

CATIA Data Security (DS9) - OEM application

BPA Delivery 8 for V5R20 (V5.8) ***User Guide***

Table of Contents

Table of Contents	2
Introduction	3
Installation Check	4
The Export Command	5
The Import Command	12
The CheckStatus Command	14
The OEM Batch Application	16
Help About - CATIA Data Security	18

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 files from a directory specified by the user. Sub-directories are supported.
2. Encrypt them together with allowed suppliers information. CATIA V5 files are protected by DRM and can carry DRM authorizations: “read only”, “expiry date” and “allow unprotected”.
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, except if the option “Keep Origin Files” is checked.

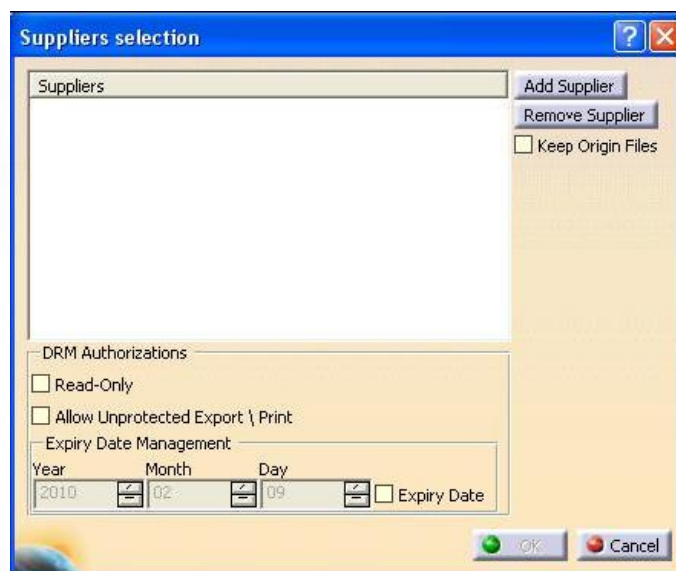
File types

All the files will be encrypted, but only the CATIA V5 formats below are protected by DRM in the CATIA session:

- CATPart
- CATProduct
- CATDrawing
- CATShape
- CATAnalysis
- CATMaterial
- CATProcess
- CATSystem
- CATSwl
- 3dxml
- cgr
- catalog

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)

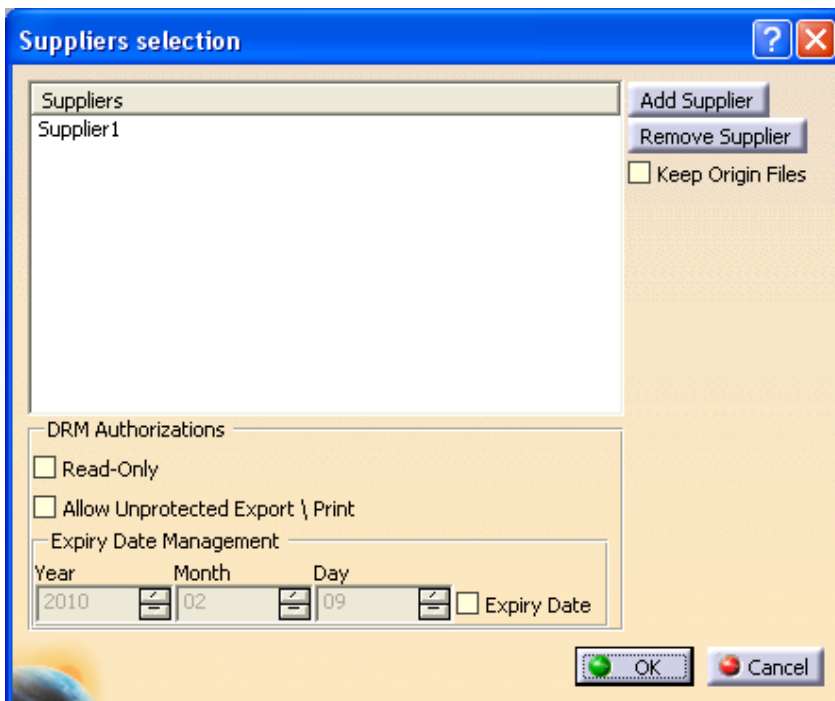
For example:



The same "Add a supplier" dialog box, but now the "User ID" field contains the text "Supplier1" and the "Password" field contains four asterisks "****". The "OK" and "Cancel" buttons remain at the bottom.

