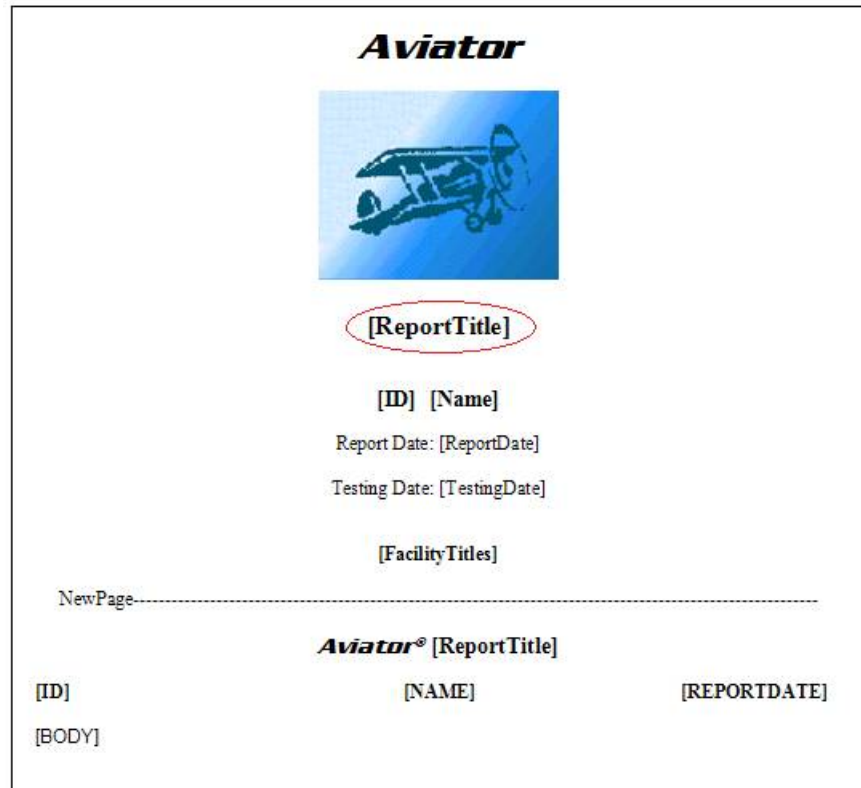


Valpar Software and Microsoft Word

The Basics of Report Generation

Valpar Software Products use Microsoft Word to generate reports. A collection of DOC and DOCM files are installed with the Software. We call these "skeleton" files because they provide only the barest outline of the report. For example, here is AR.DOC, the one Aviator skeleton file:



To generate a report, the Software makes a copy of this file with a new name and several data-files using information that the Software has collected about the Client. The Software then starts Word and tells it what file to open, namely, the new skeleton file.

The skeleton file contains several macros (see Appendix A). The AutoStart macro is executed when Word starts opens the skeleton file and its job is to get the ball rolling. Another macro does the heavy lifting to generate the report. It looks for things in [square brackets] and replaces them with information from the data files. This entails a lot of flickering and flashing until - presto! - there's the report.

On the following pages are the most common problems associated with Word.

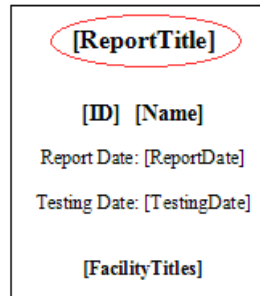
First and Foremost

Word must NOT be running (i.e., no Word documents are open) when the user clicks "Generate" to create a Valpar Report.

Macros must be Enabled

Valpar Software uses Microsoft Word and custom macros (see Appendix A) to generate reports. Macros are sometimes associated with security problems so quite often Word will be configured to ignore macros which will cause Valpar report generation to fail.

