ASTRADYNE
www.astradyne-uk.com

Technical Document

Document No:	**10-01003**
Document Title:	**OS/400 Security Toolkit**
Category:	**Hints, Tips & FAQ**
Functional Area:	**Security**
OS/400 Release:	

Document Description:

The Security Toolkit for OS/400 is a set of tools to audit and manage security and users. The Security Toolkit provides two menus:

The SECTOOLS (Security Tools) menu is used to run Security Toolkit commands interactively.

The SECBATCH (Submit or Schedule Security Reports to Batch) menu is used to run the Security Toolkit report commands in batch. The SECBATCH menu has two parts. The first part of the menu uses the Submit Job (`SBMJOB`) command to submit reports for immediate processing in batch. The second part of the menu uses the Add Job Schedule Entry (`ADDJOBSCDE`) command. You use it to schedule security reports to be run regularly at a specified day and time.

Notes:

- You must have the QSECLIB library in your library list. If the primary language on your system is not one of the Security Toolkit languages, you must also have the appropriate QSYS29xx libraries in your library list.
- Review information APAR II09315 for answers to commonly asked questions, known problems, and associated PTFs. To order the cover letter, you can use the `SNDPTFORD` command.

SECTOOLS

The SECTOOLS menu options and commands that relate to users profiles are described briefly below. To access this menu, at the OS/400 command line type the following on any command line:

```
GO SECTOOLS
```

Check profiles for default passwords: Use the Check Default Passwords (`CHKDFTPWD`) command to report on and take action on user profiles that have a password equal to the user profile name.

Display active profile list: Use the Display Active Profile List (`DSPACTPRFL`) command to display or print the list of user profiles that are exempt from `PRCINACTPRF` or `ANZPRFACT` processing.

Change active profile list: Use the Change Active Profile List (CHGACTPRFL) command to add and remove user profiles from the exemption list for the PRCINACPRF and ANZPRFACT commands. A user profile that is on the active profile list is permanently active (until you remove the profile from the list). The PRCINACPRF and ANZPRFACT commands do not disable a profile that is on the active profile list, no matter how long the profile has been inactive.

Process inactive profiles: Use the Process Inactive Profiles (PRCINACPRF at V3R1 or V3R6) or Analyse Profile Activity (ANZPRFACT at V3R2, V3R7 and later) command to disable user profiles that have not been used for a specified number of days. Specify the number of days of inactivity before user profiles are disabled. The job is run daily at 1:00 A.M. You can use the CHGACTPRFL command to exempt user profiles from being disabled.

Display activation schedule: Use the Display Activation Schedule (DSPACTSCD) command to display or print information about the schedule for enabling and disabling specific user profiles. You create the schedule with the SCDPRFACT command.

Schedule profile activation: Use the Schedule Profile Activation (SCDPRFACT) command to make a user profile available for sign on only at certain times of the day or week. For each user profile that you schedule, the system creates job schedule entries for the enable and disable times.

Display expiration schedule: Use the Display Expiration Schedule (DSPEXPSCD) command to display or print the list of user profiles that are scheduled to be disabled or removed from the system in the future. You use the SCDPRFEXP command to set up user profiles to expire.

Schedule profile expirations: Use the Schedule Profile Expiration (SCDPRFEXP) command to schedule a user profile for removal. You can remove it temporarily (by disabling it) or you can delete it from the system. This command uses a job schedule entry that runs every day at 00:01 (1 minute after midnight).

Change security auditing: Use the Change Security Auditing (CHGSECAUD) command to set up security and to change the system values that control security auditing.

Display security auditing: Use Display Security Auditing (DSPSECAUD) command to display information about the security audit journal and the system values the control security auditing.

SECBATCH

The SECBATCH menu options and associated commands for security reports are described briefly below. To access this menu, at the OS/400 command line type:

```
GO SECBATCH
```

The menu options on your system may differ slightly because some menu options are not available on every version of OS/400.

Adopted object information: Use the Print Adopted Object Information (PRTADPINF) command to print a list of objects that adopt the authority of the specified user profile.

Audit record report: Use the Print Audit Record Report (PRTAUDRPT) command to display or print information about entries in the security audit journal.

Authorization list authorities: When you use the Print Private Authorities (**PRTPVTAUT**) command for *AUTL objects, you receive a list of all the authorization lists on the system. The report includes the users who are authorized to each list and what authority the user have to the list.

Command authority: This option uses the Print Publicly Authorized Objects (**PRTPUBAUT**) command for object type (*CMD) to submit a batch job that will print a list of commands in a library that do not have public authority of *EXCLUDE.

Communications information: Use the Print Communications Information (**PRTCMNINF**) command to print the security related settings for objects that affect communications on your system.

Document authority: This option uses the Print Publicly Authorized Objects (**PRTPUBAUT**) command for object type (*DOC) to submit a batch job that will print a list of documents in a folder that do not have public authority of *EXCLUDE.

File authority: This option uses the Print Publicly Authorized Objects (**PRTPUBAUT**) command for object type (*FILE) to submit a batch job that will print a list of files in a library that do not have public authority of *EXCLUDE.

Folder authority: This option uses the Print Publicly Authorized Objects (**PRTPUBAUT**) command for object type (*FLR) to submit a batch job that will print a list of folders on the system that do not have public authority of *EXCLUDE.

Job description authority: Use the Print Job Description Authority (**PRTJOBDAUT**) command to print a list of job descriptions that specify a user profile and have public authority that is not *EXCLUDE.

Library authority: This option uses the Print Publicly Authorized Objects (**PRTPUBAUT**) command for object type (*LIB) to submit a batch job that will print a list of libraries on the system that do not have public authority of *EXCLUDE.

Object authority: Use the Print Publicly Authorized Objects (**PRTPUBAUT**) command to print a list of objects whose public authority is not *EXCLUDE.

Private authority: Use the Print Private Authorities (**PRTPVTAUT**) command to print a list of the private authorities to objects of the specified type in the specified library or folder.

Print queue: Use the Print Queue Report (**PRTQAUT**) command to print the security settings for output queues and job queues on your system.

Subsystem descriptions: Use the Print Subsystem Description (**PRTSBSDAUT**) command to print the security related communications for the subsystem descriptions on your system.

System security attributes: Use the Print System Security Attributes (**PRTSYSSECA**) command to print a list of security related system values and network attributes to a spooled file.

Trigger programs: Use the Print Trigger Programs (**PRTTRGPGM**) command to print a list of trigger programs that are associated with database files on your system.

User objects: Use the Print User Objects (`PRTUSROBJ`) command to print a list of the user objects (objects not supplied by IBM) that are in a library.

User profile information: Use the Print User Profile Information (`PRTUSRINF`) command to analyze user profiles that meet specified criteria.

Check object integrity: Use the Check Object Integrity (`CHKOBJITG`) command to determine whether operable objects (such as programs) have been changed without using a compiler.