Click on OK.

The supplier “Supplier1” is now listed and can be selected:

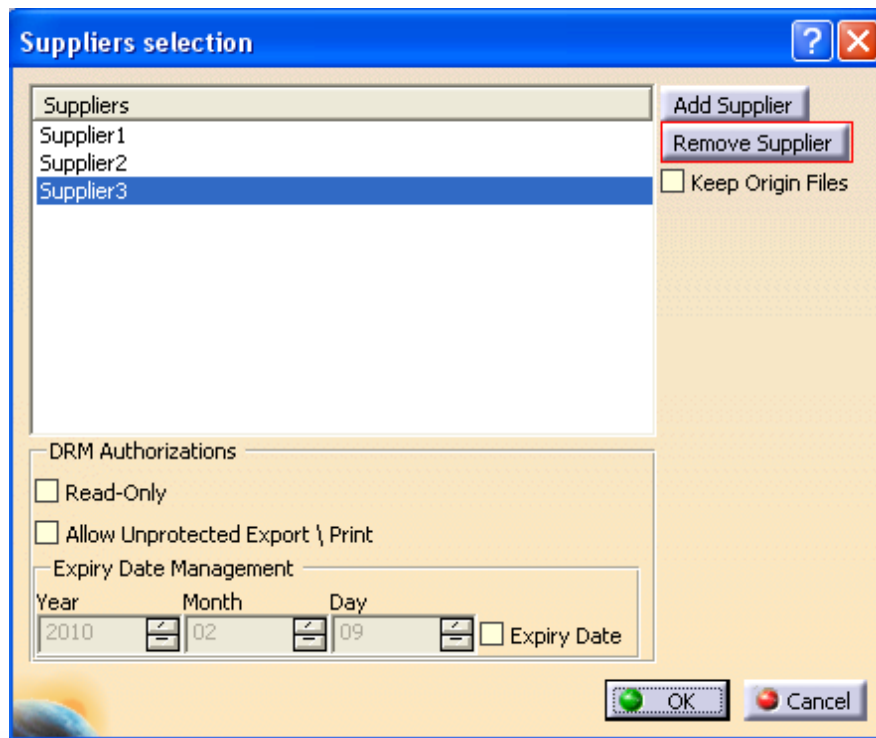


A dialog box titled "Suppliers selection" with a question mark icon and a close button. It features a list box on the left containing the name "Supplier1". To the right of the list box are three buttons: "Add Supplier", "Remove Supplier", and a checkbox labeled "Keep Origin Files". Below the list box is a section titled "DRM Authorizations" containing two unchecked checkboxes: "Read-Only" and "Allow Unprotected Export \ Print". Below that is a section titled "Expiry Date Management" containing three spin boxes for "Year", "Month", and "Day" (showing values 2010, 02, and 09 respectively), followed by an unchecked checkbox labeled "Expiry Date". At the bottom right are "OK" and "Cancel" buttons.

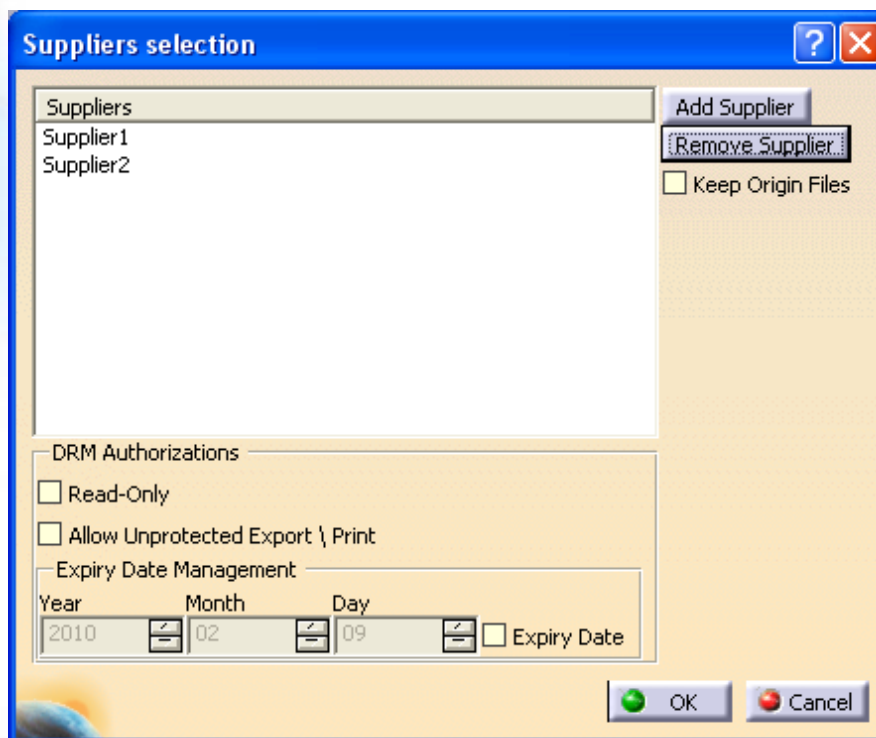
Multi-selection is possible, using CTRL-click or SHIFT-click.

