Solution Deployment Plan



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 version for review |
|  |  |  |  |
|  |  |  |  |

Reviewers

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

Table of Contents

[1 Summary and Objectives 7](#_Toc391030822)

[2 Deployment Scope 7](#_Toc391030823)

[2.1 Seats 8](#_Toc391030824)

[2.2 Components 8](#_Toc391030825)

[2.3 Deployment Strategy 13](#_Toc391030826)

[2.4 Deployment Schedule 14](#_Toc391030827)

[3 Deployment Resources 15](#_Toc391030828)

[3.1 Deployment Information 15](#_Toc391030829)

[3.2 Deployment Tools 16](#_Toc391030830)

[4 Solution Deployment Process 16](#_Toc391030831)

[4.1 Prepare the Environment – Architecture Prerequisites 17](#_Toc391030832)

[4.1.1 Environment Preparation Procedure 17](#_Toc391030833)

[4.2 Preparing the Environment – Configure the Directory 18](#_Toc391030834)

[4.2.1 Active Directory Environment Preparation Procedure – Group Policy Objects 18](#_Toc391030835)

[4.2.2 Verification Procedure 20](#_Toc391030836)

[4.3 Activate Azure Rights Management Services 21](#_Toc391030837)

[4.3.1 Dependencies Validation 21](#_Toc391030838)

[4.3.2 Activating Azure RMS 22](#_Toc391030839)

[4.3.3 Verification Procedure 22](#_Toc391030840)

[4.4 Configure Azure Rights Management Services and Templates 23](#_Toc391030841)

[4.4.1 Installing Windows PowerShell for Azure Rights Management 23](#_Toc391030842)

[4.4.2 Delegate Permissions 23](#_Toc391030843)

[4.4.3 Configuring Custom Rights Policy Templates 24](#_Toc391030844)

[4.4.4 Enabling Logging 25](#_Toc391030845)

[4.4.5 Verification Procedure 25](#_Toc391030846)

[4.5 Deploying Client Components 26](#_Toc391030847)

[4.5.1 Deploying Rights Management Services Client Installation Components 26](#_Toc391030848)

[4.5.2 Installing RMS-Enabled Applications 26](#_Toc391030849)

[4.5.3 Verification Procedure 27](#_Toc391030850)

[4.6 Deploying Azure Rights Management Services Trusts 27](#_Toc391030851)

[4.7 Validating Azure Rights Management Services Functionality 28](#_Toc391030852)

[4.7.1 Active Directory Rights Management Services Usage General Validation - Intranet Users 28](#_Toc391030853)

[4.7.2 Active Directory Rights Management Services Usage General Validation - Extranet Users 28](#_Toc391030854)

[4.8 Integration with Server-side Applications 29](#_Toc391030855)

[4.9 Integration with Microsoft Exchange 2013 30](#_Toc391030856)

[4.10 Integration with Microsoft Exchange 2010 31](#_Toc391030857)

[4.11 Integration with Exchange Online / Office 365 32](#_Toc391030858)

[4.12 Integration with SharePoint Server 32](#_Toc391030859)

[4.13 Integration with SharePoint Online 33](#_Toc391030860)

[4.14 Integration with File Classification Infrastructure and Work Folders 33](#_Toc391030861)

**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. Summary and Objectives

The main goal behind the Solution Deployment Plan is to minimize risks to the production environment while deploying the *Information Protection using Azure Rights* Management Services solution. The plan defines a phased approach for the solution deployment, in which each phase is designed to implement one part of the solution and allow the resolution of any identified issues before moving to the next phase.

The deployment process begins with the implementation of the necessary Azure Rights Management Services prerequisite changes, such as verifying the that the users’ have the email address attribute populated and obtaining a subscription to Azure RMS, either as a standalone subscription or as a part of a suite. The process continues with a five-step solution rollout plan. The complete process includes the following steps:

1. Prepare the Environment - Architecture Prerequisites
2. Prepare the Environment – Configure the directory
3. Enable Azure Rights Management Services
4. Configure Azure Rights Management Services and Templates
5. Implement Azure Rights Management Services Client Components
6. Implement Azure RMS integration with server-side applications

After performing the changes necessary for each step and validating the new configuration, there is a five-day period during which issues are identified and triaged. Only after the valid issues are solved does the deployment process move to the next step.

This document provides description of the deployment process, an overview of the deployment schedule, and a list of resources needed. The tasks listed in this document refer to step-by-step procedures that are explained in detail in the ***Step by Step Installation Procedures*** document.

1. Deployment Scope

Please replace all text highlighted in yellow with the values corresponding to your design decisions, or delete if inapplicable to your customer. Delete all such text in red including this one.

The scope of the deployment includes machines that are part of the **[Active Directory Forest(s) Name(s)]** Active Directory forest(s) and unmanaged machines used from the Internet to consume and protect documents using Rights Management Services (RMS).

The client machines involved in the deployment must be running the Windows 8.1, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008, or Windows Server 2008 R2 operating systems. Other operating systems are not supported by this solution.

Windows systems that do not meet the operating system (OS) version criteria listed above will not be protected by the solution and will not be included in the deployment.

Mac computers running OSX (Leopard or later) cannot be used in this solution.

Additionally, the following mobile devices can be implemented with Azure RMS: Windows Phone, iOS, Android.

* 1. Seats

The solution will protect an expected total of **[Total Number]** systems, including [Server Number] servers and [Client Number] client systems. The solution will allow for access from the interior of the organization’s network as well as from the Internet.

