

Introduction

This chapter covers the following topics:

- PAC Security Considerations
 - File Adjust Function (PACADJST)
 - Access the PAC Administrator Functions
-

PAC Security Considerations

PAC provides both online and batch security.

- Online Security
- Batch Security

Online Security

The following rules apply to PAC online security:

- The startup transaction is MENU; no profile is needed if you are using Natural Security, otherwise a profile must be defined. "Steplib" must be set to SYSTEM.
- Users who submit Predict events must be linked to SYSDICBE.
- Users who may authorize migration events are assigned when the migration path is defined by PAC. These users may or may not be a PAC administrator.

With Natural Security

- PAC user profiles can only be maintained using PAC administrator functions.
- Under Natural Security, the protection of library SYSPAC determines the user's (or group's) ability to access PAC.
- Under Natural Security, the protection of library SYSPACA determines the user's (or group's) ability to perform PAC administrator functions.
- If running Natural Version 2.3 with Natural Security, you may define library SYSPACUS as a steplib of library SYSPAC (in addition to SYSTEM). For details, see the PAC/PAA Installation documentation.

Without Natural Security

- Define steblibs
If Natural Security is not installed, the standard steplib setting and any additional site-specific steplib setting must be applied as well, using the Natural LOGON user exit.
- Modify LOGON
A sample of LOGON source is provided in library SYSPACUS.
- Move LOGON000 into the FNAT system library.

Batch Security

To accommodate environments that do not allow the same user ID to be used simultaneously for both online and batch, the PAC administrator must specify a batch user ID for each online user.

Depending on the installation standards, each user can be allocated a unique batch ID, or several users may use a single batch ID.

If a user's batch user ID is different from the online user ID, then the batch user ID also must be defined to PAC and must have the same PAC access authority as the online user ID. The batch user ID should then be included in the user's online user profile.

AUTO=ON Option

The batch jobs that carry out migration requests may use the Natural Security parameter AUTO=ON so that passwords need not be passed explicitly to Natural Security. When AUTO=ON is set, the job name on the first card of the JCL must be a valid user ID defined to Natural Security.

Alternatively, AUTO=OFF may be used if the migration jobs are modified.

Notes:

1. For Predict migrations, an additional window is displayed requesting this information at job submission time.
2. If AUTO=OFF is used for a Predict migration, then appropriate user ID and password information must be specified. This is required for Predict events because multiple logons are generated for Predict events that cannot be specified in the JCL.
3. AUTO=ON functions the same way for Predict migrations as it does for other migrations.

File Adjust Function (PACADJST)

The PAC file adjust function allows the PAC administrator to reset/adjust an internal record on the PAC system files (ACF system file and PCF system file) after PAC is installed and initialized. This ensures the integrity of the PAC system.

After renumbering the ACF and/or PCF system files using the Adabas ADADBS utility or Adabas Basic Services, and modifying the NTFILE definitions in your Natural nuclei to reflect the new physical file numbers of the changed ACF and/or PCF system files, use the following procedure:

1. Log on to the library SYSPAC using the updated Natural nucleus.

Note:

The LFILE dynamic parameter may be used temporarily.

2. At the NEXT prompt, enter the command PACADJST to invoke the File Adjust Function.

When a new ACF or PCF system file is specified, PAC verifies each file individually. If the values are not correct, an appropriate message is displayed and processing is terminated. If the values are correct, the results are displayed in a report shown in the following example:

```

The PAC Control Status has been adjusted

Application Control File  has been adjusted
Predict Control File     has been adjusted

Adjustment of Metadata follows .....

Selecting Archive Status ARCHIVE
Adjusting Application-Status Link for Application ... ADJ-APPL

```

```

Selecting Control Status CONTROL
Adjusting Application-Status Link for Application ... ADJ-APPL
Adjusting Application-Status Link for Application ... COMMON
Adjusting Application-Status Link for Application ... ORD-EXAM
Adjusting Application-Status Link for Application ... PREDICT
Adjusting Application-Status Link for Application ... ADJUST
Adjusting Application-Status Link for Application ... ADJ-APPL
Adjusting Application-Status Link for Application ... ORD-EXAM ***
    *** Processing has now successfully completed ***

```

The report displays the results of the PAC verification as follows:

- If all renumbered files are consistent with the installation files, the appropriate message is displayed for each PAC file, for example: "... File has been adjusted".
- Adjustment of metadata: When the file renumbering is completed, PAC automatically updates application status links with the new file numbers of the ACF and PCF system files.
- When the adjust function is completed, the message "Processing has now successfully completed" is displayed.

Access the PAC Administrator Functions

Access the PAC administrator functions from the NEXT prompt on the Natural system library screen by entering

- SYSPAC; then ADMIN; or
- SYSPACA; then MENU.

Note:

For Natural Security reasons, the menU program in SYSPACA logs you on to SYSPAC, checks whether you are allowed to use SYSPACA, and then executes ADMIN.

The Administrator Functions menu is displayed providing the following functions to the authorized PAC administrator:

```

16:54:55          ***** PREDICT APPLICATION CONTROL *****          2000-04-20
User SAGU          - Administrator Functions -

                Code  Function
                ----  -
                E    Archive Event Maintenance
                G    General Defaults
                L    Locked Data Maintenance
                N    Foreign Maintenance
                O    Object Version Maintenance
                T    Request Table Maintenance
                U    User Profile Maintenance
                V    View Security Maintenance
                ?    Help
                .    Exit
                ----  -

                Code ... _

Command ==>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  Menu  Exit                                     Canc

```

Code	Function	Description
E	Archive Event Maintenance	Display, finalize, modify and purge archiving events.
G	General Defaults	<ul style="list-style-type: none"> - Modify application defaults. - Maintain defaults for extended description skeletons of: application, migration events, JCL text for a job and maintenance requests. - Maintain sets of Predict generation defaults. - Maintain the default setting of applymods. - Maintain the migration paths' default. - Maintain the values of control, system and user profile defaults. - Set user exit defaults.
L	Locked Data Maintenance	Display, release and select data that has been locked.
N	Foreign Maintenance	Display the table for defining the foreign objects that are supported by your PAC installation.
O	Object Version Maintenance	Change control logs; deactivate object versions; purge object version audit history.
T	Request Table Maintenance	Maintain the status and action tables used when maintenance requests are defined to PAC.
U	User Profile Maintenance	Add, copy, modify, display, and purge the profiles of users of the PAC system.
V	View Security Maintenance	<ul style="list-style-type: none"> - Register a DDM to an application manually without, or before, using the DDM at the compilation of a Natural object. - Prohibit the use of all DDMs of a particular name at migrations to the compartment of a particular application. - Restrict the use of all DDMs of a particular name at migrations to the compartment of a particular application to "access only" - i.e. to prohibit the use of the DDM in the compiled objects for storing, updating, or deleting.