

Adobe Experience Manager SharePoint IFilter for Document Security Protected Document

Legal Notices

For more information, see http://help.adobe.com/en_US/legalnotices/index.html.

Content

Supported Platforms	2
Configure Microsoft SharePoint 2010	2
Configure Microsoft SharePoint 2013	5
Configure AEM forms IFilter	6
Prerequisites.....	6
Client Certificate Configuration	6
Configure Client Certificate for AEM forms IFilter Service.....	6
Client Certificate Registry Setting	7
Configure SharePoint/FAST Search Server for SharePoint to use AEM forms IFilter	8
Troubleshooting AEM forms IFilter	9
Opening Document Security protected PDF documents in Acrobat/Reader.....	9
Run iFiltTst on an unprotected document.....	9
Run iFiltTst on a protected PDF document.....	10
Run Indexing for a protected PDF document.....	10
Known Limitations.....	11

Microsoft Windows full-text search engines like the Desktop Indexing Service and the SharePoint Index server provide native text search for document formats such as txt, doc, and docx. This implies that you cannot use these search engines to perform full text search on AEM forms Document Security protected PDF documents. AEM forms now allows you to configure and use the Document Security IFilter service to allow your SharePoint users to perform full-text search on AEM forms Document Security protected PDF documents.

This package contains the **AEM forms SharePoint IFilter for Document Security Protected Documents**. This IFilter is used with SharePoint and allows SharePoint to search for the text within PDF documents which have been Rights protected using AEM forms Document Security server with Mutual Authentication support.

Supported Platforms

Application	Operating System
Microsoft Office SharePoint Server 2010 and Microsoft Office SharePoint Server 2013	Windows Server 2008 x64 SP1 Windows Server 2010 x64 SP1
FAST Search Server 2010 for SharePoint (SharePoint/FAST Search Server)	Windows Server 2008 x64 SP1 Windows Server 2010 x64 SP1
Adobe LiveCycle ES4 or higher AEM 6.0 forms with Service Pack 1 or higher	All supported platforms. For details, see <ul style="list-style-type: none">LiveCycle ES4 Supported Platform Combinations.AEM 6.0 forms Supported Platform Combinations.
Adobe Acrobat / Reader 11 or higher	Windows Server 2008 x64 SP1 Windows Server 2010 x64 SP1

Note: If you use AEM forms IFilter with Microsoft Office SharePoint Server 2013, ensure that you have hotfix KB2883000 installed. You can visit <https://support.microsoft.com/en-us/kb/2882989> to obtain the hotfix.

Configure Microsoft SharePoint 2010

Perform the following steps to add AEM SharePoint IFilter for indexing pdf files to Microsoft SharePoint 2010:

