IMPLEMENTATION REFERENCE GUIDE



Information Protection Using Azure Rights Management Services

Prepared for

[Customer Name]

June 20, 2014

Version .1

Prepared by

**Author**

Add Author Position to Doc Properties

Add Author Email to Doc Properties

Contributors

**Add Contributors to Doc Properties**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1.0 | Initial draft |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 7](#_Toc391034983)

[2 Assumptions 7](#_Toc391034984)

[3 Scope and Requirements 7](#_Toc391034985)

[3.1 Solution Architecture Blueprint 8](#_Toc391034986)

[3.2 Additional Customer Requirements 9](#_Toc391034987)

[4 Customer Environment Considerations 10](#_Toc391034988)

[4.1 Active Directory Considerations 10](#_Toc391034989)

[4.1.1 Active Directory Architecture – Objects 10](#_Toc391034990)

[4.2 Domain Names System (DNS), FQDN, and Server Name Considerations 12](#_Toc391034991)

[5 Azure Rights Management Services Architecture Design 12](#_Toc391034992)

[5.1 System Requirements 12](#_Toc391034993)

[5.2 Administrative Accounts 12](#_Toc391034994)

[5.3 Cryptographic Mode 13](#_Toc391034995)

[5.4 High Availability 13](#_Toc391034996)

[5.4.1 Azure Rights Management Service 14](#_Toc391034997)

[5.4.2 Directory Synchronization Tool 14](#_Toc391034998)

[5.4.3 AD FS 14](#_Toc391034999)

[5.4.4 RMS Connector 14](#_Toc391035000)

[6 Logging Design 15](#_Toc391035001)

[7 Hardware Security Modules 16](#_Toc391035002)

[7.1 Introduction 16](#_Toc391035003)

[7.2 Benefits 16](#_Toc391035004)

[7.3 Requirements 17](#_Toc391035005)

[8 Client Side Considerations 18](#_Toc391035006)

[8.1 Client Requirements 18](#_Toc391035007)

[8.1.1 Rights Management Services Client 18](#_Toc391035008)

[8.1.2 Microsoft Rights Management Sharing Application 19](#_Toc391035009)

[8.1.3 XML Paper Specification (XPS) 19](#_Toc391035010)

[8.1.4 Operating System and RMS-Enabled Applications 19](#_Toc391035011)

[8.2 Client Deployment 20](#_Toc391035012)

[8.2.1 Rights Management Services Service Discovery and Configuration Settings 21](#_Toc391035013)

[8.3 Rights Policy Template Configuration 22](#_Toc391035014)

[8.3.1 Rights Management Services Policy Templates Deployment 22](#_Toc391035015)

[8.3.2 Rights Management Services Service Discovery 23](#_Toc391035016)

[9 Server Integration Capabilities 25](#_Toc391035017)

[9.1 RMS Connector 25](#_Toc391035018)

[9.1.1 RMS Connector Considerations 25](#_Toc391035019)

[9.1.2 RMS Connector Requirements 26](#_Toc391035020)

[9.2 On-premises Exchange Integration 26](#_Toc391035021)

[9.2.1 Enabling Azure RMS Integration with On-Premises Exchange 29](#_Toc391035022)

[9.2.2 Transport Protection Rules 29](#_Toc391035023)

[9.2.3 Transport Decryption 33](#_Toc391035024)

[9.2.4 Journal Report Decryption 35](#_Toc391035025)

[9.2.5 Information Rights Management in Outlook Web App 36](#_Toc391035026)

[9.3 Integration with Exchange Online 39](#_Toc391035027)

[9.3.1 Enabling IRM integration with Exchange Online 40](#_Toc391035028)

[9.4 SharePoint Integration 40](#_Toc391035029)

[9.4.1 File Storage in SharePoint 44](#_Toc391035030)

[9.4.2 Group Protection in SharePoint 2013/Online 44](#_Toc391035031)

[9.4.3 On-premises SharePoint Integration 45](#_Toc391035032)

[9.4.4 Integration with SharePoint Online 45](#_Toc391035033)

[9.5 Integration with File Classification Infrastructure (FCI) 45](#_Toc391035034)

[9.5.1 Integration with Work Folders 47](#_Toc391035035)

[9.5.2 Enabling Azure RMS Integration with File Classification Infrastructure (FCI) 48](#_Toc391035036)

[10 Microsoft Rights Management Software Development Kit (SDK) 49](#_Toc391035037)

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar mark-ups in red. To turn this feature off, do the following:

1. Click **File**.
2. Click the **Options** on the left.
3. Click **Proofing**.
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl + H to open the **Find and Replace** box
2. Make sure your cursor is in the **Find what** box.
3. Click the **More** button at the bottom left.
4. Click the **Format** button at the bottom left and select **Style**.
5. Scroll down, locate select the **Visible Guidance**.
6. Make sure the **Replace with** box is empty.
7. Click **Replace All**.
8. If not empty - click the format button in the lower left-hand corner. Scroll down and choose **(no style)**, then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Introduction

The purpose for this implementation reference guide is to assist the consultant in designing and implementing Azure Rights Management Services (Azure RMS) in an enterprise environment.

This document contains guidance to assist the consultant in creating the Architecture and Design document for the customer, and follows the same basic document structure. This guidance is based on the recommended practices from Microsoft Services and from the Product Group.

The document is intended for the use of the consultant and is not expected to be delivered to the end customer.

1. Assumptions

The guide assumes that the reader is familiar with Rights Management Services technology. Consultants can acquire this knowledge by using step-by-step guides and other resources available on TechNet:

* Azure RMS Overview: <http://technet.microsoft.com/en-us/library/jj585024.aspx>

1. Scope and Requirements

This document provides reference guidance for designing information protection using Rights Management Services and for documenting it in the *Solution Architecture and Design* document. The design covers the following components of the solution:

* Azure RMS management
* Directory Synchronization
* Client configuration
* Mobile client configuration
* (Optional) Server-side application integration

Designing the solution basically consists of translating the customer requirements and the business scenarios defined during the Envisioning phase. These requirements and business scenarios are collected from the *Environmental Assessment Questionnaire* sent to the customer prior to the engagement, from discussion in the Envisioning Workshop, and from analyzing the network and security policy documents.

There are several optional configurations for Rights Management Services to extend the Rights Management Services to accommodate the specific business and technical requirements. The configurations include:

* Federated Identity support
* Creating and deploying rights policy templates
* Non-Microsoft mobile devices (iOS and Android)
* Integration with Exchange Server to protect data in motion
* Integration with SharePoint Server to protect data at rest
* Integration with FCI and/or Work Folders to protect data at rest
  1. Solution Architecture Blueprint

The following figure provides a visual description of the basic solution architecture blueprint.

Figure 1 Basic Solution Architecture and Components

The Azure Rights Management Services solution is a cloud service and utilizes Azure Active Directory and other infrastructure servers to add the following components to the customer production environment:

* **Azure Rights Management Services Reporting** is a component that stores Rights Management Services critical information and log data, comprising of Configuration, Directory Services, and Logging databases. This cloud service is available by Microsoft.
* **Azure Active Directory** is the directory component used by Rights Management Services to store User and Group accounts and associated email address. Rights Management Services relies on this Directory Service to authenticate users who participate in the Rights Management Services domain. The Rights Management Services service is registered in the directory to enable the users to receive the respective Rights Management Services certificates and licenses. On-premises Active Directories can be synced to Azure Active Directory using Directory Synchronization.
* **RMS Sharing Application** will consist of the Rights Management Services Client software, working together with Information Rights Management (IRM)-aware applications such as MicrosoftOffice 2010/2013 Professional Plus, and File Explorer to protect any file type.
  1. Additional Customer Requirements

The previous blueprint should cover the basic customer requirements for an Azure Rights Management Services solution. The following table lists some of the additional customer requirements and how they would affect the design of the solution.

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Design Impact** | **Guidance Available** |
| Solution needs to have high availability/contingency mechanisms. | Use network load balancing (NLB) or other load-balancing mechanisms for Directory Synchronization and supporting components | Section 5.4 |
| Solution should support Federated Identify solution. | Design and deploy Active Directory Federation Services solution. | Section 5.5.4 |
| Solution should support external users | Utilize RMS for Individuals | Section 5.7 |

Table 1 Requirements and Solution Design Impact

1. Customer Environment Considerations

Information about the customer environment should be collected through an Environmental Assessment Questionnaire sent to the customer prior to the Envisioning Workshop. This section details how this information affects the Rights Management Services solution.

* 1. Active Directory Considerations

Azure Rights Management Services requires Azure Active Directory to manage users and groups to assign specific privileges to the documents. The healthy management of Azure Active Directory is critical for Azure Rights Management Services deployment and operations.

