

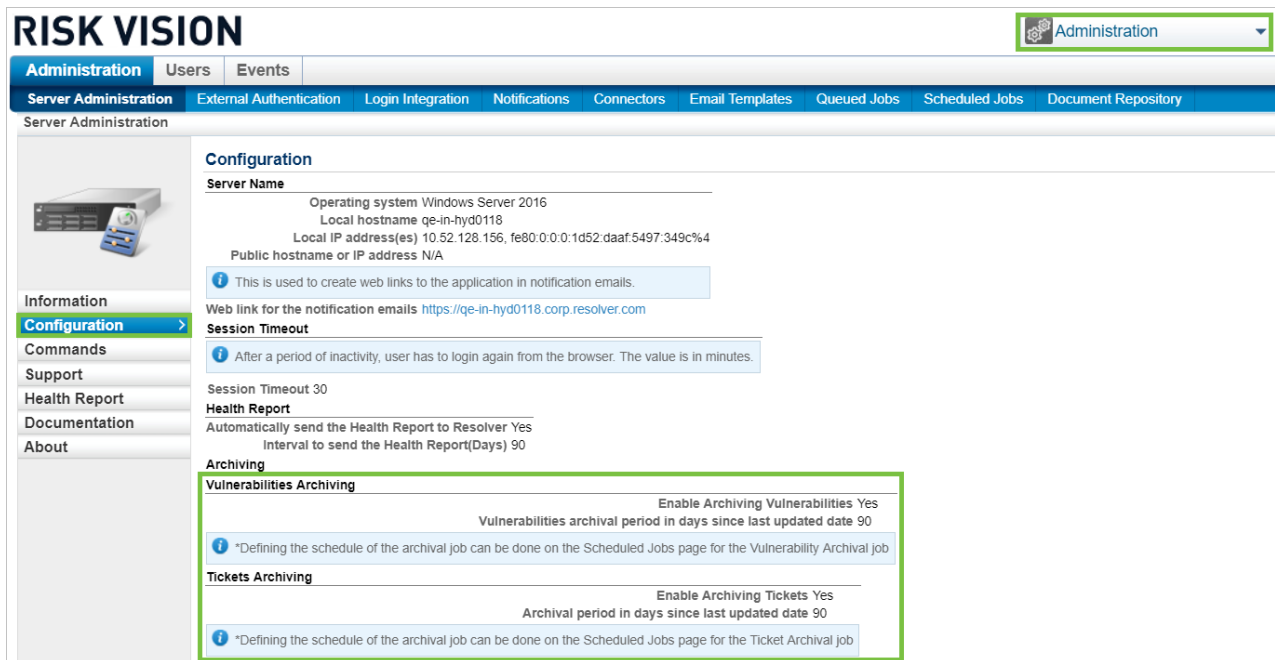
Version 9.1-GA (9.1.384.4) Release Notes

See the [Version 9.1-GA \(9.1.384.4\) Feature Overview Video](#) article for a video introduction to these features.

New Features

Vulnerability and Ticket Archiving

RiskVision now provides configuration settings to archive vulnerabilities and tickets. When configured, vulnerabilities and/or tickets that have not been updated within a customer-defined time frame, such as the last 90 days, will be archived. The benefit to archiving these objects is that the scalability and performance for non-archived records will improve because there will be fewer records in the tables to query and perform operations against.



KRI Enhancements

KRI assessments have received two categories of enhancements. First, they can now be restarted and archived. When restarted, users will not be able to edit prior periods. This will enable KRI assessments to behave more like traditional assessments. Second, KRI assessments now support a comment per KRI period so that specific KRI values can be explained.

Question 1 of 12 Help

Quarterly-count

Quarterly-count

Q4 2018 241 Count Includes entire quarter. More information

Q3 2018 202 Count Only includes the months of August and September.

Comments Implementation Remediation Evidence Applicable Entities Change History Responses

Click to enter text Keep this comment private

Follow up Risk Report

SAML LDAP Group Support

Customers using SAML for authentication will now be able to import LDAP groups associated with user records from their Identity Provider. These LDAP groups can then be used to map user roles in Resolver RiskVision.

Ticket Instances Tab

Tickets now have a Vulnerability Instances tab that shows which vulnerabilities relate to which entities on a ticket. This tab also allows users to mark specific instances as resolved.

