

Data Exchange Security (DS9) - OEM application

BPA Delivery 6 for V5R19 (V5.6)
User Guide

Table of Contents

Table of Contents	2
Introduction.....	3
Installation Check	4
The Export Command	5
The Import Command.....	10
The CheckStatus Command.....	12

Introduction

This document describes the commands included in the BPA DS9 at OEM Site, and the way to use them.

Installation Check

After successful installation of BPA DS9 at OEM, start CATIA with the environment specified during installation.

The CATIA Security toolbar should be visible.



The following environment variables should also be defined in the DS9_OEM.txt file installed:

ToSuppliers

To set the location (directory) of the target directory during Export operation

FromSuppliers

To set the location (directory) of the origin directory during Import operation

AuthorizationFilePath

To set the location of the text file containing the list of suppliers / passwords. The text file may be empty.

The Export Command

Description:

The Export command performs the following actions:

1. Read all the CATIA V5 files from a directory specified by the user. Sub-directories are supported.
2. Encrypt them together with allowed suppliers information, read only status and expiry date if needed.
3. Copy them into the directory specified by the environment variable *ToSuppliers*. Specific sub-folders are created for each supplier and for each encryption operation.
4. Delete the processed files from the origin folder.

File types

The following files will be processed (encrypted and copied to the destination folder):

- All CATIA V5 format files, which extension starts with CAT
- 3dxml
- cgr
- xls files (Excel) cannot be encrypted but are copied “as is” to the destination folder
- All other files will be ignored by the commands (not copied to the destination folder)

Click on the “Export” icon



At first launch, the panel below appears. It is empty because no suppliers have been defined.



Defining a new supplier

Click on the “AddSupplier” button. The panel below appears:



A dialog box titled "Add a supplier" with a question mark icon and a close button. It contains two text input fields: "User ID" and "Password". Below the fields are two buttons: "OK" (with a green circular icon) and "Cancel" (with a red circular icon).

Type in a supplier name and a password (only single byte ASCII characters are allowed)

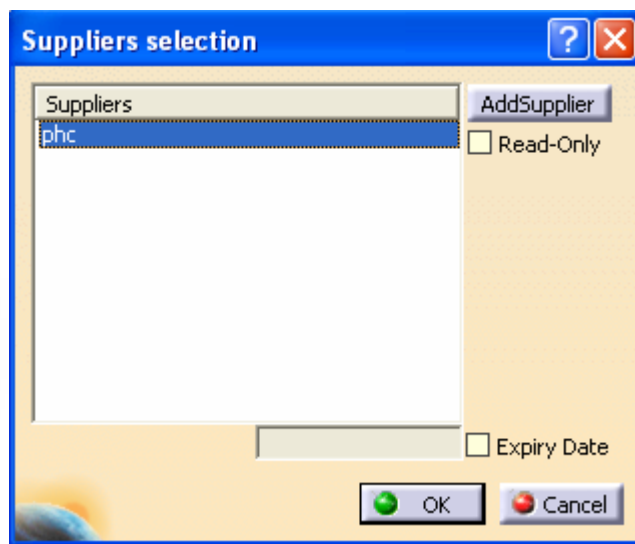
For example:



The same "Add a supplier" dialog box, but with the "User ID" field containing the text "phc" and the "Password" field containing three asterisks "***". The "OK" and "Cancel" buttons remain at the bottom.

Click on OK

The supplier “phc” is now listed and can be selected:



A dialog box titled "Suppliers selection" with a question mark icon and a close button. It features a list box labeled "Suppliers" containing the entry "phc". To the right of the list box is an "AddSupplier" button and a "Read-Only" checkbox. Below the list box is an "Expiry Date" checkbox. At the bottom are "OK" and "Cancel" buttons.