When designing your Azure Rights Management Services environment, you should consider the following aspects of the customer Active Directory implementation:

* **The scope of a Rights Management Services subscription is the Windows Azure tenant**. If the customer has users deployed in multiple tenants, then each forest tenant requires its own subscription to Azure RMS
* **User and group accounts in Azure Active Directory can be synchronized from an on-premises Active Directory forest**. There are several tools that can be used to synchronize accounts, including the Directory Synchronization Tool, Azure Active Directory Sync, and Microsoft Identity Manager (MIM).
* **Active Directory Federation Services provides a single sign-on experience to Azure Rights Management Services and other Software as a Service (SaaS) applications integrated with Windows Azure.**  An implementation of AD FS may require the deployment of Web Application Proxy, which is a server role that includes the Active Directory Federation Services Proxy role.
  + 1. Active Directory Architecture – Objects

The following Active Directory user and computer objects are needed for Rights Management ServicesImplementation.

| **Active Directory Object** | **Description** | **Detail Options** |
| --- | --- | --- |
| **Directory Synchronization servers computer accounts** | * All servers in the Directory Synchronization Cluster must be Active Directory domain members. | * + These accounts/objects are created automatically when the computer is joined to the domain. |
| **Directory Synchronization Admin account** | * Create a user account to administer Directory Synchronization. | * + This account must have administrator privileges to Azure Rights Management. By default, global administrators have Azure RMS privileges.   + This user is needed to operate Directory Synchronization |
| **Azure Rights Management Services Admin account** | * Create a user account to administer Azure Rights Management Services architecture. | * + This account must have administrator privileges to Azure Rights Management. By default, global administrators have Azure RMS privileges.   + This user is needed to operate the RMS Connector |
| **SuperUser group** | * This sensitive group is used to grant access to Azure Rights Management Services-protected documents, even though members of this group do not have explicit rights to the documents. | * + This feature is disabled by default.   + It is highly recommended you audit the assigned Superuser group changes   + It is recommended to use an Azure Active Directory-restricted group to better manage its membership.   + The Superuser group might need to be enabled and assigned in order to use certain functionality such as Exchange Online/2013/2010 integration features. |
| **Users** | * Azure Rights Management Servicesusers must be members of a domain, and use their domain account. | * + Either user or inetOrgPerson objects can be used to represent users.   + The mail attribute must be populated with an RFC 822-compliant email address.   + The proxyAddress multi-valued attribute can store previous or alternate email addresses. |
| **Groups** | * Azure Active Directory groups to be used for the assignment of rights to documents and email. | * + Azure RMS can utilize Distribution Groups or Security Groups for the assignment of rights.   + Groups must be mail-enabled. |
| **Schema** | * The Active Directory Schema must be extended to support certain scenarios | * + If the customer will use the proxyAddress attribute and has not deployed Microsoft Exchange Server, the Active Directory schema must be extended. If the customer will not use the proxyAddress attribute or if the customer has deployed Exchange Server, no action is required   + If the customer will use the simple delegation feature, the Active Directory schema must be extended to add the msRMSDelegator and msRMSDelegatorBL attributes |
| **Active Directory Federation Services admin account (optional)** | * Create a dedicated user account to administer Active Directorycomponent. | * + For security and scalability reasons, this account does not need to have high privileges, such as Domain Admin. Make it a member of Domain Users only and or local Administrator in each Active Directory Federation Services. |

**Table 2 –** Common Active Directory Objects required by RMS

* 1. Domain Names System (DNS), FQDN, and Server Name Considerations

It is good practice to use a fully qualified domain name (FQDN) CNAME for the supporting components in the Azure RMS solution. The following table shows the recommended practices for naming in a Rights Management Services architecture.

| **Solution Scenario** | **Considerations** | **Detail** |
| --- | --- | --- |
| **Fully qualified domain name (FQDN)** | We highly recommend using FQDN names for all URLs rather than NetBIOS names. We also recommend using a FQDN name that is lower case, as some fields in AD FS are case sensitive. | FQDN names are used when configuring the RMS Connector with on-premises server workloads. For example, an RMS Connector server would have the FQDN of connector.contoso.com.  FQDN names are also used when configuring the Directory Synchronization Tool and AD FS deployments |
| **Use alias/virtual names instead of server names** | For scalability reasons, you should configure this feature. | * We recommend using virtual names so that the platform can be scaled as needed and recovered in case of a disaster. * This should be true for all RMS Connector servers in the setup. * DNS A records or CNames can be used to direct these names to the actual server. |

Table 3 DNS, URL, and Server Name Considerations

1. Azure Rights Management Services Architecture Design
   1. System Requirements

Azure Rights Management Services is managed by Microsoft and therefore, no Azure RMS server needs to be implemented into the customer environment.

* 1. Administrative Accounts

To better delegate control of your Azure Rights Management Services environment a new administrative role has been created. By default, Office 365 Global Administrator accounts have full control to manage Azure RMS settings. To grant rights to another administrator within the organization to administer Rights Management, you can specify a user or group account in Azure Active Directory using Windows PowerShell.

The following group and roles are added to the Rights Management Services components.

| Group and Roles | Description |
| --- | --- |
| Office 365 Global Administrators | The Office 365 Global Administrators hold administrator privileges on the Azure RMS tenant. Global Administrators are enabled to manage all Rights Management Services policies and settings, from enabling the service to viewing Azure RMS reports. As a recommended practice, membership of this group should be restricted to only user accounts that need full administrative control of Office 365. |
| Rights Management Services Role Based Administrator | Rights Management Services Role Based Administrators hold administrator privileges on the Azure RMS tenant. Rights Management Services Role Based Administrators are enabled to manage all Rights Management Services policies and settings, from enabling the service to viewing Azure RMS reports. However, they do not, by default, have permission to administer other aspects of Office 365 and Windows Azure. As a recommended practice, membership of this group should be restricted to only user accounts that need full administrative control of Rights Management Services |

Figure 2 Administrative Accounts

The Rights Management Services administrative role give you the opportunity to delegate Rights Management Services tasks without giving full administrative control over the entire Office 365 tenant. It is recommended to create an Active Directory security groups for the administrative role.

* 1. Cryptographic Mode

Azure RMS runs with Cryptographic Mode 2 which is an updated and enhanced RMS cryptographic implementation. It supports RSA 2048 for signature and encryption, and SHA-256 for signature. Cryptographic Mode 2 provides with enhanced security, however, it does not support Windows XP or Windows Server 2003 clients.

* 1. High Availability

The following sections detail how and why to make the Rights Management Service and supporting components highly available in the organization.

* + 1. Azure Rights Management Service

Azure Rights Management Service is delivered as a Windows Azure service and is therefore subject to the 99.9% uptime Windows Azure Service Level Agreement. Therefore, there is no action required to make the Azure Rights Management Service high available.

* + 1. Directory Synchronization Tool

It is not possible to install more than one instance of the Directory Synchronization Tool in an Active Directory forest. However, the Directory Synchronization Tool is a very lightweight install and a new instance can typically be stood up in under 30 minutes, assuming a blank virtual machine or hardware is available. While the Directory Synchronization Tool is unavailable, no new users will be synchronized to Azure Active Directory. However, existing users will continue to be able to access Azure RMS and other cloud-hosted applications.

* + 1. AD FS

AD FS can be designed with high availability and resiliency to provide authentication service for Azure RMS. When AD FS is unavailable, users will not be able to authenticate to the Azure RMS service to receive new use licenses or new certificates. Therefore, for the duration that AD FS is unavailable, users will not be able to open protected content they have not opened before and new users will not be able to bootstrap to the service. A full discussion of how to make AD FS highly available is beyond the scope of this engagement. For more information about how to make AD FS highly available, review the following TechNet articles:

* [AD FS 2.0 High Availability and High Resiliency Walkthrough](http://social.technet.microsoft.com/wiki/contents/articles/1841.adfs-2-0-high-availability-and-high-resiliency-walkthrough.aspx) (<http://social.technet.microsoft.com/wiki/contents/articles/1841.adfs-2-0-high-availability-and-high-resiliency-walkthrough.aspx>)
* [AD FS 2.0 Deployment Topology Considerations](http://technet.microsoft.com/library/gg982489(v=ws.10)) (<http://technet.microsoft.com/library/gg982489(v=ws.10))>
* [AD FS 2.0 Design Guide](http://technet.microsoft.com/library/dd807036(v=ws.10)) (<http://technet.microsoft.com/library/dd807036(v=ws.10))>
  + 1. RMS Connector

For most purposes, joining one or more RMS Connector servers to a cluster is the recommenced way to increase the availability and redundancy of your deployment. To achieve high availability, create two or more instances of the RMS Connector, define a connection URL server name, and configure a load balancing system. The connector URL can be any name under a namespace that you control. There are no special requirements for this name and it does not need to be configured on the connector servers themselves. This name does not have to resolve on the Internet unless the Exchange, SharePoint, or FCI servers are going to be communicating with the connector over the Internet.

Once the name is created in DNS and is configured for an IP address, configure load balancing for that address. You can use any IP-based load balancer for this purpose, including the Network Load Balancing (NLB) feature in Windows Server. Use the following settings to configure the NLB cluster:

* **Ports**: 80 (for HTTP) or 443 (for HTTPS)
* **Affinity**: None
* **Distribution Method**: Equal

1. Logging Design

Azure RMS logs every request that it makes for the organization, which includes requests from end users, such as for use licenses or certificates, actions performed by RMS administrators in the organizations, and actions performed by Microsoft operators to support the RMS deployment.

These RMS logs can be used to support the following scenarios:

* **Analyze for business insights**: RMS writes logs in W3C extended log format into an Azure storage account that you provide. You can then direct these logs into a repository of your choice (such as a database, an online analytical processing (OLAP) system, or a map-reduce system) to analyze the information and produce reports. As an example, you could identify who is accessing your RMS-protected data. You can determine what RMS-protected data people are accessing, and from what devices and from where. You can find out whether people can successfully read protected content. You can also identify which people have read an important document that was protected.
* **Monitor for abuse**: RMS logging information is available to you in near-real time, so that you can continuously monitor your company’s use of RMS. 99.9% of logs are available within 15 minutes of an RMS-initiated action. For example, you might want to be alerted if there is a sudden increase of people reading RMS-protected data outside standard working hours, which could indicate that a malicious user is collecting information to sell to competitors. Or, if the same user apparently accesses data from two different IP addresses within a short time frame, which could indicate that a user account has been compromised.
* **Perform forensic analysis**: If you have an information leak, you are likely to be asked who recently accessed specific documents and what information did a suspected person access recently. You can answer these type of questions when you use RMS and logging because people who use protected content must always get an RMS license to open documents and pictures that are protected by RMS, even if these files are moved by email or copied to USB drives or other storage devices. This means that you can use RMS logs as a definitive source of information for forensic analysis when you protect your data by using RMS.

