Scheduled Jobs

System Jobs are regularly-scheduled tasks that the RiskVision solution performs routinely in the background. Jobs in the System Jobs group can be viewed along with other queued jobs, such as reports. Jobs including system jobs and scheduled reports can be accessed by other users if they have a user role with the Scheduled Job View permission. In order to activate, deactivate, delete, run, or reschedule a job, you will need to have the Scheduled Job Manage permission along with the Scheduled Job View permission.

To run a system job now, check the System Job and click **Run**.

To enable or disable a system job, check the System Job and click **Activate/Deactivate**.

Click on an active system job to view more details, including:

- **Job Start**. When the job was created
- **Last Executed**. When the job was last run
- **Next Executions**. A list of upcoming dates and times when the job will be run

Default System Jobs

System job	Description	Job Details
Affected Entities Notification Sender	Sends notification for the affected entities of newly imported or updated vulnerabilities.	From the "Threat Management preferences" page: If Automatically create ticket is set to **Yes**, then this job creates tickets for each vulnerability (which has affected entities). If Acknowledge the vulnerability when the tickets are automatically created is set to **Yes**, then this job will acknowledge each vulnerability (which has affected entities). For all the affected entities , system notifications will be sent. Default value = **"enabled"** To enable this job set com..job.effectedEntities NotificationSenderJob.disable= true
Alert Rule Processor	Evaluates alert rules and sends notifications if risk or compliance scores have crossed set thresholds.	
Assessment Objects Carry Forward	Gets snapshot of assessment related objects	The Assessment Objects Carry Forward job is required to archive questionnaire data and objects attached to the assessment, such as findings, tickets, exceptions, and to carry forward these objects to the continued assessment.
Control Results Updater	Updates control results from the Connectors that are in use. RiskVision has the capability to pull information/data from connectors. When such data is populated, this job updates all results (such as - passed, failed, scores etc) in their respective tables.	This job updates the assessment **(agl_apc) with vulnerability data. Based on this data, scores and updated scores will be calculated for this APC entry.** This job reads the survey question results table and updates the compliance level score for assessments (agl_apctable). This job also updates the vulnerability links related to the entity. This job updates control responses from the Common Control Framework (see Additional Program Options settings of automatically answering unanswered controls using results from related controls.). This job applies compliance score from the related controls and applies answers from the related controls when controls have exactly the same set of choices. Vulnerabilities are related to the following Additional Program Options: • Automatically fail controls when vulnerabilities, mapped to the controls, are reported in the entity. • Automatically pass controls when vulnerabilities, mapped to the controls, are

System job	Description	Job Details
		not present or closed in the entity. • Automatically update controls when data feeds, mapped to the controls, are reported in the entity.
CrowdStrike Falcon Intelligence Connector	CrowdStrike Falcon Intelligence Connector pulls intelligence reports and persists into RiskVision Database.	Downloads threat intelligence data from the CrowdStrike Falcon Intelligence service, parses the data, places it into the RiskVision database, and correlates it with the National Vulnerability Database CVE data, if CVE references are provided by CrowdStrike Falcon Intelligence.
Daily Server and Database Hot Backup	Performs RiskVision Server, database, JasperReports Server, and Jaspersoft repository backup to a folder. The Jasper Repository contains Jasper Report repository internal data. This is a feature provided by Jaspersoft itself.	This job performs: • A Server files backup (data folder etc). • Database backup. If the database is Oracle, then specify "SYSTEM" user encrypted password for property "database.oracle.admin.password.encrypted" and also set `com.agiliance.admin.backup.BackupManager.skipOracleBackup= true` `Default Value = "false."` • Jasper database backup, and • Jasper repository backup. You can save a database backup in .exe file format. Note that running the Daily Server and Database Hot Backup jobs at the same time as other jobs may result in the database backup jobs failing. When this happens, an error message that reads "The database backup job failed as it could not get the following tables ..." will be returned in the **catalina.log**. For RiskVision version 9.3.5 or later, add the `com.agiliance.admin.backup.BackupManager.IgnoredDatabaseTableNames=` property to a**giliance.properties**. Then restart the Tomcat and rerun the database backup job. This will allow for the Daily Server and Database Hot Backup jobs to run at the same time as other jobs without causing the database backup jobs to fail. For customers using a version below 9.3.5, the only workaround is to stop all jobs and then run the database backup jobs. Also note that running the Daily Server and Database Hot Backup jobs on a multi-tier setup may return the following error message in the logs: "BackupManager - Database backup failed due to error: com.agiliance.common.ALException:". If this happens, install Microsoft Visual C++ 2013 at the application's server side for smoother database backup. See the RiskVision System Requirements for further details.
Database Statistics Updater	Updates MySQL database table statistics. This system job is disabled by default. It is recommended that this job is enabled for MySQL. The duration needs to set appropriately since this activity takes a lot of time and effects all other operations. only recommends turning on this job when advised to by Support to troubleshoot an issue. This job is not available when using the Oracle database. Instead, use the DBMS_STATS.GATHER_SCHEMA_STATS procedure to gather statistics for all	This job updates all the required hashing techniques that are used to retrieve the objects, internal index tables etc. These statistics are used by optimizers for better performance. For example - performance, When doing collect stats on fields/indexes , the system collects the information like: total row counts of the table, how many distinct values are there in the column, how many rows per value, is the column indexed, if so unique or non unique etc.

