



Carsten's Corner: IBM SECTOOLS and the Submit Authority Reports (SBMAUTRPT) Command

[System iNetwork Systems Management Newsletter](#)

[Carsten Flensburg](#)

Carsten Flensburg

Wed, 01/19/2011 (All day)

The many security tools hiding behind the IBM CL command GO SECTOOLS provide access to a wealth of security-related CL commands that will help you establish an overview of the current security state of your system, as well as detect changes in your system security configuration if you run the commands on a regular basis. A couple of the commands included in SECTOOLS, Print Private Authority (PRTPVTAUT) and Print Publicly Authorized Objects (PRTPUBAUT), help you monitor the private and public authorities assigned to objects on your system. To help explain the function of the two commands, and the need for the SBMAUTRPT (Submit Authority Reports) command, here's an excerpt from IBM's documentation:

The PRTPVTAUT command allows you to print a report of all the private authorities for objects of a specified type in a specified library, folder or directory. The report will list all objects of the specified type and the users that are authorized to the object. This is a way to check for different sources of authority to objects. This command will print three reports for the selected objects. The first report (Full Report) will contain all of the private authorities for each of the selected objects.

The second report (Changed Report) will contain additions/changes to the private authorities to the selected objects if the PRTPVTAUT command was previously run for the specified objects in the specified library or folder. Any new objects of the selected type, new authorities to existing objects, or changes to existing authorities to the existing objects will be listed in the 'Changed Report'. The third report (Deleted Report) will contain any deletions of privately authorized users from the specified objects since the PRTPVTAUT command was previously run. Any objects that were deleted or any users that were removed as privately authorized users will be listed in the 'Deleted Report'.

*The PRTPUBAUT command allows you to print a report of the specified objects that do not have public authority of *EXCLUDE. For *PGM objects, only the programs that do not have public authority of *EXCLUDE that a user can call (the program is either user domain or the system security level (QSECURITY system value) is 30 or below) will be included in the report. This is a way to check for objects that every user on the system is authorized to access.*

*This command will print two reports. The first report (Full Report) will contain all of the specified objects that do not have public authority of *EXCLUDE. The second report (Changed Report) will contain the objects that now do not have public authority of *EXCLUDE that did have public authority of *EXCLUDE or did not exist when the PRTPUBAUT command was previously run.*

As you can see, the PRTPVTAUT and PRTPUBAUT commands are quite powerful and capable of creating a comprehensive and detailed documentation of the object authority management activities performed on your system. Run regularly, these commands will allow you to pinpoint exactly which objects have been changed and how since the reports were last run. The commands cover all object

classes, including QSYS.LIB and IFS objects. As for the former, however, there is a challenge if you want to print authority reports covering ALL object types in a library. The PRTPVTAUT and the PRTPUBAUT commands can only be run for one specific object type at a time.

So you will need to extract a list of all object types present in the specific library and then, for each object type found, run the authority report command of your choice. Such a procedure will, of course, take some time to carry out, and you risk missing an object type or two in a moment's distraction. So to ease the process and eliminate any potential errors, I wrote the Submit Authority Report (SBMAUTRPT) command.

Submit Authority Reports (SBMAUTRPT)		
Type choices, press Enter.		
Library	_____	Name
Authority report command	*PRTPVTAUT	*PRTPVTAUT,
*PRTPUBAUT		
Changed report only	*NO	*NO, *YES
Authority type	*OBJECT	*OBJECT, *FIELD,
*ALL		
Job description	*USRPRF	Name, *USRPRF
Library	_____	Name, *LIBL, *CURLIB
Output queue	*CURRENT	Name, *CURRENT,
*USRPRF, *JOB		
Library	_____	Name, *LIBL, *CURLIB

You simply specify the library you want to include on the reports and which of the authority report commands to run (*PRTPUBAUT or *PRTPVTAUT) and the rest is taken care of by the SBMAUTRPT command processing program. For each object type encountered in the specified library, the selected authority report command is submitted. The values specified for the changed report only and authority type parameters are appended to the authority report command string, and the job description and output queue parameters are assigned to the Submit Job (SBMJOB) command run for each object type. This allows you to control how the job is run and in which output queue the printed output is placed. Please refer to the SBMAUTRPT command's comprehensive online help text for more details.

The following sources are involved in creating the SBMAUTRPT command:

```
CBX804  -- RPGLE  -- Submit Authority Reports - CPP
```

```
CBX804H -- PNLGRP -- Submit Authority Reports - Help
CBX804V -- RPGLE  -- Submit Authority Reports - VCP
CBX804X -- CMD    -- Submit Authority Reports

CBX804M -- CLP     -- Submit Authority Reports - Build command
```

To create all above objects, compile and run CBX804M, following the instructions in the source header. As always, you'll also find compilation instructions in the respective source headers.

[Download a zip file with all the Source Code Here.](#)

IBM documentation:

[Print Private Authority CL command](#)

[Print Public Authority CL command](#)

[Checking for different sources of authority to objects \(PRTPVTAUT\)](#)

[Checking for objects that do not have public authority of *EXCLUDE \(PRTPUBAUT\)](#)

[Configuring the system to use security tools](#)

[Managing security](#)

[System security tools](#)

Source URL: <http://iprodeveloper.com/security/carstens-corner-ibm-sectools-and-submit-authority-reports-sbmautrpt-command>