RMS logging is optional. When you use RMS logging, there is no change in how RMS works and the logging process itself is free. However, to access the information, you must provide an Azure storage account for the logs and you will be charged for this storage. This storage account supports direct reading but it is not optimized to be used in this way. To reduce costs and optimize performance, we recommend that you download logs to local storage using Windows PowerShell or a custom application using the Azure Storage SDK.

Customer has decided to not provide an Azure storage account for logs and plans to retain approximately 1 year of logging information. Customer will use Windows PowerShell/a custom application to download logs to on-premises storage.

1. Hardware Security Modules

The following sections discuss the various considerations around the benefits of using Hardware Security Modules (HSMs) with Azure RMS in the Bring your own Key (BYOK) scenario.

* 1. Introduction

Hardware Security Modules are physical devices that provide a hardened, tamper-resistant environment for management and secure storage for digital keys used in Azure RMS and other applications. Microsoft requires the sole use of Thales HSMs to guarantee compliance with Microsoft datacenters. Additionally, the use of HSMs at the outset of the Azure RMS deployment is required.

Customer has decided not to implement Azure RMS with the BYOK scenario.

* 1. Benefits

HSMs provide organizations the ability to securely manage their private keys on-premises. The following table provides a summary of the benefits of implementing a Thales HSM in the Azure RMS deployment:

|  |  |
| --- | --- |
| **Benefit** | **Description** |
| **Secure Key Storage** | HSMs provide a tamper-resistant environment for the storage of private keys. All Thales HSMs are certified to meet the highest security standards. |
| **Compliance** | HSMs are FIPS 140-2 Level 3 Standard: the most widely accepted benchmark for hardware security in both enterprise and government environments. |
| **Extensibility** | Using a Thales HSM for key storage allows the Azure RMS environment to be extensible to on-premises per a future migration. Microsoft uses solely Thales HSMs for key storage in Azure RMS, therefore, a Thales HSM is required for Azure RMS. |

* 1. Requirements

The following prerequisites are required to support the BYOK scenario:

|  |  |
| --- | --- |
| Requirement | Details |
| Thales Hardware Security Module and associated components | Only Thales HSMs can be used in the BYOK scenario  The Thales nShield Connect, nShield Solo, or nShield Edge can be used in the BYOK scenario  To deploy the BYOK scenario you should have a basic operational knowledge of Thales HSMs |
| A subscription that supports Azure RMS | Note that you cannot use BYOK with the RMS for Individuals offering or Exchange Online |
| Offline x64 workstation\* | Not required if you travel to Redmond and transfer you key in person  Windows 7 or later  Thales nShield software version 11.50 or later |
| Online workstation\* | Not required if you travel to Redmond and transfer you key in person  Windows 7 or later |

Once the tenant key is created, there are two methods to transfer the key to the Microsoft datacenters:

* **Transfer the key over the Internet**: This requires some extra configuration steps, such as downloading and using a toolset and Windows PowerShell cmdlets. However, you do not have to physically be in a Microsoft facility to transfer your tenant key. Security is maintained through the process.
* **Transfer the key in person**: This requires that you contact Microsoft Customer Support Services (CSS) to schedule a key transfer appointment for Azure RMS. You must travel to a Microsoft office in Redmond, Washington, United States of America to transfer your tenant key to the Azure RMS security world.

Customer has decided to transfer the tenant key over the Internet/in person.

1. Client Side Considerations

The following sections discuss the various considerations around the requirements and deployment of the client configuration.

* 1. Client Requirements

Rights Management Services has the following requirements for client computers.

* + 1. Rights Management Services Client

| **OS** | **Requirement** |
| --- | --- |
| Windows 7  Windows 8  Windows 8.1  Windows Server 2008  Windows Server 2008 R2  Windows Server 2012  Windows Server 2012 R2 | Rights Management Service Client 2.1 (<http://www.microsoft.com/en-us/download/details.aspx?id=38396>) |

Table 29 –Rights Managment Services Client and Operative System Requirements

* + 1. Microsoft Rights Management Sharing Application

|  |  |
| --- | --- |
| **OS** | **Requirement** |
| Windows 7  Windows 8  Windows 8.1 | Microsoft Rights Management sharing application for Windows (<http://www.microsoft.com/en-us/download/details.aspx?id=40857>) |
| Windows RT  Windows Phone  iOS Mobile Devices  Android Mobile Devices | Microsoft Rights Management Sharing application (<https://portal.aadrm.com/home/download>) |

Table 30 – Microsoft Rights Management Sharing Applications

* + 1. XML Paper Specification (XPS)

| **OS** | [**Requirements**](http://www.microsoft.com/whdc/xps/viewxps.mspx) |
| --- | --- |
| Windows 7, Windows 8, and Windows 8.1 | None (already includes XPS Viewer) |

**Table 31** – XPS Viewer

* + 1. Operating System and RMS-Enabled Applications

| **OS** | **Office Version for content creation and consumption** | **Office Products** | **Editions** |
| --- | --- | --- | --- |
| Windows 7, Windows 8, and Windows 8.1  Windows Server 2008, Windows Server 2008 R2 | Microsoft Office 2010  Microsoft Office 2013 | Microsoft Office Word  Microsoft Office Excel  Microsoft Office PowerPoint  Microsoft Office Outlook  Microsoft Office InfoPath | Microsoft Office 2010 Professional Plus (Read and author content)  Microsoft Office 2013 Professional Plus (Read and author content)  All other versions of Office 2007 and 2010, including Office readers (Read content) |
| Windows Server 2008  Windows Server 2008 R2  Windows Server 2012  Windows Server 2012 R2 | Microsoft Office SharePoint 2010 Standard  Microsoft Office SharePoint 2010 Enterprise  Microsoft SharePoint Server 2013 Standard  Microsoft SharePoint Server 2013 Enterprise | - | - |

**Table 32** – RMS-aware Applications

* 1. Client Deployment

Deploying these software components to clients can be a challenge for large Azure Rights Management Services deployments, where manually installing client software is not an option. The following software distribution technologies can be used to deploy the RMS Client and RMS App.

* **Microsoft Systems Center Operations Manager (SCOM) 2012 R2 or Microsoft System Center Configuration Manager (SCCM) 2012 R2**. Organizations running SCOM 2012 R2 or SCCM 2012 R2 can use these solutions to silently deploy the Rights Management Services Client to end user computers.
* **Group Policies Objects (GPOs)**. Active Directory GPOs can be used to deploy software packages packaged using Windows Installer.

The client deployment can be achieved using software distribution infrastructure such as Systems Center Operations Manager 2012 R2, System Center Configuration Manager 2012 R2, or Active Directory Group Policy (Software Distribution). It is recommended to distribute the Rights Management Services client ahead of or at the same time as any deployment of Office so that the Rights Management Services users who try to use the IRM functionality will not be asked to download and install the Rights Management Services client software.

Please note that while Windows 7 operating systems already include the Rights Management Services client, a later version has been released (KB970099) which needs to be deployed through one of these methods, if it was not updated via the client’s normal update processes.

The following links provide you an example about how to install Rights Management Services Client.

* **How to Deploy the Rights Management Services Client**

1. <http://technet.microsoft.com/en-us/library/cc747749(WS.10).aspx>

* **How to Deploy the Rights Management Sharing Application**

1. <http://technet.microsoft.com/en-us/library/dn339003(v-ws.10).aspx>

* **Setting Up SMS or Group Policy to Support Client Deployment**

1. <http://technet.microsoft.com/en-us/library/cc747703(WS.10).aspx>
   * 1. Rights Management Services Service Discovery and Configuration Settings

The following table presents an example of client configuration settings to be deployed.

|  | **Configuration Setting** | **Recommended Providers** | **Explanation** |
| --- | --- | --- | --- |
| **1** | *RMS Client Deployment* | *SCCM/GPO/Other* |  |
| **2** | *RMS App* | *SCCM/GPO/Other* |  |
| **3** | *XPS Viewer* | *SCCM/GPO/Other* |  |
| **4** | *Office 2010/2013 Professional* | *SCCM/GPO/Other* |  |
| **5** | *Machine Certificate* | *Office 2013/RMS App* |  |
| **6** | *RAC Acquisition* | *Office 2013/RMS App* |  |
| **7** | *RMS Templates* | *Office 2013/RMS App* | *Files will be deployed through automated process for users with Office 2013 and the RMS App* |
| **9** | *XPS RMS Template Settings* | *Office 2013/RMS App* |  |
| **10** | *EUL (Licensing)* | *From documents* |  |

**Table 33** – Rights Management Services Intranet Client Configuration Settings

* 1. Rights Policy Template Configuration

Rights policy templates are used to control the rights that a user or group has on a particular piece of rights-protected content. Azure Rights Management Services stores rights policy templates in the configuration database.

To ease administration of the rights policy templates, Azure Rights Management Services features rights policy template creation through a web browser. To ease distribution of rights policy templates, Azure Rights Management Services templates are automatically refreshed for Office 2010 (when users log on), Office 2013 (every 7 days), and Office 365 (continuous). However, Exchange Online requires manual configuration to refresh templates.

For more information on rights policy template configuration and deployment in Azure Rights Management Services clients, please refer to <http://technet.microsoft.com/library/dn642472.aspx#BKMK_RefreshingTemplates>.

* + 1. Rights Management Services Policy Templates Deployment

RMS-enabled client applications, such as Microsoft Office, can use Azure Rights Management Services rights policy templates, which describe a standard set of users, rights, and conditions that can be applied to rights-protected content. When a user applies a rights policy template to content, the rights and conditions it describes become part of the publishing license.

