SKYVIEW PARTNERS, LLC

World Class Security Experts

Performing an OS/400 Security Assessment

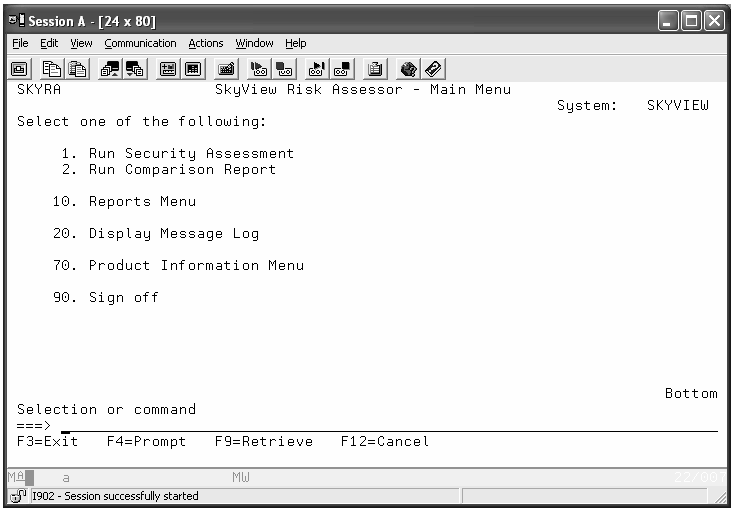
Carol Woodbury, President and Co-Founder

SkyView Partners, LLC

carol.woodbury@skyviewpartners.com

www.skyviewpartners.com

Using Risk Assessor

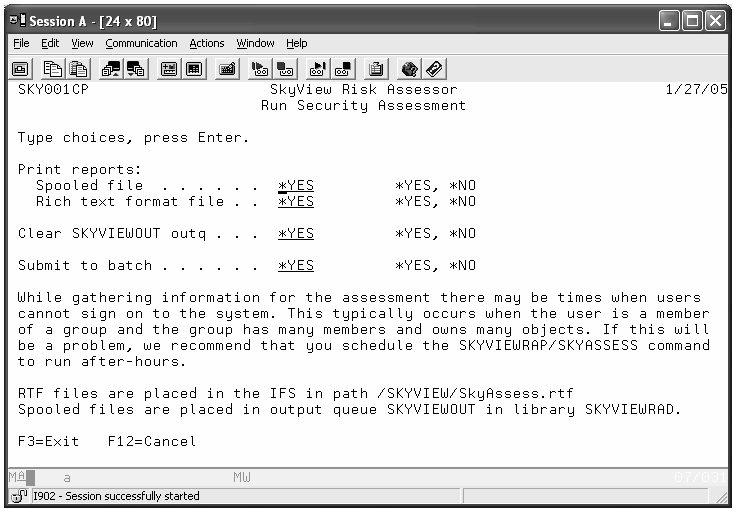


To get to this menu, sign on with a user that has *SECADM and *ALLOBJ and type **GO SKYRA**