The solution will also include integration with the following servers:

* Protect Data in Motion
  + [Number] Exchange 2010 servers used for OWA IRM, Transport Protection, Transport Decryption, Journal Decryption and/or Prelicensing
  + [Number] Exchange 2013 servers used for DLP, OWA IRM, Transport Protection, Transport Decryption, Journal Decryption and/or Prelicensing
  + An Exchange Online service used for OWA IRM, Transport Protection, Transport Decryption and Journal Decryption.
* Protect Data at Rest
  + [Number] SharePoint 2010/2013 servers used to protect [Number] libraries.
  + [Number] Windows Server 2012 R2/Windows Server 2012/Windows Server 2008 R2 file servers with File Classification Infrastructure used to protect [Number] of folders.
* Protect Data in Use
  + [Device type] mobile devices will be used to protect and consume sensitive content.
  1. Components

The *Information Protection using Azure Rights* Management Services solution has a service side and a client side.



Figure 1 – Azure Rights Management Services Architecture Components

On the service side, the solution requires the following components:

* **Azure Active Directory:**

Azure Active Directory is used to provide the following services:

* + **Authentication Services**
    - Azure RMS relies on Azure Active Directory to authenticate users who participate in the Azure RMS platform. Because of this, there is no anonymous access enabled to Azure Rights Management Services and anonymous or unauthenticated users will be unable to read RMS-protected documentation.
  + **Group Membership**
    - Azure Active Directory provides information about group membership that Azure Rights Management Services uses to grant use licenses to RMS-protected content when the publishing license grants rights to groups rather than to individual user accounts.
* **Rights Management Services:**

Azure RMS is an Azure service that provides information protection by using encryption and policy to help secure documents, files, and emails. The Azure RMS service provides the following functionality:

* + **Certification Service**
    - Certification refers to the account certification and activation activities performed by Azure RMS. Each user must acquire a set of certificates that identity that particular user to be able to participate in the Azure RMS platform.
  + **Licensing Service**
    - Licensing refers to the set of operations by which the Azure RMS Service grants access to protected content to authorized users. The Azure RMS Service grants a use license for each document to authorized users
  + **Rights Policy Templates**
    - Rights policy templates specify a predefined set of rights and conditions that can be applied to protected content, simplifying the RMS Protection for common or daily-use scenarios to the end-users. Azure RMS administrators create and manage rights policy templates.
    - When publishing protected content, the author selects the rights policy template to apply from the templates that are available on the local computer. To make rights policy templates available for use, the administrator must deploy them to user computers or the client computer should have access to a shared folder.
    - When a user attempts to consume content protected through a template, the Azure RMS Service retrieves the latest version of the rights policy template that was used to publish the content from the configuration database and issues a license based on that template.
  + **Azure RMS Trusts**
    - In Azure RMS, trust relationships are implied with any other organization supported by Azure Active Directory, including users with Office 365 or using RMS for Individuals. Users can collaborate with external parties who have Azure Active Directory, without the need to configure a trust relationship.
    - Note that this trust relationship provides the ability to collaborate; it does not automatically grant external users access to protected content. External users must be explicitly mentioned in the permission policy.
* **Logging Services:**

Azure RMS provides access to tenant logs using Windows Azure storage. RMS can log every request that it makes for an organization, which includes requests from users, actions performed by RMS administrators in an organization, and actions performed by Microsoft operators to support an RMS deployment. 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. This information is useful for a variety of reasons:

* + **Analyzing data access for business insight:** 
    - These logs can be used to create reports and drive insights such as: who is accessing sensitive data, what devices are being used for access, which locations are users accessing data from, and report on which users have read a given document.
  + **Monitoring for abuse**
    - Logs can be accessed in near-real-time (delay: < 15 minutes). This allows administrators to continuously monitor usage of the Microsoft RMS assets. For example, tenant administrators may want to be alerted if there is a spike in access of assets after business hours (why someone is trying to open lots of critical documents in a short time), or if the same user is accessing from two different IP addresses within 15 minutes (have passwords been compromised), or if someone is trying to read content from a remote location (we don’t have any staff there).
  + **Performing Forensics** 
    - When there is an information leak the logging information can help determine the users that recently accessed the leaked document and what information a specific user accessed recently.
    - 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, you must provide an Azure storage account for the logs and you will be charged for this storage.

The Client components of Azure RMS are as follows:

| **Operating System** | **RMS Client** | **Rights Management Enabled Applications** | **Rights Management Sharing Application (RMS App)** | **XML Paper Specification** |
| --- | --- | --- | --- | --- |
| Windows 8/Windows 8.1 | ***RMS Client 2.x should be installed*** | Office 2013 or Office 2010 | Extends RMS protection to files of any file types and enables additional client-side scenarios  ***(can be installed)*** | Allows the creation and consumption of RMS-protected XML Paper Specification (XPS)  ***(preinstalled)*** |
| Windows 7 | ***Preinstalled, though should be upgraded to RMS Client 2.x*** | Office 2013 or Office 2010  ***(should be installed)*** | Extends RMS protection to files of any file types and enables additional client-side scenarios  ***(can be installed)*** | Allows the creation and consumption of RMS-protected XML Paper Specification (XPS)  ***(preinstalled)*** |
| Windows Server 2008 | ***Preinstalled, though should be upgraded to RMS Client 2.x*** | Office 2013 or Office 2010  **(can be installed on servers performing Terminal Services roles)** | Provides access to certain RMS-protected content using Internet Explorer  **(can be installed on servers performing Terminal Services roles)** | Allows the creation and consumption of RMS-protected XML Paper Specification (XPS)  **(can be installed on servers performing Terminal Services roles)** |
| Windows Server 2008 R2 | ***Preinstalled, though should be upgraded to RMS Client 2.x*** | Office 2013 or Office 2010  **(can be installed on servers performing Terminal Services roles)** | Provides access to certain RMS-protected content using Internet Explorer  **(can be installed on servers performing Terminal Services roles)** | ***(preinstalled)*** |
| Windows Server 2012 | ***RMS Client 2.x should be installed*** | Office 2013 or Office 2010 **(can be installed on servers performing Terminal Services roles)** |  | Allows the creation and consumption of RMS-protected XML Paper Specification (XPS)  **(can be installed on servers performing Terminal Services roles)** |
| Windows Server 2012 R2 | ***RMS Client 2.x should be installed*** | Office 2013 or Office 2010 **(can be installed on servers performing Terminal Services roles)** |  | Allows the creation and consumption of RMS-protected XML Paper Specification (XPS)  **(can be installed on servers performing Terminal Services roles)** |

Table 1 – Azure Rights Management Services Client Components

The components mentioned above relate to each other in a way that impact the solution deployment process. These intrinsic relationships between solution components were taken into account when developing the deployment plan for the Azure Rights Management Services solution.

