White Paper 2013

PDF Security Suite:



Foxit[®] PDF Security Suite Integrated with Microsoft[®] Active Directory[®] Rights Management Service





foxitsoftware.com

Contents

| Introduction |
|--|
| Foxit PDF Security Suite Environments |
| Enforce AD RMS Policies for PDF documents in SharePoint Environments |
| Enforce AD RMS Policies for PDF documents in Exchange Environments |
| Enforce AD RMS Policies for PDF documents in Desktop Environments5 |
| Components of Foxit PDF Security Suite |
| Foxit PDF Secure RMS Protector6 |
| Foxit PhantomPDF™ Business6 |
| Foxit Reader7 |
| PDF Security Suite in SharePoint Environments |
| IT Manager Deployment7 |
| Authoring Protection Process in SharePoint10 |
| Accessing Protected PDF Documents in SharePoint Environments11 |
| PDF Security Suite in Exchange Environments |
| IT Manager Deployment13 |
| Authoring Protection Process in Exchange Environments15 |
| Accessing Protected PDF Documents in Exchange Environments15 |
| PDF Security Suite in Desktop Environments16 |
| Authoring Protection Process in Desktop Environments16 |
| Accessing Protected PDF Documents in Desktop Environments16 |
| RMS PDF Protection Tool |
| Conclusion |
| Contact Us |

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[®] Active Directory[®] 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[®] documents only, Microsoft provides a RMS Software Development Kit (SDK) for software companies to extend AD RMS support beyond Office documents. Foxit[®] 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[®] 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™*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[®] 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



3

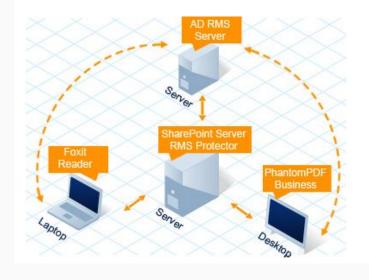
- 2) Takes advantage of the security templates already in place
- 3) Requires no additional training to IT administrators
- Transparent to end users they continue to use the same solution they have already learned to use
- 5) Is extremely cost effective.

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[®], Exchange[®], 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

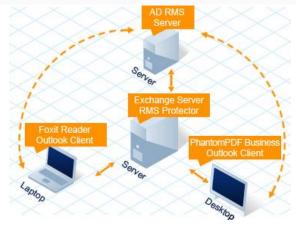
Enterprises share files in a number of ways. One of the most common is with a SharePoint server with protection provided by an AD RMS server. In this environment, Microsoft Office files are shared on the SharePoint server and then get encrypted and policy protected upon download to a client. Foxit PDF 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.





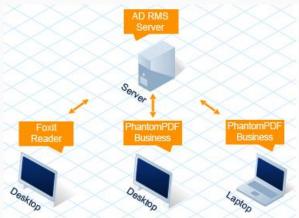
Enforce AD RMS Policies for PDF documents in Exchange Environments

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 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.





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[®] 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[®] 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

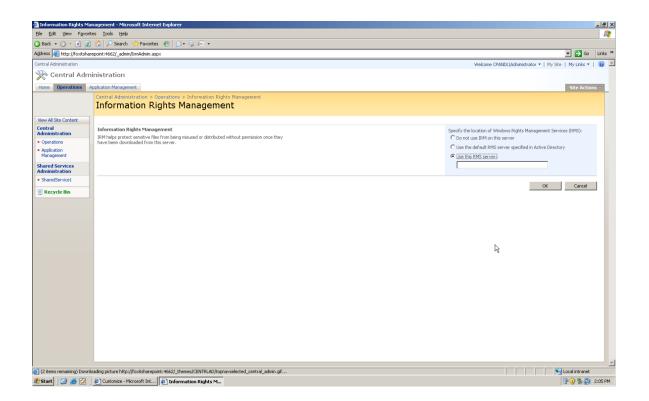
To deploy AD RMS protected files in SharePoint environments is very easy and is consistent with deploying protected Microsoft Office files.

IT Manager Deployment

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

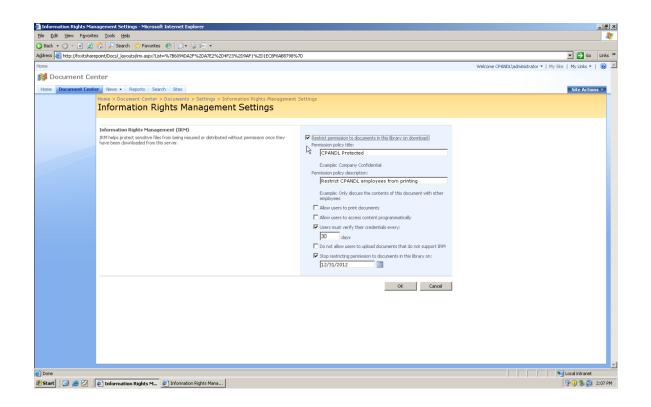
7

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



 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.





