General Specifications

Model VP6E5110
Access Control Package

CENTUM VP

GS 33J10D20-01EN

[Release 6]

■ GENERAL

Model VP6E5110 Access Control Package provides CENTUM VP systems with functions to control access from operators, system engineers, users of Report Package, and recipe engineers by authenticating the individuals who attempt access, thus protecting the system and data from any break-ins or unauthorized access. These functions facilitate management of system engineers who access the system using System View or using a Builder program, Report Package users who attempt to create or modify related files, and recipe engineers who access the system using Recipe Management Function, in addition to conventional system access control by means of user names and passwords. This document describes three kinds of sophisticated management offered by Access Control Package: namely, system engineer management (user management for System View and Builders), Report Package user management, and recipe engineer management (user management for Recipe Management Function).

■ FUNCTION SPECIFICATIONS

● System Engineer Management (System View/Builder)

Access Control
Can limit the access to the project-database for each system engineer. This enables to clearly define the separate roles.

For instance, system engineer A can modify the drawing from one to ten of FCS0101. System engineer B cannot modify FCS data but can create, delete, and modify the graphic of entire HIS.

Access Controllable Unit
Access Control can be specified for each computer.

Applicable Project of Access Control
Access Control can perform on the default or the current project. It cannot perform on the user-defined project.

System Engineer Group and System Engineer
A system engineer group is a fundamental unit for specifying the authorities to perform engineering.

All system engineers must belong to one of the groups and register the engineer name (ID); password; legal name.

A system engineer can perform an engineering depending on the authority its group entitled.

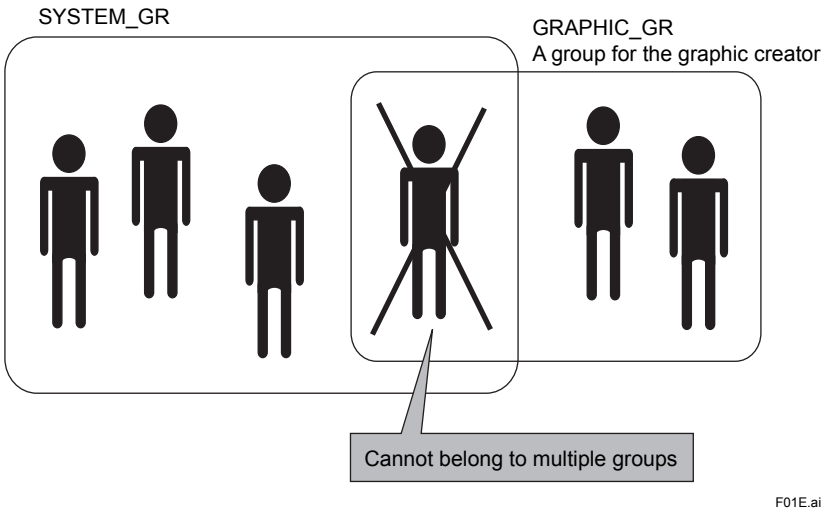

Figure An Example of System Engineers and Groups

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan
Tel: 81-422-52-5634 Fax: 81-422-52-9802

GS 33J10D20-01EN

2nd Edition Mar. 17, 2015 (YK)

The Scope of Authority
The minimum unit for entitling authorities to a system engineer group is a builder unit as the graphic or the drawing.

The Authority Types

Read: Can read files.
If only Read is entitled, cannot select 'Overwrite and Save' or 'Download' on Builder.

Write: Can write into files.
Can also 'Save' and 'Download' the existing files.

Create: Can create and delete an object on System View.
To create a station or to delete a window, need to be entitled this authority.

System Engineer Authentication and Authority Check
This verifies identity and if the system engineer has the authority to perform the job.

Table System Engineer Authentication and the Timing of Authority Check

Timing	Engineer Authentication	Authority Check
Logging into System View	X	–
Creating and Deleting a project (etc.) on System View	–	X
Starting Builder	–	X
Overwriting and Saving at Builder (*1)	–	–
Downloading at Builder (*1)	X	–
Logging off from System View	–	–

X: Will be performed. –: Not performed.

*1: When starting up Builder, System View will check the authority for Write. If the engineer does not have the authority, it is started in Read Only mode, so this person actually will not be able to select the menu.

● Report Package User Management

Access Control
Capable of controlling access from users of Report Package who attempt to create or modify a report configuration file or report print image file.

Access Controllable Unit
Each computer in which Report Package is used performs access control. Where two or more computers run Report Package, Model VP6E5110 Access Control Package or Model VP6E5170 Access Administrator Package should be needed in each of these computers, with access control also being set up in each computer.

Scope of Access Control
User access to any report configuration file or report print image file via Report Package is controlled without exception. Access control settings cannot be made differently for each report configuration or report print image file.

User Groups
Access privileges given to a user of Report Package are determined by the user group to which the user belongs. There are two user groups: the operator group and the manager group. All users of Report Package must belong to one of these groups.

Authority Types
For report configuration files:

Create: Only users entitled with Create authority can create and delete a report configuration file.