Reports with text in square brackets, such as:



[ReportTitle]

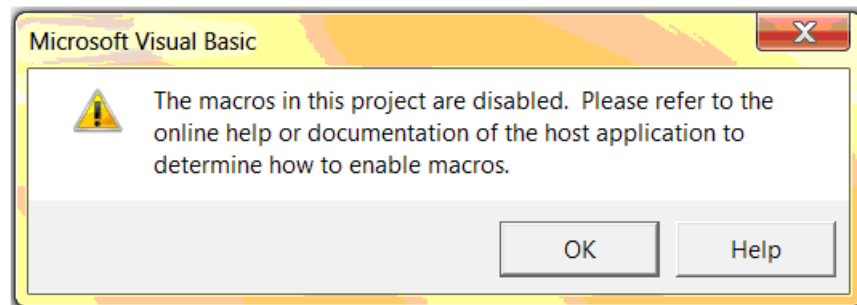
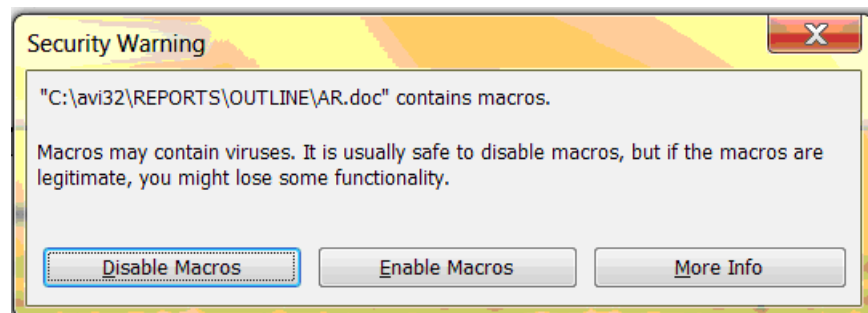
[ID] [Name]

Report Date: [ReportDate]

Testing Date: [TestingDate]

[FacilityTitles]

or security warnings such as:



are sure indicators that Word Macros are not enabled.


There are ways to fix this, described in [Appendix A](#), depending on which version of Word you have. If you work in a facility that has an IT Guru or an IT department it would be wise to consult with them before making any changes.

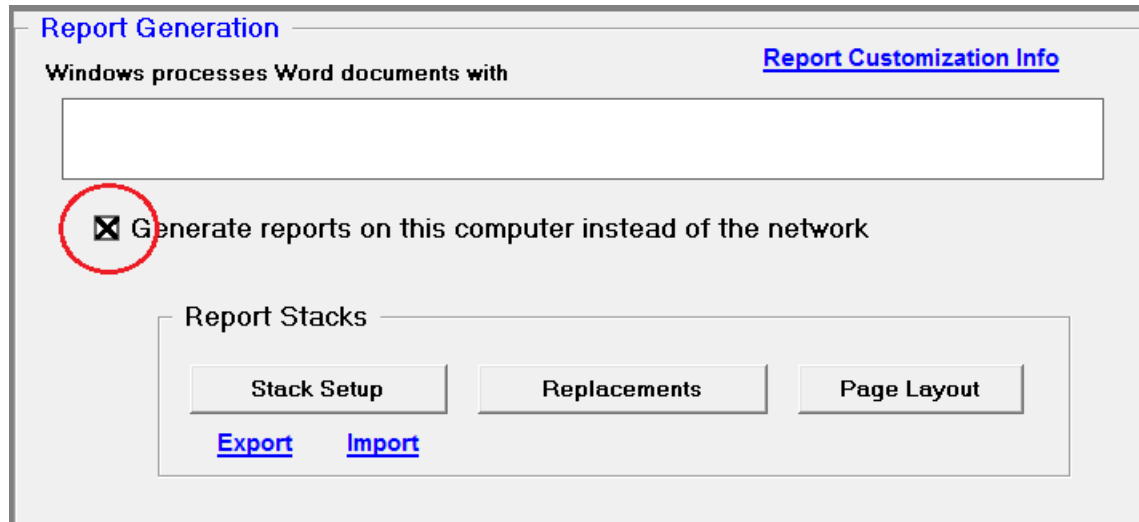
Access Rights - Runtime Error 70 - Permission Denied

Users must have "Modify Rights" to the directory in which the Software is installed, including all of its subdirectories. This is something for your IT person to fix.