Some Rights Management Services-enabled client applications, including Office 2013 and the RMS App, can automatically retrieve the rights policy templates from the Azure RMS service. To automatically obtain the rights policy templates for a specific user, that user must log on to Office or the RMS app with Azure Active Directory credentials. The following table specifies how templates are refreshed for end users.

| **Software** | **Update Method** |
| --- | --- |
| **Exchange Online** | * Manual configuration required to refresh templates * Performed by importing the RMS Trusted Publishing Domain again |
| **Office 365** | * Automatically refreshed |
| **Office 2013** | * Automatically refreshed every 7 days * A refresh can be forced: * One time refresh: delete the %localappdata%\Microsoft\MSIPC\Templates folder on the user computer * To change the refresh period: alter the following registry key: HKEY\_\_CURRENT\_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC\**TemplateUpdateFrequency** |
| **Office 2010** | * Refreshed when users log on |

**Table 34 –** Rights Management Services Templates Deployment

It is important to highlight that the Office 2010 UI is limited to displaying 20 templates at a time. Office 2013 UI can display up to 100 templates.

* + 1. Rights Management Services Service Discovery

Because several Rights Management Services architecture scenarios exist, as do several applications that use Rights Management Services in many different configurations, Microsoft provides different options to configure/override Rights Management Services default settings to provide information about the Certification cluster, Licensing-Only cluster, and other client-specific parameters. They are described in the following subsections.

* + - 1. Rights Management Services Service Discovery Settings (options)

The following table presents the different options available to configure the Rights Management Services Clients, the scope of each tool, and the results when these parameters are mixed.

| **Solution Component** | **Detail** | **Scope** | **Considerations** |
| --- | --- | --- | --- |
| **MSIPC/MSDRM registry entries** | * Provides the capability to override or assign the Certification and Licensing URLs | * Configured in client computer under HKLM | * Allow to modify Licensing Cluster URL/entries (used in Licensing Cluster and trusted publishing domain scenarios) * Commonly used for external clients that cannot connect to SCP (extranet/Internet) computers |
| **Microsoft Office IRM registry entries** | * IRM application settings that can override default installation procedures | * Configured in client computer under HKLM and HKCU | * Registry settings location/ entries depend on IRM Application (Office 2003/2007 and so on). * Enable you to configure additional settings such as template paths and Rights Management Services block usage, block passport authentication option in the client side, and so on |

**Table 36** – Rights Management Services Service Discovery Settings

* + - 1. Rights Management Services Architecture—Rights Management Services Service Discovery Settings (Precedence) and Implementation Strategy

The following table presents the precedence/override settings applied when you deploy/customize the Service Discovery and registry settings with different applications.

| **Solution Component** | **Applied** | **Precedence** | **Intranet Implementation Recommended Practice** | **Extranet/Non-Domain Joined Implementation Recommended Practice** |
| --- | --- | --- | --- | --- |
| **Microsoft Office IRM registry entries** | * IRM application IRM settings that can override default installation procedures | * Precedence * Override all other settings * Last to be applied | * + Use SCP for Certification Cluster.   + Use configuration in Certification Cluster for Licensing-Only clusters   + Use MSDRM/MSIPC or Office IRM application settings only when required | * + Configure Certification and Licensing Server, when required, using MSDRM/MSIPC   + Use Office IRM application settings only when required |
| **Microsoft DRM registry entries** | * Provides the capability to override or assign the Certification and Licensing URLs | * Override SCP Settings * Last to be applied |
| **Service Connection Point for RMS** | * Identifies the connection URL for the service to the RMS-enabled clients that are in your organization. Clients will not be able to discover Rights Management Services to request use licenses, PLs, or RACs without a valid SCP | * First applied * Resides in Active Directory SCP information |
| **XPS Registry Settings** | * Provides Rights Management Services Templates path for XPS Viewer | * N/A * Required for XPS to use Rights Management Services Policy Templates | * + Use MSDRM/MSIPC registry entries or XPS-specific entries | * + Use MSDRM/MSIPC registry entries or XPS specific entries and deploy through script |

**Table 37** – Rights Management Services Service Discovery Settings Implementation Strategy

1. Server Integration Capabilities

The following sections discuss how to integrate Azure RMS with server-side applications, including Exchange Server, Exchange Online, SharePoint Server, and File Classification Infrastructure through the RMS Connector.

* 1. RMS Connector

The RMS Connector enables server-side applications the ability to communicate with Azure RMS. The RMS Connector is a small-footprint service that is installed on-premises, on Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 servers. When installed, the Connector relays communication between the on-premises servers and the cloud service. The RMS Connector supports Exchange Server, SharePoint Server and File Classification Infrastructure.

* + 1. RMS Connector Considerations

The following table presents the considerations required for the RMS Connector:

| **Solution Component** | **Potential Benefits** | **Consequences** |
| --- | --- | --- |
| **Activate Azure RMS** | * Provides Azure RMS protection | * Enables on-premises servers to protect sensitive information. |
| **Directory Synchronization** | * Synchronizes on-premises Active Directory and Azure Active Directory | * Enables Azure Active Directory to work with the users and groups in an on-premises Active Directory. |
| **Enable federation** | * Provides users with a single sign on experience | * Enables a seamless user experience by using single sign-on to the RMS service. Without federation, users will be prompted for credentials before accessing rights-protected content. |
| **Two RMS Connector servers** | * Provides high availability for communication from on-premises servers | * Enables the ability to continue to use server-side IRM integration if a single node fails |

* + 1. RMS Connector Requirements
* A 64-bit physical or virtual computer running one of the following operating systems:
  + Windows Server 2012 R2
  + Windows Server 2012
  + Windows Server 2008 R2
* At least 1 GB of RAM
* A minimum of 64 GB of disk space
* At least one network interface
* Access to the Internet via a firewall (or web proxy) that does not require authentication
* Must be in a forest or domain that trusts other forest in the organization that contain installations of Exchange or SharePoint servers that you want to use with the RMS Connector
  1. On-premises Exchange Integration

In the traditional configuration, email protection with Azure RMS is mostly a client-side operation. Outlook encrypts and applies a policy to an email message and its attachments, and another Outlook client decrypts and enforces the policy. This is possible regardless of the email server platform. The following table provides a summary of the IRM features introduced in each version of Exchange:

| **Exchange Version** | **IRM Features** |
| --- | --- |
| **Exchange 2010** | * Prelicensing * Transport Protection Rules * Transport Decryption * Journal Report Decryption * IRM Decryption for Search * IRM-enabled Outlook Web App * IRM-enabled Unified Messaging |
| **Exchange 2013** | * Integration with Exchange Data Loss Prevention |
| **Exchange Online in Office 365** | * All the above features, excluding prelicensing and Outlook Protection Rules, are available in Exchange Online |

Exchange has become RMS-aware, and it can perform certain tasks with protected email that improve the experience for users and administrators.

The RMS pre-licensing agent, which is a software component of Exchange that performs a task in response to an application event, is used to deliver protected content to email recipients through Microsoft Office Outlook 2010 and later and Windows Phone.

The RMS pre-licensing agent improves the experience of Exchange users when they open rights-protected email messages. Users no longer have to wait for the email client to contact an RMS cluster to open a rights-protected message. This functionality improves the offline and mobile device synchronization scenarios. In the offline scenario, when a user is running Outlook in cache mode, rights-protected messages are pre-licensed so that if a user opens the rights-protected message when the user is offline, the content is accessible. For mobile devices that synchronize with Exchange 2010 and later, rights-protected messages that are synchronized to the devices running Windows Phone 7.5 and later.

The RMS pre-licensing agent is part of the Exchange 2010, and 2013 installation. Pre-licensing is performed by Hub Transport servers, and other server roles in the Exchange Server infrastructure do not interact directly with Azure RMS.

The RMS Client must be installed on the Exchange Hub Transport server(s) that hosts the RMS pre-licensing agent. We recommend deploying the latest version of the RMS Client. The RMS Client 1.0 is installed by default on Windows Server 2008 - X64; however, you must deploy the KB979099 update or the RMS Client 2.x on these servers. Once the RMS client is installed on the Exchange Hub Transport servers, the RMS pre-licensing agent can be enabled or disabled by executing the following commands:

Disable-TransportAgent "AD RMS Prelicensing Agent"

and

Enable-TransportAgent "AD RMS Prelicensing Agent"

After you enable or disable the agent, you must restart the transport service by running the following commands:

Net stop MSExchangeTransport

Net start MSExchangeTransport

This functionality is also available on Exchange Server 2013.

Starting with Exchange Server 2010, additional functionality has been made available to make the user experience more seamless and to enable additional management capabilities.

In addition to Exchange Prelicensing, IRM features in Exchange Server 2010 and later include:

* **Transport Protection Rules**. Provides rules-based automatic IRM protection of email messages.
* **Transport Decryption**. Gives trusted agents plaintext access to IRM-protected messages. This enables messages and attachments to be archived and scanned for malware.
* **Journal Report Decryption**. Enables IRM-protected messages to be decrypted for journaling.
* **IRM Decryption for Search**. Gives Exchange Search the ability to index content in IRM-protected messages.
* **IRM-enabled Outlook Web App**. Enables users to send and open IRM-protected messages in Microsoft Office Outlook Web App (OWA) in any OWA-supported browser without requiring the installation of client software.
* **IRM-enabled Unified Messaging**. Allows users listen to protected voicemail messages in OWA, Outlook, and on the telephone, and provides a “Do Not Forward” policy for private voicemail.

In addition to the above features, IRM features in Exchange Server 2013 and later include:

* **Integration with Exchange Data Loss Prevention**. Provides rules-based automatic IRM protection of email messages.

Configuring Azure RMS to enable these Exchange 2010/2013 features requires installing and configuring the RMS Connector and modifying registry settings on the Exchange server

* + 1. Enabling Azure RMS Integration with On-Premises Exchange

Natively, on-premises server workloads are unable to communicate with Azure RMS. To configure Azure RMS integration with on-premises Exchange, you must first install and configure the RMS Connector as referenced in section 8.1. Once the RMS Connector is installed, you will allow the Exchange servers to utilize the Connector. Then you will edit the registry settings in the Exchange server in order to allow the server to contact your Azure RMS service. Finally, you will enable Exchange IRM through the Exchange Management Shell. For more information on how to configure the RMS Connector and Exchange servers, see the Deploying the [Azure Rights Management Connector](http://technet.microsoft.com/en-us/library/dn375964.aspx#BKMK_ExchangeServer) Technet article (<http://technet.microsoft.com/en-us/library/dn375964.aspx#BKMK_ExchangeServer>).

