Detailed Design



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 for discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

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

Table of Contents

[1 Introduction 7](#_Toc391038758)

[2 Audience 7](#_Toc391038759)

[3 <<Customer Name>> Azure RMS Architecture 8](#_Toc391038760)

[3.1 Azure Rights Management Services Architecture Components 8](#_Toc391038761)

[3.2 Solution Physical Design 10](#_Toc391038762)

[3.2.1 Windows Azure Tenant 10](#_Toc391038763)

[3.2.2 Active Directory Considerations 11](#_Toc391038764)

[4 Azure Rights Management Services Design 12](#_Toc391038765)

[4.1 Server List 13](#_Toc391038766)

[4.2 Availability Model 13](#_Toc391038767)

[4.3 Administration and Service Accounts 13](#_Toc391038768)

[4.4 Windows Security and Distribution Groups 15](#_Toc391038769)

[4.5 OUs and Group Policies 16](#_Toc391038770)

[4.6 Azure RMS Templates 18](#_Toc391038771)

[4.7 Client Design 19](#_Toc391038772)

[4.7.1 Rights Management Services Client 20](#_Toc391038773)

[4.7.2 Rights Management Sharing Application 20](#_Toc391038774)

[4.7.3 XML Paper Specification (XPS) client 21](#_Toc391038775)

[4.7.4 Operating System and RMS Enabled Applications 21](#_Toc391038776)

[4.7.5 Installation Mode 22](#_Toc391038777)

[4.8 Windows Firewall Configuration 23](#_Toc391038778)

[4.9 System Recommendations 23](#_Toc391038779)

[4.9.1 RMS Connector Server Hardware and Components 23](#_Toc391038780)

[4.9.2 Directory Synchronization Tool Server Hardware and Software Configuration 24](#_Toc391038781)

[4.9.3 Database Configuration 24](#_Toc391038782)

[4.10 Security Design 25](#_Toc391038783)

[4.10.1 Rights Management Services Account Certificates 25](#_Toc391038784)

[4.10.2 Azure RMS Private Key 26](#_Toc391038785)

[4.10.3 Rights Management Services User Authentication 26](#_Toc391038786)

[4.11 Server Integration Configuration 27](#_Toc391038787)

[4.11.1 RMS Connector 27](#_Toc391038788)

[4.11.2 Integration with SharePoint 2013/2010 27](#_Toc391038789)

[4.11.3 Integration with SharePoint Online 28](#_Toc391038790)

[4.11.4 Exchange Prelicensing 28](#_Toc391038791)

[4.11.5 Integration with On-premises Exchange Server 2013/2010 29](#_Toc391038792)

[4.11.6 Integration with Exchange Online 30](#_Toc391038793)

[4.11.7 Integration with File Classification Infrastructure and Work Folders 31](#_Toc391038794)

**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

Azure Rights Management Services (Azure RMS) is a technology that provides persistent protection to digital data using encryption, certificates, and authentications. The technology requires careful planning and review before deployment. Therefore, the Azure RMS design needs to be documented and examined to properly verify that all required goals are have been incorporated and the solution aligns with <<Customer Name>>’s vision. This ensures that the desired Rights Management Services development and deployment will be achieved with minimal issues.

This document is intended to act as the primary point of reference for the <<Customer Name>>’s Information Protection Using Azure Rights Management Services solution design to be used during deployment and configuration.

After surveying and fully understanding <<Customer Name>>’s requirements and identifying its expectations, a technical solution using Azure Rights Management Services was designed and is detailed in this document. The design defined in this document is derived from the one defined during the Envisioning Workshop, incorporating the detailed information and requirements surveyed afterwards.

This document provides an overview of the solution components and how they interact with each other, and then goes into detail on the configuration for each of these components.

This document does not cover the implementation strategy for the solution, which is detailed in a separate *Deployment Plan* document.

1. Audience

This paper is intended for the <<Customer Name>> teams (and their managers) who have the responsibility for architecting, designing, and operating information protection solutions within the organization.

1. <<Customer Name>> Azure RMS Architecture

*This section expands on the high-level design developed during the Envisioning Workshop and documented afterwards. Use the corresponding materials from the Envisioning Workshop and details gathered afterwards to complete this section as needed.*

<<Customer Name>> chose to use Azure Rights Management Services to build an Information Protection solution that can address their business and technical requirements.

Rights Management Services is a security technology that works with applications to help safeguard the digital content—no matter where it goes—for people who need to protect sensitive web content, documents, and e-mail. Users can define exactly who can open, read, modify, and redistribute the content. Organizations can create rights policy templates that enforce policies that can be applied to content. Responding to customer demand for improved content protection, Microsoft designed Rights Management Services as an extensible platform, capable of integration into third-party applications as well as into Microsoft Office.

