Foxit PDF Secure RMS Protector

(SharePoint extensions)

User Manual

Anti-Grain Geometry - Version 2.3

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

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.

Getting Started

This section provides everything you'll need to know about getting started with Foxit PDF IFilter, including its system requirement, installation and uninstallation.

System requirements

Computer	Operating System	Requirement
RMS Server	Windows Server 2003 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

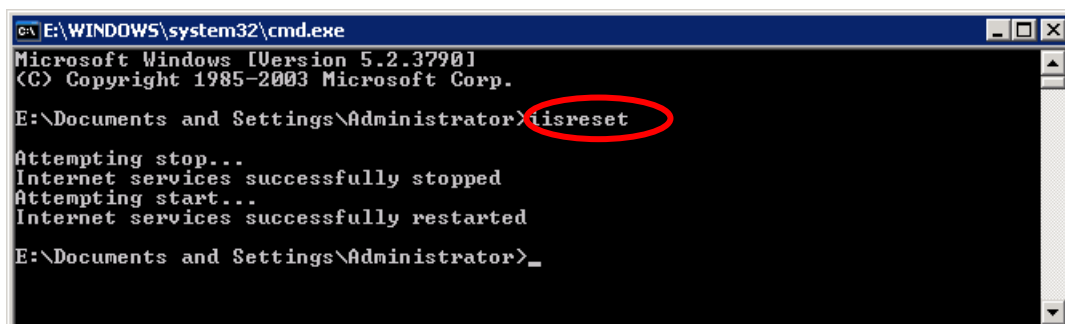## Installing Foxit PDF Secure RMS Protector on SharePoint Server

To install Foxit PDF Secure RMS Protector, please do the following:

- Stop the IIS Admin service: Start > Settings > Control Panel > Administrator Tools > Services > IIS Admin Service > Stop. Close window.

- Run the Foxit PDF Secure RMS Protector Setup program to install the filter on the server.

- Perform an iisreset:

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

  2. Close the windows.

## Uninstalling Foxit PDF Secure RMS Protector

To uninstall, please perform the following:

- Open the Start Menu > Settings > select "Control Panel".
- Click on the "Add or Remove Programs" tab.

- Click on the "Foxit PDF Secure RMS Protector" record and then on the "Remove" 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 do the following:

- In the Foxit PDF Secure RMS Protector dialog box, select Remove Foxit PDF Secure RMS Protector
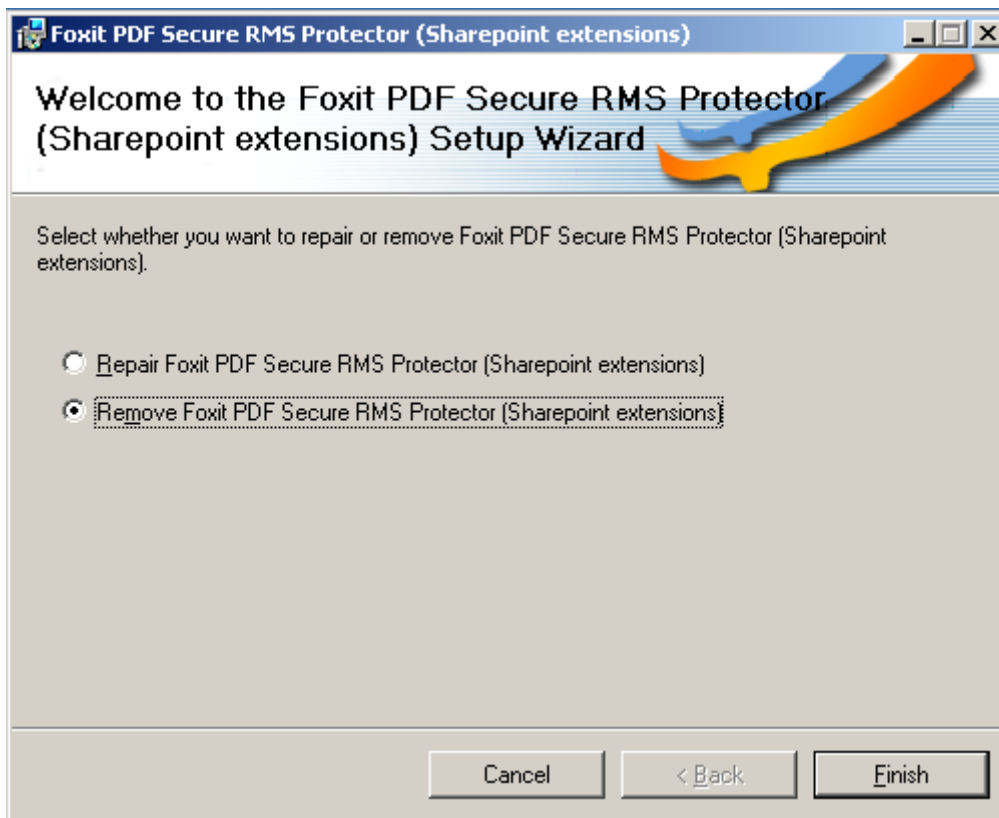
- Click Finish button to uninstall it completely.