Removing a supplier

Select the supplier(s) to remove and click on the “Remove Supplier” button.



The supplier(s) are removed from the list.



Set DRM Authorizations: Read-Only, Allow Unprotected Export \ Print, Expiry Date

Three parameters can be set: read-only, allow unprotected export and expiry date. These parameters will affect only the [CATIA V5 files protected by DRM](#).

Read-Only

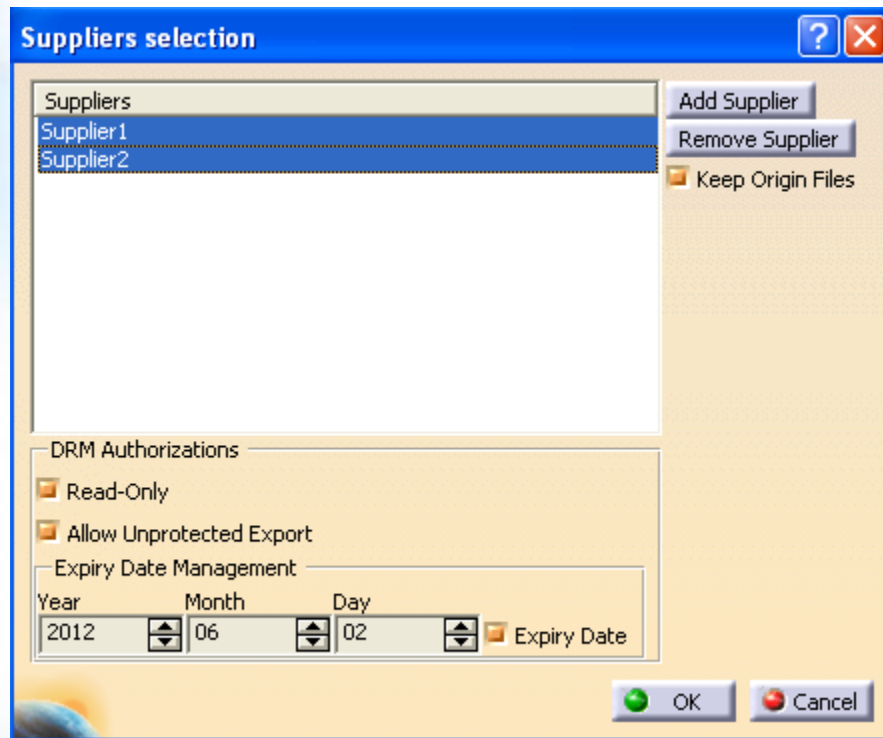
If the “Read-Only” box is checked, suppliers will be able to open and edit the files but not to save the modifications. A file “DS9ReadMe.txt” containing the message “The files in this folder are encrypted and protected with a Read-only attribute. You may be able to modify them inside CATIA, but Save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

Allow Unprotected Export \ Print

If the “Allow Unprotected Export \ Print” box is checked, suppliers will be able to save the files into non-encryptable formats (STEP, IGES). A file “DS9ReadMe.txt” containing the message “The files in this folder are encrypted with a Unprotected Export attribute. **Caution: Export into non-encryptable formats (IGES, STEP) is allowed.**” will be created in each supplier directory and in this way the OEM has given the right to print his CATIA data, so the supplier(s) will be able to print it or be able to do a print screen of the displayed data, if the rights are not given & the supplier(s) try to print the data a DRM error message will be displayed and the print screen keyboard button is not usable.

