



## Ways to Use SkyView Audit Journal Reporter

**SkyView Audit Journal Reporter** is an i5/OS & IBM i product that provides pre-defined audit reports on the security events recorded in the i5/OS audit journal. As your security and compliance experts, we've examined the audit journal entries, determined what information is needed, and formatted the reports so you don't have to have knowledge of the intricacies of the i5/OS audit journal.

You just have to decide which reports to run and what profiles or objects to run them against.

The following are some of the **Ways to Use SkyView Audit Journal Reporter**:

- **Monitor for invalid sign on attempts.** The Audit Journal Reporter (AJR) invalid sign on report lists invalid sign on attempts for all profiles or a list of profiles of your choosing. For example, you may want the report to list only invalid sign on attempts for QSECOFR.
- **Move to security level 40 (or 50) from level 30.** The only way to know whether it's safe to move a system from security level 30 to 40 (or 50) is to audit for potential issues. An AJR report is specifically designed to look for audit entries that identify issues that will occur at security level 40 so you can address them prior to moving to a higher security level.
- **Determine who or what process has caused something within Policy Minder to become non-compliant.** Policy Minder identifies a new user added to an authorization list or a new private authority granted to a file or a user profile with a new special authority. The next step is to discover who made the change. Details in the AJR reports allow you to understand when the change was made and by whom.
- **Compare the programs created or re-compiled into a production library with change management tickets.** Adherence to change management processes is a requirement for most auditors – both internal and external. The AJR report listing new objects created into production libraries will list both new and re-compiled programs, allowing you to compare these to approved change management requests or help desk tickets.
- **Determine who or what process deleted an object.** An object (a file or program) disappears from the system. Regardless of whether the deletion was accidental or deliberate, it's vital to discover how the object was deleted. The AJR deleted objects report provides the details you need so you can take the appropriate steps to ensure the object isn't deleted again.
- **List all of the actions taken by a particular user.** Auditors may require you to document all of the actions taken by powerful users. This complex report is made easy by running the AJR report listing all actions taken by specific users.
- **Discover if someone has tried to access critical files (such as files containing private or confidential data) without authority.** You can setup an AJR authority failure report so you can know whether someone is trying to access files containing private data (such as HR data, SSNs or credit card numbers.) If they don't have sufficient authority, an authority failure entry is generated – the AJR report contains the object (file) name, profile attempting to access the object and time the attempt was made.



- **Audit the use of an object by users outside ‘normal’ processes.** In addition to finding users that attempt to use a particular file or other object without sufficient authority, you may want to review the users who actually use or change those files. AJR has reports that list the profiles that have either read or changed specific files and allows you to eliminate ‘known’ activity. This leaves you with a report of users who have accessed the files outside of normal processes.
- **Report on who changes system values.** You’ve all seen it – a system value is changed and you’re left wondering who changed the value. Even worse is not knowing what the previous value was so you can change it back. The AJR system values reports list the system value changed, who and when it was changed as well as the current and previous values.
- **Monitor the use of particular commands.** Perhaps you want to secure a particular command – Work with Query (WRKQRY) or Start SQL (STRSQL) for example. You need to determine who is using the command before securing it so you don’t break automated processes or prevent legitimate users from running the command. The AJR report listing the users of specific commands makes this very easy.
- **Find out more details when a user receives a “Not authorized to object xxx...” message.** On occasion, users receive a “Not authorized...” message and the reason is not obvious. The AJR authority failure report lists the program running when the failure occurred, the profile not authorized (which may not be the user receiving the message) and the object to which the profile is not authorized.
- **Discover if someone is trying to sign on with IBM profiles QSECOFR, QPGMR, QSYSOPR, QUSER, QSRV or QSRVBAS.** In most cases, IBM profiles should not be used for sign on. In the rare case that they are (for example when QSRV is used for IBM service personnel), it should be a known event. All other sign ons or sign on attempts may be points for investigation.
- **Find out when the QSECOFR password is changed.** Changing the QSECOFR password is usually a well-defined process. The AJR report listing these password changes should be part of this well-defined and known process. This AJR report will notify you of changes outside of the normal process.
- **Monitor the auditing values for critical or sensitive objects.** Many regulations, including PCI and SOX, require that audit settings for cardholder files and programs as well as financial files and programs have ALL accesses logged in order to effectively recreate the activity audit trail if necessary. The AJR audit attribute reports lists changes to the audit attributes of these critical programs and files.
- **Detect when critical job descriptions and subsystem descriptions have been changed.** Changes to a subsystem’s routing entries need to be monitored to ensure the change does not provide a method of compromising your system’s security. For systems at security level 30, reviewing changes to the user profile attribute of a job description is critical since the user making the change is not required to have authority to the new profile named. The AJR reports for these scenarios provide the details you need to effectively review these changes.