Azure Rights Management in **Enterprise Mobility Suite**

SYSFORE

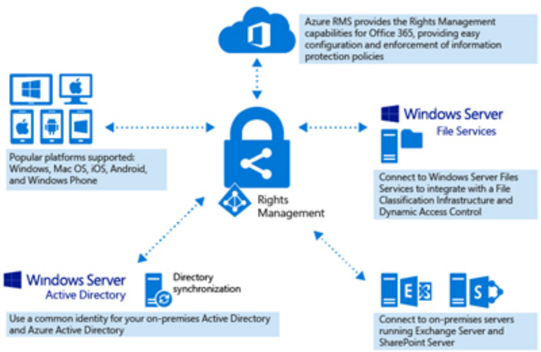
Microsoft Partner
Gold Cloud Platform

Azure Rights Management (Azure RMS) is an information protection solution for organizations that want to protect their data in today's challenging working environment. Azure Rights Management is a cloud service, and is integrated into other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory. It can also be used within your on-premises applications and services.

CHALLENGES FACED IN A WORK ENVIRONMENT

The emergence of the Bring Your Own Devices (BYOD) and the need to be Internet connected at all time, has resulted in users accessing the data from all mobile devices and at all times. They bring their own devices to work and share company information with all their partners and colleagues. The email, file sharing sites and cloud services are areas where this sensitive information can be shared.

The traditional IT protection offered by the on-premises infrastructure is limited by firewalls, access control lists and permissions. This limits effectiveness when you want to protect your company data while still empowering your users to work efficiently.



Azure RMS provides the Rights Management capabilities for Office 365, providing easy configuration and enforcement of information protection policies

Popular platforms supported: Windows, Mac OS, iOS, Android, and Windows Phone

Connect to Windows Server Files Services to integrate with a File Classification Infrastructure and Dynamic Access Control

Use a common identity for your on-premises Active Directory and Azure Active Directory

Connect to on-premises servers running Exchange Server and SharePoint Server

OVERCOME THE CHALLENGES WITH AZURE RIGHTS MANAGEMENT

Rights Management uses encryption, identity,and authorization policies to help secure your files and email. It works across multiple devices—phones, tablets, and PCs. Information can be protected both within your organization and outside your organization because that protection remains with the data, even when it leaves your organization's boundaries.

In the traditional access controls, protection is very specific and within a set location. Using the RMS, any protection that is applied, stays with the files and emails, independently of the location—inside or outside your organization, networks, file servers, and applications. This information protection solution keeps you in control of your data, even when it is shared with other people.

Using the Azure Rights Management, you can specify policies regarding what files or emails can be accessed, used or consumed. All these tasks are simplified and streamlined by using standardized policy templates.

The persistent protection that Azure RMS provides not only helps to secure your company data, but might also be legally mandated for compliance, legal discovery requirements, or simply good information management practices.

In addition, authorized people and services (such as search and indexing) can continue to read and inspect the data that Azure RMS protects. This is not easily accomplished with other information protection solutions that use peer-to-peer encryption. This is a crucial element in maintaining control of your organization's data.

HOW IS AZURE RIGHTS MANAGEMENT DIFFERENT FROM ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICE

- Active Directory Rights Management Services (ADRMS) has been available for many years as an on-premises solution for customers to protect Office documents. Microsoft Azure Rights Management is a new cloud-based solution designed to deliver the same level of protection to customers using Office 365.
- It supports Multi-Factor Authenticationfor computers and mobiles, while AD RMS supports smart card authentication.
- Azure RMS supports the RMS sharing application for Windows, Mac computers, and mobile devices. In addition, the RMS sharing application supports the sharing withpeople in another organization, email notification, a document tracking site for users, which includes the ability to revoke a document. All this is not supported in the AD RMS.
- Azure RMS supports information rights management (IRM) capabilities in Microsoft Online services such as Exchange Online and SharePoint Online, as well as Office 365. It also supports on-premises Microsoft server products, such as Exchange Server, SharePoint Server, and file servers that run Windows Server and File Classification Infrastructure (FCI).
- There are default rights policy templates that restrict access of the content to your own organization; one that provides read-only viewing of protected content and another template that provides write or modify permissions for the protected content.
- You can also create your own custom templates which the users can define their own set of permissions.

CONCLUSION

In a nutshell, the Azure Rights Management is an integral part of the Enterprise Mobility Service of Microsoft. It provides a comprehensive policy-based enterprise solution to help protect your valuable information, no matter whom you share it with.

It is a simple communication management system which integrates with your existing workloads such as Exchange, SharePoint and Office 365 to provide restricted access to your files and documents.

Easily implemented and enforced to provide standard policies which improve the data security.