Azure Rights Management Services allows documents to be shared and sent in e-mail messages while helping maintain control over who can view or edit the document. Once a document or an e-mail message is protected with this technology, the access and usage restrictions are enforced no matter where the information goes; even if the file is sent outside the firewall. Because Azure RMS protection is embedded in the file, usage restrictions will persistently be enforced.

* 1. Azure Rights Management Services Architecture Components

The following components are part of the Azure Rights Management Services architecture:

* Directory Service
* Azure Rights Management Service hosted by Windows Azure
* Rights Management Services Clients (Windows 8.1, Windows 8 and Windows 7)
* RMS-aware applications (Microsoft Office 2013, 2010, Rights Management Sharing Application, etc.)
* RMS compatible mobile devices (Windows Phone, iOS, Android)
* Windows Azure Storage Account (optional)
* RMS Connector servers (optional)
* SharePoint Server 2013/2010 libraries and SharePoint Online services (optional)
* Exchange Server 2013/2010 servers and Exchange Online services (optional)
* Windows Server 2012 R2/Windows Server 2012 File Classification Infrastructure (optional), Windows Server 2012 R2 and Windows 8.1 Work Folders (optional)
* Hardware Security Module (optional)
* Identity synchronization tool
* Active Directory Federation Services (optional)

The Directory Service is a core architectural component used by Azure Rights Management Services as Azure RMS relies on the Directory Service to authenticate users who participate in the Rights Management Services environment. Directory Service is also required to validate effective user permissions using group expansion based on Active Directory service group membership.

The Rights Management Services Client will consist of the Rights Management Services Client software, RM-enabled applications such as Microsoft Office 2013 Professional Plus, Microsoft Office 2010 Professional Plus, and the XPS client. Optionally, the Rights Management Sharing Application can be used to extend Azure RMS protection to files of any file type and support additional client-side scenarios.



Figure 1 - Rights Management generic solution Architecture and Components

* 1. Solution Physical Design

*Paste the services to be provided by the solution. The items listed below are provided as examples.*

The core criteria for the Azure RMS design are listed below.

* The solution must provide protection capabilities to users in the core Intranet forests at <<Customer Name>>.
* The solution will be extensible to external users using cloud-based authentication such as Azure RMS or RMS for Individuals.
* The solution must simplify operations, maintenance, and implementation as much as possible.
* The solution must maximize the protection of the Azure RMS cluster through the use of a Hardware Security Module
* Content Pre-licensing will be provided to all users of Exchange that are using Exchange 2010 or later servers installed in the Intranet forest.
* Transport Protection Rules, Outlook Protection Rules, Transport Decryption, and Journal Decryption will be provided to users of Exchange 2010 or later servers installed in the Intranet Forest.
* Automated protection of documents stored in SharePoint libraries supported by servers in the aforementioned forests will be supported.
* Automated protection of documents stored in file servers supported by servers in the aforementioned forests and documents synchronized by Work Folders will be supported
  + 1. Windows Azure Tenant

*Customize these paragraphs as per your customer requirements.*

<<Customer Name>> has already signed up for and configured a Windows Azure tenant that the organization can use with Azure RMS.

<<Customer Name>> has not signed up for and configured a Windows Azure tenant.

The following table lists the cloud tenants that will be involved directly in the Azure RMS infrastructure.

|  |  |  |
| --- | --- | --- |
| Tenant Name (.onmicrosoft.com) | Domain Name | Windows Azure account name |
|  |  |  |
|  |  |  |

* + 1. Active Directory Considerations

*Customize these paragraphs as per your customer requirements.*

<<Customer Name>> will provide Azure RMS-based services to users in their Intranet forest. As such, certification and licensing services will be provided by Azure RMS.

*Select the appropriate option from below based on your customer’s decisions:*

<<Customer Name>> has chosen to use the Directory Synchronization Tool to synchronize the existing on-premises Active Directory user and group accounts with Azure Active Directory.

<<Customer Name>> has chosen to use the Azure Active Directory Sync Tool to synchronize the existing on-premises Active Directory user and group accounts with Azure Active Directory.

<<Customer Name>> has chosen to use Microsoft Identity Manager to synchronize the existing on-premises Active Directory user and group accounts with Azure Active Directory.

<<Customer Name>> has also chosen to deploy federation services to enable a seamless end user experience through single sign-on.

<<Customer Name>> can limit access to Azure RMS services by declining to assign specific users an Azure RMS license. No additional action is necessary.

