

HCLSoftware

HCL BigFix AEX

Release Notes

Version 12.1

18th December 2025



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.hcltechsw.com.

Copyright © 2025 HCL Technologies Limited.

Table of Contents

1	Executive Summary.....	5
2	Key Features	6
2.1	Flexible Deployment Choice -SaaS and On-Premise Version	6
2.2	Bring Your Own Vector DB and PG Vector Support	6
2.3	Agent Studio & Agentic UI – Next-Generation No-Code / Low-Code Agent Creation	6
2.4	Integrated Tools & MCP Catalog.....	6
2.5	Workflow Builder & Enterprise Workflow Engine	7
2.6	Dashboards & Operations Insights.....	7
2.7	List of Supported OTB Tools.....	7
3	HCL BigFix AEX Reference Architecture	9
4	HCL BigFix AEX Deployment Architecture.....	10
4.1	For SaaS -.....	10
4.2	For On-Premise -	10
5	Secure Release Checklist and Reports	11
5.1	Release Checklist (SaaS & On-premise)	11
5.2	Packages included in HCL BigFix AEX (SaaS & On - Premise).....	11
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 – Self Heal Client.....	23
5.3.6	SAST Report – Self Heal Microservice	24
5.3.7	SAST Report – AEX Analytics	24
5.3.8	SAST Report – AEX Functions	24
5.4	HCL AppScan DAST Reports	24
5.4.1	DAST Report – AEX Web (SaaS).....	24
5.4.2	DAST Report – Global Admin (SaaS).....	25

5.4.3	DAST Report – AEX (On-Premise).....	25
5.5	Mend Security Reports (SaaS & On-premise)	25
5.6	Security Penetration Testing Report	26
5.7	PSIRT Details.....	26
5.8	Load Testing Reports.....	26
5.8.1	For SaaS -.....	26
5.8.2	For On-Premise -	27
6	SaaS Security Controls.....	28
7	Application Security Controls (SaaS & On-premise).....	29
8	Known Issues	31
9	Looking Forward	32

1 Executive Summary

AEX v12.1 marks a step forward in platform maturity, enterprise control, and extensibility. This release unlocks **On-Premise Deployment** choice, giving customers complete control over data residency, security, and infrastructure. Support for customer-managed vector databases like **PGVector** expands flexibility in retrieval architecture and model hosting. At the heart of v12.1 is a revamped Agentic AI Studio with a modern UI and deeper integration with MCP, making it easier to embed and configure tools from **external MCP servers** directly into agents.

Enterprise orchestration takes a leap forward with a new **Workflow Engine and Kafka-based event automation**, enabling robust, cross-domain autonomous execution. Operational visibility gets boost with the Agent Performance Dashboard, live alerts, last-seen data, time zone filtering, and improved RTO diagnostics.

This release also introduces a **secure runtime sandbox** for isolated and safe agent execution. **Enhanced Self-Heal and Agent Assist capabilities** bring greater resilience and responsiveness across use cases. Additionally, our out-of-the-box tool creation features streamline the development process, allowing teams to accelerate the delivery of custom agents. Together, these updates position AEX as the most scalable, governable, and extensible platform for deploying autonomous agents across IT, HR, Cloud, and business operations.

2 Key Features

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

2.1 Flexible Deployment Choice -SaaS and On-Premise Version

AEX v12.1 expands deployment flexibility by adding an on-premise version in addition to the existing SaaS offering. Organizations can now choose the deployment model that best aligns with their security, regulatory, and infrastructure needs.

Key Enhancements:

- Newly introduced on-prem deployment for secure or regulated environments with continued availability of the existing SaaS offering.
- Support for on-prem vector databases and locally hosted LLMs

Business Impact:

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

2.2 Bring Your Own Vector DB and PG Vector Support

This release expands flexibility in enterprise RAG and data architecture by supporting Bring Your Own Vector DB and customer-controlled embedding stores.

Key Enhancements:

- Support for PG Vector and customer-managed vector databases
- Greater control over embeddings, data residency, and retrieval strategies

Business Impact:

Provides enterprises with complete ownership of vector storage, alignment with governance and compliance mandates, and the ability to optimize cost and performance based on their internal AI and data strategy.

2.3 Agent Studio & Agentic UI – Next-Generation No-Code / Low-Code Agent Creation

AEX v12.1 delivers an enhanced, intuitive Agent Studio that enables business users, developers, and IT teams to design and orchestrate intelligent multi-agent systems without writing code.

Key Enhancements

- Drag-and-drop canvas for rapid agent creation
- Integrated MCP tool browsing and assignment
- Unified tools catalog with internal & external API connectors
- Streamlined agent configuration and orchestration workflows

2.4 Integrated Tools & MCP Catalog

AEX strengthens its extensibility with a unified tool framework and deeper MCP integration.

Key Enhancements:

- Automatic creation of MCP tools through Gateway endpoints
- Tool discovery, version updates, and deletion synchronization

- Richer metadata and configuration options directly inside Agent Studio

Business Impact:

Simplifies integration management, accelerates customization, and broadens cross-system automation coverage.