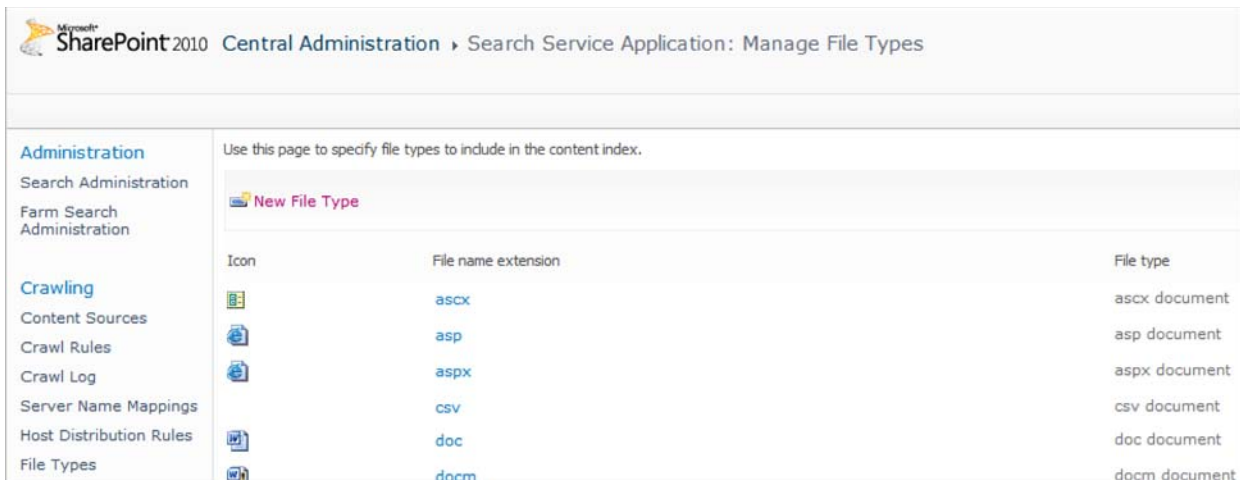
1. Download the Adobe PDF file icon from <http://www.adobe.com/misc/linking.html#producticons> or use the Adobe PDF file icon installed at \Program Files\Adobe\Adobe PDF iFilter 11 for 64-bit platforms\pdf.gif.
2. Copy Adobe PDF file icon at \Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\IMAGES\.
3. Add the mapping entry to the doclcon.xml file. The mapping entry is added to the doclcon.xml file to keep the pdf icon in SharePoint while it displays the search results:
 - a). Open the \Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\XML\doclcon.xml file for editing.

- b). Add the following code in the docIcon.xml file:
<Mapping Key="pdf" Value="pdf.gif" />

```
<Mapping Key="vs1" value="icvs1.gif" OpenControl="" />
<Mapping Key="vss" value="icvss.gif" EditText="Microsoft Visio" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="vst" value="icvst.gif" EditText="Microsoft Visio" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="vsu" value="icvsu.gif" OpenControl="" />
<Mapping Key="vsw" value="icvsw.gif" OpenControl="" />
<Mapping Key="vsx" value="icvsx.gif" EditText="Microsoft Visio" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="vtx" value="icvtx.gif" EditText="Microsoft Visio" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="wdp" value="ichdp.gif" />
<Mapping Key="webpart" value="icdwp.gif" OpenControl="" />
<Mapping Key="wm" value="icwm.gif" OpenControl="" />
<Mapping Key="wma" value="icwma.gif" OpenControl="" />
<Mapping Key="wmd" value="icwmd.gif" OpenControl="" />
<Mapping Key="wmp" value="icwmp.gif" OpenControl="" />
<Mapping Key="wms" value="icwms.gif" OpenControl="" />
<Mapping Key="wmv" value="icwmv.gif" OpenControl="" />
<Mapping Key="wmx" value="icwmx.gif" OpenControl="" />
<Mapping Key="wmz" value="icwmz.gif" OpenControl="" />
<Mapping Key="wsf" value="icwsf.gif" OpenControl="" />
<Mapping Key="xla" value="icxla.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xlam" value="icxlam.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xls" value="icxls.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xlsb" value="icxlsb.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xlsm" value="icxlsm.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xlsx" value="icxlsx.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xlt" value="icxlt.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xltb" value="icxltb.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xltm" value="icxltm.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xltx" value="icxltx.png" EditText="Microsoft Excel" OpenControl="SharePoint.OpenDocuments" />
<Mapping Key="xml" value="icxml.gif" />
<Mapping Key="xps" value="icxps.gif" OpenControl="" />
<Mapping Key="xsd" value="icxsd.gif" />
<Mapping Key="xsl" value="icxsl.gif" />
<Mapping Key="xsn" value="icxsn.gif" EditText="Microsoft InfoPath" OpenControl="SharePoint.OpenXMLDocuments" />
<Mapping Key="xslt" value="icxslt.gif" />
<Mapping Key="xst" value="icxst.gif" OpenControl="" />
<Mapping Key="pdf" value="pdf.gif" />
</Default>
<Mapping value="icgen.gif" />
</Default>
</DocIcons>
```

- c). Save and close the file.

