





## Contents

Contents2
Introduction4
Foxit PDF Security Suite Environments5
Enforce AD RMS Policies for PDF documents in SharePoint Environments 5
Enforce AD RMS Policies for PDF documents in Exchange Environments6
Enforce AD RMS Policies for PDF documents in Desktop Environments
Components of Foxit PDF Security Suite7
Foxit PDF Secure RMS Protector7
Foxit PhantomPDF™ Business8
Foxit Reader 8
PDF Security Suite in SharePoint Environments9
IT Manager Deployment9
Authoring Protection Process in SharePoint 12
Accessing Protected PDF Documents in SharePoint Environments
PDF Security Suite in Exchange Environments
IT Manager Deployment 15
Authoring Protection Process in Exchange Environments
Accessing Protected PDF Documents in Exchange Environments
PDF Security Suite in Desktop Environments17
Authoring Protection Process in Desktop Environments
Accessing Protected PDF Documents in Desktop Environments
RMS PDF Protection Tool



Conclusion	20
About Foxit Software	21



## Introduction

The rapid growth of online documents has been fueled by the efficiency gains that businesses and governmental organizations realize by storing documents digitally rather than traditional paper. Portable Document Format (PDF) has become a dominate file format for sharing and archiving documents since the format allows the reliable reproduction of information on many different platforms and only requires the use of widely available PDF reader software to view the documents. Effectively managing digital access to the large and growing number of documents with sensitive and confidential information becomes a vital challenge to IT organizations.

Microsoft<sup>®</sup> Active Directory<sup>®</sup> Rights Management Services (AD RMS) provides protection to digital documents that meet enterprise and governmental security governance requirements. Since Microsoft's support of AD RMS protects Microsoft Office<sup>®</sup> documents only, Microsoft provides a RMS Software Development Kit (SDK) for software companies to extend AD RMS support beyond Office documents. Foxit<sup>®</sup> has utilized this RMS SDK to seamlessly extend AD RMS to provide protection to PDF documents.

AD RMS is used for restricting access of rights-protected content to authorized users only. It uses a client/server architecture, using Windows Server<sup>®</sup> 2003 or Windows Server 2008 to host the AD RMS server that issues RMS licenses. The Foxit PDF Security Suite, consisting of Foxit Reader, PhantomPDF<sup>™</sup> Business, and PDF RMS Protector, provides a solution which implements the RMS client APIs explicitly. Foxit is able to help customers who have deployed AD RMS to enhance their security environment to include PDF documents. The Foxit PDF Security Suite also supports Azure Active Directory Rights Management (AAD RM).

## The Foxit Reader is a Microsoft preferred PDF reader for AD RMS, SharePoint<sup>®</sup> 2013, and SharePoint Online in Office 365 environments.

For IT professionals who need to improve information security, meet compliance requirements, and save time and money, Foxit PDF Security Suite is a cost effective solution that provides AD RMS policy protection of PDF documents and selective enablement of PDF features - including forms fill out and document editing.



Since Foxit PDF Security Suite is an extension of AD RMS, IT organizations immediately realize benefits. Foxit PDF Security Suite:

- 1) Doesn't require a new solution to be deployed and managed
- 2) Takes advantage of the security templates already in place
- 3) Requires no additional training to IT administrators
- Transparent to end users they continue to use the same solution they have already learned to use
- 5) Is extremely cost effective.

## **Foxit PDF Security Suite Environments**

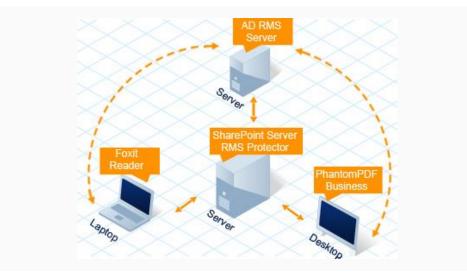
For organizations that incorporate AD RMS that need to include rights management for PDF files, Foxit PDF Security Suite seamlessly extends Microsoft AD RMS to provide policy protection to PDF documents in SharePoint<sup>®</sup>, Exchange<sup>®</sup>, and/or desktop solutions. These protected PDF documents can be read by the AD RMS-aware Foxit Reader.