Configuring AD RMS to Work with SPS-SRV

To add SPS-SRV to Local Intranet

- Log on to SPS-SRV as domain administrator, e.g, WIONS\administrator.

- Click **Start**, point to **Control Panel**, and then click **Internet Options**.

- Click the **Security** tab, click **Local Intranet**, and then click the **Sites** button

- Type **http://SPS-SRV,** and then click **Add**. Note: SPS-SRV is the computer name of MOSS server.

- Click **Close**, and then click **OK**

To add the domain user to SharePoint site

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

- Click **Site Actions**，point to **Site Settings**, and then click **People and Groups**.

- Click **New**, and then click **Add Users**.

- Type domain user, such as **lnd1@winos.cn;lnd2@wions.cn** in the **Users/Groups** box, and then click **OK**. A list of users who have permission to use the SharePoint is displayed.
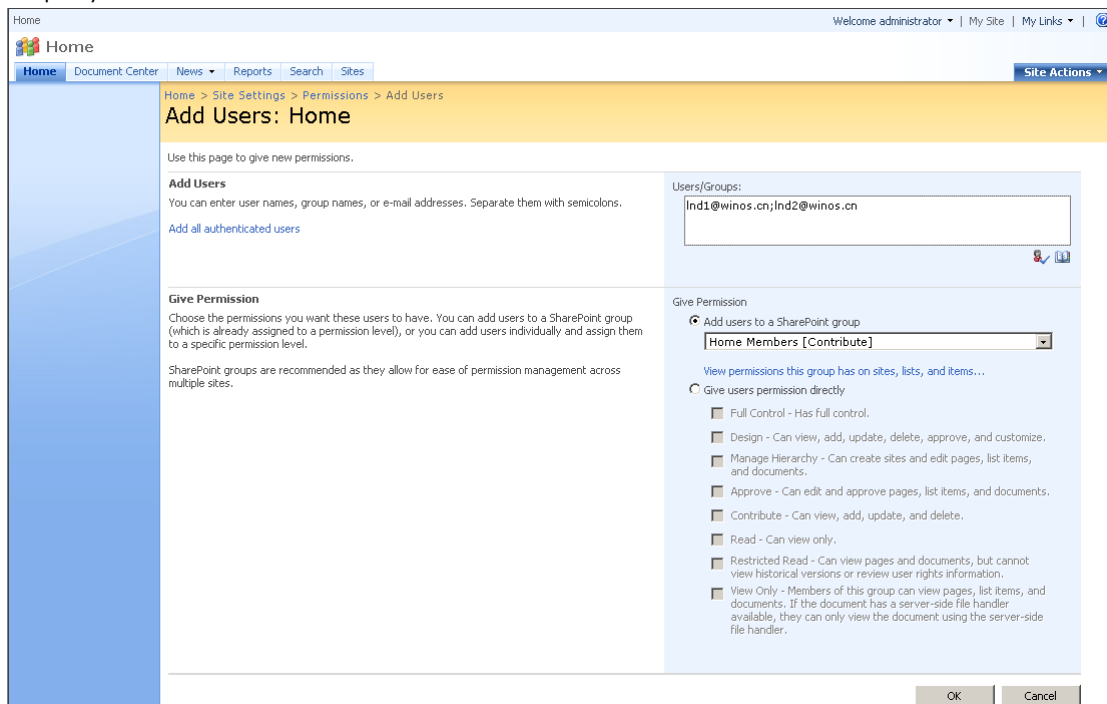
To add SPS-SRV to the AD RMS Certification Pipeline

