

Locking Down Axys Files

Diane Herrera
CSSI

If you've used Axys for any length of time, you've undoubtedly run across the following situations:

1. someone inadvertently changed a price in a price file
2. someone changed a security in sec.inf
3. someone changed netwide.inf
4. someone changed a type characteristic in type.inf
5. and so on...

...and the culprit is always that mysterious character "Wasn't Me." In this article, we'll go over some of the ways you can lock down your most critical Axys files to prevent unauthorized changes.

The first step is to divide your list of users into groups according to job function:

- **Reports Only** – this group of people only need to run reports. They view the data they do not change or update anything on the system.
- **Reconcilers** – this group posts transactions to cli files
- **Dataport-ers** – this group performs dataport functions. Dataport translate/post, security updates, price file updates, split file updates.
- **Performance Update-ers** – this group maintains performance files, updates index data.

The Reports Only group is the easiest one to handle. For this group of users, simply change the Axys icon on their desktops to point to rep32.exe instead of axys32.exe. Now whenever any member of this group clicks on the Axys icon, they see the Axys Reports window. In addition, I would suggest editing the toolbar for these users to remove the "Return to Axys" icon.

One final suggestion for this group of users... Using rmtree32.exe, remove the following three items from the Perf menu

- Update Performance History (persave.rep)
- Consolidate Performance History Transactions (perlink.rep)
- Erase Performance Data (perdel.rep)

The "Reports Only" folks do not need access to these three functions. You can add them to the custom report menu for the crew that do need to update/erase performance data. (Yes, you can have different custom report menus for different users...that's a subject for yet another article.)

For the remaining users, each of which needs update access to various files and folders, work with your LAN administrator to create user groups. Place userids into the user groups according to job function. Once you have userids assigned to user groups, then your LAN administrator can restrict access using standard network security functionality. You may need to experiment to find the exact configuration that works best in your office, but here's a place to start:

1. \prf, \pbf, and \dex folders – Only the Performance Update-ers need update access. Everyone else read-only
2. \dataport and \dxdata folders – Dataport-ers need update access. Everyone else read-only.
3. \inf and \pri folders – Dataport-ers (and possibly Performance Update-ers if you want to allow it) need update access. Everyone else read-only.
4. \cli and \grp folders – Reconcilers and Dataporters need update access (and possibly Performance Update-ers if you allow it). Everyone else read only.

In addition to establishing user groups and folder permissions, I would recommend setting the read-only attribute on the following two files

- netwide.inf

- type.inf

This will not prevent a user (who has access) from deliberately removing the read-only attribute and modifying it, but it will prevent casual users from accidentally changing things.

If you implement these security measures and find that you still have the mysterious “Wasn’t Me” user changing data, then there are ways to find out who last modified a file. The Windows Operating system has “File Auditing” capabilities that allow you to see which user(s) access and/or modify certain files. The File Auditing has to be setup by your LAN administrator (and, as a warning, it can degrade your server performance if excessive auditing is done). There are also third-party tools and utilities that assist with the file-auditing task. See FileAudit on www.softwreshelf.com for one such utility.

About the author: Diane Herrera is president of CSSI, a software and consulting firm located in King of Prussia, PA. CSSI specializes in getting data into and out of the Axys system, and in developing custom applications that communicate with Axys. CSSI also develops custom Axys reports and teaches classes in Replang, Advent’s Report Writing Language. E-mail: dherrera@cssi.org. Phone: 610-992-9287.