

General Logon Authorization

This chapter covers the following topics:

- User ID Considerations
 - Program Authorization
 - Password Considerations
-

User ID Considerations

In order to establish communication with Com-plete, a user must supply a valid user ID and password.

Initially, two user IDs are defined:

- SAGADMIN, the ID for the system administrator;
- SYSCOM, a model user ID for other users.

Using the administrator ID SAGADMIN, you can define further user IDs for other users. If a user ID has been defined to Com-plete, the profile defined for that user ID is used whenever a user logs on with that user ID.

If a user logs on with a user ID unknown to Com-plete, the user is assigned the profile specified by the MODEL parameter in the TPFXTAB subtable (see the section **The ACSTAB Table** in this chapter). This is typically the provided default SYSTPF, but you can define other model profiles as required.

Program Authorization

Any programs to be executed under Com-plete must be added to the menu list maintained on the system data set, and must also be specified in the user's profile (see the UUTIL functions UM, ML and UP). Users cannot invoke programs that are not listed in the profile assigned to their user ID, except USTACK.

USTACK can be invoked as a direct call, as specified by the TPFPGM parameter {TPFPGM=(DCALL,USTACK)}. Under normal circumstances, you are advised for the sake of convenience, to provide a fairly comprehensive default user profile (SYSTPF). This is recommended because the TPFXTAB subtable ultimately determines which programs can actually be started by the user.

Password Considerations

Without External Security

The following considerations apply if the target Com-plete system is not running under the control of an external security system (SECSYS sysparm is not specified).

1. If the user ID entered by the user is defined in the Com-plete system, the supplied password is validated by Com-plete during the logon process, and if correct, the user is logged on. The user is assigned a profile according to the specifications in the system data set.

Note:

If a user is defined to the target Com-plete system but the logon specifies a model user ID, then the profile will be taken from the model user ID and not from the definition of the user ID logging on. See the MODEL parameter in ACSTAB.

2. If the user ID entered by the user is not defined in the Com-plete system and a MODEL user ID exists, the supplied password is not validated by Com-plete. The user is logged on and assigned a profile according to the MODEL definition.
3. If the user ID entered by the user is not defined in the Com-plete system and no MODEL user ID exists, the logon request is rejected.

With External Security

The following considerations apply if the target Com-plete system is running under the control of an external security system (SECSYS sysparm is specified).

1. If the user ID entered by the user is defined in the Com-plete system, the supplied password is validated by the external security system during the logon process, and if correct, the user is logged on. The user is assigned a profile according to the specifications in the system data set.

Note:

If a user is defined to the target Com-plete system but the logon specifies a model user ID, then the profile will be taken from the model user ID and not from the definition of the user ID logging on. See the MODEL parameter in ACSTAB.

2. If the user ID entered by the user is not defined in the Com-plete system and a MODEL user ID exists, the supplied password is validated by the external security system. If the password is correct, the user is logged on and assigned a profile according to the MODEL definition. The security profile (ACEE) defined by the external security system is taken.
3. If the user ID entered by the user is not defined in the Com-plete system and not defined to the external security system, the user is logged on only if a MODEL user ID exists. The user is assigned a profile according to the MODEL definition, but no ACEE is provided. This means that any request for items protected by the external security system will be rejected (but see the note below).

Note:

If the MODEL user ID is defined to the external security system, the security profile (ACEE) defined in the security system for the MODEL user ID is used.