* 1. Deployment Strategy

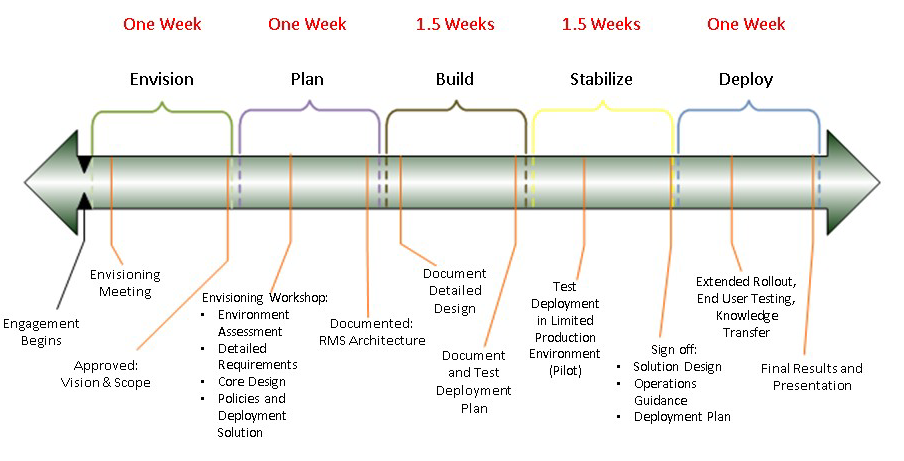
Customer Name will use a phased approach for the deployment of the Information Protection Using Azure Rights Management Services solution. This approach allows the early identification and remediation of any issue affecting the production environment and reduces risk, while providing an easy rollback mechanism at every stage of the deployment.

The first step before actually deploying the solution is to create all the necessary prerequisites such as user attributes, user groups and, if required, Hardware Security Modules (HSMs). These configurations will provide the basis for the team to start rolling out the solution to the production environment.

After creating the groups and policies, the solution will be deployed in six phases. These phases are detailed in the *Implementation Operations Guide* and are summarized below:

1. **Prepare the Environment - Architecture Prerequisites** – All solution prerequisite components should be in place before implementing the solution. Some critical components, such as Private Key storage containers like Hardware Security Modules (HSMs), cannot be added or modified after implementation of the solution. Adding those components after initial implementation requires the entire Azure Rights Management Services architecture to be reimplemented.
2. **Prepare the Environment – Configure the Directory** – During this phase, all the Active Directory components are configured and on-premises Active Directory is synchronized to Azure Active Directory using the Directory Synchronization Tool. Optionally, Active Directory Federation Services is deployed to pass authentication through to the on-premises directory.
3. **Activate Azure Rights Management Services**– This step occurs after all solution prerequisites are in place, and all the preparation tasks are executed. This includes activating the Azure Rights Management Service in the tenant.
4. **Configure Azure Rights Management Services** **and Templates –** After Azure Rights Management Service is activated, the Azure RMS configuration is performed according to Customer Name’s requirements. This configuration includes components such as Azure Rights Management Services user restriction, administration delegation, and creating the rights policy templates.
5. **Implement Azure Rights Management Services** **Client** **Components –** After the Azure RMS service has been activated and configured, the client components must be distributed and configured for the end users.
6. **Implement Azure Rights Management Services** **with Server-side Applications –** Azure RMS can integrate with Microsoft server-side applications such as Microsoft Exchange and Microsoft SharePoint. These integrations will be configured according to the requirements.
   1. Deployment Schedule

A macro schedule of activities is shown in the following figure. Highlighted items are deployment related:

Figure 2 - Solution Deployment Schedule

Between each deployment phase, the project team will be performing configuration testing, tracking any issues that may appear and resolving the problems. The next phase begins only after the previous one is considered stabilized.

A more detailed schedule is available in the *Project Plan document*, which is a Microsoft Project file which includes detailed information about each phase and timeline.

1. Deployment Resources
   1. Deployment Information

The following information should be available prior to deployment of the solution:

* A Solution Design Document containing a description of the solution architecture and all the necessary planning information for developing the solution. This information should include:
  + A complete list of server and client components that will be included in the solution. These systems include Active Directory, Azure Active Directory, Azure Rights Management Services, Azure RMS Logging Service, and clients identified during the solution planning.
  + The complete list of use cases that comprise the Customer Name corporate requirements that will be solved by the Information Protection using Azure Rights Management Services solution, and detailed list of access methods.
  + Deployment Step by Step guide, that details the procedure to implement each of the tasks described in this document.
* All configuration items should be resolved including all server and cluster names, cluster URLs, groups and accounts to be used, IP addresses, and other definitions. Typically these will be documented in the Detailed Design document.
* Names and contacts of the resources able to perform changes in the environment, including changes to Active Directory, mail and document library servers to be affected, Hardware Security Modules, and other elements in the affected environment.
  1. Deployment Tools

The following software tools will be used during the solution deployment:

* **Ping, Telnet, and DNS Lookup**

These tools allows an administrator to validate the virtual name configuration and networking using the appropriate virtual name, Fully Qualified Domain Name (FQDN), and the respective TCP/IP ports used by the configured supporting components of the Azure Rights Management Services.