For more information on how to enable Exchange IRM, see the [Configure IRM to Use Microsoft Azure Rights Management](http://technet.microsoft.com/en-us/library/dn151475(v=exchg.150).aspx) Technet article (<http://technet.microsoft.com/en-us/library/dn151475(v=exchg.150).aspx>).

* + 1. Transport Protection Rules

To help protect sensitive information, organizations create messaging policies that provide guidelines about how to handle this information. In Exchange Server 2010/2013, you can use transport protection rules to implement these messaging policies by inspecting message content, encrypting sensitive email content, and using rights management to control access to the content.

Transport protection rules enable you to use transport rules to IRM-protect messages by applying an RMS rights policy template or by specifying the Do Not Forward rule.

Messages containing business-critical information or personally identifiable information (PII) can be identified by using a combination of transport rule conditions, including regular expressions to identify text patterns such as social security numbers or credit card numbers. Organizations require different levels of protection for sensitive information. Some information may be restricted to employees, contractors, or partners, while other information may be restricted only to full-time employees. The desired level of protection can be applied to messages by applying an appropriate rights policy template. As illustrated in the following figure, you can create a transport protection rule to inspect message content for the words "Company Confidential", and automatically IRM-protect the message.

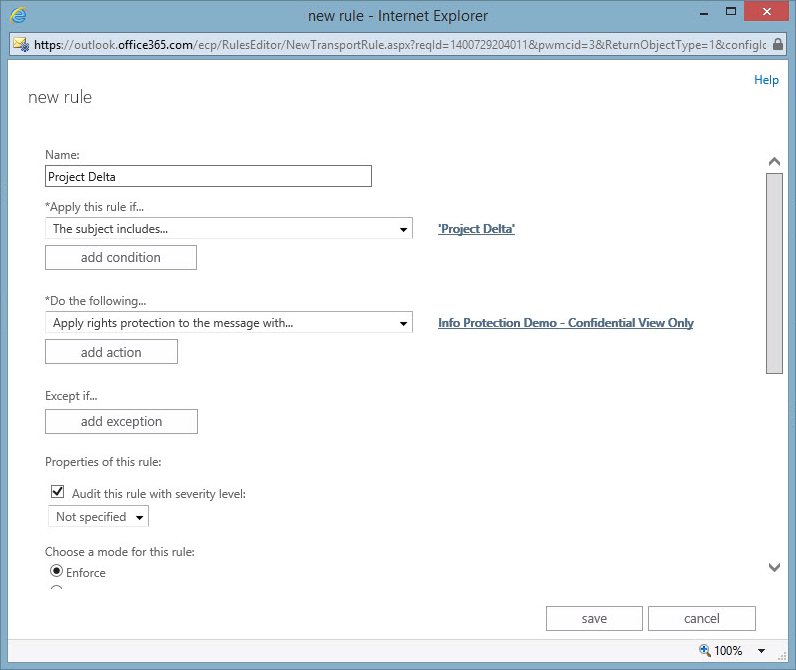


Figure 14: Creating a Transport Protection Rule

Users frequently send business-critical information and PII in email attachments using common Microsoft Office file formats such as Microsoft Office Word, Excel, and PowerPoint. All of these file formats support persistent protection via IRM, and you can make sure that the business-critical information and PII in these documents are properly protected. Transport protection rules apply the same protection to email messages and attachments in supported file formats.

Once a message is identified that matches a transport protection rule’s conditions, it will apply the protection specified in the rule. After that, the message is delivered in protected form to its recipients as a standard IRM-protected message. The sender does not see the protection of the outbound taking place, as the protection takes place after the message has left his or her mailbox and the message in the sender’s sent items folder remains unprotected.

* + - 1. http://i.msdn.microsoft.com/Global/Images/clear.gifTransport Rules Agent and Encryption Agent

When you use transport protection rules to IRM-protect messages based on rule conditions, the Transport Rules agent on the Hub Transport server inspects messages. If they meet all the conditions and none of the exceptions, it flags the message to be IRM-protected. The Encryption agent, a built-in transport agent that fires on the OnRoutedMessage event, actually applies IRM protection to the message. The Encryption agent acts on messages only if IRM is enabled for internal messages.

When the transport service is restarted, and it processes the first message that requires IRM encryption, the Encryption agent must be able to reach an Azure RMS server. For subsequent messages, the agent does not need to contact the Azure RMS server.

When planning to use transport protection rules, you must consider the type of information you want to protect and plan on creating rules accordingly. In Exchange 2010/2013, transport rules have a large number of predicates that enable you to inspect message content, including supported attachments, message headers, sender and recipient addresses, their Active Directory attributes such as department, distribution group membership, and management relationships of the sender with recipients. For more details about transport rule predicates available in Exchange 2010/2013, see the [Transport Rule Conditions](http://technet.microsoft.com/en-us/library/dd638183.aspx) TechNet article (<http://technet.microsoft.com/en-us/library/dd638183.aspx>).

You must also consider the messaging traffic in your organization, and the number of messages that will be protected using transport protection rules. Applying IRM protection to a large number of messages requires more resources on the Hub Transport server. Additionally, protecting a large number of messages or all messages also affects the client experience, particularly for Microsoft Outlook users.

* + - 1. Integration with Data Loss Prevention in Exchange Server 2013

The Data Loss Prevention (DLP) feature in Exchange Server 2013 can help you identify, monitor, and protect sensitive information in your organization through deep content analysis.

DLP policies are packages that contain sets of conditions, which are made up of transport rules, actions, and exceptions that you create in the Exchange Administration Center (EAC) and then activate to filter email messages. One action that you can configure in your DLP policies is to protect the message with Azure RMS.

DLP is a premium feature that requires an Exchange Enterprise Client Access License (CAL). For more information about CALs and server licensing, see the [Exchange Server 2013 licensing](http://office.microsoft.com/en-us/exchange/microsoft-exchange-server-licensing-licensing-overview-FX103746915.aspx) (<http://office.microsoft.com/en-us/exchange/microsoft-exchange-server-licensing-licensing-overview-FX103746915.aspx>) Microsoft web page.

* + - 1. Outlook Protection Rules

In addition to Transport Protection Rules, Exchange 2010/2013 supports Outlook protection rules to help organizations protect against the risk of information leakage by automatically applying IRM-protection to messages in Outlook 2010 and later. Unlike with Transport Protection Rules, Outlook Protection Rules protect messages before they leave the Outlook client. This protection is also applied to any attachments using supported file formats. Outlook Protection Rules only apply to Office 2010 and later clients.

When you create Outlook protection rules on an Exchange 2010/2013 server, the rules are automatically distributed to Outlook 2010/2013 by using Exchange Web Services. For Outlook 2010/2013 to apply the rule, the AD RMS rights policy template you specify must be available on users' computers.

Outlook protection rules are similar to transport protection rules. Both are applied based on message conditions, and both protect messages by applying an RMS rights protection template. However, transport protection rules are applied on the Hub Transport server by the Transport Rules agent. Outlook protection rules are applied in Outlook 2010/2013, before the message leaves the user's computer. Messages protected by an Outlook protection rule enter the transport pipeline with IRM protection already applied. Additionally, messages protected with an Outlook protection rule are also saved in an encrypted format in the Sent Items folder of the sender's mailbox.

When you use transport protection rules, users have no indication of whether a message is going to be automatically protected on the Hub Transport server. When an Outlook protection rule is applied to a message in Outlook 2010/2013, users know if a message will be IRM-protected. If required, users can also select a different rights policy template.

To create Outlook protection rules, you must use the [**New-OutlookProtectionRule**](http://technet.microsoft.com/en-us/library/dd298182.aspx) cmdlet in the Exchange Management Shell. There’s no UI in the Management Console to create Outlook Protection Rules.

When creating a rule, you can specify whether the user can override it, either by removing IRM-protection applied by the rule or by applying a different RMS rights policy template than the one specified in the rule. If a user overrides the IRM protection applied by an Outlook protection rule, Outlook 2010/2013 inserts the **X-MS-Outlook-Client-Rule-Overridden** header in the message, which enables you to determine that the rule was overridden by the user.

Outlook protection rules predicates are somewhat more limited than those for Transport Protection Rules. In particular, the ability to identify messages by content or by group membership of the sender or recipients is not present for Outlook Protection Rules, which enable you to use three predicates to automatically apply IRM protection in Outlook 2010/2013:

* **FromDepartment:** The FromDepartment predicate looks up the sender's department attribute in Active Directory and automatically IRM-protects the message if the sender's department matches the department specified in the rule. For example, you can create an Outlook protection rule to automatically protect all messages sent by the Research department.
* **SentTo:** Your organization may need to protect messages sent to certain sensitive recipients, such as the All Company or Finance distribution groups. Using the SentTo predicate, you can create an Outlook protection rule to automatically IRM-protect messages sent to specified recipients.
* **SentToScope:** The SentToScope predicate enables you to create an Outlook protection rule to automatically IRM-protect messages sent inside or outside the organization. For example, you can use the SentToScope predicate with the FromDepartment predicate to IRM-protect messages sent by a particular department to internal users.

Once Outlook identifies that a message matches an Outlook Protection Rule, it will enable protection just as if the user had selected the corresponding option manually. Depending on the rule settings, the user might be able to disable or change protection or protection will be mandatory. Once sent, the protected message acts as a manually protected message.

* + 1. Transport Decryption

Transport decryption is a capability that allows the email servers and related infrastructure to access to IRM-protected messaging content to enforce messaging policies.

