ASTRADYNE
www.astradyne-uk.com

Technical Document

Document No:	**10-01002**
Document Title:	**Security Levels**
Category:	**Hints, Tips & FAQ**
Functional Area:	**Security**
OS/400 Release:	

Document Description:

The system provides the following levels of security:

10 No system-enforced security

Note: IBM dropped support for this security level from V4R3 of the operating system. IBM will not accept APARs for problems that cannot be re-created at security level 20 or higher. Also, the QSECURITY system value can no longer be set to 10.

20 Sign-on security

30 Sign-on and resource security

40 Sign-on and resource security; integrity protection

50 Sign-on and resource security; enhanced integrity protection

Security Level 10

At security level 10, you have minimal security protection. When a new user signs on, the system creates a user profile with the profile name equal to the user ID specified on the sign-on display. If the same user signs on later with a different user ID, a new user profile is created.

The system performs authority checking at all levels of security. Because all user profiles created at security level 10 are given *ALLOBJ special authority, users pass every authority check and have access to all resources. To test the effect of moving to a higher security level, remove *ALLOBJ special authority from user profiles and grant those profiles the authority to use specific resources. However, this does not provide security protection. Anyone can sign on with a new user ID, and a new profile is created with *ALLOBJ special authority. This cannot be prevented this at security level 10.

Security Level 20

In addition to the functions provided at security level 10, security level 20 provides the following additional security functions:

- Both user ID and password are required to sign on.
- Only a security officer or someone with *SECADM special authority can create user profiles.
- The limit capabilities value specified in the user profile is enforced.

Security Level 30

In addition to the functions provided at security level 20, security level 30 provides the following additional security functions:

- Users must be specifically given authority to use resources on the system.
- Only user profiles created with the *SECOFR security class are given *ALLOBJ special authority automatically.

Security Level 40

Security level 40 prevents potential integrity or security risks from programs that could circumvent security in special cases. Security functions at level 40 include:

- Preventing the use of unsupported interfaces
- Preventing the use of restricted instructions
- Protecting job descriptions
- Preventing signing on without password
- Enhanced hardware storage protection
- Protecting a program's associated space
- Protecting a job's address space

Security Level 50

Security level 50 provides enhanced integrity protection for installations with strict security requirements. Security level 50 is designed to meet the requirements defined by the U.S. Department of Defence for C2 security. It provides enhanced integrity protection in addition to what is provided by security level 40. Running your system at security level 50 is required for C2 security.

See the **Security Reference** manual for a more detailed description of the security levels.