

Retrieval

If the user has no READ access at object type level, the function is not executed. A window containing the valid object types for the current user appears or an error message is given.

The system behavior when protected objects are encountered depends on the type of retrieval function. These can be divided up into three groups:

- List oriented functions
These functions provide information on the existence of objects. They do not provide information on the objects themselves. If no attributes or restrictions are specified, objects will also be retrieved for which the user has no READ access. This makes the output as complete as possible without the user learning anything about the attributes of an object.
- Display oriented functions
These functions provide information on attributes or associations of objects. If a user does not have READ access to an object, the object will be suppressed completely.
- Attribute oriented functions
These functions always provide information on attributes or associations of objects. If a user does not have READ access to an object, the object will be suppressed completely to prevent the user from gaining information about a protected object on the basis of attributes or associations.

List-Oriented Functions

These functions provide information on the existence of objects. They do not provide information on the objects themselves. If no attributes or restrictions are specified, objects will also be retrieved for which the user has no READ access. This makes the output as complete as possible without the user learning anything about the attributes of an object. Objects for which the user does not have READ access are marked with >>>protected<<<.

The following retrieval functions belong to this group:

- List/Select objects
- List/Select objects with no parent
- List/Select objects with no child
- List/Select dummy/placeholder objects. See also Additional Information.
- List/Select extract related to no object
- List/Select keyword related to no object
- List/Select owner with no user
- List/Select users related to no object
- List/Select unused storagespace

Result of List-Oriented Functions

The result of these functions depends on whether attributes or restrictions were entered as selection criteria:

Without attributes and restrictions

All objects are displayed, even those to which the user does not have READ access. Only the IDs are displayed together with the remark >>>protected<<<. See example below.

This has the following advantages:

- the lists are complete
- the user learns nothing about a protected object apart from the fact that it exists.

```

13:18:48          ***** P R E D I C T 4.2.2 *****          2002-07-31
Plan 0              - Select File -

  Cmd  File ID                Type  Fnr   DDM Impl Other
  ---  ---
  ___  CHD-CUSTOMER-CUST        I
  ___  CHD-D_FORMATE            D
  ___  CHD-DEPENDING-ON        S      53
  ___  CHD-DESCRIPTOR          >>> protected <<<
  ___  * CHD-ESQ_FILE          B                                *
  ___  CHD-EXPANDED            >>> protected <<<
  ___  CHD-FB-TEST-U1          U      75
  ___  CHD-FB-TEST-U2          U      75
  ___  CHD-FB-TEST-U3          U      75

```

In this example you can also see that field Cmd is not available for protected objects.

With attributes and restrictions

Only objects for which the user has at least READ access are displayed.

The user does not find out that objects were not shown for security reasons. The remark >>>protected<<< does not appear.

This has the following advantage:

- the user could otherwise discover that objects have a certain value for a particular attribute, which would undermine the READ protection defined by the Security administrator.

If the user does not have READ access to a range of objects - for example all files of type A that start with USER1 - the message "No objects found" is given when he specifies File ID=USER1* and File type=A.

Additional Security Checks

Each object is checked for READ access. The following additional checks are performed for the individual functions:

Select objects

An additional check is performed when an object is placed in the workplan with a command:

- the user can only select objects for which he has at least READ access
- the field Cmd is locked for objects for which the user has no READ access
- if a command is entered, the system checks that the user is allowed to execute the corresponding function.
- if an asterisk is entered, only valid commands are displayed for selection.

List/Select Dummy/Placeholder objects

- Only parent objects are checked against security.
- For the functions Link and Unlink:
the user needs MODIFY access to the parent object.
- For the function Add:
the user needs ADD access to the child object
- For the function Select:
the user needs READ access to the child object.
- For the function Purge:
no security check is performed.

List/Select owner with no user

- Only the READ access for the owner is checked. If no READ access has been defined for an owner, the output of the object in which the owner is defined is replaced by the remark >>>protected<<<.

Select owners with no user

- READ access for the owner is checked. If no READ access has been defined for an owner, the owner is marked >>>protected<<<.

Display-Oriented Functions

With display-oriented functions, the user wants to find out about attributes or associations of objects. If a user does not have READ access to an object, the object is suppressed completely.

Note:

Response times can be slow if a large number of protected objects are processed by this type of function. After a few seconds, the user is asked whether he wants to cancel the function or continue.

This group includes the following functions:

Single-level output

- Display objects
- Display objects with no parents
- Display objects with no child
- Display extracts related to no object
- Display keywords related to no objects
- Display users related to no object
- Display unused storagespaces
- Difference of files

Note:

With the functions above, extracts, keywords and users are regarded as objects in their own right. With other functions, they are regarded as attributes of another object and are evaluated accordingly. See Attribute-oriented Functions.

Multi-level output

- Display/List objects with children
- Display/List objects with parents
- Display dummy/placeholder objects
- Execute retrieval model
- List files related to a file

Result of Display-oriented Functions

As with list-oriented functions, the result of display-oriented functions depends on whether attributes or restrictions were specified as selection criteria.