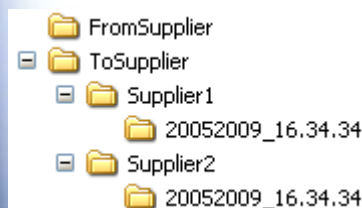
Expiry Date

If the “Expiry Date” box is checked: select the expiry date with format, 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.



When all the parameters are set, click on “OK” button.

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 ddMMyyyy_hh.mm.ss.



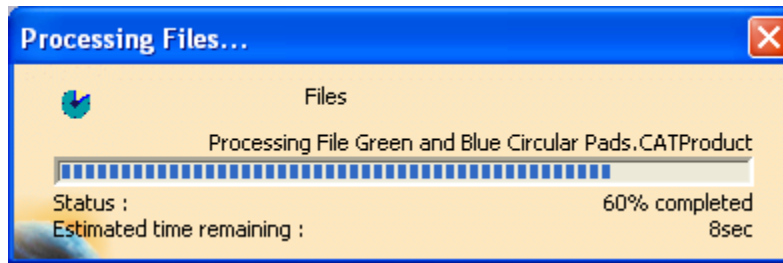
In the panel below, select the Origin Directory, from which the non-encrypted data will be read.



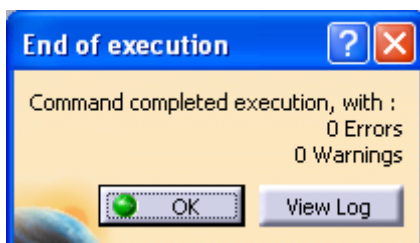
Once the folder is selected, press OK.

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.

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, except if you checked the "Keep Origin Files" option.

The Import Command

Description:

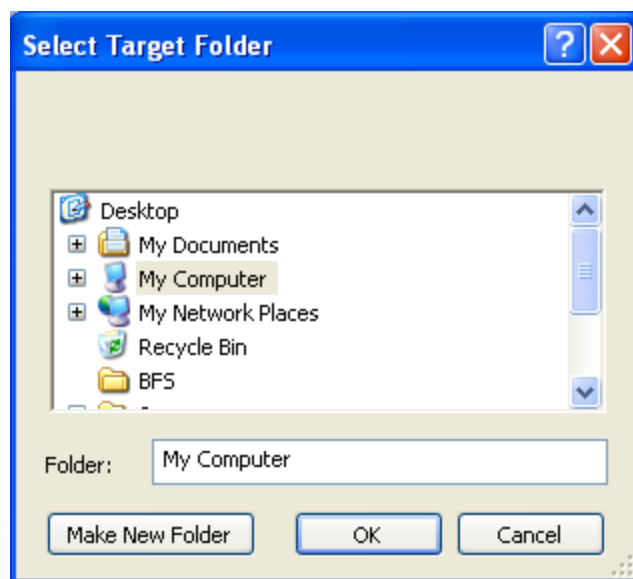
The Import command performs the following actions:

1. Read all the 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 from the "FromSuppliers" folder if required.

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 below, select the Target Directory, where the decrypted data will be stored.



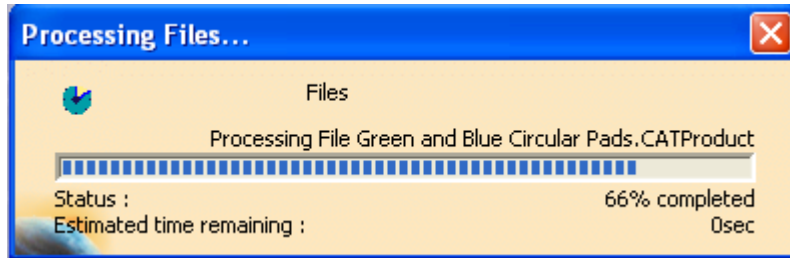
Once the folder is selected, press OK.

A panel appears to ask if the origin files must be kept (YES: the origin files will be kept, NO: the origin files will be deleted). Click on the desired answer.

