Information Rights Management in SharePoint

by André Vala
About Me...

André Vala
SharePoint Solutions Architect
Office & SharePoint Solutions Team Leader

andre.vala@create.pt
@atomicvee
http://blogit.create.pt/andrevala
http://www.linkedin.com/in/andrevala
Agenda

What is it?  Why do I need it?  How does it work?  How do I set it up?  How do I use it?  Related topics  Conclusions
Glossary

- **AD**: Active Directory
- **AD RMS**: Active Directory Rights Management Services
- **Azure RMS**: Azure Rights Management, also known as Azure Active Directory Rights Management Services (AADRMS).
- **IRM**: Information Rights Management
- **OWA**: Office Web Apps
- **RMS**: Rights Management Server/Services
What is it?
What is it?

- Set of technologies that **protect** an organization’s sensitive information from unauthorized access and **control** how the information is used.
- Uses encryption, identity and authorization policies
- Protection **stays with the files**, independently of their location
- Works across **multiple devices** – phones, tablets and PCs
Why do I need it?
The Scenario

WHY DO I NEED IT?

Document with **sensitive** information

Stored in SharePoint document library and **protected** by permissions

SharePoint Server

John has **Read** permissions on the document library

John
WHY DO I NEED IT?

The Problem

John can view its contents
John can download it

John can copy it
John can edit it

John can print it
John can send it to Jane
WHY DO I NEED IT?

The Problem

As soon as the information leaves SharePoint, it’s **no longer protected**

No protection information is included in the file and, so, the **information is free**
WHY DO I NEED IT?

The Solution

John can view its contents
John can download it

John cannot copy it
John cannot edit it

John cannot print it
John cannot send it to Jane

SharePoint Server

John

Jane
WHY DO I NEED IT?

DEMO
Demo Summary

- Difference between using IRM and not using it
- IRM support in Office Web Apps
- IRM support in Office Client
How does it work?
How does it work?

- In SharePoint, IRM protection is applied to:
  - Files in document libraries
  - Files attached to list items (but not the list items)
- Protection is applied to a file by an **IRM Protector** according to its file type
- SharePoint (on premises and online) includes protectors for:
  - Microsoft Office 97-2003 file formats (.doc, .xls, .ppt)
  - Office Open XML file formats (.docx, .xlsx, .pptx)
  - PDF file format
  - XML Paper Specification (XPS) file format
Content creation

1. User uploads **unprotected** document to IRM-enabled document library

**That's it!**

Even in IRM-enabled document libraries (or lists), documents **are not protected or encrypted when stored**.

This allows the search service to crawl the contents of the files, even in IRM-enabled libraries and lists.
Content creation

User uploads **protected** document to IRM-enabled document library

1. Issuance License validation
2. Document is **unprotected** (decrypted), document library ID is verified and document is stored.

**Important!**

File contents are never sent to RMS when protecting, unprotecting, sharing or viewing a protected document.
Content consumption

HOW DOES IT WORK?

1. User requests document from IRM-enabled document library

2. Generate **Issuance License** (IL) which includes:
   - Document key (used to encrypt the file content)
   - List of users with access to the document (SharePoint and the user that requested the document)
   - Document library ID

3. **Protect** (encrypt) the document.

4. Return document to the user.

**Important!**

Protection is applied every time a user requests a file from an IRM-enabled library. The protected document will be accessible only to the user that requested it.
HOW DOES IT WORK?

Permission mapping

IRM protection applied depends on the permissions of the user on the document library that contains the file.

<table>
<thead>
<tr>
<th>SharePoint Permissions</th>
<th>IRM Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Permissions</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
<tr>
<td>Manage Web Site</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
<tr>
<td>Edit Items</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
<tr>
<td>Manage Lists</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
<tr>
<td>Add and Customize Pages</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
<tr>
<td>View Items</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
<tr>
<td>Other</td>
<td><img src="check" alt="Full Control" /> <img src="check" alt="Read" /> <img src="check" alt="Edit" /> <img src="check" alt="Copy" /> <img src="check" alt="Save" /> <img src="check" alt="Print" /></td>
</tr>
</tbody>
</table>

*If permission is explicitly set*
HOW DOES IT WORK?

With IRM you can...

- Prevent an **authorized viewer** from:
  - Copying a document
  - Modifying a document
  - Printing a document
  - Copy and pasting the contents of a document
  - Copying the contents of a document using Print Screen on Windows
- Prevent an **unauthorized viewer** from viewing the content of a document if it is sent in an email after being downloaded from the server
- Restrict access to content to a specific period of time, after which users must confirm their credentials
With IRM you cannot...