- Log on to ADRMS-SRV as CPANDL\Administrator.
- Click **Start**, and then click **Computer**.
- Navigate to C:\Inetpub\wwwroot_wmcs\Certification
- Right-click **ServerCertification.asmx**, click **Properties**, and then click the **Security** tab.
- Click **Advanced**, click **Edit**, select the **Include inheritable permissions from this object's parent** check box, and then click **OK** two times.

- Click **Edit**, and then click **Add**

- Click **Object Types**, select the **Computers** check box, and then click **OK**

- Type the computer name of MOSS server, such as **SPS-SRV**, and then click **OK**

- Click **OK** to close the **ServerCertification.asmx Properties** sheet.

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

- Click **Start**, and then click **Command Prompt**.

- Type **iisreset**, and then press ENTER

To enable Information Rights Management in Office SharePoint Server 2007

Please do the following:

- Log on to SharePoint Server as administrator

- Click **Start**, point to **Administrative Tools**, and then click **SharePoint 3.0 Central Administration**.

- Click **Operations**, and then click **Information Rights Management**.

- Click **Use the default RMS server specified in Active Directory**.

- Click **OK**.

Working with Foxit PDF Secure RMS Protector

To setting permission of groups in SharePoint site

- Navigate to **Documents** page, log on administrator@winos.cn, left-clicking the **Settings** down arrow and select **Document Library Settings**.
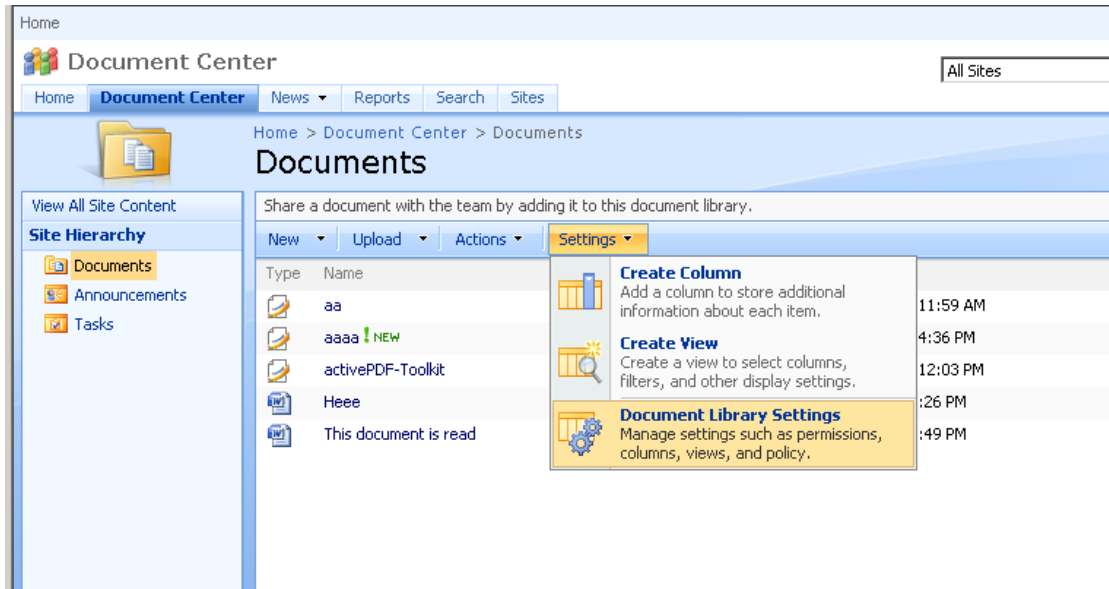
- Click **Permissions for this document library** under Permissions and Management on Customize Documents page.

- Please click **Home Members** on Permissions:Documents page.

