RightsWATCH and the RMS Sharing App in an Azure environment

RightsWATCH brings significant feature and functionality to the Azure RMS enterprise. RightsWATCH allows information to be classified according to the corporate security policy; it can mark/tag information in accord with that policy; and, it protects the information using the enterprise-class Azure RMS protection. All of this is accomplished without requiring additional work or effort from the user. The result is a security paradigm which supports a positive user experience, leading to quicker, more widespread Azure RMS adoption with tighter security across the enterprise. In this way, RightsWATCH drives greater ROI and accelerates implementation of the corporate security policy.

Coexistence with native Azure RMS features

RightsWATCH brings a streamlined user interface allowing information to be protected in a simpler, more streamlined fashion. However, it does not interfere with some of the advanced Azure RMS apps and features which users may wish to use, such as the RMS Sharing App. In fact, RightsWATCH works hand in hand with these apps and features to ensure optimum security across the enterprise.

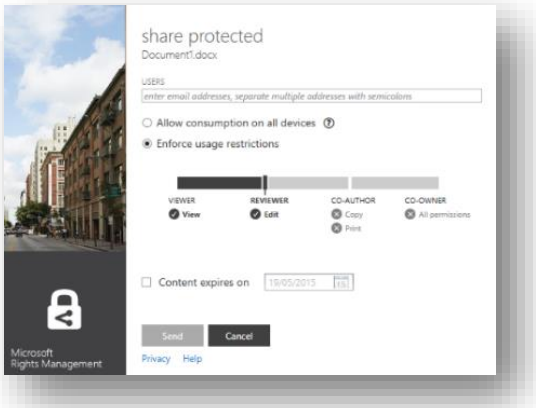
RMS Sharing App

The RMS Sharing App is an app which can be installed on Windows, Mac, Android, and iOS platforms to allow files to be protected using RMS. It is a recommended download for Azure RMS users and environments.

Share Protected feature of the RMS Sharing App

When the RMS Sharing App is installed on Windows, users are able to send RMS protected files to other parties whether they are in the same corporate network (i.e. email domain) as the sender, or not. A Shared Protected button is added to the Microsoft Office toolbar to allow quick application of RMS protection in Word, Excel, PowerPoint and Outlook.

Share Protected is always a user-driven action. If the user decides to protect a file and share with a third party, they click on the Share Protected button to send an RMS protected file to the other user. A pop-up is displayed to the user. He or she completes the selections in the pop-up making decisions regarding rights and permissions



RightsWATCH
data-centric security

Simple, in-workflow interface:

- Dynamic policy engine (content/context/ metadata) to avoid need for any user action
- Custom permissions, rights policy templates
- Watermarking and fingerprinting to be applied for the user, in accord with policy

Integrated dynamic classification engine:

- Multi–level security model giving greater control and granularity
- Role-based access and usage
- Data classification as per company policy
- Watermarking and fingerprinting per classification policy

Full BYOD support for mobile platforms:

- Read/create RMS protected email on mobile devices
- Read RMS protected Office files on mobile devices
- Read RMS protected PDF files on mobile devices
- Read Other files (.PFILE) on mobile devices

Centralized admin and activity monitoring:

- Content and license expiration
- Tracking: Save, Print, Forward, Export, etc.
- Tracking of Opens, Denied Access
- Audit trail and forensics (information tracking)

Easy leverage and exploitation of Azure, RMS and Office 365:

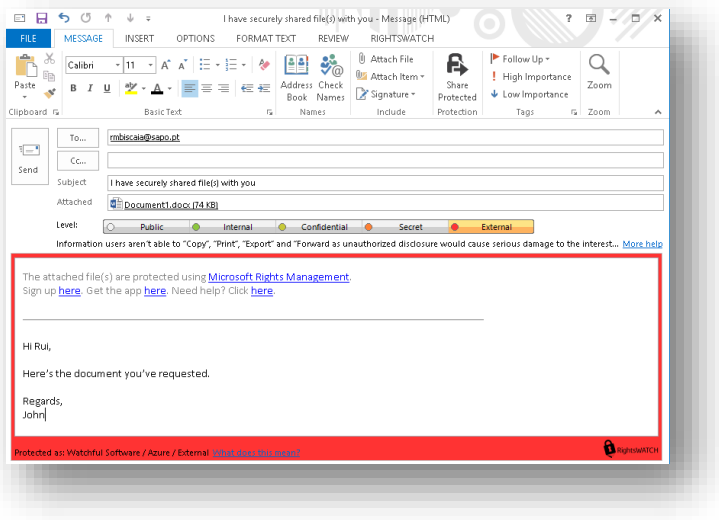
- SharePoint on-premises integration
- Webmail on-premises support (OWA)
- RMS protection of MS Outlook, MS Office files, PDF files and Other (.PFILE)

about the recipients and the file being transmitted. These selections include recipient email addresses, devices on which consumption is allowed, user rights which are allowed, and an optional expiration date attached to the file.

Once the sender clicks on the Send button, the MS Office file is automatically attached to an email in Outlook. Be aware, only the attachment is RMS protected, not the email. Information protected via Share Protected is handled outside of corporate policy; it is a user-discretionary action and decision to apply RMS protection. Any file can be shared. In this way, Sensitive data can find its way to people not intended to have access to it. Any recipient can open the file if they have an Azure RMS account. Azure RMS accounts are available for individuals and corporate users. Once again, the Share Protected feature only applies to the attached FILE… it does not encrypt or protect the email.

How can RightsWATCH enhance Share Protected?

RightsWATCH ensures corporate security policy maintenance when information is shared using the Share Protected method. If the file was previously protected with RightsWATCH using RMS protection, then sharing will be allowed under Share Protected IF AND ONLY IF the user has the usage attribute “Export” active on the file. This means that a user who only has the right to “read” an MS Office file will not be able to share that file even using Share Protected, because RightsWATCH maintains the corporate policy.



RightsWATCH also ensures that corporate policy is not violated by protecting the email which is automatically generated by Share Protected in addition to the file. This means that with RightsWATCH on top of Share Protected, the email message itself can be classified and protected, according to corporate policy, thus preventing any Share Protected file from being accessed by those that should not have access to it.

The Protect in-place feature of the RMS Sharing App

The RMS Sharing App also allows RMS information to be protected ‘in place’, enabling an RMS template to be applied to information ‘at rest’; i.e. not being shared currently. In order to do this, the user would navigate using Windows Explorer, and then right-click on the file to be protected. From the menu list, the user would select Protect in-place. The user then has to select either Custom Permissions or Corporate Template. If the user selects Custom Permissions a Share Protected-like dialog box is engaged, and the user executes the decision and enters the information.

If the user selects Corporate Template, he or she will be presented with a list of RMS templates that the company has created. The user determines which RMS template to apply to properly protect the information according to corporate policy. Having RightsWATCH deployed on top of Azure RMS, means **all sensitive information is dynamically protected according to policy at the moment of creation making it unnecessary for a user to select a Corporate Template.**

More info available at www.watchfulsoftware.com and info@watchfulsoftware.com