▼ Linked To

Entities Vulnerabilities Vulnerability Instances All Others

Resolve Filter by - Show all - Refresh

Name	Identifier	Severity	Risk Score	Resolution
None.				

Error Tracking

A common request we receive from customers is to provide more tools to diagnose performance degradation. To that end, we have provided the following new charts on the Server Administration page:

1. Recent Connector Activity: Connectors that have been active in the last thirty minutes
2. Currently Running Jobs
3. Slow Running Queries

RISK VISION Administration Phani Administrator | User Settings | Help | Log Out

Administration Users Events

Server Administration External Authentication Login Integration Notifications Connectors Email Templates Queued Jobs Scheduled Jobs Document Repository

Server Administration

Job Name	Job Group	Execution status
Vulnerability Summary Update	System Jobs	Executing since 1 minutes 29 seconds
Trending Data Collection for Ad Hoc Views	System Jobs	Executing since 1 minutes 31 seconds
Vulnerability Affected Entities Incremental Updates Job	System Jobs	Executing since 1 minutes 27 seconds

▼ Slow Running Queries

Number	Id	Duration in seconds	Action	Sql Statement
1	232	151	Sending data	select this_SEVERITY as y0_from AGL_ASSET_TO_VULNERABILITY this_group by this_SEVERITY
2	236	90	Sending data	SELECT H3.vulnerability_id, H3.systemtenant_id FROM (SELECT H2.vulnerability_id, H2.systemtenant_id, COUNT(H2.asset_id) assets_count FROM (SELECT A2.vulnerability_id, A2.asset_id, A2.systemtenant_id FROM AGL_ASSET_TO_VULNERABILITY A2V INNER JOIN AGL_VULNERABILITY V ON V.vulnerability_id = A2V.vulnerability_id AND (1 OR V.vulnerability_id IN (0)) UNION ALL SELECT V2CPE.vulnerability_id, OS.asset_id, A.systemtenant_id FROM AGL_VULNERABILITY_TO_CPE V2CPE INNER JOIN AGL_OPERATINGSYSTEM OS ON OS.cpe_id = V2CPE.cpe_id AND (1 OR V2CPE.vulnerability_id IN (0)) INNER JOIN AGL_ASSET A ON A.asset_id = OS.asset_id UNION ALL SELECT V2CPE.vulnerability_id, APP.asset_id, A.systemtenant_id FROM AGL_VULNERABILITY_TO_CPE V2CPE INNER JOIN AGL_APPLICATION APP ON APP.cpe_id = V2CPE.cpe_id AND (1 OR V2CPE.vulnerability_id IN (0)) INNER JOIN AGL_ASSET A ON A.asset_id = APP.asset_id UNION ALL SELECT H0.vulnerability_id, H1.systemtenant_id FROM (SELECT V.vulnerability_id, H2.ticket_id FROM AGL_VULNERABILITY V INNER JOIN AGL_TICKETOBJECT H2 ON H2.object_id = V.vulnerability_id AND (1 OR V.vulnerability_id IN (0))) H0 INNER JOIN (SELECT A.asset_id, E2a.ticket_id, A.systemtenant_id FROM AGL_ASSET A INNER JOIN AGL_TICKETOBJECT E2a ON E2a.object_id = A.asset_id) H1 ON H1.ticket_id = H0.ticket_id) H2 GROUP BY H2.vulnerability_id, H2.systemtenant_id) H3 LEFT OUTER JOIN AGL_VULNERABILITYEXTENSION VE ON VE.vulnerability_id = H3.vulnerability_id WHERE H3.assets_count != 0 AND VE.vulnerabilityextension_id IS NULL ORDER BY H3.systemtenant_id
3	242	86	Sending data	INSERT INTO agl_aggr_asset_list SELECT av.asset_id, av.vulnerability_id FROM agl_aggr_asset_to_vulnerability av INNER JOIN agl_object_cdc ON cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_ticketobject', 'agl_vuln_to_threatobject', 'agl_asset_to_vulnerability', 'agl_vulnerability_to_cpe', 'agl_exceptionrequest_to_vulnobj', 'agl_vulnerability_to_patch', 'agl_exceptionrequest') AND cdc.column_name IN ('vulnerability_id', 'object_id') AND cdc.object_id = av.vulnerability_id AND cdc.action_flag IN ('U', 'D') UNION SELECT av.asset_id, cdc.object_id FROM agl_object_cdc cdc LEFT JOIN agl_aggr_asset_to_vulnerability av ON cdc.object_id = av.vulnerability_id WHERE cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_ticketobject', 'agl_exceptionrequest_to_vulnobj', 