- Please choose the permission you want, for example, you can choose **Contribute-Can view, add, updata, and delete**. Click **OK**.
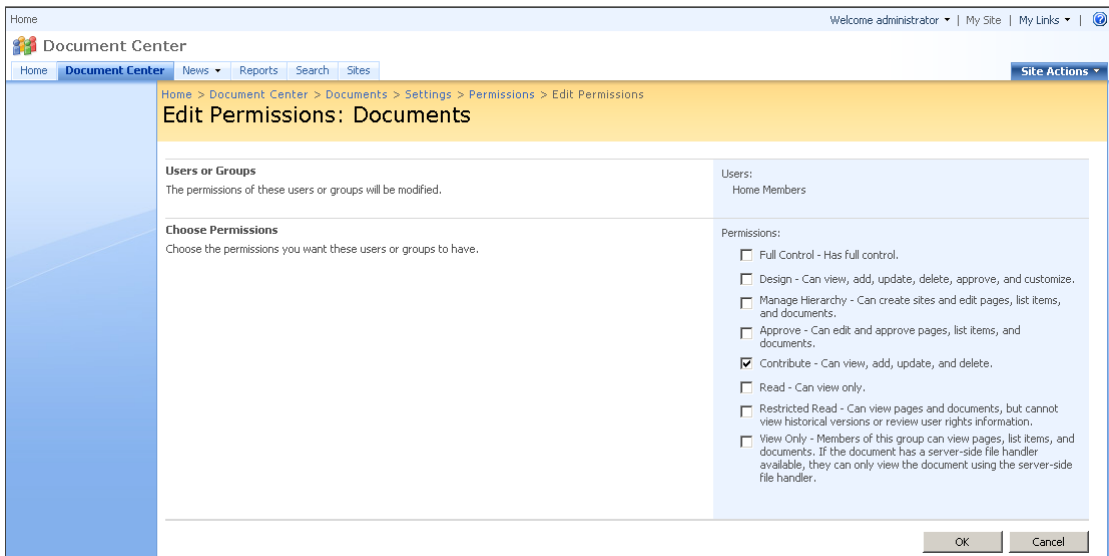