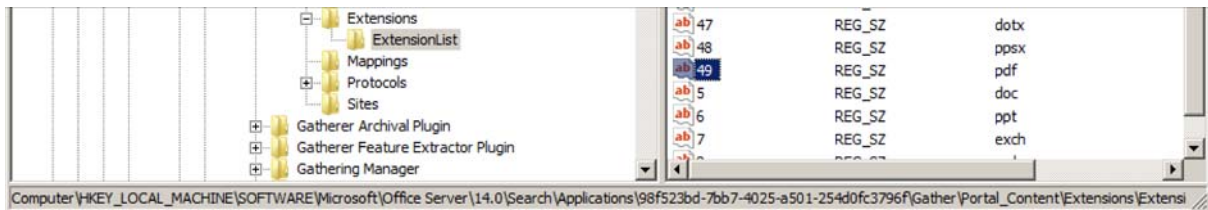
- 4. Add the .pdf file type to the SharePoint content index.



- 5. Perform the following steps to verify that the PDF is added to the registry.

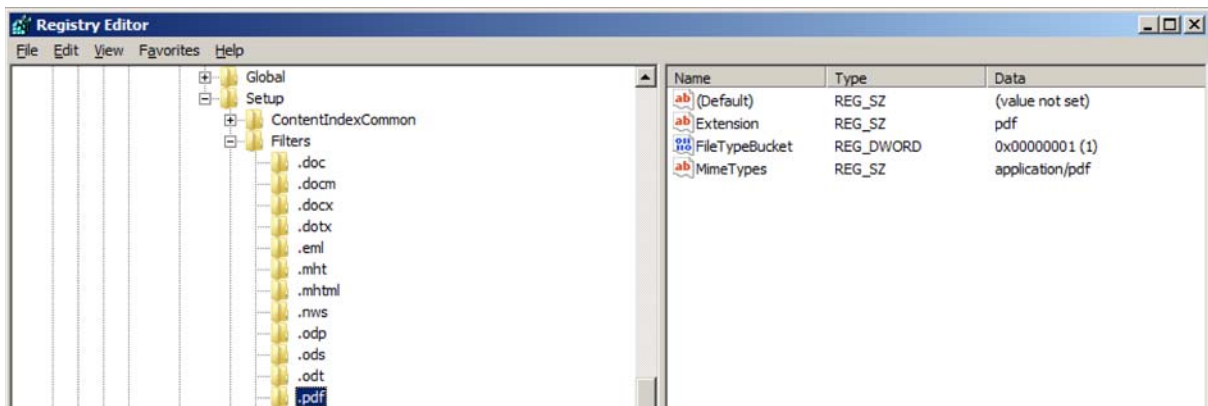
- a). Open the registry editor and navigate to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OfficeServer\14.0\Search\Applications\{site
GUID}\Gather\Portal_Content\Extensions\ExtensionList.

- b). If the PDF extension is not present, right click on right-side Extension List pane and choose **New > String Value**.
- c). Provide a name to the new Registry Key. For example, 49.
- d). Double click the newly created Registry Key. For the Value data field, type pdf.



6. Verify that PDF has the correct settings at second registry location. In the registry editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server\14.0\Search\Setup\Filters\pd and verify the following values. If values do not exist, edit the keys are and set the values as listed below:

- <REG_SZ> Default = <value not set>
- <REG_SZ> Extension = pdf
- <REG_DWORD> FileTypeBucket = 1