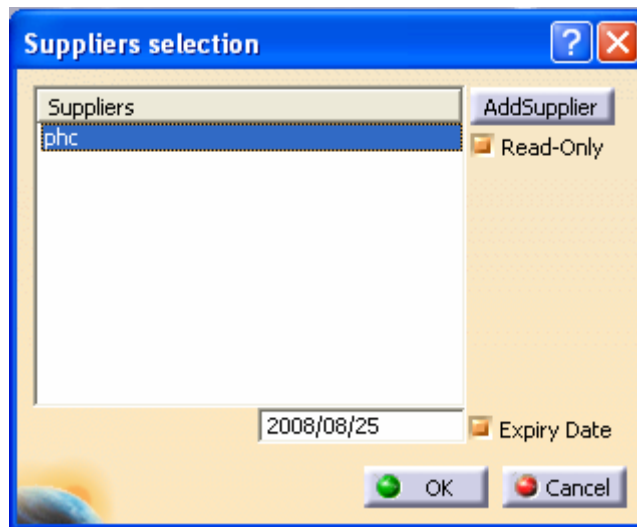
Multi-selection is possible, using CTRL-click or SHIFT-click to allow access of the files to more than one person.

Set Read-Only and Expiry Date

Two parameters can be set: read-only and expiry date.

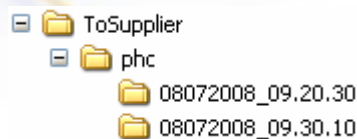
If the Read-Only box is checked, suppliers will be able to open and edit the files but not to save the modifications. A file “DS9ReadMe.txt” containing the message “The files in this folder are encrypted and protected with a Read-only attribute. You may be able to modify them inside CATIA, but Save will not be allowed” will be created in each supplier directory.

If the Expiry Date box is checked: enter the expiry date with format yyyy/mm/dd, then the files cannot be opened after this date on the supplier side. A file “DS9ReadMe.txt” containing the message “The files in this folder are encrypted and carry a validity date information. Open and use of these files will be possible only until yyyy/mm/dd” will be created in each supplier directory.

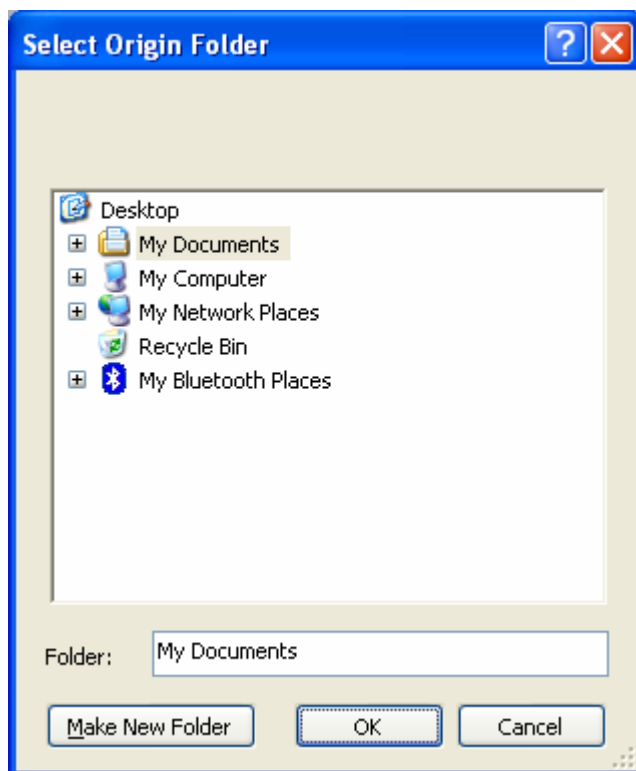


Click on OK

The folder selection panel appears. The Export command will always store the encrypted files into the directory specified by the environment variable “ToSuppliers”. Under this directory, a sub-folder is created for each supplier selected during execution of the Export command. At each execution of the Export command, a sub-folder is created under each applicable “supplier” folder. The name of this new folder is the time stamp of the Export command beginning of execution. The format is ddMMyy_hh.mm.ss.



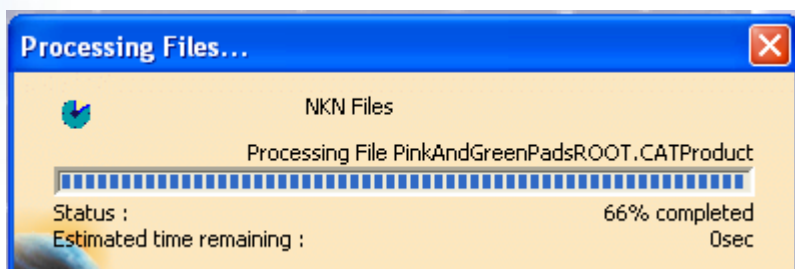
In the panel below, you select the Origin Directory, from which the non-encrypted data will be read.



