

# Other tips

---

This document describes some useful tips, which may be helpful in reproduction.

## Page Heap

---

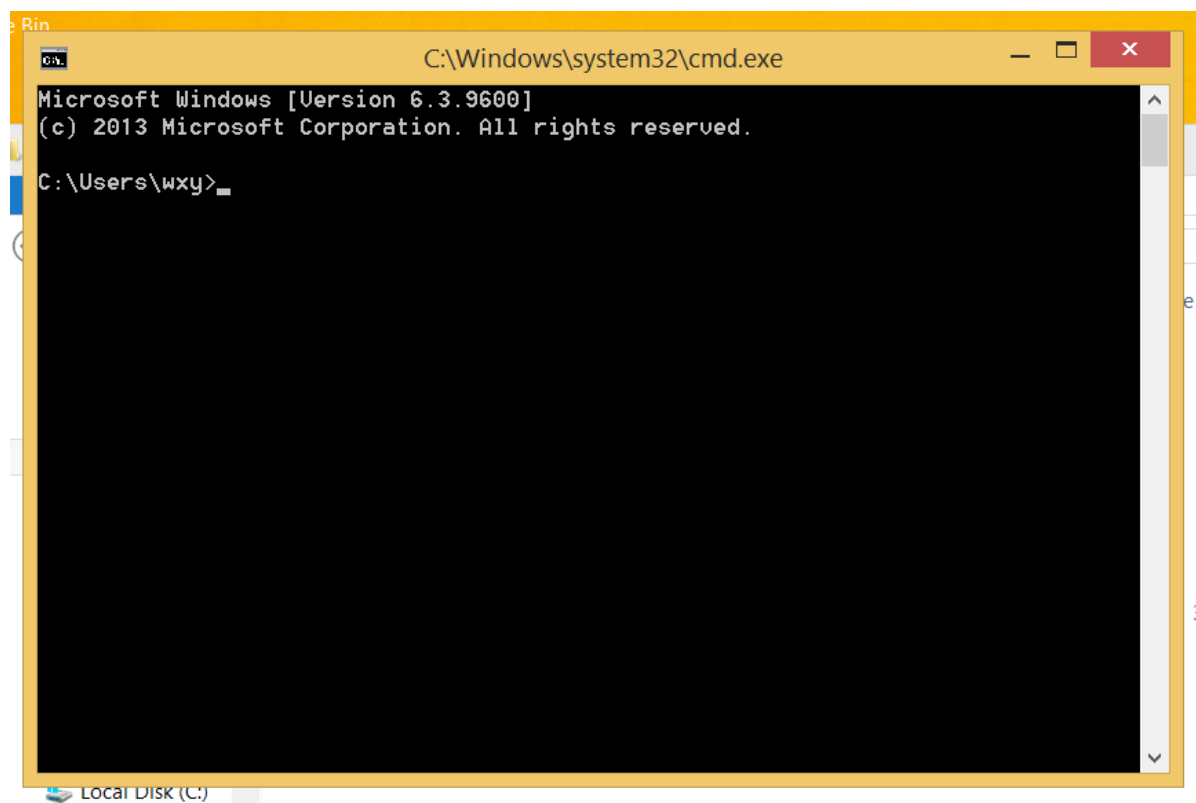
Page Heap is a kind of mechanism that Windows system implements to check if a software has heap overflow or other similar problems. Page Heap will slow down the execution of software greatly, so we only turn on Page Heap feature when fuzzing.

The detailed information could be found at (<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/gflags-and-pageheap>)

## how to use

turn on Page Heap (we use Adobe Reader as an example)