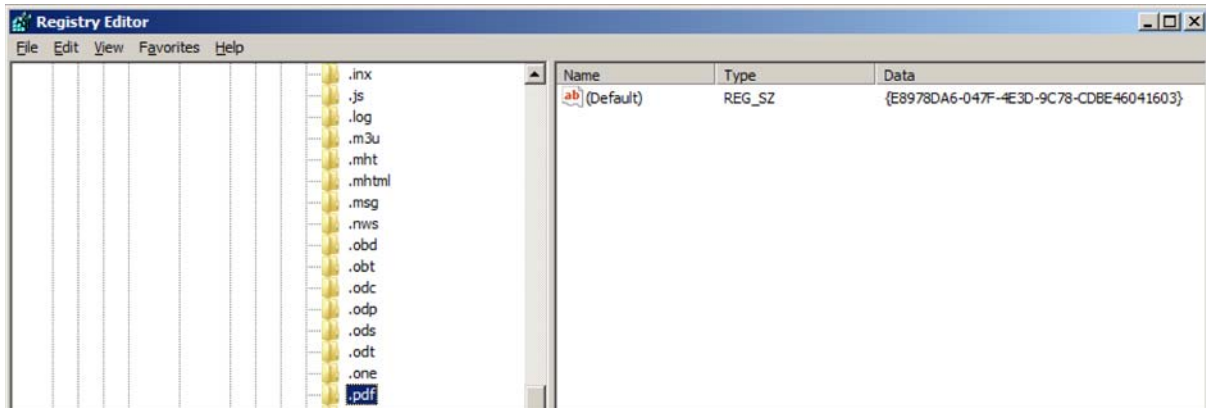


- <REG_SZ> MimeTypes = application/pdf

7. Verify that PDF has the correct settings at third registry location.

In the registry editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server\14.0\Search\Setup\ContentIndexCommon\Filters\Extension\pdf and verify the value: <REG_MULTI_SZ> Default = {303A447D-860E-4e72-ADB0-DB74999F8E3A} exists.

If the specified value does not exist or is different, replace it with the above mentioned value.



- Restart all SharePoint services and Internet Information Server (IIS). Open the command prompt as an administrator and run the following commands in the listed order,
 - `net stop oseach14`
 - `net start oseach14`
 - `iisreset`

Configure Microsoft SharePoint 2013

Perform the following steps to replace the in-built PDF filter of Microsoft SharePoint 2013 to AEM SharePoint IFilter:

- Click Start and run **SharePoint 2013 Management Shell** as an administrator.
- Run the following commands to replace in-built IFilter with a third party IFilter
 - `$ssa = Get -SPEnterpriseSearchServiceApplication`
 - `Set -SPEnterpriseSearchFileFormatState -SearchApplication $ssa PDF $TRUE $TRUE`
- Run the following command to verify that the third party IFilter has replace in-built IFilter:
 - `Get -SPEnterpriseSearchFileFormat -SearchApplication $ssa pdf`If the command returns `UseFilter: True`, then the third party IFilter has sucessfully replace in-built IFilter.
- Close **SharePoint 2013 Management Shell**.
- Open command prompt as an administrator and run the following command:
 - `iisreset`The command resets the internet information server.
- To restart Microsoft SharePoint Search Service, run the following commands in the listed order ,
 - `net stop spsearchhostcontroller`
 - `net start spsearchhostcontroller`
 - `net stop oseach15`
 - `net start oseach15`

Configure AEM forms IFilter

This section details the steps to set up AEM forms IFilter (to index and search Document Security protected PDF documents) with SharePoint/FAST Search Server, while using mutual authentication with the Document Security server.

Note: The configuration steps described in this section need to be carried out on a system where SharePoint/FAST Search Server is installed.

Prerequisites

- **Install the client certificate used to authenticate against AEM forms server on SharePoint/FAST Search Server.**

To ensure that the client certificate has been installed successfully, do one of the following:

- Open an Document Security protected PDF document using Adobe Reader or Acrobat
- Access the Document Security end-user web application. Open this URL [https://\[hostname\]:\[port\]/edc/Login.do](https://[hostname]:[port]/edc/Login.do) in web browser. Authentication should use the client certificate by default

- **Enable Windows Search Service on SharePoint/FAST Search Server.**

To configure the Windows Search Service, follow the steps in the following article:

<http://www.win2008workstation.com/win2008/enable-windows-search-service>

To ensure that Windows Search Service has been enabled, check that mssprxy.dll is present in C:\windows\system32 directory.