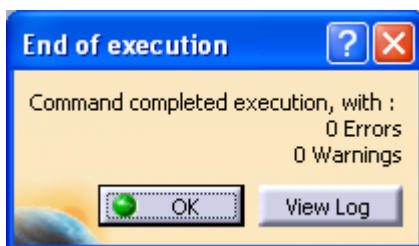
Once the folder is selected, press OK.

The encryption operation starts.

Depending on the number and size of the files, it may take some time, but you can follow the execution with the progress bar displayed on-screen.



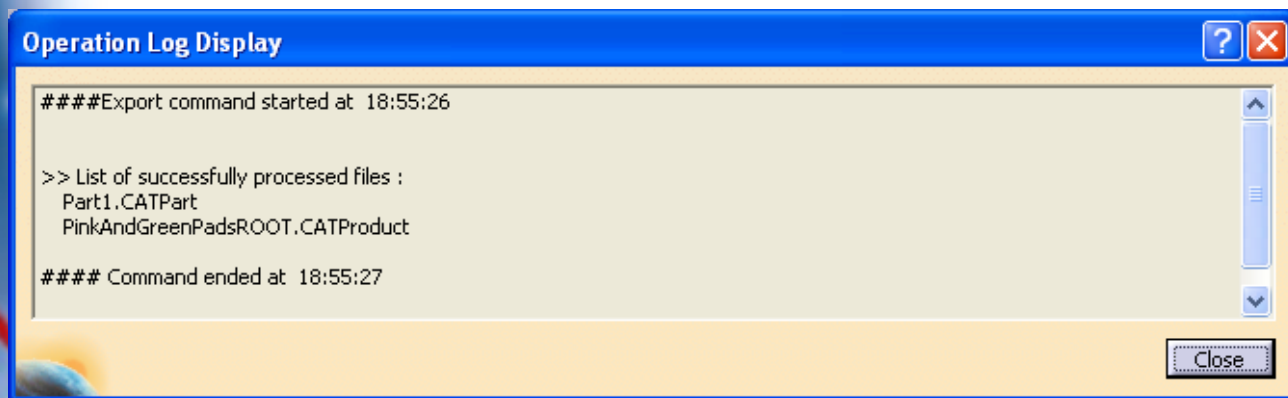
At the end of execution, a panel will show the number of errors and warnings:



Errors occur when a file could not be successfully encrypted

Warnings occur when a file could not be deleted before or after the operation, or in case non-CATIA V5 files were ignored.

For more detailed information, press "View Log":



The log also displays the list of encrypted files.

Command execution is finished: the encrypted files are available for shipping to your supplier in the directory specified by "ToSuppliers", and the original files have been deleted.

The Import Command

Description:

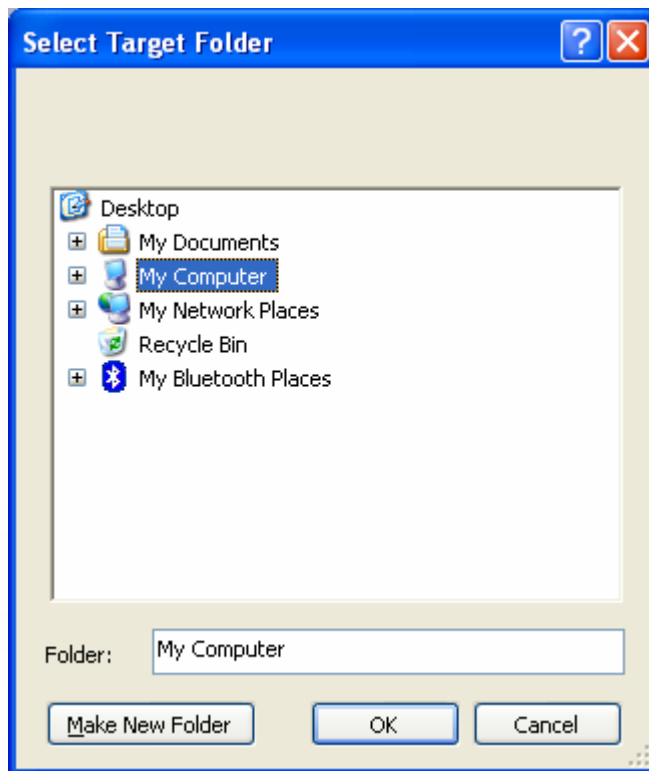
The Import command performs the following actions:

1. Read all the CATIA V5 files from the directory specified by the environment variable "FromSuppliers". Sub-directories are supported.
2. Decrypt them.
3. Copy them into the directory specified by the user.
4. Delete the processed files and the "DS9ReadMe.txt" files from the "FromSuppliers" folder.

Click on the "Import" icon 

The folder selection panel appears. The Import command will always read the encrypted files from the directory specified by the environment variable "FromSuppliers".

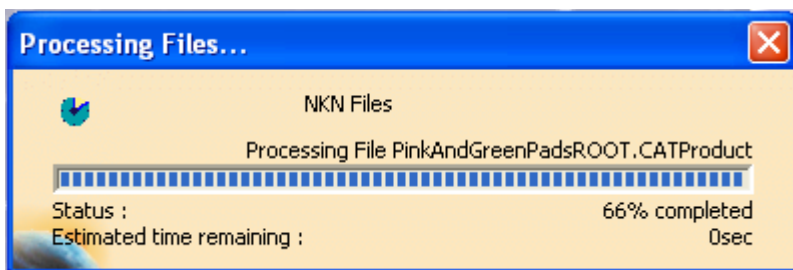
In the panel bellow, you select the Target Directory, where the decrypted data will be stored.



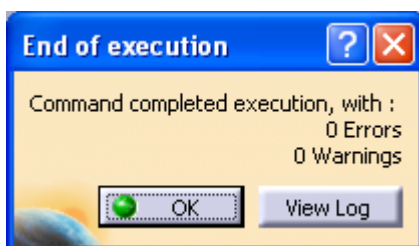
Once the folder is selected, press OK.

The decryption operation starts.

Depending on the number and size of the files, it may take some time, but you can follow the execution with the progress bar displayed on-screen.



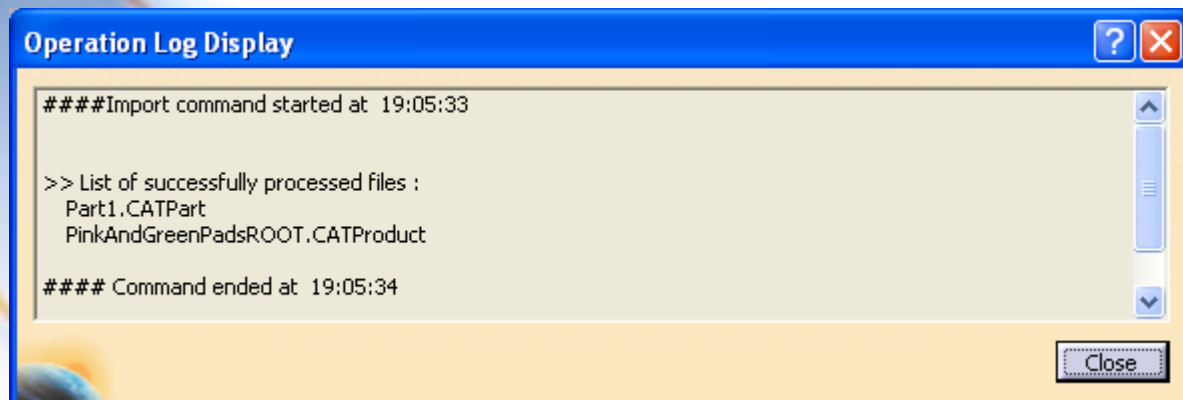
At the end of execution, a panel will show the number of errors and warnings:



Errors occur when a file could not be successfully decrypted.

Warnings occur when a file could not be deleted before or after the operation, or in case non-CATIA V5 files were ignored.

For more detailed information, press "View Log":



The log also displays the list of decrypted files.

Command execution is finished: the decrypted files are available in the directory specified by the user (they can be safely re-injected in your PDM system if needed), and the original files have been deleted.