SKYVIEW PARTNERS, LLC

www.skyviewpartners.com

Running an Assessment

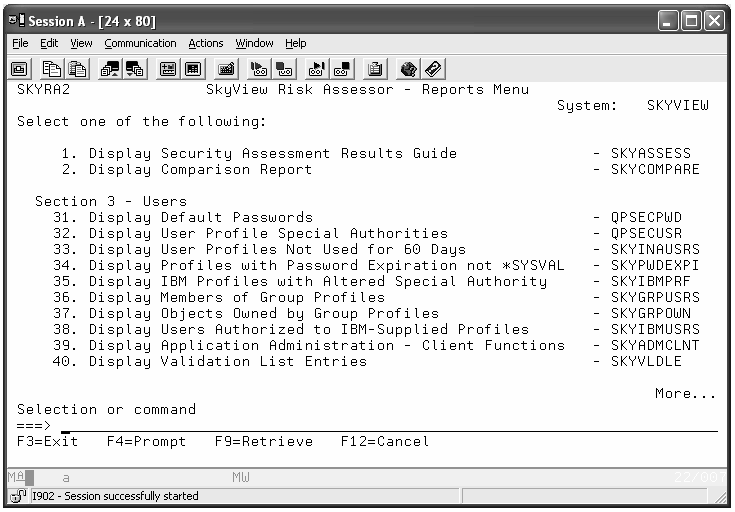


Take **Option 1** to run an Assessment

- Interactively
- In batch

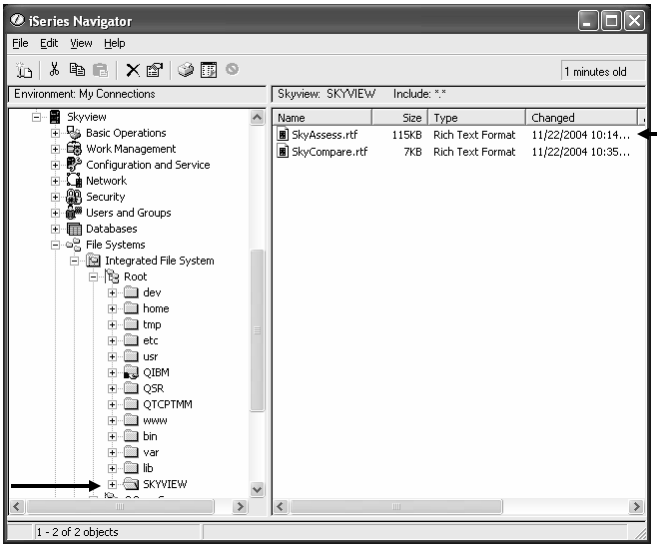
Or schedule the SKYASSESS command (in SKYVIEWRAP)

Reviewing the Reports



Option 10 from the Main Menu provides access to all reports – including the **Assessment Results Guide** and all **Supplemental reports**

Using SkyAssess.rtf



Open iSeries Navigator

Navigate to and open the SKYVIEW directory.

Drag and drop SkyAssess.rtf to your desktop.

Open with Word

Your Security Plan

Section 1: Your Security Plan

Step 1 - Examine your System Values

The security and integrity of your system cannot be guaranteed because you are not running at security level 40 or 50. This is the most important step you can take towards securing your system and ensuring both operating system and data integrity. Moving to security level 40 will ensure that no unsupported interfaces are used, data cannot be modified without detection and users cannot exploit job descriptions that name user profiles to masquerade as another user. Detailed steps you will want to take before moving to security level 40 can be found under the explanation for the QSECURITY system value.

In addition, the system is at a security level where users, by default, are allowed access to all objects on the system. Access control to sensitive files and confidential information cannot be achieved at this security level. Details about moving from security level 20 can be found under the explanation for the QSECURITY system value.

The following system values have settings that do not meet the recommended settings. Examine the recommended settings in Section 2 - System Values. Make sure to read the Considerations Before Changing section if one is included. Because of the side effects that changing some system values produce, it is possible that your business requirements will require that you leave the system value at its less secure setting.

- QSECURITY
- QALWOBJRST
- QCRTAUT
- QLMTDEVSSN

Section 2: System Values - Security

Security System Values

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QSECURITY	30	40 or 50	X
QALWOBJRST	*ALWPTF *ALWPGMADP	*ALWPTF or *NONE	X
QALWUSRDMN	*ALL	*ALL	
QAUTOCFG	0	0	
QAUTOVRT	600	0 or a fixed number	
QCRTAUT	*ALL	*USE or *EXCLUDE	X
QDSPSGNINF	1	0 or 1	
QFRCCVNRST	4	3	
QINACTITV	30	30	
QINACTMSGQ	*DSCJOB	*DSCJOB	
QDSCJOBITV	30	60	
QLMTDEVSSN	0	1	X
QLMTSECOFR	0	1	X
QMAXSIGN	4	5	
QMAXSGNACN	2	2 or 3	
QRETSVRSEC	0	0	
QRMTIPL	0	0	
QRMTSIGN	*VERIFY	*REJECT or *FRCSIGNON	X
QRMTSRVATR	0	0	
QSHRMEMCTL	1	0	X
QUSEADPAUT	QUSEADPAUT	Authorization list name	
QVFYOBJRST	3	3 or 5	

System Values - Passwords

Password System Values

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QPWDEXPITV	*NOMAX	90	X
QPWDLVL	3	Anything but 0	
QPWDRQDDIF	0	1	X
QPWDMINLEN	4	7	X
QPWDMAXLEN	25	10	
QPWDRQDDGT	0	1	X
QPWDLMTAJC	1	0	X
QPWDLMTCHR	*NONE	*NONE	
QPWDLMTREP	2	2	
QPWDPOSDIF	0	0	
QPWDVLDPGM	*NONE	*NONE	

System Values - Auditing

Auditing System Values

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QAUDCTL	*AUDLVL *OBJAUD *NOQTEMP	*AUDLVL *OBJAUD *NOQTEMP	
QAUDLVL	*SECURITY *CREATE *AUTFAIL *SERVICE *DELETE	*AUTFAIL *CREATE *DELETE *SAVRST *SECURITY *SERVICE	X
QCRTOBJAUD	*NONE	*NONE	
QAUDFRCLVL	*SYS	*SYS	
QAUDENDACN	*NOTIFY	*NOTIFY	

System values – System library list

- **Look for libraries listed indicating their *PUBLIC authority is greater than *USE and they are in the system portion of the library list.**

Section 3: Users

Use of IBM-Supplied User Profiles

Altered IBM Profiles

Altering IBM-supplied profiles can be dangerous.