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



| Edit View Favo | | s <u>H</u> elp Search 📌 Favorites 🙆 🔗 • | | | | | _ 8 |
|----------------|----------|--|---------------------------------------|--|--|---|-------|
| | | | | 1%2D1EC8E6488798%7D docibal ist=%786 | 094DA2F%2DA7E2%2D4F23%2D9AF1%2D1EC8F6A88798%7D | ▼ 📑 G0 | Links |
| ie ie | | | | , | | Welcome CPANDL\administrator • My Site My Links • | |
| 🖡 Document C | Center | | | | | | |
| Document Ce | nter Nev | vs • Reports Search Sites | | | | Site Action | ns 🔻 |
| | | Document Center > Documents | | | | | |
| | | nissions: Docume | | | | | |
| | | s page to assign users and groups perr | nission to this library. This library | does not inherit permissions from its parent W | eb site. | | |
| | | 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 | Home 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 | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| one | | | | | | 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.
- 2. After PDF document creation, authors upload the PDF files to the IRM service enabled Document Library.





| 🎒 Upload Document - Mic | rosoft Internet Explorer | _ <u>_</u> × |
|-----------------------------|--|---|
| Ele Edit View Favorite | | 🕂 👘 🖓 |
| | 🔥 🔎 Search 👷 Favorites 🛛 😥 🕼 🔹 | |
| Address 🙋 http://foxitshare | point/Docs/_Jayouts/Upload.aspx?List=%786094DA2F%2DA7E2%2D4F23%2D9AF1%2D1EC8F6A88798%7D8RootFolder=%2FDocs%2FDocuments8Source=http%3A | %2F%2Ffoxitsharepoint%2FDocs%2FDocuments%2FForms%2FAllItem 🗾 🛃 Go 🛛 Links 🎽 |
| Home > Document Center | | Welcome CPANDL\administrator 🔻 My Site My Links 👻 🙆 🕰 |
| 💕 Document Ce | nter | |
| Home Document Cent | er News - Reports Search Sites | Site Actions * |
| | Home > Document Center > Documents > Upload Document | |
| | Upload Document: Documents | |
| | | |
| | Upload Document Browse to the document you intend to upload. | Name: |
| | er or rad de une secontente y de la testa de septembri | Browse |
| | | Add as a new version to existing files |
| | Version Comments | Version Comments: |
| | Type comments describing what has changed in this version. | Version Comments: |
| | Choose file | |
| | Look jn: DNn-ProtectedPDF - C C C C | T |
| | Source and the source of the s | |
| | 1040ez.pdf | OK Cancel |
| | My Recent FoxtPDFSecure_RMS_Protector20_SharePoint_extensions_user_guide.pdf Documents | |
| | | |
| | Desktop | |
| | | |
| | | |
| | My Documents | |
| | | |
| | My Computer | |
| | 1 | |
| | My Network File game: ptor20_SharePoint_extensions_user_guide.pdf 💌 | |
| | Places Files of type: All Files (".") | |
| | | |
| | | <u>_</u> |
| Done Done | | Local intranet |
| 🏄 Start 🛛 🚱 🥭 💋 🗍 | 🖉 Upload Document - M 👩 Information Rights Mana | 📑 🌒 🗞 🗐 2:09 PM |

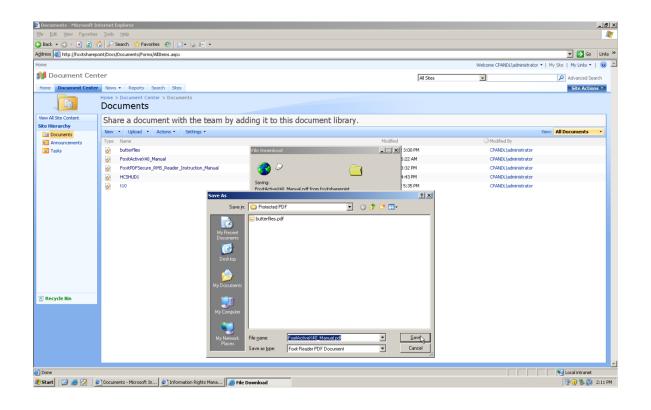
Accessing Protected PDF Documents in SharePoint Environments