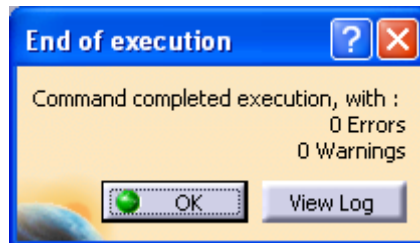


The decryption operation starts.

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.



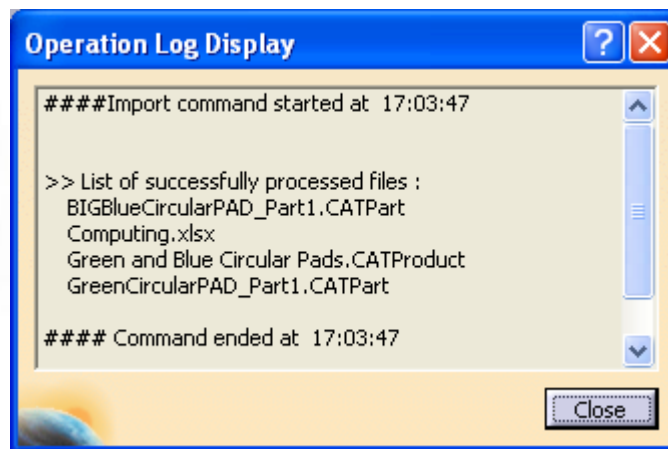
At the end of execution, a panel will show the number of errors and warnings:



Errors occur when a file could not be successfully decrypted.

Warnings occur when a file could not be deleted before or after the operation.

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).

The CheckStatus Command

Description:

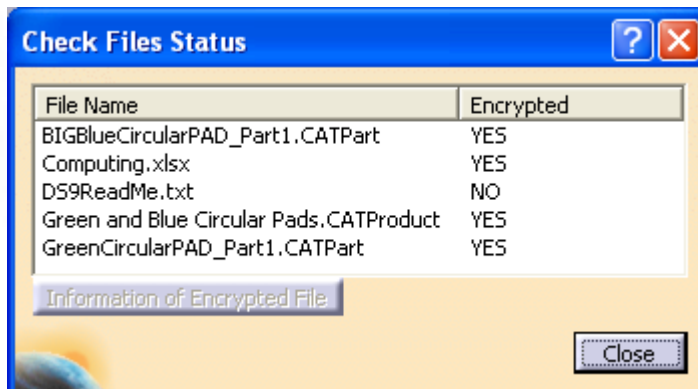
The CheckStatus command allows to view in a given directory which files are encrypted (or not) and to get information about suppliers, read-only status, allow unprotected export option and expiry date of encrypted files.

Click on the “Check Status” icon 

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

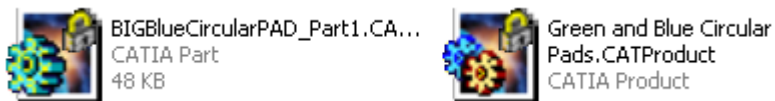


After selecting the folder, click “OK”

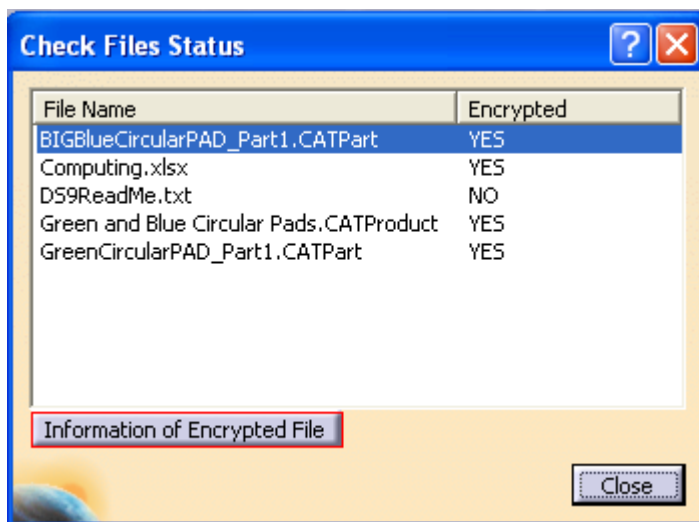


All the files present in the selected folder are listed in this panel, together with their encryption status (YES for an encrypted file, NO for a non-encrypted file).