The following table lists forests that will be involved directly in the Azure RMS infrastructure.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Active Directory Forest | Active Directory Domains Involved | Synchronization Method | RMS Functionality Provided in the Forest | Business and Technical Decisions |
| Intranet | DomainName |  | Certification for users in the forest.  Licensing provided to users in this forest as well as to users in other forests integrated in the Azure RMS infrastructure such as those in the extranet.  Certification and licensing for internal Azure RMS-enabled servers such as SharePoint Server 2010, and 2013 and Exchange 2010 and Exchange 2013 servers. | RMS capabilities needed for users in all the domains in the forest. |
| Extranet | DomainName |  | Certification needed for external users with accounts provisioned in the DMZ.  Activation services for SharePoint servers installed in the DMZ. | RMS activation capabilities needed for extranet users requiring access to documents protected on the intranet. |

Table 1 –Rights Management Services and Active Directory Solution Design - Forest Details

1. Azure Rights Management Services Design

Because of <<Customer Name>> business requirements, access methods, and current platform the final Azure Rights Management Services architecture is as follows:

*Paste the Azure RMS Architecture Design Diagram from the Envisioning Workshop here*

Figure 2 –Rights Management Services <<Customer Name>> Solution Design

The design described above includes the following features:

*Customize these paragraphs as per your customer requirements.*

* Azure RMS document and email protection capabilities for all internal users.
* Azure RMS document and email protection for users in the Extranet forest.
* Support for Exchange pre-licensing capabilities for all the Exchange servers in the internal forests.
* Support for IRM integration capabilities for all the Exchange 2010 servers in the internal forests.
* Support for IRM integration capabilities for all the Exchange 2013 servers in the internal forests
* Support for IRM integration capabilities for all the SharePoint 2013 servers in the internal forests
* Support for IRM integration capabilities for all Windows Server 2012 file servers in the internal forests
* Support for IRM integration capabilities for Windows Server 2012 R2 file servers running Work Folders in the internal forests
  1. Server List

| **Server Name** | **Cluster** | **IP Address** | **Default Gateway** | **DNS Servers** | **OS version** | **Roles/Features** | **Additional Software** | **Disk Configuration** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Intranet |  |  |  | Windows Server 2008 R2 | RMS Connector |  | Single 300 GB NTFS disk |
|  | Intranet |  |  |  | Windows Server 2008 R2 | RMS Connector |  | Single 300 GB NTFS disk |
|  | Intranet |  |  |  | Windows Server 2008 R2 | Directory Synchronization Tool |  | Single 300 GB NTFS disk |
|  | Intranet |  |  |  | Windows Server 2012 R2 | AD FS |  | Single 300 GB NTFS disk |

Table 2 – AD RMS Server Information

* 1. Availability Model

*Select and customize the appropriate paragraphs as per your customer requirements.*

All servers will be deployed in clusters to provide adequate availability and scalability. Clusters will be formed by two or more servers load balanced by (Microsoft Network Load Balancing | an external Load Balancing service) to provide a single external view of the cluster.

* 1. Administration and Service Accounts

The following Active Directory service accounts have been defined for the Rights Management Services architecture:

*Customize this table as per your customer’s naming conventions, the AD RMS architecture and their requirements and decisions.*

| Username/Group | Type | Active Directory Forest/Domain | Group Membership and Rights | Comments |
| --- | --- | --- | --- | --- |
| **sys\_rms** | User | <<Customer Name>>.com | * Domain Users * Member of the local Azure RMS Enterprise Admins group in each node * **In each AD RMS node in the intranet:** Rights Management Services Service Group | The service account under which the RMS services run on both certification and licensing services in the <<Customer Name>> forest. |
| **sys\_rms** | User | <<Customer Name>>Extranet.com | * Domain Users * Member of the local RMS Enterprise Admins group in each node * **In each AD RMS node in the extranet:** Rights Management Services Service Group | The service account under which the RMS services run on both certification and licensing services in the [Extranet] forest. |
| **UUG\_<<Customer Name>>\_RMSADMINISTRATORS** | Group | <<Customer Name>>.com | * Domain Users * Member of the local AD RMS Enterprise Admins group in each node * **In each RMS node** **in both clusters:** IIS Admin (granted by setup to the local RMS Enterprise Admins group) | Accounts that will be used for installing, configuring and administering the RMS service in the intranet and extranet forests. |
| **UUG\_<<Customer Name>>\_RMSSUPERUSERS** | Group | <<Customer Name>>.com | * Scope: Universal * Type: Security | Group containing users with ability to access all content protected by RMS in all the environments hosted by the licensing services at <<Customer Name>>.  Functionality initially DISABLED |
| **UUG\_<<Customer Name>>\_RMSAUDITORS** | Group | <<Customer Name>>.com | * Scope: Universal * Type: Security | Users with the capability to generate and view RMS reports. Assigned to Help Desk and support users in the <<Customer Name>> forest. |

Table 3 –Rights Management Services Service Accounts

* 1. Windows Security and Distribution Groups

In order to simplify the Rights Management Services implementation and usage, the following Windows Security and Distribution Groups will be defined and populated.