* **RMS Diagnosis Tools**

**Advanced Mode** of the IRMDiagnosticsTool can be used to analyze the status of a client machine after attempting to perform an IRM operation. This feature is also known as IRMCheck. The latest version of IRMDiagnosticsTool can be downloaded from [here](http://blogs.technet.com/rmssupp/archive/2008/12/04/protecting-your-assests-exclusive-new-version-of-irmcheck-released-here.aspx).

**Diagnostic Mode** of the IRMDiagnosticsTool is a tool that can be used to obtain traces of the RMS activity at the client and server side. This feature is also known as DebugView.

1. Solution Deployment Process

Customize the tests to match the deployment plan created for the customer.

This section describes in detail the deployment process to be used for the Information Protection Using Azure Rights Management Services solution. This process refers to step by step procedures, the details of which can be found in the Step by Step Deployment Guide document.

* 1. Prepare the Environment – Architecture Prerequisites

Before the deployment process begins and users start using RMS, it is necessary to prepare the prerequisites that must be in place before activating the solution.

* + 1. Environment Preparation Procedure

The following procedure should be followed to prepare the environment for solution deployment:

* **Validate Active Directory Architecture and Functionality**
  + Validate Active Directory architecture and the respective Active Directory forests populated by future Azure Rights Management Services users. Prior to implementation, validate that Microsoft Exchange is in place or that the Microsoft Exchange Schema Extension has been deployed.
  + Validate group policy functionality and domain and forest compatibility level.
* **Validate users and groups**
  + Validate that user accounts for users of the system have their mail attribute populated, and that groups to be used for rights assignment are mail-enabled.
  1. Preparing the Environment – Configure the Directory

Before activating the Azure Rights Management Service, Azure Active Directory must be populated with the accounts of the users that will create and consume protected content. This population is best performed using the Directory Synchronization Tool, which synchronizes user and group accounts from the on-premises Active Directory to Azure Active Directory.

Azure Active Directory supports the following directory integration scenarios:

* **Directory Sync with Password Sync Scenario**: Used when you want to enable your users to sign in to Windows Azure AD and other services using the same user name and password as they use to log onto your corporate network and resources. Password sync is a feature of the Directory Sync tool.
* **Directory Sync with Single Sign-on Scenario**: Used to provide users with the most seamless authentication experience as they access Microsoft cloud services while logged on to the corporate network. In order to set up single sign-on, organizations need to deploy a security token service on-premises, such as Active Directory Federation Services (AD FS). Once it has been set up, users can use their Active Directory corporate credentials (user name and password) to access the services in the cloud and their existing on-premises resources.

Directory Synchronization can be configured in a multi-forest scenario using Forefront Identity Manager.

These preparatory steps should not have any impact on production systems, but special care should be taken when performing any configuration change in a production Active Directory environment.

* + 1. Active Directory Environment Preparation Procedure – Group Policy Objects

The following procedure should be followed in all Active Directory domains to prepare them for the solution deployment:

* **Configure RMS and Office IRM Settings using Group Policies**
  + The recommended way to configure the Rights Management Services client and Office IRM configurations in domain-joined workstations is using the appropriate *.*ADM or .ADMX policy template files provided for the relevant version of Microsoft Office. Some of the RMS client settings are stored in HKEY\_LOCAL\_MACHINE (HKLM) hive in the registry, so deploying through Group Policy Objects allows for greater flexibility for non-administrative users than other mechanisms.
    - **RMS Rights Policy Template path:** Specify a place where the templates are going to be located. In general, this should be a path under the user’s local profile. Setting this path does *not* get the templates deployed, and template deployment must be done through other mechanisms (explained later).
    - Note that Microsoft Office 2013/2010 can automatically obtain rights policy templates from the Azure RMS service without user or administrator action.
    - If using a 32-bit version of Microsoft Office on an x64 Operating System, place the keys below under the WoW6432Node registry branch.
    - Be aware that the registry values below are of the type REG\_EXPANS\_SZ. While using a REG\_SZ value might work, it will not allow using environment variables (such as the User’s Profile Path) as part of the value and cause Office to fail locating the templates.
    - Use the following registry locations:
      * **Microsoft Office 2013**

HKCU\Software\Microsoft\Office\15.0\Common\DRM

REG\_EXPAND\_SZ: AdminTemplatePath

Value: <path to your RMS templates>

* + - * **Microsoft Office 2010**

HKCU\Software\Microsoft\Office\14.0\Common\DRM

REG\_EXPAND\_SZ: AdminTemplatePath

Value: <path to your RMS templates>

* + - * **XPS Viewer**

HKCU\Software\Microsoft\XPSViewer\Common\DRM

REG\_EXPAND\_SZ: AdminTemplatePath

Value: <path to templates>

* + **Disabling RMS functionality in Microsoft Office:** 
    - * **Microsoft Office 2013 or 2010**

HKCU\Software\Microsoft\Office\*X*.0\Common\DRM (where X=the Office Version Number)

REG\_DWORD: Disable

Value: 0=Enable protection capabilities, 1=disable protection capabilities

* + **Disabling RMS authoring functionality:** 
    - * **Microsoft Office 2013 or 2010**

HKCU\Software\Microsoft\Office\*X*.0\Common\DRM

REG\_DWORD: DisableCreation

Value: 0=Enable protection capabilities, 1=disable protection capabilities

* + Customized message wrapper text for non RMS enabled clients:
    - * **Microsoft Office 2013 or 2010**

HKCU\Software\Microsoft\Office\*X*.0\Common\DRM

REG\_SZ: DownlevelText

Value: Text that you want to appear in the wrapper email for non RMS enabled clients.