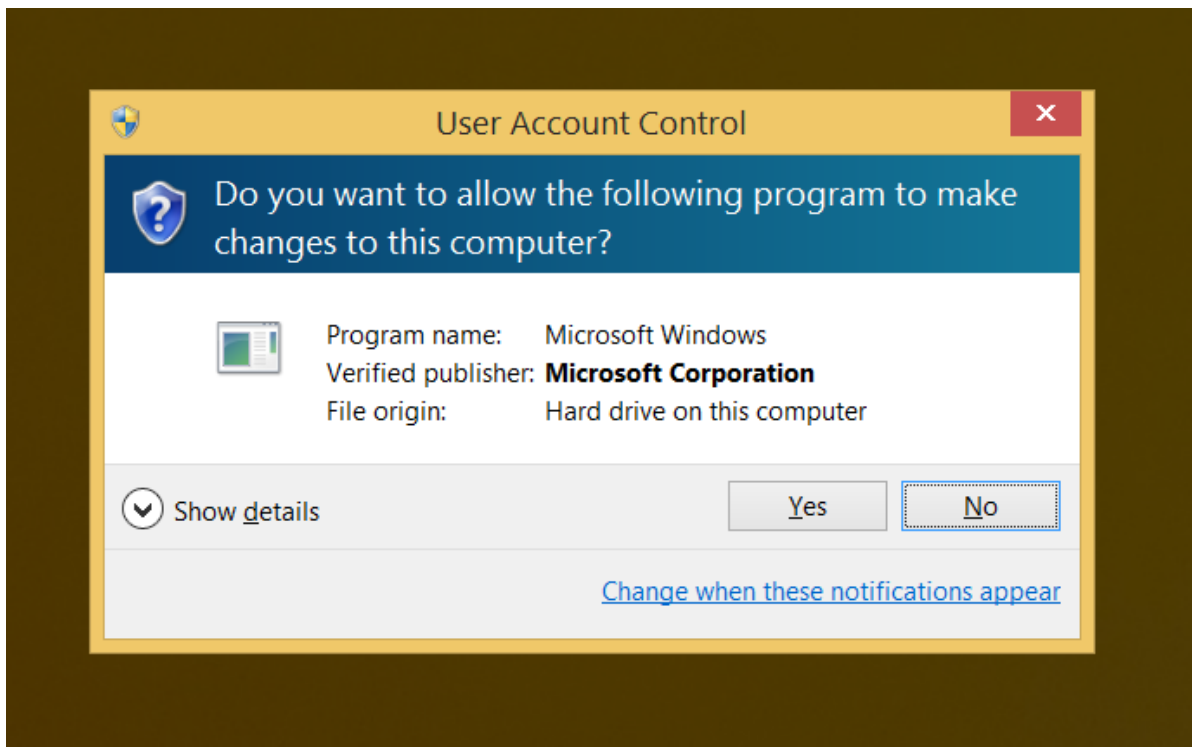
1. open cmd.exe



2. execute the following command

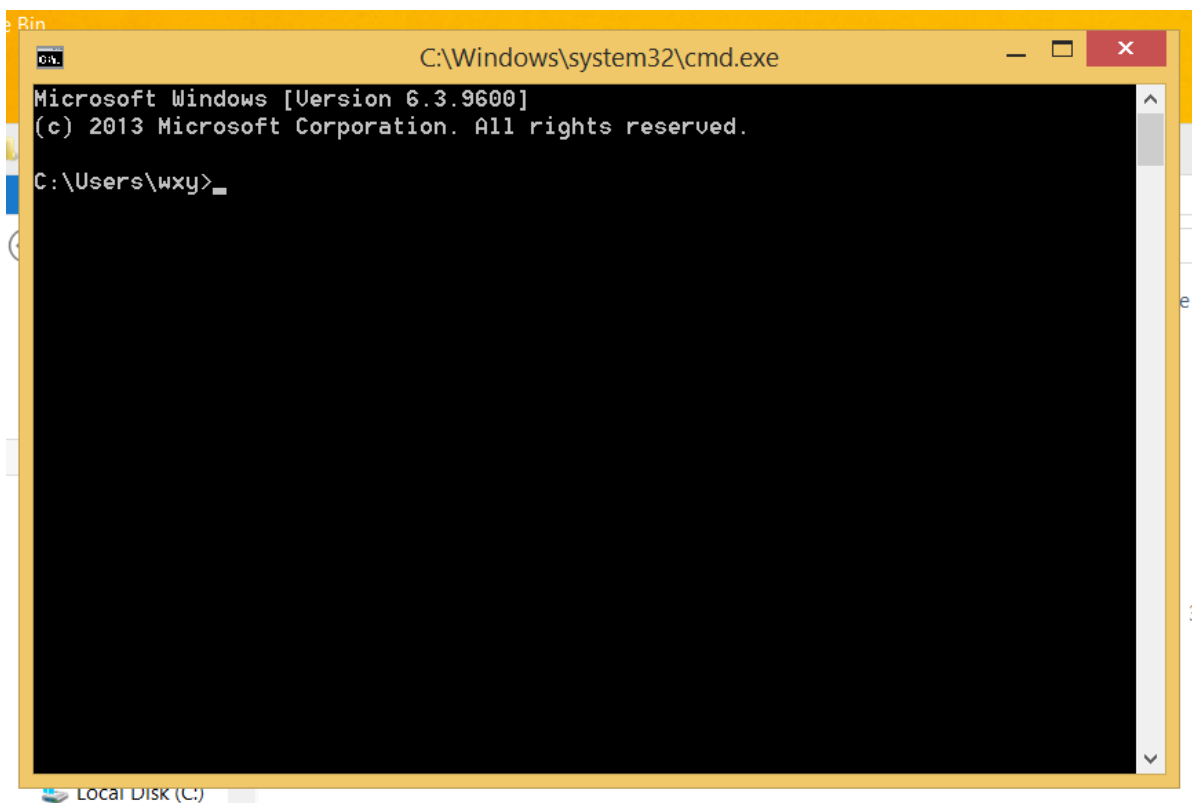
```
"C:\Program Files (x86)\windows Kits\8.1\Debuggers\x86\gflags.exe" /p /enable  
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"
```