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

1. 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.

| 💋 Foxik Reader | _ <u>- </u> |
|---|--------------------------|
| : File Edit View Tools Comments Forms Help | |
| 🗀 🔛 🖏 😄 🖃 🛐 🕘 🔌 📄 🛍 🏯 • 🔏 👪 ========== 🛤 > 🚉 • | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Foxit Reader | v i |
| | × |
| Permission to this document is currently restricted. Application must connect to | |
| http://ADRMS.Winos.cn/_wmcs/licensing to verify your credentials and download your permissions. | |
| | |
| Don't show this message again OK Cancel | |
| http://products.foxitsoftware.com/support.php | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Authorizing. Please wait |
| | 70% |
| | |
| | |
| 灯 Start 🛛 🚠 💻 🍘 🖉 Documents - Windows In 📝 Foxit Reader | 😥 🗐 📵 12:46 AM |





| FoxitPhantomPDF51_QuickGuide(print).pdf (SECURED) - Foxit Reader | | | _ 0 × |
|--|---|----------------------|-------------------|
| : File Edit View Tools Comments Forms Help | | | 2 |
| 🔤 🔲 🖶 🖃 🖬 ! 🖳 🕎 🕹 k 🖹 🛱 | A M Pocument Properties | x D., | 1 |
| WINOS Protected - Restrict WINOS employees from printing | Description Security Fonts | | View permission × |
| | Document Security Security Method: RMS Encrypt | on | |
| | Protection Policy Information | | |
| | WINOS Protected - Restrict WINOS emp | loyees from printing | |
| Foxit | The following users have permission to ac | cess this document: | |
| | User | RMS Right | |
| | emily1@winos.cn | Change | |
| | PDF Rights VIEW: Allowed OWNER: Not Allowed VIEW RIGHTS DATA: Not Allowed PRINT HIGH: Allowed FRLI FORM: Allowed ANNOTATE: Allowed ANNOTATE: Allowed MODIFY: Allowed EXTRACT ACCESS: Allowed EXTRACT ACCESS: Allowed EXTRACT ACCESS: Allowed License Expiration date: UnKnown | | |
| 🎊 Start 🛛 🚠 🗮 🏉 🛛 🏉 Documents - Windows In 📝 FoxitPha | antomPDF51 | | 😡 🗐 📢 12:52 AM |

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 | | | | | _8× |
|---|--|---|--|--------------------------|---------------------|
| G 🕞 - 🍌 - Computer | r ▼ Local Disk (C:) ▼ inetpub ▼ wwwroot ▼ | _wmcs - certification | | 👻 🚱 Search certification | 2 |
| Organize 👻 📄 Open 👻 | New folder | | | | 💷 🔹 🛄 🔞 |
| A Favorites E Desktop Desktop Devinads Desuminads Provinads Provinads | Name - ertification.asmx global.asax hobelbeviceCertification.asmx erver.asmx ServerCertification.asmx ServerCertification.asmx web.config toin.asmx Date modified: 6/10/2009 2:03 PT Size: 119 bytes | Several filteration General Security De Object name: C-line Group or user names: Reg. Anternational filteration Reg. System Full control Mody Read Securite Read Write Special permissions For special permissions Cick (Atrans). Learn about access co | Select Users, Computers, Service Accounts, or Groups Select Wisers, Computers, Service Accounts, or Groups Computers From this location. ppend.com Common Queries Name: Sets with | | |
| | Size IIS Oyles | | | | 1-18 AM |
| 灯 Start 🔤 🛃 | i | | | * 🖻 | 1:18 AM 4/6/2012 |

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

| 😹 Exchange Management Console | | | | | | 6 |
|--|--|-------------------------------|---------------------------------|------------------------|-----------------|-----------------------------|
| Ele Action View Help | | | | | | |
| (= e) 🖄 📅 🔢 📷 | | | | | | |
| 8 Microsoft Exchange | 🗟 Hub Transport | | | | 6 objects | Actions |
| Microsoft Exchange On-Premises (e 🔝 Organization Configuration | Remote Domains Accepted Domains E-mail | Address Policies Transport Ru | les Journal Rules Send Connecto | ors Edge Subscriptions | Global Settings | Hub Transport |
| 📇 Malbox | Y Create Filter | | | | | New Remote Domain |
| Client Access | Name | Priority A | State Co | mment | 1 | 🚳 New Accepted Domain |
| Unified Messaging | test exchange 0304 | 0 | Enabled | winneric | | Snew E-mail Address Policy |
| Server Configuration | admin to test transport rule emily0304 | 1 | Enabled | | | New Transport Rule |
| Recipient Configuration Toolbox | transport rule for test 0304 | 2 3 | Enabled Enabled | | | New Journal Rule |
| _ | using rms template for sending email | 4 | Enabled | | | New Send Connector |
| | Test Transport Rule for Encryption | 5 | Enabled | | | 🗞 New Edge Subscription |
| | | | | | | Export List |
| | | | | | | View |
| | | | | | | |
| | | | | | | Q Refresh |
| | | | | | | 👔 Help |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | <u> </u> | | | | | II |
| 1 F | | | | | | |
| 🎝 Start 🐰 🗾 🚞 | 8 | | | | | * 🕞 👘 🥼 1:19 AM 4/6/2012 |

