SECURITY PATROL

by Vincent LeVeque

Locked Out of a Used AS/400?

QUESTION: I recently purchased an AS/400 with V3R1. However, I cannot access it, because it is password-protected and I do not know the password. The broker I bought it from told me that there is a way to access it by using Dedicated Service Tools (DST) to reset the QSECOFR password, but I have not been able to figure out how to do it and he could not remember. Could you please help me?

ANSWER: First, remember that you can always sign onto the console as QSECOFR, even if the password has been forgotten. Essentially, the trick is to sign onto DST with the appropriate password and then select the menu options that will allow you to reset the master security officer's password to its original default. The default DST password in this case is QSECOFR. If you do not have the password for the QSECOFR account and the DST password is still at the default (good assumption but a very bad security practice), your chances of getting back QSECOFR access are reasonably good.

I will explain the procedure in some detail for you. Assume you have access to the system console and can set the AS/400's console key position to manual. If you're on a box that doesn't have an actual key, you have to set the panel to manual position by cycling through the console buttons until you reach manual position. (You may need to refer to your system's user guide to determine which set of numbers indicates manual position.) Now input 21 into the console's LED panel on the CPU and press Enter; the DST sign-on screen will appear. The default DST password is QSECOFR; use this user profile and password to sign on. Select the Change DST Password menu and choose option 4 from this menu to reset the default security officer account QSECOFR to its default password, QSECOFR. If successful, you will get a confirmation message. This process is described in passages 4.27 and 4.28 of the *OS/400 Security—Reference V4R4* publication for Version 4. (This process does not require an IPL, but there is an alternative process, which is also described in *OS/400 Security—Reference V4R4*, that can be performed during a manual IPL.)

Now that you have reset the QSECOFR password for your used AS/400, you should take some security precautions to ensure that unauthorized individuals do not reset it. I would recommend doing the following:

- Locate the key in a secure place.
- Change the security officer password to something nontrivial and not easily guessed.
- Change the default DST passwords to something nontrivial. There are actually three separate DST accounts with the following default passwords:
- The *basic-capability DST* default password (option 1 in the Change DST Password menu) is 11111111.
- The *full-capability DST* default password (option 2 in the Change DST Password menu) is 22222222.
- The *security-capability DST* default password (option 3 in the Change DST Password menu) is the one you used to change the QSECOFR password and, as stated above, is QSECOFR.

Be sure to store these in a secure location for those occasions when they will be needed. In addition, be sure to physically secure your computer and its console. Access to the console and CPU keylock can be a very dangerous thing. Only trained and authorized staff should do so and only for specifically authorized tasks.

Resetting the QSECOFR password by using DST generates an appropriate audit journal event. The journal entry type of this event is CP with "command name" DST. Checking for these events will warn you of possible unauthorized QSECOFR password resets.

And what if you are unlucky enough to have bought a used system where the DST password has been changed and the QSECOFR password is unknown? Let's just hope you never find yourself in that situation, but if you do, your only option is to reinstall the operating system. Hopefully, the party that sold you the used system provided the media for this process. If not, you need to contact IBM regarding your options.

The OfficeVision User Who Wouldn't Die

QUESTION:

My company migrated to V4R4 and eliminated OfficeVision as part of the process. The problem is that I can't delete old OfficeVision users; I get an error when I use the Delete User Profile (DLTUSRPRF) command. I've checked to make sure these users no longer own any objects. I've also tried using the Remove Directory Entry (RMVDIRE) command, assuming that removing the users from the system directory first would do the trick. Unfortunately, I get an error message with this command as well. Short of reinstalling OfficeVision, what can I do?

ANSWER: Each user installed on OfficeVision has the following components:

- User profile (which is preexisting or created by the OfficeVision enrollment process)
- System distribution directory entry (which allows users to send information to one another)
- OfficeVision enrollment record

To add a user, you must have *SECADM authority or be an OfficeVision administrator.

The system distribution directory entry is essential to OfficeVision; each OfficeVision user has one identified by a two-part user ID and address. This address is entered by the OfficeVision administrator and is a site-defined network address. A user may have more than one address. If a user does have more than one, you can use one of the preexisting directory entries or create a new one.

The system distribution directory is really a directory service and originally supported SNADS addresses. With V3R1, it supported X.400 and cc:mail (for details on mail protocols, see "E-message in a Bottle," *MC*, November 1999); with V4R1, it supported Simple Mail Transfer Protocol/Multipurpose Internet Mail Extension (SMTP/MIME); and, with V4R3, it added Lightweight Directory

Access Protocol (LDAP) support. Also note that, since V3R1, SNADS has interfaced with Mail Server Framework (MSF) to permit connectivity with other mail systems as part of AnyMail. OfficeVision uses SNADS as its underlying distribution service.