2.5 Workflow Builder & Enterprise Workflow Engine

The workflow engine has been significantly strengthened to support cross-system, event-driven orchestration at enterprise scale.

Key Enhancements:

- Visual workflow builder for designing multi-step automations
- Kafka-based event publishing and consumption
- Advanced governance: schema validation, resume-on-error, retry-on-error
- Conditional polling for external system dependencies

2.6 Dashboards & Operations Insights

AEX v12.1 enhances visibility and control through intelligent dashboards that provide actionable insights into system health and agent performance.

Key Enhancements:

- Agent Performance Dashboard with CSAT, latency, token usage, and tool success metrics.
- Cognitive dashboards with timezone filters, notifications, and live activity views.
- Deeper RTO tracking for ITSM operations

Business Impact:

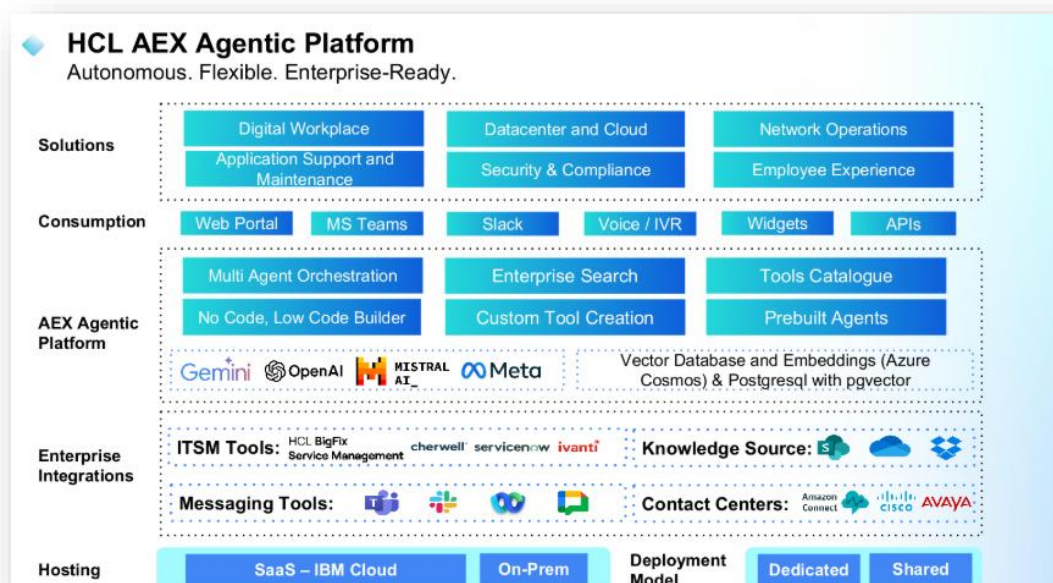
Empowers teams to optimize AI performance, measure ROI, and maintain operational excellence

2.7 List of Supported OTB Tools

Tool	Description
Cloudant Tool (IBM Cloudant)	Connects AEX agents to IBM Cloudant as a JSON document store for operational, configuration, and conversation data.
Confluence Tool	Integrates AEX agents with Atlassian Confluence to read and write knowledge content.
GitHub Tool	Connects AEX to GitHub / GitHub Enterprise for repository, issue and PR operations.
Gmail Tool	Provides integration with Gmail so agents can drive email-based workflows.
Jira Tool	Integrates AEX with Atlassian Jira for issue lifecycle management.
LinkedIn Tool	Controlled integration with LinkedIn for authenticated users, focused on recruiting, sales and branding assistants.
Salesforce Tool	Generic CRUD connector to Salesforce, allowing AEX agents to interact with standard and custom CRM objects.
Remedy Tool (BMC Remedy)	Integrates AEX with BMC Remedy ITSM for organizations using Remedy as their primary ticketing platform.