*Customize this table as per your customer’s naming conventions, the Azure RMS architecture and their requirements and decisions.*

| **Group** | **Email Address/Proxy Address** | **Active Directory Forest/Domain** | **Role/Group Purpose** | **Group Type** | **Group Nesting** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- |
| **UUG\_RMS\_AUTHORS** |  | <<Customer Name>>.com | Used for deployment and configuration purposes | Scope: Universal  Type: Security | This group doesn’t belong to another group.  It contains all Groups that will use RMS with capability to consume and protect documents. |  |
| **UUG\_RMS\_READERS** |  | <<Customer Name>>.com | Used for deployment and configuration purposes | Scope: Universal  Type: Security | This group doesn’t belong to another group.  It contains all Groups that will use RMS with capability to only consume protected documents. |  |
| **UUG\_<<Customer Name>>\_FTEEMPLOYEES** |  | <<Customer Name>>.com | Used for content restriction and template definition | Scope: Universal  Type: Security | Contains all the groups that define all full time employees in the organization. |  |
| **UUG\_<<Customer Name>>\_ALLEMPLOYEES** |  | <<Customer Name>>.com | Used for content restriction and template definition | Scope: Universal  Type: Security | Contains all the groups that define all full time employees, vendors, and contractors in the organization. |  |

Table 4 – Active Directory Rights Management Services User Groups

* 1. OUs and Group Policies

The following Group Policies Objects (GPO) will be implemented in order to configure special client-side Rights Management Services and IRM settings for the Rights Management Services Architecture in <<Customer Name>>. If these settings will be applied to all users, they can be configured in the same GPO (with the exception of Rights Management Services Restriction).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Group Policy Name | Purpose | OU Level (linked) | GPO Status Configuration | GPO Settings (Location) | Others/Details |
| Internet Explorer Settings | Configure Intranet Pipeline in Local Intranet Zone and Extranet Pipeline in the Trusted Zone | Domain Level | User Configuration Settings Only | GPO\User Configuration\Windows Settings\Internet Explorer Maintenance\Security Zones and Content Ratings | Allows Credentials Request to clients when FQDN used.  No GPO Filtering applied (default permissions) |
| Office 2010/2013 Rights Management Services User Settings | Configure Rights Management Services Templates and additional Rights Management Services user Settings including:  DisablePassportCertification  IncludeHTML  DownlevelText | Domain Level | User Configuration Settings Only | Use RMS Group Policy Templates  GPO\User Configuration\Administrative Templates\Microsoft Office 2010 System\Manage Restricted Permissions\  GPO\User Configuration\Administrative Templates\Microsoft Office 2013 System\Manage Restricted Permissions\ | Provides Rights Management Services Templates and additional IRM settings for Rights Management Services clients.  GPO Filtering could be applied (only UUG\_RMS\_AUTHORS and UUG\_RMS\_READERS for example)  *To be used depending on the customer requirements. For more information see* [*http://technet.microsoft.com/en-us/library/dd772637(WS.10).aspx*](http://technet.microsoft.com/en-us/library/dd772637(WS.10).aspx) |
| Office 2010/2013 Rights Management Services Deny Rights Management Services Usage | **Disable** registry entry to disable Rights Management Services usage | OU/Domain level | User Configuration Settings Only | Use RMS Group Policy Templates  GPO\User Configuration\Administrative Templates\Microsoft Office 2010 System\Manage Restricted Permissions\  GPO\User Configuration\Administrative Templates\Microsoft Office 2013 System\Manage Restricted Permissions\ | Disable Rights Management Services Features in client side (requires ACL modifications in Rights Management Services servers)  *To be used depending on the customer deployment plan. For more information see* [*http://technet.microsoft.com/en-us/library/dd772637(WS.10).aspx*](http://technet.microsoft.com/en-us/library/dd772637(WS.10).aspx) |
| Office 2010/2013 Rights Management Services Rights Management Services Read-Only Usage | **DisableCreation** registry entry to disable Rights Management Services authoring | OU/Domain level | User Configuration Settings Only | Use RMS Group Policy Templates  GPO\User Configuration\Administrative Templates\Microsoft Office 2010 System\Manage Restricted Permissions\  GPO\User Configuration\Administrative Templates\Microsoft Office 2013 System\Manage Restricted Permissions\ | Disable Rights Management Services Features in client side (requires ACL modifications in Rights Management Services servers)  GPO Filtering could be applied, for example to non-pilot participants  *To be used depending on the customer deployment plan. For more information see* [*http://technet.microsoft.com/en-us/library/dd772637(WS.10).aspx*](http://technet.microsoft.com/en-us/library/dd772637(WS.10).aspx) |
| XPS Client Configuration | Configure Rights Management Services Templates Path for XPS Client usage | OU/Domain level | User Configuration Settings Only | Use RMS Group Policy Templates | GPO Filtering could be applied |
| RMS Client Installation using GPO | Install Rights Management Services Client v1.0 SP2 | OU/Domain level | Computer Configuration Settings Only | Deploy RMS client | Install Rights Management Services Client in users PCs  GPO Filtering could be applied |