Security for document objects in OfficeVision has its own set of commands, and you need to use these specific commands instead of regular OS/400 object authority commands to determine OfficeVision security. The Display DLO Authority (DSPDLOAUT) command shows authority for document objects. The Edit DLO Authority (EDTDLOAUT) command edits access authority. Other commands include Add DLO Authority (ADDDLOAUT), Change DLO Authority (CHGDLOAUT), Remove DLO Authority (RMVDLOAUT), Change DLO Owner (CHGDLOOWN), and Change DLO Primary Group (CHGDLOPGP).

The "normal" process for removing a user from OfficeVision requires the following steps. However, these steps assume you still have OfficeVision installed, which you don't. For your situation, you need to understand where various OfficeVision objects are stored, find them, and delete them from your system one at a time. I'm providing this procedure for the benefit of those who wish to remove the OfficeVision users before they remove the OfficeVision software. I get to your situation shortly, so just bear with me.

First, execute the Remove Office Enrollment (RMVOFCENR) command. Option OWNOBJOPT(*DELETE) will automatically delete all user-owned OfficeVision objects as part of removing the user. Without this option, you will have to first delete the objects, then delete the user. If you do not want to delete all DLO objects owned by the user, use the CHGDLOOWN command. This command changes ownership of the objects from the deleted user to a specified new user. Use CHGDLOOWN if you want to save the prior user's document objects by assigning them to another user.

Second, use the RMVDIRE command to remove the user's specified entry in the system distribution directory. The user may have more than one entry in the system distribution directory. To remove all these entries, try RMVDIRE USRID(*user address*) USRD(*ALL).

DLTUSRPRF is the last step in the process. Only after all associated document objects and directory entries are removed can you delete the profile. To remove a user from the system distribution directory, make sure you have first checked for the following:

- The user is no longer enrolled in OfficeVision/400.
- The user is no longer a Client Access/400 user.
- All objects in the Document Interchange Architecture (DIA) library that are owned by the user have been deleted; use the Delete DLO (DLTDLO) command to remove these.
- Mail sent to but not yet received by the user has been removed.

We now know how to remove OfficeVision users with OfficeVision still installed. Getting back to your original question, how do you do this when you no longer have OfficeVision available and cannot execute these commands. It's possible but requires understanding where OfficeVision objects are stored and which ones define users to OfficeVision.

Many OfficeVision configuration objects are stored in QUSRSYS. These objects are maintained across releases and restored when you load your old system's information onto your new system. Even though the software that created and maintained these objects is no longer around, the objects still exist in ghostly fashion. Absent reinstalling OfficeVision, your best tactic is to exorcise these ghostly remnants by deleting them directly. In the case of user profiles, the relevant QUSRSYS objects are those matching the characters QAOFENR*. Delete them and see whether you can now delete these old profiles. If you'd like a thorough cleanup of old OfficeVision objects, delete everything in QUSRSYS, starting with QAOF*.

It's never a good idea to blindly delete IBM-provided objects. Although a general delete of the QUSRSYS objects described above will clear out OfficeVision users, you may want to know specifically which objects you are deleting and what purpose they serve. In general, Office database files are located in library QUSRSYS. In this library, the database files for personal directories are QAOFDDH, QAOFODTY, QAOFDH, QAOFDHH, and QAOFDTH. Other Office files in QUSRSYS include the following:

- QAOFENRA—Office enrollment file for users
- QAOFODTY/QAOFOMLH—mail files
- QAOSDIACxx—journal receivers

The following are libraries besides QUSRSYS that contain objects relevant to OfficeVision:

- QOFC—library containing OfficeVision programs and other objects
- QBBCSRCH—library containing text search objects
- QDCT—IBM-supplied dictionaries
- QDOC—local system folders and documents (Since V3R1, this library has been replaced with the /QDLS file system under the AS/400 Integrated File System.)

One final note: Before you start deleting objects, make sure you have a complete system backup handy just in case!

Vincent LeVeque is a senior security engineer for **Science Applications International Corporation (SAIC),** a large yet strangely little-known technology services firm. With more than 30,000 employees, it is one of the biggest employee-owned firms in the United States. Vincent has worked with IBM midrange systems since 1983, when he started programming on the S/38. He can be reached via email at *vleveque@earthlink.net.*

REFERENCES AND RELATED MATERIALS

- "E-message in a Bottle," D. Ellis Green, *MC*, November 1999
- *OS/400 Security—Reference V4R4* (SC41-5302-03, CD-ROM QB3ALC03)