3. click yes



turn off Page Heap

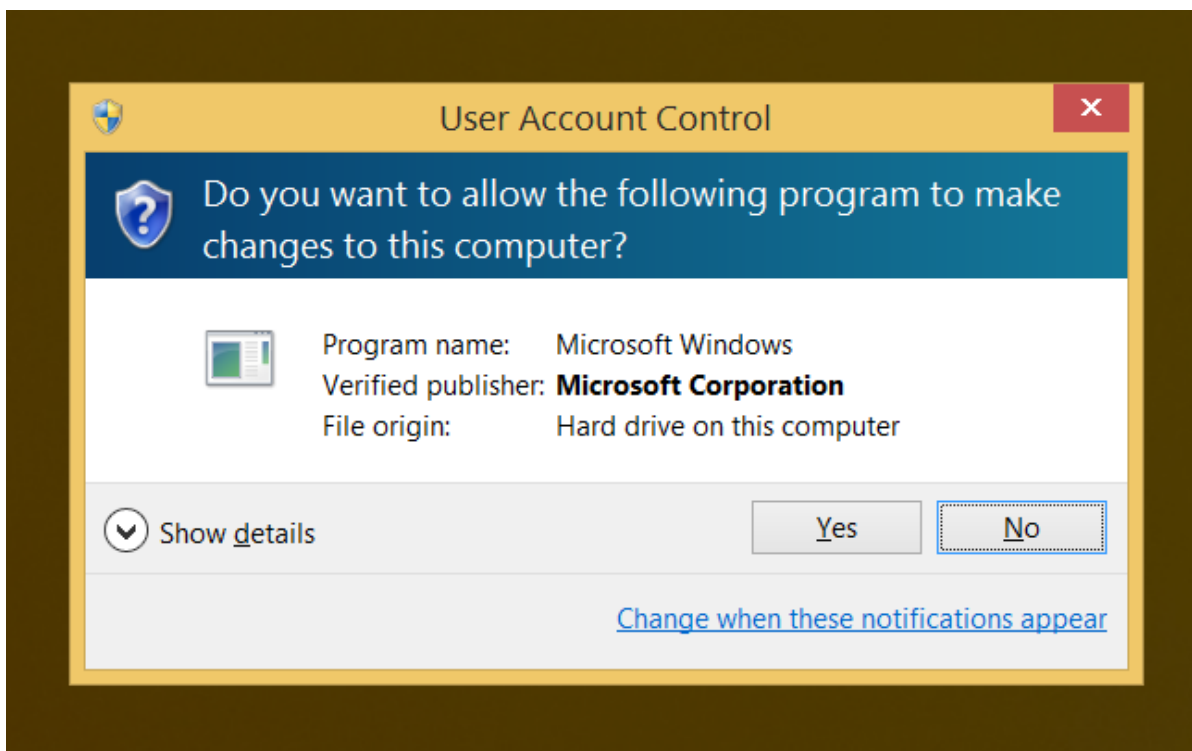
1. open cmd.exe



2. execute the following command

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /disable  
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"
```

3. click yes



## useful commands

turn on Page Heap on Adobe

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /enable
```

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"
```

turn off Page Heap on Adobe

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /disable
```

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"
```

turn on Page Heap on Foxit(version 10.1.1)

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /enable
```

```
"C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitReader.exe"
```

turn off Page Heap off Foxit(version 10.1.1)

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /disable
```

```
"C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitReader.exe"
```

turn on Page Heap on Foxit(version 11.2.1)

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /enable
```

```
"C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\FoxitPDFReader.exe"
```

turn off Page Heap on Foxit(version 11.2.1)