### Enforce AD RMS Policies for PDF documents in SharePoint Environments

Enterprises share files in a number of ways. One of the most common is with a SharePoint server with protection provided by an AD RMS server. In this environment, Microsoft Office files are shared on the SharePoint server and then get encrypted and policy protected upon download to a client. Foxit PDF Security Suite RMS Protector extends these AD RMS capabilities to include PDF documents. The RMS-aware Foxit Reader enforces AD RMS policy protected PDF files for operations like reading, printing, copying, and annotating. For PDF edit capabilities, PhantomPDF *Business* provides edit functionality in addition to the capabilities of the Foxit Reader.

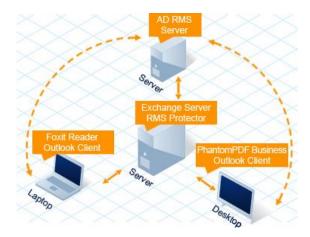


Foxit<sup>®</sup> PDF Security Suite Integrated with Microsoft<sup>®</sup> Active Directory<sup>®</sup> Rights Management Service



#### Enforce AD RMS Policies for PDF documents in Exchange Environments

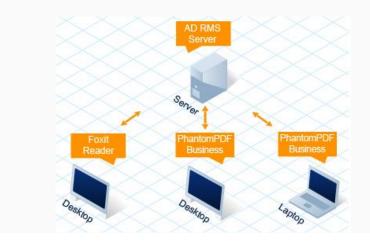
Another common way for enterprises to share files is through email. An Exchange server in an AD RMS environment can enforce rights management services to Microsoft Office files that are attachments to email messages. Similar to SharePoint environments, Foxit PDF Security Suite RMS Protector extends these AD RMS capabilities in these environments to include PDF documents. The AD RMS-aware Foxit Reader enforces AD RMS policy protected PDF files for operations like reading, printing, copying, and annotating. For PDF edit capabilities, PhantomPDF *Business* provides edit functionality in addition to the capabilities of the Foxit Reader.





### Enforce AD RMS Policies for PDF documents in Desktop Environments

Enterprises also share files located on their desktop systems. In these environments, the Foxit PhantomPDF *Business* solution deployed on each PDF file sharing desktop system extends these AD RMS capabilities to include PDF documents. PhantomPDF *Business* also seamlessly integrates into the Microsoft Office Word, PowerPoint and Excel desktop solutions. The AD RMSaware Foxit Reader enforces AD RMS policy protected PDF files for operations like reading, printing, copying, and annotating. For PDF edit capabilities, PhantomPDF *Business* provides edit functionality in addition to the capabilities of the Foxit Reader.



## **Components of Foxit PDF Security Suite**

#### Foxit PDF Secure RMS Protector

Foxit PDF Secure RMS protector is installed on any SharePoint or Exchange server communicating with an AD RMS server. Once installed, this application extends all Microsoft AD RMS features to any PDF file posted to the SharePoint Server or Exchange email message through the application of security templates in RMS. Foxit PDF Secure RMS Protector seamlessly integrates into a SharePoint or Exchange workflow to automatically and transparently extend AD RMS policy protection to any PDF document.

#### System Requirements

Microsoft Office SharePoint Server (MOSS 2007, 2010 and 2013)



- Microsoft Exchange Server 2010 and 2013
- Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit),
   Windows Server 2012 (32-bit and 64-bit)
- 1GB memory, 10MB free disk space

#### Foxit PhantomPDF™ Business

Foxit PhantomPDF Business extends the usage control benefits of AD RMS on desktop/client systems to all your PDF documents and allows the author the control of document features within each PDF. It also enforces AD RMS policy protection on operations like printing, copying, annotating, editing, forwarding, and deleting PDF files whether those files are downloaded from a SharePoint server or other desktop systems.

#### System Requirements

**Operating Systems** 

- Microsoft Windows<sup>®</sup> XP Home, Professional, or Tablet PC Edition with Service Pack 2 or 3 (32-bit & 64-bit).
- Windows Vista Home Basic, Home Premium, Business, Ultimate, or Enterprise with or without Service Pack 1 (32-bit & 64-bit).
- Windows 7 (32-bit & 64-bit)

Recommended Minimum Hardware for Better Performance

- 1.3 GHz or faster processor.
- 512 MB RAM (Recommended: 1 GB RAM or greater).
- 700 MB of available hard drive space.
- 800x600 screen resolution.