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 | | | | | _ <u>_</u> × |
|---|---------------------------------|-------------|---|-----------|---------------------------|
| ← ⇒ 2 m 2 m | | | | | |
| Microsoft Exchange | 🗟 Hub Transp | ort | | 6 objects | Actions |
| Microsoft Exchange On-Premises (e All Organization Configuration | Remote Domains / | | 2 | 25 | Hub Transport 🔺 |
| 📇 Malbox | Y Create Filter | New T | ransport Rule | | New Remote Domain |
| Client Access | Name | New T | | | New Accepted Domain |
| Unified Messaging | test exchange (| | Introduction | | New E-mail Address Policy |
| Server Configuration Recipient Configuration | admin to test transport rule fo | 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 |
| a Toolbox | content | Actions | predefined conditions. If the condition is true for a message, the rule actions are applied to it. | | New Journal Rule |
| | using rms templi | Exceptions | Name: | | New Send Connector |
| | in test transport | Create Rule | | | 🍖 New Edge Subscription |
| | | Completion | Comment: | | Export List |
| | | | | | View |
| | | | | | Q Refresh |
| | | | | | 👔 Help |
| | | | - | | |
| | | | I ✓ Enable Rule | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | Help | < Back Next > Cancel | | |
| | | | | | |
| | | | | | |
| | | | | | , |
| 🎝 Start 🐰 🗾 🚞 | 8 | | | | * 🕞 👘 🕼 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:

- 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.



15

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.

| 🔀 FoxitPhan | tomPDF51_ | QuickGuide | (print).pdf (SEC | EURED) - Fo | xit Phanto | mPDF | | | | | | | | _ 8 > | ĸ |
|-------------|----------------|--------------|------------------|-------------|------------|-----------------------|-------------------|------------------------|--------------------|--------------------|----------|----------|---|------------------|----|
| | Basic | View | Edit | Fo | rms | Commonte Des | inn | Destact | Considert | Oreanian | | × | 1 | a 🕜 🛃 | |
| 0 | 7 | 1 | | | | ocument properties | _ | | | | | <u>م</u> | | | |
| 0 | 1 | / | | 0 | | Description Initial \ | ew Se | ecurity F | onts | | | | | | |
| Cloudy | Arrow | Line | Rectangle | Oval | Polygo | Document Security | | | | | | | | | |
| | 💷 📀 🕟 | 📑 🦛 🔿 | 50 | | | Security Meth | d: | RMS Encryptio | n 💌 | Change ! | Settings | | | | |
| | tomPDF51_Q | | | | _ | | | | _ | | | | | b • | |
| | | 0 | | | | Protection Policy In | ormation – | | | | | | | | × |
| U WINOS | Protected - Re | strict WINOS | employees from | printing | _ | WINOS Protecter | - Restrict | WINOS employ | rees from printing | | | | | view permission | |
| | | | | | | The following user | have perr | nission to acces | ss this document | | | | | | 1 |
| | | | | | | User | | | RMS Right | | | | | | |
| | | | | | | emily1@winos.cn | | | Change | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | PDF Rights | | | | | | _ | | | |
| | | | | | ® | | VIEW: | Allowed Not Allowed | | | | | | | |
| 😼 🛛 | | | | 4 | | | | Not Allowed | | | | | | | |
| | | | | | | VIEW NIGHT | PRINT: | | | | | | | | |
| 0 | | | | | | | T HIGH: | | | | | | | | |
| | | | | | | | L FORM: | | | | | | | | |
| | | | | | | | OTATE: SEMBLE: | | | | | | | | |
| | | | | | | | MODIFY: | | | | | | | | |
| | | | | | | EXTRACT | ACCESS: | Allowed | | | | | | | |
| | | | | | | E | (TRACT: | Allowed | | | | | | | |
| | | | | | | License Expiration | late: Unli | mited | Content Exp | ration date: Unlin | nited | | | | |
| | | | | | | | - I office | | | | | | | | |
| | | | | | | L | | | | | | | | | |
| | | | | | | | | | | ОК | Car | ncel | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | 1000 | | | | | | -1 |
| 灯 Start 📗 | a 📼 🏉 | / 🏉 Di | ocuments - Windo | ows In | FoxitPha | ntomPDF51 | | | | | | | | 🧓 🔂 🛃 🏠 12:57 AM | ĩ |

