

Classification: Internal

# HCLSoftware

## HCL BigFix AEX

**Agentic AI Platform**  
**Release Note**  
Version 13.0



The data contained in this document shall not be duplicated, used, or disclosed as a whole or in part for any purpose. If a contract is awarded to chosen parties because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets.

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at [www.hcl-software.com](http://www.hcl-software.com)

Copyright © 2026 HCL Technologies Limited.

# Table of Contents

|          |                                                                                   |           |
|----------|-----------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Executive Summary .....</b>                                                    | <b>5</b>  |
| <b>2</b> | <b>Key Features .....</b>                                                         | <b>6</b>  |
| 2.1      | Agent Observability and Traceability .....                                        | 6         |
| 2.2      | Centralized Role-Based Access Control (RBAC) .....                                | 6         |
| 2.3      | Prompt Engineering Suggestions .....                                              | 6         |
| 2.4      | Agentic AI Studio Enhancements .....                                              | 7         |
| 2.5      | Agent Versioning and Comparison .....                                             | 7         |
| 2.6      | Enhanced Knowledge Management Studio .....                                        | 7         |
| 2.7      | A2A Client: Agent-to-Agent Protocol Support .....                                 | 8         |
| 2.8      | Workflow Enhancements .....                                                       | 8         |
| 2.9      | Agent Portability .....                                                           | 8         |
| 2.10     | Agent Guardrails .....                                                            | 9         |
| 2.11     | Agent Risk and Prompt Evaluation .....                                            | 9         |
| 2.12     | Flexible Deployment Choice -SaaS and On-Premise Version .....                     | 10        |
| 2.13     | Kill Switch .....                                                                 | 10        |
| 2.14     | List of Supported OTB Tools .....                                                 | 10        |
| <b>3</b> | <b>HCL BigFix AEX Reference Architecture .....</b>                                | <b>12</b> |
| <b>4</b> | <b>HCL BigFix AEX Deployment Architecture .....</b>                               | <b>13</b> |
| 4.1      | For SaaS .....                                                                    | 13        |
| 4.2      | For On-Premise - (Customer managed Datacentre using Kubernetes on RHEL VMs) ..... | 13        |
| 4.3      | On-Premise (Customer managed Azure Subscription using AKS) .....                  | 14        |
| <b>5</b> | <b>Secure Release Checklist and Reports .....</b>                                 | <b>15</b> |
| 5.1      | Release Checklist (SaaS & On-premise) .....                                       | 15        |
| 5.2      | Packages included in HCL BigFix AEX (SaaS & On-Premise) .....                     | 15        |
| 5.3      | HCL AppScan SAST Reports (SaaS & On-premise) .....                                | 22        |
| 5.3.1    | SAST Report - AEX .....                                                           | 22        |

|          |                                                                   |           |
|----------|-------------------------------------------------------------------|-----------|
| 5.3.2    | SAST Report - Global Admin .....                                  | 23        |
| 5.3.3    | SAST Report - Secure Gateway .....                                | 23        |
| 5.3.4    | SAST Report - Scheduler .....                                     | 23        |
| 5.3.5    | SAST Report - AEX Analytics .....                                 | 24        |
| 5.3.6    | SAST Report - AEX Functions.....                                  | 24        |
| 5.3.7    | SAST Report - AEX Utilities.....                                  | 24        |
| 5.4      | HCL AppScan DAST Reports .....                                    | 25        |
| 5.4.1    | DAST Report - AEX Web (SaaS).....                                 | 25        |
| 5.4.2    | DAST Report - Global Admin (SaaS) .....                           | 26        |
| 5.4.3    | DAST Report - AEX (On-Premise) .....                              | 26        |
| 5.5      | Mend Security Reports (SaaS & On-premise).....                    | 26        |
| 5.6      | Security Penetration Testing Report.....                          | 27        |
| 5.7      | PSIRT Details .....                                               | 27        |
| 5.8      | Load Testing Reports .....                                        | 28        |
| 5.8.1    | For SaaS - .....                                                  | 28        |
| 5.8.2    | For On-Premise - .....                                            | 29        |
| 5.8.3    | For AKS Environment - .....                                       | 29        |
| <b>6</b> | <b>SaaS Security Controls .....</b>                               | <b>31</b> |
| <b>7</b> | <b>Application Security Controls (SaaS &amp; On-Premise).....</b> | <b>32</b> |
| <b>8</b> | <b>Known Issues .....</b>                                         | <b>34</b> |
| <b>9</b> | <b>Looking Forward .....</b>                                      | <b>36</b> |

# 1 Executive Summary

AEX v13 marks a significant advancement in the platform's evolution as an enterprise-grade agentic AI solution, with a strong focus on governance, portability, operational visibility, and execution at scale. This release strengthens the core capabilities enterprises need to build, manage, secure, and extend AI agents across increasingly complex business environments.

A major theme of v13 is trust and governance. With enhanced agent observability and traceability, centralized role-based access control, and expanded agent guardrails and risk evaluation, kill switch, organizations gain deeper visibility into agent behaviour, clearer auditability, stronger policy enforcement, and improved control over both agent design and runtime execution. The addition of input and output safeguards, along with PII and secret checks during knowledge onboarding, further strengthens safe enterprise adoption.

This release also improves the builder and lifecycle management experience through enhancements in the Agentic AI Studio, agent versioning and comparison, prompt engineering guidance, Knowledge Management Studio, and agent portability across environments. Together, these capabilities help teams create agents more efficiently, govern changes more effectively, and migrate complex agent configurations across development, staging, and production environments with greater consistency and lower operational risk.

On the execution and interaction front, AEX v13 expands platform reach with agent-to-agent protocol support and broader workflow enhancements that improve orchestration flexibility, extensibility, and runtime transparency.

Overall, AEX v13 reinforces the platform's direction as a governed, extensible, and enterprise-ready agentic AI platform – designed not only to accelerate intelligent automation, but also to ensure that agents can be deployed safely, migrated reliably, and operated with the visibility and control required by modern enterprises.

## 2 Key Features

This release includes the following list of new features & enhancements.

### 2.1 Agent Observability and Traceability

AEX v13 strengthens enterprise governance and runtime visibility through enhanced agent observability and traceability, helping teams monitor agent health, understand execution behaviour, and investigate issues with greater clarity.

**Key Enhancements:**

- Improved visibility into agent execution and failures across the lifecycle
- Better traceability of agent actions, decisions, tool calls, and system interactions
- Chronological view of execution flow to support troubleshooting and analysis
- Stronger auditability for agent-driven workflows and operational monitoring

**Business Impact:**

Helps enterprises improve agent reliability, simplify debugging, strengthen governance, and maintain better operational control as agent deployments scale.

### 2.2 Centralized Role-Based Access Control (RBAC)

AEX v13 enhances access governance with more centralized role-based access control, enabling enterprises to manage permissions with greater consistency across the platform.

**Key Enhancements:**

- More centralized administration of role-based permissions
- Better control over access to platform functions and agent-related operations
- Improved alignment of user access with enterprise governance requirements
- Stronger access separation across administrative and operational responsibilities

**Business Impact:**

Helps enterprises strengthen governance, reduce unauthorized access risks, and manage agentic operations with clearer and more scalable role-based control.

### 2.3 Prompt Engineering Suggestions

AEX v13 improves the agent design experience with Prompt Engineering Suggestions that help users refine prompts and strengthen agent behaviour during setup and tuning.

**Key Enhancements:**

- Guided suggestions to improve prompt quality
- Better support for refining instructions and agent behaviour
- Improved usability during agent configuration and iteration

**Business Impact:**

Helps builders create higher-quality agents faster, reduces trial-and-error during setup, and improves the consistency of agent responses.

## 2.4 Agentic AI Studio Enhancements

AEX v13 enhances the Agentic AI Studio with stronger builder capabilities for governed agent creation, including guardrail controls and improved reusable starting points for agent design.

**Key Enhancements:**

- Support for input and output gates through guardrail controls
- Better governance during agent design and response flow management
- Reusable agent template capabilities for faster setup
- Improved builder experience for creating and configuring agents more efficiently

**Business Impact:**

Accelerates agent creation while strengthening governance, helping enterprises build reusable, policy-aligned agents with greater speed and consistency.

## 2.5 Agent Versioning and Comparison

AEX v13 introduces agent versioning and comparison capabilities to make change management more controlled and transparent.

**Key Enhancements:**

- Save and manage multiple agent versions
- Switch between versions and rollback when needed
- Compare prompts and configurations across versions
- Improved lifecycle management for agent changes and updates

**Business Impact:**

Helps teams safely evolve agents over time, reduce deployment risk, and maintain stronger control over prompt and configuration changes.

## 2.6 Enhanced Knowledge Management Studio

AEX v13 enhances the Knowledge Management Studio with a richer UI and stronger content-processing capabilities to improve retrieval quality and governance.