Table 5 –Rights Management Services and Active Directory Solution Design – Group Policy Configuration

* 1. Azure RMS Templates

*Please provide the list of RMS Templates based on the decisions made so far. The customer will likely adjust the definitions on their reviewing of this document.*

*Include a description on how the templates will be deployed to Windows 8.1, Windows 8, and Windows 7 clients. The following options are provided as examples.*

Templates will be deployed through the Scheduled tasks provided on Windows 8, Windows 7, and Windows Vista SP1.The tasks will be enabled through GPO.

Clients with the AD RMS Client 2.1 and using Microsoft Office 2013 will automatically retrieve the rights policy templates without any user or administrator configuration.

The templates will be deployed on all clients through Logon Scripts. The logon scripts will copy all templates to all clients.

The templates will be deployed on all clients through Logon Scripts. The logon scripts will contain specific intelligence to copy only certain templates to each client based on logic based on the user’s group membership. The script to implement this logic will be built and tested by <<Customer Name>>.

The templates will be hosted on a central location and clients will access them directly from this location. Offline folders will be used to provide access to the template list while the user is offline.

The templates will be deployed to all clients through packages distributed through Microsoft System Center Configuration Manager | Microsoft Systems Management Server. The package to implement this will be built and tested by <<Customer Name>>.

The following is a high level summary of the Azure RMS Templates that need to be created with the objective to support the usage scenarios presented in previous sections.

| **RMS Template Name** | **Objective** | **Groups to which the template will be deployed**  *(generally “all users”)* | **Scope** | **Restrictions** |
| --- | --- | --- | --- | --- |
| Executives Confidential | Limit access to executive information to CXOs and assistants | * Executives | * Executives | * Read * Edit * Copy |
| FTE Confidential | Limit Vendors’ and Temporary employees’ access to critical information | * All users | * Full Time Employees | * Read-only |
| * Executives | * Full Control |

* 1. Client Design

The RMS Client is installed on end-user machines and is required to communicate between the Azure RMS service and RMS-aware applications such as Microsoft Word 2013. The RMS Client 2.x is the latest version of the AD RMS Client and we recommend deploying this version on all client machines.

The activation of the RMS client software establishes a lockbox and computer certificate for the currently logged-on user. Activation is a local process and does not require a network connection. Once activation is successful, the first use of Azure RMS by an enabled application obtains a user certificate for the user. The RMS client can be installed on each client computer in the organization by using SMS, Group Policy, Windows Update, or an administrative script..

* + 1. Rights Management Services Client

*Please customize the list for your customer’s software versions.*

| **OS** | **Requirement** | **Deployment mechanism** |
| --- | --- | --- |
| Windows 8.1  Windows 8  Windows 7  Windows Server 2012 R2  Windows Server 2012  Windows Server 2008 R2  Windows Server 2008 | Rights Management Service Client 2.1 (<http://www.microsoft.com/en-us/download/details.aspx?id=38396>). | Microsoft Update/WSUS or System Center Configuration Manager |

Table 6 –Rights Management Services Client and Operative System Requirements

* + 1. Rights Management Sharing Application

*If the RMS App will be used in the customer environment, customize this section accordingly.*

|  |  |  |  |
| --- | --- | --- | --- |
| **OS** | **Requirement** | **Deployment mechanism** |  |
| Windows 8.1  Windows 8  Windows 7 | Microsoft Rights Management sharing application for Windows (<http://www.microsoft.com/en-us/download/details.aspx?id=40857>) | GPO/Systems Management Server/System Center Configuration Manager/Embedded in OS image/manual installation/other |  |
| Windows RT  iOS Mobile Devices  Android Mobile Devices | Microsoft Rights Management Sharing application (<https://portal.aadrm.com/home/download>) | Windows Intune/manually through the App Store |  |

Table 7 –RMA Installation

* + 1. XML Paper Specification (XPS) client

*If XPS will be used in the customer environment, customize this section accordingly.*

|  |  |
| --- | --- |
| OS | [Requirements](http://www.microsoft.com/whdc/xps/viewxps.mspx) |
| Windows 8.1, Windows 8, and Windows 7 | None (already includes XPS Viewer) |
| Windows Server 2003  Windows Server 2003 R2 | [Microsoft .NET Framework 3.0](http://www.microsoft.com/downloads/details.aspx?FamilyID=10cc340b-f857-4a14-83f5-25634c3bf043&DisplayLang=en) |