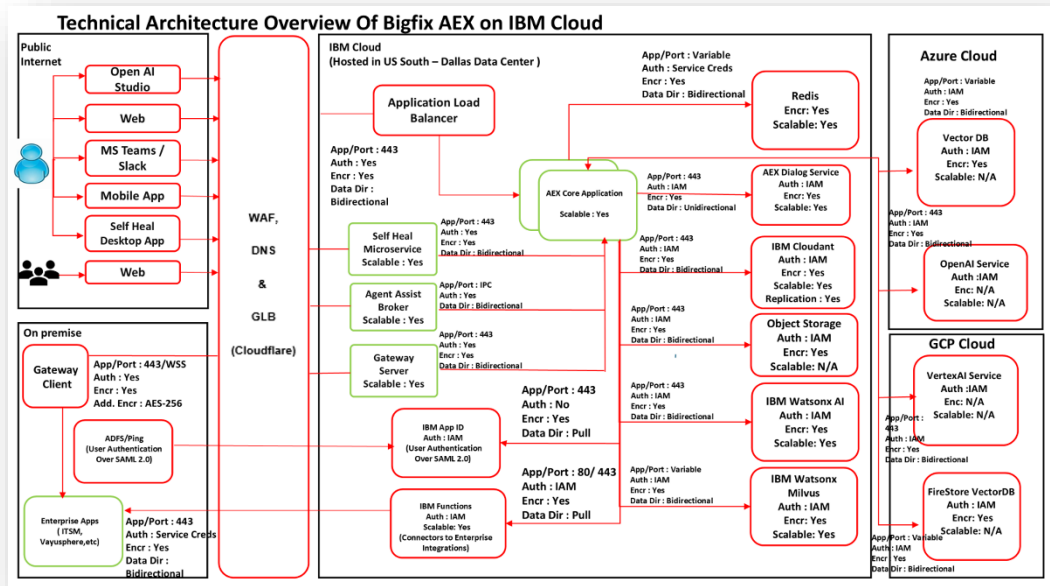
SharePoint Tool	Connects AEX to SharePoint Online for list and document operations within Microsoft 365.
Slack Tool	Integrates AEX with Slack for ChatOps, notifications, and collaboration.
HCL BigFix SM (SX) Tool (SX ITSM)	Provides integration with SX ITSM systems, enabling AEX agents to work with SX incidents.
Systrack Tool (Lakeside Systrack)	Integrates AEX with Lakeside Systrack for rich endpoint telemetry and diagnostics, powering Digital Employee Experience (DEX) scenarios.
Workday Tool	Integrates AEX with Workday for HR and employee lifecycle data.
Ansible Tool	Allows AEX agents to execute Ansible playbooks for configuration management and remediation.
Azure VM Tool	Integrates AEX with Azure Virtual Machines to manage VM lifecycle operations.
HCL BigFix Tool (HCL BigFix)	Integrates AEX with HCL BigFix for endpoint management, patch compliance, and action status tracking.

3 HCL BigFix AEX Reference Architecture

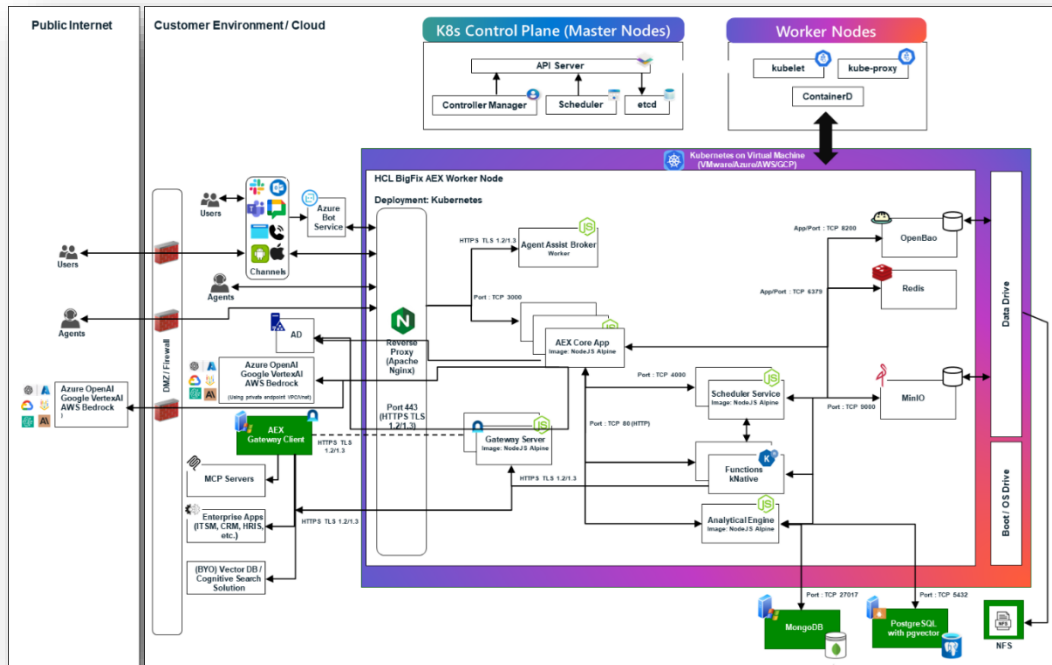


4 HCL BigFix AEX Deployment Architecture

4.1 For SaaS -



4.2 For On-Premise -



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	✓	
Quality objectives have been met for current release (including Functional / Load testing)	Pass/Fail	✓	97% closure rate for defects
Export Classification with Country specific import requirements completed	Pass/Fail	✓	
Certificate of Originality Approved	Pass/Fail	✓	
OneTrust Product Privacy Assessment Approved	Pass/Fail	✓	
Threat Model and Secure Design Review	Pass/Fail	✓	
Security Testing - SAST	Pass/Fail	✓	No Critical/High/Medium issues
Security Testing - DAST	Pass/Fail	✓	No Critical/High/Medium issues
Security Testing – Pen Testing for OWASP Top 10 for Web and Gen AI	Pass/Fail	✓	No Critical/High/Medium issues
Open-Source Vulnerability scanning via Mend	Pass/Fail	✓	1 Medium and 1 High Issue tracked under PSIRT Record
Security Hotspot, Code smell and Code quality analysis using SonarQube	Pass/Fail	✓	A rating for all parameters
Service Description document completed with HCLSW Legal	Pass/Fail	✓	
New Release Training delivered to PS and support team	Pass/Fail	✓	
Pricing approvals and CRM part code creation completion	Pass/Fail	✓	
Marketing activities completion (including GTM collaterals, Launch webinars, Sales enablement sessions etc).	Pass/Fail	✓	
Online Product documentation and lifecycle page update	Pass/Fail	✓	