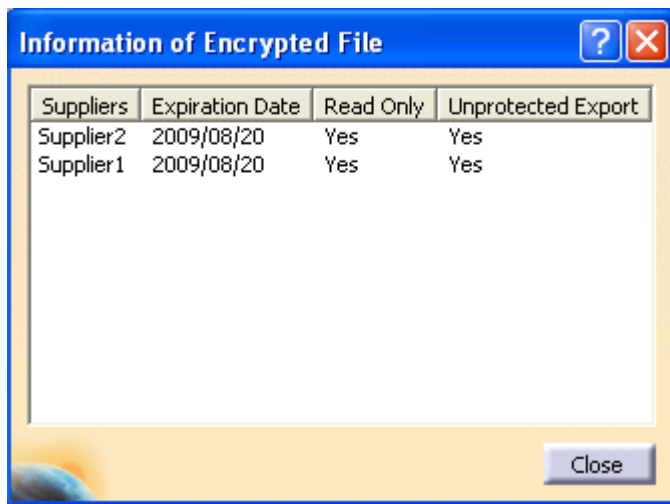
The encryption status can also be checked directly in Windows Explorer. The icons of all the encrypted files have a lock to identify them.



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), the Read-Only status and the Unprotected Export status are displayed.



The OEM Batch Application

Description:

The OEM Batch application "ISPDS9Batch" allows running Export Command or Import Command in batch mode.

For easy description, we suppose the installation as follows:

<CATIA_Path>: the CATIA installation path, such as D:\ds\B19

<DS9_Env>: the DS9 OEM environment path, such as D:\ds\DS9\DS9OEM\CATEnv

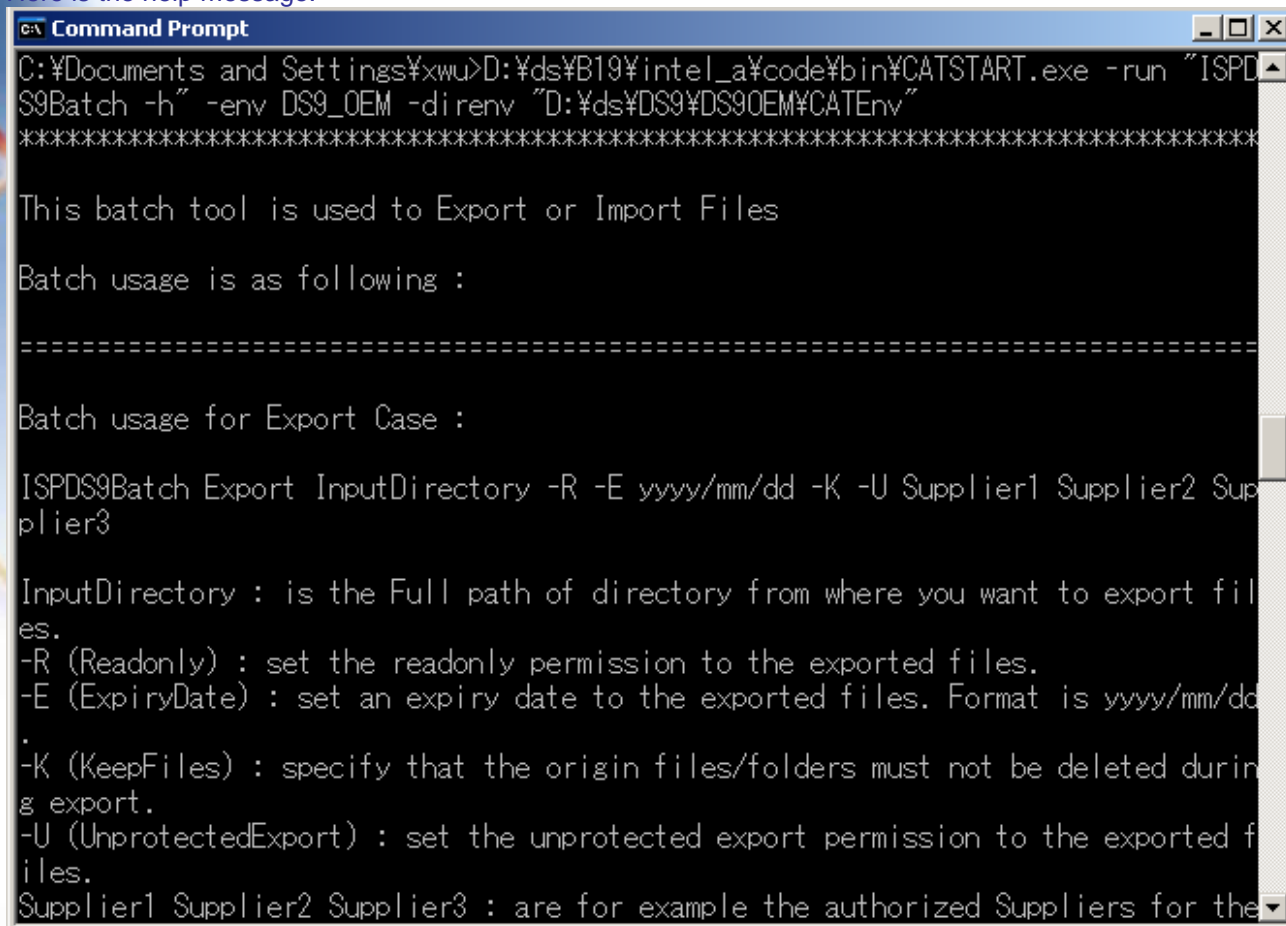
1. Display the help information of OEM Batch Application