**Key Enhancements:**

- Enhanced UI for knowledge management workflows
- Support for recursive chunking and semantic chunking
- Better content preparation for improved retrieval quality
- Sensitive-content scans during upload for PII and secrets detection

- Support for knowledge management on workflow console

**Business Impact:**

Improves knowledge ingestion quality, strengthens governance during content onboarding, and helps enterprises build more accurate and trustworthy retrieval-driven agent experiences.

## 2.7 A2A Client: Agent-to-Agent Protocol Support

AEX v13 expands interoperability with A2A client support, enabling AEX agents to securely consume and collaborate with external agents.

**Key Enhancements:**

- Support for agent-to-agent protocol-based communication
- Ability to consume external agents as part of broader workflows
- Secure message exchange and action triggering across agents
- Improved support for distributed and collaborative agentic use cases

**Business Impact:**

Enables more connected enterprise automation by allowing AEX agents to work alongside external agents, extending orchestration beyond a single-platform boundary.

## 2.8 Workflow Enhancements

AEX v13 strengthens workflow design and execution with multiple enhancements focused on usability, extensibility, visualization, and enterprise orchestration.

**Key Enhancements:**

- Execution flow visualization for better runtime transparency and troubleshooting
- Tool Library support within workflows for stronger reusability and orchestration
- Trigger node redesign for a more streamlined workflow authoring experience
- NiFi node support for broader enterprise workflow integration
- Quality-of-life improvements for workflow design and administration
- Proxy execution enhancements for shell, SSH, Python, and related execution scenarios
- Support for custom HTTP API call nodes to improve extensibility

**Business Impact:**

Improves workflow flexibility, visibility, and ease of use while enabling enterprises to build and manage more powerful cross-system automations.

## 2.9 Agent Portability

AEX v13 enhances agent lifecycle management with Agent Portability, enabling Tenant Administrators to selectively export an Agent along with its nested dependencies and reliably import it between different AEX environment (example- Development environment to Production environment).

**Key Enhancements:**

- Selective export of a LLM agent together with its dependent components
- Support for packaging nested dependencies including child agents, tools, workflows, functions, and global variables
- Reliable import into another environment with dependency validation
- Better consistency of agent configurations across dev, staging, and production environments
- Safer backup and migration of complex agent logic

**Business Impact:**

Helps enterprises simplify migration of complex agents across environments, reduce configuration drift, improve deployment consistency, and lower the risk of packaging or rollout errors.

## 2.10 Agent Guardrails

AEX v13 strengthens safe and governed agent execution with enhanced guardrails across both agent design and runtime interactions. This includes support for input and output guardrails, prompt and risk evaluation, and content checks for sensitive data during knowledge onboarding.

**Key Enhancements:**

- Support for input guardrails to help identify unsafe, adversarial, or policy-violating inputs before generation
- Support for output guardrails to validate responses against enterprise policies before they are returned to the user
- Sensitive-content checks for PII and secrets during knowledge upload and onboarding
- Improved governance controls for safer and more policy-aligned agent behaviour across the lifecycle

**Business Impact:**

Helps enterprises deploy agents more safely by strengthening policy enforcement, improving visibility into prompt and agent readiness, reducing the risk of sensitive-data exposure, and supporting more governed execution in enterprise environments.

## 2.11 Agent Risk and Prompt Evaluation

AEX v13 strengthens governance with Agent Risk and Prompt Evaluation, helping teams assess prompt quality and identify higher-risk agent behaviour before wider deployment.

**Key Enhancements:**

- Evaluation of prompts to improve quality and reliability
- Risk-oriented assessment of agent behaviour during design and validation
- Better visibility into prompt readiness before agent rollout
- Stronger support for governed and policy-aligned agent development

**Business Impact:**

Helps enterprises improve trust in agent behaviour, reduce rollout risk, and establish a stronger quality gate for production-ready agents.

## 2.12 Flexible Deployment Choice –SaaS and On-Premise Version

AEX v13 expands deployment flexibility by adding an Azure Public Cloud deployment support (Subscription owned by Customer) for AEX in addition to the existing On-Premise VMware (Customer owned Datacenter) based deployment and SaaS offering on IBM Cloud.

Organizations can now choose the deployment model that best aligns with their security, regulatory, and infrastructure needs.

### **Key Enhancements:**

Newly introduced Azure Public Cloud deployment for secure or regulated environments using Azure Native Services like Azure Kubernetes Service, Azure DocumentDB, Azure Key Vault, Azure Object storage, Azure Managed Redis and Azure Database for PostgreSQL.

### **Business Impact:**

Gives enterprises complete control over infrastructure, data, and compliance, expanding AEX's applicability across government, BFSI, healthcare, and high-security industries.

## 2.13 Kill Switch

AEX v13 introduces an Agent Kill Switch capability to help administrators quickly disable an agent when it should no longer be available for execution or user interaction. This control is available directly from the Agent Library through the three-dot menu on the agent card.

### **Key Enhancements:**

- Ability to disable an agent directly from the Agent Library
- Channel-level visibility during disablement, showing all channels where the agent is configured
- Option to disable the agent from associated channels through the 'disable confirmation' flow
- Disabled agents no longer show Play or Configure options, preventing further execution or modification from the card
- Centralized operational control to restrict agent availability when required

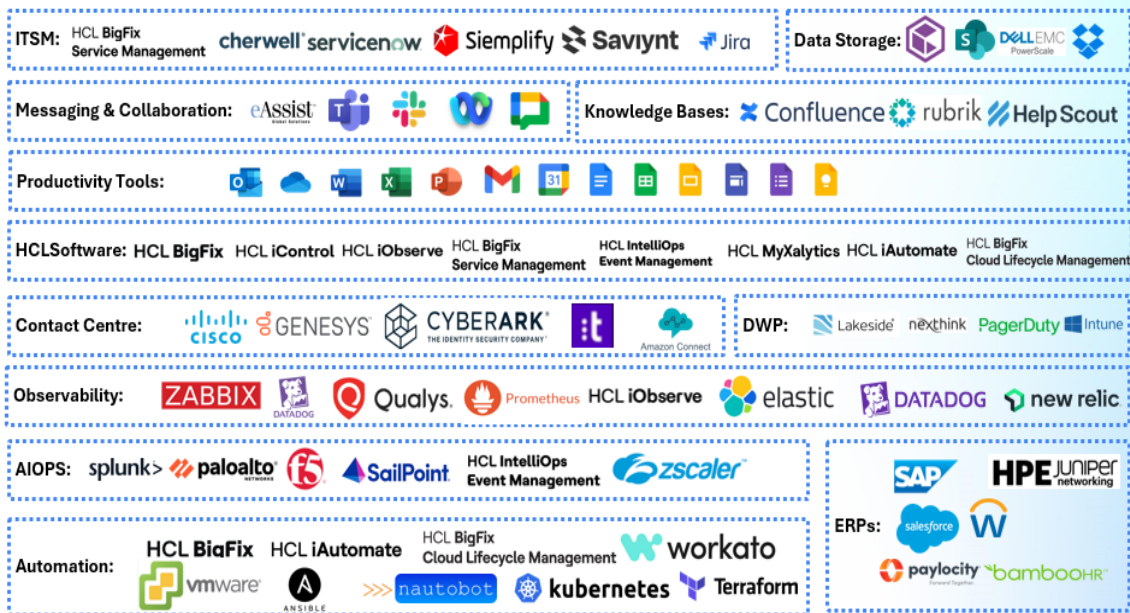
### **Business Impact:**

Improves operational control and governance by allowing administrators to quickly restrict agent availability across configured channels. This helps reduce risk in scenarios where an agent needs to be paused, withdrawn from user access, or prevented from further execution while review or corrective action is performed.