Client Certificate Configuration

When you install a client certificate (by double-clicking the certificate), it is typically installed in the personal store of the current user. However, the AEM forms IFilter service requires that:

1. The client certificate must be installed in the personal store of LOCAL_MACHINE.
2. The AEM forms IFilter solution has permissions to access the certificate.

To make the configuration changes to the installed certificate, a Certificate Configuration tool, WinHttpCertCfg.exe, from Microsoft has to be used. This tool is part of Windows Server Resource Kit Tools and can be downloaded from:

<http://www.microsoft.com/en-us/download/details.aspx?id=17657>

For further details on WinHttpCertCfg.exe, see:

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa384088\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384088(v=vs.85).aspx)

Configure Client Certificate for AEM forms IFilter Service

After you have downloaded and installed the Windows Server Resource Kit Tools, use the Certificate Configuration tool (WinHttpCertCfg.exe) present in the C:\Program Files (x86)\Windows Resource Kits\Tools directory to configure the client certificate as required by the AEM forms IFilter solution.

1. Export the client certificate installed earlier from Internet options or the Certificate Manager Tool (Certmgr.msc) to a PFX file.

Ensure that the private key is also exported.

Note: Ensure that you use the same name of the PFX file created above, in all the subsequent steps described in the document.

2. To install the client certificate in the personal store of LOCAL_MACHINE, open the command prompt in elevated mode (with administrator privileges) and execute the following command:

```
WinHttpCertCfg.exe -i <PFX file name>.pfx -c LOCAL_MACHINE\My -a <Account> -p <PFX password>
```

where

<PFX file name> is the client certificate exported in previous step

<Account> is the user account on the machine being configured

<PFX password> is the password which is used to import the certificate and the private key

Example

```
WinHttpCertCfg.exe -i <Exported client certificate file name> -c LOCAL_MACHINE\My -a username -p password
```

3. To grant AEM forms IFilter service permissions to access the client certificate, open the command prompt in elevated mode (with administrator privileges) and execute the following command:

```
WinHttpCertCfg.exe -g -c LOCAL_MACHINE\MY -s <SubjectStr> -a "LOCAL SERVICE"
```

where

<SubjectStr> is a case-insensitive search string for finding the first enumerated certificate with a subject name that contains this substring.

Example

```
WinHttpCertCfg.exe -g -c LOCAL_MACHINE\MY -s smith -a "LOCAL SERVICE"
```

Client Certificate Registry Setting

SharePoint indexing/crawling service uses the client certificate to authenticate against Document Security Server. This client certificate needs to be specified in the registry.

To configure the certificate, add a registry setting:

Type: REG_SZ

Name: Thumbprint SHA1 Hash

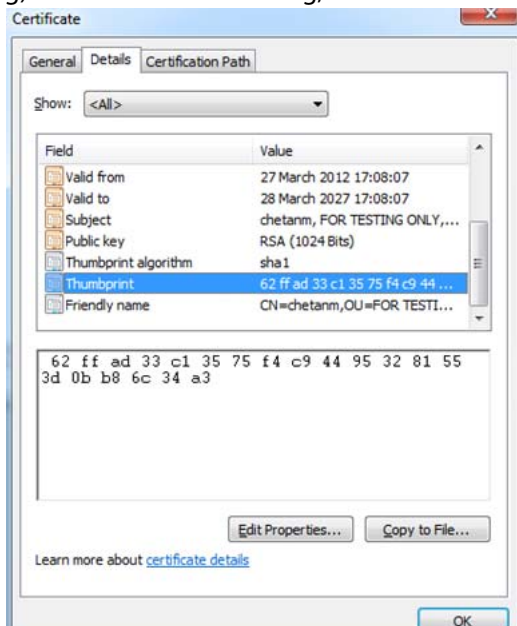
Registry Location: HKLM\Software\Adobe\LiveCycle IFilter\Certificate Settings.