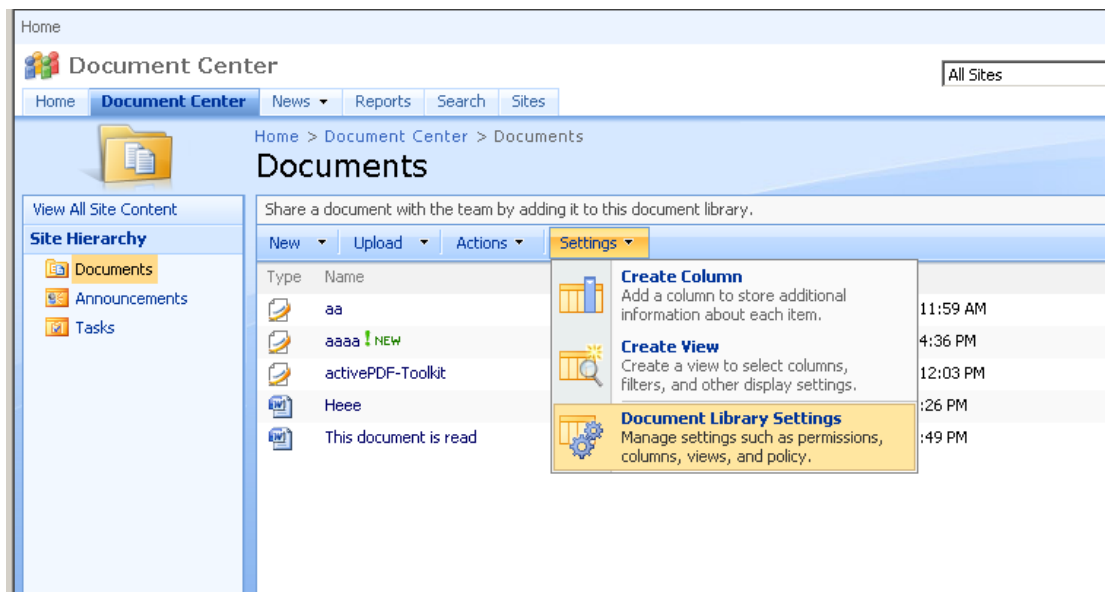- Return to **Documents** page, log on lnd1@winos.cn, to download a pdf file to your load host.
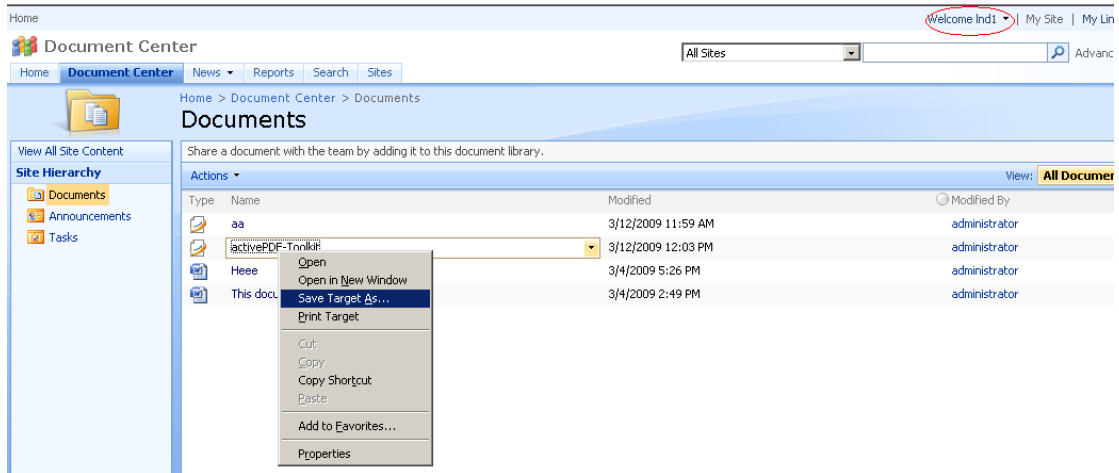
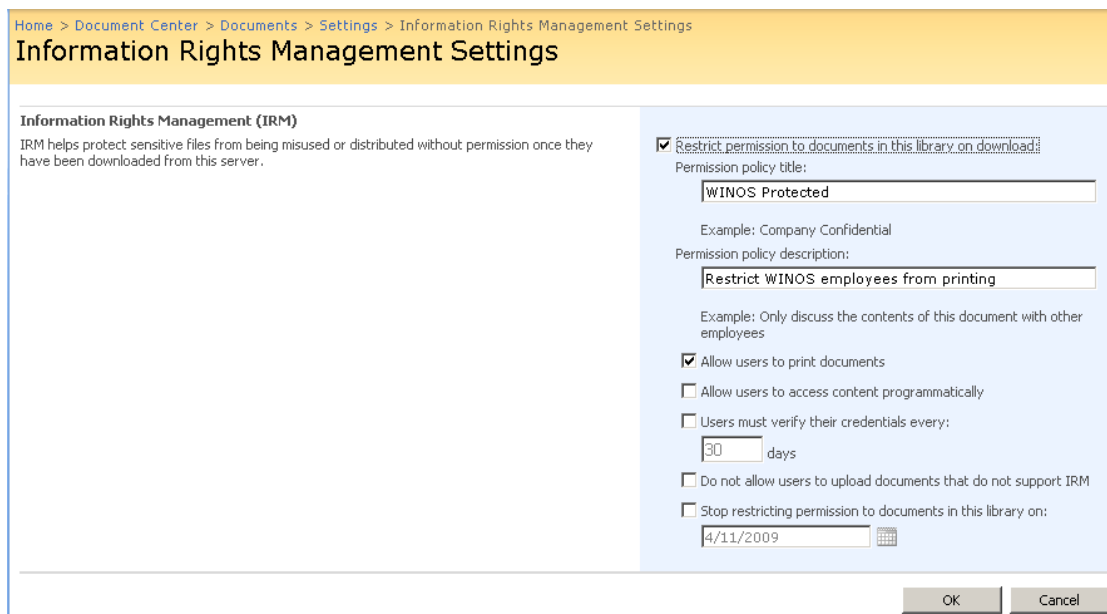- Open