

Protecting your Environment with Predict Security

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.

Predict definitions are not protected in Natural Security as default. This means that when Predict is delivered, each user has access to every object and can execute any Predict function. Predict Security only takes effect when access to objects, object types or functions is explicitly restricted for individual users or groups of users.

This section covers the following topics:

- Adding Security Definitions
- Natural Security External Object Types for Predict
- Activating Predict Security
- Where to find more Information

Adding Security Definitions

Default Definitions

Standard definitions for Natural Security must be added with the Special Function Maintain NSC Definitions > Add NSC Default Definitions. See Maintain NSC Definitions in the section **Special Functions** in the **Predict Administration documentation**.

Additional Security Definitions

If you wish, you can create your own Security definitions for any object in Natural Security - either for an individual user or for a group of users.

Natural Security External Object Types for Predict

The following Natural Security (NSC) external object types and their standard definitions are added in Natural Security with the special function Maintain NSC Definitions > Add NSC Default Definitions.

- Prd-Docu-Objects
- Prd-Ext-Objects
- Prd-3gl-XREF-Library
- Prd-Function

These are described in more detail below.

Prd-Docu-Objects

For this NSC external object type, the default definitions for main object types and object subtypes are automatically added in Natural Security with special function Maintain NSC Definitions > Add NSC Default Definitions. For example: FI and FI-A for files or files of type Adabas C. User-defined object types are also added with this function.

All instances must be added manually in Natural Security. With the special function Mass Grant you can create security definitions in Natural Security on the basis of data in Predict. Objects for which you wish to create security definitions must be placed in an extract. See Mass Grant in the section **Special Functions** in the **Predict Administration documentation**.

There are three strategies you can follow when protecting objects:

- Protect **Individual objects**
Example: The file SALARY can only be read/modified by certain Users.
- Protect a **range of objects**
Use naming conventions to group objects and take advantage of asterisk notation in Natural Security.
Example: User USER1 has been denied READ access to file objects in general, but READ access for files that begin with his User ID. The more specific authorization has priority.
- Protect **all objects** of a particular type.

Other Object Types

With NSC external object type PRD-Docu-Object you can also protect the following:

- Association types
- Object types (for UDEs, only applies to Metadata Administration)
- Retrieval models
- Implementation plans

Prd-Ext-Objects

All external object types that can be processed with Predict functions can be maintained by Predict Security. Instances of this NSC external object type are for example CO (COBOL copy code) or D2 (DB2 database). The instances are automatically added in Natural Security with special function Maintain NSC Definitions > Add NSC Default Definitions.

Security definitions for Prd-Ext-Objects are used to protect functions.

Example: A user without ADD or MODIFY access to object type CO cannot execute the function Generate COBOL Copy Code.

Prd-3gl-XREF-Library

A security check is carried out when you access XREF data in 3GL libraries from Predict (Preprocessor, List XREF for 3GL). This check accesses the security definition for the 8-character library name in Natural Security. If you wish to protect 3GL libraries, you must define security objects of this type manually in Natural Security.

Prd-Function

As a rule, security definitions in Predict are defined at object type or object level. The following areas of Predict do not process any objects in Predict and are therefore protected with objects of NSC external object type Prd-Function in Natural Security.

Resources of the NSC external object type Prd-Function are divided into the following groups:

- Special Functions
- Coordinator
- Defaults, including extended description skeletons
- LIST XREF for 3GL

For this NSC external object type, the instances are automatically added in Natural Security.

Activating Predict Security

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.

Where to find more Information

The Predict Security documentation provides you with all the information you need to set up your Security environment and gives a detailed description of how the individual Predict functions behave when working with objects that are protected with Predict Security.