Some IBM-supplied profiles have been altered to have more capability than their default setting. This can be a dangerous practice depending on how these profiles are used.

Some IBM-supplied user profiles are shipped with special authorities. The table below indicates what changes, if any, have been made to the special authorities granted to the QPGMR, QSRV, QSRVBAS, QSYSOPR and QUSER IBM-supplied user profiles.

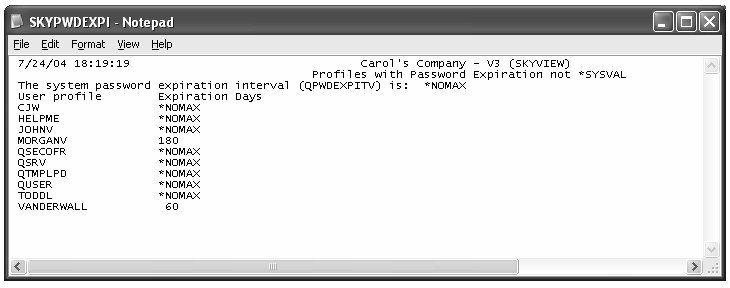
User Profile	Authority	Added or Removed
QPGMR	*ALLOBJ	Removed
QSRV	*ALLOBJ	Removed
QSRV	*SAVSYS	Removed
QSRVBAS	*ALLOBJ	Removed
QSRVBAS	*SAVSYS	Removed
QSYSOPR	*IOSYSCFG	Added
QSYSOPR	*ALLOBJ	Removed
QUSER	*ALLOBJ	Removed

Users

Password Expiration Interval

The expiration of passwords can be controlled through the user profile's password expiration interval attribute. This value defaults to use the system value QPWDEXPITV. You might want to set your powerful users' expiration interval to something less than the system value.

The SKYPWDEXPI report lists users whose password expiration interval is not set to *SYSVAL.



Option 34 from the Reports menu

Users–Reports that often yield "surprises"

- Default passwords
- Inactive users
- Users with authority to IBM profiles
- Profiles not *PUBLIC *EXCLUDE
- Commands that can be run by Limited Capability users

Section 4: Object Authorities

Section 4: Object Authorities

Most systems do not have a robust object authority scheme in place. Most objects (libraries, files, folders, etc) have the default *PUBLIC authority of *CHANGE. Unfortunately, given today's highly networked environment, *CHANGE authority and even *USE provides too much authority for most objects.

Libraries

We recommend that most libraries have *PUBLIC authority no greater than *USE. This is to prevent users from creating objects into libraries. Some libraries require *CHANGE authority because objects are supposed to be created into them. One example of this is the library QGPL. However, we do not believe there is any reason for a library to have *PUBLIC authority *ALL. *ALL authority allows anyone to actually delete the entire library - rarely a desired action.

Recommendations:

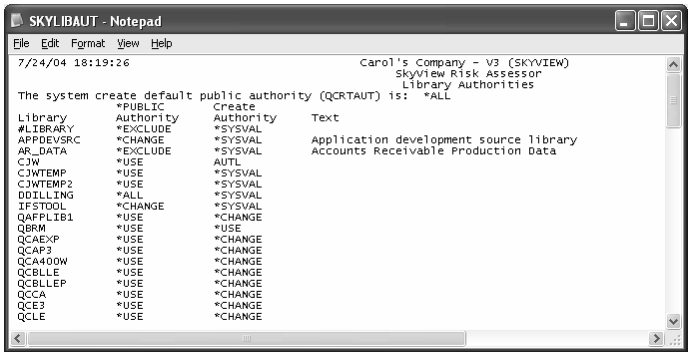
- The SKYLIBAUT report lists all libraries on the system and their *PUBLIC authority. We recommend you examine all libraries with *PUBLIC authority greater than *USE to determine if any of the libraries can have their authorities reduced.
- Analyze the public authority settings for all libraries. Be careful changing third-party application libraries. You can often reduce their *PUBLIC authority to *EXCLUDE and then you will want to authorize the appropriate users to the applications libraries. But we don't recommend changing the authority to the application objects themselves (such as files) without a thorough analysis. It can be done, but not without some planning.

Users Authorized to Create Libraries

You may want to limit which users are allowed to create libraries.

The *PUBLIC authority for the Create Library (CRTLIB) command on this system is *EXCLUDE.

