

Securing Your Printed Output

by Carol Woodbury

One aspect of security that more of you are attempting to address is that of printed output. When reports containing private data are generated, it is important the only the users who have a business need to see the data are allowed access to the outq containing the report. However, how one secures outqs is not at all obvious; therefore, many of you resort to giving your users *SPLCTL (spool control) special authority. Unfortunately, once you given someone *SPLCTL, you cannot keep your spooled files private. *SPLCTL special authority allows the user to see every spooled file on the system. This article describes your options for avoiding granting users *SPLCTL special authority.

The Components

Who can start and stop writers as well as who can see and manage spooled files depend on a combination of several components:

- Whether or not the profile has *JOBCTL (job control) or *SPLCTL (spool control) special authorities
- The authority the profile has to the outq
- The settings of the outq's Display Data, Authority Check and Operator Control

Let's look at how each of these components contributes to the big picture of securing output.

Special Authorities

Two special authorities--*SPLCTL and *JOBCTL --are major factors in determining who can see and manage spooled files as well as who can start printer writers. *SPLCTL is the equivalent of *ALLOBJ special authority for spool files. Just as you can't prevent a user with *ALLOBJ authority from accessing any object on the system, you cannot prevent a user with *SPLCTL authority from accessing a spooled file. What about securing the outq in which the spooled files are contained, you ask? A user with *SPLCTL only needs *EXECUTE authority to the library containing the outq. No authority to the outq itself is required when the user has *SPLCTL. Besides, the user can get to the spooled files through all of the spooled file commands even if the user has been excluded from the outq. Rather than spending energy attempting to limit what a user with *SPLCTL can access, your time will be better spent determining the appropriate outq settings that will allow them to do their jobs allowing you to remove the user's *SPLCTL special authority.

When an outq is created with the default settings, *JOBCTL special authority enables the management and display of all spooled files; the management of output queues; and the starting, stopping, and holding of writers. If your outqs were created with and left at the default settings, all those user profiles that were created back when the *PGMR user class included *JOBCTL as well as all those developers who have been made members of the IBM profile QPGMR can display and control the printed output on your system. For some of you, that is likely to be a very scary realization.

Security-Relevant Output Queue Attributes

Of the attributes you can configure on an outq, three are security-relevant: Display Data (DSPDTA), Authority Check (AUTCHK), and Operator Control (OPRCTL). Each has a role in determining which users can see or manage spooled files that belong to another user.

Some points to remember:

- The settings of these attributes apply to all spooled files in a particular outq. You cannot secure an individual spooled file differently from the other spooled files in the outq.
- Regardless of the settings of the DSPDTA, AUTCHK, or OPRCTL attributes, you can always display and manage spooled files that you own.
- Spooled files are owned by the profile that created the spooled file. OS/400 does not allow you to change the ownership of a spooled file.

Display Data

Display Data's purpose is to protect the contents of spooled files. In other words, it restricts who can view a spooled file owned by another user. The settings of DSPDTA determine whether a user can run the following commands:

- Display Spooled File (DSPSPLF)
- Copy Spooled File (CPYSPLF)
- Send Spooled File (SNDNETSPLF)
- Change Spooled File Attributes (CHGSPLFA) to move the spooled file between outqs

DSPDTA has three values: *NO (the default), *YES, and *OWNER.

If DSPDTA is *NO (the default), one of the following must be true to be able to display, send, or copy a spooled file owned by someone else:

- The OPRCTL parameter is *YES, and the user has *JOBCTL special authority.
- The AUTCHK parameter is *DTAAUT, and the user has *CHANGE authority to the outq.
- The AUTCHK parameter is *OWNER, and the user trying to perform the operation owns the outq.

If DSPDTA is *YES, any user with *READ authority to the output queue can display, copy, or send a spooled file that is owned by someone else. Because the default *PUBLIC authority setting for outqs is *CHANGE, setting DSPDTA to *YES without changing the *PUBLIC authority setting to *EXCLUDE allows anyone on the system to see and manage all spooled files contained in the outq. If you want a publicly available outq, then *YES is the setting you want.

