

# CHECK-SECURITY

<b>File</b>	45
<b>Op-Sys</b>	OS/390
<b>Statement</b>	PROCESS
<b>Task</b>	Asks an external security system (RACF, ACF2, TOP-SECRET) whether user is authorized to use a given resource, for example, a dataset.

## Common Fields for all Operating Systems

Dictionary Field Name	F/L	Mu	DE	Remarks
ERROR-CODE	N3			
ERROR-TEXT	A58			
NODE	N5		D	
NODE-NAME	A16		D	
SYSTEM-MESSAGE-CODE	A10			

## Additional Fields Supported for OS/390

Dictionary Field Name	F/L	Mu	DE	Remarks
ENTITY	A200		D	
CLASS	A8		D	
ATTRIBUTE	A8		D	
INSTALLATION-PARMS	A250		D	
ALLOWED	A8			

## Field Descriptions

Field Name	Type/Length	Operating System
ALLOWED	(A8)	OS/390

Output field. Access allowed indicator. One of these values will appear in this field:

Value	Explanation
ERROR- <i>nn</i>	Error returned by security system.
NO	Access not allowed.
NOSEC	Security not installed.
YES	Access allowed.

Field Name	Type/Length	Operating System
ATTRIBUTE	(A8)	OS/390

Entity attribute. Check whether user is allowed to access the resource with one of the following attributes as defined in the security system:

Attribute	Explanation
ALTER	Permission to change external attributes of resource.
CONTROL	Permission to create resource.
READ	Permission to read resource.
UPDATE	Permission to update resource.

Field Name	Type/Length	Operating System
CLASS	(A8)	OS/390

Class of entity, for example DATASET. Default is FACILITY.

Field Name	Type/Length	Operating System
ENTITY	(A200)	OS/390

Entity to be security checked.

Field Name	Type/Length	Operating System
INSTALLATION-PARMS	(A250)	OS/390

Installation parameters to be passed to security system.