Legend	
Pass	✓
Fail	✗

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 (SaaS)	Core Packages (On premise)
AEX	81	81
AEX Analytics	16	16
AEX Functions	23	23
Global Admin	33	NA

Secure Gateway	12	12
Scheduler	17	17
Self-Heal Client (Agent)	21	NA
Self-Heal Client (Admin Services)	23	NA
Self-Heal Microservice	21	NA
Total	247	149

AEX

Library Name	Version	Description	License Type
@aws-sdk/client-ec2	3.772.0	AWS EC2 client for JavaScript	Apache 2.0
@azure/arm-compute	22.4.0	Azure Compute Management SDK	MIT
@azure/identity	4.8.0	Azure Identity authentication 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 for Passport	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	Template engine for Adaptive Cards	MIT
async	3.2.6	Async utilities for Node.js	MIT
aws-sdk	2.1692.0	AWS SDK for JavaScript	Apache 2.0
axios	1.7.8	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 services	MIT
busboy	1.6.0	Multipart form parser	MIT
compression	1.8.1	Compression middleware for Node.js	MIT

connect-flash	0.1.1	Flash message middleware	MIT
connect-redis	6.0.0	Redis session store	MIT
cookie-parser	1.4.7	Cookie parsing middleware	MIT
deepmerge	3.3.0	Deep merge utility	MIT
eld	1.0.0		
email-signature-detector	0.0.6	Detect email signatures	MIT
exceljs	4.4.0	Excel file creation & parsing	MIT
expect-ct	0.1.1	Expect-CT header middleware	MIT
express	4.17.3	Web framework	MIT
express-handlebars	6.0.7	Handlebars templating for Express	MIT
express-session	1.18.2	Session middleware	MIT
extract-zip	2.0.1	Unzip utility	BSD-2
form-data	4.0.0	Form-data encoder	MIT
generate-password	1.4.2	Password generator	MIT
geoip-country	4.1.50	GeoIP lookup	LGPL
googleapis	114.0.0	Google API client library	Apache 2.0
ibm-cloud-sdk-core	5.1.0	IBM Cloud SDK core utilities	Apache 2.0
ibm-cos-sdk	1.13.4	IBM Cloud Object Storage SDK	Apache 2.0
ibm-watson	10.0.0	IBM Watson API client	Apache 2.0
ibmcloud-appid	7.0.0	IBM AppID authentication SDK	Apache 2.0
joi	17.11.1	Object schema validation	BSD-3
json2csv	4.5.1	Convert JSON to CSV	MIT
jsontoxml	1.0.1	JSON → XML converter	MIT
jsonwebtoken	9.0.2	JWT implementation	MIT
lusca	1.6.1	Web security middleware	MIT
mammoth	1.9.0	DOCX to HTML/Markdown converter	BSD-2
markdown-it	12.3.2	Markdown parser	MIT

mime-types	2.1.35	MIME utilities	MIT
minio	8.0.5	MinIO S3-compatible SDK	Apache 2.0
mobile-detect	1.4.3	Mobile device detection	MIT
module-alias	2.2.2	Alias module paths	MIT
moment	2.30.1	Date/time library	MIT
mongodb	5.6.0	MongoDB Node.js driver	Apache 2.0
morgan	1.10.1	HTTP request logger	MIT
mssql	11.0.1	MS SQL client	MIT
multer	2.0.0	File upload middleware	MIT
nocache	3.0.1	Disable client-side caching	MIT
node-wordnet	0.1.12	WordNet dictionary interface	MIT
nodemailer	7.0.7	Email sending library	MIT
passport	0.6.0	Authentication framework	MIT
password-validator	4.1.1	Password validation library	MIT
pdf-parse	1.1.1	PDF text extraction	MIT
pg	8.14.1	PostgreSQL client	MIT
pg-format	1.0.4	SQL formatting utility	MIT
polly-tts	1.0.4	AWS Polly text-to-speech wrapper	MIT
qrcode	1.5.0	QR code generator	MIT
qs	6.11.1	Querystring parser	BSD-3
recursive-readdir	2.2.3	Recursive directory reader	MIT
redis	3.1.2	Redis client	MIT
slackify-html	1.0.1	Convert HTML to Slack formatting	MIT
slackify-markdown	4.4.0	Convert Markdown to Slack formatting	MIT
socket.io	4.2.0	Real-time WebSocket server	MIT

socket.io-client	4.2.0	Real-time WebSocket client	MIT
speakeasy	2.0.0	2-factor authentication library	MIT
striptags	3.2.0	Remove HTML tags	MIT
svg-captcha	1.4.0	Generate SVG captchas	MIT
tesseract.js	6.0.0	OCR engine	Apache 2.0
twilio	4.21	Twilio API client	MIT
uuid	8.3.2	UUID generator	MIT
web-push	3.6.7	Web Push notifications	MIT
wndb-with-exceptions	3.0.2	WordNet DB with exceptions	