- Prevent users from taking pictures of a document that is displayed on a screen
- Prevent users from manually copying the content of a document that is displayed on a screen and retyping it in a new document
- Prevent copying of the content through the use of third-party screen-capture programs
- Prevent erasure, theft, capture or transmission by malicious software such as trojan horses, viruses, keyloggers and spyware.
- Open protected documents on client applications, as External Users in SharePoint Online
How do I set it up?
Cloud and On Premises

- IRM is available for SharePoint Server and SharePoint Online (Office 356) but each one rely on different Rights Management components
  - SharePoint Online depends on Azure RMS
  - SharePoint Server can be used with AD RMS or Azure RMS (via RMS Connector)
## Azure RMS vs AD RMS

**How do I set it up?**


<table>
<thead>
<tr>
<th>Feature</th>
<th>Azure RMS</th>
<th>Active Directory RMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports On-Premises Servers (SharePoint Server, Exchange Server and File Servers that run Windows Server with File Classification Infrastructure (FCI))</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Online Services (SharePoint Online, Exchange Online and Office 365)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Trust between organizations and users within an organization</td>
<td>Supports implicit trust between organizations and users that use Office 365, Azure RMS or RMS for individuals.</td>
<td>Requires explicit trust using trusted user domains (TUD) or federated trust via ADFS.</td>
</tr>
<tr>
<td>Default rights policy templates</td>
<td>2</td>
<td>Not available</td>
</tr>
<tr>
<td>Support for creating new policy templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum supported versions of Office</td>
<td>Office 2010 with RMS Sharing App</td>
<td>2007 Office for Mac 2011 is supported</td>
</tr>
<tr>
<td>Minimum supported version of Windows client</td>
<td>Windows 7</td>
<td>Windows Vista SP2</td>
</tr>
<tr>
<td>RMS Sharing App support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cryptographic Mode support</td>
<td>Mode 2</td>
<td>Mode 1 (default) Requires additional configuration for Mode 2.</td>
</tr>
<tr>
<td>Key lengths and encryption algorithms</td>
<td>RSA 2048 for public key cryptography SHA 256 for signing operations AES 128 for symmetric encryption</td>
<td>RSA 1024 and RSA 2048 for public key cryptography SHA 1 and SHA 256 for signing operations AES 128 for symmetric encryption</td>
</tr>
</tbody>
</table>
Requirements

- To use IRM with **Azure RMS** you need:
  - A cloud subscription for RMS
  - Azure AD directory
  - Client devices
  - Client applications
  - Internet connectivity and access to dependent cloud services

Cloud Subscription

- At least one of the following subscriptions
  - Office 365
    - Enterprise E3 or E4
    - Education A3 or A4
    - Government G3 or G4
  - Azure RMS Standalone subscription
  - Enterprise Mobility Suite subscription
  - RMS for Individuals Subscriptions (just for consumption)

## Client Devices and Applications

<table>
<thead>
<tr>
<th>Device OS</th>
<th>Word, Excel, PowerPoint</th>
<th>Protected PDF</th>
<th>Email</th>
<th>Generic Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td>TITUS Docs</td>
<td>Foxit Reader (Azure RMS only) RMS Sharing App TITUS Docs</td>
<td>NitroDesk OWA for iOS TITUS Mail</td>
<td>TITUS Docs RMS Sharing App</td>
</tr>
<tr>
<td></td>
<td>Office Online (view)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>GigaTrust App</td>
<td>GigaTrust App Foxit Reader (Azure RMS only) RMS Sharing App</td>
<td>9Folders GigaTrust App NitroDesk OWA for Android Samsung Email (S3+) TITUS Classification for Mobile</td>
<td>RMS Sharing App</td>
</tr>
<tr>
<td></td>
<td>Office Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MacOS X</td>
<td>Office 2011 (AD RMS only)</td>
<td>RMS Sharing App</td>
<td>Outlook 2011 (AD RMS only) Outlook for Mac</td>
<td>RMS Sharing App</td>
</tr>
<tr>
<td></td>
<td>Office Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows RT</td>
<td>Office 2013 RT</td>
<td>Not Supported</td>
<td>Outlook 2013 RT Mail App for Windows</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td>Office Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Phone 8.1</td>
<td>Office Mobile (AD RMS only)</td>
<td>RMS Sharing App</td>
<td>Outlook Mobile</td>
<td>RMS Sharing App</td>
</tr>
<tr>
<td>Blackberry 10</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Blackberry Email</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

HOW DO I SET IT UP?

DEMO
HOW DO I SET IT UP?

Demo Summary

- Setting up IRM in Office 365 requires two simple steps
  1. Activate Azure RMS in your Office 365 Tenant
  2. Activate Rights Management in SharePoint Online

More info: Set up Information Rights Management (IRM) in SharePoint admin center
INFORMATION RIGHTS MANAGEMENT