## 2.14 List of Supported OTB Tools

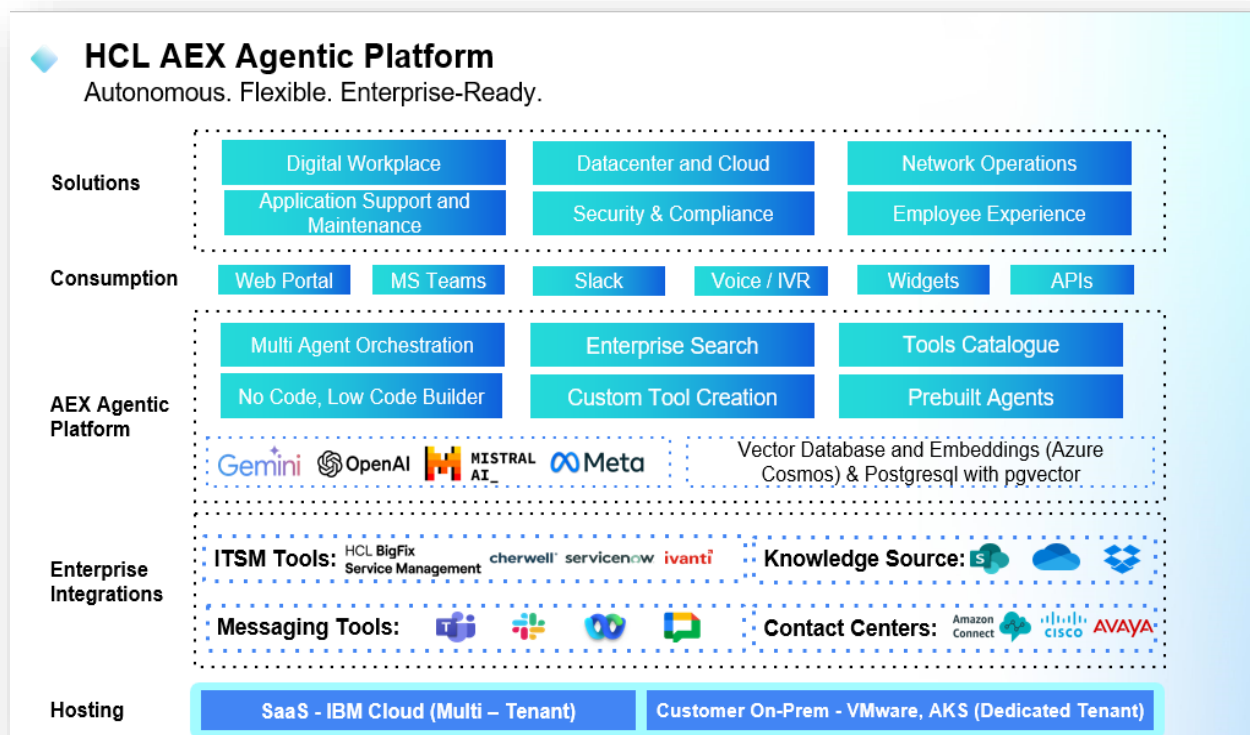
HCL BigFix AEX provides a flexible tool integration framework that enables agents and workflows to connect with enterprise systems through out-of-the-box tools, MCP-based integrations, and custom API integrations. These integrations allow AEX agents to retrieve information, execute actions, automate service requests, trigger workflows, and support cross-system orchestration across IT, HR, productivity, observability, automation, and business application ecosystems.

The tools listed below represent the supported out-of-the-box and feasible integration ecosystem for AEX.



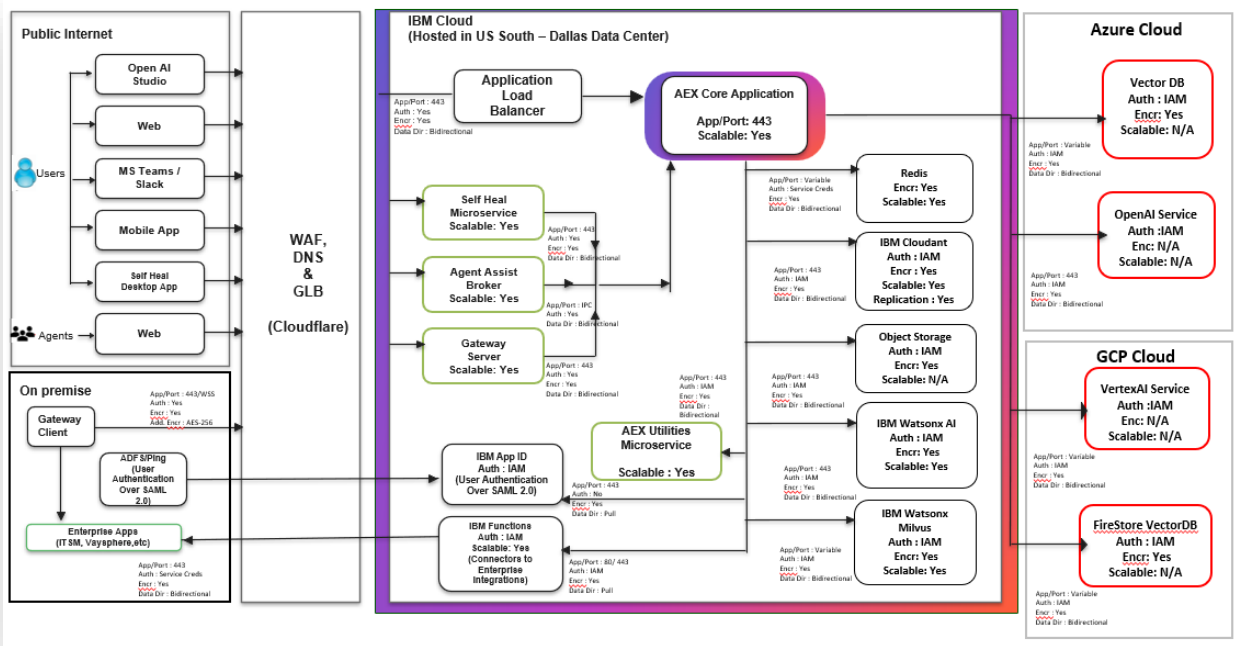
HCLSoftware

### 3 HCL BigFix AEX Reference Architecture



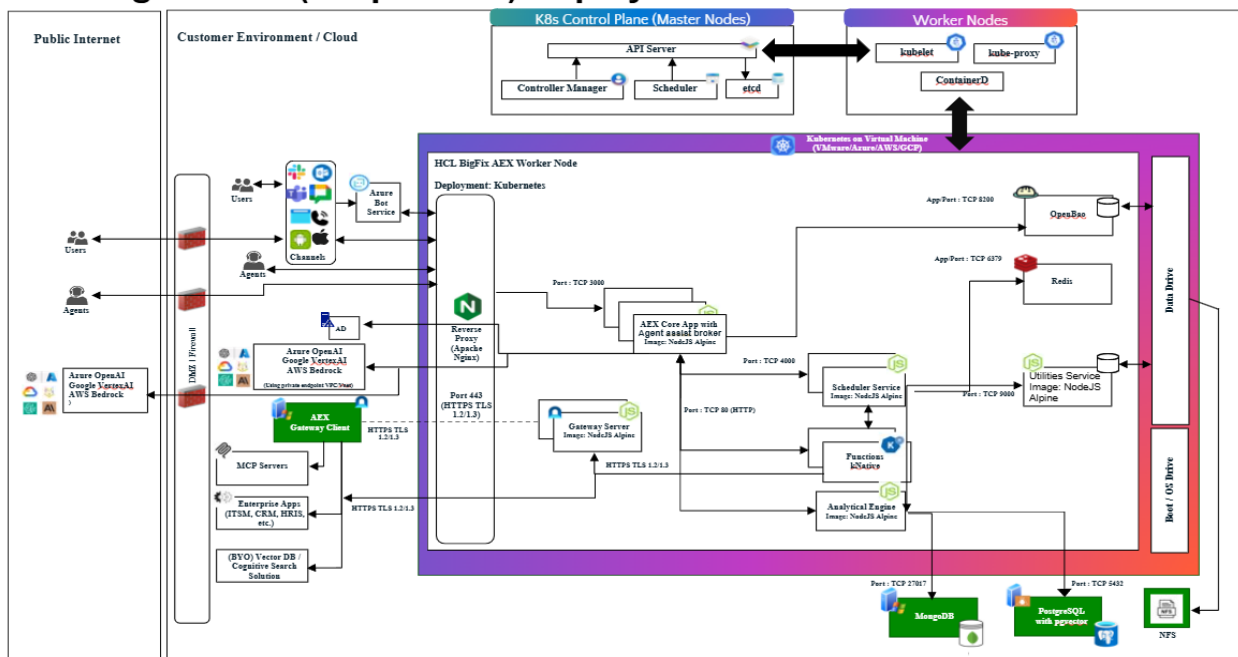
## 4 HCL BigFix AEX Deployment Architecture

### 4.1 For SaaS



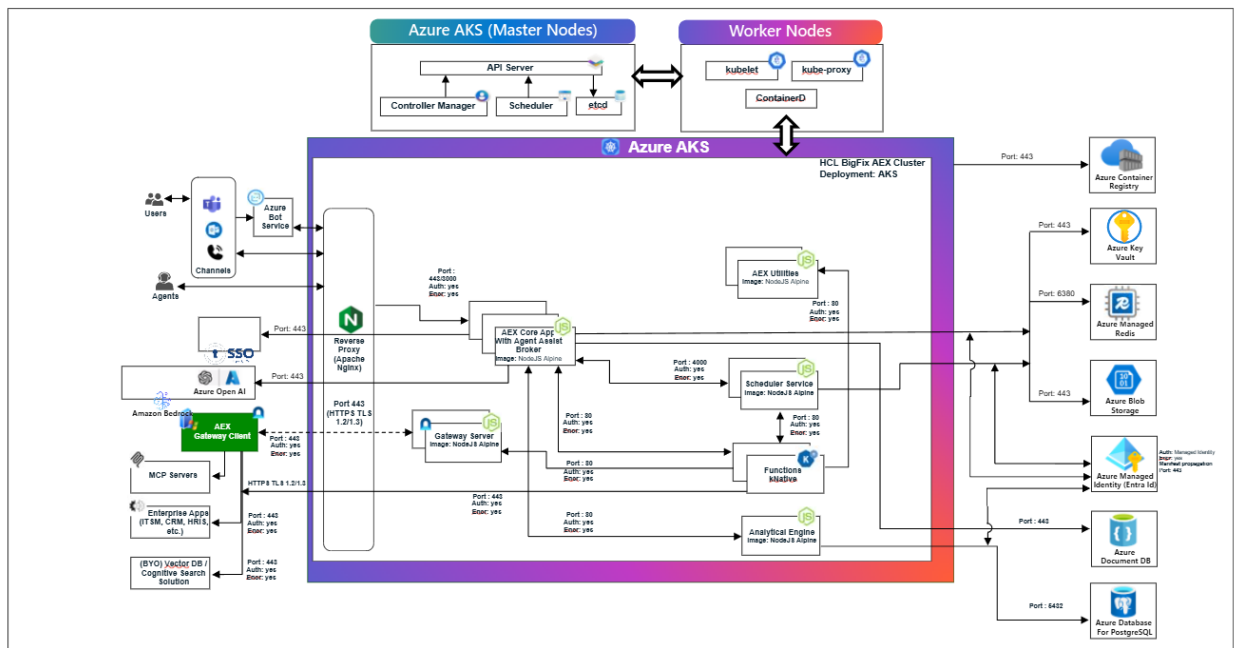
### 4.2 For On-Premise - (Customer managed Datacentre using Kubernetes on RHEL VMs)