* + Some additional registry settings are available if required for RMS-enabled applications, such as restriction of LiveID services and enabling usage of RMA for documents. For more information see [AD RMS Client Deployment and Usage Considerations](http://technet.microsoft.com/en-us/library/jj159267(WS.10).aspx).
* **Control Azure Rights Management Services Usage**
  + Even in an organization that plans to enable Azure RMS usage for all their users it is recommended to limit the use of Azure RMS to specific groups for Azure RMS users and Azure RMS recipients (users that are able to consume RMS protected content but not author it) for a phased deployment. It is possible to restrict Azure Rights Management Services usage by not granting a license in Windows Azure to users that should not be able to create or consume protected content with Azure RMS.
    1. Verification Procedure

The following steps validate the correct functionality of this phase:

* **Group Policy Settings for RMS Authors**
  + Create a test user and add it to the group to which the corresponding Group Policy has been applied.
  + Validate the user inherits all configuration settings by checking Internet Explorer configuration, Trusted Root Configuration and the Registry location for Active Directory Rights Management Services settings (although not used at the moment).
  + Also use the Resultant Set of Policy MMC console to check for the application of the right settings.
* **Group Policy Settings for RMS Consumers**
  + Create a test user and add it to the group to which the corresponding Group Policy has been applied.
  + Validate the user inherits all configurations and that the RMS creation Interface is disabled from the client computer. Validate that Active Directory Rights Management Services settings are disabled or disappear depending on the version of Microsoft Office being used.
  1. Activate Azure Rights Management Services

This section presents the activities to be executed when activating the Azure Rights Management Service in the configured tenant.

* + 1. Dependencies Validation

In order to have a successful implementation process of this server component, it is recommended the following prerequisites and dependencies are revalidated and in place:

* Cloud subscription that supports Azure RMS
  + E3/E4 subscriptions to Office 365
  + Azure RMS Standalone
  + Enterprise Mobility Suite
* Active Directory settings
  + AD functionality
  + Email address attribute populated for all users and groups
  + Microsoft Exchange schema extensions in place
  + Simple delegation schema extension in place (if used)
* Directory Synchronization
  + Directory Synchronization functioning properly
* Active Directory Federation Services
  + Active Directory Federation Services (if applicable) functioning properly
  + Web Application Proxy (if applicable) functioning properly
* Secure Private Key Storage (if applicable)
  + Thales Hardware Security Module (HSM) functioning properly
* Messaging components
  + Microsoft Exchange (if applicable) functioning properly
* Collaboration components
  + Microsoft SharePoint (if applicable) functioning properly
* File Server components
  + File Classification Infrastructure (if applicable) functioning properly
  + Work Folders (if applicable) functioning properly

This procedure requires Global Administrator privilege or equivalent in the tenant.

* + 1. Activating Azure RMS

*Note: repeat this section for each tenant where Azure RMS will be enabled.*

After the tasks identified in the previous sections have been completed, the Azure RMS service is ready to be activated.

Activating the Azure RMS service requires Global Administrator privileges when executing the process in the Office 365 admin center. The activation is performed by accessing the Office 365 admin center using a web browser, such as Internet Explorer.

To activate the Azure RMS service, open the Office 365 admin center with appropriate credentials, navigate to the Rights Management section, and select to activate the service. You will be asked to confirm the activation.

*Note: For detailed step by step procedures for activating Azure RMS, see the corresponding section of the**Step by Step Installation Procedures.*

* + 1. Verification Procedure

The following steps validate the correct functionality of this phase:

* **Validate that the Rights Management Status within the Office 365 console displays Active and that the Activate option is replaced with Deactivate.** 
  1. Configure Azure Rights Management Services and Templates

This section presents the activities to be executed after activating the Azure Rights Management Services service. Most of these activities will be done through the Windows Azure portal and using Windows PowerShell.

* + 1. Installing Windows PowerShell for Azure Rights Management

Some operations in Azure RMS can be configured using the Windows Azure administration portal. However, other operations can only be performed using Windows PowerShell. Each administrator that will administer the Azure RMS service should install Windows PowerShell and the associated administration modules to be ready to configure the RMS service.

To install the administration module, first verify that the client is running Windows Vista/Windows Server 2008 or later and has Windows PowerShell 2.0 or later installed. Also verify that Microsoft .NET Framework 4.0 or later and Microsoft Online Services Sign-In Assistant 7.0 or later is installed on the client computer. Then download and installed the Azure AD Rights Management Administration Tool from the Microsoft Download Center (<http://www.microsoft.com/en-us/download/details.aspx?id=30339>).

To begin to configure Azure RMS, start Windows PowerShell with the Run as administration option and enter the following command: Connect-AadrmService. Enter appropriate permissions and then you can begin to administer the Azure RMS serve. To see which commands are available enter the following command: Get-Command –Module aadrm.

* + 1. Delegate Permissions

After the Azure RMS service has been activated, you can grant administrative rights to Azure Rights Management within the organization. By default, all Office 365 global administrators can administer the Rights Management service. If you have to grant rights to another administrator within your organization, you can do so using Windows PowerShell.

To perform this task, confirm that you have downloaded and installed the Azure AD Windows PowerShell module. For more information about the Azure AD Windows PowerShell module, see the Installing Windows PowerShell for Azure Rights Management section of this document. From Windows PowerShell, run the Connect-MsolService command and the Get-MsolGroup command to look up the GUID of the security group you created to administer role-based administrative rights for Rights Management. Then run the Add-RoleBased Administrator command to add the desired group.