AEX Analytics

Library Name	Version	Description	License Type
@ibm-cloud/cloudant	0.12.10	IBM Cloudant Node.js SDK for interacting with Cloudant NoSQL DB	Apache 2.0
@presidio-dev/hai-guardrails	1.11.1	Guardrails and safety middleware for AI pipelines, part of Microsoft Presidio HAI tooling	MIT
compression	1.7.4	Node.js compression middleware	MIT
express	4.18.2	Fast, unopinionated, minimalist web framework for Node.js	MIT
gibberish-detective	1.0.3	Detects whether text is gibberish using Markov models and statistical scoring	MIT
ibm-cos-sdk	1.13.0	IBM Cloud Object Storage SDK for JavaScript	Apache 2.0
ioredis	5.3.0	A robust, full-featured Redis client with cluster support and auto-failover	MIT
ioredis-cache	2.0.0	Simple promise-based caching layer built on top of IORedis	MIT
md5	2.3.0	JavaScript implementation of the MD5 hashing algorithm	BSD 3
minio	8.0.6	MinIO client SDK for object storage compatible with Amazon S3 APIs	Apache 2.0
mongoose	8.19.2	Elegant MongoDB object modeling for Node.js	MIT
node-cron	3.0.2	Cron-like job scheduler for Node.js with recurrence and pattern rules	MIT
pg	8.8.0	PostgreSQL client for Node.js (pure JS & libpq)	MIT
rapidoc	9.3.8	Lightweight web component for rendering OpenAPI documentation	MIT
sequelize	6.28.0	Promise-based ORM for SQL databases including Postgres, MySQL, MariaDB, SQLite, SQL Server	MIT

swagger-jsdoc	6.2.8	Generates OpenAPI (Swagger) specification from JSDoc comments	MIT
---------------	-------	---	-----

AEX Functions

Library Name	Version	Description	License Type
@ibm-cloud/cloudant	0.12.0	IBM Cloudant Node.js SDK	Apache 2.0
adaptivecards	2.9.0	Adaptive Cards UI rendering framework	MIT
axios	1.7.8	HTTP client for Node.js and browser	MIT
docx	9.5.1	Create and edit .docx files in Node.js	MIT
ejs	3.1.10	Embedded JavaScript templating engine	Apache 2.0
exceljs	4.4.0	Excel generation and parsing	MIT
express	5.1.0	Fast, unopinionated web framework	MIT
form-data	4.0.5	Create form-data streams for uploads	MIT
ibm-cloud-sdk-core	5.1.0	Core utilities for IBM Cloud SDKs	Apache 2.0
ibm-watson	10.0.0	IBM Watson API client	Apache 2.0
jsonwebtoken	9.0.0	JSON Web Token implementation	MIT
jszip	3.10.1	ZIP file creation & parsing	MIT
mammoth	1.11.0	Convert .docx to HTML/Markdown	BSD-2
markdown-it	12.3.2	Modern Markdown parser	MIT
moment	2.29.4	Date/time manipulation library	MIT
mongodb	5.6.0	Official MongoDB driver for Node.js	Apache 2.0
nodemailer	7.0.7	Email sending library	MIT
pdf-parse	1.1.0	PDF text extraction tool	MIT
pptxgenjs	4.0.1	Generate PowerPoint (.pptx) presentations	MIT
qrcode	1.5.0	QR code generator	MIT
qs	6.11.1	Querystring parsing with nested support	BSD-3
utf8	3.0.0	UTF-8 string encoding/decoding	MIT

uuid	8.3.2	UUID generator	MIT
------	-------	----------------	-----

Global Admin

Library Name	Version	Description	License Type
@fastify/cookie	9.3.1	Fastify plugin for parsing & signing cookies	MIT
@fastify/formbody	7.4.0	Fastify plugin to parse URL-encoded bodies	MIT
@fastify/multipart	8.3.1	Multipart/form-data parser plugin	MIT
@fastify/passport	2.4.0	Passport authentication integration for Fastify	MIT
@fastify/session	10.8.0	Session management plugin for Fastify	MIT
@fastify/static	7.0.4	Serve static files with Fastify	MIT
@fastify/url-data	5.4.0	Fastify plugin to access URL components	MIT
@fastify/view	8.2.0	Templating engine support for Fastify	MIT
@ibm-cloud/cloudant	0.12.0	IBM Cloudant Node.js SDK	Apache 2.0
async	3.2.4	Higher-order functions & async utilities	MIT
axios	1.7.8	Promise-based HTTP client	MIT
bee-queue	1.4.0	High-performance Redis-backed job queue	MIT
busboy	1.6.0	Streaming parser for HTML form-data	MIT
connect-redis	6.0.0	Redis session store for Connect/Express	MIT
csvtojson	2.0.10	Convert CSV files to JSON	MIT
ejs	3.1.10	Embedded JavaScript templating engine	Apache 2.0
fastify	4.28.1	Fast, low-overhead web framework	MIT
form-data	4.0.0	Create multipart/form-data streams	MIT
ibm-cos-sdk	1.6.1	IBM Cloud Object Storage SDK	Apache 2.0
ibmcloud-appid	7.0.0	IBM Cloud App ID authentication SDK	Apache 2.0
joi	17.8.3	Object schema validation library	BSD 3
json2csv	4.5.4	Convert JSON to CSV	MIT