Without attributes and restrictions

Single-level output

- Only objects to which the user has at least READ access are displayed. If the user does not have READ access, the object is suppressed. This means:
 - The remark >>>protected<<< does not appear.
However, a message is given indicating how many objects were not displayed due to security: >>>nn Object(s) suppressed because of security protection<<<.
 - If a retrieval operation returns only objects to which the user has no access, the message "You are not authorized to read this object" is given

Multi-level output

- On the **first** retrieval level, the same checks are performed as for single-level output. See above.
- If protected objects are found on **other** retrieval levels (for example the child objects with function programs with children) the ID of the object together with the remark >>>protected<<< is output, but no information on attributes or associations is given.

The example below shows that on the first retrieval level 46 files (together with an unknown number of dependent objects) have been suppressed due to security. In addition, the user does not have sufficient access for some related objects and these are marked >>>protected<<<.

```

13:25:54          ***** P R E D I C T 4.2.2 *****          2002-07-31
                   - List File with Children -                   Page:    2

File ID ..... CHD-FB-TEST-U1
Type ..... ADABAS userview

Cnt  child File ID          Type   Fnr   DDM Impl Other
-----
  1  ARH-BT1                >>> protected <<<
  2  ARH-OT1                >>> protected <<<

>>> 46 File(s) suppressed because of security protection <<<
***** End of Report *****

```

With attributes and restrictions

Objects to which the user has no READ access are suppressed **completely**. This means:

- The remark >>>protected<<< does not appear
- No message is given to indicate how many objects were suppressed due to security.
- The user is not informed that objects were not displayed due to security.

If the user has no READ access to a range of objects - for example all files of type A that start with USER1 - and specifies File ID=USER1* and File type=A, he receives the message "No files found".

Additional Information

Difference of files

- User must have at least READ access for both files.
- A message is given if the function cannot be executed for security reasons.

Attribute-Oriented Functions

This group contains the following functions:

- List Vista numbers
- Explode IMS databases
- List/Select verifications to regenerate
- List fields and related views
- List fields related to a Z file
- List/Select objects with no owner
- Users related to objects
- Cross reference extract
- Cross reference owner
- Cross reference keyword
- Extract related to objects
- all field retrieval functions

Note:

Objects of type field are handled as attributes of file objects. If the user does not have READ access to the file, he is not able to determine which fields are contained in the file.

Result of Attribute-Oriented Functions

These functions evaluate

- attributes of an object (for example Vista numbers), or
- links to objects that are regarded as attributes in Predict Security. These are:
 - Extract
 - Field
 - Keyword
 - Owner

To prevent the user gaining information on attributes or links, an object to which he has no READ access is suppressed totally. This means:

- IDs of protected objects do not appear in the retrieval report.
- The comment >>>protected<<< does not appear.
- No message is given at the end of the report as to how many objects were suppressed due to security
- If the user has no READ access to a range of objects - for example all files starting with USER1 - the message "No objects found" is given.

Additional Security Checks

In addition to the check for READ access to the object, the following checks are performed for the individual functions:

List Vista numbers

- If the user has no READ access to the network, this object is suppressed completely and not evaluated further.
- If the user does have READ access to the network, each individual object within the network whose Vista number falls within the specified range is checked (database, file, Vista element).
If no READ access has been granted for these objects they are suppressed completely.

Cross reference field

See function Implode fields.

Explode IMS database

- The first check is for READ access to the database object.
- If the user has READ access, each subordinate object is checked for READ access.
- Objects for which no READ permission exists are marked >>>protected<<<, no checks on subordinate objects are performed.

List/Select objects with no owner

Objects for which no READ access has been defined are not included in the output. The owner is regarded as an attribute of the object.

Users related to objects

This function evaluates the owner as attribute of the object.

All Field Retrieval Functions (except Implode fields, Cross reference fields)

- Object type field is regarded by Predict Security as attribute of object type file. Security checks are only performed on the files containing the fields.
- Fields of a file for which the user has no READ are not included in the output.

Implode fields

- A field is not evaluated if the user has no READ access for the file.
- If the user does have READ access, each object is checked for READ access
- Protected objects are marked >>>protected<<< and not evaluated further.

List/Display fields related to a Z-file

- If the user has only READ access - but no MODIFY or DELETE access - to the standard file, a security check is performed for each subsequent field/file.
- If the user has MODIFY or DELETE access to the standard file, **all** subsequent files are output. This is because this function is designed to predict the effects of a change to the standard file. Rippling depends only on the MODIFY access to the standard files. See Force Standard.

Cross Reference Keywords/Owners, Extracts related to Objects

If a user has MODIFY or DELETE access to an extract, keyword or owner, all related objects are displayed - irrespective of the READ access to these objects. This is done for the following reason:

When extracts, keywords or owners are deleted, all objects linked to these objects must be updated for reasons of consistency. The three functions above are designed to provide a **complete** list of objects affected by the deletion of an extract, keyword or owner.