Repeat these steps for all users and groups that you wish to grant administrative rights to Azure Rights Management.

* + 1. Configuring Custom Rights Policy Templates

Azure RMS contains two default rights policy templates that are available to all end users in the tenant immediately upon the activation of the Azure RMS service. These rights policy templates are as follows:

* *Company* Confidential: This template grants permission to view and edit content to internal users and denies the right to copy or print.
* *Company* Confidential Read Only: This template grants permission to view content to internal users and denies the right to copy, edit, print, or save.

For many organizations, the default templates might be sufficient. However, some organizations may want to create custom rights policy templates to achieve specific organizational goals. After the Azure RMS service has been activated, it is useful to create a first group of Rights Policy Templates to allow for practical testing. The templates defined in this phase can be deleted later and should only be used for testing purposes.

* Create initial Rights Policy Templates for testing:
  + Create Azure Rights Management Services Templates
    - From the Azure Management Portal, navigate to the Rights Management section and create the templates as per the specification in the Design document.
  + Publish templates to users:
    - From the Azure Management Portal, after you have successfully created the rights policy template, click Publish to make the template visible for users.
  + Implement template deployment mechanisms:

*Modify this section according to your template deployment mechanisms.*

* + - In Office 365 rights policy templates are automatically refreshed and no additional steps are required.
    - In Office 2013 rights policy templates are automatically refreshed on a schedule. By default, rights policy templates are refreshed every 7 days. You can force a refresh sooner by using a registry key.
    - In Office 2010 rights policy templates are refreshed automatically upon user log on and no additional steps are required.
    1. Enabling Logging

Logging in Azure RMS enables you to view logs for every administrator action and request for protected content in near-real-time. Azure RMS can write log records for each transaction as part of the basic service. These logs can be made available to Customer Name, if Customer Name provides a Windows Azure storage account to store the logs. Customer Name can decide how much history of logs to pay for or they can move data into the on-premises environment.

To exercise the usage logging feature, the following prerequisites must be in place:

* A Windows Azure subscription.
* Windows PowerShell for rights management.

Once the prerequisites are in place, the following steps must be performed:

* **Set up a Windows Azure storage account**
  + Navigate to Storage section of the Windows Azure management portal and create a new storage account.
  + Make a note of the primary access key used for your Windows Azure storage account access
* **Configure the Storage Account**
  + Connect to Azure RMS service using Windows PowerShell and run the commands required to specify the Storage Account used with Azure RMS
* **Enabling Logging**
  + From Windows PowerShell, while connected to the Azure RMS service, run the command required to enable Azure RMS logging.

For more information on Azure logging, see [Logging and Analyzing Azure Rights Management Usage](http://technet.microsoft.com/en-us/library/dn529121.aspx).

* + 1. Verification Procedure

The following steps validate the correct functionality of this phase:

* **Validate rights policy templates**
  + Validate that users can see the newly created and published rights policy template after the refresh interval has passed or after a refresh has been forced.
* **Validate the Azure RMS Logging**
  + First create and consume protected RMS content to create entries in the log
  + Verify the availability of logs by logging in to the Azure management portal. Logging information should be available within 15 minutes of the activity
  1. Deploying Client Components
     1. Deploying Rights Management Services Client Installation Components
        1. Legacy and Windows Vista Clients

Windows Vista and earlier operating systems are not compatible with Azure RMS. Users with these operating systems will be unable to create and consume protected content using Azure RMS. To enable legacy users to use Azure RMS, upgrade the operating system to Windows 7 or later.

* + - 1. Windows 7 Clients

Although Windows 7 include all prerequisites for using RMS, a later client is available as the RMS Client 2.x and it must be installed unless it has already been automatically deployed through Microsoft Update.

* + - 1. Windows 8.1/Windows 8 Clients

The Windows 8.1 and Windows 8 operating systems do not include a version of the RMS Client. We recommend deploying the RMS Client 2.x to machines running on this operating system.

* + - 1. RMS Sharing Application

The RMS Sharing Application is an optional client-side application that extends support for Azure RMS to all file formats. It also enables additional client-side protection scenarios and is available on Windows, Windows RT, iOS, and Android devices.

The RMS Sharing Application is supported on Windows 8.1, Windows 8, and Windows 7 clients and the installation package includes the RMS Client 2.x.

* + 1. Installing RMS-Enabled Applications

*If your customer has already deployed the required versions of Office, you can delete this section.*

After installation of the identified prerequisites, installation of one of the following RMS-enabled applications is required:

* **Office Suites for Document Protection and Consumption**
  + Microsoft Office Professional Plus 2010/2013
* **Office Suites for Document Consumption Only**
  + Microsoft Office 2010/2013 Standard
  + Microsoft Office 2010/2013 Professional
  + Word and Excel document readers
* **Office Client RMS-enabled Applications**
  + Microsoft Office Word
  + Microsoft Office Excel
  + Microsoft Office PowerPoint
  + Microsoft Office Outlook
  + Microsoft Office InfoPath
* **Others – RMS-enabled Applications**
  + XPS viewer enables saving Office documents in XPS formats (through Print to XPS or Save As), and then assigning RMS permissions.
    1. Verification Procedure

The following steps validate the correct functionality of this phase for either internal or external users:

* Validate appropriate internal functionality protecting and consuming documents
* Validate that clients inherit Azure Rights Management Services Settings (templates configuration and others)
* Validate functionality for protecting and consuming content through Rights Policy Templates
* Validate RMA and XPS functionality as appropriate
  1. Deploying Azure Rights Management Services Trusts

Azure RMS trust relationships are implied with any other organization supported by Azure Active Directory, including users with Office 365 or using RMS for Individuals. Users can collaborate with external parties who have Azure Active Directory, without the need to configure a trust relationship.