jsonwebtoken	9.0.0	JSON Web Token implementation	MIT
jwk-to-pem	2.0.7	Convert JSON Web Keys to PEM format	MIT
mime-types	2.1.24	Lookup and resolve MIME types	MIT
module-alias	2.2.2	Custom module resolution aliases	MIT
mongoose	6.0.12	MongoDB object modeling library	MIT
nodemailer	7.0.7	Email sending library for Node.js	MIT
qs	6.11.1	Querystring parser with nested object support	BSD 3
redis	3.1.2	High-performance Redis client	MIT
sendmail	1.6.1	Zero-dependency email sending utility	MIT
svg-captcha	1.4.0	Generate SVG-based CAPTCHAs	MIT
uuidv4	6.1.0	Generate RFC-4122 version 4 UUIDs	MIT

Secure Gateway

Library Name	Version	Description	License Type
@socket.io/redis-adapter	8.2.1	Redis adapter for Socket.IO enabling multi-node scaling	MIT
async	3.2.0	Higher-order functions and utilities for asynchronous programming	MIT
axios	1.13.2	Promise-based HTTP client for browser and Node.js	MIT
ejs	3.1.5	Embedded JavaScript templating engine	Apache 2.0
express	4.15.2	Fast, unopinionated, minimalist web framework	MIT
extract-zip	2.0.1	Unzip files using pure JavaScript	BSD 2
ibm-cos-sdk	1.7.0	IBM Cloud Object Storage SDK for JavaScript	Apache 2.0
multer	2.0.0	Middleware for handling multipart/form-data	MIT
redis	3.1.2	High-performance Redis client for Node.js	MIT
socket.io	4.8.1	Node.js realtime framework server	MIT
uuid	8.3.2	RFC4122-compliant UUID generator	MIT

qs	6.11.2	Querystring parser supporting nested objects	BSD 3
----	--------	--	-------

Scheduler

Library Name	Version	Description	License Type
@ibm-cloud/cloudant	0.12.3	IBM Cloudant Node.js SDK	Apache 2.0
async	3.2.4	Async utilities and control-flow helpers	MIT
axios	1.9.0	Promise-based HTTP client	MIT
bull	4.11.5	Redis-based job & task queue for Node.js	MIT
fastify	4.29.1	Fast, low-overhead web framework	MIT
ibm-cloud-sdk-core	5.3.2	Core utilities for IBM Cloud SDKs	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 S3-compatible object storage SDK	Apache 2.0
module-alias	2.2.2	Create custom module path aliases	MIT
mongodb	6.17.0	Official MongoDB driver for Node.js	Apache 2.0
nodemailer	7.0.7	Email sending library	MIT
openwhisk	3.21.4	Apache OpenWhisk serverless SDK	Apache 2.0
qs	6.11.2	Querystring parsing supporting nested objects	BSD-3
twilio	5.5.2	Twilio API client for SMS, voice, messaging	MIT
uuid	11.1.0	RFC4122 UUID generator	MIT

Self-Heal Client (Agent)

Library Name	Version	Description	License Type
axios	1.13.2	Promise-based HTTP client for Node.js and browser	MIT
body-parser	1.20.0	Parse incoming request bodies in Express	MIT
ejs	3.1.9	Embedded JavaScript templating engine	Apache 2.0
ejs-electron	3.0.0	Use EJS templates inside Electron apps	MIT
electron-alert	0.1.20	Alert/notification component for Electron apps	MIT
express	4.18.2	Fast, unopinionated web framework	MIT
http-proxy-agent	7.0.2	HTTP proxy agent for outgoing requests	MIT
https-proxy-agent	7.0.6	HTTPS proxy agent	MIT
inversify	6.0.2	Dependency injection framework for TypeScript/JS	MIT
jquery	3.7.1	DOM manipulation & utility toolkit	MIT
keytar	7.9.0	Native credential/keychain storage	MIT
moment	2.30.1	Date/time manipulation library	MIT
node-schedule	2.1.1	Job scheduling for Node.js	MIT
plist	3.1.0	Parse and build macOS/iOS PLIST files	MIT
reflect-metadata	0.2.2	Metadata reflection API (commonly used with DI)	Apache 2.0
simple-plist	1.3.1	Simplified plist parser and writer	MIT
socket.io-client	4.2.0	Realtime WebSocket client	MIT
systeminformation	5.27.11	System diagnostics & hardware information library	MIT
winreg	1.2.5	Access Windows Registry from Node.js	MIT
winston	3.3.3	Logging library for Node.js	MIT
winston-daily-rotate-file	4.5.2	Daily rotating file transport for Winston	MIT