the download pdf file by Foxit Reader, left-click **View Permission** to see the **RMS Right**.
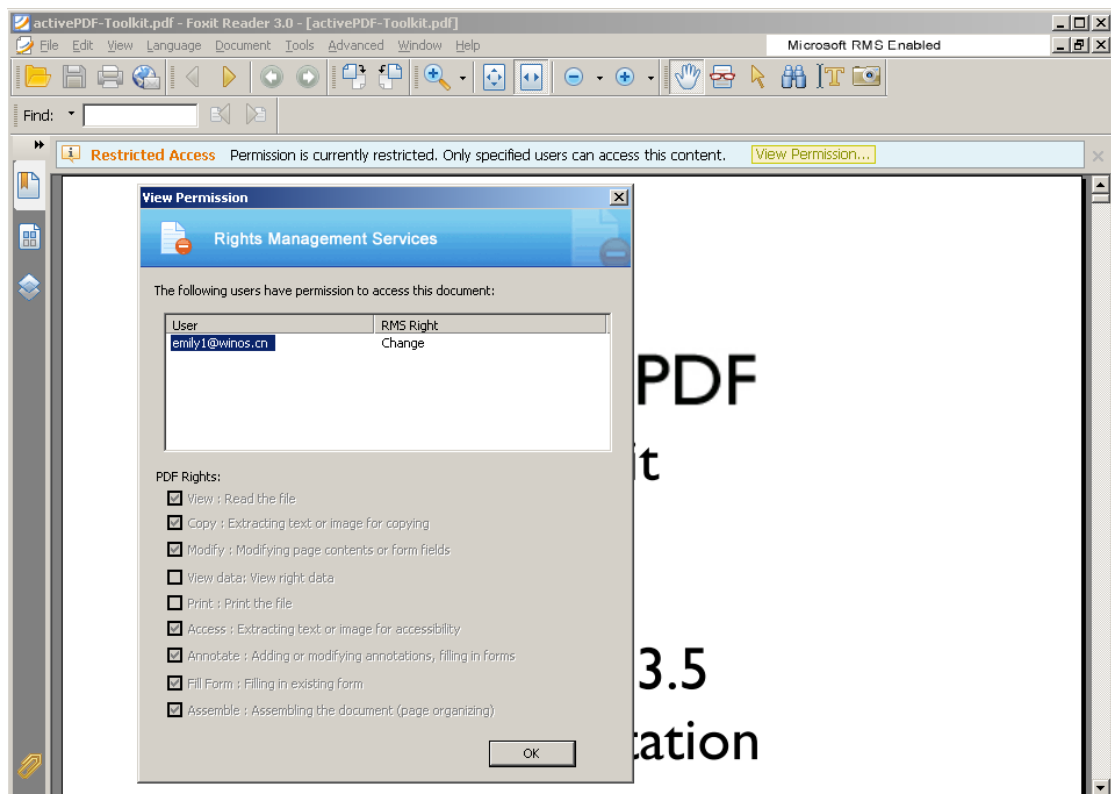
To restrict the print permissions using RMS

