

# Protecting Predict With Other Security Systems

This section describes how to protect your Predict environment with other methods not described in the preceding sections.

This section covers the following topics:

- Protecting Predict using Adabas Security
  - Protecting Predict with User Exit U-SEC
- 

## Protecting Predict using Adabas Security

With Adabas Security, access to files can be protected with passwords. The password used to control access to the Predict system file can be specified in the Natural Security definition of the library SYSDIC.

User-specific access rights for the Predict system file can be defined by creating special links from individual users to the library SYSDIC. User-specific password and access rights are then defined in the Natural Security definition of the special link.

Defining access rights for the Predict system file with Adabas Security passwords using Natural Security requires the following:

- The desired Adabas password must be entered in the Restrictions map of the Natural Security definition for the library SYSDIC or the special link.
- The command mode must be disallowed for the library SYSDIC.

If a user-specific password is specified for the Predict system file, the password specified in the NATPARM module or as dynamic parameter is not in effect when the user is working. After leaving the library SYSDIC\* the old password is restored.

### **Warning:**

If as a result of protecting the Predict system file by value, the fields K\* are write-protected, XRef data cannot be written to Predict. CATALOGing and STOWing Natural programs with XREF set to Y is then impossible.

## Protecting Predict with User Exit U-SEC

If you set default parameter General Defaults > Protection > Protect current Predict file to Y and do not specify a database and file number of a Natural Security file, the user exit U-SEC is called.

The parameters of this user exit are described in the PDA U-SECP.

This user exit is delivered in source form and allows you to define your own security checks. If the current user does not have sufficient access, you can set the message DIC1534 ("You are not authorized...").

This user exit also provides an interface to other security products such as RACF.

This user exit also contains a description of the parameters available. See the section User Exits in the **Predict Administration documentation**.