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /disable
```

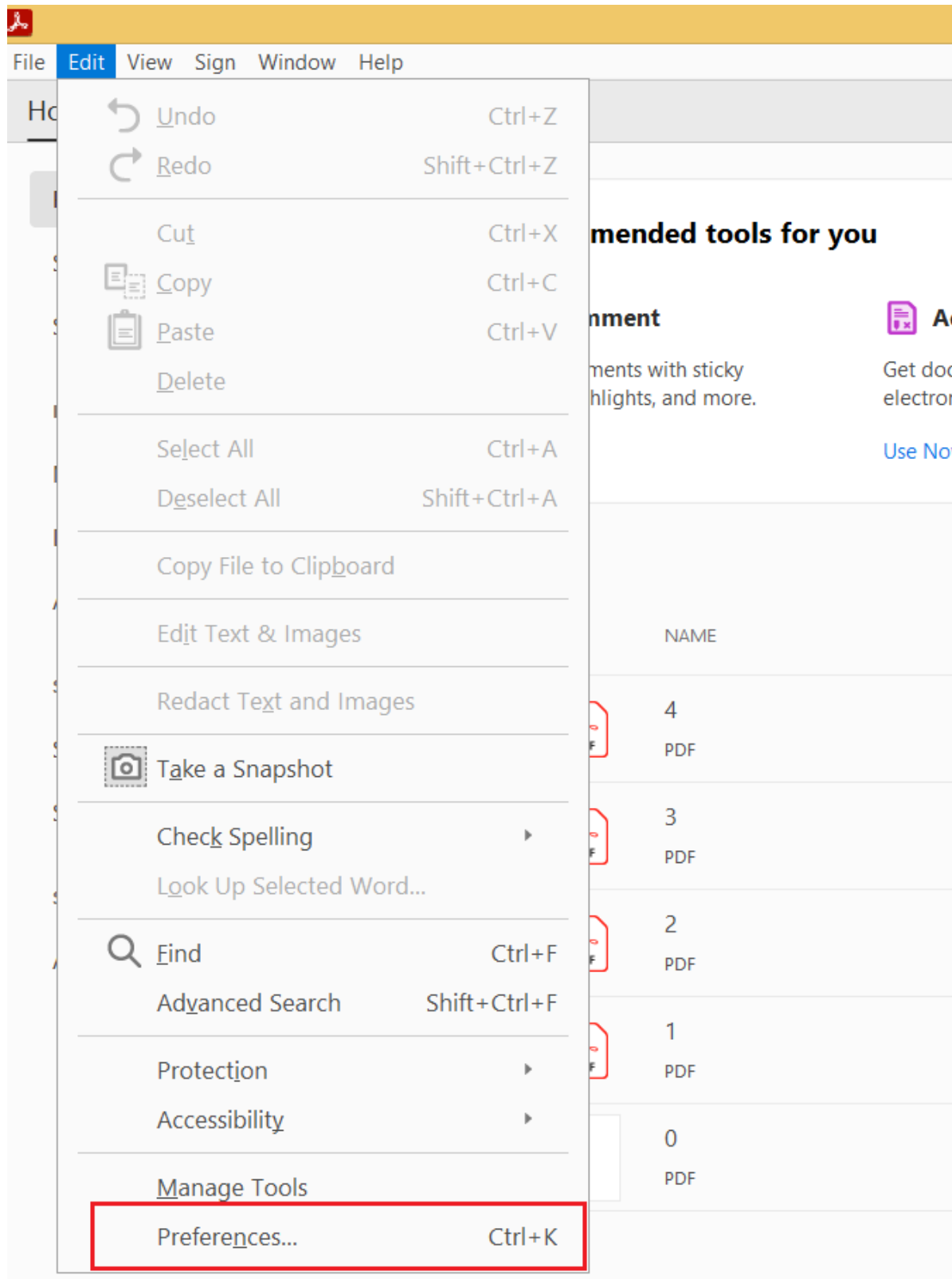
```
"C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\FoxitPDFReader.exe"
```

## Privilege Location Setting in PDF Reader

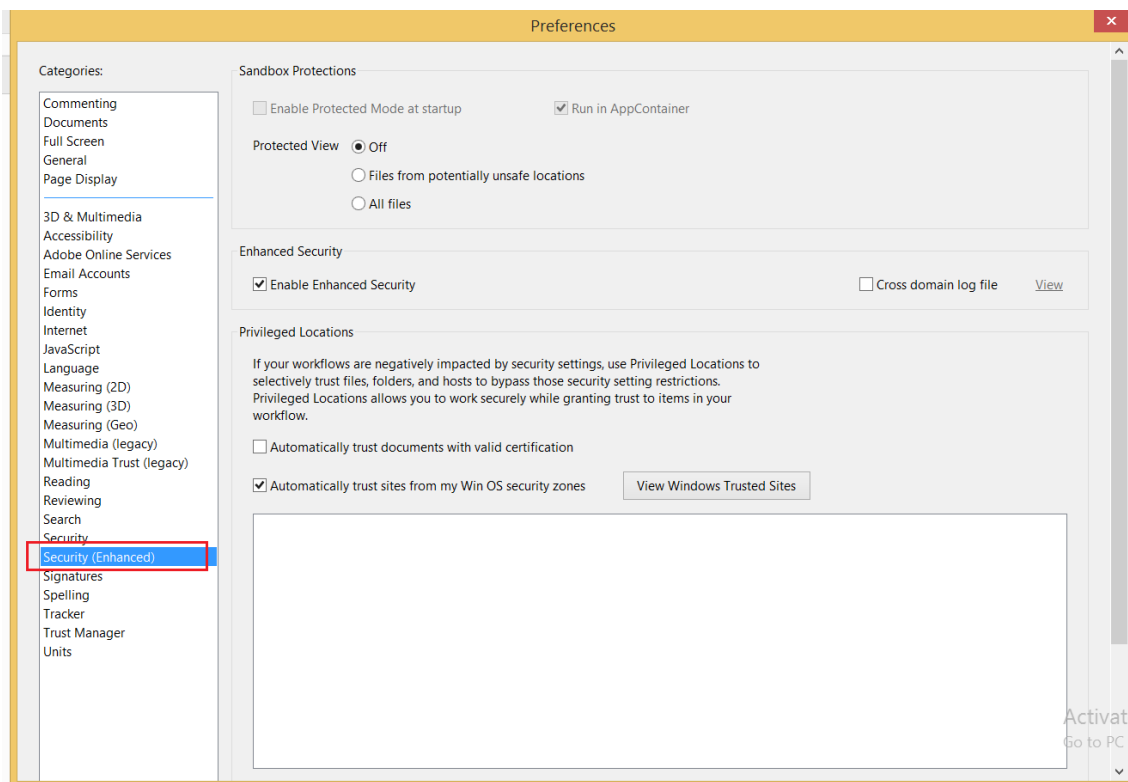
