Foxit PDF Secure RMS Protector

(SharePoint Extensions)

User Manual

© 2011 Foxit Corporation

All rights reserved.

Copyright © 2011 Foxit Corporation. All Rights Reserved.

No part of this document can be reproduced, transferred, distributed or stored in any format without the prior written permission of Foxit.

Anti-Grain Geometry - Version 1.1

Copyright (C) 2002-2005 Maxim Shemanarev
(http://www.antigrain.com)

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Contents

Chapter 1 - Overview 5
Chapter 2 - Getting Started 6
System Requirements for MOSS 2007 6
System Requirements for MOSS 2010 6
Corresponding permissions of Foxit PDF Secure RMS Reader and MOSS .. 7
Installing Foxit PDF Secure RMS Protector on a SharePoint Server 7
Uninstalling Foxit PDF Secure RMS Protector 11
Check the version of Foxit PDF Secure RMS Protector 12
Chapter 3 - Configuring AD RMS to Work with SPS-SRV 13
For MOSS 2007 13
To add SPS-SRV to Local Intranet 13
To add SPS-SRV to the AD·RMS Certification Pipeline 13
To activate Information Rights Management in Office SharePoint Server 2007 14
To restrict permissions using AD·RMS 14
For MOSS 2010 14
To add SPS-SRV to Local Intranet 14
To add SPS-SRV to the AD·RMS Certification Pipeline 15
To activate Information Rights Management in Office SharePoint Server 2010 15
To restrict permissions using AD·RMS 16
Chapter 4 - Working with Foxit PDF Secure RMS Protector. 17
For MOSS 2007 17
To add the domain user to SharePoint site 17
To set the group permission in SharePoint site 17
To restrict the print permissions using RMS 19
For MOSS 2010 21
To add the domain user to SharePoint site 21
To set group permission in SharePoint site 22
To restrict the print permissions using RMS 24
Chapter 5 - For Exchange 2010 27
Getting Started 27
System requirements 27
Corresponding permissions of Foxit PDF Secure RMS Reader and Exchange 27
Installing Foxit PDF Secure RMS Protector on an Exchange Server ... 27
Uninstalling Foxit PDF Secure RMS Protector 29
Check the version of Foxit PDF Secure RMS Protector 30
Configuring AD·RMS to Integrate with Exchange Server 2010 in a Single Forest 31

To register a service connection point 31
To give Exchange servers permissions to access the server certification pipeline 32
To set up the Exchange Server super users group 33
To set InternalLicensingEnable true by ExchangeManagement Shell . 33
Working with Foxit PDF Secure RMS Protector..... 34
Chapter 6 - FAQ 38
Contact Us 39

Chapter 1 - Overview

Traditionally, sensitive information can only be controlled by limiting access to the networks or computers where the information is stored. After access is given to users, however, there are no restrictions on what can be done with the content or to whom it can be sent. Microsoft Information Rights Management (IRM) enables you to create a persistent set of access controls that live with the content, rather than a specific network location, which will help you control access to files even after they leave your direct control.

Foxit PDF Secure RMS protector extends all the benefits of AD RMS to any PDF document. In addition, Foxit PDF Secure RMS protector provides creation and control of rights to unique PDF features.

Microsoft's Active Directory Rights Management (AD • RMS) solves security problems for enterprise documents created in Microsoft Office. With the inclusion of AD RMS in Windows Server2008, AD RMS has quickly become the default standard for document rights protection.

For the enterprises, they can enforce security policies easily to protect sensitive information, as well as enable each PDF document with additional features such as forms fill out and annotations.

Chapter 2 - Getting Started

This section provides system requirements, install and uninstall instructions for the RMS Protector.

System Requirements for MOSS 2007

Computer	Operating System	Requirement
RMS Server/ ADRMS Server	Windows Server •2003 with Service Pack • 1 (SP1)/Windows Server • 2008 with Service Pack • 1 (SP1)	RMS, Internet Information Services (IIS) 6.0, World Wide Web Publishing Service, Message Queuing (also known as MSMQ), and Microsoft SQL Server™ • 2005 Standard Edition
DC	Windows Server •2003 with SP1	Active Directory, Domain Name System (DNS)
ADRMS-DB	Windows • Server • 2003 with SP1	Microsoft SQL Server™ • 2005 with Service Pack • 2 (SP2)
SharePoint Server Such as named SPS-SRV	Windows Server •2003 with SP1	Office SharePoint Server • 2007 with RMS Client installed, and has been added this Server to DC

System Requirements for MOSS 2010

Computer	Operating System	Requirement
ADRMS Server	Windows Server •2008 with Service Pack • 1 (SP1)	RMS, Internet Information Services (IIS) 6.0, World Wide Web Publishing Service, Message Queuing (also known as MSMQ)
DC	Windows Server •2003 with SP1	Active Directory, Domain Name System (DNS)
ADRMS-DB	Windows • Server • 2008 with SP1	Microsoft SQL Server™ •2008 R2
SharePoint Server Such as named SPS-SRV	Windows Server •2008 with SP2	Office SharePoint Server • 2010 and has been added this Server to DC

Corresponding permissions of Foxit PDF Secure RMS Reader and MOSS

SharePoint service provides three levels rights: Full control, Change, and Read.

Level	Rights of Foxit PDF Secure RMS Reader
Full control	View, Copy, Modify, Print, View Data, Access, Annotate, Fill Form, Assemble
Change	View, Copy, Modify, Access, Annotate, Fill Form, Assemble
Read	View

The user only can print the document if its library IRM settings have been configured to allow document printing.

Installing Foxit PDF Secure RMS Protector on a SharePoint Server

To install Foxit PDF Secure RMS Protector:

- Stop the IIS Admin service: Start > Settings > Control Panel > Administrator Tools > Services > IIS Admin Service > Stop. Then Close the window.
- Run the Foxit PDF Secure RMS Protector Setup program to install the protector on the server.

- Download PDF icon from http://www.foxitsoftware.com/pdf/ifilter/pdficon.gif.
- For MOSS 2007,

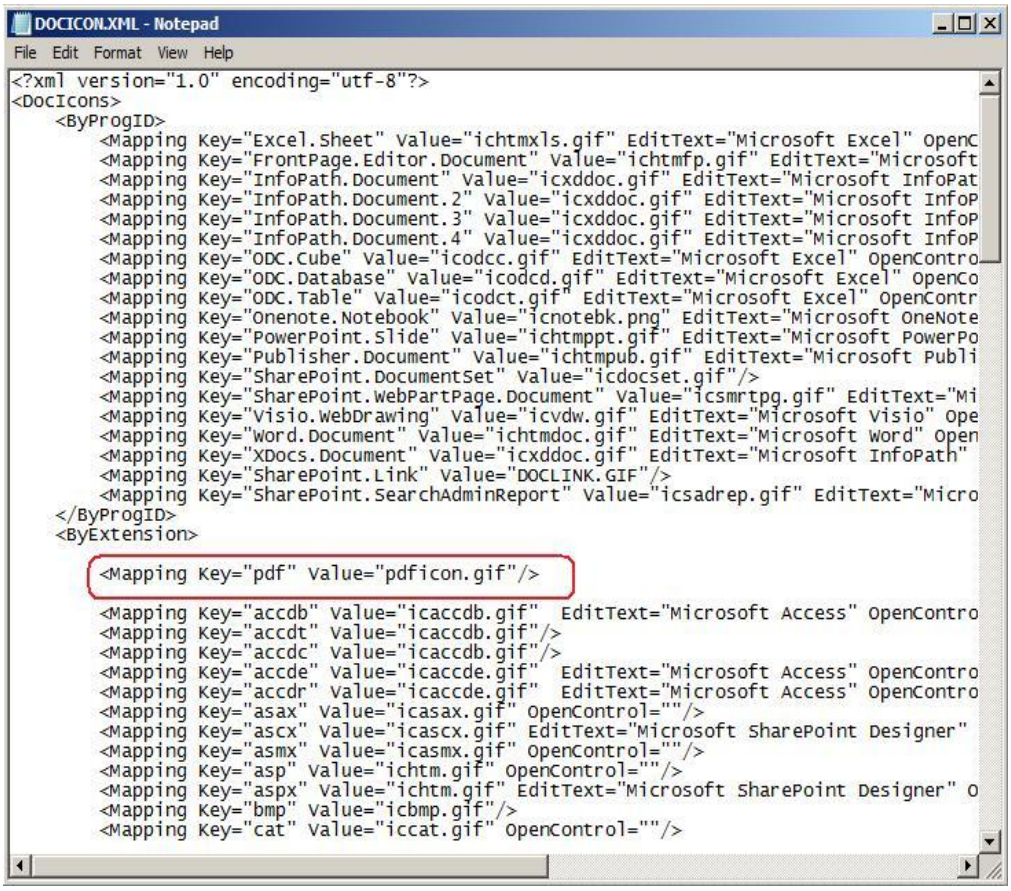
1. copy the downloaded.GIF file to "Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Template\Images".

2. Edit the file "Drive:\Program Files\Common Files\Microsoft Shared\Web server extensions\12\Template\Xml\DOCICON.XML":

   a. Right-click DOCICON.XML file > click Open With > select Notepad.

   b. Add an entry for the .pdf extension as the file's name. For example, type the ICPDF as the name of the .gif file:

   <Mapping Key="pdf" Value="pdficon.gif"/>



c. Click Save on the File menu, and then quit Notepad.

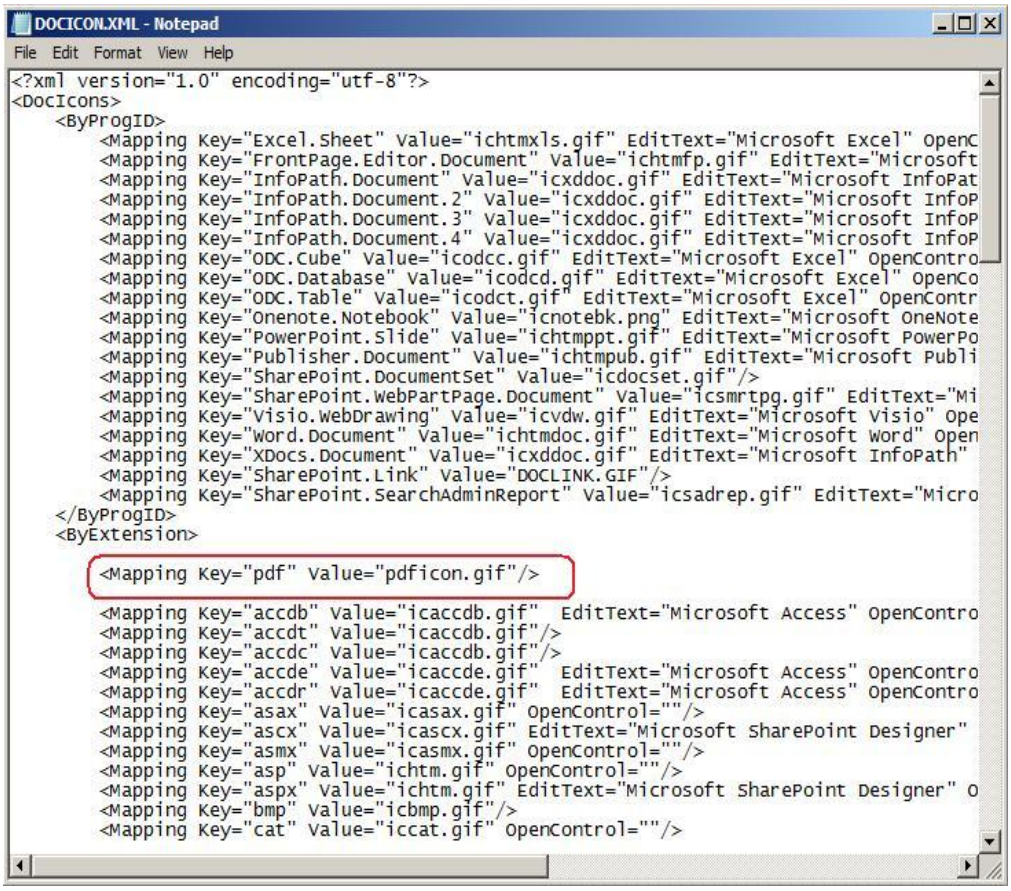
- For MOSS 2010,

1. copy the downloaded.GIF file to "Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\Template\Images"
2. Edit the file “Drive:\Program Files\Common Files\Microsoft Shared\Web server extensions\14\Template\Xml\DOCICON.XML”:

   a. Right-click DOCICON.XML file > click Open With > select Notepad.

   b. Add an entry for the .pdf extension as the file’s name. For example, type the ICPDF as the name of the .gif file:

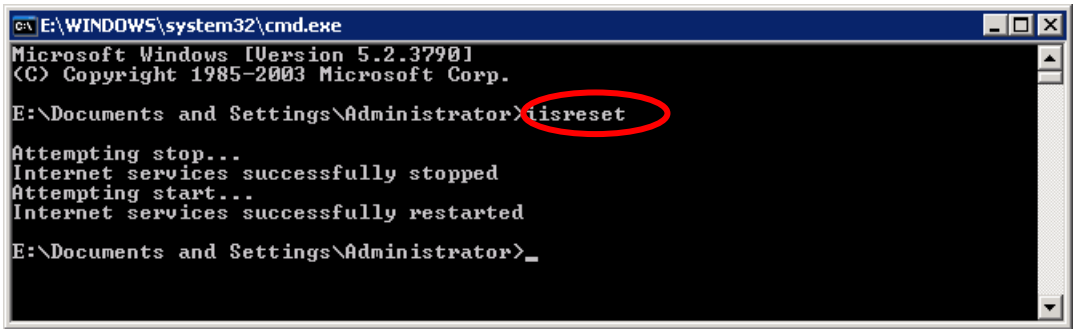
   <Mapping Key="pdf" Value="pdficon.gif"/>



c. Click Save on the File menu, and then quit Notepad.