If DSPDTA is *OWNER, the following rules apply:

- Only the owner of the spooled file (or a user with *SPLCTL special authority) can display, copy, send or move the file.
- If OPRCTL is *YES and the user has *JOBCTL, the user will be able to hold, change, delete, and release the spooled files on the outq. However, the user will not be able to display, copy, send, or move the spooled files. The idea is that an operator (a user who would normally be given *JOBCTL) can manage the entries on an outq but not see the contents.

You may want to use DSPDTA *OWNER if you have an outq containing confidential information that you want your operators to manage the writers for but not allow them to see the outq's contents.

Authority Check

Authority Check's purpose is to control who can manage spooled files owned by others, who can manage the output queues containing spooled files owned by others, and who can start and stop the writers associated with the outqs. OS/400 checks the AUTCHK parameter to determine which users are allowed to run the following commands:

- Change Spooled File Attributes (CHGSPLFA)
- Delete Spooled File (DLTSPLF)
- Hold Spooled File (HLDSPLF)
- Release Spooled File (RLSSPLF)
- Change Output Queue (CHGOUTQ)
- Clear Output Queue (CLROUTQ)
- Hold Output Queue (HLDOUTQ)
- Release Output Queue (RLSOUTQ)

AUTCHK has two parameters: *OWNER (the default) and *DTAAUT.

If AUTCHK is *OWNER (the default), only the owner of the outq can change or delete (in other words, manage) the spooled files of other users contained in the outq.

If AUTCHK is *DTAAUT, the user must have *READ, *ADD, and *DLT authority (or *CHANGE authority) to the outq containing the spooled files to manage spooled files owned by others.

Operator Control

Operator Control's purpose is to control whether users with *JOBCTL are allowed to manage the outq and associated writers and work with (display and manage) spooled files owned by others.

OPRCTL has two values: *YES (the default) and *NO.

If OPRCTL is *YES (the default), users with *JOBCTL special authority can view spooled files, manage (hold, release, and delete) spooled files, manage (change, clear, and hold) the OUTQ containing other users' spooled files, and start the writers associated with the outq.

If OPRCTL is *NO, the user is not explicitly prevented from displaying or managing spooled files or managing outqs and writers, but the user's the ability to do so must come from the user meeting the criteria of one of the other attributes. In other words, the fact that a user has *JOBCTL doesn't give them extra capabilities in this case.

Scenarios

Scenario 1: The HR Department prints reports with salary information. Only the users in the HR Department should be able to see these reports and manage how and when they're printed. Create the outq with the following attributes:

```
CRTOUTQ OUTQ(HR_LIB/HR_OUTQ) DSPDTA(*YES) OPRCTL(*NO) +
```

AUTCHK(*OWNER) AUT(*EXCLUDE)

Have the HR group own the outq so they can manage the spooled files as well as start the writer to print the documents.

CHGOBJOWN OBJ(HR_LIB/HR_OUTQ) OBJTYP(*OUTQ) NEWOWN(HR_GROUP)

Scenario 2: The Accounting Department prints confidential reports, but the operators need to manage the spooled files and route them to the writer loaded with the appropriate form. Create the outq with the following attributes:

CRTOUTQ OUTQ(ACCT_LIB/ACCT_OUTQ) DSPDTA(*OWNER) OPRCTL(*YES) +
AUTCHK(*OWNER) AUT(*EXCLUDE)

Grant authority to Accounting so they can use the outq:

GRTOBJAUT OBJ(ACCT_LIB/ACCT_OUTQ) OBJTYP(*OUTQ) USER(ACCT_GRP) +
AUT(*CHANGE)

If I Do Nothing, What Is the Risk to My Output?

If you leave the outq attributes set to their default settings--DSPDTA(*NO), AUTCHK(*OWNER), and OPRCTL(*YES)--users with *JOBCTL special authority can manage (start and stop) all writers and spooled files (hold, release, etc.) Users who do not have *JOBCTL will only be able to see and manage their own spooled files. And, of course, users with *SPLCTL can see all output and manage all writers regardless of the outq settings.

*Carol Woodbury is President and co-founder of [SkyView Partners, Inc.](#), a firm specializing in [security policy and compliance management software](#) as well as security consulting and remediation services. Carol has over 16 years in the security industry, 10 of those working for IBM's Enterprise Server Group as the AS/400 Security Architect and Chief Engineering Manager of Security Technology. Carol's second book, *Experts' Guide to OS/400 and i5/OS Security*, is available at www.amazon.com.*