<CATIA_Path>\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch -h" -env DS9_OEM -direnv <DS9_Env>

For example:

D:\ds\B19\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch -h" -env DS9_OEM -direnv "D:\ds\DS9\DS9OEM\CATEnv"

Here is the help message:



```

C:\Documents and Settings\xwu>D:\ds\B19\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch -h" -env DS9_OEM -direnv "D:\ds\DS9\DS9OEM\CATEnv"
*****
This batch tool is used to Export or Import Files

Batch usage is as following :

=====

Batch usage for Export Case :

ISPDS9Batch Export InputDirectory -R -E yyyy/mm/dd -K -U Supplier1 Supplier2 Supplier3

InputDirectory : is the Full path of directory from where you want to export files.
-R (Readonly) : set the readonly permission to the exported files.
-E (ExpiryDate) : set an expiry date to the exported files. Format is yyyy/mm/dd.
-K (KeepFiles) : specify that the origin files/folders must not be deleted during export.
-U (UnprotectedExport) : set the unprotected export permission to the exported files.
Supplier1 Supplier2 Supplier3 : are for example the authorized Suppliers for the
  
```

2. Run Export Command in batch mode

```
<CATIA_Path>\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch Export InputDirectory -R -E  
yyyy/mm/dd -K -U Supplier1 Supplier2 Supplier3" -env DS9_OEM -direnv <DS9_Env>
```

Each parameter is defined as follows:

InputDirectory: the Full path of directory from where you want to export files

-R: Readonly

Set the readonly permission to the exported files.

-E: ExpiryDate

Set an expiry date to the exported files. Format is yyyy/mm/dd

-K: KeepFiles

Specify that the origin files/folders must not be deleted during export.

-U: UnprotectedExport

Set the unprotected export permission to the exported files.

Supplier1 Supplier2 Supplier3

The authorized Suppliers for the Current Exported Files

At least one supplier must be specified here.

For example:

```
D:\ds\B19\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch Export D:\original -R -E  
2009/09/30 -K -U Supp1 Supp2" -env DS9_OEM -direnv "D:\ds\DS9\DS9OEM\CATEnv"
```

3. Run Import Command in batch mode

```
<CATIA_Path>\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch Import InputDirectory -K" -env  
DS9_OEM -direnv <DS9_Env>
```

Each parameter is defined as follows:

InputDirectory: the Full path of directory to where you want to Import Files

-K: KeepFiles

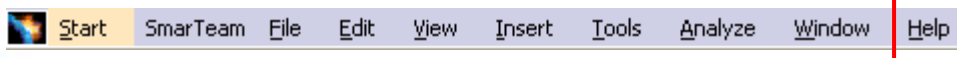
Specify that the origin files/folders must not be deleted during import

For example:

```
D:\ds\B19\intel_a\code\bin\CATSTART.exe -run "ISPDS9Batch Import D:\imported -K" -env  
DS9_OEM -direnv "D:\ds\DS9\DS9OEM\CATEnv"
```

Help About - CATIA Data Security

4. Click on Help in the Menu bar.



5. Now click on About CATIA Data Security.

