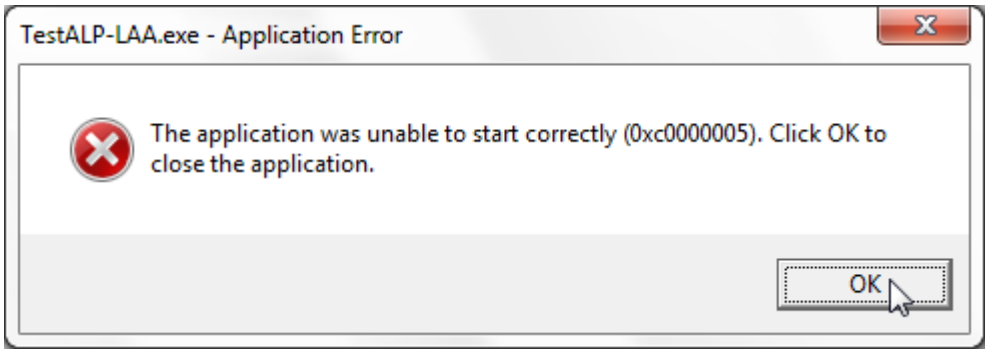
ALP-4.1 Issue with LargeAddressAware

1 API Misbehavior

The ALP-4.1 controller suite is a software accessory for the DLP® Discovery™ 4100 Starter Kit. It provides an easy-to-use application programming interface (API). This is a Windows® dynamic link library (DLL), so ALP can be used from any development environment or programming language that supports DLL import.

We have received reports about misbehavior when loading alpD41.dll. In these cases an “access violation” error message box appears. This happens as soon as the alpD41.dll is loaded, thus prohibiting successful load and usability of the API.

Example: 32-bit Windows application “TestALP-LAA.exe” implicitly linked to alpD41.dll. NTSTATUS 0xC00000005 means STATUS_ACCESS_VIOLATION. Other ways to load the library result in similar message boxes and equivalent error codes.



2 Affected Software

The cause could be tracked down to one specific software environment. Processes are affected that run in the Windows 32-bit On Windows 64-bit (WOW64) emulation layer. That means 32-bit applications started on 64-bit Windows operating system have this issue. Additionally they must have the IMAGE_FILE_LARGE_ADDRESS_AWARE flag set. This flag is set for example by the /LARGEADDRESSAWARE linker option. It allows 32-bit applications to use up to 4 GB of memory on WOW64. Without this flag, memory is limited to 2 GB.

3 Work-Arounds

3.1 Use 64-bit Application

The recommended work-around is using a native x64 version of the application.

3.2 Rebuild without /LARGEADDRESSAWARE

Most 32-bit applications do not require more than 2 GB of memory. They can safely live without the /LARGEADDRESSAWARE flag.

If source code is available, then please rebuild your application without the "/LARGEADDRESSAWARE" linker flag. Refer to your build tools documentation about how to do so.

3.3 Reset the IMAGE_FILE_LARGE_ADDRESS_AWARE Flag from an EXE File

If the application is only available in its binary version, it can even be adjusted to be not LARGEADDRESSAWARE.

Please use the tools DUMPBIN.EXE and EDITBIN.EXE to do so. Both are contained in Microsoft Visual Studio, available from Microsoft.com.

Example: Dumpbin /headers tells whether the LARGEADDRESSAWARE flag is set. Editbin /largeaddressaware:no resets this flag. The command-line log file below shows how to adjust an existing EXE file. It shows the image headers of the EXE file before and after resetting the flag. (Information of interest is highlighted; many less important lines have been stripped.)

```
F:\Alp41-LargeAddressAware>dumpbin /headers TestALP-LAA.exe
Microsoft (R) COFF/PE Dumper Version 8.00.50727.762
Copyright (C) Microsoft Corporation.  All rights reserved.


Dump of file TestALP-LAA.exe

PE signature found

File Type: EXECUTABLE IMAGE

FILE HEADER VALUES
             14C machine (x86)
               6 number of sections
        4F1FD0ED time date stamp Wed Jan 25 10:52:45 2012
               0 file pointer to symbol table
               0 number of symbols
              E0 size of optional header
             123 characteristics
                   Relocations stripped
                   Executable
                   Application can handle large (>2GB) addresses
                   32 bit word machine

OPTIONAL HEADER VALUES
             10B magic # (PE32)
…
F:\Alp41-LargeAddressAware>editbin /largeaddressaware:no TestALP-LAA.exe
Microsoft (R) COFF/PE Editor Version 8.00.50727.762
Copyright (C) Microsoft Corporation.  All rights reserved.
```

```
F:\Alp41-LargeAddressAware>dumpbin /headers TestALP-LAA.exe
Microsoft (R) COFF/PE Dumper Version 8.00.50727.762
Copyright (C) Microsoft Corporation.  All rights reserved.


Dump of file TestALP-LAA.exe
…
               E0 size of optional header
              103 characteristics
                    Relocations stripped
                    Executable
                    32 bit word machine

OPTIONAL HEADER VALUES
              10B magic # (PE32)
…
```

3.4 Use 32-bit Windows

If all other solutions fail, then the application can be run on a 32-bit version of the Windows operating system.

4 More Information

For more details, please refer to:

- “WOW64 Implementation Details” (http://msdn.microsoft.com/en-us/library/aa384274.aspx),
- “Memory Limits for Windows Releases” (http://msdn.microsoft.com/en-us/library/windows/desktop/aa366778(v=vs.85).aspx)
- “LOADED_IMAGE structure” (http://msdn.microsoft.com/en-us/library/windows/desktop/ms680349(v=vs.85).aspx)
- “/LARGEADDRESSAWARE (Handle Large Addresses)” (http://msdn.microsoft.com/en-us/library/wz223b1z(v=vs.100).aspx)
- “EDITBIN Reference” (http://msdn.microsoft.com/en-us/library/xd3shwhf(v=vs.100).aspx)
- “DUMPBIN Reference” (http://msdn.microsoft.com/en-us/library/c1h23y6c.aspx)