Administration

Security Checks for all Administration Functions

The user needs the following access:

- READ access to the documentation object database, dataspace, file or storagespace is checked when the function is called.
- ADD/DELETE/MODIFY/READ access to the external object type is checked depending on the function. See table below.

Function	Access Mode	
	Documentation Object	**External Object**
Disconnect	READ	READ
Display	READ	READ
Purge	READ	DELETE
Purge Vista elements	READ	DELETE
Refresh file	READ	DELETE
Rename	READ	MODIFY for old name, ADD for new name
Select	READ	READ

If the user does not have the permission required for a function, an error message is given.

Select

This function implicitly evaluates attributes or associations of an object. To prevent the user finding out any information about READ-protected objects, the display is suppressed completely if the user does not have READ access to either documentation or external object. The user is not informed that objects were not displayed due to security.

Display

This function implicitly evaluates attributes or associations of an object. To prevent the user finding out any information about READ-protected objects, the display is suppressed if the user does not have READ access to either documentation or external object. A message is given before the ’End of Report’ indicating that objects were suppressed due to security, but the user does not discover how many objects were not displayed.

Purge

If other external objects are deleted with this function (for example processing rules with a DDM or Table with a DB2 database), only the main object is checked against security. Security definitions for these dependent objects are checked in the external environment, and an additional check by Predict would be superfluous.

Copyright Software AG 2003