For most practical purposes, RMS-protected messages can be viewed as black boxes by the messaging infrastructure, to which the content of the messages is not relevant. But content encryption can sometimes prevent certain operations from being performed on the protected messages by the servers. These restrictions could include:

* **Inability to apply messaging policies.** Messages encrypted with most client-based encryption solutions, including S/MIME, prevent content inspection on the server. Without content inspection, an organization cannot validate that all messages sent or received by its users comply with messaging policies. For example, to comply with a legal regulation, you have configured a transport rule to detect PII, such as a social security number, and automatically apply a disclaimer to the message. If the message is encrypted, the Transport Rules agent on the Hub Transport server cannot access message content, and therefore will not apply the disclaimer. This results in a violation of the policy.
* **Decreased security. If antivirus** software is unable to scan encrypted message content, this represents an organization to risk from malicious content such as viruses and worms. Encrypted messages are generally considered to be trusted by most users, thereby increasing the likelihood of a virus spreading throughout your organization. For example, you've configured an Outlook protection rule to automatically apply IRM protection to all messages sent to the All Employees distribution list with the Company Confidential rights management service (RMS) template. A user's workstation is infected with a virus that propagates by automatically using Reply All to reply to messages. If the message carrying the virus is encrypted, the antivirus scanner cannot scan the message.
* **Impact to custom transport agents.** Many organizations develop custom transport agents for different purposes, such as meeting additional processing requirements for compliance, security, or custom message routing. Custom transport agents developed by an organization to inspect or modify messages are unable to process encrypted messages. If the custom transport agents developed by your organization cannot access message content, message encryption may prevent your organization from meeting the goals for which the custom transport agents are developed.

In Exchange 2010/2013, transport decryption enables you to temporarily decrypt IRM-protected messages in transit. IRM-protected messages are decrypted by the Decryption agent, a compliance-focused transport agent.

The Decryption agent decrypts the following types of IRM-protected messages:

* Messages protected by the user in Outlook Web App.
* Messages protected by the user in Outlook.
* Messages protected automatically by Outlook protection rules in Outlook 2010/2013.

Only messages IRM-protected by the RMS server in your organization are decrypted by the Decryption agent. Messages that have been protected by external RMS servers cannot be decrypted by the Decryption agent.

Messages that have been protected by Transport Protection rules do not need to be decrypted since they are encrypted after all other transport rules have been applied.

Transport decryption is performed on the first Exchange 2010/2013 Hub Transport server that handles a message in an Active Directory forest. If a message is transferred to a Hub Transport server in another Active Directory forest, the message is decrypted again. After decryption, unencrypted content is available to other transport agents on that server. For example, the Transport Rules agent on a Hub Transport server can inspect message content and apply transport rules. Any actions specified in the rule, such as applying a disclaimer or modifying the message in any other way, can be taken on the unencrypted message. Third-party transport agents, such as antivirus scanners, can scan the message for viruses and malware. After other transport agents have inspected the message and possibly made modifications to it, it is encrypted again with the same user rights that it had before being decrypted by the Decryption agent. The same message is not decrypted again by other Hub Transport servers in the organization. Messages decrypted by the Decryption agent do not leave the Hub Transport server without being encrypted again.

* + - 1. http://i.msdn.microsoft.com/Global/Images/clear.gifConfiguring Transport Decryption

Transport decryption is configured by using the [Set-IRMConfiguration](http://technet.microsoft.com/en-us/library/dd979792.aspx) cmdlet in the Exchange Management Shell. However, before you configure transport decryption, you must provide Exchange 2010/2013 servers the right to decrypt content protected by your RMS server. This is done by adding the Federation mailbox to the super users group configured in the Azure RMS service in your organization.

Exchange 2010/2013 allows two different settings when enabling transport decryption:

* **Mandatory.** When transport decryption is set to Mandatory, the Decryption agent rejects the message and returns an NDR to the sender if a permanent error is returned when decrypting a message. If an organization does not want a message to be delivered if it cannot be successfully decrypted and actions such as antivirus scanning and transport rules are applied, it must choose this setting.
* **Optional.** When transport decryption is set to Optional, the Decryption agent uses a best-effort approach. Messages that can be decrypted are decrypted, but messages with a permanent error on decryption are also delivered. If an organization prioritizes message delivery over messaging policy, it should use this setting.
  + 1. Journal Report Decryption

If an organization encrypts messages by using traditional solutions such as S/MIME, their records managers will not be able to inspect or search the encrypted content. Archiving encrypted messages that contain inaccessible and unsearchable content may not meet business, regulatory, or compliance requirements. When faced with an electronic discovery (eDiscovery) request, an inability to decrypt, search, and present content from encrypted messages can be a challenge, and failure to do so may expose the organization to legal and financial risks.

Also, an organization's messaging policies may require journaled messages to be decrypted so the content can be accessible to eDiscovery tools, automated processes, or records managers who access a journaling mailbox. Journal report decryption in Exchange 2010/2013 can help them meet these requirements.

Journal report decryption allows an Exchange server to save a clear-text copy of IRM-protected messages in journal reports, along with the original, IRM-protected message. If the IRM-protected message contains any supported attachments that were protected by the Azure RMS service in your organization, the attachments are also decrypted.

Decryption is performed by the Journal Report Decryption agent, a compliance-focused transport agent. The Journal Report Decryption agent fires on the **OnCategorizedMessage** event. Messages protected in-transit using transport protection rules are already encrypted by the Encryption agent, which fires on the **OnRoutedMessage** event, before they get to the Journal Report Decryption agent. The Journal Report Decryption agent decrypts these messages.

The agent decrypts the following types of IRM-protected messages:

1. Messages that were protected by the user in Outlook Web App.
2. Messages that were protected by the user in Outlook.
3. Messages that were protected automatically in Outlook 2010/2013 by using Outlook protection rules.
4. Messages that were protected automatically in transit by using transport protection rules.

|  |
| --- |
| **Dd876936.important(en-us,EXCHG.141).gifImportant:** |
| Only messages that were IRM-protected by the Azure RMS service in your organization are decrypted by the Journal Report Decryption agent. The agent does not decrypt an attachment if it is not protected at the same time as the message (and therefore does not have the same use license), or if an IRM-protected file is attached to an unprotected message. |

* + - 1. http://i.msdn.microsoft.com/Global/Images/clear.gifConfiguring Journal Report Decryption

Journal report decryption is configured using the [Set-IRMConfiguration](http://technet.microsoft.com/en-us/library/dd979792.aspx) cmdlet in the Exchange Management Shell. However, before you configure journal report decryption, you must assign Exchange 2010 servers the permissions to decrypt content that is IRM-protected by your Azure RMS server. To do this, you add the Federation mailbox to the super users group configured in your organization's Azure RMS service.

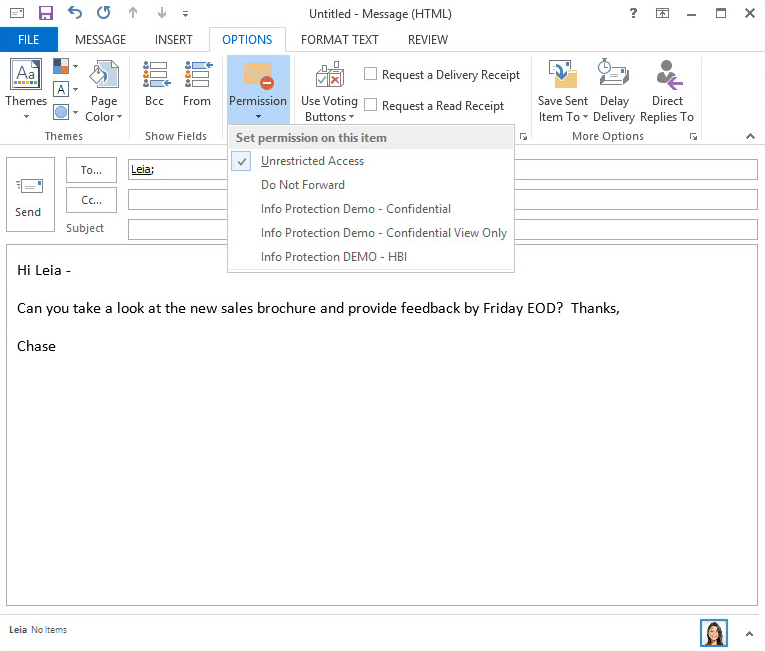
After you enable journal report decryption, the journaling mailbox may contain journal reports with sensitive information in an unencrypted form. We recommend that access to the journaling mailbox be monitored closely and restricted only to authorized individuals. This is a recommended practice even if you are not using IRM protection for email.

* + 1. Information Rights Management in Outlook Web App

In Exchange 2010/2013, IRM in Outlook Web App enables your users to access the rich IRM functionality offered by Exchange to apply persistent IRM-protection to messaging content. This capability does not require that the client computer being used to access the protected content has the Rights Management Services Client, that it has the Rights Management Add-on for Internet Explorer or that the computer is running Internet Explorer or even Windows. The client computer using OWA has to be using a browser that supports the full version of OWA.

The IRM capabilities in OWA follow closely those available in the Outlook 2010/2013 client, including:

* **Send IRM-protected messages.** As shown in the following figure, Outlook Web App users can use the permissions drop-down list and select a rights policy template to apply to the message. This enables users to send IRM-protected messages from within Outlook Web App. Messages are IRM-protected by Client Access servers.