Table 8 –XPS Client installation

* + 1. Operating System and RMS Enabled Applications

*Please customize this section for your customer.*

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

**Table 9** – RMS-enabled Applications

* + 1. Installation Mode

The following installation methods will be used to deploy the required software components.

| **Module** | **Note** |
| --- | --- |
| AD RMS Client 2.1 | Installed through System Center Configuration Manager/Systems Management Server/ |
| Rights Management Services Client V1.0 SP2 (KB 970099) | Updated through Windows Update on Windows 7 |
| Rights Management Sharing Application | Not to be installed |
| XPS Viewer | Not to be installed |
| Office IRM-enabled Applications | Already deployed. |
| Rights Policy Templates | Office 2013 users automatically retrieve rights policy templates when using the AD RMS Client 2.1  Windows 8.1, Windows 8, and Windows 7: to be deployed through custom template deployment task.  Windows 8.1, Windows 8, and Windows 7: to be deployed through Logon Script.  Windows 8.1, Windows 8, and Windows 7: to be deployed through standard template deployment task |

**Table 10** – Installation Module

* 1. Windows Firewall Configuration

Communication with the Azure RMS service occurs over HTTPS. Each user and machine that will communicate with RMS must be able to connect to the internet over Port 443.

* 1. System Recommendations

The following tables describe the hardware and software components required to run, or that are recommended to satisfy the availability and sizing requirements for this project.

* + 1. RMS Connector Server Hardware and Components

*This is not the infrastructure sizing, but the specification of the server units to use. Customize based on your customer’s server specifications.*

| **Component** | **Recommended configuration** |
| --- | --- |
| CPU | Two Pentium 4 or higher CPU cores, x64 required for Windows Server 2008 R2 and later. |
| Memory | 1024 megabytes (MB) of RAM or higher, 2048 MB preferred. |
| Hard Disk | 64 gigabyte (GB) of free hard disk space. |
| NIC | One Gb network interface card (two required if NLB is to be used) |
| Internet | Access to the Internet via a firewall or web proxy that does not require authentication |
| Location | Must be in a forest or domain that trusts other forests in the organization that contain installations of Exchange or SharePoint servers that you want to use with the RMS Connector |

Table 11 – The Rights Management Services Hardware Information

| **Software** |  |
| --- | --- |
| Operating System | Microsoft Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 |
| Rights Management Services | Active Directory Rights Management Services server role (included in the Operating System) |

Table 12 – The Rights Management Services Software Information

* + 1. Directory Synchronization Tool Server Hardware and Software Configuration

Hardware recommendations for the Directory Synchronization Tool Server depend on the number of Active Directory objects that will be synchronized to Azure Active Directory. The following table assumes a deployment of a maximum of 50,000 objects. For more information about hardware recommendations for Active Directory deployments with more than 50,000 objects, see the [Prepare for directory synchronization](http://msdn.microsoft.com/en-us/library/azure/jj151831.aspx) MSDN article (http://msdn.microsoft.com/en-us/library/azure/jj151831.aspx).

|  |  |
| --- | --- |
| **Hardware** | **Recommendations** |
| CPU | 1.6 GHz, x64. |
| Memory | 4096 MB of RAM or higher |
| Hard Disk | 70 GB of free hard disk space. |
| NIC | One Gb network interface card (two required if NLB is to be used) |

Table 13 –Directory Synchronization Tool Hardware Information

|  |  |
| --- | --- |
| **Software** |  |
| Operating System | Microsoft Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008 |
| .NET Framework | Microsoft .NET Framework 3.5 SP1  Microsoft .NET Framework 4.0 |
| Windows PowerShell | Windows PowerShell |

Table 14 – Directory Synchronization Tool Software Information

* + 1. Database Configuration

A storage account in Windows Azure stores all of the Azure Rights Management Services logging information. The information that is in this account is sensitive because its disclosure could affect user privacy. Microsoft has put forth extra efforts to confirm that no Personally Identifiable Information **(**PII) is logged, and that all information logged to this account is protected with the appropriate security measures. No additional security modifications of this account are needed. If the logging content is downloaded and moved to a logging database (to reduce storage costs), you should verify that the appropriate protection mechanisms are applied to the new environment.

* 1. Security Design

The following sections details the security design of the Azure RMS solution.

* + 1. Rights Management Services Account Certificates

The organization must identify the users who are trusted entities within its Rights Management Services. To do so, Rights Management Services issues Rights Management Services Account Certificates that associate user accounts with specific computers.

There are two types of RM account certificates.