3. Perform an iisreset:

1. Click Start > Run > type "cmd" in the Open dialog box> click OK > type "iisreset" at the command prompt > Enter.



2. Close the windows.

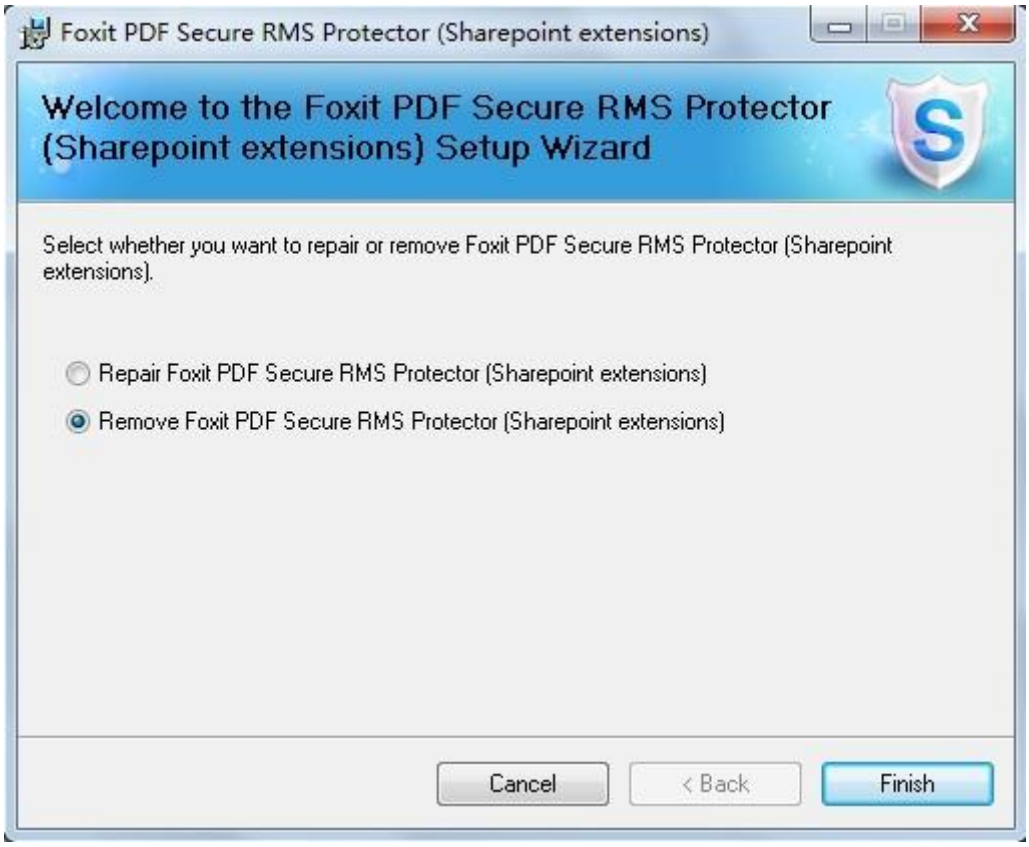
Uninstalling Foxit PDF Secure RMS Protector

To uninstall:

- Open the Start Menu > Settings > select "Control Panel".
- Click the "Add or Remove Programs" tab.
- Click the "Foxit PDF Secure RMS Protector" record and then click the "Remove/Uninstalled" button to uninstall it.

Or you can double-click the SharePointPDFProtector.msi setup file that you have used to install Foxit PDF Secure RMS Protector, and perform the following:

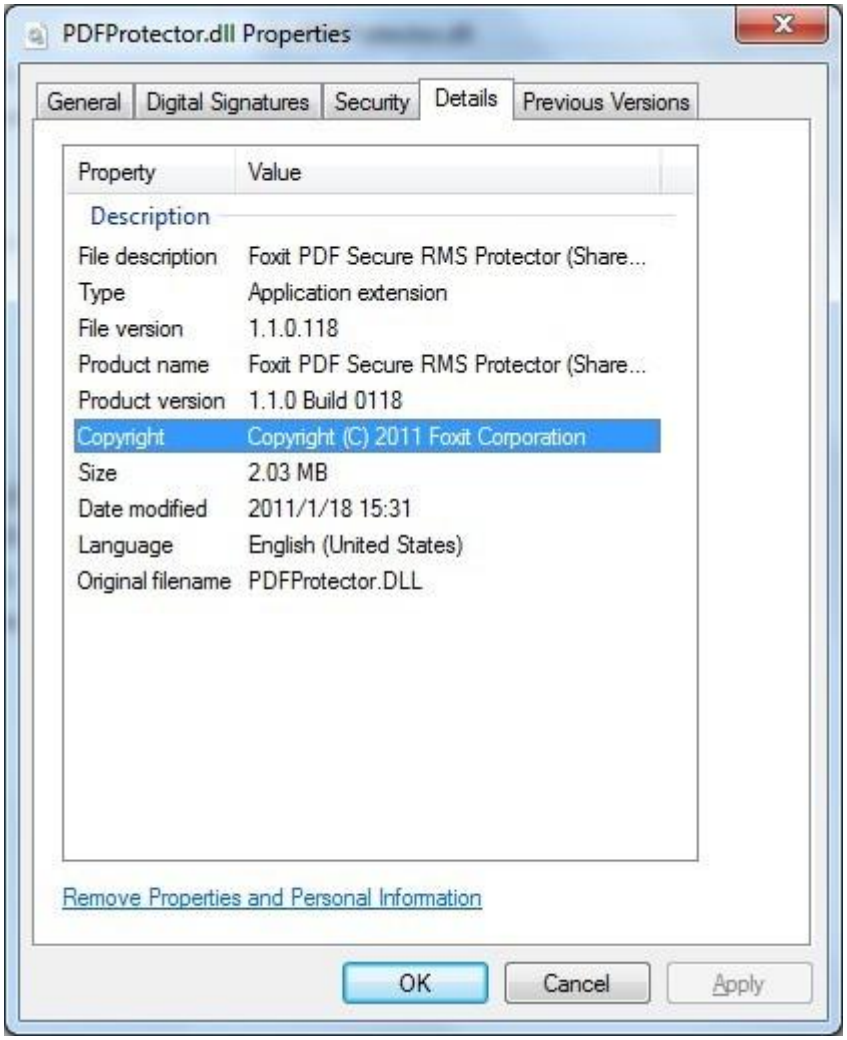
- In the Foxit PDF Secure RMS Protector dialog box, select Remove Foxit PDF Secure RMS Protector



- Click Finish button to complete removal.

Check the version of Foxit PDF Secure RMS Protector

- Please navigate to the folder where Foxit PDF Secure RMS Protector installed. Right-click PDFProtector.dll > choose Properties > click the Details tab, then you can examine the version information of Foxit PDF Secure RMS Protector:



Chapter 3 - Configuring AD RMS to Work with SPS-SRV

Note: If you have configured AD • RMS when you were installing SharePoint, please skip this chapter.

For MOSS 2007

To add SPS-SRV to Local Intranet

- Log on SPS-SRV as domain administrator, e.g., WIONS\administrator.
- Click **Start**. Point to **Control Panel**, and then click **Internet Options**.
- Click the **Security** tab, and choose **Local Intranet**, and then click the **Sites** button
- Type **http://SPS-SRV,** and then click **Add**. Note: SPS-SRV is the computer's name of MOSS server.
- Click **Close**, and then choose **OK**

To add SPS-SRV to the AD • RMS Certification Pipeline

4. Log on ADRMS-SRV as CPANDL\Administrator.
5. Click **Start**, and then click **Computer**.
6. Navigate to C:\Inetpub\wwwroot_wmcs\Certification.
7. Right-click **ServerCertification.asmx**, and choose **Properties**, and then click the **Security** tab.
8. Click **Advanced**>**Edit**, and select the check box **Include inheritable permissions from this object's parent**. Then click **OK** two times.
9. Click **Edit**, and then click **Add.**
10. Click **Object Types**, and select the check box **Computers**, then click **OK.**
11. Type the computer's name of MOSS server, such as **SPS-SRV**, and then click **OK.**
12. Click **OK** to close the **ServerCertification.asmx Properties** sheet.

The default Read & Execute and Read permissions are configured for the SPS-SRV computer account object and other accounts' are all inherited from the parent folder.

13. Click **Start**, and then click **Command Prompt**.
14. Type **iisreset**, and then press ENTER.

To activate Information Rights Management in Office SharePoint Server 2007

Please do the following:

15. Log on SharePoint Server as the administrator.
16. Click **Start**, and point to **Administrative Tools**, then click **SharePoint 3.0 Central Administration**.
17. Click **Operations**, and choose **Information Rights Management**.
18. Click **Use the default RMS server specified in Active Directory**.
19. Click **OK**.

To restrict permissions using AD • RMS

- Log on as CPANDL\administrator.
- Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
- Type **http://SPS-SRV** in the address bar, and then click **Go**.
- Click **Shared Documents**, and choose **Library page**, and then click **Library Settings button**.
- Under the **Permissions and Management** heading, click **Information Rights Management**.
- Select the check box **Restrict permission to documents in this library on download**.
- Type **CPANDL Protected** in the **Permissions policy title** box.
- Type **Restrict CPANDL employees from printing** in the **Permission policy description** box.
- Click **OK**.

For MOSS 2010

To add SPS-SRV to Local Intranet

- Log on SPS-SRV as domain administrator, e.g., CPANDL\administrator.
- Click **Start**, and point to **Control Panel**, then choose **Internet Options**.

- Click the **Security** tab, and choose **Local Intranet**, and then click the **Sites** button.
- Type **http://SPS-SRV,** and then click **Add**. Note: SPS-SRV is the computer's name of MOSS2010 server.
- Click **Close**, and then click **OK.**

To add SPS-SRV to the AD • RMS Certification Pipeline

20. Log on ADRMS-SRV as CPANDL\Administrator.
21. Click **Start**, and then click **Computer**.
22. Navigate to C:\Inetpub\wwwroot_wmcs\Certification.
23. Right-click **ServerCertification.asmx**, and click **Properties**, then choose the **Security** tab.
24. Click **Advanced** and choose the **Edit**. Select the check box **Include inheritable permissions from this object's parent**, and then click **OK** two times.
25. Click **Edit**, and then click **Add**
26. Click **Object Types**, select the check box **Computers**, and then click **OK**
27. Type the computer's name of MOSS server, such as **SPS-SRV**, and then click **OK**
28. Click **OK** to close the **ServerCertification.asmx Properties** sheet. The default Read & Execute and Read permissions are configured for the SPS-SRV computer account object and other accounts are all inherited from the parent folder.
29. Click **Start**, and then click **Command Prompt**.
30. Type **iisreset**, and then press ENTER

To activate Information Rights Management in Office SharePoint Server 2010

Please do the followings:

31. Log on SharePoint Server as administrator.
32. Click **Start**, and point to **Administrative Tools**, then click **SharePoint 2010 Central Administration**.
33. Click **Security (on the left)**, and then click **Configure Information Rights Management under the Information policy heading.**
34. Click **Use the default RMS server specified in Active Directory**.

