

General Information

General Security Concept in Predict

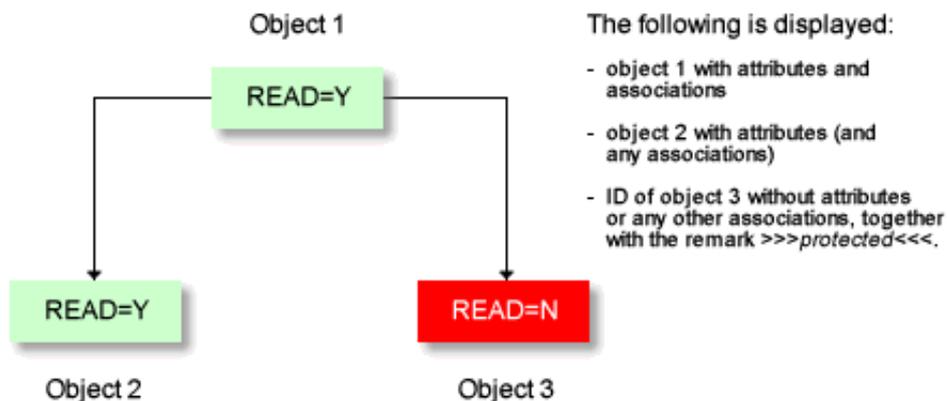
Various security systems are based on the concept of see protection. This means that generally speaking a user is only able to see the objects and their IDs to which he has been granted access. This concept is not compatible with an open system such as Predict: the whole point of Predict retrieval functions is that objects are displayed together with their related objects.

If Predict were to suppress protected objects completely, the user might draw the wrong conclusions - for example empty link lists would be displayed although links to protected objects are present.

Predict uses the following strategy:

- Attributes or associations of an object are only displayed if the user has at least READ access to that object.
- If a user does not have READ access to an object, the most he will be able to see of that object is its ID.
- If an object can be displayed, the IDs of all other objects to which the main object is linked can also be displayed. Under no circumstances, however, can attributes or associations be displayed for an object to which the current user does not have READ access.

Example

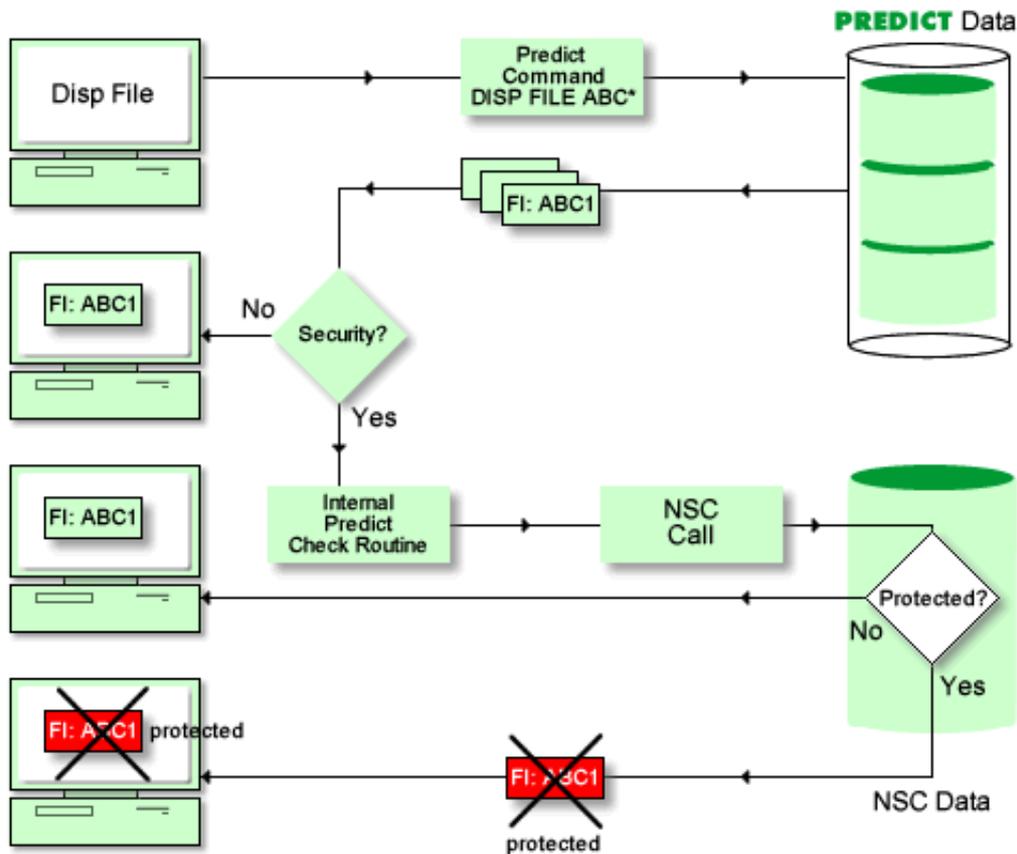


Sample Function

The diagram below illustrates what happens when function Display file is executed for all files starting with ABC*.

The command DISP FILE ABC* retrieves all files starting with ABC.

- If Predict Security is not active, no security check is performed and all the objects are displayed.
- If Predict Security is active, a security check is performed for each object in the retrieval report:
 - If the user has access to the object, the object is displayed.
 - If the user does not have access, the object is suppressed.



Response Times

Definitions in Natural Security have a large influence on response times. We therefore recommend the following:

- The security administrator should inform each user of his access rights. If the users know the scope of their access rights, they can formulate their queries more effectively and will spend less time 'groping around in the dark'. Access rights can also be displayed using the special function Display NSC definitions. See Maintain NSC Definitions in the section **Special Functions** in the **Predict Administration documentation**.
- Disallow READ access sparingly. If a user is going to link objects, it makes sense that he can read them. This is particularly important with keywords. Not having READ access also slows down response times.

Security Check in the Main Menu

The security check is called

- in the command interpreter: after entering the command
- in the main menu: when entering the object type or when selecting a type from a selection window.

This routing performs the following checks:

- **Generate:**
ADD or MODIFY access to external object types
- **Incorporate:**
READ access to external object types

- **Compare:**
READ access to external object types
- **Retrieval, Active Retrieval:**
READ access to Predict object type
- **Maintenance:**
ADD, MODIFY or DELETE access to Predict object type
- **File Implementation:**
ADD, MODIFY , READ or DELETE access to Implementation Plans (object type -I)
- **Administration:**
READ access to Predict object type
- **Defaults, Special Functions:**
EXECUTE access to the corresponding function

No checks are performed for the following:

- **What is new, Help system**