## HCL BigFix AEX (On-premise) Deployment Architecture



### 4.3 On-Premise (Customer managed Azure Subscription using AKS)

#### HCL BigFix AEX (Azure) Deployment Architecture



## 5 Secure Release Checklist and Reports

### 5.1 Release Checklist (SaaS & On-premise)

| Release Checklist (SaaS & On-Premise)                                                                        | Criteria  | Status                              | Improvement / Comments                               |
|--------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------|------------------------------------------------------|
| Feature development for current release completed and verified                                               | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Quality objectives have been met for current release (including Functional / Load testing)                   | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Export Classification with Country specific import requirements completed                                    | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Certificate of Originality Approved                                                                          | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| OneTrust Product Privacy Assessment Approved                                                                 | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Threat Model and Secure Design Review                                                                        | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Security Testing - SAST                                                                                      | Pass/Fail | <input checked="" type="checkbox"/> | No Critical/High/Medium issues                       |
| Security Testing - DAST                                                                                      | Pass/Fail | <input checked="" type="checkbox"/> | No Critical/High/Medium issues                       |
| Security Testing - Pen Testing for OWASP Top 10 for Web and Gen AI                                           | Pass/Fail | <input checked="" type="checkbox"/> | No Critical/High/Medium issues                       |
| Open-Source Vulnerability scanning via Mend                                                                  | Pass/Fail | <input checked="" type="checkbox"/> | 3 Medium and 1 High Issue tracked under PSIRT Record |
| Security Hotspot, Code smell and Code quality analysis using SonarQube                                       | Pass/Fail | <input checked="" type="checkbox"/> | A rating for all parameters                          |
| Service Description document completed with HCLSW Legal                                                      | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| New Release Training delivered to PS and support team                                                        | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Pricing approvals and CRM part code creation completion                                                      | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Marketing activities completion (including GTM collaterals, Launch webinars, Sales enablement sessions etc). | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |
| Online Product documentation and lifecycle page update                                                       | Pass/Fail | <input checked="" type="checkbox"/> |                                                      |

| Legend |                                     |
|--------|-------------------------------------|
| Pass   | <input checked="" type="checkbox"/> |
| Fail   | <input checked="" type="checkbox"/> |

### 5.2 Packages included in HCL BigFix AEX (SaaS & On-Premise)

This section lists all top-level packages included in various components of HCL BigFix AEX along with their license type, version, and description.

| Component Name | Core Packages | Core Packages (On premise) |
|----------------|---------------|----------------------------|
| AEX            | 82            | 82                         |
| AEX Analytics  | 18            | 18                         |
| AEX Functions  | 23            | 23                         |
| Global Admin   | 34            | NA                         |
| Secure Gateway | 12            | 12                         |
| AEX Utilities  | 12            | 12                         |
| Scheduler      | 21            | 21                         |
| Total          | 202           | 168                        |

#### AEX

| Library Name                     | Version | Description                                                                            | License Type |
|----------------------------------|---------|----------------------------------------------------------------------------------------|--------------|
| @a2a-js/sdk                      | 0.3.13  | A2A JavaScript SDK / JavaScript library for Agent-to-Agent protocol-based applications | Apache 2.0   |
| @aws-sdk/client-ec2              | 3.1002  | AWS EC2 client for JavaScript                                                          | Apache 2.0   |
| @azure/arm-compute               | 22.4.0  | Azure Compute Management SDK                                                           | MIT          |
| @azure/cosmos                    | 4.5.1   | Azure Cosmos DB client library                                                         | MIT          |
| @azure/identity                  | 4.8.0   | Azure Identity authentication library                                                  | MIT          |
| @azure/keyvault-secrets          | 4.10.0  | Azure Key Vault Secrets client library                                                 | MIT          |
| @azure/storage-blob              | 12.28.0 | Azure Blob Storage client library                                                      | MIT          |
| @google-cloud/translate          | 9.1.0   | Google Cloud Translation API client                                                    | Apache 2.0   |
| @ibm-cloud/cloudant              | 0.12.0  | IBM Cloudant SDK                                                                       | Apache 2.0   |
| @ibm-functions/iam-token-manager | 1.0.3   | IAM token manager for IBM Cloud Functions                                              | Apache 2.0   |
| @node-saml/passport-saml         | 5.1.0   | SAML authentication strategy for Passport                                              | MIT          |
| @redis/entraid                   | 5.11.0  | Microsoft Entra ID authentication support for Redis                                    | MIT          |
| @socket.io/redis-adapter         | 8.2.1   | Redis adapter for scaling Socket.IO                                                    | MIT          |
| @zilliz/milvus2-sdk-node         | 2.5.11  | Milvus vector database client                                                          | Apache 2.0   |
| adaptive-expressions             | 4.22.1  | Adaptive expressions for Bot Framework                                                 | MIT          |
| adaptivecards                    | 2.9.0   | Adaptive Cards UI framework                                                            | MIT          |

|                          |          |                                            |              |
|--------------------------|----------|--------------------------------------------|--------------|
| adaptivecards-templating | 2.2.0    | Templating engine for Adaptive Cards       | MIT          |
| async                    | 3.2.6    | Asynchronous utility functions for Node.js | MIT          |
| aws-sdk                  | 2.1692.0 | AWS SDK for JavaScript                     | Apache 2.0   |
| axios                    | 1.15.0   | Promise-based HTTP client                  | MIT          |
| bcrypt                   | 5.1.1    | Password hashing library                   | MIT          |
| botbuilder               | 4.17.1   | Microsoft Bot Framework SDK                | MIT          |
| botframework-connector   | 4.23.1   | Bot Framework connector client             | MIT          |
| busboy                   | 1.6.0    | Streaming parser for HTML form data        | MIT          |
| compression              | 1.8.1    | Node.js compression middleware             | MIT          |
| connect-flash            | 0.1.1    | Flash message middleware for Express       | MIT          |
| connect-redis            | 7.1.1    | Redis session store for Express            | MIT          |
| cookie-parser            | 1.4.7    | Cookie parsing middleware                  | MIT          |
| deepmerge                | 3.3.0    | Object merge utility                       | MIT          |
| eld                      | 1.0.0    | Language detection utility                 | MIT          |
| email-signature-detector | 0.0.6    | Email signature detection utility          | MIT          |
| exceljs                  | 4.4.0    | Excel file generation and parsing library  | MIT          |
| express                  | 4.17.3   | Web application framework for Node.js      | MIT          |
| express-handlebars       | 6.0.7    | Handlebars view engine for Express         | BSD 3-Clause |
| express-session          | 1.18.2   | Session middleware for Express             | MIT          |
| extract-zip              | 2.0.1    | ZIP extraction utility                     | BSD 2-Clause |
| form-data                | 4.0.0    | Form data creation library                 | MIT          |
| generate-password        | 1.4.2    | Password generation utility                | MIT          |
| geoip-country            | 4.1.50   | GeoIP country lookup utility               | MIT          |
| googleapis               | 114.0.0  | Google APIs client library for Node.js     | Apache 2.0   |
| ibm-cloud-sdk-core       | 5.1.0    | Core SDK utilities for IBM Cloud services  | Apache 2.0   |
| ibm-cos-sdk              | 1.13.4   | IBM Cloud Object Storage SDK               | Apache 2.0   |
| ibm-watson               | 10.0.0   | IBM Watson services SDK                    | Apache 2.0   |
| ibmcloud-appid           | 7.0.0    | IBM Cloud App ID SDK                       | Apache 2.0   |
| joi                      | 17.11.1  | Object schema validation library           | BSD 3-Clause |