35. Click **OK**.

To restrict permissions using AD • RMS

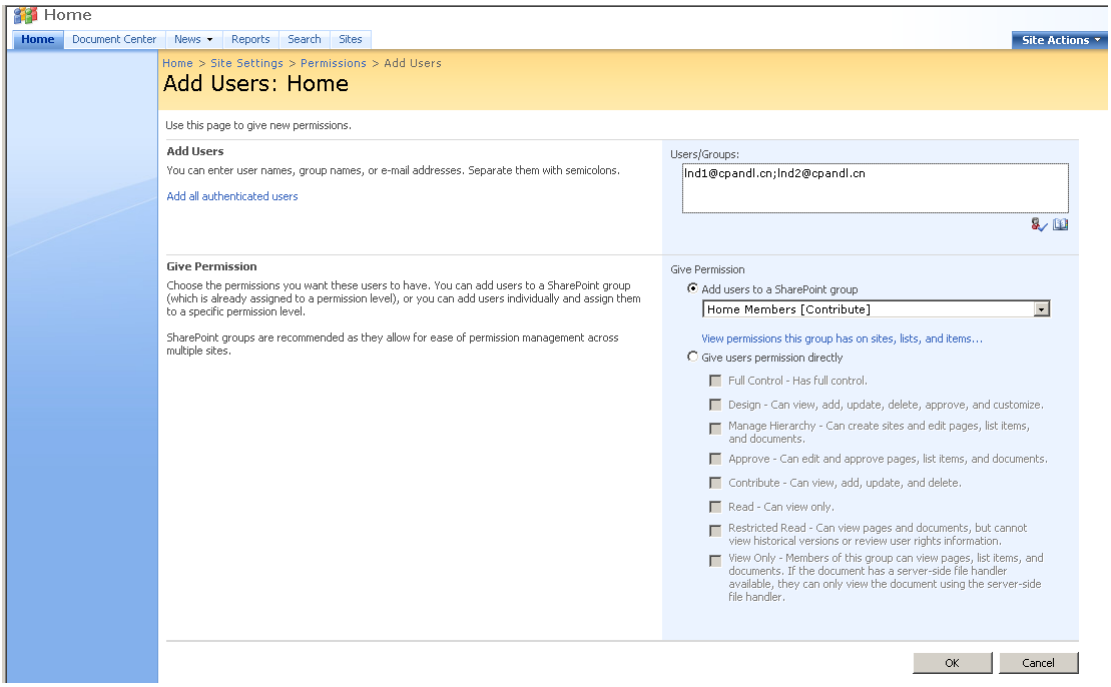
- Log on as CPANDL\administrator.
- Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
- Type **http://SPS-SRV** in the address bar, and then click **Go**.
- Click **Shared Documents**, and choose **Library page**, and then click **Library Settings button**.
- Under the **Permissions and Management** heading, click **Information Rights Management**.
- Select the check box **Restrict permission to documents in this library on download**.
- Type **CPANDL Protected** in the **Permissions policy title** box.
- Type **Restrict CPANDL employees from printing** in the **Permission policy description** box.
- Click **OK**.

Chapter 4 - Working with Foxit PDF Secure RMS Protector

For MOSS 2007

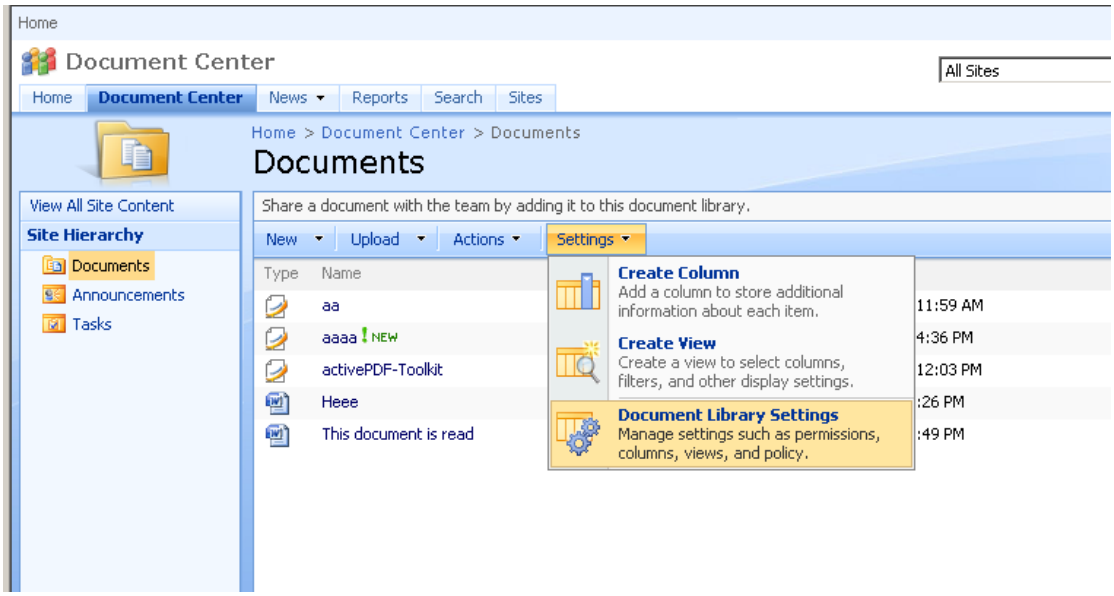
To add the domain user to SharePoint site

36. In the same Office SharePoint Server 2007 site, click **Home**.
37. Click **Site Actions** and point to **Site Settings**, and then click **People and Groups**.
38. Click **New**, and then choose **Add Users**.
39. Type domain users' names, such as **lnd1@cpandl.cn;lnd2@cpandl.cn** in the **Users/Groups** box, and then click **OK**. A list of users who have the permission to use the SharePoint will be displayed.



To set the group permission in SharePoint site

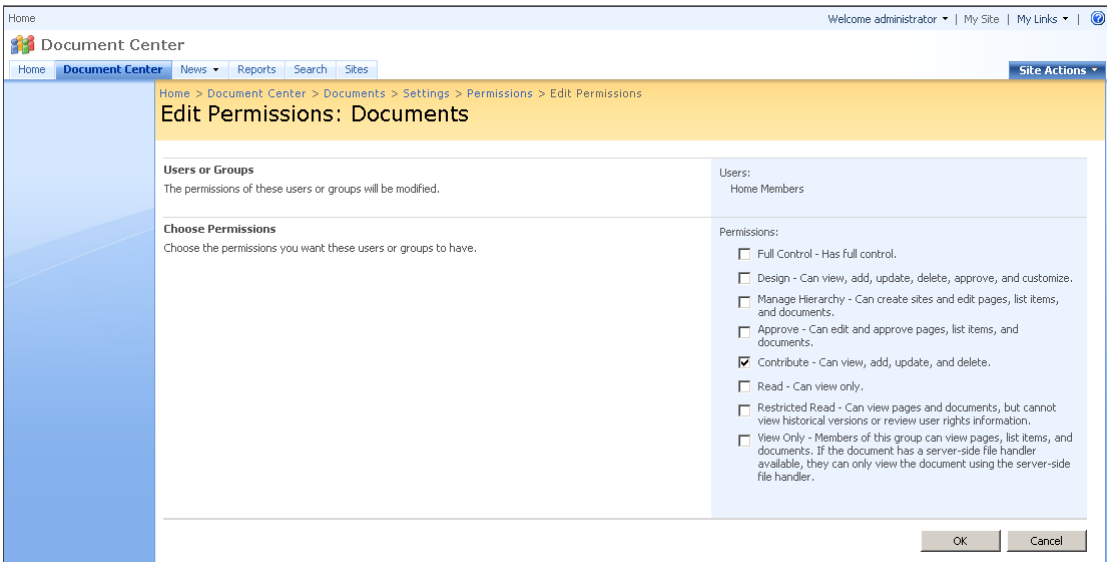
40. Navigate to the **Documents** page, log on as administrator@cpandl.com, clicking the **Settings** drop-down box and select **Document Library Settings**.



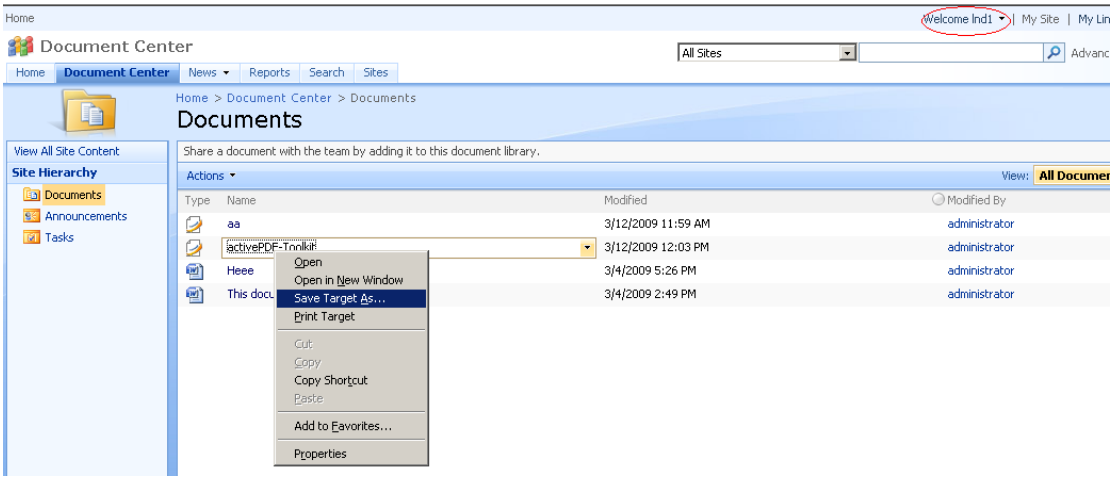
41. Click **Permissions for this document library** under Permissions and Management on the Customize Documents page.

42. Please click **Home Members** on "Permissions: Documents" page.

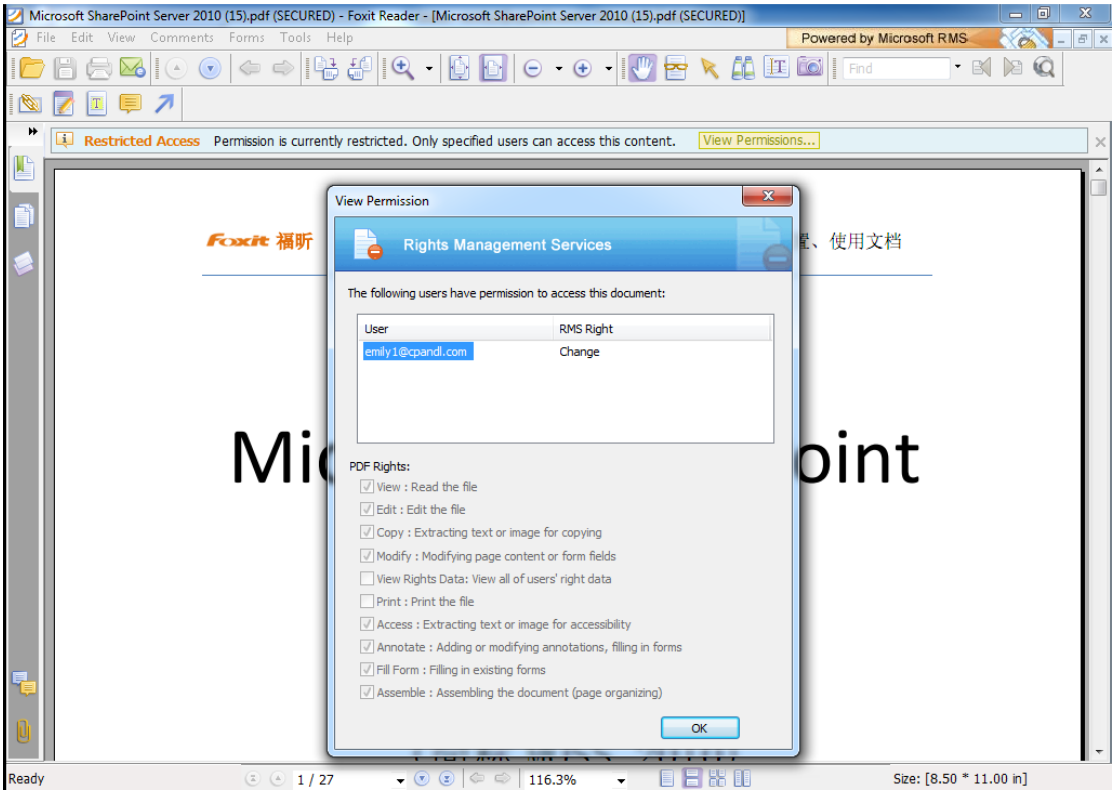
43. Please choose the permission you need, for example, you can choose the **Contribute-Can view, add, update, and delete**. Then click **OK**.