#### **Foxit Reader**

The Foxit Reader is a small, fast, and feature rich PDF viewer which allows you to open, view, and print any PDF file. Unlike other PDF readers, Foxit Reader also includes easy to use collaboration features like the ability to add annotations, fill out forms, and add text to PDF documents. It also enforces AD RMS policy protection on operations like printing, copying,



annotating, editing, forwarding, and deleting PDF files whether those files are downloaded from a SharePoint server, attached as an email message, or located on other desktop systems.

The Foxit Reader is a Microsoft preferred PDF reader for AD RMS, SharePoint<sup>®</sup> 2013, and SharePoint Online in Office 365 environments.

### **System Requirements**

**Operating Systems** 

- Microsoft Windows XP Home, Professional, or Tablet PC Edition with Service Pack
   2 or 3 (32-bit & 64-bit).
- Windows Vista Home Basic, Home Premium, Business, Ultimate, or Enterprise with or without Service Pack 1 (32-bit & 64-bit).
- Windows 7 (32-bit & 64-bit).

## PDF Security Suite in SharePoint Environments

To deploy AD RMS protected files in SharePoint environments is very easy and is consistent with deploying protected Microsoft Office files.

## **IT Manager Deployment**

IT Managers need to follow these simple steps for the initial deployment:

1. In SharePoint's Central Administration, insert the proper Microsoft AD RMS server URL to establish a connection.



🗿 Information Rights Management - Microsoft Internet Explorer		_ 8 ×
Ele Edit Yew Favorites Iools Help		
🔾 Back + 🕐 - 💌 😰 🐔 🔑 Search 🔅 Favorites 🥴 😥 + 😓 📼 +		
Agdress (@) http://fcoxlssharepoint:4662/_sdmin/IrmAdmin.aspx	💌 🔁 Go	Links »
Central Administration Welcome CPANDL (Administration + )	Ny Site   My Links 🔻	0 🔺
🔆 Central Administration		
Home Operations Application Management	Site Actions	s 🔻
Central Administration > Operations > Information Rights Management Information Rights Management		
View All Ste Content		
Central Administration         Information Rights Management         Specify the location of Windows Rights Management           BM helps protect sensitive files from being misued or distributed without permission once they application Management         C Do not use IRM on this server         C Do not use IRM on this server           Specify the location of Windows Rights Management         C Use the default RMS server specified in Active (Ise the default RMS server specified in Active Shared Services)         C Use the default RMS server specified in Active (Ise this RMS server)		
Administration		
SharedService1     OK	Cancel	1.11
R		
[2 Rems remaining) Downloading picture http://footkharepoint:4662/ themes/CENTRLAD/topnavselected_central_admin.gf	Nocal intranet	

 In SharePoint's Document Center, setup the Document Library to enable the Microsoft AD RMS (also called IRM) service. This Document Library will contain the PDF files that require protection.



🙆 Information Rights Man	agement Settings - Microsoft Internet Explorer		_ 6 ×
Eile Edit View Favorite	is <u>T</u> ools <u>H</u> elp		
🔇 Back 🔹 🕤 🖌 📓 😰	🏠 🔎 Search 👷 Favorites 🛷 😥 😥 🕡 🔹		
Address 🙆 http://foxitshare	point/Docs/_Jayouts/irm.aspx?List=%7B6094DA2F%2DA7E2%2D4F23%2D9AF1%2D1EC8F6AB8798%	57D	💌 ラ Go Links "
Home			Welcome CPANDL\administrator 🔹   My Site   My Links 💌   🙆 💆
駌 Document Cer	nter		
Home Document Cente	er News - Reports Search Sites		Site Actions -
	Home > Document Center > Documents > Settings > Information Rights Management Information Rights Management Settings	Settings	
	Information Rights Management (IRM) IRM hetep potes enabler files from being misused or distributed without permission once they have been downloaded from this server.		
		CK Cancel	
Done			Local intranet
🏄 Start 🛛 🔂 🥌 💋 📗	Information Rights M		🕎 😧 🏷 😰 2:07 PM

3. In the Document Center's Permission page, setup users and group permissions for the Document Library with IRM services.