Normally, some binding calls in the PDF Readers can not be called, in consideration of security risk, so we need to add our tool's path to privilege location. Next we will talk about how to do it.

# Adobe Reader

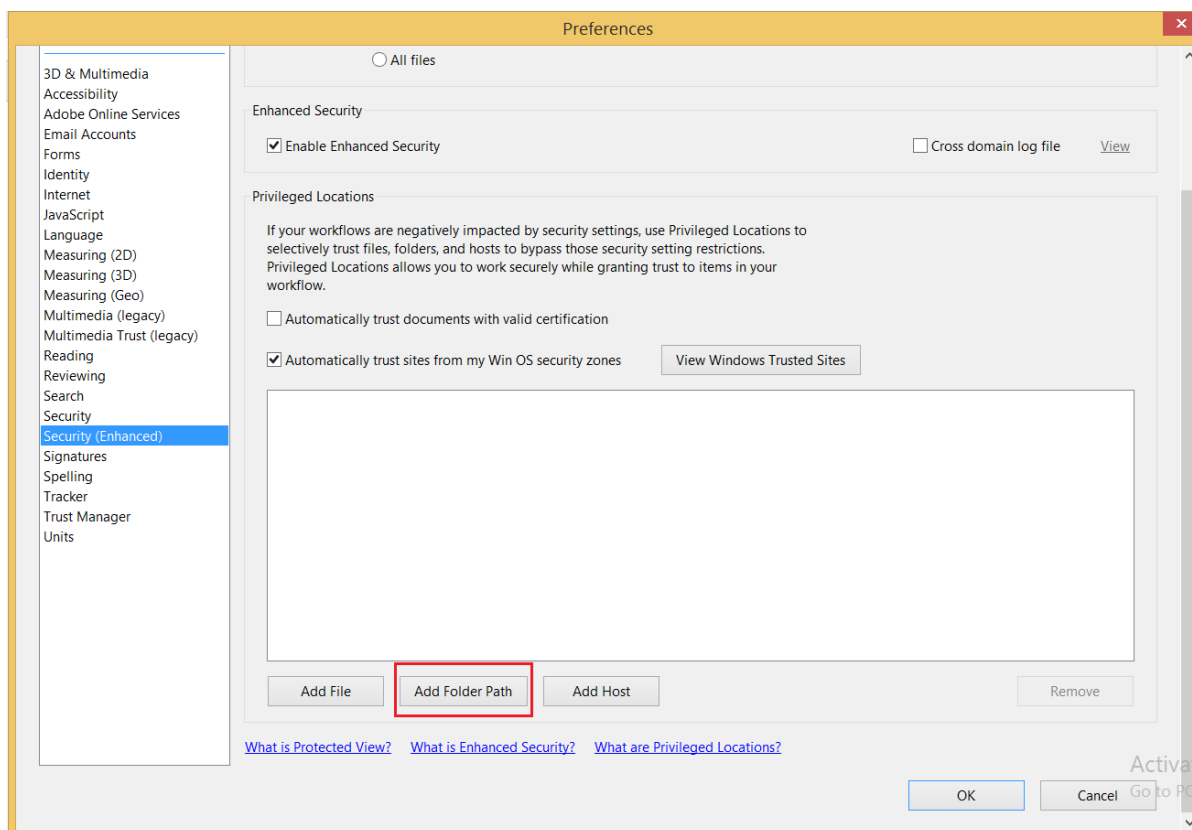