* **IRM-protected attachments.** When users send an IRM-protected message from Outlook Web App, any files attached to the message also receive the same IRM protection and are protected by using the same rights policy template as the message. In Exchange 2010/2013, IRM protection is applied to files associated with Microsoft Office Word, Excel, and PowerPoint, as well as .xps files and email messages. IRM protection is applied to an attachment only if it is not already IRM-protected.
* **Read IRM-protected messages.** Messages protected by senders using your organization's Azure RMS cluster are rendered in the preview pane in Outlook Web App. No add-ins need to be installed, and the computer does not need to be enrolled in the Azure RMS deployment. When a user opens a message or views it in the preview pane, the message is decrypted by using the use license added by the pre-licensing agent. After decryption, the message is displayed in the preview pane. If a pre-license is not available, Outlook Web App requests one from the Azure RMS server and then renders the message.

|  |
| --- |
| **Dd876891.note(en-us,EXCHG.141).gifNote:** |
| IRM in Outlook Web App cannot prevent users from taking screen captures by using Print Screen functionality in the way Outlook and other Office applications do. This impacts the EXTRACT right, which prevents message content from being copied, if specified in the AD RMS rights policy template. |

* **Cross-browser, multiple platform IRM support.** IRM in Outlook Web App offers cross-browser, multiple-platform IRM support. IRM in Outlook Web App is supported in all browsers supported by Exchange 2010/2013, including on Apple Macintosh and Linux operating systems. To learn more about supported browsers and operating systems, see [Outlook Web App Supported Browsers](http://go.microsoft.com/fwlink/?LinkID=129362).
* **WebReady Document Viewing.** In Exchange 2010 SP1 and later, users can view supported IRM-protected attachments by using WebReady Document Viewing. This enables users to view supported attachments without having to download the attachment or use the associated application. To learn more about WebReady Document Viewing, including the supported file formats, see [Understanding File and Data Access for Outlook Web App](http://technet.microsoft.com/en-us/library/dd298113.aspx).
  + - 1. http://i.msdn.microsoft.com/Global/Images/clear.gifEnabling IRM in Outlook Web App

To enable IRM in Outlook Web App, you must add the Federation mailbox, a system mailbox created by Exchange 2010/2013 Setup, to the super users group in AD RMS. For details, see [Add the Federation Mailbox to the AD RMS Super Users Group](http://technet.microsoft.com/en-us/library/ee424431.aspx). This allows Exchange 2010/2013 servers to access IRM-protected messages.

You must also enable IRM in Outlook Web App by using the [Set-IRMConfiguration](http://technet.microsoft.com/en-us/library/dd979792.aspx) cmdlet in the Exchange Management Shell. This enables IRM in Outlook Web App for your Exchange 2010/2013 organization. You can disable or enable IRM in Outlook Web App for an Outlook Web App virtual directory. You can also control IRM in Outlook Web App at the following levels of granularity:

* **Per-Outlook Web App virtual directory.** To enable or disable IRM in Outlook Web App for an Outlook Web App virtual directory, use the **Set-OWAVirtualDirectory** cmdlet and set the IRMEnabled parameter to $false or $true (default). This enables you to disable IRM in Outlook Web App for one virtual directory on an Exchange 2010 Client Access server, while keeping it enabled on another virtual directory on a different Client Access server.
* **Per-Outlook Web App mailbox policy.** To enable or disable IRM in Outlook Web App for an Outlook Web App mailbox policy, use the **Set-OWAMailboxPolicy** cmdlet and set the IRMEnabled parameter to $false or $true (default). This enables you to enable IRM in Outlook Web App for one set of users and disable it for another set of users by assigning them a different Outlook Web App mailbox policy.
  1. Integration with Exchange Online

Email has been one of the services where customers have been moving more eagerly to the cloud. Cloud-based versions of Exchange have been available for a while, and Exchange Online in Office 365is a very popular service that is beginning to get traction even in large enterprises. With the launch of Office 365, more customers are beginning the transition to the cloud and the email service is a very critical component of this platform.

Some customers deploying Azure RMS might have moved at least some of their email server roles to the cloud, so integrating Azure RMS with those servers might be a requirement. Fortunately, Exchange Online in Office 365 can be integrated with Azure RMS, enabling customers to host their email platform while retaining control over their sensitive information.

While RMS-protected email can be delivered through Exchange Online regardless of IRM Integration, without being capable of decrypting protected email or applying IRM protection in the cloud the Exchange Online services would be unable to provide certain capabilities, such as OWA access to protected email and attachments and transport protection and decryption. So Azure RMS and Exchange Online have been designed so they can work together to provide these services.

While in theory it could be possible to do this by configuring Exchange Online to call the Azure RMS service whenever a license is required, this would have created a significant amount of traffic, latencies, and dependencies to the RMS services. In order to avoid this, the Exchange Online service has been enhanced with a subset of the capabilities of an RMS server that can locally issue licenses to protect and consume content at the Exchange Online server level without having to call back to the Azure RMS service. This is enabled by an operation by which the full Server Licensor Certificate (including the private keys) of Azure RMS, plus copies of the Rights Policy Templates, are exported to the Exchange Online services via a Trusted Publishing Domain. This way, the Exchange Online server has the capability to provide an enhanced experience for IRM-protected content to its users without having to contact the on-premises RMS cluster for each operation.

The capabilities that are provided at the Exchange Online servers with this integration are basically all the Exchange 2013 integration capabilities except for Exchange Prelicensing and Outlook Protection Rules. That is:

* OWA IRM, with the ability to author and consume protected email in the browser
* Web-ready IRM document viewing
* Transport Protection Rules
* Transport decryption for software such as online antivirus, including Forefront Online Protection for Exchange
* Journaling Decryption
* Email content indexing

Pre-licensing capabilities for Exchange Online are not available at this time, nor are Outlook Protection Rules. All the other capabilities mentioned are implemented exactly as they would in Exchange 2013.

* + 1. Enabling IRM integration with Exchange Online

In order for Exchange Online to use IRM integration, the following steps must be performed:

1. Deploy Azure RMS
2. Individually enable IRM integration capabilities in Exchange Online as with an on-premises Exchange deployment.

Once these steps are performed, individual IRM integration capabilities other than pre-licensing and Outlook Protection Rules will be available in the Exchange Online installation, and they can be managed like their on-premises counterparts.

* 1. SharePoint Integration

One of the most interesting capabilities in Azure RMS is the integration with SharePoint 2010, 2013, and SharePoint Online. SharePoint is able to store RMS-protected documents as encrypted blobs without caring much about the document’s contents, but if a document is encrypted in a way that cannot be decrypted by SharePoint, the document will not be indexed and users will not be able to utilize search capabilities to find the document based on its content. With Azure RMS and SharePoint 2010 or later, explicit support for this combination is included in the products through the inclusion of the Office Protector component in SharePoint that allows for the automatic application of IRM policies to documents downloaded from libraries based on portal users’ rights.

With SharePoint Services, IRM is available for files that are located in document libraries and stored as attachments to list items. SharePoint site administrators can elect to protect downloads from a document library with IRM. When a user attempts to download a file from the library, SharePoint verifies that the user has permissions to the given file, and issues an IRM license to the user that enables access to the file at the appropriate permissions level. SharePoint then downloads the file to the user's computer in an encrypted, rights-managed file format.

IRM is enabled at the SharePoint document-library level by an administrator, and protection includes the following options:

* Whether or not users can print documents that are rights-managed.
* Whether the user can run Microsoft Visual Basic for Applications (VBA) and other custom code in the file.
* The number of days for which the license is valid. After the specified number of days has passed, the license expires, and the user must download the file again from the document library.
* Whether to allow users to upload file types that do not support IRM.
* Optionally, the date to stop restricting permissions to the document library. After the specified date passes, SharePoint removes all rights-management restrictions from the documents in the library.

When a SharePoint administrator enables IRM for a list or library, it can protect any file type in that list or library for which a protector is installed on all front-end Web servers. A protector is a program that controls the encryption and decryption of rights-managed files of a specific file format.

SharePoint 2010 includes protectors for the following file types:

* Microsoft Office 2007 InfoPath forms
* The 97-2003 file formats for the following Microsoft Office programs: Word, Excel, and PowerPoint
* The Office Open XML Formats for Microsoft Office Word, Excel, and PowerPoint
* The XML Paper Specification (XPS) format

SharePoint 2013 includes the above protectors and also protectors for the following file types:

* PDF files (requires an RMS-aware PDF reader to open the protected files)
* The ability to view protected content in the web interface

The ability to protect different file types depends on the availability of protectors for those file types. If an organization plans to use Azure RMS to protect other file types in addition to those listed above, the server administrator will need to check for the availability of such protectors from the applications manufacturers or from third parties specialized in RMS-based solutions. If they exist, those protectors need to be installed in the SharePoint server.

When IRM is enabled for a library, rights management applies to all of the files in that library. When it is enabled for a list, rights management applies only to files that are attached to list items, not the actual list items.

SharePoint assigns the rights that will be applied to a document for the user downloading it based on the access control list (ACL) on the library. If a user has access to the library, documents are delivered to the user with rights management applied to allow access to the user only with rights depending on the options set for the library and the access level the user has to the library.



**Figure 15:** SharePoint protected document flow

A typical document flow in SharePoint with Azure RMS protection is as follows:

1. A content author (publisher) posts a Microsoft Office document to a SharePoint document library that has Azure RMS protection enabled.
2. The document is stored in the SharePoint database unencrypted and unprotected. If the document was protected with IRM by the user, protection is stripped at this point. If the document was protected manually by a user before uploading to the library, the existing protection is preserved.
3. A different user (document consumer) with read access to the documents in the library requests the document from the SharePoint server.
4. The server retrieves the document from the database.
5. The server uses the user’s Rights Account Certificate and its Client Licensor Certificate to assign rights to the user to the document requested depending on the users rights on the documents in the library with additional restrictions according to the policies established in the library, and applies the rights to the document.
6. The protected document is sent to the user, and the user opens it in the Office application with the help of the Rights Management Client with the rights defined by the policy.

When people download files in an IRM-enabled list or library, the files are encrypted so that only authorized people can view them. Each rights-managed file also contains an issuance license that imposes restrictions on the people who view the file. Typical restrictions include making a file read-only, disabling the copying of text, preventing people from saving a local copy, and preventing people from printing the file. Client programs that can read IRM-supported file types use the issuance license within the rights-managed file to enforce these restrictions. This is how a rights-managed file retains its protection even after it is downloaded from the server.