Write: Users entitled with Write authority can open, modify, and load a report configuration file.

For report print image files:

Create: Only users entitled with Create authority can delete a report print image file.

Write: Users entitled with Write authority can modify and print a report print image file, convert it to a PDF file, and save it to a computer in which audit trail data is archived, but cannot delete it.

Note: There is no "Read" authority for report files. Only users entitled with Write authority can open report files.

The authority of the manager group and operator group for report files is fixed as shown in the following table and cannot be modified.

User Group Name	Authority	Report Configuration Files	Report Print Image Files
Manager group	Create	Entitled for all files	Entitled for all files
	Write	Entitled for all files	Entitled for all files
Operator group	Create	Not entitled	Not entitled
	Write	Not entitled	Entitled for all files

Report Package User Authentication and Authority Check

When a user logs on to Report Package, user authority is checked, and the actions of that user are restricted according to the privileges given. Users belonging to the manager group have privileges to perform all actions.

Report Package performs user authentication whenever the package is started, or the printing of a file or an action which will affect an output file is attempted.

● Recipe Engineer Management (Recipe Management)

Access Control

Can limit the access to create and modify Master Recipe for each recipe engineer.

Access Controllable Unit

Access Control can be specified for each computer.

Applicable Project of Access Control

Access Control can perform on all projects. Project attribute does not affect.

Recipe Engineer Group and Recipe Engineer

A recipe engineer group is a fundamental unit for specifying the authorities to operate recipe management functions. All recipe engineers must belong to one of the groups and register the recipe engineer name; password; legal name. A recipe engineer can operate recipe management functions depending on the authority its group entitled.

The Scope of Authority

The maximum unit for entitling authorities to a recipe engineer group is a project, and the minimum unit is a recipe.

The recipe subgroup is not in the authority scope.

The Authority Types

Engineers are entitled to use the following authorities.

- Read (*1): Start Recipe Builder/Recipe Procedure Builder for viewing recipes and recipe operations. The Recipe View and the Recipe Builders start up in read-only mode.
- Write: Create and edit recipes and recipe operations. Deleting and downloading of the recipes and recipe operations are not allowed. Create, delete, and edit of a project and a recipe group are not allowed.
- Delete: Delete recipes and recipe operations. Downloading a recipe is not allowed. Create, delete, and edit a project and a recipe group are not allowed.
- Download: Download recipes from Recipe View and Recipe Builders. Create, delete, and edit a project and a recipe group are not allowed.
- Engineering (*2): Create, delete, and edit a project and a recipe group. Delete all recipe operations. Start Recipe Builder/Recipe Procedure Builder for viewing recipes. Create, edit, delete, and download a recipe are not allowed.

*1: All recipe engineers are automatically entitled Read authority and cannot set the authority scope.

*2: Engineering authority can be used in combination with recipe-related authorities such as Read, Write, Delete and Download. (i.e. A recipe engineer with Engineering and Download authorities)

Recipe Engineer Authentication and Authority Check

This verifies identity and if the recipe engineer has the authority to perform the job.

Table Recipe Engineer Authentication and the Timing of Authority Check

Timing	Recipe Engineer Authentication	Authority Check
Logging onto Recipe View	X	–
Creating and Deleting a project/ a recipe group on Recipe View Change of property Deleting all recipe operations	X	X
Creating and Deleting a recipe/ recipe operation on Recipe View	–	X
Starting Builder	–	X
Overwriting and Saving at Builder	–	X
Downloading	X	X
Logging off from Recipe View	–	–

X: Will be performed. –: Not performed.

● System Administrator and Engineer

After the package is installed, various setting must be done to use Access Control Function. An engineer who actual performs Engineering cannot set them. Only system administrators can set these requirements. System engineers, recipe engineers, and users of Report Package are referred to collectively as 'engineer' in this section.

The tasks of a system administrator and an engineer are as described as below:

System Administrator
- Network administration
- Specify and edit the engineer security file
  Register engineer name
  Sets the access right for each engineer group

Engineer
- Setting the password during the first logon
- Inputting the passwords when editing or downloading in the builders

■ OPERATING ENVIRONMENT

● Hardware requirements

Follows the requirement of VP6E5100 Standard Engineering Function.

● Software requirements

Supported Service Packs are the same as for VP6E5100 Standard Engineering Function operating environment.

Access Control Package can be used with VP6E5100 Standard Engineering Function. This package can also be used with VP6H6530 Report Package or VP6E5166 Recipe Management Package.

The package cannot be performed on the computer with only Graphic Builder is used.

■ MODELS AND SUFFIX CODES

		Description
Model	VP6E5110	Access Control Package
Suffix Codes	-V	Software license
	1	Always 1
	1	English version

■ ORDERING INFORMATION

Specify the model and suffix codes when ordering.

■ TRADEMARKS

- CENTUM is a registered trademark of Yokogawa Electric Corporation.
- Other company and product names appearing in this document are trademarks or registered trademarks of their respective holders.