44. Return to **Documents** page, log on as lnd1@cpandl.com, to download a pdf file to your host.



45. Open the download pdf file by Foxit PDF Secure RMS Reader, and left-click **View Permission** to see the **RMS Right**.



To restrict the print permissions using RMS

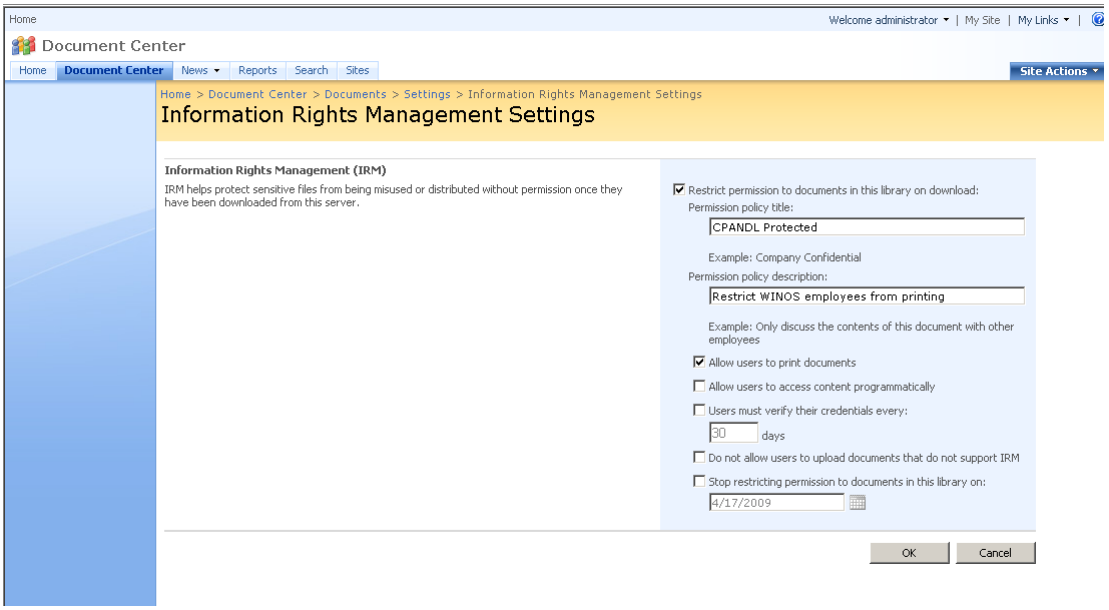
46. In the same Office SharePoint Server 2007 site, click Home.

47. Click **Document Center**, and then click **Documents.**

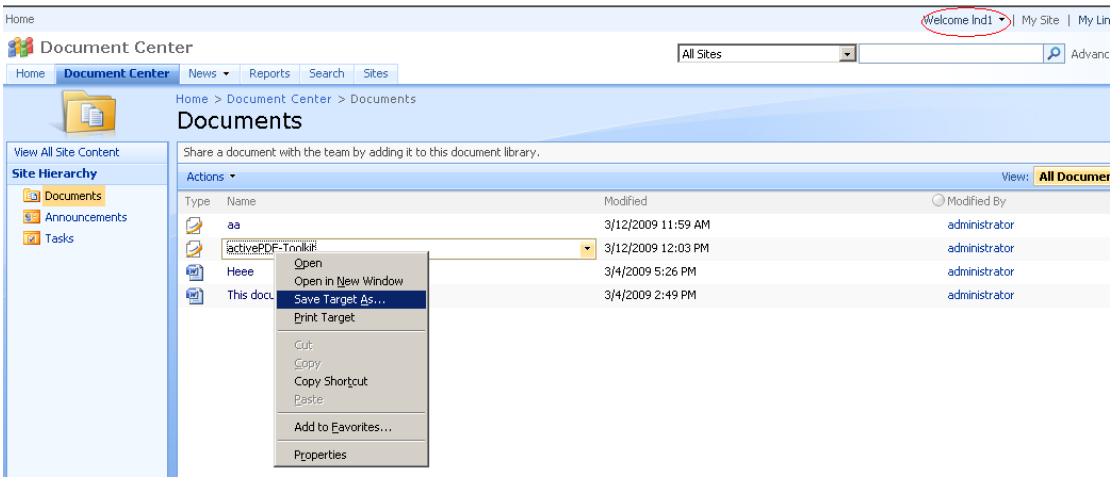
48. On the **Documents** page, left-clicking the **Settings** drop-down box and select **Document Library Settings**.

49. On settings page, choose **Information Rights Management** under Permissions and Management.

50. Choose **Allow users to print documents**, and then click **OK**.

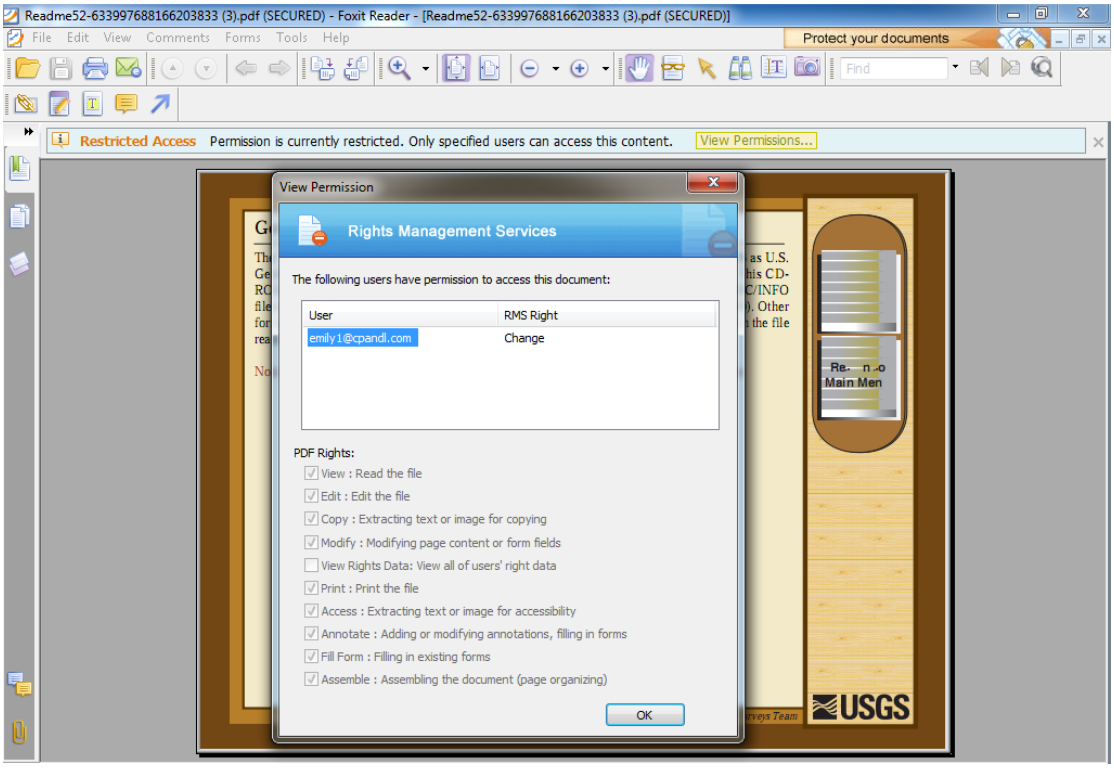


51. Return to **Documents** page, for example log on as lnd1@cpandl.cn, right-click a pdf file and **choose Save Target AS...** to save a pdf file to the local host.



52. Open the download pdf file by Foxit PDF Secure RMS Reader. Left-click **View Permission** to view the RMS Right of this file. Please see the following

picture.



For MOSS 2010

To add the domain user to SharePoint site

- Click **Start**, and point to **All Programs**, then click **Internet Explorer**.
- Type **http://SPS-SRV** in the address bar, and then click **Go**. This operation will open the default Office SharePoint Server 2010 site that was created during installation.
- Click **Site Actions**, and point to **Site Settings**, and then click **People and Groups under the Users and Permissions heading**.
- Click **New**, and then click **Add Users**.
- Type domain users' names, such as **lnd1@cpandl.cn;lnd2@cpandl.cn** in the **Users/Groups** box, and then click **OK**. A list of users who have the permissions to use the SharePoint will be displayed.

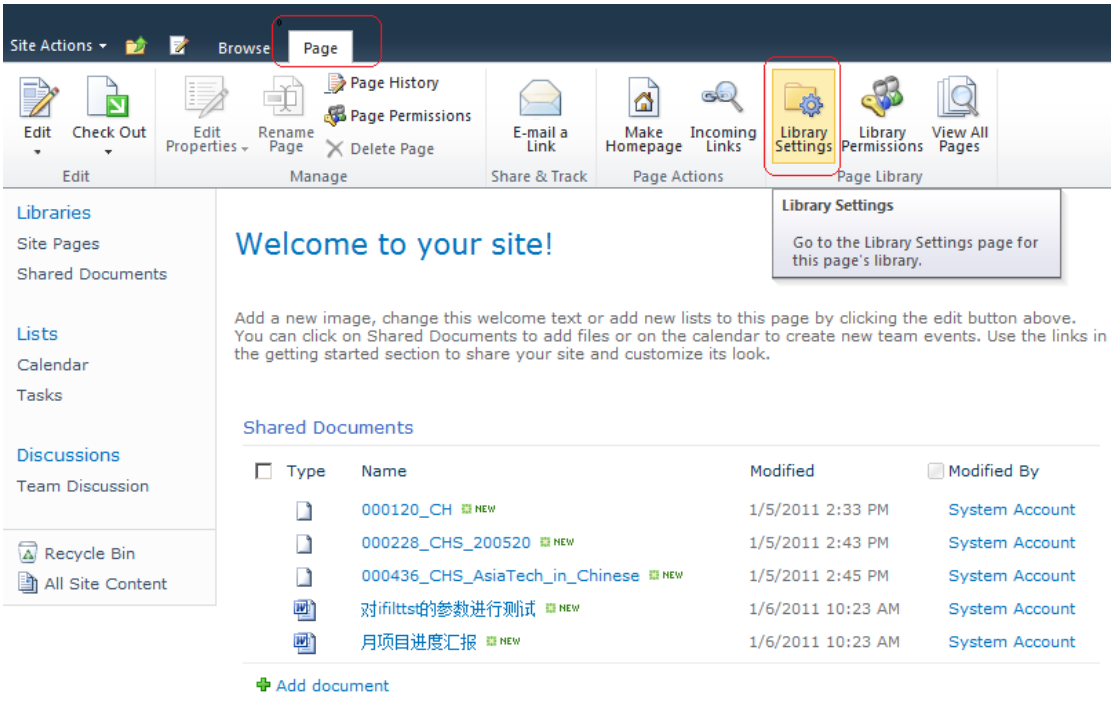
To set group permission in SharePoint site

Log on as CPANDL\Administrator.