1. Open Adobe Reader, click **Edit->Preference**



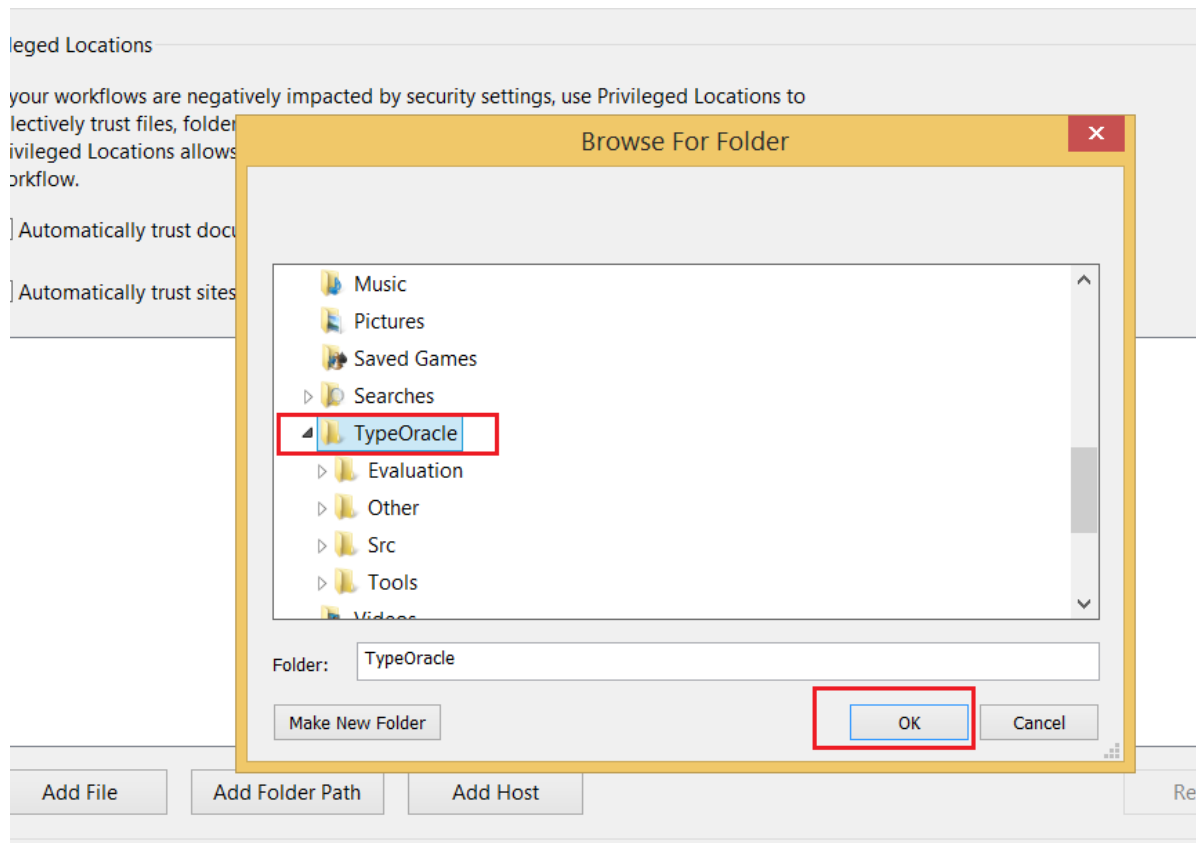
2. Click **Security(Enhanced)** button



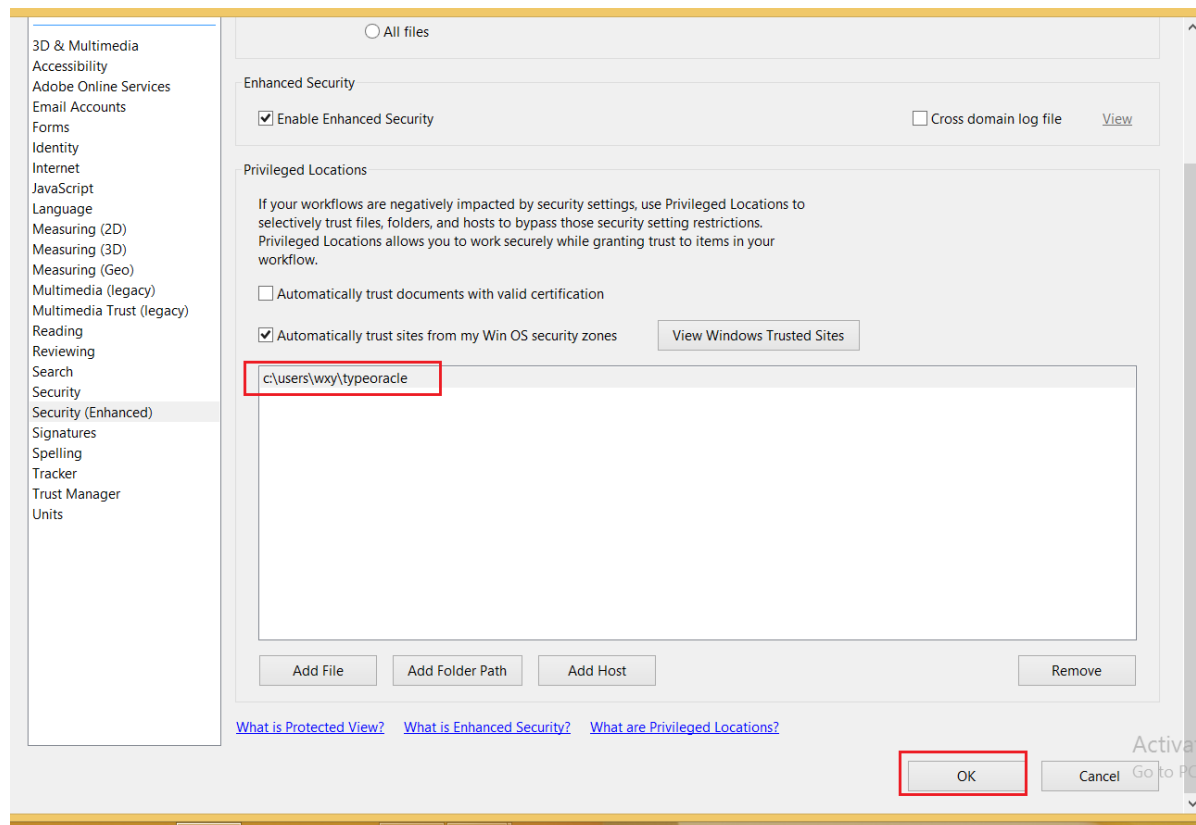
### 3. click Add Folder Path



### 4. choose our tool's path and click