|                    |        |                                               |              |
|--------------------|--------|-----------------------------------------------|--------------|
| jose               | 5.10.0 | JSON Object Signing and Encryption library    | MIT          |
| jsonwebtoken       | 9.0.2  | JSON Web Token implementation                 | MIT          |
| lusca              | 1.6.1  | Security middleware for Express               | Apache 2.0   |
| mammoth            | 1.9.0  | DOCX to HTML/text conversion library          | BSD 2-Clause |
| markdown-it        | 12.3.2 | Markdown parser                               | MIT          |
| mime-types         | 2.1.35 | MIME type lookup utility                      | MIT          |
| minio              | 8.0.5  | MinIO object storage client                   | Apache 2.0   |
| mobile-detect      | 1.4.3  | Mobile device detection utility               | MIT          |
| module-alias       | 2.2.2  | Module path aliasing utility                  | MIT          |
| moment             | 2.30.1 | Date and time manipulation library            | MIT          |
| mongodb            | 6.21.0 | MongoDB driver for Node.js                    | Apache 2.0   |
| morgan             | 1.10.1 | HTTP request logger middleware                | MIT          |
| mssql              | 11.0.1 | Microsoft SQL Server client for Node.js       | MIT          |
| multer             | 2.1.1  | File upload middleware for Express            | MIT          |
| nocache            | 3.0.1  | Middleware to disable client-side caching     | MIT          |
| nodemailer         | 8.0.5  | Email sending library                         | MIT          |
| passport           | 0.6.0  | Authentication middleware for Node.js         | MIT          |
| password-validator | 4.1.1  | Password policy validation library            | MIT          |
| pdf-parse          | 1.1.1  | PDF text extraction utility                   | MIT          |
| pg                 | 8.14.1 | PostgreSQL client for Node.js                 | MIT          |
| pg-format          | 1.0.4  | PostgreSQL query formatting utility           | MIT          |
| polly-tts          | 1.0.4  | Text-to-speech utility using Amazon Polly     | MIT          |
| qrcode             | 1.5.0  | QR code generation library                    | MIT          |
| qs                 | 6.11.1 | Query string parsing and stringifying library | BSD 3-Clause |
| recursive-readdir  | 2.2.3  | Recursive directory reading utility           | MIT          |
| redis              | 4.7.1  | Redis client for Node.js                      | MIT          |
| slackify-html      | 1.0.1  | HTML to Slack-compatible markdown converter   | MIT          |

|                   |       |                                                     |            |
|-------------------|-------|-----------------------------------------------------|------------|
| slackify-markdown | 4.4.0 | Markdown to Slack-compatible format converter       | MIT        |
| socket.io         | 4.2.0 | Real-time bidirectional event communication library | MIT        |
| socket.io-client  | 4.2.0 | Socket.IO client library                            | MIT        |
| speakeasy         | 2.0.0 | Two-factor authentication token utility             | MIT        |
| striptags         | 3.2.0 | HTML tag stripping utility                          | MIT        |
| svg-captcha       | 1.4.0 | SVG CAPTCHA generation library                      | MIT        |
| tesseract.js      | 6.0.0 | OCR library for image text extraction               | Apache 2.0 |
| twilio            | 4.21  | Twilio API client library                           | MIT        |
| uuid              | 8.3.2 | UUID generation library                             | MIT        |
| web-push          | 3.6.7 | Web push notification library                       | MIT        |

#### AEX Analytics

| Library Name                 | Version | Description                                                 | License Type |
|------------------------------|---------|-------------------------------------------------------------|--------------|
| @azure/keyvault-secrets      | 4.10.0  | Azure Key Vault Secrets client library                      | MIT          |
| @azure/identity              | 4.8.0   | Azure Identity authentication library                       | MIT          |
| @azure/storage-blob          | 12.28.0 | Azure Blob Storage client library                           | MIT          |
| @ibm-cloud/cloudant          | 0.12.10 | IBM Cloudant SDK                                            | Apache 2.0   |
| @presidio-dev/hai-guardrails | 1.10.1  | HAI Guardrails package for AI safety and policy enforcement | Apache 2.0   |
| compression                  | 1.7.4   | Node.js compression middleware                              | MIT          |
| express                      | 4.18.2  | Web application framework for Node.js                       | MIT          |
| gibberish-detective          | 1.1.1   | Utility for detecting gibberish or low-quality text         | MIT          |
| ibm-cos-sdk                  | 1.13.0  | IBM Cloud Object Storage SDK                                | Apache 2.0   |
| ioredis                      | 5.3.0   | Redis client for Node.js                                    | MIT          |
| ioredis-cache                | 2.0.0   | Redis-based caching utility                                 | MIT          |
| minio                        | 8.0.6   | MinIO object storage client                                 | Apache 2.0   |
| mongoose                     | 8.19.2  | MongoDB object modeling library for Node.js                 | MIT          |
| node-cron                    | 3.0.2   | Cron-like task scheduler for Node.js                        | ISC          |
| pg                           | 8.8.0   | PostgreSQL client for Node.js                               | MIT          |
| rapidoc                      | 9.3.8   | API documentation rendering tool for OpenAPI specifications | MIT          |
| sequelize                    | 6.28.0  | Promise-based ORM for Node.js supporting SQL databases      | MIT          |
| swagger-jsdoc                | 6.2.8   | Generates Swagger/OpenAPI documentation from JSDoc comments | MIT          |

#### AEX Functions

| Library Name | Version | Description | License Type |
|--------------|---------|-------------|--------------|
|--------------|---------|-------------|--------------|

|                     |        |                                               |              |
|---------------------|--------|-----------------------------------------------|--------------|
| @ibm-cloud/cloudant | 0.12.0 | IBM Cloudant SDK                              | Apache 2.0   |
| adaptivecards       | 2.9.0  | Adaptive Cards UI framework                   | MIT          |
| axios               | 1.15.0 | Promise-based HTTP client                     | MIT          |
| docx                | 9.5.1  | DOCX document generation library              | MIT          |
| ejs                 | 3.1.10 | Embedded JavaScript templating engine         | Apache 2.0   |
| exceljs             | 4.4.0  | Excel file generation and parsing library     | MIT          |
| express             | 5.1.0  | Web application framework for Node.js         | MIT          |
| form-data           | 4.0.5  | Form data creation library                    | MIT          |
| ibm-cloud-sdk-core  | 5.1.0  | Core SDK utilities for IBM Cloud services     | Apache 2.0   |
| ibm-watson          | 10.0.0 | IBM Watson services SDK                       | Apache 2.0   |
| jsonwebtoken        | 9.0.3  | JSON Web Token implementation                 | MIT          |
| jszip               | 3.10.1 | ZIP file creation and reading library         | MIT          |
| mammoth             | 1.11.0 | DOCX to HTML/text conversion library          | BSD 2-Clause |
| markdown-it         | 12.3.2 | Markdown parser                               | MIT          |
| moment              | 2.29.4 | Date and time manipulation library            | MIT          |
| mongodb             | 5.6.0  | MongoDB driver for Node.js                    | Apache 2.0   |
| nodemailer          | 8.0.5  | Email sending library                         | MIT          |
| pdf-parse           | 1.1.0  | PDF text extraction utility                   | MIT          |
| pptxgenjs           | 4.0.1  | PowerPoint presentation generation library    | MIT          |
| qrcode              | 1.5.0  | QR code generation library                    | MIT          |
| qs                  | 6.11.1 | Query string parsing and stringifying library | BSD 3-Clause |
| utf8                | 3.0.0  | UTF-8 encoding and decoding utility           | MIT          |
| uuid                | 8.3.2  | UUID generation library                       | MIT          |

## Global Admin

| Library Name        | Version | Description                                            | License Type |
|---------------------|---------|--------------------------------------------------------|--------------|
| @fastify/cookie     | 11.0.2  | Cookie parsing and serialization plugin for Fastify    | MIT          |
| @fastify/formbody   | 8.0.2   | Form body parsing plugin for Fastify                   | MIT          |
| @fastify/http-proxy | 11.4.3  | HTTP proxy plugin for Fastify                          | MIT          |
| @fastify/multipart  | 9.4.0   | Multipart form-data and file upload plugin for Fastify | MIT          |
| @fastify/passport   | 3.0.2   | Passport authentication integration for Fastify        | MIT          |
| @fastify/session    | 11.1.1  | Session management plugin for Fastify                  | MIT          |
| @fastify/static     | 9.0.0   | Static file serving plugin for Fastify                 | MIT          |
| @fastify/url-data   | 6.0.3   | URL data parsing plugin for Fastify                    | MIT          |
| @fastify/view       | 11.1.1  | Template rendering plugin for Fastify                  | MIT          |
| @ibm-cloud/cloudant | 0.12.0  | IBM Cloudant SDK                                       | Apache 2.0   |
| async               | 3.2.4   | Asynchronous utility functions for Node.js             | MIT          |
| axios               | 1.15.0  | Promise-based HTTP client                              | MIT          |
| bee-queue           | 1.4     | Redis-backed job queue for Node.js                     | MIT          |
| busboy              | 1.6.0   | Streaming parser for HTML form data                    | MIT          |
| connect-redis       | 6.0.0   | Redis session store for Express-compatible sessions    | MIT          |
| csvtojson           | 2.0.10  | CSV to JSON conversion utility                         | MIT          |
| ejs                 | 3.1.10  | Embedded JavaScript templating engine                  | Apache 2.0   |
| fastify             | 5.7.2   | Fast and low-overhead web framework for Node.js        | MIT          |
| form-data           | 4.0.0   | Form data creation library                             | MIT          |
| ibm-cos-sdk         | 1.6.1   | IBM Cloud Object Storage SDK                           | Apache 2.0   |
| ibmcloud-appid      | 7.0.0   | IBM Cloud App ID SDK                                   | Apache 2.0   |