Self-Heal Client (Admin Services)

Library Name	Version	Description	License Type
archiver	7.0.1	Create ZIP and archive files in Node.js	MIT
argon2	0.43.0	Password hashing library using Argon2 algorithm	MIT
axios	1.9.0	Promise-based HTTP client	MIT
body-parser	1.20.0	Parse incoming request bodies for Express	MIT

crypto	1.0.1	Cryptographic functions (Node.js wrapper)	MIT
express	4.18.2	Fast, minimalist web framework	MIT
http-proxy-agent	7.0.2	HTTP proxy agent for Node.js outbound requests	MIT
https	1.0.0	HTTPS utility module for Node.js	MIT
https-proxy-agent	7.0.6	HTTPS proxy agent	MIT
inversify	6.0.2	Dependency injection framework for TypeScript/JS	MIT
jsonwebtoken	9.0.2	Implementation of JSON Web Tokens	MIT
keytar	7.9.0	Native credential/keychain storage	MIT
mkdirp	3.0.1	Recursive directory creation utility	MIT
moment	2.30.1	Date and time manipulation library	MIT
node-forge	1.3.1	Cryptographic library for web/Node.js	BSD 3
node-schedule	2.1.1	Job scheduling for Node.js	MIT
p-limit	6.1.0	Limit the number of concurrent promises	MIT
reflect-metadata	0.2.2	Metadata reflection API	Apache 2.0
systeminformation	5.23.5	Hardware/system diagnostics library	MIT
unzipper	0.12.3	Unzip utility for Node.js	MIT
uuid	9.0.0	UUID generator	MIT
winston	3.3.3	Logging library for Node.js	MIT
winston-daily-rotate-file	4.5.2	Daily rotating log file transport for Winston	MIT

Self-Heal Microservice

Library Name	Version	Description	License Type
@ibm-cloud/cloudant	0.12.0	IBM Cloudant Node.js SDK	Apache 2.0
argon2	0.43.0	Password hashing library using Argon2	MIT
async	3.2.4	Async utilities and control-flow helpers	MIT
axios	1.9.0	Promise-based HTTP client	MIT
compression	1.7.4	Node.js compression middleware	MIT

csvtojson	2.0.10	Convert CSV files to JSON	MIT
express	4.17.1	Fast, unopinionated web framework	MIT
express-session	1.17.3	Session middleware for Express	MIT
ibm-cos-sdk	1.13.3	IBM Cloud Object Storage SDK	Apache 2.0
md5	2.3.0	MD5 hashing utility	BSD-3
module-alias	2.2.3	Custom module path aliasing	MIT
moment	2.29.4	Date/time manipulation library	MIT
multer	2.0.1	Middleware for multipart/form-data uploads	MIT
node-forge	1.3.1	Cryptographic tools for Node.js	BSD-3
redis	3.1.2	Redis client for Node.js	MIT
socket.io	4.2.0	Real-time WebSocket communication framework	MIT
socket.io-client	4.2.0	Real-time WebSocket client	MIT
socket.io-redis	6.1.1	Redis adapter for Socket.IO v2/v3	MIT
unzipper	0.12.3	Unzip utility for Node.js	MIT
uuid	9.0.0	UUID generator	MIT
ws	8.13.0	WebSocket client/server implementation	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
Total	0

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
Total	0

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
Total	0

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
Total	0

5.3.5 SAST Report – Self Heal Client

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
Total	0

5.3.6 SAST Report – Self Heal Microservice

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
Total	0

5.3.7 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
Total	0

5.3.8 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
Total	0

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
Total	0

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
Total	0

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
Total	0

5.5 Mend Security Reports (SaaS & On-premise)

The Mend Scan identified two security issues: one Medium severity item (PSIRT-PRB0155407) and one High severity item concerning container image scanning (PSIRT-PRB0163714, JIRA ID - SC-213158). PSIRT records are now established for both.

Mend Security Results	
■ Critical	0
■ High	1
■ Medium	1
■ Low	0
■ Informational	0
Total	0

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
Total	0

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
PRB0155407 (Medium Severity)	Mend Scan	Grpc-js package Vulnerability detected in the HCL AEX (CVE-2024-37168) The web application is affected with Grpc-js package Vulnerability. Application utilizing affected versions of a JavaScript-based gRPC framework may be vulnerable to excessive memory usage, potentially leading to performance degradation or application crashes due to memory exhaustion.
PRB0163714 (High Severity)	Mend Scan	Glob package Vulnerability detected in the HCL BigFix AEX (CVE-2025-64756) 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.