Note that this trust relationship provides the ability to collaborate; it does not automatically grant external users access to protected content. External users must be explicitly mentioned in the permission policy.

* 1. Validating Azure Rights Management Services Functionality

This section presents the activities to be executed to validate Azure Rights Management Services functionality either in the intranet and extranet clients.

* + 1. Active Directory Rights Management Services Usage General Validation - Intranet Users

The following steps should be executed for the intranet usage test:

* Protect documents and emails by assigning permissions to users and mail-enabled groups.
* Protect documents and emails by assigning permissions using Rights Policy templates.
* Consume documents using Office RMS-aware applications and validate that Rights Policy template restrictions are as expected.
* Consume documents using the RMS App, using Outlook Web Access (OWA) (if available) and using a workstation without the Microsoft Office application installed.
* Protect XPS documents and emails by assigning permissions to users and mail-enabled groups.
* Protect XPS documents and emails by assigning permissions using Rights Policy templates.
* Consume XPS documents and validate that Rights Policy template restrictions are as expected.
* Validate that additional Azure Rights Management Services configuration settings have been successfully propagated to the clients.
  + 1. Active Directory Rights Management Services Usage General Validation - Extranet Users

The following steps should be executed for the extranet usage test. If required, repeat the following test in domain-joined and non-domain joined workstations.

* Validate configuration scripts you create include all of the appropriate settings before configuring the workstation to use RMS.
* Protect documents and emails by assigning permissions to users and mail-enabled groups.
* Protect documents and emails by assigning permissions using Rights Policy templates.
* Consume documents using Office RMS-aware applications and validate that the Rights Policy template restrictions are as expected.
* Consume documents using the RMS App, using Outlook Web Access (OWA) (if available) and using a workstation without the Microsoft Office application installed.
* Protect XPS documents and emails by assigning permissions to users and mail-enabled groups.
* Protect XPS documents and emails by assigning permissions using Rights Policy templates.
* Consume XPS documents and validate that the Rights Policy template restrictions are as expected.
* Validate that additional Active Directory Rights Management Services configuration settings have been successfully propagated to the clients.
  1. Integration with Server-side Applications

*Delete this section if server-side IRM integration capabilities will not be used in this environment. Otherwise, customize the sections for the functionality that will be enabled.*

Azure RMS can be integrated with the following Microsoft server-side applications:

* Microsoft Exchange Server 2013/2010
* Microsoft SharePoint Server 2013/2010
* File Classification Infrastructure and Work Folders in Windows Server 2012/2012 R2

This integration is provided through the RMS Connector, which is a small-footprint component, deployed on premises, that proxies the communication between the server-side applications and the Azure RMS service. In order to implement integration with these server-side applications, the following tasks need to be performed:

* Create a DNS alias for the RMS Connector, for example, rmsconnector.contoso.com
* Install the RMS Connector application on at least two computers in the organization to provide fault tolerance.
* Configure the RMS Connectors for load balancing and high availability using any IP-based load balancer technology.
* Authorize the Exchange/SharePoint/FCI servers to use the RMS Connector
* If desired, configure the RMS connector for a web proxy server. If your connector server is installed in a network that does not have direct Internet connectivity and requires manual configuration of a web proxy server for outbound Internet access, you must configure the registry on the server for the RMS connector.
* Configure the on-premises servers to use the connector by manually editing the registry or automating the process using the server configuration tool for the Microsoft RMS connector.
  1. Integration with Microsoft Exchange 2013

*Delete this section if Exchange 2013 IRM capabilities will not be used in this environment. Otherwise, customize the sections for the functionality that will be enabled.*

Azure RMS will be integrated with Microsoft Exchange 2013 to provide enhanced functionality to users and administrator. The following steps need to be followed to implement such integration.

In order to enable IRM functionality in Exchange 2013, the following tasks need to be performed:

* Install the RMS Client on the Exchange Server machines
* Authorize the Exchange servers in the RMS Connector Administration Tool
* Configure the Exchange servers to use the RMS Connector by either running the server configuration tool for the Microsoft RMS Connector or performing manual registry edits.
* Enable IRM support in OWA for the Exchange servers by running the following Windows PowerShell commands:

1. Set-OWAMailboxPolicy –Identity Default -IRMEnabled $true
2. Set-IRMConfiguration -OWAEnabled $true
3. Set-IRMConfiguration -SearchEnabled $true

* Data Loss Prevention policies can be integrated with Azure RMS in the Exchange Control Panel
* Transport Protection Rules don’t need to be enabled; they can be created in the Exchange Control Panel or directly through the following PowerShell command:

*Customize this sample command line as needed.*

1. New-TransportRule -Name "Secure Communication between Sales and Finance"
2. -BetweenMemberOf1 Sales@Woodgrovebank.com
3. -BetweenMemberOf2 financial@Woodgrovebank.com
4. -ApplyRightsProtectionTemplate "Woodgrove Bank - Confidential"
5. -ExceptIfSubjectContainsWords "DNP"

For information on enabling other IRM functionality in Exchange 2013, see:

[Understanding Journal Report Decryption](http://technet.microsoft.com/en-us/library/dd876936(v=exchg.150).aspx)

[Understanding Transport Decryption](http://technet.microsoft.com/en-us/library/dd638122(v=exchg.150).aspx)

[Understanding Outlook Protection Rules](http://technet.microsoft.com/en-us/library/dd638178(v=exchg.150).aspx)

* 1. Integration with Microsoft Exchange 2010

*Delete this section if Exchange 2010 IRM capabilities will not be used in this environment. Otherwise, customize the sections for the functionality that will be enabled.*

Azure RMS will be integrated with Microsoft Exchange 2010 to provide enhanced functionality to users and administrator. The following steps need to be followed to implement such integration.