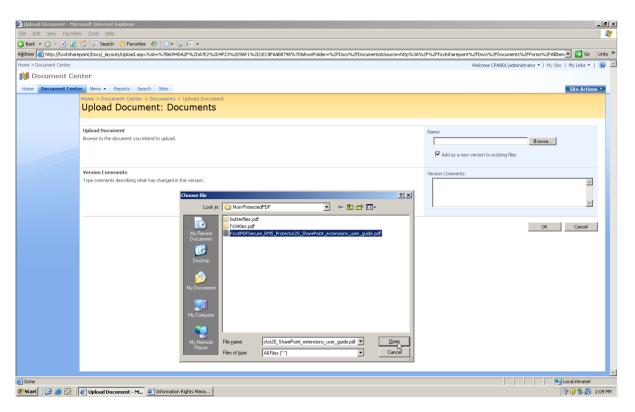
Edit View Fav		osoft Internet Explorer Is <u>H</u> elp				
		Search 👷 Favorites 🕢 🍰 - 😓	(w) •			
				=1%2D1EC8F6AB8798%7D,doclib8List=%7B6	094DA2F%2DA7E2%2D4F23%2D9AF1%2D1EC8F6AB8798%7D	💌 🛃 Go 🛛 L
					Wel	come CPANDL\administrator 🔹   My Site   My Links 🔹   (
Document (	Center					
Document C	enter Ne	ws - Reports Search Sites				Site Actions
		Document Center > Documents > S missions: Document				
	Use th	is page to assign users and groups permissi	on to this library. This library	does not inherit permissions from its parent W	eb site.	
	New	Actions				
		O Users/Groups	Туре	User Name	Permissions	
		Approvers	SharePoint Group	Approvers	Approve	
		Designers	SharePoint Group	Designers	Design	
		FOXITSHAREPOINT\Administrator	User	FOXITSHAREPOINT\administrator	Full Control	
		Hierarchy Managers	SharePoint Group	Hierarchy Managers	Manage Hierarchy	
		Home Members	SharePoint Group	Home Members	Read, Restricted Read, View Only	
		Home Owners	SharePoint Group	Home Owners	Full Control	
		Home Visitors	SharePoint Group	Hame Visitors	Read	
		Quick Deploy Users	SharePoint Group	Quick Deploy Users	Limited Access	
		Restricted Readers	SharePoint Group	Restricted Readers	Restricted Read	
		Style Resource Readers	SharePoint Group	Style Resource Readers	Limited Access	
		user1	User	CPANDL\user1	Design	
		user2	User	CPANDL/user2	View Only	
		user3	User	CPANDL/user3	Full Control	
		Viewers	SharePoint Group	Viewers	View Only	
ne						Local intranet

### **Authoring Protection Process in SharePoint**

PDF document authors need to follow these simple steps to distribute sensitive PDF documents through SharePoint:

- 1. The documents' authors create PDF documents on their desktop systems.
- After PDF document creation, authors upload the PDF files to the IRM service enabled Document Library.



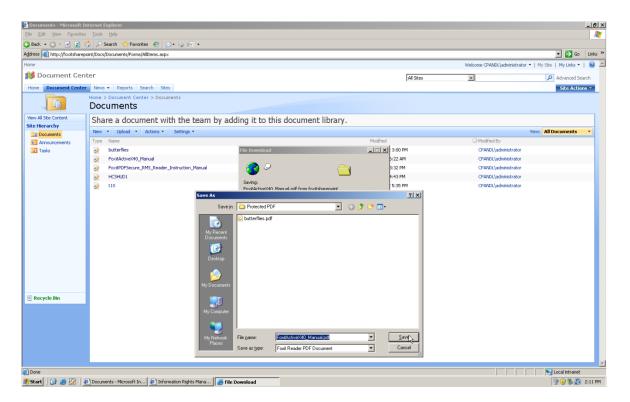


### Accessing Protected PDF Documents in SharePoint Environments

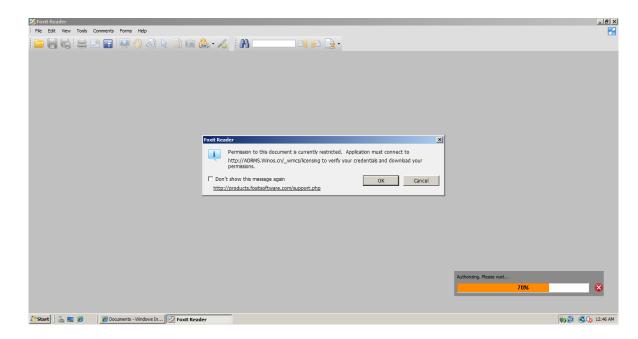
For those who need to access protected PDF documents can follow these simple steps:

 Login to the SharePoint environment, navigate to the Document Library, and click on the file to open or download the PDF file. The Foxit client application (Foxit Reader or Foxit PhantomPDF) then calls the AD RMS Client, which contacts the RMS server, which validates the user and issues a "user license".