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 following table provides the details around same:

Module Name	Maximum User Count Against Which Test Case Passed	Results
Login – LUMS Authentication	100 users	Average response time for all pages: 11.06s (1 user/3 seconds ramp up)
Knowledge Search – Using Collections	500 users	Average response time for all pages: 6.223s (1 user/3 seconds ramp up)
Knowledge Search – Using Multiple Collections	500 users	Average response time for all pages: 3.42s (1 user/2.5 seconds ramp up)
Ticket creation using ServiceNow Tool	500 users	Average response time for all pages: 4.064s (1 user/2.5 seconds ramp up)
Knowledge Search – Using Single Collections	500 users	Average response time for all pages: 51.86s (100 users/ second ramp up)
Knowledge Search – Using Multiple Collections	200 users	Average response time for all pages: 47.39s (40 users/ second ramp up)
Ticket creation using ServiceNow Tool	500 users	Average response time for all pages: 45.98s (100 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	500 users	Average response time for all pages: 32.47s (10 users/ second ramp up)
Ticket creation using ServiceNow Tool	500 users	Average response time for all pages: 62.35s (10 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	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. 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. 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.
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	The HCL BigFix AEX platform has the following compliance certification/attestation available for SaaS: • ISO 27001 • SOC 2 Type II • CERT – IN Additionally for SaaS and On-premise ISO 27034 is planned for Q1 2026.

7 Application Security Controls (SaaS & On-premise)

Control	Description
Data at rest and in transit encryption	SaaS - • Data in Transit: All communication between users, services, and external systems is encrypted using HTTPS TLS 1.2/1.3. • 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). On-Prem- • Data in Transit: All communication between users, services, and external systems is encrypted using HTTPS TLS 1.2/1.3. • 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
Authentication & Authorization	• 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. • 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. • API Security: All API endpoints require authentication, either through API keys (e.g., Azure OpenAI) or OAuth 2.0 (e.g., IBM Watson).
Content Filtering & Prompt Validation (using Azure and GCP native content filtering service)	• Real-Time Content Filtering: Built-in content moderation checks for toxic, harmful, or restricted content using classifiers and guardrails before generating output. • Prompt Injection Protection: Input sanitization and pattern recognition techniques are used to detect and neutralize prompt injection attempts. • Output Filtering: Sensitive terms, data leakage, or prohibited topics are blocked before reaching the user.
Security Testing	• Follows a comprehensive security testing framework covering threat modelling, SAST, DAST, Mend, Sonar, and Prisma. • Includes penetration testing by HCLSW Security team aligned with OWASP Top 10 for Web and GenAI risks.
Secure Gateway	• Integrates seamlessly within the customer's on-premise environment. • Routes all communication through a secure, encrypted tunnel. • Uses end-to-end encryption to protect internal and external interactions from interception.

Responsible AI - Risk & Incident Management	• Conducts an AI Risk Assessment for every major release. • Maintains structured processes for identifying, reporting, and resolving AI-related security incidents.
Responsible AI - Human Oversight	• Incorporates human-in-the-loop workflows for sensitive or high-impact agent actions. • Provides safeguards to maintain operational safety during agent execution.
Responsible AI - PII Protection	• Follows a “purposeful, limited, and minimized” approach for handling PII. • Uses regex-based sanitization to redact sensitive data and prevent exposure. • Processes only the minimal data required for operational needs. • Allows display of a customizable banner to notify users not to provide or prompt any sensitive/PII data when interacting with AI agents.
Responsible AI - Accuracy & Transparency	• Supports tuning of AI hyperparameters to improve accuracy and groundedness. • Promotes transparency and clarity in AI-driven workflows.

8 Known Issues

The v12.1 release of HCL BigFix AEX Force 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	Workflows > Schema->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. RCA - 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.	Both
16532	Medium	Knowledge Spaces-> 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". RCA- 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.	Both
16411	Medium	User Management-> Routes ->User is able to create a route access entry even when the route description field is left empty. RCA - Whitespaces validation was missing in input fields	Both
16538	Medium	Agent GUI Builder-> Knowledge Configuration->If user deselect the collection under knowledge configuration list, then entire list items and other screen options gets disappears and blank panel appears. RCA - 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.	Both
16601	Medium	Tools->Agent Assist Tool-> 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. RCA - 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.	SAAS
16443	Low	Agent Performance Dashboard->Quality metrics ->Security Overview graph and Quality Metrics Trends graph are not as per the window size. RCA - Browser zoom triggers window resize 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.	Both

9 Looking Forward

The upcoming launch of AEX v13 will significantly advance the platform's capabilities, setting a new benchmark for intelligent, secure, and flexible enterprise automation. Looking ahead, our focus will be keenly directed towards delivering critical features that establish security, enhance competitive intelligence, and optimize deployment flexibility:

- **RAG Pipeline Management** - A simple, no-code way to create and reuse content processing pipelines, making it easier to set up and manage RAG-based experiences.
- **Agent Identity Management** - Each agent will have its own recognizable identity that aligns with how users are managed in the organization, ensuring consistent and controlled access.
- **Agent Traceability & Audit Logging** – An enhanced, clean, UI-based timeline will show everything an agent does in order, giving users clear visibility and helping with reviews and audits.
- **Agent Portability** - Agents can be easily moved between environments along with their related tools and settings, making migration and setup much smoother.
- **AEX Copilot** - A built-in assistant inside the admin console to help users quickly handle day-to-day tasks like managing agents and workflows.
- **Agent-to-Agent Protocol Support** - Agents will be able to communicate and work together more naturally, enabling smoother coordination across tasks.

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

hcltechsw.com