'agl_vulnerability_id') AND cdc.action_flag IN ('U') UNION SELECT av.asset_id, av.vulnerability_id FROM agl_aggr_asset_to_vulnerability av INNER JOIN (SELECT av.vulnerability_id FROM agl_aggr_asset_to_vulnerability av INNER JOIN agl_object_cdc ON cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_ticketobject', 'agl_exceptionrequest_to_vulnobj', 'agl_asset_to_hierarchy', 'agl_classification', 'agl_ownership', 'agl_operatingsystem', 'agl_application', 'agl_hierarchy', 'agl_customattributes', 'agl_asset') AND cdc.column_name IN ('asset_id', 'object_id') AND cdc.object_id = av.asset_id AND cdc.action_flag IN ('U', 'D') UNION SELECT vc.vulnerability_id FROM agl_operatingsystem os INNER JOIN AGL_APPLICATION APP ON APP.cpe_id = os.cpe_id AND cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_cpe', 'agl_operatingsystem') AND cdc.column_name = 'cpe_id' AND cdc.object_id = os.cpe_id AND cdc.action_flag IN ('U', 'D') INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = os.cpe_id UNION SELECT vc.vulnerability_id FROM agl_application app INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = app.cpe_id AND cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_cpe', 'agl_application') AND cdc.column_name = 'cpe_id' AND cdc.object_id = app.cpe_id AND cdc.action_flag IN ('U', 'D') INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = app.cpe_id UNION SELECT os.vulnerability_id FROM agl_operatingsystem os ON os.cpe_id = os.cpe_id UNION SELECT app.asset_id, vc.vulnerability_id FROM agl_application app INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = app.cpe_id AND cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_vulnerability_to_cpe', 'agl_exceptionrequest', 'agl_ticketobject', 'agl_ticket') AND cdc.column_name IN ('vulnerability_id', 'object_id', 'ticket_id') AND cdc.object_id = vc.vulnerability_id AND cdc.action_flag IN ('U', 'D') INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = os.cpe_id UNION SELECT app.asset_id, vc.vulnerability_id FROM agl_application app INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = app.cpe_id AND cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_vulnerability_to_cpe', 'agl_exceptionrequest', 'agl_ticketobject', 'agl_ticket') AND cdc.column_name IN ('vulnerability_id', 'object_id', 'ticket_id') AND cdc.object_id = vc.vulnerability_id AND cdc.action_flag IN ('U', 'D') INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = os.cpe_id UNION SELECT app.asset_id, vc.vulnerability_id FROM agl_application app ON vc.cpe_id = app.cpe_id UNION SELECT os.asset_id, vc.vulnerability_id FROM agl_operatingsystem os INNER JOIN AGL_APPLICATION APP ON APP.cpe_id = os.cpe_id AND cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_asset', 'agl_ownership', 'agl_classification') AND cdc.column_name IN ('asset_id') AND cdc.object_id = os.asset_id AND cdc.action_flag IN ('U') INNER JOIN AGL_VULNERABILITY_TO_CPE VC ON VC.cpe_id = os.cpe_id UNION SELECT app.asset_id, vc.vulnerability_id FROM agl_application app INNER JOIN AGL_APPLICATION APP ON APP.cpe_id = app.cpe_id AND cdc.modified_date_time >= v.incr_date AND cdc.table_name IN ('agl_asset', 'agl_ownership', 'agl_classification') AND

You can also view further information about active server jobs by going to **Administration>Scheduled Jobs**. The **Current Status** column shows the status of scheduled jobs. When a job is triggered, its status will change to *Executing from 'xx'* seconds. Finished jobs have a status of *Not Executing*.


Health Reports

The Health Report now shows the number of attachments, as well as the aggregate storage space consumed by the Attachments folder.