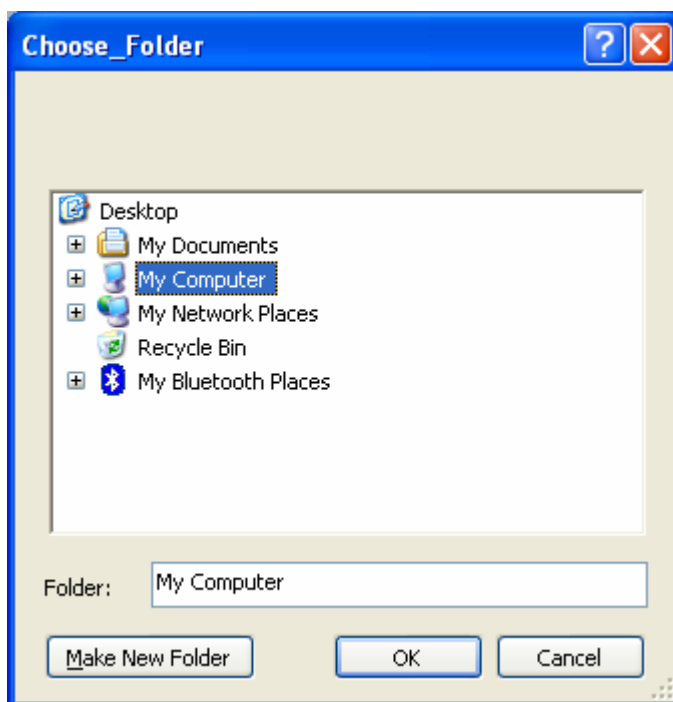
The CheckStatus Command

Description:

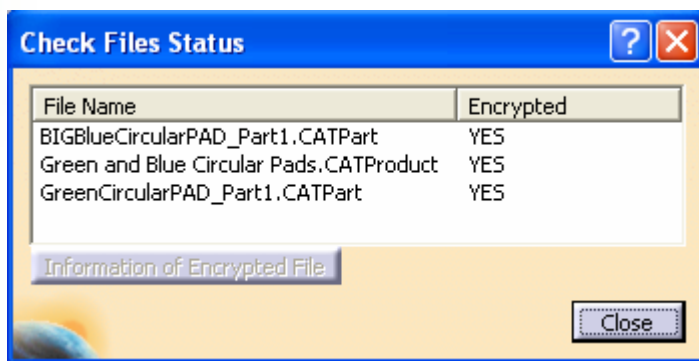
The CheckStatus command allows to view in a given directory which files are encrypted (or not) and to get information about suppliers, read-only status and expiry date of encrypted files.

Click on the “Check Status” icon 

The folder selection panel appears. Select the folder you want to investigate.

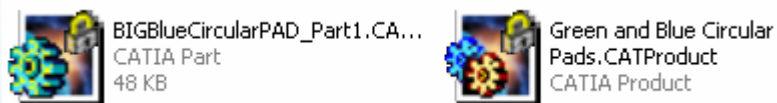


After selecting the folder, click “OK”

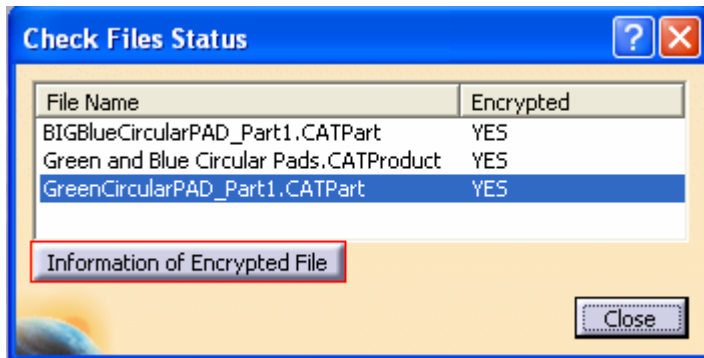


All CATIA V5 files present in the selected folder are listed in this panel, together with their encryption status (YES for an encrypted file, NO for a non-encrypted file).

The encryption status can also be checked directly in Windows Explorer. The icons of all the encrypted files have a lock to identify them.



In the Check Files Status window, select a file and click on “Information of Encrypted File”



The list of suppliers, the expiration date (if available) and the Read-Only status are displayed.