|              |        |                                               |              |
|--------------|--------|-----------------------------------------------|--------------|
| joi          | 17.8.3 | Object schema validation library              | BSD 3-Clause |
| json2csv     | 4.5.4  | JSON to CSV conversion utility                | MIT          |
| jsonwebtoken | 9.0.0  | JSON Web Token implementation                 | MIT          |
| jwk-to-pem   | 2.0.7  | Converts JSON Web Keys to PEM format          | Apache 2.0   |
| mime-types   | 2.1.24 | MIME type lookup utility                      | MIT          |
| module-alias | 2.2.2  | Module path aliasing utility                  | MIT          |
| mongoose     | 6.0.12 | MongoDB object modeling library for Node.js   | MIT          |
| nodemailer   | 8.0.5  | Email sending library                         | MIT          |
| qs           | 6.11.1 | Query string parsing and stringifying library | BSD 3-Clause |
| redis        | 3.1.2  | Redis client for Node.js                      | MIT          |
| sendmail     | 1.6.1  | Sendmail-compatible email sending library     | MIT          |
| svg-captcha  | 1.4.0  | SVG CAPTCHA generation library                | MIT          |
| uuidv4       | 6.1.0  | UUID v4 generation utility                    | MIT          |

### Secure Gateway

| Library Name             | Version | Description                                         | License Type |
|--------------------------|---------|-----------------------------------------------------|--------------|
| @azure/identity          | 4.0.0   | Azure Identity authentication library               | MIT          |
| @azure/keyvault-secrets  | 4.7.0   | Azure Key Vault Secrets client library              | MIT          |
| @redis/entraid           | 5.10.0  | Microsoft Entra ID authentication support for Redis | MIT          |
| @socket.io/redis-adapter | 8.2.1   | Redis adapter for scaling Socket.IO                 | MIT          |
| async                    | 3.2.0   | Asynchronous utility functions for Node.js          | MIT          |
| axios                    | 1.15.0  | Promise-based HTTP client                           | MIT          |
| ejs                      | 3.1.5   | Embedded JavaScript templating engine               | Apache 2.0   |
| express                  | 4.15.2  | Web application framework for Node.js               | MIT          |
| qs                       | 6.14.2  | Query string parsing and stringifying library       | BSD 3-Clause |
| redis                    | 4.7.0   | Redis client for Node.js                            | MIT          |
| socket.io                | 4.8.3   | Real-time bidirectional event communication library | MIT          |
| uuid                     | 8.3.2   | UUID generation library                             | MIT          |

### AEX Utilities

| Library Name      | Version | Description                                | License Type |
|-------------------|---------|--------------------------------------------|--------------|
| @asciidoctor/core | 3.0.0   | AsciiDoc processing library for JavaScript | MIT          |
| csv-parse         | 5.5.0   | CSV parsing library                        | MIT          |
| exceljs           | 4.4.0   | Excel file generation and parsing library  | MIT          |
| express           | 4.18.2  | Web application framework for Node.js      | MIT          |
| jsonwebtoken      | 9.0.3   | JSON Web Token implementation              | MIT          |
| mammoth           | 1.6.0   | DOCX to HTML/text conversion library       | BSD 2-Clause |
| multer            | 2.1.1   | File upload middleware for Express         | MIT          |
| officeparser      | 5.2.2   | Office document parsing utility            | MIT          |

|                     |       |                                              |     |
|---------------------|-------|----------------------------------------------|-----|
| pdf-parse           | 2.2.2 | PDF text extraction utility                  | MIT |
| sendmail            | 1.6.1 | Sendmail-compatible email sending library    | MIT |
| turndown            | 7.1.0 | HTML to Markdown converter                   | MIT |
| turndown-plugin-gfm | 1.0.2 | GitHub-flavored Markdown plugin for Turndown | MIT |

### Scheduler

| Library Name            | Version  | Description                                     | License Type |
|-------------------------|----------|-------------------------------------------------|--------------|
| @azure/identity         | 4.6.0    | Azure Identity authentication library           | MIT          |
| @azure/keyvault-secrets | 4.10.0   | Azure Key Vault Secrets client library          | MIT          |
| @azure/storage-blob     | 12.26.0  | Azure Blob Storage client library               | MIT          |
| @ibm-cloud/cloudant     | 0.12.3   | IBM Cloudant SDK                                | Apache 2.0   |
| async                   | 3.2.4    | Asynchronous utility functions for Node.js      | MIT          |
| axios                   | 1.15.0   | Promise-based HTTP client                       | MIT          |
| bull                    | 4.11.5   | Redis-backed queue library for Node.js          | MIT          |
| fastify                 | 5.7.4    | Fast and low-overhead web framework for Node.js | MIT          |
| ibm-cloud-sdk-core      | 5.3.2    | Core SDK utilities for IBM Cloud services       | Apache 2.0   |
| ibm-cos-sdk             | 1.14.1   | IBM Cloud Object Storage SDK                    | Apache 2.0   |
| aws-sdk                 | 2.1692.0 | AWS SDK for JavaScript                          | Apache 2.0   |
| jsonwebtoken            | 9.0.2    | JSON Web Token implementation                   | MIT          |
| minio                   | 8.0.5    | MinIO object storage client                     | Apache 2.0   |
| module-alias            | 2.2.2    | Module path aliasing utility                    | MIT          |
| mongoose                | 6.17.0   | MongoDB driver for Node.js                      | Apache 2.0   |
| nodemailer              | 8.0.5    | Email sending library                           | MIT          |
| openwhisk               | 3.21.4   | Apache OpenWhisk client library                 | Apache 2.0   |
| qs                      | 6.11.2   | Query string parsing and stringifying library   | BSD 3-Clause |
| socket.io-client        | 4.8.3    | Socket.IO client library                        | MIT          |
| twilio                  | 5.5.2    | Twilio API client library                       | MIT          |
| uuid                    | 11.1.0   | UUID generation library                         | MIT          |

## 5.3 HCL AppScan SAST Reports (SaaS & On-premise)

### 5.3.1 SAST Report - AEX

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

### 5.3.2 SAST Report – Global Admin

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

### 5.3.3 SAST Report – Secure Gateway

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

### 5.3.4 SAST Report –

Scheduler

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

### 5.3.5 SAST Report – AEX Analytics

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

### 5.3.6 SAST Report – AEX Functions

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

### 5.3.7 SAST Report – AEX Utilities

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

| HCL AppScan SAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

## 5.4 HCL AppScan DAST Reports

### 5.4.1 DAST Report – AEX Web (SaaS)

No security vulnerabilities were found in the DAST Report, as detailed in the table below.

| HCL AppScan DAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

#### 5.4.2 DAST Report – Global Admin (SaaS)

No security vulnerabilities were found in the DAST Report, as detailed in the table below.

| HCL AppScan DAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

#### 5.4.3 DAST Report – AEX (On-Premise)

No security vulnerabilities were found in the DAST Report, as detailed in the table below.

| HCL AppScan DAST Results |          |
|--------------------------|----------|
| ■ Critical               | 0        |
| ■ High                   | 0        |
| ■ Medium                 | 0        |
| ■ Low                    | 0        |
| ■ Informational          | 0        |
| <b>Total</b>             | <b>0</b> |

#### 5.5 Mend Security Reports (SaaS & On-premise)

The Mend Scan identified two medium severity security issues (**PSIRT- PRB0170901** and **PSIRT ID: PRB0169924**). PSIRT records are now established for both.

| Mend Security Results |   |
|-----------------------|---|
| ■ Critical            | 0 |
| ■ High                | 0 |
| ■ Medium              | 2 |
| ■ Low                 | 0 |
| ■ Informational       | 0 |

|              |          |
|--------------|----------|
| <b>Total</b> | <b>0</b> |
|--------------|----------|

## 5.6 Security Penetration Testing Report

For Current release HCLSW Security Team conducted Penetration Testing for all the components of HCL BigFix AEX (SaaS & On-Premise) based on OWASP Top 10 guideline for Web and Gen AI.

