



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Rules System Rules Authoring Tool

9.0.003.01

9.0.003.01

Genesys Rules System Rules Authoring Tool Release Notes

9.x Genesys Rules System Rules Authoring Tool is part of 9.x starting in **9.0.000.13**.

Release Date	Release Type	Restrictions	AIX	Linux	Mac	Solaris	Windows
06/19/24	General			X			X

What's New

This release contains the following new features and enhancements:

- Due to the security vulnerability (CVE-2022-3509, CVE-2021-22569, CVE-2021-22570, CVE-2022-3510, and CVE-2022-3171) and lack of usage, **Protobuf-java v2.4.1** library has been removed. (GRS-4287)
- Due to the security vulnerability (CVE-2019-12415 and CVE-2022-26336) and lack of usage, **Apache Poi v3.17** library has been removed. (GRS-4284)
- Due to the security vulnerability (BDSA-2022-1920, CVE-2021-31811, and CVE-2021-31812) and lack of usage, **PDFbox lib v2.0.23** has been removed. (GRS-4283)
- Due to the security vulnerability (CVE-2023-5072, CVE-2022-45688), the **JSON** library is updated from v20090211 to v20230303. (GRS-4286)
- Due to the security vulnerability (CVE-2024-25710, CVE-2021-35515, CVE-2021-35516, CVE-2021-36090, and CVE-2021-35517), the **Apache common-compresser** library is updated from v1.20 to v1.26.1. (GRS-4285)
- Due to the security vulnerability (CVE-2023-24998), the **Apache commons-fileupload** library is updated from v1.3.3 to v1.5. (GRS-4281)
- Due to the security vulnerability (CVE-2022-30973, CVE-2022-33879, CVE-2022-30126,

Helpful Links

Releases Info

- [List of 9.0.x Releases](#)
- [9.0.x Known Issues](#)

Product Documentation

- [Genesys Rules System Rules Authoring Tool](#)

Genesys Products

- [List of Release Notes](#)

CVE-2022-25169, CVE-2018-11762, CVE-2019-10094, CVE-2020-1951, CVE-2019-10088, CVE-2020-1950, CVE-2020-9489, CVE-2018-11761, CVE-2018-11796, CVE-2018-8017, CVE-2018-17197, and CVE-2021-28657), the **Apache tika** library is updated from v1.18 to v1.28.5. (GRS-4280)

- Due to the security vulnerability (CVE-2022-46337), the **Derby** library is updated from v10.14.2.0 to v10.17.1.0. (GRS-4278)
- Due to the security vulnerability (BDSA-2016-1748 (CVE-2023-2976), BDSA-2020-3736 (CVE-2020-8908), and BDSA-2018-1358 (CVE-2018-10237), the **Google-Guava** library is updated from v17.0 to v33.1.0-jre. (GRS-4246)
- Due to the security vulnerability (BDSA-2024-0720 (CVE-2024-29025), the **Netty** library is updated from 4.1.101 to 4.1.109. (GRS-4245)

Resolved Issues

This release contains the following resolved issues:

In the GRAT application, XML files with the **entity** tags are restricted in all the XML import function. (GRS-4125)

An issue where date was not displayed on the **Rules** tab in the French language pack is now fixed. (GRS-4073)

Upgrade Notes

No special procedure is required to upgrade to release 9.0.003.01.