2. The Foxit client application then renders the file and enforces the assigned rights.





💋 FoxitPhantomPDF51_QuickGuide(print).pdf (SECURED) - Foxit Reade	2r		_ 6 ×
File Edit View Tools Comments Forms Help			
🗀 🔚 🛃 🖨 💷 🖬 🖳 🕎 🔕 📐 🗟 🕼	a 🕰 🗸 🧭 i 🕰		
	Document Properties	2	<u>دا</u>
WINOS Protected - Restrict WINOS employees from printing	Description Security For		🖉 view permission 🗡
•	Description Secondy [For	105	
	Document Security		
	Security Method:	RMS Encryption	
	Protection Policy Information		
	WINOS Protected - Restrict	WINOS employees from printing	
		mission to access this document:	
<b>Foxit</b>	The following users have per		
	User emily1@winos.cn	RMS Right	
		energe	
	PDF Rights	Allowed	
		Allowed Not Allowed	
	VIEW RIGHTS DATA:		
		Allowed	
	PRINT HIGH:		
	FILL FORM:		
	ANNOTATE: ASSEMBLE:		
	ASSEMBLE: MODIFY:		
	EXTRACT ACCESS:		
	EXTRACT:	Allowed	
	Line Enternation Inc.		
	License Expiration date: Uni	Known Content Expiration date: Unlimited	
		OK Cancel	
		OK Cancer	
Start 🔒 🔳 🍘 🖉 Documents - Windows In 📝 FoxitPh	antemPDEE1		🙀 🗐 🕷 🗽 12:52 AM
	Million Di Sk_m		NO EN CONTRACTOR NOT

#### ts - Windows In... 📝 Fe

## **PDF Security Suite in Exchange Environments**

To deploy AD RMS protected files in Exchange environments is very easy and is consistent with deploying protected Microsoft Office files.

#### **IT Manager Deployment**

IT Managers need to follow these simple steps for the initial deployment:

1. Set up Exchange Server environment with the proper Microsoft AD RMS server URL to setup the connection.



🕌 certification							_ 6 ×
😋 🕞 🗸 🕨 🗸 Computer	• Local Disk (C:) • inetpub • www.root • _	wmcs - certification			✓ Gearch certification		2
Organize 👻 📄 Open 👻	New folder					8E • E	1 0
Y Pavorites     E Desktop     Downods     Wasc     Accent Places     Marcent Places     Music     Music     Wenents     Music     Wenents     Wasc     Wasc	Name *  Confliction asmx Confliction Conflic	General Security De Opert name: C-Vre Grup or user name: R, Authenciceted Us R, SYSTEM To change permission Permissions for Authen Uses Full control Modify Read Securic Read Securic Read Securic Read Securit Read	Select Users, Computers, Service Accounts, or Groups Select Users, Computers Computers Frandition Frandition Common Quetes Name: Starts with   Description: Starts with   Description: Starts with   Description: Starts with   Common Quetes Name: Starts with   Common Quetes  Name: Starts  Common Quetes  Comm	2 X Object Types Locations Find New Stop Friend Cancel			
ASMX File	ion.asmx Date modified: 6/10/2009 2:03 PM Size: 119 bytes	Date created: 1/1					
🎝 Start 🛃 🗾	1				* 🕞 🖗	1:10 4/6/	8 AM /2012 ⋿

2. Set up email security rules with Microsoft AD RMS (also called IRM) service enabled.

emises (e				6 objects	Actions
ation Remote Domains Accepted Domains E-mail	Address Policies Transport	Rules Journal Rules Sen	Connectors Edge Subscription	s Global Settings	Hub Transport
Create Filter					New Remote Domain
Name	Priority	State	Comment		🕺 New Accepted Domain
test exchange 0304	0	Enabled	Comment		💷 New E-mail Address Policy
admin to test transport rule emily0304	1	Enabled			New Transport Rule
transport rule for test 0304	2	Enabled			New Journal Rule
iii content	3	Enabled			II –
using rms template for sending email	4	Enabled Enabled			New Send Connector
lest transport Rule for Encryption	2	chabled			🍖 New Edge Subscription
					Export List
					View
					Refresh
					👔 Help

3. Set up "key words" (key words are triggers for AD RMS to protect files), users, and group permissions for the email/email attachment with Exchange Server's IRM features.