System job	Description	Job Details
	objects in a schema.	
Detailed Compliance and Risk History for Entities and Dynamic Groups	Takes a snapshot of compliance scores and risk scores for entities and dynamic groups. The scores are computed for each control, questionnaire, sub-control, question, and so on, for all entities and dynamic groups.	This job updates: Asset compliance risk history table (agl_assetcompliancerisk**history**) with the contents of entity compliance risk table (agl_assetcompliancerisk). Virtual group compliance risk history table (**agl_vgcompliancerisk**history**) with the contents of virtual group compliance risk table (agl_virtualgroupcompliancerisk).** This follows a retention policy based on the property com.agiliance.admin.scheduler AssetAndVirtualGroupCompliance RiskScoreHistoryUpdateJob.maximum HistoryRetentionTime". Default Value = 2 years. (Which means any data more than 2 years old is removed from each table respectively.)
Dynamic Group Entity Map Builder	Completely rebuilds the Dynamic Group Entity Map and updates policy assignments.	This job rebuilds the Dynamic Group entity mapping for new dynamic groups
Dynamic Group Entity Map Updater	Updates the Dynamic Group Entity Map and policy assignment for all entity changes.	This job rebuilds the Dynamic Group entity mapping for new dynamic groups, by updating the existing association.
Entity/Dynamic Group Score History	Takes a snapshot of all entities and Dynamic Group's risk and compliance scores.	The 'Entity/Dynamic Group Score History' uses the classification criticality to calculate assessment's compliance score and the Dynamic Group's score. This job then updates this to the Dynamic Group history table (agl_virtualgroupscorehistory). Similarly the entity score history table (agl_assetscorehistory) is also updated with required scores such as compliance, risk, confidentiality and integrity etc.
ERM Risk Mapper	Creates risks from failed controls in related Compliance Manager and Vendor Risk Manager programs.	To use this job, enable the featureAutomatically identify risks from failed controls for the following Compliance Manager or Vendor Risk Manager programand set its value as true.
Events Archive	Archives events that are more than three months old.	This job archives events which are of more than three months old. This duration is not editable.
Exception Request Checker	Checks for the time stamp before processing exceptions.	If the exception "**start time**" is between the last execution time and current day end time **11:59 AM**, it is marked as approved. If the "**end time**" is between one day after the execution and the current day time **12:00 AM**, the exception is marked as expired. Assessments are also marked with required expiration of exceptions.
FireEye ISight Connector	FireEye ISight Connector pulls intelligence reports and persists into RiskVision Database.	Downloads threat intelligence data from the FireEye iSight service, parses the data, places it into the RiskVision database, and correlates it with the National Vulnerability Database CVE data, if CVE references are provided by the FireEye

iSight service.