All security vulnerabilities were remediated and validated before the release by the HCLSW Security team with no vulnerabilities remaining for both SaaS and On-Premise, as detailed in the table below.

| Security Penetration Testing Results |          |
|--------------------------------------|----------|
| ■ Critical                           | 0        |
| ■ High                               | 0        |
| ■ Medium                             | 0        |
| ■ Low                                | 0        |
| ■ Informational                      | 0        |
| <b>Total</b>                         | <b>0</b> |

## 5.7 PSIRT Details

As part of HCL Software Product Security Incident Response (PSIRT) process, for current release 2 PSIRT records were created for security issue. Following is the description of PSIRT ID.

| Issue id                        | Source    | Issue Description                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PRB0163714<br>(High Severity)   | Mend Scan | <p>Glob package Vulnerability detected in the HCL BigFix AEX (CVE-2025-64756)</p> <p><b>This vulnerability stands closed now</b></p> <p>As part of the Container Image Scanning process, a vulnerability involving the glob package was detected within the HCL BigFix AEX Product. A security flaw in the glob command-line interface due to inadequate input validation has been discovered.</p> |
| PRB0170901<br>(Medium Severity) | Mend Scan | <p>Elliptic package Vulnerability detected in the HCL BigFix AEX (CVE-2025-14505)</p> <p>This is a transitive dependency of jwk-to-pem. We are already using the latest version of jwk-to-pem (2.0.7)</p>                                                                                                                                                                                          |
| PRB0169924<br>(Medium Severity) | Mend Scan | <p>file-type package Vulnerability detected in the HCL BigFix AEX (CVE-2026-31808)</p> <p>AEX does not utilize the vulnerable components of these packages, either directly or indirectly. These are trivial dependencies and do not impact our security posture.</p>                                                                                                                              |

|                                 |                         |                                                                                                                                                                                                                                                                |
|---------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PRB0169926<br>(High Severity)   | Prisma<br>(Cortex) Scan | Swiper package Vulnerability detected in the HCL BigFix AEX<br>(CVE-2026-27212)<br><br>AEX does not utilize the vulnerable components of these packages, either directly or indirectly. These are trivial dependencies and do not impact our security posture. |
| PRB0170900<br>(Medium Severity) | Prisma<br>(Cortex) Scan | WS package Vulnerability detected in the HCL BigFix AEX<br>(CVE-2021-32640)<br><br>This is a transitive dependency of @zilliz/milvus2-sdk-node. We are already using the latest version of @zilliz/milvus2-sdk-node (2.6.13).                                  |

## 5.8 Load Testing Reports

### 5.8.1 For SaaS -

As part of the current release load testing was performed using HCL OneTest tool and HCL Playwright K6 tool. Following table provides the details around same:

| Module Name                                                           | Maximum User Count<br>Against Which Test Case<br>Passed | Results                                                                 |
|-----------------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------|
| Login – LUMS Authentication                                           | 1000 users                                              | Average response time for all pages: 1.542s (200 users/ second ramp up) |
| Login – LUMS Authentication                                           | 1000 users                                              | Average response time for all pages: 40 sec (5 users/ second ramp up)   |
| Ticket creation using ServiceNow Tool                                 | 1000 users                                              | Average response time for all pages: 44 sec (200 users/ second ramp up) |
| Ticket creation using ServiceNow Tool                                 | 1000 users                                              | Average response time for all pages: 1.8 min (5 users/ second ramp up)  |
| AEX – Agent Assist Flow-<br>Adding 50 user requests in<br>Agent Queue | 50 users                                                | Average response time for all pages: 62 sec (5 users/ second ramp up)   |

|                                               |            |                                                                            |
|-----------------------------------------------|------------|----------------------------------------------------------------------------|
| Agent Assist Flow User and Agent Interaction  | 50 users   | Average response time for all pages: 1.24 min (5 users/ second ramp up)    |
| Knowledge Search – Using Multiple Collections | 1000 users | Average response time for all pages: 27.77 sec (200 users/ second ramp up) |
| Knowledge Search – Using Multiple Collections | 1000 users | Average response time for all pages: 2.83 min (5 users/ second ramp up)    |

### 5.8.2 For On-Premise –

As part of the current release load testing was performed using HCL Playwright K6 tool and following table provides the details around same:

| Module Name                                                    | Maximum User Count Against Which Test Case Passed | Results                                                                  |
|----------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------|
| Login – LUMS Authentication                                    | 1000 users                                        | Average response time for all pages: 31 sec (5 users/ second ramp up)    |
| Ticket creation using ServiceNow Tool                          | 1000 users                                        | Average response time for all pages: 1.18 min (5 users/ second ramp up)  |
| AEX – Agent Assist Flow-Adding 50 user requests in Agent Queue | 50 users                                          | Average response time for all pages: 48 sec (5 users/ second ramp up)    |
| Agent Assist Flow User and Agent Interaction                   | 50 users                                          | Average response time for all pages: 50.26 sec (5 users/ second ramp up) |
| Knowledge Search – Using Multiple Collections                  | 1000 users                                        | Average response time for all pages: 2.83 min (5 users/ second ramp up)  |

### 5.8.3 For AKS Environment –

| Module Name | Maximum User Count Against Which Test Case Passed | Results |
|-------------|---------------------------------------------------|---------|
|-------------|---------------------------------------------------|---------|

|                                                                |           |                                                                          |
|----------------------------------------------------------------|-----------|--------------------------------------------------------------------------|
| Login – LUMS Authentication                                    | 500 users | Average response time for all pages: 38.96 sec (5 users/ second ramp up) |
| Ticket creation using ServiceNow Tool                          | 200 users | Average response time for all pages: 1.76 min (5 users/ second ramp up)  |
| AEX – Agent Assist Flow-Adding 50 user requests in Agent Queue | 50 users  | Average response time for all pages: 60 sec (5 users/ second ramp up)    |
| Agent Assist Flow User and Agent Interaction                   | 50 users  | Average response time for all pages: 1.25 min (5 users/ second ramp up)  |
| Knowledge Search – Using Multiple Collections                  | 200 users | Average response time for all pages: 2.88 min (5 users/ second ramp up)  |

## 6 SaaS Security Controls

| Control                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data at rest and in transit encryption for Cloud Services | All IBM Cloud services including but not limited to Cloudant Database, Object Storage (used for hosting base platform) as well as other public cloud vendors like Azure/AWS (for Gen AI Service) are deployed with Encryption at rest enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Data protection                                           | <p>As part of HCL BigFix AEX platform daily backups are taken and with a retention period after which the data will be scraped or purged securely. The default retention period involves archival after 1 year or a period in compliance with customer security policy.</p> <p>Post 1 year, the data will be archived for 3 months, which can be restored in case requested by customers. The data retention period can be customized as per the customer's requirement.</p> <p>Application logs are retained for up to 30 days, and access logs are retained for up to 1 year. Additional backup and restore capacity and services are available upon request and for an additional charge.</p> |
| DDoS and WAF protection                                   | HCL BigFix AEX platform leverages Cloudflare for DDoS protection. It also includes a robust Web Application Firewall (WAF) that helps detect and block malicious traffic, such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 threats, before they reach the application                                                                                                                                                                                                                                                                                                                                                                                                   |
| 24*7 Security Monitoring                                  | HCL BigFix AEX platform leverages HCL managed Devo SIEM Solution for 24*7 security monitoring.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Compliance Attestation                                    | <p>The HCL BigFix AEX platform has the following compliance certification/attestation available for SaaS:</p> <ul style="list-style-type: none"><li>• ISO 27001</li><li>• ISO 27034</li><li>• SOC 2 Type II</li><li>• SOC 3</li><li>• CERT - IN</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## 7 Application Security Controls (SaaS & On-Premise)