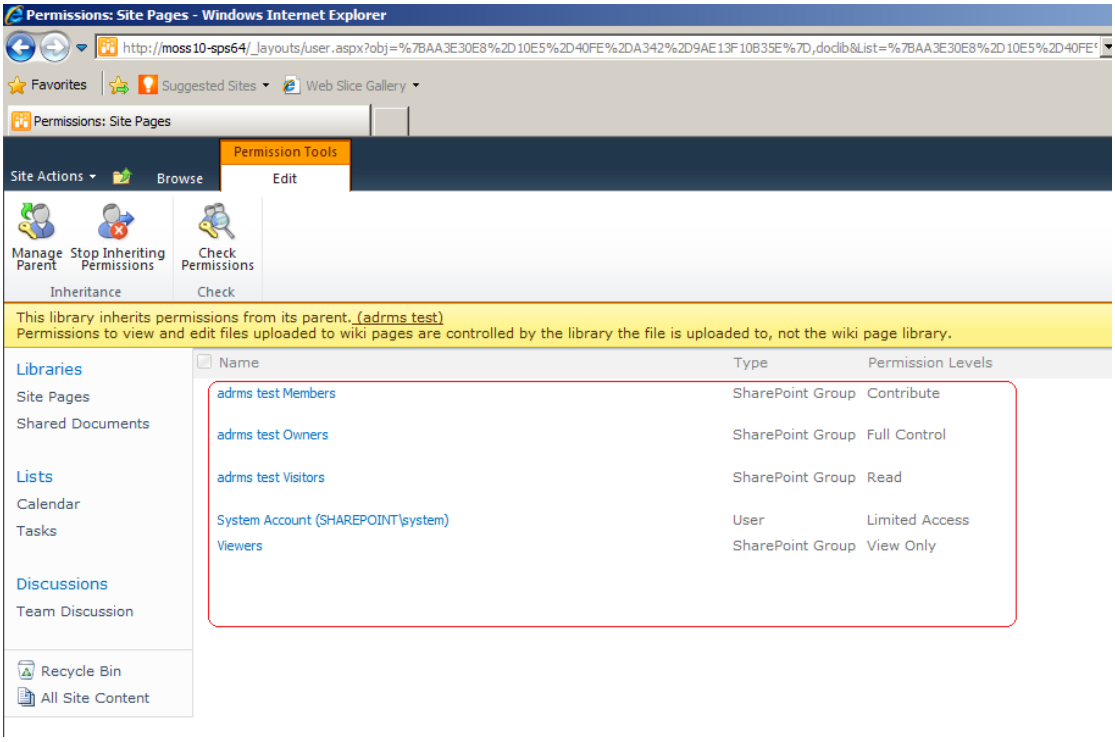
Click **Start**, and point to **All Programs**, and then click **Internet Explorer**.

Type **http://SPS-SRV** in the address bar, and then click **Go**.

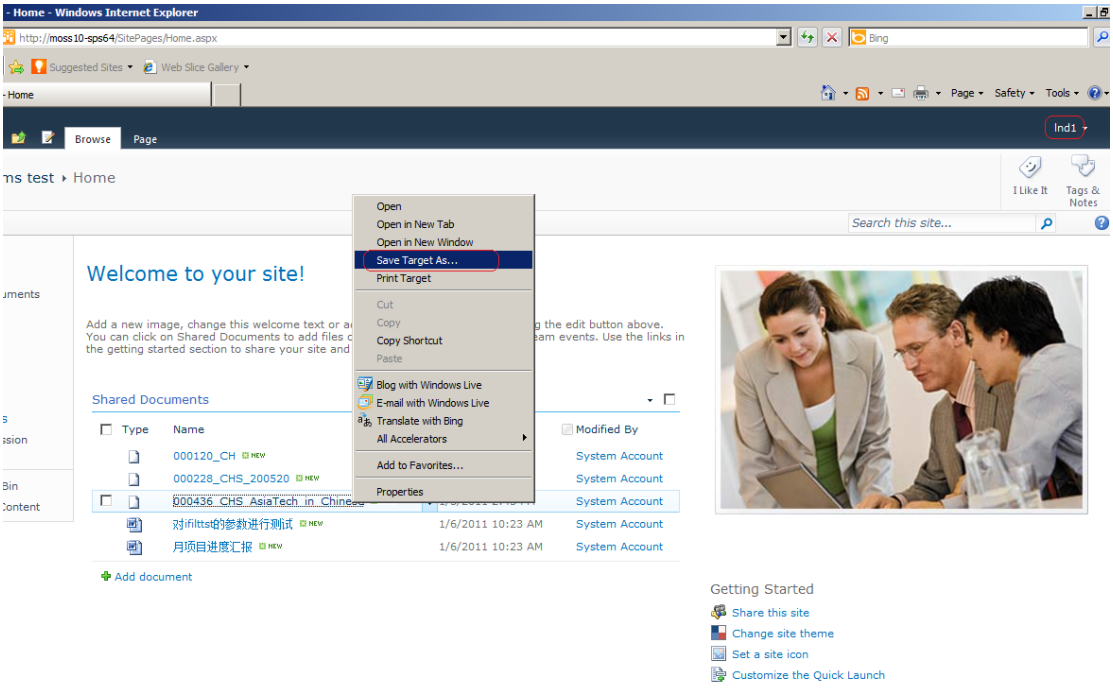
Click **Shared Documents** and **Library page**, then click **Library Settings button**.



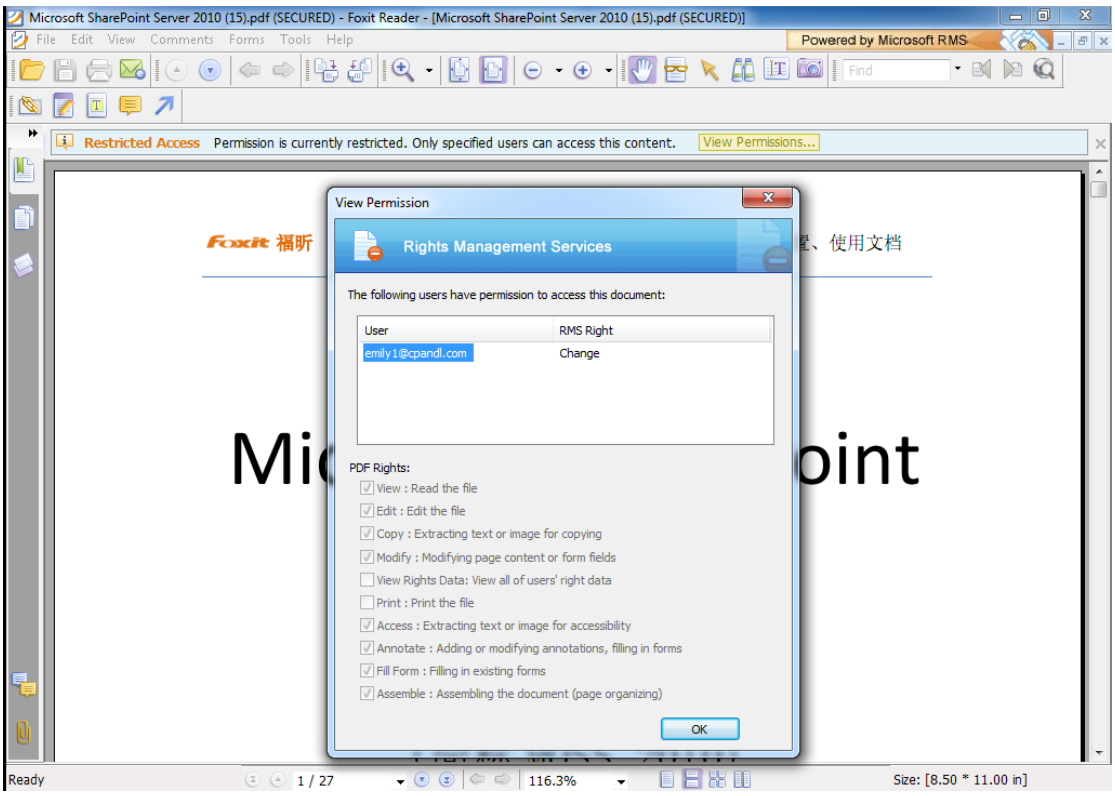
53. Click **Permissions for this document library** under Permissions and Management on Customize Documents page.



54. Return to **Shared Documents** page, log on as lnd1@cpandl.com(one of ADRMS test Members), to download a pdf file to your load host.

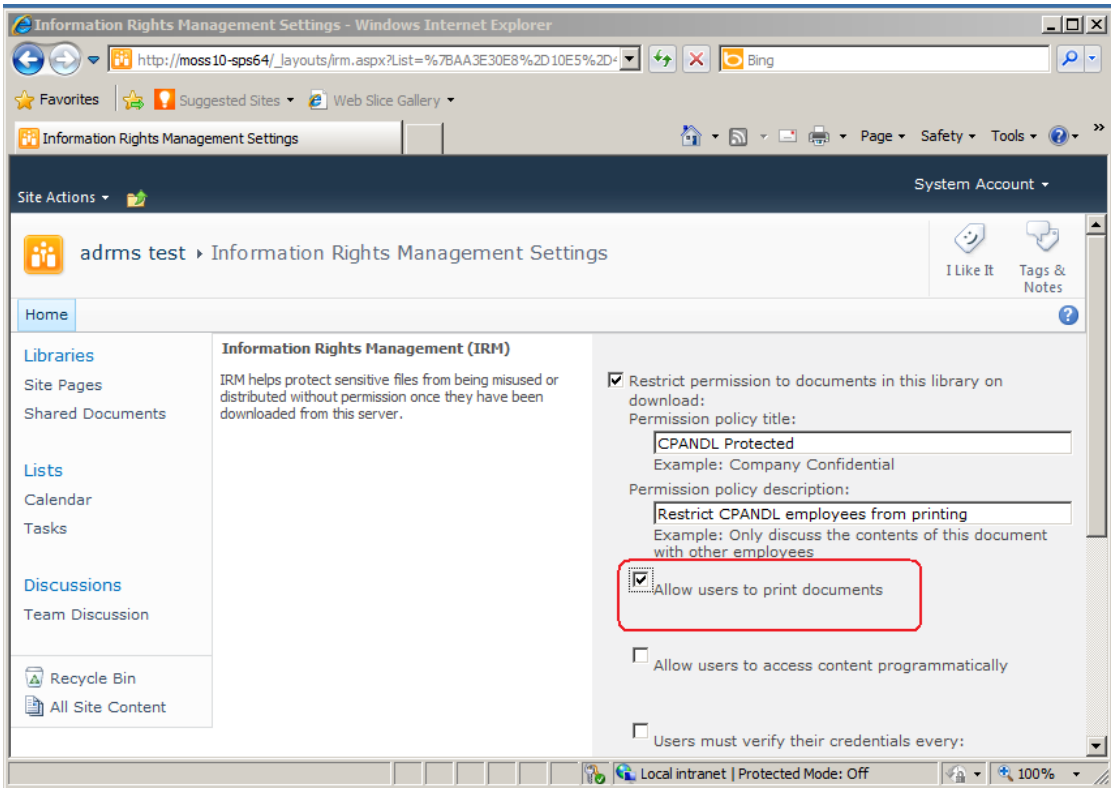


55. Open the download pdf file by Foxit PDF Secure RMS Reader, and left-click **View Permission** to see the **RMS Right**.

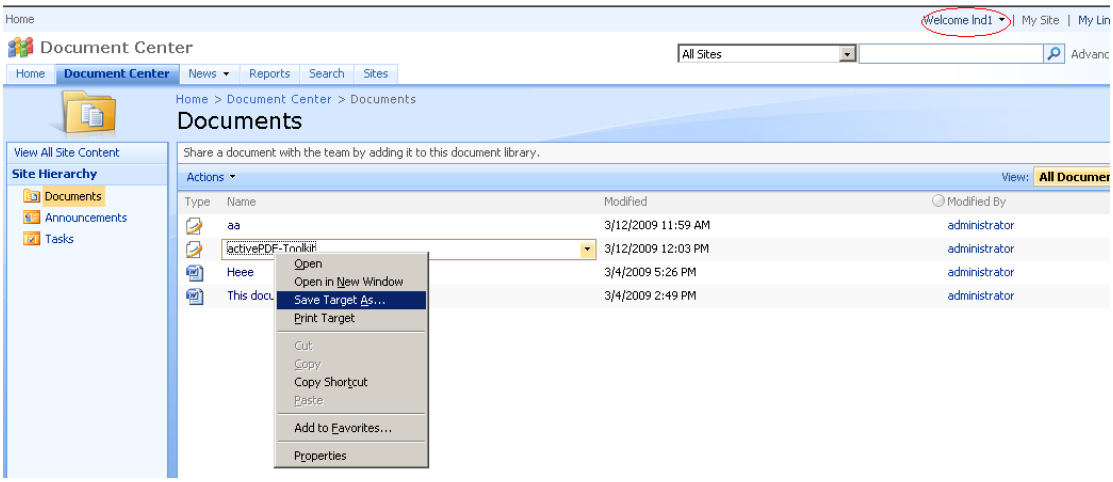
56. 