System job	Description	Job Details
LDAP Teams Synchronization	Synchronizes Team membership with group affiliations in an external LDAP directory, such as Active Directory.	This job synchronizes users for teams that are imported from LDAP, with the SystemUsertable.
LDAP Users Synchronization	Synchronizes user attributes for users that are imported from LDAP.	This job synchronizes user attributes for users that are imported from LDAP, with the SystemUsertable.
Notification Escalator	Responsible for sending out workflow escalations and reminders.	By default the job is executed only once per day and is controlled by the property **com..scheduledJob.reminderOrEscalationJobs.runOnlyOnceADay= true** Default Value = true. This job will run checks based on the following properties: **com.agiliance.notification.assessmentAdvanceChecker.enabled=true** com.agiliance.notification.ticketEscalationChecker.enabled=true com.agiliance.notification.exceptionWFAlertChecker.enabled=true com.agiliance.notification.surveyWFAlertChecker.enabled=true com..notification.ticketReminderChecker.enabled=true Depending on the property, respective checker is called. For example, if com..notification.assessmentAdvanceChecker.enabled=true, then AssessmentAdvanceCheckeris invoked. **AssessmentAdvanceChecker**moves the workflow based on workflow configuration. When you customize a workflow, the **Auto Advance**check-box in workflow options must be enabled. Ticket escalation escalates tickets, Exception alert checker checks for exceptions which are "expired" and sends notifications, Survey checker checks for alerts (which are already defined), and matches them with the workflow alerts. Ticket reminder checks for tickets for which reminders have to be sent.
Notification Sender	Sends e-mail notifications other than escalations and reminders.	
Patch Status Updater	Updates the patch status of vulnerability instances for newly created or updated patches and vulnerabilities.	
Program	Updates Dynamic Group entities in programs automatically. This job will flag entities which have been added to or	To execute the job, the options Add entity automatic and Remove entity automatic should be enabled while creating a project.

System Job	Description	Job Details
Updater	removed from Dynamic Groups for addition to or deletion for assessment creation or deletion.	If they are enabled and if any entity added to Dynamic Group or removed from group, corresponding assessments are created and updated.
Purge Job Queue	Purges old and non-active jobs in the job queue database.	This job will purge the jobs in the queue - the ones that not new or not started yet. This job checks for the status of the jobs along with duration. This job will purge jobs which are in "Suspended", "Done" or "Error" state. This job enforces the property **com..dal.dao.JobPersistenceDAO.keepNDays=7** Default Value = 7. Any job after 7 days is removed.
Questionnaire Change Notification Sender	Sends questionnaire change notifications by e-mail.	
Report Summary Builder	Builds report summaries.	This job populates the tables and views which are used for reporting.
Risk Analysis Calculator	Calculates risk analysis metrics.	The job updates scores at the assessment level. Examples of attributes updated include confidentiality, integrity, availability, overall risk score and also overall compliance score of an assessment are updated.
Scan Summary Update	Updates the scan summary, summarizing the information about the data that is part of a scan. Scan summary job updates summary information per scan for findings e.g. total findings, number of passed/failed, number of mapped to control/entity for current scans only.	This job updates the summary information per scan for findings. This job updates agl_scantable. Scan is linked to finding table and the fields like **passed findings** and **failed findings** and so on are updated.
System Monitoring	Monitors the health of the system. Provides health monitoring information, which is displayed on the Server Administration page. All the metrics displayed in Health Report are calculated by this job.	This job provides the health monitoring information, that is displayed on the **Server Administration** page. This job also provides information on resources, license expiration date and sent notifications.
System User Maintenance	Performs system user maintenance, such as unlocking user accounts. A user account can be locked out due to a password policy violation, For example - after n number of failed log in attempts. The 'System Monitoring Job' unlocks the user after a certain wait period.	This job performs system user maintenance. Currently, the maintenance job includes unlocking user accounts. If a user account is locked out due to password policy violations, such as consecutive number of failed logins, this job will unlock it after the wait period. The property to set password unlock is **password.unlockWaitPeriod=12.** Default Value = 12 hours.