| Control                                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data at rest and in transit encryption                                                               | <p>SaaS -</p> <ul style="list-style-type: none"> <li>• Data in Transit: All communication between users, services, and external systems is encrypted using HTTPS TLS 1.2/1.3.</li> <li>• Data at Rest: All data stored within the platform, including logs, configurations, and user-related data, is encrypted at rest using AES-256 encryption standards, as supported by the underlying cloud providers. Encryption keys are managed securely, leveraging the cloud provider's Key Management Services (KMS).</li> <li>• On-Prem-</li> <li>• Data in Transit: All communication between users, services, and external systems is encrypted using HTTPS TLS 1.2/1.3.</li> <li>• Data at Rest: Encrypts all stored data using OS- or storage-layer mechanisms (MongoDB, PostgreSQL and NFS). For secret encryption OpenBao Vault is used which leverages AES-256 encryption for data at rest</li> <li>• Azure -</li> <li>• Data in Transit: All communication between users, services, and external systems is encrypted using HTTPS TLS 1.2/1.3.</li> <li>• Data at Rest: AES-256 encryption standards</li> </ul> |
| Authentication & Authorization                                                                       | <ul style="list-style-type: none"> <li>• Single Sign-On (SSO): User authentication is managed via SSO, integrating with Customer provided enterprise Identity Providers (e.g., ADFS, Azure AD, Okta, PingFederate) over SAML 2.0.</li> <li>• Role-Based Access Control (RBAC): A fine-grained RBAC model is enforced to ensure users and services have access only to the resources necessary for their roles.</li> <li>• API Security: All API endpoints require authentication, either through API keys (e.g., Azure OpenAI) or OAuth 2.0 (e.g., IBM Watson).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Content Filtering & Prompt Validation<br>(using Azure, AWS and GCP native content filtering service) | <ul style="list-style-type: none"> <li>• Real-Time Content Filtering: Built-in content moderation checks for toxic, harmful, or restricted content using classifiers and guardrails before generating output.</li> <li>• Prompt Injection Protection: Input sanitization and pattern recognition techniques are used to detect and neutralize prompt injection attempts.</li> <li>• Output Filtering: Sensitive terms, data leakage, or prohibited topics are blocked before reaching the user.</li> <li>• Runtime Safeguards: Input and output safeguards help enforce scope, confidentiality, and safe response behaviour during agent execution.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Testing                            | <ul style="list-style-type: none"> <li>Follows a comprehensive security testing framework covering threat modelling, SAST, DAST, Mend, Sonar, and Prisma.</li> <li>Includes penetration testing by HCLSW Security team aligned with OWASP Top 10 for Web and GenAI risks.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Secure Gateway                              | <ul style="list-style-type: none"> <li>Integrates seamlessly within the customer's on-premise environment.</li> <li>Routes all communication through a secure, encrypted tunnel.</li> <li>Uses end-to-end encryption to protect internal and external interactions from interception.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Responsible AI - Risk & Incident Management | <ul style="list-style-type: none"> <li>Conducts an AI Risk Assessment for every major release.</li> <li>Maintains structured processes for identifying, reporting, and resolving AI-related security incidents.</li> <li>Kill Switch &amp; Controlled Operations supports rapid disablement of misbehaving agents through kill switch / agent state controls to reduce operational risk.</li> </ul>                                                                                                                                                                                                                                                                                                                      |
| Responsible AI - Human Oversight            | <ul style="list-style-type: none"> <li>Incorporates human-in-the-loop workflows for sensitive or high-impact agent actions.</li> <li>Provides safeguards to maintain operational safety during agent execution.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Responsible AI - PII Protection             | <ul style="list-style-type: none"> <li>Follows a "purposeful, limited, and minimized" approach for handling PII.</li> <li>Uses regex-based sanitization to redact sensitive data and prevent exposure.</li> <li>Processes only the minimal data required for operational needs.</li> <li>Allows display of a customizable banner to notify users not to provide or prompt any sensitive/PII data when interacting with AI agents.</li> </ul>                                                                                                                                                                                                                                                                             |
| Responsible AI - Accuracy & Transparency    | <ul style="list-style-type: none"> <li>Supports tuning of AI hyperparameters to improve accuracy and groundedness.</li> <li>Promotes transparency and clarity in AI-driven workflows.</li> <li>Provides visibility into agent execution flow, including conversation steps, tool calls, and outcomes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                         |
| Traceability, Auditability & Observability  | <ul style="list-style-type: none"> <li>Provides execution transparency across conversation turns, tool calls, outcomes, and timelines.</li> <li>Supports step-level payload inspection and auditability for governance, troubleshooting, and investigations.</li> <li>Enables operational monitoring of agent behaviour and execution flow.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                   |
| Guardrails                                  | <ul style="list-style-type: none"> <li>Multi-Layer Guardrails architecture is applied across knowledge ingestion, runtime input/output handling, and agent execution to help enforce safe, scoped, and policy-aligned behaviour</li> <li>Guardrails help restrict agents to their intended domain, reduce unsafe or unauthorized actions, and support grounded responses.</li> <li>Runtime Protection via Input and output safeguards help detect unsafe prompts, protect confidential information, and prevent restricted or non-compliant responses from reaching users.</li> <li>Guardrails work together with tool authorization, traceability, and approval controls to support operational governance .</li> </ul> |

## 8 Known Issues

The v13 release of HCL BigFix AEX has the following issues categorized by severity:

- Critical Severity: 0 Issues
- High Severity: 0 Issues
- Medium Severity: 5 Issues
- Low Severity: 1 Issues

| Issue ID | Severity | Issue Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SAAS/On-Premise Issue |
|----------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 16426    | Medium   | <p><b>Workflows → Schema</b>→ Min Value and Max Value fields are accepting invalid inputs. The system allows negative numbers and other non-numeric values without triggering any validation errors. This issue occurs for both Number and String field types.</p> <p><b>RCA</b> - While creating field in schema for workflow, minimum value input field is taking higher number as an input than maximum input field. this validation check has been applied and code is merged.</p>                                                                                 | Both                  |
| 16532    | Medium   | <p><b>Knowledge Spaces</b>→ After creating a new collection in knowledge spaces, if user uploads txt, pdf, ppt or doc file and next user tries to search this file under collection or search using file content, the system returns "No result found".</p> <p><b>RCA</b>- The OutOfDiskSpace error occurred exclusively in our staging environment due to its limited resource configuration being shared across multiple teams. With many people testing simultaneously, the volume of data grew rapidly and exceeded the capacity of the smaller staging setup.</p> | Both                  |
| 16411    | Medium   | <p><b>User Management</b>→ <b>Routes</b> →User is able to create a route access entry even when the route description field is left empty.</p> <p><b>RCA</b> - Whitespaces validation was missing in input fields</p>                                                                                                                                                                                                                                                                                                                                                  | Both                  |
| 16538    | Medium   | <p><b>Agent GUI Builder</b>→ <b>Knowledge Configuration</b>→If user deselect the collection under knowledge configuration list, then entire list items and other screen options get disappears and blank panel appears.</p>                                                                                                                                                                                                                                                                                                                                            | Both                  |

|       |        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |      |
|-------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|       |        | <b>RCA</b> - In agent builder if user tries to update/select the collection after scrolling down content gets scrolled up. CSS fix has been applied to it.                                                                                                                                                                                                                                                                                                                                                                |      |
| 16601 | Medium | <p><b>Tools→Agent Assist Tool→</b> When user deploy agent assist tool with different names and add use this tool to an agentic flow-then agent assist functionality is not working, user is not able to connect to the human agent.</p> <p><b>RCA</b> - Following an infrastructure upgrade to support multi-instance tool deployment, the internal "Agent Assist" tool failed to execute. The issue was traced to legacy hardcoded checks that failed to recognize the tool under the new dynamic naming convention.</p> | SAAS |
| 16443 | Low    | <p><b>Agent Performance Dashboard→Quality metrics</b><br/>→Security Overview graph and Quality Metrics Trends graph are not as per the window size.</p> <p><b>RCA</b> - Browser zoom triggers window resizes events but zoom changes the CSS pixel ratio and viewport scaling in a way that does not proportionally resize the chart container. Echarts' resize relies on container dimensions, which may not correctly reflect the visual scale after zoom.</p>                                                          | Both |
| 19903 | Medium | <p><b>Agent Studio→ Agents→</b> After creating an agent, when user adds any prompt in model with minimum 2 characters and tries to update the agent, user is getting an error pop up saying 'Failed to update agent. Please try again'</p> <p><b>RCA:</b> The prompt length check is missing in UI, so that's stopping agent to get updated.</p>                                                                                                                                                                          | Both |

## 9 Looking Forward

Looking ahead, AEX v14 is expected to further strengthen the platform's governance, control, interoperability, and user experience across key enterprise scenarios. The next release is focused on making AEX easier to manage at scale while improving collaboration between agents, administrators, and support teams.

Key areas of focus include:

- **VM-Based AEX Deployment Architecture** – AEX is planned to support a new VM-based architecture without any dependency on Kubernetes with executable installers, enabling deployment and scaling in virtual machine environments without dependency on self-managed or cloud-managed Kubernetes.
- **Workflow Versioning & Governance** – Enhanced controls for managing workflow versions, publishing updates with greater confidence, and maintaining better governance across workflow lifecycles.
- **Enhanced RBAC** – More granular and scalable role-based access controls to support clearer separation of duties and stronger enterprise administration.
- **A2A AEX Server** – Expanded agent-to-agent interoperability, enabling AEX to participate more effectively in broader multi-agent ecosystems.
- **Enhanced Agent Assist** – Improved support for service desk and operator-facing scenarios, with richer assistance capabilities and stronger contextual guidance for human agents.
- **Agent Governance Dashboard** – It will provide governance-focused insights such as policy and guardrail status. This will help administrators and governance teams monitor agents with greater control, consistency, and enterprise accountability.
- **Agent Identity Management** – AEX agent will have its own enterprise-manageable identity, aligned to organizational identity and access systems. It will improve traceability by making agent-level activity easier to track, audit, and govern across deployments.
- **Enhanced Voice Support on AEX** – Continued evolution of voice capabilities to support more natural and enterprise-ready voice interactions across business use cases.
- These upcoming capabilities are designed to strengthen AEX as a foundation for secure and scalable autonomous operations in enterprise environments.

**Disclaimer:** This roadmap is intended to outline general product direction. This roadmap is intended for information purposes only and may not be incorporated into any contract. These documents are not a commitment to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for HCL BigFix AEX product remains at the sole discretion of HCLSoftware.

# **HCLSoftware**

[hcl-software.com](https://hcl-software.com)

---