To restrict the print permissions using RMS

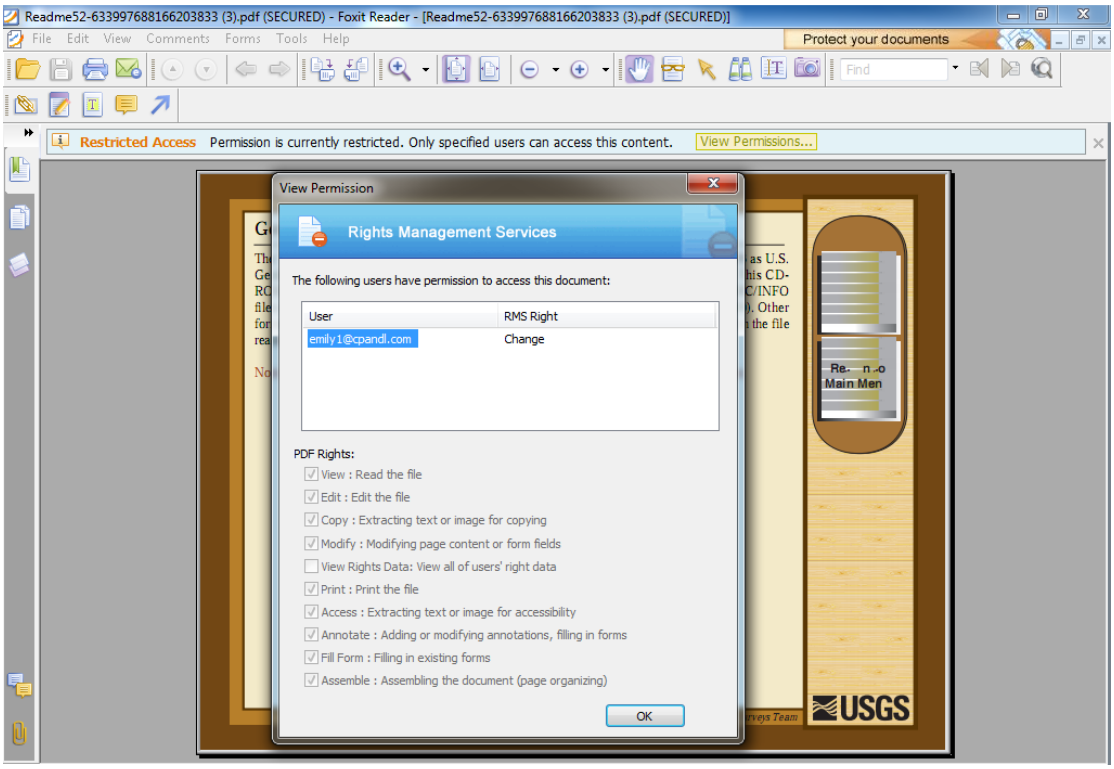
57. In the same Office SharePoint Server 2010 site, click Home.
58. Click **Shared Documents** and **Library** page**,** then click **Library Settings button**.
59. On the settings page, choose **Information Rights Management** under Permissions and Management.
60. Choose **Allow users to print documents**, and click **OK**.



61. Return to **Shared Documents** page, for example log on as lnd1@cpandl.com, and right-click a pdf file and **choose Save Target AS...** to save a pdf file to the local host.



62. Open the download pdf file by Foxit PDF Secure RMS Reader. Left-click **View Permission** to view the RMS Right of this file. Please see the following picture.


Readme52-633997688166203833 (3).pdf (SECURED) - Foxit Reader - [Readme52-633997688166203833 (3).pdf (SECURED)]
File Edit View Comments Forms Tools Help
Protect your documents
Restricted Access Permission is currently restricted. Only specified users can access this content.
View Permissions...
View Permission
Rights Management Services
The following users have permission to access this document:
User
RMS Right
emily1@cpandl.com
Change
PDF Rights:
View : Read the file
Edit : Edit the file
Copy : Extracting text or image for copying
Modify : Modifying page content or form fields
View Rights Data: View all of users' right data
Print : Print the file
Access : Extracting text or image for accessibility
Annotate : Adding or modifying annotations, filling in forms
Fill Form : Filling in existing forms
Assemble : Assembling the document (page organizing)
OK
USGS

Chapter 5 - For Exchange 2010

Getting Started

This section provides everything about getting started with Foxit PDF Secure RMS Protector you'll need to know, including its system requirements, install and uninstall instructions.

System requirements

Computer	Operating System	Requirement
ADRMS Server	Windows Server 2008 R2	RMS, Internet Information Services (IIS) 6.0, World Wide Web Publishing Service, Message Queuing (also known as MSMQ)
DC	Windows Server 2003 with SP1	Active Directory, Domain Name System (DNS)
ADRMS-DB	Windows Server 2003 with SP1	Microsoft SQL Server™ 2005
Exchange Server 2010 Such as named EX01	Windows Server 2008 with SP2 or Windows Server 2008 R2	Exchange Server 2010 and has been added this Server to DC
Client	Win7	Client , Outlook 2010

Corresponding permissions of Foxit PDF Secure RMS Reader and Exchange

Exchange service provides there levels rights: Full control, Change, Read.

Level	Rights of Foxit PDF Secure RMS Reader
Full control	View, Copy, Modify, Print, View Data, Access, Annotate, Fill Form, Assemble
Change	View, Copy, Modify, Access, Annotate, Fill Form, Assemble
Read	View

The user can only print the document if the document library IRM settings have been configured to allow document printing.

Installing Foxit PDF Secure RMS Protector on an Exchange

Server

To install Foxit PDF Secure RMS Protector:

63. Stop the IIS Admin service: Start > Settings > Control Panel > Administrator Tools > Services > IIS Admin Service > Stop. Close window.
64. Run the Foxit PDF Secure RMS Protector Setup program to install the protector on the server.

65. After installing ,restart IIS, MSExchangeTransport, msftesql-Exchange:

    1. Click Start > Run > type "cmd" in the Open line> click OK, and execute the following commands:

    net stop MSExchangeTransport

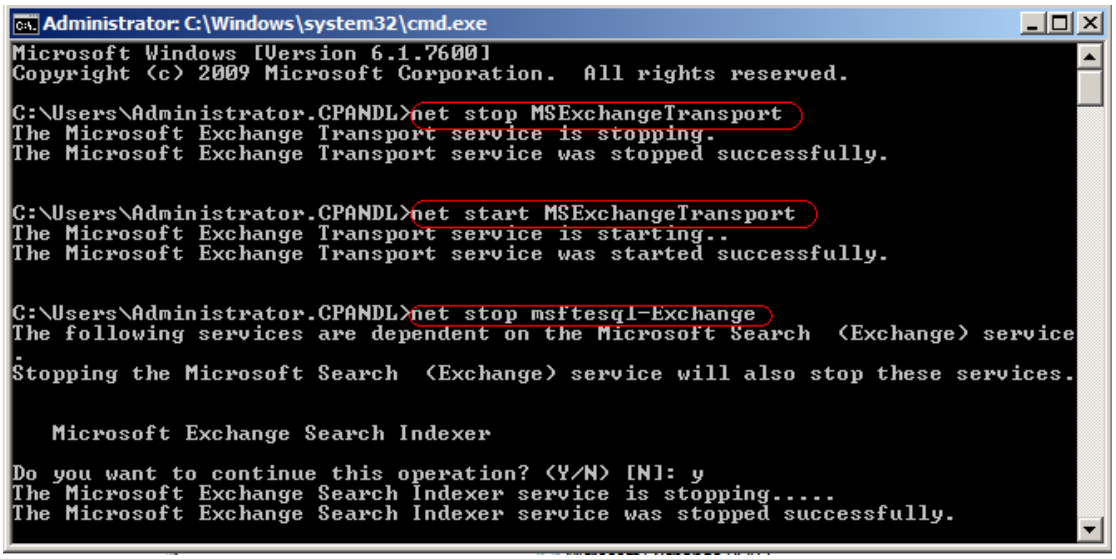
    net start MSExchangeTransport

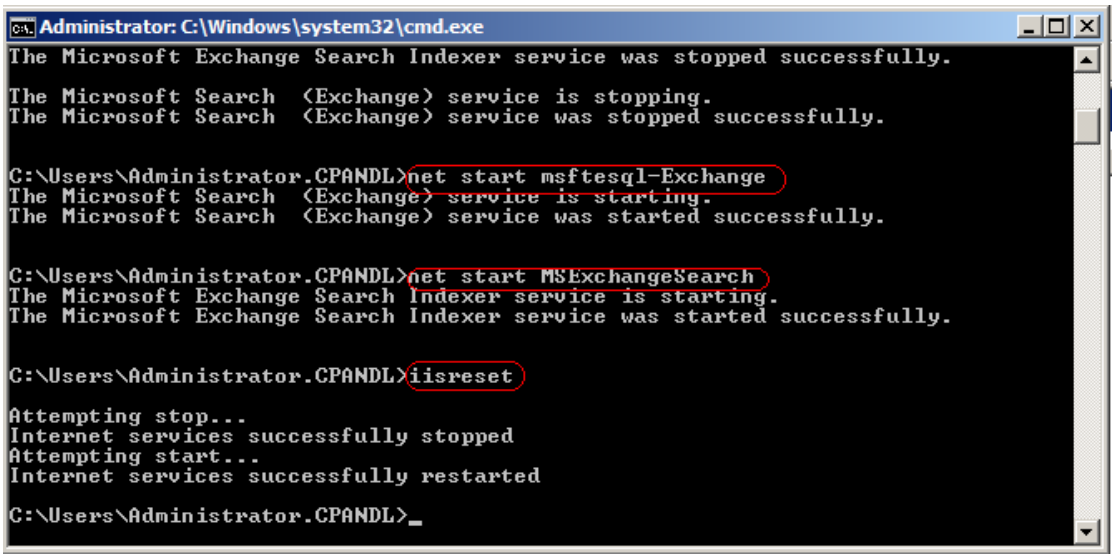
    net stop msftesql-Exchange

    net start msftesql-Exchange

    net start MSExchangeSearch

    iisreset





2. Close the windows.

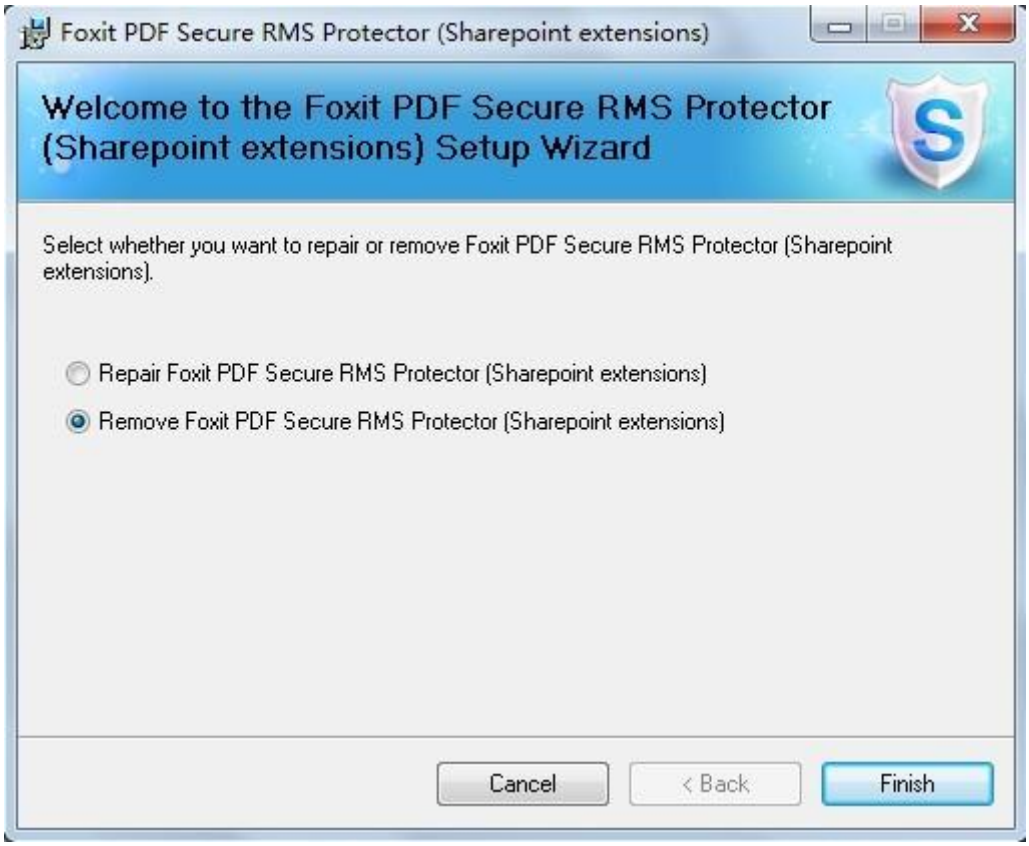
Uninstalling Foxit PDF Secure RMS Protector

To uninstall:

- Open the Start Menu > Control Panel->Programs->Programs and Features
- Click the "Foxit PDF Secure RMS Protector" record and then click the "Uninstall" button to uninstall it.