OK

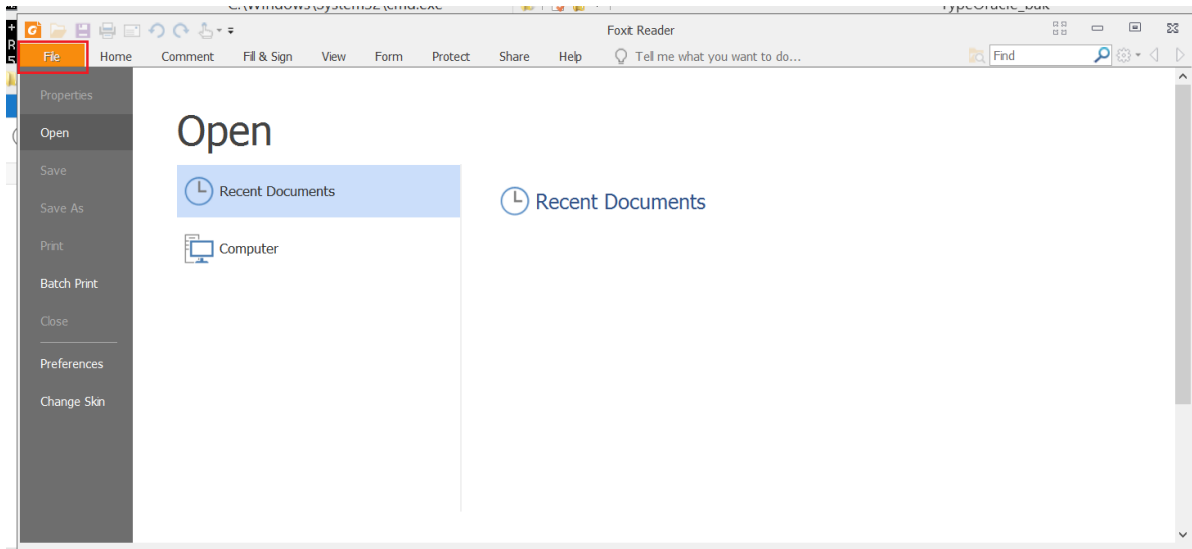


5. After it, we can see that our tool's path has been added to privilege location, then click OK button

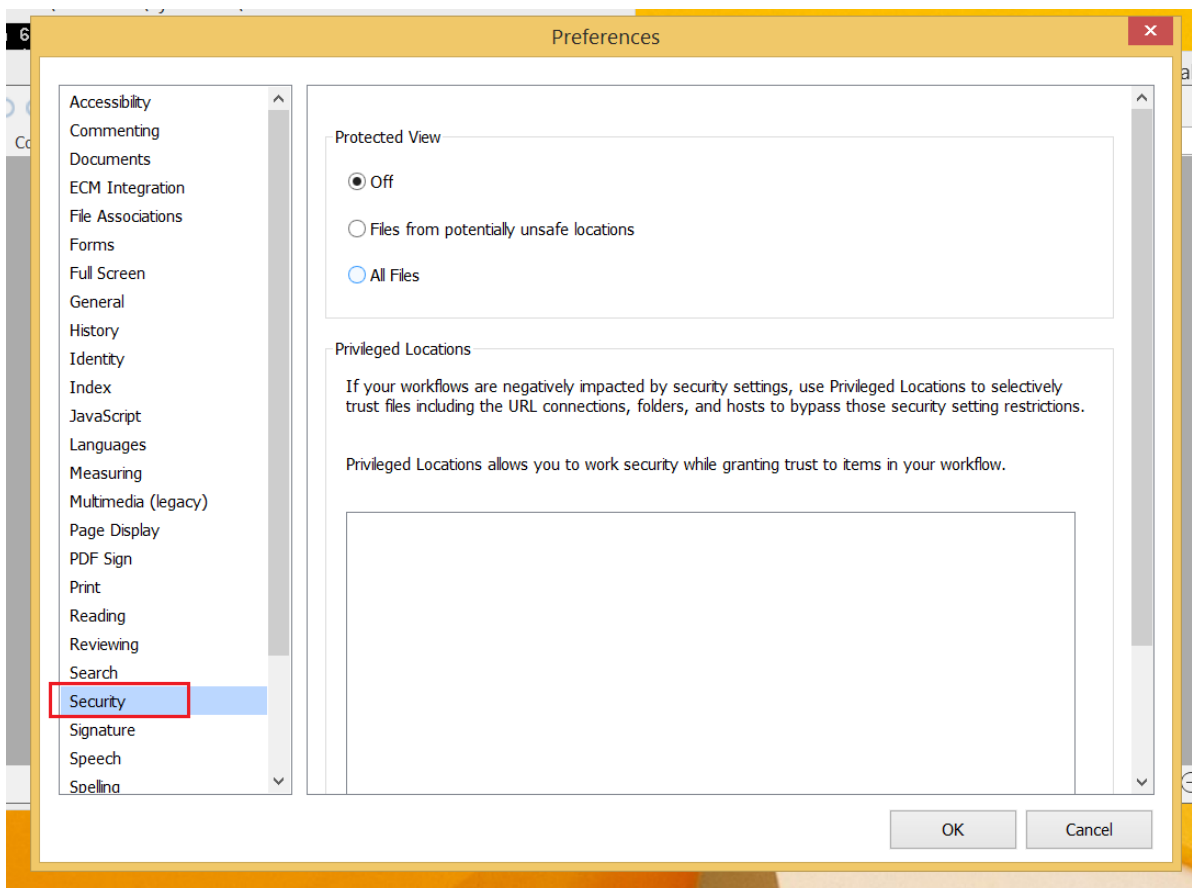


# Foxit Reader

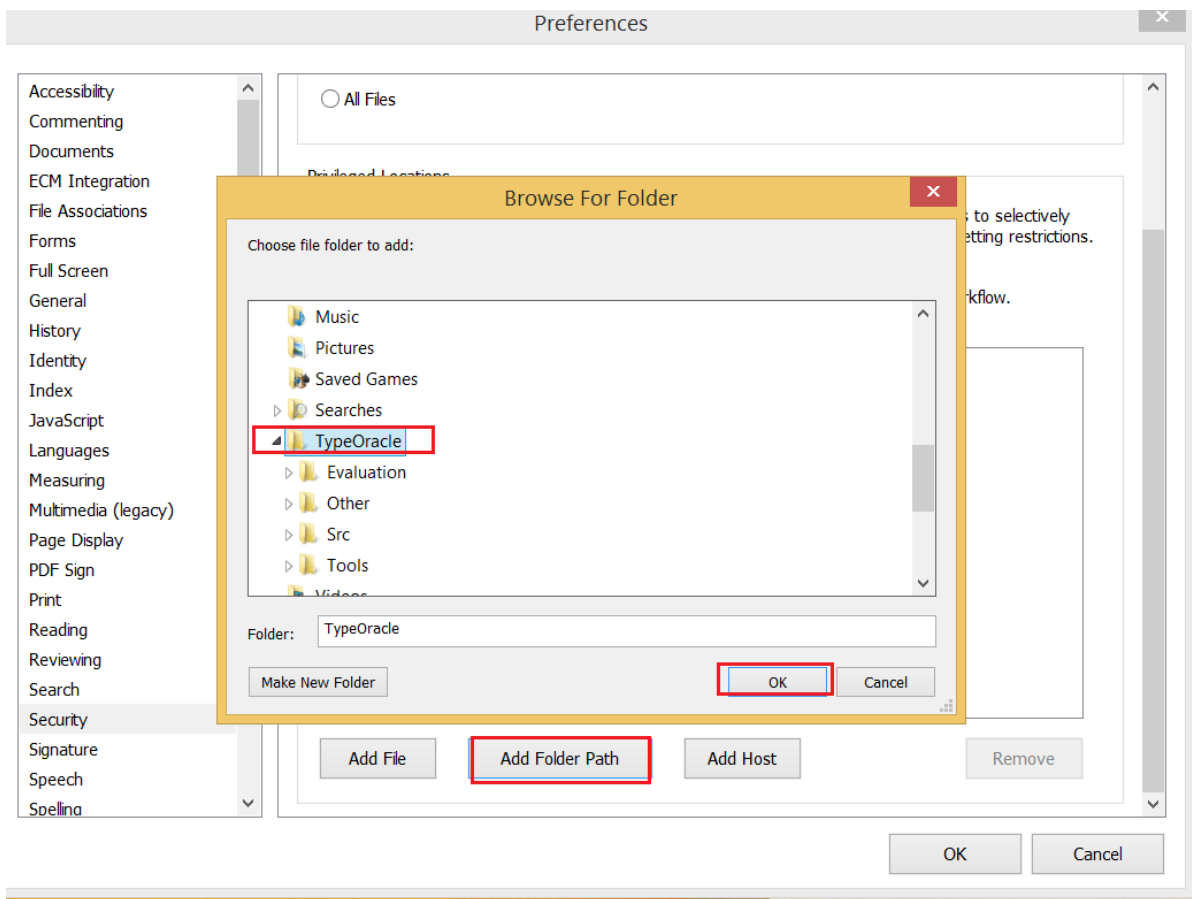
1. Open Foxit Reader, click **File**



2. click **Preferences** , then click Security



3. click **Add Folder Path** , choose our tool's path, and click OK button



4. now we can see that our tool's path has been added to privilege location, then click OK button