Object Authorities - SKYLIBAUT



Option 41 from the Reports menu

Looks like an IBM report, but provides more

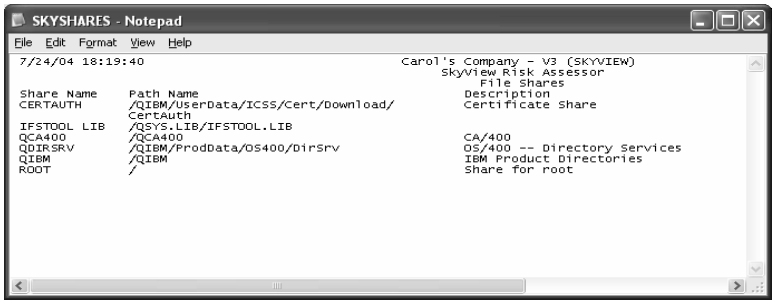
- **All libraries**
- **QCRTAUT**
- **Create authority settings**

Object Authorities – File Shares

File Shares

File shares are created through iSeries Navigator to allow directories within the IFS to be available via your network. Just because a directory has a file share associated with it does not necessarily mean that everyone with access to the network has access to the directory. After the directory (or path) is made available to the network, OS/400 or i5/OS security takes over. So if a directory has been excluded for the general public, only those users with *ALLOBJ or those that have been given explicit authority to the path can access it. Unfortunately, given the default authorities (that is, wide-open nature) of most of the file systems on OS/400 and i5/OS, most directories, once made available on the network are available to everyone.

IBM ships some default shares. To see a list of file shares defined for your system, see the SKYSHARES report.



Option 44 from the Reports menu

Section 5: Exit points

- **Intent is to raise your awareness of the potential for Trojan horses**
  - Network exit points
  - Trigger programs
  - User profile command exits
  - Command exits
  - Network attributes
  - IFS scan exits (new in V5R3)

SKY VIEW PARTNERS, LLC

Section 6: TCP/IP

Section 6: TCP/IP Security

TCP/IP provides interesting security challenges. You have some configuration options that help manage the security aspects of each server. These are discussed below. Part of TCP/IP security demands that you monitor the users having *IOSYSCFG special authority. (Configuring and managing TCP/IP requires *IOSYSCFG.) *IOSYSCFG was discussed in the User section of this assessment.

Auto-Start Values

The auto-start value determines which servers are started when the Start TCP/IP (STRTCP) command runs. The table below lists the current setting for each server. Please review this table. If you are not using the application, you should not have the server auto-start. If you don't want one of these servers automatically being started, you can change the auto-start parameter using the appropriate CHGxxxA command, where xxx is the server name. For example, CHGFTPA (Change FTP Attributes).

TCP/IP Server	Auto-Start Value
*SNMP	*YES
*ROUTED	*NO
*BOOTP	*NO
*TFTP	*NO
*DNS	*NO

SKY VIEW PARTNERS, LLC

Section 7: Adopted Authority

Section 7: Adopted Authority

Adopted authority is a way that you can temporarily give authority away. Adopted authority is an attribute of a program - the user profile attribute. When the program is defined as User Profile *OWNER that means that when a user runs that program, the authority checked by OS/400 or i5/OS will be first the authority of the user running the program and then the authority of the owner of the program. Adopted authority gives application owners great flexibility in how to authorize and secure objects owned and accessed by the application. However, this flexibility can also be abused and you need to monitor programs that adopt authority - especially the authority of powerful users.

→ The SKYADPAUT report lists the objects that adopt *ALLOBJ special authority. The intent of these objects should be understood and monitored to make sure no one is abusing the use of adopted authority.

SKYVIEW PARTNERS, LLC

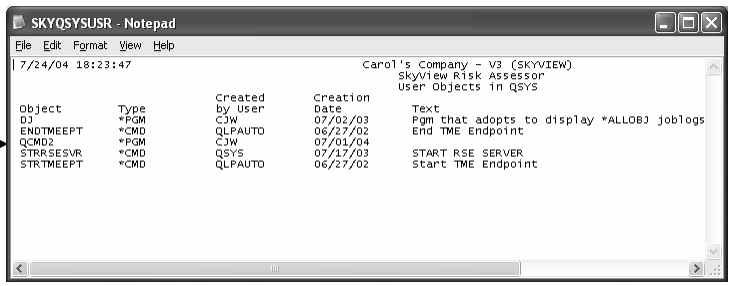
Section 8: Miscellaneous

Section 8: Miscellaneous Security Topics

User Objects in QSYS

When someone with evil intent wants to harm your system, they will sometimes try to "hide" a rogue program or other object in the QSYS library, believing that it will not come under scrutiny because some administrators assume that everything in QSYS comes from IBM. The SKYQSYSUSR report lists the user created objects in QSYS. You will want to review this report to understand these objects and ensure they are appropriate.

→



→

Option 84 from the Reports menu

Looks like an IBM report, but filters out more extraneous info

SKYVIEW PARTNERS, LLC