Value: <Thumbprint SHA1 Hash of the client certificate>

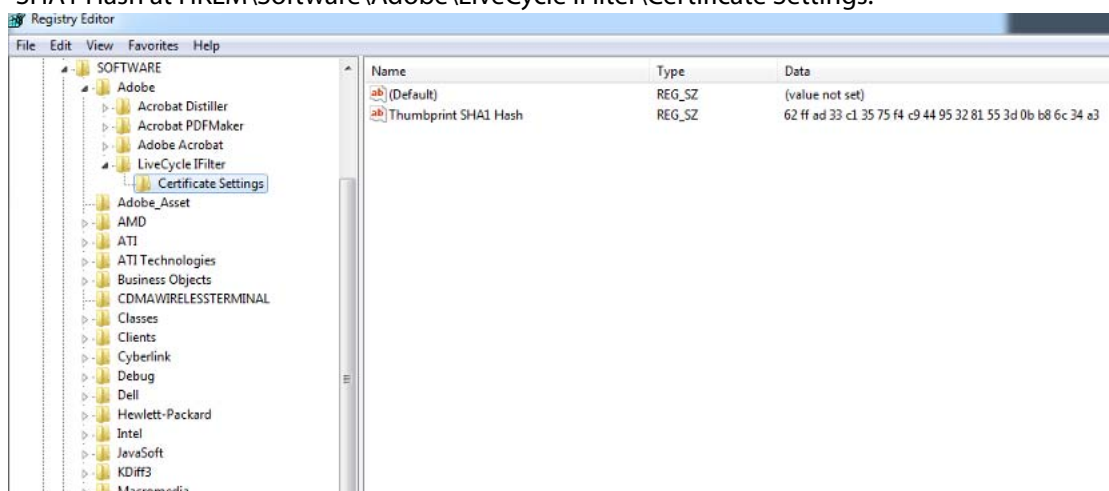
To obtain the SHA1 Hash value:

- e). Open certmgr.msc or Internet Options in Internet Explorer.
The list of certificates installed on the system are displayed.
- f). Double-click the client certificate for which you need to obtain the SHA1 Hash value.
The Certificate dialog displays.

g). In the Certificate dialog, click the Details tab and select the Thumbprint field.



h). Copy the value of the Thumbprint field and paste this value in the registry field Thumbprint SHA1 Hash at HKLM\Software\Adobe\LiveCycle IFilter\Certificate Settings.



Note: Ensure that while copying the Thumbprint value from the certificate, no extra spaces/characters are copied.

Configure SharePoint/FAST Search Server for SharePoint to use AEM forms IFilter

To configure SharePoint/FAST Search Server to use AEM forms IFilter, follow the steps in the article: <http://msdn.microsoft.com/library/ff795798.aspx>

You can now use SharePoint/FAST Search Server to index and search Document Security protected PDF documents.

The following section describes a set of steps to follow if you are unable to get your IFilter solution up and running.

Troubleshooting AEM forms IFilter

This section details sequential steps you need to follow if you are unable to index Document Security protected PDF documents using the IFilter solution. The section describes a set of scenarios to test. If you do not get the expected results, you need to follow the troubleshooting steps to resolve the specific issue.

Important: The steps described in this section must be carried out sequentially.

Opening Document Security protected PDF documents in Acrobat/Reader

On the SharePoint/FAST Search Server, open an Document Security protected PDF document (in Acrobat/Reader) which uses Mutual Authentication.

Expected result

The document should open without requiring any explicit authentication.

Troubleshooting

If the document does not open.

1. Verify the server configuration.
2. Verify that the user whose certificate is installed on the system has required permissions to open the document.

Run iFiltTst on an unprotected document

Run iFiltTst on an unprotected document using the command `ifiltst.exe /i <file-name> /v 3 /d`.

Note: iFiltTst is an IFilter Test Suite and can be downloaded from the Microsoft Website.

Along with iFiltTst.exe another file iFiltTst.ini is present in the same directory. This ini file defines the tests to be run on the document. This file is a necessary pre-requisite for running iFiltTst cases. Test No. 1 is sufficient for sanity testing. Tests 2 - 6 can be commented out in the iFiltTst.ini file.