Word and Server Access for Network Versions of Valpar Products

Your IT department may have Windows security policies in place on your server that prevent Word from accessing the DOCM files that are used to create reports. You can work around this as follows:

- 1) Login as the Manager
- 2) Click  in the row of buttons across the middle of the screen
- 3) Check the box shown below and exit the Manager Menu.



Valpar Software generates reports by creating a DOCM (or DOC for older versions of Word) file, and one or more TXT files. It then starts Word, which opens the DOCM and populates it with data in the TXT files. Normally all of these files are created in a subdirectory named reports\TempXX, where XX is the station number of the computer. For network versions of the Software this files will be on a server.

With this checkbox checked, the Software will create a path on the work station. The name depends on which Valpar Software you have:

C:\Aviator3Reports\
C:\Joule3Reports\
C:\Pro3000Reports\
C:\VCATreports

The Software will create the temporary DOC, DOCM and TXT files there. Presumably, work station permissions can be set to allow this.

NOTE: If Joule fails to create C:\JouleReports because of a security policy (runtime error 76, for example), a higher permissioned user can do the setup manually:

- 1) create the folder.
- 2) Set the security on the folder to give Joule users Modify rights.
- 3) Copy file JWORD.DOT from the Joule folder on the network to C:\JouleReports .

Appendix A - Macros

Microsoft Word is powered by a programming language called VBA (Visual Basic for Applications) plus a collection of programming "objects" that interface with VBA to do all of the things that Word does. For example:

- * select text
- * insert a picture
- * change fonts and font sizes
- * replace "this text" with "that text"

VBA has all sorts of capabilities to do non-Word sorts of things, such as:

- * delete files
- * download malicious code from the Internet
- * send an email to everyone in your email address list

It is generally a bad idea to let just any old macro run on your computer because there are a lot of bad hackers out there. Microsoft's answer to this problem for Office (Word, Excel, etc.) has evolved over the years and currently has these components:

- 1) Let the user create "Trusted Locations". Files in these directories are exempt from macro blocking. Your IT gurus can use Windows Security methods to control putting a file into a Trusted Location.

There is a "Trust Center" within Word where these things can be configured. Here's a link to a good how-to site:

<https://www.howtogeek.com/250834/how-to-disable-the-security-warning-message-bar-in-microsoft-office-programs/>

- 2) Let the user set a "macro security level". These vary by Word Revision. Typical settings for macro execution are Never, Always, and Ask first. Here are instructions for various versions of Word.

WORD 2003:

1. Open WORD 2003
2. Click on Tools
3. Click on Macro then on security
4. Choose low or medium
5. Click OK and close WORD 2003

If you choose medium then each time you generate a report Word will ask if you want to enable Macros and you will need to respond in the positive. A low setting just runs the Macro and opens the report.

Word 2007:

1. Open WORD 2007
2. Click on the Office icon in the upper left corner which will display a drop-down menu.
3. Click on Word options in the lower right corner of the drop-down menu.

4. Click the "Trust Center" link in the left pane.
5. Click on the "Trust Center Settings" button on right pane.
6. Select "Enable all Macros"
7. Put a check in the "Trust access to the VBA project object model" Check box
8. Click Ok on this screen and then OK on the next screen and close WORD 2007

Word 2010 and later:

1. Open WORD
2. Click on the File Tab and then click on Options.
3. In the Options dialog box click the "Trust Center" link in the left pane.
4. Click on the "Trust Center Settings" button on right pane.
5. Select "Enable all Macros"
6. Put a check in the "Trust access to the VBA project object model" Check box
7. Click Ok on this screen and then OK on the next screen and close WORD