Also, to provide Resolver with important metrics to use for scalability and performance testing and to aid in prioritization of future scalability and performance optimizations, Health Reports will now be automatically sent to Resolver. You can disable this functionality or adjust how frequently Health Reports are sent.

Administration	Users	Events
Server Administration	External Authentication	Login Integration
	Notifications	Connectors
	Email Templates	

Server Administration



Information

Configuration >

Commands

Support

Health Report

Documentation

About

Configuration

Server Name

Operating system Windows Server 2016
Local hostname qe-in-hyd0118
Local IP address(es) 10.52.128.156, fe80:0:0:0:1d52:daaf:5497:349c%4
Public hostname or IP address N/A

i This is used to create web links to the application in notification emails.

Web link for the notification emails <https://qe-in-hyd0118.corp.resolver.com>

Session Timeout

i After a period of inactivity, user has to login again from the browser. The value is in minutes.

Session Timeout 30

Health Report

Automatically send the Health Report to Resolver Yes
Interval to send the Health Report(Days) 90

RiskVision Permissions

A new permissions check that restricts users access to RiskVision pages based on user permissions has been added and tested against RiskVision default roles. However, while rare, customers with custom roles may run into access issues with specific pages. These are unintended issues and should be reported to [Resolver Support](#) as soon as they are encountered.

Bug Fixes

- RRV-1326: Files attached to findings carried forward for restarted assessments will now be accessible.
- RRV-931: Fixed an issue with OpenSSL that caused the Apache Service to log SSL warnings.
- RRV-993: JasperReports Server was upgraded to version 6.4.3 to resolve the following [TIBCO vulnerabilities](#): CVE 2018-5429, 2018-5430, and 2018-5431.
- RRV-1025: The following issues no longer occur:
 - When evidence and files attached to objects such as entities, findings, and tickets are deleted in the UI, they will be deleted from the data/attachments folder.
 - When assessments are restarted, evidence files are linked and not copied, which will result in less storage space being consumed.
- RRV-70: The load time of the Control Results page has been improved.

- RRV-71: Filtering the Control Results page by *Show Applicable* now has improved performance.
- RRV-72: Assessment workflows no longer transition slowly.
- RRV-1757, RRV-1729 and RRV-1892: Documents attached to findings and responses now load correctly.
- RRV-1768: Fixed an issue where documents attached to entities displayed the incorrect version number.
- RRV-935: Users who synchronize findings to the current workflow definitions are no longer added as stakeholders to the related findings.

Known Issues

Tracking ID	Description
RRV-1017	<p>JasperReports Server is unresponsive after saving a scheduled report in Internet Explorer.</p> <p>Workaround:This issue can be resolved by refreshing the page</p>
RV-22319	<p>Not all Microsoft® Word documents can be imported as RiskVision policy documents.</p> <p>Workaround: Most issues can be resolved by manually editing the imported document or by copying and pasting one section at a time.</p>
RV-24010	<p>The default choice template (a drop-down list) does not work with table-type questions.</p> <p>Workaround: Create a new choice template for use with table-type questions.</p>
RRV-2593	<p>An error message is generated when exporting a JasperReports Server repository using the script js-export.bat. This is the result of a JasperReports Server bug that creates an error message when one should not be created. The export is fine, and will be</p>

	able to be successfully imported into the same or another instance of JasperReports Server.
RRV-2660	An error message is generated when executing the command: <code>js-export --everything --output-zip repository.zip >>test.log</code> . This is a known issue for Amazon Corretto 8. The export and import of repository.zip is successful and there are no known issues due to this error.
RV-29911	Preferred ownership issues:
RV-29915	<ul style="list-style-type: none"> • Viewing assessment details in a program can reveal all stakeholders in the workflow, rather than only the preferred owners in the current stage.
RV-35429	
RV-35741	<ul style="list-style-type: none"> • Enabling preferred ownership on a workflow that is already in use only applies to subsequent preferred ownership assessments that use the workflow.
RV-36862	
RV-36717	<ul style="list-style-type: none"> • Deleting preferred ownership from controls after the launch of assessments does not change the assignment of controls to stakeholders.
RV-40613	
RV-40620	<ul style="list-style-type: none"> • If content in a program is added at the group level, and if it has preferred ownership added at the control level, duplicate controls will be created when the program is edited, or when assessments within that program are restarted. <p>Workaround: Assign the preferred ownership at the same level as the content added in a program. For example, if the preferred ownership is assigned to the content at the group level, assign the content to the program at the group level. If the preferred ownership is assigned to the content at the control level, assign the content to the program at the control level.</p> <ul style="list-style-type: none"> • Preferred ownership works only in the first stage of assessment workflows with branching. • Controls assigned to the assessment stakeholders do not get updated after editing the program to select the following program option: Do not assess controls with preferred