😣 Exchange Management Console					×
File Action View Help					
🗢 🔿 🙍 🖬 🛛 🖬					
8 Microsoft Exchange	Actions				
Microsoft Exchange On-Premises (e     m) Organization Configuration	Remote Domains 4			gs )	Hub Transport 🔺
Maibox Clent Access Clent Access Unified Messaging Server Configuration	Create Filter     Name     test exchange 0     admin to test tra	Introduction	Transport Rule		Image: New Remote Domain           Image: New Accepted Domain           Image: New E-mail Address Policy           Image: New Transport Rule
Recipient Configuration Toolbox	transport rule fe	Conditions	This wizard helps you create a new transport rule. Transport Rules check each message for predefined conditions. If the condition is true for a message, the rule actions are applied to		New Transport Rule
I DOIDOX	content	Actions	it.		New Send Connector
	Test Transport I	Exceptions	Name:		New Edge Subscription
		Create Rule			Export List
		Completion	Comment:		View
					G Refresh
					2 Help
			×		
			7 Enable Rule		
4 <b>  </b>   •		Help	<back next=""> Cancel</back>		
	,				,
灯 Start 🔚 🛛 🚞					* 🕞 👘 🎲 1:23 AM

#### **Authoring Protection Process in Exchange Environments**

After PDF creation, document authors just need to attach the sensitive PDF document into an Outlook email message for distribution.

### Accessing Protected PDF Documents in Exchange Environments

For those who need to access protected PDF documents can follow these simple steps:

- 1. After recipient attempts to open the sensitive PDF documents via email, the Foxit application calls the AD RMS Client, which contacts the RMS server, which validates the user and issues a "user license".
- 2. The Foxit client application then renders the file and enforces the assigned rights.

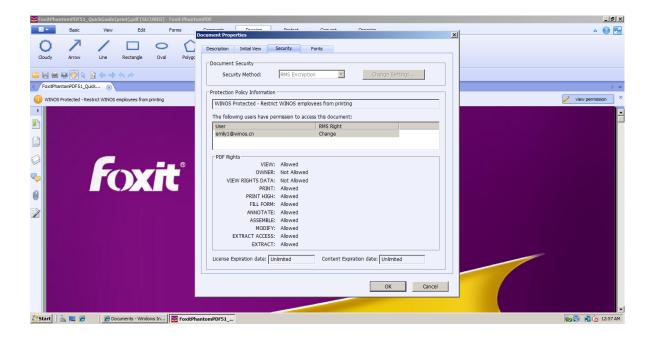
## **PDF Security Suite in Desktop Environments**

#### **Authoring Protection Process in Desktop Environments**

To protect files in desktop environments, PDF authors should follow these simple steps:



1. Authors of sensitive PDF documents use Foxit PhantomPDF Business's RMS Encrypt feature (within the Protect section) to protect the document.



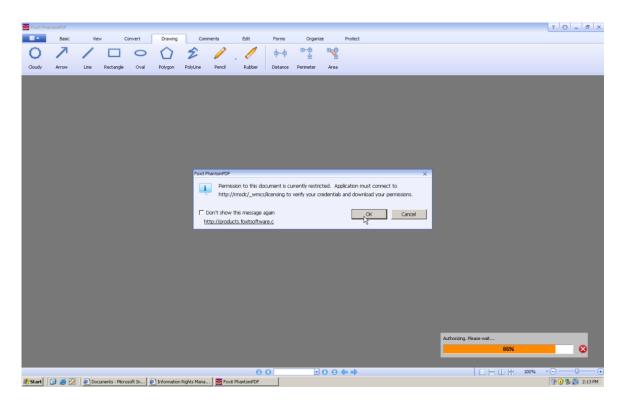
2. After the encryption is completed, authors can distribute the PDF files via email, USB, etc.