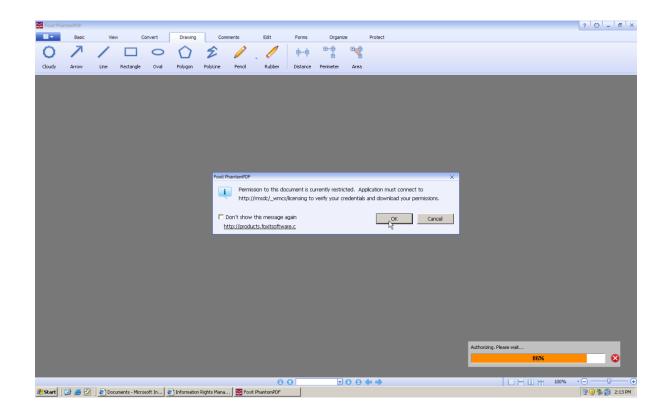
2. After the encryption is completed, authors can distribute the PDF files via email, USB, etc.

Accessing Protected PDF Documents in Desktop Environments

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

- 1. 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".
- The Foxit client application then renders the file and enforces the assigned rights.





| FoxitPhantomPDF51_QuickGuide(print).pdf (SECURED) - Foxit Phant | omPDF | _ <u>_</u> , |
|---|---|-----------------------|
| Basic View Edit Forms | Commente Dravine Dratest Convert Orannian | * 😗 🛃 |
| 0 7 / 0 0 0 | Description Initial View Security Fonts | |
| Cloudy Arrow Line Rectangle Oval Polygo | Document Security | |
| 🗀 😸 🖶 🐶 k 🔒 🖛 🔸 🥕 | Security Method: RMS Encryption Change Settings | |
| FoxitPhantomPDF51_Quick | | Þ 👻 |
| WINOS Protected - Restrict WINOS employees from printing | Protection Policy Information | 💋 view permission 🛛 × |
| | WINOS Protected - Restrict WINOS employees from printing | |
| In the second | The following users have permission to access this document: | |
| | User RMS Right emily1@winos.cn Change | |
| | | |
| | PDF Rights | |
| | VIEW: Allowed | |
| | OWNER: Not Allowed VIEW RIGHTS DATA: Not Allowed | |
| | PRINT: Allowed | |
| | PRINT HIGH: Allowed | |
| | FILL FORM: Allowed | |
| | ANNOTATE: Allowed ASSEMBLE: Allowed | |
| | MODIFY: Allowed | |
| | EXTRACT ACCESS: Allowed | |
| | EXTRACT: Allowed | |
| | License Expiration date: Unlimited Content Expiration date: Unlimited | |
| | OK Cancel | |
| 🎊 Start 🛛 🚠 💻 🏉 🔰 🌈 Documents - Windows In 🛛 🗮 FoxitPl | hantomPDF51 | 😡 🗊 🔹 👍 12:57 AM |





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[®] 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
- 4) Transparent to end users they continue to use the same solution they have already learned
- 5) Is extremely cost effective

To see for yourself how Foxit PDF Security Suite can seamlessly extend AD RMS to PDF files, try it free for 30 days. Foxit PDF Security Suite can be downloaded for a free 30-day trial by clicking here.



Contact Us

Feel free to contact us should you need any information or require support for our products. We are always here, ready to serve you better.

- Office Address: Foxit Corporation 42840 Christy Street. Suite 201 Fremont CA 94538 USA
- Mailing Address: Foxit Corporation 42840 Christy Street. Suite 201 Fremont CA 94538 USA
- Sales:
 1-866-680-3668 (24/7)
- Support: 1-866-MYFOXIT or 1-866-693-6948(24/7)
- *Fax:* 510-405-9288
- Website:
 www.foxitsoftware.com
- E-mail:

Sales and Information - sales@foxitsoftware.com Marketing Service - marketing@foxitsoftware.com Technical Support - support@foxitsoftware.com Website Questions - webmaster@foxitsoftware.com





Copyright © 2013 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 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.

