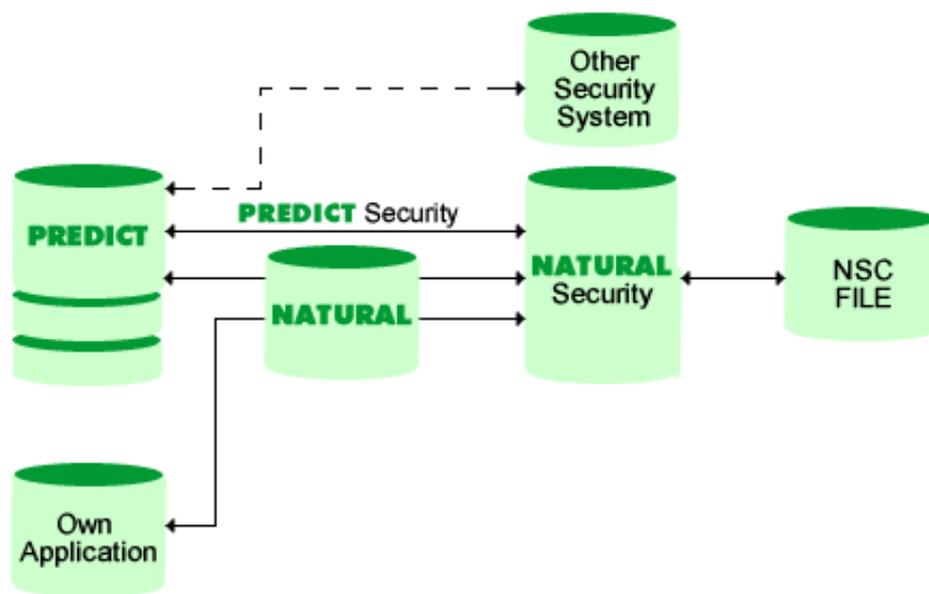


Introduction

The Predict Security System controls access to a Predict environment using security definitions stored in a Natural Security file.

An individual environment can be defined for each user or group of users and protected against unauthorized access.



This section covers the following topics:

- Terminology
- Predict Security using Natural Security
- Internal Check Routine
- Security Conflicts
- Command DISSEC

Terminology

Link ID

When a user logs on to a library, the Link ID is determined as follows:

- If the user is linked directly to the library, the link ID is the same as the user ID.
- If the user is linked to the library indirectly as member of a group, the link ID is the group ID.

See your **Natural Security documentation** for more information.

Natural Security File

This file contains the security definitions used by the Predict Security System for protecting objects against unauthorized access.

NSC External Object

In terms of Predict security, an instance of an external object type.

NSC External Object Type

In terms of Predict security, an external object type is a class of objects to be protected. The following external object types are available for protecting Predict data:

- PRD-Docu-Object
- PRD-Ext-Object
- PRD-Function
- PRD-3GL-Library

Predict Security

Predict Security means the following:

- the external object types in Natural Security, for example PRD-Docu-Object
- the security profiles defined to limit access to instances of external object types.

Security Object

A security definition in Natural Security.

Predict Security using Natural Security

Predict Security is realized with the Software AG product Natural Security. This product allows you to

- define the persons who can process the protected objects
- define the objects to be protected

Predict transfers the administrative functions listed above to Natural Security. A security object is a security definition valid for one of the following data types:

- Documentation objects
 - All object types
 - Documentation object types, either predefined or user-defined
 - Subtype of a predefined object type (for example file of type Adabas C)
 - All objects of an object type or subtype
 - Range of documentation objects (for example all files that start with USER1)
 - Fully qualified documentation object (for example file USER1-FI-ADA2)
- Special Objects
 - Retrieval Model
 - Association Type
 - Object Type
 - Implementation Plan
- External Objects
 - External object type (for example DDMs)
- Predict Functions
 - Entire group of functions, for example Special Functions
 - Individual functions, for example Special Function Reposition implementation data.
- XRef data
 - XRef data in all 3GL libraries

- XRef data in a range of 3GL libraries
- XRef data in a fully qualified 3GL library

Internal Check Routine

When a Predict function is called, an internal Predict routine generates an Natural Security call. This call checks the security definitions in Natural Security for

- the current link ID
- the function the user wants to execute
- the data the user wants to access.

Activating Natural Security via Parameter in Predict

The Security Check does not depend on whether Natural Security is installed. The Predict parameter Protect current Predict file in the General Defaults > Protection screen determines whether Predict Security is called. This parameter can be defined for each FDIC file.

Security Check when Calling Predict

The system checks whether the current user is authorized to logon to library SYSDIC.

Security Conflicts

If the user does not have the necessary access rights, the system behavior depends on the type of security conflict:

- If the user does not have access to a function, the function is not executed and an error message appears.
- If the user executes a retrieval function and does not have READ access to certain objects or object types, the system behavior depends on whether the retrieval function was implicitly or explicitly limited by attributes or restrictions:
 - Retrieval function not limited by restrictions or attributes:
Only the ID of the read-protected object with the remark >>>protected<<< is output.
 - Retrieval function limited by restrictions or attributes:
Objects are suppressed completely.
See Retrieval.
- If the user executes a function other than retrieval and has insufficient access to an object or object type, the function is not executed and an error message is given.

Example: User has MODIFY but no DELETE access to objects of type file. He cannot delete files.

For more information see the section Handling Protected Objects in Predict in this documentation.

Command DISSEC

With the command DISSEC, users can display their own individual security definitions that have been defined for them by the Security Administrator. This command can be entered in the command line from any point within Predict.

This command corresponds to the Special Function Maintain NSC Definitions > Display NSC Definitions. See Maintain NSC Definitions in the section **Special Functions** in the **Predict Administration documentation**.