Or you can double-click the PDFProtector.msi setup file that you have used to install Foxit PDF Secure RMS Protector, and then do the followings:

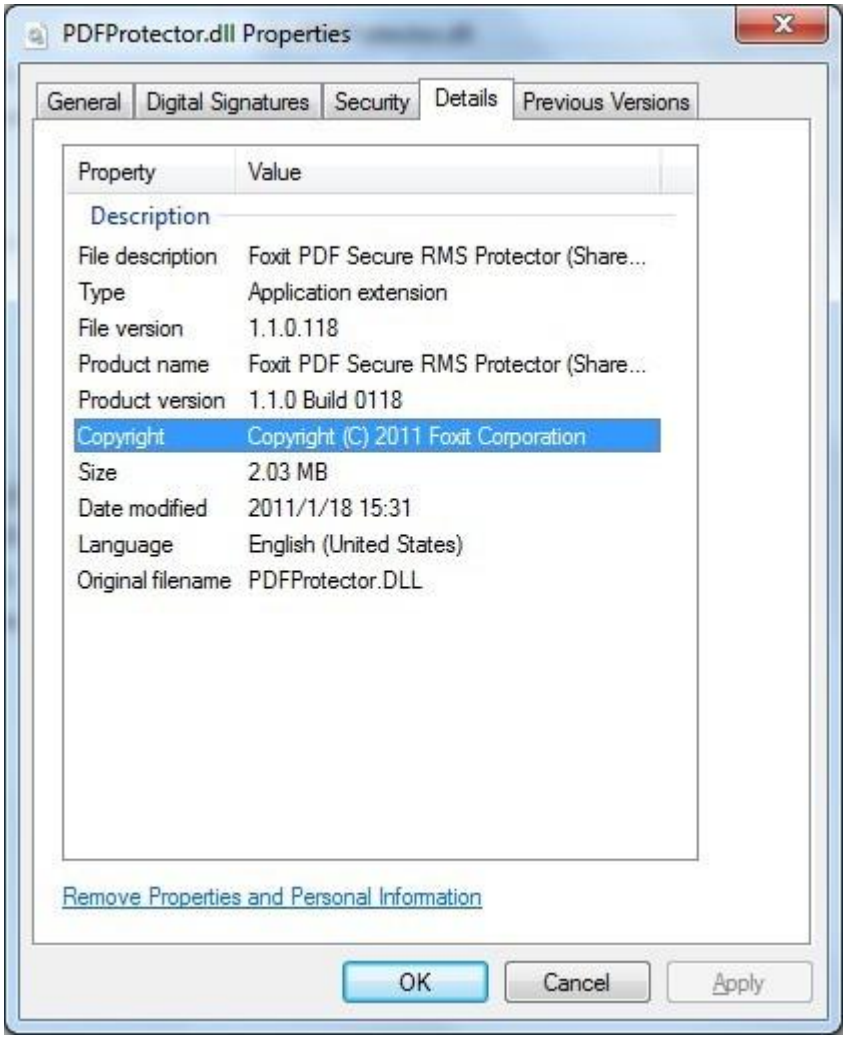
- In the Foxit PDF Secure RMS Protector dialog box, select Remove Foxit PDF Secure RMS Protector



- Click Finish button to uninstall it completely.

Check the version of Foxit PDF Secure RMS Protector

- Please navigate to the folder where Foxit PDF Secure RMS Protector installed. Right-click PDFProtector.dll > choose Properties > click the Details tab, then you can examine the version information of Foxit PDF Secure RMS Protector ,as shown:



Configuring AD • RMS to Integrate with Exchange Server 2010 in a Single Forest

Note: If you have configured AD • RMS when you were installing Exchange, please skip this operation.

To register a service connection point

1. Log on ADRMS server as CPANDL\ADRMSADMIN in the cluster on which you want to register an SCP.
2. Open the Active Directory Rights Management Services console.
3. Right-click the AD • RMS cluster, and then click **Properties.**
4. Click the **SCP** tab.

5. Select the **Change SCP** check box.
6. Click the **Set the SCP to current certification cluster** option, and then click **OK**.
7. Click **Yes** to confirm.

To give Exchange servers permissions to access the server certification pipeline

1. Log on an ADRMS server as CPANDL\administrator in the AD • RMS cluster.
2. Click **Start**, and then click **Computer**.
3. Navigate to %systemdrive%\Inetpub\wwwroot_wmcs\Certification.
4. Right-click **ServerCertification.asmx**, and then click **Properties**.
5. In the **ServerCertification.asmx Properties** dialog box, click the **Security** tab.
6. Click the **Continue** button or the **Edit** button.
7. In the **Permissions for ServerCertification.asmx** dialog box, click **Add**.
8. In the **Select User, Computer, Service Account, or Group** dialog box, click **Object Types**, and select the **Computers** check box, then click **OK**.
9. Type **Exchange Servers** to add the Exchange Servers group, or type the names of the Exchange servers that you want to add, separated by semicolons.
10. Click **Check Names**, and then click **OK.**
11. Under **Allow**, make sure that the **Read & execute** and the **Read** check boxes are selected.
12. Click **OK**.

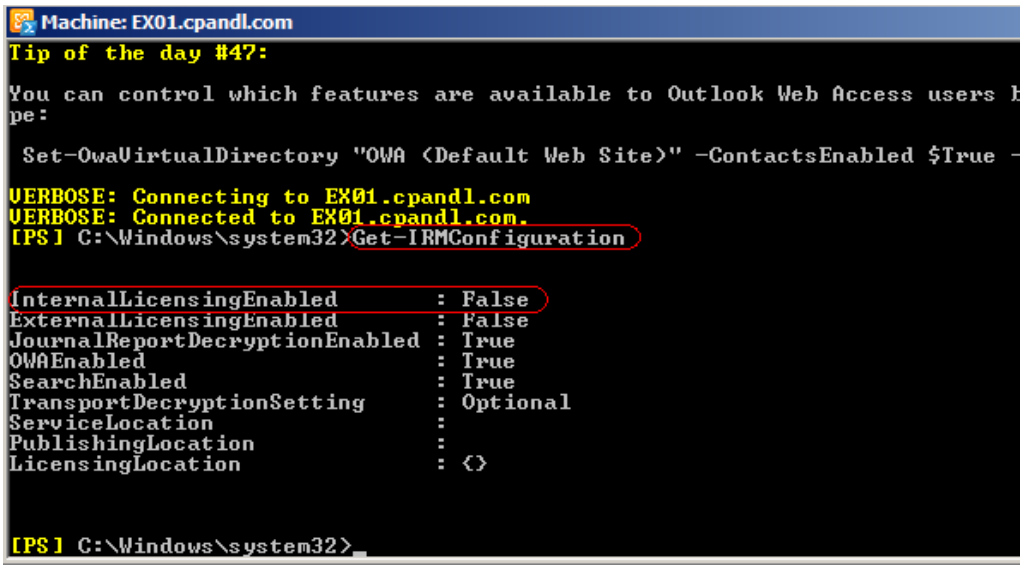
13. If the AD • RMS Service Group does not appear in the **Group or user names** list, repeat the steps 6–11 to add it.
14. Click **OK** to close all dialog boxes.
15. Repeat the steps 1–14 on all other servers in the AD • RMS cluster.

To set up the Exchange Server super users group

1. Log on AD • RMS server as CPANDL\ADRMSADMIN, and open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Security Policies**, and then click **Super Users**.
3. In the **Actions** pane, click **Enable Super Users**.
4. In the results pane, click **Change Super User Group** to open the **Super Users** properties sheet.
5. In the **Super user group** box, type the e-mail address of the designated super users group, or click **Browse** to navigate through the defined users and groups in the directory.(Such as SuperRMSAdmin@cpandl.com)
6. Click **OK**.

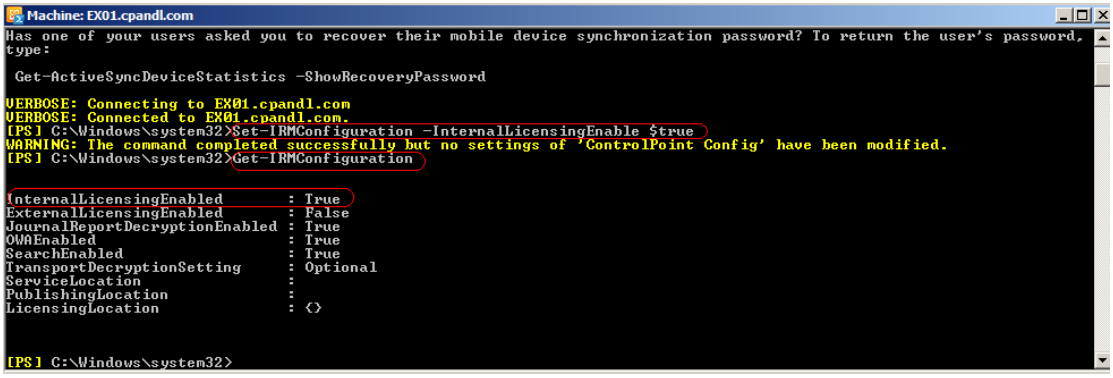
To set InternalLicensingEnable true by ExchangeManagement Shell

1. Log on as **CPANDL\Administrator** to **EXO1**
2. Navigate to Start->All Programs->Microsoft Exchange Server 2010->Exchange Management Shell
3. Type "Get-IRMConfiguration"



4. Type " Set-IRMConfiguration -InternalLicensingEnable $true" to enable licensing.

5. Type " Get-IRMConfiguration " again ,to check InternalLicensingEnalbe is true.

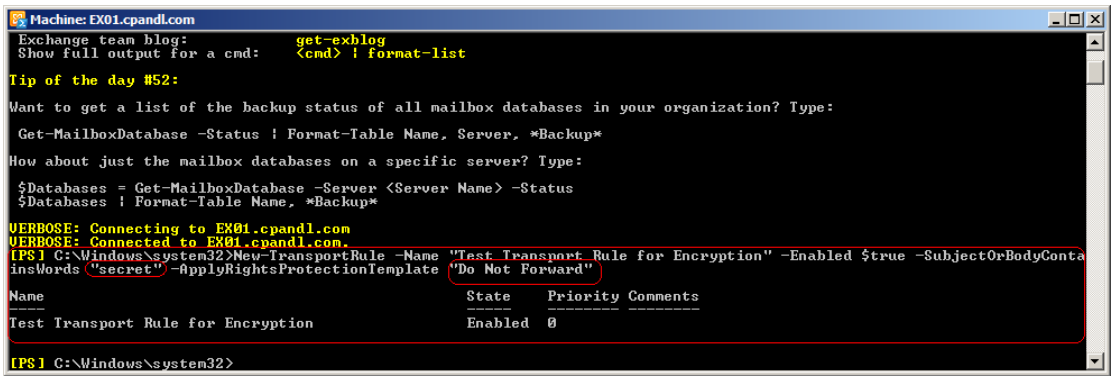


Working with Foxit PDF Secure RMS Protector

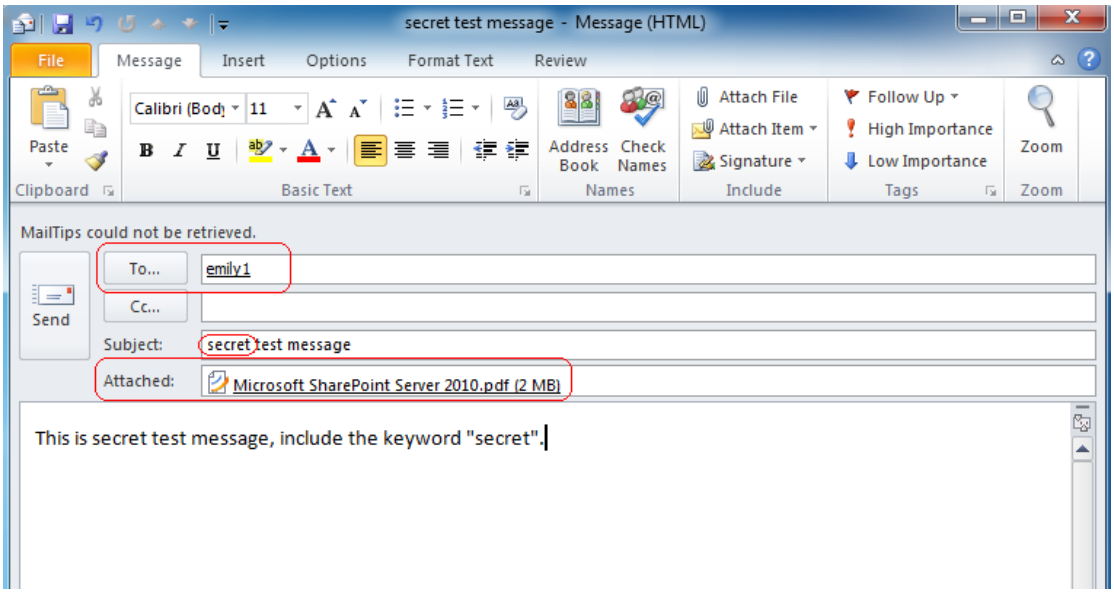
1. Log on as CPANDL\Administrator to EX01
2. Open the Exchange Management Shell.
3. Enter the following task and parameters:

New-TransportRule -Name "Test Transport Rule for Encryption" -Enabled $true -

SubjectOrBodyContainsWords "secret" -ApplyRightsProtectionTemplate "Do Not Forward"



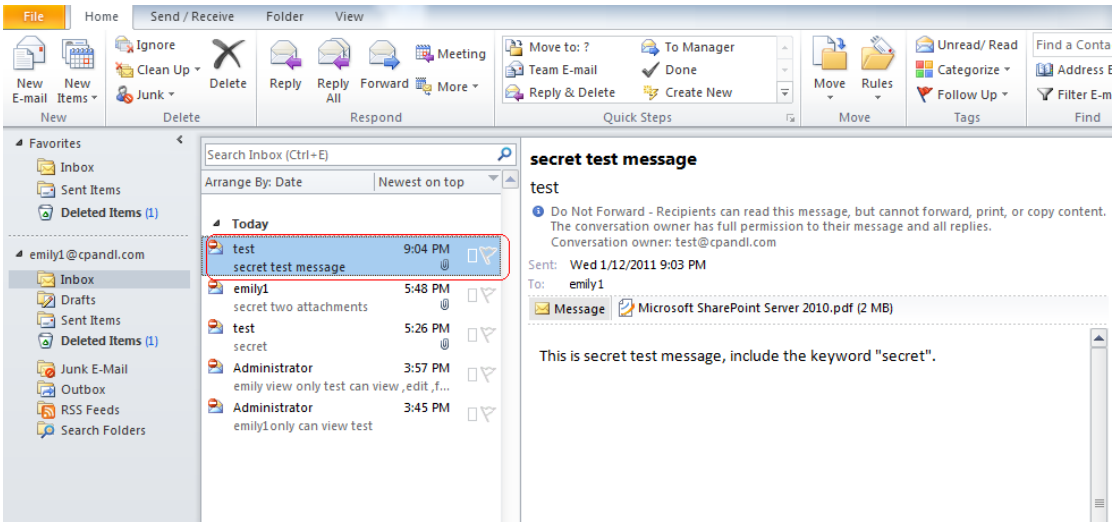
4. Log on as CPANDL\test to **Client,** and open **Microsoft Outlook 2010**, new an Email (for example, send an e-mail to emily1@cpandl.com). The Email includes the PDF attachment.



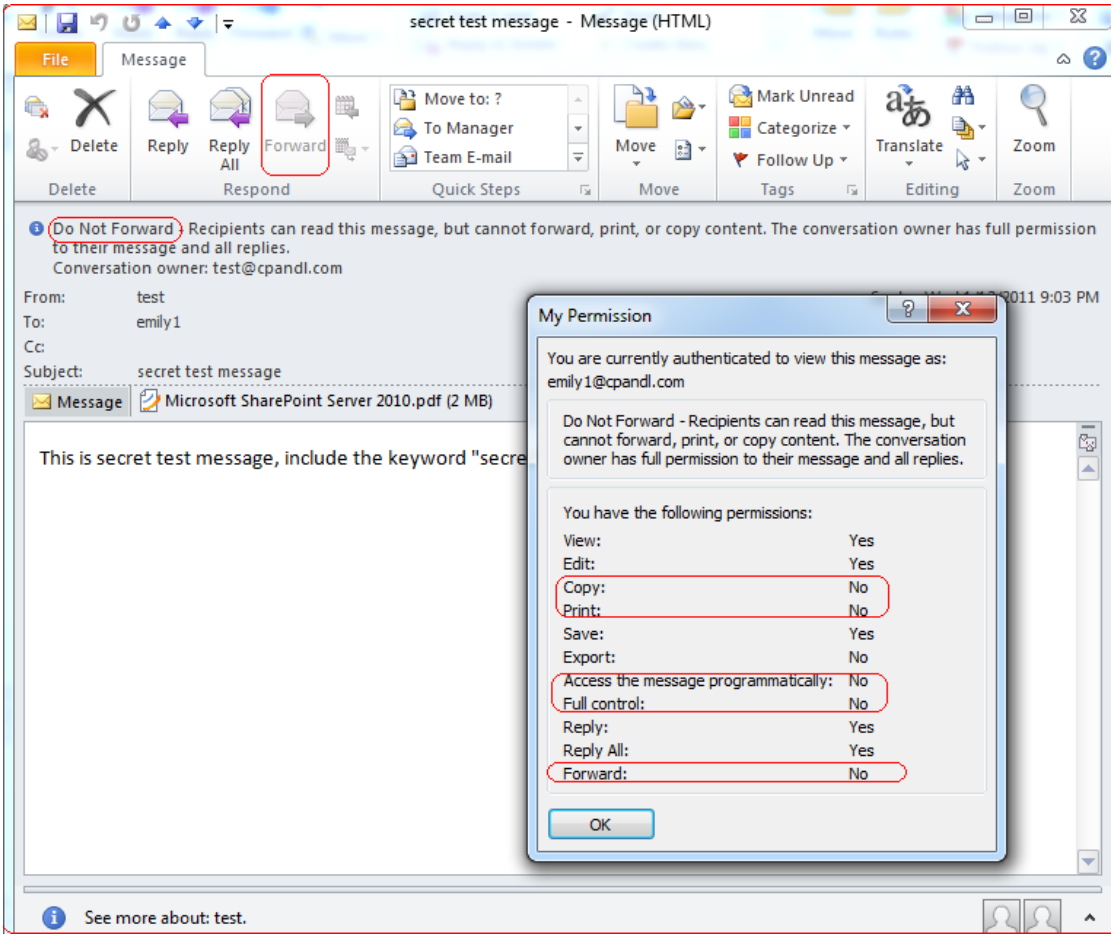
And then click **Send.**

5. Log off and log on as **CPANDL\emily1** to the Client

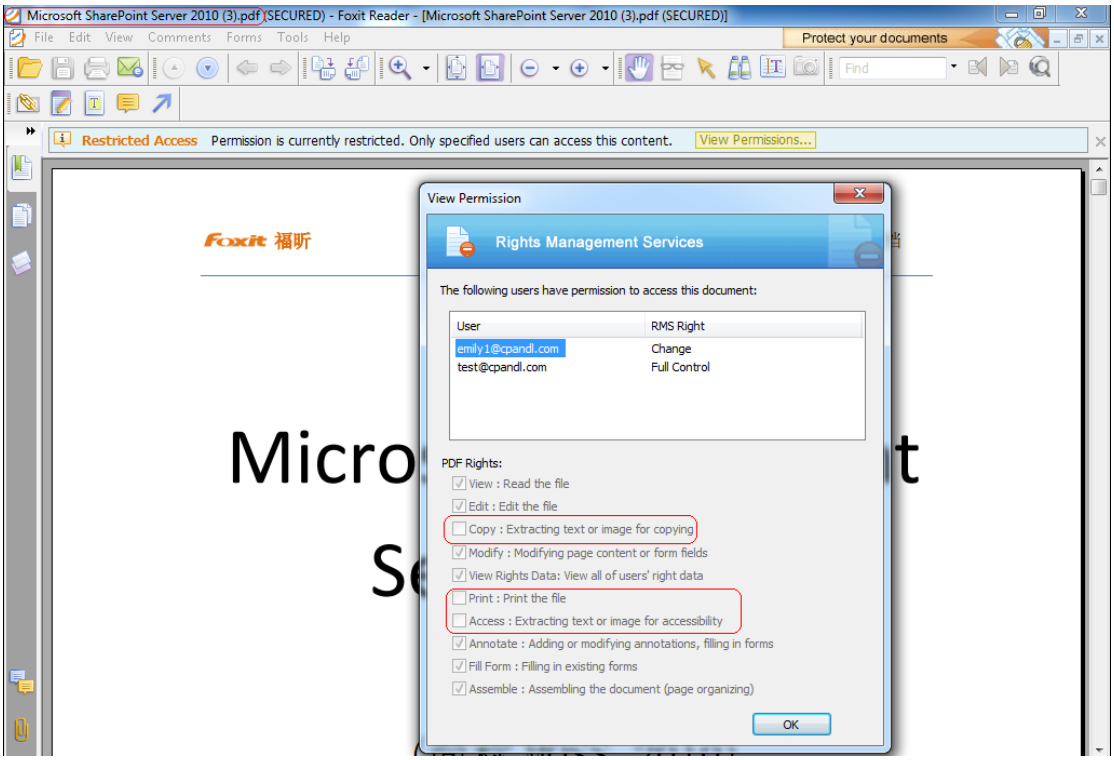
6. Open **Microsoft Outlook 2010.** In the inbox, we can see the email which has been tested to send.



7. Double click the email. We can see the email did not get forwarded. View the permission, and the detail permission is displayed as shown below-----My Permission.



8. Double click the pdf attachment to open it. We can see the permission shown below: not allowed to be printed, copied, or accessed.



Chapter 6 - FAQ

1. **In the SharePoint environment, do we need to perform iisreset after installing the Foxit PDF Protector?**

   Yes. Foxit PDF Protector will not work immediately when it is installed. Please perform **iisreset** to ensure that the SharePoint server invokes Foxit PDF Protector.

2. **Why is the PDF downloaded from the SharePoint Document Library still unprotected after installing the Foxit PDF Protector?**

   First, check that the IRM protection rules have been configured in the **SharePoint Document Library**. For example, ([Library Name]->Setting->Information Rights Management Settings->Restrict permission to documents in this library on downloads).
   Then, clear your browser's Temporary Internet Files. For example, (IE8: Internet Options->General->Delete->check Temporary Internet files->click delete).

3. **Why doesn't the Foxit PDF Protector work after being used for some period of time?**

   Because you can only use the Free Trial version for 30 days. If you want to continue using the Foxit PDF Protector, please contact us by sending an email to sales@foxitsoftware.com to get the formal product license.

4. **I got the authorized license file. How can I use it?**

   Please copy the license file to the same folder where you installed Foxit PDF Protector.
   Note: Please ensure that all the users in the domain have the basic permission to "Read" and "Read & Execute", or the license file may not work.

Contact Us

Feel free to contact us should you need any information or have any problems with our products. We are always here, ready to serve you better.

- *Office Address:*
  Foxit Corporation
  39819 Paseo Padre Parkway
  Fremont CA 94538
  USA
- *Mailing Address:*
  Foxit Corporation
  39819 Paseo Padre Parkway
  Fremont CA 94538
  USA
- *Sales:*
  1-866-MYFOXIT or 1-866-693-6948 (8AM-5PM PST Monday - Friday)
  510-438-9090 (8AM-5PM PST Monday - Friday)
- *Support:*
  1-866-MYFOXIT or 1-866-693-6948 (8AM-5PM PST Monday - Friday)
  979-446-0280 (6AM-5PM PST Monday - Friday)
- *Fax:*
  510-435-9288
- *Website:*
  www.foxitsoftware.com
- *E-mail:*
  Sales and Information - sales@foxitsoftware.com
  Technical Support - support@foxitsoftware.com
  Marketing Service - marketing@foxitsoftware.com