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

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

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

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

- Choose **Allow users to print documents**, click **OK**.

- Return to **Documents** page, for example log on lnd1@winos.cn, right-click a pdf file and **choose Save Target AS…** to save a pdf file to the local host.
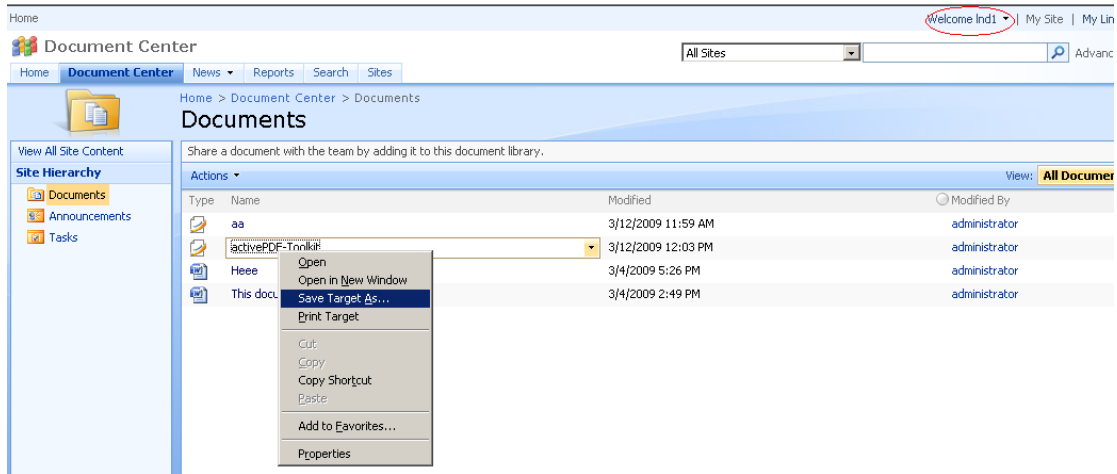
- Open the download pdf file by Foxit reader. Left-click **View Permission** to view the RMS Right of this file. Please see the following picture.
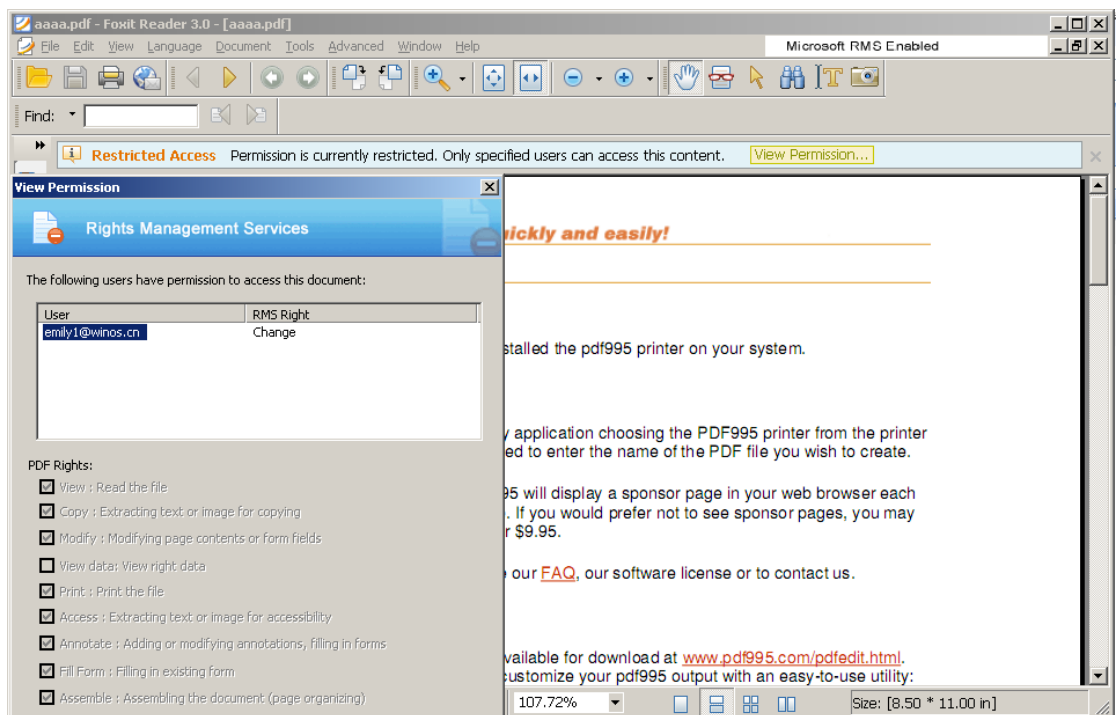
More Help

For more information on how to work with Microsoft Office SharePoint Server (MOSS), please refer to Microsoft Office SharePoint Server (MOSS) Help included in the product.

FAQ

1. **What are the system requirements for the *Foxit PDF Secure RMS Protector*？**

   It need to install on Office SharePoint Server 2007 with RMS client had installed, this sever must be joined to the domain. If your MOSS environment does not install RMS client, please to install it before install Foxit PDF Secure RMS Protector.

2. **How can I tell which version of *Foxit PDF Secure RMS Protector* I am running?**

   Please navigate to the path which Foxit PDF Secure RMS Protector installed. Right-click PDFProtector.dll, choose Properties, click Version page, you can see the version of it.

3. **How to associate about Foxit reader and MOSS?**

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

Level	Corresponding rights of Foxit Reader
Full contoll	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.

4. **Who do I contact if I have problems with *Foxit PDF Secure RMS Protector?***

   You can send the email to **support@foxitsoftware.com**; foxiters will resolve and reply it as soon as possible when we receive the email.