How do I use it?
### Configuring IRM on a Document Library

#### HOW DO I USE IT?

**Protected › Settings**

<table>
<thead>
<tr>
<th>List Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Protected</td>
</tr>
<tr>
<td>Web Address: <a href="https://createitportugal.sharepoint.com/sites/esp2015/Protected/Forms/AllItems.aspx">https://createitportugal.sharepoint.com/sites/esp2015/Protected/Forms/AllItems.aspx</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>- List name, description and navigation</td>
</tr>
<tr>
<td>- Versioning settings</td>
</tr>
<tr>
<td>- Advanced settings</td>
</tr>
<tr>
<td>- Validation settings</td>
</tr>
<tr>
<td>- Column default value settings</td>
</tr>
<tr>
<td>- Audience targeting settings</td>
</tr>
<tr>
<td>- Rating settings</td>
</tr>
<tr>
<td>- Form settings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions and Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Delete this document library</td>
</tr>
<tr>
<td>- Save document library as template</td>
</tr>
<tr>
<td>- Permissions for this document library</td>
</tr>
<tr>
<td>- Manage files which have no checked in version</td>
</tr>
<tr>
<td>- Information Rights Management</td>
</tr>
<tr>
<td>- Workflow Settings</td>
</tr>
<tr>
<td>- Enterprise Metadata and Keywords Settings</td>
</tr>
<tr>
<td>- Information management policy settings</td>
</tr>
</tbody>
</table>

- IRM is configured on the document library or list level

- IRM is configured in 3 groups of settings
  - IRM library settings
  - Document access rights
  - Group protection and credentials interval
HOW DO I USE IT? > CONFIGURING IRM ON A DOCUMENT LIBRARY

IRM Library Settings

Set additional IRM library settings
This section provides additional settings that control the library behavior.

- Do not allow users to upload documents that do not support IRM
- Stop restricting access to the library at 4/30/2015
- Prevent opening documents in the browser for this Document Library

Prevents uploads of documents that do not support IRM, which means:
- File types for which there are no protectors installed
- File types that SharePoint cannot decrypt
- File types that are IRM protected in another program

Removes all IRM restrictions after a specific date

Prevents documents to be opened in the browser, forcing users to open them in IRM-Enlightened applications such as Microsoft Office client applications.

This can be important because, when using Office Web Apps, *screen capture cannot be prevented* as it is in the client applications.
**Document access rights**

**Configure document access rights**
This section controls the document access rights (for viewers) after the document is downloaded from the library; read only viewing right is the default. Granting the rights below is reducing the bar for accessing the content by unauthorized users.

- [ ] Allow viewers to print
- [ ] Allow viewers to run script and screen reader to function on downloaded documents
- [ ] Allow viewers to write on a copy of the downloaded document
- [ ] After download, document access rights will expire after these number of days (1-365) 90

**Prevents users from printing the document**

**Prevents code/macros to run on a document**

**Prevents users from making local editable copies of a document**

Prevents access to a document a specific number of days after it was downloaded.
Set group protection and credentials interval

Use the settings in this section to control the caching policy of the license the application that opens the document will use and to allow sharing the downloaded document with users that belong to a specified group.

- Users must verify their credentials using this interval (days): 30
- Allow group protection. Default group:
  Enter a name or email address...

Sets the duration of the document access license, in days. After the specified interval, users will be requested to validate their credentials to have access to its contents.

Specifies a group of users that can share the document, even after its downloaded.
HOW DO I USE IT?

DEMO
INFORMATION RIGHTS MANAGEMENT

Related Topics
RMS Sharing App

- RMS-Enlightened client application
- Can protect/unprotect files of any type
- Available for
  - Windows (desktop PC)
  - MacOS X (10.6.6 or above)
  - Windows Phone 8.1
  - Android (4.0.3 or above)
  - iOS (version 7.0 or above)

More info: https://portal.aadrm.com/Home/Download
RMS SHARING APP

DEMO
Logging and Auditing

- RMS logs can be used for auditing access to protected documents
- RMS logging is optional and is **not enabled by default**

**Requirements**
- An IT-managed RMS Subscription (not RMS for Individuals)
- Azure Subscription (to store the logs)
- Windows PowerShell for Rights Management

Azure RMS Logs

- Stored in an Azure storage account as blobs, in W3C extended log format
- Can take around 15 minutes for a log message to appear
- You can download the logs using PowerShell or Azure Storage SDK
- Each log message includes (among other information):
  - Date and time of the request
  - Request type (request made to the RMS API)
  - User ID
  - Content ID
  - Correlation ID (to map requests to ULS)
  - Client information (similar to User Agent strings in browsers)
  - Client IP address

LOGGING AND AUDITING

DEMO
Conclusions
Conclusions

- IRM is a great way to protect sensitive information stored in SharePoint.
- IRM can be used with SharePoint Server or SharePoint Online.
- IRM protection is embedded in the document and travels with it.
- IRM protection is applied at the library level for all documents.
- To use IRM with PDF files, a specific reader application is required.
- Any file type can be protected using the RMS Sharing App.
- RMS logging can be used for security auditing of protected information.
References

- Microsoft Rights Management Services
- RMS for IT Professionals
- Azure Rights Management
- Comparing Azure Rights Management and AD RMS
- Requirements for Azure Rights Management
- Set up Information Rights Management (IRM) in SharePoint admin center
- Apply Information Rights Management to a list or library
- RMS Sharing App
- Logging and Analyzing Azure Rights Management Usage
Thank you!

andre.vala@create.pt
@atomicvee
http://blogit.create.pt/andrevala
http://www.linkedin.com/in/andrevala