The whole process is transparent to both users and does not require special operations from them, while the platform provides assurance the documents will be always protected according to the policies defined for the library.

The types of restrictions that are applied to a file when it is downloaded from a list or library are based on the individual user’s permissions on the SharePoint site that contains the file. The following table explains how the permissions on SharePoint sites correspond to IRM permissions.

|  |  |
| --- | --- |
| SharePoint permissions | IRM permissions |
| Manage Permissions, Manage Web Site | **Full control** (as defined by the client program): This permission generally enables a user to read, edit, copy, save, and modify permissions of rights-managed content. |
| Edit Items, Manage Lists, Add and Customize Pages | **Edit, Copy, and Save**: A user can print a file only if the **Allow users to print documents** check box is selected on the Information Rights Management Settings page for the list or library. |
| View Items | **Read**: A user can read the document, but cannot copy or modify its content. A user can print only if the **Allow users to print documents** check box is selected on the Information Rights Management Settings page for the list or library. |
| Other | No other permissions correspond directly to IRM permissions. |

* + 1. File Storage in SharePoint

Because companies often have restrictions that require their files to be stored in non-encrypted formats, SharePoint does not internally store files in rights-protected (encrypted) file formats. However, SharePoint calls an IRM protector to convert the stored file to an encrypted format each time a user downloads the file. Similarly, when a user uploads a file that was previously protected by the SharePoint protector after being downloaded from the same library, SharePoint calls the appropriate IRM protector to convert the document to a non-encrypted format before it is stored.

As a result, it is not necessary to create custom solutions to enable searching or archiving of document libraries where IRM is enabled. Storing the files in unencrypted format enables the current Search indexing service to crawl content stored on the servers.

Most companies that use SharePoint also use its search capabilities extensively, and combining this discoverability with the ability for the platform to keep the documents protected after delivery to the users is an excellent solution to deliver flexible access to information without compromising confidentiality or privacy. With SharePoint, search results are scoped to user permissions, so the user never sees search results that include content to which they do not have access.

* + 1. Group Protection in SharePoint 2013/Online

When documents are downloaded from an IRM-enabled SharePoint document library, by default each supported file type is encrypted and rights are restricted to the authenticated user who downloaded the documents. Other users who have rights to the same library must get their own copy. One of the new features that SharePoint 2013 supports is to protect a library for a group. An admin can choose an Active Directory group and use it to stamp the usage license for the file. Then, documents that are downloaded can be used by all the members of the group, and the user who downloaded the copy can transfer the copy to any member of the group directly.

* + 1. On-premises SharePoint Integration

Natively, on-premises server workloads are unable to communicate with Azure RMS. To configure Azure RMS integration with an on-premises SharePoint instance, you must first install and configure the RMS Connector as referenced in section 8.1. Once the RMS Connector is installed, you will allow the SharePoint servers and corresponding service accounts to utilize the Connector. Then you will edit the registry settings in the SharePoint server in order to allow the server to contact your Azure RMS service. Finally, you will enable SharePoint IRM through the SharePoint Administration Console. Once IRM has been enabled, document libraries and lists can be configured to use Azure RMS. For more information on how to configure the RMS Connector and SharePoint servers, see the [Deploying the Azure Rights Management Connector](http://technet.microsoft.com/en-us/library/dn375964.aspx#BKMK_ConfiguringSharePoint) Technet article (<http://technet.microsoft.com/en-us/library/dn375964.aspx#BKMK_ConfiguringSharePoint>).

For more information on how to enable SharePoint IRM, see the [Set up Information Rights Management (IRM) in SharePoint admin center](http://office.microsoft.com/en-us/office365-sharepoint-online-enterprise-help/set-up-information-rights-management-irm-in-sharepoint-admin-center-HA102895193.aspx) article (<http://office.microsoft.com/en-us/office365-sharepoint-online-enterprise-help/set-up-information-rights-management-irm-in-sharepoint-admin-center-HA102895193.aspx>).

* + 1. Integration with SharePoint Online

IRM integration with SharePoint Online relies on Azure RMS to encrypt and assign usage restrictions. Currently, SharePoint Online contains the same feature set as SharePoint 2013 including protection to document libraries and lists, Group Protection, and limiting uploaded content to IRM-enabled applications. To use IRM integration in SharePoint Online, you must first have an Azure RMS subscription, then enable the IRM service through the SharePoint admin center.

For more information on how to configure IRM with SharePoint Online, see the [Set up Information Rights Management (IRM) in SharePoint admin center](For%20more%20information%20on%20how%20to%20configure%20the%20RMS%20Connector%20and%20SharePoint%20servers,%20see%20the%20Deploying%20the%20Azure%20Rights%20Management) article (<http://office.microsoft.com/en-us/office365-sharepoint-online-enterprise-help/set-up-information-rights-management-irm-in-sharepoint-admin-center-HA102895193.aspx>).

* 1. Integration with File Classification Infrastructure (FCI)

FCI is a new feature within File Server Resource Manager starting with Windows Server 2008 R2 that defines classification properties, automatically classifies files based on location and content, and applies file management tasks such as file expiration and custom commands. One such task that FCI can perform on files is to protect them with manual Azure RMS protection (requires Windows Server 2012 or later) or a rights policy template. For example, using FCI, an administrator could create classification properties such as High Business Impact and Low Business Impact. Then the administrator could create a classification rule that assigns a value of High Business Impact to files that contain a certain regular expression pattern (such as would correspond to a social security) or string pattern or are located in particular folders. Finally, the administrator could create a task that automatically applies Azure RMS protection to files that have been tagged with the High Business Impact classification property.

Integration with File Classification Infrastructure provides a mechanism to automatically protect sensitive information, as defined by the administrator, with Azure RMS. End users can forget to apply Azure RMS protection to sensitive files. When an end user saves such a file to a file server that has FCI installed and integrated with Azure RMS, FCI will periodically scan new files saved to the file server for matches to particular content or folder location. It will discover and classify the new unprotected document and then apply the Azure RMS protection. The next time the user opens the document, he will find that it has been protected with Azure RMS.

The following diagram depicts a user creating a document and storing it on a file server equipped with FCI. The document is then protected with RMS.



* + 1. Integration with Work Folders

Work Folders is a role service for file servers running Windows Server 2012 R2 and later that provides a consistent way for users to access their work files from their PCs and devices. This functionality is powered by the Work Folders service, which is part of the File and Storage Services role. With Work Folders, users can store and access work files on personal computers and devices, often referred to as bring-your-own device (BYOD), in addition to corporate PCs. Users gain a convenient location to store work files, and they can access them from anywhere. Organizations maintain control over corporate data by storing the files on centrally managed file servers, and optionally specifying user device policies such as encryption and lock-screen passwords.

Work Folders can be deployed on file servers that also have File Classification Infrastructure installed. This scenario extends the automatic protection of data at rest in file servers to the end users. End users may save an unprotected document to their documents folder. The document is then redirected to a corresponding folder on the file server. Once the document is saved, FCI scans the document, discovers that the file contains specific content or is saved to a particular location that prompts FCI to apply a particular classification property. FCI then applies Azure RMS protection to the file. The next time the user accesses the document, she will find that the document is now protected with Azure RMS.

The following diagram depicts a user creating a document and storing it in the Work Folders store on his computer. Work Folders syncs the file to the file server and RMS is applied to the document. Work Folders syncs the file to the local computer and the user locally stores a protected copy of the file:



Note that Work Folders requires client computers run Windows 8.1 or later or Windows RT 8.1 or later.

* + 1. Enabling Azure RMS Integration with File Classification Infrastructure (FCI)

Natively, on-premises server workloads are unable to communicate with Azure RMS. To configure Azure RMS integration with File Classification Infrastructure (FCI), you must first install and configure the RMS Connector as referenced in section 8.1. Once the RMS Connector is installed, you will allow the FCI servers to utilize the Connector. Then you will edit the registry settings in the FCI server in order to allow the server to contact your Azure RMS service. Finally, you will implement FCI policies to apply Azure RMS protection to documents. For more information on how to configure the RMS Connector and FCI servers, see the [Deploying the Azure Rights Management Connector](http://technet.microsoft.com/en-us/library/dn375964.aspx#BKMK_FileServer) Technet article (<http://technet.microsoft.com/en-us/library/dn375964.aspx#BKMK_FileServer>).

1. Microsoft Rights Management Software Development Kit (SDK)

The Microsoft RMS SDK  platform enables developers to build applications that leverage Azure RMS to provide information protection. The RMS SDK 3.0 handles support for mobile device applications. The RMS SDK 2.1 handles complex security practices such as key management, encryption and decryption processing, and offers a simplified API for easy application development.

These RMS SDKs can be used to customize an Azure RMS deployment. For example, the RMS SDK 2.1 can be used in the following scenarios:

* Extend granular-level permissions to applications that are not RMS aware by default, such as CAD systems or Adobe Photoshop.
* Automatically apply RMS protection to data upon download from a repository, such as an SAP application.
* Automatically decrypt protected content to make the content available to server-side applications such as Data Loss Prevention applications.

The RMS SDK 2.1 is available from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=38397) (<http://www.microsoft.com/en-us/download/details.aspx?id=38397>).

The RMS SDK 3.0 is available for Windows Phone 8, Windows Store, Android, OS X, and iOS from the Microsoft Download Center:

|  |  |
| --- | --- |
| SDK 3.0 | Download Location |
| Windows Phone 8 | <http://www.microsoft.com/en-us/download/details.aspx?id=39703> |
| Windows Store | <http://www.microsoft.com/en-us/download/details.aspx?id=39701> |
| Android | <http://www.microsoft.com/en-us/download/details.aspx?id=39705> |
| OS X | <http://www.microsoft.com/en-us/download/details.aspx?id=40849> |
| iOS | <http://www.microsoft.com/en-us/download/details.aspx?id=39702> |