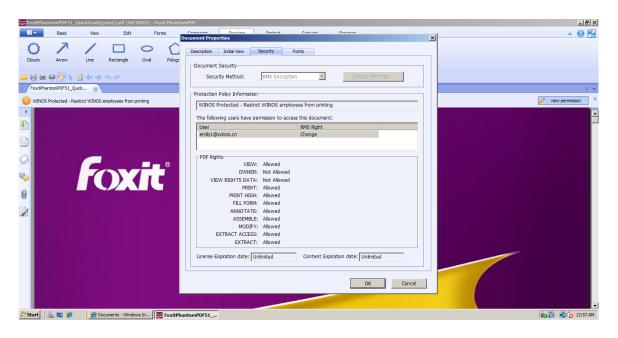
### Accessing Protected PDF Documents in Desktop Environments

For those who need to access protected PDF documents can follow these simple steps:

- After recipient receives the PDF documents, the Foxit application calls the AD RMS Client, which contacts the RMS server, which validates the user and issues a "user license".
- 2. The Foxit client application then renders the file and enforces the assigned rights.









# Foxit<sup>®</sup> PDF Security Suite Integrated with Microsoft<sup>®</sup> Active Directory<sup>®</sup> Rights Management Service

## **RMS PDF Protection Tool**

The RMS PDF Protection Tool encrypts and protects PDF files with permissions and authorization settings through programmatic interfaces to prevent sensitive information from being printed, edited, and copied by unauthorized users in Microsoft Active Directory<sup>®</sup> Rights Management Services (AD RMS) environments. The programmatic interfaces provide both Command Line Interfaces (CLI) for IT administrators to run in scripts or on-demand and C programming interfaces for developers to incorporate into existing applications.

Key features of the RMS PDF Protection Tool include:

- Programmatic protection (encrypt) and unprotection (decrypt) of PDF files with specified RMS rights policies. Shields the details of the implementation, allowing the user to protect and unprotect PDF files programmatically using a few simple interfaces.
- 2. Batch protection and unprotection of PDF files. Allows bulk, on-demand, and event-based file protection and unprotection.
- 3. Retrieval of official Rights Policy Templates from RMS servers in real-time.
- 4. Application of dynamic security watermarks. Dynamic security watermarks automatically display viewer identity information on protected PDF files in case users copy confidential information by using screen shots, cameras, mobile phone cameras, video capture, or other similar methods.
- 5. Generation of activity log files that keep a history of what files are protected/unprotected and when they were protected/unprotected.
- 6. Out of box integration with File Categorization Infrastructure (FCI).
- 7. Consistent design with the Microsoft AD RMS Bulk Protection Tool and AD RMS SDK 2.1, providing a consistent user experience to protect PDF documents in a similar workflow as protecting Microsoft Office® documents. Applies uniform security and permission settings across documents file formats.
- 8. Supports any file sharing/file repository environment to protect and unprotect files.

## Conclusion

Enhancing the value of existing IT infrastructure investments by extending AD RMS services to PDF documents is a big benefit to IT professionals. Foxit PDF Security Suite provides seamless



integration with AD RMS in SharePoint, Exchange, and desktop environments. This solution is easily installed and deployed across the enterprise. The Foxit Reader is available for download allowing for no hassle maintenance.

For organizations which are using AD RMS for their digital rights management solution, Foxit PDF Security Suite is the obvious solution for protecting sensitive PDF documents since it:

- 1) Doesn't require a new solution to be deployed and managed
- 2) Takes advantage of the security templates already in place
- 3) Requires no additional training to IT administrators
- Transparent to end users they continue to use the same solution they have already learned
- 5) Is extremely cost effective

## **About Foxit Software**

Foxit is a leading software provider of fast, affordable, and secure PDF solutions. Businesses and consumers increase productivity by using Foxit's cost-effective products to securely work with PDF documents and forms. Foxit is the #1 pre-installed PDF software, shipped on one-third of all new Windows PCs, including those from HP<sup>®</sup>, Acer, and ASUS<sup>®</sup>.

Foxit's Software Development Kits (SDKs) help developers reduce costs and improve time to market by easily integrating industry-leading PDF technology into application workflows. This technology shares the same underlying technology that powers Google's open-source PDFium project, as well as PDF reading in the Chrome browser and Android phones.

Winner of numerous awards, Foxit has over 475 million users and has sold to over 100,000 customers located in more than 200 countries. Since Foxit products are compliant with the ISO 32000-1/PDF 1.7 standard, they are compatible with existing PDF documents and forms.



Copyright © 2017 Foxit Software Incorporated. 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.