* **Standard**A standard account certificate enables the user to create, to view, and to use restricted content on a specific computer. The user can access the restricted content only for the specific number of days determined by the administrator of the Rights Management Services server.
* **Temporary**  
  A temporary account certificate enables the user to view restricted content on a specific computer. The user can view the restricted content only for the specific number of minutes determined by the administrator of the Rights Management Services server.

Each certificate must be assigned a specific expiration date. The expiration date affects the duration of the users’ ability to access content offline. If it is not specified some users would be able to read the content even though the domain account had been removed from the Active Directory. The expiration date design is based on the corporate policy, taking into account human resource and machine replacements, and temporary resource access policy in the organization. It is recommended that this date be designed carefully.

It must be cautioned that Office 2007 will provide standard RACs even to non-domain joined users, instead of the Temporary RAC in order to perform the responses from the external VPN clients by eliminating the needs of the frequent CLC or RAC renewals.

|  |  |
| --- | --- |
| **Account Certificate** | **Duration** |
| **Standard** | **365 days (default)** |
| **Temporary** | **15 minutes** |

Table 15 – RM Account Certificate Expiration Dates

* + 1. Azure RMS Private Key

Although hardware security module-based private key protection can be used within the Azure Rights Management Services solution, through the BYOK feature, and is mostly required for high-secure environments, software-based private key protection is also a valid option. The software-based private key protection will be created and managed by Microsoft.

Software-based key protection is the method that will be used in <<Customer Name>>’s environment during the initial rollout. The private keys will be stored in the Azure RMS cluster databases as protected by a strong password.

* + 1. Rights Management Services User Authentication

Normally, Rights Management Services user authentication is required when the user reads the Rights Management Services-protected document. The Rights Management Services server validates the user using Windows integrated authentication.

Since users have already been authenticated in order to acquire a Rights Accounts Certificate, which is required to request a use license or to protect content, Windows Integrated Authentication to the licensing pipeline serves only the function of protecting the RMS servers from attack, and since the RMS cluster will only be accessible internally during the initial rollout, there’s no incremental risk in configuring the RMS pipeline for anonymous access, which is what will be done in <<Customer Name>>’s environment for the Intranet cluster.

Additional considerations will apply in this external access scenario.

|  |  |
| --- | --- |
| **Configuration** | **Impact** |
| **Require a Connection (No license Caching)** | If this policy is enabled, there will be no license caching capabilities in the RMS client; every time user requires a RAC or EUL, that user will need to provide credentials to the server. This option will not be enabled by default in the clients or templates. |

Table 16 – Authentication considerations with Rights Management Services

* 1. Server Integration Configuration
     1. RMS Connector

*If on-premises server workloads, such as Exchange, SharePoint, and File Classification Infrastructure are in use at the customer, or plan to be used, and need to be integrated with Azure RMS for automated content protection, list the RMS Connector servers to be implemented below*

The following RMS Connector servers are expected to be implemented:

| **RMS Connector Server** | **Forest** | **Purpose** | **Options** |
| --- | --- | --- | --- |
| **Connector01** | Corp | Front line | Servers utilizing this connector  FQDN  SSL? |
| **Connector02** | Corp | High availability | Servers utilizing this connector  FQDN  SSL? |

* + 1. Integration with SharePoint 2013/2010

*If SharePoint 2013/2010 libraries are in use at the customer, or plan to be used, and need to be integrated with Azure RMS for automated content protection, list the libraries to be integrated below.*

The following SharePoint libraries are expected to be integrated with Azure RMS:

| **SharePoint Server** | **Library** | **Forest** | **SharePoint Version** | **Extranet** | **AD FS enabled** | **Options** |
| --- | --- | --- | --- | --- | --- | --- |
| **SharePoint01** | **ManagementPlans** | Corp | SharePoint 2013 Enterprise (x64)/SharePoint 2010 Enterprise (x64) | No |  | Policy Name  Print-enabled  License Duration  Non-IRM enabled documents support |
| **SharePointExtranet** | **PriceLists** | Extranet | SharePoint 2013 Enterprise (x64)/SharePoint 2010 Enterprise (x64) | Yes | With Contoso | Policy Name  Print-enabled  License Duration  Non-IRM enabled documents support |

* + 1. Integration with SharePoint Online

*If SharePoint Online libraries are in use at the customer, or plan to be used, and need to be integrated with Azure RMS for automated content protection, list the libraries to be integrated below.*

The following SharePoint libraries are expected to be integrated with Azure RMS:

| **Library** | **SharePoint Version** | **Extranet** | **AD FS enabled** | **Options** |
| --- | --- | --- | --- | --- |
| **ManagementPlans** | SharePoint Online | No |  | Policy Name  Print-enabled  License Duration  Non-IRM enabled documents support |
| **PriceLists** | SharePoint Online | Yes | With Contoso | Policy Name  Print-enabled  License Duration  Non-IRM enabled documents support |

* + 1. Exchange Prelicensing

*If the requirements for Exchange Prelicensing are met (listed in the table below) indicate if Exchange Prelicensing will be enabled.*

Exchange Prelicensing enables users to open protected emails and attachments without having to have an Internet connection at the time of consumption.