Expected results

1. iFiltTst.exe should not display any error message on the console.
2. A non-zero size <file-name>.dmp file should be created. The dmp file should contain text of the unprotected PDF document.

Troubleshooting

1. Ensure that the command prompt running iFiltTst.exe has administrative privileges.
2. Ensure that mssprxy.dll is present on the system at C:\windows\system32.

This is part of the Windows Search Service. If this dll is not present, then enable Windows Search Service as described in [Prerequisites](#) section of this document.

3. Ensure that the AEM forms IFilter service is running on the system.
 - a). To view the list of services running on the system, open the Microsoft Management Console. To open the console, type `services.msc` in the Windows Run dialog box and click OK.

- b). Verify that the AEM forms IFilter service is listed in the Microsoft Management Console and the status is set to Started.

Run iFiltTst on a protected PDF document

Run iFiltTst on an Document Security protected PDF document using the command `ifiltst.exe /i <file-name> /v 3 /d`.

Note: iFiltTst is an IFilter Test Suite and can be downloaded from the Microsoft Website.

Along with iFiltTst.exe another file iFiltTst.ini is present in the same directory. This ini file defines the tests to be run on the document. This file is a necessary pre-requisite for running iFiltTst cases. Test No. 1 is sufficient for sanity testing. Tests 2 - 6 can be commented out in the iFiltTst.ini file.

Expected results

1. iFiltTst.exe should not display any error message on the console.
2. A non-zero size `<file-name>.dmp` file should be created. The dmp file should contain the text contents of the PDF document.

Troubleshooting

1. Ensure that the command prompt running iFiltTst.exe has administrative privileges.
2. Ensure that Apache Proxy is disabled in IFilter.
The registry value `HKLM\Software\Adobe\PDF Filter\LiveCycle Rights Management\Http Proxy Settings\HttpProxyEnable` should either be absent or set to 0.
HttpProxyEnable is of type REG_DWORD.
3. Ensure that the user whose certificate is installed on the system has Copy permission on the Document Security protected PDF document.
4. Ensure the firewall settings are not blocking network traffic to Rights Management server.
5. Ensure that the AEM forms IFilter service is running on the system.

a). To view the list of services running on the system, open the Microsoft Management Console. To open the console, type `services.msc` in the Windows Run dialog box and click OK.

b). Verify that the AEM forms IFilter service is listed in the Microsoft Management Console and the status is set to Started.

Run Indexing for a protected PDF document

Upload an Document Security protected PDF document on the SharePoint server and run indexing.

Expected results

1. The crawl logs should indicate that the indexing of the Document Security Protected PDF documents is successful.
2. The contents of the Document Security protected PDF document should be searchable.

Troubleshooting

1. Ensure you are able to index/search unprotected PDF documents.

If you are unable to index/search unprotected PDF documents, follow the instructions at:

[Configure Client Certificate for AEM forms IFilter Service](#)

2. Ensure the firewall settings are not blocking network traffic to Rights Management server.
3. Ensure that the AEM forms IFilter service is running on the system.
 - a). To view the list of services running on the system, open the Microsoft Management Console. To open the console, type services.msc in the Windows Run dialog box and click OK.
 - b). Verify that the AEM forms IFilter service is listed in the Microsoft Management Console and the status is set to Started.
4. If warning messages related to Timeouts are seen in the crawl logs of the SharePoint/FAST Search Server for Document Security protected PDF documents then try increasing the timeout value of crawler.

Known Limitations

- During a Crawl on SharePoint/FAST Search Server, if any corrupted files are found in the crawl, the crawl operation may not be performed on some non-corrupt files as well.

Resolution

If the non-corrupt files are crawled again, crawling would be successful.

- If you have large files (a file with size around 20 MB is considered large) or have a large number of chunks, the indexing for such files might fail. The issue occurs due to process time-out or out of memory problems.