	<p>ownership configured when the entities being assessed have no owners that correspond to the preferred owners associated with the control.</p>
RV-30240	<p>A custom dashboard or chart that uses the comment column from the agl_ramitigationtable will fail to execute the query.</p> <p>Workaround: To execute the custom query successfully, rename the comment column to mitigation_comment.</p>
RV-31601	<p>The cache does not update immediately when controls and subcontrols are updated.</p> <p>Workaround: Wait a few minutes for the controls and subcontrols to be updated in the relevant assessments.</p>
RV-33240	<p>When propagation is enabled, answering the parent entity assessment will not update the scores of its child entities on the Program Details page>Assessments tab. Scores are updated correctly on the Assessment Details page > Control Results tab of the parent.</p> <p>Workaround: To update the scores, select the child entity, then select Propagate Control Results from the More Actions dropdown list.</p>
RV-33301	<p>When a user tries to run a Jaspersoft report after logging out of RiskVision, the report appears to run but is not rendered. The reason the report appears to run is that the Jaspersoft user interface is still available.</p> <p>Workaround: Close the browser where the Jaspersoft application is running.</p>
RV-33316	<p>Creating a Table chart-type of Policies no longer executes the query. This issue persists only with the Oracle database.</p> <p>Workaround: To build the chart without errors, ensure that the Selected Columns contain any string-type column at the top and the Audience column is moved down the selected list.</p>

RV-35412	<p>Risks added to an assessment cannot be removed, even if the stakeholder changes the answer choice from any assessment workflow stage.</p> <p>Workaround: Manually delete the risks.</p>
RV-36406	<p>Adding the same input control multiple times when importing a RiskVision chart does not produce the desired results.</p> <p>Workaround: If you need to have the same input control more than once, create a new input control with a different resource ID.</p>
RV-36472	<p>It may not be possible to create an assessment that contains a dynamic group of more than 17,000 entities.</p> <p>Workaround: Whenever a dynamic group contains more than 17,000 entities, split the excess entities into a separate dynamic group and then run the assessment.</p>
RV-36615	<p>It is impossible to export JasperReports Server Fusion charts to formats other than PDF and HTML.</p>
RV-37639	<p>The schema name is saved in the database in uppercase, even if the user entered it in lowercase when creating the schema:</p> <ol style="list-style-type: none"> 1. Whenever hyphens are used in the schema name during import, the schema name is converted to uppercase. Example "schema-name" becomes SCHEMA- NAME. 2. When an export is performed with the original name (schema name in lower case), a "schema not found" error message is thrown. Export is successful if the schema name is given in uppercase. <p>Workaround: Avoid using hyphens in schema names. If you must use a hyphen, reference the schema name using uppercase</p>

RV-37753	Risks are not auto-identified and text-type sub controls fail when scoring for text-type questions is enabled in Questionnaire Presentation Options.
RV-37965	The Jasper Reports Server installation fails if the length of the installation path is longer than 260 characters.
RV-38326	The JasperReports Tomcat service fails to start on a computer if the Jasper Reports Server installation path contains special characters, such as \$, %, &, and @. The service does not start even when it is attempted manually.
RV-39271	Users with an assigned <i>Vulnerability severity</i> filter receive an error message when accessing the entity. Workaround: Use <i>Entity Vulnerability General.Severity for this entity</i> as a condition instead of <i>Vulnerability General.Severity</i> .
RV-39409	It is not possible to advance a workflow stage if it is assigned a team of more than 200 stakeholders.
RV-39650	Control results are not propagated down to related entities if multiple assessments for the related entities are created after the controls results have been propagated by the source entity. Workaround: Execute Propagate control results from the Monitor Actions drop-down on the Programs > Assessments page.
RV-41364	Entities cannot be copied if they are imported into RiskVision without a primary owner. Workaround: Assign a primary owner to all imported entities before copying them.
RV-42362	Users with an Entity filter condition of <i>Classification. Internal or external</i> encounter an exception when running reports. Workaround: Avoid using the <i>Classification. External or internal</i> attribute within any filter conditions. Use the <i>Entity. Internal or External</i> attribute instead.

