

FLASH PLAYER 8 AND SOBT COURSEWARE COMPATIBILITY

Macromedia's newest player has a new security model for Flash content run from a local source that blocks potentially unsafe activity. SOBT courseware that contains Flash files have been severely impacted by these new security enhancements. Due to this you may see a warning from the Flash Player similar to the following:

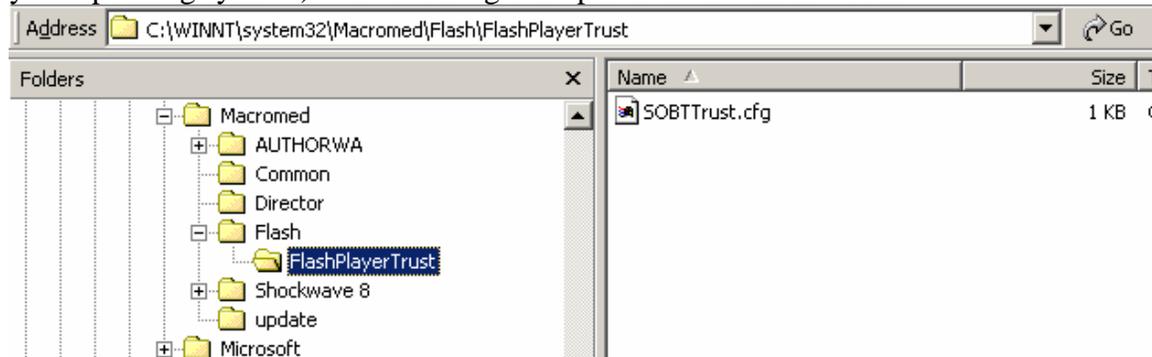


Fortunately Macromedia has published information on how to allow content created in previous versions of Flash to run in the new player in a trusted mode.

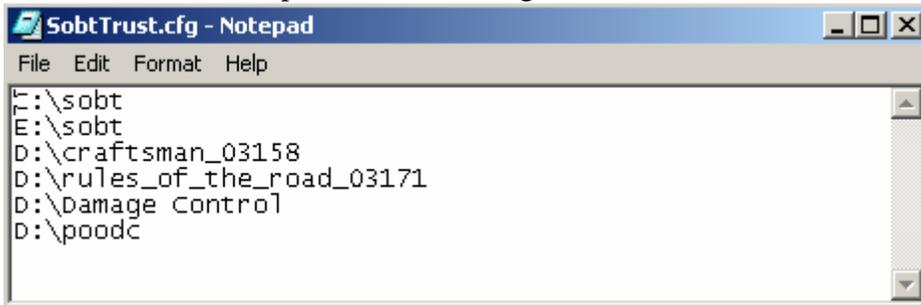
Two possible options that you could implement to allow Flash content in SOBT courseware to play without running into the new security barriers are:

OPTION ONE - Implement Macromedia's fix for relaxing security for local Flash content. Local content is content launched from the CD ROM drive, the local hard drive or a mapped network share. The process for this would be:

Step One – Create a new folder at C:\WINNT\System32\Macromed\Flash\ called FlashPlayerTrust. (Admin privileges may be needed for creation of folders in the System32 directory and the path to the System32 directory may vary depending on your operating system.) The following example is for Windows 2000.



Step Two – Open Notepad to create a file. Add trusted locations for SOBT courseware. An example of what this might look like is:



```
SobtTrust.cfg - Notepad
File Edit Format Help
C:\sobt
E:\sobt
D:\craftsman_03158
D:\rules_of_the_road_03171
D:\Damage Control
D:\poodc
```

Step Three – Save the file using “Save As...” vice save.

- Under “File name:” type SOBTrust.cfg.
- Under “Save as type:” select “All files”
- Under “Encoding:” select **Unicode**
- Save the file to the new folder created in Step One above.

The listing in the example above represents:

- C:\sobt - Trust Flash and HTML page intercommunication in the sobt folder on the local hard drive.
- E:\sobt - Trust Flash and HTML page intercommunication in the sobt folder on this mapped shared network drive.
- D:\craftsman_03158 - Trust Flash and HTML page intercommunication in this course when played from the CD drive.
- D:\rules_of_the_road_03171 - Trust Flash and HTML page intercommunication in this course when played from the CD drive.
- D:\Damage Control - Trust Flash and HTML page intercommunication in this course when played from the CD drive.
- D:\poodc - Trust Flash and HTML page intercommunication in this course when played from the CD drive.
- Additional specific entries as needed...

CAUTION – Do not use the system drive path (C:\). This will allow all content on the hard drive, CD ROM player, and all mapped drives to be trusted and should NOT be used. This will totally defeat the new security capabilities of Flash Player 8 which is not recommended and highly discouraged! A more specific approach should be implemented, as shown above, that targets only trusted content in very specific paths.

Notes:

- If you wish to include comments in this file then the comment line must end with the pound sign - #.
- The approach in Steps 1 – 3 lets you relax the security for trusted legacy content yet keep the computer secure from attacks from malicious Flash content.
- This is the only viable option for boats employing the SOBT CMI - AICC file-based format courses run via the SOBT CMI program or launched via the browser

for no-credit viewing. This is not a web-based format and as such, all content run would be considered “local” to the Flash Player.

- If you wish to automate Steps 1-3 the following DOS commands would accomplish the exact same thing:

```
Rem Make Directories if they don't exist
md %systemroot%\system32\Macromed
md %systemroot%\system32\Macromed\Flash
md %systemroot%\system32\Macromed\Flash\FlashplayerTrust
```

```
Rem Create a file if it doesn't exist and write text line in it.
echo C:\sobt>>%systemroot%\system32\Macromed\Flash\FlashplayerTrust\SOBTTrust.cfg
echo E:\sobt>>%systemroot%\system32\Macromed\Flash\FlashplayerTrust\SOBTTrust.cfg
echo D:\craftsman_03158>>%systemroot%\system32\Macromed\Flash\FlashplayerTrust\SOBTTrust.cfg
echo D:\rules_of_the_road>>%systemroot%\system32\Macromed\Flash\FlashplayerTrust\SOBTTrust.cfg
echo D:\Damage Control>>%systemroot%\system32\Macromed\Flash\FlashplayerTrust\SOBTTrust.cfg
echo D:\pooldc>>%systemroot%\system32\Macromed\Flash\FlashplayerTrust\SOBTTrust.cfg
```

OPTION TWO – The Web Server approach.

This option can only be used for the newer SCORM formatted courseware which is designed to be run from a web server or from a web-based Learning Management System (LMS) over HTTP. It cannot be used for SOBT CMI formatted courses which will not work properly if run from a web server. The exams will fail and other errors may occur since they were not created to work in this environment.

This option is applicable to SCORM formatted courses that have or don't have Flash content in them. It is an easy way to make them available to everyone on your network if you do not yet have an LMS installed aboard, and will get around the new Flash Player 8 security restrictions. The new security restrictions impact local content but not HTTP content.

Please note that SCORM formatted courses can **also** be run from the local file system and if run in that fashion will fall under OPTION ONE if they have Flash content in them.

A typical setup would involve:

Step One - Create a virtual directory in IIS on the web server that maps to the sobt directory. Many will have this directory already if they have the SOBT CMI program set up to use a network share for courses and the progress tracking database. Adding SCORM formatted courses to that folder will not impact the existing CMI network setup.

Step Two - Create an HTML Links Page with links to the no_lms_start.htm page of each SCORM course in the sobt folder.

Step Three - Create a link on your home page/portal page that launches the Links Page which will allow the student to launch one of the SCORM formatted courses in the browser and print out a completion certificate at the end.