

## What's New in SkyView Risk Assessor, Version 2.1

We're excited to tell you about the enhancements included in Risk Assessor Version 2.1. The new and enhanced reports will provide you with a more comprehensive analysis of your i5/OS security configuration than ever before.

### New Reports

- **Private authorities to User profiles** – This new supplemental report, SKYPVTUSRS, lists users that have been granted a private authority of \*USE or greater to other user profiles. The report also lists the profile's owner. Users with \*USE to another profile have the potential of masquerading as that profile, specifying the profile when jobs are submitted, using a job description that specifies the profile, etc. It is also helpful to know what user owns the profiles as exposures may exist there as well. (Owning a profile provides the owner with the authority to use the profile as their own; therefore, end users, programmers, etc should not own profiles.)
- **Object authorities by library** – The new SKYOBJAUT supplemental report lists – by library – the number of files, programs (including service programs) and commands that have been set to \*PUBLIC authority of \*ALL, \*CHANGE, \*USE, \*EXCLUDE, \*AUTL or User defined. This overview of application objects' \*PUBLIC authority setting will provide better analysis of the true condition of your applications' security scheme, enabling you to determine if you need to modify your object level security scheme or find an automated process for ensuring your security scheme is properly implemented.
- **Users authorized to authorization lists** - This new supplemental report, SKYAUTL, lists the authorization lists' owner and the users authorized to each authorization list. This will help you review who has authority to the list and serve as a reminder to remove those users who no longer need access. This report replaces the simple list of authorization lists that used to be in the Object Authority section of the SKYASSESS document.

### Enhanced Reports

Numerous reports have been enhanced to provide a more comprehensive analysis of your system as well as more completely describe the scope of the risks discovered.

- More items are listed in the "**Your Security Plan**" section of the SKYASSESS document. Items such as when a Guest profile for the NetServer has been defined will be listed.
- The default password report, **SKYDFTPWD**, is now sorted by the profiles' Status. Profiles with a Status of \*ENABLED will be listed first, then profiles with Status of \*DISABLED. Also, the profiles' last used date has been added and is displayed along with the profiles' last sign on date so that you can understand whether or not the profile is in use.
- The **Profiles with \*PUBLIC authority \*USE or greater** in the User section of the SKYASSESS report has been enhanced to list the profiles' special authorities. This allows you to determine the risk of having the profile be useable by all users on the system.
- The **Powerful User and Powerful Groups** sections in the User section of the SKYASSESS report has been clarified when describing the number of users on the system with each special authority. Providing the number of users with each special authority in a less confusing manner allows you to more accurately determine the risk associated with the assignment of special authorities.
- Several additional pieces of information have been added to the library authority, **SKYLIBAUT**, report. This supplemental report now lists the value of the default object auditing setting (QCRTOBJAUD) in addition to the default public authority setting (QCRTAUT). Columns have also been added to include the authorization list name (if the library is secured by an authorization list) and the library's create object auditing value (in addition to the library's create authority setting.) This expanded report along

with the new report SKYAUTL will provide a more accurate picture of how libraries are secured. For example, if a library is \*PUBLIC \*EXCLUDE but is secured with an authorization list to which all users are authorized, the library is really not secure. The addition of the library auditing information will provide insight into how object auditing is configured on the system.

**Notes:**

- Upgrading to Risk Assessor Version 2.1 is included as part of your maintenance and *does not* require a new authority code. If you are upgrading to 2.1 from Risk Assessor Version 1, it *does* require a new authority code.
- Risk Assessor Version 2.1 is supported on OS/400 and i5/OS Versions V5R1 and beyond.