RV-42602	<p>Entities cannot be retrieved for users with the filter condition <i>EntityCustomAttributes_CustomText_1</i>.</p> <p>Workaround: Filtering based on CLOB-type columns on the RiskVision server is not supported. Any report attribute to be excluded from filtering must be marked as a non-filterable ('filterable="false"') in the ReportAttributes.xml file.</p>
RV-42629	<p>Data in RiskVision doesn't honor the EntityCustomAttributes_CustomEncryptedString_1 filter.</p> <p>Workaround: Any report attribute to be excluded from filtering must be marked as non-filterable ('filterable="false"') in the ReportAttributes.xml file. ACL filters with conditions based on encrypted fields are not supported.</p>
RV-42839	<p>Unable to load data to users with the Incident filter condition of <i>Incident_Incident_Comment</i> ACL. Filtering based on CLOB-type columns is not supported on the RiskVision server.</p> <p>Workaround: To prevent report attributes based on CLOB or similar columns from being displayed in Filter Manager's filter condition field list, mark the report attributes as non-filterable ('filterable="false"') in ReportAttributes.xml file.</p>
RV-42991	<p>Exceptions requested from Home-Exception Requests are not displayed in the Exceptions tab and Control results drill down.</p> <p>Workaround: Create the exceptions at the assessment level, not on the Home > Exceptions page.</p>
RV-43058	<p>The filter condition <i>Entity Custom Attributes. Custom Rational Number 3</i> generates an error.</p> <p>Workaround: Add the Custom Attributes extensions for Float in the ReportAttributes.xml file:</p> <p>Restart Tomcat Services.</p>

RV-45781	<p>After upgrading from version 7.0 to version 8.5HF2, RV user and sysadmin cannot login to Standalone Jasper.</p> <p>Workaround: After upgrading RiskVision, perform the following steps to login to Standalone Jasper:</p> <ol style="list-style-type: none"> 1. Log in to RiskVision with a user that has admin privileges. 2. Click R7 Analytics. The Jasper home page is displayed. 3. Navigate to Manage > Users. 4. Click Add User and enter the necessary information. 5. Go to the %Home%\Reportserver\ReportServer\postgresql\bin folder and open pgAdmin3. 6. Connect to the RiskVision database. 7. Open the jiuser table. 8. Copy the password of the newly created user. 9. Find the sysadmin or rvjasperuser user and change their password to the copied password. 10. Restart Jasper services 11. Verify that sysadmin or rvjasperuser user can login to Jasper Standalone using the new password.
RV-46606	<p>Horizontal scroll bars are missing in JasperReportsServer dashboards that require horizontal scrolling. This is a bug in JasperReports Server version 6.3.0 and will be fixed in a future JasperReports Server release.</p>

System Requirements

The following hardware requirements represent the **minimum** system requirements to install Resolver RiskVision™ V. 9.1. These specifications are for planning purposes only. To learn about the recommended hardware and software for your environment, contact Resolver Support.

Hardware	Minimum

Total number of CPU cores	8
Memory	16 GB
Disk Space	At least 100 GB of free disk space

Supported Versions

This release supports the following versions of third-party software:

Product	Version
Operating System	Microsoft Windows Server® 2008 R2 SPI Standard x64 Edition and Windows Server® 2012 R2 Standard x64, Windows Server® 2016
Amazon Coretto (JDK)	8
Apache Tomcat	8.5.32
Apache Web Server	2.4.33
Apache OpenOffice	4.1.4
Jasper Reports Server	6.4.3
MySQL	5.7.22
Oracle	12.1.0.2.0
Web Browser	Internet Explorer® 11, Edge, Mozilla Firefox®, Google Chrome®
Adobe® Flash browser plug-in	Adobe® Flash Player, version 11 (optional)

JasperReports Server 6.4.3 comes with the following technologies:

Product	Version
PostgreSQL	9.3.20
Apache Tomcat	8.0.48
Oracle JDK 8	1.8.0_151 (8u151)