In order to enable IRM functionality in Exchange 2010, the following tasks need to be performed:

* Install the RMS Client on the Exchange Server machines
* Authorize the Exchange servers in the RMS Connector Administration Tool
* Configure the Exchange servers to use the RMS Connector by either running the server configuration tool for the Microsoft RMS Connector or performing manual registry edits.
* Enable Exchange Prelicensing on the server by running the following command:

Set-IRMConfiguration –InternalLicensingEnabled $true

This is required for all other IRM integration in Exchange as well.

* Enable IRM support in OWA for the Exchange servers by running the following Windows PowerShell commands:

1. Set-OWAMailboxPolicy –Identity Default -IRMEnabled $true
2. Set-IRMConfiguration -OWAEnabled $true
3. Set-IRMConfiguration -SearchEnabled $true

* Transport Protection Rules don’t need to be enabled, they can be created directly through the following PowerShell command:

*Customize this sample command line as needed.*

1. New-TransportRule -Name "Secure Communication between Sales and Finance"
2. -BetweenMemberOf1 Sales@Woodgrovebank.com
3. -BetweenMemberOf2 financial@Woodgrovebank.com
4. -ApplyRightsProtectionTemplate "Woodgrove Bank - Confidential"
5. -ExceptIfSubjectContainsWords "DNP"

For information on enabling other IRM functionality in Exchange 2010, see:

[Understanding Journal Report Decryption](http://technet.microsoft.com/en-us/library/dd876936(EXCHG.140).aspx?v=14.0.639.21&t=exchgf1)

[Understanding Transport Decryption](http://technet.microsoft.com/en-us/library/dd638122.aspx)

[Understanding Outlook Protection Rules](http://technet.microsoft.com/en-us/library/dd638178.aspx)

* 1. Integration with Exchange Online / Office 365

Integration with Exchange Online offers similar capabilities as for on-premises Exchange 2013, but there’s the prerequisite to enable cross-premises IRM integration by exporting a TPD between the on-premises RMS cluster to be used for RMS licensing and the Exchange Online service.

The following steps must be followed to perform this key exchange:

1. Open Windows PowerShell.
2. Type the following command in Windows PowerShell and press Enter: $LiveCred = Get-Credential
3. Type the following command in Windows PowerShell and press Enter: $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri <https://ps.outlook.com/powershell/> -Credential $LiveCred -Authentication Basic –AllowRedirection
4. Type the following command in Windows PowerShell and press Enter: Import-PSSession $Session
5. Type the following command in Windows PowerShell and press Enter: Set-IRMConfiguration –RMSOnlineKeySharingLocation https://sp-rms.na.aadrm.com/TenantManagement/ServicePartner.svc"
6. Type the following command in Windows PowerShell and press Enter: Import-RMSTrustedPublishingDomain -RMSOnline -name "RMS Online”
7. Type the following command in Windows PowerShell and press Enter: Set-IRMConfiguration -InternalLicensingEnabled $true

After these steps, you can enable the IRM functionality by using the same mechanisms as in an on-premises Exchange 2013 server such as those listed above.

* 1. Integration with SharePoint Server

*Delete this section if SharePoint IRM capabilities will not be used in this environment. Otherwise, customize the sections for the functionality that will be enabled.*

Azure RMS will be integrated with Microsoft SharePoint Server to provide enhanced functionality to users and administrator. The following steps need to be followed to implement such integration.

In order to enable IRM functionality in SharePoint, the following tasks need to be performed:

* Install the RMS Client on the SharePoint Server machines
* Authorize the SharePoint servers in the RMS Connector Administration Tool
* Configure the SharePoint servers to use the RMS Connector by either running the server configuration tool for the Microsoft RMS Connector or performing manual registry edits.
* Use the Central Administration console to configure SharePoint to use the Azure RMS server specified in Active Directory. Registry settings will route this to the RMS Connector
* Enable IRM in the individual document libraries using the Document Library Settings page.
  1. Integration with SharePoint Online

*Delete this section if SharePoint Online IRM capabilities will not be used in this environment. Otherwise, customize the sections for the functionality that will be enabled.*

Azure RMS will be integrated with SharePoint Online to provide enhanced functionality to users and administrator. The following steps need to be followed to implement such integration.

In order to enable IRM functionality in SharePoint Online, the following tasks need to be performed:

* Use the SharePoint admin center to configure SharePoint Online to use the Azure RMS service specified in the configuration.
* Enable IRM in the individual document libraries using the Document Library Settings page.
  1. Integration with File Classification Infrastructure and Work Folders

*Delete this section if FCI IRM capabilities will not be used in this environment. Otherwise, customize the sections for the functionality that will be enabled.*

Azure will be integrated with File Classification Infrastructure to provide enhanced functionality to users and administrator. The following steps need to be followed to implement such integration.

In order to enable IRM functionality in FCI, the following tasks need to be performed:

* Install the RMS Client on the FCI machines
* Authorize the FCI servers in the RMS Connector Administration Tool
* Configure the FCI servers to use the RMS Connector by either running the server configuration tool for the Microsoft RMS Connector or performing manual registry edits.
* Create the Classification Properties, Classification Rules, and File Management tasks in the File Server Resource Manager console that will be used to discover and protect sensitive information.
* Repeat these steps for each FCI serer that will use the RMS Connector.

In order to enable IRM functionality with Work Folders, the following tasks need to be performed:

* Install Work Folders on file servers
* Create security groups for Work Folders
* Create sync shares for user data
* If using multiple file servers, perform the following additional tasks need to be performed:
  + Obtain SSL certificates to protect the URL published by Work Folders
  + Create DNS records to allow users to sync across the Internet
  + Bind the SSL certificate on the sync servers