System job	Description	Job Details
Search Index	Automatically recreates search indexes.	This job periodically checks the various RiskVision pages to determine if any search indexes are out of sync. If they are, then the job rebuilds the search indexes for the pages that are out of sync.
Threat Summary Update	Updates the Entities at Risk, Related Tickets, Targeted Vulnerabilities and Related Incidents columns of the Threats Grid.	This job updates Entities at Risk, Related Tickets, Targeted Vulnerabilities and Related Incidents columns of the Threats
Trending Data Collection for Ad Hoc Views	Collects metrics based on Ad Hoc queries.	The Trending Data Collection for Ad Hoc Views job provides a means to trend data that can be collected using a user written query.
Trending Data Collection for CM Dashboard	Collects trending metrics from ad hoc queries for the Compliance Manager dashboard.	The Trending Data Collection for CM Dashboard job provides a means to collect trend data specifically for Compliance Manager dashboard.
Trending Data Collection for Tickets	Collects ticket trending metrics	The Trending Data Collection for Tickets job provides a means to collect trend data specifically for tickets
Update Objects	Runs object update tasks such as entity classification propagation.	This job updates the Entity classification and profile evaluation for a given entity.
Update Questionnaire	Updates questionnaires to help quickly render the Home > Questionnaires grid.	
Upload Repository Cleaner	Cleans up temporary files created by the upload component.	
Update Questionnaires for Always On Assessments	Updates the Home -> Questionnaires page for Always On-restarted assessments.	The Update Questionnaires for Always On Assessments job is required to ensure that the questionnaires for Always On Assessments appear on the Home -> Questionnaires page of each user who is assigned questions for the continued assessment.
Vulnerability Summary Update	Updates vulnerability summaries, including information such as affected entities count.	This job updates the vulnerability and the CPE summary, including information such as affected entites, affected entites with tickets, and unresolved affected entitesetc. The job updates the agl_vulnerability, agl_vulnerabilityExtensionand **agl_CPE** tables and their corresponding link tables. Entity group totals are not updated. Only the affected entites are updated.
Vulnerability Affected Entities Full Refresh Job	Updates the affected entity groups for the Affected Entities tab of a vulnerability throughout the system.	By default this job is secheduled to run every Saturday morning at 5 AM. The user can reschedule this to be hourly, daily, weekly, or monthly as needed. Users can choose to rebuild the grouping cache by clicking the **Rebuild Grouping Cache** button under Threat management Preferences -> Groupings tab.
Vulnerability Affected Entities Incremental Updates Job	Vulnerability Affected Entities Incremental Updates Job	This job is used to call the daily update of affected entities.

System job	Description	Job Details
Vulnerability Instance Exception Updater	Calculates the Applied Exception Status for every unresolved vulnerability instance.	After calculating the Applied Exception Status, this job updates the status column with the relevant status.
Vulnerability Risk Score Calculator	Vulnerability Risk Score Calculator	The job only recalculates risk scores for entities whose vulnerabilities or relevant entity attributes have changed, but RiskVision recommends first testing the performance impact of the job in your environment if you decide to run it multiple times per day.
Vulnerability Risk Score Initiator	Vulnerability Risk Score Initiator	If you want to apply change of score system throughout the application, then the Vulnerability Risk Score Initiator job will refresh the scores and re-calculate everything based on new score system.
Weekly Backup of Attachments	Performs backup of ticket and policy document attachments.	This job creates a complete back-up of the attachment directory. Weekly Backup of attachments will only create a backup of the attachments folder. All the evidence are stored as attachments.
Workflow Reminder	Sends workflow reminders by e-mail.	

Further details of the system jobs are explained in the table below:

System job	Recommended Schedule	Demand On System Resources	Required
Affected Entites Notification Sender	Every 30 minutes	Medium	Not required for customers who do not have Threat and Vulnerability Manager or vulnerability notifications.
Alert Rule Processor	Daily at 5:30 p.m.	Low	Not required by customers who are not using compliance or risk score alerting.
Control Results Updater	Every 5 hours	High	Only required by customers using Compliance Manager and Enterprise Risk Manager.
Daily Server and Database Hot Backup	Daily at 6:30 a.m.	High	Yes. strongly recommends leaving this job enabled.
Database Statistics Updater	Weekly, Sunday at 1:30 p.m.	Low	No. You cannot run the Database Statistics Updater job during the execution of the Daily Server and Database Hot Backup job.
Detailed Compliance and Risk History for Entities and Dynamic Groups	Monthly, on the 1st, at 2:30 p.m.	Medium	No, but if this job is disabled you will not be able to trend on risk and compliance scores.
Dynamic Group Entity Map Builder	Daily at 2:30 p.m.	High	Yes. This job is required for Dynamic Groups to work and Dynamic Groups are essential to the functioning of the product.
Dynamic Group Entity Map Updater	Every 15 minutes	High	Yes. This job is required for Dynamic Groups to work and Dynamic Groups are essential to the functioning of the product.
Entity/Dynamic Group Score History	Daily at 12:30 p.m.	Medium	No.