Users of the following Exchange Servers meet the prerequisites for supporting Exchange prelicensing.

| **User group** | **Exchange Version** | **Office Version** | **Can be upgraded** |
| --- | --- | --- | --- |
| **Regular users** | Exchange Server 2013 or Exchange Server 2010 | Office 2013 or Office 2010 | Yes |
|  |  |  |  |
|  |  |  |  |

* + 1. Integration with On-premises Exchange Server 2013/2010

*Include this section if your customer has Exchange Server 2013/2010 deployed and wants to implement the integration functionality indicated below. Customize according to your customer’s environment and decisions.*

<<Customer Name>> has deployed Exchange 2013/2010 as their email infrastructure. Exchange 2013/2010 can be integrated with Azure RMS to provide specific enhanced functionality.

The functionality in the table below will be implemented as part of this deployment.

| **Capability** | **Purpose** | **Details** |
| --- | --- | --- |
| **Transport Decryption** | Enable server Antivirus scanning to scan protected messages (available on specific antivirus software) | To be used with anti-virus and antispam agents |
| **Data Loss Prevention** | To protect messages or attachments that contain sensitive information | *Specify policies to be implemented, their conditions and actions* |
| **Transport Protection Rules** | To protect messages tagged with keywords  To protect messages or attachments containing special patterns  To protect messages between certain groups. | *Specify rules to be implemented, their conditions and actions* |
| **Outlook Protection Rules** | To protect messages tagged with keywords  To protect messages or attachments containing special patterns  To protect messages between certain groups. | *Specify rules to be implemented, their conditions and actions*  *Specify if the rules will be mandatory*  *Confirm Microsoft Outlook 2013/2010 is available in the clients* |
| **Journal Decryption** | To provide automated decryption of messages sent to the journaling mailbox | *Indicate journaling mailbox configuration if known* |
| **OWA IRM** | To enable users to author and consume protected content inside a browser | *Indicate browser platforms to be used.*  *Indicate if Exchange Server 2010 SP1 or later will be used, enabling in-browser attachment viewing.*  *Indicate if this option will be enabled per-server or per-mailbox of for all users.* |

* + 1. Integration with Exchange Online

*Include this section if your customer uses Microsoft Exchange Online/Microsoft Office 365 and wants to implement the integration functionality indicated below.*

<<Customer Name>> is using Exchange Online as part of their email platform. Microsoft Exchange Online in Microsoft Office 365 can be integrated with Azure RMS to provide specific enhanced functionality.

The functionality in the table below will be implemented as part of this deployment.

| **Capability** | **Purpose** | **Details** |
| --- | --- | --- |
| **Transport Decryption** | Enable server Antivirus scanning to scan protected messages (available on specific antivirus software) | To be used with anti-virus and antispam agents |
| **Data Loss Prevention** | To protect messages or attachments that contain sensitive information | *Specify policies to be implemented, their conditions and actions* |
| **Transport Protection Rules** | To protect messages tagged with keywords  To protect messages or attachments containing special patterns  To protect messages between certain groups. | *Specify rules to be implemented, their conditions and actions* |
| **Journal Decryption** | To provide automated decryption of messages sent to the journaling mailbox | *Indicate journaling mailbox configuration if known* |
| **OWA IRM** | To enable users to author and consume protected content inside a browser | *Indicate browser platforms to be used.*  *Indicate if using Exchange Server 2010 SP1, enabling in-browser attachment viewing.*  *Indicate if this option will be enabled per-server or per-mailbox of for all users.* |

* + 1. Integration with File Classification Infrastructure and Work Folders

*Include this section if your customer has FCI deployed and wants to implement the integration functionality indicated below. Customize according to your customer’s environment and requirements.*

<<Customer Name>> has deployed FCI and Work Folders on their file servers. FCI in Windows Server 2012 R2 and Windows Server 2012 can be integrated with Azure RMS to provide specific enhanced functionality.

The functionality in the table below will be implemented as part of this deployment.

| **File Server** | **Folder Classifier** | **Content Classifier** | **Forest** | **FCI version** | **Extranet** |
| --- | --- | --- | --- | --- | --- |
| **FileServer01** | **ManagementPlans** | String Patterns:   * Confidential * Project Alpha   Regular Expressions:   * Social Security numbers | Corp | Windows Server 2012 | No |
| **FileServer Extranet** | **PriceLists** | String Patterns:   * Confidential * Project Alpha   Regular Expressions:   * Social Security numbers | Extranet | Windows Server 2012 | Yes |