with the Java Integration feature to configure and manage integrations more efficiently and consistently. (AP-30884)

- **Improved User-Friendly Error Message for ConstraintViolationException on Client Code Input.** An error message displayed when a ConstraintViolationException is thrown due to exceeding the maximum length of a client code has been customized to be more user-friendly. The change affected the input fields where users create a new client and enter the client code exceeding the maximum allowed length. The purpose of this change was to provide users with a clear and understandable error message when they input a client code that violates the maximum length constraint, enhancing user experience. This was a customer-facing change, as it improves the error message seen by end-users during client creation in the UI. The change was made to the backend logic that handles these exceptions. (AP-31169)

- **Security Vulnerabilities Remediation through Library Upgrades**. The affected libraries, org.apache.httpcomponents.client5:httpclient5 and org.apache.tomcat.embed:tomcat-embed-core, were upgraded to newer versions, 5.4.3 and 10.1.40 respectively. This action mitigated several known security vulnerabilities (CVE-2025-27820, CVE-2025-24813, CVE-2024-50379, CVE-2024-56337, CVE-2025-31651, CVE-2025-31650). This change does not directly reflect in the UI, as it impacts the backend libraries of the application. The primary purpose of this change was to address and remediate critical security vulnerabilities identified in the specified packages, thereby enhancing the security posture of the backend system. This change primarily impacted the backend infrastructure of the application. It indirectly benefits end-users by ensuring a more secure and robust service environment but is not directly customer-facing. (AP-31185)

- **Enable SAML SP Metadata Generation Without Authentication System Activation.** The system now allows the generation of SAML Service Provider (SP) metadata even if the authentication system is not enabled. It performs necessary validation checks and generates SP metadata using provided information such as authentication system code and certificates, if any. This change is reflected on the authentication system page, where a highlighted link is provided. Clicking this link lets the user download the SP metadata XML. The purpose of this change is to allow Identity Provider (IDP) providers to obtain SP metadata needed to configure SAML authentication, even if the SP authentication system is not yet enabled. This facilitates easier setup and testing of SAML configurations before full activation. This change primarily affects backend operations but is customer-facing as it benefits users setting up SAML authentication configurations. (AP-31269)

- **Implementation of a Unified Header for Autonomics Platform.** A unified header with a waffle menu was implemented for the Autonomics platform that can display links to other SoundHound applications when expanded. The change appears in the header section of the Autonomics user interface. The purpose of this change was to unify the user interface across different SoundHound applications to improve navigation and accessibility, enhancing overall user experience. This change is customer-facing, affecting users who interact with the Autonomics platform and other linked SoundHound applications through the UI. (AP-31280)

- **Implement Audit Log for Script Errors in SAML and LDAP Authentication Systems.** Script errors for Client and Login Group scripts in both SAML and LDAP authentication systems are now being captured in the Audit log. Additionally, a Request ID is provided for LDAP script errors. For SAML, this change doesn't directly affect the UI as it logs errors backend. For LDAP, if the UI does not show the message alongside the Request ID, a separate UI-specific ticket will be created to address this. The purpose of this change is to enhance the debug ability and monitoring of authentication system processes by logging script errors in the Audit log. This will assist in more efficiently identifying and resolving script-related issues. This change primarily affects the backend systems, enhancing internal logging and tracking capabilities. Customer-facing impact is minimal unless a UI adjustment is required to show messages along with the Request ID for LDAP. (AP-31286)

- **Enable All Locksmith Element Types in Connection Selector for Greater Flexibility.** The change allows users to select Locksmith elements of any type for all connection types, rather than filtering them based on predetermined connection types. The change was implemented in the connection selector interface within the UI, impacting how users choose Locksmith elements when establishing connections. The purpose of this change is to provide flexibility by recognizing that multiple Locksmith types (such as Generic Password, SSH, or Certificate) may be applicable to a connection type, such as SSH. By checking applicability at runtime, it ensures accurate selection and compatibility. This change is customer-facing, as it alters how customers interact with the interface when selecting Locksmith elements for connections. (AP-31318)

1.6 Sub-Tasks

None in this release.