System Job	Recommended Schedule	Demand On System Resources	Required
ERM Risk Mapper	Daily at 11:30 a.m.	Medium	No. This job is only required by customers using the auto-risk identification feature.
Events Archive	Monthly at 7:00 p.m	Medium	Yes. This job is required to prevent logs from taking up a lot of space in the database.
Exception Request Checker	Daily at 6:30 p.m.	Medium	No. This job is required by customers using exceptions.
LDAP Teams Synchronization	Daily at 5:30 p.m.	High	No. This job is required by customers who are using teams and are managing teams by syncing them to LDAP.
LDAP Users Synchronization	Weekly, Friday at 10:30 a.m.	High	No. This job is required by customers who have users authenticating against their LDAP directory.
Notification Escalator	Daily at 3:30 p.m.	Low	No. This job is required by customers who are using the escalation feature and the reminder feature of workflows.
Notification Sender	Every 15 minutes	Low	No. This job is required by customers using notifications.
Patch Status Updater	Every 30 minutes	High	No. This job is only required by customers who are using Threat and Vulnerability Manager and who are tracking patches via Threat and Vulnerability Manager.
Program Updater	Every 2 hours	High	No. This job is only required by customers who are assigning dynamic groups to programs.
Purge Job Queue	Daily at 5:30 p.m.	Low	Yes. This job should be run to maintain the efficiency and performance of the database.
Questionnaire change Notification Sender	Every 30 minutes	Low	No. Customers only need this when they want to send out questionnaire change notifications to let users who are responsible for answering questions know when the content in the questions has changed or new questions has been added.
Report Summary Builder	Daily at 11:30 a.m.	High	No. Customers who are using legacy RiskVision reports and Jasper reports are the only ones who require this job.
Risk Analysis Calculator	Daily at 6:30 p.m.	High	No. This job is only required by customers who are using the Enterprise Risk Manager application.
Scan Summary Update	Daily at 1:00 p.m.	Medium	No. This job is only required by customers who are using Threat and Vulnerability Manager application.
System Monitoring	Every 5 minutes	Low	Yes. This job is used to monitor the health of the RiskVision server.
System User Maintenance	Every 30 minutes	Low	Yes.
Search Index	Every 4 Hours	High	Yes. This job runs at regular intervals to make sure that the search index is updated. If the search index is being rebuilt from the Admin user interface, then this job will be idle and will not try rebuilding the search all over again. Search indexes are only rebuilt when they are out of sync.

System Job	Recommended Schedule	Demand On System Resources	Required
Update Objects	Every 10 minutes	Medium	Yes.
Update Questionnaire	Every 4 hours	High	Yes.
Upload Repository Cleaner	Every 30 minutes	Low	Not required, but recommended to clean up temporary files.
Vulnerability Summary Update	Every 60 minutes	High	No. This job is only required for customers using Threat and Vulnerability Manager.
Weekly Backup of Attachments	Weekly, Sunday at 6:30 a.m.	Medium	No. This is not required for customers who are performing their own backups of attachments.
Workflow Reminder	Daily at 3:30 p.m.	Low	No. This is only required for customers who are using the reminder feature of workflows.
Assessment Objects Carry Forward	Daily Once	Low	Yes. This is used for Assessments Snapshot process. It is a light weight job assuming there will be very few assessments queued up for snapshot process per execution.
Update Questionnaires for Always On Assessments	Daily Once	Low	This is a post-update step run after assessments snapshot process. Correct data will be visible in My Questionnaires page after this job execution which also releases lock on Assessments for edits.
Vulnerability Risk Score Calculator	Daily Once	Low	Yes. This is used to process enhanced risk score for vulnerabilities.
Vulnerability Risk Score Initiator	Daily Once	High	Yes. This job processes enhanced risk score for all the vulnerabilities and entities and so resource intensive.
Vulnerability Affected Entities Incremental Updates Job	Once	Low	Yes. This is used for vulnerability entities grouping.
CrowdStrike Falcon Intelligence Connector	Daily Once	Medium	Yes. This job is required to get the threat object information.
FireEye ISight Connector	Daily Once	Medium	Yes. This job is required to get the threat object information.
Threat Summary Update	Hourly	Low	Yes. This job allows to update the related tickets, entitys at risk and targeted vulnerabiltiy count.
Trending Data Collection for Ad Hoc Views	Daily Once	High	Yes. This job is required to enable any trend data collection.
Trending Data Collection for Tickets	Daily Once	High	Yes. This job is required to enable any trend data collection for ticket.
Trending Data Collection for CM Dashboard	Daily Once	High	Yes. This job is required to enable any trend data collection for " Average Compliance Score, Open Assessments, Open Mitigations, Open Findings/Open Tickets/Open Exceptions, and Program Compliance Score Trend".

About Scheduled Jobs

Jobs include running a report, creating a new policy and control framework, or other task that may take a significant amount of time to complete.

Run a report manually or schedule a report to run at a specific time or interval to create a report job. The **Queued Jobs** page displays information about pending jobs.